## **Zowe Version 1.25 Documentation**



## Table of contents:

- Zowe overview
- Zowe overview
  - Zowe demo video
  - Component overview
    - Zowe Application Framework
    - API Mediation Layer
    - Zowe CLI
    - Zowe Explorer
    - Zowe Client Software Development Kits (SDKs)
    - Zowe Launcher
    - Zowe Mobile Incubator
    - ZEBRA (Zowe Embedded Browser for RMF/SMF and APIs) Incubator
    - Zowe Workflow wiZard Incubator
  - Zowe Third-Party Software Requirements and Bill of Materials
- Zowe architecture
- Zowe architecture
  - Zowe architecture with high availability enablement on Sysplex
  - Zowe architecture when running in Kubernetes cluster
  - Zowe architecture when using Docker image
  - App Server
  - ZSS
  - API Gateway
  - API Catalog
  - API Discovery
  - Caching service
  - Caching service
  - MVS, JES, and USS UI
    - File API and JES API
  - Cross memory server
- Frequently Asked Questions
- Frequently Asked Questions
  - Zowe FAQ
    - What is Zowe?
    - Who is the target audience for using Zowe?
    - What language is Zowe written in?

- What is the licensing for Zowe?
- Why is Zowe licensed using EPL2.0?
- What are some examples of how Zowe technology might be used by z/OS products and applications?
- What is the best way to get started with Zowe?
- What are the prerequisites for Zowe?
- What's the difference between using Zowe with or without Docker?
- Is the Zowe CLI packaged within the Zowe Docker download?
- Does ZOWE support z/OS ZIIP processors?
- How is access security managed on z/OS?
- How is access to the Zowe open source managed?
- How do I get involved in the open source development?
- When will Zowe be completed?
- Can I try Zowe without a z/OS instance?
- Zowe CLI FAQ
  - Why might I use Zowe CLI versus a traditional ISPF interface to perform mainframe tasks?
  - With what tools is Zowe CLI compatible?
  - Where can I use the CLI?
  - Which method should I use to install Zowe CLI?
  - How can I get help with using Zowe CLI?
  - How can I use Zowe CLI to automate mainframe actions?
  - How can I contribute to Zowe CLI?
- Zowe Explorer FAQ
  - Why might I use Zowe Explorer versus a traditional ISPF interface to perform mainframe tasks?
  - How can I get started with Zowe Explorer?
  - Where can I use Zowe Explorer?
  - How do I get help with using Zowe Explorer?
  - How can I use Secure Credential Store with Zowe Explorer?
  - How can I use FTP as my back-end service for Zowe Explorer?
  - How can I contribute to Zowe Explorer?
- Version 1.25 (October 2021)
- Version 1.25 (October 2021)
  - Notable changes
  - New features and enhancements
    - Zowe installation and packaging
    - Zowe API Mediation Layer
    - Zowe Application Framework
    - Zowe CLI

- Zowe Explorer
- Zowe JES/MVS/USS Explorers
- Bug fixes
  - Zowe API Mediation Layer
  - Zowe Application Framework
  - Zowe CLI
  - Zowe Explorer
- Version 1.24 (September 2021)
- Version 1.24 (September 2021)
  - New features and enhancements
    - Zowe installation and configuration
    - Zowe API Mediation Layer
    - Zowe App Server
    - Zowe CLI
    - Zowe Explorer
  - Bug fixes
    - Zowe installation and configuration
    - Zowe API Mediation Layer
    - Zowe App Server
    - Zowe CLI
    - Zowe Explorer
  - Known Issues
- Version 1.23 (July 2021)
- Version 1.23 (July 2021)
  - New features and enhancements
    - Zowe API Mediation Layer
    - Zowe App Server
    - Zowe CLI
    - Zowe Explorer
  - Bug fixes
    - Zowe API Mediation Layer
    - Zowe App Server
    - Zowe CLI
    - Zowe Explorer
- Previous versions
- Previous versions
  - Version 1.22.0 LTS (June 2021)
    - Notable changes

- New features and enhancements
- Bug fixes
- Version 1.21.0 LTS (April 2021)
  - New features and enhancements
  - Bug fixes
- Version 1.20.1 LTS (March 2021)
  - Bug fixes
- Version 1.20.0 LTS (March 2021)
  - New features and enhancements
  - Bug Fixes
- Version 1.19.1 LTS (February 2021)
  - Notable changes
  - New features and enhancements
  - Bug fixes
- Version 1.19.0 LTS (February 2021)
  - Notable changes
  - New features and enhancements
  - Bug Fixes
- Version 1.18.0 LTS (January 2021)
  - Notable changes
  - New features and enhancements
  - Bug Fixes
- Version 1.17.0 LTS (November 2020)
  - Notable changes
  - New features and enhancements
  - Bug fixes
- Version 1.16.0 LTS (October 2020)
  - Notable changes
  - New features and enhancements
  - Bug fixes
  - Zowe Explorer
- Version 1.15.0 LTS (September 2020)
  - Notable changes
  - New features and enhancements
  - Bug fixes
- Version 1.14.0 LTS (August 2020)
  - Notable changes
  - New features and enhancements

- Bug fixes
- Version 1.13.0 LTS (July 2020)
  - Notable changes
  - New features and enhancements
  - Bug fixes
- Version 1.12.0 LTS (June 2020)
  - New features and enhancements
  - Bug fixes
- Version 1.11.0 LTS (May 2020)
  - New features and enhancements
  - Bug fixes
- Version 1.10.0 LTS (April 2020)
  - New features and enhancements
  - Bug fixes
- Version 1.9.0 LTS (February 2020)
  - New features and enhancements
  - Bug fixes
- Version 1.8.1 (February 2020)
  - Bug fixes for Zowe CLI
- Version 1.8.0 (February 2020)
  - New features and enhancements
  - Bug fixes
- Version 1.7.1 (December 2019)
  - New features and enhancements
  - Bug fixes
- Version 1.7.0 (November 2019)
  - New features and enhancements
  - Bug fixes
- Version 1.6.0 (October 2019)
  - What's new in the Zowe App Server
  - What's new in Zowe CLI
  - What's new in the Visual Studio Code (VSC) Extension for Zowe
- Version 1.5.0 (September 2019)
  - What's new in API Mediation Layer
  - What's new in the Zowe App Server
  - What's new in Zowe CLI and Plug-ins
- Zowe SMP/E Alpha (August 2019)
- Version 1.4.0 (August 2019)

- What's new in API Mediation Layer
- What's new in the Zowe App Server
- What's new in Zowe CLI and Plug-ins
- Version 1.3.0 (June 2019)
  - What's new in API Mediation Layer
  - What's new in the Zowe App Server
  - What's new in Zowe CLI and Plug-ins
- Version 1.2.0 (May 2019)
  - What's new in the Zowe installer
  - What's new in API Mediation Layer
  - What's new in the Zowe App Server
  - What's new in Zowe CLI and Plug-ins
  - What's new in Zowe USS API
- Version 1.1.0 (April 2019)
  - What's new in Zowe system requirements
  - What's new in the Zowe App Server
  - What's new in the Zowe CLI and Plug-ins
  - What's new in API Mediation Layer
- Version 1.0.1 (March 2019)
  - What's new in Zowe installation on z/OS
  - What's new in the Zowe App Server
  - What's new in Zowe CLI
  - What's new in the Zowe REST APIs
  - What's changed
- Version 1.0.0 (February 2019)
  - What's new in API Mediation Layer
  - What's new in Zowe CLI
  - What's new in the Zowe Desktop
  - What's new in the Zowe App Server
  - What's changed
  - Known issues
- Getting started with Zowe
- Getting started with Zowe
  - Learning about Zowe
  - Install and use
    - Zowe versions for use with other products and plugins
  - Getting involved
- Zowe CLI quick start

- Zowe CLI quick start
  - Installing
    - Software Requirements
    - Installing Zowe CLI core from public npm
    - Installing CLI plug-ins
  - Issuing your first commands
    - Listing all data sets under a high-level qualifier (HLQ)
    - Downloading a partitioned data-set (PDS) member to local file
  - Using profiles
    - Profile types
    - Creating a zosmf profile
    - Using a zosmf profile
  - Writing scripts
    - Example:
  - Next Steps
- Information roadmap for Zowe API Mediation Layer
- Information roadmap for Zowe API Mediation Layer
  - Fundamentals
  - Installing
  - Configuring and updating
  - Using Zowe API Mediation Layer
  - Onboarding APIs
  - Security
  - Contributing to Zowe API Mediation Layer
  - Troubleshooting and support
  - Community resources
- Information roadmap for Zowe Application Framework
- Information roadmap for Zowe Application Framework
  - Fundamentals
  - Installing
  - Configuring and updating
  - Using Zowe Application Framework
  - Developing Zowe Desktop plug-ins
    - Samples
  - Contributing to Zowe Application Framework
  - Troubleshooting and support
  - Community resources
- Information roadmap for Zowe CLI

- Information roadmap for Zowe CLI
  - Fundamentals
  - Quick start
  - Installing
  - Configuring and updating
  - Using Zowe CLI and plug-ins
  - Developing a Zowe CLI plug-in
  - Contributing to Zowe CLI
  - Troubleshooting and support
  - Community resources
- Information Roadmap for Zowe Explorer
- Information Roadmap for Zowe Explorer
  - Fundamentals
  - Installing and configuring
  - Using Zowe Explorer
  - Extending Zowe Explorer
  - Contributing to Zowe Explorer
  - Troubleshooting and support
  - Community resources
- Information roadmap for Zowe Client SDKs
- Information roadmap for Zowe Client SDKs
  - Fundamentals
  - Installing
  - Using Zowe Client SDKs
    - Zowe Node.js SDK
    - Zowe Python SDK
  - Contributing to Zowe Client SDKs
  - Troubleshooting and support
  - Community resources
- Information roadmap for Zowe Mobile
- Information roadmap for Zowe Mobile
  - Fundamentals
  - Installing
  - Community resources
- Zowe learning resources
- Zowe learning resources
  - Blogs
  - Videos

- Webinars
- Community
- Training
- Overview
- Overview
- Installation roadmap
- Installation roadmap
  - Stage 1: Plan and prepare
  - Stage 2: Install the Zowe z/OS runtime
  - Stage 3: Configure the Zowe z/OS runtime
  - Stage 4: Verify the installation
  - Looking for troubleshooting help?
- Planning the installation
- Planning the installation
  - Topology of the Zowe z/OS launch process
    - RUNTIME\_DIR
    - INSTANCE\_DIR
    - KEYSTORE\_DIRECTORY
- UNIX System Services considerations for Zowe
- UNIX System Services considerations for Zowe
  - What is USS?
  - Setting up USS for the first time
  - Language environment
  - OMVS segment
  - Address space region size
- System requirements
- System requirements
  - z/OS system requirements
    - z/OS
    - Node.js
    - Java
    - z/OSMF (Optional)
  - User ID requirements
    - ZWESVUSR
    - ZWESIUSR
    - ZWEADMIN
    - zowe\_user
  - Network requirements

- Zowe Docker requirements
- Zowe Desktop requirements (client PC)
- Feature requirements
  - Multi-Factor Authentication (MFA)
  - Single Sign-On (SSO)
- Installing Node.js on z/OS
- Installing Node.js on z/OS
  - Supported Node.js versions
  - How to obtain IBM SDK for Node.js z/OS
  - Hardware and software prerequisites
  - Installing the PAX edition of Node.js z/OS
  - Installing the SMP/E edition of Node.js z/OS
- Configuring z/OSMF
- Configuring z/OSMF
  - z/OS requirements for z/OSMF configuration
  - Configuring z/OSMF
  - z/OSMF REST services for the Zowe CLI
- Configuring z/OSMF Lite (for non-production use)
- Configuring z/OSMF Lite (for non-production use)
  - Introduction
  - Assumptions
  - Software Requirements
    - Minimum Java level
    - WebSphere® Liberty profile (z/OSMF V2R3 and later)
    - System settings
    - Web browser
  - Creating a z/OSMF nucleus on your system
    - Running job IZUNUSEC to create security
    - Running job IZUMKFS to create the z/OSMF user file system
    - Copying the IBM procedures into JES PROCLIB
    - Starting the z/OSMF server
    - Accessing the z/OSMF Welcome page
    - Mounting the z/OSMF user file system at IPL time
  - Adding the required REST services
    - Enabling the z/OSMF JOB REST services
    - Enabling the TSO REST services
    - Enabling the z/OSMF data set and file REST services
    - Enabling the z/OSMF Workflow REST services and Workflows task UI

- Troubleshooting problems
  - Common problems and scenarios
  - Tools and techniques for troubleshooting
- Appendix A. Creating an IZUPRMxx parmlib member
- Appendix B. Modifying IZUSVR1 settings
- Appendix C. Adding more users to z/OSMF
  - Before you Begin
  - Procedure
  - Results
- Installing Zowe runtime from a convenience build
- Installing Zowe runtime from a convenience build
  - Obtaining and preparing the convenience build
  - Installing the Zowe runtime
    - Step 1: Locate the install directory
    - Step 2: Choose a runtime USS folder
    - Step 3: Choose a dataset HLQ for the SAMPLIB and LOADLIB
    - Step 4 (Method 1): Install the Zowe runtime using shell script
    - Step 4 (Method 2): Install the Zowe runtime using z/OSMF Workflow
  - Next steps
- Installing Zowe SMP/E
- Installing Zowe SMP/E
  - Introduction
    - Zowe description
    - Zowe FMIDs
  - Program materials
    - Basic machine-readable material
    - Program source materials
    - Publications useful during installation
  - Program support
    - Statement of support procedures
  - Program and service level information
    - Program level information
    - Service level information
  - Installation requirements and considerations
    - Driving system requirements
    - Target system requirements
    - FMIDs deleted
  - Installation instructions

- SMP/E considerations for installing Zowe
- SMP/E options subentry values
- Overview of the installation steps
- Download the Zowe SMP/E package
- Allocate file system to hold the download package
- Upload the download package to the host
- Extract and expand the compressed SMPMCS and RELFILEs
- Sample installation jobs
- Create SMP/E environment (Optional)
- Perform SMP/E RECEIVE
- Allocate SMP/E target and distributions libraries
- Allocate, create and mount ZSF files (Optional)
- Allocate z/OS UNIX paths
- Create DDDEF entries
- Perform SMP/E APPLY
- Perform SMP/E ACCEPT
- Run REPORT CROSSZONE
- Cleaning up obsolete data sets, paths, and DDDEFs
- Activating Zowe
  - File system execution
- Zowe customization
- Installing Zowe SMP/E build with z/OSMF workflow
- Installing Zowe SMP/E build with z/OSMF workflow
  - Activating Zowe
    - File system execution
  - Zowe customization
- Docker Installation Roadmap (Technical Preview)
- Docker Installation Roadmap (Technical Preview)
  - Stage 1: Plan and prepare
  - Stage 2: Install the Zowe runtime on z/OS
  - Stage 3: Configure the Zowe z/OS runtime
  - Stage 4: Verify the installation
  - Stage 5: Install Docker image
  - Stage 6: Configure Docker container
  - Looking for troubleshooting help?
- Installing Zowe runtime Docker Image (Technical Preview)
- Installing Zowe runtime Docker Image (Technical Preview)
  - Installing via Docker Hub

- Installing via direct download
  - Loading an image from .tar file
- Confirming the installation
- Upgrading
- Verifying authenticity using Docker signing
- Configuring Zowe runtime Docker Container (Technical Preview)
- Configuring Zowe runtime Docker Container (Technical Preview)
  - Working with Docker mounts
  - Quick start for the Zowe runtime in Docker
    - Customizing Zowe container start script
    - Using an instance directory external to the Zowe container
    - Using external certificates
    - Starting the container
  - Using Zowe-based products, plugins and apps
  - Zowe's docker mount locations
- Configuring the z/OS system for Zowe
- Configuring the z/OS system for Zowe
  - Grant users permission to access z/OSMF
  - Configure an ICSF cryptographic services environment
  - Configure security environment switching
  - Configure address space job naming
  - Configure multi-user address space (for TSS only)
  - User IDs and groups for the Zowe started tasks
  - Configure ZWESVSTC to run under ZWESVUSR user ID
  - Configure ZWESLSTC to run Zowe high availability instances under ZWESVUSR user ID
  - Configure the cross memory server for SAF
  - Configure main Zowe server to use identity mapping
    - Using RACF
    - Using ACF2
    - Using TSS
- Configuring Zowe certificates
- Configuring Zowe certificates
  - Northbound Certificate
  - Southbound Certificate
  - Trust store
  - Certificates in the Zowe architecture
  - Keystore versus key ring
  - Keystore directory creation

- Configuring Zowe certificates in UNIX files
- Configuring Zowe certificates in UNIX files
  - Generate a certificate with default values
  - Generate a certificate with custom values
  - Configure zowe-setup-certificates.env to use existing certificates
  - Using web tokens for SSO on ZLUX and ZSS
    - Customizing the ZWESSOTK JCL
    - Enabling SSO
  - Hints and tips
- Configuring Zowe certificates in a key ring
- Configuring Zowe certificates in a key ring
  - Customizing the ZWEKRING JCL
    - PRODUCT variable
    - HOSTNAME and IPADDRESS
    - ZOWERING and LABEL labels
    - ROOTZFCA label
  - Results
  - Cleanup
- Installing and configuring the Zowe cross memory server (ZWESISTC)
- Installing and configuring the Zowe cross memory server (ZWESISTC)
  - PDS sample library and PDSE load library
  - Load module
    - APF authorize
    - Key 4 non-swappable
  - PARMLIB
  - PROCLIB
  - SAF configuration
  - Summary of cross memory server installation
  - Starting and stopping the cross memory server on z/OS
  - Zowe auxiliary service
    - When to configure the auxiliary service
    - Installing the auxiliary service
- Creating and configuring the Zowe instance directory
- Creating and configuring the Zowe instance directory
  - Introduction
  - Prerequisites
  - Creating an instance directory
  - Updating the instance.env configuration file

- Zowe prerequisites
- Domain, Hostname and IP Address
- Component groups
- Keystore configuration
- Address space names
- Ports
- API Mediation Layer configuration
- Cross memory server
- Extensions
- Updating the zowe.yaml configuration file
  - Known limitations for Zowe high availability
  - Creating the zowe.yaml file
  - High level overview of YAML configuration file
  - Extract sharable configuration out of zowe.yaml
  - Configuration override
  - YAML configurations certificate
  - YAML configurations zowe
  - YAML configurations java
  - YAML configurations node
  - YAML configurations zOSMF
  - YAML configurations components
  - YAML configurations halnstances
- Hints and tips
- Installing and starting the Zowe started task (ZWESVSTC)
- Installing and starting the Zowe started task (ZWESVSTC)
  - Step 1: Copy the PROCLIB member ZWESVSTC
  - Step 2: Configure ZWESVSTC to run under the correct user ID
  - Step 3: Launch the ZWESVSTC started task
    - Option 1: Starting Zowe from a USS shell
    - Option 2: Starting Zowe with the z/OS START command
- Start API Mediation Layer as a standalone component
- Start API Mediation Layer as a standalone component
- Zowe Auxiliary Address space
- Zowe Auxiliary Address space
- Configure Zowe with z/OSMF Workflows
- Configure Zowe with z/OSMF Workflows
  - Configure z/OS Security Manager
  - Configure Zowe certificates

- Configure Zowe Cross Memory Server
- Create and configure the Zowe instance directory and start the Zowe started task
- Register and execute workflow in the z/OSMF web interface
- Zowe high availability installation roadmap
- Zowe high availability installation roadmap
  - Stage 1: Plan and prepare
  - Stage 2: Install the Zowe runtime
  - Stage 3: Configure the Zowe high availability runtime
  - Stage 4: Verify the installation
  - Looking for troubleshooting help?
- Configuring Sysplex for high availability
- Configuring Sysplex for high availability
  - Sysplex environment requirements
  - Configuring Sysplex Distributor
- Configuring z/OSMF for high availability in Sysplex
- Configuring z/OSMF for high availability in Sysplex
  - Sysplex environment requirements
  - Setting up z/OSMF nucleus
    - Requirements of z/OSMF HA parmlib member in Sysplex
  - Configuring z/OSMF for high availability
- Configuring the Caching Service for HA
- Configuring the Caching Service for HA
  - Creating a VSAM data set
- Installing and starting the Zowe high availability started task (ZWESLSTC)
- Installing and starting the Zowe high availability started task (ZWESLSTC)
  - Step 1: Copy the PROCLIB member ZWESLSTC
  - Step 2: Configure ZWESLSTC to run under the correct user ID
  - Step 3: Launch the ZWESLSTC started task
    - Before you begin
    - Procedure
    - Next steps
- Verifying Zowe installation on z/OS
- Verifying Zowe installation on z/OS
  - Verifying Zowe Application Framework installation
  - Verifying API Mediation installation
  - Verifying z/OS Services installation
- Stopping the Zowe server components started task
- Stopping the Zowe server components started task

- Stopping the ZWESVSTC started task
- Stopping the ZWESLSTC started task
- Upgrading the z/OS system for Zowe
- Upgrading the z/OS system for Zowe
  - Upgrading the instance directory
    - Important note for users upgrading to v1.14
  - Updating the PROCLIB members
  - Updating the cross memory server load modules
  - Updating the system and security configuration
  - Upgrading the keystore directory
  - Service disruption during upgrades
    - Zowe extensions
- Uninstalling Zowe from z/OS
- Uninstalling Zowe from z/OS
- Introduction
- Introduction
  - Known limitations
- Prerequisites
- Prerequisites
  - Kubernetes cluster
  - kubectl tool
- Downloading and installing
- Downloading and installing
  - Downloading
    - Downloading configuration samples
    - Downloading container images
  - Installing
- Configuring
- Configuring
  - 1. Create namespace and service account
  - 2. Create Persistent Volume Claim (PVC)
  - 3. Create and modify ConfigMaps and Secrets
  - 4. Expose API Mediation Layer components
    - 4a. Create service
    - 4b. Port forwarding (minikube)
    - 4c. Create Ingress (Bare-metal)
    - 4d. Create Route (OpenShift)
  - Customizing or manually creating ConfigMaps and Secrets

- Starting, stopping, and monitoring
- Starting, stopping, and monitoring
  - Starting Zowe containers
  - Monitoring Zowe containers
    - Monitoring Zowe containers via UI
    - Monitoring Zowe containers via CLI
  - Stopping, pausing, or removing Zowe containers
- System requirements
- System requirements
  - Client-side
  - Host-side
  - Free disk space
- Installing the ssh2 Package for Zowe CLI
- Installing the ssh2 Package for Zowe CLI
  - Windows
  - Unix
  - MacOS
- Installing Zowe CLI
- Installing Zowe CLI
  - Methods to install Zowe CLI
    - Installing Zowe CLI from a local package
    - Installing Zowe CLI from an online registry
- Install CLI from Online Registry Via Proxy
- Install CLI from Online Registry Via Proxy
- Updating Zowe CLI
- Updating Zowe CLI
  - Migrating to Long-term Support (LTS) version
  - Identify the currently installed version of Zowe CLI
  - Identify the currently installed versions of Zowe CLI plug-ins
  - Update Zowe CLI from the online registry
  - Update or revert Zowe CLI to a specific version
  - Update Zowe CLI from a local package
- Uninstalling Zowe CLI
- Uninstalling Zowe CLI
- Zowe CLI Development Roadmap (Technical Preview)
- Zowe CLI Development Roadmap (Technical Preview)
- Install the Zowe CLI @next version
- Install the Zowe CLI @next version

- Install Zowe CLI from npm
- Install Zowe CLI from a download
- Using Daemon Mode (Technical Preview)
- Using Daemon Mode (Technical Preview)
  - Feature overview
  - Install the zowex native executable
  - Starting Zowe in daemon mode
- Using Global Profile Configuration (Technical Preview)
- Using Global Profile Configuration (Technical Preview)
  - Feature overview
    - Benefits
    - Changes to secure credential storage
  - Initializing global configuration
  - Initializing user-specific configuration (Optional)
  - Editing global configuration
  - Managing credential security
  - Tips for efficient configuration
    - Command option order of precedence
    - Tips for using the base profile
  - Sharing global configuration
  - Example configurations
- Installing Zowe Explorer
- Installing Zowe Explorer
  - Software Requirements
  - Installing
  - Configuration
  - Relevant Information
- Zowe Explorer Profiles
- Zowe Explorer Profiles
  - Working with Zowe Explorer profiles
    - Associate Profile
  - Enabling Secure Credential Store with Zowe Explorer
    - For Zowe CLI users
  - Use Base Profile and Token with Existing Profiles
    - Access services through API ML with SSO
    - Log in to the Authentication Service
- Configuring Zowe Application Framework
- Configuring Zowe Application Framework

- Configuring the framework as a Mediation Layer client
  - Enabling the Application Server to register with the Mediation Layer
  - Accessing the Application Server
- Setting up terminal application plug-ins
  - Setting up the TN3270 mainframe terminal application plug-in
  - Setting up the VT Terminal application plug-in
- Configuration file
- Network configuration
  - HTTP
  - HTTPS
  - Network example
- Configuration Directories
  - Directories example
  - Old defaults
- Application plug-in configuration
  - Plug-ins directory example
- Logging configuration
- ZSS configuration
  - Connecting App Server to ZSS
  - Configuring ZSS for HTTPS
  - Installing additional ZSS instances
  - Configuring AT-TLS on Client System
- Controlling access to applications
  - Controlling application access for all users
  - Controlling application access for individual users
- Controlling access to dataservices
  - Defining the RACF ZOWE class
  - Enabling RBAC
  - Creating authorization profiles
  - Creating generic authorization profiles
  - Configuring basic authorization
  - Endpoint URL length limitations
- Multi-factor authentication configuration
  - Session duration and expiration
  - Configuration
- Enabling tracing
  - Zowe Application Server tracing
  - Log levels

- Enabling tracing for ZSS
- Zowe Application Framework logging
  - Controlling the logging location
  - Retaining logs
- Administering the servers and plugins using an API
- Configuring Zowe CLI
- Configuring Zowe CLI
  - Setting CLI log levels
  - Setting the CLI home directory
- Configuring the Zowe APIs
- Configuring the Zowe APIs
- Advanced Gateway features configuration
- Advanced Gateway features configuration
  - Prefer IP Address for API Layer services
  - SAF as an Authentication provider
  - Enable Jwt token refresh endpoint
    - Change password with SAF provider
  - Gateway retry policy
  - Gateway client certificate authentication
  - Gateway timeouts
  - CORS handling
  - Encoded slashes
  - Connection limits
  - Routed instance header
  - Distributed load balancer cache
  - Replace or remove the Catalog with another service
  - API Mediation Layer as a standalone component
  - SAF Resource Checking
    - Checking providers
- API Gateway configuration parameters
- API Gateway configuration parameters
  - Runtime configuration
    - Environment variables
  - Service configuration
  - Zuul configuration
  - Hystrix configuration
  - AT-TLS
- Getting started tutorial

- Getting started tutorial
  - Learning objectives
  - Estimated time
  - Prerequisites and assumptions
  - Logging in to the Zowe Desktop
  - Querying JES jobs and viewing related status in JES Explorer
  - Using the 3270 Terminal in the Zowe Desktop to view the job
  - Editing a data set in MVS Explorer
  - Using the Zowe CLI to edit a data set
  - Viewing the data set changes in MVS Explorer
  - Next steps
    - Go deeper with Zowe
    - Try the Extending Zowe scenarios
    - Give feedback
- Using the Zowe Desktop
- Using the Zowe Desktop
  - Navigating the Zowe Desktop
    - Accessing the Zowe Desktop
    - Logging in and out of the Zowe Desktop
    - Changing user password
    - Updating an expired password
    - Pinning applications to the task bar
    - Personalizing the Desktop
    - Changing the desktop language
  - Zowe Desktop application plug-ins
    - Hello World Sample
    - IFrame Sample
    - z/OS Subsystems
    - 3270 Terminal
    - VT Terminal
    - API Catalog
    - Editor
    - Workflows
    - JES Explorer
    - MVS Explorer
    - USS Explorer
  - Using the Workflows application plug-in
    - Logging on to the system

- Updating the data display
- Configuration
- Adding a z/OSMF server
- Testing a server connection
- Setting a server as the default z/OSMF server
- Removing a server
- Reload a server configuration
- Save a server configuration
- Workflows
- Searching workflows
- Defining a workflow
- Viewing tasks
- Task work area
- Performing a task
- Checking a task
- Managing tasks
- Viewing warnings
- Using the Editor
- Using the Editor
  - Specifying a highlighting language
  - Open a dataset
  - Deleting a file or folder
  - Opening a directory
  - Creating a new directory
  - Creating a new file
  - Hotkeys
- Using API Catalog
- Using API Catalog
  - API Versioning
  - View Service Information and API Documentation in the API Catalog
  - Swagger "Try it out" functionality in the API Catalog
    - Make a request
  - Static APIs refresh functionality in the API Catalog
- Using Zowe CLI
- Using Zowe CLI
  - Displaying help
    - Top-level help
    - Group, action, and object help

- Launch local web help
- Viewing web help
- How command precedence works
- Issuing commands
- Using profiles
  - Displaying profile help
  - Service profiles
  - Base profiles
  - Profile best practices
- Testing connection to z/OSMF
- Integrating with API Mediation Layer
  - How token management works
  - Logging in
  - Logging out
  - Accessing a service through API ML
  - Accessing multiple services with SSO
  - Accessing services through SSO + one service not through APIML
  - Accessing services through SSO + one service through API ML but not SSO
- Working with certificates
  - Configure certificates signed by a Certificate Authority (CA)
  - Extend trusted certificates on client
  - Bypass certificate requirement
- Using environment variables
  - Formatting environment variables
  - Setting environment variables in an automation server
- Using the prompt feature
- Writing scripts
- Understanding core command groups
- Extending Zowe CLI
- Extending Zowe CLI
- Software requirements for Zowe CLI plug-ins
- Software requirements for Zowe CLI plug-ins
- Installing Zowe CLI plug-ins
- Installing Zowe CLI plug-ins
  - Installing plug-ins from an online registry
  - Installing plug-ins from a local package
  - Validating plug-ins
  - Updating plug-ins

- Update plug-ins from an online registry
- Update plug-ins from a local package
- Uninstall Plug-ins
- IBM® CICS® Plug-in for Zowe CLI
- IBM® CICS® Plug-in for Zowe CLI
  - Use cases
  - Commands
  - Software requirements
  - Installing
  - Creating a user profile
- IBM<sup>®</sup> Db2<sup>®</sup> Database Plug-in for Zowe CLI
- IBM® Db2® Database Plug-in for Zowe CLI
  - Use cases
  - Commands
  - Software requirements
  - Installing
    - Installing from an online registry
    - Installing from a local package
  - Addressing the license requirement
    - Server-side license
    - Client-side license
  - Creating a user profile
    - SQL0805N: Database BIND
- IBM® z/OS FTP Plug-in for Zowe CLI
- IBM<sup>®</sup> z/OS FTP Plug-in for Zowe CLI
  - Use cases
  - Commands
  - Software requirements
  - Installing
  - Creating a user profile
- IBM<sup>®</sup> IMS<sup>™</sup> Plug-in for Zowe CLI
- IBM<sup>®</sup> IMS<sup>™</sup> Plug-in for Zowe CLI
  - Use cases
  - Commands
  - Software requirements
  - Installing
  - Creating user profiles
- IBM<sup>®</sup> MQ Plug-in for Zowe CLI

- IBM® MQ Plug-in for Zowe CLI
  - Use cases
  - Using IBM MQ plug-in commands
  - Software requirements
  - Installing
  - Creating a user profile
- Secure Credential Store Plug-in for Zowe CLI
- Secure Credential Store Plug-in for Zowe CLI
  - Use Cases
  - Commands
  - Software requirements
  - Installing
  - Using
    - Securing your credentials
    - Deactivating the plug-in
- Using Zowe Explorer
- Using Zowe Explorer
  - Usage Tips
  - Sample Use Cases
    - Work with Data Sets
    - Work with USS Files
    - Work with jobs
    - MVS and TSO Commands
- Using Zowe SDKs
- Using Zowe SDKs
  - API documentation
  - Software requirements
    - Node.js
    - Python
  - Getting started
    - Install SDK from online registry
    - Install SDK from local package
  - Using
    - Using Node.js
    - Using Python
  - Contributing
- Extending Zowe
- Extending Zowe

- Extend Zowe CLI
- Extend Zowe API Mediation Layer
  - Dynamic API registration
  - Static API registration
- Add a plug-in to the Zowe Desktop
- Sample extensions
  - Sample Zowe API and API Catalog extension
  - Sample Zowe Desktop extension
- Packaging z/OS extensions
- Packaging z/OS extensions
  - Zowe server component package format
  - Zowe component manifest
  - Sample manifests
- Install, upgrade, and configure Zowe server component
- Install, upgrade, and configure Zowe server component
  - Install with zowe-install-component.sh (Technical Preview)
  - Upgrade with zowe-upgrade-component.sh (Technical Preview)
  - Configure with zowe-configure-component.sh (Technical Preview)
  - Install and configure manually
    - Zowe core components
    - Zowe extensions
  - Verify with zowe-verify-component.sh (Technical Preview)
- Zowe server component runtime lifecycle
- Zowe server component runtime lifecycle
  - Zowe runtime lifecycle
  - Zowe component runtime lifecycle
    - Validate
    - Configure
    - Start
- Developing for Zowe CLI
- Developing for Zowe CLI
  - How can I contribute?
  - Getting started
    - Tutorials
    - Plug-in Development Overview
    - Imperative CLI Framework Documentation
    - Contribution Guidelines
- Setting up your development environment

- Setting up your development environment
  - Prerequisites
  - Initial setup
  - Branches
    - Clone zowe-cli-sample-plugin and build from source
    - (Optional) Run the automated tests
  - Next steps
- Installing the sample plug-in
- Installing the sample plug-in
  - Overview
  - Installing the sample plug-in to Zowe CLI
  - Viewing the installed plug-in
  - Using the installed plug-in
  - Testing the installed plug-in
  - Next steps
- Extending a plug-in
- Extending a plug-in
  - Overview
    - Creating a Typescript interface for the Typicode response data
    - Creating a programmatic API
    - Exporting interface and programmatic API for other Node.js applications
    - Checkpoint
    - Defining command syntax
    - Defining command handler
    - Defining command to list group
    - Checkpoint
  - Using the installed plug-in
  - Summary
  - Next steps
- Developing a new plug-in
- Developing a new plug-in
  - Overview
    - Cloning the sample plug-in source
    - Changing package.json
    - Adjusting Imperative CLI Framework configuration
    - Adding third-party packages
    - Creating a Node.js programmatic API
    - Exporting your API

- Checkpoint
  - Defining commands
- Trying your command
- Bringing together new tools!
- Next steps
- Implementing profiles in a plug-in
- Implementing profiles in a plug-in
  - Next steps
- Onboarding Overview
- Onboarding Overview
  - Prerequisites
  - Service Onboarding Guides
    - Recommended guides for services using Java
    - Recommended guides for services using Node.js
    - Guides for Static Onboarding and Direct Call Onboarding
    - Documentation for legacy enablers
  - Verify successful onboarding to the API ML
    - Verifying service discovery through Discovery Service
    - Verifying service discovery through the API Catalog
  - Sample REST API Service
- Onboarding a REST API service with the Plain Java Enabler (PJE)
- Onboarding a REST API service with the Plain Java Enabler (PJE)
  - Introduction
  - Onboarding your REST service with API ML
  - Prerequisites
  - Configuring your project
    - Gradle build automation system
    - Maven build automation system
  - Configuring your service
    - REST service identification
    - Administrative endpoints
    - API info
    - API routing information
    - API Catalog information
    - Authentication parameters
    - API Security
    - SAF Keyring configuration
    - Eureka Discovery Service

- Custom Metadata
- Registering your service with API ML
- Validating the discoverability of your API service by the Discovery Service
- Troubleshooting
- API Mediation Layer onboarding configuration
- API Mediation Layer onboarding configuration
  - Introduction
  - Configuring a REST service for API ML onboarding
  - Plain Java Enabler service onboarding API
    - Automatic initialization of the onboarding configuration by a single method call
  - Validating successful onboarding with the API Mediation Layer
  - Loading YAML configuration files
    - Loading a single YAML configuration file
    - Loading and merging two YAML configuration files
- Onboarding a service with the Zowe API Meditation Layer without an onboarding enabler
- Onboarding a service with the Zowe API Meditation Layer without an onboarding enabler
  - Introduction
  - Registering with the Discovery Service
    - API Mediation Layer Service onboarding metadata
  - Sending a heartbeat to API Mediation Layer Discovery Service
  - Validating successful onboarding with the API Mediation Layer
  - External Resources
- Onboarding a Spring Boot based REST API Service
- Onboarding a Spring Boot based REST API Service
  - Outline of onboarding a REST service using Spring Boot
  - Selecting a Spring Boot Enabler
  - Configuring your project
    - Gradle build automation system
    - Maven build automation system
  - Configuring your Spring Boot based service to onboard with API ML
    - Sample API ML Onboarding Configuration
    - API ML Onboarding Configuration Sample
    - SAF Keyring configuration
    - Custom Metadata
  - Registering and unregistering your service with API ML
    - Unregistering your service with API ML
    - Basic routing
  - Adding API documentation

- Validating the discoverability of your API service by the Discovery Service
- Troubleshooting
- Onboarding a Micronaut based REST API service
- Onboarding a Micronaut based REST API service
  - Set up your build automation system
  - Configure the Micronaut application
    - Add API ML configuration
    - Add Micronaut configuration
    - (Optional) Set up logging configuration
  - Validate successful registration
- Onboarding a Node.js based REST API service
- Onboarding a Node.js based REST API service
  - Introduction
  - Onboarding your Node.js service with API ML
  - Prerequisites
  - Installing the npm dependency
  - Configuring your service
  - Registering your service with API ML
  - Validating the discoverability of your API service by the Discovery Service
- Onboard a REST API without code changes required
- Onboard a REST API without code changes required
  - Identify the APIs that you want to expose
  - Define your service and API in YAML format
  - Route your API
  - Customize configuration parameters
  - Add and validate the definition in the API Mediation Layer running on your machine
  - Add a definition in the API Mediation Layer in the Zowe runtime
  - (Optional) Check the log of the API Mediation Layer
  - (Optional) Reload the services definition after the update when the API Mediation Layer is already started
- Zowe API Mediation Layer Single-Sign-On Overview
- Zowe API Mediation Layer Single-Sign-On Overview
  - Zowe API ML client
  - API service accessed via Zowe API ML
  - Existing services that cannot be modified
  - Further resources
- Obtaining Information about API Services
- Obtaining Information about API Services

- API ID in the API Mediation Layer
- Protection of Service Information
- API Endpoints
  - Obtain Information about a Specific Service
  - Obtain Information about All Services
  - Obtain Information about All Services with a Specific API ID
  - Response Format
- API Mediation Layer Message Service Component
- API Mediation Layer Message Service Component
  - Message Definition
  - Creating a message
  - Mapping a message
    - API ML Logger
- Zowe API Mediation Layer Security
- Zowe API Mediation Layer Security
  - How API ML transport security works
    - Transport layer security
    - Authentication
    - Zowe API ML services
    - Zowe API ML TLS requirements
    - Authentication for API ML services
    - Authorization
    - JWT Token
    - z/OSMF JSON Web Tokens Support
    - API ML truststore and keystore
    - API ML SAF Keyring
    - Discovery Service authentication
    - Setting ciphers for API ML services
  - ZAAS Client
    - Pre-requisites
    - API Documentation
    - Getting Started (Step by Step Instructions)
  - Certificate management in Zowe API Mediation Layer
    - Running on localhost
    - Zowe runtime on z/OS
- API Mediation Layer routing
- API Mediation Layer routing
  - Terminology

- APIML Basic Routing (using Service ID and version)
  - Implementation Details
- Basic Routing (using only the service ID)
- Enabling PassTicket creation for API Services that Accept PassTickets
- Enabling PassTicket creation for API Services that Accept PassTickets
  - Overview
  - Outline for enabling PassTicket support
  - Security configuration that allows the Zowe API Gateway to generate PassTickets for an API service
    - ACF2
    - Top Secret
    - RACF
  - API services that support PassTickets
    - API Services that register dynamically with API ML that provide authentication information
    - API Services that register dynamically with API ML but do not provide metadata
    - API services that are defined using a static YAML definition
  - Adding YAML configuration to API services that register dynamically with API ML
- Custom Metadata
- Custom Metadata
- Using the Caching Service
- Using the Caching Service
  - Architecture
  - Storage methods
    - VSAM
    - Redis
    - InMemory
  - How to start the service
  - Methods to use the Caching service API
  - Configuration properties
  - Authentication
    - Direct calls
    - Routed calls through API Gateway
- Using VSAM as a storage solution through the Caching service
- Using VSAM as a storage solution through the Caching service
  - Understanding VSAM
    - VSAM configuration
- Using Redis as a storage solution through the Caching service
- Using Redis as a storage solution through the Caching service
  - Understanding Redis

- Redis replica instances
- Redis Sentinel
- Redis SSL/TLS
- Redis and Lettuce
- Redis configuration
- Overview
- Overview
  - How Zowe Application Framework works
  - Tutorials
  - Samples
    - Sample Iframe App
    - Sample Angular App
    - Sample React App
    - User Browser Workshop Starter App
- Plug-ins definition and structure
- Plug-ins definition and structure
  - Application plug-in filesystem structure
    - Root files and directories
    - Dev and source content
    - Runtime content
    - Default user configuration
    - App-to-App Communication
    - Documentation
  - Location of plug-in files
    - pluginsDir directory
  - Plug-in definition file
  - Plug-in attributes
    - General attributes
    - Application attributes
    - Application web content attributes
    - IFrame application web content
    - Plugin Definition Schema Revision Notes
    - Application Dataservices
    - Application Configuration Data
- Building plugin apps
- Building plugin apps
  - Building web content
  - Building app server content

- Building zss server content
- Tagging plugin files on z/OS
- Building Javascript content (\*.js files)
- Installing
- Packaging
- Installing Plugins
- Installing Plugins
  - By filesystem
    - Adding/Installing
    - Removing
    - Upgrading
    - Modifying without server restart (Exercise to the reader)
  - By REST API
    - Old plugins folder
- Embedding plugins
- Embedding plugins
  - How to interact with embedded plugin
  - How to destroy embedded plugin
  - How to style a container for the embedded plugin
  - Applications that use embedding
- Dataservices
- Dataservices
  - Defining dataservices
    - Router-type specific attributes
    - Import-type specific attributes
    - External-type specific attributes
  - Defining Java dataservices
    - Prerequisites
    - Defining Java dataservices
    - Defining Java Application Server libraries
    - Java dataservice logging
    - Java dataservice limitations
  - Using dataservices with RBAC
  - Dataservice APIs
    - Router-based dataservices
    - ZSS based dataservices
  - Documenting dataservices
- Authentication API

- Authentication API
  - Handlers
    - Handler installation
    - Handler configuration
    - Handler context
    - Handler capabilities
    - Examples
    - High availability (HA)
  - REST API
    - Check status
  - Authenticate
  - User not authenticated or not authorized
    - Not authenticated
    - Not authorized
    - Refresh status
    - Logout
    - Password changes
- Internationalizing applications
- Internationalizing applications
  - Internationalizing Angular applications
  - Internationalizing React applications
  - Internationalizing application desktop titles
- Zowe Desktop and window management
- Zowe Desktop and window management
  - Loading and presenting application plug-ins
  - Plug-in management
  - Application management
  - Windows and Viewports
  - Viewport Manager
  - Injection Manager
    - Plug-in definition
    - Logger
    - Launch Metadata
    - Viewport Events
    - Window Events
    - Window Actions
  - Framework API examples
- Configuration Dataservice

- Configuration Dataservice
  - Resource Scope
  - REST API
    - REST query parameters
    - REST HTTP methods
    - Administrative access and group
  - Application API
  - Internal and bootstrapping
  - Packaging Defaults
  - Plug-in definition
  - Aggregation policies
  - Examples
- URI Broker
- URI Broker
  - Accessing the URI Broker
  - Functions
    - Accessing an application plug-in's dataservices
    - Accessing application plug-in's configuration resources
    - Accessing static content
    - Accessing the application plug-in's root
    - Server queries
- Application-to-application communication
- Application-to-application communication
  - Why use application-to-application communication?
  - Actions
    - Action target modes
    - Action types
    - Loading actions
    - App2App via URL
    - Dynamically
    - Saved on system
  - Recognizers
    - Recognition clauses
    - Loading Recognizers at runtime
    - Recognizer example
  - Dispatcher
  - Registry
  - Pulling it all together in an example

- Configuring IFrame communication
- Configuring IFrame communication
- Error reporting UI
- Error reporting UI
  - ZluxPopupManagerService
  - ZluxErrorSeverity
  - ErrorReportStruct
  - Implementation
    - Declaration
    - Usage
    - HTML
- Logging utility
- Logging utility
  - Logging objects
  - Logger IDs
  - Accessing logger objects
    - Logger
    - Component logger
  - Logger API
  - Component Logger API
  - Log Levels
  - Logging verbosity
    - Configuring logging verbosity
  - Using log message IDs
    - Message ID logging examples
- Using Conda to make and manage packages of Application Framework Plugins
- Using Conda to make and manage packages of Application Framework Plugins
  - Initial Conda setup
  - Managing Conda channels
  - Searching for packages
  - Using Conda with Zowe
    - Setting environment variables temporarily:
    - Setting environment variables persistently
    - Installing a Zowe plugin
    - Zowe plugin configuration
    - Zowe package structure
  - Building Conda packages for Zowe
    - Defining package properties

- Creating build step
- Lifecycle scripts
- Adding configuration to Conda packages
- Creating and adding Zowe extension containers
- Creating and adding Zowe extension containers
  - 1. Build and publish a component image to a registry
  - 2. Define Deployment object
  - 3. Start your component
- Extending Zowe Explorer
- Extending Zowe Explorer
- Developing for Zowe SDKs
- Developing for Zowe SDKs
- Zowe Conformance Program
- Zowe Conformance Program
  - Introduction
  - How to participate
  - How to suggest updates to the Zowe conformance program
- Troubleshooting
- Troubleshooting
  - Known problems and solutions
  - Collecting data for Zowe problems
  - Verifying a Zowe release's integrity
  - Understanding the Zowe release
- Understanding the Zowe release
- Understanding the Zowe release
  - Zowe releases
    - Patch
    - Minor release
    - Major release
  - Check the Zowe release number
- Capturing diagnostics to assist problem determination
- Capturing diagnostics to assist problem determination
  - Running the diagnostic support script
  - Problems that may occur running the diagnostic script
    - IKJ56328I JOB job name REJECTED
- Verify Zowe runtime directory
- Verify Zowe runtime directory
  - Step 1: Obtain the verify tool (Required for versions before v1.14)

- Step 2: Verify your runtime directory
- Step 3: Review results
  - Mismatch
  - Match
- zowe-verify-authenticity.sh parameters
- Use of zowe-verify-authenticity.sh by zowe-support.sh
- Troubleshooting installation and startup of Zowe z/OS components
- Troubleshooting installation and startup of Zowe z/OS components
  - How to check if ZWESVSTC startup is successful
    - Check the startup of API Mediation Layer
    - Check the startup of Zowe Desktop
    - Check the startup of Zowe File and Jobs API servers
    - Check the startup of Zowe Secure Services
  - Unable to launch Zowe with { FSUM7351 }
  - Unable to create BPXAS instances
  - Errors caused when running the Zowe desktop with node 8.16.1
  - Cannot start Zowe and UNIX commands not found with FSUM7351
  - Various warnings show when connecting Zowe with another domain
- Troubleshooting Kubernetes environments
- Troubleshooting Kubernetes environments
  - ISSUE: /tmp directory is not writable
    - ISSUE: Permission denied showing in pod log
    - ISSUE: Deployment and ReplicaSet failed to create pod
    - ISSUE: Failed to create services
- Troubleshooting API ML
- Troubleshooting API ML
  - Enable API ML Debug Mode
  - Change the Log Level of Individual Code Components
  - Known Issues
    - API ML stops accepting connections after z/OS TCP/IP stack is recycled
    - SEC0002 error when logging in to API Catalog
    - API ML throws I/O error on GET request and cannot connect to other services
    - Certificate error when using both an external certificate and Single Sign-On to deploy Zowe
    - Browser unable to connect due to a CIPHER error
    - API Components unable to handshake
    - Java z/OS components of Zowe unable to read certificates from keyring
- Error Message Codes
- Error Message Codes

- API mediation utility messages
  - ZWEAM000I
- API mediation common messages
  - ZWEAO102E
  - ZWEAO104W
  - ZWEAO105W
  - ZWEAO106W
  - ZWEAO401E
- Common service core messages
  - ZWEAM100E
  - ZWEAM101E
  - ZWEAM102E
  - ZWEAM103E
  - ZWEAM104E
  - ZWEAM400E
  - ZWEAM500W
  - ZWEAM501W
  - ZWEAM502E
  - ZWEAM503E
  - ZWEAM504E
  - ZWEAM505E
  - ZWEAM506E
  - ZWEAM507E
  - ZWEAM508E
  - ZWEAM509E
  - ZWEAM510E
  - ZWEAM511E
  - ZWEAM600W
  - ZWEAM700E
  - ZWEAM701E
- Security common messages
  - ZWEAT100E
  - ZWEAT103E
  - ZWEAT403E
  - ZWEAT409E
  - ZWEAT410E
  - ZWEAT411E
  - ZWEAT412E

- ZWEAT413E
- ZWEAT414E
- ZWEAT415E
- ZWEAT416E
- ZWEAT601E
- ZWEAT602E
- ZWEAT603E
- Security client messages
  - ZWEAS100E
  - ZWEAS101E
  - ZWEAS103E
  - ZWEAS104E
  - ZWEAS105E
  - ZWEAS120E
  - ZWEAS121E
  - ZWEAS130E
  - ZWEAS131E
- ZAAS client messages
  - ZWEAS100E
  - ZWEAS120E
  - ZWEAS121E
  - ZWEAS122E
  - ZWEAS170E
  - ZWEAS400E
  - ZWEAS401E
  - ZWEAS404E
  - ZWEAS417E
  - ZWEAS130E
  - ZWEAS500E
  - ZWEAS501E
  - ZWEAS502E
  - ZWEAS503E
- Discovery service messages
  - ZWEAD400E
  - ZWEAD401E
  - ZWEAD700W
  - ZWEAD701E
  - ZWEAD702W

- ZWEAD703E
- ZWEAD704E
- Gateway service messages
  - ZWEAG500E
  - ZWEAG700E
  - ZWEAG701E
  - ZWEAG702E
  - ZWEAG704E
  - ZWEAG705E
  - ZWEAG706E
  - ZWEAG707E
  - ZWEAG708E
  - ZWEAG709E
  - ZWEAG710E
  - ZWEAG711E
  - ZWEAG712E
  - ZWEAG100E
  - ZWEAG101E
  - ZWEAG102E
  - ZWEAG103E
  - ZWEAG104E
  - ZWEAG105E
  - ZWEAG106W
  - ZWEAG107W
  - ZWEAG108E
  - ZWEAG109E
  - ZWEAG110E
  - ZWEAG120E
  - ZWEAG121E
  - ZWEAG130E
  - ZWEAG131E
  - ZWEAG140E
  - ZWEAG141E
- API Catalog messages
  - ZWEAC100W
  - ZWEAC101E
  - ZWEAC102E
  - ZWEAC103E

- ZWEAC104E
- ZWEAC700E
- ZWEAC701W
- ZWEAC702E
- ZWEAC703E
- ZWEAC704E
- ZWEAC705W
- ZWEAC706E
- ZWEAC707E
- ZWEAC708E
- ZWEAC709E
- Troubleshooting Zowe Application Framework
- Troubleshooting Zowe Application Framework
  - Desktop apps fail to load
  - NODEJSAPP disables immediately
  - Cannot log in to the Zowe Desktop
    - ZSS server unable to communicate with X-MEM
    - ZLUX unable to communicate with zssServer
    - ZLUX unable to communicate with API Mediation Layer
  - Server startup problem ret=1115
  - Application plug-in not in Zowe Desktop
  - Error: You must specify MVD\_DESKTOP\_DIR in your environment
  - Error: Zowe Desktop address space fails to start { ZWED0115E }
  - Warning: Problem making eureka request { Error: connect ECONNREFUSED }
  - Warning: ZWED0159W Plugin (org.zowe.zlux.proxy.zosmf) loading failed.
  - Warning: ZWED0050W Could not read swagger doc folder (..)
  - Warning: ZWED0047W Swagger file for server (...) not found
  - Unable to log in to the explorers when using Zowe V1.13 or V1.14
- Gathering information to troubleshoot Zowe Application Framework
- Gathering information to troubleshoot Zowe Application Framework
  - z/OS release level
  - Zowe version and release level
  - Log output from the Zowe Application Server
  - Error message codes
  - Javascript console output
  - Screen captures
- Raising a Zowe Application Framework issue on GitHub
- Raising a Zowe Application Framework issue on GitHub

- Raising a bug report
- Raising an enhancement report
- Troubleshooting z/OS Services
- Troubleshooting z/OS Services
  - z/OSMF JVM cache corruption
    - Isolate the started task user IDs
    - Update z/OSMF to not use JVM class caching
  - Unable to generate unique CeaTso APPTAG
  - z/OS Services are unavailable
- Troubleshooting Zowe CLI
- Troubleshooting Zowe CLI
  - Problem
    - Environment
  - Before reaching out for support
  - Resolving the problem
- Gathering information to troubleshoot Zowe CLI
- Gathering information to troubleshoot Zowe CLI
  - Identify the currently installed CLI version
  - Identify the currently installed versions of plug-ins
  - Environment variables
    - Log levels
    - Home directory
  - Home directory structure
    - Location of logs
    - Profile configuration
  - Node.js and npm
    - npm configuration
    - npm log files
- z/OSMF troubleshooting
- z/OSMF troubleshooting
  - Alternate methods
- Known Zowe CLI issues
- Known Zowe CLI issues
  - EACCESS error when issing npm install command
  - Command not found message displays when issuing npm install commands
  - npm install -g Command Fails Due to an EPERM Error
  - Sudo syntax required to complete some installations
  - npm install -g command fails due to npm ERR! Cannot read property 'pause' of undefined error

- Node.js commands do not respond as expected
- Installation fails on Oracle Linux 6
- Raising a CLI issue on GitHub
- Raising a CLI issue on GitHub
  - Raising a bug report
  - Raising an enhancement report
- Troubleshooting Zowe Explorer
- Troubleshooting Zowe Explorer
  - Before reaching out for support
- Known Zowe Explorer issues
- Known Zowe Explorer issues
  - Data Set Creation Error
  - Opening Binary Files Error
- Raising a Zowe Explorer issue on GitHub
- Raising a Zowe Explorer issue on GitHub
  - Raising a bug report
  - Submitting a feature request
- Troubleshooting Zowe Launcher
- Troubleshooting Zowe Launcher
  - Enable Zowe Launcher Debug Mode
- Error Message Codes
- Error Message Codes
  - Zowe Launcher informational messages
    - ZWEL0001I
    - ZWEL0002I
    - ZWEL0003I
    - ZWEL0004I
    - ZWEL0005I
  - Zowe Launcher error messages
    - ZWEL0030E
    - ZWEL0038E
    - ZWEL0040E
- Contribute to Zowe
- Contribute to Zowe
  - Report bugs and enhancements
  - Fix issues
  - Send a Pull Request
  - Report security issues

- Contribution guidelines
- Promote Zowe
- Helpful resources
- Code categories
- Code categories
  - Programming languages
  - Component-specific guidelines and tutorials
- General code style guidelines
- General code style guidelines
  - Whitespaces
  - Naming Conventions
    - Functions and methods
    - Variables
- Pull requests guidelines
- Pull requests guidelines
- Documentation Guidelines
- Documentation Guidelines
  - Contributing to external documentation
  - Component Categories
    - Server Core
    - Server Security
    - Microservices
    - Zowe Desktop Applications
    - Web Framework
    - CLI Plugins
    - Core CLI Imperative CLI Framework
  - Programming Languages
    - Typescript
    - Java
    - C
- Introduction
- Introduction
  - Clear
  - Consistent
  - Smart
- Colors
- Colors
  - Color palette

- Light theme
- Dark theme
- Color contrast | WCAG AA standards
- Typography
- Typography
  - Typeface
  - Font weight
  - Body copy
  - Line scale
  - Line-height
  - Embed font
  - Import font
  - Specify in CSS
- Grid
- Grid
  - 12 column grid
  - Gutters
  - Columns
  - Margins
- Iconography
- Iconography
- Application icon
- Application icon
  - General rules
  - Shape, size, and composition
  - Colors and shades
    - Verify the contrast
    - Use the Zowe palette
    - Layer Shadows
    - Use the long shadow for consistency.
- Contributing to Zowe Documentation
- Contributing to Zowe Documentation
  - Before You Get Started
  - Getting Started Checklist
  - The Zowe Documentation Repository
  - Sending a GitHub Pull Request
  - Opening An Issue for Zowe Documentation
  - Documentation Style guide

- Headings and titles
- Technical elements
- Tone
- Word usage
- Graphics
- Abbreviations
- Structure and format
- Word usage
- Zowe CLI command reference guide
- Zowe CLI command reference guide
- Zowe API reference
- Zowe API reference
- Zowe Binaries Bill of Materials
- Zowe Binaries Bill of Materials
  - Zowe PAX
  - Zowe CLI Package
  - Zowe CLI Plugins

Version: v1.25.x LTS

## **Zowe overview**

Zowe<sup>™</sup> is an open source software framework that allows mainframe development and operation teams to securely manage, control, script, and develop on the mainframe. It was created to host technologies that benefit the IBM Z platform for all members of the Z community, including Integrated Software Vendors (ISVs), System Integrators, and z/OS consumers. Like Mac or Windows, Zowe comes with a set of APIs and OS capabilities that applications build on and also includes some applications out of the box. Zowe offers modern interfaces to interact with z/OS and allows you to work with z/OS in a way that is similar to what you experience on cloud platforms today. You can use these interfaces as delivered or through plug-ins and extensions that are created by clients or third-party vendors. Zowe is a project within the Open Mainframe Project.

### Zowe demo video

Watch this video to see a quick demo of Zowe.

Download the deck for this video | Download the script

### **Component overview**

Zowe consists of the following components:

- Zowe Application Framework
- API Mediation Layer
- Zowe CLI
- Zowe Explorer
- Zowe Client Software Development Kits SDKs
- Zowe Launcher
- Zowe Mobile Incubator
- ZEBRA (Zowe Embedded Browser for RMF/SMF and APIs) Incubator

### **Zowe Application Framework**

A web user interface (UI) that provides a virtual desktop containing a number of apps allowing access to z/OS function. Base Zowe includes apps for traditional access such as a 3270 terminal and a VT Terminal, as well as an editor and explorers for working with JES, MVS Data Sets and Unix System Services.

### 📖 Learn more

The Zowe Application Framework modernizes and simplifies working on the mainframe. With the Zowe Application Framework, you can create applications to suit your specific needs. The Zowe Application Framework contains a web UI that has the following features:

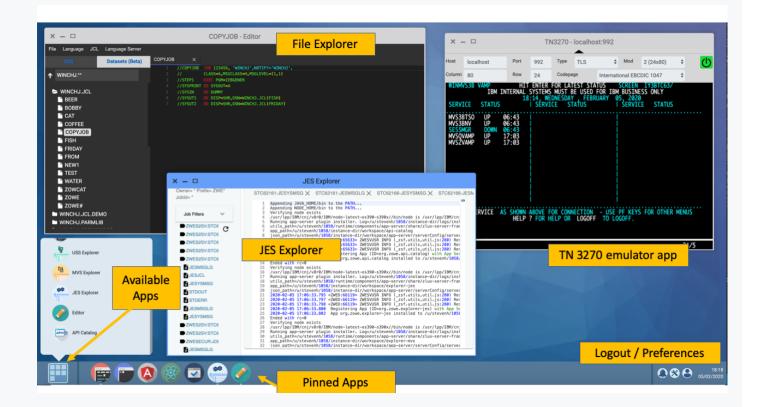
- The web UI works with the underlying REST APIs for data, jobs, and subsystem, but presents the information in a full screen mode as compared to the command line interface.
- The web UI makes use of leading-edge web presentation technology and is also extensible through web UI plug-ins to capture and present a wide variety of information.
- The web UI facilitates common z/OS developer or system programmer tasks by providing an editor for common text-based files like REXX or JCL along with general purpose data set actions for both Unix System Services (USS) and Partitioned Data Sets (PDS) plus Job Entry System (JES) logs.

The Zowe Application Framework consists of the following components:

### • Zowe Desktop

The desktop, accessed through a browser. The desktop contains a number of applications, including a TN3270 emulator for traditional Telnet or TLS terminal access to z/OS, a VT Termnial for SSH commands, as well as rich web GUI applications including a JES Explorer for working with jobs

and spool output, a File Editor for working with USS directories and files and MVS data sets and members. The Zowe desktop is extensible and allows vendors to provide their own applications to run within the desktop. See Extending the Zowe Desktop. The following screen capture of a Zowe desktop shows some of its composition as well as the TN3270 app, the JES Explorer, and the File Editor open and in use.



#### Zowe Application Server

The Zowe Application Server runs the Zowe Application Framework. It consists of the Node.js server plus the Express.js as a webservices framework, and the proxy applications that communicate with the z/OS services and components.

#### ZSS Server

The ZSS Server provides secure REST services to support the Zowe Application Server. For services that need to run as APF authorized code, Zowe uses an angel process that the ZSS Server calls using cross memory communication. During installation and configuration of Zowe, you will see the steps needed to configure and launch the cross memory server.

#### • Application plug-ins

Several application-type plug-ins are provided. For more information, see Using the Zowe Application Framework application plug-ins.

### **API Mediation Layer**

Provides a gateway that acts as a reverse proxy for z/OS services, together with a catalog of REST APIs and a dynamic discovery capability. Base Zowe provides core services for working with MVS Data Sets, JES, as well as working with z/OSMF REST APIs. The API Mediation Layer also provides a framework for Single Sign On (SSO).

#### Learn more

The API Mediation Layer provides a single point of access for mainframe service REST APIs. The layer offers enterprise, cloud-like features such as high-availability, scalability, dynamic API discovery, consistent security, a single sign-on experience, and documentation. The API Mediation Layer facilitates secure communication across loosely coupled microservices through the API Gateway. The API Mediation Layer consists of three components: the Gateway, the Discovery Service, and the Catalog. The Gateway provides secure communication across loosely coupled API services. The Discovery Service enables you to determine the location and status of service instances running inside the API ML ecosystem. The Catalog provides an easy-to-use interface to view all discovered services, their associated APIs, and Swagger documentation in a user-friendly manner.

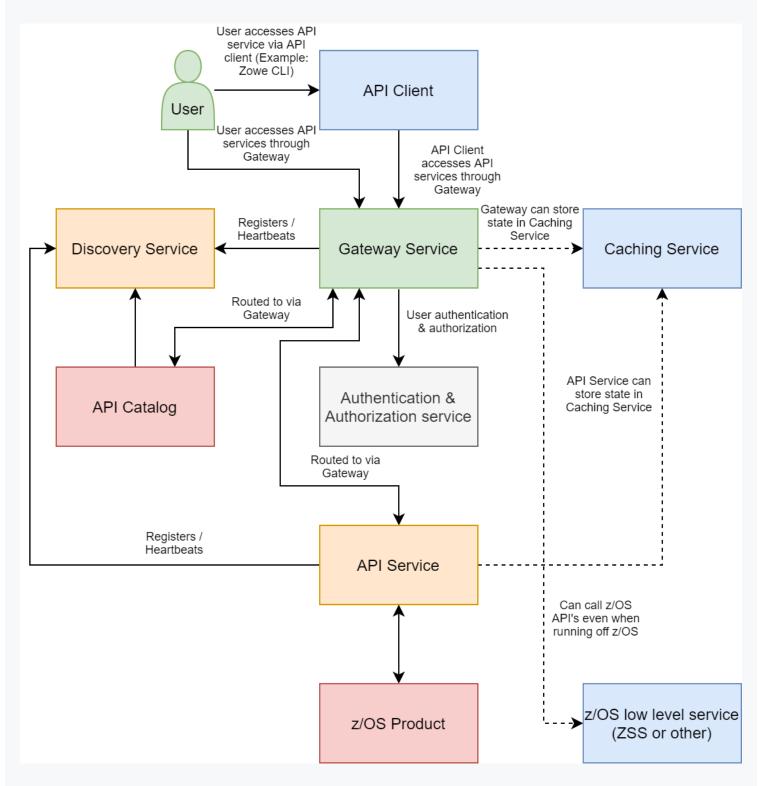
#### **Key features**

- Consistent Access: API routing and standardization of API service URLs through the Gateway component provides users with a consistent way to access mainframe APIs at a predefined address.
- Dynamic Discovery: The Discovery Service automatically determines the location and status of API services.
- High-Availability: API Mediation Layer is designed with high-availability of services and scalability in mind.
- Caching Service: This feature is designed for Zowe components in a high availability configuration. It supports the High Availability of all components within Zowe, allowing components to be stateless by providing a mechanism to offload their state to a location accessible by all instances of the service, including those which just started.
- Redundancy and Scalability: API service throughput is easily increased by starting multiple API service instances without the need to change configuration.
- Presentation of Services: The API Catalog component provides easy access to discovered API services and their associated documentation in a user-friendly manner. Access to the contents of the API Catalog is controlled through a z/OS security facility.

• Encrypted Communication: API ML facilitates secure and trusted communication across both internal components and discovered API services.

### **API Mediation Layer architecture**

The following diagram illustrates the single point of access through the Gateway, and the interactions between API ML components and services:



Components

The API Layer consists of the following key components:

### **API Gateway**

Services that comprise the API ML service ecosystem are located behind a gateway (reverse proxy). All end users and API client applications interact through the Gateway. Each service is assigned a unique service ID that is used in the access URL. Based on the service ID, the Gateway forwards incoming API requests to the appropriate service. Multiple Gateway instances can be started to achieve highavailability. The Gateway access URL remains unchanged. The Gateway is built using Netflix Zuul and Spring Boot technologies.

### **Discovery Service**

The Discovery Service is the central repository of active services in the API ML ecosystem. The Discovery Service continuously collects and aggregates service information and serves as a repository of active services. When a service is started, it sends its metadata, such as the original URL, assigned serviceld, and status information to the Discovery Service. Back-end microservices register with this service either directly or by using a Eureka client. Multiple enablers are available to help with service on-boarding of various application architectures including plain Java applications and Java applications that use the Spring Boot framework. The Discovery Service is built on Eureka and Spring Boot technology.

#### **Discovery Service TLS/SSL**

HTTPS protocol can be enabled during API ML configuration and is highly recommended. Beyond encrypting communication, the HTTPS configuration for the Discovery Service enables heightened security for service registration. Without HTTPS, services provide a username and password to register in the API ML ecosystem. When using HTTPS, only trusted services that provide HTTPS certificates signed by a trusted certificate authority can be registered.

#### **API Catalog**

The API Catalog is the catalog of published API services and their associated documentation. The Catalog provides both the REST APIs and a web user interface (UI) to access them. The web UI follows the industry standard Swagger UI component to visualize API documentation in OpenAPI JSON format for each service. A service can be implemented by one or more service instances, which provide exactly the same service for high-availability or scalability.

### **Catalog Security**

Access to the API Catalog can be protected with an Enterprise z/OS Security Manager such as IBM RACF, ACF2, or Top Secret. Only users who provide proper mainframe credentials can access the Catalog. Client authentication is implemented through the z/OSMF API.

### Caching Service

It provides an API in high-availability mode which offers the possibility to store, retrieve and delete data associated with keys. The service will be used only by internal Zowe applications and will not be exposed to the internet.

### **Onboarding APIs**

Essential to the API Mediation Layer ecosystem is the API services that expose their useful APIs. Use the following topics to discover more about adding new APIs to the API Mediation Layer and using the API Catalog:

- Onboarding Overview
- Onboard an existing Spring Boot REST API service using Zowe API Mediation Layer
- Onboard an existing Node.js REST API service using Zowe API Mediation Layer
- Using API Catalog

To learn more about the architecture of Zowe, see Zowe architecture.

### Zowe CLI

Zowe CLI is a command-line interface that lets you interact with the mainframe in a familiar, off-platform format. Zowe CLI helps to increase overall productivity, reduce the learning curve for developing mainframe applications, and exploit the ease-of-use of off-platform tools. Zowe CLI lets you use common tools such as Integrated Development Environments (IDEs), shell commands, bash scripts, and build tools for mainframe development. Though its ecosystem of plug-ins, you can automate actions on systems such as IBM Db2, IBM CICS, and more. It provides a set of utilities and services for users that want to become efficient in supporting and building z/OS applications quickly.

💷 Learn more

Zowe CLI provides the following benefits:

- Enables and encourages developers with limited z/OS expertise to build, modify, and debug z/OS applications.
- Fosters the development of new and innovative tools from a computer that can interact with z/OS.
   Some Zowe extensions are powered by Zowe CLI, for example the Visual Studio Code Extension for Zowe.
- Ensure that business critical applications running on z/OS can be maintained and supported by existing and generally available software development resources.
- Provides a more streamlined way to build software that integrates with z/OS.

**Note:** For information about software requirements, installing, and upgrading Zowe CLI, see Installing Zowe.

### **Zowe CLI capabilities**

With Zowe CLI, you can interact with z/OS remotely in the following ways:

- Interact with mainframe files: Create, edit, download, and upload mainframe files (data sets) directly from Zowe CLI.
- **Submit jobs:** Submit JCL from data sets or local storage, monitor the status, and view and download the output automatically.
- Issue TSO and z/OS console commands: Issue TSO and console commands to the mainframe directly from Zowe CLI.
- Integrate z/OS actions into scripts: Build local scripts that accomplish both mainframe and local tasks.
- **Produce responses as JSON documents:** Return data in JSON format on request for consumption in other programming languages.

For detailed information about the available functionality in Zowe CLI, see Zowe CLI Command Groups.

For information about extending the functionality of Zowe CLI by installing plug-ins, see Extending Zowe CLI.

### **More Information:**

- System requirements for Zowe CLI
- Installing Zowe CLI

### **Zowe Explorer**

Zowe Explorer is a Visual Studio Code extension that modernizes the way developers and system administrators interact with z/OS mainframes. Zowe Explorer lets you interact with data sets, USS files, and jobs that are stored on z/OS. The extension complements your Zowe CLI experience and lets you use authentication services like API Mediation Layer. The extension provides the following benefits:

- Enabling you to create, modify, rename, copy, and upload data sets directly to a z/OS mainframe.
- Enabling you to create, modify, rename, and upload USS files directly to a z/OS mainframe.
- Providing a more streamlined way to access data sets, uss files, and jobs.
- Letting you create, edit, and delete Zowe CLI zosmf compatible profiles.
- Letting you use the Secure Credential Store plug-in to store your credentials securely in the settings.
- Letting you leverage the API Mediation Layer token-based authentication to access z/OSMF.

For more information, see Information roadmap for Zowe Explorer.

### Zowe Client Software Development Kits (SDKs)

The Zowe Client SDKs consist of programmatic APIs that you can use to build client applications or scripts that interact with z/OS. The following SDKs are available:

- Zowe Node.js Client SDK
- Zowe Python Client SDK

For more information, see Using the Zowe SDKs.

### **Zowe Launcher**

Provides an advanced launcher for Zowe z/OS server components in a high availability configuration. It performs the following operations:

- Stopping the Zowe server components using the STOP (or P) operator command
- Stopping and starting specific server components without restarting the entire Zowe instance using MODIFY (or F) operator command

### **Zowe Mobile - Incubator**

Lets you interact with your Zowe instance running on the mainframe from your mobile.

For more information, see Information roadmap for Zowe Mobile.

### ZEBRA (Zowe Embedded Browser for RMF/SMF and APIs) - Incubator

Provides re-usable and industry compliant JSON formatted RMF/SMF data records, so that many other ISV SW and users can exploit them using open-source SW for many ways.

For more information, see the ZEBRA documentation or visit the ZEBRA test/trial site.

### Zowe Workflow wiZard - Incubator

The Workflow wiZard delivers a workflow builder which simplifies the creation of z/OSMF workflows. The workflow builder reads a library of templates along with a set of properties, determines which steps are necessary based upon rules that use property values, determines a suitable order to satisfy the workflow engine requirements, inserts variable definitions when required, and outputs workflow XML.

For more information, see the Workflow Template Reference.

### Zowe Third-Party Software Requirements and Bill of Materials

- Third-Party Software Requirements (TPSR)
- Bill of Materials (BOM)

Version: v1.25.x LTS

# Zowe architecture

Zowe<sup>™</sup> is a collection of components that together form a framework that allows Z-based functionality to be accessible across an organization. This includes exposing Z-based components such as z/OSMF as Rest APIs. The framework provides an environment where other components can be included and exposed to a broader non-Z based audience.

The following diagram depicts the high-level Zowe architecture.

The diagram shows the default port numbers that are used by Zowe. These are dependent on each instance of Zowe and are held in the Zowe instance directory configuration file <code>instance.env</code>. For more information, see Creating and configuring the Zowe instance directory.

Zowe components can be categorized by location: server or client. While the client is always an end user tool such as a PC, browser or mobile device, the server components can be further categorized by what machine they run on.

Zowe server components can be installed and run entirely on z/OS, but a subset of the components can alternatively run on Linux or z/Linux via Docker. While on z/OS, many of these components run under Unix System Services (USS). The ones that do not run under USS must remain on z/OS when using Docker in order to provide connectivity to the mainframe.

# Zowe architecture with high availability enablement on Sysplex

The following diagram depicts the difference in locations of Zowe components when deploying Zowe into Sysplex with high availability enabled as opposed to running all components on a single z/OS system.

To enable high availability for Zowe, the ZWESLSTC started task is used instead of using ZWESVSTC. Also, the configuration details are held in a zowe.yaml configuration file instead of instance.env. zowe.yaml contains settings for each high availability instance that the launcher starts. The diagram above shows that **ZWESLSTC** has started two Zowe instances running on two separate LPARs that can be on the same, or different, sysplexes.

- The Sysplex distributor port sharing enables the API Gateway 7554 ports to be shared so incoming requests can be routed to either the gateway on LPAR A or LPAR B.
- The discovery servers on each LPAR communicate with each other and share their registered instances, which allows the API gateway on LPAR A to dispatch APIs to components either on its own LPAR, or else to components on LPAR B. As indicated on the diagram, each component has two input lines: one from the API gateway on its own LPAR and one from the gateway on the other LPAR. When one of the LPARs goes down, the other LPAR remains operating within the sysplex providing high availability to clients that connect through the shared port irrespective of which Zowe instance is serving the API requests.

The zowe.yaml file can be configured to start Zowe instances on more than two LPARS, and also to start more than one Zowe instance on a single LPAR, providing a grid cluster of Zowe components that can meet availability and scalability requirements.

Each LPAR's configuration entries in zowe.yaml control which components will be started. This allows you to start just the desktop and API Mediation Layer on the first LPAR, and start all of the Zowe components on the second LPAR. Because the desktop on the first LPAR is available to the second LPAR's gateway, all desktop traffic will be routed there.

The caching services for each Zowe instance, whether on the same LPAR or distributed across the sysplex, are connected to each other by the same shared VSMA file. This allows state sharing so that each instance behaves similarly to the user irrespective of where their request is routed.

For simplification of the diagram above, the Zowe Explorer API and UI servers are not shown as being started. If you define them to be started in the zowe.yaml configuration file, they would behave the same as the servers illustrated. That means, they will register to their API discovery server which will then communicate with other discovery servers on other Zowe instances on either the same or other LPARs. The API traffic received by any API gateway on any Zowe instance will be routed to any of the Zowe Explorer API or UI components that are available.

To learn more about Zowe with high availability enablement, see Zowe high availability installation roadmap.

### Zowe architecture when running in Kubernetes cluster

The following diagram depicts the difference in locations of Zowe components when deploying Zowe into Kubernetes cluster as opposed to running all components on a single z/OS system.

The components on z/OS run under the Zowe started task ZWESVSTC, which has its own user ID ZWESVUSR and includes a number of servers each with their own address space. The ZWESVSTC started task has a STDOUT file that includes log and trace information for its servers. Sever error messages are written to STDERR. For problem determination, see Troubleshooting.

When deploying other server components into container orchestration software like Kubernetes, Zowe follows standard Kubernetes practices and the cluster can be monitored and managed with common Kubernetes administration methods.

- All Zowe workloads are running on a dedicated namespace (zowe by default) to distinguish from other workloads in same Kubernetes cluster.
- Zowe has it's own ServiceAccount to help on managing permissions.
- Server components uses similar instance.env or zowe.yaml on z/OS, which are stored in ConfigMap and Secret, to configure and start.
- Server components can be configured using same certificates used on z/OS components.
- Zowe claims it's own Persistent Volume to share files across components.
- Each server components are running in separated containers.
- Components may register themselves to Discovery with their own Pod name within the cluster.
- Zowe workloads use zowe-launch-scripts initContainers step to prepare required runtime directories.
- Only necessary components ports are exposed outside of Kubernetes with Service.

### Zowe architecture when using Docker image

**Technical Preview** The Zowe Docker build is a technical preview.

The following diagram depicts the difference in locations of Zowe components when using Docker as opposed to running all components on z/OS.

The components on z/OS run under the Zowe started task ZWESVSTC, which has its own user ID ZWESVUSR and includes a number of servers each with their own address space. The ZWESVSTC started task has a STDOUT file that includes log and trace information for its servers. Sever error messages are written to STDERR. For problem determination, see Troubleshooting.

When Docker is used, server components not running on z/OS instead run in a Linux environment provided via the Docker container technology. The servers run as processes within the container which log to STDOUT and STDERR of that container, with some components also write to the Zowe instance's log directory.

### App Server

The App Server is a node.js server that is responsible for the Zowe Application Framework. It provides the Zowe desktop, which is accessible through a web browser via port 8544. The Zowe desktop includes a number of applications that run inside the Application Framework such as a 3270 emulator and a File Editor.

The App Server server logs are written to <INSTANCE\_DIR>/logs/appServer-yyyy-mm-dd-hhmm.log. The Application Framework provides REST APIs for its services that are included on the API catalog tile Zowe Application Framework that can be viewed at https://<ZOWE\_HOST\_IP>:7554/ui/v1/apicatalog/#/tile/ZLUX/zlux.

### ZSS

The Zowe desktop delegates a number of its services to the ZSS server which it accesses through the http port 8542. ZSS is written in C and has native calls to z/OS to provide its services. ZSS logs are written STDOUT and STDERR for capture into job logs, but also as a file into

### **API Gateway**

The API Gateway is a proxy server that routes requests from clients on its northbound edge, such as web browsers or the Zowe command line interface, to servers on its southbound edge that are able to provide data to serve the request. It is also responsible for generating the authentication token used to provide single sign-on (SSO) functionality. The API Gateway homepage is <a href="https://<ZOWE\_HOST\_IP>:7554">https://<ZOWE\_HOST\_IP>:7554</a>, that after authentication allows you to navigate to the API Catalog.

### **API Catalog**

The API Catalog provides a list of the API services that have registered themselves as catalog tiles. These allow you to view the available APIs from Zowe's southbound servers as well as test REST API calls.

### **API Discovery**

The API Discovery server acts as the registration service broker between the API Gateway and its southbound servers. It can be accessed through the URL <a href="https://<ZOWE\_HOST\_IP>:7552">https://<ZOWE\_HOST\_IP>:7552</a>. You can view a list of registered API services on the API discovery homepage.

### **Caching service**

The Caching service aims to provide an API which offers the possibility to store, retrieve and delete data associated with keys. The service is used only by internal Zowe applications and will not be exposed to the internet. Its URL is <a href="https://czowe\_HOST\_IP>:7555">https://czowe\_HOST\_IP>:7555</a>. For more information about the Caching service, see its documentation.

### **Caching service**

The Caching service aims to provide an API which offers the possibility to store, retrieve and delete data associated with keys. The service is used only by internal Zowe applications and will not be exposed to the internet. Its URL is <a href="https://closelengthete:https:/

### MVS, JES, and USS UI

Zowe provides a number of rich GUI web applications for working with z/OS. This includes the MVS Explorer for data sets, the JES Explorer for jobs, and the USS Explorer for the Unix File System. You can access them through the Zowe desktop.

The File API server provides a set of REST APIs for working with z/OS data sets and Unix files. These APIs are used by the MVS and USS Explorer apps.

The JES API server provides a set of REST APIs for working with JES. These APIs are used by the JES Explorer application.

Both the File API and JES API servers are registered as tiles on the API catalog, so you can view the Swagger definition and test API requests and responses.

### **Cross memory server**

The Cross memory server is a low-level privileged server for managing mainframe data securely. For security reasons, it is not an HTTP server. Instead, it has a trust relationship with ZSS. Other Zowe components can work through ZSS in order to handle z/OS data that would otherwise be unavailable or insecure to access from higher-level languages and software.

Unlike all of the servers described above which run under the ZWESVSTC started task as address spaces for USS processes, the cross memory server has its own separate started task ZWESISTC and its own user ID ZWESIUSR that runs the program ZWESIS01.

```
Version: v1.25.x LTS
```

# **Frequently Asked Questions**

Check out the following FAQs to learn more about the purpose and function of Zowe™.

- Zowe FAQ
- Zowe CLI FAQ
- Zowe Explorer FAQ

### Zowe FAQ

### What is Zowe?

Click to hide answer

Zowe is an open source project within the Open Mainframe Project that is part of The Linux Foundation. The Zowe project provides modern software interfaces on IBM z/OS to address the needs of a variety of modern users. These interfaces include a new web graphical user interface, a script-able command-line interface, extensions to existing REST APIs, and new REST APIs on z/OS.

### Who is the target audience for using Zowe?

Click to hide answer

Zowe technology can be used by a variety of mainframe IT and non-IT professionals. The target audience is primarily application developers and system programmers, but the Zowe Application Framework is the basis for developing web browser interactions with z/OS that can be used by anyone.

### What language is Zowe written in?

Click to hide answer

Zowe consists of several components. The primary languages are Java and JavaScript. Zowe CLI and Desktop are written in TypeScript. ZSS is written in C, while the cross memory server is written in metal

### What is the licensing for Zowe?

Click to hide answer

Zowe source code is licensed under EPL2.0. For license text click here and for additional information click here.

In the simplest terms (taken from the FAQs above) - "...if you have modified EPL-2.0 licensed source code and you distribute that code or binaries built from that code outside your company, you must make the source code available under the EPL-2.0."

### Why is Zowe licensed using EPL2.0?

Click to hide answer

The Open Mainframe Project wants to encourage adoption and innovation, and also let the community share new source code across the Zowe ecosystem. The open source code can be used by anyone, provided that they adhere to the licensing terms.

# What are some examples of how Zowe technology might be used by z/OS products and applications?

Click to hide answer

The Zowe Desktop (web user interface) can be used in many ways, such as to provide custom graphical dashboards that monitor data for z/OS products and applications.

Zowe CLI can also be used in many ways, such as for simple job submission, data set manipulation, or for writing complex scripts for use in mainframe-based DevOps pipelines.

The increased capabilities of RESTful APIs on z/OS allows APIs to be used in programmable ways to interact with z/OS services.

### What is the best way to get started with Zowe?

#### Click to hide answer

Zowe provides a convenience build that includes the components released-to-date, as well as IP being considered for contribution, in an easy to install package on Zowe.org. The convenience build can be easily installed and the Zowe capabilities seen in action.

To install the complete Zowe solution, see Installing Zowe.

To get up and running with the Zowe CLI component quickly, see Zowe CLI quick start.

### What are the prerequisites for Zowe?

#### Click to hide answer

Prerequisites vary by component used, but in most cases the primary prerequisites are Java and NodeJS on z/OS and the z/OS Management Facility enabled and configured. For a complete list of software requirements listed by component, see System requirements for z/OS components and System requirements for Zowe CLI.

### What's the difference between using Zowe with or without Docker?

#### **Technical Preview**

#### Click to hide answer

Docker is a download option for Zowe that allows you to run certain Zowe server components outside of z/OS. The Docker image contains the Zowe components that do not have the requirement of having to run on z/OS: The App server, API Mediation Layer, and the USS/MVS/JES Explorers.

Configurating components with Docker is similar to the procedures you would follow without Docker, however tasks such as installation and running with Docker are a bit different, as these tasks become Linux oriented, rather than utilizing Jobs and STCs.

**NOTE:** z/OS is still required when using the Docker image. Depending on which components of Zowe you use, you'll still need to set up z/OS Management Facility as well as Zowe's ZSS and Cross memory servers.

### Is the Zowe CLI packaged within the Zowe Docker download?

#### **Technical Preview**

Click to hide answer

At this time, the Docker image referred to in this documentation contains only Zowe server components. It is possible to make a Docker image that contains the Zowe CLI, so additional Zowe content, such as the CLI, may have Docker as a distribution option later.

If you are interested in improvements such as this one, please be sure to express that interest to the Zowe community!

### Does ZOWE support z/OS ZIIP processors?

#### Click to hide answer

Only the parts of Zowe that involve Java code are ZIIP enabled. The API Mediation Layer composed of the API Gateway, Discovery and Catalog servers along with any Java-based services that work with them such as the Jobs and Datasets servers are ZIIP enabled. Also, the CLI and VSCode Explorer make large use of z/OSMF, which is Java so they are ZIIP enabled as well. More details on portions of Zowe which are Java (ZIIP) enabled can be found here.

This leaves C and NodeJS code which are not ZIIP enabled, BUT, we have a tech preview available currently that allows execution of Java as well as NodeJS code, on Linux or zLinux via Docker. With the tech preview, only the C code remains on z/OS, which is not ZIIP enabled.

### How is access security managed on z/OS?

Click to hide answer

Zowe components use typical z/OS System authorization facility (SAF) calls for security.

### How is access to the Zowe open source managed?

#### Click to hide answer

The source code for Zowe is maintained on an Open Mainframe Project GitHub server. Everyone has read access. "Committers" on the project have authority to alter the source code to make fixes or enhancements. A list of Committers is documented in Committers to the Zowe project.

### How do I get involved in the open source development?

#### Lick to hide answer

The best way to get started is to join a Zowe Slack channel and/or email distribution list and begin learning about the current capabilities, then contribute to future development.

For more information about emailing lists, community calendar, meeting minutes, and more, see the Zowe Community GitHub repo.

For information and tutorials about extending Zowe with a new plug-in or application, see Extending on Zowe Docs.

### When will Zowe be completed?

Lick to hide answer

Zowe will continue to evolve in the coming years based on new ideas and new contributions from a growing community.

### Can I try Zowe without a z/OS instance?

#### Click to hide answer

IBM has contributed a free hands-on tutorial for Zowe. Visit the Zowe Tutorial page to learn about adding new applications to the Zowe Desktop and and how to enable communication with other Zowe components.

The Zowe community is also currently working to provide a vendor-neutral site for an open z/OS build and sandbox environment.

Zowe is also compatible with IBM z/OSMF Lite for non-production use. For more information, see Configuring z/OSMF Lite on Zowe Docs.

### **Zowe CLI FAQ**

# Why might I use Zowe CLI versus a traditional ISPF interface to perform mainframe tasks?

#### Click to hide answer

For developers new to the mainframe, command-line interfaces might be more familiar than an ISPF interface. Zowe CLI lets developers be productive from day-one by using familiar tools. Zowe CLI also lets developers write scripts that automate a sequence of mainframe actions. The scripts can then be executed from off-platform automation tools such as Jenkins automation server, or manually during development.

### With what tools is Zowe CLI compatible?

#### Lick to hide answer

Zowe CLI is very flexible; developers can integrate with modern tools that work best for them. It can work in conjunction with popular build and testing tools such as Gulp, Gradle, Mocha, and Junit. Zowe CLI runs on a variety of operating systems, including Windows, macOS, and Linux. Zowe CLI scripts can be abstracted into automation tools such as Jenkins and TravisCI.

### Where can I use the CLI?

Click to hide answer	
Usage Scenario	Example

Usage Scenario	Example
Interactive use, in a command prompt or bash terminal.	Perform one-off tasks such as submitting a batch job.
Interactive use, in an IDE terminal	Download a data set, make local changes in your editor, then upload the changed dataset back to the mainframe.
Scripting, to simplify repetitive tasks	Write a shell script that submits a job, waits for the job to complete, then returns the output.
Scripting, for use in automated pipelines	Add a script to your Jenkins (or other automation tool) pipeline to move artifacts from a mainframe development system to a test system.

# Which method should I use to install Zowe CLI?

📖 Click to hide answer

You can install Zowe CLI using the following methods:

- Local package installation: The local package method lets you install Zowe CLI from a zipped file that contains the core application and all plug-ins. When you use the local package method, you can install Zowe CLI in an offline environment. We recommend that you download the package and distribute it internally if your site does not have internet access.
- **Online NPM registry:** The online NPM (Node Package Manager) registry method unpacks all of the files that are necessary to install Zowe CLI using the command line. When you use the online registry method, you need an internet connection to install Zowe CLI

# How can I get help with using Zowe CLI?

- You can get help for any command, action, or option in Zowe CLI by issuing the command 'zowe -help'.
- For information about the available commands in Zowe CLI, see Command Groups.
- If you have questions, the Zowe Slack space is the place to ask our community!

# How can I use Zowe CLI to automate mainframe actions?

Click to hide answer

- You can automate a sequence of Zowe CLI commands by writing bash scripts. You can then run your scripts in an automation server such as Jenkins. For example, you might write a script that moves your Cobol code to a mainframe test system before another script runs the automated tests.
- Zowe CLI lets you manipulate data sets, submit jobs, provision test environments, and interact with mainframe systems and source control management, all of which can help you develop robust continuous integration/delivery.

# How can I contribute to Zowe CLI?

Click to hide answer

As a developer, you can extend Zowe CLI in the following ways:

- Build a plug-in for Zowe CLI
- Contribute code to the core Zowe CLI
- Fix bugs in Zowe CLI or plug-in code, submit enhancement requests via GitHub issues, and raise your ideas with the community in Slack.

Note: For more information, see Developing for Zowe CLI.

# **Zowe Explorer FAQ**

# Why might I use Zowe Explorer versus a traditional ISPF interface to perform mainframe tasks?

#### Click to hide answer

The Zowe Explorer VSCode extension provides developers new to the mainframe with a modern UI, allowing you to access and work with the data set, USS, and job functionalities in a fast and streamlined manner. In addition, Zowe Explorer enables you to work with Zowe CLI profiles and issue TSO/MVS commands.

### How can I get started with Zowe Explorer?

#### Click to hide answer

First of all, make sure you fulfill the following Zowe Explorer software requirements:

- Get access to z/OSMF.
- Install Node.js v8.0 or later.
- Install VSCode.
- Configure TSO/E address space services, z/OS data set, file REST interface, and z/OS jobs REST interface. For more information, see z/OS Requirements.

Once the software requirements are fulfilled, create a Zowe Explorer profile.

#### Follow these steps:

- 1. Navigate to the explorer tree.
- 2. Click the + button next to the DATA SETS, USS, or JOBS bar.
- 3. Select the **Create a New Connection to z/OS** option.
- 4. Follow the instructions, and enter all required information to complete the profile creation.

You can also watch Getting Started with Zowe Explorer to understand how to use the basic features of the extension.

#### Where can I use Zowe Explorer?

Lick to hide answer

You can use Zowe Explorer either in VSCode or in Theia. For more information about Zowe Explorer in Theia, see the Theia Readme.

### How do I get help with using Zowe Explorer?

Click to hide answer

- Use the Zowe Explorer channel in Slack to ask the Zowe Explorer community for help.
- Open a question or issue directly in the Zowe Explorer GitHub repository.

### How can I use Secure Credential Store with Zowe Explorer?

Lick to hide answer

Activate the Secure Credential Store plug-in in Zowe Explorer.

#### Follow these steps:

- 1. Open Zowe Explorer.
- 2. Navigate to the VSCode settings.
- 3. Open Zowe Explorer Settings.
- 4. Add the **Zowe-Plugin** value to the Zowe Security: Credential Key entry field.
- 5. Restart VSCode.
- 6. Create a profile.

Your Zowe Explorer credentials are now stored securely.

For more information, see the Enabling Secure Credential Store page.

#### How can I use FTP as my back-end service for Zowe Explorer?

Check out the GitHub article about the FTP extension with the information on how to build, install, and use FTP as your back-end service for working with Unix files.

# How can I contribute to Zowe Explorer?

Lick to hide answer

As a developer, you may contribute to Zowe Explorer in the following ways:

- Build a Zowe Explorer extension.
- Contribute code to core Zowe Explorer.
- Fix bugs in Zowe Explorer, submit enhancement requests via GitHub issues, and raise your ideas with the community in Slack.

Note: For more information, see Extending Zowe Explorer.

# Version 1.25 (October 2021)

Welcome to the Version 1.25.0 release of Zowe!

To see a full list of release enhancements and fixes, see New features and enhancements and Bug fixes.

**Release demo:** Join the Zowe System Demo on November 1 to see a demo of what's new in this release, and ask the community questions. Check out the Zowe calendar for detailed call-in information.

**Download v1.25.0 build:** Want to try new features as soon as possible? You can download the v1.24.0 build from Zowe.org.

# **Notable changes**

#### **Running Zowe in Kubernetes**

With v1.25.0 release, Zowe provides new downloadable zowe-containerization-1.25.0.zip to help you deploy Zowe into Kubernetes cluster. Check the Zowe architecture when running in Kubernetes cluster section to learn more about architecture differences, and follow instructions in Installing Zowe containers to deploy.

# New features and enhancements

### Zowe installation and packaging

- Deprecating Node.js SDK for z/OS version 8 #2364
- Optional activating class CDT in ZWESECUR JCL #2353

- Add controller for public key provisioning. This feature makes it possible to retrieve public keys to verify JWT tokens. (#1824) (5acb9e9), closes #1824
- Per service configuration to direct the API Gateway to add headers. This feature enables APIML to add or override headers in responses. (#1812) (25bbdbe), closes #1812

- Per service configuration to ignore certain headers on the API Gateway. This feature makes it possible to select which headers are stripped from requests that go through the Gateway to a particular service. (#1806) (b258732), closes #1806
- Certificate authentication for static API refresh endpoint. This feature makes it possible to authenticate via certificates for the static refresh endpoint in the API Catalog. (#1782) (d4a91b0), closes #1782
- Server Sent Events Handler for accessing Turbine SSE events through API Gateway. This feature enables the Gateway to route server-sent events. (#1723) (9bea501), closes #1723
- Service onboarding Wizard improvements (#1772) (20dd70b), closes #1772
- Controllers are now provided which makes it possible to delete the static definition file. (#1759) (e4c22dc), closes #1759
- Provide compression for specific paths only. It is now possible to delegate compression of a response to the API ML while limiting the paths that are compressed. (#1755) (cc612e5), closes #1755
- Static API enpoints protected by SAF check. Static API definition files are now only available to authorized users. (#1764) (e2d95df), closes #1764
- Static Definition creation endpoints in API Catalog. Controllers are now provided which make it possible to either create or override the static definition file. (#1735) (2976db5), closes #1735
- Service onboarding Wizard Automatic registration of static definition. Static definitions now can be automatically onboarded. (#1751) (3228249), closes #1751
- Service onboarding Wizard can now produce NodeJS & Micronaut enablers configurations. Configuration files have been added for the NodeJS and Micronaut onboarding methods. (#1733) (1e077e8), closes #1733
- Service onboarding Wizard UX tweaks have been introduced to improve Wizard usablity. (#1752) (47c5414), closes #1752

### **Zowe Application Framework**

- Unified container and non-container behavior. Changed how app-server scripts locate app-server directories so that they work in container mode, where the folder layout is different.
- If the hostname is not explicitly specified, use GATEWAY\_HOST environment variable over ZOWE\_EXPLORER\_HOST to find mediation layer gateway.
- Zlux Server Framework improved callRootService when targeting agents such as ZSS to issue the direct request to destination rather than using an additional loopback request to the app-server. This improves performance, reduces the need for the app-server being a client of itself, and allows for more request options when calling the agent.
- Allowed timeout parameter to be specified in a callService or callRootService command, such as when needing a long timeout to request an agent response.

- Removed the requirement for app-server to be a client of itself when using the callService API by adding the option for requests to this API to be executed that is internal to app-server. This option is compatible with the pre-existing use of callService however, it is disabled by default to avoid disruption. You can enable it by setting the server configuration property node.internalRouting=true.
- Allowed new pluginDefinition webContent destination variable for substitution,
   ZWE\_EXTERNAL\_PORT that matches the environment variable value, or if absent, the gateway or appserver ports conditional to configuration.
- App-server's uninstall-app.sh script is now available in the instance bin folder.
- Zss's zis-plugin-install.sh script is now available in the instance bin/utils folder.
- Added an endpoint for PassTicket generation.
- Added an endpoint for user information.
- Added method to read and set loglevel of dataservices.
- Updated material UI.
- Updated webpack build and dev configuration.

The following enhancements were added to the Editor:

- Added previously selected content comparison (Diff viewer).
- Removed the Cancel button and replaced it with 'X' button on all dialogue pop-ups.
- Added toggle bar to show and hide File Explorer.

# Zowe CLI

The following enhancements were added to the **core CLI**:

- Removed the misleading workflow-name option for the zowe zos-workflows list definition-file-details help example. #659
- Exposed new option modifyVersion for the zowe zos-jobs delete job and zowe zosjobs cancel job commands. #1092
- Add support for PEM certificate based authentication.
- Update post-install script to display a message when the CLI successfully installs due to increased error messaging from USS SDK when optional pre-requisites are not installed.

The following enhancement was added to the **Imperative CLI Framework**:

- Export the Imperative Command Tree on the data object of the zowe --ac command when --rfj is specified.
- Implemented the ability to authenticate using client certificates in PEM format.

# **Zowe Explorer**

- Added a check to ensure that a base profile exists before running the function that combines base and service profiles #1500.
- Added Imperative logger access for extenders #1433.
- Added documentation for Imperative logger for extenders #1467.
- Implemented separate console windows for TSO and MVS commands #1478.

# Zowe JES/MVS/USS Explorers

• Replaced the File APIs with z/OSMF APIs

# **Bug fixes**

- Add handling in case of PassTicketException (#1810) (f962361), closes #1810
- Add https://\${ZOWE\_EXTERNAL\_HOST}:\${ZWE\_EXTERNAL\_PORT} to ZAF API Catalog pluign definition (#1829) (6527a32), closes #1829
- api-catalog app failed to load in desktop if Gateway service is registered as NodePort (#1827) (ec45915), closes #1827
- Add ZAF pluginDefinition.json to API Catalog package (#1822) (4745548), closes #1822
- Define appfwPlugins instead of desktoplframePlugins for API Catalog ZAF plugin definition (#1814) (371cc0b), closes #1814
- Periodically update the Gateway url during Gateway Lookup (#1817) (7016ea5), closes #1817
- PJE enabler sample and password validation fixes (#1819) (45a4001), closes #1819
- Display multiple APIs with multiple different versions in API catalog (#1800) (6400aa3), closes #1800
- Handle API Catalog errors during parsing apiversions and wrong URLs in service definition (#1788) (7a0346f), closes #1788
- Support for ZOSMF APAR PH34201 (#1795) (5503e4b), closes #1795
- Fix flaky unit test (#1771) (58d9656), closes #1771

- API Catalog static definition file generation (#1761) (b6790cb), closes #1761
- ZAAS client to not send a certificate during authentication requests (#1763) (691036a), closes #1763

# **Zowe Application Framework**

- Fixed an issue with using app2app where incorrectly formatted data would not honor launch/message requesthp.
- app-server would ignore when VERIFY\_CERTIFICATE=false was set, and try to verify APIML servers. This would lead to login failures when APIML server was on a different system than app-server. Now, app-server will verify APIML certificates based on VERIFY\_CERTIFICATE value.
- Fixed an issue where app-server could throw an uncaught exception when a proxied server had a socket error.

The following bugs were fixed in the Editor:

- Fixed an issue where switching from the Diff viewer to code editing body causes rendering bugs.
- Fixed an issue when fileCopy incorrectly processed files tagged as binary and mixed.
- Fixed an issue where Unixfile Copy and Rename API doesn`t support distinct error status response.
- Fixed an issue where dataset contents API returns invalid error status for undefined length dataset update request.
- Fixed an issue where Unixfile Copy service incorrectly processed files tagged as binary and mixed.
- Fixed an issue where Unixfile Copy and Rename directory API does not support forceOverwrite query.
- Fixed the error message and phantom tab when opening undefined length dataset.

# Zowe CLI

The following bugs were fixed in **core Zowe CLI**:

- Reverts hiding the cert-key-file path so users can see what path was specified and check if the file exists.
- Updated dependencies to resolve problems with the ansi-regex package.

#### The following bug was fixed in the **Imperative CLI Framework**:

 Reverts hiding the cert-key-file path so users can see what path was specified and check if the file exists

- Updated dependencies to resolve problems with the ansi-regex package
- Updated js-yaml to resolve a potential security issue

The following bug was fixed in the **z/OS FTP Plug-in**:

• Fixed Windows path problem when using delete uss-file command.

# **Zowe Explorer**

- Fixed the bug that caused the check credentials pop-up to disappear too quickly #1486
- Fixed the bug that kept the command text box while escaping the process of entering a TSO command. Now the command text box does not pop up if you cancel entering a TSO command #1479. Thanks
   @katelynienaber
- Fixed the bug that caused issues with deleting data set members in Ecplipse Theia or Che #1487
- Fixed the bug that caused the deletion of selected data sets while removing a single data set member by using the right-click action. #1483

# Version 1.24 (September 2021)

Welcome to the Version 1.24.0 release of Zowe!

To see a full list of release enhancements and fixes, see New features and enhancements and Bug fixes.

Release demo: Watch the Zowe v1.24 System Demo to see a demo of what's new in this release.

**Download v1.24.0 build:** Want to try new features as soon as possible? You can download the v1.24.0 build from Zowe.org.

# **New features and enhancements**

## Zowe installation and configuration

- We have removed Technical Preview badges related to high availability. Any feedbacks related to this feature are always welcome.
- These new utility tools are added to instance bin/utils directory: zowe-installcomponent.sh and zowe-configure-component.sh. They are convenience links of similar utility tools existing in runtime bin/utils directory.
- Improve error handling and add more user-friendly error messages when jar command is not in PATH PR#2314

- SAF resource access controller that allows the authorized user to query the SAF resource access levels (#1734) (680f4b9), closes #1734
- Compress routed response with GZIP based on the routed service's preference (#1728) (85b5948), closes #1728
- Introduce REST provider for SAF IDT tokens (#1714) (047c54e), closes #1714
- Refresh endpoint for prolonging a valid JWT token (#1719) (f918916), closes #1719
- Introduce error codes for SAF authentication (#1692) (89ac5a2), closes #1692
- Support SAF IDT as the authentication scheme. The application now properly recognizes the scheme and fills the X-SAF-Token header with the token produced by the SafAuthenticationService

(#1688) (26a84c0), closes #1688

- Conditional full debug logging for API Mediation Layer (#1662) (81bc46f), closes #1662
- AT-TLS aware API Mediation Layer. API ML now provides the same functionality to clients when TLS is handled by the z/OS Communication Server. (#1621) (be26a9a), closes #1621
- Distributed authentication based load balancing (#1602) (4e7d993), closes #1602
- Add support for stomp v1.2 websocket protocol (#1697) (d1057e0), closes #1697

# **Zowe App Server**

- Add ciphers for use with TLS 1.3
- sso-auth plugin now sends error.body containing a server's error response so that it can be shown in browser if appropriate
- Version numbers of plugins are shown when loading, even if loading failed.
- Added the ability to refresh the file properties in File Tree, when an already exiting untagged file is saved with an encoding type.
- Added the ability to use the latest USS encoding when saving an exiting file.
- USS Explorer: Replaced the File APIs with zOSMF APIs #131

### Zowe CLI

The following enhancements were added to the core CLI:

- Exposed new option start for the zowe zos-files list data-set command. #495
- Updated Imperative to add the following features:
  - Improved command suggestions for mistyped commands, add aliases to command suggestions
  - The plugins validate command will return an error code when plugins have errors if the new --fail-on-error option is specified. Also adds --fail-on-warning option to return with an error code when plugins have warnings. #463
- Renamed the zos-files --responseTimeout option to --response-timeout in help docs for consistency. #803

The following enhancement was added to the **Imperative CLI Framework**:

- Improved command suggestions for mistyped commands, add aliases to command suggestions
- The plugins validate command will return an error code when plugins have errors if the new -- fail-on-error option is specified. Also adds --fail-on-warning option to return with an error

code when plugins have warnings. #463

The following enhancement was added to the **Db2 Plug-in**:

• Update ibm\_db dependency to support Node v16 #82

The following enhancement was added to the **z/OS FTP Plug-in**:

- Support listing USS files with file name pattern containing \*.
- Support listing loadlib members
- Clear password error message
- Support listing jobs without default prefix \*.

# **Zowe Explorer**

- Improved integration tests for greater efficiency #1430
- Added a reminder to the PR template to create a PR from master to next after PR is merged into master branch #1446
- Added @zowe/cli dependency to API #1445
- Added the ability to register custom profile types in **ProfilesCache** for extenders #1419
- Added the ability to pass account and other information from tso profile #1378
- Added profiles cache to extenders #1390

# **Bug fixes**

# Zowe installation and configuration

- Support of node.js v14.17.2 is excluded due to encoding issues we noticed. Please check System requirements Node.js
- Fixes issue on ZWEN0SS0 jcl that permission is removed before DELT0KEN command PR#2310 fixes issue #2309

- Configurable timeout to verify the zOSMF availability (#1738) (82fa3bf), closes #1738
- Exclude tls\_rsa ciphers for Websocket client (#1737) (df013bf), closes #1737

- Hide log messages with no value (#1744) (50cff16), closes #1744
- PerServiceGzipFilter checks for correct URI pattern (#1732) (b7ae93f), closes #1732
- Add agentkeepalive dependency to Catalog frontend because of failing build (#1698) (7f6db61), closes #1698
- Correctly handle websocket connections for new path pattern (#1701) (2db9a7e), closes #1701
- Prevent API ML run with unsecure connection in AT-TLS mode (#1689) (2139218), closes #1689
- Accommodating keystore parameters with spaces (#1676) (a784d26), closes #1676
- Discovery health and info endpoints: authentication and enablement (#1612) (b52d076), closes #1612
- Serve swagger url over http in Gateway HTTP mode (#1646) (3b35a10), closes #1646
- Load balancer remote cache fixes (#1636) (129b33c), closes #1636
- QueryTest typo in class name (#1634) (a040847), closes #1634
- Reuse jetty client (#1658) (11d575a), closes #1658
- Publish spring onboarding enabler in format consistent with other projects (#1608) (dac35b1), closes #1608

# **Zowe App Server**

- IP Explorer was not installed upon upgrade, only on new installs.
- Fix zis-plugin-install.sh script to properly exit on error with extended-install
- Fixed issue where server could not bind to a hostname value for node.https.ipAddresses
- Fixed issue where if the server started slowly, a timeout at cluster storage setup could be encountered.
- Fix no agent section causing server error (makes trivial-auth work)

# Zowe CLI

The following bugs were fixed in **core Zowe CLI**:

- Fixed capitalization of handler paths for zowe files rename ds and zowe files rename dsm commands.
- Fixed regression where characters are not correctly escaped in web help causing extra slashes ("\") to appear. #644

The following bug was fixed in the **Imperative CLI Framework**:

 Fixed regression where characters are not correctly escaped in web help causing extra slashes ("\") to appear. #644

# **Zowe Explorer**

- Fix for the issue that caused mismatching of GitHub VSIX Zowe Explorer releases #1442
- Status icons now reset when refreshing the explorer views #1404
- Fixed the issue that prevented the expected error message No valid value for z/OS URL.
   Operation Cancelled from being displayed while escaping the host text box during the creation or update of a profile #1426
- Fixed the issue that invoked profile validation before updating a profile. Now a profile is validated only after the update #1415
- Fixed the issue of Zowe profiles encoding value when opening a USS file in the text editor #1400

# **Known Issues**

• API Catalog app cannot be loaded from Zowe Desktop in Sysplex deployment

# Version 1.23 (July 2021)

Welcome to the Version 1.23.0 release of Zowe!

To see a full list of release enhancements and fixes, see New features and enhancements and Bug fixes.

Release demo: Check out the Zowe demo video for v1.23 to see a demo of what's new in this release.

**Release blog:** Read this blog Zowe 1.23 Release Highlights written by Joe Winchester for a deeper dive of the major enhancements and changes for this release.

**Download v1.23.0 build:** Want to try new features as soon as possible? You can download the v1.23.0 build from Zowe.org.

# New features and enhancements

- Authentication based server-side load balancing. A service can now configure itself with the Authentication-based load balancing scheme whereby a user is directed to the same instance of a service for a given period of time (#1576) (4ad382e), closes #1576.
- Catalog: authenticate with client certificate for /apidoc/\*\* endpoints (#1568) (79dedfd), closes #1568

- Gateway: authenticate with client certificate for /gateway/services/\*\* endpoint (#1568) (d0d7b0af92de20fe606076e90f48604018cdf099), closes #1568
- Make cookie samesite configurable. The configuration parameter apiml.auth.cookieProperties.cookieSameSite makes it possible for users to configure the SameSite attribute of the apimlAuthenticationToken cookie (#1545) (135904c), closes #1545
- Services can now configure their desired load balancer behavior (#1536) (db0c070), closes #1536

## **Zowe App Server**

- Automatically create APIML static definition for ZSS when app-server is running in Docker.
- Disable impersonation for OMVS Service.
- Any HA incompatible security plugins are disabled if Zowe runs in HA mode.
- Updated proxy utility to treat PATCH similarly to PUT and POST
- Cleanup: Removed 'x-powered-by' header
- Get list of Discovery Services using environment variable, and provide the list for Eureka JS Client, in order to have it failover connection to the next one on the list when the one it's currently talking to fails.

### Zowe CLI

The following enhancements were added to the core CLI:

- Expanded help text of --data-set-type on create data set command by adding an example of creating PDSE. #52
- Added a --volume-serial option to the zowe zos-files list data-set command. Use this option to filter data sets by volume serial. #61
- Removed 'z/OS' from zos-files help upload and download commands. #60
- Added new aliases for zos-files commands in delete, download, and list relating to USS files. You can now interact with uf or uss. #983

The following enhancement was added to the Imperative CLI Framework:

Improved the way that HTTP response chunks are saved, reducing time complexity from O(n<sup>2</sup>) to O(n).
 This dramatically improves performance for larger requests. #618

### **Zowe Explorer**

- Added the feature that automatically includes a missing profile in the Jobs view when submitting a job.
   #1386
- Added the extender documentation for KeytarApi for Secure Credential Store. #1384
- Added a new setting that enables you to hide Zowe Explorer's temporary downloads folder from a workspace. #1373
- Added the command to refresh a particular job and get the latest information and content for its spool files. #1363
- Added the function that enables you to delete multiple datasets and data set members. #1323
- Added the feature that enables you to use multiple VS Code windows for files opened via Zowe Explorer. #1347
- Added the command to refresh USS directory file names without the entire tree collapsing. #1369
- Added the refresh data set member names option. You can now retrieve a new list of members from the mainframe. #1343
- Added the best practice documentation for error handling. #1335
- Added the developer guide for adding commands to core Zowe Explorer menus. #1332
- Standardized context group names. #1340

# **Bug fixes**

# **Zowe API Mediation Layer**

- Fix login error handling when auth service is not available (#1579) (1221573), closes #1579
- Handle multiple discovery service instances in static refresh (#1582) (d7237ce), closes #1582
- Improve redis configuration for users (#1589) (b1f7088), closes #1589
- Properly display API Catalog status on Gateway homepage (#1581) (b8dd9cd), closes #1581
- Change order of authentication filters on Login endpoint (#1526) (3b93e9b), closes #1526
- Wrong use of certificates in ZAAS client (#1514) (964c4fa), closes #1514

# **Zowe App Server**

- Sync state of certificate verification of zlux with keystore configuration, so that certificate verification can be turned on or off centrally.
- relativeTo parsing may have failed depending upon path length and contents, leading to skipped plugin loading.

- HTTP server did not send empty files correctly.
- Removed warning ZWED0144W about failure to read keyrings by having terminal proxy read the tls options loaded by the server instead of loading twice.
- Dynamic plugins could not be loaded due to parameter mismatch.

# Zowe CLI

The following bugs were fixed in **core Zowe CLI**:

- Fixed inconsistencies in punctuation for command descriptions by adding missing periods. #66
- Updated Imperative version to fix web help issues.

The following bugs were fixed in the **Imperative CLI Framework**:

- Added missing periods at the end of command group descriptions for consistency. #55
- Fixed web help examples description typo at line 440 in packages/cmd/src/CommandPreparer.ts. #612
- Fixed Markdown special characters not being escaped in web help for descriptions of positional options and examples. #620
- Fixed subgroups not being displayed under their own heading in web help. #323

The following bug was fixed in the **Secure Credential Store Plug-in**:

• Updated the Keytar dependency to v7.7 to be compatible with Node.js v16.

# **Zowe Explorer**

- Removed non-functioning code from invalid credentials for Theia #1371
- Fixed the issue with USS Search and Update Profile errors for profiles without credentials #1391
- Fixed the error message that popped up when accessing a profile from Favorites #1344
- Fixed the issue that prevented the Allocate Like feature from working correctly #1322

# **Previous versions**

Learn about what is new, changed, or removed in Zowe™ in version 1.22.0 and earlier.

- Version 1.22.0 LTS (June 2021)
- Version 1.21.0 LTS (April 2021)
- Version 1.20.1 LTS (March 2021)
- Version 1.20.0 LTS (March 2021)
- Version 1.19.1 LTS (February 2021)
- Version 1.19.0 LTS (February 2021)
- Version 1.18.0 LTS (January 2021)
- Version 1.17.0 LTS (November 2020)
- Version 1.16.0 LTS (October 2020)
- Version 1.15.0 LTS (September 2020)
- Version 1.14.0 LTS (August 2020)
- Version 1.13.0 LTS (July 2020)
- Version 1.12.0 LTS (June 2020)
- Version 1.11.0 LTS (May 2020)
- Version 1.10.0 LTS (April 2020)
- Version 1.9.0 LTS (February 2020)
- Version 1.8.1 (February 2020)
- Version 1.8.0 (February 2020)
- Version 1.7.1 (December 2019)
- Version 1.7.0 (November 2019)
- Version 1.6.0 (October 2019)
- Version 1.5.0 (September 2019)
- Zowe SMP/E Alpha (August 2019)
- Version 1.4.0 (August 2019)
- Version 1.3.0 (June 2019)
- Version 1.2.0 (May 2019)
- Version 1.1.0 (April 2019)
- Version 1.0.1 (March 2019)

• Version 1.0.0 (February 2019)

# Version 1.22.0 LTS (June 2021)

Welcome to the Version 1.22.0 release of Zowe! You can find some of the highlights included in this release in the **Notable changes** section. To see a full list of release enhancements and fixes, see **New features and enhancements** and **Bug fixes**.

**Blog and video:** Check out this blog that summarizes some of the major enhancements and changes for this release. You can also watch a video on Open Mainframe Project's Youtube Channel see a demo of what's new in this release.

**Download v1.22.0 build:** Want to try new features as soon as possible? You can download the v1.22.0 build from Zowe.org.

### **Notable changes**

#### Configure Zowe for high availability (Technical Preview)

You can deploy Zowe in Parallel Sysplex for high availability with several enhancements shipped with v1.22.0 release.

- By deploying Zowe in Sysplex, comparing to a single instance of Zowe, you are configuring and starting multiple Zowe instances. See how Zowe architecture is changed with high availability.
- In addition to the instance.env file that is used to configure Zowe, now you can use a new YAML configuration file zowe.yaml to configure multiple Zowe instances in more granular level. See Updating the zowe.yaml configuration file for more information.
- The new ZWESLSTC started task can monitor status of microservices running within Zowe and restart the missing microservice(s) when needed. See Configure ZWESLSTC to run Zowe High Availability under ZWESVUSR user ID for more information.

To get started with Zowe high availability, see Zowe high availability installation roadmap.

#### New tool for verifying an installed Zowe server component (Technical Preview)

You can verify an installed Zowe server component (extension) for a Zowe instance by using the bin/zowe-verify-component.sh tool that Zowe ships in this release. The zowe-verifycomponent.sh tool checks and verifies whether a specified component is up and running. You can use it to verify both core and external Zowe components. This tool is for technical preview now and we are happy to hear any feedback.

For more information, see Verify with zowe-verify-component.sh.

# New features and enhancements

#### Zowe API Mediation Layer

- Deterministic routing based on the provided headers is now available. Clients can now specify which instance of a service the user should be routed to. This enables reusability of underlying resources such as LPARs associated with a specific service instance (#1496) (ed91f25), closes #1496.
- Basic authentication via Websocket is now fully supported (#1482) (112da99), closes #1482.
- Passwords can be changed via SAF. An endpoint is exposed allowing users to change passwords using this API ML endpoint (#1471) (3f3c2af), closes #1471.
- A self-service application is now available that can run in the infrastructure of the user to verify whether certificates are properly created and configured (#1441) (e694c0f), closes #1441

#### Zowe App Server

- Plugins can push state out to the Caching Service for high availability storage via a storage API, available to dataservices as remoteStorage
- Plugins can push state out to the In-Memory Storage via a storage API, available to dataservices as localStorage
- Add "remoteStorage" pointer to dataservice struct, for accessing high availability remote storage in addition to or alternatively to local storage.
- Plugins can push state out to the Caching Service for high availability storage via a improved storage API, available to dataservices as context.storage
- Storage API V2 added which has parameters to specify whether plugin cache and state should be stored local to a worker, in the cluster, or remote for high availability
- Decrease verbosity and duplication of startup logs. Log messages omitted have been moved to debug messaging.
- Change missing swagger warning message to debug as it is a warning for developers, not for end users.

#### Zowe CLI

The following enhancements were made to the FTP Plug-in:

- Added retcode in the output of the view job-status-by-jobid and submit command to be consistent with ZOSMF plugin.
- Added --rdw to download dataset command to download variable-length dataset.

#### **Zowe Explorer**

- Added the refresh data set member names option. You can now retrieve a new list of members from the mainframe. #1343
- Added the best practice documentation for error handling. #1335
- Added the developer guide for adding commands to core Zowe Explorer menus. #1332
- Standardized context group names. #1340

#### Zowe JES/MVS/USS Explorers

The following enhancements were added to the **MVS Explorer**:

- Updated material ui
- Updated webpack build and dev config

The following enhancements were added to the USS Explorer:

- Updated material ui from 0.18 to 4.x, react from v15 to v16
- Updated webpack config for local build config
- Updated packages for security updates

# **Bug fixes**

#### Zowe installation and configuration

- Several issues related to ZWEKRING #2089 and ZWESSOTK #2144 sample JCLs are fixed with #2101.
- Fixed issue #2120 about handling external certificate authorities when using keyring.
- Fixed several issues described in #1976 related to install and configuration when z/OSMF is absent.

- Use the apiml.service.id in the API Catalog as used in other services. (#1475) (7bc8f99), closes #1475
- Change the registration to use the correct hostname in instanceId (#1473) (1d6caa8), closes #1473

- The HTTP client is not closed when generating a passticket. The ZAAS client can now reuse connections and provide correct login with passtickets (#1470) (ed9f929), closes #1470.
- Configurable jwt alias at startup via environment variable (#1442) (0e3df7a), closes #1442
- Use the actual hostname instead of the one provided by Spring Cloud (#1434) (6b8c38a), closes #1434
- Distinguish lib and fat jars (#1398) (f771a40), closes #1398
- Accept list of Discovery services in the Catalog. If the Catalog fails to contact to the Discovery service, the Catalog tries to contact another service from the list (#1376) (42ae70d), closes #1376

#### Zowe App Server

- Prefer internal IP/hostname over external one when stating to discovery server where app-server is located. For many users there is no behavior difference because the values are the same.
- Dataset contents API doesn't skip empty records while reading a dataset
- ZSS now takes into account relativeTo attribute when loading plugin dlls
- Dataservice loading did not warn if program control was missing, which is essential, so plugin loading would fail silently in that case.
- Fix /server/agent route when using APIML
- Fix issue with CORS rejection when accessing zss through APIML gateway

#### Zowe CLI

The follow bug was fixed in **Zowe CLI**:

• Ensured that the like field will always be added to all allocate like requests. #1017

#### The following bugs were fixed in the **Secure Credential Store Plug-in**:

- Updated the Keytar and prebuild-install dependencies to make offline install possible for npm@7 users.
- Updated the Keytar dependency to v7.7 to be compatible with Node.js v16.

The following bugs were fixed in the **Imperative CLI Framework**:

- Fixed active command tree item not updating in web help when scrolling. #425
- Fixed main page of web help not staying scrolled to top of page when loaded. #525

#### The following bug was fixed in the **FTP Plug-in**:

• Expose meta data for Zowe Explorer FTP extension.

#### **Zowe Explorer**

- Fixed the error message that popped up when accessing profiles from Favorites. #1344
- Fixed the issue that prevented the Allocate Like feature from working correctly. #1322

# Version 1.21.0 LTS (April 2021)

Check out this blog that summarizes some of the major enhancements and changes for this release. You can also watch a video on Open Mainframe Project's Youtube Channel see a demo of what's new in this release.

### New features and enhancements

#### Zowe installation and configuration

- Introduced a new non-strict verify certificates mode which can be customized as
   NONSTRICT\_VERIFY\_CERTIFICATES in zowe-setup-certificates.env
   Comparing to strict
   VERIFY\_CERTIFICATES mode, this non-strict mode will not validate certificate Common Name or
   Subject Alternative Name (SAN). However, Zowe will still validate if the certificate authorities are trusted in the trust store. This change was introduced with issue zowe/api-layer#1334 and fixed by #2062.
- Added two new JCLs (ZWESSKTK and ZWEN0SS0) to the PDS sample library SZWESAMP.
   ZWESSKTK can be used to create SSO PKCS#11 token and set up required security configurations.
   ZWEN0SS0 can be used to remove the PKCS#11 token and related security changes. This issue is described in zowe-install-packaging#2052 and fixed by #2094.
- Reduced the amount of checking of Java and node levels. #1997, #2063
- Added a list to the ZWESECUR JCL for the client cert PERMIT to match the other RACF commands. #1971, #2063

- The dockered deployment of Zowe now supports Redis as an off-platform storage for the Caching service. (a7f4ad), #1128
- Configuration of the API ML run is now permitted where the hostname in the certificate is not verified in a strict manner. The certificate Common Name or Subject Alternate Name (SAN) are not checked. This facilitates deployment to Marist when certificates are valid but do not contain a valid hostname. This configuration is for development purposes only and should not be used for production. (2da761a), #1334

- Caching service: The alphanumeric constraint for keys stored in the service has been removed. (237420)#1317
- An endpoint has been added to delete all keys for a specific service. (0c3e01), #1253

#### Zowe App Server

- app-server now supports reaching ZSS through TLS without the need for AT-TLS, by reading new properties within the "agent" config #151
- Synchronize user preference setting for TLS verification so that app-server matches the value used by APIML; VERIFY\_CERTIFICATES #165
- ZSS cookie is now sent to the browser, rather than having the app-server mediate the ZSS connection, so that ZSS can be used through APIML in the case that SSO is not enabled. #274
- ZSS now uses HTTPS by default, rather than relying upon AT-TLS for the purpose. AT-TLS is still available, but now unless ZOWE\_ZSS\_SERVER\_TLS=false is set, ZSS will use the keystore data for its HTTPS configuration, and when HTTPS is enabled will bind to ZOWE\_EXPLORER\_HOST value, as the other servers do, instead of 127.0.0.1 by default as ZSS would for HTTP.
- Added function to toggle the file explorer
- Added calls to the function in open file and open dataset so that when the user inputs the string with a true in the url it will hide the file explorer
- Added a global "environment" object in Zowe ZLUX which allows for retrieving select environment properties from the zowe instance for conditional decision-making
- The Zowe desktop uses the new environment object to determine whether to contact ZSS through appserver or through APIML depending on if ZSS is found on APIML
- app-server will contact ZSS through APIML if APIML is enabled and app-server finds that APIML is accessible from APIML
- sso-auth plugin no longer keeps ZSS cookie within app-server; the cookie will now be sent to and used from the browser to facilitate high availability

#### Zowe CLI

The following enhancements were added to the **core CLI**:

- Added the option --jcl-symbols to the jobs submit command to enable users to specify JCL symbol names and values.
- Made changes to definition files for zowe ssh commands #603
- Added a standard data set template with no parameters set.

The following enhancement was added to the **Imperative CLI Framework**:

• Added headers[] option to TextUtils.getTable().#369

#### Zowe Explorer

• Added the Issue TSO Commands feature #1245

# **Bug fixes**

#### Zowe installation and configuration

• Fixed an issue where Zowe runs with the prefer IP address parameter set true as default. #2063.

**Important!** With this fix, the APIML\_PREFER\_IP\_ADDRESS configuration in instance.env is deprecated and Zowe will always use false as the value.

- Fixed an issue that the Zowe 1.19.1 zowe-setup-certificates.sh script failed if not executed from the correct dir. #2062
- Fixed script zowe-support.sh not working. #2049
- Fixed validate\_certificate\_domain reports false negative on wildcard domains. #2117

#### **Zowe API Mediation Layer**

- Stop leaking X-Certificate headers (b2737a)[#1328}(https://github.com/zowe/api-layer/pull/1328)
- Remove the wait from start.sh to reduce address spaces (2ba780)#1335
- Make the version endpoint available at the URL: /application/version (0ac95a4)#1312
- Load the JWT secret properly when concurrently loaded and requested (1644a8c), #1255
- Swagger v2 yaml parsed and rendered (a1f2cc0) #1229

#### Zowe App Server

- app-server now registers to APIML using the fully qualified hostname found from ZOWE\_EXPLORER\_HOST or ZOWE\_EXTERNAL\_HOSTS. Previously, it used the short hostname reported by the OS. This resolves bugs about hostname mismatch. #153
- Set the hostname used for Eureka to match the value of ZWE\_EXTERNAL\_HOSTS if exists, or otherwise ZOWE\_EXLORER\_HOST, for the purpose of avoiding certificate verification issues between app-server and APIML under certain circumstances

- Set the cookie path to root in order to avoid multiple cookies when the browser tries to set path automatically
- Use the hostname given by Zowe config in order to avoid errors from the hostname certificate matching when accessing the app server through APIML
- ZSS tile on the API Catalog has been fixed due to HTTPS mode listening on the hostname of ZOWE\_EXPLORER\_HOST to align with the other zowe servers.
- ZSS dataset write REST API has improved handling of when a client sends fixed dataset content with too little padding #209

#### Zowe CLI

The following bugs were fixed in the **Imperative CLI Framework**:

- Print a subset of the stdout and stderr buffers when calling mProgressApi's endBar() to prevent duplication of output.
- Replaced this with ImperativeConfig.instance in ImperativeConfig.getCallerFile().#5

The following bugs were fixed in the **Secure Credential Store Plug-in**:

Updated the Keytar and prebuild-install dependencies to make offline installation possible for npm@7 users.

The following bugs were fixed in the **FTP Plug-in**:

- Fixed list jobs problems.
- Updated list jobs unit test and system test.

#### Zowe Explorer

- Fixed the issue that caused the USS tree to collapse after renaming a folder #1259
- Fixed the issue that prevented jobs with an octothorpe (#) in the name from opening #1253

# Version 1.20.1 LTS (March 2021)

### **Bug fixes**

**Zowe Installation and Configuration** 

• Fixed an issue when importing external certificate authorities. #2032

# Version 1.20.0 LTS (March 2021)

Check out this blog that summarizes some of the major enhancements and changes for this release.

## New features and enhancements

#### Zowe API Mediation Layer

- Feature: x509 authentication scheme. This feature supports authentication with a client certificate in southbound services whereby users can decide which part of the certificate to use. (#1208) (94dbf37), closes #1208
- Feature: Add NodeJS sample service and enabler. This feature makes it possible for a service based on NodeJS to register with API ML in a similar way as with other onboarding enablers. (#1140) (c86a289), closes #1140
- Feature: Allow Zowe to run without a jwtsecret if the jwtsecret is not required. (#1203) (7dc6dad), closes #1203
- Feature: Introduce token validation providers. This feature provides a future mechanism of token validation whereby custom endpoint can be provided that requires authentication. (#1142) (80cc790), closes #1142
- Feature: Reject eviction strategy has been added to VSAM. If storage is full, and ZWE\_CACHING\_EVICTION\_STRATEGY is set to reject this feature prevents the Caching Service from removing entries, but returns a status code 507 with the message, "Insufficient storage space limit". (#1112) (70c2d71), closes #1112 (80cc790), closes #1142
- Feature: Base information (SSO, API ID) about a service is now displayed in the API Catalog. (#1116) (4b61377), closes #1116 #1116
- Feature (Caching Service): Production logging for the Caching Service. This feature limits messages sent to Spool to the bare minimum, thereby improving the information returned to the caller. (#1185) (7adffb1), closes #1185

#### Zowe App Server

- Added a manifest file, a validate script, and refactored configure, start, and app-server scripts to better conform to Zowe lifecycle management standards #144
- Added a method to read user and group server timeout information from a JSON file #248
- Added a quick search to the File Tree that filters opened files, folders, and datasets #197

- Added a preferences menu to customize the editing behavior and color theme. The preferences can be previewed in realtime, but can also be saved to the app-server so that they are applied every time the editor is opened. #195
- Added undo and redo menu items when editing a file #195

#### Zowe CLI

The following enhancements were added to the **core CLI**:

- Updated the Imperative version to handle GZIP compression on REST requests.
- Added a like option to the zowe zos-files create data-set command. Use this option to like datasets. #771
- Added a --protocol option to allow you to specify the HTTP or HTTPS protocol used. The default value remains HTTPS.#498
- Added an example for running a Db2 command with the zowe zos-console issue command command. #641

The following enhancement was added to the **Imperative CLI Framework**:

 Added decompression support for REST responses with Content-Encoding gzip, deflate, or br. #318

The following enhancements were added to the **IBM Db2 Plug-in**:

- Added a semicolon after each sql statement when exporting a table.
- Added a help example for how to pass output values when calling a Db2 stored procedure.

The following enhancement was added to the FTP Plug-in:

• Added allocate command to allocate sequential or partitioned dataset.

#### Zowe Explorer

- Added the monorepo landing Readme that contains the high-level overview of the repository folders such as packages folder, instructions on how to contribute to the project and links to Medium articles providing additional useful information about Zowe Explorer and Zowe #1199.
- Added the previously selected RejectUnauthorized value to the placeholder text of the entry field while updating an existing profile. In addition, the value is highlighted and shown at the top of the selection list #1218.

- Added the pre-filled and pre-selected filename of the copied member to the entry field while performing the paste member action #1183.
- Added the multiple deletion of jobs feature #1128.
- Improved error handling for the data set copy/paste member, migrate, and recall functions #1219.

For more information about the Zowe Explorer release notes, see Changelog.

## **Bug Fixes**

#### **Zowe API Mediation Layer**

- Bugfix (authentication): Support specific z/OSMF version. This fix allows the user to force the authentication token that is used. (#1241) (2da761a), closes #1241
- Bugfix (authentication): Ignore wrong or non-existing SAF classes when SAF is not used (#1216) (c5ea311), closes #1216
- Bugfix (enabler): Add unregistration method to the the Node.js enabler. (#1214) (1ecd5c7), closes #1214
- Bugfix: Enable /api/v1/gateway path format for the /auth/logout, /auth/login, /auth/query, and /auth/passticket endpoints (#1126) (13ac9a5), closes #1126
- Bugfix: Accept swagger/openapi in yaml format (#1202) (0c412b0), closes #1202

#### Zowe CLI

The following bug was fixed in the **core CLI**:

• Removed the conflicting alias -o for --protocol option.

The following bugs were fixed in the **Imperative CLI Framework**:

- Added Protocol to the Error Details coming from the AbstractRestClient. #539
- Fixed vulnerabilities by replacing marked with markdown-it and sanitize-html.
- Fixed plugin install failing to install package from private registry.

The following bugs were fixed in the the **Secure Credential Store Plug-in**:

- Updated the Keytar dependency to v7 to be compatible with Node.js v15.
- Provided additional instruction in readme for npm@7 users.

#### **Zowe Explorer**

- Fixed the issue that prevented the list of recently opened files from being displayed upon request. You can access a list of recently opened files by pressing the Ctrl+Alt+R (Windows) or Command+Option+R (Mac) key combination #1208.
- Fixed the issue that prevented file picker from functioning. The file picker feature lets you filter your datasets in the tree by pressing the Ctrl+Alt+P (Windows) or Command+Option+P (Mac) key combination #992.
- Fixed the issue that caused the content from a previously filtered USS directory instead of the currently filtered USS directory to be served #1134.

For more information about the Zowe Explorer release notes, see Changelog.

# Version 1.19.1 LTS (February 2021)

# **Notable changes**

#### SMPE PTF

With the continuous optimization of the Zowe build size, now the Zowe release can fit in one PTF. This single PTF UO01969 will supersede PTF UO01967 and UO01968 from the v1.19.0 release.

### New features and enhancements

#### Zowe CLI

The following enhancements were added to the core CLI:

• Updated Imperative version to support npm@7. This fixes an error when installing plugins.

The following enhancements were added in the Imperative CLI Framework:

• Fixed plugin install commands which were broken in npm@7. #457

# **Bug fixes**

#### SMPE PTF

• Fixed the missing HOLD data about extra steps the system programmer should take after applying the PTF. It explains new configuration options that are introduced in instance.env and also a reconfiguration step where zowe-configure-instance.sh is mandatory.

#### Zowe CLI

The following bugs were fixed in the **Imperative CLI Framework**:

• Fixed incorrect formatting of code blocks in web help. #535

# Version 1.19.0 LTS (February 2021)

### **Notable changes**

#### Package manifest and component installer

Each Zowe extension and each core component can now use a manifest file to describe itself. The manifest file defines the name and purpose of the component. It also provides information about how this component should be installed, configured, started and tested. For more information, see Packaging z/OS extensions.

Two tools, zowe-install-component.sh and zowe-configure-component.sh, are introduced in this release for technical preview. The zowe-install-component.sh helps you install any Zowe server component (extension). Zowe core components are also installed with this tool. The zowe-configure-component.sh tool helps you configure an installed Zowe server component (extension) for a Zowe instance. Zowe core components are also configured with this tool. In order to be compatible with the tools, it is recommended that the components follow Zowe server component package format standard.

#### X.509 client certificate authentication support for API Mediation Layer (Technical Preview)

This feature is released for technical preview in Zowe 1.19. Previously, users were required to provide credentials (usually basic authentication) to make a login call against the API Gateway. From release 1.19 you can now use the x509 client certificate for calls to authenticate in the API ML, whereby information from the certificate verifies the user's identity through SAF and then returns a proper JWT.

If you would like to offer feedback about using client certificate authentication, please create an issue against the Zowe api-layer repository.

#### Standalone run of Zowe API Mediation Layer

You can now start the API Mediation Layer independently of other Zowe components. This allows you to minimize the resources used when you use Zowe as a Devops tool instead of a Virtual Desktop tool.

#### New features and enhancements

#### **Zowe API Mediation Layer**

- The connection limit of the Gateway has been configured to support multiple long-running requests by service. #843
- The size of API Mediation Layer has been reduced to fit within 150MB. #909
- You can now configure whether or not the Catalog appears on the Gateway homepage #727
- Connection limits have been enhanced to improve latency times when making requests through the API ML. This feature also enables concurrent requests. #987
- The connection limit log messages have been enhanced. New messages indicate when too many connections occur. #987
- The /api/v1/gateway/services/{serviceId} endpoint has been added which provides information about a service in API ML for API clients. You can now view information to choose the applicable available API service without having a trusted service certificate. Proper SAF authorization is required. #873
- The size limitation in the InMemory cache for proper handling is now supported when size limitations are reached. #998
- The 'Remove Oldest' eviction mechanism for Caching Service has been implemented to limit the volume of data in the cache.#998
- CORS origins per service has been configured so that onboarded services can request that CORS behavior for a route be delegated to the API Mediation Layer. #997
- The 'Reject eviction' strategy to the Caching Service has been implemented to limit the volume of data in the cache.#998
- Debug logging to x.509 Client certificate authentication classes has been added. This feature enables users to determine the cause of system problems during client certificate authentication setup.

#### **Zowe App Server**

- Dispatcher actions have been added to the iFrame adapter. #302
- Support has been added to a new destination property for iFrame pluginDefinition.json. iFrame with the new destination property will now make requests to /web/iFrame. #296
- The compression-webpack-plugin has been updated from 3.1.0 to 4.0.0 #304
- Support for a new destination property to iFrame pluginDefinition.json has been added, as well as a new double iFrame default template. #257
- Axios has been updated from 0.19.2 to 0.21.1 in /test/webapp/websocket #259
- The option to refresh file content has been added to the Editor. #185
- Refresh buttons have been added to USS and MVS. #108

- Additional keybindings and other improvements have been added to the Editor. #182
  - You can now move between open file tabs by using the following hotkeys: Alt + (PAGEUP or <) and Alt + (PAGEDOWN or >)
  - After closing a tab, or multiple tabs, you can now undo the close by using the following hotkeys:
     CTRL + ALT + T
  - The search function hotkey has been changed from **ALT + S** to **ALT + S**.
  - You can now hide/show the File Tree by using the following hotkeys: **ALT + B**.
- Existing code highlighters have been reorganized in order to improve their readability. Additionally, a
  new code highlighter for the REXX language has been added. This new code highlighter detects files
  and datasets wherein the files should end with the .rexx prefix, but the datasets may contain the rexx or
  exec qualifiers. #181

#### **Zowe Explorer**

• Updated Keytar and Jest dev deps for Node 14.

#### Zowe JES/MVS/USS Explorers

The following features and enhancements were added to the **JES Explorer**:

- Introduced the menu shortcuts and confirmation dialog before canceling or purging the job for JES explorer. #235
- Refactored JES packaging and installation scripts, and folder renames to accommodate new iframe capability in ZLUX. #236
- Added manifest for API ML and App Framework installation using new plugin installation process. #234

The following features and enhancements were added to the **MVS Explorer**:

- Refactored MVS packaging and installation scripts, and folder renames, to accommodate new iframe capability in ZLUX. #164
- Added manifest for API ML and App Framework installation using new plugin installation process. #164

# **Bug Fixes**

- API ID is not sent to Eureka in metadata by the Java enabler #991
- Fixed tcp connections that are stuck open. #1009

#### **Zowe App Server**

- In previous versions, sso-auth URL encoding that used the % sign would always return with authorization:false when using RACF. This issue has been resolved in this version. #258 #27
- Fixes a bug in the Editor that prevented the unsaved changes symbol from being displayed. #185
- Stopped event propagation in the Editor in order to resolve a conflict with Firefox. #183
- Fixes a bug in the Editor that would cause the Languages menu to disappear when closing all tabs, then clicking undo. #182

#### Zowe CLI

The following bug was fixed in the **core CLI**:

• Updated the Imperative version to fix a vulnerability.

The following bugs were fixed in the **Imperative CLI Framework**:

- Fixed vulnerabilities by updating marked #515
- Fixed an issue where TypeError has been raised by Logger.getCallerFileAndLineTag() when there was not filename for a stack frame. #449

# Version 1.18.0 LTS (January 2021)

# **Notable changes**

#### Zowe Docker build Technical Preview is available

The Zowe Docker build enables you to run a subset of the Zowe server-side components outside z/OS. The Docker build runs in combination with the convenience or SMP/E build. You can download the build directly via the .tar file, or as a cloud download from Docker Hub. Separate downloads exist for z/Linux ("s390x") and other Linux ("amd64" for intel & amd systems).

For more information, see Docker Installation Roadmap. To download the Docker build technical preview, visit Zowe.org.

# New features and enhancements

**Zowe API Mediation Layer** 

- Version 1.18.0 introduces a feature allowing users to run the Zowe API Mediation Layer as a standalone component. After downloading and installing the current Zowe SMPE package, you can then configure and deploy only the Zowe API Mediation Layer without the other Zowe components. #856
- You can now configure more detailed logging outside of Spool. #709
- High Availability: The start script per API ML service has been componentized. You can now launch and restart API Mediation Layer components individually. #862
- High Availability: It is now possible to distinguish between internal and external traffic through port separation, whereby each port uses a unique certificate; one presenting an internal certificate, and the other an external certificate. #910
- API version is now automatically set to the version tab selected in the API Catalog so users can easily grab the Base Path. #943
- API Catalog versioning has been improved with the addition of the API differences tab. This feature enables you to compare versions of two APIs. #923

## Zowe App Server

- The Zowe App Framework's "single app mode" is now based on code shared with the Desktop, allowing it to support the Desktop's notification API and app2app communication. #67 #292
  - This is backward compatible with apps that have previously used single app mode.
  - In the case where app2app communication is used and spawns a second app, that app will spawn in a window but will not be able to be minimized due to single app mode having no Desktop, and therefore no way to restore a minimized window.
- ZSS plug-ins can now issue HTTP requests as HTTP clients, provided by a new library in zowecommon-c. #179

## Zowe CLI

The following enhancements were added to the **core CLI**:

- Added a --replace option to the zowe zos-files copy data-set command. Use this option if you want to replace like-named members in the target data set. #808
- Improved a cryptic error message that was shown if the TSO address space failed to start for the zowe zos-tso issue command command. #28

The following enhancements were added to the **Imperative CLI Framework**:

• Added an arrayAllowDuplicate option to the ICommandOptionDefinition interface. By default, the option value is set to true and duplicate values are allowed in an array. Specify false if

you want Imperative to throw an error for duplicate array values. #437

• Expose trim parameter from wrap-ansi within TextUtils.wordWrap()

## The following enhancement was added to the **IBM Db2 Plug-in**:

• Added a help example for how to pass output values when calling a Db2 stored procedure.

The following enhancement was added to the **FTP Plug-in**:

• Move the reusable code from handlers to api folder.

#### Zowe JES/MVS/USS Explorers

The following features and enhancements were added to the **JES Explorer**:

• Added webdevSever proxy setting in webpack.config.js to enable https for local development.

# **Bug Fixes**

#### **Zowe API Mediation Layer**

- ZaasJwtService enhancement on JWT parsing and error handling. #897
- Upgrade dependencies for the Enablers. #933

## Zowe App Server

- The zss server log verbosity seen when using the TN3270 desktop app has been reduced. #188
- Keep-alive parsing has been temporarily disabled to patch a memory leak. A permanent fix that will allow the use of keep-alive parsing is scheduled to be implemented in the next release. #186
- The warning messages on the zss server startup have been removed due to a shell syntax problem.
   #238
- In previous versions, static app2app recognizers would not be loaded from storage because they were treated as actions instead of as recognizers. This issue has been resolved in this release. #297

#### Zowe CLI

The following bugs were fixed in the **core CLI**:

 Removed "[object Object]" text that appeared in some error messages. The proper text "Imperative API Error" is now displayed. #836

- Improved performance of zowe zos-files list commands when long lists are printed to console.
   #861
- Updated Imperative dependency version to one that does not contain a vulnerable dependency.

The following bug was fixed in the **Imperative CLI Framework**:

• Updated opener dependency due to command injection vulnerability on Windows - GHSL-2020-145

# Version 1.17.0 LTS (November 2020)

# **Notable changes**

#### z/OSMF workflow for configuring Cross Memory Server

You can now use the z/OSMF workflow to install, configure, and launch the cross memory server if you want to use the Zowe desktop. The z/OSMF workflow also lets you create APF-authorized load libraries that are required to install and configure the cross memory server. For more information, see Configure Zowe Cross Memory Server with z/OSMF workflow.

#### **Zowe Client SDKs**

A new Zowe incubation project - the Zowe Client SDKs (Software Development Kits) is now available for Node.js, Python, and Swift programming languages. You can leverage these SDKs to rapidly develop off-platform applications and automation.

For more information about the Node.js and Python SDKs, see Using Zowe SDKs. For more information about the Swift SDK, see the Swift SDK Readme.

# New features and enhancements

The following features and enhancements were added.

## Zowe installation

• You can now start ZSS independent of the Zowe Application Framework server by specifying the LAUNCH\_COMPONENT\_GROUP "ZSS". If DESKTOP is specified instead of ZSS, ZSS will still be included as a prerequisite to the Application Framework server. #1632

- Zowe instance configuration script (zowe-configure-instance.sh) can now skip checking for Node.js by passing in the \_s flag since Node.js may not be needed if the components to be launched don't require it. #1677
- The run-zowe.sh script can also skip the checking for Node.js by setting the environment variable SKIP\_NODE=1 for the cases where the components to be launched don't require Node.js.
- Exported the EXTERNAL\_CERTIFICATE\_AUTHORITIES variable to the zowe-certificates.env file such that it may be used by the Application Framework server. #1742
- A new documentation chapter Upgrading the z/OS System for Zowe has been included, that describes the steps to take when upgrading an existing Zowe installation.

## Zowe API Mediation Layer

- Multiple versions of one API are now presented in the Catalog if configured to do so. Users can now switch between different versions within the Catalog to see differences in API documentation between versions. #844
- Setting APIML\_DEBUG\_MODE\_ENABLED in instance.env is properly passed on to the all API ML services. #901

- ZSS no longer requires NodeJS for its configure.sh script.
- Added support for DER-encoded X.509 certificates.
- You are now able to change tags for all files in the directory excluding subdirectories. For example,
   POST /unixfile/chtag/u/user/tmp?codeset=1047&type=text&recursive=false should change tags only for files in u/user/tmp without changing tags for files in subdirectories. #176
- Multiple enhancements in the Editor for USS file and directory actions, including: #84 #102 #93
  - The ability to cut, copy, & paste files into a directory, such as the currently active directory.
  - Re-ordered context menu options.
  - Improved error messages by including more detail.
  - Added support to see a file's current tag and change it.
  - chown & chmod enhancement that pre-populates the owner and group fields when opening the ownership and properties dialogs. It also adds owner and group information to the file properties dialog.

#### Zowe CLI

The following enhancements were added to the core CLI:

- Zowe CLI was tested and confirmed to be compatible with Node.js v14.
- Published the programmatic interfaces in Zowe CLI as separate Software Development Kits (SDKs).
   #750
- The "@zowe/cli" package still includes both API and CLI methods. In addition, the following SDK packages are now available:
  - @zowe/provisioning-for-zowe-sdk
  - @zowe/zos-console-for-zowe-sdk
  - @zowe/zos-files-for-zowe-sdk
  - @zowe/zos-jobs-for-zowe-sdk
  - @zowe/zos-tso-for-zowe-sdk
  - @zowe/zos-uss-for-zowe-sdk
  - @zowe/zos-workflows-for-zowe-sdk
  - @zowe/zosmf-for-zowe-sdk
  - @zowe/core-for-zowe-sdk

The following enhancement was added to the Imperative CLI Framework:

• Exposed the trim parameter from wrap-ansi within TextUtils.wordWrap().#458

The following enhancement was made to enable support for Node.js v14 for the **Secure Credential Store Plug-in**:

• Enabled support on Node.js v14 by updating Keytar dependency to v6. #28

The following enhancement was made to enable support for Node.js v14 for the **IBM Db2 Plug-in**:

• Enabled support for Node.js v14 by updating dependencies. #60

## Zowe Explorer

• Added login and logout functions for base profiles. You can now log in to API Mediation Layer and generate a token for your base profile. #914

#### Zowe JES/MVS/USS Explorers

The following features and enhancements were added to the **JES Explorer**:

- Added ability to refresh content of an open job output file via context menu entry on the job file #549
- Major material ui update from v1.x to 4.x, and minor react update. Accordion and snackbar changes as required by latest material-ui version.

# **Bug fixes**

The following bugs were fixed.

## **Zowe API Mediation Layer**

- Improved returned information while logging out via logout on Gateway. #831
- Updated API paths for the API ML in the API Catalog to use the service id in front. #853

## Zowe App Server

- Make use of external certificate authorities referenced during keystore setup time.
- ZSS startup would issue warnings about failure to write yml files for APIML in the case APIML was not also being used.
- Bugfix: In previous versions, external certificate authorities were not registered with the app server properly and would sometimes contribute to a SELF\_SIGNED\_CERT\_IN\_CHAIN error when using the mediation layer. This issue has been resolved by adding external CA certs to the app-server CA array. #138

## Zowe CLI

The following bug was fixed in the **core CLI**:

• Fixed incorrect syntax of example for zowe files create data-set-vsam in the help. #823

The following bug was fixed in the **Imperative CLI Framework**:

• Updated opener dependency due to command injection vulnerability on Windows. For more information, see GHSL-2020-145.

## Zowe Explorer

• Fixed the empty profile folders in Favorites issue. #1026

- Fixed the initialization error that occurred when base profiles were used while being logged out from API ML. #1063
- Fixed the issue preventing the tree refresh function from updating extender profiles. #1078

# Version 1.16.0 LTS (October 2020)

# Notable changes

## Certificate management and keyring support

- In V1.15, the JCL member ZWEKRING was added to the sample PDS library SZWESAMP. This member contains commands to create a keyring that can contain the Zowe certificate(s) and a local certificate authority. In this release, the JCL member ZWENOKYR was added to SZWESAMP that contains the inverse commands, so it can be used to remove the keyring, the Zowe certificate(s), and the certificate authority.
- In V1.15, the JCL member ZWEKRING and the supporting code in the Zowe runtimes for working with certificates held in keyrings were provided in beta format for early technical preview for RACF only. In this release, the commands in ZWEKRING, ZWEN0KYR and the supporting code in the Zowe runtimes for working with keyrings and certificates in RACF, TopSecret, and ACF/2 are now a supported piece of functionality.
- A new documentation section is added to help you understand the configuration scenarios around Zowe certificates, and the relationship to a Zowe instance directory and Zowe runtime. See Topology for the Zowe z/OS launch process.

## Additional TN3270 terminal configuration options

Additional TN3270 terminal configuration options can now be specified within the instance.env configuration file. These choices, such as codepage and terminal dimensions, affect server defaults but do not change the pre-existing ability for you to set your own preferences within the Desktop at runtime. A list of the available options can be found here.

# New features and enhancements

The following features and enhancements were added.

## **Zowe installation**

- Moved explorer-ui-server out of explorers into new shared folder under Zowe Runtime Directory. #1545, #207, #37
- Created zowe-setup-keyring-certificates.env and removed the overloaded properties from zowe-setup-certificates.env to try to simplify the user experience when setting up certificates in the keyring and USS keystore modes. #1603

#### **Zowe API Mediation Layer**

- ZAAS Client can now use HTTP so that the Application Transparent Transport Layer Security (AT-TLS) can be used for communication to ZAAS. #813
- Implemented the logout functionality in ZAAS Client. #808
- Added a more helpful and actionable description to message ZWEAM511E, which occurs when API ML does not trust the certificate provided by the service. #818

#### Zowe App Server

• The install-app.sh script used to install App Server plugins can now be used without Node.js. If Node.js is not detected when the script is executed, this behavior will be automated. You can also force this behavior with the environment variable INSTALL\_NO\_NODE=1, such as in the following example:

```
    INSTALL_NO_NODE=1 ./install-app.sh ~/zlux-editor #137
```

- ZSS is now automatically registered to the API Mediation Layer when both are present, using a static registration file. #208
- Additional environment variables are now supported, which provides more options for TN3270 for the instance.env configuration file #1176 while also allowing TN3270 host to be specified during installation configuration. #1125. The following new environment variables are now supported in instance.env #108:
  - o ZOWE\_ZLUX\_TELNET\_HOST = string
  - o ZOWE\_ZLUX\_SSH\_HOST = string
  - o ZOWE\_ZLUX\_TN3270\_ROW = number
  - o ZOWE\_ZLUX\_TN3270\_COL = number
  - ZOWE\_ZLUX\_TN3270\_MOD = numbers 2-5 as well as "dynamic" or other variations of the word
  - ZOWE\_ZLUX\_TN3270\_CODEPAGE = ccsid number or string as seen in the ui

- The Agent API now provides limited information without the need for authentication. Non-admins are able to view a subset of the information available to admins, specifically regarding the functionality of Zowe. Examples of the information available to non-admins are: OS architecture and environment variables for Zowe configuration such as the components used and the ports they are accessible on. #211
  - /server/agent/environment (limited info)
  - /server/agent/services
- The ZSS /unixfile API has been updated to include an option to force file content to be sent or received as a specific encoding. If not specified, the pre-existing behavior of automatically choosing encoding based on tagging and file extensions will be used. #160
- The app server can now read and use keys, certificates, and certificate authorities contained with PKCS12 files. This is in addition to existing support for PEM-encoded files as well as z/OS keyrings.
   #244

#### Zowe CLI

The following enhancements were added to the **core CLI**:

- Added a --pattern option to the zowe files list all-members command. The option lets you restrict returned member names to only names that match a given pattern. The argument syntax is the same as the "pattern" parameter of the ISPF LMMLIST service. #810
- Added new options --lrecl and --recfm to the zos-files create command. Use these options to specify a logical record length and record format for data sets that you create. #788

#### Zowe Explorer

- Added the Allocate Like feature. #904
- Added the ability to disable/enable profile validation. #922
- Added the ability to access other profiles during profile validation. #953
- Grouped Favorites by profile for Datasets, USS, and Jobs. #168
- Once entered, datasets and members are displayed in uppercase. #962
- Updated the environment check for Theia compatibility. #1009

#### Zowe JES/MVS/USS Explorers

The following enhancement was added to the **Explorer UI Server**:

• Explorer UI Server is now published as separate pax and decoupled out of explorers. #37

The following features and enhancements were added to the **JES Explorer**:

- Moved explorer-ui-server out of explorers into new shared folder under Zowe Runtime Directory. Changed JES lifecycle start script to use new shared location. #207
- Added context menu entry for download JCL used to submit a job. #335
- Updated webpack to latest version, added .npmrc to specify npm registry as config. #222

The following features and enhancements were added to the **MVS Explorer**:

- Extracted out explorer-ui-server, changed MVS lifecycle start script and packaging script accordingly. #151
- Added loading icon to editor menu bar when opening a dataset's contents. #291
- Added . npmrc to specify npm registry as config.

The following features and enhancements were added to the USS Explorer:

- Extracted out explorer-ui-server, changed USS lifecycle start script and packaging script accordingly. #100
- Added . npmrc to specify npm registry as config.

# **Bug fixes**

The following bugs were fixed.

## Zowe API Mediation Layer

- Changed the default expiration time value for JWT token to 8h for consistency with the z/OSMF default.
   #615
- Reduced excessive and unhelpful log messages. #672
- Added the Base Path field in the API Catalog if one is available, which can override the Swagger Base Path. This causes the proper Base Path to be displayed in the event that the api doc is not populated properly. #810
- Removed overwriting of the Swagger Base Path, which resulted in malformed API routes when the base URL is shared among multiple services. #852
- API ML was previously not reporting SSL certificate errors when servers were unable to communicate. Now, if a SSLException occurs, SSL certificate errors are reported. #698

• Fixed language in log messages for consistency. #830

#### **Zowe App Server**

In previous versions, the environment arch and os fields were incorrect. This has been fixed, and the updated response from /server/agent/environment service is #213:

#### Zowe CLI

The following bug was fixed in the **FTP plug-in for Zowe CLI**:

• Fixed an issue where the view spool-file-by-id command retrieved incorrect contents. #61

# **Zowe Explorer**

- Fixed USS renaming issues. #911
- Fixed the deletion of datasets issue. #963.
- Removed errors in Favorites items caused by profiles that are created by other extensions. #968

# Version 1.15.0 LTS (September 2020)

# Notable changes

#### Keyring support

Prior to v1.15, the Zowe z/OS components were only able to use a certificate held in a USS Java KeyStore. In v1.15, the Zowe z/OS components can now use a certificate that is held in a z/OS keyring as described in Configuring Zowe certificates in a keyring.

For more information about Zowe certificates, certificate authorities, trust stores, and how they are used by Zowe, see Configuring Zowe Certificates.

#### Auto-Save plug-in data

Plug-in developers can now make use of the new autosave feature, which can automatically save state data based on what the developer intends to retain, at regular time intervals. This is to protect against client crashes, and in the case of a crash, the apps are reopened upon desktop login and restored with the saved state. This new capability furthers the larger goal of high availability and fault tolerance for all Zowe components.

#### Support for starting Zowe API ML without z/OSMF on your system

By default, the API Gateway uses z/OSMF as an authentication provider. With the release of Zowe 1.15 it is now possible to switch to SAF as the authentication provider instead of z/OSMF. So, if you want to securely run the Zowe API ML but your system does not have z/OSMF, simply select SAF as your authentication provider. For more information on how to switch to SAF, see API Gateway configuration parameters.

# New features and enhancements

The following features and enhancements were added:

## **Zowe API Mediation Layer**

- The API Path Pattern now supports serviceId as the first element. This improves the consistency of the URL when processing through the Gateway or outside of the Gateway. #688
- The SAF Provider can now be used as a possible authentication provider. This removes the API ML dependency on z/OSMF for authentication enabling SAF to obtain the JWT. #472
- The Swagger URL is now provided for z/OSMF. This URL provides full documentation containing the Try It Out functionality if the z/OSMF version supports the Swagger endpoint. Alternatively, the URL provides the info endpoint to directly enable access to Zowe endpoints. #665
- The default configuration of API ML now supports character encoding. #777

#### ZSS

A new endpoint has been added to the Agent API. This new endpoint will return a list of services to the user. #209

- Sample request: GET /server/agent/services
- Sample response:

#### **Zowe App Server**

- Added a feature that allows users to auto save plug-in data by subscribing to the event. By default, the feature will auto save every 5 minutes, but this interval can be customized. #250
  - This feature is enabled via the Plugin Definition. "autosave": true
- You are now able to select multiple jobs in the job tree, which allows for functions such as purging multiple jobs at once. #274, #204

#### Zowe CLI

The following features and enhancements were added to the **core CLI**:

- Added a --responseTimeout option to the z/OS Files APIs, CLI commands, and z/OSMF profiles.
   Specify --responseTimeout <###> to set the number of seconds that the TSO servlet request runs before a timeout occurs. The default is 30 seconds. You can set the option to 5 600 seconds (inclusive). #760
- Added the --encoding option for the zowe zos-files upload dir-to-pds command. This option lets you upload multiple members with a single command. #764

The following features and enhancements were added to the Imperative CLI Framework:

- Added support for dynamically generated cookie names. Updated
   AbstractSession.storeCookie() to process cookie names that are not fully known at build-time.
   #431
- Added the SSO Callback function, which allows applications to call their own functions while validating session properties (that is, host, port, user, password, token, and so on). The callback option is named getValuesBack. #422

The following features and enhancements were added to the **Secure Credential Store Plug-in**:

- Added the scs revert command. Use the command to revert securely stored credentials in your user profiles to be stored in plain text. #22
- Changed the scs update and scs revert commands so that they fail if Secure Credential Manager is not enabled. #23

## Zowe JES/MVS/USS Explorers

The following features and enhancements were added to the **JES Explorer**:

- Changed the packaging and lifecycle start.sh script to add explorer-ui-server keyring support.
   #1177
- Added app bar, along with settings, and local storage to store user preferences and remember the last search filter. #487
- Notifications preference can set duration for snack bar notification. #273

The following features and enhancements were added to the **MVS Explorer** and **USS Explorer**:

Changed the packaging and lifecycle start.sh script to add explorer-ui-server keyring support.
 #1177

• Added ability to collapse and resize jobs tree. #259

# **Bug fixes**

The following bugs were fixed.

#### **Zowe API Mediation Layer**

- Fixed SSL validation when Eureka is running in HTTP mode. When the scheme is HTTP, SSL configuration is not verified since it is not used. #792
- Fixed a problem in error handling when no api-doc is available. Now a specific return code and message is generated when a problem occurs when obtaining or transforming the api-doc. #571

#### ZSS

- When RBAC is disabled, only the following services will be available. #210
  - /server/agent/environment (with limited information)
  - /server/agent/services

## Zowe App Server

- External CA certificates to the Zowe ZWED\_node\_https\_certificateAuthorities array only after checking to see if the certificates exist, which prevents it from pointing to nothing, resulting in it breaking. #136
- In previous versions, the component.json file was only being created when users upgraded their Zowe system to a more recent version. Performing an initial installation would not result in the component.json file being created. In this version, this bug has been resolved, and the component.json file is created both when upgrading and performing an initial installation. #135

## Zowe CLI

The following bugs were fixed in the **core CLI**:

- Renamed the z/OS Files API option from storeclass to storclass. This fixed an issue where the CLI could define the wrong storage class on create dataset commands. #503
- Fixed an issue where the output of the zowe zos-uss issue ssh command would sometimes omit the last line. #795

The following bug was fixed in the **Imperative CLI Framework**:

• Fixed an issue with ConnectionPropsForSessCfg where the user would be prompted for user/password even if a token was present. #436

#### Zowe JES/MVS/USS Explorers

The following bugs were fixed in the **JES Explorer**:

- Fixed a bug where no jobs would show after auth token expired and user logs back in. #408
- Added default value for ZOWE\_EXPLORER\_FRAME\_ANCESTORS at lifecycle start script. It resolves #44.
- Fixed an issue where job tree height is greater than app container which makes the page scrollable.
   #484

The following bugs were fixed in the **MVS Explorer**:

- Fixed an issue where the dataset tree and the content viewer were not aligned. #484
- Added default value for ZOWE\_EXPLORER\_FRAME\_ANCESTORS at lifecycle start script. It resolves #44.

The following bugs were fixed in the **USS Explorer**:

• Added default value for ZOWE\_EXPLORER\_FRAME\_ANCESTORS at lifecycle start script. It resolves #44.

# Version 1.14.0 LTS (August 2020)

# Notable changes

## Zowe Node APIs

Did you know that you can leverage the Zowe Node APIs directly? The Zowe Node APIs are the programmatic APIs that enable Zowe CLI to interface with the mainframe. You can use the APIs to build your own applications or automation scripts, independent of Zowe CLI. For more information and usage examples, see the Zowe CLI readme file.

# Support for verifying Zowe release integrity

Zowe now provides a new tool to verify that the code in the Zowe runtime directory installed on your z/OS® system is identical to the released code. The tool comprises a script file <code>zowe-verify-authenticity.sh</code>, plus the files it needs to check the release contents.

If the contents of the Zowe runtime directory have been modified, then it may result in unpredictable behavior. For more information about the tool, see Verify Zowe runtime directory.

# New features and enhancements

The following features and enhancements were added.

# Zowe installation

- If you are upgrading to Zowe v1.14 from a previous release, and the value of ZOWE\_EXPLORER\_HOST does not match the host and domain that you put into your browser to access Zowe, you must update your configuration due to updated referrer-based security. See Important note for users upgrading to v1.14 for information on updating your configuration.
- Allow the user to verify the authenticity of a Zowe driver. The script <a href="mailto:zowe-verify-authenticity.sh">zowe-verify-authenticity.sh</a> will check that a Zowe <a href="mailto:R00T\_DIR">R00T\_DIR</a> for an installed release matches the contents for when that release was created, which assists with support and troubleshooting. To verify pre-1.14 releases, the script and its associated code are available separately (see #1552). For more information, see the new topic Verify Zowe Runtime Directory that describes the operation of the script.
- Allow multiple domains (names/IP Addresses) when generating certificates. This also includes SMP/E
   HOLDDATA for the affected function Zowe Configuration. #1511
- Included z/OSMF workflows for Zowe z/OS configuration. #1527
- Added warning if ZWESVSTC runs under user ID IZUSVR . #1534
- [Docs] Changed the documentation so that SZWEAUTH PDSE load library members should not be copied elsewhere, but instead the original installation target SZWEAUTH PDSE should be APF-authorized and used as the runtime load library. This also includes SMP/E HOLDDATA for the affected function STC JCL as well as changes to topics Installing and configuring the Zowe cross memory server (ZWESISTC) and Installing and starting the Zowe started task (ZWESVSTC).
- [Docs] Added a new topic Installing and configuring Zowe z/OS components using scripts.

# **API Mediation Layer**

- Prevented crashing of API ML when null routes are set. #767
- Added support to the X-Forwarded-\* Headers. #769
- Improved the configuration validator for the enablers to improve message specificity when one or more parameters required for setup are missing. #760

- Using a cross-memory server without REUSASID=YES may result in an ASID shortage. This pullrequest adds a check that will print a warning if REUSASID=YES is not detected. #145
- In previous versions, the server used the property InstanceID instead of ZOWE\_INSTANCE. In order to maintain backwards compatibility, these properties are now unified when the value of ZOWE\_INSTANCE is non-default. Additionally, the server uses these values whenever an instance number is needed, such as in the case of determining profile names for RBAC use #130
- The packaged size of the Editor has been significantly reduced by removing uncompressed versions of files that have compressed variants and .map files which were used for development debugging. #160
- The ZSS /unixfile REST API now supports the changing of permissions on a file or folder, similar to chmod, by calling /unixfile/chmod. The behavior is documented in swagger. #195 #132
- A notification will be displayed when users attempt to upload a wallpaper image that is too large. #254
- The desktop personalization panel's color selection UI now has an extra highlight around the selected color to make the selection more apparent. #236
- Users can now recall migrated datasets in the Editor (via the File Tree) by clicking on them. #78

#### Zowe CLI

The following features and enhancements were added to the **core CLI**:

- Added the command zowe zos-files delete migrated-data-sets to delete migrated data sets. #716
- Added a new --fail-fast option to the zowe zos-files download all-members command. The option defaults to true, which preserves existing behavior. Set the option to false to continue downloading members if one or more of the downloads fails. #759
- Updated the Imperative CLI Framework version. #744

## z/OS FTP Plug-in for Zowe CLI:

The following enhancement was added to the z/OS FTP Plug-in:

- The following flags were added to the zowe zos-ftp submit data-set command: #55
  - --wait Specify a query interval and max times to query as comma-separated, numeric values.
     For example, specify 5,12 to query the job status every 5 seconds up to 12 times.
  - --wait-for-output Wait for the job to enter OUTPUT status.
  - --wait-for-active Wait for the job to enter ACTIVE status.

#### Zowe Explorer

The following features and enhancements were added to the **Zowe Explorer**:

- Added a webpack that works with localization and logging.
- Allowed extenders to load the saved profile sessions upon activation.
- Added an automatic re-validation for invalid profiles.

Also, check out the Zowe Explorer FAQ to learn more about the purpose and function of the VS Code extension.

# **Bug fixes**

The following bugs were fixed.

- Bugfix: ZSS will now maintain the connection if users respond to the 404 message with the request
   Connection: Keep-Alive #147
  - **NOTE:** The code only recognizes **Connection:** Keep-Alive. Other "Keep-Alive" properties will be ignored.
- Bugfix: If a load module is incorrectly copied to STEPLIB, the z/OS loader will fail to load it. In these cases, an available copy in LPA will be used instead, if one is available. The problem with LPA is that any IDENTIFY calls to a module with an incorrect version number may cause serious issues. This pull-request ensures that ZWESIS01 comes from private storage. #146
- Bugfix: Fixes various issues that would occur when the number in the **Content-length** response header was different from the actual content length. #150
- Bugfixes for default plugin config and terminal handler location. This change was made in order to include the <u>\_internal</u> folder. <u>storageDefaults</u> other than <u>\_internal</u> are already supported. For more information, see the wiki. #229
  - This fix allows the server-side plugin config to exist within its own folder, rather than in the instance directory. As a result, plugins no longer have to perform a copy operation during installation.
  - You can now specify terminal proxy handler overrides within \$INSTANCE\_DIR, which was previously only possible within \$R00T\_DIR. \$R00T\_DIR modification is not recommended and not conformant for Zowe plugins.
- Bugfix: The process of auto-converting untagged USS ebcdic files when using the ZSS /unixfile REST API has been improved by determining if the files are text or binary based on a list of file extensions. The

API behavior towards unknown extensions has been changed from assuming text to now assuming binary. This fixed some cases where text files were not readable through the REST API. #148 #152

- Bugfix: When using ZSS's /unixfile/contents REST API, large files would occasionally cause an incorrect HTTP message to be sent because the content-length header did not match the actual content length. This could result when there is a conversion error. This issue has been solved by updating the API, allowing it to use the transfer encoding type "chunked" instead, which allows these previously broken files to be sent successfully. #150
- Bugfix: Some file actions in the Editor would generate URLs that included multiple slashes in a row, which may cause errors on servers that receive such requests. In this update, the URI Broker now removes multiple slashes when they are encountered, which may additionally improve behavior in other apps that use the URI Broker for the ZSS REST API /unixfile. #251
- Bugfix: During ZSS initialization, certain warning log messages were not displayed, such as the warning about lack of permission to use ICSF to generate a random number. This issue has been resolved by initializing the logger responsible for issuing the messages. #143
- Bugfix: In order to conserve log space, ZSS no longer prints debug information regarding HTTP dispatch. #156
- Bugfix: In previous versions, the app framework build process referenced webpack incorrectly, leading to an unnecessary build-time error if webpack was not installed globally. This issue has been resolved. #248
- Bugfix: In previous versions, developing with the app framework would show linting warnings in VSCode. This issue has been resolved by updating tsconfig.json #240
- Bugfix: Some app server configuration values could not be specified via environment variables due to the limited characters allowed in variables. A new syntax has been made to allow these edge-case configuration values to be specified, and this new syntax is seen here: #230
  - Overall behavior is described in the wiki.

## Zowe CLI

The following bug was fixed in Imperative CLI Framework:

- Fix update profile API storing secure fields incorrectly when called without CLI args.
- Fixed a compilation error when building the CLI from source.#770

## Zowe Explorer

- Fixed the bug related to saving USS files.
- Fixed the bug related to the deletion of datasets.

# Version 1.13.0 LTS (July 2020)

# **Notable changes**

Zowe CLI added the ability to access mainframe services through API Mediation Layer using single-sign on (SSO) and multi-factor authentication (MFA). Use Zowe CLI to log in to API Mediation Layer and receive a token that is used for secure authentication to one or more services. For more information, see Integrating CLI with API Mediation Layer.

The CLI also supports a type of profile named "base profile" that lets you store configuration information for multiple services. For more information, see Using Profiles.

# New features and enhancements

The following features and enhancements were added.

#### **Zowe installation**

- Updated <a href="mailto:zowe-configure-instance">zowe-configure-instance</a> upgrade to update ROOT\_DIR. This allows you to move the Zowe runtime to a different place when you install a new version of Zowe. #1414
- Updated the port validation logic to reduce false negatives. #1399
- Updated the Zowe installation and configuration to tolerate ZERT Network Analyzer better. #1124

## **API Mediation Layer**

- Added Cross-origin resource sharing (CORS) Headers Support.
- Introduced an option to set connection timeout for a service.
- Provided SAF Keyrings support for a ZAAS Client.
- Introduced Spring Boot enabler configuration validation.

- The app server is now able to use more than one certificate authority (CA). This allows the server to validate other server's authenticity by recognizing the CA that another server may have used #128
- The dispatcher.invokeAction method now returns promise, which provides the ability to wait until dispatcher.invokeAction finishes and handles errors #59
- The ngx-color picker has been replaced by a custom hue selection bar, lightness swatches bar, and color palette, allowing for a more customizable personalization experience #235

- In this version, cross-launch via URL has been implemented, allowing for integration between the Application Framework and applications. This feature enables users to bookmark a set of app2app communication actions (in the form of a URL) that will be executed when opening the webpage #234
- Bookmarking features have been added to the TN3270 emulator #30
  - Users can now save connection preferences on a per-user level. Clicking the floppy disk icon saves user settings to that user's scope.
  - Codepages have been reorganized so that the numbers are shown first, making it easier for users to navigate to their favorites
  - The buttons found in this feature have been realigned
- Several features have been added to the Zowe Editor #153
  - Globally increased the shortest duration of snackbar notifications from 2 seconds to 3 seconds
  - Added a "Close All" button in the menu (hot key is Alt + W + Shift)
  - A snackbar notification will be displayed when users attempt to open a file that they do not have permission to open
  - Added an "Undo" option to the Close All feature to reopen tabs & files
- Login activity and session activity is now synchronized across multiple desktop tabs #242
  - When a user logs out of a desktop tab, all other active tabs will also log out
  - When a user performs an action on a desktop tab, the other tabs register this activity, which stops them from timing out

## Zowe CLI

The following features and enhancements were added to the **core Zowe CLI**:

- Added the ability to log into and out of API ML using a token. #718
- Added the --base-profile option to all commands that use profiles to let them make use of base profiles that contain shared values. #718
- CLI commands now prompt for any of the following option values if the option is missing: host, port, user, and password. #718
- Added character encoding/code page support for download and upload data set operations in the API library and the CLI. #632
- Added the --encoding option to the zosmf profile type. #632
- Introduced an API to delete migrated data sets. #715.

The following features and enhancements were added to the Imperative CLI Framework:

- Added the ConnectionPropsForSessCfg.addPropsOrPrompt function to store credentials, such as a token, in a session configuration object. #718
  - CLI plug-ins must implement this function to create sessions in order to consume automatic tokenhandling and prompt for mission options features.
  - Connection information is obtained from the command line in the following order: Environment variables, service profiles, base profiles, or a default option value.
  - If connection information is not supplied to any core CLI command, the user is prompted for:
    - host
    - port
    - user
    - password

The prompt times out after 30 seconds so that automated scripts will not fail.

• Added base profiles, a type of profile that can store values and provide them to other profile types, such as zosmf profiles. #402

The following properties can be stored in a base profile:

- host
- port
- user
- password
- rejectUnauthorized
- tokenType
- tokenValue
- Added login and logout commands to retrieve and delete tokens. #405
  - Added a showToken flag to display the token and not save it to the user profile.
  - Added the ability to create a user profile upon login, if no profile of that type existed previously.
- Added the --dd flag, which lets users create a profile without using the default values specified for that profile. #718

- If a token is present in the underlying REST session object, Imperative uses the token for authentication.
- CLI help text includes new options such as tokenValue. Plug-in developers might need to update mismatched snapshots in automated tests.
- Updated the version of TypeScript from v3.7.4 to v3.8.0.
- Updated the version of TSLint from v5.x to v6.1.2.
- Update log4js to improve Webpack compatibility for extenders.

#### **Zowe Explorer**

The following features and enhancements were added to **Zowe Explorer**:

- Added a credentials check feature that allows users to update their credentials if they receive an authorization error.
- Added a star icon that clearly denotes data sets, USS files, and jobs as favorites.
- Added a profile validation feature that checks whether a profile is valid. The feature is triggered when any action is performed with the profile. Validated profiles are indicated by a green mark.
- Disallowed case sensitivity for profiles with same names.
- Enabled editing of search filters.
- Enabled editing of ASCII files in USS.
- Improved text in confirmation dialogs.
- Reorganized the Data Sets context menu to match the order of commands recommended by VSCode.

## **Bug fixes**

The following bugs were fixed.

#### ZSS

• Bugfix: ICFS error message is not printed. In this version, the issue has been resolved #143

#### **Zowe App Server**

• Bugfix: Changing editor syntax in the MVS explorer caused a callstack limit exception. This was due to a trap focus conflict between the Orion editor and the modal part within the ui Select component on

syntax change. In this version, the issue has been resolved by disabling disableEnforceFocus for the syntax selector #129

- Bugfix: An Infinite Auth loop would occur on explorer apps due to APIML and z/OSMF auth timeouts mismatch. In this version, the issue has been resolved by adding a force login flag if a datasets request comes back as 401 #124
- Bugfix: When using the JES Explorer to view Spool files of a job, users cannot open a spool file that has the same name as one already open. This issue has been resolved by adding a unique id to content tabs to allow opening of overlapping names #188
- Bugfix: The Env var for TERM gets set to "linux", which is not recognized by USS. This issue has been resolved through the removal of rxjs-compat #29
- Bugfix: NGX-monaco-editor library has been removed in order to fix a bug. This now allows the Editor to open and view files after the second instance of opening them #155
  - Removed use of node-sass, so that native compilation is not required
  - Updated to typescript 3.7 from version 2.7.2
  - Updated to monaco 0.20 from version 0.13. The monaco changelog can be found here

#### Zowe CLI

- Fixed an issue where CLI web help failed to load in Internet Explorer 11. #393.
- Fixed an issue where the --help-web option did not function on macOS when the DISPLAY environment variable was undefined. #322.
- Updated Imperative version to include security fixes.
- Updated Imperative version to fix a problem where users could not use a service profile after storing a token in a base profile.
- Fixed an issue where optional secure fields were not deleted when overwriting a profile.

# Version 1.12.0 LTS (June 2020)

# New features and enhancements

The following features and enhancements were added.

#### **Zowe installation**

• Keystore directory generation updated to add new parameters. If you wish to enable SSO for the desktop you need to rerun the zowe-setup-certificates.sh script during the upgrade process,

with new values in the zowe-setup-certificates.env file. #1347 / Doc: #1162

- Added a -l optional parameter to the zowe-support.sh script. This parameter allows you to specify the custom log directory used in installation and configuration when collecting support data.
   #1322 / Doc: #1165
- Added the validate only mode of Zowe. This allows you to check whether all the component validation checks of the Zowe installation pass without starting any of the components. #1335 / Doc: #1181
- Separated ZSS component from the Zowe App Server component. #1320
- Introduced z/OSMF Workflows that accomplish the following Zowe installation and configuration tasks:
   Install Zowe runtime using z/OSMF Workflows.
  - Configure z/OS Security Manager.
  - Configure Zowe certificates.
  - Create and configure the Zowe instance directory, and run the Zowe started task.

#### **API Mediation Layer**

- Provided Zowe Authentication and Authorization Service (ZAAS) client.
- Refreshed the static client definitions from the API Catalog UI.
- Switched to sso-auth instead of apiml-auth.
- Added logout endpoint API documentation.
- Made j jwt only a test dependency.
- Fixed the order of fetching the JWT from a request.
- Implemented request retrying for service instances.

## ZSS

- ZSS now follows the Zowe Component scheme, as part of the DESKTOP component group #177
- Read JWT token information from environment variables, if they exist, to further support SSO during a standard installation. #178
- In previous versions, ZIS did not use the version information provided in zss/version.txt. In this version, the ZIS build uses version.txt the same way that ZSS uses it. #184

- Added SSO token name and label to convert-env.sh for use with ZSS. #118
- Script has been updated to allow ZSS to be a separate component. #117

- The app-server will favor and use a SAF keyring if defined for use in Zowe, rather than a unix file for keys, certificates, and certificate authorities. #116
- The process for making bundled plugins using R00T\_DIR has been upgraded #123
- Updates have been implemented for modal keyboard accessibility. #148:
  - Editor now has keyboard navigation in the browsing tree and pop-up modals.
  - Pop-ups can be traversed with Tab/Tab + Shift.
- Desktop redesign suite and personalization settings have been implemented. #221
- Right-click context menus have been implemented for the new desktop style. #216
- A new attribute has been implemented to load plugins from different relative paths. #212

#### Zowe CLI

The following features and enhancements were added to the **core Zowe CLI**:

- Added the zowe files hrec ds command to recall data sets. #556
- Made the account option optional in TSO profiles. #709
- Made user and host options optional in SSH profiles. #709

The following features and enhancements were added to the **z/OS FTP Plug-in for Zowe CLI**:

- Added the zowe zos-ftp list data-set-members command to find members in a PDS. #45
- Added the zowe zos-ftp make uss-directory command. #47

#### Zowe Explorer

Review the Zowe Explorer Change Log to learn about the latest features, enhancements, and fixes.

You can install the latest version of the extension from the Visual Studio Code Marketplace.

# **Bug fixes**

The following bugs were fixed.

# Zowe installation

 Minor enhancements to add log directory validation and remove unnecessary log file splitting. #1334, #1300

- When the automatically detected hostname that Zowe is installed on cannot be resolved, use the IP address instead. This covers the scenario when the USS hostname command returned a system name that wasn't externally addressable. #1279
- Fixed an issue that could cause an upgraded version of Zowe to try and use an old version of plug-ins, by switching the desktop to use a relative reference to find plugins. #1326

## ZSS

- Bugfix: Fixed a segfault when no config file is provided by moving all the zowelog invocations to a location where the logging environment is ready. Additionally, cleanup logic has been introduced to ensure that we free the STC base resources before leaving main. #187
- Bugfix: In previous versions, if a warning message is produced by the compiler, the build process is considered successful. This is often dangerous as warnings can indicate passing the wrong type or redefinition of a #define, which should be considered bugs. The following changes have been implemented to make the build process more strict #188:
  - Make sure there are no warning messages in the current build.
    - Update deps to remove the httpfileservice.c warning message, and pick up a minor type fix.
    - Ensure side-deck file/SYSDEFSD DD by adding the dll option to the linker.
  - Adjust the compiler env variable that controls the severity.
  - Ensure no ZSS binary is created if RC != 0.

- Bugfix: Logout of sso-auth was not working because it was expecting apiml parameters that should have been there but were controlled by the env var APIML\_ENABLE\_SSO. In this version, the issue has been resolved. #126
- Bugfix: In this release, many bugs picked up by the Sonar scan for core Zowe repositories have been resolved #214
- Bugfix: Plugin api would not respond if a plugin could not load due to a dependency not being met. That
  plugin would not be placed in the array that checks when the processing has finished, so a response
  would never be generated. #208
- Bugfix: Fixed a logout cookie bug and sso-auth behavior bug in order to fully support SSO. Additionally, tokenInjector was removed as it is no longer required with the introduction of SSO. #209
- Bugfix: Fixed lease information for API ML #218
- Bugfix: In previous versions, the user was never shown the logout screen when the plugin would detect zss, but not apiml. In this version, this issue has been resolved. #221

• Bugfix: Fixed issue where localhost & 127.0.0.1 were always used even when not true. Additionally, each worker in the cluster attempted registration even though, from an outside perspective, it is 1 server. In this version, the server uses a real hostname and tries to find the ip that best matches what apiml would be able to use #203

#### Zowe CLI

Updated Yargs in Zowe Imperative CLI Framework to fix vulnerabilities.

# Version 1.11.0 LTS (May 2020)

# New features and enhancements

The following features and enhancements were added:

#### **API Mediation Layer**

The following new feature was added to the Zowe API Mediation Layer in this version:

• The 'Try it out' functionality has been added to test for public and private endpoints.#258

#### **API ML Changelog**

#### ZSS

- A new query parameter (?addQualifiers) which can be appended to /datasetMetadata/ allows for searching that more closely represents the search behavior of 3.4 #108
- Added support for changing log levels via REST API #173

- Updated the JES Explorer, MVS Explorer, and USS Explorer apps to support single sign-on from the Zowe API Mediation Layer. #344 #345 #346
- Modals in the Editor now have an "X" icon to close the modal. #130
- An event emitter for session changes, login, logout, and sessionExpire for Angular, React, and iFrame applications has been added #210
- Session events have been added to mvdhosting #53
- Updates made to generate\_zlux\_certificates.sh because apiml\_cm.sh has been moved into the zoweinstall-packaging repo #110

- Zowe Web browser plugin, which can be used to view webpages that are not Zowe apps, has been added. #194
- Translations have been added for labels and buttons for password reset forms #215, #218
- Browser-based apiml token, auth simplification #196:
  - i. API mediation layer token is now held in the browser upon login via the Desktop. This also allows for the Desktop to do single-sign-on login with the token if it is already present in the browser.
  - ii. Auth plugins no longer need to be specified explicitly within the server configuration file, the capability remains for backwards compatibility. The server will now auto-detect the auth plugins that are available
  - iii. Auth plugins can now be of more than one type, to satisfy environments that have plugins that need access to APIs of similar but different types
- New shortcuts have been added to navigate the start menu with a keyboard #213
- Sessions are now maintained based on most recent activity across tabs #219
- Support for password changing, including expired password changing, has been implemented #193

#### Zowe APIs

#### **Zowe Jobs APIs**

- Version 2 APIs now support single sign-on from the Zowe API Mediation Layer #21
- Updated embedded Spring Boot version #89

#### **Zowe Data Set and Unix Files APIs**

- Version 2 APIs now support single sign-on from the Zowe API Mediation Layer #18
- Updated embedded Spring Boot version #151
- Added incomplete connect timeout parameter to prevent Slowloris DOS attacks #158

#### Zowe CLI

Reference the appropriate version in each of the following changelogs to learn about CLI features, enhancements, and fixes:

#### **Core CLI Changelogs:**

- Zowe CLI v6.11.0
- Imperative CLI Framework v4.6.0
- Secure Credential Store Plug-in v4.0.4

## CLI Plug-in Changelogs:

- IBM CICS Plug-in v4.0.2
- IBM DB2 Plug-in v4.0.6
- IBM FTP Plug-in v1.0.2
- IBM IMS Plug-in v2.0.1
- IBM MQ Plug-in v2.0.1

#### Zowe Explorer

Review the Zowe Explorer Change Log to learn about the latest features, enhancements, and fixes.

You can install the latest version of the extension from the Visual Studio Code Marketplace.

#### **Zowe installer**

- Added a -l parameter to the zowe-install.sh, zowe-setup-certificates.sh, zowe-install-xmem.sh, and zowe-install-proc.sh scripts. This parameter allows you to specify where the setup scripts write trace logs.
- Improved port validation to assist determining whether Zowe's ports are available.

## Zowe troubleshooting

Improved the troubleshooting script zowe-support.sh to assist with offline problem determination.
 See Capturing diagnostics to assist problem determination.

#### Zowe documentation

- Added a topic Zowe runtime lifecycle that describes the use of the EXTENDER\_COMPONENTS value in the instance.env file. See Creating and configuring the Zowe instance directory.
- Improved the Zowe architecture information to include a more current architecture topology diagram and more details on the individual Zowe services, where they log their data, and how to perform highlevel problem determination.
- Added new problem determination scenarios and resolution. See Troubleshooting Zowe Application Framework
- Added information on how to determine which release of Zowe is installed. See Zowe releases.
- Added a Zowe resources topic, which provides a list of resources that supplement the documentation on this site.

# **Bug fixes**

The following bugs were fixed:

# ZSS

• Bugfix: Fixed a below-the-line leak in the QSAM code #138

## Zowe App Server

- Bugfix: Material dialogs no longer overlap over the login screen #145
- Bugfix: Re-login to same desktop session would duplicate items in the launch menu. In this version, the session is cleared on logout, fixing the duplication issue #208
- Bugfix: Bugfix for websockets to prevent server throwing exception on malformed message #189
- Bugfix: Fixed app server configuration bug where min worker count was ignored when max worker count was not defined #187
- Bugfix: Added missing pluginID argument for setStorageAll method. #191
- Bugfix: app-server agent information was not available to plugins if it was specified via command line arguments #111

# Version 1.10.0 LTS (April 2020)

# New features and enhancements

The following features and enhancements were added:

# **API Mediation Layer**

The following new feature was added to the Zowe API Mediation Layer in this version:

• Zowe API ML can now use z/OSMF to provide JSON Web Tokens (JWT). #433

## ZSS

- Fast EBCDIC to UTF8 character translation is now supported by using the TROO instruction with a "EBCDIC 1047 to ISO/IEC 8859-1" translation table. #127
- Performance improvements in character conversion, JSON and collections code. #162
- The code now prints fewer warnings when AT-TLS is not set up. #130

- ZSS logs belonging in the ZSS repo have been refactored so that they now use the Zowe logger and message IDs. #163
- Config variable names have been updated to stay consistent with IBM terminology. #165

- The sample-react-app README has been updated to state prerequisites. #20
- An example of how to use the Zowe Desktop's built-in context menu has been added. #31
- Sample angular app has been updated for angular 6 best practices use of HttpClient, RxJS #33
- Simple conda build scripts have been added. #46
- App server logs now have IDs prefixed, for easy lookup in future documentation. #49
- Enhancements for plugin adding. #51
- App server logs now have IDs prefixed, for easy lookup in future documentation #102.
- App server now defaults to prevent apps from being embedded in an iframe that does not come from the same origin. #104
- The jes-explorer has been updated to support Single Sign On functionality offered by the api-layer.
   #160
- Desktop now has key bindings to minimize (ctrl-alt-down), maximize windows (ctrl-alt-up), and show launchbar menu (ctrl-alt-m). #176
- App server "router"-type dataservices now have a new Storage API within their context object, for standardized in-server state persistence. #178
- App server can now add plugins on-demand without a restart, by re-scanning plugins directory via REST API /plugins. #179
- App server can now be configured to set HTTP headers that will default and possibly override those of the plugins. #180
- App server /auth API now returns which handler is the default. #183
- Events and actions for viewports and windows are now accessible to iframe via the standardized window.ZoweZLUX.iframe object. #184
- Focus on app2app, as well as some package updates. #188
- 3 features:
  - i. Desktop can now filter the list of apps by search query.
  - ii. Desktop cleanup has reduced the bootstrapping server requests by half.
  - iii. Desktop now can load new apps added to the server without a page reload. #189
- Desktop's DOM now has lang attribute as soon as the language preference is known. #190
- Desktop login screen updated with new Zowe logo. #204

• JES, MVS Explorers now have support for APIML's Single Sign On feature #344

#### Zowe CLI

The Secure Credential Store plug-in is now packaged with tools that build dependencies locally. This fixes an issue where the installation could fail at sites with firewall restrictions. #9

**Tip:** Zowe CLI release notes are now aggregated in changelogs. Reference the appropriate version in each changelog to learn about features, enhancements, and fixes.

#### **Core CLI Changelogs:**

- Zowe CLI v6.10.1
- Secure Credential Store Plug-in v4.0.3

#### **CLI Plug-in Changelogs:**

- IBM CICS Plug-in v4.0.2
- IBM DB2 Plug-in v4.0.5
- IBM FTP Plug-in: v1.0.1
- IBM IMS Plug-in: v2.0.1
- IBM MQ Plug-in: v2.0.1

#### **Zowe Explorer**

Review the Zowe Explorer Change Log to learn about the latest features, enhancements, and fixes.

You can install the latest version of the extension from the Visual Studio Code Marketplace.

# **Bug fixes**

The following bugs were fixed:

#### Zowe z/OS Installation

Bugfix: zowe-configure-instance.sh does not allow the -c instance directory location to be an existing Zowe runtime. This caused a deadlock and running out of BPXAS instances. See Unable to create BPXAS instances. #1123

- Bugfix: subloggers would not inherit message translation maps from parent loggers. #24
- Bugfix: sample-angular-app could not be run from a folder outside of \$ROOT\_DIR. #34
- Bugfix: Menu locations were wrong when multiple apps opened because the numbers used partially came from the previous instance. #36
- Bugfix: Apps that were the target of app2app communication were not put into focus. #50
- Bugfix: Developers could not run app-server without a certificate authority. #98
- Bugfix: App server could not work with self-signed/invalid TLS certificates sometimes used in test/development, because the configuration option broke. The option has been restored. #103
- Bugfix: App server instance settings initialization had inconsistent write permissions. #105
- Bugfix: App server no longer issues warning about failure to load undefined log file. #182
- Bugfix: Fixes unformatted messages when a language is not specified. #186
- Bugfix: Editor would not work for unix files when used through api mediation layer due to encoded slash.
   #187
- Bugfix: App framework's right click menu could go off screen vertically at the bottom. #200
- Bugfix: zosmf-auth no longer issues configuration warning during startup. #398
- Doc Bugfix: Sample react app did not state its dependence on the sample angular app. #405
- Bugfix: Substitute zosmf-auth for apiml-auth to remove warning. #1232

# Version 1.9.0 LTS (February 2020)

Zowe v1.9.x is designated as the current Zowe Long-term Support (LTS) version.

# New features and enhancements

The following features and enhancements were added:

## **API Mediation Layer**

The following new features and enhancements have been made to the Zowe API Mediation Layer in this version:

- Support of special characters has been added to API Mediation Layer core services. In addition, all onboarding enablers now support special characters as well.
- Custom metadata support has been added to the onboarding enablers. Additional parameters can now be easily added to an expandable parameter array. This feature may be used for security configuration in the future.

- Passticket support has been added to API ML Core Services and onboarding enablers. This makes it easier to authenticate existing mainframe applications with the API Mediation Layer.
- New versions of Spring Boot based onboarding enablers (V1 and V2) have been released. These
  enablers support the new version of the metadata required by the Discovery Service. The new versions
  of the enablers consume significantly less disk space.

The following bug fixes have been introduced:

- A fix of a critical authentication issue with some versions of z/OSMF has been applied.
- A fix has been applied to support multipart requests.
- A fix has been applied to the z/OSMF authorization header.

- Added support for Node.js z/OS V12. See Installing Node.js on z/OS for details.
- A new endpoint for removing dataservices has been added #62
- Functionality for removing data sets has been added #65
- Deletion of data sets and their members is now supported #88
- Deletion of data sets and their members is now supported #85
- The following helper functions have been added to test caller's environment #115:
  - A function to test whether the caller is running in SRB
  - A function to test whether the caller is in cross-memory mode
  - A function to test whether the caller is holding a CPU, CMS, CML or local lock
- The logout endpoint has been re-added for zss #100
- Added support of SRB and locked callers to the Cross-Memory server's PC space switch routine #153
- This pull request add the following features #120: Ability to use the lock-free queue intrusively which allows a more flexible storage management on the user's side Functions to copy to/from foreign address space using destination/source keys and ALETs
- Reformatted the save as modal in zowe editor #129
- Added snackbar notification for directory error #131
- Removed language server tab in editor #134
- Explicitly call zss for logout to make sure cookies are known to be invalid #28
- The following changes have been made to Zlux server framework logging #174:
  - Added English resource files for messages
  - Added code to all error, warning, debug and informational logged outputs
  - Replaced most console.log calls with logger calls

- Support for HTTP-Strict-Transport-Security. Custom headers for static content are now available #173
- Functionality for controlling application access for individual users has been added #216
- Out-of-band multi-factor authentication is now supported #225

### Zowe CLI

To leverage the new features and plug-ins available in this version, you must follow the steps in Migrating to the LTS version.

The following new CLI plug-ins are added:

- IBM® z/OS FTP Plug-in for Zowe CLI
- IBM<sup>®</sup> IMS<sup>™</sup> Plug-in for Zowe CLI
- IBM<sup>®</sup> MQ Plug-in for Zowe CLI
- Secure Credential Store for Zowe CLI

The following new features and enhancements are added in this version:

- Notable Change: The zowe zos-files download ds and zowe zos-files download uf commands no longer put the full content in the response format json (--rfj) output. More information.
- Notable Change: The --pass option is changed to --password for all commands and profiles (zosmf, cics, etc...). The aliases --pw and --pass still function. To update a profile, issue the zowe profiles update command and use the new option name --password.
- Notable Change: You can enter PROMPT\* as a value for any CLI option to enable interactive prompting. If you wrote scripts in which any option is defined with the exact value PROMPT\*, the script will not execute properly in this version. For more information, see Using the prompt for sensitive options.
- Zowe CLI was tested and confirmed to run on Unix System Services (USS) on z/OS. For more information, refer to blog Installing Node.js on the Mainframe.

(The IBM Db2 and Secure Credential Store plug-ins for Zowe CLI will *not* run on z/OS due to native code requirements.)

• The zowe files copy command was added for copying the contents of a data set or member to another data set or member. #580

- Zowe CLI now exploits Node.js stream APIs for download and upload of spool files, data sets, and USS files. (#331)
- The following new commands were added for interacting with file systems:

```
    zowe zos-files list fs #429
```

- zowe zos-files mount fs #431
- zowe zos-files unmount fs #432
- The following new commands were added for creating USS files and directories:

```
    zowe zos-files create file #368
```

```
    zowe zos-files create dir #368
```

The IBM® CICS® Plug-in is updated with the following functionality:

- Define, enable, install, discard, disable, and delete CICS URIMaps. #53 #49 #48 #51 #50 #52
- Define and delete CICS web services. #58 #59
- Add and remove CSD Groups to/from CSD Lists #60.

### **Zowe Explorer**

Review the Zowe Explorer Change Log to learn about the latest features, enhancements, and fixes.

You can install the latest version of the extension from the Visual Studio Code Marketplace.

Watch a video on how to work with data sets using Zowe Explorer.

### **Bug fixes**

The following bugs were fixed:

### Zowe App Server

• URL encoding with % sign were always returning with authorization: false with RACF #27

- Users are no longer able to delete the initial "/" in the address bar for selected files #379
- The search bar text for datasets has been changed from "Enter a dataset" to "Enter a dataset query". The Address bar text for files has been changed from "Enter a directory" to "Enter an absolute path" #60

# Version 1.8.1 (February 2020)

# **Bug fixes for Zowe CLI**

A bug was fixed where Zowe CLI installation could fail and users could receive the following error message when installing Zowe CLI v1.8.0:

To install the fix, download the new v1.8.1 package from Zowe.org and retry the installation process.

# Version 1.8.0 (February 2020)

# New features and enhancements

The following features and enhancements were added.

### Installation of Zowe z/OS components

- The installation now just needs two parameters configured: the USS location of the runtime directory and a data set prefix where a SAMPLIB and LOADLIB will be created. The runtime directory permissions are set to 755 and when Zowe is run, no data is written to the runtime directory.
- The way to configure Zowe is changed. Previously, you configured Zowe at installation time with the zowe-install.yaml file. This file has been removed and is no longer used in this release.
- A new directory <u>zowe-instance-dir</u> has been introduced that contains configuration data used to launch Zowe. This allows more than one Zowe instance to be started from the same Zowe runtime directory. A new file <u>instance.env</u> within each <u>zowe-instance-dir</u> directory controls which ports are allocated to the Zowe servers as well as location of any dependencies such as Java, z/OSMF or node. No configuration data is specified at install time. The data is only read, validated and used at launch time. The <u>instance.env</u> file contains a parameter value <u>LAUNCH\_COMPONENT\_GROUPS</u> that allows you to control which Zowe subsystems to launch, for example you can run the Zowe desktop and not the API Mediation Layer, or vice-versa; you can run just the API Mediation Layer and not the Zowe desktop. The <u>zowe-instance-dir</u> directory is also where log files are collected. Static extensions to

the API Mediation Layer are recorded in the Zowe instance directory as well as any plug-in extensions to the Zowe desktop. This allows the runtime directory to be fully replaced during PTF upgrades or moving to later Zowe releases while preserving configuration data and extension definitions that are held in the instance directory.

- A new directory keystore-directory has been introduced outside of the Zowe runtime directory which is where the Zowe certificate is held, as well as the truststore for public certificates from z/OS services that Zowe communicates to (such as z/OSMF). A keystore directory can be shared between multiple Zowe instances and across multiple Zowe runtimes.
- All configuration of z/OS security that was done by Unix shell scripts during installation and configuration has been removed. A JCL member ZWESECUR is provided that contains all of the JCL needed to configure permissions, user IDs and groups, and other steps to prepare and configure a z/OS environment to successfully run Zowe. Code is included for RACF, Top Secret, and ACF/2.
- The Zowe cross memory server installation script zowe-install-apf-server.sh is removed. In this release, the steps for configuring z/OS security are included in the ZWESECUR JCL member.
- Previously, Zowe runs its two started tasks under the user ID of IZUSVR and admin of IZUADMIN. These belong to z/OSMF and are no longer used in this release. Instead, Zowe includes two new user IDs of ZWESVUSR (for the main Zowe started task), ZWESIUSR (for the cross memory server), and ZWEADMIN as a group. These user IDs are defaults and different ones can be used depending on site preferences.
- Previously, the main Zowe started task is called ZOWESVR . Now it is called ZWESVSTC .
- Previously, the cross memory started task is called ZWESIS01. Now it is called ZWESISTC.
- The script zowe-verify.sh is no longer included with Zowe. Now the verification is done at launch time and dependent on the launch configuration parameters. It is no longer done with a generic script function that zowe-verify.sh used to provide.

For more information about how to install Zowe z/OS components, see Installation roadmap.

### **API Mediation Layer**

- The API Catalog backend has been modified to support the OpenAPI 3.0 version. The API Catalog now supports the display of API documentation in the OpenAPI 3.0 format.
- A new Eureka metadata definition has been developed to enable service registration that does not require using existing pre-prepared enablers. Both new and old metadata versions are supported by the Discovery Service. Corresponding documentation to onboard a service with the Zowe API ML without an onboarding enabler has also been refactored.

 The plain Java enabler has been redesigned for simple and straight-forward API service configuration. Configuration parameters have been refactored to remove duplicates and unused parameters, and improve consistency with other parameters. Documentation to Onboard a REST API service with the Plain Java Enabler (PJE) has also been refactored.

### Zowe App Server

- The app server now issues a message indicating it is ready, how many plug-ins loaded, and where it can be accessed from #355
- Restructured the App server directories to separate writable configuration items from read-only install content #911 #627 #87 #43
- Move install-app script to instance directory bin folder for ease of use #966
- Access control for app visibility 216
- The following features and enhancements were made in the default apps:
  - UI changes for write support for datasets in editor #340
  - Support for QSAM and VSAM deletion in the ZSS dataset REST API #339
  - Editor: Dataset deletion capability [#229][#337]
  - Editor: File deletion UI changes #338
  - Editor fix: When saving a new file use the opened directory in the dialog #233
  - Editor fix: Disable text area for datasets in the absence of write ability #342
  - Editor fix: When saving a new file use the opened directory in the dialog #233

### Zowe CLI

- The Zowe CLI REST API now supports the following capabilities for managing data sets:
  - Rename sequential and partitioned data sets. #571
  - Migrate data sets. #558
  - Copy data sets to another data set and copy members to another member. #578
- The Zowe CLI REST API now supports HTTP ETags in response data. The ETag mechanism allows client applications to cache data more efficiently. ETAgs can also prevent simultaneous, conflicting updates to a resource. #598

### Zowe Explorer

Review the Zowe Explorer Change Log to learn about the latest features, enhancements, and fixes.

You can install the latest version of the extension from the Visual Studio Code Marketplace.

Check the new "Getting Started with Zowe Explorer" video to learn how to install and get started with the extension. For more information, see Zowe Explorer Extension for VSCode.

# **Bug fixes**

The following bugs were fixed.

### Zowe App Server

- Use of environment variables (\_TAG\_REDIR\_XXX) required to run Zowe with node v12 #333
- install-app.sh script would not work without first server run, improper permissions #373

### Zowe CLI

- Fixed an issue where zowe zos-jobs submit stdin command returned an error when handling data from standard in. #601
- Updated dependencies to address potential vulnerabilities. Most notably, Yargs is upgraded from v8.0.2 to v15.0.2. #333

# Version 1.7.1 (December 2019)

### New features and enhancements

The following features and enhancements were added.

### Zowe App Server

- A backup routine for when a non-administrator tries to access the API. Instead of executing privileged commands and failing, it will execute a command to get their profile, and return only the information in their scope. This is a feature that most people won't need, since you'd ideally want to be an administrator if you were using this API, but the functionality is there. (#114)
- The ability to retrieve profiles only by prefix. This can be done by looking for a profile with a "." at the end. This will act as a wildcard which extracts everything matching that prefix. (#114)

### Zowe SMP/E installation

The pre-release of the Zowe SMP/E build is updated to be based on Zowe Version 1.7.1.

# **Bug fixes**

The following bugs were fixed.

### **Zowe App Server**

- Fixed a bug where the end of an acid is cut off when getting the access list of a group, resulting in invalid output in the response.(#114)
- Fixed a bug where all of the different administrator suffixes weren't defined, so it was incorrectly returning administrators. (#114)

# Version 1.7.0 (November 2019)

### New features and enhancements

The following features and enhancements were added.

### **API Mediation Layer**

- Cleanup Gateway dependency logs (#413)
- Cleanup Gateway our code (#417)
- Cleanup Discovery Service dependency logs (#403)
- Cleanup Discovery Service our code (#407)
- External option to activate DEBUG mode for APIML (#410)

#### **Zowe App Server**

• Introduced the "SJ" feature to the JES Explorer application (#282)

You can now right-click a job label and click "Get JCL" to retrieve the JCL used to submit the job. This JCL can then be edited and resubmitted.

- File Explorer now offers a right click Delete option for files and folders (#43)
- Prevented creation/deletion of files and folders queued for deletion. (#48)
- Updated back-end API to give more accurate delete responses. (#93)

- IFrame adapter: added support for plugin definition, logger, and launch metadata. (#174)
- IFrame app-to-app communication support (#174)
- Removed unnecessary warning suppression (#23)
- Dispatcher always sends message, even when context doesn't exist (#174)
- Support constructor injectables via Iframe adapter (#174)
- Browser tab for the desktop now includes opened app name. (#175)
- File Explorer now offers a right click file and folder Properties menu. (#180)
- File Explorer now offers a right click dataset Properties menu. (#49)
- Made it possible to specify config properties via command line arguments for the App server. (#81)
- Allow override of configuration attributes using a -D argument syntax. (#154)
- Allow specifying environment variables that can be interpreted as JSON structures. (#156)

### Zowe Explorer (Extension for VSCode)

- The name of the extension was changed from "VSCode Extension for Zowe" to "Zowe Explorer".
- The VSCode Extension for Zowe contains various changes in this release. For more information, see the VSCode Change Log.

### **Bug fixes**

The following bugs were fixed.

### **API Mediation Layer**

Fixed a typo in Gateway startup script. (#427)

### Zowe App Server

Fixed notification click, time stamp, inconsistent notification manager pop up clicks, empty notification bubbles, and safari issue. (#171)

### Zowe CLI

This version of Zowe CLI contains various bug fixes that address vulnerabilities.

# Version 1.6.0 (October 2019)

No changes were made to API ML or Zowe CLI in this release.

### What's new in the Zowe App Server

The following features and enhancements are added:

- Added two NodeJS issues to the App Framework Troubleshooting section. #786
- Added a REST API for new core dataservices to administer the servers and plugins. #82
- Added pass through express router ws patcher in case plug-ins need it. #152, #149
- Updated security plugins to manage proxied headers so that unnecessary things are not put into the browser.#152, #26
- Clear cookie on complete logout.#152

### What's new in Zowe CLI

The following enhancement was added:

• The --wait-for-output and the --wait-for-active options were added. You can append these options to a zowe zos-jobs submit command to either wait for the job to be active, or wait for the job to complete and enter OUTPUT status. If you do not specify --vasc, you can use these options to check job return codes without issuing zowe zos-jobs view job-status-by-jobid <jobid>.

### What's new in the Visual Studio Code (VSC) Extension for Zowe

The Visual Studio Code (VSC) Extension for Zowe lets you interact with data sets and USS files from a convenient graphical interface. Review the Change Log to learn about the latest improvements to the extension.

You can download the latest version from the VSC Marketplace.

# Version 1.5.0 (September 2019)

# What's new in API Mediation Layer

The following features and enhancements are added:

- The Discovery Service UI now enables the user to log in using mainframe credentials or by providing a valid client certificate.
- API Catalog REST endpoints now accept basic authentication by requiring the user to provide a username and password.

The following bugs are fixed:

• A defect has been resolved where previously an authentication message was thrown in the service detail page in the API Catalog when the swagger JSON document link was clicked. The message requires the user to provide mainframe credentials but did not link to an option to authenticate. Now, a link is included to provide the user with the option to authenticate.

# What's new in the Zowe App Server

The following features and enhancements are added:

- Adds dynamic logging functionality for plugins (#60, #63)
- Top Secret updates to the security lookup API (#71, #72, #74)
- Accept basic auth header as an option for login (#80)
- JSON parsing enhancements for UTF8, and printing to buffer (#67)
- Optimization, memory bugfix and improved tracing for authentication (#72)
- Performance optimization for app thumbnail snapshots: Fixed a bug causing slowdown relative to number of apps open (#131)
- Translations: Added missing language translations about session lifecycle (#137)
- Logger reorganized for Zowe-wide log format unification. Includes i18n-able message ID support & new info. See #90 (#17, #119, #116, #142, #35, #19, #132, #146, #126, #139, #67, #133, #21)
- Establish rules & recommendations for conformance (#142)
- Launchbar menu of apps now has same context menu properties as pinned apps (#140)
- Properties App now shows the ID of the chosen plugin (#140)
- Added group permission for plugin access when installing via install script (#125)
- Updated URIBroker include new parameter for searching datasets with included trailing qualifiers (#34, #138)

- App2App communication now allows you to target a specific app instance, as well as to request minimization or maximization (#38, #148)
- Configuration Dataservice now can load plugin defaults from the plugin's own folder (#129)
- Configuration Dataservice can now support GET like HEAD (#140)
- Configuration Dataservice can now utilize binaries as opposed to JSON. This mode does not process the objects, just stores & retrieves. (#130)
- Added a notification menu, popup & API where messages can be sent by administrators to individual or all end users (#36, #144)
- Doc: Configuration Dataservice Swagger document updated for new features (#136)
- Desktop now supports loading a custom wallpaper, and the launchbar & maximized window style has been changed to improve screen real estate (#151)
- The App Server configuration and log verbosity can now be viewed and updated on-the-fly via a REST API (#66, #128)
- The App Server environment parameters and log output can now be viewed via a REST API (#66, #128)
- The App Server can now have Application plugins added, removed, and upgraded on-the-fly via a REST API (#137, #69)
- A dataservice can now import another import dataservice, as long as this chain eventually resolves to a non-import dataservice (#139)
- You can now open any Zowe App in its own browser tab by right clicking its icon and choosing "Open in new browser window" (#149, #150)
- Icons improved for datasets that are migrated/archived (#30)
- Support App2App to open a given dataset (#87, #35)
- Navigate the editor menu bar via keyboard (#85)
- Add keyboard shortcuts to open and close tabs (#81)
- Add loading indicator for dataset loading (#34)
- Compress the terminals with gzip for improved initial load time, same as was done with the editor previously (#22, #23)
- Made the following enhancements to the JES Explorer App
  - Add ability to open and view multiple Spool files at once (#99)
  - Migrate from V0 to V1 of Material UI (#98)
  - Migrate from V15 to V16 of React (#98)

### The following bugs are fixed:

• New directories/files from Unix file API would have no permissions (#75)

- Properties App can now be reused when clicking property of a second app (#140)
- Logout did not clear dispatcher App instance tracking (#32)
- Iframe Apps were not gaining mouse focus correctly (#37, #145)
- Remove placeholder swagger from swagger response when plugin-provided swagger is found (#139)
- ZSS Dataservices could fail due to incorrect impersonation environment variable setting (\_BPX\_SHAREAS) (#68)
- Restore focus of text on window restore (#84)
- Reposition menu from menu bar on Edge/Firefox (#82)
- Could not open the SSH terminal in single window mode (#21)

### What's new in Zowe CLI and Plug-ins

The following commands and enhancements are added:

You can append --help-web to launch interactive command help in your Web browser. For more information, see Interactive Web Help. (#238)

# Zowe SMP/E Alpha (August 2019)

A pre-release of the Zowe SMP/E build is now available. This alpha release is based on Zowe Version 1.4.0. Do not use this alpha release in production environment.

- To obtain the SMP/E build, go to the Zowe Download website.
- For more information, see Installing Zowe SMP/E Alpha.

# Version 1.4.0 (August 2019)

### What's new in API Mediation Layer

This release of Zowe API ML contains the following improvements:

- JWT token configuration
  - RS256 is used as a token encryption algorithm
  - JWT secret string is generated at the time of installation and exported as a .pem file for use by other services

- JWT secret string is stored in a key store in PKCS 11 format under "jwtsecret" name
- SonarQube problems fixed
  - Various fixes from SonarQube scan
- API Mediation Layer log format aligned with other Zowe services:
- Added an NPM command to register certificates on Windows. The following command installs the certificate to trusted root certification authorities:
- Cookie persistence changed
  - Changed the API Mediation Layer cookie from persistent to session. The cookie gets cleared between browser sessions.
- Fixed high CPU usage occurrence replicated in Broadcom (#282)
  - Changed configuration of LatencyUtils to decrease idle CPU consumption by API ML services
- API Mediation layer now builds using OpenJDK with OpenJ9 JVM

### What's new in the Zowe App Server

Made the following fixes and enhancements:

- Added the ability for the App Server Framework to defer to managers for dataservices that are not written in NodeJS or C. The first implementation is a manager of Java servlet type dataservices, where the App Server manages Tomcat instances when Tomcat is present. (#158)
- Added a tomcat xml configuration file with substitutions for values (ports, keys, certificates) necessary for the App Server to manage one or more instances of Tomcat for hosting servlet dataservices. Also added a new section to the zluxserver.json file to describe dataservice providers such as the aforementioned Tomcat Java Servlet one. (#49)
- Added Swagger API documentation support. Application developers can include a Swagger 2.0 JSON or YAML file in the app's /doc/swagger directory for each REST data service. Each file must have the same name as the data service. Developers can then reference the files at runtime using a new app route: /ZLUX/plugins/PLUGINID/catalogs/swagger. They can reference individual services at: /ZLUX/plugins/PLUGINID/catalogs/swagger/SERVICENAME. If swagger documents are not present, the server will use contextual knowledge to show some default values. (#159)
- The following new REST and cross-memory services have been added (#32):

- Extract RACF user profiles
- Define/delete/permit general RACF resource profiles (limited to a single class)
- Add/remove RACF groups
- Connect users to RACF groups (for a limited set of group prefixes)
- Check RACF user access levels (limited to a single class)
- Fixed multiple issues in the File Editor App. (#88)
- Fixed multiple ZSS file and dataset API issues (#49 #42 #40 #44 #45)
- Remove several CSS styles from the Desktop to prevent bleed-in of styles to Apps (#117)
- Fixed incorrect count of open Apps upon logging in more than once per browser session (#123) Add OMVS information API to uribroker (#116)
- Enhanced auth plugin structure for application framework that lists auth capabilities (#118 #14 #19)
- Improved searching for node libraries for dataservices within an plugin (#114)
- Editor & File Explorer Widget Changes
  - Unix directory listing now starts in the user's home directory (#16)
  - JCL syntax coloring revision (#73)
  - Cursor, scroll position and text selection is now kept while switching tabs in editor (#71)
  - Editor now scrolls tab bar to newest tab when opening, and tab scrolling improved when closing tabs (#69)
  - Tab name, tooltip, and scroll fixes (#55 #60 #63)
  - Change in double and single click behavior of file explorer widget (#21)
  - Fix to show language menu on new file (#62)
  - Fix to keep language menu within the bounds of app window (#59)
  - Fix to the delete file prompt (#61)
  - Fix to allow closing of multiple editor instances (#22)
  - Fix to query datasets correctly by making queries uppercase (#65)
- Fixed issue where the cascading position of new windows were wrong when that application was maximized. (#102)
- Fixed issue where the file tabs in File Editor app were vertically scrollable, and where the close button would not be accessible for long file names. (#170)
- Updated the package lock files in all repositories to fix vulnerable dependencies. (#163)
- Fixed an issue where the Desktop used the roboto-latin-regular font for all text, which would not display well with non-latin languages. Now the fallback font is sans-serif. (#118)

# What's new in Zowe CLI and Plug-ins

You can now explore the Zowe CLI command help in an interactive online format. See Zowe CLI Web Help.

The following new commands and enhancements are added:

- The VSCode Extension for Zowe now supports manipulation of USS files. (#32)
- You can now archive z/OS workflows using a wildcard. (#435)
- The z/OS Workflows functionality is now exported to an API. Developers can leverage the exported APIs to create applications and scripts without going through the CLI layer. (#482)
- The CLI now exploits all "z/OS data set and file REST interface" options that are provided in z/OSMF v2.3. (#491)

The following bugs are fixed:

- Fixed an issue where examples for zowe files list uss-files were slightly incorrect. (#440)
- Improved error message for zowe db2 call procedure command. (#22)

# Version 1.3.0 (June 2019)

# What's new in API Mediation Layer

This release of Zowe API ML contains the following user experience improvements:

- Added authentication endpoints (/login, /query) to the API Gateway
- Added the Gateway API Swagger document (#305)
  - Fixed the bug that causes JSON response to set incorrectly when unauthenticated
  - Fixed error messages shown when a home page cannot be modified
- Added a new e2e test for GW, and update the detail service tile (#309)
- Removed a dependency of integration-enabler-java on the gateway-common (#302)
- Removed access to the Discovery service UI with basic authentication (#313)
- Fixed the issue with the connection logic on headers to pass in the websocket (#275)
- Fixed the bug 264: Bypass the API Gateway when the server returns 302 (#276)
- Fixed the issue that causes the API ML Services display as UP, and makes the API doc available in the Catalog regardless whether the API ML Services stop (#287)
- Fixed the issue that prevents the API Catalog to load under zLux 9 (314)

### What's new in the Zowe App Server

Made the following fixes and enhancements:

- Added internationalization to the Angular and React sample applications. (#133)
- Made the following enhancements to the ZSS server:
  - Added support for Zowe on z/OS version 2.4. (#15)
  - Updated documentation for query parameter to file API. (#48)
- Made the following enhancements to security:
  - App Server session cookie is now a browser session cookie rather than having an expiration date.
     Expiration is now tracked on the server side. (#132, #97, #81)
  - Added a "mode=base64" option to the unixfile API. (#127)
- Added a port to the cookie name to differentiate multiple servers on same domain. (#95)
- Made the following fixes and enhancements to the Code Editor application:
  - Added a menu framework to provide options specific to the current file/data set type. (#131)
  - Added ISPF-like syntax highlighting for JCL. (#48)
  - Fixed an issue by notifying users if the editor cannot open a file or data set. (#148)
  - Fixed an issue with event behavior when a tab is closed. (#135)
  - Fixed an issue with not showing the content of files in Chrome and Safari. (#100)
  - Fixed an issue with files shown without alphabetical sorting. (#85)
- Made the following fixes and enhancements to the TN3270 application (#96):
  - Fixed an issue where the application could not be configured to default to a TLS connection.
  - Fixed an issue where it could not handle a TN3270 connection, only TN3270E. Improved preference saving. Administrators can now store default values for terminal mod type, codepage, and screen dimensions.
- Made the following fixes and enhancements for App2App for IFrames (#24, #107):
  - Fixed an issue with an exception when handling App2App communication with IFrames.
  - Added experimental support for App2App communication with an IFrame application as destination.
- Made the following enhancements to support TopSecret:
  - Added a user-profiles endpoint. (#113)
  - Added an endpoint extraction for groups. (#129)
- Fixed an issue with app names not being internationalized when translations were present. (#85)
- Fixed Russian language errors in translation files. (#100)
- Fixed several issues with using the Application Server as a proxy. (#93)
- Fixed an issue with the App Server throwing exceptions when authorization plugins were installed but not requested. (#94)

- Fixed an issue with ZSS consuming excessive CPU during download. (#147)
- Fixed documentation issue by replacing "zLUX" with "Zowe Application Framework" and "MVD" with "Zowe Desktop." (#214)
- Fixed an issue with an incorrect translation for word "Japanese" in Japanese. (#108)

# What's new in Zowe CLI and Plug-ins

The following new commands and enhancements are added:

- Return a list of archived z/OSMF workflows with the zowe zos-workflows list arw command.
   (#391)
- Return a list of systems that are defined to a z/OSMF instance with the zowe zosmf list systems command. (#348)
- The zowe uss issue ssh command now returns the exit code of the shell command that you issued. (#359)
- The zowe files upload dtu command now supports the metadata file named
   .zosattributes. (#366)

The following bugs are fixed:

- Fixed an issue where zowe workflow ls aw commands with the --wn option failed if there was a space in the workflow name. (#356)
- Fixed an issue where zowe zowe-files delete uss command could fail when resource URL includes a leading forward-slash. (#343).

# Version 1.2.0 (May 2019)

Version 1.2.0 contains the following changes since Version 1.1.0.

### What's new in the Zowe installer

- Made the following installer improvements:
  - Check whether ICSF is configured before checking Node version to avoid runaway CPU.
  - Warn if the host name that is determined by the installer is not a valid IP address.

- Fixed a bug where a numeric value is specified in ZOWE\_HOST\_NAME causing errors generating the Zowe certificate.
- Made the following improvements to the zowe-check-prereqs.sh script:
  - Improvements for checking and validating the telnet and ssh port required by the Zowe Desktop applications.

# What's new in API Mediation Layer

This release of Zowe API ML contains the following user experience improvements:

- Prevented the Swagger UI container on the service detail page from spilling.
- Added a check for the availability of the z/OSMF URL contained in the configuration. z/OSMF is used to verify users logging into the Catalog.
- Made PageNotFound error visible only in the debug log level.
- Added zD&T-compatible ciphers and the TLS protocol restricted to 1.2.
- Introduced support for VSCode development.
- Introduced a common cipher configuration property.
- Fixed URL transformation defects.
- Fixed reporting that the Catalog is down when it is started before the Discovery Service.
- Removed the bean overriding error message from the log.
- Fixed the state manipulation mechanism in the Catalog. As a result, no restoring of the application state is performed.
- Fixed the Catalog routing mechanism for a users who is already logged in so that the user is not prompted to log in again.
- A timeout has been set for Catalog login when z/OSMF is not responding.
- A tile change in the Catalog is now propagated to the UI.
- Fixed a problem with an incorrect service homepage link in the Catalog.
- The Catalog Login button has been disabled when the login request is in progress.

# What's new in the Zowe App Server

- Improved security by adding support for RBAC (Role Based Access Control) to enable Zowe to determine whether a user is authorized to access a dataservice.
- Added Zowe Desktop settings feature for specifying the Zowe desktop language.
- Added German language files.

- Fixed a bug by adding missing language files.
- Enabled faster load times by adding support for serving the Zowe Application Framework core components, such as the Desktop, as compressed files in gzip format.
- Added support for application plug-ins to serve static content, such as HTML, JavaScript, and images, to browsers in gzip and brotli compressed files.
- Fixed a Code Editor bug by separating browsing of files and data sets.

# What's new in Zowe CLI and Plug-ins

The Zowe CLI core component contains the following improvements and fixes:

- The zos-uss command group is added to the core CLI. The commands let you issue Unix System Services shell commands by establishing an SSH connection to an SSH server. For more information, see .
- The zowe zos-workflows command group now contains the following active-workflowdetails options:
  - --steps-summary-only | --sso (boolean): An optional parameter that lets you list (only) the steps summary.
  - --skip-workflow-summary | --sws (boolean): An optional parameter that lets you skip the default workflow summary.
- Zowe CLI was updated to correct an issue where the zowe zos-workflows start command ignored the -- workflow-name argument.
- Updated and clarified the description the -- overwrite option for the zowe zos-workflows create workflow-from-data-set command and the Zowe zos-workflows create workflow-from-uss-file command.
- The CLI Reference Guide is featured on the Zowe Docs home page. The document is a comprehensive guide to commands and options in Zowe CLI.
- You can now click the links on the Welcome to Zowe help section and open the URL in a browser window. Note that the shell application must support the capability to display and click hyperlinks.

### What's new in Zowe USS API

Made the following enhancements:

- Chtag detection and ASCII/EBDCIC conversion on GET & PUT requests. For details, see this issue.
- New optional header on GET Unix file content request to force conversion from ebcdic to ascii. For details, see this issue.
- New response header on GET Unix file content requests: E-Tag for overwrite detection and validation.
   For details, see this issue.
- Reintroduced PUT (update) Unix file content endpoint. For details, see this issue.
- Reintroduced DELETE Unix file content endpoint. For details, see this issue.
- Reintroduced POST (create) Unix file or directory endpoint. For details, see this issue.
- Fixed a problem with incorrect return error when the user requests to view contents of a USS folder they do not have permission to. Now it returns a 403 (Forbidden) error. For details, see this issue.

# Version 1.1.0 (April 2019)

Version 1.1.0 contains the following changes since the last 1.0.x version.

### What's new in Zowe system requirements

z/OSMF Lite is now available for non-production use such as development, proof-of-concept, demo and so on. It simplifies the setup of z/OSMF with only a minimal amount of z/OS customization, but provides key functions that are required. For more information, see Configuring z/OSMF Lite (for non-production use).

### What's new in the Zowe App Server

- Made the following user experience improvements:
  - Enabled the Desktop to react to session expiration information from the Zowe Application Server. If a user is active the Desktop renews their session before it expires. If a user appears inactive they are prompted and can click to renew the session. If they don't click, they are logged out with a session expired message.
  - Added the ability to programmatically dismiss popups created with the "zlux-widgets" popup manager.
- Made the following security improvements:
  - Encoded URIs shown in the App Server 404 handler, which prevents some browsers from loading malicious scripts.
  - Documented and support configuring HTTPS on ZSS.
  - For ZSS API callers, added HTTP response headers to instruct clients not to cache HTTPS responses from potentially sensitive APIs.

- Improved the Zowe Editor App by adding app2app communication support that allows the application to open requested directories, dataset listings, and files.
- Improved the Zowe App API by allowing subscription to close events on viewports instead of windows, which allows applications to better support Single App Mode.
- Fixed a bug that generated an extraneous RACF audit message when you started ZSS.
- Fixed a bug that would sometimes move application windows when you attempted to resized them.
- Fixed a bug in the "Getting started with the ZOWE WebUi" tutorial documentation.
- Fixed a bug that caused applications that made ZSS service requests to fail with an HTTP 401 error because of dropped session cookies.

# What's new in the Zowe CLI and Plug-ins

This release of Zowe CLI contains the following new and improved capabilities:

- Added APIs to allow the definition of workflows
- Added the option max-concurrent-requests to the zowe zos-files upload dir-to-uss command
- Added the option overwrite to the zowe zos-workflows create commands
- Added the option workflow-name to the zowe zos-workflows commands
- Added the following commands along with their APIs:
  - zowe zos-workflows archive active-workflow
  - zowe zos-workflows create workflow-from-data-set
  - zowe zos-workflows create workflow-from-uss-file
  - zowe zos-workflows delete active-workflow
  - zowe zos-files list uss-files

This release of the Plug-in for IBM DB2 Database contains the following new and improved capabilities:

- Implemented command line precedence, which lets users issue commands without the need of a DB2 profile.
- The DB2 plug-in can now be influenced by the ZOWE\_OPT\_ environment variables.

### What's new in API Mediation Layer

• Made the following user experience improvements:

- Documented the procedure for changing the log level of individual code components in *Troubleshooting API ML*.
- Documented a known issue when the API ML stops accepting connections after z/OS TCP/IP is recycled in the *Troubleshooting API ML*.

# Version 1.0.1 (March 2019)

Version 1.0.1 contains the following changes since the last version.

# What's new in Zowe installation on z/OS

During product operation of the Zowe Cross Memory Server which was introduced in V1.0.0, the z/OSMF user ID IZUSVR or its equivalent must have UPDATE access to the BPX.SERVER and BPX.DAEMON FACILITY classes. The install script will do this automatically if the installing user has enough authority, or provide the commands to be issued manually if not. For more information, see Installing the Zowe Cross Memory Server on z/OS

### What's new in the Zowe App Server

- Made the following improvements to security:
  - Removed the insecure SHA1 cipher from the Zowe App Server's supported ciphers list.
  - Added instructions to REST APIs to not cache potentially sensitive response contents.
  - Set secure attributes to desktop and z/OSMF session cookies.
- Fixed a bug that caused the configuration data service to mishandle PUT operations with bodies that were not JSON.
- Fixed a bug that prevented IFrame applications from being selected by clicking on their contents.
- Fixed various bugs in the File Explorer and updated it to use newer API changes.
- Fixed a bug in which App2App Communication Actions could be duplicated upon logging in a second time on the same desktop.

# What's new in Zowe CLI

- Create and Manage z/OSMF Workflows using the new <a href="mailto:zos-workflows">zos-workflows</a> command group. For more information, see Zowe CLI command groups.
- Use the @lts-incremental tag when you install and update Zowe CLI core or plug-ins. The tag ensures that you don't consume breaking changes that affect your existing scripts. Installation

procedures are updated to reflect this change.

- A CLI quick start guide is now available for users who are familiar with command-line tools and want to get up and running quickly.
- IBM CICS Plug-in for Zowe CLI was updated to support communication over HTTPS. Users can enable
   https by specifying --protocol https
   when creating a profile or issuing a command. For
   backwards compatibility, HTTP remains the default protocol.

# What's new in the Zowe REST APIs

Introduced new Unix files APIs that reside in the renamed API catalog tile z/OS Datasets and Unix files service (previously named z/OS Datasets service). You can use these APIs to:

- List the children of a Unix directory
- Get the contents of a Unix file

### What's changed

- Zowe explorer apps
  - JES Explorer: Enhanced Info/Error messages to better help users diagnose problems.
  - MVS Explorer: Fixed an issue where Info/Error messages were not displayed when loading a Dataset/Members contents.

# Version 1.0.0 (February 2019)

Version 1.0.0 contains the following changes since the Open Beta release.

### What's new in API Mediation Layer

- HTTPs is now supported on all Java enablers for onboarding API microservices with the API ML.
- SSO authentication using z/OSMF has been implemented for the API Catalog login. Mainframe credentials are required for access.

### What's new in Zowe CLI

- Breaking change to Zowe CLI: The --pass command option is changed to --password for all core Zowe CLI commands for clarity and to be consistent with plug-ins. If you have zosmf profiles that you created prior to January 11, 2019, you must recreate them to use the --password option. The aliases --pw and --pass still function when you issue commands as they did prior to this breaking change. You do not need to modify scripts that use --pass.
- The @next npm tag used to install Zowe CLI is deprecated. Use the @latest npm tag to install the product with the online registry method.

### What's new in the Zowe Desktop

- You can now obtain information about an application by right-clicking on an application icon and then clicking **Properties**.
- To view version information for the desktop, click the avatar in the lower right corner of the desktop.
- Additional information was added for the Workflow application.
- The titlebar of the active window is now colored to give an at-a-glance indication of which window is in the foreground.
- Window titlebar maximize button now changes style to indicate whether a window is maximized.
- Windows now have a slight border around them to help see boundaries and determine which window is active.
- Multiple instances of the same application can be opened and tracked from the launchbar. To open multiple instances, right-click and choose **Open New**. Once multiple instances are open, you can click the application icon to select which application to bring to the foreground. The number of orbs below the application icon relates to the number of instances of the application that is open.
- Desktop framework logging trimmed and formalized to the Zowe App Logger. For more information, see https://github.com/zowe/zlux/wiki/Logging.
- The UriBroker was updated to support dataservice versioning and UNIX file API updates.
- Removed error messages about missing components.js by making this optional component explicitly declared within an application. By using the property "webContent.hasComponents = true/false".

- Set the maximum username and password length for login to 100 characters each.
- Applications can now list webContent.framework = "angular" as an alias for "angular2".
- Fixed a bug where the desktop might not load on high latency networks.

### What's new in the Zowe App Server

- HTTP support was disabled in favor of HTTPS-only hosting.
- The server can be configured to bind to specific IPs or to hostnames. Previously, the server would listen on all interfaces. For more information, see https://github.com/zowe/zlux-app-server/pull/30.
- The core logger prefixes for the Zowe App Server were changed from "\_unp" to "\_zsf".
- Dataservices are now versioned, and dataservices can depend on specific versions of other dataservices. A plug-in can include more than one version of a dataservice for compatibility. For more information, see https://github.com/zowe/zlux/wiki/ZLUX-Dataservices.
- Support to communicate with the API Mediation Layer with the use of keys and certificates was added.
- Trimmed and corrected error messages regarding unconfigured proxies for clarity and understanding. For more information, see https://github.com/zowe/zlux-server-framework/pull/33.
- Fixed the nodeCluster.sh script to have its logging and environment variable behavior consistent with nodeServer.sh.
- Removed the "swaggerui" plug-in in favor of the API Catalog.
- Bugfix for /plugins API to not show the installation location of the plug-in.
- Bugfix to print a warning if the server finds two plug-ins with the same name.
- Added the ability to conditionally add HTTP headers for secure services to instruct the browser not to cache the responses. For more information, see https://github.com/zowe/zlux-serverframework/issues/36.
- Added a startup check to confirm that ZSS is running as a prerequisite of the Zowe App Server.
- Bugfix for sending HTTP 404 response when content is missing, instead of a request hanging.

• Added tracing of login, logout, and HTTP routing so that administrators can track access.

### What's changed

- Previously, APIs for z/OS Jobs services and z/OS Data Set services are provided sing an IBM WebSphere Liberty web application server. In this release, they are provided using a Tomcat web application server. You can view the associated API documentation corresponding to the z/OS services through the API Catalog.
- References to zlux-example-server were changed to zlux-app-server and references to zlux-proxy-server were changed to zlux-server-framework.

### **Known issues**

### Paste operations from the Zowe Desktop TN3270 and VT Terminal applications

**TN3270 App** - If you are using Firefox, the option to use Ctrl+V to paste is not available. Instead, press Shift + right-click to access the paste option through the context menu.

Pressing Ctrl+V will perform paste for the TN3270 App on other browsers.

**VT Terminal App** - In the VT Terminal App, Ctrl+V will not perform a paste operation for any browser.

**Note:** In both terminals, press Shift + right-click to access copy and paste options through the context menu.

**z/OS Subsystems App** - The z/OS Subsystems application is being removed temporarily for the 1.0 release. The reason is that as the ZSS has transitioned from closed to open source some APIs needed to be reworked and are not complete yet. Look for the return of the application in a future update.

# **Getting started with Zowe**

If you just started exploring Zowe, follow the path in this topic.

# Learning about Zowe

Learn what is Zowe, how Zowe works and what it can do for you.

### • Introduction video

Begin your journey with Zowe through this introductory video which is designed to give you an overview of Zowe's various components and features and get you familiar with them quickly.

### • Zowe overview

Refer to the overview topics to walk through basic concepts of Zowe, its components and benefits.

### • Zowe architecture

Review the Zowe architecture to understand how Zowe works.

### • Zowe FAQs

If you have a question, it's a good idea to try the FAQ, which answers the most commonly asked questions about Zowe.

### Release notes

Check out what's new with Zowe.

### • Zowe learning resources

Find a list of helpful Zowe resources on the web, including blogs, videos, webinars, courses, trials, and so on.

# Install and use

Now you know that Zowe consists of several components. You can determine which Zowe components to install and use. Follow the component-specific information roadmaps to install, use, and troubleshoot Zowe components. You can also get information about how to contribute to each specific component.

# Zowe versions for use with other products and plugins

While it is generally recommended that you use more recent releases of Zowe, users who intend to use Zowe as a prerequisite for a commercial product or plugin should refer to the documentation for those products to determine which versions of Zowe are compatible and have been tested with the commercial product in question.

Components to install and use	Information roadmaps
Zowe Application Framework, Zowe API Mediation Layer (these are installed as z/OS server components)	Information roadmap for Zowe Application Framework, Information roadmap for Zowe API Mediation Layer -
Zowe Explorer	Information roadmap for Zowe Explorer
Zowe CLI	Information roadmap for Zowe CLI
Zowe Client SDKs (under development)	Information roadmap for Zowe client SDKs
Zowe Mobile (Incubator)	Information roadmap for Zowe Mobile

# **Getting involved**

There are many ways to contribute to Zowe, and we welcome contributions! Read the contributor's guide to get started on the code and guidelines.

# Zowe CLI quick start

Get started with Zowe™ CLI quickly and easily.

**Note:** This section assumes some prerequisite knowledge of command-line tools and writing scripts. If you prefer more detailed instructions, see Installing Zowe CLI.

- Installing
- Issuing your first commands
- Using profiles
- Writing scripts
- Next Steps

# Installing

### **Software Requirements**

Before you install Zowe CLI, download and install Node.js and npm. Use an LTS version of Node.js that is compatible with your version of npm. For a list of compatible versions, see Node.js Previous Releases.

(Linux only): On graphical Linux, install gnome-keyring and libsecret on your computer before you install the Secure Credential Store. On headless Linux, follow the procedure documented in the SCS plug-in Readme.

### Installing Zowe CLI core from public npm

Issue the following commands in sequence to install the core CLI.

The "core" includes Zowe CLI and Secure Credential Store, which enhances security by encrypting your username and password.

### Installing CLI plug-ins

The command installs most open-source plug-ins, but the IBM Db2 plug-in requires additional configuration to install.

# Issuing your first commands

Issue zowe --help to display full command help. Append --help (alias -h) to any command to see available command actions and options.

To interact with the mainframe, type zowe followed by a command group, action, and object. Use options to specify your connection details such as password and system name.

# Listing all data sets under a high-level qualifier (HLQ)

# Downloading a partitioned data-set (PDS) member to local file

See Command Groups for a list of available functionality.

# **Using profiles**

Zowe profiles let you store configuration details such as username, password, host, and port for a mainframe system. Switch between profiles to quickly target different subsystems and avoid typing connection details on every command.

### **Profile types**

Most command groups require a <code>zosmf-profile</code>, but some plug-ins add their own profile types. For example, the CICS plug-in has a <code>cics-profile</code>. The profile type that a command requires is defined in the <code>PROFILE OPTIONS</code> section of the help response.

**Tip:** The first **zosmf** profile that you create becomes your default profile. If you don't specify any options on a command, the default profile is used. Issue **zowe profiles** -h to learn about listing profiles and setting defaults.

# Creating a zosmf profile

Notes:

- The port defaults to 443 if you omit the --port option. Specify a different port if your host system does not use port 443.
- If z/OSMF is configured for high availability in Sysplex, create the CLI zosmf-profile with DVIPA address/hostname to ensure availability of REST services. For more information, see Configuring z/OSMF high availability in Sysplex.

# Using a zosmf profile

For detailed information about issuing commands, using profiles, and more, see Using CLI.

# Writing scripts

You can write Zowe CLI scripts to streamline your daily development processes or conduct mainframe actions from an off-platform automation tool such as Jenkins or TravisCI.

# **Example:**

You want to delete a list of temporary datasets. Use Zowe CLI to download the list, loop through the list, and delete each data set using the zowe zos-files delete command.

For more information, see Writing scripts.

# **Next Steps**

You successfully installed Zowe CLI, issued your first commands, and wrote a simple script! Next, you might want to:

- Issue the zowe --help command to explore the product functionality, or review the online web help.
- Learn about using environment variables to store configuration options.
- Learn about integrating with API Mediation Layer.
- Write scripts and integrate them with automation server, such as Jenkins.
- See what plug-ins are available for the CLI.
- Learn about developing for the CLI (contributing to core and developing plug-ins).

# Information roadmap for Zowe API Mediation Layer

This roadmap outlines information resources that are applicable to the various user roles who are interested in Zowe API Mediation Layer. These resources provide information about various subject areas, such as learning basic skills, installation, developing, and troubleshooting for Zowe API Mediation Layer.

The following definition of skill levels about Zowe assist you with gathering the most relevant resources for you.

- Beginner: You're starting out and want to learn the fundamentals.
- Intermediate: You have some experience but want to learn more in-depth skills.
- Advanced: You have lots of experience and are looking to learn about specialized topics.

# **Fundamentals**

Zowe skill level: Beginner

### Zowe API Mediation Layer overview

New to API Mediation Layer? This overview topic introduces the key features, main components, benefits, and architecture of the API Mediation Layer.

### • Architecture

Review the Zowe architecture to understand how the API Mediation Layer works in the Zowe framework.

# Installing

Zowe skill level: Beginner

System requirements

Review this topic to ensure that your system meets the requirements for installing the API Mediation Layer. The API Mediation Layer is one of the server-side components.

### • Planning

This article includes details about planning for installation, the Zowe z/OS launch process, and information about the Zowe runtime directory, instance directory, and keystore directory.

### • Installing API Mediation Layer

This article provides an overview of the essential steps involved in installing the API Mediation Layer.

# **Configuring and updating**

Zowe skill level: Intermediate

### Configuring API Mediation Layer

#### • API Gateway configuration parameters

This article introduces the default configuration of the API Mediation Layer and how to change the parameters to meet your needs.

#### • Configuring the Zowe APIs

This article explains how to configure security for the Zowe API Mediation Layer.

• Advanced Gateway features configuration

This article is for system programmers who want to configure advanced Gateway features of the API Mediation Layer, such as the Gateway retry policy, connection limits, Gateway timeouts, and other advanced Gateway features.

### • Upgrading the z/OS system for Zowe

Learn how to upgrade the z/OS system for Zowe.

# **Using Zowe API Mediation Layer**

#### • Using API Catalog

Learn how to use the API Catalog to view what services are running in the API Mediation Layer. Through the API Catalog, you can also view associated API documentation corresponding to a service, descriptive information about the service, and the current state of the service.

#### • Blog: Introducing "Try it out" functionality in the Zowe API Mediation Layer

This blog describes one key functionality of the Zowe API Mediation Layer to validate that services are returning the expected responses.

#### • Docs: Zowe API reference guide

Discover and learn about Zowe APIs that you can use.

# **Onboarding APIs**

Zowe skill level: Advanced

#### Extend Zowe API Mediation Layer

Learn how you can extend the Zowe API Mediation Layer. Extenders make it possible to build and onboard additional API services to the API ML microservices ecosystem. REST APIs can register to the API Mediation Layer, which makes them available in the API Catalog, and for routing through the API Gateway.

#### Onboarding overview

This article provides details about onboarding a REST API service to the Zowe API Mediation Layer.

#### • Zowe API ML repository

To start working with the code immediately, check out this code repository.

# Security

#### API Mediation Layer Security

This article describes how API ML uses Transport Layer Security (TLS). Use this guide to familiarize yourself with the API ML security concepts.

#### Zowe API Mediation Layer Single-Sign-On Overview

This article provides an overview of the API ML single-sign-on feature, the principle participants in the SSO process, and links to detailed Zowe SSO documentation.

#### • Blog: The ZAAS Client: a library for the API Mediation Layer

This blog introduces you to Zowe Authentication and Authorization Service (ZAAS) Client — a library that contains methods for retrieval of JWT tokens, PassTickets, as well as verifying JTW token information.

#### • Blog: Single-Sign-On to z/OS REST APIs with Zowe

This blog takes a deeper dive into the SSO feature of API ML.

• Blog: Zowe client certificate authentication

# **Contributing to Zowe API Mediation Layer**

Zowe skill level: Advanced

### Contributing guidelines

This document is a summary of conventions and best practices for development within Zowe API Mediation Layer.

### Conformance Program

This topic introduces the Zowe Conformance Program. Conformance provides Independent Software Vendors (ISVs), System Integrators (SIs), and end users greater confidence that their software will behave as expected. As vendors, you are invited to submit conformance testing results for review and

approval by the Open Mainframe Project. If your company provides software based on Zowe CLI, you are encouraged to get certified today.

### Blog: Zowe Conformance Program Explained

This blog describes the Conformance Program in more details.

# **Troubleshooting and support**

### Troubleshooting API ML

Learn about the tools and techniques that are available to help you troubleshoot and resolve problems. You can also find a list of common issues about Zowe API ML.

#### • Error Message Codes

Use the message code references and the corresponding reasons and actions to help troubleshoot issues.

#### • Sumit an issue

If you have an issue that is specific to Zowe API Mediation Layer, you can submit an issue against the api-layer repo.

# **Community resources**

### • Slack channel

Join the #zowe-api Slack channel to ask questions about Zowe API ML, propose new ideas, and interact with the Zowe community.

#### • Zowe API ML squad meetings

You can join one of the Zowe API ML squad meetings to get involved.

#### • Zowe Blogs on Medium

Read a series of blogs about Zowe on Medium to explore use cases, best practices, and more.

Community Forums

Look for discussion on Zowe topics on the Open Mainframe Project Community Forums.

# Information roadmap for Zowe Application Framework

This roadmap outlines information resources that are applicable to the various user roles who are interested in Zowe Application Framework. These resources provide information about various subject areas, such as learning basic skills, installation, developing, and troubleshooting for Zowe Application Framework.

The following definition of skill levels about Zowe will help you gather most relevant resources for you.

- Beginner: You're starting out and want to learn the fundamentals.
- Intermediate: You have some experience but want to learn more in-depth skills.
- Advanced: You have lots of experience and are looking to learn about specialized topics.

### **Fundamentals**

Zowe skill level: Beginner

#### Zowe Application Framework overview

New to Zowe Application Framework? This overview topic introduces what is Zowe Application Framework and the main components and benefits.

#### • Architecture

Review the Zowe architecture to understand how Zowe Application Framework works in the Zowe framework.

#### • An Introduction to the Zowe Virtual Desktop

This blog gives you an overview of the Zowe Desktop.

### Installing

Zowe skill level: Beginner

#### • System requirements

Review this topic to ensure that your system meets the requirements for installing the Zowe Application Framework. Zowe Application Framework is one of the server-side components.

#### • Planning

This article provides details about planning for the installation, the Zowe z/OS launch process, and so on.

#### Installing Zowe Application Framework

This article provides an overview of the essential steps involved in installing Zowe Application Framework. If you want to use Docker for the installation, instead follow the link below.

#### Installing Zowe Application Framework using Docker

Learn how to use Docker to install Zowe.

## **Configuring and updating**

Zowe skill level: Intermediate

#### Configuring Zowe Application Framework

This information describes how to configure the Zowe Application Framework as a Mediation Layer client, configure connections for the terminal application plug-ins, modify the Zowe Application Server and Zowe System Services (ZSS) configuration, and so on.

#### • Upgrading the z/OS system for Zowe

Learn how to upgrade Zowe API Mediation Layer to a more recent version.

### **Using Zowe Application Framework**

#### • Using the Zowe Desktop

Learn about how to navigate the Zowe Desktop and use a list of pre-installed application plug-ins.

#### • Using the Editor

Learn how to use the Editor application plug-in.

#### • Tutorial: Getting started tutorial

This tutorial walks you through the Zowe Desktop with several simple tasks to help you get familiar with it.

### **Developing Zowe Desktop plug-ins**

Zowe skill level: Advanced

#### Developing for Zowe Application Framework

Learn how you can extend the Zowe Application Framework by adding a plug-in to the Zowe Desktop.

#### Zowe Application Framework repository

If you want to start working with the code immediately, check out this code repository.

#### • Zowe App Server scripts

This is the default setup of the Zowe App Server, built upon the zLUX framework. Within, you will find a collection of build, deploy, and run scripts as well as configuration files that will help you to configure a simple App Server and add a few Apps.

#### Samples

- Sample iframe App
- Sample Angular App
- Sample React App

# **Contributing to Zowe Application Framework**

#### Conformance Program

This topic introduces the Zowe Conformance Program. Conformance provides Independent Software Vendors (ISVs), System Integrators (SIs), and end users greater confidence that their software will behave as expected. As vendors, you are invited to submit conformance testing results for review and approval by the Open Mainframe Project. If your company provides software based on Zowe CLI, you are encouraged to get certified today.

#### Blog: Zowe Conformance Program Explained

This blog describes the Conformance Program in more details.

### **Troubleshooting and support**

#### Troubleshooting Zowe Application Framework

Learn about the tools and techniques that are available to help you troubleshoot and resolve problems. You can also find a list of common issues about Zowe Application Framework.

#### • Sumit an issue

If you have an issue that is specific to Zowe Application Framework, you can submit an issue against the zlux repo.

### **Community resources**

Slack channel

Join the Slack channel to ask questions, propose new ideas, and interact with the Zowe community.

#### • Zowe WebUI squad meetings

You can join one of the Zowe WebUI squad meetings to get involved.

Zowe Blogs on Medium

Read a series of blogs about Zowe on Medium to explore use cases, best practices, and more.

### Community Forums

Look for discussion on Zowe topics on the Open Mainframe Project Community Forums.

# **Information roadmap for Zowe CLI**

This roadmap outlines the information resources that are available for all user roles who are interested in Zowe CLI. These resources provide information about various subject areas, such as learning basic skills, installation, developing, and troubleshooting for Zowe CLI.

The following definition of skill levels about Zowe will help you gather most relevant resources for you.

- Beginner: You're starting out and want to learn the fundamentals.
- Intermediate: You have some experience but want to learn more in-depth skills.
- Advanced: You have lots of experience and are looking to learn about specialized topics.

## **Fundamentals**

Zowe skill level: Beginner

• Zowe CLI overview

New to Zowe CLI? This overview topic introduces what is Zowe CLI.

• Architecture

Review the Zowe architecture to understand how Zowe CLI works in the Zowe framework.

#### • Zowe CLI FAQs

If you have a question, it's a good idea to try the FAQ, which answers the most commonly asked questions about Zowe CLI.

# **Quick start**

Zowe skill level: Beginner

• Zowe CLI quick start

Get started with Zowe CLI quickly and easily.

• Blog: Getting Started with Zowe CLI

This blog enables you to get started with Zowe CLI quickly.

### Installing

Zowe skill level: Beginner

#### • System requirements

Review this topic to ensure that your system meets the requirements for installing Zowe CLI.

#### • Installing Zowe CLI

Follow the steps to install a new release of Zowe CLI.

### **Configuring and updating**

Zowe skill level: Intermediate

#### Configuring Zowe CLI

This topic explains how to configure Zowe CLI, such as changing log levels and setting the home directory location.

#### Updating Zowe CLI

Learn how to update Zowe CLI to a more recent version using different methods.

### Using Zowe CLI and plug-ins

Zowe skill level: Intermediate

#### • Using Zowe CLI

Learn about how to use Zowe CLI, including connecting to the mainframe, managing profiles, integrating with API Mediation Layer, and more.

#### • Zowe CLI extensions and plug-ins

This information guides you to explore the extensions and plug-ins available to Zowe CLI and install plug-ins to extend the capabilities of Zowe CLI. Plug-ins add functionality to the product in the form of new command groups, actions, objects, and options.

#### • Docs: Zowe CLI command reference guide

View detailed documentation on commands, actions, and options in Zowe CLI. The reference document is based on the @zowe-v1-lts version of the CLI. You can read an interactive online version, download a PDF document, or download a ZIP file containing the HTML for the online version:

- Browse online
- Download CLI reference in PDF format
- Download CLI reference in ZIP format
- Best practices

Are you looking for recommendations and tips on how to best use Zowe CLI to meet your needs? These resources provide best practices recommendations.

- Blog: Zowe CLI Tips & Tricks
- Zowe CLI and TSO commands

This blog shows how to configure and use the TSO command feature of Zowe.

# **Developing a Zowe CLI plug-in**

Zowe skill level: Advanced

Zowe CLI extenders can build plug-ins that provide new commands.

• Developing for the CLI

Learn about developing for Zowe CLI.

#### • Zowe CLI core repository

If you want to start working with the code immediately, check out this code repository.

#### • Tutorials

Follow these tutorials to get started working with a sample plug-in.

# **Contributing to Zowe CLI**

Zowe skill level: Advanced

#### • Contributing guidelines

This document is a summary of conventions and best practices for development within Zowe CLI or development of Zowe CLI plug-ins. The guidelines contain critical information about working with the code, running/writing/maintaining automated tests, developing consistent syntax in your plug-in, and ensuring that your plug-in integrates with Zowe CLI properly.

#### Conformance Program

This topic introduces the Zowe Conformance Program. Conformance provides Independent Software Vendors (ISVs), System Integrators (SIs), and end users greater confidence that their software will behave as expected. As vendors, you are invited to submit conformance testing results for review and approval by the Open Mainframe Project. If your company provides software based on Zowe CLI, you are encouraged to get certified today.

#### Blog: Zowe Conformance Program Explained

This blog describes the Conformance Program in more details.

### **Troubleshooting and support**

Troubleshooting Zowe CLI

Learn about the tools and techniques that are available to help you troubleshoot and resolve problems. You can also find a list of common issues about Zowe CLI.

#### • Sumit an issue

If you have an issue that is specific to Zowe CLI, you can submit an issue against the zowe-cli repo.

### **Community resources**

#### • Slack channel

Join the #zowe-cli Slack channel to ask questions about Zowe CLI, propose new ideas, and interact with the Zowe community.

#### • Zowe CLI squad meetings

You can join one of the Zowe CLI squad meetings to get involved.

#### • Zowe CLI Blogs on Medium

Read a series of blogs about Zowe CLI on Medium to explore use cases, best practices, and more.

#### Community Forums

Look for discussion on Zowe topics on the Open Mainframe Project Community Forums.

# **Information Roadmap for Zowe Explorer**

This roadmap outlines the information resources that are applicable to the users who are interested in Zowe Explorer. These resources provide information about various subject areas, such as learning basic skills, installation, developing, and troubleshooting for Zowe Zowe Explorer.

The following definition of skill levels about Zowe Explorer helps you find the most relevant resources:

- Beginner: You're starting out and want to learn the fundamentals.
- Intermediate: You have some experience but want to learn more in-depth skills.
- Advanced: You have lots of experience and are looking to learn about specialized topics.

## **Fundamentals**

Zowe skill level: Beginner

#### • Zowe Explorer overview

New to Zowe Explorer? This overview topic introduces the key features, main components, and benefits of Zowe Explorer.

#### • Zowe Explorer FAQs

If you have a question, review the FAQ, which answers the most commonly asked questions about Zowe Explorer.

#### • Blog: Visual Studio Code for Mainframe Via the Zowe Explorer Extension

This Meduim article outlines the basics of Zowe Explorer, including Getting Started videos.

## Installing and configuring

Zowe skill level: Beginner

#### • Installing Zowe Explorer

This page includes the system requirements and steps for installing the Zowe Explorer.

- Video: Getting started with Zowe Explorer (Part 1)
- Video: Getting started with Zowe Explorer (Part 2)

These videos help you to get started with Zowe Explorer and show the basic data set use cases.

• Zowe Explorer Profiles

This page describes how to create and work with Zowe Explorer profiles. Having a profile enables you to use all functions of the extension, activate the Secure Credential Store plug-in to securely store credentials, and more.

### **Using Zowe Explorer**

Zowe skill level: Intermediate

#### Using Zowe Explorer

This page includes usage tips and sample use cases for data sets, USS files, JOBs, and TSO commands. Familiarize yourself with the extension and make the best use of available options and features.

### **Extending Zowe Explorer**

Zowe skill level: Advanced

#### Extend Zowe Explorer

This page describes how to create an extension for Zowe Explorer to introduce more functionalities.

• Zowe Explorer FTP Extension

This document in Zowe Explorer repository describes how to install and use the FTP extension, which adds the FTP protocol to the Zowe Explorer VS Code extension, allowing you to use z/OS FTP Plug-in for Zowe CLI profiles to connect and interact with z/OS USS.

#### • Zowe Explorer repository

The GitHub repository of contains the source code of Zowe Explorer and other Zowe Explorer-related extensions. Check out the landing page README in the repository to find out how to contribute to the extension.

#### • Developing for Eclipse Theia

This article contains information on how to develop for Eclipse Theia.

### **Contributing to Zowe Explorer**

Zowe skill level: Advanced

#### Contributing guidelines

This document is intended to be a living summary of conventions & best practices for development of the Visual Studio Code Extension for Zowe.

#### Conformance Program

This topic introduces the Zowe Conformance Program. Conformance provides Independent Software Vendors (ISVs), System Integrators (SIs), and end users greater confidence that their software will behave as expected. As vendors, you are invited to submit conformance testing results for review and approval by the Open Mainframe Project. If your company provides software based on Zowe CLI, you are encouraged to get certified today.

#### Blog: Zowe Conformance Program Explained

This Medium article provide more details about the Conformance Program, including useful references.

## **Troubleshooting and support**

Troubleshooting Zowe Explorer

Learn about the tools and techniques that are available to help you troubleshoot and resolve problems. You can also find the list of Zowe Explorer issues.

#### • Submit an issue

If you have an issue that is specific to Zowe Explorer, you can submit an issue against the vscodeextension-for-zowe repository.

### **Community resources**

#### • Slack channel

Join the **#** zowe-explorer Slack channel to ask questions, propose new ideas, and interact with the Zowe community.

#### • Zowe Explorer squad meetings

You can join one of the Zowe Explorer squad meetings to get involved.

#### • Zowe Blogs on Medium

Read a series of blog articles about Zowe on Medium to explore use cases, best practices, and more.

#### • Community Forums

Look for discussion on Zowe topics on the Open Mainframe Project Community Forums.

```
Version: v1.25.x LTS
```

# **Information roadmap for Zowe Client SDKs**

This roadmap outlines information resources that are applicable to the various user roles who are interested in Zowe Client Software Development Kits (SDKs) which is a Zowe component still under development. These resources provide information about various subject areas, such as learning basic skills, installation, developing, and troubleshooting for Zowe Client SDKs.

The following definition of skill levels about Zowe will help you gather most relevant resources for you.

- Beginner: You're starting out and want to learn the fundamentals.
- Intermediate: You have some experience but want to learn more in-depth skills.
- Advanced: You have lots of experience and are looking to learn about specialized topics.

# **Fundamentals**

Zowe skill level: Beginner

Zowe Client SDK overview

New to Zowe Client SDKs? This overview topic briefly introduces what it is.

• Blog: Zowe SDKs - Build z/OS Connected Applications Faster

This blog introduces the Zowe SDKs and their benefits.

# Installing

Zowe skill level: Beginner

System requirements

Review this topic to ensure that your system meets the requirements for installing Zowe Client SDKs.

• Installing Zowe SDK

Follow the steps to install Zowe SDKs. You can pull the packages from an online registry, or download the packages from Zowe.org to install locally.

# **Using Zowe Client SDKs**

Zowe skill level: Intermediate

#### Zowe Node.js SDK

• Using Zowe Node.js SDKs

This information provides links to different pakcage Readmes that describes how to use the Zowe Node SDK.

• Docs: Node.js SDK reference guide

Refer to the following Zowe Client SDK reference guides for information about the API endpoints:

- Browse Node SDK reference guide online
- Download SDK reference guide in ZIP format
- Zowe SDK Sample Scripts

This repository contains some sample scripts that utilize various components of the Zowe SDKs organized by use cases.

#### **Zowe Python SDK**

• Using Zowe Python SDKs

This information provides links to different pakcage Readmes that describes how to use the Zowe Python SDK.

Docs: Python SDK reference guide

Refer to the following Zowe Client SDK reference guides for information about the API endpoints:

• Browse Python SDK reference guide online

• Download SDK reference guide in PDF format

# **Contributing to Zowe Client SDKs**

Zowe skill level: Advanced

#### Contributing guidelines

This document is a summary of guidelines for development within Zowe SDKs. You can contribute to add features, enhancements, and bug fixes to the source code.

### **Troubleshooting and support**

#### • Sumit an issue

If you have an issue that is specific to Zowe SDKs, you can submit an issue against the zowe-cli repo.

### **Community resources**

#### Slack channel

Join the #zowe-cli Slack channel to ask questions about Zowe CLI and Zowe SDKs, propose new ideas, and interact with the Zowe community.

#### Zowe CLI squad meetings

You can join one of the Zowe CLI squad meetings to discuss Zowe SDKs issues and contibute to Zowe SDKs.

#### Zowe Blogs on Medium

Read a series of blogs about Zowe on Medium to explore use cases, best practices, and more.

#### Community Forums

Look for discussion on Zowe topics on the Open Mainframe Project Community Forums.

```
Version: v1.25.x LTS
```

# **Information roadmap for Zowe Mobile**

This roadmap outlines the information resources that are available for all user roles who are interested in the Zowe Mobile Application that is still under incubation. These resources provide information about various subject areas, such as learning basic skills, installation, developing, and troubleshooting for Zowe Client SDKs.

The following definition of skill levels about Zowe will help you gather most relevant resources for you.

- Beginner: You're starting out and want to learn the fundamentals.
- Intermediate: You have some experience but want to learn more in-depth skills.
- Advanced: You have lots of experience and are looking to learn about specialized topics.

# **Fundamentals**

Zowe skill level: Beginner

#### Blog: Zowe On The Go: A Mobile Application For Modern Mainframers

This blog by Jessielaine Punongbayan, introduces what is the Zowe mobile application, how it's developed, its architecture, use case and so on.

Video: A Mobile Application For Modern Mainframers

Watch this video that introduces the Zowe Mobile App in about 1 minute.

Video: The Zowe Mobile Application

This video gives a demo of what the Zowe Mobile App would look like on your phone.

# Installing

Zowe skill level: Beginner

#### Zowe Mobile Application repository

This README file in the Zowe Mobile App source code repository describes the prerequisites and steps for installing this app.

## **Community resources**

• Slack channel

Join the Zowe Slack community to ask questions about Zowe Mobile App, propose new ideas, and interact with the Zowe community.

#### • Zowe Blogs on Medium

Read a series of blogs about Zowe on Medium to explore use cases, best practices, and more.

• Community Forums

Look for discussion on Zowe topics on the Open Mainframe Project Community Forums.

Version: v1.25.x LTS

# **Zowe learning resources**

Learn more about Zowe from these blog posts, videos, and other resources.

# Blogs

- Zowe blogs on Medium
- Zowe blogs on Open Mainframe Project website

Want to contribute a blog? Details for how to contribute to the Zowe blogs on Medium site are at Zowe Blog Guidelines.

## Videos

As well as Zowe videos owned and managed by the community, there are a number of external youtubers who host Zowe related content.

- Zowe Demos playlist from Bill Pereira
- Mainframe Bytes channel from Jessielaine Punongbayan

# Webinars

Find out what's happening with Zowe in the Zowe Quarterly Update Webinar Series.

- Zowe Quarterly Update Webinar: July 2021
- Zowe Quarterly Update Webinar: April 2021
- Zowe Quarterly Update Webinar: January 2021
- Zowe Quarterly Update Webinar: October 2020

The OMP Youtube channel also offers other webinars about Zowe.

- Treat Yourself to a Guided, Comprehensive Tour of Zowe Desktop Applications
- Zowe Webinar Feb. 22, 2019
- Open Mainframe Project Webinar: Zowe Virtual Hackathon

# Community

#### Join us on Slack

- Slack invite link
- Introduction to Zowe Slack channels

#### Learn more about the community

• Zowe community GitHub repo

Find out information about Zowe sub-projects, GitHub repos, mailing lists, community meeting minutes, contribution guidelines, and so on.

#### Connect with the community through meetings

• Zowe meeting calendar

You can join one of the Zowe meetings to get latest Zowe updates and get involved in different squads and initiatives.

## Training

#### Courses

#### • Zowe Basics

Interskill Learning offers a free training course that introduces the components that comprise Zowe and the benefits of using Zowe and how its capabilities can be extended.

#### Trials

• Zowe trial

The Zowe trial hosted by IBM is a fully configured z/OS environment with Zowe preinstalled and set up along with a set of integrated easy-to-follow tutorials that walk you through the basics of Zowe and gives you hands-on experience of extending Zowe. This no-charge trial is available in two hours for three days.

#### • Get started with the Zowe Web UI

This online tutorial hosted by IBM guides you to add new apps to the Zowe Web UI. It provides a public hosted Zowe instance that allows you to perform the steps in a z/OS environment.

# **Overview**

The installation of Zowe<sup>™</sup> consists of the following processes:

• installation of the Zowe server components.

You can install the components either on z/OS only or you can install the components both on z/OS and on Docker.

• installation of Zowe CLI on a desktop computer.

The Zowe server components provide a web desktop that runs a number of applications such as API Mediation Layer that includes the Single Sign-on (SSO) capability, organization of the multiple Zowe servers under a single website, and other useful features for z/OS developers.

Because Zowe is a set of components, before installing Zowe, use this guide to determine which components you want to install and where you want to install them.

Consider the following scenarios:

- If you plan to use Zowe CLI on PC only, you may not need to install the Zowe server components. Note: Some CLI plug-ins require the installation of components on z/OS. If you plan to use core Zowe CLI groups from your PC, the z/OS you connect to does not require any components of Zowe to be installed on z/OS, unless you want to take advantage of advanced authentication methods such as single signon or multi-factor authentication.
- If you use the Docker technical preview to run the Linux parts of Zowe in a container, you only need to configure the Zowe z/OS component to start the ZSS server.

# Installation roadmap

When you install Zowe<sup>™</sup> on z/OS, you install the following two parts:

- 1. The Zowe runtime, which consists of the following components:
  - Zowe Application Framework (ZLUX)
  - Zowe API Mediation Layer
  - Z Secure Services (ZSS)
  - z/OS Explorer Services
- 2. The Zowe Cross Memory Server, which is an APF authorized server application that provides privileged services to Zowe in a secure manner.

Zowe provides the ability for some of its unix components to be run not under USS, but as a Linux Docker container, see Installing Zowe Server Components using Docker. Technical Preview

If you want to configure Zowe for high availability, see Installing Zowe Server Components in Sysplex for instructions.

Review the installation diagram and the introduction in this topic to see the general installation sequence and the most important tasks that are to be performed during installation and configuration. You can click each step on the diagram for detailed instructions.

## **Stage 1: Plan and prepare**

Before you start the installation, review the information on hardware and software requirements and other considerations. See Planning the installation for details.

# Stage 2: Install the Zowe z/OS runtime

1. Ensure that the software requirements are met. The prerequisites are described in System requirements.

#### 2. Choose the method of installing Zowe on z/OS.

The Zowe z/OS binaries are distributed in the following formats. They contain the same contents but you install them by using different methods. You can choose which method to use depending on your needs.

#### • Convenience build

The Zowe z/OS binaries are packaged as a PAX file. You install this build by running shell script within a UNIX System Services (USS) shell. Convenience builds are full product installs.

#### • SMP/E build

The Zowe z/OS binaries are packaged as the following files that you can download. You install this build through SMP/E.

- A pax.Z file, which contains an archive (compressed copy) of the FMIDs to be installed.
- A readme file, which contains a sample job to decompress the pax.Z file, transform it into a format that SMP/E can process, and invoke SMP/E to extract and expand the compressed SMP/E input data sets.

While the procedure to obtain and install the convenience build or SMP/E build are different, the procedure to configure a Zowe runtime are the same irrespective of how the build is obtained and installed.

- 3. Obtain and install the Zowe build.
  - For how to obtain the convenience build and install it, see Installing Zowe runtime from a convenience build.
  - For how to obtain the SMP/E build and install it, see Installing Zowe SMP/E.

After successful installation of either a convenience build or an SMP/E build, there will be a zFS folder that contains the unconfigured Zowe runtime <RUNTIME\_DIR>, a SAMPLIB library SZWESAMP that contains sample members, and a load library SZWEAUTH that contains load modules. The steps to prepare the z/OS environment to launch Zowe are the same irrespective of the installation method.

# Stage 3: Configure the Zowe z/OS runtime

You can configure the Zowe runtime with one of the following methods depending on your needs.

- Use JCL and shell scripts
- Use z/OSMF Workflows

Tip: We recommend you open the links to this configuration procedure in new tabs.

1. Configure the z/OS security manager to prepare for launching the Zowe started tasks. For instructions, see Configuring the z/OS system for Zowe and Configuring Zowe with z/OSMF workflows.

A SAMPLIB JCL member ZWESECUR is provided to assist with the configuration. You can submit the ZWESECUR JCL member as-is or customize it depending on site preferences.

If Zowe has already been launched on the z/OS system from a previous release of Version 1.8 or later, then you are applying a newer Zowe build. You can skip this security configuration step unless told otherwise in the release documentation.

2. Configure the Zowe TLS. For instructions, see Configuring Zowe certificates and Configuring Zowe with z/OSMF workflows.

If you have already created a keystore directory from a previous release of Version 1.8 or later, then you may reuse the existing keystore directory.

The Zowe keystore directory contains the key used by the Zowe desktop and the Zowe API mediation layer to secure its TLS communication with clients (such as web browsers or REST AI clients). The keystore directory also has a truststore where public keys of any servers that Zowe communicates to (such as z/OSMF) are held.

A keystore directory needs to be created for a Zowe instance to be launched successfully, and a keystore directory can be shared between Zowe instances and between Zowe runtimes, including between different Zowe releases, unless specified otherwise in the release documentation.

- 3. Configure and start the ZWESISTC cross memory server and install the load libraries. For instructions, see Installing and configuring the Zowe cross memory server (ZWESISTC) and Configuring the Zowe cross memory server with z/OSMF workflow.
- 4. Create and customize an instance directory that contains configuration data required to launch a Zowe runtime and is where log files are stored. For instructions, see Creating and configuring the Zowe instance directory and Configuring Zowe with z/OSMF workflows.

A single Zowe runtime can be launched multiple times from different instance directories, each specifying different port ranges, applications to include at start-up, paths of associated runtimes (Java,

Node, z/OSMF).

Next, you will install and configure the Zowe started tasks. Zowe has two high-level started tasks: ZWESVSTC that launches the Zowe desktop and API mediation layer address spaces, and ZWESISTC that is a cross memory server that runs all of the APF-authorized code. The JCLs for the tasks are included in the PDS SAMPLIB SZWESAMP installed by Zowe and the load modules for the cross memory server are included in the PDS load library SZWEAUTH.

#### Note

For more information about Gateway and Discovery Service parameters that can be set during the Zowe runtime configuration, see API Gateway runtime configuration parameters and Discovery Service runtime configuration parameters.

5. Configure and start the ZWESVSTC started task. For instructions, see Installing the Zowe started task (ZWESVSTC).

## **Stage 4: Verify the installation**

Verify that Zowe is installed correctly on z/OS. See Verifying Zowe installation on z/OS.

## Looking for troubleshooting help?

If you encounter unexpected behavior when installing or verifying the Zowe runtime on z/OS, see the Troubleshooting section for tips.

# **Planning the installation**

The following information is required during the installation process. Software and hardware prerequisites are covered in the next section.

- The zFS directory where you will install the Zowe runtime files and folders. For more details of setting up and configuring the UNIX Systems Services (USS) environment, see UNIX System Services considerations for Zowe.
- A HLQ that the installation can create a load library and samplib containing load modules and JCL samples required to run Zowe.
- Multiple instances of Zowe can be started from the same Zowe z/OS runtime. Each launch of Zowe has its own zFS directory that is known as an instance directory.
- For Zowe in a high availability configuration, there will be only one instance directory which must be created on a shared file system (zFS directory) where all LPARs in a Sysplex can access. To install Zowe in a Parallel Sysplex environment, a YAML configuration file is used to customize the Zowe high availability instances.
- (If not using Docker) Zowe uses a zFS directory to contain its northbound certificate keys as well as a truststore for its southbound keys. Northbound keys are one presented to clients of the Zowe desktop or Zowe API Gateway, and southbound keys are for servers that the Zowe API gateway connects to. The certificate directory is not part of the Zowe runtime so that it can be shared between multiple Zowe runtimes and have its permissions secured independently.
- Zowe has the following started tasks:
  - ZWESISTC is a cross memory server that the Zowe desktop uses to perform APF-authorized code. More details on the cross memory server are described in Configuring the Zowe cross memory server.
  - ZWESASTC is a cross memory Auxiliary server that is used under some situations in support of a Zowe extension. Auxiliary server is started, controlled, and stopped by the cross memory server, so no need to start it manually. More details are described in Zowe auxiliary service
  - ZWESVSTC brings up other parts of the Zowe runtime on z/OS as requested. This may include Desktop, API mediation layer, ZSS, and more, but when using Docker likely only ZSS will be used

here.

• ZWESLSTC is used for Zowe high availability configuration rather than ZWESVSTC. It brings up and stops Zowe high availability instances, or specific Zowe components without restarting the entire Zowe high availability instances.

In order for above started tasks to run correctly, security manager configuration needs to be performed. This is documented in Configuring the z/OS system for Zowe and a sample JCL member ZWESECUR is shipped with Zowe that contains commands for RACF, TopSecret, and ACF2 security managers.

#### Notes:

- To start the API Mediation Layer as a standalone component, see API Mediation Layer as a standalone component.
- If you plan to use API ML with basic authentication and JSON web token authentication, you need to run only ZWESVSTC. No need to run ZWESISTC and ZWESASTC.
- If you plan to use API ML with x509 client-side certificate authentication, you need to run
   ZWESISTC and ZWESVSTC.

### **Topology of the Zowe z/OS launch process**

The following diagram depicts the high-level structure of a Zowe installation and runtime.

#### RUNTIME\_DIR

The runtime directory <RUNTIME\_DIR> contains the binaries and executable files. You can create a runtime directory in one of the following ways:

- Executing the zowe-install.sh script contained within the install directory of a Zowe convenience build.
- Installing the Zowe SMP/E FMID AZWE001 using the JCL members in the REL4 member.
- Executing the z/OSMF worklow script ZWERF01 contained in the SMP/E FMID AZWE001.

During execution of Zowe, the runtime directory contents are not modified. Maintenance or APAR release for Zowe replaces the contents of the runtime directory and are rollup PTFs.

### INSTANCE\_DIR

The instance directory <INSTANCE\_DIR> is required to launch Zowe. It is created with the script <RUNTIME\_DIR>/bin/zowe-configure-instance.sh. More than one instance directory can be created and used to launch multiple instances of Zowe sharing the same runtime directory <RUNTIME\_DIR>.

Zowe instances are started by running the script <INSTANCE\_DIR>/bin/zowe-start.sh. This creates a started task with the PROCLIB member ZWESVSTC that is provided with the samplib SZWESAMP created during the installation of Zowe. The JCL member ZWESVSTC starts a USS shell under which it launches its address spaces.

The instance directory file instance.env is used to configure a Zowe launchable. The file is executed during the launch of Zowe and specifies shell variables such as ports and location of dependent directories and services on z/OS.

The instance.env file sets the location of the <RUNTIME\_DIRECTORY> as well as the <KEYSTORE\_DIRECTORY>

**Note:** Alternatively, from v1.22.0 release, you can use a YAML format configuration file <code>zowe.yaml</code> instead of <code>instance.env</code> to configure the Zowe runtime for high availability. To learn more about the <code>zowe.yaml</code> file, see Updating the zowe.yaml configuration file.

### KEYSTORE\_DIRECTORY

Zowe uses certificates to encrypt data as well as a truststore. The keystore directory <KEYSTORE\_DIRECTORY> controls where the certificates are located, either in a JavaKeystore or a z/OS keyring. A <KEYSTORE\_DIRECTORY> is created by using the script <RUNTIME\_DIR>/bin/zowe-setupcertificates.sh.

# UNIX System Services considerations for Zowe

The Zowe z/OS component runtime requires USS to be configured. As shown in the Zowe architecture, a number of servers run under UNIX System Services (USS) on z/OS. Review this topic for knowledge and considerations about USS when you install and configure Zowe.

- Introduction
- Setting up USS for the first time
- Language environment
- OMVS segment
- Address space region size

# What is USS?

The UNIX System Services element of z/OS® is a UNIX operating environment, which is implemented within the z/OS operating system. It is also known as z/OS UNIX. z/OS UNIX files are organized in a hierarchy, as in a UNIX system. All files are members of a directory, and each directory in turn is a member of another directory at a higher level in the hierarchy. The highest level of the hierarchy is the *root* directory. The z/OS UNIX files system is also known as zFS.

For more information on USS, see the following resources:

- Introduction to z/OS UNIX for z/OS 2.2
- Introduction to z/OS UNIX for z/OS 2.3
- Introduction to z/OS UNIX for z/OS 2.4

# Setting up USS for the first time

If you have not enabled USS for your z/OS environment before, the SMP/E distribution of Zowe provides a number of JCL jobs to assist with this purpose. You can consult with your USS administrator if you need more information such as the USS file system.

# Language environment

To ensure that Zowe has enough memory, the recommended HEAP64 site should be large enough.

# **OMVS** segment

Users who install Zowe to run Zowe scripts need to have an OMVS segment. If the user profile doesn't have OMVS segment, the following situations might occur:

- When you access USS through TSO OMVS, you will see the following message:
- When you access USS through SSH, you will see the following message:

### Address space region size

Java as a prerequisite for Zowe requires a suitable z/OS region size to operate successfully while you install and configure Zowe. It is suggested that you do not restrict the region size, but allow Java to use what is necessary. Restricting the region size might cause failures with storage-related error messages such as the following one:

You can fix the storage-related issue by making one of the following changes:

• ASSIZEMAX parameter

The ASSIZEMAX parameter is the maximum size of the process's virtual memory (address space) in bytes.

To specify the JVM maximum address space size on a per-user basis, set the ASSIZEMAX configuration parameter to the value of 2147483647.

**Note:** Running a shell script via TSO OMVS will run the shell in the TSO address space, unless you specify <u>BPX\_SHAREAS=N0</u> when invoking OMVS. If you are using TSO OMVS to install Zowe, you will need export <u>BPX\_SHAREAS=N0</u> to make the ASSIZEMAX change effective.

• SIZE parameter of TSO segment

Set SIZE operand of TSO segment to the value of 2096128.

**Note:** If you set export \_BPX\_SHAREAS=YES in your shell setup as recommended, Java will run in the TSO address space and the SIZE change will work.

• ulimit -A

The maximum address space size for the process should be at least 250 M, in units of 1024 bytes. For example, ulimit -A 250000.

**Note:** Running ulimit -a displays the current process limits.

Version: v1.25.x LTS

# System requirements

Before installing Zowe<sup>™</sup> z/OS components, ensure that your z/OS environment meets the prerequisites. The prerequisites you need to install depend on what Zowe z/OS components you want to use and how you want to install and configure Zowe on z/OS. Therefore, assess your installation scenario and install the prerequisites that meet your needs.

All Zowe server components can be installed on a z/OS environment, while some can alternatively be installed on Linux or zLinux via Docker. The components provide a number of services that are accessed through a web browser such as an API catalog and a web desktop.

- z/OS system requirements
  - z/OS
  - Node.js
  - Java
  - z/OSMF (Optional)
- User ID requirements
  - ZWESVUSR
  - ZWESIUSR
  - ZWEADMIN
  - zowe\_user
- Network requirements
- Zowe Docker requirements
- Zowe Desktop requirements (client PC)
- Feature requirements
  - Multi-Factor Authentication MFA
  - Single Sign-On SSO

# z/OS system requirements

Be sure your z/OS system meets the following prerequisites.

• z/OS version in active support, such as Version 2.3 and Version 2.4

**Note:** z/OS V2.2 reached end of support on 30 September 2020. For more information, see the z/OS v2.2 lifecycle details https://www.ibm.com/support/lifecycle/details?q45=Z497063S01245B61.

- zFS volume with at least 833 mb of free space for Zowe server components, their keystore, instance configuration files and logs, and third-party plug-ins.
- (Optional, recommended) z/OS OpenSSH V2.2.0 or later

Some features of Zowe require SSH, such as the Desktop's SSH terminal. Or, you want to install and manage Zowe via SSH, as an alternative to OMVS over TN3270.

• (Optional, recommended) Parallel Sysplex.

To deploy Zowe for high availability, a Parallel Sysplex environment is recommended. Please check Configuring Sysplex for high availability for more information.

#### Node.js

• Node.js v8.x (except v8.16.1), v12.x, or v14 (except v14.17.2)

Node is not included with z/OS so must be installed separately. To install Node.js on z/OS, follow the instructions in Installing Node.js on z/OS.

**Note:** If you are a software vendor building extensions for Zowe, when using Node.js v12.x or later, it is highly recommended that plug-ins used are tagged. For more information, see Tagging on z/OS.

#### Java

• IBM SDK for Java Technology Edition V8 or later

### z/OSMF (Optional)

(Optional, recommended) IBM z/OS Management Facility (z/OSMF) Version 2.2, Version 2.3 or Version 2.4.

z/OSMF is included with z/OS so does not need to be separately installed. If z/OSMF is present, Zowe will detect this when it is configured and use z/OSMF for the following purposes:

- Authenticating TSO users and generating a single sign-on JSON Web Token (JWT). Ensure that the z/OSMF JWT Support is available via APAR and associated PTFs. If z/OSMF is not available, then Zowe is still able to provide SSO by generating its own JWT and making direct SAF calls.
- REST API services for Files (Data Sets and USS), JES, and z/OSMF workflows. These are used by some Zowe applications such as the Zowe Explorers in the Zowe Desktop. If z/OSMF REST APIs are not present, other Zowe desktop application, such as the File Editor that provides access to USS directories and files as well as MVS data sets and members, will work through the Zowe Z Secure Services (ZSS) component to access z/OS resources.

#### Tips:

- For non-production use of Zowe (such as development, proof-of-concept, demo), you can customize the configuration of z/OSMF to create what is known as "z/OS MF Lite" that simplifies the setup of z/OSMF. As z/OS MF Lite only supports selected REST services (JES, DataSet/File, TSO and Workflow), you will observe considerable improvements in startup time as well as a reduction in the efforts involved in setting up z/OSMF. For information about how to set up z/OSMF Lite, see Configuring z/OSMF Lite (non-production environment).
- For production use of Zowe, see Configuring z/OSMF.

# **User ID requirements**

Specific user IDs with sufficient permissions are required to run or access Zowe.

## ZWESVUSR

This is a started task ID used to run the PROCLIB ZWESVSTC.

The task starts a USS environment using **BPXBATSL** that executes the core Zowe Desktop (ZLUX) node.js server, the Java API Mediation Layer, and the Z Secure Services C component. To work with USS, the user ID **ZWESVUSR** must have a valid OMVS segment.

Class	ID	Access	Reason
CSFSERV	CSFRNGL	READ	To generate symmetric keys using ICSF that is used by Zowe Desktop cookies

Class	ID	Access	Reason
FACILITY	ZWES.IS	READ	To allow Zowe ZWESVSTC processes to access the Zowe ZIS cross memory server
FACILITY	BPX.SERVER + BPX.DEAMON	UPDATE	To allow the Zowe Desktop ZLUX server to run code on behalf of the API requester's TSO user ID. For more information, see Security Environment Switching.
FACILITY	IRR.RUSERMAP	READ	To allow Zowe to map an X.509 client certificate to a z/OS identity
FACILITY	BPX.JOBNAME	READ	To allow z/OS address spaces for unix processes to be renamed for ease of identification
FACILITY	IRR.RADMIN.LISTUSER	READ	To allow Zowe to obtain information about OMVS segment of the user profile using LISTUSER TSO command

## ZWESIUSR

This is a started task ID used to run the PROCLIB ZWESISTC that launches the cross memory server (also known as ZIS). It must have a valid OMVS segment.

## ZWEADMIN

This is a group that ZWESVUSR and ZWESIUSR should belong to. It must have a valid OMVS segment.

#### zowe\_user

If z/OSMF is used for authentication and serving REST APIs for Zowe CLI and Zowe Explorer users, the TSO user ID for end users must belong to one or both of the groups IZUUSER or IZUADMIN.

# **Network requirements**

The following ports are required for Zowe. These are default values. You can change the values by updating variable values in the instance.env file. For more information, see Configuring the Zowe instance directory.

Port number	Variable name	Purpose
7552	CATALOG_PORT	Used to view API swagger / openAPI specifications for registered API services in the API Catalog.
7553	DISCOVERY_PORT	Discovery server port which dynamic API services can issue APIs to register or unregister themselves.
7554	GATEWAY_PORT	The northbound edge of the API Gateway used to accept client requests before routing them to registered API services. This port must be exposed outside the z/OS network so clients (web browsers, VS Code, processes running the Zowe CLI) can reach the gateway.
7555	ZWE_CACHING_SERVICE_PORT	Port of the caching service that is used to share state between different Zowe instances in a high availability topology.
8545	JOBS_API_PORT	Port of the service that provides REST APIs to z/OS jobs used by the JES Explorer.
8546	JES_EXPLORER_UI_PORT	Port of the JES Explorer GUI for viewing and working with jobs in the Zowe Desktop.
8547	FILES_API_PORT	Port of the service that provides REST APIs to MVS and USS file systems.
8548	MVS_EXPLORER_UI_PORT	Port of the MVS Explorer GUI for working with data sets in the Zowe Desktop.

Port number	Variable name	Purpose
8550	USS_EXPLORER_UI_PORT	Port of the USS Explorer GUI for working with USS in the Zowe Desktop.
8544	ZOWE_ZLUX_SERVER_HTTPS_PORT	The Zowe Desktop (also known as ZLUX) port used to log in through web browsers.
8542	ZOWE_ZSS_SERVER_PORT	Z Secure Services (ZSS) provides REST API services to ZLUX, used by the File Editor application and other ZLUX applications in the Zowe Desktop.

## **Zowe Docker requirements**

Technical Preview The Zowe Docker build is a technical preview.

Docker is a technology for delivering a set of software and all its prerequisites and run them in an isolated manner to reduce installation steps and to eliminate troubleshooting environmental differences. Docker can run on many operating systems, but currently the Zowe Docker image is for x86 Linux (Intel, AMD) and zLinux ("s390x"). Support for platforms such as zCX, Windows, and more will be added over time.

To get Docker for Linux, you should check your Linux software repository. Whether using Ubuntu, Red Hat, SuSE, and many other types of Linux, you can install Docker the same way you install other software on Linux through the package manager.

Once you have Docker, the Zowe Docker image has the following requirements

- 4 GB free RAM, 8 GB recommended
- 4 GB free disk space
- Network access to the z/OS host. The Linux host must be able to communicate with the z/OS host.

When using Docker the USS components of Zowe will run off z/OS in the Linux container, however a z/OS installation of Zowe is still required for the ZSS and cross memory server.

**Note:** The subsections of z/OS requirements such as for API Mediation Layer, Web Explorers, and Application Framework are not required because they are included in the Docker install.

# Zowe Desktop requirements (client PC)

The Zowe Desktop is powered by the Application Framework which has server prereqs depending on where it is installed

- Zowe Application Framework on z/OS requirements
- Application Framework on Docker prerequisites

The Zowe Desktop runs inside of a browser. No browser extensions or plugins are required. The Zowe Desktop supports Google Chrome, Mozilla Firefox, Apple Safari and Microsoft Edge releases that are at most 1 year old, except when the newest release is older. For Firefox, both the regular and Extended Support Release (ESR) versions are supported under this rule.

Currently, the following browsers are supported:

- Google Chrome V79 or later
- Mozilla Firefox V68 or later
- Safari V13 or later
- Microsoft Edge 79

If you do not see your browser listed here, please contact the Zowe community so that it can be validated and included.

# Feature requirements

Zowe has several optional features that have additional prerequisites as follows.

## Multi-Factor Authentication (MFA)

Multi-factor authentication is supported for several components, such as the Desktop and API Mediation Layer. Multi-factor authentication is provided by third-party products which Zowe is compatible with. The following are known to work:

• IBM Z Multi-Factor Authentication.

For information on using MFA in Zowe, see Multi-Factor Authentication.

## Single Sign-On (SSO)

Zowe has an SSO scheme with the goal that each time you use use multiple Zowe components you should only be prompted to login once.

Requirements:

- IBM z/OS Management Facility (z/OSMF)
- (Optional, recommended) PKCS#11 token setup is required when using ZSS, the Desktop, and Application Framework with SSO. See Creating a PKCS#11 Token for more information.

# Installing Node.js on z/OS

#### Note: This section is not required if using Docker or only using the CLI.

Before you install Zowe<sup>™</sup> on z/OS, you must install IBM SDK for Node.js on the same z/OS server that hosts the Zowe Application Server and z/OS Explorer Services. Review the information in this topic to obtain and install Node.js.

- Supported Node.js versions
- How to obtain IBM SDK for Node.js z/OS
- Hardware and software prerequisites
- Installing the PAX edition of Node.js z/OS
- Installing the SMP/E edition of Node.js z/OS

# Supported Node.js versions

The following Node.js versions are supported to run Zowe. See the Hardware and software prerequisites section for the prerequisites that are required by Zowe.

The corresponding IBM Knowledge Center for Node.js - z/OS lists all the prerequisites for Node.js. Some software packages, which might be listed as prerequisites there, are **NOT** required by Zowe. Specifically, you do **NOT** need to install Python, Make, Perl, or C/C++ runtime or compiler. If you can run **node** --version successfully, you have installed the prerequisites required by Zowe.

- v8.x (except v8.16.1)
  - z/OS V2R2: PTFs UI62788, UI46658, UI62416, UI62415 (APARs PH10606, PI79959, PH10740, PH10741)
  - z/OS V2R3: PTFs UI61308, UI61375, UI61747 (APARs PH0710, PH08352, PH09543)
  - z/OS V2R4: PTFs UI64839, UI64940, UI64837, UI64830 (APARs PH14559, PH16038, PH15674, PH14560)

**Known issue:** There is a known issue with node.js v8.16.1 and Zowe desktop encoding. See the GitHub issue for details.

**Workaround:** Use node.js v8.16.2 or later, which is available at https://www.ibm.com/caen/marketplace/sdk-nodejs-compiler-zos. Download the pax.Z file.

- v12.x
  - z/OS V2R2: PTFs UI62788, UI46658, UI62416, UI62415 (APARs PH10606, PI79959, PH10740, PH10741)
  - z/OS V2R3: PTFs UI61308, UI61375, UI61747 (APARs PH0710, PH08352, PH09543)
  - z/OS V2R4: PTFs UI64839, UI64940, UI64837, UI64830, UI65567 (APARs PH14559, PH16038, PH15674, PH14560, PH17481)
- v14 (except v14.17.2)
  - z/OS V2R3: PTFs UI61308, UI61375, UI61747 (APARs PH07107, PH08352, PH09543)
  - z/OS V2R4: PTFs UI64830, UI64837, UI64839, UI64940, UI65567 (APARs PH14560, PH15674, PH14559, PH16038, PH17481)

**Known issue:** There is a known issue with node.js v14.17.2. It will cause the error of ZWESLSTC not found in "<dsn-prefix>.SZWESAMP" when you run the zowe-install-proc.sh utility.

# How to obtain IBM SDK for Node.js - z/OS

You can obtain IBM SDK for Node.js - z/OS for free in one of the following ways:

- Order the SMP/E edition through your IBM representative for production use
- Use the PAX edition for non-production deployments

For more information, see the blog "How to obtain IBM SDK for Node.js - z/OS, at no charge".

# Hardware and software prerequisites

To install Node.js for Zowe, the following requirements must be met.

The corresponding IBM Knowledge Center for Node.js - z/OS lists all the prerequisites for Node.js. Some software packages, which might be listed as prerequisites there, are **NOT** required by Zowe. Specifically, you do **NOT** need to install Python, Make, Perl, or C/C++ runtime or compiler.

If you can run **node** --version successfully, you have installed the Node.js prerequisites required by Zowe.

#### Hardware:

IBM zEnterprise® 196 (z196) or newer

#### Software:

- z/OS UNIX System Services enabled
- Integrated Cryptographic Service Facility (ICSF) configured and started

ICSF is required for Node.js to operate successfully on z/OS. If you have not configured your z/OS environment for ICSF, see Cryptographic Services ICSF: System Programmer's Guide. To see whether ICSF has been started, check whether the started task ICSF or CSF is active.

# Installing the PAX edition of Node.js - z/OS

Follow these steps to install the PAX edition of Node.js - z/OS to run Zowe.

- 1. Download the pax.Z file to a z/OS machine.
- 2. Extract the pax.Z file inside an installation directory of your choice. For example:

pax -rf <path\_to\_pax.Z\_file> -x pax

- 3. Add the full path of your installation directory to your PATH environment variable:
- 4. Run the following command from the command line to verify the installation.

If Node.js is installed correctly, the version of Node.js is displayed.

5. After you install Node.js, set the *NODE\_HOME* environment variable to the directory where Node.js is installed. For example, NODE\_HOME=/proj/mvd/node/installs/node-v6.14.4-os390-s390x.

# Installing the SMP/E edition of Node.js - z/OS

To install the SMP/E edition of Node.js, see the documentation for IBM SDK for Node.js - z/OS. Remember that the software packages Perl, Python, Make, or C/C++ runtime or compiler that the Node.js documentation might mention are **NOT** needed by Zowe.

# Version: v1.25.x LTS Configuring z/OSMF

The following information contains procedures and tips for meeting z/OSMF requirements. For complete information, go to IBM Knowledge Center and read the following documents.

- IBM z/OS Management Facility Configuration Guide
- IBM z/OS Management Facility Help

# z/OS requirements for z/OSMF configuration

Ensure that the z/OS system meets the following requirements:

Requirements	Description	Resources in IBM Knowledge Center
AXR (System REXX)	z/OS uses AXR (System REXX) component to perform Incident Log tasks. The component enables REXX executable files to run outside of conventional TSO and batch environments.	System REXX
Common Event Adapter (CEA) server	The CEA server, which is a co-requisite of the Common Information Model (CIM) server, enables the ability for z/OSMF to deliver z/OS events to C-language clients.	Customizing for CEA
Common Information Model (CIM) server	z/OSMF uses the CIM server to perform capacity-provisioning and workload-management tasks. Start the CIM server before you start z/OSMF (the IZU* started tasks).	Reviewing your CIM server setup

Requirements	Description	Resources in IBM Knowledge Center
CONSOLE and CONSPROF commands	The CONSOLE and CONSPROF commands must exist in the authorized command table.	Customizing the CONSOLE and CONSPROF commands
Java level	IBM® 64-bit SDK for z/OS®, Java Technology Edition V8 or later is required.	Software prerequisites for z/OSMF
TSO region size	To prevent <b>exceeds maximum region size</b> errors, verify that the TSO maximum region size is a minimum of 65536 KB for the z/OS system.	N/A
User IDs	User IDs require a TSO segment (access) and an OMVS segment. During workflow processing and REST API requests, z/OSMF might start one or more TSO address spaces under the following job names: userid; substr(userid, 1, 6) CN (Console).	N/A

# **Configuring z/OSMF**

#### Follow these steps:

1. From the console, issue the following command to verify the version of z/OS:

Part of the output contains the release, for example,

2. Configure z/OSMF.

z/OSMF is a base element of z/OS V2.2 and V2.3, so it is already installed. But it might not be configured and running on every z/OS V2.2 and V2.3 system.

In short, to configure an instance of z/OSMF, run the IBM-supplied jobs IZUSEC and IZUMKFS, and then start the z/OSMF server. The z/OSMF configuration process occurs in three stages, and in the following order:

- Stage 1 Security setup
- Stage 2 Configuration
- Stage 3 Server initialization

This stage sequence is critical to a successful configuration. For complete information about how to configure z/OSMF, see Configuring z/OSMF for the first time if you use z/OSV2.2 or Setting up z/OSMF for the first time if V2.3.

**Note:** In z/OS V2.3, the base element z/OSMF is started by default at system initial program load (IPL). Therefore, z/OSMF is available for use as soon as you set up the system. If you prefer not to start z/OSMF automatically, disable the autostart function by checking for **START** commands for the z/OSMF started procedures in the *COMMNDxx parmlib* member.

The z/OS Operator Consoles task is new in Version 2.3. Applications that depend on access to the operator console such as Zowe<sup>™</sup> CLI's RestConsoles API require Version 2.3.

3. Verify that the z/OSMF server and angel processes are running. From the command line, issue the following command:

If jobs IZUANG1 and IZUSVR1 are not active, issue the following command to start the angel process:

After you see the message ""CWWKB0056I INITIALIZATION COMPLETE FOR ANGEL"", issue the following command to start the server:

The server might take a few minutes to initialize. The z/OSMF server is available when the message ""CWWKF0011I: The server zosmfServer is ready to run a smarter planet."" is displayed.

4. Issue the following command to find the startup messages in the SDSF log of the z/OSMF server:

You could see a message similar to the following message, which indicates the port number:

In this example, the port number is 443. You will need this port number later.

Point your browser at the nominated z/OSMF STANDALONE Server home page and you should see its Welcome Page where you can log in.

**Note:** If your implementation uses an external security manager other than RACF (for example, Top Secret for z/OS or ACF2 for z/OS), you provide equivalent commands for your environment. For more information, see the following product documentation:

- Configure z/OS Management Facility for Top Secret
- Configure z/OS Management Facility for ACF2

# z/OSMF REST services for the Zowe CLI

The Zowe CLI uses z/OSMF Representational State Transfer (REST) APIs to work with system resources and extract system data. Ensure that the following REST services are configured and available.

z/OSMF REST services	Requirements	Resources in IBM knowledge Center
Cloud provisioning services	Cloud provisioning services are required for the Zowe CLI CICS and Db2 command groups. Endpoints begin with /zosmf/provisioning/	Cloud provisioning services
TSO/E address space services	TSO/E address space services are required to issue TSO commands in the Zowe CLI. Endpoints begin with /zosmf/tsoApp	TSO/E address space services
z/OS console services	z/OS console services are required to issue console commands in the Zowe CLI. Endpoints begin with /zosmf/restconsoles/	z/OS console services
z/OS data set and file REST interface	z/OS data set and file REST interface is required to work with mainframe data sets and UNIX System Services files in the Zowe CLI. Endpoints begin with /zosmf/restfiles/	z/OS data set and file REST interface

z/OSMF REST services	Requirements	Resources in IBM knowledge Center
z/OS jobs REST interface	z/OS jobs REST interface is required to use the zos-jobs command group in the Zowe CLI. Endpoints begin with /zosmf/restjobs/	z/OS jobs REST interface
z/OSMF workflow services	z/OSMF workflow services is required to create and manage z/OSMF workflows on a z/OS system. Endpoints begin with /zosmf/workflow/	z/OSMF workflow services

Zowe uses symbolic links to the z/OSMF bootstrap.properties,

jvm.security.override.properties, and ltpa.keys files. Zowe reuses SAF, SSL, and LTPA configurations; therefore, they must be valid and complete.

For more information, see Using the z/OSMF REST services in IBM z/OSMF documentation.

To verify that z/OSMF REST services are configured correctly in your environment, enter the REST endpoint into your browser. For example: https://mvs.ibm.com:443/zosmf/restjobs/jobs

#### Notes:

- Browsing z/OSMF endpoints requests your user ID and password for defaultRealm; these are your TSO user credentials.
- The browser returns the status code 200 and a list of all jobs on the z/OS system. The list is in raw JSON format.

# Configuring z/OSMF Lite (for non-production use)

This section provides information about requirements for z/OSMF Lite configuration.

**Disclaimer:** z/OSMF Lite can be used in a non-production environment such as development, proof-ofconcept, demo and so on. It is not for use in a production environment. To use z/OSMF in a production environment, see Configuring z/OSMF.

- Configuring z/OSMF Lite (for non-production use)
  - Introduction
  - Assumptions
  - Software Requirements
    - Minimum Java level
    - WebSphere® Liberty profile (z/OSMF V2R3 and later)
    - System settings
    - Web browser
  - Creating a z/OSMF nucleus on your system
    - Running job IZUNUSEC to create security
      - Before you begin
      - Procedure
      - Results
      - Common errors
    - Running job IZUMKFS to create the z/OSMF user file system
      - Before you begin
      - Procedure
      - Results
      - Common errors
    - Copying the IBM procedures into JES PROCLIB
      - Before you begin
      - Procedure
      - Results

- Common errors
- Starting the z/OSMF server
  - Before you begin
  - Procedure
  - Results
- Accessing the z/OSMF Welcome page
  - Before you begin
  - Procedure
  - Results
  - Common errors
- Mounting the z/OSMF user file system at IPL time
  - Before you begin
  - Procedure
  - Results
- Adding the required REST services
  - Enabling the z/OSMF JOB REST services
    - Procedure
    - Results
    - Common errors
  - Enabling the TSO REST services
    - Before you begin
    - Procedure
    - IZUTSSEC
    - Results
  - Enabling the z/OSMF data set and file REST services
    - Before you begin
    - Procedure
    - Results
    - Common errors
  - Enabling the z/OSMF Workflow REST services and Workflows task UI
    - Before you begin
    - Procedure
    - Results
- Troubleshooting problems

- Common problems and scenarios
  - System setup requirements not met
- Tools and techniques for troubleshooting
  - Common messages
- Appendix A. Creating an IZUPRMxx parmlib member
- Appendix B. Modifying IZUSVR1 settings
- Appendix C. Adding more users to z/OSMF
  - Before you Begin
  - Procedure
  - Results
- Appendix A. Creating an IZUPRMxx parmlib member
- Appendix B. Modifying IZUSVR1 settings
- Appendix C. Adding more users to z/OSMF

# Introduction

IBM® z/OS® Management Facility (z/OSMF) provides extensive system management functions in a taskoriented, web browser-based user interface with integrated user assistance, so that you can more easily manage the day-to-day operations and administration of your mainframe z/OS systems.

By following the steps in this guide, you can quickly enable z/OSMF on your z/OS system. This simplified approach to set-up, known as "z/OSMF Lite", requires only a minimal amount of z/OS customization, but provides the key functions that are required by many exploiters, such as the open mainframe project (Zowe<sup>™</sup>).

A z/OSMF Lite configuration is applicable to any future expansions you make to z/OSMF, such as adding more optional services and plug-ins.

It takes 2-3 hours to set up z/OSMF Lite. Some steps might require the assistance of your security administrator.

For detailed information about various aspects of z/OSMF configuration such as enabling the optional plugins and services, see the IBM publication *z/OSMF Configuration Guide*.

# Assumptions

This document is intended for a first time z/OSMF setup. If z/OSMF is already configured on your system, you do not need to create a z/OSMF Lite configuration.

This document is designed for use with a single z/OS system, not a z/OS sysplex. If you plan to run z/OSMF in a sysplex, see *z/OSMF Configuration Guide* for multi-system considerations.

It is assumed that a basic level of security for z/OSMF is sufficient on the z/OS system. IBM provides a program, IZUNUSEC, to help you set up basic security for a z/OSMF Lite configuration.

System defaults are used for the z/OSMF environmental settings. Wherever possible, it is recommended that you use the default values. If necessary, however, you can override the defaults by supplying an IZUPRMxx member, as described in Appendix A. Creating an IZUPRMxx parmlib member.

It is recommended that you use the following procedures as provided by IBM:

- Started procedures IZUSVR1 and IZUANG1
- Logon procedure IZUFPROC

Information about installing these procedures is provided in Copying the IBM procedures into JES PROCLIB.

# **Software Requirements**

Setting up z/OSMF Lite requires that you have access to a z/OS V2R2 system or later. Also, your z/OS system must meet the following minimum software requirements:

- Minimum Java level
- WebSphere® Liberty profile (z/OSMF V2R3 and later)
- System settings
- Web browser

## Minimum Java level

Java<sup>™</sup> must be installed and operational on your z/OS system, at the required minimum level. See the table that follows for the minimum level and default location. If you installed Java in another location, you must specify the JAVA\_HOME statement in your IZUPRMxx parmlib member, as described in Appendix A. Creating an IZUPRMxx parmlib member.

z/OS Version	Minimum level of Java™	Recommended level of Java	Default location
z/OS V2R2	IBM® 64-bit SDK for z/OS®, Java Technology Edition V7.1 (SR3), with the PTFs for APAR PI71018 and APAR PI71019 applied <b>OR</b> IBM® 64-bit SDK for z/OS®, Java Technology Edition V8, with the PTF for APAR PI72601 applied.	IBM® 64-bit SDK for z/OS®, Java™ Technology Edition, V8 SR6 (5655-DGH)	/usr/lpp/java/J7.1_64
z/OS V2R3	IBM® 64-bit SDK for z/OS®, Java™ Technology Edition, V8 SR4 FP10 (5655-DGH)	IBM® 64-bit SDK for z/OS®, Java™ Technology Edition, V8 SR6 (5655-DGH)	/usr/lpp/java/J8.0_64

## WebSphere® Liberty profile (z/OSMF V2R3 and later)

z/OSMF V2R3 uses the Liberty Profile that is supplied with z/OS, rather than its own copy of Liberty. The WebSphere Liberty profile must be mounted on your z/OS system. The default mount point is: /usr/lpp/liberty\_zos. To determine whether WebSphere® Liberty profile is mounted, check for the existence of the mount point directory on your z/OS system.

If WebSphere® Liberty profile is mounted at a non-default location, you need to specify the location in the IZUSVR1 started procedure on the keyword **WLPDIR=**. For details, see Appendix B. Modifying IZUSVR1 settings.

Note: Whenever you apply PTFs for z/OSMF, you might be prompted to install outstanding WebSphere Liberty service. It is recommended that you do so to maintain z/OSMF functionality.

## System settings

Ensure that the z/OS host system meets the following requirements:

- Port 443 (default port) is available for use.
- The system host name is unique and maps to the system on which z/OSMF Lite will be configured.

Otherwise, you might encounter errors later in the process. If you encounter errors, see Troubleshooting problems for the corrective actions to take.

## Web browser

For the best results with z/OSMF, use one of the following web browsers on your workstation:

- Microsoft Internet Explorer Version 11 or later
- Microsoft Edge (Windows 10)
- Mozilla Firefox ESR Version 52 or later.

To check your web browser's level, click **About** in the web browser.

# Creating a z/OSMF nucleus on your system

The following system changes are described in this chapter:

- Running job IZUNUSEC to create security
- Running job IZUMKFS to create the z/OSMF user file system
- Copying the IBM procedures into JES PROCLIB
- Starting the z/OSMF server
- Accessing the z/OSMF Welcome page
- Mounting the z/OSMF user file system at IPL time

The following sample jobs that you might use are included in the package and available for download:

- IZUAUTH
- IZUICSEC
- IZUNUSEC\_V2R2
- IZUNUSEC\_V2R3
- IZUPRM00
- IZURFSEC
- IZUTSSEC
- IZUWFSEC

#### **Download sample jobs**

Check out the video for a demo of the process:

## Running job IZUNUSEC to create security

The security job IZUNUSEC contains a minimal set of RACF® commands for creating security profiles for the z/OSMF nucleus. The profiles are used to protect the resources that are used by the z/OSMF server, and to grant users access to the z/OSMF core functions. IZUNUSEC is a simplified version of the sample job IZUSEC, which is intended for a more complete installation of z/OSMF.

**Note:** If your implementation uses an external security manager other than RACF (for example, Top Secret or ACF2), provide equivalent commands for your environment. For more information, see the following product documentation:

- Configure z/OS Management Facility for Top Secret
- Configure z/OS Management Facility for ACF2

#### Before you begin

In most cases, you can run the IZUNUSEC security job without modification. To verify that the job is okay to run as is, ask your security administrator to review the job and modify it as necessary for your security environment. If security is not a concern for the host system, you can run the job without modification.

#### Procedure

- 1. If you run z/OS V2R2 or V2R3, download job IZUNUSEC in the sample jobs package and upload this job to z/OS. If you run z/OS V2R4, locate job IZUNUSEC at SYS1.SAMPLIB.
- 2. Review and edit the job, if necessary.
- 3. Submit IZUNUSEC as a batch job on your z/OS system.
- 4. Connect your user ID to IZUADMIN group.
  - i. Download job IZUAUTH in the sample jobs package and customize it.
  - ii. Replace the 'userid' with your z/OSMF user ID.
  - iii. Submit the job on your z/OS system.

#### Results

Ensure the IZUNUSEC job completes with return code 0000.

To verify, check the results of the job execution in the job log. For example, you can use SDSF to examine the job log:

- 1. In the SDSF primary option menu, select Option ST.
- 2. On the SDSF Status Display, enter **S** next to the job that you submitted.
- 3. Check the return code of the job. The job succeeds if '0000' is returned.

#### **Common errors**

Review the following messages and the corresponding resolutions as needed:

Symptom	Cause	Resolution
Message IKJ56702I:The job isINVALID data issubmitted moreissuedthan once.		You can ignore this message.
Job fails with an authorization error.	Your user ID lacks superuser authority.	Contact your security admin to run IZUNUSEC. If you are using RACF®, select a user ID with SPECIAL attribute which can issue all RACF® commands.

Symptom	Cause	Resolution
Your installationJob fails with anuses the RACFauthorization error.PROTECT-ALLoption.		See Troubleshooting problems.
ADDGROUP and ADDUSER commands are not executed.	The automatic GID and UID assignment is required.	Define SHARED.IDS and BPX.NEXT.USER profiles to enable the use of AUTOUID and AUTOGID.

## Running job IZUMKFS to create the z/OSMF user file system

The job IZUMKFS initializes the z/OSMF user file system, which contains configuration settings and persistence information for z/OSMF.

The job mounts the file system. On a z/OS V2R3 system with the PTF for APAR PI92211 installed, the job uses mount point /global/zosmf. Otherwise, for an earlier system, the job mounts the file system at mount point /var/zosmf.

#### Before you begin

To perform this step, you need a user ID with "superuser" authority on the z/OS host system. For more information about how to define a user with superuser authority, see the publication *z/OS UNIX System Services*.

#### Procedure

- 1. In the system library SYS1. SAMPLIB, locate job IZUMKFS.
- 2. Copy the job.
- 3. Review and edit the job:
  - Modify the job information so that the job can run on your system.
  - You must specify a volume serial (VOLSER) to be used for allocating a data set for the z/OSMF data directory.

4. Submit IZUMKFS as a batch job on your z/OS system.

#### Results

The z/OSMF file system is allocated, formatted, and mounted, and the necessary directories are created.

To verify if the file system is allocated, formatted, locate the following messages in IZUMKFS job output.

Sample output:

#### **Common errors**

Review the following messages and the corresponding resolutions as needed

Symptom	Cause	Resolution
Job fails with FSM error. Your user ID lacks superuser authority.		For more information about how to define a user with superuser authority, see the publication <i>z/OS UNIX System Services</i> .
Job fails with an authorization error.	Job statement errors.	See Troubleshooting problems.

## Copying the IBM procedures into JES PROCLIB

Copy the z/OSMF started procedures and logon procedure from SYS1.PROCLIB into your JES concatenation. Use **\$D PROCLIB** command to display your JES2 PROCLIB definitions.

#### Before you begin

Locate the IBM procedures. IBM supplies procedures for z/OSMF in your z/OS order:

- ServerPac and CustomPac orders: IBM supplies the z/OSMF procedures in the SMP/E managed proclib data set. In ServerPac and SystemPac, the default name for the data set is SYS1.IBM.PROCLIB.
- CBPDO orders: For a CBPDO order, the SMP/E-managed proclib data set is named as SYS1.PROCLIB.
- Application Development CD.

#### Procedure

Use ISPF option 3.3 or 3.4 to copy the procedures from SYS1.PROCLIB into your JES concatenation.

- IZUSVR1
- IZUANG1
- IZUFPROC

#### Results

The procedures now reside in your JES PROCLIB.

#### **Common errors**

Review the following messages and the corresponding resolutions as needed

Symptom	Cause	Resolution
Not authorized to copy into PROCLIB.	Your user ID doesn't have the permission to modify PROCLIB.	Contact your security administrator.
Abend code B37 or E37.	The data set runs out of space.	Use IEBCOPY utility to compress PROCLIB dataset before you copy it.

## Starting the z/OSMF server

z/OSMF processing is managed through the z/OSMF server, which runs as the started tasks IZUANG1 and IZUSVR1. z/OSMF is started with the START command.

#### Before you begin

Ensure that you have access to the operations console and can enter the START command.

#### Procedure

In the operations console, enter the START commands sequentially:

Note: The z/OSMF angel (IZUANG1) must be started before the z/OSMF server (IZUSVR1).

You must enter these commands manually at subsequent IPLs. If necessary, you can stop z/OSMF processing by entering the STOP command for each of the started tasks IZUANG1 and IZUSVR1.

Note: z/OSMF offers an autostart function, which you can configure to have the z/OSMF server started automatically. For more information about the autostart capability, see *z/OSMF Configuration Guide*.

#### Results

When the z/OSMF server is initialized, you can see the following messages displayed in the operations console:

### Accessing the z/OSMF Welcome page

At the end of the z/OSMF configuration process, you can verify the results of your work by opening a web browser to the Welcome page.

#### Before you begin

To find the URL of the Welcome page, look for message IZUG349I in the z/OSMF server job log.

#### Procedure

1. Open a web browser to the z/OSMF Welcome page. The URL for the Welcome page has the following format: https://hostname:port/zosmf/

#### Where:

- *hostname* is the host name or IP address of the system in which z/OSMF is installed.
- port is the secure port for the z/OSMF configuration. If you specified a secure port for SSL encrypted traffic during the configuration process through parmlib statement HTTP\_SSL\_PORT,

port is required to log in. Otherwise, it is assumed that you use the default port 443.

- 2. In the z/OS USER ID field on the Welcome page, enter the z/OS user ID that you use to configure z/OSMF.
- 3. In the z/OS PASSWORD field, enter the password or pass phrase that is associated with the z/OS user ID.
- 4. Select the style of UI for z/OSMF. To use the desktop interface, select this option. Otherwise, leave this option unselected to use the tree view UI.
- 5. Click Log In.

#### Results

If the user ID and password or pass phrase are valid, you are authenticated to z/OSMF. The Welcome page of IBM z/OS Management Facility tab opens in the main area. At the top right of the screen, Welcome <*your\_user\_ID>* is displayed. In the UI, only the options you are allowed to use are displayed.

You have successfully configured the z/OSMF nucleus.

#### Common errors

The following errors might occur during this step:

Symptom	Cause	Resolution
z/OSMF welcome page does not load in your web browser.	The SSL handshake was not successful. This problem can be related to the browser certificate.	See Certificate error in the Mozilla Firefox browser.
To log into z/OSMF, enter a valid z/OS user ID and password. Your account might be locked after too many incorrect log-in attempts.	The user ID is not connected to the IZUADMIN group.	Connect your user ID to the IZUADMIN group.

Symptom	Cause	Resolution
To log into z/OSMF, enter a valid z/OS user ID and password. Your account might be locked after too many incorrect log-in attempts.	The password is expired.	Log on to TSO using your z/OS User ID and password, you will be asked to change your password if it's expired.

## Mounting the z/OSMF user file system at IPL time

Previously, in Running job IZUMKFS to create the z/OSMF user file system, you ran job IZUMKFS to create and mount the z/OSMF user file system. Now you should ensure that the z/OSMF user file system is mounted automatically for subsequent IPLs. To do so, update the BPXPRMxx parmlib member on your z/OS system.

#### Before you begin

By default, the z/OSMF file system uses the name IZU.SIZUUSRD, and is mounted in read/write mode. It is recommended that this file system is mounted automatically at IPL time.

If you do not know which BPXPRMxx member is active, follow these steps to find out:

1. In the operations console, enter the following command to see which parmlib members are included in the parmlib concatenation on your system:

D PARMLIB

- 2. Make a note of the BPXPRMxx member suffixes that you see.
- 3. To determine which BPXPRMxx member takes precedence, enter the following command:
  - D OMVS

The output of this command should be similar to the following:

In this example, the member BPXPRMST takes precedence. If BPXPRMST is not present in the concatenation, member BPXPRM3T is used.

#### Procedure

Add a MOUNT command for the z/OSMF user file system to your currently active BPXPRMxx parmlib member. For example:

On a z/OS V2R3 system with the PTF for APAR PI92211 installed:

On a z/OS V2R2 or V2R3 system without PTF for APAR PI92211 installed:

#### Results

The BPXPRMxx member is updated. At the next system IPL, the following message is issued to indicate that the z/OSMF file system is mounted automatically.

# **Adding the required REST services**

You must enable a set of z/OSMF REST services for the Zowe framework.

The following system changes are described in this topic:

- Enabling the z/OSMF JOB REST services
- Enabling the TSO REST services
- Enabling the z/OSMF data set and file REST services
- Enabling the z/OSMF Workflow REST services and Workflows task UI

## Enabling the z/OSMF JOB REST services

The Zowe framework requires that you enable the z/OSMF JOB REST services, as described in this topic.

#### Procedure

None

#### Results

To verify if the z/OSMF JOB REST services are enabled, open a web browser to our z/OS system (host name and port) and add the following REST call to the URL:

GET /zosmf/restjobs/jobs

The result is a list of the jobs that are owned by your user ID. For more information about the z/OSMF JOB REST services, see *z/OSMF Programming Guide*.

#### **Common errors**

Review the following messages and the corresponding resolutions as needed:

#### Symptom 1

401 Unauthorized

#### Cause

The user ID is not connected to IZUADMIN or IZUUSER.

#### Resolution

Connect your user ID to IZUADMIN or IZUUSER.

#### Symptom 2

HTTP/1.1 500 Internal Server Error {"rc":16,"reason":-1,"stack":"JesException: CATEGORY\_CIM rc=16 reason=-1 cause=com.ibm.zoszmf.util.eis.EisConnectionException: IZUG911I: Connection to \"http:\//null:5988\" cannot be established, or was lost and cannot be re-established using protocol \"CIM\".....Caused by: WBEMException: CIM\_ERR\_FAILED (JNI Exception type CannotConnectException:\nCannot connect to local CIM server. Connection failed.)

#### Cause

For JES2, you may have performed one of the following "Modify" operations: Hold a job, Release a job, Change the job class, Cancel a job, Delete a job (Cancel a job and purge its output), or you are running JES3 without configuring CIM Server.

#### Resolution

If you are running JES2, you can use *synchronous support for job modify operations* which does not required CIM. If you are running JES3, follow the *CIM setup instructions* to configure CIM on your system.

## **Enabling the TSO REST services**

The Zowe framework requires that you enable the TSO REST services, as described in this topic.

#### Before you begin

Ensure that the common event adapter component (CEA) of z/OS is running in full function mode.

1. To check if the CEA address space is active, enter the following command:

D A,CEA

- 2. If not, start CEA in full function mode. For detailed instructions, see *System prerequisites for the CEA TSO/E address space services*.
- 3. To verify that CEA is running in full function mode, enter the following command:

F CEA,D

The output should look like the following:

#### Procedure

- 1. If you run z/OS V2R2 and V2R3, download job IZUTSSEC in the sample jobs package and upload this Job to z/OS. If you run z/OS V2R4, locate job IZUTSSEC at SYS1.SAMPLIB.
- 2. Review and edit job IZUTSSEC before you submit. You can review the IZUTSSEC section below for more details.
- 3. Submit IZUTSSEC as a batch job on your z/OS system.

#### IZUTSSEC

IBM provides a set of jobs in SYS1.SAMPLIB with sample RACF commands to help with your z/OSMF configuration and its prerequisites. The IZUTSSEC job represents the authorizations that are needed for the z/OSMF TSO/E address space service. Your security administrator can edit and run the job. Generally, your z/OSMF user ID requires the same authorizations for using the TSO/E address space services as when you perform these operations through a TSO/E session on the z/OS system. For example, to start an application in a TSO/E address space requires that your user ID be authorized to operate that application. In addition, to use TSO/E address space services, you must have:

- READ access to the account resource in class ACCTNUM, where account is the value specified in the COMMON\_TSO ACCT option in parmlib.
- READ access to the CEA.CEATSO.TSOREQUEST resource in class SERVAUTH.
- READ access to the proc resource in class TSOPROC, where proc is the value specified with the COMMON\_TSO PROC option in parmlib.
- READ access to the <SAF\_PREFIX>.\*.izuUsers profile in the EJBROLE class. Or, at a minimum, READ access to the <SAF\_PREFIX>.IzuManagementFacilityTsoServices.izuUsers resource name in the EJBROLE class. You must also ensure that the z/OSMF started task user ID, which is IZUSVR by default,

has READ access to the CEA.CEATSO.TSOREQUEST resource in class SERVAUTH. To create a TSO/E address space on a remote system, you require the following authorizations:

- You must be authorized to the SAF resource profile that controls the ability to send data to the remote system (systemname), as indicated: CEA.CEATSO.FLOW.systemname
- To flow data between different systems in the sysplex, you must be authorized to do so by your external security manager, such as a RACF database with sysplex-wide scope. For example, to flow data between System A and System B, you must be permitted to the following resource profiles:
  - CEA.CEATSO.FLOW.SYSTEMA
  - CEA.CEATSO.FLOW.SYSTEMB

#### Results

The IZUTSSEC job should complete with return code 0000.

## Enabling the z/OSMF data set and file REST services

The Zowe framework requires that you enable the z/OSMF data set and file REST services.

#### Before you begin

1. Ensure that the message queue size is set to a large enough value. It is recommended that you specify an IPCMSGQBYTES value of at least 20971520 (20M) in BPXPRMxx.

Issue command D 0MVS, 0 to see the current value of IPCMSGQBYTES, if it is not large enough, use the SET0MVS command to set a large value. To set this value dynamically, you can enter the following operator command:

#### SETOMVS IPCMSGQBYTES=20971520

- 2. Ensure that the TSO REST services are enabled.
- 3. Ensure that IZUFPROC is in your JES concatenation.
- 4. Ensure that your user ID has a TSO segment defined. To do so, enter the following command from TSO/E command prompt:

LU userid TSO

Where *userid* is your z/OS user ID.

The output from this command must include the section called **TSO information**, as shown in the following example:

#### Procedure

- 1. If you run z/OS V2R2 and V2R3, download job IZURFSEC in the sample jobs package and upload it to z/OS. If you run z/OS V2R4, locate job IZURFSEC at SYS1.SAMPLIB.
- 2. Copy the job.
- 3. Examine the contents of the job.
- 4. Modify the contents as needed so that the job will run on your system.
- 5. From the TSO/E command line, run the IZURFSEC job.

#### Results

Ensure that the IZURFSEC job completes with return code 0000.

To verify if this setup is complete, try issuing a REST service. See the example in *List data sets* in the z/OSMF programming guide.

#### Common errors

Review the following messages and the corresponding resolutions as needed:

Symptom	Cause	Resolution
REST API doesn't return expected data with rc=12, rsn=3, message: message queue size "SIZE" is less than minimum: 20M	The message queue size for CEA is too small.	Ensure that the message queue size is set to a large enough value. It is recommended that you specify an IPCMSGQBYTES value of at least 20971520 (20M) in BPXPRMx.

## Enabling the z/OSMF Workflow REST services and Workflows task UI

The Zowe framework requires that you enable the z/OSMF Workflow REST services and Workflows task UI.

#### Before you begin

1. Ensure that the JOB REST services are enabled.

- 2. Ensure that the TSO REST services are enabled.
- 3. Ensure that the dataset and file REST services are enabled.

#### Procedure

- 1. If you run z/OS V2R2 and V2R3, download job IZUWFSEC in the sample jobs package and upload this job to z/OS. If you run z/OS V2R4, locate job IZUWFSEC at SYS1.SAMPLIB.
- 2. Copy the job.
- 3. Examine the contents of the job.
- 4. Modify the contents as needed so that the job will run on your system.
- 5. From the TSO/E command line, run the IZUWFSEC job.

#### Results

Ensure the IZUWFSEC job completes with return code 0000.

To verify, log on to z/OSMF (or refresh it) and verify that the Workflows task appears in the z/OSMF UI.

At this point, you have completed the setup of z/OSMF Lite.

Optionally, you can add more users to z/OSMF, as described in Appendix C. Adding more users to z/OSMF.

# **Troubleshooting problems**

This section provides tips and techniques for troubleshooting problems you might encounter when creating a z/OSMF Lite configuration. For other types of problems that might occur, see *z*/OSMF Configuration Guide.

## **Common problems and scenarios**

This section discusses troubleshooting topics, procedures, and tools for recovering from a set of known issues.

#### System setup requirements not met

This document assumes that the following is true of the z/OS host system:

Port 443 is available for use. To check this, issue either TSO command NETSTAT SOCKET or TSO command NETSTAT BYTE to determine if the port is being used.

- The system host name is unique and maps to the system on which z/OSMF Lite is being installed. To
  retrieve this value, enter either "hostname" z/OS UNIX command or TSO command "HOMETEST". If
  your system uses another method of assigning the system name, such as a multi-home stack, dynamic
  VIPA, or System Director, see z/OSMF Configuration Guide.
- The global mount point exists. On a z/OS 2.3 system, the system includes this directory by default. On a z/OS 2.2 system, you must create the global directory at the following location: /global/zosmf/.

If you find that a different value is used on your z/OS system, you can edit the IZUPRMxx parmlib member to specify the correct setting. For details, see Appendix A. Creating an IZUPRMxx parmlib member.

## Tools and techniques for troubleshooting

For information about working with z/OSMF log files, see z/OSMF Configuration Guide.

#### Common messages

If you see above error messages, check if your IZUANG0 procedure is up to date.

For descriptions of all the z/OSMF messages, see z/OSMF messages in IBM Knowledge Center.

# Appendix A. Creating an IZUPRMxx parmlib member

If z/OSMF requires customization, you can modify the applicable settings by using the IZUPRMxx parmlib member. To see a sample member, locate the IZUPRM00 member in the SYS1.SAMPLIB data set. IZUPRM00 contains settings that match the z/OSMF defaults.

Using IZUPRM00 as a model, you can create a customized IZUPRMxx parmlib member for your environment and copy it to SYS1.PARMLIB to override the defaults.

The following IZUPRMxx settings are required for the z/OSMF nucleus:

- HOSTNAME
- HTTP\_SSL\_PORT
- JAVA\_HOME.

The following setting is needed for the TSO/E REST services:

• COMMON\_TSO ACCT(IZUACCT) REGION(50000) PROC(IZUFPROC)

Descriptions of these settings are provided in the table below. For complete details about the IZUPRMxx settings and the proper syntax for updating the member, see *z*/OSMF Configuration Guide.

If you change values in the IZUPRMxx member, you might need to customize the started procedure IZUSVR1, accordingly. For details, see Appendix B. Modifying IZUSVR1 settings.

To create an IZUPRMxx parmlib member, follow these steps:

- 1. Copy the sample parmlib member into the desired parmlib data set with the desired suffix.
- 2. Update the parmlib member as needed.
- 3. Specify the IZUPRMxx parmlib member or members that you want the system to use on the IZU parameter of IEASYSxx. Or, code a value for IZUPRM= in the IZUSVR1 started procedure. If you specify both IZU= in IEASYSxx and IZUPARM= in IZUSVR1, the system uses the IZUPRM= value you specify in the started procedure.

Setting	Purpose	Rules	Default
HOSTNAME(hostname)	Specifies the host name, as defined by DNS, where the z/OSMF server is located. To use the local host name, enter asterisk (*), which is equivalent to \@HOSTNAME from previous releases. If you plan to use z/OSMF in a multisystem sysplex, IBM recommends using a dynamic virtual IP address (DVIPA) that resolves to the correct IP address if the z/OSMF server is moved to a different system.	Must be a valid TCP/IP HOSTNAME or an asterisk (*).	Default: *

Setting	Purpose	Rules	Default
HTTP_SSL_PORT(nnn)	Identifies the port number that is associated with the z/OSMF server. This port is used for SSL encrypted traffic from your z/OSMF configuration. The default value, 443, follows the Internet Engineering Task Force (IETF) standard. <b>Note:</b> By default, the z/OSMF server uses the SSL protocol SSL_TLSv2 for secure TCP/IP communications. As a result, the server can accept incoming connections that use SSL V3.0 and the TLS 1.0, 1.1 and 1.2 protocols.	Must be a valid TCP/IP port number. Value range: 1 - 65535 (up to 5 digits)	Default: 443
COMMON_TSO ACCT(account- number) REGION(region-size) PROC(proc-name)	Specifies values for the TSO/E logon procedure that is used internally for various z/OSMF activities and by the Workflows task.	The valid ranges for each value are described in <i>z/OSMF</i> <i>Configuration</i> <i>Guide</i> .	Default: 443 ACCT(IZUACCT) REGION(50000) PROC(IZUFPROC)
USER_DIR=filepath	z/OSMF data directory path. By default, the z/OSMF data directory is located in /global/zosmf. If you want to use a different path for the z/OSMF data directory, specify that value here, for example: USER_DIR= /the/new/config/dir.	Must be a valid z/OS UNIX path name.	Default: /global/zosmf/

# Appendix B. Modifying IZUSVR1 settings

You might need to customize the started procedure IZUSVR1 for z/OSMF Lite.

To modify the IZUSVR1 settings, follow these steps:

# 1. Make a copy

- 2. Apply your changes
- 3. Store your copy in PROCLIB.

Setting	Purpose	Rules	Default
WLPDIR='directory- path'	WebSphere Liberty server code path.	The directory path must: Be a valid z/OS UNIX path name Be a full or absolute path name Be enclosed in quotation marks Begin with a forward slash ('/').	Default: /usr/lpp/zosmf/liber

Setting	Purpose	Rules	Default
USER_DIR=filepath	z/OSMF data directory path. By default, the z/OSMF data directory is located in /global/zosmf. If you want to use a different path for the z/OSMF data directory, specify that value here, for example: USER_DIR= /the/new/config/dir.	Must be a valid z/OS UNIX path name.	Default: /global/zosmf,

# Appendix C. Adding more users to z/OSMF

Your security administrator can authorize more users to z/OSMF. Simply connect the required user IDs to the z/OSMF administrator group (IZUADMIN). This group is permitted to a default set of z/OSMF resources (tasks and services). For the specific group permissions, see Appendix A in *z/OSMF Configuration Guide*.

You can create more user groups as needed, for example, one group per z/OSMF task.

# **Before you Begin**

Collect the z/OS user IDs that you want to add.

## Procedure

1. On an RACF system, enter the CONNECT command for the user IDs to be granted authorization to z/OSMF resources:

```
CONNECT userid GROUP(IZUADMIN)
```

## Results

The user IDs can now access z/OSMF.

# Installing Zowe runtime from a convenience build

You install the Zowe™ convenience build by obtaining a PAX file for a build and using this to create the Zowe runtime environment.

After you obtain the PAX file, you can take the following steps to complete the installation.

- Step 1: Locate the install directory
- Step 2: Choose a runtime USS folder
- Step 3: Choose a dataset HLQ for the SAMPLIB and LOADLIB
- Step 4 (Method 1): Install the Zowe runtime using shell script
- Step 4 (Method 2): Install the Zowe runtime using z/OSMF Workflow

# Obtaining and preparing the convenience build

The Zowe installation file for Zowe z/OS components is distributed as a PAX file that contains the runtimes and the scripts to install and launch the z/OS runtime.

For each release, there is a PAX file that is named zowe-V.v.p.pax, where

- V indicates the Major Version
- v indicates the Minor Version
- p indicates the Patch Version

The numbers are incremented each time a release is created, so the higher the numbers, the later the release. For more information about the Zowe release number, see Understanding the Zowe release.

To download the PAX file, open your web browser and click the **Zowe z/OS Convenience build** button on the **Zowe Download** website to save it to a folder on your desktop.

After you have the zowe–V.v.p.PAX file, follow these steps.

1. **(Optional)** Verify the integrity of the PAX file to ensure that the file you download is officially distributed by the Zowe project. This step is only needed if you are unsure of the provenance of the PAX file and

want to ensure that it is an original Zowe release driver.

Follow the instructions in the **Verify Hash and Signature of Zowe Binary** section on the postdownload page <a href="https://dlxozlojgf8voe.cloudfront.net/post\_download.html?">https://dlxozlojgf8voe.cloudfront.net/post\_download.html?</a> version=V.v.p after you download the official build. For example, the post-download page for Version 1.4.0 is <a href="https://dlxozlojgf8voe.cloudfront.net/post\_download.html?version=1.4.0">https://dlxozlojgf8voe.cloudfront.net/post\_download.html?</a>

2. Transfer the PAX file to z/OS.

#### Follow these steps:

a. Open a terminal in Mac OS/Linux, or command prompt in Windows OS, and navigate to the directory where you downloaded the Zowe PAX file.

b. Connect to z/OS using SFTP. Issue the following command:

If SFTP is not available or if you prefer to use FTP, you can issue the following command instead:

**Note:** When you use FTP, switch to binary file transfer mode by issuing the following command:

c. Navigate to the target directory that you want to transfer the Zowe PAX file into on z/OS.

**Note:** After you connect to z/OS and enter your password, you enter the UNIX file system. The following commands are useful:

- To see what directory you are in, type pwd.
- To switch directory, type cd.
- To list the contents of a directory, type ls.
- To create a directory, type mkdir.

d. When you are in the directory you want to transfer the Zowe PAX file into, issue the following command:

Where *zowe-V.v.p* is a variable that indicates the name of the PAX file you downloaded.

**Note:** When your terminal is connected to z/OS through FTP or SFTP, you can prepend commands with 1 to have them issued against your desktop. To list the contents of a directory on your desktop, type 11s where 1s lists contents of a directory on z/OS.

3. When the PAX file is transferred, expand the PAX file by issuing the following command in an SSH session:

Where *zowe-V.v.p* is a variable that indicates the name of the PAX file you downloaded.

This will expand to a file structure.

# Installing the Zowe runtime

The first installation step is to create a USS folder that contains the Zowe runtime artifacts. This is known as the <RUNTIME\_DIR>.

## Step 1: Locate the install directory

Navigate to the directory where the installation archive is extracted. Locate the /install directory.

# Step 2: Choose a runtime USS folder

For Zowe to execute, it must be installed into a runtime directory or **<RUNTIME\_DIR>**. This directory will be created during the installation process and the user who performs the installation must have write permission for the installation to succeed.

If you are installing an upgrade of Zowe, the runtime directory used should be the existing <RUNTIME\_DIR> of where the previous Zowe was installed. Upgrading Zowe is only supported for Version 1.8 or later.

For an enterprise installation of Zowe, a <RUNTIME\_DIR> could be /usr/lpp/zowe/v1. For users who test Zowe for themselves, it could be ~/zowe/v1.

# Step 3: Choose a dataset HLQ for the SAMPLIB and LOADLIB

During installation, two PDS data sets are created: the SZWESAMP data set and the SZWEAUTH data set. These are not used at runtime and there is a further step needed to promote these to the z/OS execution environment but they contain required JCL and load modules.

You must know the <DATA\_SET\_PREFIX> into which to create the SZWESAMP and the SZWEAUTH PDS data sets. If a <DATA\_SET\_PREFIX> of OPENSRC.ZWE is specified, the PDS data sets

**OPENSRC.ZWE.SZWESAMP** and **OPENSRC.ZWE.SZWEAUTH** will be created during installation. The storage requirements are included here.

Library DDNAME	Member Type	Target Volume	Туре	Org	RECFM	LRECL	No. of 3390 Trks	No. of DIR BIks
SZWEAUTH	APF Load Modules	ANY	U	PDSE	U	0	15	N/A
SZWESAMP	Samples	ANY	U	PDSE	FB	80	15	5

The SZWESAMP data set contains the following members.

Member name	Purpose
ZWESECUR	JCL member to configure z/OS user IDs and permissions required to run Zowe
ZWENOSEC	JCL member to undo the configuration steps performed in ZWESECUR and revert z/OS environment changes.
ZWEKRING	JCL member to configure a z/OS keyring containing the Zowe certificate
ZWENOKYR	JCL member to undo the configuration steps performed in ZWEKRING
ZWESVSTC	JCL to start Zowe
ZWEXMSTC	JCL to start the Zowe cross memory server
ZWESIP00	Parmlib member for the cross memory server
ZWESASTC	Started task JCL for the cross memory Auxiliary server
ZWESIPRG	Console commands to APF authorize the cross memory server load library

Member name	Purpose	
ZWESISCH	PPT entries required by Cross memory server and its Auxiliary address spaces to run in Key(4)	

The SZWEAUTH data set is a load library containing the following members.

Member name	Purpose	
ZWESIS01	Load module for the cross memory server	
ZWESAUX	Load module for the cross memory server's auxiliary address space	

#### Step 3a: Choose a log directory (optional)

By default, during installation and configuration, various logs will be created in /global/zowe/logs if it is writable, or ~/zowe/logs. If neither of these directories exists, or is writable by the user who installs Zowe, or you want to override and provide your own directory that contains logs, you can specify this with the -l parameter.

Next, you can install the Zowe runtime via different methods.

# Step 4 (Method 1): Install the Zowe runtime using shell script

You install the Zowe runtime by executing the zowe-install.sh script passing in the arguments for the USS runtime directory and the prefix for the SAMPLIB and loadlib PDS members.

In this documentation, the steps of creating the runtime directory and configuring the runtime directory are described separately. The configuration step is the same for a Zowe runtime whether it is installed from a convenience build or from an SMP/E distribution.

# Step 4 (Method 2): Install the Zowe runtime using z/OSMF Workflow

A z/OSMF workflow provides the ability to encapsulate a task as a set of dependent steps. These can be divided across different areas of an organization and can form the basis for the automated auditable processes.

z/OSMF workflows consist of a workflow definition that users then operate and manage as workflow tasks. z/OSMF Workflow tasks can help to guide the activities of system programmers, security administrators, and others who are responsible for managing the configuration of the system. For more information on z/OSMF workflows, see z/OS 2.2 workflows, z/OS 2.3 workflows, and z/OS 2.4 workflows.

Zowe provides a z/OSMF workflow definition that can be used to create a runtime environment from the Zowe convenience build. Register and execute the z/OSMF workflow to create a runtime environment with the z/OSMF web interface.

Perform the following steps to register and execute the Zowe runtime installation workflow in the z/OSMF web interface:

- 1. Log in to the z/OSMF web interface.
- 2. Select **Workflows** from the navigation tree.
- 3. Select Create Workflow from the Actions menu.
- 4. Enter the complete path to the workflow definition file in the **Workflow Definition field**.
  - The path to the workflow definition file is
     <extracted\_pax\_folder>/files/workflows/ZWEWRF04.xml file.
- 5. (Optional) Enter the path to the customized variable input file that you prepared in advance.
  - The path to the variable input file is located is
     <extracted\_pax\_folder>/files/workflows/ZWEWRF04.properties file.
  - Create a copy of the variable input file. Modify the file as necessary according to the built-in comments. Set the field to the path where the new file is located. When you execute the workflow, the values from the variable input file override the workflow variables default values.
- 6. Select the system where you want to execute the workflow.
- 7. Select Next.
- 8. Specify the unique workflow name. 10.Select or enter an Owner Use ID and select **Assign all steps to owner user ID**.
- 9. Select Finish.

The workflow is registered in z/OSMF and ready to execute.

- 10. Select the workflow that you registered from the workflow list.
- 11. Execute the steps in order. The following steps are displayed that are ready to execute manually:
  - Define Variables
    - Define the values for variables for the convenience build runtime installation.
  - Allocate ZFS data set
    - Execute the step to allocate the zFS data set for the Zowe USS.
  - Zowe make dir
    - Execute the step create a directory for the Zowe USS file system.
  - Mount ZFS
    - Execute the step to mount the zFS data set to the created directory
  - Set Mountpoint Owner
    - Execute the step to sets the user who executes the step as the owner of the mountpoint.
    - Run install script Execute the step executes the Zowe convenience build install script.
- 12. Perform the following steps to execute each step individually:
  - i. Double-click the title of the step.
  - ii. Select the **Perform** tab.
  - iii. Review the step contents and update the input values as required.
  - iv. Select Next.
  - v. Repeat the previous two steps to complete all items until the option Finish is available.
  - vi. Select **Finish**.

For general information about how to execute z/OSMF workflow steps, watch the z/OSMF Workflows Tutorial.

After you execute each step, the step is marked as Complete. The workflow is executed.

# Next steps

For a z/OS system where you install Zowe 1.8 or later for the first time, follow the instructions in Stage 3: Configure the Zowe runtime that describes how to configure the z/OS environment and create a keystore directory.

If you have previously installed Zowe 1.8 or later, then you already have an instance directory that needs to be updated. If you have not installed Zowe 1.8 or later before, you will need to create an instance directory to

be able to launch Zowe. For instructions, see Creating and configuring the Zowe instance directory.

Zowe has two started tasks that need to be installed and configured ready to be started. These are the Zowe server, see Installing the Zowe started task (ZWESVSTC) and the Zowe cross memory server, see Installing and configuring the Zowe cross memory server (ZWESISTC).

# Installing Zowe SMP/E

#### Contents

- Introduction
  - Zowe description
  - Zowe FMIDs
- Program materials
  - Basic machine-readable material
  - Program publications
  - Program source materials
  - Publications useful during installation
- Program support
  - Statement of support procedures
- Program and service level information
  - Program level information
  - Service level information
- Installation requirements and considerations
  - Driving system requirements
    - Driving system machine requirements
    - Driving system programming requirements
  - Target system requirements
    - Target system machine requirements
    - Target system programming requirements
    - DASD storage requirements
  - FMIDs deleted
- Installation instructions
  - SMP/E considerations for installing Zowe
  - SMP/E options subentry values
  - Overview of the installation steps
  - Download the Zowe SMP/E package
  - Allocate file system to hold the download package
  - Upload the download package to the host

- Extract and expand the compressed SMPMCS and RELFILEs
  - GIMUNZIP
- Sample installation jobs
- Create SMP/E environment (optional)
- Perform SMP/E RECEIVE
- Allocate SMP/E Target and Distributions Libraries
- Allocate, create and mount ZSF Files (Optional)
- Allocate z/OS UNIX Paths
- Create DDDEF Entries
- Perform SMP/E APPLY
- Perform SMP/E ACCEPT
- Run REPORT CROSSZONE
- Cleaning up obsolete data sets, paths, and DDDEFs
- Activating Zowe
  - File system execution
- Zowe customization

# Introduction

This program directory is intended for system programmers who are responsible for program installation and maintenance. It contains information about the material and procedures associated with the installation of Zowe Open Source Project (Base). This publication refers to Zowe Open Source Project (Base) as Zowe.

The Program Directory contains the following sections:

- **Program Materials** identifies the basic program materials and documentation for Zowe.
- **Program Support** describes the support available for Zowe.
- **Program and Service Level Information** lists the APARs (program level) and PTFs (service level) that have been incorporated into Zowe.
- Installation Requirements and Considerations identifies the resources and considerations that are required for installing and using Zowe.
- Installation Instructions provides detailed installation instructions for Zowe. It also describes the procedures for activating the functions of Zowe, or refers to appropriate publications.

# **Zowe description**

Zowe<sup>™</sup> is an open source project created to host technologies that benefit the Z platform. It is a sub-project of Open Mainframe Project which is part of the Linux Foundation. More information about Zowe is available at https://zowe.org.

# **Zowe FMIDs**

Zowe consists of the following FMIDs:

• AZWE001

# **Program materials**

Basic Machine-Readable Materials are materials that are supplied under the base license and are required for the use of the product.

# Basic machine-readable material

The distribution medium for this program is via downloadable files. This program is in SMP/E RELFILE format and is installed using SMP/E. See Installation instructions for more information about how to install the program.

# **Program source materials**

No program source materials or viewable program listings are provided for Zowe in the SMP/E installation package. However, program source materials can be downloaded from the Zowe GitHub repositories at https://github.com/zowe/.

# Publications useful during installation

Publications listed below are helpful during the installation of Zowe.

Publication Title	Form Number
IBM SMP/E for z/OS User's Guide	SA23-2277
IBM SMP/E for z/OS Commands	SA23-2275

Publication Title	Form Number
IBM SMP/E for z/OS Reference	SA23-2276
IBM SMP/E for z/OS Messages, Codes, and Diagnosis	GA32-0883

These and other publications can be obtained from https://www.ibm.com/shop/publications/order.

# Program support

This section describes the support available for Zowe.

Because this is an alpha release of the Zowe FMID package for early testing and adoption, no formal support is offered. Support is available through the Zowe community. See Community Engagement for details. Slack is the preferred interaction channel.

Additional support may be available through other entities outside of the Open Mainframe Project and Linux Foundation which offers no warranty and provides the package under the terms of the EPL v2.0 license.

## Statement of support procedures

Report any problems which you feel might be an error in the product materials to the Zowe community via the Zowe GitHub community repo at https://github.com/zowe/community/issues/new/choose. You may be asked to gather and submit additional diagnostics to assist the Zowe Community for analysis and resolution.

# **Program and service level information**

This section identifies the program and relevant service levels of Zowe. The program level refers to the APAR fixes that have been incorporated into the program. The service level refers to the PTFs that have been incorporated into the program.

## **Program level information**

All issues of previous releases of Zowe that were resolved before August 2019 have been incorporated into this packaging of Zowe.

# **Service level information**

The Zowe SMP/E package is a distribution of Zowe version 1.9.0 with an FMID of AZWE001.

Subsequent releases of the Zowe z/OS components are delivered as rollup PTFs on zowe.org.

- For Zowe v1.19.1 v1.21.0, the Zowe release is packaged as one single PTF.
- For other versions, the Zowe release is packaged as two co-requisite PTFs, which are made available in a single .zip file.

Zowe release	PTF 1	PTF 2
1.10.0	UO01939	UO01940
1.11.0	UO01942	UO01943
1.12.0	UO01945	UO01946
1.13.0	UO01948	UO01949
1.14.0	UO01951	UO01952
1.15.0	UO01953	UO01954
1.16.0	UO01955	UO01956
1.17.0	UO01958	UO01959
1.18.0	UO01965	UO01966
1.19.0	UO01967	UO01968
1.19.1	UO01969	
1.20.0	UO01970	
1.20.1	UO01980	
1.21.0	UO01981	

Zowe release	PTF 1	PTF 2
1.22.0	UO01982	UO01983
1.23.0	UO01984	UO01991

# Installation requirements and considerations

The following sections identify the system requirements for installing and activating Zowe. The following terminology is used:

- Driving System: the system on which SMP/E is executed to install the program.
- *Target system:* the system on which the program is configured and run.

Use separate driving and target systems in the following situations:

- When you install a new level of a product that is already installed, the new level of the product will replace the old one. By installing the new level onto a separate target system, you can test the new level and keep the old one in production at the same time.
- When you install a product that shares libraries or load modules with other products, the installation can disrupt the other products. By installing the product onto a separate target system, you can assess these impacts without disrupting your production system.

## **Driving system requirements**

This section describes the environment of the driving system required to install Zowe.

#### Driving system machine requirements

The driving system can be run in any hardware environment that supports the required software.

#### Driving system programming requirements

Program	Product	Minimum	Minimum Service Level will	Included in the
Number	Name	VRM	satisfy these APARs	shipped product?

Program Number	Product Name	Minimum VRM	Minimum Service Level will satisfy these APARs	Included in the shipped product?
5650-ZOS	z/OS	V2.2.0 or later	N/A	No

#### Notes:

- SMP/E is a requirement for Installation and is an element of z/OS but can also be ordered as a separate product, 5655-G44, minimally V03.06.00.
- Installation might require migration to a new z/OS release to be service supported. See https://www-01.ibm.com/software/support/lifecycle/index\_z.html.

Zowe is installed into a file system, either HFS or zFS. Before installing Zowe, you must ensure that the target system file system data sets are available for processing on the driving system. OMVS must be active on the driving system and the target system file data sets must be mounted on the driving system.

If you plan to install Zowe in a zFS file system, this requires that zFS be active on the driving system. Information on activating and using zFS can be found in z/OS Distributed File Service zSeries File System Administration (SC24-5989).

# **Target system requirements**

This section describes the environment of the target system required to install and use Zowe.

Zowe installs in the z/OS (Z038) SREL.

#### Target system machine requirements

The target system can run in any hardware environment that supports the required software.

#### Target system programming requirements

#### Installation requisites

Installation requisites identify products that are required and must be present on the system or products that are not required but should be present on the system for the successful installation of Zowe.

Mandatory installation requisites identify products that are required on the system for the successful installation of Zowe. These products are specified as PREs or REQs.

Zowe has no mandatory installation requisites.

Conditional installation requisites identify products that are not required for successful installation of Zowe but can resolve such things as certain warning messages at installation time. These products are specified as IF REQs.

Zowe has no conditional installation requisites.

#### **Operational requisites**

Operational requisites are products that are required and must be present on the system, or, products that are not required but should be present on the system for Zowe to operate all or part of its functions.

Mandatory operational requisites identify products that are required for this product to operate its basic functions. The following table lists the target system mandatory operational requisites for Zowe.

Program Number	Product Name and Minimum VRM/Service Level
5650-ZOS	IBM z/OS Management Facility V2.2.0 or higher
5655-SDK	IBM SDK for Node.js - z/OS V8.16.0 or higher
5655-DGH	IBM 64-bit SDK for z/OS Java Technology Edition V8.0.0

Conditional operational requisites identify products that are not required for Zowe to operate its basic functions but are required at run time for Zowe to operate specific functions. These products are specified as IF REQs. Zowe has no conditional operational requisites.

#### Toleration/coexistence requisites

Toleration/coexistence requisites identify products that must be present on sharing systems. These systems can be other systems in a multi-system environment (not necessarily Parallel Sysplex<sup>TM</sup>), a shared DASD environment (such as test and production), or systems that reuse the same DASD environment at different time intervals.

Zowe has no toleration/coexistence requisites.

#### Incompatibility (negative) requisites

Negative requisites identify products that must *not* be installed on the same system as Zowe.

Zowe has no negative requisites.

#### DASD storage requirements

Zowe libraries can reside on all supported DASD types.

#### Total DASD space required by Zowe

Library Type	Total Space Required in 3390 Trks	Description		
Target	45 Tracks	1		
Distribution	12045 Tracks	/		
File System(s)	21000 Tracks	/		
Web 38666 Tracks Download		These are temporary data sets, which can be removed after the SMP/E install.		

#### Notes:

- 1. For non-RECFM U data sets, we recommend using system-determined block sizes for efficient DASD utilization. For RECFM U data sets, we recommend using a block size of 32760, which is most efficient from the performance and DASD utilization perspective.
- 2. Abbreviations used for data set types are shown as follows.
  - U Unique data set, allocated by this product and used by only this product. This table provides all the required information to determine the correct storage for this data set. You do not need to refer to other tables or program directories for the data set size.
  - **S** Shared data set, allocated by this product and used by this product and other products. To determine the correct storage needed for this data set, add the storage size given in this table to

those given in other tables (perhaps in other program directories). If the data set already exists, it must have enough free space to accommodate the storage size given in this table.

• **E** - Existing shared data set, used by this product and other products. This data set is not allocated by this product. To determine the correct storage for this data set, add the storage size given in this table to those given in other tables (perhaps in other program directories). If the data set already exists, it must have enough free space to accommodate the storage size given in this table.

If you currently have a previous release of Zowe installed in these libraries, the installation of this release will delete the old release and reclaim the space that was used by the old release and any service that had been installed. You can determine whether these libraries have enough space by deleting the old release with a dummy function, compressing the libraries, and comparing the space requirements with the free space in the libraries.

For more information about the names and sizes of the required data sets, see Allocate SMP/E target and distribution libraries.

- 3. Abbreviations used for the file system path type are as follows.
  - **N** New path, created by this product.
  - **X** Path created by this product, but might already exist from a previous release.
  - **P** Previously existing path, created by another product.
- 4. All target and distribution libraries listed have the following attributes:
  - The default name of the data set can be changed.
  - The default block size of the data set can be changed.
  - The data set can be merged with another data set that has equivalent characteristics.
  - The data set can be either a PDS or a PDSE, with some exceptions. If the value in the "ORG" column specifies "PDS", the data set must be a PDS. If the value in "DIR Blks" column specifies "N/A", the data set must be a PDSE.
- 5. All target libraries listed have the following attributes:
  - These data sets can be SMS-managed, but they are not required to be SMS-managed.
  - These data sets are not required to reside on the IPL volume.
  - The values in the "Member Type" column are not necessarily the actual SMP/E element types that are identified in the SMPMCS.

6. All target libraries that are listed and contain load modules have the following attributes:

- These data sets cannot be in the LPA, with some exceptions. If the value in the "Member Type" column specifies "LPA", it is advised to place the data set in the LPA.
- These data sets can be in the LNKLST.
- These data sets are not required to be APF-authorized, with some exceptions. If the value in the "Member Type" column specifies "APF", the data set must be APF-authorized.

#### Storage requirements for SMP/E work data sets

Library DDNAME	TYPE	ORG	RECFM	LRECL	No. of 3390 Trks	No. of DIR Blks
SMPWRK6	S	PDS	FB	80	(20,200)	50
SYSUT1	U	SEQ			(20,200)	0

In the table above, (20,200) specifies a primary allocation of 20 tracks, and a secondary allocation of 200 tracks.

#### Storage requirements for SMP/E data sets

Library DDNAME	TYPE	ORG	RECFM	LRECL	No. of 3390 Trks	No. of DIR Blks
SMPPTS	S	PDSE	FB	80	(12000,3000)	50

The following figures describe the target and distribution libraries and file system paths required to install Zowe. The storage requirements of Zowe must be added to the storage required by other programs that have data in the same library or path.

**Note:** Use the data in these tables to determine which libraries can be merged into common data sets. In addition, since some ALIAS names may not be unique, ensure that no naming conflicts will be introduced before merging libraries.

#### Storage requirements for Zowe target libraries

**Note:** These target libraries are not required for the initial FMID install of Zowe SMP/E but will be required for subsequent SYSMODS so are included here for future reference.

Library DDNAME	Member Type	Target Volume	Туре	Org	RECFM	LRECL	No. of 3390 Trks	No. of DIR BIks
SZWEAUTH	APF Load Modules	ANY	U	PDSE	U	0	15	N/A
SZWESAMP	Samples	ANY	U	PDSE	FB	80	15	5

#### Zowe file system paths

DDNAME	TYPE	Path Name
SZWEZFS	Х	/usr/lpp/zowe/SMPE

#### Storage requirements for Zowe distribution libraries

**Note:** These target libraries are not required for the initial alpha drop of Zowe SMP/E but will be required for subsequent drops so are included here for future reference.

Library DDNAME	TYPE	ORG	RECFM	LRECL	No. of 3390 Trks	No. of DIR Blks
AZWEAUTH	U	PDSE	U	0	15	N/A
AZWESAMP	U	PDSE	FB	80	15	5
AZWEZFS	U	PDSE	VB	6995	12000	30

The following figures list data sets that are not used by Zowe, but are required as input for SMP/E.

Data Set Name	ТҮРЕ	ORG	RECFM	LRECL	No. of 3390 Trks	No. of DIR Blks
hlq.ZOWE.AZWE001.F1	U	PDSE	FB	80	5	N/A

Data Set Name	TYPE	ORG	RECFM	LRECL	No. of 3390 Trks	No. of DIR Blks
hlq.ZOWE.AZWE001.F2	U	PDSE	FB	80	5	N/A
hlq.ZOWE.AZWE001.F4	U	PDSE	VB	6995	9000	N/A
hlq.ZOWE.AZWE001.SMPMCS	U	SEQ	FB	80	1	N/A
z/OS UNIX file system	U	zFS	N/A	N/A	17095	N/A

**Note:** These are temporary data sets, which can be removed after the SMP/E installation.

# **FMIDs deleted**

Installing Zowe might result in the deletion of other FMIDs.

To see which FMIDs will be deleted, examine the ++VER statement in the SMPMCS of the product. If you do not want to delete these FMIDs now, install Zowe into separate SMP/E target and distribution zones.

**Note:** These FMIDs are not automatically deleted from the Global Zone. If you want to delete these FMIDs from the Global Zone, use the SMP/E REJECT NOFMID DELETEFMID command. See the SMP/E Commands book for details.

#### **Special considerations**

Zowe has no special considerations for the target system.

# Installation instructions

This section describes the installation method and the step-by-step procedures to install and activate the functions of Zowe.

#### Notes:

• If you want to install Zowe into its own SMP/E environment, consult the SMP/E manuals for instructions on creating and initializing the SMPCSI and SMP/E control data sets.

- You can use the sample jobs that are provided to perform part or all of the installation tasks. The SMP/E jobs assume that all DDDEF entries that are required for SMP/E execution have been defined in appropriate zones.
- You can use the SMP/E dialogs instead of the sample jobs to accomplish the SMP/E installation steps.

# SMP/E considerations for installing Zowe

Use the SMP/E RECEIVE, APPLY, and ACCEPT commands to install this release of Zowe.

# SMP/E options subentry values

The recommended values for certain SMP/E CSI subentries are shown in the following table. Using values lower than the recommended values can result in failures in the installation. DSSPACE is a subentry in the GLOBAL options entry. PEMAX is a subentry of the GENERAL entry in the GLOBAL options entry. See the SMP/E manuals for instructions on updating the global zone.

Subentry	Value	Comment
DSSPACE	(1200,1200,1400)	Space allocation
PEMAX	SMP/E Default	IBM recommends using the SMP/E default for PEMAX.

# **Overview of the installation steps**

Follow these high-level steps to download and install Zowe Open Source Project (Base).

- 1. Download the Zowe SMP/E package
- 2. Allocate file system to hold web download package
- 3. Upload the download package to the host
- 4. Extract and expand the compress SMPMCS and RELFILEs
- 5. Sample installation jobs
- 6. Create SMP/E environment (optional)
- 7. Perform SMP/E RECEIVE
- 8. Allocate SMP/E target and distribution libraries
- 9. Allocate, create and mount ZSF files (Optional)
- 10. Allocate z/OS UNIX paths

- 11. Create DDDEF Entries
- 12. Perform SMP/E APPLY
- 13. Perform SMP/E ACCEPT
- 14. Run REPORT CROSSZONE
- 15. Cleaning up obsolete data sets, paths, and DDDEFs

## Download the Zowe SMP/E package

To download the Zowe SMP/E package, open your web browser and go to the Zowe Download website. Click the **Zowe SMP/E FMID AZWE001** button to save the file to a folder on your desktop.

You will receive one ZIP package on your desktop. You can extract the following files from the package.

#### • AZWE001.pax.Z (binary)

The SMP/E input data sets to install Zowe are provided as compressed files in AZWE001.pax.Z. This pax archive file holds the SMP/E MCS and RELFILES.

#### • AZWE001.readme.txt (text)

The README file AZWE001.readme.txt is a single JCL file containing a job with the job steps you need to begin the installation, including comprehensive comments on how to tailor them. There is a sample job step that executes the z/OS UNIX System Services pax command to extract package archives. This job also executes the GIMUNZIP program to expand the package archives so that the data sets can be processed by SMP/E.

Review this file on your desktop and follow the instructions that apply to your system.

## Allocate file system to hold the download package

You can either create a new z/OS UNIX file system (zFS) or create a new directory in an existing file system to place AZWE001.pax.Z. The directory that will contain the download package must reside on the z/OS system where the function will be installed.

To create a new file system, and directory, for the download package, you can use the following sample JCL (FILESYS).

Copy and paste the sample JCL into a separate data set, uncomment the job, and modify the job to update required parameters before submitting it.

Expected Return Codes and Messages: You will receive a return code of 0 if this job runs correctly.

# Upload the download package to the host

Upload the AZWE001.readme.txt file in text format and the AZWE001.pax.Z file in binary format from your workstation to the z/OS UNIX file system. The instructions in this section are also in the AZWE001.readme.txt file that you downloaded.

**Note:** Ensure you download the pax file in a different file system than where you put Zowe runtime.

There are many ways to transfer the files or make them available to the z/OS system where the package will be installed. In the following sample dialog, we use FTP from a Microsoft Windows command line to do the transfer. This assumes that the z/OS host is configured as an FTP host/server and that the workstation is an FTP client. Commands or other information entered by the user are in bold, and the following values are assumed.

If you are not sure which protocol or port to use to transfer the files or any access that might be needed, you may need to consult with the network administrator.

User enters:	Values	
mvsaddr	TCP/IP address or hostname of the z/OS system	
tsouid	Your TSO user ID	
tsopw	Your TSO password	
d:	Location of the downloaded files	
@zfs_path@	z/OS UNIX path where to store the files. This matches the @zfs_path@ variable you specified in the previous step.	

**Important!** The AZWE001.pax.Z file must be uploaded to the z/OS driving system in binary format, or the subsequent UNPAX step will fail.

This step of tranferring the files can take a long time to run, depending on the capacity of your system, and on what other jobs are running. Sample FTP upload scenario:

**If you are unable to connect with ftp and only able to use sftp**, the commands above are the same except that you will use *sftp* at the command prompt instead of *ftp*. Also, because *sftp* only supports binary file transfer, the *ascii* and *binary* commands should be omitted. After you transfer the AZWE001.readme.txt file, it will be in an ASCII codepage so you need to convert it to EBCDIC before it can be used. To convert AZWE001.readme.txt to EBCDIC, log in to the distribution system using ssh and run an ICONV command.

#### \_C:>/ssh tsouid@mvsaddr\_

\_tsouid@mvsaddr's password: **tsopw\_** /u/tsouid:> cd:@zfs\_path@ @zfs\_path:> @zfs\_path:> @zfs\_path:>iconv -f ISO8859-1 -t IBM-1047 AZWE001.readme.txt > AZWE001.readme.EBCDIC @zfs\_path:>rm AZWE001.readme.txt @zfs\_path:>mv AZWE001.readme.EBCDIC AZWE001.readme.txt @zfs\_path:>exit C:>/

## **Extract and expand the compressed SMPMCS and RELFILEs**

The AZWE001.readme.txt file uploaded in the previous step holds a sample JCL to expand the compressed SMPMCS and RELFILEs from the uploaded AZWE001.pax.Z file into data sets for use by the SMP/E RECEIVE job. The JCL is repeated here for your convenience.

- @*zfs\_path*@ matches the variable that you specified in the previous step.
- If the oshell command gets a RC=256 and message "pax: checksum error on tape (got ee2e, expected 0)", then the archive file was not uploaded to the host in binary format.
- GIMUNZIP allocates data sets to match the definitions of the original data sets. You might encounter errors if your SMS ACS routines alter the attributes used by GIMUNZIP. If this occurs, specify a non-SMS managed volume for the GINUMZIP allocation of the data sets. For example:
- Normally, your Automatic Class Selection (ACS) routines decide which volumes to use. Depending on your ACS configuration, and whether your system has constraints on disk space, units, or volumes, some supplied SMP/E jobs might fail due to volume allocation errors. See GIMUNZIP for more details.

#### GIMUNZIP

The GIMUNZIP job may issue allocation error messages for SYSUT1 similar to these:

The job will end with RC=12. If this happens, add a TEMPDS control statement to the existing SYSIN as shown below:

where, **&VOLSER** is a DISK volume with sufficient free space to hold temporary copies of the RELFILES. As a guide, this may require 1,000 cylinders, or about 650 MB.

# Sample installation jobs

The following sample installation jobs are provided in hlq.ZOWE.AZWE001.F1, or equivalent, as part of the project to help you install Zowe:

Job Name	Job Type	Description	RELFILE
ZWE1SMPE	SMP/E	(Optional) Sample job to create an SMP/E environment	ZOWE.AZWE001.F1
ZWE2RCVE	RECEIVE	Sample SMP/E RECEIVE job	ZOWE.AZWE001.F1
ZWE3ALOC	ALLOCATE	Sample job to allocate target and distribution libraries	ZOWE.AZWE001.F1
ZWE4ZFS	ALLOMZFS	(Optional) Sample job to allocate, create mountpoint, and mount zFS data sets	ZOWE.AZWE001.F1
ZWE5MKD	MKDIR	Sample job to invoke the supplied ZWEMKDIR EXEC to allocate file system paths	ZOWE.AZWE001.F1
ZWE6DDEF	DDDEF	Sample job to define SMP/E DDDEFs	ZOWE.AZWE001.F1
ZWE7APLY	APPLY	Sample SMP/E APPLY job	ZOWE.AZWE001.F1
ZWE8ACPT	ACCEPT	Sample SMP/E ACCEPT job	ZOWE.AZWE001.F1

**Note:** When Zowe is downloaded from the web, the RELFILE data set name will be prefixed by your chosen high-level qualifier, as documented in the Extract and expand the compressed SMPMCS and RELFILEs section.

You can access the sample installation jobs by performing an SMP/E RECEIVE (refer to Perform SMP/E RECEIVE), then copy the jobs from the RELFILES to a work data set for editing and submission.

You can also copy the sample installation jobs from the product files by submitting the following job. Before you submit the job, add a job statement and change the lowercase parameters to uppercase values to meet the requirements of your site.

See the following information to update the statements in the sample above:

- IN:
  - **filevol** is the volume serial of the DASD device where the downloaded files reside.
- OUT:
  - **jcl-library-name** is the name of the output data set where the sample jobs are stored.
  - **dasdvol** is the volume serial of the DASD device where the output data set resides. Uncomment the statement is a volume serial must be provided.

The following supplied jobs might fail due to disk space allocation errors, as mentioned above for GIMUNZIP. Review the following sections for example error and actions that you can take to resolve the error.

- ZWE2RCVE
- ZWE1SMPE and ZWE4ZFS
- ZWEMKDIR, ZWE1SMPE, ZWE2RCVE, ZWE3ALOC, ZWE4ZFS and ZWE5MKD

#### ZWE2RCVE

Add space and directory allocations to this SMPCNTL statement in the preceding ZWE1SMPE job:

This makes it as below:

#### ZWE1SMPE and ZWE4ZFS

Example error

Uncomment the VOLUMES(...) control statements and refer to the comments at the start of the JCL job for related necessary changes.

#### ZWEMKDIR, ZWE1SMPE, ZWE2RCVE, ZWE3ALOC, ZWE4ZFS and ZWE5MKD

#### Example error

Uncomment the VOL=SER=&... control statements and refer to the comments at the start of the JCL job for related necessary changes.

# Create SMP/E environment (Optional)

A sample job ZWE1SMPE is provided or you may choose to use your own JCL. If you are using an existing CSI, do not run the sample job ZWE1SMPE. If you choose to use the sample job provided, edit and submit ZWE1SMPE. Consult the instructions in the sample job for more information.

**Note:** If you want to use the default of letting your Automatic Class Selection (ACS) routines decide which volume to use, comment out the following line in the sample job ZWE1SMPE.

#### // SET CSIV0L=#csivol

Expected Return Codes and Messages: You will receive a return code of 0 if this job runs correctly.

# Perform SMP/E RECEIVE

Edit and submit sample job ZWE2RCVE to perform the SMP/E RECEIVE for Zowe. Consult the instructions in the sample job for more information.

Expected Return Codes and Messages: You will receive a return code of 0 if this job runs correctly.

# Allocate SMP/E target and distributions libraries

Edit and submit sample job ZWE3ALOC to allocate the SMP/E target and distribution libraries for Zowe. Consult the instructions in the sample job for more information.

Expected Return Codes and Messages: You will receive a return code of 0 if this job runs correctly.

# Allocate, create and mount ZSF files (Optional)

This job allocates, creates a mountpoint, and mounts zFS data sets.

If you plan to install Zowe into a new z/OS UNIX file system, you can edit and submit the optional ZWE4ZFS job to perform the following tasks. Consult the instructions in the sample job for more information.

• Create the z/OS UNIX file system

- Create a mountpoint
- Mount the z/OS UNIX file system on the mountpoint

The recommended z/OS UNIX file system type is zFS. The recommended mountpoint is /usr/lpp/zowe.

Before running the sample job to create the z/OS UNIX file system, you must ensure that OMVS is active on the driving system. zFS must be active on the driving system if you are installing Zowe into a file system that is zFS.

If you create a new file system for this product, consider updating the BPXPRMxx PARMLIB member to mount the new file system at IPL time. This action can be helpful if an IPL occurs before the installation is completed.

See the following information to update the statements in the previous sample:

- **#dsn** is the name of the data set holding the z/OS UNIX file system.
- /usr/lpp/zowe is the name of the mountpoint where the z/OS UNIX file system will be mounted.

Expected Return Codes and Messages: You will receive a return code of 0 if this job runs correctly.

## Allocate z/OS UNIX paths

The target system HFS or zFS data set must be mounted on the driving system when running the sample ZWE5MKD job since the job will create paths in the HFS or zFS.

Before running the sample job to create the paths in the file system, you must ensure that OMVS is active on the driving system and that the target system's HFS or zFS file system is mounted on the driving system. zFS must be active on the driving system if you are installing Zowe into a file system that is zFS.

If you plan to install Zowe into a new HFS or zFS file system, you must create the mountpoint and mount the new file system on the driving system for Zowe.

The recommended mountpoint is */usr/lpp/zowe*.

Edit and submit sample job ZWE5MKD to allocate the HFS or zFS paths for Zowe. Consult the instructions in the sample job for more information.

If you create a new file system for this product, consider updating the BPXPRMxx PARMLIB member to mount the new file system at IPL time. This action can be helpful if an IPL occurs before the installation is completed.

Expected Return Codes and Messages: You will receive a return code of 0 if this job runs correctly.

## **Create DDDEF entries**

Edit and submit sample job ZWE6DDEF to create DDDEF entries for the SMP/E target and distribution libraries for Zowe. Consult the instructions in the sample job for more information.

Expected Return Codes and Messages: You will receive a return code of 0 if this job runs correctly.

# Perform SMP/E APPLY

In this step, you run the sample job ZWE7APLY to apply Zowe. This step can take a long time to run, depending on the capacity of your system, and on what other jobs are running.

#### **Follow these steps**

1. Ensure that you have the latest HOLDDATA; then edit and submit sample job ZWE7APLY to perform an SMP/E APPLY CHECK for Zowe. Consult the instructions in the sample job for more information.

The latest HOLDDATA is available through several different portals, including http://service.software.ibm.com/holdata/390holddata.html. The latest HOLDDATA may identify HIPER and FIXCAT APARs for the FMIDs you will be installing. An APPLY CHECK will help you determine whether any HIPER or FIXCAT APARs are applicable to the FMIDs you are installing. If there are any applicable HIPER of FIXCAT APARs, the APPLY CHECK will also identify fixing PTFs that will resolve the APARs, if a fixing PTF is available.

You should install the FMIDs regardless of the status of unresolved HIPER or FIXCAT APARs. However, do not deploy the software until the unresolved HIPER and FIXCAT APARs have been analyzed to determine their applicability. That is, before deploying the software either ensure fixing PTFs are applied to resolve all HIPER or FIXCAT APARs, or ensure the problems reported by all HIPER or FIXCAT APARs are not applicable to your environment.

To receive the full benefit of the SMP/E Causer SYSMOD Summary Report, do *not* bypass the PRE, ID, REQ, and IFREQ on the APPLY CHECK. The SMP/E root cause analysis identifies the cause only of *errors* and not of *warnings* (SMP/E treats bypassed PRE, ID, REQ, and IFREQ conditions as warnings, instead of errors).

Here are sample APPLY commands:

- i. To ensure that all recommended and critical service is installed with the FMIDs, receive the latest HOLDDATA and use the APPLY CHECK command as follows
- Some HIPER APARs might not have fixing PTFs available yet. You should analyze the symptom flags for the unresolved HIPER APARs to determine if the reported problem is applicable to your environment and if you should bypass the specific ERROR HOLDs in order to continue the installation of the FMIDs.
- This method requires more initial research, but can provide resolution for all HPERs that have fixing PTFs available and not in a PE chain. Unresolved PEs or HIPERs might still exist and require the use of BYPASS.
- ii. To install the FMIDs without regard for unresolved HIPER APARs, you can add the BYPASS(HOLDCLASS(HIPER)) operand to the APPLY CHECK command. This will allow you to install FMIDs, even though one of more unresolved HIPER APARs exist. After the FMIDs are installed, use the SMP/E REPORT ERRSYSMODS command to identify unresolved HIPER APARs and any fixing PTFs.
- This method is quicker, but requires subsequent review of the Exception SYSMOD report produced by the REPORT ERRSYSMODS command to investigate any unresolved HIPERs. If you have received the latest HOLDDATA, you can also choose to use the REPORT MISSINGFIX command and specify Fix Category IBM.PRODUCTINSTALL-REQUIREDSERVICE to investigate missing recommended service.
- If you bypass HOLDs during the installation of the FMIDs because fixing PTFs are not yet available, you can be notified when the fixing PTFs are available by using the APAR Status Tracking (AST) function of the ServiceLink or the APAR Tracking function of Resource Link.
- 2. After you take actions that are indicated by the APPLY CHECK, remove the CHECK operand and run the job again to perform the APPLY.

**Note:** The GROUPEXTENDED operand indicates the SMP/E applies all requisite SYSMODs. The requisite SYSMODS might be applicable to other functions.

**Expected Return Codes and Messages from APPLY CHECK:** You will receive a return code of 0 if the job runs correctly.

**Expected Return Codes and Messages from APPLY:** You will receive a return code of 0 if the job runs correctly.

# Perform SMP/E ACCEPT

Edit and submit sample job ZWE8ACPT to perform an SMP/E ACCEPT CHECK for Zowe. Consult the instructions in the sample job for more information.

To receive the full benefit of the SMP/E Causer SYSMOD Summary Report, do not bypass the PRE, ID, REQ, and IFREQ on the ACCEPT CHECK. The SMP/E root cause analysis identifies the cause of errors but not warnings (SMP/E treats bypassed PRE, ID, REQ, and IFREQ conditions as warnings rather than errors).

Before you use SMP/E to load new distribution libraries, it is recommended that you set the ACCJCLIN indicator in the distribution zone. In this way, you can save the entries that are produced from JCLIN in the distribution zone whenever a SYSMOD that contains inline JCLIN is accepted. For more information about the ACCJCLIN indicator, see the description of inline JCLIN in the SMP/E Commands book for details.

After you take actions that are indicated by the ACCEPT CHECK, remove the CHECK operand and run the job again to perform the ACCEPT.

**Note:** The GROUPEXTEND operand indicates that SMP/E accepts all requisite SYSMODs. The requisite SYSMODS might be applicable to other functions.

**Expected Return Codes and Messages from ACCEPT CHECK:** You will receive a return code of 0 if this job runs correctly.

If PTFs that contain replacement modules are accepted, SMP/E ACCEPT processing will link-edit or bind the modules into the distribution libraries. During this processing, the Linkage Editor or Binder might issue messages that indicate unresolved external references, which will result in a return code of 4 during the ACCEPT phase. You can ignore these messages, because the distribution libraries are not executable and the unresolved external references do not affect the executable system libraries.

**Expected Return Codes and Messages from ACCEPT:** You will receive a return code of 0 if this job runs correctly.

# Run REPORT CROSSZONE

The SMP/E REPORT CROSSZONE command identifies requisites for products that are installed in separate zones. This command also creates APPLY and ACCEPT commands in the SMPPUNCH data set. You can use the APPLY and ACCEPT commands to install those cross-zone requisites that the SMP/E REPORT CROSSZONE command identifies.

After you install Zowe, it is recommended that you run REPORT CROSSZONE against the new or updated target and distribution zones. REPORT CROSSZONE requires a global zone with ZONEINDEX entries that describe all the target and distribution libraries to be reported on.

For more information about REPORT CROSSZONE, see the SMP/E manuals.

#### Cleaning up obsolete data sets, paths, and DDDEFs

The web download data sets listed in DASD storage requirements are temporary data sets. You can delete these data sets after you complete the SMP/E installation.

## **Activating Zowe**

#### **File system execution**

If you mount the file system in which you have installed Zowe in read-only mode during execution, then you do not have to take further actions to activate Zowe.

## **Zowe customization**

You can find the necessary information about customizing and using Zowe on the Zowe doc site.

- For more information about how to customize Zowe, see Configuring Zowe after installation.
- For more information about how to use Zowe, see Using Zowe.

# Installing Zowe SMP/E build with z/OSMF workflow

z/OSMF workflow simplifies the procedure to create an SMP/E environment for Zowe. Register and execute the Zowe SMP/E workflow to create SMP/E environment in the z/OSMF web interface. Perform the following steps to register and execute the Zowe workflow in the z/OSMF web interface:

- 1. Log in to the z/OSMF web interface.
- 2. Select Workflows from the navigation tree.
- 3. Select Create Workflow from the Actions menu.
- 4. Enter the complete path to the workflow definition file in the **Workflow Definition filed**.

The workflow is located in the ZWEWRF01 member of the hlq.Z0WE.AZWE001.F4 data set.

5. (Optional) Enter the path to the customized variable input file that you prepared in advance.

The variable input file is located in ZWEYML01 member of the hlq.Z0WE.AZWE001 data set.

Create a copy of the variable input file. Modify the file as necessary according to the built-in comments. Set the field to the path where the new file is located. When you execute the workflow, the values from the variable input file override the workflow variables default values.

- 6. Select the system where you want to execute the workflow.
- 7. Select Next.
- 8. Specify the unique workflow name.
- 9. Select or enter an Owner Use ID and select Assign all steps to owner user ID.
- 10. Select Finish.

The workflow is registered in z/OSMF and ready to execute.

11. Select the workflow that you registered from the workflow list.

12. Execute the steps in order.

For general information about how to execute z/OSMF workflow steps, watch the z/OSMF Workflows Tutorial.

- 13. Perform the following steps to execute each step individually:
  - i. Double-click the title of the step.
  - ii. Select the **Perform** tab.
  - iii. Review the step contents and update the input values as required.
  - iv. Select Next.
  - v. Repeat the previous two steps to complete all items until the option **Finish** is available.
  - vi. Select Finish.
    - After you execute each step, the step is marked as **Complete**. The workflow is executed.

After you complete executing all the steps individually, the Zowe SMP/E is created.

#### **Activating Zowe**

#### File system execution

If you mount the file system in which you have installed Zowe in read-only mode during execution, then you do not have to take further actions to activate Zowe.

#### **Zowe customization**

You can find the necessary information about customizing and using Zowe on the Zowe doc site.

- For more information about how to customize Zowe, see Configuring Zowe after installation.
- For more information about how to use Zowe, see Using Zowe.

# Docker Installation Roadmap (Technical Preview)

Technical Preview The Zowe Docker build is a technical preview. Technical previews are for testing only and not ready for production. Any feedback that you can provide is highly appreciated. There are three parts to using Docker to install Zowe™.

- The Zowe z/OS runtime which contains the ZSS component.
- The Zowe Cross Memory Server. This is an authorized server application that provides privileged services to Zowe in a secure manner.
- The Zowe Docker image, which runs on a Linux or zLinux host. It consists of three components: Zowe Application Framework, z/OS Explorer Services, and Zowe API Mediation Layer.

Using the Zowe Docker bundle first requires setting up your z/OS system for Zowe. The steps for z/OS setup are detailed on the page: Installing Zowe Server Components on z/OS.

**NOTE**: If you want to install all server components on z/OS instead of using Docker, completing the z/OS install instructions in the above document is all that is required.

Review the installation diagram and the introduction in this topic to see the general installation sequence and the most important tasks that are to be performed during installation and configuration.

**NOTE**: You can click each step on the diagram for detailed instructions.

### **Stage 1: Plan and prepare**

Before you start the installation, review the information on hardware and software requirements and other considerations. See Planning the installation for details.

## Stage 2: Install the Zowe runtime on z/OS

Complete the tasks in **Stage 2** of z/OS Installation Roadmap.

## Stage 3: Configure the Zowe z/OS runtime

First you must complete the tasks in **Stage 3** of z/OS installation Roadmap.

After, you should edit or review the chosen Component groups in the Zowe instance directory that was created. For use with Docker, only the Component group ZSS is required. This means that at minimum, the file instance.env will have the value LAUNCH\_OMPONENT\_GROUPS=ZSS set. See Creating and configuring the Zowe instance directory.

### **Stage 4: Verify the installation**

Verify that Zowe is installed correctly on z/OS. See Verifying Zowe installation on z/OS.

### Stage 5: Install Docker image

Get the latest Docker Image for the Zowe Server Components. See Installing Zowe runtime Docker Image.

### **Stage 6: Configure Docker container**

Extract and customize the start script, instance directory, and keystore before running a Docker container. See Configuring Zowe runtime Docker Container.

## Looking for troubleshooting help?

If you encounter unexpected behavior when installing or verifying the Zowe runtime on z/OS, see the Troubleshooting section for tips.

Version: v1.25.x LTS

# Installing Zowe runtime Docker Image (Technical Preview)

#### **Technical Preview**

Docker is a way to create a pre-packaged set of software and configuration called an "Image". Images are used to create Docker "Containers", which run the Image contents in isolation from the other software running on the same system. Docker containers are the runtime environment, and Images are what they are crated from.

The majority of the Zowe server runtime is available in the form of a Docker Image, among other options. To use this image, you must have set up the Zowe server runtime on z/OS, z/OSMF, or both depending on which Zowe components you will use.

If you have not set up the Zowe server runtime on z/OS, please follow the steps found in Docker Installation Roadmap.

This guide assumes you are using Linux or zLinux and have already downloaded Docker itself. If you have not yet done so, please review System Requirements.

### **Installing via Docker Hub**

Zowe's Docker Image is hosted on Docker Hub, which is the default location from which you can use the Docker command line utility to download and update Docker Images. On Docker Hub, the Zowe server runtime image is named ompzowe/server-bundle.

You can download a Docker Image by using the Docker command line utility **docker pull imagename** where *imagename* is one of the following:

- The latest version of zowe, ompzowe/server-bundle:latest
- The latest version for the platform you are running on, such as omprove/server-bundle:amd64 for Linux
- Older versions can be found with the version tag, such as omprove/server-bundle:v1.20.0
- A specific version by referencing the version's digest, such as ompzowe/serverbundle@sha256:bdbc0617b02e16a452f6d4de50b8b13e56592e309b4c68f9ea52c82303ad57e

• If you want the source code for all of the content in the image, that is available in the accompanying image with -sources prefix tag, such as ompzowe/server-bundle:latest-sources

The latest digests can be seen on the image's tags page.

## Installing via direct download

You can install a Docker Image that has been downloaded as a .tar archive from anywhere, such as Zowe.org.

#### Loading an image from .tar file

To install a Docker Image that you have downloaded as a tar file from somewhere, transfer the file to the destination host and then run the following command: docker image load -i path\_to\_tar

## **Confirming the installation**

The **docker images** command lists the images a system currently has, which make them available for creating containers from.

## Upgrading

Once installed, it is possible to upgrade an image by using **docker pull** with the same *imagename* as before, or by using **docker image load** to load another image of the same type. Newer containers can be created from newer images. In Zowe, configuration can be persisted between containers. More information on this subject can be found in Configuring Docker Container documentation.

If you see this and want to clean up the older images to preserve storage space, you can run the command docker rmi IMAGE\_ID to remove an image, where IMAGE\_ID is the code seen from the images command.

## Verifying authenticity using Docker signing

Dockerhub is equiped with an option authenticity verification feature that you can use to ensure that the Zowe release you are pulling from Dockerhub is legitimate.

Note: With this verification turned on, you will not be able to download images that are not signed.

To turn use this feature, you must set the environment variable DOCKER\_CONTENT\_TRUST=1, then use the "docker pull" command on images that you want to download. This feature can be set to be either temporary or permanent.

**Temporary example** DOCKER\_CONTENT\_TRUST=1 docker pull ompzowe/server-bundle:amd64

#### Permanent example

- 1. Add export DOCKER\_CONTENT\_TRUST=1 to your shell profile, such as echo export DOCKER\_CONTENT\_TRUST=1 >> .profile
- 2. Login again so that the export can take effect.
- 3. Use docker commands, such as docker pull ompzowe/server-bundle:amd64

Version: v1.25.x LTS

# Configuring Zowe runtime Docker Container (Technical Preview)

#### **Technical Preview**

Configuring the Zowe runtime Docker Image has similarities to configuring runtime instance on z/OS. However, there are three major differences:

- Ports are managed between Docker and the host rather than in the instance.env file
- Plugins can be added from the host by using a Docker mount
- External certificates can be used from a Docker mount

### **Working with Docker mounts**

Docker has a feature called a "mount", which allows you to share a folder from the host system into one or more containers. Zowe can use the mount feature in order to share important settings and content, such as certificates and plugins between multiple instances of Zowe. Additionally, mounts keep these objects intact when upgrading between Zowe versions.

## Quick start for the Zowe runtime in Docker

The Zowe Docker Image comes with a sample script for starting a container of Zowe, plus a basic instance configuration.

- 1. Note the ID of the image.
- 2. Start a container of the image without starting Zowe yet by using the environment value ZOWE\_START=0
- 3. Make note of the new container's ID.
- 4. Copy the samples out.

This will generate a sample script for running docker containers, start.sh, and a sample instance as the folder instance.

It is recommended to customize start.sh, however test installs can skip to Starting the container.

Within start.sh, you will be able to see parameters to customize ports, specify which Zowe components to start, specify where the z/OS system is located, and more.

Note: The Zowe keystore cannot be copied in this way because it does not exist initially. If you need to initialize a keystore, you can start Zowe in the container temporarily by omitting ZOWE\_START=0 and run a docker cp command to copy out /global/zowe/keystore to make desired edits.

#### **Customizing Zowe container start script**

There are many different ways to configure a Zowe docker container:

- -h <hostname> hostname of docker host (hostname of your laptop, for example, myhost.acme.net)
- --env ZOWE\_IP\_ADDRESS=<ip> The IP which the servers should bind to. Should not be a loopback address.
- --env ZOSMF\_HOST=<zosmf\_hostname> z/OSMF hostname (for example, mf.acme.net)
- --env ZOSMF\_PORT=<zosmf\_port> z/OSMF port (for example, 1443)
- --env ZWED\_agent\_host=<zss\_hostname> ZSS host (for example, mf.acme.net)
- --env ZWED\_agent\_http\_port=<zss\_port> ZSS port z/OSMF port (for example, 60012).
- --env LAUNCH\_COMPONENT\_GROUPS=<DESKTOP or GATEWAY> What component you want to start.
  - DESKTOP only desktop
  - GATEWAY only GATEWAY + explorers
  - GATEWAY, DESKTOP both
- -v [LOCAL\_KEYSTORE]: /home/zowe/certs:rw Uses external keys and certificates for HTTPS.
   Keystore directory structure is the same as with Zowe on z/OS.
- --env EXTERNAL\_CERTIFICATE=<keystore.p12> location of p12 keystore. (optional)
- --env EXTERNAL\_CERTIFICATE\_ALIAS=<alias> valid alias within keystore. (optional)
- --env EXTERNAL\_CERTIFICATE\_AUTHORITIES=<CA.cer> location of x509 Certificate Authority (optional)
- -v [LOCAL\_APPS\_DIR]:/home/zowe/apps:ro Adds App Framework Apps to the container.
- -v [LOCAL\_INSTANCE\_DIR]:/home/zowe/external\_instance:rw (Recommended) Uses a

Zowe instance directory from outside the container. Recommended to save preferences between

upgrades and to have multiple containers of Zowe sharing configurations.

• --env EXTERNAL\_INSTANCE=/home/zowe/external\_instance - Used together with the -v command to use an external instance directory.

## Note: External certificates are optional, but recommended to resolve self-signed certificate warnings.

#### Using an instance directory external to the Zowe container

Each Zowe container comes with a simple instance directory setup, but it is recommended that this only be used for development, as changes made to the instance will not remain after upgrade and it prevents sharing configuration across multiple containers.

Instead, having an instance directory external to the container solve these issues.

If you have migrated the instance directory from z/OS, copied the simple instance directory from the container, or otherwise have a pre-existing instance directory, you can use it with a Zowe container by using a volume mount command in the start script.

See Creating and configuring the Zowe instance directory to review options for instance directory configuration.

#### Using external certificates

Zowe's keystore can be used to configure which keys and certificates will be used by Zowe for HTTPS connections.

The keystore directory configuration and functionality for Docker is identical to the configuration and functionality on z/OS, except for limitations on storage types. Currently, the Zowe bundle Docker image only supports file-based keys and certificates, such as P12 and PEM files.

To use external certificates, the external instance must set the value of KEYSTORE\_DIRECTORY to /home/zowe/certs, and the keystore directory should exist outside of Docker but mounted to each Docker container via the \_v docker command, for example \_v [LOCAL\_KEYSTORE]:/home/zowe/certs:rw

See Configuring Zowe certificates for more information.

#### Starting the container

The recommended way to start your first container is by running the start.sh script. You can choose to run it with nohup, &, or the docker --detach command as ways to run the container independent of the terminal.

When the container is running, the servers' log output may be printed to the screen depending on the above commands, but the servers will also log to a folder within the instance directory, **\$INSTANCE\_DIR/logs**.

After startup, you can verify that Zowe is running by opening the browser to:

- API Mediation Layer: https://your\_hostname:7554
- App Framework: https://your\_hostname:8544

Or, if the ports were modified, <a href="https://your\_hostname:\$GATEWAY\_PORT">https://your\_hostname:\$APP\_SERVER\_PORT</a> and

## Using Zowe-based products, plugins and apps

To use Zowe-based software with the docker container, you must make that software visible to the Zowe that is within Docker by mapping a folder on your host machine to a folder visible within the docker container.

To share a host directory *HOST\_DIR* into the docker container destination directory *CONTAINER\_DIR* with read/write access, simply add this line to your docker run command: -v [HOST\_DIR]: [CONTAINER\_DIR]: ro

You can have multiple such volumes, but for Zowe Application Framework plugins, the value of *CONTAINER\_DIR* must be //home/zowe/apps

Application Framework plugins within the root directory of */home/zowe/apps* will be automatically installed at start up, but if you have a product which has subdirectories of plugins, it may need manual installation or configuration.

For those plugins, you can run their scripts or Zowe's own install-app.sh script by executing a command in Docker, such as: docker exec -it [CONTAINER\_ID] /home/zowe/instance/bin/install-app.sh [APPLICATION\_DIR]

Note: When installing Application Framework plugins, you can attempt to load them without a server restart via either clicking "Refresh Applications" in the launchbar menu of the Zowe Desktop, or by

doing an HTTP GET call to /plugins?refresh=true to the app server. Some plugins may still need a server restart. Consult product documentation for specifics.

## **Zowe's docker mount locations**

When attempting to share certificates, plugins, or instance configuration to a Zowe container, the mount destination is fixed and therefore the following must be used:

- Certificates: The Zowe keystore destination must be /home/zowe/certs
- App framework plugins: The folder that contains all plugins must be /home/zowe/apps
- Instance configuration: The folder that contains the contents of a Zowe **\$INSTANCE\_DIR** must be /home/zowe/external\_instance

## Configuring the z/OS system for Zowe

Configure the z/OS security manager to prepare for launching the Zowe started tasks.

If Zowe has already been launched on a z/OS system from a previous release of Version 1.8 or later, then you are applying a newer Zowe build. You can skip this security configuration step unless told otherwise in the release documentation.

A SAMPLIB JCL member ZWESECUR is provided to assist with the security configuration. You can submit the ZWESECUR JCL member as-is or customize it depending on site preferences. The JCL allows you to vary which security manager you use by setting the *PRODUCT* variable to be one of RACF, ACF2, or TSS.

If ZWESECUR encounters an error or a step that has already been performed, it will continue to the end, so it can be run repeatedly in a scenario such as a pipeline automating the configuration of a z/OS environment for Zowe installation.

It is expected that the security administrator at a site will want to review, edit where necessary, and either execute ZWESECUR as a single job or else execute individual TSO commands one by one to complete the security configuration of a z/OS system in preparation for installing and running Zowe.

If you want to undo all of the z/OS security configuration steps performed by the JCL member ZWESECUR, Zowe provides a reverse member ZWENOSEC that contains the inverse steps that ZWESECUR performs. This is useful in the following situations:

- You are configuring z/OS systems as part of a build pipeline that you want to undo and redo configuration and installation of Zowe using automation.
- You have configured a z/OS system for Zowe that you no longer want to use and you prefer to delete the Zowe user IDs and undo the security configuration settings rather than leave them enabled.

If you run ZWENOSEC on a z/OS system, then you will no longer be able to run Zowe until you rerun ZWESECUR to reinitialize the z/OS security configuration.

When you run the ZWESECUR JCL, it does not perform the following initialization steps. Therefore, you must complete these steps manually for a z/OS environment.

• Grant users permission to access z/OSMF

- Configure an ICSF cryptographic services environment
- Configure multi-user address space (for TSS only)

The ZWESECUR JCL performs the following initialization steps so you do not need to perform them manually if you have successfully run the JCL. These steps are included for reference if you prefer to manually configure the z/OS environment or want to learn more about user IDs, groups, and associated security permissions that are required to operate Zowe.

- User IDs and groups for the Zowe started tasks
- Configure ZWESVSTC to run under ZWESVUSR user ID
- Configure ZWESLSTC to run high availability instances under ZWESVUSR user ID
- Configure the cross memory server for SAF

#### Grant users permission to access z/OSMF

TSO user IDs using Zowe must have permission to access the z/OSMF services that are used by Zowe. They should be added to the group with appropriate z/OSMF privileges, IZUUSER or IZUADMIN by default. This step is not included in ZWESECUR because it must be done for every TSO user ID who wants to access Zowe's z/OS services. The list of those user IDs is not known by ZWESECUR and will typically be the operators, administrators, developers, or anyone else in the z/OS environment who is logging in to Zowe.

**Note:** You can skip this section if you use Zowe without z/OSMF. Zowe can operate without z/OSMF but services that use z/OSMF REST APIs will not be available, specifically the USS, MVS, and JES Explorers and the Zowe Command Line Interface files, jobs, workflows, tso, and console groups.

For every TSO user ID that is going to log on to Zowe and use services that require z/OSMF,

- If you use RACF, issue the following command:
- If you use ACF2, issue the following commands:
- If you use Top Secret, issue the following commands:

## Configure an ICSF cryptographic services environment

The zssServer uses cookies that require random number generation for security. To learn more about the zssServer, see the Zowe architecture. Integrated Cryptographic Service Facility (ICSF) is a secure way to

generate random numbers.

If you have not configured your z/OS environment for ICSF, see Cryptographic Services ICSF: System Programmer's Guide for more information. To see whether ICSF has been started, check whether the started task ICSF or CSF is active.

If you run Zowe high availability on a Sysplex, ICSF needs to be configured in a Sysplex environment to share KDS data sets across systems in a Sysplex. For detailed information, see Running in a Sysplex Environment

The Zowe z/OS environment configuration JCL member ZWESECUR does not perform any steps related to ICSF that is required for zssServer that the Zowe desktop uses. Therefore, if you want to use Zowe desktop, you must perform the steps that are described in this section manually.

To generate symmetric keys, the ZWESVUSR user who runs Zowe server started task requires READ access to CSFRNGL in the CSFSERV class.

Define or check the following configurations depending on whether ICSF is already installed:

- The ICSF or CSF job that runs on your z/OS system.
- The configuration of ICSF options in SYS1.PARMLIB(CSFPRM00), SYS1.SAMPLIB, SYS1.PROCLIB.
- Create CKDS, PKDS, TKDS VSAM data sets.
- Define and activate the CSFSERV class:
  - If you use RACF, issue the following commands:
  - If you use ACF2, issue the following commands (note that profile-prefix and profilesuffix are user-defined):

(repeat for userids IKED, NSSD, and Policy Agent)

 If you use Top Secret, issue the following command (note that profile-prefix and profilesuffix are user defined):

(repeat for user-acids IKED, NSSD, and Policy Agent)

- Determine whether you want SAF authorization checks against CSFSERV and set CSF.CSFSERV.AUTH.CSFRNG.DISABLE accordingly.
- Refer to the z/OS 2.3.0 z/OS Cryptographic Services ICSF System Programmer's Guide: Installation, initialization, and customization.
- CCA and/or PKCS #11 coprocessor for random number generation.
- Enable FACILITY IRR.PROGRAM.SIGNATURE.VERIFICATION and RDEFINE CSFINPV2 if required.

## **Configure security environment switching**

Typically, the user ZWESVUSR that the Zowe server started task runs under needs to be able to change the security environment of its process to allow API requests to be issued on behalf of the logged on TSO user ID, rather than the server's user ID. This capability provides the functionality that allows users to log on to the Zowe desktop and use apps such as the File Editor to list data sets or USS files that the logged on user is authorized to view and edit, rather than the user ID running the Zowe server. This technique is known as **impersonation**.

To enable impersonation, yo	ou must grant t	he user l	D ZWESVUS	SR associated	with the Zov	ve server started
task UPDATE access to the	BPX.SERVER	and BP	X.DAEMON	profiles in the	FACILITY	class.

You can issue the following commands first to check whether you already have the impersonation profiles defined as part of another server configuration, such as the FTPD daemon. Review the output to confirm that the two impersonation profiles exist and the user ZWESVUSR who runs the Zowe server started task has UPDATE access to both profiles.

- If you use RACF, issue the following commands:
- If you use Top Secret, issue the following commands:
- If you use ACF2, issue the following commands:

If the user ZWESVUSR who runs the Zowe server started task does not have UPDATE access to both profiles follow the instructions below.

- If you use RACF, complete the following steps:
  - i. Activate and RACLIST the FACILITY class. This may have already been done on the z/OS environment if another z/OS server has been previously configured to take advantage of the ability

to change its security environment, such as the FTPD daemon that is included with z/OS Communications Server TCP/IP services.

- ii. Define the impersonation profiles. This may have already been done on behalf of another server such as the FTPD daemon.
- iii. Having activated and RACLIST the FACILITY class, the user ID ZWESVUSR who runs the Zowe server started task must be given update access to the BPX.SERVER and BPX.DAEMON profiles in the FACILITY class.

where <zowe\_stc\_user> is ZWESVUSR unless a different user ID is being used for the z/OS environment.

| Activate these changes |

iv. Issue the following commands to check whether permission has been successfully granted:

- If you use Top Secret, complete the following steps:
  - i. Define the BPX Resource and access for <zowe\_stc\_user>.

where <zowe\_stc\_user> is ZWESVUSR unless a different user ID is being used for the z/OS environment.

- ii. Issue the following commands and review the output to check whether permission has been successfully granted:
- If you use ACF2, complete the following steps:
  - i. Define the BPX Resource and access for <zowe\_stc\_user>.

where <zowe\_stc\_user> is ZWESVUSR unless a different user ID is being used for the z/OS environment.

ii. Issue the following commands and review the output to check whether permission has been successfully granted:

### Configure address space job naming

The user ID ZWESVUSR that is associated with the Zowe started task must have READ permission for the BPX.JOBNAME profile in the FACILITY class. This is to allow setting of the names for the different z/OS UNIX address spaces for the Zowe runtime components. See Address space names.

To display who is authorized to the profile, issue the following command:

Additionally, you need to activate facility class, permit BPX.JOBNAME, and refresh facility class:

For more information, see Setting up the UNIX-related FACILITY and SURROGAT class profiles in the "z/OS UNIX System Services" documentation.

## Configure multi-user address space (for TSS only)

The Zowe server started task either ZWESVSTC or ZWESLSTC is multi-user address space, and therefore a TSS FACILITY needs to be defined and assigned to the started task. Then, all acids signing on to the started task will need to be authorized to the FACILITY.

The following example shows how to create a new TSS FACILITY.

#### Example:

In the TSSPARMS, add the following lines to create the new FACILITY:

For more information about how to administer Facility Matrix Table, see How to Perform Facility Matrix Table Administration.

To assign the FACILITY to the started task, issue the following command:

To authorize a user to sign on to the FACILITY, issues the following command:

## User IDs and groups for the Zowe started tasks

Zowe requires a user ID ZWESVUSR to execute its main z/OS runtime started task. This user ID must have a valid OMVS segment.

Zowe requires a user ID ZWESIUSR to execute the cross memory server started task ZWESISTC. This user ID must have a valid OMVS segment.

Zowe requires a group ZWEADMIN that both ZWESVUSR and ZWESIUSR should belong to. This group must have a valid OMVS segment.

If you have run ZWESECUR, you do not need to perform the steps described in this section, because the TSO commands to create the user IDs and groups are executed during the JCL sections of ZWESECUR.

If you have not run ZWESECUR and are manually creating the user ID and groups in your z/OS environment, the commands are described below for reference.

- To create the ZWEADMIN group, issue the following command:
- To create the ZWESVUSR user ID for the main Zowe started task, issue the following command:
- To create the ZWESIUSR group for the Zowe cross memory server started task, issue the following command:

## Configure ZWESVSTC to run under ZWESVUSR user ID

When the Zowe started task ZWESVSTC is started, it must be associated with the user ID ZWESVUSR and group ZWEADMIN. A different user ID and group can be used if required to conform with existing naming standards.

If you have run ZWESECUR, you do not need to perform the steps described in this section, because they are executed during the JCL section of ZWESECUR.

If you have not run ZWESECUR and are configuring your z/OS environment manually, the following steps describe how to configure the started task ZWESVSTC to run under the correct user ID and group.

- If you use RACF, issue the following commands:
- If you use ACF2, issue the following commands:
- If you use Top Secret, issue the following commands:

# Configure ZWESLSTC to run Zowe high availability instances under ZWESVUSR user ID

You need Zowe started task ZWESLSTC for Zowe high availability. When the Zowe started task ZWESLSTC is started, it must be associated with the user ID ZWESVUSR and group ZWEADMIN. A different user ID and group can be used if required to conform with existing naming standards.

If you have run ZWESECUR, you do not need to perform the steps described in this section, because they are executed during the JCL section of ZWESECUR.

If you have not run ZWESECUR and are configuring your z/OS environment manually, the following steps describe how to configure the started task ZWESLSTC to run under the correct user ID and group.

- If you use RACF, issue the following commands:
- If you use ACF2, issue the following commands:
- If you use Top Secret, issue the following commands:

#### **Configure the cross memory server for SAF**

Zowe has a cross memory server that runs as an APF-authorized program with key 4 storage. Client processes accessing the cross memory server's services must have READ access to a security profile **ZWES.IS** in the **FACILITY** class. This authorization step is used to guard against access by non-priviledged clients.

If you have run ZWESECUR you do not need to perform the steps described in this section, as they are executed during the JCL section of ZWESECUR.

If you have not run ZWESECUR and are configuring your z/OS environment manually, the following steps describe how to configure the cross memory server for SAF.

Activate the FACILITY class, define a ZWES.IS profile, and grant READ access to the user ID ZWESVUSR. This is the user ID that the main Zowe started task runs under.

To do this, issue the following commands that are also included in the ZWESECUR JCL member. The commands assume that you run the Zowe server under the ZWESVUSR user.

- If you use RACF, issue the following commands:
  - To see the current class settings, use:

- To define and activate the FACILITY class, use:
- To RACLIST the FACILITY class, use:
- To define the ZWES.IS profile in the FACILITY class and grant Zowe's started task userid READ access, issue the following commands:

where <zowe\_stc\_user> is the user ID ZWESVUSR under which the Zowe server started task runs.

• To check whether the permission has been successfully granted, issue the following command:

This shows the user IDs who have access to the ZWES.IS class, which should include Zowe's started task user ID with READ access.

- If you use ACF2, issue the following commands:
- If you use Top Secret, issue the following commands, where owner-acid can be IZUSVR or a different ACID:

#### Notes:

- The cross memory server treats "no decision" style SAF return codes as failures. If there is no covering profile for the ZWES.IS resource in the FACILITY class, the request will be denied.
- Cross memory server clients other than Zowe might have additional SAF security requirements. For more information, see the documentation for the specific client.

#### Configure main Zowe server to use identity mapping

This security configuration is necessary for API ML to be able to map client certificate to a z/OS identity. A user running API Gateway must have read access to the RACF general resource IRR.RUSERMAP in the FACILITY class. To set up this security configuration, submit the ZWESECUR JCL member. For users upgrading from version 1.18 and lower use the following configuration steps.

#### **Using RACF**

If you use RACF, verify and update permission in the FACILITY class.

#### Follow these steps:

- 1. Verify user ZWESVUSR has read access.
- 2. Add user ZWESVUSR permission to read.
- 3. Activate changes.

#### Using ACF2

If you use ACF2, verify and update permission in the FACILITY class.

#### Follow these steps:

- 1. Verify user ZWESVUSR has read access.
- 2. Add user ZWESVUSR permission to read.

#### Using TSS

If you use TSS, verify and update permission in FACILITY class.

#### Follow these steps:

- 1. verify user ZWESVUSR has read access.
- 2. Add user ZWESVUSR permission to read.

```
Version: v1.25.x LTS
```

## **Configuring Zowe certificates**

As a system administrator, review this article to learn about the key concepts of Zowe certificates.

Zowe uses a certificate to encrypt data for communication across secure sockets. An instance of Zowe references a USS directory referred to as a **KEYSTORE\_DIRECTORY** which contains information about where the certificate is located.

## **Northbound Certificate**

The Zowe certificate is used by the API Mediation Layer on its northbound edge when identifying itself and encrypting <a href="https://">https://</a> traffic to web browsers or REST client applications. If the Zowe Command Line Interface (CLI) is configured to use the Zowe API Mediation Layer, then the CLI is a client of the Zowe certificate. For more information, see Using the Zowe Command Line Interface, Integrating with the API Mediation Layer.

## **Southbound Certificate**

As well as being a server, Zowe itself is a client to services on the southbound edge of its API Mediation Layer. Zowe communicates to these services over secure sockets. These southbound services use certificates to encrypt their data, and Zowe uses a trust store to store its relationship to these certificates. The southbound services that are started by Zowe itself and run as address spaces under its ZWESVSTC started task (such as the API discovery service, the explorer JES REST API server) re-use the same Zowe certificate used by the API Mediation Layer on its northbound client edge.

## **Trust store**

In addition to Zowe using the intra-address space of certificates, Zowe uses external services on z/OS (such as z/OSMF or Zowe conformant extensions that have registered themselves with the API Mediation Layer) to encrypt messages between its servers. These services present their own certificate to the API Mediation Layer, in which case the trust store is used to capture the relationship between Zowe's southbound edge and these external certificates. To disable the trust store validation of southbound certificates, set the value

VERIFY\_CERTIFICATES=true to false in the zowe-setup-certificates.env file in the KEYSTORE\_DIRECTORY. A scenario when this is recommended is if the certificate presented to the API Mediation Layer is self-signed, such as from an unknown certificate authority. For example, the z/OSMF certificate may be self-signed. In this case, Zowe API Mediation Layer does not recognize the signing authority.

To enable certificate validation without hostname validation, set

NONSTRICT\_VERIFY\_CERTIFICATES=true. Using this setting, the certificate Common Name or Subject Alternate Name (SAN) is not checked. This facilitates deployment to environments where certificates are valid but do not contain a valid hostname. This configuration is for development purposes only and should not be used for production.

The utility script <code>zowe-setup-certificates.sh</code> or the <code>ZWEKRING</code> JCL can help you import z/OSMF certificate authority into trust store. If you are not using Zowe to generate certificates or want to trust other external services, you can customize <code>zowe-setup-certificates.env</code> or <code>ZWEKRING</code> JCL to import them as external certificate authorities.

A proper setup of trust store is mandatory to successfully start Zowe with VERIFY\_CERTIFICATES or NONSTRICT\_VERIFY\_CERTIFICATES enabled in zowe-setup-certificates.env and used by zowe-setup-certificates.sh.

### **Certificates in the Zowe architecture**

The Zowe architecture diagram shows the Zowe API Mediation Layer positioned on the client-server boundary between applications such as web browsers or the Zowe CLI accessing z/OS services. The following diagram is a section of the architecture annotated to describe the role of certificates and trust stores.

The lines shown in bold red are communication over a TCP/IP connection that is encrypted with the Zowe certificate.

- On the northbound edge of the API gateway, the certificate is used between client applications such as web browsers, Zowe CLI, or any other application wishing to access Zowe's REST APIs.
- On the southbound edge of the API Gateway, there are a number of Zowe micro services providing HTML GUIs for the Zowe desktop or REST APIs for the API Catalog. These also use the Zowe certificate for data encryption.

The lines in bold green are external certificates for servers that are not managed by Zowe, such as z/OSMF itself or any Zowe conformant REST API or App Framework servers that are registered with the API Mediation Layer. For the API Mediation Layer to be able to accept these certificates, they either need to be signed by a recognized certificate authority, or else the API Mediation Layer needs to be configured to accept unverified certificates. Even if the API Mediation Layer is configured to accept certificates signed by unverified CAs on its southbound edge, client applications on the northbound edge of the API gateway will be presented with the Zowe certificate.

### Keystore versus key ring

Zowe supports certificates that are stored in a USS directory **Java KeyStore** format.

Beginning with release 1.15, Zowe is including the ability to work with certificates held in a **z/OS Keyring**. Support for Keyring certificates is currently incomplete and being provided as a beta technical preview for early preview by customers. If you have any feedback using keyrings please create an issue in the zoweinstall-packaging repo. It is expected that in a future release keyring support will be made available as a fully supported feature.

## **Keystore directory creation**

The KEYSTORE\_DIRECTORY is created by running the script <RUNTIME\_DIR>/bin/zowe-setupcertificates.sh. This script has a number of input parameters that are specified in a configuration file whose location is passed as an argument to the -p parameter.

The configuration file <RUNTIME\_DIR>/bin/zowe-setup-certificates.env is provided for setting up a Keystore directory that contains the Zowe certificate in JavaKeystore format. The configuration file <RUNTIME\_DIR>/bin/zowe-setup-certificates-keyring.env is provided for setting up a Keystore directory that references the Zowe certificate held in a z/OS keyring.

The .env configuration file should be customized based on security rules and practices for the z/OS environment. Once the script has been successfully executed and the KEYSTORE\_DIRECTORY is created successfully, it is referenced by a Zowe launch instance.env file. A KEYSTORE\_DIRECTORY can be used by more than one instance of Zowe. See Creating and configuring the Zowe instance directory for more information.

The Zowe launch diagram shows the relationship between a Zowe instance directory, a Zowe runtime directory, the Zowe keystore directory, and (if used to store the Zowe certificate) the z/OS keyring.

You create a KEYSTORE\_DIRECTORY in USS by using the script zowe-setup-certificates.sh (1) with a -p argument that specifies a .env configuration file.

- If the -p argument file zowe-setup-certificates.env (2) is used, the KEYSTORE\_DIRECTORY will contain the certificate, the certificate authority, the trust store, and the JWT Secret.
- If the -p argument file zowe-setup-keyring-certificates.env (3) is used, the
   KEYSTORE\_DIRECTORY contains no certificates and is a pass-through to configure a Zowe instance to use a z/OS keyring.

The JCL member ZWEKRING (4) is used to create a z/OS Keyring to hold the Zowe certificate and its signing certificate authority.

At launch time, a Zowe instance is started using the script <INSTANCE\_DIR>/bin/zowe-start.sh which takes configuration arguments from <INSTANCE\_DIR>/instance.env. The argument (5) KEYSTORE\_DIRECTORY=<KEYSTORE\_DIRECTORY> specifies the path to the keystore directory that Zowe will use.

**Note:** If you generated your own server certificate, and you want to enable Client Authentication for it, your server certificate must contain the TLS Web Client Authentication (1.3.6.1.5.5.7.3.2) value in the Extended Key Usage section. Additionally, the Digital signature and/or key agreement must also be set as extension value in the Key Usage section. For more information, see key usage extensions and extended key usage.

For more information on the Zowe launch topology, see Topology of the Zowe z/OS launch process.

## **Configuring Zowe certificates in UNIX files**

A keystore directory is used by Zowe to hold the certificate used for encrypting communication between Zowe clients and the Zowe z/OS servers. The keystore directory also holds the truststore used to hold public keys of any servers that Zowe trusts. When Zowe is launched, the instance directory configuration file instance.env specifies the location of the keystore directory. For more information, see Creating and configuring the Zowe instance directory.

If you created a keystore directory from a previous release of Version 1.8 or later, you can reuse the existing keystore directory with the newer version of Zowe.

You can use the existing certificate signed by an external certificate authority (CA) for HTTPS ports in the API Mediation Layer and the Zowe Application Framework. Alternatively, you can permit the Zowe configuration script to generate a self-signed certificate by the local API Mediation CA.

If you permit the Zowe configuration to generate a self-signed certificate, be sure to import the certificates into your browser to avoid untrusted network traffic challenges. For more information, see Import the local CA certificate to your browser.

**Note:** If you do not import the certificates into your browser when you access a Zowe web page, you may be challenged that the web page cannot be trusted. Depending on the browser you are using, you may have to add an exception to proceed to the web page. Some browser versions may not accept the Zowe certificate because the certificate is self-signed and the signing authority is not recognized as a trusted source. Manually importing the certificate into your browser ensures that the source is trusted, thereby preventing authenication challenges.

If you have an existing server certificate that is signed by an external CA, use this certificate as your Zowe certificate. An example is a CA managed by the IT department of your company, which already ensured that any certificates signed by that CA are trusted by browsers in your company because they have included the CA of the company in the truststore in company browsers. This avoids the need to manually import the local CA into each browser of the client machine.

To avoid requiring each browser to trust the CA that signed the Zowe certificate, you can use a public certificate authority such as *Symantec*, *Comodo*, *Let's Encrypt*, or \_GoDaddy\_to create a certificate. These certificates are trusted by all browsers and most REST API clients. This option, however, requires a manual process to request a certificate and may incur a cost payable to the publicly trusted CA.

We recommend that you start with the local API Mediation Layer CA for an initial evaluation.

You can use the <RUNTIME\_DIR>/bin/zowe-setup-certificates.sh script in the Zowe runtime directory to configure certificates with the set of defined environment variables. The environment variables which act as parameters for the certificate configuration are held in the file <RUNTIME\_DIR>/bin/zowe-setup-certificates.env.

**Note:** In order to enable Client Authentication in your generated certificate, your server certificate must contain the TLS Web Client Authentication (1.3.6.1.5.5.7.3.2) value in the Extended Key Usage section. Additionally, the Digital signature and/or key agreement must be also set as an extension value in the Key Usage section. For more information, see Key usage extentions and extended key usage in the HCL Software documention.

#### Generate a certificate with default values

You can generate a certificate with default values. Use a script to read the default variable values that are provided in the <RUNTIME\_DIR>/bin/zowe-setup-certificates.env file. This script generates the certificate signed by the local API Mediation CA and keystores in the /global/zowe/keystore location. To set up certificates with the default environment variables, run the following script in the Zowe runtime directory:

This script generates the keystore in /global/zowe/keystore.

**Note:** As z/OS installations access to this location is restricted to privileged users, ensure that this step is performed by a system programmer with site knowledge of where the certificate should be stored so that the public key is readable but and that the private key access is controlled.

#### Generate a certificate with custom values

We recommend that you review all parameters in the zowe-setup-certificates.env file, and customize the values for variables to meet your requirements. One example is to set your preferred location to generate certificates and keystores.

Use the the following procedure to customize the values for variables in the zowe-setupcertificates.env file.

Follow these steps:

- 1. Copy the bin/zowe-setup-certificates.env file from the read-only location to a new <p
- 2. Customize the values for the variables based on the descriptions that are provided in the zowesetup-certificates.env file.
- 3. Execute the following command with the customized environment file:

where:

<your\_directory>

specifies the location of your customized environment file

#### <log-directory>

is an optional parameter that overrides the default log output directory of /global/zowe/logs, if it is writable, or ~/zowe/logs.

The keystore and certificates are generated based on the customized values in the bin/zowe-setupcertificates.env file.

The zowe-setup-certificates.sh command also generates the zowe-certificates.env file in the KEYSTORE\_DIRECTORY directory. This file is used in the Zowe instance configuration step. For more information, see Creating and configuring the Zowe instance directory.

# Configure zowe-setup-certificates.env to use existing certificates

The following procedure shows how to configure the zowe-setup-certificates.env file to use the existing certificates.

#### Follow these steps:

1. Update the value of **EXTERNAL\_CERTIFICATE**. The value needs to point to a keystore in PKCS12 format that contains the certificate with its private key. The file needs to be transferred as a binary to the z/OS system.

- 2. Update the value of KEYSTORE\_PASSWORD. The value is a password to the PKCS12 keystore specified in the EXTERNAL\_CERTIFICATE variable.
- 3. Update the value of EXTERNAL\_CERTIFICATE\_ALIAS to the alias of the server certificate in the keystore.

**Note:** If you do not know the certificate alias, run the following command where externalCertificate.p12 is a value of EXTERNAL\_CERTIFICATE in the zowe-setupcertificates.env file.

Expected output:

In this case, the alias can be found in Alias name: apiml. Therefore, set EXTERNAL\_CERTIFICATE\_ALIAS=apiml.

4. Update the value of EXTERNAL\_CERTIFICATE\_AUTHORITIES to the path of the public certificate of the certificate authority that has signed the certificate. You can add additional certificate authorities separated by spaces.

Be sure to specify the complete value *in quotes*. This can be used for certificate authorities that have signed the certificates of the services that you want to access through the API Mediation Layer.

5. (Optional) If you have trouble getting the certificates and you want only to evaluate Zowe, you can switch off the certificate validation by setting VERIFY\_CERTIFICATES=false and NONSTRICT\_VERIFY\_CERTIFICATES=false. This setting continues to use HTTPS, but the API Mediation Layer will not validate any certificate.

**Important!** Switching off certificate evaluation is a non-secure setup. Please talk to your system administrator before you do so and only use these options for troubleshooting purpose.

The following script is the part of zowe-setup-certificates.env file that uses existing certificates:

You may encounter the following message:

This error must be resolved before you can proceed with the next installation step.

Note:

On many z/OS systems, the certificate for z/OSMF is not signed by a trusted CA and is a self-signed certificate by the z/OS system programmer who configured z/OSMF. Based on the configuration, there is chance zowe-setup-certificates.sh may not be able to detect z/OSMF certificate and certificate authority successfully. In this case, you can define ZOSMF\_CERTIFICATE= manually to let Zowe trust the certificate you determined.

If the certificate is from a recognized CA but for a different host name, which can occur when a trusted certificate is copied from one source and reused within a z/OS installation for different servers other than that it was originally created for. We recommended to regenerate certificates with correct HOSTNAME= option.

Switching off VERIFY\_CERTIFICATES, especially NONSTRICT\_VERIFY\_CERTIFICATES is not recommended. It may expose security risks to your z/OS system.

## Using web tokens for SSO on ZLUX and ZSS

Users can use ZWESSOTK JCL to create a PKCS#11 token and configure required security setup. The ZWESSOTK JCL is provided as part of the PDS sample library SZWESAMP that is delivered with Zowe.

Before you submit the JCL, you must customize it and review it with a system programmer who is familiar with z/OS certificates. The JCL member contains commands for two z/OS security managers: RACF and TopSecret. Adding support of ACF/2 is a work in progress.

The ZWESSOTK JCL contains commands for the following scenarios:

- Defining security requirements needed by following steps and using the PKCS#11 token.
- Creation of a locally generated certificated can be used as JWT secret if it does not already exist.
- Creation of PKCS#11 token.
- Binding JWT secret certificate to the PKCS#11 token.

#### Customizing the ZWESSOTK JCL

To customize the ZWESSOTK JCL, edit the JCL variables at the beginning of the JCL and carefully review and edit all the security commands that are valid for your security manager. Review the information in this section when you customize the JCL.

#### **PRODUCT** variable

The **PRODUCT** variable specifies the z/OS security manager. The default value is **RACF**. Change the value to **ACF2** or **TSS** if you are using ACF2 or Top Secret for z/OS as your z/OS security manager.

#### JWTDSNAM variable

If you already have a certificate you want to use as JWT secret, you can set the data set name and uncomment section Import JWT secret below.

#### JWTLABEL variable

This is the certificate label of the JWT secret. This variable has a default value of jwtsecret. This label name should match the value of PKCS11\_T0KEN\_LABEL in zowe-setup-certificates.env.

#### SSOTOKEN variable

This is the PKCS#11 token name will be created by ZWESSOTK JCL. This token name should match the value of PKCS11\_T0KEN\_NAME in zowe-setup-certificates.env.

#### **Enabling SSO**

To enable SSO, you should run zowe-setup-certificates.sh with values of PKCS11\_TOKEN\_NAME and PKCS11\_TOKEN\_LABEL matching what you defined in ZWESSOTK JCL.

If you have already Zowe certificate generated, you should edit the zowe-certificates.env file in the KEYSTORE\_DIRECTORY directory, set the PKCS11\_TOKEN\_NAME and PKCS11\_TOKEN\_LABEL with values which you have defined in ZWESSOTK JCL, and restart Zowe.

If you are upgrading from an old version of Zowe, you can

- rerun zowe-setup-certificates.sh,
- then overwrite KEYSTORE\_DIRECTORY in your instance.env to the newly generated keystore directory.

#### Hints and tips

Learn about some hints and tips that you might find useful when you create certificates.

You create the certificates by running the script zowe-setup-certificates.sh. You do not need to rerun the script after the first time you install Zowe, unless instructed otherwise by SMP/E HOLDDATA or the

release notes for that release.

The creation of the certificates is controlled by the zowe-setup-certificates.env file, and you should have placed a copy of that file in your instance directory INSTANCE\_DIR.

#### 1. Keystore

In your copy of the zowe-setup-certificates.env file, specify the location where you want the zowe-setup-certificates.sh script to place the keys it generates.

By default, a keystore can be shared by all instances, which is also recommended. The default location is /global/zowe/keystore. You can use a different shared location if you prefer. The Zowe instance uses the keystore that you specify in instance.env in your instance directory INSTANCE\_DIR. This can be the shared location or you can create another keystore in a different location for that instance and use that one instead. A single, shared keystore is recommended.

#### 2. Hostname and IP address

You specify the hostname and IP address with the following keywords in the zowe-setupcertificates.env file.

The certificates require the value of **HOSTNAME** to be an alphabetic hostname. Numeric hostnames such as an IP address are not allowed.

The zowe-setup-certificates.sh script attempts to discover the IP address and hostname of your system if you leave these unconfigured in zowe-setup-certificates.env.

On systems with their own internal IP domain, the hostname might not resolve to the external IP address. This happens on ZD&T ADCD-derived systems, where the hostname is usually S0W1.DAL-EBIS.IHOST.COM which resolves to 10.1.1.2. When the script cannot determine the hostname or the external IP address, it will ask you to enter the IP address manually during the dialog. If you have not specified a value for HOSTNAME in zowe-setup-certificates.env, then the script will use the given IP address as the hostname. This will fail because certificates cannot have a numeric hostname.

Therefore, you must specify an alphabetic hostname such as the following one on ZD&T systems before you run the script <code>zowe-setup-certificates.sh</code>.

The values of HOSTNAME and IPADDRESS that the script discovered are appended to the zowesetup-certificates.env file unless they were already set in that file or as shell environment variables before you ran the script.

## **Configuring Zowe certificates in a key ring**

Zowe is able to work with certificates held in a **z/OS Keyring**. For background on Zowe certificates, see Configuring Zowe certificates. To configure Zowe certificates in a key ring, run the ZWEKRING JCL that contains the security commands to create the key ring and manage the certificates that Zowe will use. The ZWEKRING JCL is provided as part of the PDS sample library SZWESAMP that is delivered with Zowe.

Before you submit the JCL, you must customize it and review it with a system programmer who is familiar with z/OS certificates and key rings. The JCL member contains commands for three z/OS security managers: RACF, TopSecret, and ACF/2.

The ZWEKRING JCL contains commands for the following scenarios:

- Creation of a local CA which is used to sign a locally generated certificate, both of which are placed into the key ring.
- (Beta) Importing an existing certificate already held in z/OS to the key ring for use by Zowe.
- (Beta) Creation of a locally generated certificated and signing it with an existing certificate authority, and placing the certificate into the key ring.

**Note:** The scenarios marked **Beta** are provided for technical preview. If you have any feedback on using key rings, create an issue in the Zowe community repo at https://github.com/zowe/community.

After you run the ZWEKRING JCL, a key ring that contains the Zowe certificate is created. In order for a Zowe instance to work with the keystore certificate, you also need to create a USS keystore directory. This USS keystore directory does not contain any certificates, but is required for the Zowe instance.env file to configure the Zowe shell correctly so that the keystore certificate can be located by the Zowe runtime.

To create the USS keystore directory after successfully running ZWEKRING JCL member, run the script <a href="https://www.script.com/www.scrip

## **Customizing the ZWEKRING JCL**

To customize the **ZWEKRING** JCL, edit the JCL variables at the beginning of the JCL and carefully review and edit all the security commands that are valid for your security manager. Review the information in this section when you customize the JCL.

#### **PRODUCT** variable

The **PRODUCT** variable specifies the z/OS security manager. The default value is **RACF**. Change the value to **ACF2** or **TSS** if you are using ACF2 or Top Secret for z/OS as your z/OS security manager.

#### HOSTNAME and IPADDRESS

The Zowe certificate is used on the northbound edge of the API Mediation Layer to encrypt data between web browser and other client applications such as the Zowe command line interface. These client applications will validate that the network TCP/IP address that they have accessed the encrypted data from matches the network address in the certificate. If the address does not match, the browser will not continue as it will consider the site as unsecure.

To ensure that the browser is able to establish a secure connection, set the HOSTNAME and IPADDRESS in the ZWEKRING JCL member to match the hostname and TCP/IP address of the Zowe API Mediation Layer.

#### ZOWERING and LABEL labels

The ZOWERING label is used for the name of the key ring created. The default value is ZoweKeyring. The LABEL label specifies the certificate name and defaults to localhost.

- The value of the ZOWERING label should match the value of the ZOWE\_KEYRING variable in the zowe-setup-keyring-certificates.env file.
- The value of the LABEL label should match the value of the KEYSTORE\_ALIAS variable in the zowe-setup-keyring-certificates.env file.

#### **ROOTZFCA** label

The R00TZFCA label connects the root CA of the z/OSMF certificate with the Zowe key ring.

#### When to set this label?

The value of the parameter VERIFY\_CERTIFICATES and NONSTRICT\_VERIFY\_CERTIFICATES in the zowe-certificates.env file in the KEYSTORE\_DIRECTORY controls whether Zowe's servers validate the authenticity of any southbound certificates at runtime. If the NONSTRICT\_VERIFY\_CERTIFICATES value is true, then the certificate must be signed by a recognized certificate authority (CA), and if the value is false then Zowe services will not validate authenticity of the certificate. If the VERIFY\_CERTIFICATES value is true, beyond the validation of NONSTRICT\_VERIFY\_CERTIFICATES, Zowe will also validate if the certificate "Common Name" or "Subject Alternate Name" (SAN) matches the domain name. This section of the keystore configuration is only required if you are using VERIFY\_CERTIFICATES=true or NONSTRICT\_VERIFY\_CERTIFICATES=true.

When you set VERIFY\_CERTIFICATES=true or NONSTRICT\_VERIFY\_CERTIFICATES=true, then Zowe will validate the authenticity of the z/OSMF certificate, so the root CA of the z/OSMF certificate must be connected with the Zowe key ring. You can connect them by setting the label ROOTZFCA.

If you are unsure of the root CA you can find it by listing the chain of the z/OSMF certificate using the following commands:

• RACF

You can use the CERTAUTH certificate label as the value of R00TZFCA.

• Top Secret

If you see a line like DIGICERT = ZOSMFCA ACCESSORID = CERTAUTH, you should use CERTAUTH record ID ZOSMFCA as the value of ROOTZFCA.

• ACF2

You should use CERTAUTH record ID as the value of R00TZFCA.

### Results

When the ZWEKRING JCL runs successfully, it will create a key ring named ZoweKeyring owned by ZWESVUSR containing the following:

- The Zowe certificate (called localhost)
- The local CA (called ZoweCert)

The certificate used to encrypt the JSON Web Token (JWT) required for single sign-on (called jwtsecret)

When the zowe-setup-certificates.sh script executes successfully, it will generate the USS
KEYSTORE\_DIRECTORY that contains the file zowe-certificates.env. This file is used in the Zowe
instance configuration step. See Creating and configuring the Zowe instance directory.

## Cleanup

The JCL member ZWENOKYR provided in the PDS sample library SZWESAMP contains the inverse commands contained in ZWEKKRING. This allows an environment to be cleaned up and have one or more certificates, key rings, and certificate authorities created by ZWEKRING removed from the z/OS environment. This is useful if you are creating a DevOps pipeline to install and configure and environment for Zowe using ZWEKRING and want to clean that environment before rerunning the pipeline.

## Installing and configuring the Zowe cross memory server (ZWESISTC)

The Zowe cross memory server provides privileged cross-memory services to the Zowe Desktop and runs as an APF-authorized program. The same cross memory server can be used by multiple Zowe desktops. If you wish to start Zowe without the desktop (for example bring up just the API Mediation Layer), you do not need to install and configure a cross memory server and can skip this step. The cross memory server is needed to be able to log on to the Zowe desktop and operate its apps such as the File Editor.

To install and configure the cross memory server, you must define APF-authorized load libraries, program properties table (PPT) entries, and a parmlib. This requires familiarity with z/OS.

- PDS sample library and PDSE load library
- Load module
  - APF authorize
  - Key 4 non-swappable
- PARMLIB
- PROCLIB
- SAF configuration
- Summary of cross memory server installation
- Starting and stopping the cross memory server on z/OS
- Zowe auxiliary service
  - When to configure the auxiliary service
  - Installing the auxiliary service

## PDS sample library and PDSE load library

The cross memory server runtime artifacts, the JCL for the started tasks, the parmlib, and members containing sample configuration commands are found in the SZWESAMP PDS sample library.

The load modules for the cross memory server and an auxiliary server it uses are found in the SZWEAUTH PDSE.

The location of SZWESAMP and SZWEAUTH for a convenience build depends on the value of the zoweinstall.sh -h argument. For more information, see Install Zowe z/OS convenience build.

For an SMP/E installation, SZWESAMP and SZWEAUTH are the SMP/E target libraries whose location depends on the value of the #thlq placeholder in the sample member AZWE001.F1(ZWE3AL0C).

The cross memory server is a long running server process that, by default, runs under the started task name ZWESISTC with the user ID ZWESIUSR and group of ZWEADMIN.

The ZWESISTC started task serves the Zowe desktop that is running under the ZWESVSTC started task, and provides it with secure services that require elevated privileges, such as supervisor state, system key, or APF-authorization.

The user ID ZWESIUSR that is assigned to the cross memory server started tasks must have a valid OMVS segment and read access to the load library SZWEAUTH and PARMLIB data sets. The cross memory server loads some functions to LPA for its PC-cp services.

To install the cross memory server, enable the PROCLIB, PARMLIB, and load module. This topic describes the steps to do this manually.

If you want to install and configure the cross memory server by using scripts, see Scripted installation and configuration of Zowe z/OS components.

## Load module

The cross memory server load module ZWESIS00 is installed by Zowe into a PDSE SZWEAUTH. For the cross memory server to be started, the load module needs to be APF-authorized and the program needs to run in key(4) as non-swappable.

#### **APF** authorize

APF authorize the PDSE SZWESAUTH. This allows the SMP/E APPLY and RESTORE jobs used for applying maintenance to be operating on the runtime PDSE itself when PTF maintenance is applied.

Do not add the SZWEAUTH data set to the system LNKLIST or LPALST concatenations.

To check whether a load library is APF-authorized, you can issue the following command:

where the value of DSNAME is the name of the SZWEAUTH data set as created during Zowe installation that contains the ZWESIS01 load module.

Issue one of the following operator commands to dynamically add the load library to the APF list (until next IPL), where the value of DSNAME is the name of the SZWEAUTH data set, as created during Zowe installation.

- If the load library is not SMS-managed, issue the following operator command, where volser is the name of the volume that holds the data set:
- If the load library is SMS-managed, issue the following operator command:

Add one of the following lines to your active PROGxx PARMLIB member, for example SYS1.PARMLIB(PROG00), to ensure that the APF authorization is added automatically after next IPL. The value of DSNAME is the name of the SZWEAUTH data set, as created during Zowe installation:

- If the load library is not SMS-managed, add the following line, where **volser** is the name of the volume that holds the data set:
- If the load library is SMS-managed, add the following line:

The PDS member SZWESAMP(ZWESIMPRG) contains the SETPROG statement and PROGxx update for reference.

#### Key 4 non-swappable

The cross memory server load module ZWESIS01 must run in key 4 and be non-swappable. For the server to start in this environment, add the following PPT entries for the server and address spaces to the SCHEDxx member of the system PARMLIB.

The PDS member SZWESAMP(ZWESISCH) contains the PPT lines for reference.

Then, issue the following command to make the SCHEDxx changes effective:

## PARMLIB

The ZWESISTC started task must find a valid ZWESIPxx PARMLIB member in order to be launched successfully. The SZWESAMP PDS created at installation time contains the member ZWESIP00 with

default configuration values. You can copy this member to another data set, for example your system PARMLIB data set, or else leave it in SZWESAMP.

If you choose to leave ZWESIPxx in the installation PDS SZWESAMP used at installation time, this has advantages for SMP/E maintenance because the APPLY and RESTORE jobs will be working directly against the runtime library.

Wherever you place the ZWESIP00 member, ensure that the data set is listed in the PARMLIB DD statement of the started task ZWESISTC.

## PROCLIB

For the cross memory server to be started, you must move the JCL PROCLIB ZWESISTC member from the installation PDS SAMPLIB SZWESAMP into a PDS that is on the JES concatenation path.

You need to update the ZWESISTC member in the JES concatenation path with the location of the load library that contains the load module ZWESI00 by editing the STEPLIB DD statement of ZWESISTC. Edit the PARMLIB DD statement to point to the location of the PDS that contains the ZWESIP00 member.

For example, the sample JCL below shows ZWESVSTC where the APF-authorized PDSE containing ZWESI00 is ZWESVUSR.SZWEAUTH and the PDS PARMLIB containing ZWESIP00 is ZWESVUSR.SZWESAMP.

## **SAF configuration**

You must configure the z/OS system in order to correctly run the cross memory server. The steps to perform this are included in the JCL member ZWESECUR that is used to configure a z/OS environment for Zowe, and documented in the section Configure the cross memory server for SAF.

## Summary of cross memory server installation

You can start the cross memory server using the command /S ZWESISTC once the following steps have been completed.

• JCL member ZWESVSTC is copied from SZWESAMP installation PDS to a PDS on the JES concatenation path.

- The PDSE Load Library SZWEAUTH is APF-authorized, or Load module ZWESI00 is copied to an existing APF Auth LoadLib.
- The JCL member ZWESVSTC DD statements are updated to point to the location of ZWESI00 and ZWESIP00.
- The load module ZWESI00 must run in key 4 and be non-swappable by adding a PPT entry to the SCHEDxx member of the system PARMLIB PPT PGMNAME(ZWESI00) KEY(4) NOSWAP.

### Starting and stopping the cross memory server on z/OS

The cross memory server is run as a started task from the JCL in the PROCLIB member ZWESISTC. It supports reusable address spaces and can be started through SDSF with the operator start command with the REUSASID=YES keyword:

The ZWESISTC task starts and stops the ZWESASTC task as needed. Do not start the ZWESASTC task manually.

To end the Zowe cross memory server process, issue the operator stop command through SDSF:

#### Note:

The starting and stopping of the ZWESVSTC started task for the main Zowe servers is independent of the ZWESISTC cross memory server, which is an angel process. If you are running more than one ZWESVSTC instance on the same LPAR, then these will be sharing the same ZWESISTC cross memory server. Stopping ZWESISTC will affect the behavior of all Zowe servers on the same LPAR that use the same cross-memory server name, for example ZWESIS\_STD. The Zowe Cross Memory Server is designed to be a long-lived address space. There is no requirement to recycle regularly. When the cross-memory server is started with a new version of its load module, it abandons its current load module instance in LPA and loads the updated version.

To diagnose problems that may occur with the Zowe ZWESVSTC not being able to attach to the ZWESISTC cross memory server, a log file zssServer-yyyy-mm-dd-hh-mm.log is created in the instance directory /logs folder each time a Zowe ZWESVSTC instance is started. More details on diagnosing errors can be found in Zowe Application Framework issues.

## **Zowe auxiliary service**

Under some situations in support of a Zowe extension, the cross memory server will start, control, and stop an auxiliary address space. This run as a ZWESASTC started task that runs the load module ZWESAUX.

#### When to configure the auxiliary service

Under normal Zowe operation, you will not see any auxiliary address spaces started. However, if you have installed a vendor product running on top of Zowe, this may use the auxiliary service so it should be configured to be launchable. A vendor product documentation will specify whether it needs the Zowe auxiliary service to be configured so ensure that it is needed before attempting the configuration steps.

If you are just using core Zowe functionality, you **do not** need to configure the auxiliary service. Even with the Zowe auxiliary service configured, there is no situation under which you should manually start the ZWESASTC started task.

#### Installing the auxiliary service

To install the auxiliary service to allow it to run, you take similar steps to install and configure the cross memory server as described above, but with a different JCL PROBLIC member and a different load module. There is no PARMLIB for the auxiliary service.

- JCL member ZWESASTC is copied from SZWESAMP installation PDS to a PDS on the JES concatenation path.
- The PDSE load library SZWEAUTH is APF-authorized, or load module ZWESAUX is copied to an existing APF Auth LoadLib.
- The load module ZWESAUX must run in key 4 and be non-swappable by adding a PPT entry to the SCHEDxx member of the system PARMLIB PPT PGMNAME(ZWESAUX) KEY(4) NOSWAP.

#### Important!

The cross memory ZWESISTC task starts and stops the ZWESASTC task as needed. Do not start the ZWESASTC task manually.

# Creating and configuring the Zowe instance directory

The Zowe instance directory or **<INSTANCE\_DIRECTORY>** contains configuration data required to launch a Zowe runtime. This includes port numbers, location of dependent runtimes such as Java, Node, z/OSMF, as well as log files. When Zowe is started, configuration data will be read from files in the instance directory and logs will be written to files in the instance directory.

Note: The creation of an instance directory will set default values for users who want to run all Zowe z/OS components. If you are using Docker, you must make a small configuration change to disable the components on z/OS that will instead run in Docker.

## Introduction

The purpose of the instance directory is to hold information in the z/OS File System (zFS) that is created (such as log files) or modified (such as preferences) or configured (such as port numbers) away from the zFS runtime directory for Zowe. This allows the runtime directory to be read-only and to be replaced when a new Zowe release is installed, with customizations being preserved in the instance directory.

Multiple instance directories can be created and used to launch independent Zowe runtimes from the same Zowe runtime directory.

The Zowe instance directory contains a file instance.env that stores the Zowe configuration data. The data is read each time Zowe is started. You can modify instance.env to configure the Zowe runtime. See Updating the instance.env configuration file for more information.

Alternatively, from v1.22.0 release, you can use a YAML format configuration file zowe.yaml instead of instance.env to configure the Zowe runtime. See Updating the zowe.yaml configuration file for more information.

The instance directory <INSTANCE\_DIRECTORY>/bin contains other key scripts as follows:

- zowe-start.sh is used to start the Zowe runtime by launching the ZWESVSTC started task.
- zowe-stop.sh is used to stop the Zowe runtime by terminating the ZWESVSTC started task.

• zowe-support.sh can be used to capture diagnostics around the Zowe runtime for troubleshooting and off-line problem determination, see Capturing diagnostics to assist problem determination.

#### High availability considerations:

- If you plan to run Zowe in a Sysplex for high availability, the instance directory should be placed in a shared USS file system. This way, all Zowe instances within the Sysplex can read and write to the same instance directory.
- zowe.yaml is required if you want to start Zowe in high availability mode.

## Prerequisites

Before creating an instance directory, ensure that you have created a keystore directory that contains the Zowe certificate. See Creating Zowe certificates for instructions. Also, ensure that you have already configured the z/OS environment. See Configuring the z/OS system for Zowe for instructions.

## **Creating an instance directory**

To create an instance directory, use the zowe-configure-instance.sh script.

Navigate to the Zowe runtime directory **<**RUNTIME\_DIR> and execute the following commands:

If you have an instance directory that is created from a previous release of Zowe 1.8 or later and are installing a newer release of Zowe, then you should run zowe-configure-instance.sh -c <PATH\_T0\_INSTANCE\_DIR> pointing to the existing instance directory to have it updated with any new

values. The release documentation for each new release will specify when this is required, and the file manifest.json within each instance directory contains information for which Zowe release it was created from.

In order to allow the ZWESVSTC started task to have permission to access the contents of the Instance.sh script sets the group ownership of the top level
directory and its child to be ZWEADMIN. If a different group is used for the ZWESVSTC started task you can specify this with the optional -g argument, for example.

## Updating the instance.env configuration file

To operate Zowe, a number of zFS folders need to be located for prerequisites on the platform. Default values are selected when you run zowe-configure-instance.sh. You might want to modify the values.

#### **Contents in this section**

- Zowe prerequisites
- Domain, Hostname and IP Address
- Component groups
- Keystore configuration
- Address space names
- Ports
  - Terminal ports
- API Mediation Layer configuration
- Cross memory server
- Extensions

#### **Zowe prerequisites**

- JAVA\_HOME : The path where 64-bit Java 8 or later is installed. Only needs to be specified if not already set as a shell variable. Defaults to /usr/lpp/java/J8.0\_64.
- NODE\_HOME : The path to the Node.js runtime. Only needs to be specified if not already set as a shell variable.
- ROOT\_DIR: The directory where the Zowe runtime is located, also referred to as the <rul><RUNTIME\_DIR>. Defaults to the location of where zowe-configure-instance was executed.
- ZOSMF\_PORT : The port used by z/OSMF REST services. Defaults to value determined through running netstat .
- Z0SMF\_H0ST : The host name of the z/OSMF REST API services.
- ZOWE\_EXPLORER\_HOST: The hostname of where the Explorer servers are launched from. Defaults to running hostname -c. Ensure that this host name is externally accessible from clients who want to use Zowe as well as internally accessible from z/OS itself.
- ZOWE\_IP\_ADDRESS : The IP address of your z/OS system which must be externally accessible to clients who want to use Zowe. This is important to verify for IBM Z Development & Test Environment

and cloud systems, where the default that is determined through running ping and dig on z/OS returns a different IP address from the external address.

#### Domain, Hostname and IP Address

- ZOWE\_EXPLORER\_HOST: The hostname of where the Explorer servers are launched from. Defaults to running hostname -c. Ensure that this host name is externally accessible from clients who want to use Zowe as well as internally accessible from z/OS itself.
- ZOWE\_IP\_ADDRESS : The IP address of your z/OS system which must be externally accessible to clients who want to use Zowe. This is important to verify for IBM Z Development & Test Environment and cloud systems, where the default that is determined through running ping and dig on z/OS returns a different IP address from the external address.

When configuring a Zowe instance through the instance.env file, ZOWE\_IP\_ADDRESS and ZOWE\_EXPLORER\_HOST are used to specify where the Zowe servers can be reached.

However, these values may not reflect the website name that you access Zowe from. This is especially true in the following cases:

- You are using a proxy
- The URL is a derivative of the value of ZOWE\_EXPLORER\_HOST, such as myhost versus myhost.mycompany.com

In these cases, it may be necessary to specify a value for ZWE\_EXTERNAL\_HOSTS in the form of a commaseparated list of the addresses from which you want to access Zowe in your browser.

```
In the previous example, ZWE_EXTERNAL_HOSTS could include both myhost and myhost.mycompany.com. In the instance.env, this would look like:
ZWE_EXTERNAL_HOSTS=myhost,myhost.mycompany.com
```

This configuration value maybe used for multiple purposes, including referrer-based security checks. In the case that the values are not specified, referrer checks will use the default values of ZOWE\_IP\_ADDRESS, ZOWE\_EXPLORER\_HOST, and the system's hostname. Therefore, if these values are not what you put into your browser, you will want to specify ZWE\_EXTERNAL\_HOSTS to set the correct value.

• ZOWE\_EXPLORER\_FRAME\_ANCESTORS : The MVS, USS, and JES Explorer are served by their respective explorer UI address spaces. These are accessed through the Zowe desktop where they are hosted as iFrames. To protect against double iFrame security vulnerabilities, browsers all of the valid

address that may be used by the browser must be explicitly declared in this property. The default values are: "\${ZOWE\_EXPLORER\_HOST}:\*,\${ZOWE\_IP\_ADDRESS}:\*". If there are any other URLs by which the Zowe Explorers can be served, then these should be appended to the preceding comma-separated list.

#### **Component groups**

**LAUNCH\_COMPONENT\_GROUPS**: This is a comma-separated list of which z/OS microservice groups are started when Zowe launches.

- GATEWAY will start the API mediation layer that includes the API catalog, the API gateway, and the API discovery service. These three address spaces are Apache Tomcat servers and use the version of Java on z/OS as determined by the JAVA\_HOME value. In addition to the mediation layer, the z/OS Explorer services are included here as well.
- DESKTOP will start the Zowe desktop that is the browser GUI for hosting Zowe applications such as the 3270 Terminal emulator or the File Explorer. It will also start ZSS. The Zowe desktop is a node application and uses the version specified by the NODE\_HOME value.
- ZSS will start the ZSS server without including the Desktop and Application Framework server. This can be used with Docker so that you do not run servers on z/OS that will already be running within Docker. This may also be useful if you want to utilize ZSS core features or plug-ins without needing the Desktop. ZSS is a pre-requisite for the Zowe desktop, so when the DESKTOP group is specified then the zss server will be implicitly started. For more information on the zssServer and the technology stack of the Zowe servers see Zowe architecture.
- Vendor products may extend Zowe with their own component group that they want to be lifecycled by the Zowe ZWESVSTC started task and run as a Zowe sub address space. To do this, specify the fully qualified directory provided by the vendor that contains their Zowe extension scripts. This directory will contain a start.sh script (required) that is called when the ZWESVSTC started task is launched, a configure.sh script (optional) that performs any configuration steps such as adding iFrame plug-ins to the Zowe desktop, and a validate.sh script (optional) that can be used to perform any pre-launch validation such as checking system prerequisites. For more information about how a vendor can extend Zowe with a sub address space, see the Extending section.

Note: If you are using Docker, it is recommended to remove GATEWAY and DESKTOP from LAUNCH\_COMPONENT\_GROUPS by setting LAUNCH\_COMPONENT\_GROUPS=ZSS. This will prevent duplication of servers running both in Docker and on z/OS. Technical Preview

#### **Keystore configuration**

• **KEYSTORE\_DIRECTORY**: This is a path to a zFS directory containing the certificate that Zowe uses to identify itself and encrypt https:// traffic to its clients accessing REST APIs or web pages. This also contains a truststore used to hold the public keys of any z/OS services that Zowe is communicating to, such as z/OSMF. The keystore directory must be created the first time Zowe is installed onto a z/OS system and it can be shared between different Zowe runtimes. For more information about how to create a keystore directory, see Configuring Zowe certificates.

#### Address space names

Individual address spaces for different Zowe instances and their subcomponents can be distinguished from each other in RMF records or SDSF views by specifying how they are named. Address space names are 8 characters long and made up of a prefix ZOWE\_PREFIX, instance ZOWE\_INSTANCE followed by an identifier for each subcomponent.

- ZOWE\_PREFIX : This defines a prefix for Zowe address space STC names. Defaults to ZWE .
- ZOWE\_INSTANCE : This is appended to the ZOWE\_PREFIX to build up the address space name. Defaults to 1
- A subcomponent will be one of the following values:
  - AC API ML Catalog
  - AD API ML Discovery Service
  - AG API ML Gateway
  - **DS** App Server
  - **EF** Explorer API Data Sets
  - **EJ** Explorer API Jobs
  - SZ ZSS Server
  - UD Explorer UI Data Sets
  - **UJ** Explorer UI Jobs
  - **UU** Explorer UI USS

The STC name of the main started task is ZOWE\_PREFIX + ZOWE\_INSTANCE + SV.

#### Example:

the first instance of Zowe API ML Gateway identifier will be as follows:

**Note:** If the address space names are not assigned correctly for each subcomponents, check that the step Configure address space job naming has been performed correctly for the z/OS user ID ZWESVUSR.

#### Ports

When Zowe starts, a number of its microservices need to be given port numbers that these microservices use to provide access to their services. You can leave default values for components that are not in use. The two most important port numbers are the GATEWAY\_PORT which is for access to the API Gateway through which REST APIs can be viewed and accessed, and ZOWE\_ZLUX\_SERVER\_HTTPS\_PORT which is used to deliver content to client web browsers logging in to the Zowe desktop. All of the other ports are not typically used by clients and used for intra-service communication by Zowe.

- CATALOG\_PORT : The port the API Catalog service will use. Used when LAUNCH\_COMPONENT\_GROUPS includes GATEWAY.
- DISCOVERY\_PORT : The port the discovery service will use. Used when LAUNCH\_COMPONENT\_GROUPS includes GATEWAY.
- GATEWAY\_PORT : The port the API gateway service will use. Used when
   LAUNCH\_COMPONENT\_GROUPS includes GATEWAY. This port is used by REST API clients to access z/OS services through the API mediation layer, so should be accessible to these clients. This is also the port used to log on to the API catalog web page through a browser.
- JOBS\_API\_PORT : The port the jobs API service will use. Used when LAUNCH\_COMPONENT\_GROUPS includes GATEWAY.
- FILES\_API\_PORT : The port the files API service will use. Used when LAUNCH\_COMPONENT\_GROUPS includes GATEWAY.
- JES\_EXPLORER\_UI\_PORT : The port the jes-explorer UI service will use. Used when LAUNCH\_COMPONENT\_GROUPS includes GATEWAY.
- MVS\_EXPLORER\_UI\_PORT : The port the mvs-explorer UI service will use. Used when LAUNCH\_COMPONENT\_GROUPS`` includes GATEWAY.
- USS\_EXPLORER\_UI\_PORT : The port the uss-explorer UI service will use. Used when LAUNCH\_COMPONENT\_GROUPS includes GATEWAY.
- ZOWE\_ZLUX\_SERVER\_HTTPS\_PORT : The port used by the Zowe desktop. Used when
   LAUNCH\_COMPONENT\_GROUPS includes DESKTOP. It should be accessible to client machines with browsers wanting to log on to the Zowe desktop.
- ZOWE\_ZSS\_SERVER\_PORT : This port is used by the ZSS server. Used when LAUNCH\_COMPONENT\_GROUPS includes DESKTOP or ZSS.

**Note:** If all of the default port values are acceptable, the ports do not need to be changed. To allocate ports for the Zowe runtime servers, ensure that the ports are not in use.

To determine which ports are not available, follow these steps:

- 1. Display the list of ports that are in use with the following command:
- 2. Display the list of reserved ports with the following command:

#### **Terminal ports**

**Note:** Unlike the ports needed by the Zowe runtime for its Zowe Application Framework and z/OS Services which must be unused, the terminal ports are expected to be in use.

- ZOWE\_ZLUX\_SSH\_PORT : The Zowe desktop contains an application VT Terminal which opens a terminal to z/OS inside the Zowe desktop web page. This port is the number used by the z/OS SSH service and defaults to 22. The USS command netstat -b | grep SSHD1 can be used to display the SSH port used on a z/OS system.
- ZOWE\_ZLUX\_TELNET\_PORT: The Zowe desktop contains an application 3270 Terminal which opens a 3270 emulator inside the Zowe desktop web page. This port is the number used by the z/OS telnet service and defaults to 23. The USS command netstat -b | grep TN3270 can be used to display the telnet port used on a z/OS system.
- ZOWE\_ZLUX\_SECURITY\_TYPE : The *3270 Terminal* application needs to know whether the telnet service is using tls or telnet for security. The default value is blank for telnet.

#### **API Mediation Layer configuration**

The following parameters can be set to customize the configuration of all API Mediation Layer components:

• APIML\_DEBUG\_MODE\_ENABLED : When this parameter is set to true, detailed logging of activity by the API mediation layer occurs. This can be useful to diagnose unexpected behavior of the API gateway, API discovery, or API catalog services. Default value is false.

The following parameters can be set to customize the configuration of the Discovery:

• ZWE\_DISCOVERY\_SERVICES\_LIST: A comma-separated list of the endpoints for each Discovery Service instance. The default value is

https://\${ZOWE\_EXPLORER\_HOST}:\${DISCOVERY\_PORT}/eureka/.

The following parameters can be set to customize the configuration of the Gateway:

- APIML\_ALLOW\_ENCODED\_SLASHES : When this parameter is set to true, the Gateway allows encoded characters to be part of URL requests redirected through the Gateway.
- APIML\_CORS\_ENABLED: When this parameter is set to true, CORS are enabled in the API Gateway for Gateway routes api/v1/gateway/\*\*.
- APIML\_PREFER\_IP\_ADDRESS : Set this parameter to true to advertise a service IP address instead of its hostname. **Note**, this configuration is deprecated. Zowe start script will ignore this value and always set it to false.
- APIML\_GATEWAY\_TIMEOUT\_MILLIS: Specifies the timeout for connection to the services in milliseconds.
- APIML\_SECURITY\_X509\_ENABLED : Set this parameter to true, to enable the client certificate authentication functionality through ZSS.
- APIML\_SECURITY\_Z0SMF\_APPLID : The z/OSMF APPLID used for PassTicket.
- APIML\_SECURITY\_AUTH\_PROVIDER : The authentication provider used by the API Gateway. By default, the API Gateway uses z/OSMF as an authentication provider. It is possible to switch to SAF as the authentication provider instead of z/OSMF.

The following values are used to customize the configuration of Caching Service.

- ZWE\_CACHING\_SERVICE\_PORT=7555 : The port the Caching Service will use.
- ZWE\_CACHING\_SERVICE\_PERSISTENT= : This field sets the storage type used to persist data in the Caching Service. Valid options are REDIS or VSAM. REDIS is currently only supported as an off-Z storage solution. VSAM is only supported on Z.
- ZWE\_CACHING\_SERVICE\_VSAM\_DATASET : This field sets the VSAM dataset name to be used to store Caching Service data. This field is required if ZWE\_CACHING\_SERVICE\_PERSISTENT is set to VSAM, otherwise this field is not needed.

Refer to detailed section about API Gateway configuration

#### **Cross memory server**

• ZOWE\_ZSS\_XMEM\_SERVER\_NAME : For the Zowe Desktop to operate communication with the Zowe cross memory server. The default procedure name ZWESIS\_STD is used for the cross memory server. However, this can be changed in the ZWESISTC PROBLIC member. This might occur to match local naming standards, or to allow isolated testing of a new version of the cross memory server while an

older version is running concurrently. The Zowe desktop that runs under the ZWESVSTC started task will locate the appropriate cross memory server running under its started task ZWESISTC using the ZOWE\_ZSS\_XMEM\_SERVER\_NAME value. If this handshake cannot occur, users will be unable to log in to the Zowe desktop. See Troubleshooting: ZSS server unable to communicate with X-MEM.

- ZWES\_ZIS\_LOADLIB: The dataset name where the Zowe cross memory server (ZIS) load library resides. Having this value defined can help in automation around ZIS and ZIS plugins.
- ZWES\_ZIS\_PLUGINLIB: The dataset name where plugins for ZIS should be placed. When this is specified, components that contain ZIS plugins will have their load library content placed here.
- ZWES\_ZIS\_PARMLIB: The dataset name where parameters about ZIS should be placed. Having this value defined is necessary for automatically installing ZIS plugins that are within a component.

#### **Extensions**

- ZWEAD\_EXTERNAL\_STATIC\_DEF\_DIRECTORIES : Full USS path to the directory that contains static API Mediation Layer .yml definition files. For more information, see Onboard a REST API without code changes required. Multiple paths should be semicolon separated. This value allows a Zowe instance to be configured so that the API Mediation Layer can be extended by third party REST API and web UI servers.
- EXTERNAL\_COMPONENTS : For third-party extenders to add the full path to the directory that contains their component lifecycle scripts. For more information, see Zowe lifecycle Zowe extensions.
- ZWE\_DISCOVERY\_SERVICES\_LIST: (Work in progress) **Do not modify this value** from its supplied default of https://\${ZOWE\_EXPLORER\_HOST}:\${DISCOVERY\_PORT}/eureka/.
- ZWE\_CACHING\_SERVICE\_PORT=7555 : (Work in progress) This port is not yet used so the value does not need to be availale.
- ZWE\_CACHING\_SERVICE\_PERSISTENT : (Work in progress) This is used to set the storage type used to persist cached data. Valid options are REDIS or VSAM.
- ZWE\_CACHING\_SERVICE\_VSAM\_DATASET : (Work in progress)

### Updating the zowe.yaml configuration file

Instead of using instance.env to configure the Zowe runtime, you can also use a zowe.yaml file to configure Zowe in more granular level. zowe.yaml is also required to start Zowe in high availability mode. To make Zowe runtime recognize the zowe.yaml configuration, you must create a zowe.yaml file and remove the instance.env file from the instance directory. See Creating the zowe.yaml file for instructions.

**Note:** In the following sections, we refer configuration keys with concatenation of key names and dots. For example, if you want to update the configuration key <code>zowe.internalCertificate.keystore.type</code> with value <code>PKCS12</code>, you should set value for this entry in the <code>zowe.yaml</code>:

To learn more about the YAML format, please visit yaml.org.

#### **Contents in this section**

- Known limitations for Zowe high availability
- Creating the zowe.yaml file
- High level overview of YAML configuration file
- Extract sharable configuration out of zowe.yaml
- Configuration override
- YAML configurations certificate
- YAML configurations zowe
- YAML configurations java
- YAML configurations node
- YAML configurations zOSMF
- YAML configurations components
  - Configure component gateway
  - Configure component discovery
  - Configure component api-catalog
  - Configure component caching-service
  - Configure component app-server
  - Configure component zss
  - Configure component jobs-api
  - Configure component files-api
  - Configure component explorer-jes
  - Configure component explorer-mvs
  - Configure component explorer-uss
  - Configure external extension
- YAML configurations halnstances

#### Known limitations for Zowe high availability

- To allow Sysplex Distributor to route traffic to the Gateway, you can only start one Gateway in each LPAR within the Sysplex. All Gateways instances should be started on the same port configured on Sysplex Distributor.
- Zowe App Server should be accessed through the Gateway with a URL like <a href="https://dvipa-domain>:<external-port>/zlux/ui/v1">https://dvipa-domain>:<external-port>/zlux/ui/v1</a>.

#### Creating the zowe.yaml file

There are two ways to create a zowe.yaml file.

- Copy the example file <instance-dir>/bin/example-zowe.yaml to <instancedir>/zowe.yaml and modify it based on your configuration.
- Convert from an existing instance.env file by using a utility tool in <instancedir>/bin/utils/convert-to-zowe-yaml.sh shipped with Zowe. Issue the following command to convert an instance.env file to zowe.yaml format:

where, the <instance-dir> is your instance directory path.

After zowe.yaml is created, you should add new haInstances section and define ha-instance(s) you want to start in your Sysplex.

#### High level overview of YAML configuration file

The YAML configuration file has few high level sections:

- **zowe** : defines global configurations specific to Zowe, including default values.
- **java**: defines Java configurations used by Zowe components.
- **node** : defines node.js configurations used by Zowe components.
- **ZOSMF** : tells Zowe your z/OSMF configurations.
- **components** : defines detailed configurations for each Zowe component or extension. Each component or extension may have a key entry under this section. For example, components.gateway is configuration for API Mediation Layer Gateway service.
- **haInstances**: defines customized configurations for each High Availability (HA) instance. You should predefine all Zowe HA instances you want to start within your Sysplex.

#### Extract sharable configuration out of zowe.yaml

The Zowe YAML configuration file supports a special @include annotation that can be used in any level of the configuration. This enables you to organize your YAML configuration files and extract sharable configurations to a separate YAML file.

For example, you can define a sharable certificate configuration file <keystore-dir>/zowecertificates.yaml like this:

Then in your <instance-dir>/zowe.yaml, you can import this certification file like this:

#### **Configuration override**

Inside zowe.yaml, you can define default values and they may be overridden in more granular level configurations. This can happen in several ways:

• Component can override default certificate configuration. For specific entry of certification configuration, if it's not overridden, it will fall back to default configurations. For example, in this configuration:

App Server will use the certificate alias app-server instead of localhost from the same keystore defined in zowe.internalCertificate.keystore.file. And it will use the exact same truststore defined in zowe.internalCertificate.trustStore.file.

HA instance component configuration haInstances.
 haInstances.
 can override global level component configurations components.
 components.
 components.
 components.
 level can be overridden in haInstances.
 ha instances.
 components.
 level.
 For example, in this configuration:

App Server on lpar2a HA instance will not be started. On lpar2b HA instance, it will be started but on port 28544.

#### YAML configurations - certificate

In Zowe YAML configuration, certificate definition shares the same format and this format can be used in several configuration entries. For example, zowe.externalCertificate,

zowe.internalCertificate, components.<component>.certificate, and haInstances.

<ha-instance>.components.<component>.certificateThe certificate definition may include the following entries:

- keystore.type: Defines the type of the keystore. If you are using keystore, this value usually should be PKCS12. If you are using keyring, this value should be JCERACFKS.
- keystore.file: Defines the path of the keystore file. If you are using keyring, this should look like safkeyring:///<keyring-owner>/<keyring-name>. For example, safkeyring:///ZWESVUSR/ZoweKeyring.
- keystore.alias: represents the alias name of the certificate stored in keystore. If you are using keyring, this is the certificate label connected to the keyring.
- keystore.password : Defines the password of the keystore.
- trustStore.file: Defines the path to the truststore file. If you are using keyring, this should look like safkeyring:///<keyring-owner>/<keyring-name>, usually will be the same value of keystore.file.
- trustStore.certificateAuthorities : defines extra certificate authorities you will trust. This should point to CA files in PEM format.
- pem.key : Defines the private key file in PEM format. This can be used by applications that do not support either PKCS12 keystore format or z/OS keyring.
- pem.certificate: Defines the public key file in PEM format. This can be used by applications that do not support either PKCS12 keystore format or z/OS keyring.
- pem.certificateAuthority: Defines certificate authorities in PEM format. This can be used by applications that do not support either PKCS12 keystore format or z/OS keyring.

Note: With the zowe.yaml configuration, all certificate related configurations are merged into the zowe.yaml file. <keystore-dir>/zowe-certificates.env will not be used.

#### YAML configurations - zowe

The high-level configuration zowe supports these definitions:

- zowe.runtimeDirectory: Tells Zowe the runtime directory connected to this Zowe instance. This is equivalent to the ROOT\_DIR variable in the instance.env file.
- zowe.extensionDirectory : Tells Zowe where you put the runtime of all your extensions. This is equivalent to the ZWE\_EXTENSION\_DIR variable in the instance.env file.
- zowe.jobPrefix : Defines the Zowe job prefix for the ZWESVSTC started task. This is equivalent to the ZOWE\_PREFIX variable in the instance.env file.

- zowe.identifier: Defines the Zowe job identifier for the ZWESVSTC started task. This is equivalent to the ZOWE\_INSTANCE variable in the instance.env file.
- zowe.externalDomains: Defines a list of external domains that will be used by the Zowe instance. This configuration is an array of domain name strings. This is equivalent to the ZWE\_EXTERNAL\_HOSTS variable in the instance.env file but should be represented as an array. In Sysplex deployment, this is the DVIPA domain name defined in Sysplex Distributor. For example,
- zowe.externalPort : Defines the port that will be exposed to external Zowe users. By default, this value is set based on the GATEWAY\_PORT variable in the in the instance.env file. In Sysplex deployment, this is the DVIPA port defined in Sysplex Distributor. See Configure Sysplex Distributor for more information.
- zowe.environments : Defines extra environment variables to customize the Zowe runtime. This configuration is a list of key / value pairs. This is equivalent to adding new environment variables to the instance.env file. For example,
- zowe.externalCertificate: Defines the northbound certificate facing Zowe users. These configurations are defined in <keystore-dir>/zowe-certificates.env.

**Note:** This configuration is not the same as the EXTERNAL\_CERTIFICATE configuration in zowesetup-certificates.env. In zowe-setup-certificates.env, EXTERNAL\_CERTIFICATE means that the certificate is not generated by the zowe-setup-certificates.sh utility script.

- zowe.internalCertificate: Defines the default southbound certificate used within Zowe services. These configurations are defined in <keystore-dir>/zowe-certificates.env. By default, this is the same as zowe.externalCertificate.
- zowe.sso.token.name: Defines SSO token name. This is equivalent to the PKCS11\_TOKEN\_NAME variable in <keystore-dir>/zowe-certificates.env.
- zowe.sso.token.label: Defines the certificate label that binds to SSO token. This is equivalent to the PKCS11\_TOKEN\_LABEL variable in <keystore-dir>/zowe-certificates.env.
- zowe.launcher: The launcher section defines defaults about how the Zowe launcher should act upon components.
- zowe.launcher.restartIntervals : An array of positive integers that defines how many times a component should be tried to be restarted if it fails, and how much time to wait in seconds for that

restart to succeed before retrying.

- zowe.launcher.minUptime: The minimum amount of time a zowe component should be running in order to be declared as started successfully.
- zowe.launcher.shareAs: Whether or not the launcher should start components in the same address space as it. See documentation for \_BPX\_SHAREAS for details.

#### YAML configurations - java

The high-level configuration java supports these definitions:

• home : Defines the path to the Java runtime directory. This is equivalent to the JAVA\_HOME variable in the instance.env file.

#### **YAML configurations - node**

The high-level configuration node supports these definitions:

• home : Defines the path to the Node.js runtime directory. This is equivalent to the NODE\_HOME variable in the instance.env file.

#### YAML configurations - zOSMF

The high-level configuration **z0SMF** supports these definitions:

- z0SMF.host : Defines the hostname of your z/OSMF instance. This is equivalent to the Z0SMF\_H0ST variable in the instance.env file.
- zOSMF.port : Defines the port of your z/OSMF instance. This is equivalent to the ZOSMF\_PORT variable in the instance.env file.
- z0SMF.applId : Defines the application ID of your z/OSMF instance. This is equivalent to the APIML\_SECURITY\_Z0SMF\_APPLID variable in the instance.env file.

#### YAML configurations - components

All Zowe components and extensions can have a dedicated section under the components high-level configuration.

In this section, <component> represents any Zowe components or extensions. For all components and extensions, these are the common definitions.

- components.<component>.enabled : Defines if you want to start this component in this Zowe instance. This is a much detailed granular definition of the LAUNCH\_COMPONENT\_GROUPS variable in instance.env. This allows you to control each component instead of a group. For external components, also known as extensions, this configuration also replaces the EXTERNAL\_COMPONENTS variable in instance.env.
- components.<component>.certificate: you can customize a component to use different certificate from default values. This section follows same format defined in YAML configurations certificate. If this is not customized, the component will use certificates defined in zowe.internalCertificate.
- components.<component>.launcher: Any component can have a launcher section which overrides the overall Zowe Launcher default defined in zowe.launcher.

#### **Configure component gateway**

These configurations can be used under the components.gateway section:

- port : Defines the port which the gateway should be started on. This is equivalent to the GATEWAY\_PORT variable in instance.env.
- debug : Defines whether to enable debug mode for gateway. This is equivalent to the APIML\_DEBUG\_MODE\_ENABLED variable in instance.env but with better granular level.
- apiml.service.allowEncodedSlashes : When this parameter is set to true, the Gateway allows encoded characters to be part of URL requests redirected through the Gateway. This is equivalent to the APIML\_ALLOW\_ENCODED\_SLASHES variable in instance.env.
- apiml.service.corsEnabled : When this parameter is set to true, CORS are enabled in the API Gateway for Gateway routes api/v1/gateway/\*\*. This is equivalent to the APIML\_CORS\_ENABLED variable in instance.env.
- apiml.service.preferIpAddress: Set this parameter to true to advertise a service IP address instead of its hostname. Note: This configuration is deprecated. Zowe start script will ignore this value and always set it to false. This is equivalent to the APIML\_PREFER\_IP\_ADDRESS variable in instance.env.
- apiml.gateway.timeoutMillis: Specifies the timeout for connection to the services in milliseconds. This is equivalent to the APIML\_GATEWAY\_TIMEOUT\_MILLIS variable in instance.env.

- apiml.security.x509.enabled : Set this parameter to true to enable the client certificate authentication functionality through ZSS. This is equivalent to the APIML\_SECURITY\_X509\_ENABLED variable in instance.env.
- apiml.security.x509.externalMapperUrl: Defines the URL where Gateway can query the mapping of client certificates. This is equivalent to the APIML\_GATEWAY\_EXTERNAL\_MAPPER variable in instance.env.
- apiml.security.zosmf.applid: Defines the z/OSMF APPLID used for PassTicket. This is equivalent to the APIML\_SECURITY\_ZOSMF\_APPLID variable in instance.env. This should have the same value of zOSMF.applid. This entry is kept for backward compatibility.
- apiml.security.auth.provider: Defines the authentication provider used by the API Gateway. This is equivalent to the APIML\_SECURITY\_AUTH\_PROVIDER variable in instance.env.
- apiml.security.authorization.endpoint.url: Defines the URL to the authorization endpoint. This endpoint tells Gateway if a user has a particular permission on SAF profile. For example, permission to the APIML.SERVICES profile of ZOWE class. This is equivalent to the APIML SECURITY AUTHORIZATION ENDPOINT URL variable in instance.env.
- apiml.security.ssl.verifySslCertificatesOfServices: Defines whether APIML should verify certificates of services in strict mode. Setting to true will enable the strict mode where APIML will validate if the certificate is trusted in turststore, and also if the certificate Common Name or Subject Alternate Name (SAN) matches the service hostname. This is equivalent to the VERIFY\_CERTIFICATES variable defined in <keystore-dir>/zowe-certificates.env.
- apiml.security.ssl.nonStrictVerifySslCertificatesOfServices : Defines whether APIML should verify certificates of services in non-strict mode. Setting the value to true will enable the non-strict mode where APIML will validate if the certificate is trusted in turststore, but ignore the certificate Common Name or Subject Alternate Name (SAN) check. Zowe will ignore this configuration when strict mode is enabled with

apiml.security.ssl.verifySslCertificatesOfServices. This is equivalent to the NONSTRICT\_VERIFY\_CERTIFICATES variable defined in <keystore-dir>/zowe-certificates.env.

- apiml.server.maxConnectionsPerRoute: Specifies the maximum connections for each service. This is equivalent to the APIML\_MAX\_CONNECTIONS\_PER\_ROUTE variable in instance.env.
- apiml.server.maxTotalConnections: Specifies the total connections for all services registered under API Mediation Layer. This is equivalent to the APIML\_MAX\_TOTAL\_CONNECTIONS variable in instance.env.

#### Configure component discovery

These configurations can be used under the components.discovery section:

- port : Defines the port which discovery should be started on. This is equivalent to the DISCOVERY\_PORT variable in instance.env.
- debug : Defines whether to enable debug mode for gateway. This is equivalent to the APIML\_DEBUG\_MODE\_ENABLED variable in instance.env but with better granular level.
- apiml.service.preferIpAddress: Set this parameter to true to advertise a service IP address instead of its hostname. Note: This configuration is deprecated. The Zowe start script will ignore this value and always set it to false. This is equivalent to the APIML\_PREFER\_IP\_ADDRESS variable in instance.env.
- apiml.security.ssl.verifySslCertificatesOfServices : Defines whether APIML should verify certificates of services in strict mode. Setting to true will enable the strict mode where APIML will validate both if the certificate is trusted in turststore, and also if the certificate Common Name or Subject Alternate Name (SAN) matches the service hostname. This is equivalent to the VERIFY\_CERTIFICATES variable defined in <keystore-dir>/zowe-certificates.env.
- apiml.security.ssl.nonStrictVerifySslCertificatesOfServices: Defines whether APIML should verify certificates of services in non-strict mode. Setting to true will enable the nonstrict mode where APIML will validate if the certificate is trusted in turststore, but ignore the certificate Common Name or Subject Alternate Name (SAN) check. Zowe will ignore this configuration if strict mode is enabled with apiml.security.ssl.verifySslCertificatesOfServices. This is equivalent to the NONSTRICT\_VERIFY\_CERTIFICATES variable defined in <keystoredir>/zowe-certificates.env.
- alternativeStaticApiDefinitionsDirectories: Specifies the alternative directories of static definitions. This is equivalent to the APIML\_MAX\_CONNECTIONS\_PER\_ROUTE variable in instance.env.
- apiml.server.maxTotalConnections: Specifies the total connections for all services registered under API Mediation Layer. This is equivalent to the ZWEAD\_EXTERNAL\_STATIC\_DEF\_DIRECTORIES variable in instance.env.

#### Configure component api-catalog

These configurations can be used under the components.api-catalog section:

• port : Defines the port which API Catalog should be started on. This is equivalent to the CATALOG\_PORT variable in instance.env.

- debug : Defines if we want to enable debug mode for gateway. This is equivalent to the APIML\_DEBUG\_MODE\_ENABLED variable but with better granular level.
- environment.preferIpAddress : Set this parameter to true to advertise a service IP address instead of its hostname. Note: This configuration is deprecated. Zowe start script will ignore this value and always set it to false. This is equivalent to the APIML\_PREFER\_IP\_ADDRESS variable in instance.env.

#### **Configure component caching-service**

These configurations can be used under the components.caching-service section:

- port : Defines the port which Caching Service should be started on. This is equivalent to the ZWE\_CACHING\_SERVICE\_PORT variable in instance.env.
- debug : Defines if we want to enable debug mode for gateway. This is equivalent to the APIML\_DEBUG\_MODE\_ENABLED variable in instance.env but with better granular level.
- **storage.mode**: Sets the storage type used to persist data in the Caching Service. This is equivalent to the ZWE\_CACHING\_SERVICE\_PERSISTENT variable in instance.env.
- storage.size: Specifies amount of records before eviction strategies start evicting. This is
  equivalent to the ZWE\_CACHING\_STORAGE\_SIZE variable in instance.env.
- storage.evictionStrategy: Specifies eviction strategy to be used when the storage size is achieved. This is equivalent to the ZWE\_CACHING\_EVICTION\_STRATEGY variable in instance.env.
- storage.vsam.name: Specifies the data set name of the caching service VSAM data set. This is
  equivalent to the ZWE\_CACHING\_SERVICE\_VSAM\_DATASET variable in instance.env.
- storage.redis.masterNodeUri: Specifies the URI used to connect to the Redis master instance in the form username:password@host:port. This is equivalent to the CACHING\_STORAGE\_REDIS\_MASTERNODEURI variable in instance.env.
- storage.redis.timeout: Specifies the timeout second to Redis. Defaults to 60 seconds. This is
  equivalent to the CACHING\_STORAGE\_REDIS\_TIMEOUT variable in instance.env.
- storage.redis.sentinel.masterInstance: Specifies the Redis master instance ID used by the Redis Sentinel instances. This is equivalent to the
   CACHING\_STORAGE\_REDIS\_SENTINEL\_MASTERINSTANCE variable in instance.env.
- storage.redis.sentinel.nodes: Specifies the array of URIs used to connect to a Redis Sentinel instances in the form username:password@host:port. This is equivalent to the CACHING\_STORAGE\_REDIS\_SENTINEL\_NODES variable in instance.env.

- storage.redis.ssl.enabled: Specifies the boolean flag indicating if Redis is being used with SSL/TLS support. Defaults to true. This is equivalent to the
   CACHING\_STORAGE\_REDIS\_SSL\_ENABLED variable in instance.env.
- storage.redis.ssl.keystore: Specifies the keystore file used to store the private key. This is
  equivalent to the CACHING\_STORAGE\_REDIS\_SSL\_KEYSTORE variable in instance.env.
- storage.redis.ssl.keystorePassword: Specifies the password used to unlock the keystore. This is equivalent to the CACHING\_STORAGE\_REDIS\_SSL\_KEYSTOREPASSWORD variable in instance.env.
- **storage.redis.ssl.truststore**: Specifies the truststore file used to keep other parties public keys and certificates. This is equivalent to the CACHING\_STORAGE\_REDIS\_SSL\_TRUSTSTORE variable in instance.env.
- storage.redis.ssl.truststorePassword: Specifies the password used to unlock the truststore. This is equivalent to the CACHING\_STORAGE\_REDIS\_SSL\_TRUSTSTOREPASSWORD variable in instance.env.
- environment.preferIpAddress: Set this parameter to true to advertise a service IP address instead of its hostname. Note: this configuration is deprecated. Zowe start script will ignore this value and always set it to false. This is equivalent to the APIML\_PREFER\_IP\_ADDRESS variable in instance.env.
- apiml.security.ssl.verifySslCertificatesOfServices: Specifies whether APIML should verify certificates of services in strict mode. Set to true will enable strict mode that APIML will validate both if the certificate is trusted in turststore, and also if the certificate Common Name or Subject Alternate Name (SAN) match the service hostname. This is equivalent to the VERIFY\_CERTIFICATES variable defined in <keystore-dir>/zowe-certificates.env.
- apiml.security.ssl.nonStrictVerifySslCertificatesOfServices: Defines whether APIML should verify certificates of services in non-strict mode. Setting to true will enable nonstrict mode where APIML will validate if the certificate is trusted in turststore, but ignore the certificate Common Name or Subject Alternate Name (SAN) check. Zowe will ignore this configuration if strict mode is enabled with apiml.security.ssl.verifySslCertificatesOfServices. This is equivalent to the NONSTRICT\_VERIFY\_CERTIFICATES variable defined in <keystoredir>/zowe-certificates.env.

#### Configure component app-server

These configurations can be used under the components.app-server section:

• port : Defines the port which App Server should be started on. This is equivalent to the ZOWE\_ZLUX\_SERVER\_HTTPS\_PORT variable in instance.env.

#### **Configure component zss**

These configurations can be used under the components.zss section:

- port : Defines the port which ZSS should be started on. This is equivalent to the ZOWE\_ZSS\_SERVER\_PORT variable in instance.env.
- crossMemoryServerName: Defines the procedure name of cross memory server. This is equivalent to the ZOWE\_ZSS\_XMEM\_SERVER\_NAME variable in instance.env.
- tls: Defines whether ZSS service has enabled TLS. This is equivalent to the ZOWE\_ZSS\_SERVER\_TLS variable in instance.env.

#### Configure component jobs-api

These configurations can be used under the components.jobs-api section:

• port : Defines the port which Jobs API should be started on. This is equivalent to the JOBS\_API\_PORT variable in instance.env.

#### Configure component files-api

These configurations can be used under the components.files-api section:

• port : Defines the port which Files API should be started on. This is equivalent to the FILES\_API\_PORT variable in instance.env.

#### **Configure component explorer-jes**

These configurations can be used under the components.explorer-jes section:

- port : Defines the port which JES UI Explorer should be started on. This is equivalent to the JES\_EXPLORER\_UI\_PORT variable in instance.env.
- frameAncestors : Defines the frame ancestors supported by UI Explorer. This is equivalent to the ZOWE\_EXPLORER\_FRAME\_ANCESTORS variable in instance.env but in better granular level.

#### Configure component explorer-mvs

These configurations can be used under the components.explorer-mvs section:

- port : Defines the port which MVS UI Explorer should be started on. This is equivalent to the MVS\_EXPLORER\_UI\_PORT variable in instance.env.
- frameAncestors : Defines the frame ancestors supported by UI Explorer. This is equivalent to the ZOWE\_EXPLORER\_FRAME\_ANCESTORS variable in instance.env but in better granular level.

#### **Configure component explorer-uss**

These configurations can be used under the components.explorer-uss section:

- port : Defines the port which USS UI Explorer should be started on. This is equivalent to the USS\_EXPLORER\_UI\_PORT variable in instance.env.
- frameAncestors : Defines the frame ancestors supported by UI Explorer. This is equivalent to the ZOWE\_EXPLORER\_FRAME\_ANCESTORS variable in instance.env but in better granular level.

#### Configure external extension

You can define a **components.**<extension-id> section and use common component configuration entries.

For example, enable my-extension:

#### YAML configurations - halnstances

All Zowe high availability instances should have a dedicated section under the haInstances high-level configuration.

In this section, <ha-instance> represents any Zowe high availability instance ID.

For all high availability instances, these are the common definitions.

- haInstances.<ha-instance>.hostname: Defines the host name where you want to start this instance. This could be the host name of one LPAR in your Sysplex.
- haInstances.
   haInstances.
   ip: Defines the IP address where you want to start this instance.
   This could be the IP address of one LPAR in your Sysplex.
- haInstances.<ha-instance>.components.<component>: Optional settings you can override component configurations for this high availability instance. See Configuration override for more details.

## Hints and tips

Learn about some hints and tips that you might find useful when you create and configure the Zowe instance.

When you are configuring Zowe on z/OS, you need to create certificates, and then create the Zowe instance.

The creation of a Zowe instance is controlled by the **instance.env** file in your instance directory **INSTANCE\_DIR**.

1. Keystore

Edit the instance.env file to set the keystore directory to the one you created when you ran zowesetup-certificates.sh.

The keyword and value in instance.env should be the same as in zowe-setupcertificates.env, as shown below

2. Hostname and IP address

The zowe-configure-instance.sh script handles the IP address and hostname the same way zowe-setup-certificates.sh does.

In instance.env, you specify the IP address and hostname using the following keywords:

The ZOWE\_EXPLORER\_HOST value must resolve to the external IP address, otherwise you should use the external IP address as the value for ZOWE\_EXPLORER\_HOST.

The zowe-configure-instance.sh script will attempt to discover the IP address and hostname of your system if you leave these unset.

When the script cannot determine the hostname or the IP address, it will ask you to enter the IP address manually during the dialog. If you have not specified a value for ZOWE\_EXPLORER\_HOST, then the script will use the IP address as the hostname.

The values of ZOWE\_EXPLORER\_HOST and ZOWE\_IP\_ADDRESS that the script discovered are appended to the instance.env file unless they were already set in that file or as shell environment variables before you ran the script.

# Installing and starting the Zowe started task (ZWESVSTC)

Zowe has a number of runtimes on z/OS: the z/OS Service microservice server, the Zowe Application Server, and the Zowe API Mediation Layer microservices. A single PROCLIB member ZWESVSTC is used to start all of these microservices. This member is installed by Zowe into the SAMPLIB data set SZWESAMP during the installation either a convenience build or SMP/E.

This topic describes how to configure the z/OS runtime in order to launch Zowe. You can do these manually (as described in this topic) or use script to install and configure the Zowe main server. see Installing and Configuring Zowe z/OS components using scripts.

## Step 1: Copy the PROCLIB member ZWESVSTC

When the Zowe runtime is launched, it is run under a z/OS started task with the PROCLIB member named ZWESVSTC. A sample PROCLIB is created during installation into the PDS SZWESAMP(ZWESVSTC). To launch Zowe as a started task, you must copy this member to a PDS that is in the PROCLIB concatenation path.

## Step 2: Configure ZWESVSTC to run under the correct user ID

The ZWESVSTC should be configured as a started task under the ZWESVUSR user ID with the administrator user ID of ZWEADMIN. If you do not have these IDs already created, the commands to create the user ID and group are supplied in the PDS member ZWESECUR. See Configuring the z/OS system for Zowe. To associate the ZWESVSTC started task with the user ID and group, see Configuring a z/OS system for Zowe. This step will be done once per z/OS environment by a system programmer who has sufficient security privileges.

## Step 3: Launch the ZWESVSTC started task

You can launch the Zowe started task in two ways. To see whether the started task has successfully launched see Troubleshooting installation and startup of Zowe z/OS components

#### **Option 1: Starting Zowe from a USS shell**

To launch the ZWESVSTC started task, run the zowe-start.sh script from a USS shell. This reads the configuration values from the instance.env file in the Zowe instance directory.

where,

<*ZOWE\_INSTANCE\_DIR*> is the directory where you set the instance directory to. This script starts **ZWESVSTC** for you so you do not have to log on to TSO and use SDSF.

#### **Option 2: Starting Zowe with the z/OS START command**

You can use SDSF to start Zowe.

If you issue z/OS command S ZWESVSTC, the JCL will need to know the instance directory containing the launch and configuration information. To do this add the INSTANCE parameter on the START command when you start Zowe in SDSF:

The **\$ZOWE\_INSTANCE\_DIR** argument is the fully qualified path to the USS directory containing the **instance.env** file containing the Zowe configuration.

The JOBNAME='ZWEXSV' argument is optional and the started task will operate correctly without it, however having it specified ensures that the address spaces will be prefixed with ZWEXSV which makes them easier to find in SDSF or locate in RMF records.

If you have a default instance directory you want you always start Zowe with, you can tailor the JCL member ZWESVSTC at this line

to replace the **instance\_directory** with the location of the Zowe instance directory that contains the configurable Zowe instance directory.

## Start API Mediation Layer as a standalone component

As a Zowe user, follow the procedure in this article to start the API Mediation Layer independently of other Zowe components. By default, the Gateway, Zowe System Services, and Virtual Desktop start when Zowe runs. To limit consumed resources when the Virtual Desktop or Zowe System Services are not required, it is possible to specify which components start in the context of Zowe. No change is required during the installation process to support this setup.

Once Zowe is installed, use the following procedure to limit which components start.

#### Follow these steps:

- 1. Open the file <Zowe instance directory>/instance.env.
- 2. Add the property ZWE\_LAUNCH\_COMPONENTS at the end of the instance.env file and set discovery, gateway, api-catalog
- 3. Restart Zowe&trade.

To learn more about the related section of the environment file, see Creating and configuring the Zowe instance directory. We recommend you open this page in a new tab.

## **Zowe Auxiliary Address space**

The cross memory server runs as a started task ZWESISTC that uses the load module ZWESIS01.

In some use cases, the Zowe cross memory server has to spawn child address spaces, which are known as auxiliary (AUX) address spaces. The auxiliary address spaces run as the started task ZWESASTC using the load module ZWESAUX and are started, controlled, and stopped by the cross memory server.

An example of when an auxiliary address space is used is for a system service that requires supervisor state but cannot run in cross-memory mode. The service can be run in an AUX address space which is invoked by the Cross Memory Server acting as a proxy for unauthorized users of the service.

Do not install the Zowe auxiliary address space unless a Zowe extension product's installation guide explicitly asks for it to be done. This will occur if the extension product requires services of Zowe that cannot be performed by the cross memory server and an auxiliary address space needs to be started.

A default installation of Zowe does not require auxiliary address spaces to be configured.

You do not start or stop the ZWESASTC manually.

# **Configure Zowe with z/OSMF Workflows**

As a system programmer, after you install Zowe, you can register and execute the z/OSMF workflows in the web interface to complete the Zowe configuration. z/OSMF helps to simplify the Zowe configuration tasks and reduce the level of expertise that is needed for Zowe configuration.

Ensure that you meet the following requirements before you start the Zowe configuration:

- Installed and configured z/OSMF
- Installed Zowe with either SMP/E build or convenience build

You can complete the following tasks with the z/OSMF workflows:

- Configure z/OS Security Manager to prepare for launching the Zowe started tasks
- Configure Zowe certificates
- Configure Zowe Cross Memory Server
- Create and configure the Zowe instance directory and start the Zowe started task

## **Configure z/OS Security Manager**

Configure the z/OS security manager to prepare for launching the Zowe started tasks. The workflow definition file is provided to assist with the security configuration. The workflow definition file allows you to configure z/OS security manager by using one of RACF, ACF2, or TSS security systems.

Register the **ZWESECUR.xml** workflow definition file in the z/OSMF web interface to configure z/OS security manager. The path to the workflow definition file is cpathPrefix>/workflows/.

Perform the following steps after you register the workflow definition file:

#### 1. Define Values for Variables

Review all the parameters and customize the values for variables to meet the z/OS security requirements. We recommend that the security administrator at your site reviews and edits the values for security group variables.

Zowe package includes the variable input file that is **ZWESECUR.properties**. Optionally, you can use this file to customize the values for variables in advance. Upload the prepared properties file while your

register the workflow definition. Values from this file override the default values for the workflow variables.

#### 2. Execute JCL

Execute the step to complete the z/OS security manager configuration.

After you execute these steps, the groups, user IDs and started tasks are assigned based on the customized values. For instructions on how to register and execute the workflow, see Register and execute workflow in the z/OSMF Web Interface.

## **Configure Zowe certificates**

z/OSMF workflow lets you generate certificate signed by the Zowe API Mediation Layer and keystores in the specified location. Zowe uses the keystore directory to hold the certificate to encrypt communication between Zowe clients and the Zowe z/OS servers. The keystore directory also holds the truststore that is used to hold public keys of any servers that Zowe trusts.

Register the ZWEWRF05 member that is located <pathPrefix>/workflows/ZWEWRF05.xml data set in the z/OSMF web interface. After you register the workflow definition file, you can execute the following steps.

#### 1. Define Variables

Review all the parameters and customize the values for variables to meet the z/OS security requirements.

#### 2. Generate new custom zowe-setup-certificates.env file

Execute the step to generate a new custom zowe-setup-certificates.env file based on the custom values that you provide for variables in the first step.

#### 3. Execute zowe-setup-certificates.sh

Execute the step to run the shell script to generate the custom certificates based on the defined values for variables and values for parameters in the provided environment file.

After you execute these steps, the keystore and certificates are successfully generated based on the custom values. For general instruction on how to register and execute the workflow, see Register and execute workflow in the z/OSMF Web Interface.

## **Configure Zowe Cross Memory Server**

The Zowe cross memory server provides privileged cross-memory services to the Zowe Desktop and runs as an APF-authorized program. Multiple Zowe desktop instances can use the same cross memory server. Use the z/OSMF workflow to install, configure, and launch the cross memory server if you want to use the Zowe desktop. The z/OSMF workflow also lets you create APF-authorized load libraries that are required to install and configure the cross memory server.

Register the ZWEWRF06.xml workflow definition file that is located in <pathPrefix>/workflows/. After you complete the workflow registration, Perform the following steps to configure the Zowe cross memory server:

#### 1. Define values for Variables

The workflow includes the list of Zowe cross memory server configuration and the started task variables. Enter the custom values for variables based on your mainframe environment and Zowe cross memory server configuration requirements.

Zowe package includes ZWEWRF06.properties variable input file and the path is <pathPrefix>/workflows/ZWEWRF05.properties. Optionally you can use this file to customize the values for variables in advance. Upload the prepared properties file when your register the workflow definition file. Values from this file override the default values for the workflow variables.

#### 2. Allocate Cross Memory Server Data Sets

Execute the step to allocate Target DSN for PARMLIB, Target DSN for PROCLIB, and log directory data sets that are required for XMEM configuration.

#### 3. Copy artifacts

Execute the step to populate the data sets that are allocated in the previous step with the necessary artifacts such as load modules, parmlib members and others. This step also copies the cross memory

server STC to the proclib.

#### 4. Add PPT entries to the system PARMLIB

The cross memory server and its auxiliary address spaces must run in key 4 and be non-swappable. For the server to start in this environment, add the following PPT entries for the server and address spaces to the SCHEDxx member of the system PARMLIB. PPT PGMNAME(ZWESIS01) KEY(4) NOSWAP

The PDS member SZWESAMP contains the PPT lines for reference. Issue the following command to make the SCHEDxx changes effective. /SET\_SCH=xx

For more information, see Key 4 non-swappable.

#### 5. Retrieve the LOADLIB volume

This step allows you to automatically retrieve the VOLUME for non-SMS LOADLIB. Run this step to retrieve the actual VOLUME of the LOADLIB.

#### 6. APF Authorize Load Library

Creates APF-authorized load library that is required to install and configure the cross memory server. Execute the step to APF authorize the XMEM LOADLIB.

#### 7. Start the XMEM Server

Execute this step to start the Cross Memory Server started task.

After you complete these steps, the Zowe cross memory server is configured and installed to start the Zowe Desktop instance. For instruction on how to register and execute the workflow, See, Register and execute workflow in the z/OSMF Web Interface.

# **Create and configure the Zowe instance directory and start the Zowe started task**

The Zowe instance directory contains configuration data that is required to launch a Zowe runtime. This includes port numbers, location of dependent runtimes such as Java, Node, z/OSMF, as well as log files. When Zowe is started, configuration data is read from files in the instance directory and logs will be written to files in the instance directory. Zowe has three runtimes namely: the z/OS Service microservice server, the Zowe Application Server, and the Zowe API Mediation Layer microservices.

After you register the workflow definition file, perform the following steps to complete the process:

#### 1. Define Variables

The workflow includes the list of instance configuration and the Zowe started task variables. Enter the values for variables based on your mainframe environment, Zowe instance configuration, and started task requirements.

#### 2. Create a Zowe instance

Execute the step to create a Zowe instance directory. This step creates instances for all the micro services. That is z/OS Service microservice server, the Zowe Application Server, and the Zowe API Mediation Layer microservices.

#### 3. Change the instance configuration

Execute the step to configure the Zowe instance. The configuration of the Zowe instance depends on the values for variables that you defined in the first step.

**Note:** If you are planning to use Docker, be sure to select only to start LAUNCH\_COMPONENT\_GROUP=ZSS, otherwise more components of Zowe than necessary will be run on z/OS, such as API Mediation Layer and the App Framework. You can skip configuration for those components here, as they will run in Docker.\*\*

#### 4. Copy the STC to the procedure library

Skip this step if the procedure library is empty.

#### 5. Start the Zowe instance

Execute the step to start the instance.

After you execute each step, the step is marked as Complete. After completing the workflow execution, you can view the Zowe started task.

# Register and execute workflow in the z/OSMF web interface

z/OSMF workflow simplifies the procedure to configure and start Zowe. Perform the following steps to register and execute the workflow in the z/OSMF web interface:

- 1. Log in to the z/OSMF web interface and select **Use Desktop Interface**.
- 2. Select the Workflows File.
- 3. Select Create Workflow from the Actions menu.

The **Create Workflow** panel appears.

- 4. Enter the complete USS path to the workflow you want to register in the **Workflow Definition File** field.
  - If you installed Zowe with the SMP/E build, the workflow is located in the SMP/E target zFS file system that was mounted during the installation.
  - Optional) Enter the complete USS path to the edited workflow properties file in the Workflow Variable Input File field. Use this file to customize product instances and automate workflow execution, saving time and effort when deploying multiple standardized Zowe instances. Values from this file override the default values for the workflow variables.

The sample properties file is located in the same directory with the workflow definition file. Create a copy of this file, and then modify as described in the file. Set the field to the path where the new file is located. Note: if you use the convenience build, the workflows and variable input files are located in the USS runtime folder in files/workflows

The following table provides the list of Zowe Components Workflow Definition files and their corresponding variable input files.

Configuration Tasks	Workflow Definition File Name	Properties File Name	Workflow Definition File Path	١
------------------------	-------------------------------------	----------------------	-------------------------------	---

Configuration Tasks	Workflow Definition File Name	Properties File Name	Workflow Definition File Path
Configure z/OS Security Manager	ZWESECUR.xml	ZWESECUR.properties	<pathprefix>/workflows/ /ZWESECUR.xml</pathprefix>
Configure Zowe Certificates	ZWEWRF05.xml	ZWEWRF05.properties	<pathprefix>/workflows/ /ZWEWRF05.xml</pathprefix>
Configure Cross Memory Server	ZWEWRF06.xml	ZWEWRF06.properties	<pathprefix>/workflows/ /ZWEWRF06.xml</pathprefix>
Create Instance Directory and Start the Zowe started Task	ZWEWRF03.xml	ZWEWRF03.properties	<pathprefix>/workflows/ /ZWEWRF03.xml</pathprefix>

5. Select the System where the workflow runs.

#### 6. Select Next.

- 7. Specify a unique Workflow name.
- 8. Select or enter an Owner user ID, and select Assign all steps to owner user ID.
- 9. Select Finish.

The **workflow** is registered in z/OSMF. The workflow is available for execution to deploy and configure the Zowe instance.

- 10. Execute the steps in order. Perform the following steps to execute each step individually:
  - a. Double-click the title of the step.

b. Select the **Perform** tab.

c. Review the step contents and update the input values as required.

d. Select Next.

Repeat the previous two steps to complete all items until the option Finish is available.

#### 11. Select Finish.

After you execute each step, the step is marked as Complete. The workflow is executed.

## Zowe high availability installation roadmap

To install Zowe on a Sysplex, there are two parts:

- 1. The Zowe runtime, which consists of the following components. An advanced launcher is used to perform the initialization and shutdown of these components.
  - Zowe Application Framework
  - z/OS Explorer Services
  - Zowe API Mediation Layer
  - ZSS
- 2. The Zowe Cross Memory Server, which is an authorized server application that provides privileged services to Zowe in a secure manner.

Review the installation diagram and the high-level instructions in this topic to see the general installation sequence and the most important tasks that are to be performed during installation and configuration of Zowe high availability. You can click each step on the diagram for detailed instructions.

## **Stage 1: Plan and prepare**

Before you start the installation, review the information on hardware and software requirements and other considerations. See Planning the installation for details.

## **Stage 2: Install the Zowe runtime**

- 1. Ensure that the software requirements are met. The prerequisites are described in Zowe high availability requirements (host).
- 2. Choose the method of installing Zowe high availability instances on a Sysplex.

The Zowe z/OS binaries are distributed in the following formats. They contain the same contents but you install them by using different methods. You can choose which method to use depending on your needs.

#### • Convenience build

The Zowe z/OS binaries are packaged as a PAX file. You install this build by running shell script within a UNIX System Services (USS) shell. Convenience builds are full product installs.

#### • SMP/E build

The Zowe z/OS binaries are packaged as the following files that you can download. You install this build through SMP/E.

- A pax.Z file, which contains an archive (compressed copy) of the FMIDs to be installed.
- A readme file, which contains a sample job to decompress the pax.Z file, transform it into a format that SMP/E can process, and invoke SMP/E to extract and expand the compressed SMP/E input data sets.

While the procedure to obtain and install the convenience build or SMP/E build are different, the procedure to configure a Zowe runtime are the same irrespective of how the build is obtained and installed.

- 3. Obtain and install the Zowe build.
  - For how to obtain the convenience build and install it, see Installing Zowe runtime from a convenience build.
  - For how to obtain the SMP/E build and install it, see Installing Zowe SMP/E.

**Note:** To allow all LPARs in a Sysplex to access the installation and configuration of Zowe high availability instances, you must install and configure Zowe in a shared file system (zFS directory).

After successful installation of either a convenience build or an SMP/E build, there will be a shared zFS directory that contains the unconfigured Zowe runtime <RUNTIME\_DIR>, a SAMPLIB library SZWESAMP that contains sample members, and a load library SZWEAUTH that contains load modules.

## Stage 3: Configure the Zowe high availability runtime

You can configure the Zowe high availability runtime by using JCL and shell scripts.

Tip: It's recommended that you open the links in the following configuration procedure in new tabs.

1. Configure the z/OS security manager to prepare for launching the Zowe started tasks. For instructions, see Configuring the z/OS system for Zowe.

A SAMPLIB JCL member ZWESECUR is provided to assist with the configuration. You can submit the ZWESECUR JCL member as-is or customize it depending on site preferences.

If you already have this security step configured from a previous release of Version 1.8 or later, you only need to define Zowe launcher started task security configuration with the following commands.

- If you use RACF, issue the following commands:
- If you use ACF2, issue the following commands:
- If you use Top Secret, issue the following commands:

Where,

- ZLNCHSTC is the Zowe launcher task name. Default should be ZWESLSTC.
- STCGRP is the group for Zowe started tasks. Default should be ZWEADMIN.
- ZOWEUSER is the user ID for the Zowe started task. Default should be ZWESVUSR.
- 2. Create a VSAM data set which is used by the Caching Service feature of API Mediation Layer. For instructions, see Configuring Caching Service for HA.

A SAMPLIB JCL member ZWECSVSM is provided to assist with the creation of this VSAM data set. You need to customize the ZWECSVSM JCL member depending on your site preferences and then submit the JCL.

3. Configure the Zowe TLS. For instructions, see Configuring Zowe certificates.

The Zowe keystore directory must be created in a shared file system (zFS directory), so that it can be shared between all Zowe high availability instances running in a Sysplex.

The Zowe keystore directory contains the key used by the Zowe desktop and the Zowe API mediation layer to secure its TLS communication with clients (such as web browsers or REST AI clients). The keystore directory also has a truststore where public keys of any servers that Zowe communicates to (such as z/OSMF) are held.

- 4. Configure and start the ZWESISTC cross memory server and install the load libraries. For instructions, see Installing and configuring the Zowe cross memory server (ZWESISTC).
- 5. Create and customize an instance directory that contains the configuration data required to launch a Zowe runtime and is where log files and Zowe yaml configuration are stored. For instructions, see

Creating and configuring the Zowe instance directory.

One instance directory must be created on a shared file system (zFS directory). A single Zowe runtime can be launched multiple times from a shared instance directory.

6. Create and customize the <INSTANCE\_DIR>/zowe.yaml configuration file. To learn more about how to create zowe.yaml, see the Creation of zowe.yaml file section.

#### Notes:

- To learn more about zowe.yaml, see the Updating the zowe.yaml configuration file section.
- For more information about Gateway and Discovery Service parameters that can be set during the Zowe runtime configuration, see API Gateway runtime configuration parameters and Discovery Service runtime configuration parameters.
- 7. Configure and start the ZWESLSTC started task. For instructions, see Installing and starting the Zowe high availability started task (ZWESLSTC).

Zowe in high availability mode has two high-level started tasks: ZWESLSTC that launches the Zowe high availability instances, and ZWESISTC that is a cross memory server that runs all of the APF-authorized code. The JCLs for the tasks are included in the PDS SAMPLIB SZWESAMP installed by Zowe and the load modules for the cross memory server are included in the PDS load library SZWEAUTH.

## **Stage 4: Verify the installation**

Verify that Zowe is installed correctly on z/OS. See Verifying Zowe installation on z/OS.

## Looking for troubleshooting help?

If you encounter unexpected behavior when installing or verifying the Zowe runtime on z/OS, see the Troubleshooting section for tips.

# **Configuring Sysplex for high availability**

To deploy Zowe high availability, you must set up the Parallel Sysplex® environment. A Parallel Sysplex is a collection of z/OS® systems that cooperatively use certain hardware and software components to achieve a high-availability workload processing environment.

## Sysplex environment requirements

Zowe high availability instances require a Sysplex environment that consists of the following:

- One or more central processor complexes (CPCs) that can attach to a coupling facility
- At least one coupling facility
- At least one Sysplex timer
- Connection to shared DASD
- Shared SAF database, see Sharing a database with sysplex communication in data sharing mode
- Sysplex Distributor with configured Dynamic VIPA TCP/IP address, see Configuring Sysplex Distributor for instructions
- VSAM record-level sharing (RLS), see Preparing for VSAM record-level sharing
- USS Shared file system, see How to share file systems in a Sysplex
- JESPlex/JES2 Multi-Access Spool (MAS) environment
- z/OSMF high availability, see Configuring z/OSMF high availability in Sysplex
- Node.js v8.x (except v8.16.1), v12.x, or v14

Note: It is highly recommended that Node.js installed on a shared file system.

## **Configuring Sysplex Distributor**

The following example DVIPA configuration ensures the availability of Zowe in Hot-Standby mode. For example, suppose that you have a Sysplex of two z/OS systems: A, B.

1. Enable dynamic XCF on each host by adding the following TCP/IP definitions:

- IPCONFIG SYSPLEXROUTING DYNAMICXCF x.x.x.A 255.255.255.0 1 for SYSA
- IPCONFIG SYSPLEXROUTING DYNAMICXCF x.x.x.B 255.255.255.0 1 for SYSB

2. Define a DVIPA for both systems:

where,

- x.x.x.A is the home address for SYSA.
- x.x.x.B is the home address for SYSB.
- x.x.x.V is Dynamic VIP Address.
- 7554 is the port number of you Zowe API Mediation Layer Gateway. This should be the same port number you configured for zowe.externalPort in zowe.yaml. See Updating the zowe.yaml configuration file to learn more about zowe.yaml.

The **VIPADISTRIBUTE** statement with **PREFERRED** and **BACKUP** settings is used to enable automatic dynamic VIPA takeover to occur, if needed.

All Zowe instances are bound to the DVIPA x.x.x.V. With both z/OS systems active in the Sysplex, the preferred Zowe instance, SYSA receives all new incoming requests. If SYSA fails, new work requests to Zowe are routed to the server on SYSB. When SYSA resumes normal operations, new work requests for Zowe are routed to SYSA again. This is the default behavior because the AUTOSWITCHBACK parameter of the VIPADISTRIBUTE statement is in effect by default.

If you do not want the distributor to switch back to the preferred target when it becomes available, you can specify the NOAUTOSWITCHBACK parameter for the VIPADISTRIBUTE statement.

Version: v1.25.x LTS

# Configuring z/OSMF for high availability in Sysplex

z/OSMF high availability (HA) should be configured in Hot Standby mode to ensure availability of REST services. The goal of this configuration is to ensure that one z/OSMF server is always available to provide the REST services.

In Hot Standby mode, there is at least one backup (hot-standby) server and a preferred target server. Both targets are active, and both z/OSMF servers are bound to the DVIPA. The preferred z/OSMF server receives all new incoming requests. When the preferred z/OSMF server fails or the system becomes down, new requests are routed to the backup (hot-standby) server. The distributing DVIPA does not perform load balancing of requests across multiple systems. For more information, read the following articles in IBM Documentation:

- Configuring z/OSMF for availability
- Configuring z/OSMF for high availability

## Sysplex environment requirements

Before you begin, ensure that the Sysplex environment meets the following requirements for z/OSMF REST services:

- Shared SAF database. See Sharing a database with sysplex communication in data sharing mode in IBM Documentation.
- USS Shared file system. See How to share file systems in a Sysplex in IBM Documentation.
- JESPlex/JES2 Multi-Access Spool (MAS) environment
- Sysplex distributor, configured Dynamic VIPA TCP/IP address
- Extended MCS console (EMCS)

## Setting up z/OSMF nucleus

**This information is intended for a first-time z/OSMF setup.** Follow these high-level steps to create a z/OSMF nucleus on your system.

For detailed information about each step, see Create a z/OSMF nucleus on your system in IBM Documentation.

- 1. Create the z/OSMF security authorizations by running the sample JCL **SYS1.SAMPLIB(IZUSEC)**. z/OSMF security authorizations will be used by all z/OSMF servers across multiple systems.
- 2. Create a shared file system per z/OSMF server by running the sample JCL **SYS1.SAMPLIB(IZUMKFS)**. It holds configuration settings and the persistence data.
- Copy the Sample Parmlib Member SYS1.SAMPLIB(IZUPRM00) to PARMLIB and modify it according to requirements of z/OSMF HA parmlib member in Sysplex. Each system uses a different IZUPRMxx member. For example, IZUPRM0A and IZUPRM0B.
- 4. Copy the following z/OSMF procedures from **SYS1.PROCLIB** into your JES concatenation:
  - IZUSVR1 (Each z/OSMF server should use the different started procedure. For example, IZUSVRA and IZUSVRB.)
  - IZUANG1
  - IZUFPROC
- 5. Define different STARTED profiles for z/OSMF servers.

## **Requirements of z/OSMF HA parmlib member in Sysplex**

• *AUTOSTART\_GROUP*, more than one z/OSMF server (independent z/OSMF instances) is to be autostarted in a Sysplex. For instance, System A will autostart a server and similarly, System B will autostart the second z/OSMF server.

z/OSMF has a default autostart group (IZUDFLT) which is used in monoplex or single z/OS image. To have more z/OSMF servers autostarted in a Sysplex, you must associate each server and the systems it serves with a unique autostart group name. For example, AUTOSTART\_GROUP('IZUDFLA') for System A and AUTOSTART\_GROUP('IZUDFLB') for System B

- *AUTOSTART(LOCAL)* should be used by all z/OSMF instances.
- HOSTNAME, the DVIPA address will be used as the z/OSMF host name for all instances.
- *HTTP\_SSL\_PORT*, all servers are listening on the same port.
- KEYRING\_NAME, all servers should use the same key ring such as IZUKeyring.IZUDFLT.

- SERVER\_PROC, each z/OSMF server should use the different started procedure. For example, IZUSVRA and IZUSVRB.
- ANGEL\_PROC, all z/OSMF servers can connect to the same z/OSMF angel process such as IZUANG1.
- *SAF\_PREFIX*, they should use the same SAF profile prefix such as IZUDFLT.
- USER\_DIR, each instance uses a shared file system with a unique mount point for each AUTOSTART group that be automatically started. For example, /global/zosmf/zosmfa and /global/zosmf/zosmfb.

## **Configuring z/OSMF for high availability**

The following DVIPA configuration ensures the availability of z/OSMF for Hot-Standby. For example, suppose that you have a Sysplex of two z/OS systems: A, B.

- 1. Enable dynamic XCF on each host by adding the following TCP/IP definitions:
  - IPCONFIG SYSPLEXROUTING DYNAMICXCF x.x.x.A 255.255.255.0 1 for SYSA
  - IPCONFIG SYSPLEXROUTING DYNAMICXCF x.x.x.B 255.255.255.0 1 for SYSB

2. Define a dynamic VIPA (DVIPA) for both systems:

where,

- x.x.x.A is the home address for SYSA.
- x.x.x.B is the home address for SYSB.
- x.x.x.V is Dynamic VIP Address.

The **VIPADISTRIBUTE** statement with **PREFERRED** and **BACKUP** settings is used to enable automatic dynamic VIPA takeover to occur, if needed.

Both z/OSMF servers are bound to the DVIPA x.x.x.V. With both z/OS systems active in the Sysplex, the preferred z/OSMF server, SYSA receives all new incoming requests. If SYSA fails, new work requests for z/OSMF are routed to the server on SYSB. When SYSA resumes normal operations, new work requests for z/OSMF are routed to SYSA again. This is the default behavior because the AUTOSWITCHBACK parameter of the VIPADISTRIBUTE statement is in effect by default.

If you do not want the distributor to switch back to the preferred target when it becomes available, you can specify the NOAUTOSWITCHBACK parameter for the VIPADISTRIBUTE statement.

# **Configuring the Caching Service for HA**

Zowe uses the Caching Service to centralize the state data persistent in high availability (HA) mode. The Caching Service supports three storage methods: inMemory, VSAM and redis.

• inMemory

This storage method is designed for quick start of the service and should be used only for single instance scenario and development or test purpose. Do not use it in production or high availability scenario.

To use this method, leave the ZWE\_CACHING\_SERVICE\_PERSISTENT configuration blank in the instance.env configuration file. When this method is enabled, the Caching Service will not persist any data. Also, if you have multiple instances of Caching Service, the data will not be shared across these instances.

### • VSAM

**Note:** Performance issues related to the VSAM data set have been observed, so it is recommended that you use this storage method for light workload. If heavy workload is expected on Zowe components, it is recommended that you use the **redis** storage method instead.

To use this method,

- i. Set the value of ZWE\_CACHING\_SERVICE\_PERSISTENT to VSAM in the instance.env configuration file.
- ii. Create a VSAM data set. See Creating a VSAM data set for instructions.
- iii. In instance.env, configure ZWE\_CACHING\_SERVICE\_VSAM\_DATASET with the VSAM data set you created.
- redis

To enable this method, set the value of ZWE\_CACHING\_SERVICE\_PERSISTENT to redis in the instance.env configuration file. See Redis configuration for more information. To learn more about Caching Service, see Using the Caching Service.

If you are using zowe.yaml configuration other than instance.env, please check Configure component caching-service for configuration details.

## **Creating a VSAM data set**

You can use the ZWECSVSM JCL to create a VSAM data set and define required security configurations. The ZWECSVSM JCL is provided as part of the PDS sample library SZWESAMP that is delivered with Zowe.

Before you submit the ZWECSVSM JCL, you must customize it and review it with a system programmer who is familiar with z/OS VSAM data set and storage.

The following variables are available in the JCL.

• #dsname variable

This is the data set name that the ZWECSVSM JCL will create. Replace all occurrences of #dsname with the data set name that you want to specify. This data set name is the value for ZWE\_CACHING\_SERVICE\_VSAM\_DATASET in instance.env.

• MODE variable

This specifies whether you would like to use Record Level Sharing (RLS) for your VSAM data set. RLS is recommended for Sysplex deployment.

• #storclas variable

If you use the **RLS** mode, a storage class is required. Replace **#storclas** with your desired storage class name.

• #volume variable

If you set to use the **NONRLS** mode, a storage volume is required. Replace **#volume** with you desired storage volume.

#### Procedure

- 1. Customize the ZWECSVSM JCL. Edit the variables at the beginning and in the middle of the JCL.
- 2. Submit the ZWECSVSM JCL to create a VSAM data set

Version: v1.25.x LTS

# Installing and starting the Zowe high availability started task (ZWESLSTC)

Zowe has a number of runtimes on z/OS: the z/OS Service microservice server, the Zowe Application Server, and the Zowe API Mediation Layer microservices. In a high availability environment, a single PROCLIB member ZWESLSTC is used to start multiple instances of a same component. This member is installed by Zowe into the SAMPLIB data set SZWESAMP during the installation from either a convenience build or an SMP/E build.

This topic describes how to configure the z/OS runtime in order to launch Zowe for high availability instances. You can do these manually (as described in this topic) or use script to install and configure the Zowe launcher server. See Installing and Configuring Zowe z/OS components using scripts.

## Step 1: Copy the PROCLIB member ZWESLSTC

Zowe high availability instances are run under a z/OS started task with the PROCLIB member named ZWESLSTC. A sample PROCLIB member is created during installation into the PDS SZWESAMP (ZWESLSTC). To launch high availability instances as a started task, you must copy this member to a PDS that is in the PROCLIB concatenation path.

# Step 2: Configure ZWESLSTC to run under the correct user ID

ZWESLSTC should be configured as a started task under the ZWESVUSR user ID with the administrator user ID of ZWEADMIN. If you do not have these IDs already created, you can find the commands to create the user ID and group in the PDS member ZWESECUR. See Configuring the z/OS system for Zowe. To associate the ZWESLSTC started task with the user ID and group, see Configuring a z/OS system for Zowe. This step is done once per z/OS environment by a system programmer who has sufficient security privileges.

## Step 3: Launch the ZWESLSTC started task

You launch the ZWESLSTC started task with the z/OS START command.

## Before you begin

Before starting ZWESLSTC, you need to perform the following steps in PROCLIB member ZWESLSTC :

- 1. Set the parameter **INSTANCE\_DIR** to the location (fully qualified path) of the Zowe instance directory that contains the **zowe.yaml** configuration file.
- 2. Update the STEPLIB DD statement with the location of the Zowe load library (default: HLQ.PREFIX.SZWEAUTH) that contains the load module ZWELNCH.

## Procedure

You can start Zowe high availability instances by issuing the command S ZWESLSTC in SDSF. When you issue S ZWESLSTC, you must specify which high availability instance you want to launch by adding the HAINST parameter on the START command:

where, the ha-instance-id argument is the high availability instance ID that is defined in the haInstances section of the zowe.yaml configuration file. To learn more about zowe.yaml, see the Updating the zowe.yaml configuration file section.

This command enables you to start multiple instances of a same component, which eliminates single point of failure to ensure continuous operation of Zowe z/OS server components.

- If you want to have more than one Zowe high availability instance running concurrently, use the optional parameter JOBNAME with the START command to distinguish the Zowe high availability instances from each other.
- Zowe Launcher also enables you to restart a specific component of a high availability instance by using z/OS MODIFY command:

where, the ha-component-name argument is the high availability instance component that is defined in the components section of zowe.yaml configuration file. To learn more about zowe.yaml, see the Updating the zowe.yaml configuration file section.

 If you specified the JOBNAME= parameter on the START command, the instance-job-name can be used with MODIFY command to restart a specific component:

### Next steps

To check whether the ZWESLSTC started task has successfully launched, see Troubleshooting installation and startup of Zowe z/OS components for instructions.

# Verifying Zowe installation on z/OS

After the Zowe<sup>™</sup> started task ZWESVSTC is running, follow the instructions in the following sections to verify that the components are functional.

- Verifying Zowe Application Framework installation
- Verifying API Mediation installation
- Verifying z/OS Services installation

**Note:** Not all components may have been started. Which components have been started depends on your setting of the variable LAUNCH\_COMPONENT\_GROUPS in the instance.env file. If you defined the value GATEWAY, the API Mediation Layer and z/OS Services are started. If you defined the value DESKTOP, the Zowe Application Framework (also known as Zowe desktop) is started. Those using Docker may only have ZSS started. For more information, see Creating and configuring the Zowe instance directory.

## **Verifying Zowe Application Framework installation**

If the Zowe Application Framework is installed correctly, you can open the Zowe Desktop from a supported browser.

From a supported browser, open the Zowe Desktop at https://myhost:httpsPort

where,

- *myHost* is the host on which you installed the Zowe Application Server.
- *httpsPort* is the port number value ZOWE\_ZLUX\_SERVER\_HTTPS\_PORT in instance.env. For more information, see Creating and configuring the Zowe instance directory.

For example, if the Zowe Application Server runs on host *myhost* and the port number that is assigned to ZOWE\_ZLUX\_SERVER\_HTTPS\_PORT is 12345, you specify https://myhost:12345. The web desktop uses page direct to the actual initial page which is

https://myhost:12345/ZLUX/plugins/org.zowe.zlux.bootstrap/web/index.html. If the redirect fails, try the full URL.

If the desktop appears but you are unable to log on, check Cannot log into the Zowe desktop for troubleshooting tips.

## **Verifying API Mediation installation**

Use your preferred REST API client to review the value of the status variable of the API Catalog service that is routed through the API Gateway using the following URL:

where,

- *myHost* is the host on which you installed the Zowe API Mediation Layer.
- *httpsPort* is the port number value GATEWAY\_PORT in instance.env. For more information, see Creating and configuring the Zowe instance directory.

#### Example:

The following example illustrates how to use the **curl** utility to invoke API Mediation Layer endpoint and the **grep** utility to parse out the response status variable value

The response UP confirms that API Mediation Layer is installed and is running properly.

## Verifying z/OS Services installation

You can verify the installation of z/OS Services from an internet browser by entering the following casesensitive URL:

where,

gatewayPort is the port number that is assigned to GATEWAY\_PORT in the instance.env file used to launch Zowe. For more information, see Creating and configuring the Zowe instance directory.

# Stopping the Zowe server components started task

Learn how to stop the Zowe server components started tasks ZWESVSTC and ZWESLSTC.

## **Stopping the ZWESVSTC started task**

To stop the Zowe z/OS server components, the ZWESVSTC started task needs to be ended. Run the zowestop.sh script at the Unix Systems Services command prompt that is in the Zowe instance directory used to start the Zowe started task:

where ZOWE\_INSTANCE\_DIR is the directory where you set the instance directory to.

When you stop ZWESVSTC, you might get the following error message:

This error occurs when there is more than one started task named ZWESVSTC. To resolve the issue, stop the required ZWESVSTC instance by issuing the following commands:

Where ZOWE\_PREFIX and ZOWE\_INSTANCE are specified in your configuration (and default to ZWE and 1) and you can obtain the asid from the value of A=asid when you issue the following commands:

## **Stopping the ZWESLSTC started task**

z/OS STOP command is used to terminate the Zowe launcher server (ZWESLSTC) which started the Zowe high availability instance. You can use SDSF to end ZWESLSTC with the following command:

The instance-job-name specified in the JOBNAME parameter of the Zowe launcher START command can be used to terminate the relevant high availability instance. See Installing and starting the Zowe high availability started task (ZWESLSTC) for more information.

Zowe Launcher also enables you to stop a specific component of a running high availability instance by using the z/OS MODIFY command:

The ha-component-name argument is the high availability instance component that is defined in the components section of the zowe.yaml configuration file. To learn more about zowe.yaml, see the

Updating the zowe.yaml configuration file section.

The instance-job-name specified in the JOBNAME= parameter of the Zowe launcher START command can be used to terminate a specific component of a running high availability instance:

# Upgrading the z/OS system for Zowe

If you installed Zowe previously, the system is already prepared and configured to launch a Zowe instance. A Zowe configuration consists of three USS directories. See Topology of the Zowe z/OS launch process for more information.

- The runtime directory that contains the binary and executable files. See RUNTIME\_DIR for more information. This directory is read only and contains a manifest.json file that can be used to identify its release number. See Check the Zowe release number for more information. A new Zowe runtime directory is created when a new version of Zowe is installed.
- The instance directory that is used to launch the Zowe started task ZWESVSTC. See INSTANCE\_DIR for more information. The instance directory is read/write as it contains log files and the file instance.env that contains environment launch values.
- The keystore directory that contains details about certificates used by Zowe. See KEYSTORE\_DIRECTORY for more information.

Zowe installation also creates two data sets.

#### • SZWESAMP

This contains 10 members. Four of them are JCLs to configure (and unconfigure Zowe). Three are PROCLIB members. One contains PPT entries. One is a PARMLIB member and one contains console commands. See SZWESAMP data set for more information.

#### • SZWEAUTH

This is an APF-authorized PDSE load library containing the load modules ZWESIS01 for the cross memory server and ZWESAUX for the auxiliary address space. See SZWEAUTH data set for more information.

## Upgrading the instance directory

A Zowe instance directory is created using the script zowe-configure-instance.sh in the

After installing a new version of Zowe, the new runtime will either be in the same directory as the previous version, for example, /usr/lpp/zowe if SMP/E has been used, or else may be in a different directory, for example, ~/zowe/zowe-r.M.m if using a convenience build installation.

In both situations, you can keep and reuse the instance directory that is used for the previous version of Zowe to launch the new version of Zowe. To do this, run the script <code>zowe-configure-instance.sh</code> from the new <code><RUNTIME\_DIR>/bin</code> directory with the <code>-c</code> argument pointing to the location of the existing instance directory. This is the same method used to create an instance directory with default values in an empty target directory, however if <code>-c</code> argument is a pre-existing instance directory rather than wiping and creating fresh contents, the contents are updated. In the situation where the previous instance directory was created from a different runtime directory, the <code>ROOT\_DIR=</code> value in <code>instance.env</code> will be updated to reference the <code><RUNTIME\_DIR></code> from which <code>zowe-configure-instance.sh</code> was executed. In addition the <code>manifest.json</code> file in the instance directory will be updated with the <code>"version:"</code> of the <code><RUNTIME\_DIR></code>. This can be used as a way to see the Zowe version that an instance was last configured from. See Check the Zowe release number.

The zowe-configure-instance.sh script will detect if there are new configuration values that have been introduced since the instance directory was last created, and append these to instance.env with default values. New values added will be echoed in the shell running the zowe-configure-instance.sh script, and are be described in Updating the instance.env configuration file. Values in instance.env previously changed from their default, such as port values or locations of dependent runtimes, are not modified.

The zowe-configure-instance.sh script will echo any values that are added to the instance.env file.

### Important note for users upgrading to v1.14

If you are upgrading to Zowe v1.14 (or higher) from a previous release, and the value of ZOWE\_EXPLORER\_HOST does not match the host and domain that you put into your browser to access Zowe, you must update your configuration due to updated referrer-based security.

To configure your system for the version 1.14 update, perform **one** of the following tasks to update the **instance.env** configuration file:

• Define ZWE\_EXTERNAL\_HOSTS as a comma-separated list of hosts from which you would access Zowe from your browser.

- ZWE\_EXTERNAL\_HOSTS=host1, host2,...
- Define ZWE\_REFERRER\_HOSTS as a comma-separated list for the value to be applied specifically for referrer purposes.
  - ZWE\_REFERRER\_HOSTS=host1, host2,...

See Updating the instance.env configuration file for additional information on the use of instance.env files.

See Configuring a Zowe instance via instance.env file for additional information on configuring instance.env files.

## **Updating the PROCLIB members**

Zowe releases contain two proclib members, ZWESISTC and ZWESVSTC in the PDS SZWESAMP. When the previous release of Zowe was installed, these would have been copied to a PDS in the proclib concatenation path and defined to run under their respective user IDs of ZWESVUSR and ZWESIUSR. See Installing the Zowe started task (ZWESVSTC) and Installing the Zowe cross memory server (ZWESISTC).

The proclib members do not usually get updated between Zowe releases, so during an upgrade you may keep the previous JCL proclibs. If the proclib members are updated then the HOLDDATA and the release notes will describe any changes and alert you that the proclibs need to be updated. If you are upgrading Zowe and jumping releases, for example moving from 1.12 to 1.16, then you should check the HOLDDATA (for SMP/E) and the release notes for all intervening releases (1.12, 1.13, 1.14, 1.15) to see if the proclibs have changed.

## Updating the cross memory server load modules

Zowe releases contain two load modules, ZWESIS00 for the cross memory server and ZWESAUX for the auxiliary server. There are delivered in a PDSE SZWEAUTH that is created by the installation process.

If this PDSE is the same one used by the ZWESISTC proclib that starts the cross memory server, then because the installation replaces the data set and its contents no action is required. This is the recommended approach to configure a Zowe environment.

If you have copied the SZWEAUTH members to another PDSE that you are using as a runtime load module, then you should recopy the updated members to the runtime location.

## Updating the system and security configuration

The JCL member ZWESECUR delivered in the PDS member SZWESAMP contains the TSO commands used to configure a z/OS environment for launching Zowe.

The contents of **ZWESECUR** do not usually get updated between Zowe releases, so during an upgrade you should not need to rerun the JCL. If there are additions, then the HOLDDATA for the SMP/E release and the release notes will describe the changes.

## Upgrading the keystore directory

When the previous release of Zowe was configured, a keystore directory would have been created. This would either contain the Zowe certificate, or else reference a SAF keyring that contains the Zowe certificate. See Configuring Zowe certificates. The USS keystore directory is created using the script <RUNTIME\_DIR>/bin/zowe-setup-certificates.sh that is delivered with the new Zowe release, and creates the USS file <KEYSTORE\_DIRECTORY/zowe-setup-certificates.env containing key value parameters used by the Zowe runtime to locate its certificate.

Typically, the <KEYSTORE\_DIRECTORY> is compatible with later versions and can be used when moving forward to a new Zowe release. There are situations when new functionality is introduced into a Zowe release when new key values pairs may be introduced to the <KEYSTORE\_DIRECTORY>/zowe-setup-certificates.env file, in which case the new release will describe the new functionality in its HOLDDATA (for SMP/E) or release notes. If this occurs, it will be necessary to create a new KEYSTORE\_DIRECTORY in order to use the new functionality. This was the case when Zowe 1.15 introduced support for storing certificates in a SAF keyring.

Zowe provides a JCL member SZWESAMP (ZWEKRING) to create the keystore and populate it with the Zowe certificate. Unless instructed by the HOLDDATA or release notes, there is no need to re-create the keystore or certificate and ones used with previous Zowe releases can be reused.

## Service disruption during upgrades

When Zowe is upgraded, the started tasks ZWESVSTC and ZWESISTC need to be stopped and started for the changes to take effect. This will cause active operations to fail. Idle, or passive operations, such as an open webpage on the Zowe desktop may continue to work without disruption under the following circumstances:

- SSO is being used
- SSO is not being used, but a new page in the browser is opened to re-login to Zowe

In both cases, the original webpages will have access to currently valid credentials, allowing the web page to issue new operations without reloading a page. However, in-process operations that failed during the upgrade, unless retired manually or automatically may necessitate a page reload.

### **Zowe extensions**

Zowe extensions can depend on servers, databases, and other software that is outside the scope of Zowe. Therefore, you should refer to each plug-in's documentation to understand what to expect when an upgrade occurs.

#### Zowe desktop

A system programmer with admin rights may invoke the role base access control (RBAC) controlled App Server endpoint /server/reload to reload the server without the need for an end user webpage reload. This endpoint and more are documented in swagger here.

If the plug-in uses the ZSS server to provide a REST API, ZSS must be restarted causing the same disruption behavior as a Zowe server upgrade.

If the plug-in has web content that shows in the Zowe desktop without an iframe, you must reload the desktop to see the updated content.

## Uninstalling Zowe from z/OS

You can uninstall Zowe™ from z/OS if you no longer need to use it.

#### Follow these steps:

1. Stop the Zowe started task which stops all of its microservices. See Stopping Zowe Server started task

After Zowe has been stopped, its subcomponents will end which include API Mediation Layer and the Zowe desktop.

To make sure that all Zowe subcomponents are ended, you can check either SDSF, DA (Active users) or SDSF, PS (Processes) panel for ZWE\* address spaces. If any Zowe zombie processe is still running, cancel them either from SDSF, DA panel or from USS command line by using the following commands:

2. Delete the Zowe PROCLIB member from your system **PROCLIB** data set.

To do this, you can issue the following TSO DELETE command from the TSO READY prompt or from ISPF option 6:

Alternatively, you can issue the TSO DELETE command at any ISPF command line by prefixing the command with TSO:

Where zowe-proclib-member can be either ZWESVSTC or ZWESLSTC

To query which PROCLIB data set that Zowe PROCLIB member is put in, you can view the SDSF JOB log of Zowe started task and look for the following message:

If no Zowe started task JOB log is available, issue the JES2 command **\$D PROCLIB** at SDSF COMMAND INPUT line and BROWSE each of the **DSNAME=some.jes.proclib** output lines in turn with ISPF option 1, until you find the first data set that contains Zowe PROCLIB member. Then, issue the DELETE command as shown above.

After you have removed PROCLIB member from the **PROCLIB** data set it will no longer be possible to start Zowe instances.

3. Remove the USS folders containing the Zowe artifacts.

Remove the USS folders containing the Zowe runtime, the Zowe keystore-directory, and the Zowe instance directories.

4. Reverse the z/OS security and environment updates from ZWESECUR job.

As part of Zowe installation, the z/OS environment is altered to allow Zowe to operate. See Configuring the z/OS System for Zowe for details. You may leave the environment configured which allows you to install and operate a Zowe instance at a point in the future, or you may undo the configuration steps to your z/OS environment. Zowe provides a JCL member ZWENOSEC that contains the commands needed to reset a z/OS environment and undo the steps that were performed in ZWESECUR when the environment was configured for Zowe operation.

5. Reverse the z/OS key ring updates from ZWEKRING job.

The ZWEKRING JCL member provided in the SZWESAMP member can be used to create a key ring that contains the Zowe certificate(s) and certificate authority. If you want to remove the key ring and its certificate(s) and certificate authority, you can use the JCL member ZWENOKYR that contains the undo steps to reverse the configuration performed in ZWEKRING.

## Introduction

Zowe (server) containers are available for download as an alternative to running Zowe servers on z/OS through the Zowe convenience and SMP/E builds. You can choose the appropriate installation type for your use case. There are several advantages of using containers wherein you can:

- Run Zowe servers on other platforms including Linux on Z and your PC
- Run Zowe servers local to your system for rapid development
- Run redundant copies of servers for scaling capacity to meet workload requirements
- Leverage container monitoring tools

If you are new to containers, you can learn about the concepts from the Kubernetes website.

The Zowe containers are designed to be run together with extensions and Zowe utilities, and therefore are built for orchestration software that can manage the relationship and lifecycle of the containers. The following topics guide you to set up and use Zowe's containers with the Kubernetes orchestration software.

- 1. Prerequisites
- 2. Downloading and installing
- 3. Configuring the Zowe container environment
- 4. Starting, stopping, and monitoring
- 5. Known limitations

## **Known limitations**

- IP Explorer App Framework application is not currently available in Kubernetes deployment.
- You may have an issue that API Catalog is not showing up in Zowe Desktop. Temporary mitigation is restarting the api-catalog Pod.
- You may have issue to use API Catalog Try Out function. The test server is not reachable from your browser.

## **Prerequisites**

Before you install the Zowe server container, make sure that you have the required software and environments.

- Zowe installed on z/OS for users of ZSS and ZIS (default when you use the Zowe Application Framework app-server, the Zowe Desktop, or products that are based on them)
- z/OSMF installed on z/OS for users of it (default when you use gateway, API Mediation Layer, Web Explorers, or products that are based on them)
- A container runtime, such as:
  - Docker
  - CRI-O
  - containerd
- Kubernetes Cluster software
- kubectl, for initial setup and management of the cluster

**Note**: This documentation uses container terminology that may be explained within the Kubernetes Glossary.

## **Kubernetes cluster**

The Zowe containerization solution is compatible with Kubernetes v1.19+ or OpenShift v4.6+.

You can prepare a Kubernetes cluster based on your requirements in many different ways.

- For development purpose, you can set up a Kubernetes cluster on your local computer in one of the following ways:
  - Enable Kubernetes shipped with Docker Desktop
  - Set up minikube
- For production purpose, you can set up a Kubernetes cluster in one of the following ways:

- Bootstrap your own cluster by following instructions in Installing Kubernetes with deployment tools in the Kubernetes documentation.
- Provision a Kubernetes cluster from popular Cloud vendors:
  - Amazon Elastic Kubernetes Service
  - Microsoft Azure Kubernetes Service
  - IBM Cloud Kubernetes Service
  - Google Cloud Kubernetes Engine

## kubectl tool

You need kubectl CLI tool installed on your local computer where you want to manage the Kubernetes cluster. For instructions on how to install the kubectl tool, see Install Tools in the Kubernetes documentation.

Version: v1.25.x LTS

## **Downloading and installing**

Learn how to download and install Zowe's containers.

## Downloading

You can download Zowe's containers in one of the following ways:

- Downloading configuration samples
- Downloading container images

#### **Downloading configuration samples**

The easiest way to install and run Zowe's containers is by using the configuration samples that are provided on Zowe's website. If you don't already have these samples, you can download them by completing the following tasks:

- 1. Download the Zowe zowe-install-packaging repository as a .zip file.
- 2. Extract the compressed file to the system where you will run the Zowe containers.
- 3. Find the samples within the extracted folder containers/kubernetes.

#### **Downloading container images**

Downloading Zowe's container images manually is not required because this can be done automatically when applying a Kubernetes deployment configuration.

If wanted, you can download Zowe's container images manually by using the docker pull or docker load commands. This allows you to get an image from a registry or attach an image that you have downloaded directly. You can find Zowe's container images in the following location:

- Registry: zowe-docker-release.jfrog.io
- Organization: ompzowe

Full image addresses include,

zowe-docker-release.jfrog.io/ompzowe/gateway-service:latest-ubuntu

- zowe-docker-release.jfrog.io/ompzowe/app-server:latest-ubuntu
- zowe-docker-release.jfrog.io/ompzowe/explorer-jes:latest-ubuntu

Therefore, you can download these manually with the docker pull commands. For example,

docker pull zowe-docker-release.jfrog.io/ompzowe/app-server:latest-ubuntu

## Installing

You do not need to install the Zowe containers if you use Zowe's Kubernetes configuration samples. The installation is automatic.

An image could be considered "installed" when it is findable by Kubernetes. Just like downloading, this is done automatically by Kubernetes but commands such as docker pull or docker load accomplishes the same task.

## Configuring

Zowe provides sample configurations that make it easy for you to run Zowe in Kubernetes. You can use them directly or as a reference.

You can customize the configuration or make your own. If you do so, note the following objects that are expected by the container deployments:

Kind	Name	Note
Namespace	zowe	
ServiceAccount	zowe-sa	
ConfigMap	zowe- certificates-cm	Contains zowe-certificates.env with the same format as seen on z/OS keystore
Secret	zowe- certificates- secret	Contains the base64 PEM and P12 data for keystore and truststore
Ingress	discovery- ingress	Used for external access to the Discovery service
Ingress	gateway- ingress	Used for external access to the Gateway service
Route	discovery	Used for external access to the Discovery service
Route	gateway	Used for external access to the Gateway service
Service	discovery- service	Used for internal or external access to the Discovery service
Service	gateway- service	Used for external access to the Gateway service

Kind	Name	Note
Service	catalog- service	Used for access to the Catalog service
PersistentVolumeClaim	zowe- workspace- pvc	
HorizontalPodAutoscaler	*	Autoscalers exist for the various pods
PodDisruptionBudget	*	Disruption budgets exist for the various pods

To configure the Zowe container environment, complete the following procedure.

### 1. Create namespace and service account

Run the following commands to create Zowe's Namespace zowe with Service Account zowe-sa.

Note that by default, zowe-sa service account has automountServiceAccountToken disabled for security purpose.

To verify, check the following configurations.

• kubectl get namespaces should show a Namespace zowe.

This displays the default Namespace zowe, if not set.

• kubectl get serviceaccounts --namespace zowe should show a ServiceAccount zowe-sa.

This displays the default ServiceAccount zowe-sa, if not set.

### 2. Create Persistent Volume Claim (PVC)

Zowe's PVC has a default StorageClass value that may not apply to all Kubernetes clusters. Check and customize the storageClassName value of samples/workspace-pvc.yaml as needed. You can use kubectl get sc to confirm which StorageClass you can use.

After you customize the storageClassName value, apply the result by issuing the following commands:

To verify, run the following commands and check that STATUS shows as Bound.

## 3. Create and modify ConfigMaps and Secrets

Similarly, to running Zowe services on z/OS, you can use either instance.env or zowe.yaml to customize Zowe.

You can modify samples/config-cm.yaml, , and samples/certificates-secret.yaml directly. Or more conveniently, if you have Zowe ZSS/ZIS running on z/OS, the Kubernetes environment can reuse instance and keystore configuration from that installation (supported in v1.25 and later).

If you want to manually create, or later customize the ConfigMaps and Secrets, see Customizing or manually creating ConfigMaps and Secrets for details.

To create and modify ConfigMaps and Secrets by using the migrate configuration script, complete the following steps:

a. On z/OS, run the following command:

This migration script supports these parameters:

- -x: is a comma-separated list of domains you will use to visit the Zowe Kubernetes cluster. These domains and IP addresses will be added to your new certificate if needed. This is optional. The default value is localhost.
- -n : is the Zowe Kubernetes cluster namespace. This is optional. The default value is zowe.
- -u: is the Kubernetes cluster name. This is optional. The default value is cluster.local.
- -p: is the password of local certificate authority PKCS#12 file. This is optional. The default value is local\_ca\_password.
- -a: is the certificate alias of local certificate authority. This is optional. The default value is localca.
- -v: is a switch to enable verbose mode which will display more debugging information.

As a result, it displays ConfigMaps (zowe-config, zowe-certificates-cm) and Secrets (zowe-certificates-secret) Kubernetes objects which are based on the Zowe instance and keystore used. The content looks similar to samples/config-cm.yaml, samples/certificates-cm.yaml and samples/certificates-secret.yaml but with real values. Follow the instructions in the script output to copy the output and save as a YAML file configs.yaml on your server where you have set up Kubernetes.

b. Copy the file over to the computer with Kubernetes.

- c. Remove the .yaml file from z/OS for security.
- d. Apply the file into Kubernetes:

To verify:

kubectl get configmaps ---namespace zowe

This command must display the two ConfigMaps zowe-config and zowe-certificates-cm.

kubectl get secrets ---namespace zowe

This command must display a Secret zowe-certificates-secret.

### 4. Expose API Mediation Layer components

This step makes Zowe's Gateway, Discovery, and API Catalog servers available over a network.

The Gateway is always required to be externally accessible, and depending upon your environment the Discovery service may also need to be externally accessible.

The actions you need to take in this step vary depending upon your Kubernetes cluster configuration. If you are uncertain about this section, please contact your Kubernetes administrator or the Zowe community.

#### 4a. Create service

You can set up either a LoadBalancer or NodePort type Service.

**Note:** Because NodePort cannot be used together with NetworkPolicies, LoadBalancer and Ingress is a preferred configuration option.

Review the following table for steps you may take depending on the Kubernetes provider you use. If you don't need additional setups, you can skip steps 4b, 4c, 4d and jump directly to the Apply zowe section.

Kubernetes provider	Service	Additional setups required
minikube	LoadBalancer or NodePort	Port Forward
docker-desktop	LoadBalancer	none
bare-metal	LoadBalancer or NodePort	Create Ingress
cloud-vendors	LoadBalancer	none
OpenShift	LoadBalancer or NodePort	Create Route

#### Defining api-catalog service

api-catalog-service is required by Zowe, but not necessarily exposed to external users. Therefore, api-catalog-service is defined as type ClusterIP.

To define this service, run the command:

Upon success, you should see the following output:

Then, you can proceed with creating the Gateway and Discovery services according to your environment.

#### Applying Gateway Service

If using LoadBalancer, run the command:

Or if using NodePort instead, first check spec.ports[0].nodePort as this will be the port to be exposed to external. The default gateway port is not 7554 but 32554. You can use https://<your-k8s-node>: 32554/ to access APIML Gateway. Then, run the following command:

To verify either case, run the following command and check that the command displays the service gateway-service.

#### Applying Discovery service

Exposing the Discovery service is only required when there is a Zowe service or extension which needs to be registered to the API Mediation Layer but is running outside of Kubernetes, such as on z/OS. Otherwise, the discovery service can remain accessible only within the Kubernetes environment.

**Optional:** To setup the discovery service without exposing it externally, edit samples/discoveryservice-lb.yaml if using LoadBalancer type services, or samples/discovery-servicenp.yaml if using NodePort type services. In either file, specify ClusterIP as the type, replacing the NodePort or LoadBalancer value.

To enable the service externally when using LoadBalancer services, run the command:

Or if using NodePort instead, first check spec.ports[0].nodePort as this will be the port to be exposed to external. The default discovery port is not 7553 but 32553. You can use https://<your-k8s-node>:32553/ to access APIML Discovery. Then, run the following command:

To verify either case, run the following command and check that this command displays the service discovery-service :

```
kubectl get services --namespace zowe
```

Upon completion of all the preceding steps in this a. Create service section, you may need to run additional setups. Refer to "Additional setups required" in the table. If you don't need additional setups, you can skip 4b, 4c, 4d and jump directly to Apply Zowe section.

#### 4b. Port forwarding (minikube)

Kubectl port-forward allows you to access and interact with internal Kubernetes cluster processes from your localhost. For debugging or development, you may wish to port forward to make Zowe gateway or discovery service available externally quickly.

To use port-forward, run the command:

The & at the command will run the command as a background process, as otherwise it will occupy the terminal indefinitely until canceled as a foreground service.

Upon completion, you can finish the setup by applying zowe and starting it.

#### 4c. Create Ingress (Bare-metal)

An Ingress gives Services externally-reachable URLs, and may provide other abilities such as traffic load balancing.

To create Ingress, perform the following steps:

a. Edit samples/gateway-ingress.yaml and samples/discovery-ingress.yaml before applying them, by uncommenting the lines (19 and 20) for defining spec.rules[0].host and http:, and then commenting out the line below, - http:

b. Run the following commands:

To verify, run the following commands:

kubectl get ingresses --namespace zowe

This command must display two Ingresses gateway-ingress and discovery-ingress.

Upon completion, you can finish the setup by applying zowe and starting it.

#### 4d. Create Route (OpenShift)

If you are using OpenShift container platform, you must define Route instead of Ingress.

A Route is a way to expose a service by giving it an externally-reachable hostname.

To create a route, perform the following steps:

```
a. Check and set the value of spec.port.targetPort in samples/gateway-route.yaml and samples/discovery-route.yaml before applying the changes.
```

b. Run the following commands:

To verify, run the following commands:

oc get routes --namespace zowe

This command must displays the two Services gateway and discovery.

Upon completion, you can finish the setup by applying zowe and starting it.

## Customizing or manually creating ConfigMaps and Secrets

The z/OS to k8s convert tool can automatically create a config map and secret. However, if you want to customize or create your own, review the instructions in this section.

To manually create the ConfigMaps and Secrets used by Zowe containers, you must create the following objects:

- 1. A ConfigMap, with values based upon a Zowe instance's instance.env and similar to the example samples/config-cm.yaml with the following differences to the values seen on a z/OS install:
  - ZOWE\_EXPLORER\_HOST, ZOWE\_IP\_ADDRESS, ZWE\_LAUNCH\_COMPONENTS,
     ZWE\_DISCOVERY\_SERVICES\_LIST and SKIP\_NODE are not needed for Zowe running in Kubernetes and will be ignored. You can remove them.
  - JAVA\_HOME and NODE\_HOME are not usually needed if you are using Zowe base images.
  - ROOT\_DIR must be set to /home/zowe/runtime.
  - KEYSTORE\_DIRECTORY must be set to /home/zowe/keystore.
  - ZWE\_EXTERNAL\_HOSTS is suggested to define as a list domains you are using to access your Kubernetes cluster.
  - ZOWE\_EXTERNAL\_HOST=\$(echo "\${ZWE\_EXTERNAL\_HOSTS}" | awk -F, '{print \$1}' | tr -d '[[:space:]]') is needed to define after ZWE\_EXTERNAL\_HOSTS. It's the primary external domain.
  - ZWE\_EXTERNAL\_PORT (or zowe.externalPort if you are using zowe.yaml) must be the port you expose to end-user. This value is optional if it's same as default GATEWAY\_PORT 7554. With default settings,
    - if you choose LoadBalancer gateway-service, this value is optional, or set to 7554,
    - if you choose NodePort gateway-service and access the service directly, this value should be same as spec.ports[0].nodePort with default value 32554,
    - if you choose NodePort gateway-service and access the service through port forwarding, the value should be the forwarded port you set.
  - ZOWE\_ZOS\_HOST is recommended to be set to where the z/OS system where your Zowe ZSS/ZIS is running.
  - ZWE\_DISCOVERY\_SERVICES\_REPLICAS should be set to same value of spec.replicas defined in workloads/discovery-statefulset.yaml.
  - All components running in Kubernetes should use default ports:
    - CATALOG\_PORT is 7552,
    - DISCOVERY\_PORT is 7553,
    - GATEWAY\_PORT is 7554,
    - ZWE\_CACHING\_SERVICE\_PORT is 7555,
    - JOBS\_API\_PORT is 8545,

- FILES\_API\_PORT is 8547,
- JES\_EXPLORER\_UI\_PORT is 8546 ,
- MVS\_EXPLORER\_UI\_PORT is 8548,
- USS\_EXPLORER\_UI\_PORT is 8550,
- ZOWE\_ZLUX\_SERVER\_HTTPS\_PORT is 8544.
- ZOWE\_ZSS\_SERVER\_PORT should be set to the port where your Zowe ZSS is running on ZOWE\_ZOS\_HOST.
- APIML\_GATEWAY\_EXTERNAL\_MAPPER should be set to https://\${GATEWAY\_HOST}:\${GATEWAY\_PORT}/zss/api/v1/certificate/x509/map
- APIML\_SECURITY\_AUTHORIZATION\_ENDPOINT\_URL should be set to https://\${GATEWAY\_HOST}:\${GATEWAY\_PORT}/zss/api/v1/saf-auth.
- ZOWE\_EXPLORER\_FRAME\_ANCESTORS should be set to \${ZOWE\_EXTERNAL\_HOST}:\*
- ZWE\_CACHING\_SERVICE\_PERSISTENT should NOT be set to VSAM. redis is suggested. Follow Redis configuration documentation to customize other redis related variables. Leave the value to empty for debugging purpose.
- Must append and customize these 2 values:
  - ZWED\_agent\_host=\${ZOWE\_ZOS\_HOST}
  - ZWED\_agent\_https\_port=\${ZOWE\_ZSS\_SERVER\_PORT}

If you are using zowe.yaml, the above configuration items are still valid, but should use the matching
zowe.yaml configuration entries. Check Updating the zowe.yaml configuration file for more details.

- 2. A ConfigMap, with values based upon a Zowe keystore's zowe-certificates.env and similar to the example samples/certificates-cm.yaml.
- 3. A Secret, with values based upon a Zowe keystore's files, and similar to the example samples/certificates-secret.yaml.

## Starting, stopping, and monitoring

After Zowe's containers are installed and configured, you can refer to the following topics that help you manage your installation.

## **Starting Zowe containers**

The Kubernetes cluster will automatically start as many containers as needed per service according to the Deployment configuration.

To apply the deployment files, run the command:

The containers will start soon after applying the deployments.

To verify:

1. kubectl get deployments --namespace zowe

This command must show you a list of deployments including explorer-jes, gateway-service, app-server, etc. Each deployment should show 1/1 in READY column. It could take a moment before all deployments say 1/1.

2. kubectl get statefulsets ---namespace zowe

This command must show you a StatefulSet discovery which READY column should be 1/1.

3. kubectl get cronjobs --namespace zowe

This command must show you a CronJob cleanup-static-definitions which SUSPEND should be False.

### **Monitoring Zowe containers**

You can monitor Zowe containers using a UI or CLI.

#### Monitoring Zowe containers via UI

Kubernetes provides a container that allows you to manage your cluster through a web browser. When using Docker Desktop, it is already installed in the namespace kubernetes-dashboard. See the Kubernetes website for install instructions.

Metrics Server is also recommended and is required if you want to define Horizontal Pod Autoscaler. Check if you have metrics-server Service in kube-system namespace with this command kubectl get services —namespace kube-system. If you don't have, you can follow this Installation instruction to install it.

#### Monitoring Zowe containers via CLI

kubectl allows you to see the status of any kind of object with the get command. This applies to the table in the configuring section but also for the pods that run the Zowe containers.

Here are a few commands you can use to monitor your environment:

- kubectl get pods -n zowe lists the status of the components of Zowe.
- kubectl describe pods -n zowe <podid> can see more details about each pod.
- kubectl logs -n zowe <podid> will show you the terminal output of a particular pod, with -f allowing you to keep the logs open as new messages are added.
- kubectl get nodes -n zowe -owide will tell you more about the environment you're running.

### Stopping, pausing, or removing Zowe containers

To temporarily stop a component, locate the **Deployment** component and scale down to **0**. For example, if you want to stop the jobs-api container, run this command:

You can later re-enable a component by scaling the component back to 1 or more.

If you want to permanently remove a component, you can delete the component Deployment. To use jobs-api as example, run this command:

Version: v1.25.x LTS

## System requirements

Before installing Zowe™ CLI, ensure that your environment meets the prerequisites.

- Client-side
- Host-side
- Free disk space

## **Client-side**

Zowe CLI is supported on Windows, Linux, and Mac operating systems. Meet the following requirements before you install the CLI:

• **Node.js:** Install a currently supported Node.js LTS version. For an up-to-date list of supported LTS versions, see Nodejs.org.

#### 💭 ΤΙΡ

You might need to restart the command prompt after installing Node.js. Issue the command node --version to verify that Node.js is installed.

• **npm:** Install a version of Node Package Manager (npm) that is compatible with your version of Node.js.

### 

Npm is included with most Node.js installations. Issue the command <code>npm --version</code> to check your current version. You can reference the <u>Node.js release matrix</u> to verify that the versions are compatible.

- (Optional) ssh2 Package: Zowe CLI has a dependency on the ssh2 package. This package allows for more secure cryptographic ciphers to be used first on supporting hardware. See Installing the ssh2 Package for Zowe CLI.
- **Plug-in client requirements:** If you plan to install plug-ins, review the Software requirements for CLI plug-ins. You *must* meet the client requirements for the Secure Credential Store and IBM Db2 plug-ins prior to installing them.

## Host-side

Zowe CLI requires the following mainframe configuration:

- IBM z/OSMF configured and running: You do not need to install the full Zowe solution to install and use Zowe CLI. Minimally, an instance of IBM z/OSMF must be running on the mainframe before you can issue Zowe CLI commands successfully. z/OSMF enables the core capabilities such as retrieving data sets, executing TSO commands, submitting jobs, and more. If Zowe API Mediation Layer (API ML) is configured and running, CLI users can choose to connect to API ML rather than to every separate service.
- **Plug-in services configured and running:** Plug-ins communicate with various mainframe services, which must be configured and running on the mainframe prior to issuing plug-in commands. For example, the IMS plug-in requires an instance of IBM IMS on the mainframe with IMS Connect (REST services) running. For more information, see Software requirements for CLI plug-ins
- Zowe CLI on z/OS is not supported: Zowe CLI can be installed on an IBM z/OS environment and run under Unix System Services (USS). However, the IBM Db2 and Secure Credentials Store plug-ins will *not* run on z/OS due to native code requirements. As such, Zowe CLI is *not* supported on z/OS and is currently experimental.

## Free disk space

Zowe CLI requires approximately **100 MB** of free disk space. The actual quantity of free disk space consumed might vary depending on your operating system, the plug-ins that you install, and user profiles saved to disk.

## Installing the ssh2 Package for Zowe CLI

This topic describes how to install the prerequisites to enable optional security features in the ssh2 package.

The Zowe CLI has a dependency on the ssh2 package. This package allows for more secure cryptographic ciphers to be used on supporting hardware. To do this, the ssh2 package attempts to build native modules at install time. If the modules cannot be built, the dependency will continue to function without the optimal cipher list order. However, you may receive some error messages that can be safely ignored.

To load the optimal cipher list and build the native modules, verify that you meet the following prerequisites:

### Windows

Recommended:

- NodeJS
- Chocolatey
- CMake

Alternative:

- Python 3.7 or greater
- CMake
- One of the following:
  - Visual Studio Build Tools, "Visual C++ build tools" workload
  - Visual Studio Community, "Desktop development with C++" workload

## Unix

- Python 3.7 or greater
- CMake
- make
- A C/C++ Compiler (gcc-c++ or g++, for example)

## MacOS

- Python 3.7 or greater
- CMake
- XCode, including XCode Command Line Tools

## Installing Zowe CLI

Install Zowe™ CLI on your computer.

**Tip:** If you are familiar with command-line tools and want to get started using Zowe CLI quickly, see Zowe CLI quick start. You can learn about new CLI features in the Release notes.

## **Methods to install Zowe CLI**

Use one of the following methods to install Zowe CLI.

- Installing Zowe CLI from a local package
- Installing Zowe CLI from an online registry

**Note:** If you do not have access to the public npm registry at your site, you might want to install the CLI via a proxy server. See Installing Zowe CLI Via Proxy for more information.

If you encounter problems when you attempt to install Zowe CLI, see Troubleshooting Zowe CLI.

#### Installing Zowe CLI from a local package

If you do not have internet access at your site, use the following method to install Zowe CLI from a local package.

#### Follow these steps:

- 1. Address the following software requirements for the core CLI:
  - Node.js: Install a currently supported Node.js LTS version. For an up-to-date list of supported LTS versions, see Nodejs.org. ::: You might need to restart the command prompt after installing Node.js.
     Issue the command node --version to verify that Node.js is installed. :::
  - npm: Install a version of Node Package Manager (npm) that is compatible with your version of Node.js. ::: Npm is included with most Node.js installations. Issue the command <u>npm --version</u> to check your current version. You can reference the Node.js release matrix to verify that the versions are compatible. :::

::: If you are using Node.js version 16 with npm version 8 on Windows, wish to install from the TGZ, and have limited Internet access, refer to Installing Zowe CLI with Node.js 16 on Windows. :::

- (Optional) ssh2 Package: Zowe CLI has a dependency on the ssh2 package. This package allows for more secure cryptographic ciphers to be used first on supporting hardware. See Installing the ssh2 Package for Zowe CLI.
- 2. (Linux only) Address the following software requirements for Secure Credential Storage:
  - (Graphical Linux) Install gnome-keyring and libsecret on your computer.
  - (Headless Linux) Follow the procedure documented in the SCS plug-in Readme.
- 3. Navigate to Zowe.org Downloads and click the **CLI Core** button to download the core package. The "core" includes Zowe CLI and Secure Credential Store, which enhances security by encrypting your username and password.

A file named zowe-cli-package-v.r.m.zip is downloaded to your computer

4. (Optional) Click the CLI Plugins button to download the optional plugins.

A file named zowe-cli-plugins-v.r.m.zip is downloaded to your computer.

- 5. Unzip the contents of zowe-cli-package-v.r.m.zip (and optionally zowe-cli-pluginsv.r.m.zip) to a preferred location on your computer.
- 6. Open a command-line window. Issue the following commands in sequence against the extracted directory to install core Zowe CLI on your computer:

#### Notes:

- If the command returns an EACCESS error, refer to Resolving EACCESS permissions errors when installing packages globally in the npm documentation.
- On Linux, you might need to prepend sudo to your npm commands. For more information, see Troubleshooting Zowe CLI.
- 7. **(Optional)** Address the Software requirements for CLI plug-ins. You can install most plug-ins without meeting the requirements, but they will not function until you configure the back-end APIs. The IBM Db2 plug-in requires additional configuration to install.
- 8. (Optional) Issue the following command to install each available plug-in:

**Important:** Ensure that you meet the Software requirements for CLI plug-ins. You can install most plugins without meeting the requirements, but they will not function until you configure the back-end APIs. The IBM Db2 plug-in requires additional configuration to install.

Zowe CLI is installed on your computer. Issue the zowe ––help command to view a list of available commands. For information about how to connect the CLI to the mainframe, create profiles, integrate with API ML, and more, see Using CLI.

#### Installing Zowe CLI from an online registry

If your computer is connected to the Internet, you can use the following method to install Zowe CLI from an npm registry.

#### Follow these steps:

- 1. Address the following software requirements for the core CLI:
  - Node.js: Install a currently supported Node.js LTS version. For an up-to-date list of supported LTS versions, see Nodejs.org.

#### 📿 ΤΙΡ

You might need to restart the command prompt after installing Node.js. Issue the command node --version to verify that Node.js is installed.

 npm: Install a version of Node Package Manager (npm) that is compatible with your version of Node.js.

#### 

Npm is included with most Node.js installations. Issue the command <code>npm --version</code> to check your current version. You can reference the <u>Node.js release matrix</u> to verify that the versions are compatible.

- (Optional) ssh2 Package: Zowe CLI has a dependency on the ssh2 package. This package allows for more secure cryptographic ciphers to be used first on supporting hardware. See Installing the ssh2 Package for Zowe CLI.
- 2. (Linux only) Address the following software requirements for Secure Credential Storage:

- (Graphical Linux) Install gnome-keyring and libsecret on your computer.
- (Headless Linux) Follow the procedure documented in the SCS plug-in Readme.
- 3. Issue the following commands in sequence to install the core from the public npm registry. The "core" includes Zowe CLI and Secure Credential Store, which enhances security by encrypting your username and password.

#### Notes:

- If the command returns an EACCESS error, refer to Resolving EACCESS permissions errors when installing packages globally in the npm documentation.
- On Linux, you might need to prepend sudo to your npm commands. For more information, see Troubleshooting Zowe CLI.
- 4. (Optional) Address the Software requirements for CLI plug-ins. You can install most plug-ins without meeting the requirements, but they will not function until you configure the back-end APIs. The IBM Db2 plug-in requires additional configuration to install.
- 5. (Optional) To install all available plug-ins to Zowe CLI, issue the following command:

Zowe CLI is installed on your computer. Issue the zowe --help command to view a list of available commands. For information about how to connect the CLI to the mainframe, create profiles, integrate with API ML, and more, see Using CLI.

## Install CLI from Online Registry Via Proxy

This topic describes how to install Zowe CLI using the NPM install command when you are working behind a proxy server. You will need to use this installation method if your site blocks access to public npm.

You can install Zowe CLI from an online registry via proxy on Windows, macOS, or Linux operating systems:

- This method requires access to an internal server that will allow you to connect to the appropriate registries. For other installation methods, see Installing CLI.
- Your default registry must be public npm (or a mirror of public npm).
- (Optional) ssh2 Package: Zowe CLI has a dependency on the ssh2 package. This package allows for more secure cryptographic ciphers to be used first on supporting hardware. See Installing the ssh2 Package for Zowe CLI.
- If you previously installed the CLI and want to update to a current version, see Update Zowe CLI.

Follow these steps:

- 1. Identify the proxy server, including the IP address or hostname and the port number.
  - If your proxy server **does not** require login credentials, issue the following commands to add the proxy URL to the NPM config file:

*where* [proxy\_name] is the IP or hostname and [port\_number] is the port number of the proxy server.

 If your proxy server **does** require login credentials, issue the following commands to add the proxy URL, with login credentials, to the NPM config file:

*where* [username] and [password] are the required login credentials, [proxy\_name] is the IP or hostname, and [port\_number] is the port number of the proxy server.

- 2. Ensure that you meet the Software Requirements for CLI.
- 3. To install Zowe CLI, issue the following command. On Linux, you might need to prepend **sudo** to your npm commands:
- 4. Install the Secure Credential Store, which lets you store your username, password, and other sensitive information in the credential vault on your computer instead of plaintext. Issue the following command:

5. (Optional) To install open-source Zowe plug-ins, issue the following command:

Zowe CLI is installed.

- 6. (Optional) Verify that a Zowe plug-in is operating correctly.
- 7. (Optional) Test the connection to z/OSMF. See Testing Connection to z/OSMF
- 8. **(Optional)** Access the Zowe CLI Help (zowe --help) or the Zowe CLI Web Help for a complete reference of Zowe CLI. After you install the CLI, you can connect to the mainframe directly issuing a command, by creating user profiles and making use of them on commands, or by using environment variables. For more information, see Using CLI.

## **Updating Zowe CLI**

Zowe<sup>™</sup> CLI is updated continuously. You can update Zowe CLI to a more recent version using online registry method or the local package method. However, you can only update Zowe CLI using the method that you used to install Zowe CLI.

- Migrating to Long-term Support (LTS) version
- Identify the currently installed version of Zowe CLI
- Identify the currently installed versions of Zowe CLI plug-ins
- Update Zowe CLI from the online registry
- Update or revert Zowe CLI to a specific version
- Update Zowe CLI from a local package

## Migrating to Long-term Support (LTS) version

If you have an @lts-incremental version of Zowe CLI (Zowe v1.0.x - v1.8.x), you can update to @zowev1-lts (LTS version) to leverage new functionality and plug-ins.

#### Follow these steps:

- 1. Perform one of the following steps:
  - **a.** Delete the ~/.zowe/profiles directory from your computer. You can recreate the profiles manually after you update the CLI.

**b.** If you want to preserve your existing profiles, copy the contents of ~/.zowe/profiles or %homepath%\.zowe\profiles to another directory on your computer.

- 2. Delete the ~/.zowe/plugins or %homepath%\.zowe\plugins directory to uninstall all plug-ins.
- 3. Issue the following command to uninstall the pre-LTS version of core CLI

**Note:** You might receive an **ENOENT** error when issuing this command if you installed Zowe CLI from a local package (.tgz) and the package was moved from its original location. In the event that you receive the error, open an issue in the Zowe CLI GitHub repository.

- 4. Install the most recent @zowe-v1-lts version CLI and optional plug-ins. For more information, see Installing CLI.
- 5. (Optional) If you deleted your profiles in Step 1, recreate the profiles that you need manually.
- 6. (Optional) If you copied your profiles to a local directory in Step 1, follow these steps:

**a.** Move the profile configuration files that you saved in Step 1 back to the ~/.zowe/profiles or %homepath%\.zowe\profiles folder on your computer.

**b.** Issue the **zowe scs update** command to update profiles that are secured with the Secure Credential Store Plug-in.

**c.** Issue the command zowe profiles update zosmf <my-profile-name> --user <myusername> --password <my-password> to update z/osmf profiles to use the current option names.

You updated to the Zowe CLI LTS version!

Ensure that you review the Release Notes, which describes **Notable Changes** in this version. We recommend issuing familiar commands and running scripts to ensure that your profiles/scripts are compatible. You might need to take corrective action to address the breaking changes.

### Identify the currently installed version of Zowe CLI

Issue the following command:

## Identify the currently installed versions of Zowe CLI plugins

Issue the following command:

### Update Zowe CLI from the online registry

You can update Zowe CLI to the latest version from the online registry on Windows, Mac, and Linux computers.

**Note:** The following steps assume that you previously installed the CLI as described in Installing Zowe CLI from an online registry.

#### Follow these steps:

- 1. To update Zowe CLI to the most recent @zowe-v1-lts version, issue the following command:
- 2. To update existing plug-ins and install new plug-ins, issue the following command:
- 3. Recreate any user profiles that you created before you updated to the latest version of Zowe CLI.

### Update or revert Zowe CLI to a specific version

Optionally, you can update Zowe CLI (or revert) to a known version. The following example illustrates the syntax to update Zowe CLI to version 6.1.2:

### Update Zowe CLI from a local package

To update Zowe CLI from an offline (.tgz), local package, uninstall your current package then reinstall from a new package using the Install from a Local package instructions. For more information, see Uninstalling Zowe CLI from the desktop and Installing Zowe CLI from a local package.

**Important!** Recreate any user profiles that you created before the update.

## **Uninstalling Zowe CLI**

You can uninstall Zowe™ CLI from the desktop if you no longer need to use it.

**Important!** The uninstall process does not delete the profiles and credentials that you created when using the product from your computer. To delete the profiles from your computer, delete them before you uninstall Zowe CLI.

The following steps describe how to list the profiles that you created, delete the profiles, and uninstall Zowe CLI.

#### Follow these steps:

1. Open a command-line window.

Note: If you do not want to delete the Zowe CLI profiles from your computer, go to Step 5.

2. List all profiles that you created for a given command group. Issue the following command:

#### Example:

3. Delete all of the profiles that are listed for the command group by issuing the following command:

**Tip:** For this command, use the results of the list command.

**Note:** When you issue the delete command, it deletes the specified profile and its credentials from the credential vault in your computer's operating system.

#### Example:

- 4. Repeat Steps 2 and 3 for all Zowe CLI command groups and profiles.
- 5. Uninstall Zowe CLI by issuing the following command:

**Note:** You might receive an **ENOENT** error when issuing this command if you installed Zowe CLI from a local package (.tgz) and the package was moved from its original location. In the event that you receive the error, open an issue in the Zowe CLI GitHub repository.

The uninstall process removes all Zowe CLI installation directories and files from your computer.

6. Delete the ~/.zowe or %homepath%\.zowe directory on your computer. The directory contains the Zowe CLI log files and other miscellaneous files that were generated when you used the product.

**Tip:** Deleting the directory does not harm your computer.

# Zowe CLI Development Roadmap (Technical Preview)

**Technical Preview** The Zowe CLI @next release is a technical preview. Technical previews are for testing only and are not ready for production. Your feedback is valued and appreciated.

To preview the features of the @next version of Zowe CLI, install the @next release. This version may receive breaking changes and is intended to gather early feedback on what may become a future LTS release.

The @next version features:

- Global Profile Configuration Improves the initial setup of the command line interface by making service connection details easier to share and easier to store within projects. For information, see Using Global Profile Configuration.
- Daemon Mode Run Zowe CLI as a persistent background process (daemon). For information, see Using Daemon Mode.

For a more comprehensive list of features and enhancements in the @next version, see the Zowe CLI changelog.

## Install the Zowe CLI @next version

**Technical Preview** The Zowe CLI @next release is a technical preview. Technical previews are for testing only and are not ready for production. Your feedback is valued and appreciated. **Prerequisites** 

- Meet the software requirements for Zowe CLI.
- Meet the software requirements for each plug-in.

**Note:** Linux users may need to prepend **sudo** to **npm** commands. For more information, see Troubleshooting Zowe CLI.

Install the Zowe CLI @next version from the online npm registry or download it from the Zowe Downloads site:

- Install Zowe CLI from npm
- Install Zowe CLI from a download

## Install Zowe CLI from npm

**Note:** This method does not install the zowex native executable required to run Zowe daemon mode. To install the zowex native executable, see Install Zowe CLI from a download.

#### Follow these steps:

1. To install or update the core CLI, open a command-line window:

Zowe CLI is installed.

2. (Optional) Check npmjs.com for any Zowe plug-ins that have an @next version available. If an @next version is available, you can install it:

If no @next version is available, install the @latest version of the plug-in:

Optional plug-ins are installed.

3. Issue the command:

4. If you have the Secure Credential Store plug-in installed, uninstall it now to avoid unexpected behavior:

**Note:** If you have a previous instance of Zowe CLI installed, your current configuration files are ignored if zowe.config.json is found globally, at the project level, or up the directory structure.

- 5. Save the contents of the /profiles directory to another location on your computer so that you can reference or restore the profiles later. **Important!** Prior to deleting the contents of the /profiles directory, take note of any mainframe service details that you need.
- 6. Delete the following files from your local . zowe/ directory:
  - .zowe/settings/imperative.json
  - .zowe/profiles

You can now try out the technical preview features.

### Install Zowe CLI from a download

#### Follow these steps:

- 1. Navigate to Zowe Downloads and click the **Zowe vNext CLI Core** button.
- 2. Read the End User License Agreement for Zowe and click **I agree** to download the core package.

```
zowe-cli-package-next-2021MMDD.zip is downloaded to your computer (where MMDD indicates the month and day of the build).
```

- 3. (Optional) Navigate to Zowe Downloads and click the Zowe vNext CLI Plugins button to download the plugins.
- 4. **(Optional)** Read the End User License Agreement for Zowe plugins and click **I agree** to download the plugins package.

zowe-cli-plugins-next-2021MMDD.zip is downloaded to your computer (where MMDD indicates the month and day of the build).

- 5. Unzip the contents of zowe-cli-package-next-2021MMDD.zip (and optionally zowe-cliplugins-2021MMDD.zip) to a working directory.
- 6. Open a command-line window and issue the following commands to the working directory:

**Note:** If an **EACCESS** error is returned, refer to Resolving EACCESS permissions errors when installing packages globally in the npm documentation.

#### (Optional)

- 7. **(Optional)** To use daemon mode, unzip the zowex .tgz file and place the zowex (or zowex.exe) file into a directory which occurs on your PATH earlier than the directory containing the NodeJS zowe command.
- 8. If you have the Secure Credential Store plug-in installed, uninstall it now to avoid unexpected behavior:

**Note:** If you have a previous instance of Zowe CLI installed, your current configuration files are ignored if zowe.config.json is found globally, at the project level, or up the directory structure.

9. Save the contents of the /profiles directory to another location on your computer so that you can reference or restore the profiles later.

**Important!** Prior to deleting the contents of the /profiles directory, take note of any mainframe service details that you need.

10. Delete the following files from your local .zowe/ directory:

- .zowe/settings/imperative.json
- .zowe/profiles

You can now try out the technical preview features.

```
Version: v1.25.x LTS
```

## **Using Daemon Mode (Technical Preview)**

**Technical Preview** Daemon mode is available in the `@next` version of Zowe CLI. The Zowe CLI @next release is a technical preview. Technical previews are for testing only and are not ready for production. Your feedback is valued and appreciated.

If you already installed the supported version @zowe-v1-lts, switch versions to try this feature. Daemon mode will be included in the next major Zowe release, V2.0.0-LTS. You can also install the @next release of Zowe CLI.

#### Table of Contents:

- Feature overview
- Install the zowex native executable
- Starting Zowe in daemon mode

## **Feature overview**

Daemon Mode significantly improves the performance of Zowe CLI commands by running Zowe CLI as a persistent background process (daemon).

## Install the zowex native executable

You can download and install the zowex native executable from Zowe Downloads (preferred) or from the Zowe Github repository. To install the zowex native executable from Zowe Downloads, see Install Zowe CLI from a download.

To download and install the zowex native executable from the Zowe Github repository:

- 1. Navigate to the Zowe CLI GitHub repository
- 2. Under the **Release** section, click **Native Client Release**. The Download page is displayed.
- 3. Click the link to download the executable (.tgz file) for your operating system.
- 4. Unzip the zowex .tgz file and place the zowex (or zowex.exe) file into a directory which occurs on your PATH earlier than the directory containing the NodeJS zowe command.

### **Starting Zowe in daemon mode**

Verify that you have installed the @next release of Zowe CLI and the zowex native executable.

To start Zowe CLI in daemon mode:

1. Issue the command: Windows command prompt (cmd.exe):

Linux or Windows PowerShell:

The CLI responds with prompts for a username and password.

- 2. Enter the username and password.
- 3. Use zowex as your primary command instead of zowe. Example:

Version: v1.25.x LTS

# Using Global Profile Configuration (Technical Preview)

**Technical Preview** Global profiles are available in the `@next` version of Zowe CLI. The Zowe CLI `@next` release is a technical preview. Technical previews are for testing only and are not ready for production. Your feedback is valued and appreciated.

If you already installed the supported version @zowe-v1-lts, switch versions to try this feature. Global profiles will be included in the next major Zowe release, V2.0.0-LTS. You can also install the @next release of Zowe CLI.

#### Table of Contents:

- Feature overview
  - Benefits
  - Changes to secure credential storage
- Initializing global configuration
- Initializing user-specific configuration (Optional)
- Editing global configuration
- Managing credential security
- Tips for efficient configuration
  - Command option order of precedence
  - Tips for using the base profile
- Sharing global configuration
- Example configurations

# **Feature overview**

In the V1-LTS version of Zowe CLI, users issue commands from the zowe profiles group to create, edit, and manage user profiles. Each profile contains the host, port, username, and password for one mainframe service instance. While effective, users often need to duplicate values across profiles and spend time managing many profiles.

The introduction of **global profiles** simplifies profile management by letting you edit, store, and share mainframe configuration details in one location. You can use a text editor to populate global profiles with

connection details for your mainframe services.

### **Benefits**

Global profiles improve your Zowe CLI experience:

- As a user, you can manage your connection details efficiently in one location.
- As a team leader, you can share global profiles with your team members so that they can easily access mainframe services. You can add the file directly to your project in an SCM.
- As a new team member, you can onboard quickly by using your team's configuration file.

#### Changes to secure credential storage

With the introduction of global profiles, the Secure Credential Store (SCS) Plug-in is deprecated in the @next version. The zowe scs and zowe config command groups are obsolete. Secure credential encryption is now included in the core CLI.

The CLI prompts you to enter the username and password securely by default. Commands in the zowe config command group let you manage security for any option value.

# Initializing global configuration

Verify that you have installed the @next release of Zowe CLI.

You have two options to initialize the global configuration:

- Define a connection to z/OSMF (recommended).
- Create your configuration files manually.

#### Follow these steps:

1. Issue the command:

The CLI responds with prompts for a username and password.

2. Respond to the prompts with a username and password for a mainframe service such as z/OSMF.

**Note:** The **config init** command ensures that your credentials are stored securely on your computer by default.

After you respond, the zowe.config.json global configuration file is added to your local .zowe directory. This is the primary location where your MF service connection details such as host and port are defined. Use this configuration file for the following procedures.

3. Issue a Zowe CLI command to test that you can access z/OSMF. For example, list all data sets under your user ID:

A list of data sets is returned. You successfully configured Zowe CLI to access a z/OSMF instance.

If the CLI returns an error message, verify that you have access to the target system. Examine your configuration files in a text editor to verify that the information you entered is correct.

**Important!:** After the configuration files are in place (either via the zowe config init command or by manually creating the files), the now-deprecated zowe profiles commands will no longer function. Zowe CLI will return errors if you attempt to use deprecated profile commands.

# Initializing user-specific configuration (Optional)

You can generate a *user-specific* configuration file that overrides the values defined in the global zowe.config.json file.

```
To generate both global (zowe.config.json) and user (zowe.config.user.json) config files, issue the command zowe config init --global-config --user-config.
```

In your user-specific file, notice that the "defaults" object is empty and the profiles do not have any properties. You can add your connection details as properties here to override properties in <code>zowe.config.json</code>, or add add new connections.

# **Editing global configuration**

After the initial setup, you can define additional mainframe services to the global (or user-specific) configuration file.

```
Open the ~/.zowe/zowe.config.json file in a text editor or IDE on your computer. The profiles object contains connection and other frequently needed information for accessing various services. For example:
```

You can edit the details as needed and save the file.

For example, to add a new instance of z/OSMF that runs on a different mainframe LPAR, you can build on the existing config as follows:

You can continue to add more LPARs and more services within each LPAR. After you make changes, save the file and issue a Zowe CLI command to the service to verify the connection.

# Managing credential security

When you first run the zowe config init --global-config command, the profiles.base.properties.user and profiles.base.properties.password fields are defined to the "secure" array in your configuration file. This ensures that the username and password are stored securely on your computer.

To update the secure fields (for example, when you want to change your username and password), issue the zowe config secure command.

To secure a specific field, use the command zowe config set --secure <property-path>. For example, you can issue zowe config set --secure profiles.base.properties.password. If you issue the command for an option that is already secured, the CLI prompts you to enter a new option value.

You can use an editor to define options to the secure array in zowe.config.json. Any option that you
define to there becomes secure/prompted-for.

# **Tips for efficient configuration**

There are several methods to more efficiently update and maintain your configuration:

- Leverage the command option order of precedence
- Utilize a base profile or nested profiles

### Command option order of precedence

Zowe CLI uses a **command option order of precedence** by which service definitions inherit option values. Use this feature to avoid duplicating option values.

Zowe CLI checks for option values in order, skipping null values:

- 1. Explicit command-line option values
- 2. Environment variables
- 3. Service type profiles
- 4. Base type profiles
- 5. Default option value

In the example config above, the host, user, and password fields are not supplied in the service profile for "zosmf\_lpar1", because they inherit values from the base profile.

### Tips for using the base profile

Use the base profile to share option values between services. You might share option values between services in the following situations:

- You have multiple services that share the same username, password, or other value.
- You want to store a web token to access all services through Zowe API Mediation Layer.
- You want to trust a known self-signed certificate or your site does not have server certificates configured. You can define reject-unauthorized in the base profile with a value of false to apply to all services. Understand the security implications of accepting self-signed certificates at your site before you use this method.

If you have multiple LPARs and want to share option values only between services that run on the same LPAR, you can use nested profiles to achieve this (see Example 1 below).

# Sharing global configuration

You might want to share a configuration globally:

- With developers so that they can begin working with a defined set of mainframe services. The recipient of the file manually places it in their local ~/.zowe folder before issuing CLI commands.
- To add to your project directory in an SCM tool such as GitHub. This lets other developers pull the project to their local machine and make use of the defined configuration. Zowe CLI commands that you issue from within the project directory automatically use the project's config scheme.
- To enable test automation and CI/CD, letting your pipelines make use of the project configuration.

# **Example configurations**

**Example 1:** The settings are using nested profiles to access multiple services directly on multiple LPARs that share the same username and password.

**Example 2:** The settings are accessing multiple services using the API ML (where MFA/SSO is achievable via token-based authorization).

**Example 3:** The settings are accessing multiple services directly on LPAR1 and LPAR2 where username and password varies between the LPAR1 and LPAR2 services. This example is identical to Example 1 except that LPAR1 and LPAR2 each contain a secure array, instead of just one secure array in the "base" profile.

**Example 4:** Using API ML to access production services while services on a dev-test environment can be accessed directly.

Version: v1.25.x LTS

# Installing Zowe Explorer

#### chat on Slack

The Zowe Explorer extension for Visual Studio Code (VSCode) modernizes the way developers and system administrators interact with z/OS mainframes, and lets you interact with data sets, USS files and jobs. Install the extension directly to VSCode to enable the extension within the GUI. Working with data sets and USS files from VSCode can be more convenient than using 3270 emulators, and complements your Zowe CLI experience. The extension provides the following benefits:

- Enables you to create, modify, rename, copy, and upload data sets directly to a z/OS mainframe.
- Enables you to create, modify, rename, and upload USS files directly to a z/OS mainframe.
- Provides a more streamlined way to access data sets, USS files and jobs.
- Lets you create, edit, and delete Zowe CLI zosmf compatible profiles.
- Lets you use the Secure Credential Store plug-in to store your credentials securely in the settings.

**Note:** Zowe Explorer is a subcomponent of Zowe. The extension demonstrates the potential for plug-ins powered by Zowe.

- Software Requirements
- Installing
- Configuration
- Relevant Information

# **Software Requirements**

Ensure that you meet the following prerequisites before you use the extension:

- Get access to z/OSMF.
- Install Node.js v8.0 or later.
- Install VSCode.
- Configure TSO/E address space services, z/OS data set, file REST interface, and z/OS jobs REST interface. For more information, see z/OS Requirements.

• Create one Zowe CLI zosmf profile so that the extension can communicate with the mainframe.

#### Notes:

i. You can use your existing Zowe CLI zosmf profiles that are created with the Zowe CLI v.2.0.0 or later.

ii. Zowe CLI zosmf profiles that are created in Zowe Explorer can be interchangeably used in the Zowe CLI.

### Installing

- 1. Address the software requirements.
- 2. Open VSCode, and navigate to the **Extensions** tab on the left-hand side of the UI.
- 3. Type **Zowe Explorer** in the search field.

Zowe Explorer appears in the list of extensions in the left-hand panel.

- 4. Click the green **Install** button to install the extension.
- 5. Restart VSCode.

The extension is now installed and available for use.

• Note: For information about how to install the extension from a VSIX file and run system tests on the extension, see the Developer README.

You can also watch the following videos to learn how to get started with Zowe Explorer, and work with data sets.

### Configuration

Configure Zowe Explorer in the settings file of the extension. To access the extension settings, navigate to **Manage (the gear icon)** > **Settings**, then select **Extensions** > **Zowe Explorer Settings**. For example, you can modify the following settings:

• Data set creation settings: You can change the default creation settings for various data set types.

#### Follow these steps:

- 1. Click the **Edit in settings.json** button under the Data Set, USS or JOBS settings that you want to edit.
- 2. Edit the settings as needed.
- 3. Save the settings.
- Set the Temporary Folder Location: You can change the default folder location where temporary files are stored.

#### Follow these steps:

- i. Click the **Edit in settings.json** button under the Data Set, USS or JOBS settings that you want to edit.
- ii. Modify the following definition:

where /path/to/directory is the folder location that you specify.

iii. Save the settings.

# **Relevant Information**

In this section you can find useful links and other relevant to Zowe Explorer information that can improve your experience with the extension. Check the following links:

- For information about how to develop for Eclipse Theia, see Theia README.
- For information about how to create a VSCode extension for Zowe Explorer, see VSCode extensions for Zowe Explorer.
- Visit the **#zowe-explorer** channel on Slack for questions and general guidance.

# **Zowe Explorer Profiles**

After you install Zowe Explorer, you need to have a Zowe Explorer profile to use all functions of the extension. You can optionally activate the Secure Credential Store plug-in to securely store your credentials.

# **Working with Zowe Explorer profiles**

You must have a **zosmf** compatible profile before you can use Zowe Explorer. You can set up a profile to retain your credentials, host, and port name. In addition, you can create multiple profiles and use them simultaneously.

#### Follow these steps:

- 1. Navigate to the explorer tree.
- 2. Click the + button next to the **DATA SETS**, **USS** or **JOBS** bar.

**Note:** If you already have a profile, select it from the drop-down menu.

3. Select the Create a New Connection to z/OS option.

**Note:** When you create a new profile, user name and password fields are optional. However, the system will prompt you to specify your credentials when you use the new profile for the first time.

4. Follow the instructions, and enter all required information to complete the profile creation.

You successfully created a Zowe CLI zosmf profile. Now you can use all the functionalities of the extension.

If you need to edit a profile, right-click the profile and select **Update Profile** option.

In addition, you can hide a profile from the explorer tree, and permanently delete a profile. When you delete your profile permanently, the extension erases the profile from the .zowe folder. To hide or delete a profile, right-click the profile and choose one of the respective options from the list.

#### **Profile Validation**

Zowe Explorer includes the profile validation feature that helps to ensure that z/OSMF is accessible and ready for use. If a profile is valid, the profile is active and can be used. By default, the feature is automatically enabled. You can disable the feature by right-clicking on your profile and selecting the **Disable Validation for Profile** option. Alternatively, you can enable or disable the feature for all profiles in the VS Code settings.

Follow these steps:

- 1. Navigate to the VS Code settings.
- 2. Open Zowe Explorer Settings.
- 3. Enable or disable the automatic validation of profiles option.
- 4. Restart VS Code.

### Associate Profile

Extensions built on Zowe Explorer provide users with additional functionality through unique profile types, such as RSE or FTP. The "associate profiles" function allows users to link, or associate, these extension profile types with an existing zOSMF profile. Every Zowe Explorer profile has two types of association: primary and secondary. While the primary association is **zosmf**, the secondary association includes Zowe CLI plug-ins or other services you might have. Within the scope of their own extender package, associated profiles can be used to access a relevant REST API that is available to the extender.

Create a secondary association for your Zowe Explorer profiles.

#### Follow these steps:

- 1. Navigate to the explorer tree.
- 2. Right-click your profile
- 3. Select the **Associate profiles** option.
- 4. Select a secondary profile type.
- 5. Select a file name you want to create an association for.

You have successfully created the secondary association for your Zowe Explorer profile.

For more information, see Associating Zowe CLI Profiles.

### **Enabling Secure Credential Store with Zowe Explorer**

Store your credentials securely by using the Secure Credential Store (SCS) plug-in in Zowe Explorer. By default, your credentials are stored in plain text.

Activate the SCS plug-in in Zowe Explorer.

#### Follow these steps:

- 1. Open Zowe Explorer.
- 2. Navigate to the VSCode settings.
- 3. Open Zowe Explorer Settings.
- 4. Add the **Zowe-Plugin** value to the Zowe Security: Credential Key entry field.
- 5. Restart VSCode.
- 6. Create a profile.

Your Zowe Explorer credentials are now stored securely.

#### For Zowe CLI users

Ensure that you install the SCS plug-in for Zowe CLI before activating SCS in Zowe Explorer. For more information about the SCS plug-in for Zowe CLI, see Secure Credential Store plug-in for Zowe Explorer.

**Important:** If you did not install the SCS plug-in for Zowe CLI and try to activate SCS in the extension, you will not be able to use your existing profiles, and will have to recreate them.

Activate the SCS plug-in in Zowe Explorer.

- 1. Open Zowe CLI and issue the following command:
- 2. Open Zowe Explorer.
- 3. Navigate to the VSCode settings.
- 4. Open Zowe Explorer Settings.
- 5. Add the **Zowe-Plugin** value to the Zowe Security: Credential Key entry field.
- 6. Restart VSCode.

The credentials of your newly created or existing profiles are now stored securely.

# **Use Base Profile and Token with Existing Profiles**

As a Zowe user, you can leverage the base profile functionality to access multiple services through Single Sign-on. Base profiles enable you to authenticate via Zowe API Mediation Layer. You can use base profiles with more than one service profile. For more information, see Base Profiles.

Before you log in and connect your service profile, ensure that you have Zowe CLI v6.16 or higher installed.

#### Access services through API ML with SSO

Connect your service profile with a base profile and token.

#### Follow these steps:

- 1. Open Zowe CLI and run the following command: zowe auth login apiml.
- 2. Follow the instructions to complete the login process.

A local base profile is created that contains your token. For more information about the process, see Token Management.

- 3. Run Zowe Explorer and click the + icon.
- 4. Select the profile you use with your base profile with the token.

The profile appears in the tree and you can now use this profile to access z/OSMF via the API Mediation Layer.

For more information, see Integrating with API Mediation Layer.

#### Log in to the Authentication Service

If the token for your base profile is no longer valid, you can log in again to get a new token with the **Log in to Authentication Service** feature.

#### Notes:

- The feature is only available for base profiles.
- The feature supports only API Mediation Layer at the moment. Other extenders may use a different authentication service.

#### Follow these steps:

- 1. Open Zowe Explorer.
- 2. Right-click your profile.
- 3. Select the Log in to Authentication Service option.

You will be prompted to enter your username and password beforehand.

The token is stored in the default base profile .yaml file.

If you do not want to store your token, request from the server to end the session of your token. Use the **Log out from Authentication Service** feature to invalidate the token.

#### Follow these steps:

- 1. Open Zowe Explorer.
- 2. Right-click your profile.
- 3. Select the Log out from Authentication Service option.

Your token has been successfully invalidated.

# **Configuring Zowe Application Framework**

After you install Zowe<sup>™</sup>, you can optionally configure the Zowe Application Framework as a Mediation Layer client, configure connections for the terminal application plug-ins, or modify the Zowe Application Server and Zowe System Services (ZSS) configuration, as needed.

# Configuring the framework as a Mediation Layer client

For simpler Zowe administration and better security, you can install an instance of the Zowe Application Framework as an API Mediation Layer client.

This configuration is simpler to administer because the framework servers are accessible externally through a single port. It is more secure because you can implement stricter browser security policies for accessing cross-origin content.

You must use SSL certificates to configure the Zowe Application Server to communicate with the SSLenabled Mediation Layer. Those certificates were created during the Zowe installation process, and are located in the \$RUNTIME\_DIR/components/app-server/share/zlux-appserver/defaults/serverConfig directory.

#### Enabling the Application Server to register with the Mediation Layer

When you install Zowe v1.8.0 or later, the Application Server automatically registers with the Mediation Layer.

For earlier releases, you must register the Application Server with the Mediation Layer manually. Refer to previous release documentation for more information.

#### Accessing the Application Server

**Note:** Before Accessing the Application Server, first create and configure the Zowe instance directory.

To access the Application Server through the Mediation Layer, use the Mediation Layer gateway server hostname and port. For example, when accessed directly, this is Zowe Desktop URL:

https://<appservername\_port>/ZLUX/plugins/org.zowe.zlux.bootstrap/web/index.html

The port number for the Zowe Desktop is the value of the ZOWE\_ZLUX\_SERVER\_HTTPS\_PORT variable in the instance.env file in the instance directory, see Creating and configuring the Zowe instance directory.

When accessed through the API Mediation Layer, this is the Zowe Desktop URL:

https://<gwsname\_port>/ui/v1/zlux/ZLUX/plugins/org.zowe.zlux.bootstrap/web/index
.html

The port number for the API Mediation Layer is the value of the GATEWAY\_PORT variable in the instance.env file in the instance directory.

# Setting up terminal application plug-ins

Follow these optional steps to configure the default connection to open for the terminal application plug-ins.

### Setting up the TN3270 mainframe terminal application plug-in

\_defaultTN3270.json is a file in tn3270-ng2/, which is deployed during setup. Within this file, you can specify the following parameters to configure the terminal connection:

### Setting up the VT Terminal application plug-in

\_defaultVT.json is a file in vt-ng2/, which is deployed during setup. Within this file, you can specify the following parameters to configure the terminal connection:

# **Configuration file**

The Zowe App Server and ZSS rely on many required or optional parameters to run, which includes setting up networking, deployment directories, plugin locations, and more.

For convenience, the Zowe Application Server and ZSS read from a JSON file with a common structure. ZSS reads this file directly as a startup argument, while the Zowe Application Server (as defined in the zlux-server-framework repository) accepts several parameters. The parameters are intended to be read from a JSON file through an implementer of the server, such as the example in the zlux-app-server repository (the lib/zluxServer.js file). The file accepts a JSON file that specifies most, if not all, of the parameters needed. Other parameters can be provided through flags, if needed.

For an instance, the configuration file is located at and can be edited at

\$INSTANCE\_DIR/workspace/app-server/serverConfig/server.json. The defaults from which that file is generated are located at \$RUNTIME\_DIR/components/app-server/share/zlux-appserver/defaults/serverConfig/server.json

Note: All examples are based on the *zlux-app-server* repository defaults.

# **Network configuration**

**Note:** The following attributes are to be defined in the server's JSON configuration file.

The App Server can be accessed over HTTP and/or HTTPS, provided it has been configured for either.

### HTTP

To configure the server for HTTP, complete these steps:

- 1. Define an attribute *http* within the top-level *node* attribute.
- 2. Define *port* within *http*. Where *port* is an integer parameter for the TCP port on which the server will listen. Specify 80 or a value between 1024-65535.

### HTTPS

For HTTPS, specify the following parameters:

- 1. Define an attribute *https* within the top-level *node* attribute.
- 2. Define the following within *https*:
- *port*: An integer parameter for the TCP port on which the server will listen. Specify 443 or a value between 1024-65535.
- *certificates*: An array of strings, which are paths to PEM format HTTPS certificate files.
- *keys*: An array of strings, which are paths to PEM format HTTPS key files.
- *pfx*: A string, which is a path to a PFX file which must contain certificates, keys, and optionally Certificate Authorities.
- certificateAuthorities (Optional): An array of strings, which are paths to certificate authorities files.

• *certificateRevocationLists* (Optional): An array of strings, which are paths to certificate revocation list (CRL) files.

**Note:** When using HTTPS, you must specify *pfx*, or both *certificates* and *keys*.

### **Network example**

In the example configuration, both HTTP and HTTPS are specified:

# **Configuration Directories**

When running, the App Server will access the server's settings and read or modify the contents of its resource storage. All of this data is stored within a hierarchy of folders which correspond to scopes:

- Product: The contents of this folder are not meant to be modified, but used as defaults for a product.
- Site: The contents of this folder are intended to be shared across multiple App Server instances, perhaps on a network drive.
- Instance: This folder represents the broadest scope of data within the given App Server instance.
- Group: Multiple users can be associated into one group, so that settings are shared among them.
- User: When authenticated, users have their own settings and storage for the Apps that they use.

These directories dictate where the Configuration Dataservice will store content.

### **Directories example**

### **Old defaults**

Prior to Zowe release 1.8.0, the location of the configuration directories were initialized to be within the zlux-app-server folder unless otherwise customized. 1.8.0 has backwards compatibility for the existence of these directories, but they can and should be migrated to take advantage of future enhancements.

Folder	New Location	Old Location	
--------	--------------	--------------	--

Folder	New Location	Old Location	
productDir	zlux-app-server/defaults	zlux-app-server/deploy/product	Official insta server within <runtime_ server/share</runtime_ 
siteDir	<instance_dir>/workspace/app- server/site</instance_dir>	zlux-app-server/deploy/site	INSTANCE_I otherwise de within instan SITE_DIR as
instanceDir	<instance_dir>/workspace/app- server</instance_dir>	zlux-app-server/deploy/instance	
groupsDir	<instance_dir>/workspace/app- server/groups</instance_dir>	zlux-app- server/deploy/instance/groups	
usersDir	<instance_dir>/workspace/app- server/users</instance_dir>	zlux-app- server/deploy/instance/users	
pluginsDir	<instance_dir>/workspace/app- server/plugins</instance_dir>	zlux-app- server/deploy/instance/ZLUX/plugins	Defaults loca server/defau at zlux-app-:

### **Application plug-in configuration**

This topic describes application plug-ins that are defined in advance.

In the configuration file, you can specify a directory that contains JSON files, which tell the server what application plug-in to include and where to find it on disk. The backend of these application plug-ins use the server's plug-in structure, so much of the server-side references to application plug-ins use the term *plug-in*.

To include application plug-ins, define the location of the plug-ins directory in the configuration file, through the top-level attribute **pluginsDir**.

**Note:** In this example, the directory for these JSON files is the Application Server defaults. However, in an instance of Zowe it is best to provide a folder unique to that instance – usually **\$INSTANCE\_DIR/workspace/app-server/plugins**.

### **Plug-ins directory example**

# Logging configuration

For more information, see Logging Utility.

# **ZSS** configuration

Running ZSS requires a JSON configuration file that is similar or the same as the one used for the Zowe Application Server. The attributes that are needed for ZSS, at minimum, are:*productDir*, *siteDir*, *instanceDir*, *groupsDir*, *usersDir*, *pluginsDir* and *agent.http.port*. All of these attributes have the same meaning as described above for the server, but if the Zowe Application Server and ZSS are not run from the same location, then these directories can be different.

Attributes that control ZSS are in the agent object. For example, *agent.http.port* is the TCP port that ZSS will listen on to be contacted by the App Server. Define this in the configuration file as a value between 1024-65535. Similarly, if specified, *agent.http.ipAddresses* will be used to determine which IP addresses the server should bind to. Only the first value of the array is used. It can either be a hostname or an ipv4 address.

Example of the agent body:

### **Connecting App Server to ZSS**

When running the App Server, simply specify a few flags to declare which ZSS instance the App Server will proxy ZSS requests to:

- -h: Declares the host where ZSS can be found. Use as "-h \<hostname>"
- -P: Declares the port at which ZSS is listening. Use as "-P \<port>"

### **Configuring ZSS for HTTPS**

To secure ZSS communication, you can use Application Transparent Transport Layer Security (AT-TLS) to enable Hyper Text Transfer Protocol Secure (HTTPS) communication with ZSS.

Before you begin, you must have a basic knowledge of your security product, e.g. RACF, and AT-TLS, and you must have Policy Agent configured. For more information on AT-TLS and Policy Agent, see the z/OS Knowledge Center.

You must have the authority to alter security definitions related to certificate management, and you must be authorized to work with and update the Policy Agent.

To configure HTTPS communication between ZSS and the Zowe App Server, you need a key ring which contains the ZSS server certificate and its Certificate Authority (CA) certificate. You can use an internal CA to create the ZSS server certificate, or you can buy the ZSS server certificate from a well-known commercial Certificate Authority. Next you define an AT-TLS rule which points to the key ring used by the ZSS server. Then you copy the CA certificate to the Zowe App Server key store and update the Zowe App Server configuration file.

**Note:** Bracketed values below (including the brackets) are variables. Replace them with values relevant to your organization. Always use the same value when substituting a variable that occurs multiple times.

#### Creating certificates and key ring for the ZSS server using RACF

In this step you will create a root CA certificate and a ZSS server certificate signed by the CA certificate. Next you create a key ring owned by the ZSS server with the certificates attached.

Key variables:

Variable	Value
[ca_common_name]	
[ca_label]	
[server_userid]	
[server_common_name]	
[server_label]	

Variable	Value
[ring_name]	
[output_dataset_name]	

#### Note:

- [server\_userid] must be the ZSS server user ID.
- [server\_common\_name] must be the ZSS server host name.
- 1. Enter the following RACF command to generate a CA certificate:
- 2. Enter the follow RACF command to generate a server certificate signed by the CA certificate:
- 3. Enter the following RACF commands to create a key ring and connect the certificates to the key ring:
- 4. Enter the following RACF command to refresh the DIGTRING and DIGTCERT classes to activate your changes:
- 5. Enter the following RACF commands to verify your changes:
- 6. Enter the following RACF commands to allow the ZSS server to use the certificates. Only issue the RDEFINE commands if the profiles do not yet exist.

**Note**: These sample commands use the FACILTY class to manage certificate related authorizations. You can also use the RDATALIB class, which offers granular control over the authorizations.

7. Enter the following RACF command to export the CA certificate to a dataset so it can be imported by the Zowe App Server:

#### Defining the AT-TLS rule

To define the AT-TLS rule, use the sample below to specify values in your AT-TLS Policy Agent Configuration file:

#### Configuring the Zowe App Server for HTTPS communication with ZSS

Copy the CA certificate to the ZSS server. Then in the Zowe App Server configuration file, specify the location of the certificate, and add a parameter to specify that ZSS uses AT-TLS.

- 1. Enter the following command to copy the CA certificate to the correct location in UNIX System Services (USS):
- 2. In the [INSTANCE\_DIR]/workspace/app-server/serverConfig directory, open the server.json file.
- 3. In the **node.https.certificateAuthorities** object, add the CA certificate file path, for example:
- 4. In the **agent.http** object add the key-value pair "attls": true, for example:

### Installing additional ZSS instances

After you install Zowe, you can install and configure additional instances of ZSS on the same z/OS server. You might want to do this to test different ZSS versions.

The following steps assume you have installed a Zowe runtime instance (which includes ZSS), and that you are installing a second runtime instance to install an additional ZSS.

1. To stop the installed Zowe runtime, in SDSF enter the following command:

Where ZOWE\_PREFIX and ZOWE\_INSTANCE are specified in your configuration (and default to ZWE and 1)

2. Create a new Zowe instance directory by following steps in Creating and configuring the Zowe instance directory.

**Note:** In the **instance.env** configuration file, specify ports that are not used by the first Zowe runtime.

3. To restart the first Zowe runtime, in SDSF enter the following command:

Where **\$INSTANCE\_DIR** is the Zowe instance directory.

- 4. To specify a name for the new ZSS instance, follow these steps:
  - i. Copy the PROCLIB member JCL named ZWESISTC that was installed with the new runtime.
  - ii. Rename the copy to uniquely identify it as the JCL that starts the new ZSS, for example ZWESIS02.
  - iii. Edit the JCL, and in the NAME parameter specify a unique name for the cross-memory server, for example:

Where ZWESIS\_MYSRV is the unique name of the new ZSS.

- 5. To start the new ZSS, in SDSF enter the following command:
- 6. Make sure that the TSO user ID that runs the first ZSS started task also runs the new ZSS started task. The default ID is ZWESVUSR.
- 7. In the new ZSS server.json configuration file, add a "privilegedServerName" parameter and specify the new ZSS name, for example:

```
Note: The instance location of server.json is $INSTANCE_DIR/workspace/app-
server/serverConfig/server.json, and the defaults are stored in
$R00T_DIR/components/app-server/share/zlux-app-
server/defaults/serverConfig/server.json
```

- 8. To start the new Zowe runtime, in SDSF enter the following command:
- 9. To verify that the new cross-memory server is being used, check for the following messages in the ZWESVSTC server job log:

ZIS status - 0k (name='ZWESIS\_MYSRV ', cmsRC=0, description='0k', clientVersion=2)

#### **Configuring AT-TLS on Client System**

When connecting to a Zowe instance whose host system is configured to use AT-TLS for HTTPS, the connecting client/client system must also define an outbound AT-TLS rule. To define the AT-TLS rule, use the sample below to specify values in your AT-TLS Policy Agent Configuration file:

**Note:** [client\_key\_ring] is a key ring containing the client certificate. To retrieve a signed client certificate, contact the administrator of the host system.

### **Controlling access to applications**

You can control which applications are accessible (visible) to all Zowe desktop users, and which are accessible only to individual users. For example, you can make an application that is under development only visible to the team working on it.

You control access by editing JSON files that list the apps. One file lists the apps all users can see, and you can create a file for each user. When a user logs into the desktop, Zowe determines the apps that user can see by concatenating their list with the all users list.

You can also control access to the JSON files. The files are accessible directly on the file system, and since they are within the configuration dataservice directories, they are also accessible via REST API. We recommend that only Zowe administrators be allowed to access the file system locations, and you control that by setting the directories and their contents to have file permissions on z/OS that only allow the Zowe admin group read & write access. You control who can read and edit the JSON files through the REST API by controlling who can access the configuration dataservice objects URLs that serve the JSON files.

### Controlling application access for all users

- 1. Open the Zowe Application Server configuration JSON file. By default, the file is in the following location:
- 2. To enable RBAC, in the dataserviceAuthentication object add the object: "rbac": true
- 3. Navigate to the following location:
- 4. Copy the allowedPlugins.json file and paste it in the following location:
- 5. Open the copied allowedPlugins.json file and perform either of the following steps:
  - To an application unavailable, delete it from the list of objects.
  - To make an application available, copy an existing plugin object and specify the application's values in the new object. Identifier and version attributes are required.
- 6. Restart the app server.

### Controlling application access for individual users

- 1. Open the Zowe Application Server configuration JSON file. By default, the file is in the following location:
- 2. To enable RBAC, in the dataserviceAuthentication object add the object: "rbac": true
- 3. In the user's ID directory path, in the \pluginStorage directory, create

\org.zowe.zlux.bootstrap\plugins directories. For example:

- 4. In the /plugins directory, create an allowedPlugins.json file. You can use the default allowedPlugins.json file as a template by copying it from the following location:
- 5. Open the allowedPlugins.json file and specify applications that user can access. For example:

#### Notes:

- Identifier and version attributes are required.
- When a user logs in to the desktop, Zowe determines which apps they can see by concatenating the list of apps available to all users with the apps available to the individual user.
- 6. Restart the app server.

# **Controlling access to dataservices**

To apply role-based access control (RBAC) to dataservice endpoints, you must enable RBAC for Zowe, and then use a z/OS security product such as RACF to map roles and authorities to the endpoints. After you apply RBAC, Zowe checks authorities before allowing access to the endpoints.

You can apply access control to Zowe endpoints and to your application endpoints. Zowe provides endpoints for a set of configuration dataservices and a set of core dataservices. Applications can use configuration endpoints to store and their own configuration and other data. Administrators can use core endpoints to get status information from the Application Framework and ZSS servers. Any dataservice added as part of an application plugin is a service dataservice.

### **Defining the RACF ZOWE class**

If you use RACF security, take the following steps define the ZOWE class to the CDT class:

- 1. Make sure that the CDT class is active and RACLISTed.
- 2. In TSO, issue the following command:

If you receive the following message, ignore it:

- 3. In TSO, issue the following command to refresh the CDT class:
- 4. In TSO, issue the following command to activate the ZOWE class:

For more information RACF security administration, see the IBM Knowledge Center at https://www.ibm.com/support/knowledgecenter/.

### **Enabling RBAC**

By default, RBAC is disabled and all authenticated Zowe users can access all dataservices. To enable RBAC, follow these steps:

- 1. Open the Zowe Application Server configuration JSON file. In the a server instance, the configuration file is **\$INSTANCE\_DIR/workspace/app-server/serverConfig/server.json**.
- 2. In the dataserviceAuthentication object, add "rbac": true.

### **Creating authorization profiles**

For users to access endpoints after you enable RBAC, in the ZOWE class you must create System Authorization Facility (SAF) profiles for each endpoint and give users READ access to those profiles.

Endpoints are identified by URIs in the following format:

/<product>/plugins/<plugin\_id>/services/<service>/<version>/<path>

For example:

/ZLUX/plugins/org.zowe.foo/services/baz/\_current/users/fred

Where the path is /users/fred.

SAF profiles have the following format:

```
<product>.<instance_id>.<service>.<pluginid_with_underscores>.<service>.<HTTP_method>.<url_with_forward_slashes_replaced_by_periods>
```

For example, to issue a POST request to the dataservice endpoint documented above, users must have READ access to the following profile:

#### ZLUX.DEFAULT.SVC.ORG\_ZOWE\_F00.BAZ.POST.USERS.FRED

For configuration dataservice endpoint profiles use the service code CFG. For core dataservice endpoints use COR. For all other dataservice endpoints use SVC.

### **Creating generic authorization profiles**

Some endpoints can generate an unlimited number of URIs. For example, an endpoint that performs a DELETE action on any file would generate a different URI for each file, and users can create an unlimited number of files. To apply RBAC to this type of endpoint you must create a generic profile, for example:

#### ZLUX.DEFAULT.COR.ORG\_ZOWE\_F00.BAZ.DELETE.\*\*

You can create generic profile names using wildcards, such as asterisks (\*). For information on generic profile naming, see IBM documentation.

#### **Configuring basic authorization**

The following are recommended for basic authorization:

- To give administrators access to everything in Zowe, create the following profile and give them UPDATE access to it: ZLUX.\*\*
- To give non-administrators basic access to the site and product, create the following profile and give them READ access to it: ZLUX.\*.ORG\_ZOWE\_\*
- To prevent non-administrators from configuring endpoints at the product and instance levels, create the following profile and do not give them access to it: ZLUX.DEFAULT.CFG.\*\*
- To give non-administrators all access to user, create the following profile and give them UPDATE access to it: ZLUX.DEFAULT.CFG.\*.\*.USER.\*\*

#### **Endpoint URL length limitations**

SAF profiles cannot contain more than 246 characters. If the path section of an endpoint URL is long enough that the profile name exceeds the limit, the path is trimmed to only include elements that do not exceed the limit. To avoid this issue, we recommend that application developers maintain relatively short endpoint URL paths.

For information on endpoint URLs, see Dataservice endpoint URL lengths and RBAC

### **Multi-factor authentication configuration**

Multi-factor authentication is an optional feature for Zowe.

As of Zowe version 1.8.0, the Zowe App Framework, Desktop, and all apps present in the SMP/E or convenience builds support out-of-band MFA by entering an MFA assigned token or passcode into password field of the Desktop login screen, or by accessing the app-server /auth REST API endpoint.

For a list of compatible MFA products, see Known compatible MFA products.

### Session duration and expiration

After successful authentication, a Zowe Desktop session is created by authentication plugins.

The duration of the session is determined by the plugin used. Some plugins are capable of renewing the session prior to expiration, while others may have a fixed session length.

Zowe is bundled with a few of these plugins:

- **apiml-auth**: Calls the Zowe API Mediation Layer from the app-server for authentication. By default, the Mediation Layer calls z/OSMF to answer the authentication request. The session created mirrors the z/OSMF session.
- **zosmf-auth**: Calls z/OSMF auth from the app-server to answer the authentication request. The created z/OSMF session is valid for about 8 hours.
- **zss-auth**: Calls Zowe ZSS from the app-server to answer the authentication request. The created ZSS session is valid for 1 hour, but is renewable on request prior to expiration. In the Desktop, the session is automatically renewed if the user is detected as active. If the user is detected as idle, the session will expire.

When a session expires, the credentials used for the initial login are likely to be invalid for re-use, since MFA credentials are often one-time-use or time-based.

In the Desktop, Apps that you opened prior to expiration will remain open so that your work can resume after entering new credentials.

### Configuration

When you use the default Zowe SMP/E or convenience build configuration, you do not need to change Zowe to get started with MFA.

To configure Zowe for MFA with a configuration other than the default, take the following steps:

- 1. Choose an App Server security plugin that is compatible with MFA. The apiml-auth, zss-auth, and zosmf-auth plugins are all compatible.
- 2. Locate the App Server's configuration file in \$INSTANCE\_DIR/workspace/appserver/serverConfig/server.json
- 3. Edit the configuration file to modify the section dataserviceAuthentication.
- 4. Set defaultAuthentication to the same category as the plugin of choice, for example:
  - apiml-auth: "apiml"
  - zosmf-auth: "zosmf"
  - **zss-auth**: "zss"
- 5. Define the plugins to use in the configuration file by adding a section for the chosen category within dataserviceAuthentication.implementationDefaults as an object with the attribute plugins, which is an array of plugin ID strings, where the plugins each have the following IDs:
  - **apiml-auth**: "org.zowe.zlux.auth.apiml"
  - **zosmf-auth**: "org.zowe.zlux.auth.zosmf"
  - **zss-auth**: "org.zowe.zlux.auth.zss"

The following is an example configuration for zss-auth, as seen in a default installation of Zowe:

# **Enabling tracing**

To obtain more information about how a server is working, you can enable tracing within the server.json file.

For example:

Specify the following settings inside the **logLevels** object.

All settings are optional.

#### **Zowe Application Server tracing**

To determine how the Zowe Application Server (zlux-app-server) is working, you can assign a logging level to one or more of the pre-defined logger names in the server.json file.

The log prefix for the Zowe Application Server is **\_zsf**, which is used by the server framework. (Applications and plug-ins that are attached to the server do not use the **\_zsf** prefix.)

The following are the logger names that you can specify:

**\_zsf.bootstrap** Logging that pertains to the startup of the server.

**\_zsf.auth** Logging for network calls that must be checked for authentication and authorization purposes.

**\_zsf.static** Logging of the serving of static files (such as images) from an application's /web folder.

\_zsf.child Logging of child processes, if any.

**\_zsf.utils** Logging for miscellaneous utilities that the server relies upon.

**\_zsf.proxy** Logging for proxies that are set up in the server.

**\_zsf.install** Logging for the installation of plug-ins.

**\_zsf.apiml** Logging for communication with the api mediation layer.

\_zsf.routing Logging for dispatching network requests to plug-in dataservices.

\_zsf.network Logging for the HTTPS server status (connection, ports, IP, and so on)

#### Log levels

The log levels are:

- SEVERE = 0,
- WARNING = 1,
- INFO = 2,
- FINE = 3,
- FINER = 4,
- FINEST = 5

FINE, FINER, and FINEST are log levels for debugging, with increasing verbosity.

### **Enabling tracing for ZSS**

To increase logging for ZSS, you can assign a logging level (an integer value greater than zero) to one or more of the pre-defined logger names in the server.json file.

A higher value specifies greater verbosity.

The log prefix for ZSS is **\_zss**. The following are the logger names that you can specify:

**\_zss.traceLevel:** Controls general server logging verbosity.

**\_zss.fileTrace:** Logs file serving behavior (if file serving is enabled).

**\_zss.socketTrace:** Logs general TCP Socket behavior.

**\_zss.httpParseTrace:** Logs parsing of HTTP messages.

**\_zss.httpDispatchTrace:** Logs dispatching of HTTP messages to dataservices.

**\_zss.httpHeadersTrace:** Logs parsing and setting of HTTP headers.

\_zss.httpSocketTrace: Logs TCP socket behavior for HTTP.

**\_zss.httpCloseConversationTrace:** Logs HTTP behavior for when an HTTP conversation ends.

\_zss.httpAuthTrace: Logs behavior for session security.

When you are finished specifying the settings, save the server.json file.

# **Zowe Application Framework logging**

The Zowe Application Framework log files contain processing messages and statistics. The log files are generated in the following default locations:

- Zowe Application Server: \$INSTANCE\_DIR/logs/appServer-yyyy-mm-dd-hh-mm.log
- ZSS: \$INSTANCE\_DIR/logs/zssServer-yyyy-mm-dd-hh-mm.log

The logs are timestamped in the format yyyy-mm-dd-hh-mm and older logs are deleted when a new log is created at server startup.

### **Controlling the logging location**

The log information is written to a file and to the screen. (On Windows, logs are written to a file only.)

#### ZLUX\_NODE\_LOG\_DIR and ZSS\_LOG\_DIR environment variables

To control where the information is logged, use the environment variable *ZLUX\_NODE\_LOG\_DIR*, for the Zowe Application Server, and *ZSS\_LOG\_DIR*, for ZSS. While these variables are intended to specify a directory, if you specify a location that is a file name, Zowe will write the logs to the specified file instead (for example: /dev/null to disable logging).

When you specify the environment variables *ZLUX\_NODE\_LOG\_DIR* and *ZSS\_LOG\_DIR* and you specify directories rather than files, Zowe will timestamp the logs and delete the older logs that exceed the *ZLUX\_NODE\_LOGS\_TO\_KEEP* threshold.

#### ZLUX\_NODE\_LOG\_FILE and ZSS\_LOG\_FILE environment variables

If you set the log file name for the Zowe Application Server by setting the *ZLUX\_NODE\_LOG\_FILE* environment variable, or if you set the log file for ZSS by setting the *ZSS\_LOG\_FILE* environment variable, there will only be one log file, and it will be overwritten each time the server is launched.

**Note**: When you set the *ZLUX\_NODE\_LOG\_FILE* or *ZSS\_LOG\_FILE* environment variables, Zowe will not override the log names, set a timestamp, or delete the logs.

If the directory or file cannot be created, the server will run (but it might not perform logging properly).

#### **Retaining logs**

By default, the last five logs are retained. To specify a different number of logs to retain, set *ZLUX\_NODE\_LOGS\_TO\_KEEP* (Zowe Application Server logs) or *ZSS\_LOGS\_TO\_KEEP* (ZSS logs) to the number of logs that you want to keep. For example, if you set *ZLUX\_NODE\_LOGS\_TO\_KEEP* to 10, when the eleventh log is created, the first log is deleted.

### Administering the servers and plugins using an API

You can use a REST API to retrieve and edit Zowe Application Server and ZSS server configuration values, and list, add, update, and delete plugins. If an administrator has configured Zowe to use RBAC, they must authorize you to access the endpoints.

The API returns the following information in a JSON response:

API	Description
/server (GET)	Returns a list of accessible server endpoints for the Zowe Application Server.
/server/config (GET)	Returns the Zowe Application Server configuration from the zluxserver.json file.
/server/log (GET)	Returns the contents of the Zowe Application Server log file.
/server/loglevels (GET)	Returns the verbosity levels set in the Zowe Application Server logger.
/server/environment (GET)	Returns Zowe Application Server environment information, such as the operating system version, node server version, and process ID.
/server/reload (GET)	Reloads the Zowe Application Server. Only available in cluster mode.
/server/agent (GET)	Returns a list of accessible server endpoints for the ZSS server.
/server/agent/config (GET)	Returns the ZSS server configuration from the zluxserver.json file.
/server/agent/log (GET)	Returns the contents of the ZSS log file.
/server/agent/loglevels (GET)	Returns the verbosity levels of the ZSS logger.
/server/agent/environment (GET)	Returns ZSS environment information.
/server/config/:attrib (POST)	Specify values for server configuration attributes in the zluxserver.json file. You can change a subset of configuration values.

ΑΡΙ	Description
/server/logLevels/name/:componentName/level/:level (POST)	Specify the logger that you are using and a verbosity level.
/plugins (GET)	Returns a list of all plugins and their dataservices.
/plugins (PUT)	Adds a new plugin or upgrades an existing plugin. Only available in cluster mode.
/plugins/:id (DELETE)	Deletes a plugin. Only available in cluster mode.

Swagger API documentation is provided in the <RUNTIME\_DIR>/components/app-

server/share/zlux-app-server/doc/swagger/server-plugins-api.yaml file. To see it in HTML format, you can paste the contents into the Swagger editor at https://editor.swagger.io/.

**Note:** The "agent" end points interact with the agent specified in the server.json file. By default this is ZSS.

# **Configuring Zowe CLI**

This section explains how to configure Zowe CLI, such as changing log levels and setting the home directory location.

**Tip:** CLI configuration is stored on your computer in the directory C:\Users\user01\.zowe by default. The directory includes log files, profile information, and installed CLI plug-ins. When troubleshooting, refer to the logs in the imperative and zowe folders.

- Setting Zowe CLI log levels
- Setting the Zowe CLI home directory

### **Setting CLI log levels**

You can set the log level to adjust the level of detail that is written to log files:

**Important!** Setting the log level to TRACE or ALL might result in "sensitive" data being logged. For example, command line arguments will be logged when TRACE is set.

Environment Variable	Description	Values	Default
ZOWE_APP_LOG_LEVEL	Zowe CLI logging level	Log4JS log levels (OFF, TRACE, DEBUG, INFO, WARN, ERROR, FATAL)	DEBUG
ZOWE_IMPERATIVE_LOG_LEVEL	Imperative CLI Framework logging level	Log4JS log levels (OFF, TRACE, DEBUG, INFO, WARN, ERROR, FATAL)	DEBUG

### Setting the CLI home directory

You can set the location on your computer where Zowe CLI creates the *.zowe* directory, which contains log files, profiles, and plug-ins for the product:

Environment Variable	Description	Values	Default	
ZOWE_CLI_HOME	Zowe CLI home directory location	Any valid path on your computer	Your computer default home directory	

# **Configuring the Zowe APIs**

Review the security considerations for Zowe APIs and learn how to prevent the Denial of Service (DoS) attacks.

The default configuration before Zowe version 1.14.0 contains **Data sets and Unix files** and **Jobs** API microservices which might be vulnerable to DoS attacks in the form of slow https attacks. You can add additional configuration to the start script of these components in order to prevent resource starvation via slow https attacks.

- To update the configuration of the **Data sets and Unix files** component, modify the start.sh script within the runtime component directory /zowe/runtime/components/files-api/bin.
- To update the configuration of the **Jobs** component, modify the **start.sh** script within the runtime component directory /zowe/runtime/components/jobs-api/bin.

Ensure that the -Dserver.connection-timeout=8000 parameter is set. This parameter specifies how long the component waits to receive all the required information from the client that makes a request.

See a snippet of a configured start.sh script for the Jobs component as follows:

In version 1.14.0 and later, the preceding snippet reflects the default configuration.

# **Advanced Gateway features configuration**

As a system programmer who wants to configure advanced Gateway features of the API Mediation Layer, you can customize Gateway parameters by modifying either of the following files:

- <Zowe install directory>/components/gateway/bin/start-gateway.sh
- <Zowe instance directory>/instance.env

The parameters begin with the –D prefix, similar to all the other parameters in the file.

**Note:** Restart Zowe to apply changes to the parameter.

Follow the procedures in the following sections to customize Gateway parameters according to your preferences:

- Prefer IP Address for API Layer services
- SAF as an Authentication provider
- Enable Jwt token refresh endpoint
- Gateway retry policy
- Gateway client certificate authentication
- Gateway timeouts
- CORS handling
- Encoded slashes
- Connection limits
- Routed instance header
- Distributed load balancer cache
- Replace or remove catalog with another service
- API Mediation Layer as a standalone component
- SAF resource checking

### **Prefer IP Address for API Layer services**

API Mediation Layer services use the hostname when communicating with each other. This behavior can be changed so that the IP address is used instead.

#### Follow these steps:

- 1. Open the <Zowe instance directory>/instance.env configuration file.
- 2. Find the property APIML\_PREFER\_IP\_ADDRESS and set the value to true.
- 3. Restart Zowe&trade.

**Note:** Changing the value of this property might introduce problems with certificates. Ensure that the IP Address is present on the certificate SAN name.

### SAF as an Authentication provider

By default, the API Gateway uses z/OSMF as an authentication provider. It is possible to switch to SAF as the authentication provider instead of z/OSMF. The intended usage of SAF as an authentication provider is for systems without z/OSMF. If SAF is used and the z/OSMF is available on the system, the created tokens are not accepted by z/OSMF. Use the following procedure to switch to SAF.

### Follow these steps:

- 1. Open the <Zowe instance directory>/instance.env configuration file.
- 2. Find the property APIML\_SECURITY\_AUTH\_PROVIDER and set the value to saf.
- 3. Restart Zowe&trade.

Authentication requests now utilize SAF as the authentication provider. API ML can run without z/OSMF present on the system.

### **Enable Jwt token refresh endpoint**

Enable the /gateway/api/v1/auth/refresh endpoint to exchange a valid JWT token for a new token with a new expiration date. Call the endpoint with a valid JWT token and trusted client certificate. In case of z/OSMF authentication provider, enable API Mediation Layer for passticket generation and configure z/OSMF APPLID. Configure Passtickets

#### Follow these steps:

- 1. Open the file <Zowe instance directory>/instance.env.
- 2. Configure the following properties:

### • APIML\_SECURITY\_ALLOWTOKENREFRESH=true

Add this property to enable the refresh endpoint.

### • APIML\_SECURITY\_ZOSMF\_APPLID

If you use z/OSMF as an authentication provider, provide a valid APPLID. The API ML generates a passticket for the specified APPLID and subsequently uses this passticket to authenticate to z/OSMF. The default value in the installation of z/OSMF is IZUDFLT.

3. Restart Zowe.

### Change password with SAF provider

Update the user password using the SAF Authentication provider. To use this functionality, add the parameter newPassword on the login endpoint /gateway/api/v1/auth/login. The Gateway service returns a valid JWT with the response code 204 as a result of successful password change. The user is then authenticated and can consume APIs through the Gateway. If it is not possible to change the password for any reason, the response code is 401.

Use a POST REST call against the URL /gateway/api/v1/auth/login:

**Note:** It is a common practice to set the limit for changing the password in the ESM. This value is set by the parameter **MINCHANGE** for **PASSWORD**. The password can be changed once. Subsequently, it is necessary to wait the specified time period before changing the password again.

### Example:

MINCHANGE=120

where:

• 120

Specifies the number of days before the password can be reset

### **Gateway retry policy**

### directory>/components/gateway/bin/start.sh file:

All requests are disabled as the default configuration for retry with one exception: the server retries **GET** requests that finish with status code **503**. To change this default configuration, include the following parameters:

### ribbon.retryableStatusCodes

Provides a list of status codes, for which the server should retry the request.

Example: -Dribbon.retryableStatusCodes="503, 404"

### • ribbon.OkToRetryOnAllOperations

Specifies whether to retry all operations for this service. The default value is false. In this case, only GET requests are retried if they return a response code that is listed in ribbon.retryableStatusCodes. Setting this parameter to true enables retry requests for all methods which return a response code listed in ribbon.retryableStatusCodes.

Note: Enabling retry can impact server resources due to request body buffering.

### • ribbon.MaxAutoRetries

Specifies the number of times a failed request is retried on the same server. This number is multiplied with ribbon.MaxAutoRetriesNextServer. The default value is 0.

### ribbon.MaxAutoRetriesNextServer

Specifies the number of additional servers that attempt to make the request. This number excludes the first server. The default value is 5.

### **Gateway client certificate authentication**

Beginning with release 1.19 LTS, it is possible to authenticate using client certificates. The feature is functional and tested, but automated testing on various security systems is not complete. As such, the feature is provided as a beta release for early preview. If you would like to offer feedback using client certificate authentication, please create an issue against the api-layer repository. Client Certificate

authentication will move out of Beta once test automation is fully implemented across different security systems.

Use the following procedure to enable the feature to use a client certificate as the method of authentication for the API Mediation Layer Gateway.

### Follow these steps:

1. Open the <Zowe instance directory>/instance.env configuration file.

2. Configure the following properties:

### • APIML\_SECURITY\_X509\_ENABLED

This property is the global feature toggle. Set the value to true to enable client certificate functionality.

### • APIML\_SECURITY\_ZOSMF\_APPLID

When z/OSMF is used as an authentication provider, provide a valid APPLID to allow for client certificate authentication. The API ML generates a passticket for the specified APPLID and subsequently uses this passticket to authenticate to z/OSMF. The default value in the installation of z/OSMF is IZUDFLT.

**Note:** The following steps are only required if the ZSS hostname or default Zowe user name are altered:

3. Change the following property if user mapping is provided by an external API:

### • APIML\_GATEWAY\_EXTERNAL\_MAPPER

Note: Skip this step if user mapping is not provided by an external API.

The API Mediation Gateway uses an external API to map a certificate to the owner in SAF. This property informs the Gateway about the location of this API. ZSS is the default API provider in Zowe. You can provide your own API to perform the mapping. In this case, it is necessary to customize this value.

The following URL is the default value for Zowe and ZSS:

4. Add the following property if the Zowe runtime userId is altered from the default ZWESVUSR :

### • APIML\_GATEWAY\_MAPPER\_USER

Note: Skip this step if the Zowe runtime userId is not altered from the default ZWESVUSR.

To authenticate to the mapping API, a JWT is sent with the request. The token represents the user that is configured with this property. The user authorization is required to use the IRR.RUSERMAP resource within the FACILITY class. The default value is ZWESVUSR. Permissions are set up during installation with the ZWESECUR JCL or workflow.

If you customized the ZWESECUR JCL or workflow (the customization of zowe runtime user: // SET ZOWEUSER=ZWESVUSR \* userid for Zowe started task) and changed the default USERID, create the APIML\_GATEWAY\_MAPPER\_USER property and set the value by adding a new line as in the following example:

### Example:

5. Restart Zowe&trade.

### **Gateway timeouts**

Use the following procedure to change the global timeout value for the API Mediation Layer instance.

### Follow these steps:

- 1. Open the file <Zowe instance directory>/instance.env.
- 2. Find the property APIML\_GATEWAY\_TIMEOUT\_MILLIS, and set the value to the desired value.
- 3. Restart Zowe&trade.

If you require finer control, you can edit the <Zowe install

directory>/components/gateway/bin/start.sh, and modify the following properties:

• apiml.gateway.timeoutMillis

This property defines the global value for http/ws client timeout.

Add the following properties to the file for the API Gateway:

**Note:** Ribbon configures the client that connects to the routed services.

#### ribbon.connectTimeout

Specifies the value in milliseconds which corresponds to the period in which API ML should establish a single, non-managed connection with the service. If omitted, the default value specified in the API ML Gateway service configuration is used.

### • ribbon.readTimeout

Specifies the time in milliseconds of inactivity between two packets in response from this service to API ML. If omitted, the default value specified in the API ML Gateway service configuration is used.

### • ribbon.connectionManagerTimeout

The HttpClient employs a special entity to manage access to HTTP connections called by the HTTP connection manager. The purpose of an HTTP connection manager is to serve as a factory for new HTTP connections, to manage the life cycle of persistent connections, and to synchronize access to persistent connections. Internally, the connections that are managed serve as proxies for real connections. **ConnectionManagerTimeout** specifies a period during which managed connections with API ML should be established. The value is in milliseconds. If omitted, the default value specified in the API ML Gateway service configuration is used.

### **CORS** handling

You can enable the Gateway to terminate CORS requests for itself and also for routed services. By default, Cross-Origin Resource Sharing (CORS) handling is disabled for Gateway routes <code>api/v1/gateway/\*\*</code> and for individual services. After enabling the feature as stated in the prodecure below, API Gateway endpoints start handling CORS requests and individual services can control whether they want the Gateway to handle CORS for them through the Custom Metadata parameters.

When the Gateway handles CORS on behalf of the service, it sanitizes defined headers from the communication (upstream and downstream). Access-Control-Request-Method, Access-Control-Request-Headers, Access-Control-Allow-Origin, Access-Control-Allow-Methods, Access-Control-Allow-Headers, Access-Control-Allow-Credentials, Origin The resulting request to the service is not a CORS request and the service does not need to do anything extra. The list can be overridden by specifying different comma-separated list in the property APIML\_SERVICE\_IGNOREDHEADERSWHENCORSENABLED in <Zowe instance

directory>/instance.env

Additionally, the Gateway handles the preflight requests on behalf of the service, replying with CORS headers:

- Access-Control-Allow-Methods: GET, HEAD, POST, DELETE, PUT, OPTIONS
- Access-Control-Allow-Headers: origin, x-requested-with
- Access-Control-Allow-Credentials: true
- Access-Control-Allow-Origin: \* or a list of origins as configured by the service.

Use the following procedure to enable CORS handling.

### Follow these steps:

- 1. Open the file <Zowe instance directory>/instance.env.
- 2. Find the property APIML\_CORS\_ENABLED and set the value to true.
- 3. Restart Zowe&trade.

Requests through the Gateway now contain a CORS header.

### **Encoded** slashes

By default, the API Mediation Layer accepts encoded slashes in the URL path of the request. If you are onboarding applications which expose endpoints that expect encoded slashes, it is necessary to keep the default configuration. We recommend that you change the property to false if you do not expect the applications to use the encoded slashes.

Use the following procedure to reject encoded slashes.

### Follow these steps:

- 1. Open the file <Zowe instance directory>/instance.env.
- 2. Find the property APIML\_ALLOW\_ENCODED\_SLASHES and set the value to false.
- 3. Restart Zowe&trade.

Requests with encoded slashes are now rejected by the API Mediation Layer.

### **Connection limits**

By default, the API Gateway accepts up to 100 concurrent connections per route, and 1000 total concurrent connections. Any further concurrent requests are queued until the completion of an existing request. The API Gateway is built on top of Apache HTTP components that require these two connection limits for concurrent requests. For more information, see Apache documentation.

Use the following procedure to change the number of concurrent connections.

### Follow these steps:

- 1. Open the file <Zowe instance directory>/instance.env.
- 2. Find the property APIML\_MAX\_CONNECTIONS\_PER\_ROUTE and set the value to an appropriate positive integer.
- 3. Find the property APIML\_MAX\_TOTAL\_CONNECTIONS and set the value to an appropriate positive integer.

### **Routed instance header**

The API Gateway can output a special header that contains the value of the instance ID of the API service that the request has been routed to. This is useful for understanding which service instance is being called.

```
The header name is X-InstanceId, and the sample value is discoverable-
client:discoverableclient:10012. This is identical to instanceId property in the registration of
the Discovery service.
```

Use the following procedure to output a special header that contains the value of the instance ID of the API service.

### Follow these steps:

- 1. Open the file <Zowe instance directory>/instance.env.
- 2. Add the property with value APIML\_ROUTING\_INSTANCEIDHEADER=true.
- 3. Restart Zowe.

### **Distributed load balancer cache**

You can choose to distribute the load balancer cache between instances of the API Gateway. To distribute the load balancer cache, it is necessary that the caching service is running. Gateway service instances are

reuqired to have the same DN (Distinguished name) on the server certificate.

Use the following procedure to distribute the load balancer cache between instances of the API Gateway.

### Follow these steps:

- 1. Open the file <Zowe instance directory>/instance.env.
- 2. Add the property with value APIML\_LOADBALANCER\_DISTRIBUTE=true.
- 3. Restart Zowe.

### **Replace or remove the Catalog with another service**

By default, the API Mediation Layer contains API Catalog as a service showing available services. As the API Mediation Layer can be successfully run without this component it is possible to replace or remove the service from the Gateway home page and health checks. The following section describes the behavior of the Gateway home page and health checks.

The default option displays the API Catalog.

A value can also be applied to API\_GATEWAY\_CATALOG\_ID.

### **Examples:**

• none

Nothing is displayed on the Gateway home page and the Catalog is removed from /application/health

• alternative-catalog

An alternative to the API Catalog is displayed

metrics-dashboard

A possible dashboard that could appear in place of the API Catalog

### Notes:

• If the application contains the homePageUrl and statusPageRelativeUrl, then the full set of information is displayed.

- If the application contains the homePageUrl the link is displayed without the UP information.
- If the application contains the statusPageRelativeUrl then UP or DOWN is displayed based on the statusPage without the link.

Use the following procedure to change or replace the Catalog service.

### Follow these steps:

- 1. Open the file <Zowe instance directory>/instance.env.
- 2. At the end of the file with the property APIML\_GATEWAY\_CATALOG\_ID add a new line. Set the value with the following options:
  - Set the value to none to remove the Catalog service.
  - Set the value to the ID of the service that is onboarded to the API Mediation Layer.

### **API Mediation Layer as a standalone component**

You can start the API Mediation Layer independently of other Zowe components. By default, the Gateway, Zowe System Services, and Virtual Desktop start when Zowe runs. To limit consumed resources when the Virtual Desktop or Zowe System Services are not required, it is possible to specify which components start in the context of Zowe. No change is required during the installation process to support this setup.

Once Zowe is installed, use the following procedure to limit which components start.

#### Follow these steps:

- 1. Open the file <Zowe instance directory>/instance.env.
- 2. Find the property ZWE\_LAUNCH\_COMPONENTS and set discovery, gateway, api-catalog
- 3. Restart Zowe&trade .

To learn more about the related section of the environment file, see Creating and configuring the Zowe instance directory. We recommend you open this page in a new tab.

### **SAF Resource Checking**

The API ML can check for the authorization of the user on certain endpoints. Access to a SAF resource is checked with ESM.

Verification of the SAF resource is provided by the following three providers:

• endpoint

This is the highest priority provider, such as a REST endpoint call (ZSS or similar one). This option is disabled by default. In Zowe, ZSS has the API to check for SAF resource authorization.

• native

The Native JZOS classes from Java are used to determine SAF resource access. This is the default provider.

### • dummy

This is the lowest priority provider. This is the dummy implementation and is defined in a file.

**Note:** Verification of the SAF resource uses the first available provider based on the specified priority. The default configuration resolves to the native provider.

You can select a specific provider by specifying the APIML\_SECURITY\_AUTHORIZATION\_PROVIDER key in the instance.env file. Use the parameter value to strictly define a provider. If verification is disabled, select the endpoint option.

### Follow these steps:

- 1. Open the file <Zowe instance directory>/instance.env.
- 2. Add the property APIML\_SECURITY\_AUTHORIZATION\_PROVIDER and set desired value.
- 3. Restart Zowe&trade.

### Examples:

**Note:** To configure the endpoint provider, add the following additional property: APIML\_SECURITY\_AUTHORIZATION\_ENDPOINT\_ENABLED=true

To use the endpoint provider, customize the URL corresponding to the SAF resource authorization. By default, the ZSS API is configured and used.

### Follow these steps:

1. Open the file <Zowe instance directory>/instance.env.

2. Modify the property APIML\_SECURITY\_AUTHORIZATION\_ENDPOINT\_URL and set desired value. The default value for ZSS API is https://\${ZOWE\_EXPLORER\_HOST}:\${GATEWAY\_PORT}/zss/api/v1/saf-auth

3. Restart Zowe&trade.

### **Checking providers**

### **REST endpoint call**

The REST provider calls the external API to retrieve information about access rights. To enable the feature outside of the mainframe, such as when running in Docker, you can use a REST endpoint call using the GET method:

- Method: GET
- URL: {base path}/{userId}/{class}/{entity}/{level}
- Response:

**Note:** For more information about this REST endpoint call, see ZSS implementation.

### Native

The Native provider is the easiest approach to use the SAF resource checking feature on the mainframe.

Enable this provider when classes com.ibm.os390.security.PlatformAccessControl and com.ibm.os390.security.PlatformReturned are available on the classpath. This approach uses the following method described in the IBM documentation: method.

**Note:** Ensure that the version of Java on your system has the same version of classes and method signatures.

### **Dummy implementation**

The Dummy provider is for testing purpose outside of the mainframe.

Create the file saf.yml and locate it in the folder, where is application running or create file mocksaf.yml in the test module (root folder). The highest priority is to read the file outside of the JAR. A file (inner or outside) has to exist.

The following YAML presents the structure of the file:

#### Notes:

- Classes and resources are mapped into a map, user IDs into a list.
- The load method does not support formatting with dots, such as shown in the following example: **Example:** {CLASS}.{RESOURCE} Ensure that each element is separated.
- The field safAccess is not required to define an empty file without a definition.
- Classes and resources cannot be defined without the user ID list.
- When a user has multiple definitions of the same class and resource, only the most privileged access level loads.

# **API Gateway configuration parameters**

As an application developer who wants to change the default configuration of the API Mediation Layer, set the following parameters by modifying the <Zowe install directory>/components/gateway/bin/start.sh file:

- Runtime configuration
  - Environment variables
- Service configuration
- Zuul configuration
- Hystrix configuration
- AT-TLS

### **Runtime configuration**

This section describes runtime configuration properties.

• apiml.service.hostname

This property is used to set the API Gateway hostname.

• apiml.service.port

This property is used to set the API Gateway port.

• apiml.service.discoveryServiceUrls

This property specifies the Discovery Service URL used by the service to register to Eureka.

apiml.service.preferIpAddress

Set the value of this property to true to advertize a service IP address instead of its hostname.

### Notes:

If you set this property to true on the Discovery Service, ensure that you modify the value of discoveryLocations: to use the IP address instead of the hostname. Failure to modify the

discoveryLocations: value prevents Eureka from detecting registered services. As a result, the **available-replicas** is empty.

 Enabling this property may also cause issues with SSL certificates and Subject Alternative Name (SAN).

### • apiml.cache.storage.location

This property specifies the location of the EhCache used by Spring.

Note: It is necessary for the API ML process to have write access to the cache location.

### • apiml.security.ssl.verifySslCertificatesOfServices

This parameter makes it possible to prevent server certificate validation.

**Important!** Ensure that this parameter is set to true in production environments. Setting this parameter to false in production environments significantly degrades the overall security of the system.

### • apiml.security.auth.zosmfServiceId

This parameter specifies the z/OSMF service id used as authentication provider. The service id is defined in the static definition of z/OSMF. The default value is zosmf.

### • apiml.zoweManifest

This parameter lets you view the Zowe version by using the /version endpoint. To view the version requires setting up the launch parameter of the API Gateway - apiml.zoweManifest with a path to the Zowe build manifest.json file. This file is usually located in the root folder of Zowe build. If the encoding of manifest.json file is different from UTF-8 and IBM1047, ensure that you set up the launch parameter of API Gateway - apiml.zoweManifestEncoding with correct encoding.

**Note:** It is also possible to know the version of API ML and Zowe (if API ML used as part of Zowe), using the /api/v1/gateway/version endpoint in the API Gateway service in the following format:

### • apiml.security.auth.tokenProperties.expirationInSeconds

This property is relevant only when the JWT is generated by the API Mediation Layer. API ML generation of the JWT occurs in the following cases:

- z/OSMF is only available as an older version which does not support JWT tokens
- The SAF provider is used

To use a custom configuration for z/OSMF which changes the expiration of the LTPA token, it is necessary to also set the expiration in this parameter.

**Note:** The default value is 8 hours which mimicks the 8 hour default expiration of the LTPA token in *z*/OSMF.

#### Follow these steps:

- i. Open the file <Zowe install directory>/components/gateway/bin/start.sh.
- ii. Find the line that contains -cp \${ROOT\_DIR}"/components/gateway/gatewayservice.jar":/usr/include/java\_classes/IRRRacf.jar.
- iii. Before this line, add a new line in the following format:

where:

{expirationTimeInSeconds}

refers to the specific time before expiration

iv. Restart Zowe&trade.

#### • ibm.serversocket.recover

In a multiple network stack environment (CINET), when one of the stacks fails, no notification or Java<sup>™</sup> exception occurs for a Java program that is listening on an **INADDR\_ANY** socket. When new stacks become available, the Java application does not become aware of these stacks until the application rebinds the **INADDR** socket. By default, this parameter is enabled in the API Gateway. As a result, the **NetworkRecycledException** exception is thrown to the application to allow it to either fail or attempt to rebind. For more information, see the IBM documentation.

### • java.io.tmpdir

This property is a standard Java system property which is used by the disk-based storage policies. This property determines where the JVM writes temporary files, including those written by these storage policies. The default value is typically /tmp on Unix-like platforms.

#### • spring.profiles.include

This property can be used to unconditionally add active profiles. For more information, see the Spring documentation.

### server.maxTotalConnections and server.maxConnectionsPerRoute

These two properties are used to set the number of concurrent connections. Further connection requests that put the number of connections over either of these limits are queued until an existing connection completes. The API Gateway is built on top of Apache HTTP components that require these two connection limits for concurrent requests. For more information, see Apache documentation.

### **Environment variables**

You can add additional environment variables to store configuration properties for the API Mediation Layer.

**Note:** Use either dot separation, or the UPPER\_CASE naming convention when adding an additional environmental variable.

One use case for adding an environmental variable is to provide a label for a JWT secret. This secret is usually generated during Zowe installation. In some scenarios, however, users may want to use their own secret which is already created and labled differently. Use this procedure to use a customized secret.

### Follow the steps:

- 1. Open the file <Zowe instance directory>/instance.env.
- 2. Add a new line with the following property:

apiml.security.auth.jwtKeyAlias=<your\_jwtsecter\_label>.

where:

### • apiml.security.auth.jwtKeyAlias

is the label under which the secret is located. This secret is used to sign the JWT. This secret is stored in the keystore or keyring. The secret generated by the Zowe install script is stored under the default label jwtsecret.

### **Service configuration**

For information about service configuration parameters, see Onboarding a REST API service with the Plain Java Enabler (PJE).

### **Zuul configuration**

As a provider for routing and filtering, the API Gateway contains a Zuul configuration as shown in the following example.

### Example:

The Zuul configuration allows the API Gateway to act as a reverse proxy server through which API requests can be routed from clients on the northbound edge to z/OS servers on the southbound edge.

**Note:** For more information about Zuul configuration parameters, see the Spring Cloud Netflix documentation.

### Hystrix configuration

The API Gateway contains a Hystrix configuration as shown in the following example.

### Example:

Hystrix is a latency and fault tolerance library designed to isolate points of access to remote systems, services and third-party libraries, stop cascading failure, and enable resilience in complex distributed systems where failure is inevitable.

**Note:** For more information about Hystrix configuration parameters, see the Netflix - Hystrix documentation.

### AT-TLS

The communication server on z/OS provides a functionality to encrypt HTTP communication for on-platform running jobs. This functionality is refered to as Application Transparent Transport Layer Security (AT-TLS). Starting with Zowe version 1.24, it is possible to leverage AT-TLS within the API Mediation Layer. Each API ML component can run with AT-TLS rules applied. Some components, such as the Discovery service, can be made AT-TLS aware by enabling the AT-TLS profile, whereby TLS information can be utilized. Such information could be a client certificate. To enable the AT-TLS profile and disable the TLS application in API ML, update instance.env with the following environment variables:

While API ML can not handle TLS on its own, the Mediation Layer needs information about the server certificate that is defined in the AT-TLS rule. Update the instance.env file with the path to the SAF Key ring from the AT-TLS rule and specify the alias that is used for Inbound communication:

**Note:** This procedure does not configure AT-TLS on z/OS, but rather enables API ML to work with AT-TLS in place.

Version: v1.25.x LTS

# **Getting started tutorial**

### Contents

- Learning objectives
- Estimated time
- Prerequisites and assumptions
- Logging in to the Zowe Desktop
- Querying JES jobs and viewing related status in JES Explorer
- Using the 3270 Terminal in the Zowe Desktop to view the job
- Editing a data set in MVS Explorer
- Using the Zowe CLI to edit a data set
- Viewing the data set changes in MVS Explorer
- Next steps
  - Go deeper with Zowe
  - Try the Extending Zowe scenarios
  - Give feedback

### Learning objectives

This tutorial walks you through the Zowe™ interfaces, including the Zowe Desktop and Zowe CLI, with several simple tasks to help you get familiar with Zowe.

- If you are new to Zowe, start with this tutorial to explore the base Zowe features and functions.
- If you are already familiar with Zowe interfaces and capabilities, you might want to visit the **Extending** section which guides you to extend Zowe by creating your own APIs or applications.
  - Developing for API Mediation Layer
  - Developing for Zowe Application Framework
  - Developing for Zowe CLI

By the end of the session, you'll know how to:

- Log in to the Zowe Desktop
- Query jobs with filters and view the related status by using the JES Explorer

- View jobs by using the 3270 Terminal in the Zowe Desktop
- View and edit data sets by using the MVS Explorer
- Edit a data set and upload it to the mainframe by using Zowe Command-Line Interface (CLI)

As an introductory scenario, no previous knowledge of Zowe is needed.

### Estimated time

This tutorial guides you through the steps in roughly 20 minutes. If you explore other concepts related to this tutorial, it can take longer to complete.

### **Prerequisites and assumptions**

Before you begin, it is assumed that you have already successfully installed Zowe. You are ready to launch Zowe Desktop and Zowe CLI.

For information about how to install Zowe, see Installing Zowe.

### Important!

- In this tutorial, the following parameters are used as an example. Replace them with your own settings when you follow the tutorial in your environment.
  - URL to access the Zowe Desktop:
    - Using API mediation layer: https://myhost:<gateway port>/ui/v1/zlux/
    - Without the API mediation layer: https://myhost:<appserver httpsPort>/
  - Mainframe credentials:
    - Username: ibmuser
    - Password: sys1
- It is assumed that you perform the tasks in a Windows environment and that you have Visual Studio Code (VS Code) installed.

### Logging in to the Zowe Desktop

Access and navigate the Zowe Desktop to view the Zowe applications. In this tutorial, you will use the Firefox browser to log in to the Zowe Desktop.

There are two ways to log in to the Zowe Desktop:

- Through the API mediation layer: https://myhost:<gateway port>/ui/v1/zlux/
  - Example:

https://s0w1:7554/ui/v1/zlux/ZLUX/plugins/org.zowe.zlux.bootstrap/web/inde
x.html

- Directly, if the mediation layer is not used: https://myhost:<appserver httpsPort>/
  - Example
     https://s0w1:8544/ZLUX/plugins/org.zowe.zlux.bootstrap/web/index.html
- *myHost* is the host on which you are running the Zowe Application Server.
- httpsPort is the value that was assigned to node.https.port in zluxserver.json. For example, if you run the Zowe Application Server on host myhost and the value that is assigned to node.https.port in zluxserver.json is 12345, you would specify

https://myhost:12345/ZLUX/plugins/org.zowe.zlux.bootstrap/web/index.html.

### Follow these steps:

1. In the address field, enter the URL to access the Zowe Desktop. In this tutorial, the following URL is used as an example:

https://s0w1:8544/ZLUX/plugins/org.zowe.zlux.bootstrap/web/index.html

- 2. On the login page of the Zowe Desktop, enter your mainframe credentials. In this tutorial, the following ID is used as an example:
  - Username: ibmuser
  - Password: sys1
- 3. Press Enter.

Upon authentication of your user name and password, the Zowe Desktop opens. Several applications are pinned to the taskbar. Click the Start menu to see a list of applications that are installed by default. You can pin other applications to the taskbar by right-clicking the application icon and selecting **Pin to taskbar**.

Next, you will use the JES Explorer application to query the jobs with filters and view the related status.

# Querying JES jobs and viewing related status in JES Explorer

Use the Job Entry Subsystem (JES) Explorer to query JES jobs with filters and view the related status.

#### Follow these steps:

- 1. Click the Start menu in the Zowe Desktop.
- 2. Scroll down to find the JES Explorer icon and click to open it. The JES Explorer is displayed. If prompted to provide credentials for authentication, enter your mainframe credentials.
- 3. Click the **Job Filters** column to expand the filter criteria. You can filter jobs on various criteria by Owner, Prefix, Job ID, and Status. By default, the jobs are filtered by Owner. In this tutorial, the example owner is **IBMUSER**.

Owner= IBMUSER F Jobld= *	Prefix= *	
Job Filters		^
Owner	Prefix	
IBMUSER	*	
Job ID	Status	
*	*	
APPLY	RESET	

4. To query the jobs starting with SDSF and in an active status, clear the field of **Owner**, then enter SDSF\* in the **Prefix** field and select **ACTIVE** from the **Status** drop-down list, and click **APPLY**.

**Note:** Wildcard is supported. Valid wildcard characters are asterisk (\*), percent sign (%), and question mark (?).

5. From the job filter results, click the job named **SDSF**. The data sets for this job are listed.



6. Click **JESJCL** to open the JESJCL data set. The contents of this data set are displayed. You can also select other data sets to view their contents.

Tip: You can hover over the text in purple color to display a hover help window.

You used the JES Explorer to query the JES jobs with filters and viewed the related steps, files, and status.

Close the JES Explorer window. Next, you'll use the TN3270 application plug-in in the Zowe Desktop to view the same job that you viewed in this task.

# Using the 3270 Terminal in the Zowe Desktop to view the job

Use the 3270 Terminal application plug-in to view the same job that you filtered out in the previous task.

Zowe not only provides new, modern applications to interact with z/OS®, but it also integrates the traditional 3270 terminal interface that you may also be familiar with. The 3270 Terminal application plug-in provides a basic, emulated 3270 terminal connection to the mainframe via the Zowe Application Server.

### Follow these steps:

1. From the taskbar at the bottom of the Zowe Desktop, click the 3270 Terminal icon to open the 3270 Terminal application plug-in.

The 3270 Terminal panel is displayed, which offers selections to access various mainframe services.

2. Enter the following command and press Enter to log on to TSO:

LOGON ibmuser

3. On the TSO/E LOGON panel, enter the password sys1 in the **Password** field and press Enter.

You successfully log on to TSO.

- 4. When you see the following screen, press Enter. The **ISPF Primary Option Menu** is displayed.
- 5. Access SDSF to view output from a job. To do this,
  - i. Type M at the **Option** prompt and press Enter.
  - ii. Type 5 and press Enter.
- 6. To view the jobs in an active status, type **DA** at the command input prompt and press Enter. The jobs that are running are displayed.
- 7. To query the jobs that start with SDSF, type prefix sdsf; owner \* at the command input prompt and press Enter.

8. To view the contents of the job, type **S** next to the job name **SDSF** and press Enter.

The contents of the job are displayed.

Close the 3270 Terminal window. In the next step, you will use the MVS Explorer to make changes to a data set.

### **Editing a data set in MVS Explorer**

Use the MVS Explorer to create and edit a data set member and save the changes. The MVS Explorer view lets you browse the MVS file system by creating filters against data set names.

### Follow these steps:

- 1. Click the Start menu on Zowe Desktop.
- 2. Scroll down to find the MVS Explorer icon and pin this application to the desktop for later use.
- 3. Click the **MVS Explorer** icon on the taskbar. The MVS Explorer opens. The **Filter** field is pre-filled with the user name. In this tutorial, the filter string is **IBMUSER**. All the data sets matching this filter are displayed. You can expand a data set name and see the members in it.
- 4. Enter USER. Z23B. PARMLIB in the **Filter** field to locate this data set and then click to expand it. Ensure that there is no extra space before the data set member name that you enter.
- 5. Right-click the USER. Z23B. PARMLIB data set and select New Dataset Member.

USER.Z23B.PARM	LIB	C	
USER.Z23B.PARM	ILIB		
ZWESIP00	New Dataset		
	N	lew Dataset Member	
	D	elete	

6. Enter **ZTRIAL** as the data set member name and click **OK** to create the data set member.

New Dataset Member	
ZTRIAL	
	CANCEL

- 7. Click the data set member you just created and edit it by adding a new sentence, for example, First change to Zowe zTrial.
- 8. Click **SAVE** to save your edits.

The following message **Save success for USER.Z23B.PARMLIB(ZTRIAL)** pops up quickly at the bottom of the MVS Explorer window, which indicates that your edits are successfully saved.



Leave the MVS Explorer window open; we will look at the contents of the data set in a later step. If asked to leave the page, choose **Stay on Page**. Next, you will use Zowe CLI to view and add another change to the same data set.

### Using the Zowe CLI to edit a data set

Use Zowe CLI to download the same data set that you edited by using MVS Explorer in the previous step, edit it, and upload the changes to the mainframe.

Zowe CLI is a command-line interface that lets you interact with z/OS from various other platforms, such as cloud or distributed systems, to submit jobs, issue TSO and z/OS console commands, integrate z/OS actions into scripts, produce responses as JSON documents, and more. With this extensible and scriptable interface, you can tie in mainframes to distributed DevOps pipelines and build automation.

### Follow these steps:

1. Start the Command Prompt or a terminal in your local desktop. In this tutorial, it's assumed that you use Windows Command Prompt.



2. (Optional) Issue the following command to view the top-level help descriptions.

**Tip:** The command **zowe** initiates the product on a command line. All Zowe CLI commands begin with **zowe**.

3. To list the data sets of USER, enter the following command:

The following data sets are listed.

C:\Users\Administrator>zowe	zos-files	list	data-set	"USER.*"
USER.ADCD.SMPELIST				
USER.Z23B.CIDTABL				
USER.Z23B.CLIST				
USER.Z23B.HELP				
USER.Z23B.ISPLLIB				
USER.Z23B.ISPMLIB				
USER.Z23B.ISPPLIB				
USER.Z23B.ISPSLIB				
USER.Z23B.ISPTLIB				
USER.Z23B.LINKLIB				
USER.Z23B.LOADLIB				
USER.Z23B.LPALIB				
USER.Z23B.MSGENU				
USER.Z23B.PARMLIB				
USER.Z23B.PROCLIB				
USER.Z23B.STCJOBS				
USER.Z23B.SYSEXEC				
USER.Z23B.TCPPARMS				
USER.Z23B.UTAMLIB				
USER.Z23B.VTAMLST				

4. To download all the data set members of USER.Z23B.PARMLIB, enter the following command:

The message "Data set downloaded successfully" indicates that the data set members are downloaded. A file hierarchy is added to your current directory.

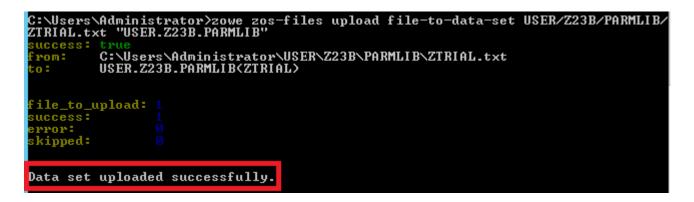
5. To open the data set member named ZTRIAL in Visual Studio Code, issue the following command against the same directory where you issued the download command:

Alternatively, navigate to the PARMLIB directory and issue code ZTRIAL.txt.

The file opens in a text editor (in this example, VS Code). You will see the changes you made in the previous step by using the MVS Explorer.

- 6. Add the text Second change to Zowe zTrial to the file and then use Ctrl+S to save your edits.
- 7. Open the Command Prompt again and upload your changes to the mainframe by entering the following command:

The following message indicates that you successfully uploaded your changes:



Congratulations! You used Zowe CLI to edit a data set member and upload the changes to mainframe.

Close the Command Prompt window. In the next step, you will open the MVS Explorer again to view the updates that you made to the data set in this procedure.

### Viewing the data set changes in MVS Explorer

Use the MVS Explorer to view the data set changes from the previous step.

### Procedure

1. Return to the Zowe Desktop and open the MVS Explorer application.

2. Locate the data set member **USER.Z23B.PARMLIB** > **ZTRIAL** and click the refresh icon. You will see the changes you just made by using Zowe CLI.

Congratulations! You explored several applications on the Zowe Desktop and learned how to work with them.

### Next steps

Here are some next steps.

### Go deeper with Zowe

In roughly 20 minutes, you used the MVS<sup>™</sup> Explorer and Zowe CLI to edit the same data set member, and used the JES Explorer and the 3270 Terminal to query the same JES job with filters, all without leaving Zowe. Now that you're familiar with Zowe components, you can continue to learn more about the project. Zowe also offers many more plug-ins for both Zowe Desktop and Zowe CLI.

For more information, see the User Guide.

For a complete list of available CLI commands, explore the Zowe CLI Command Reference Guide.

### Try the Extending Zowe scenarios

You can add your own application plug-ins to Zowe. See how easy it is to extend Zowe to create your own APIs and applications by reading the Extending section.

### **Give feedback**

Did you find this tutorial useful? You can tell us what you think about this tutorial via an online survey.

If you encounter any problems or have an idea for improving this tutorial, you can create a GitHub issue here.

# **Using the Zowe Desktop**

You can use the Zowe<sup>™</sup> Application Framework to create application plug-ins for the Zowe Desktop. For more information, see Extending the Zowe Application Framework.

### Navigating the Zowe Desktop

From the Zowe Desktop, you can access Zowe applications.

### Accessing the Zowe Desktop

From a supported browser, open the Zowe Desktop at <a href="https://fmyhost?:fhttpsPort">https://fmyhost?:fhttpsPort</a> or you can navigate to the direct Desktop URI at <a href="https://fmyhost?:fhttpsPort">https://fmyhost?:</a> fhttpsPort</a> // <a href="httpsPort">https?//fmyhost?:</a> // <a href="httpsPort">fhttpsPort</a> // <a href="httpsPort">https?//fmyhost?:</a> // <a href="httpsPort">https?//fmyhost?:</a>

Where:

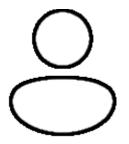
- *myHost* is the host on which you are running the Zowe Application Server.
- httpsPort is the value that was assigned to node.https.port in server.json. For example, if you run the Zowe Application Server on host myhost and the value that is assigned to node.https.port in server.json is 12345, you would specify

https://myhost:12345/ZLUX/plugins/org.zowe.zlux.bootstrap/web/index.html

### Logging in and out of the Zowe Desktop

- 1. To log in, enter your TSO credentials in the **Username** and **Password** fields.
- 2. Press Enter. Upon authentication of your user name and password, the desktop opens.

To log out, click the User icon in the lower right corner and click Sign Out.



### Changing user password

1. Open the Preferences panel by clicking on the Preferences icon in the bottom right of the desktop.



2. Click the Change Password icon. 3. Fill out the Old Password and New Password fields. 4. Upon successful password change, you will be taken to the desktop.

### Updating an expired password

- 1. Upon logging in with an expired password, a screen will be displayed prompting you to change your password.
- 2. Enter and confirm your new password in the corresponding fields.
- 3. Upon successful password change, you will be taken to the desktop.

### Pinning applications to the task bar

- 1. Click the Start menu in the bottom left corner of the home screen.
- 2. Locate the application you want to pin.
- 3. Right-click the application icon and select **Pin to taskbar**.

### **Personalizing the Desktop**

1. Click the **Preferences icon** to open the Preferences panel.



2. Click the **Personalization icon** to open the menu.



- 3. Drag an image into the wallpaper grid, or press the upload button, to upload a new Desktop wallpaper.
- 4. To set a new theme color, select a color from the palette or hue.

- 5. Use the lightness swatch bar to adjust the lightness of the color.
- Adjusting the lightness will also change the lightness of secondary text.
- 6. Select a size (small, medium, or large) to adjust the scale of the Desktop UI.

# Changing the desktop language

Use the Languages setting in the Preferences panel to change the desktop language. After you change the language and restart Zowe, desktop menus and text display in the specified language. Applications that support the specified desktop language also display in that language.

- 1. Click the Preferences icon in the lower right corner.
- 2. Click Languages.
- 3. In the Languages dialog, click a language, and then click Apply.
- 4. When you are prompted, restart Zowe.

# **Zowe Desktop application plug-ins**

Application plug-ins are applications that you can use to access the mainframe and to perform various tasks. Developers can create application plug-ins using a sample application as a guide. The following application plug-ins are installed by default:

# **Hello World Sample**

The Hello World sample application plug-in for developers demonstrates how to create a dataservice and how to create an application plug-in using Angular and using React.

# **IFrame Sample**

The IFrame sample application plug-in for developers demonstrates how to embed pre-made webpages within the desktop as an application and how an application can request an action of another application (see the source code for more information).

# z/OS Subsystems

The z/OS Subsystems plug-in helps you find information about the important services on the mainframe, such as CICS, Db2, and IMS.

# 3270 Terminal

The 3270 Terminal plug-in provides a user interface that emulates the basic functions of IBM 3270 family terminals. On the "back end," the plug-in and the Zowe Application Server connect to any standard TN3270E server.

## **VT Terminal**

The VT Terminal plug-in provides a user interface that emulates the basic functions of DEC VT family terminals. On the "back end," the plug-in and the Zowe Application Server connect to VT compatible hosts, such as z/OS UNIX System Services (USS), using standard network protocols.

# **API Catalog**

The API Catalog plug-in lets you view API services that have been discovered by the API Mediation Layer. For more information about the API Mediation Layer, Discovery Service, and API Catalog, see API Mediation Layer Overview.

### Editor

With the Zowe Editor you can create and edit files and view datasets on the system that Zowe serves.

### Workflows

From the Workflows application plug-in you can create, manage, and use z/OSMF workflows to manage your system.

### **JES Explorer**

Use this application to query JES jobs with filters, and view the related steps, files, and status. You can also purge jobs from this view.

## **MVS Explorer**

Use this application to browse the MVS<sup>™</sup> file system by using a high-level qualifier filter. With the MVS Explorer, you can complete the following tasks:

- List the members of partitioned data sets.
- Create new data sets using attributes or the attributes of an existing data set ("Allocate Like").

- Submit data sets that contain JCL to Job Entry Subsystem (JES).
- Edit sequential data sets and partitioned data set members with basic syntax highlighting and content assist for JCL and REXX.
- Conduct basic validation of record length when editing JCL.
- Delete data sets and members.
- Open data sets in full screen editor mode, which gives you a fully qualified link to that file. The link is then reusable for example in help tickets.

# **USS Explorer**

Use this application to browse the USS files by using a path. With the USS Explorer, you can complete the following tasks:

- List files and folders.
- Create new files and folders.
- Edit files with basic syntax highlighting and content assist for JCL and REXX.
- Delete files and folders.

# Using the Workflows application plug-in

The Workflows application plug-in is available from the Zowe Desktop Start menu. To launch Workflows, click the Start menu in the lower-left corner of the desktop and click the Workflows application plug-in icon. The **Users/Tasks Workflows** window opens.

## Logging on to the system

If you are prompted to log on to the system, complete these steps:

- 1. Enter your user ID and password.
- 2. Click **Sign in**.

# Updating the data display

To refresh the data on any tab, click

in the upper right corner of the window.

# Configuration

From the **Configuration** tab, you can view, add, and remove servers.

## Adding a z/OSMF server

Complete these steps to add a new z/OSMF server:

- 1. Click the **Configuration** tab.
- 2. Click the plus sign (+) on the left side of the window.
- 3. In the **Host** field, type the name of the host.
- 4. In the **Port** field, type the port number.
- 5. Click OK.

### Testing a server connection

To test the connection, click **Test**. When the server is online the **Online** indicator next to the server **Host** and **Port** is green.

## Setting a server as the default z/OSMF server

Complete these steps to set a default z/OSMF server:

- 1. Click Set as default.
- 2. Enter your user ID and password.
- 3. Click **Sign in**.

**Note:** You must specify a default server.

### **Removing a server**

To remove a server, click **x** next to the server that you want to remove.

### **Reload a server configuration**

To reload a server configuration, click **Reload**.

# Save a server configuration

To save a server configuration, click **Save**.

## Workflows

To display all workflows on the system, click the **Workflows** tab.

You can sort the workflows based on the following information:

#### Workflow

The name of the workflow.

#### Description

The description of the workflow.

#### Version

The version number.

#### Owner

The user ID of the workflow owner.

#### System

The system identifier.

#### Status

The status of the workflow (In progress or Completed).

#### Progress

Indicates how much of the workflow has been completed based on the number of tasks completed.

### Searching workflows

To locate a specific workflow, type a search string in the search box in the upper right corner of the window.

## **Defining a workflow**

To define a workflow, complete these steps:

- 1. From the **Workflows** tab, click **Actions** > **New workflow**. (By default, the **Advanced Mode** check box is selected.)
- 2. In the **Name** field, specify a descriptive name for the workflow.
- 3. In the **Workflow definition file** field, specify the primary XML file for this workflow.
- 4. In the **System** field, specify a system.
- 5. In the **Owner** field, specify the user ID of the person that is responsible for assigning the tasks in the workflow. (To set the owner to the current user, select the **Set owner to current user** check box.)
- 6. Click **OK**.

# **Viewing tasks**

To view the tasks associated with a workflow, click the **My Tasks** tab. Workflows that have assigned tasks are shown on the left side of the window. The task work area is on the right side of the window.

You can choose to view workflows that have **Pending** or **Completed** tasks or you can choose to view all workflows (**Pending** and **Completed**) and their tasks, regardless of the task status.

For each workflow, you can click the arrow to expand or collapse the task list. Assigned tasks display below each workflow. Hovering over each task displays more information about the task, such as the status and the owner.

Each task has a indicator of **PERFORM** (a step to be performed) or **CHECK** (Check the step that was performed). Clicking **CHECK** or **PERFORM** opens a work area on the right side of the window. When a task is complete, a green clipboard icon with a checkmark is displayed.

**Note:** If you are viewing tasks on a **Pending** or **Completed** tab, only those workflows that have tasks with a corresponding status, are displayed.

## Task work area

When you click **CHECK** or **PERFORM**, a work area on the right side of the window opens to display the steps to complete the task. Expand or collapse the work area by clicking

**Tip:** Hovering over the task description in the title bar of the work area window on the right side displays more information about the corresponding workflow and the step description.

# Performing a task

- 1. To perform a task that has steps that are assigned to you, click **PERFORM**.
- 2. Use the work area to perform the steps associated with the selected task. Depending on the task, you might use an embedded tool (such as another application) or you might complete a series of steps to complete the task.
- 3. If there are multiple steps to perform, click **Next** to advance to the next step for the task.
- 4. Click Finish.

Note: When a task is complete, a green clipboard icon with a checkmark is displayed next to the task.

## **Checking a task**

- 1. To check a task, click **CHECK**.
- 2. In the task work area, view the JESMSGLG, JESJCL, JESYSMSG, or SYSTSPRT output that is associated with the selected task.

## **Managing tasks**

To manage a task in the PERFORM status, click

### :

to the right of the task status. Choose from the following options:

#### Properties

Display the title and description of the task.

#### Perform

Perform the first step.

#### Skip

Skip this step.

#### **Override Complete**

Override the completion of the step. The selected step will be bypassed and will not be performed for this workflow. You must ensure that the step is performed manually.

#### Assignment

Opens the Manage Assignees window where authorized users can add or remove the user ID of the person that is assigned to the step.

#### Return

Remove ownership of the step.

### **Viewing warnings**

To view any warning messages that were encountered, click the **Warnings** tab. A message is listed in this tab each time it is encountered.

To locate a specific message, type a search string in the search box in the upper right corner of the window.

You can sort the warning messages based on the following information.

#### Message Code

The message code that is associated with the warning.

#### Description

A description of the warning.

#### Date

The date of the warning.

#### **Corresponding Workflow**

The workflow that is associated with the warning.

# **Using the Editor**

With the Zowe Editor, you can create and edit the many types of files.

# Specifying a highlighting language

- 1. Click **Language** on the editor menu bar. A dropdown menu will be displayed.
- 2. From the dropdown, select the desired language. Plain Text will be chosen by default if the automatic language detection is not able to determine the language.

# Open a dataset

To open a dataset, follow these steps:

- 1. From the **File** menu, select Open Datasets. You can also use (ALT+K).
- 2. In the Dataset field, specify the name of the dataset you want to open.
- 3. Click **Open**

# Deleting a file or folder

- 1. In the file tree, right-click on a file or folder you want to delete.
- 2. From the right-click menu, click **Delete**. A warning dialogue will appear.
- 3. Click **Delete**

# **Opening a directory**

- 1. From the **File** menu, select **Open Directory**. You can also use (ALT+O).
- 2. In the Directory field, specify the name of the directory you want to open. For example: /u/zs1234
- 3. Click **Open**

The File Explorer on the left side of the window lists the folders and files in the specified directory. Clicking on a folder expands the tree. Clicking on a file opens a tab that displays the file contents. Double-clicking on a folder will make the active directory the newly specified folder.

# **Creating a new directory**

- 1. Right-click on a location in the directory tree where you want to create a new directory.
- 2. From the right-click menu, click **Create a directory...**.
- 3. Specify a directory name in the Directory Name field.
- 4. The Path will be set to the location that you initially right-clicked to open the dialogue. You can specify a different location in the Path field.
- 5. Click Create

# **Creating a new file**

To create a new file, complete these steps:

- 1. From the File menu, select New File. You can also use (ALT+N).
- 2. From the File menu, select Save to save the newly created file. You can also use (Ctrl+S)
- 3. In the File Name field, specify the file name for the newly created file.
- 4. Choose an encoding option from the Encoding dropdown menu. The directory will be prefilled if you are creating the new file in an existing folder.
- 5. Click **Save**
- 6. To close a file, click the X icon in its tab, double-click on the tab, or use (Alt+W).

# Hotkeys

The following hotkeys can be used in the editor to navigate or perform actions with only the keyboard.

- Shift TAB: Cycle through the menu bar, browsing type, search bar, file tree, and editor component.
  - Individual options within the menu bar and individual nodes within the file tree can be navigated with the arrow keys and ENTER (to select).

Hot Key	Command	
ALT+K	Open a dataset	
ALT+O	Open a directory	

Hot Key	Command		
ALT+N	Create a new file		
ALT+W	Close tab		
ALT+W+Shift	Close all tabs		
CTRL+S	Save file		
ALT+M	Navigate Menu bar (use arrow keys)		
ALT+P	Search Bar focus		
ALT+1	Primary editing component focus		
ALT+T+CTRL	Undo close/close all		
ALT+R+Shift	Refresh active tab		
ALT+PgUp(or <)	Switch to left tab		
ALT+PgDown(or >)	Switch to right tab		
ALT+B	Show/hide left-hand side file tree		

Version: v1.25.x LTS

# Using API Catalog

As an application developer, use the API Catalog to view what services are running in the API Mediation Layer. Through the API Catalog, you can also view the associated API documentation corresponding to a service, descriptive information about the service, and the current state of the service. The tiles in the API Catalog can be customized by changing values in the <code>apiml.catalog.tile</code> section defined in the application.yml of a service. A microservice that is onboarded to the API Mediation Layer and configured appropriately, registers automatically with the API Catalog and a tile for that service is added to the Catalog.

**Note:** For more information about how to configure the API Catalog in the application.yml, see: Add API Onboarding Configuration.

# **API Versioning**

See API Catalog and Versioning for more information about the API versioning.

# View Service Information and API Documentation in the API Catalog

Use the API Catalog to view services, API documentation, descriptive information about the service, the current state of the service, service endpoints, and detailed descriptions of these endpoints.

**Note:** Verify that your service is running. At least one started and registered instance with the Discovery Service is needed for your service to be visible in the API Catalog.

### Follow these steps:

1. Use the search bar to find the service that you are looking for. Services that belong to the same product family are displayed on the same tile.

Example: Sample Applications, Endevor, SDK Application

2. Click the tile to view header information, the registered services under that family ID, and API documentation for that service.

Notes:

- The state of the service is indicated in the service tile on the dashboard page. If no instances of the service are currently running, the tile displays a message that no services are running.
- At least one instance of a service must be started and registered with the Discovery Service for it to be visible in the API Catalog. If the service that you are onboarding is running, and the corresponding API documentation is displayed, this API documentation is cached and remains visible even when the service and all service instances stop.
- Descriptive information about the service and a link to the home page of the service are displayed.

#### **Example:**

3. Select the version (v1, v2) to view the documentation of a specific API version.

#### Example:

4. Expand the endpoint panel to see a detailed summary with responses and parameters of each endpoint, the endpoint description, and the full structure of the endpoint.

#### Example:

#### Notes:

- If a lock icon is visible on the right side of the endpoint panel, the endpoint requires authentication.
- The structure of the endpoint is displayed relative to the base URL.
- The URL path of the abbreviated endpoint relative to the base URL is displayed in the following format:

#### Example:

#### /api/v1/{yourServiceId}/{endpointName}

The path of the full URL that includes the base URL is also displayed in the following format:

Both links target the same endpoint location.

# Swagger "Try it out" functionality in the API Catalog

The API Catalog enables users to call service APIs through the **Try it out** functionality. There are 2 types of endpoints:

#### • Public endpoints

Endpoints that are accessible without entering user credentials.

#### Protected endpoints

Endpoints that are only accessible by entering user credentials. These endpoints are marked with a lock icon.

#### Example:

**Note:** Before making requests to protected endpoints, authorize your session by clicking the lock icon and complete the required information in the Authorization modal shown below:

#### Example:

To demonstrate **Try it out**, we use the example of the Swagger Petstore.

#### Example:

### Make a request

This section outlines the process for making a request.

#### Follow these steps:

- 1. Expand the **POST Pet** endpoint.
- 2. Click **Try it out**.

Example:

After you click **Try it out**, the example value in the **Request Body** field becomes editable.

- 3. In the **Example Value** field, change the first id value to a random value. Change the second name value to a value of your choice, such as the name of a pet.
- 4. Click **Execute**.

Example:

The API Catalog Swagger UI submits the request and shows the *curl* that was submitted. The Responses section shows the response.

Example:

# Static APIs refresh functionality in the API Catalog

The API Catalog enables users to manually refresh static service APIs. Use the **Refresh Static APIs** option if you change a static service API and want these changes to be visible in the API Catalog without restarting the Discovery Service.

#### Example:

To refresh the status of a static service, click the **Refresh** option located in the upper right-hand side of the API Catalog UI. Successful requests return a pop-up notification that displays the message, The refresh of static APIs was successful!

#### Example:

If the request fails, a dialog appears with an error message that describes the cause of the fail.

#### Example:

**Note:** The manual **Refresh Static APIs** option applies only to static service APIs. Changes to the status of services that are onboarded to allow for dynamic discovery require a restart of the specific services where changes are applied. It is not necessary to restart the API Catalog or the Discovery Service.

# Using Zowe CLI

Learn about how to use Zowe™ CLI, including connecting to the mainframe, managing profiles, integrating with API Mediation Layer, and more.

You can use the CLI interactively from a command window on any computer on which it is installed, or run it in a container or automation environment.

Tip: If you want to use the CLI together with a screen reader to provide accessibility, we recommend using the Mac<sup>™</sup> Terminal application enabled for Accessibility through System Preferences > Accessibility. On Windows<sup>™</sup>, adjust the Properties settings in Command Prompt. For other operating systems, or for alternative terminals, check the specification for the terminal to ensure that it meets accessibility requirements.

- Using Zowe CLI
  - Displaying help
    - Top-level help
    - Group, action, and object help
    - Launch local web help
  - Viewing web help
  - How command precedence works
  - Issuing commands
  - Using profiles
    - Displaying profile help
    - Service profiles
    - Base profiles
    - Profile best practices
  - Testing connection to z/OSMF
  - Integrating with API Mediation Layer
    - How token management works
    - Logging in
    - Logging out
    - Accessing a service through API ML
    - Accessing multiple services with SSO

- Accessing services through SSO + one service not through APIML
- Accessing services through SSO + one service through API ML but not SSO
- Working with certificates
  - Configure certificates signed by a Certificate Authority (CA)
  - Extend trusted certificates on client
  - Bypass certificate requirement
- Using environment variables
  - Formatting environment variables
  - Setting environment variables in an automation server
- Using the prompt feature
- Writing scripts
- Understanding core command groups

# **Displaying help**

Zowe CLI has a command-line help system that details the commands, actions, and options available in the product.

- Top-level help
- Group, action, and object help
- Launch local web help

# **Top-level help**

To view top-level help, open a command-line and issue the following command:

Alternatively, issue the following command to display a full list of all available commands:

Tip: All Zowe CLI commands begin with zowe.

# Group, action, and object help

Append the global —help option to learn about a specific command group, action, or object.

For example, issue the following command to learn about the create action in the zos-files group:

# Launch local web help

Launch an interactive form of help in a web browser. When you issue the following command, web help is custom-generated to include commands for all currently installed plug-ins:

**Tip:** Append —help-web to a specific command or action to launch directly into the appropriate web help page.

# Viewing web help

You can download web help from this site in any of the following formats: HTML, a zip file that contains the HTML, or PDF:

- Browse Online
- Download (ZIP)
- Download (PDF)

# How command precedence works

You can provide your mainframe connection details (username, password, etc...) to Zowe CLI in several ways. Zowe CLI abides by a "command option order of precedence" that provides flexibility when issuing commands and writing scripts.

When you issue a command, the CLI searches for your command arguments in the following order:

- 1. **Options** that you specify on individual commands.
- 2. **Environment variables** that you define in the computer's operating system. For more information, see Using environment variables
- 3. **Service profiles** that you create (i.e. z/OSMF profile or another MF service).
- 4. **Base profiles** that you create (can contain credentials for use with multiple services and/or an API ML login token).
- 5. Default option value.

If you omit an option from the command line, Zowe CLI searches for an environment variable that contains a value for the option. If no environment variable exists, the CLI checks your service profiles for the value. Base profiles provide values to other service profiles such that you do not need to specify the same options (i.e. username and password) in multiple service profiles.

**Note:** If you do not provide a value using one of these methods, the default value is used. If a required option value is not located, you receive a syntax error message Missing Positional Argument or Missing Option.

# **Issuing commands**

You can provide all connection options directly on commands to access a service. For example, issue the following command to list all data sets under the name <code>ibmuser</code> on the specified system:

If you omit username, password, host, or port (and a value cannot be found in your configuration), the CLI prompts you to enter a value.

# **Using profiles**

Profiles let you store configuration details for reuse, and for logging in to authentication servers such as API Mediation layer. Create a profile that contains your username, password, and connection details for a mainframe service, then use that profile to avoid typing the information on every command. Switch between profiles to quickly target different mainframe subsystems. There are two main types of profiles:

- Service profiles: Store connection information for specific mainframe service, such as IBM z/OSMF. Plug-ins can introduce other service profile types, such as the cics profile to connect to IBM CICS.
- **Base profiles:** Store connection information for use with one or more services. Your service profiles can pull information from base profiles as needed, so that you can specify a common username and password once. The base profile can optionally store tokens to connect to Zowe API Mediation Layer, which improves security by enabling Multi-Factor Authentication (MFA) and Single Sign-on (SSO).

#### Tips:

- You can have multiple service profiles and multiple base profiles.
- Profiles are **not** required. You can choose to specify all connection details for every command.
- Profile values are stored on your computer in plaintext in C:\Users\
   <yourUsername>\.zowe\profiles (Windows) or ~/.zowe/profiles (Mac/Linux).

# **Displaying profile help**

Use help to learn about options for creating profiles. For example, for a **zosmf** profile, issue the following command:

# **Service profiles**

Create profiles that target a specific mainframe service, then use profiles to issue commands. For example, issue the following command (substituting your connection details) to create a <code>zosmf</code> service profile named <code>myprofile123</code>:

Use the profile. For example, issue the following command to list all data sets under the name *ibmuser* on the system that you specified in your profile:

**Note:** If you do not specify a profile, your default profile is used. The first profile that your create is your default. You can set a service profile as your default with the zowe profiles set-default <profileType> <profileName> command.

# **Base profiles**

Base profiles store your connection details and provide them to service profiles and commands as needed. The base profile can also contain a token to connect to services through API ML.

For example, if you use the same username and password across multiple services, you can create a base profile with your username and password. After the base profile is created, you can omit the --username and --password options when you issue commands or use service profiles such as zosmf and tso. Commands will use the values provided by the base profile. For example, create the base profile:

The first profile that you create for a service is set as your default profile. When you create subsequent profiles, you can select one as the default with the zowe profiles set-default <profileType> <profileName> command.

Use the default profile to issue a command:

**Note:** If you choose to log in to Zowe API Mediation Layer, a base profile is created for you to store a web token, host, and port.

# **Profile best practices**

According to order of precedence, base profiles are used as a fallback for service profiles. This means that after you create a base profile, you might need to update your service profiles to remove username,

password, host, and port. Otherwise, commands will use the information stored in your service profile and will ignore your base profile definition.

# **Testing connection to z/OSMF**

Optionally, issue a command at any time to receive diagnostic information from the server and confirm that Zowe CLI can communicate with z/OSMF or other mainframe APIs.

**Important!** By default, the server certificate is verified against a list of Certificate Authorities (CAs) trusted by Mozilla. This handshake ensures that the CLI can trust the server. You can append the flag --ru false to the following commands to bypass the certificate verification against CAs. If you use the --ru false flag, ensure that you understand the potential security risks of bypassing the certificate requirement at your site. For the most secure environment, system administrators configure a server keyring with a server certificate signed by a Certificate Authority (CA). For more information, see Working with certificates.

#### Without a profile

Verify that your CLI instance can communicate with z/OSMF:

#### Default profile

After you create a profile, verify that you can use your *default profile* to communicate with z/OSMF:

#### **Specific profile**

After you create a profile, verify that you can use a specific profile to communicate with z/OSMF:

The commands return a success or failure message and display information about your z/OSMF server, such as the z/OSMF version number. Report failures to your systems administrator and use the information for diagnostic purposes.

# **Integrating with API Mediation Layer**

Zowe API ML provides a single point of access to a defined set of mainframe services. The layer provides API management features such as high-availability, consistent security, and a single sign-on (SSO) and multi-factor authentication (MFA) experience.

You can access services through API ML without reauthenticating every time you issue a command. Tokens allow for a secure interaction between the client and server. When you issue commands to API ML, the layer

routes requests to an appropriate API instance based on system load and available API instances.

### How token management works

When you log in with the CLI, an API ML token is supplied and stored on your computer in place of username and password. The token allows for a secure handshake with API ML when you issue each command, such that you do not need to reauthenticate until the token expires.

**Note:** Zowe CLI also supports standard token implementations such as Java Web Tokens (JWT) and Lightweight Third-Party Authentication (LTPA).

# Logging in

To request a token and "log in" to API ML, issue the following command:

The CLI prompts you to enter your username, password (where password can be a PIN concatenated with a second factor for MFA), host, and port for the API ML instance.

Tip: If you already created a base profile, you might not be prompted for host and port.

A local base profile is created that contains your token. When you issue commands, you can omit your username, password, host, and port. Instead, provide a base path and base profile on commands to connect to API ML.

Optionally, if you do not want to store the token on disk, append the <u>--show-token</u> option to the login command. If you choose this option, you must manually supply the token on each command using the <u>--</u>token-value option.

#### Notes:

- Tokens expire after a period of time defined by your security administrator. When a token expires, you must log in again to get a new token.
- If you omit connection details from a service profile, such as **zosmf** profile, the CLI uses the information from your base profile.
- You can choose to specify all connection details on a service profile and connect directly to the service. Routing through API ML is not required.

# Logging out

Log out to expire the API ML token and remove it from your base profile.

Issue the following command:

zowe auth logout

The token is expired. Log in again to obtain a new token.

# Accessing a service through API ML

To access services through API ML using the token in your base profile, specify the following options on commands and service profiles:

- --base-path : The base path of the API ML instance that you want to access.
- --disable-defaults : Specify this flag to prevent default values from being stored in service profiles. If you do not use this flag, the defaults can override values in your base profile.

**Note:** Ensure that you *do not* provide username, password, host, or port directly on the service commands or profiles. Supplying those options causes the CLI to ignore the API ML token in your base profile and directly access the service.

#### Specifying base path

The following example illustrates a complete path for a z/OSMF instance registered to API ML. The format of base path can vary based on how API ML is configured at your site:

To access that API ML instance, create a service profile (or issue a command) with the --base-path value of api/v1. Your service profile uses the token and credentials stored in your default base profile.

Commands issued with this profile are routed through the layer to access an appropriate z/OSMF instance.

## Accessing multiple services with SSO

If multiple services are registered to the API Mediation Layer at your site, Zowe CLI lets you access the services with Single Sign-on (SSO). Log in once to conveniently access all available services.

When you are logged-in, supply the <u>--base-path</u> option on commands for each service. Ensure that you do not provide username, password, host, or port directly on your service commands or profiles. Supplying those options causes the CLI to ignore the token in your base profile and directly access the service. You might need to remove those options from existing profiles to use SSO.

For information about registering an API service at your site, see Developing for API Mediation Layer.

### Accessing services through SSO + one service not through APIML

There might be a scenario where you log in to API ML with SSO, but you also want access a different service directly (not through API ML).

To access the SSO-enabled services, log in and issue commands with the <u>--base-path</u> and <u>--base-profile</u> options. The token from your base profile is used for authentication. Remember, your command or service profile must *not* contain username, password, host, or port.

To access the other service directly (circumvent API ML), supply all connection information (username, password, host, and port) on a command or service profile. When you explicitly supply username and password in a command or service profile, the CLI always uses that connection information instead of the API ML token.

### Accessing services through SSO + one service through API ML but not SSO

You might want to access multiple services with SSO, but also access a service through API ML that is not SSO-enabled.

To perform SSO for the first set of services, log in to API ML and supply the <u>--base-path</u> and <u>--base-profile</u> on commands. For more information, see Accessing multiple services with SSO.

To access the service that is *not* SSO-enabled, explicitly provide your username and password when you issue commands. Using the **--base-path** option ensures that the request is routed to API ML, but the username and password that you provide overrides the credentials in your base profile. This lets you sign in to the individual service.

# Working with certificates

Certificates authorize communication between a server and client, such as z/OSMF and Zowe CLI. The client CLI must "trust" the server to successfully issue commands. Use one of the following methods to let the CLI communicate with the server:

- Configure certificates signed by a Certificate Authority (CA)
- Extend trusted certificates on client
- Bypass certificate requirement with CLI flag

# Configure certificates signed by a Certificate Authority (CA)

System Administrators can configure the server with a certificate signed by a Certificate Authority (CA) trusted by Mozilla. When a CA trusted by Mozilla exists in the certificate chain, the CLI automatically recognizes the server and authorizes the connection.

#### **Related information:**

- Using certificates with z/OS client/server applications in the IBM Knowledge Center.
- Configuring the z/OSMF key ring and certificate in the IBM Knowledge Center.
- Certificate management in Zowe API Mediation Layer
- Mozilla Included CA Certificate List

### **Extend trusted certificates on client**

If your organization uses self-signed certificates in the certificate chain (rather than a CA trusted by Mozilla), you can download the certificate to your computer add it to the local list of trusted certificates. Provide the certificate locally using the **NODE\_EXTRA\_CA\_CERTS** environment variable. Organizations might want to configure all client computers to trust the self-signed certificate.

This blog post outlines the process for using environment variables to trust the self-signed certificate.

### **Bypass certificate requirement**

If you do not have server certificates configured at your site, or you want to trust a known self-signed certificate, you can append the --reject-unauthorized false flag to your CLI commands. Setting the --reject-unauthorized flag to false rejects self-signed certificates and essentially bypasses the certificate requirement.

**Important!** Understand the security implications of accepting self-signed certificates at your site before you use this command.

#### **Example:**

# Using environment variables

You can define environment variables to execute commands more efficiently. Store a value such as your password in an environment variable, then issue commands without specifying your password every time.

The term environment can refer to your operating system, container environment, or automation server such as Jenkins.

You might want to assign a variable in the following scenarios:

#### • Store a value that is commonly used.

For example, you might want to specify your mainframe username as an environment variable. Now you can issue commands and omit the <u>--username</u> option, and Zowe CLI automatically uses the value that you defined in the environment variable.

#### • Override a value in existing profiles.

For example, you might want to override a value that you previously defined in multiple profiles to avoid recreating each profile. Specify the new value as a variable to override the value in profiles.

#### • Secure credentials in an automation server or container

You can set environment variables for use in scripts that run in your CI/CD pipeline. For example, can define environment variables in Jenkins so that your password is not seen in plaintext in logs. You can also define sensitive information in the Jenkins secure credential store.

# Formatting environment variables

Transform an option into the proper format for a Zowe CLI environment variable, then define a value to the variable. Transform option names according to the following rules:

- Prefix environment variables with ZOWE\_OPT\_.
- Convert lowercase letters in arguments/options to uppercase letters.
- Convert hyphens in arguments/options to underscores.

**Tip:** Refer to your operating system documentation for information about how to set and get environment variables. The procedure varies between Windows, Mac, and various versions of Linux.

#### **Examples:**

The following table provides examples of CLI options and the corresponding environment variable to which you can define a value:

Command Option	Environment Variable	Use Case
user	ZOWE_OPT_USER	Define your mainframe username to an environment variable to avoid specifying it on all commands or profiles.
reject- unauthorized	ZOWE_OPT_REJECT_UNAUTHORIZED	Define a value of true to the reject-unauthorized flag when you always require the flag and do not want to specify it on all commands or profiles.

## Setting environment variables in an automation server

You can use environment variables in an automation server, such as Jenkins, to write more efficient scripts and make use of secure credential storage. Automation tools such as Jenkins automation server usually provide a mechanism for securely storing configuration (for example, credentials). In Jenkins, you can use withCredentials to expose credentials as an environment variable (ENV) or Groovy variable.

You can either set environment variables using the SET command within your scripts, or navigate to **Manage Jenkins > Configure System > Global Properties** and define an environment variable in the Jenkins GUI. For example:

Global properties		
Disable deferred wipeout on this node		
Environment variables		
List of variables	Name	TEST_VARIABLE
	Value	test-value
	Name	

# Using the prompt feature

Zowe CLI has a command-line "prompt" feature that asks you to provide required option values. The CLI always prompts for host, port, username, and password if you do not supply them in commands or profile configuration.

You can also manually enable the prompt for any option. This is helpful to mask sensitive information on the screen while you type. You can enable a one-time prompt, or choose to always prompt for a particular option.

#### **Enable prompt**

Enable one-time prompting as needed.

#### Follow these steps:

- 1. Begin typing a command.
- 2. For the option(s) that you want to mask, insert the value "PROMPT\*". For example, prompt for your password:

The CLI prompts you to enter a value for the --password field.

3. Enter a value to complete the command.

Tip: Enter the value carefully. The backspace key does not work in prompt mode.

#### Always prompt

You can configure your environment so that the CLI *always* prompts for a particular option, such as \_\_\_ password .

To enable the feature, set an environment variable named ZOWE\_OPT\_PASSWORD with the value "PROMPT\*". With the environment variable set, the CLI automatically enables the prompt when you omit a required —password value.

**Tip** The procedure for setting environment variables is dependent on your operating systems. Refer to documentation for your OS to learn about setting environment variables.

#### Change the keyword for prompt

The default keyword that enables prompting is "PROMPT\*". You might want to change the keyword if there is a chance that "PROMPT\*" could exist as a valid value for the field. For example, if you mask the data-

set argument and are working with real mainframe data sets that begin with the characters "PROMPT\*"

To configure the keyword, choose a new value. Then define the value to to the environment variable on your computer named ZOWE\_PROMPT\_PHRASE.

# Writing scripts

You can combine multiple Zowe CLI commands in bash or shell scripts to automate actions on z/OS. Implement scripts to enhance your development workflow, automate repetitive test or build tasks, and orchestrate mainframe actions from continuous integration/continuous deployment (CI/CD) tools such as Jenkins or TravisCI.

- Sample script library
- Example: Clean up Temporary Data Sets
- Example: Submit Jobs and Save Spool Output

**Note:** The type of script that you write depends on the programming languages that you use and the environment where the script is executed. The following is a general guide to Zowe CLI scripts. Refer to third-party documentation to learn more about scripting in general.

#### Follow these steps:

1. Create a new file on your computer with the extension .sh. For example, testScript.sh.

**Note:** On Mac and Linux, an extension is not required. To make the file executable, issue the command chmod u+x testScript.

2. (Mac and Linux only) At the top of the file, specify the interpreter that your script requires. For example, type #!/bin/sh or #!/bin/bash.

**Note:** The command terminal that you use to execute the script depends on what you specify at the top of your script. Bash scripts require a bash interpreter (bash terminal), while shell scripts can be run from any terminal.

3. Write a script using a series of Zowe CLI commands.

**Tip:** You can incorporate commands from other command-line tools in the same script. You might choose to "pipe" the output of one command into another command.

4. From the appropriate command terminal, issue a command to execute the script. The command you use to execute script varies by operating system.

The script runs and prints the output in your terminal. You can run scripts manually, or include them in your automated testing and delivery pipelines.

#### Sample script library

Refer to the Zowe CLI Sample Scripts repository for examples that cover a wide range of scripting languages and use cases.

#### Example: Clean up Temporary Data Sets

The script in this example lists specified data sets, then loops through the list of data sets and deletes each file. You can use a similar script to clean up temporary data sets after use.

**Note:** This script must be run from a bash terminal.

#### Example: Submit Jobs and Save Spool Output

The script in this example submits a job, waits for the job to enter output status, and saves the spool files to local files on your computer.

**Note:** This script must be run from a bash terminal.

# Understanding core command groups

Zowe CLI contains command groups that focus on specific business processes. For example, the zosfiles command group lets you interact with mainframe data sets. This article provides a brief synopsis of the tasks that you can perform with each group. For more information, see Display Zowe CLI Help.

The commands available in the product are organized in a hierarchical structure. Command groups (for example, zos-files) contain actions (for example, create) that let you perform actions on specific objects (for example, a specific type of data set). For each action that you perform on an object, you can specify options that affect the operation of the command.

Zowe CLI contains the following command groups:

### plugins

The plugins command group lets you install and manage third-party plug-ins for the product. Plug-ins extend the functionality of Zowe CLI in the form of new commands.

With the plugins command group, you can perform the following tasks:

- Install or uninstall third-party plug-ins.
- Display a list of installed plug-ins.
- Validate that a plug-in integrates with the base product properly.

**Note:** For more information about **plugins** syntax, actions, and options, open Zowe CLI and issue the following command:

#### profiles

The profiles command group lets you create and manage profiles for use with other Zowe CLI command groups. Profiles allow you to issue commands to different mainframe systems quickly, without specifying your connection details with every command.

With the profiles command group, you can perform the following tasks:

- Create, update, and delete profiles for any Zowe CLI command group that supports profiles.
- Set the default profile to be used within any command group.
- List profile names and details for any command group, including the default active profile.

**Note:** For more information about **profiles** syntax, actions, and options, open Zowe CLI, and issue the following command:

#### provisioning

The provisioning command group lets you perform IBM z/OSMF provisioning tasks with templates and provisioned instances from Zowe CLI.

With the provisioning command group, you can perform the following tasks:

- Provision cloud instances using z/OSMF Software Services templates.
- List information about the available z/OSMF Service Catalog published templates and the templates that you used to publish cloud instances.
- List summary information about the templates that you used to provision cloud instances. You can filter the information by application (for example, DB2 and CICS) and by the external name of the provisioned

instances.

• List detail information about the variables used (and their corresponding values) on named, published cloud instances.

**Note:** For more information about provisioning syntax, actions, and options, open Zowe CLI and issue the following command:

#### zos-console

The zos-console command group lets you issue commands to the z/OS console by establishing an extended Multiple Console Support (MCS) console.

With the zos-console command group, you can perform the following tasks: **Important!** Before you issue z/OS console commands with Zowe CLI, security administrators should ensure that they provide access to commands that are appropriate for your organization.

- Issue commands to the z/OS console.
- Collect command responses and continue to collect solicited command responses on-demand.

**Note:** For more information about **zos-console** syntax, actions, and options, open Zowe CLI and issue the following command:

#### zos-files

The zos-files command group lets you interact with data sets on z/OS systems.

With the zos-files command group, you can perform the following tasks:

- Create partitioned data sets (PDS) with members, physical sequential data sets (PS), and other types of data sets from templates. You can specify options to customize the data sets you create.
- Download mainframe data sets and edit them locally in your preferred Integrated Development Environment (IDE).
- Upload local files to mainframe data sets.
- List available mainframe data sets.
- Interact with VSAM data sets directly, or invoke Access Methods Services (IDCAMS) to work with VSAM data sets.

**Note:** For more information about <u>zos-files</u> syntax, actions, and options, open Zowe CLI and issue the following command:

#### zos-jobs

The zos-jobs command group lets you submit jobs and interact with jobs on z/OS systems.

With the zos-jobs command group, you can perform the following tasks:

- Submit jobs from JCL that resides on the mainframe or a local file.
- List jobs and spool files for a job.
- View the status of a job or view a spool file from a job.

**Note:** For more information about <u>zos-jobs</u> syntax, actions, and options, open Zowe CLI and issue the following command:

#### zos-uss

The zos-uss command group lets you issue Unix System Services shell commands by establishing an SSH connection to an SSH server.

With the zos-uss command group, you can perform the following task: **Important!** Before you issue z/OS UNIX System Services commands with Zowe CLI, security administrators must provide access for your user ID to login via SSH.

• Issue z/OS UNIX System Services shell commands over an SSH connection and stream back the response.

**Note:** For more information about <u>zos-uss</u> syntax, actions, and options, open Zowe CLI and issue the following command:

#### zos-workflows

The zos-workflows command group lets you create and manage z/OSMF workflows on a z/OS system.

With the zos-workflows command group, you can perform the following tasks:

- Create or register a z/OSMF workflow based on the properties on a z/OS system
- Start a z/OSMF workflow on a z/OS system.
- Delete or remove a z/OSMF workflow from a z/OS system.
- List the z/OSMF workflows for a system or sysplex.

**Note:** For more information about **zos-workflows** syntax, actions, and options, open Zowe CLI and issue the following command:

#### zos-tso

The zos-tso command group lets you issue TSO commands and interact with TSO address spaces on z/OS systems.

With the zos-tso command group, you can perform the following tasks:

- Execute REXX scripts
- Create a TSO address space and issue TSO commands to the address space.
- Review TSO command response data in Zowe CLI.

**Note:** For more information about <u>zos-tso</u> syntax, actions, and options, open Zowe CLI and issue the following command:

#### zosmf

The zosmf command group lets you work with Zowe CLI profiles and get general information about z/OSMF.

With the zosmf command group, you can perform the following tasks:

- Create and manage your Zowe CLI zosmf profiles. Profiles let you store configuration information for use on multiple commands. You can create a profile that contains your username, password, and connection details for a particular mainframe system, then reuse that profile to avoid typing it again on every command. You can switch between profiles to quickly target different mainframe subsystems. For more information, see Using profiles.
- Verify that your profiles are set up correctly to communicate with z/OSMF on your system. For more information, see Test Connection to z/OSMF.
- Get information about the current z/OSMF version, host, port, and plug-ins installed on your system.

**Note:** For more information about **zosmf** syntax, actions, and options, open Zowe CLI and issue the following command:

# **Extending Zowe CLI**

You can install plug-ins to extend the capabilities of Zowe™ CLI. Plug-ins CLI to third-party applications are also available, such as Visual Studio Code Extension for Zowe (powered by Zowe CLI). Plug-ins add functionality to the product in the form of new command groups, actions, objects, and options.

**Important!** Plug-ins can gain control of your CLI application legitimately during the execution of every command. Install third-party plug-ins at your own risk. We make no warranties regarding the use of third-party plug-ins.

- Install plug-ins
- IBM® CICS Plug-in for Zowe CLI
- IBM® Db2® Database Plug-in for Zowe CLI
- IBM® z/OS FTP Plug-in for Zowe CLI
- IBM<sup>®</sup> IMS<sup>™</sup> Plug-in for Zowe CLI
- IBM® MQ Plug-in for Zowe CLI
- Secure Credential Store for Zowe CLI
- Visual Studio Code (VSCode) Extension for Zowe

Version: v1.25.x LTS

# Software requirements for Zowe CLI plug-ins

Before you use Zowe™ CLI plug-ins, complete the following steps:

**Important!** You can perform the required configurations for the plug-ins that you want to use **before** or **after** you install the plug-ins. However, if you do not perform the required configurations, the plug-ins will not function as designed.

Plug-in	Required Configurations
IBM CICS Plug- in for Zowe CLI	<ul> <li>Ensure that IBM CICS Transaction Server v5.2 or later is installed and running in your mainframe environment</li> <li>IBM CICS Management Client Interface (CMCI) is configured and running in your CICS region.</li> </ul>
IBM Db2 Database Plug- in for Zowe CLI	<ul> <li>Download and prepare the ODBC driver (required for only package installations) and address the licensing requirements.</li> <li>(MacOS) Download and Install Xcode.</li> </ul>
IBM z/OS FTP Plug-in for Zowe CLI	<ul> <li>Ensure that z/OS FTP service is enabled and configured with JESINTERFACELEVEL = 2.</li> <li>FTP over SSL is recommended.</li> </ul>
IBM IMS Plug-in for Zowe CLI	<ul> <li>Ensure that IBM® IMS<sup>™</sup> v14.1.0 or later is installed and running in your mainframe environment.</li> <li>Configure IBM® IMS<sup>™</sup> Connect.</li> <li>Configure IBM IMS Operations APIs to enable communication between the CLI and the IMS instance.</li> </ul>
IBM MQ Plug-in for Zowe CLI	<ul> <li>Ensure that IBM<sup>®</sup> MQ<sup>™</sup> v9.1.0 or later is installed and running in your mainframe environment. Please read this blog for more information: Exposing the MQ REST API via the Zowe API Mediation Layer</li> </ul>

Plug-in	Required Configurations	
Secure Credential Store Plug-in for Zowe CLI	<ul> <li>(Graphical Linux) Install gnome-keyring and libsecret on your computer.</li> <li>There are additional requirements for headless Linux systems. See the SCS plug-in Readme for details.</li> </ul>	

**Important!** You can perform the required configurations for the plug-ins that you want to use **before** or **after** you install the plug-ins. However, if you do not perform the required configurations, the plug-ins will not function as designed.

# Installing Zowe CLI plug-ins

Use commands in the plugins command group to install and manage Zowe™ CLI plug-ins.

**Important!** Plug-ins can gain control of your CLI application legitimately during the execution of commands. Install third-party plug-ins at your own risk. We make no warranties regarding the use of third-party plug-ins.

You can install the following Zowe plug-ins:

- IBM® CICS® Plug-in for Zowe CLI
- IBM® Db2® Plug-in for Zowe CLI
- Third-party Zowe Conformant Plug-ins

Use either of the following methods to install plug-ins:

• Install from an online NPM registry. Use this method when your computer *can* access the Internet.

For more information, see Installing plug-ins from an online registry.

 Install from a local package. With this method, you download and install the plug-ins from a bundled set of .tgz files. Use this method when your computer *cannot* access the Internet.

For more information, see Installing plug-ins from a local package.

## Installing plug-ins from an online registry

Install Zowe CLI plug-ins using npm commands on Windows, Mac, and Linux. The procedures in this article assume that you previously installed the core CLI.

### Follow these steps:

- 1. Meet the software requirements for each plug-in that you install.
- 2. Issue the following command to install a plug-in from public npm:

**Note:** Replace <my-plugin> with the installation command syntax in the following table:

Plug-in	Installation Command Syntax
IBM CICS Plug-in for Zowe CLI	<pre>@zowe/cics-for-zowe-cli@zowe-v1-lts</pre>
IBM Db2 Plug-in for Zowe CLI	<pre>@zowe/db2-for-zowe-cli@zowe-v1-lts</pre>
IBM z/OS FTP Plug-in for Zowe CLI	<pre>@zowe/zos-ftp-for-zowe-cli@zowe-v1-lts</pre>
IBM IMS Plug-in for Zowe CLI	<pre>@zowe/ims-for-zowe-cli@zowe-v1-lts</pre>
IBM MQ Plug-in for Zowe CLI	<pre>@zowe/mq-for-zowe-cli@zowe-v1-lts</pre>
Secure Credential Store Plug-in for Zowe CLI	<pre>@zowe/secure-credential-store-for-zowe- cli@zowe-v1-lts</pre>

3. (Optional) Issue the following command to install two or more plug-ins using one command. Separate the <my-plugin> names with one space.

**Note:** The IBM Db2 Plug-in for Zowe CLI requires additional licensing and ODBC driver configurations. If you installed the DB2 plug-in, see IBM Db2 Plug-in for Zowe CLI.

You installed Zowe CLI plug-ins.

## Installing plug-ins from a local package

Install plug-ins from a local package on any computer that has limited or no access to the Internet. The procedure assumes that you previously installed the core CLI.

#### Follow these steps:

- 1. Meet the software requirements for each plug-in that you want to install.
- 2. Obtain the installation files.

From the Zowe Download website, click **Download Zowe CLI** to download the Zowe CLI installation package named zowe-cli-package-\*v\*.\*r\*.\*m\*.zip to your computer.

Note: v indicates the version, r indicates the release number, and m indicates the modification number

3. Open a command-line window, such as Windows Command Prompt. Browse to the directory where you downloaded the Zowe CLI installation package (.zip file). Issue the following command, or use your preferred method to unzip the files:

### Example:

By default, the unzip command extracts the contents of the zip file to the directory where you downloaded the .zip file. You can extract the contents of the zip file to your preferred location.

4. Issue the following command against the extracted directory to install each available plug-in:

Replace <my-plugin> with the .tgz file name listed in the following table:

Plug-in	.tgz File Name
IBM CICS Plug-in for Zowe CLI	cics-for-zowe-cli.tgz
IBM Db2 Plug-in for Zowe CLI	db2-for-zowe-cli.tgz
IBM z/OS FTP Plug-in for Zowe CLI	<pre>zos-ftp-for-zowe-cli.tgz</pre>
IBM IMS Plug-in for Zowe CLI	<pre>ims-for-zowe-cli.tgz</pre>
IBM MQ Plug-in for Zowe CLI	mq-for-zowe-cli.tgz
Secure Credential Store Plug-in for Zowe CLI	<pre>secure-credential-store-for-zowe- cli.tgz</pre>

You installed Zowe CLI plug-ins.

## Validating plug-ins

Issue the plug-in validation command to run tests against all plug-ins (or against a plug-in that you specify) to verify that the plug-ins integrate properly with Zowe CLI. The tests confirm that the plug-in does not

conflict with existing command groups in the base application. The command response provides you with details or error messages about how the plug-ins integrate with Zowe CLI.

The validate command has the following syntax:

• **[plugin]** (Optional) Specifies the name of the plug-in that you want to validate. If you do not specify a plug-in name, the command validates all installed plug-ins. The name of the plug-in is not always the same as the name of the NPM package.

Plug-in	Installation Command Syntax
IBM CICS Plug-in for Zowe CLI	<pre>@zowe/cics-for-zowe-cli</pre>
IBM Db2 Plug-in for Zowe CLI	@zowe/db2-for-zowe-cli
IBM z/OS FTP Plug-in for Zowe CLI	<pre>@zowe/zos-ftp-for-zowe-cli</pre>
IBM IMS Plug-in for Zowe CLI	@zowe/ims-for-zowe-cli
IBM MQ Plug-in for Zowe CLI	@zowe/mq-for-zowe-cli
Secure Credential Store Plug-in for Zowe CLI	<pre>@zowe/secure-credential-store-for-zowe- cli</pre>

### **Examples: Validate plug-ins**

- The following example illustrates the syntax to use to validate the IBM CICS Plug-in for Zowe CLI:
- The following example illustrates the syntax to use to validate all installed plug-ins:

## **Updating plug-ins**

You can update Zowe CLI plug-ins from an online registry or from a local package.

### Update plug-ins from an online registry

Issue the update command to install the latest stable version or a specific version of a plug-in that you installed previously. The update command has the following syntax:

• [plugin...]

Specifies the name of an installed plug-in that you want to update. The name of the plug-in is not always the same as the name of the NPM package. You can use npm semantic versioning to specify a plug-in version to which to update. For more information, see npm semver.

### • [--registry \<registry>\]

(Optional) Specifies a registry URL that is different from the registry URL of the original installation.

### **Examples: Update plug-ins**

The following example illustrates the syntax to use to update an installed plug-in to the latest version:

The following example illustrates the syntax to use to update a plug-in to a specific version:

### Update plug-ins from a local package

You can update plug-ins from a local package. You acquire the media from the Zowe Download website and update the plug-ins using the zowe plugins install command.

To update plug-ins from a local package, follow the steps described in Installing plug-ins from a local package.

## **Uninstall Plug-ins**

Issue the uninstall command to uninstall plug-ins from Zowe CLI. After the uninstall process completes successfully, the product no longer contains the plug-in configuration.

The uninstall command contains the following syntax:

• [plugin]

Specifies the name of the plug-in that you want to uninstall.

The following table describes the uninstallation command syntax for each plug-in:

Plug-in	Installation Command Syntax
IBM CICS Plug-in for Zowe CLI	@zowe/cics-for-zowe-cli
IBM Db2 Plug-in for Zowe CLI	@zowe/db2-for-zowe-cli
IBM z/OS FTP Plug-in for Zowe CLI	@zowe/zos-ftp-for-zowe-cli
IBM IMS Plug-in for Zowe CLI	<pre>@zowe/ims-for-zowe-cli</pre>
IBM MQ Plug-in for Zowe CLI	<pre>@zowe/mq-for-zowe-cli</pre>
Secure Credential Store Plug-in for Zowe CLI	<pre>@zowe/secure-credential-store-for-zowe- cli</pre>

### Example:

The following example illustrates the command to uninstall the CICS plug-in:

# IBM® CICS® Plug-in for Zowe CLI

The IBM® CICS® Plug-in for Zowe<sup>™</sup> CLI lets you extend Zowe CLI to interact with CICS programs and transactions. The plug-in uses the IBM CICS® Management Client Interface (CMCI) API to achieve the interaction with CICS. For more information, see CICS management client interface on the IBM Knowledge Center.

- Use Cases
- Commands
- Software requirements
- Installing
- Creating a user profile

## Use cases

As an application developer, you can use the plug-in to perform the following tasks:

- Deploy code changes to CICS applications that were developed with COBOL.
- Deploy changes to CICS regions for testing or delivery. See the define command for an example of how you can define programs to CICS to assist with testing and delivery.
- Automate CICS interaction steps in your CI/CD pipeline with Jenkins Automation Server or TravisCI.
- Deploy build artifacts to CICS regions.
- Alter, copy, define, delete, discard, and install CICS resources and resource definitions.

## Commands

For detailed documentation on commands, actions, and options available in this plug-in, see our Web Help. It is available for download in three formats: a PDF document, an interactive online version, and a ZIP file containing the HTML for the online version.

- Browse Online
- Download (ZIP)
- Download (PDF)

## Software requirements

Before you install the plug-in, meet the software requirements in Software requirements for Zowe CLI plugins.

## Installing

Use one of the following methods to install or update the plug-in:

- Installing plug-ins from an online registry
- Installing plug-ins from a local package

## **Creating a user profile**

You can set up a CICS profile to avoid typing your connection details on every command. The profile contains your host, port, username, and password for the CMCI instance of your choice. You can create multiple profiles and switch between them if necessary. Issue the following command to create a cics profile:

The plug-in uses HTTPS by default. Use the optional flag --protocol http to override the default with HTTP.

**Note:** For more information, issue the command zowe profiles create cics --help

Version: v1.25.x LTS

# IBM® Db2® Database Plug-in for Zowe CLI

The IBM® Db2® Database Plug-in for Zowe™ CLI lets you interact with Db2 for z/OS to perform tasks through Zowe CLI and integrate with modern development tools. The plug-in also lets you interact with Db2 to advance continuous integration and to validate product quality and stability.

Zowe CLI Plug-in for IBM Db2 Database lets you execute SQL statements against a Db2 region, export a Db2 table, and call a stored procedure. The plug-in also exposes its API so that the plug-in can be used directly in other products.

[[toc]]

## Use cases

As an application developer, you can use Zowe CLI Plug-in for IBM DB2 Database to perform the following tasks:

- Execute SQL and interact with databases.
- Execute a file with SQL statements.
- Export tables to a local file on your computer in SQL format.
- Call a stored procedure and pass parameters.

## Commands

For detailed documentation on commands, actions, and options available in this plug-in, see our Web Help. It is available for download in three formats: a PDF document, an interactive online version, and a ZIP file containing the HTML for the online version.

- Browse Online
- Download (ZIP)
- Download (PDF)

## Software requirements

Before you install the plug-in, meet the software requirements in Software requirements for Zowe CLI plugins.

## Installing

Use one of the following methods to install the the Zowe CLI Plug-in for IBM Db2 Database:

- Install from an online registry
- Install from a local package

### Installing from an online registry

If you installed Zowe CLI from **online registry**, complete the following steps:

- 1. Open a commandline window and issue the following command:
- 2. Address the license requirements to begin using the plug-in.

### Installing from a local package

Follow these procedures if you downloaded the Zowe installation package:

### Downloading the ODBC driver

Download the ODBC driver before you install the Db2 plug-in.

### Follow these steps:

- 1. Download the ODBC CLI Driver. Use the table within the download URL to select the correct CLI Driver for your platform and architecture.
- 2. Create a new directory named odbc\_cli on your computer. Remember the path to the new directory. You will need to provide the full path to this directory immediately before you install the Db2 plug-in.
- 3. Place the ODBC driver in the odbc\_cli folder. **Do not extract the ODBC driver**.

You downloaded and prepared to use the ODBC driver successfully. Proceed to install the plug-in to Zowe CLI.

### Installing Xcode on MacOS

To install the Db2 CLI plug-in on MacOS, you need the command line tools, which can be obtained by installing Xcode from the App Store.

**Note:** On some versions of MacOS, you may receive the error xcrun: error: invalid active developer path as shown below:

If this occurs, a manual refresh of the command line tools is required by running the following commands:

### Installing the plug-in

Now that the Db2 ODBC CLI driver is downloaded, set the IBM\_DB\_INSTALLER\_URL environment variable and install the Db2 plug-in to Zowe CLI.

### Follow these steps:

- Open a command line window and change the directory to the location where you extracted the zowecli-bundle.zip file. If you do not have the zowe-cli-bundle.zip file, see the topic Install
   Zowe CLI from local package in Installing Zowe CLI for information about how to obtain and extract it.
- 2. From a command line window, set the IBM\_DB\_INSTALLER\_URL environment variable by issuing the following command:
  - Windows operating systems:
  - Linux and Mac operating systems:

For example, if you downloaded the Windows x64 driver (ntx64\_odbc\_cli.zip) to C:\odbc\_cli, you would issue the following command:

- 3. Issue the following command to install the plug-in:
- 4. Address the license requirements to begin using the plug-in.

## Addressing the license requirement

To successfully connect the Db2 CLI plug-in to a database on z/OS, a license needs to be present either on the client where the Zowe CLI is executed from, or else on z/OS. If you don't have a license configured when you execute Db2 CLI commands, you will receive an error SQL1598N, for example:

### Server-side license

You can execute the utility db2connectactivate on z/OS to enable a Db2 database to accept client requests. For more information, see db2connectactivate - Server license activation utility. This avoids having to apply the Db2 Connect license on each database client that connects directly to the server. It is also the preferred approach to enabling users of the Zowe Db2 CLI because it avoids individual client license distribution and configuration.

### **Client-side license**

If the utility db2connectactivate has not been executed against the Db2 database that your profile is connecting to, then it is possible to obtain the license file db2consv\_zs.lic from a copy of DB2 Connect and use this for client configuration. This will need to be done separately for each client PC.

1. Locate your client copy of the Db2 license file db2consv\_zs.lic.

**Note:** The license must be of version 11.5 if the Db2 server is not **db2connectactivated**. You can buy a db2connect license from IBM. The connectivity can be enabled either on server using db2connectactivate utility or on client using client side license file. To know more about DB2 license and purchasing cost, please contact IBM Customer Support.

2. Copy your Db2 license file db2consv\_za.lic and place it in the following directory.

**Tip:** By default, <zowe\_home> is set to ~/.zowe on \*UNIX Aand Mac systems, and C:\Users\ <Your\_User>\.zowe on Windows systems.

After the license is copied, you can use the Db2 plugin functionality.

## **Creating a user profile**

Before you start using the IBM Db2 plug-in, create a profile with details of the Db2 system you're connecting to.

- The Db2 server host name
- The Db2 server port number
- The database name (you can also use the location)

To get the Db2 system information, the following two methods can be used.

• Issue the command –DISPLAY DDF in the Db2 SPUFI command on z/OS

or

View the JES spool for the MSTR job for the Db2 subsystem and search for the message DSNL0041.
 For example, for the database DI2E the JES job DI2EMSTR will have an entry with similar to:

The DOMAIN is used for the <hostname>, the TCPPORT for the <port> and the LOCATION for the <database> in the zowe create profile command.

In addition to the host, port and database you'll need

- The user name
- The password
- If your Db2 systems use a secure connection, you can also provide an SSL/TSL certificate file.

To create a db2 profile in Zowe CLI, issue the following command with your connection details for the Db2 instance:

**Note** For more information, issue the command zowe profiles create db2-profile --help

### SQL0805N: Database BIND

To be able to run remote SQL commands against a Db2 database, you must invoke a **BIND** command against it. If the **BIND** command is not run, you will see an error that contains **SQL0805N** similar to the log below:

If you receive this error, a user with DBADM authority must run the BIND command. This will typically be done by a Db2 System Programmer. More information can be found in the Db2 product documentation and The Bind process.

# IBM® z/OS FTP Plug-in for Zowe CLI

The IBM® z/OS FTP Plug-in for Zowe™ CLI lets you extend Zowe CLI to access z/OS datasets, USS files, and submit JCL. The plug-in uses the z/OS FTP service to achieve the interaction with z/OS.

- Use Cases
- Commands
- Software requirements
- Installing
- Creating a user profile

## Use cases

As a z/OS user, you can use the plug-in to perform the following tasks:

- List, view, rename, and download z/OS datasets or USS files.
- Upload local files or stdin to z/OS datasets or USS files.
- List, view, and download job status or job spool files.
- Delete a z/OS dataset, USS file, or job.

## Commands

For detailed documentation on commands, actions, and options available in this plug-in, see our Web Help. It is available for download in three formats: a PDF document, an interactive online version, and a ZIP file containing the HTML for the online version.

- Browse Online
- Download (ZIP)
- Download (PDF)

## Software requirements

Before you install the plug-in, meet the software requirements in Software requirements for Zowe CLI plugins.

## Installing

Use one of the following methods to install or update the plug-in:

- Installing plug-ins from an online registry
- Installing plug-ins from a local package

## **Creating a user profile**

You can create a zftp user profile to avoid typing your connection details on every command. A zftp profile contains the host, port, username, and password for the z/OS instance to which you want to connect. You can create multiple profiles and switch between them as needed.

Issue the following command:

**Note:** There is an option named --secure-ftp that is set to true by default. If FTPS (FTP over SSL) is not enabled in z/OS FTP service, we recommend using --secure-ftp false. FTPS is not equivalent to SFTP (FTP over SSH).

**Note:** For more information about the syntax, actions, and options, for a profiles create command, open Zowe CLI and issue the following command:

# IBM<sup>®</sup> IMS<sup>™</sup> Plug-in for Zowe CLI

The IBM IMS Plug-in for Zowe CLI lets you extend Zowe CLI such that it can interact with IMS resources (regions, programs and transactions). You can use the plug-in to start, stop, and query regions and start, stop, query, and update programs and transactions.

**Note:** For more information about IMS, see IBM Information Management System (IMS) on the IBM Knowledge Center.

[[toc]]

## **Use cases**

As an application developer or DevOps administrator, you can use IBM IMS Plug-in for Zowe CLI to perform the following tasks:

- Refresh IMS transactions, programs, and dependent IMS regions.
- Deploy application code into IMS production or test systems.
- Write scripts to automate IMS actions that you traditionally perform using ISPF editors, TSO, and SPOC.

## Commands

For detailed documentation on commands, actions, and options available in this plug-in, see our Web Help. It is available for download in three formats: a PDF document, an interactive online version, and a ZIP file containing the HTML for the online version.

- Browse Online
- Download (ZIP)
- Download (PDF)

## Software requirements

Before you install the plug-in, meet the software requirements in Software requirements for Zowe CLI plugins.

## Installing

Use one of the following methods to install or update the plug-in:

- Installing plug-ins from an online registry
- Installing plug-ins from a local package

## **Creating user profiles**

You can set up an *ims* profile to retain your credentials, host, and port name. You can create multiple profiles and switch between them as needed. Issue the following command to create an *ims* profile:

### Example: Setting up an IMS profile

The following example creates an ims profile named 'ims123' to connect to IMS APIs at host zos123 and port 1490. The name of the IMS plex in this example is 'PLEX1' and the IMS region we want to communicate with has a host of zos124 and a port of 1491:

Note: For more information, issue the command zowe profiles create ims-profile --help.

# IBM® MQ Plug-in for Zowe CLI

The IBM MQ Plug-in for Zowe CLI lets you issue MQSC commands to a queue manager. MQSC commands let you to perform administration tasks. For example, you can define, alter, or delete a local queue object.

**Note:** For more information about MQSC commands and the corresponding syntax, see MQSC commands on the IBM Knowledge Center.

[[toc]]

## Use cases

You can use the plug-in to execute MQSC Commands. With MQSC commands you can manage queue manager objects (including the queue manager itself), queues, process definitions, channels, client connection channels, listeners, services, namelists, clusters, and authentication information objects.

# Using IBM MQ plug-in commands

For detailed documentation on commands, actions, and options available in this plug-in, see our Web Help. It is available for download in three formats: a PDF document, an interactive online version, and a ZIP file containing the HTML for the online version.

- Browse Online
- Download (ZIP)
- Download (PDF)

## Software requirements

Before you install the plug-in, meet the software requirements in Software requirements for Zowe CLI plugins.

## Installing

Use one of the following methods to install or update the plug-in:

- Installing plug-ins from an online registry
- Installing plug-ins from a local package

## **Creating a user profile**

You can create an model user profile to avoid typing your connection details on every command. An model profile contains the host, port, username, and password for the MQ Rest API server of your choice. You can create multiple profiles and switch between them as needed.

### Follow these steps:

1. Create an mq profile:

The result of the command displays as a success or failure message. You can use your profile when you issue commands in the mq command group.

**Tip:** For more information about the syntax, actions, and options, for a profiles create command, open Zowe CLI and issue the following command:

# Secure Credential Store Plug-in for Zowe CLI

The Secure Credential Store (SCS) Plug-in for Zowe CLI lets you store your credentials securely in the credential manager of your operating system. The plug-in invokes a native Node module, keytar, that manages user IDs and passwords in a credential manager.

- Use Cases
- Commands
- Software requirements
- Installing
- Using

## **Use Cases**

Zowe CLI stores credentials (mainframe username and password) in plaintext on your computer by default. You can use the SCS plug-in to store credentials more securely and prevent your credentials from being compromised as a result of a malware attack or unlawful actions by others.

## Commands

For detailed command, actions, and option documentation for this plug-in, see our Web Help (available online or as PDF or ZIP):

- Browse Online
- Download (ZIP)
- Download (PDF)

## Software requirements

Before you install the plug-in, meet the software requirements in Software requirements for Zowe CLI plugins.

**Note:** If you're using npm@7, an Internet connection is required during installation of the Secure Credential Store plug-in. Additionally, there is a prerequisite on Windows for npm@7 users: npm install -g

## Installing

Use one of the following methods to install or update the plug-in:

- Installing plug-ins from an online registry
- Installing plug-ins from a local package

Note: Existing user profiles are not automatically updated to securely store credentials.

## Using

The plug-in introduces a new command group, zowe scs, that lets you update existing user profiles and enable/disable the plug-in.

### Securing your credentials

User profiles that you create *after* installing the plug-in will automatically store your credentials securely.

To secure credentials in existing user profiles (profiles that you created prior to installing the SCS plug-in), issue the following command:

Profiles are updated with secured credentials.

#### **Example: Secure credentials**

The following is an example of securely stored credentials in a user profile configuration file:

#### Example: Default credential management

The following is an example of credentials that are stored with the *default* credential manager:

### Deactivating the plug-in

If you do not want to use the SCS Plug-in for Zowe CLI, choose one of the following methods to deactivate the plug-in:

### Uninstall the Plug-in

Issue the zowe plugins uninstall @zowe/secure-credential-store-for-zowe-cli command to delete the plug-in from your computer.

When you uninstall the plug-in, existing profiles become invalid and you must recreate them. For more information, see Using profiles.

### Reset the Configuration of Credential Manager

Issue the zowe config reset CredentialManager command to reset the value of the credential manager configuration to default, which deactivates the plug-in.

Version: v1.25.x LTS

# **Using Zowe Explorer**

Review this section to familiarize yourself with the extension and make the best use of available options and features. The section contains usage tips and sample use cases for data sets, USS files, JOBs, and TSO commands.

## Usage Tips

Make the best use of the extension with the following tips:

- Data set, USS and jobs persistence settings: You can store any of data sets, USS files, or jobs permanently in the Favorites tab. Right-click on a data set, USS file, or job and click Add Favorite.
- Identify syntax errors with a syntax highlighter: Zowe Explorer supports a syntax hightlighter for data sets. To enhance the experience of using the extension, you can download an extension that highlights syntax.
- Edit a profile: You can edit existing profiles by clicking the **pencil** button next to the **magnifying glass** button in the explorer tree. The feature lets you modify the information inside your profile.
- Delete a profile: You can permanently delete profiles by right-clicking the profile and selecting the Delete Profile option. The feature deletes a profile from your . zowe folder. Alternatively, you can delete a profile from the VSCode Command Palette.

### Follow these steps:

- i. Press **F1** on your keyboard.
- ii. Select the Zowe: Delete a Profile Permanently option.
- Hide a profile: You can hide a profile from profile tree by right-clicking the profile and selecting the
   Hide Profile option. If necessary, add the profile back by clicking the + button from the explorer tree.
- **Open recent members**: Zowe Explorer lets you open a list of members you worked on earlier. You can access the list by pressing Ctrl+Alt+R or Command+Alt+R.

## Sample Use Cases

Review the following use cases to understand how to use Zowe Explorer.

- Work with Data Sets
- Work with USS Files
- Work with jobs
- MVS and TSO Commands

### Work with Data Sets

You can use the following functionalities when interacting with data sets:

- View data sets and use multiple filters: You can view multiple data sets simultaneously and apply filters to show specified data sets.
- View data sets with member filters: You can apply filters to show specified data set members.
- Refresh the list of data sets:
- Rename data sets: You can rename specified data sets.
- Copy data set members: You can copy a specified data sets and members.
- Edit and upload a data set member: You can instantly pull data sets and data set members from the mainframe, edit them and upload back.
- Prevent merge conflicts: You can prevent merge conflicts by using the Save functionality.
- Create data sets and specify the parameters: You can create a new data set and specify parameter values.
- Create data sets and data set members: You can create a new data set and data set members.
- Delete a data set member and a data set: You can delete a data set and data set member.
- View and access multiple profiles simultaneously: You can work with data sets from multiple profiles.
- **Submit a JCL**: You can submit a jcl from a chosen data set.
- Allocate Like: You can create a copy of a chosen data set with the same parameters.

### View data sets and use multiple filters

- 1. Navigate to the explorer tree.
- 2. Open the **DATA SETS** bar.
- 3. Select the profile that you want to filter.
- 4. Click the Search Data Sets by Entering Patterns magnifying glass.
- 5. From the drop-down, enter the patterns that you want to filter.

The data sets that match your pattern(s) display in the explorer tree.

**Tip:** To provide multiple filters, separate entries with a comma. You can append or postpend any filter with an \*, which indicates wildcard searching. You cannot enter an \* as the entire pattern.

### View data sets with member filters

- 1. Navigate to the explorer tree.
- 2. Open the **DATA SETS** bar.
- 3. Click the **magnifying glass** icon.
- 4. Enter a search pattern in the HLQ.ZZZ.SSS(MEMBERNAME) format to filter out and display the specified member in the tree.

### Refresh the list of data sets

- 1. Navigate to the explorer tree.
- 2. Click **Refresh All** button on the right of the **DATA SETS** explorer bar.

#### Rename data sets

- 1. Navigate to the explorer tree.
- 2. Open the **DATA SETS** bar.
- 3. Select a data set you want to rename.
- 4. Right-click the data set and select the **Rename Data Set** option.
- 5. Change the name of the data set.

### Copy data set members

- 1. Navigate to the explorer tree.
- 2. Open the **DATA SETS** bar.
- 3. Select a member you want to copy.
- 4. Right-click the member and select the **Copy Data Set** option.
- 5. Right-click the data set where the member belongs and select the **Paste Data Set** option.
- 6. Enter the name of the copied member.

### Edit and upload a data set member

- 1. Navigate to the explorer tree.
- 2. Open the **DATA SETS** bar.
- 3. Open a profile.
- 4. Select the PDS member (or PS) that you want to download.

**Note:** To view the members of a PDS, click on the PDS to expand the tree.

The PDS member displays in the text editor window of VSC.

- 5. Edit the document.
- 6. Navigate back to the PDS member (or PS) in the explorer tree, and click the **Save** button.

Your PDS member (or PS) is uploaded.

**Note:** If someone else has made changes to the PDS member (or PS) while you were editing it, you can merge your conflicts before uploading to the mainframe.

#### **Prevent merge conflicts**

- 1. Navigate to the explorer tree.
- 2. Open the **DATA SETS** bar.
- 3. Open a member of a data set you want to edit.
- 4. Edit the member.
- 5. Press Ctrl+S or Command+S (OSx) to save you changes.
- 6. (Optional) Resolve merge conflicts if necessary.

#### Create data sets and specify the parameters

1. Navigate to the explorer tree.

2. Open the **DATA SETS** bar.

- 3. Right-click the profile you want to create a data set with and select **Create New Data Set**.
- 4. Enter a name for your data set.
- 5. From the drop-down menu, select the data set type that you want to create.
- 6. Select Edit Attributes in the drop-down menu.

The attributes list for the data set appears. You can edit the following attributes:

- Allocation Unit
- Average Block Length
- Block Size
- Data Class
- Device Type
- Directory Block
- Data Set Type
- Management Class
- Data Set Name
- Data Set Organization
- Primary Space
- Record Format
- Record Length
- Secondary Space
- Size
- Storage Class

- Volume Serial
- 7. Select the attribute you want to edit, provide the value in the command palette, and click **Enter**.
- 8. (Optional) Edit the parameters of your data set.
- 9. Select the + Allocate Data Set option to create the data set. You successfully created a data set.

### Create data sets and data set members

- 1. Navigate to the explorer tree.
- 2. Open the **DATA SETS** bar.
- 3. Right + click on the profile where you want to create a data set and select **Create New Data Set**.
- 4. Enter a name for your data set.
- 5. From the drop-down menu, select the data set type that you want to create.
- 6. Select +Allocate Data Set to create your data set.
- 7. Right-click your newly-created data set and select **Create New Member**.
- 8. Enter a name for your new data set member and click **Enter**. The member is created and opened in the workspace.

### Delete a data set member and a data set

- 1. Navigate to the explorer tree.
- 2. Open the **DATA SETS** bar.
- 3. Open the profile and PDS containing the member.
- 4. Right-click on the PDS member that you want to delete and select **Delete Member**.
- 5. Confirm the deletion by clicking **Yes** on the drop-down menu.

Note: Alternatively, you can select 'No' to cancel the deletion.

6. To delete a PDS, right-click the PDS and click **Delete PDS**, then confirm the deletion.

**Note:** You can delete a PDS before you delete its members.

### View and access multiple profiles simultaneously

- 1. Navigate to the explorer tree.
- 2. Open the **DATA SETS** bar.
- 3. Click the **Add Profile** button on the right of the **DATA SET** explorer bar.
- 4. Select the profile that you want to add to the view as illustrated by the following screen.

#### Allocate Like

- 1. Navigate to the explorer tree.
- 2. Open the **DATA SETS** bar.
- 3. Right-click the data set and select the Allocate Like (New File with Same Attributes) option.
- 4. Enter the new data set name.

### Work with USS Files

You can use the following functionalities when interacting with USS files:

- View Unix System Services (USS) files: You can view multiple USS files simultaneously.
- Refresh the list of files: You can refresh the list of files.
- Rename USS files: You can rename USS files.
- Download, edit, and upload existing USS files: You can instantly pull USS files from the mainframe, edit them and upload back.
- Create and delete USS files and directories: Enables you to easily create and delete both USS files and directories.
- View and access multiple USS profiles simultaneously: Enables you to work with USS files from multiple profiles.

### View Unix System Services (USS) files

- 1. Navigate to the explorer tree.
- 2. Open the Unix System Services (USS) bar.

- 3. Select the profile that you want to filter.
- 4. Click the Search Unix System Services (USS) by Entering a Path magnifying glass.
- 5. From the drop-down, enter the path that you want as the root of your displayed tree. All child files and directories of that root file are displayed in the explorer tree.

**Note:** You will not be able to expand directories or files that you are not authorised for.

### Refresh the list of files

- 1. Navigate to the explorer tree.
- 2. Click **Refresh All** button on the right of the **Unix System Services (USS)** explorer bar as illustrated by the following screen:

### **Rename USS files**

- 1. Navigate to the explorer tree.
- 2. Open the **USS** bar.
- 3. Select a USS file you want to rename.
- 4. Right-click the USS file and select the **Rename USS file** option.
- 5. Change the name of the USS file.

### Download, edit, and upload existing USS files

1. Click the file that you want to download.

Note: To view the files within a directory, click the directory to expand the tree.

The file is displayed in the text editor window of VSC.

Note: If you define file associations with syntax coloring, the suffix of your file will be marked up.

- 2. Edit the document.
- 3. Press Ctrl+S or Command+S (OSx) to save the file

Your file is uploaded.

### Create and delete USS files and directories

#### **Create a directory**

- 1. Navigate to the explorer tree.
- 2. Open the Unix System Services (USS) bar.
- 3. Select a directory where you want to add the new directory.
- 4. Select the **Create directory** button and specify the directory name. The directory is created.

### Create a file

- 1. Navigate to the explorer tree.
- 2. Open the Unix System Services (USS) bar.
- 3. Select a directory where you want to add the new file to.
- 4. Select the **Create file** button and specify the file name. The file is created.

### Delete a file

- 1. Navigate to the explorer tree.
- 2. Open the Unix System Services (USS) bar.
- 3. Select a file you want to remove.
- 4. Select the **Delete** button and click \*Yes\*\* to confirm. The file is deleted.

### Delete a directory

- 1. Navigate to the explorer tree.
- 2. Open the Unix System Services (USS) bar.
- 3. Select a directory you want to remove.
- 4. Select the **Delete** button and click **Yes** to confirm. The directory and all child files and directories are deleted.

- 1. Navigate to the explorer tree.
- 2. Open the Unix System Services (USS) bar.
- 3. Click the Add Session button on the right of the Unix System Services (USS) explorer bar.
- 4. Select the profile that you want to add to the view as illustrated by the following screen.

### Work with jobs

You can use the following functionalities when interacting with jobs:

- View a job: You can view multiple jobs simultaneously.
- Download spool content: You can download spool content on your computer.

### View a job

- 1. Navigate to the explorer tree.
- 2. Open the **JOBS** bar.
- 3. Select a directory with JCL files.
- 4. Right-click on the JCL you want to view, and click Get JCL.

### Download spool content

- 1. Navigate to the explorer tree.
- 2. Open the **JOBS** bar.
- 3. Select a directory with JCL files.
- 4. Click the **Download** icon next to a folder with the spool content.
- 5. Save the file on your computer.

### **MVS and TSO Commands**

### **Issue MVS commands**

1. Right-click on your profile and search for the **Issue MVS Command** option. Select the **Zowe:Issue MVS Command** option.

Alternatively, press the F1 key on your keyboard, then select "the Zowe:Issue MVS Command option.

- 2. Enter a new command or select a saved command.
- 3. Press Enter to execute the command.

#### Issue TSO commands

1. Right-click on your profile and search for the **Issue TSO Command** option. Select the **Zowe:Issue TSO Command** option.

Alternatively, press the F1 key on your keyboard, then select "the Zowe:Issue TSO Command option.

- 2. Enter a new command or select a saved command.
- 3. Press Enter to execute the command.

The output is displayed.

Version: v1.25.x LTS

# Using Zowe SDKs

Leverage the Zowe Client Software Development Kits (SDKs) to build client applications and scripts that interface with the mainframe.

The SDKs include programmatic APIs, each of which performs a particular mainframe task. For example, one API package provides the ability to upload and download z/OS data sets. You can leverage that package to rapidly build a client application that interacts with data sets.

The following SDKs are available.

- Zowe Node.js Client SDK
- Zowe Python Client SDK

# **API documentation**

For details about the available API endpoints, browse or download the API Reference documentation.

## Software requirements

### Node.js

If you install Node SDK packages from the online registry, the required dependencies are installed automatically.

If you download Node SDK packages from Zowe.org, the folder contains dependencies that you must install manually. Extract the TGZ files from the folder, copy the files to your project, and issue the following commands to install the dependencies.

## Python

If you install Python SDK packages from the online registry, the required dependencies are installed automatically.

If you download the Python SDK packages from Zowe.org, the downloaded folder contains dependencies that you must install manually. Extract the WHL files from the folder, copy the files to your project, and issue

## **Getting started**

To get started, import the SDK packages to your project. You can pull the packages from an online registry, or download the packages from Zowe.org to install locally.

### Install SDK from online registry

Pull the packages from an online registry such as npm or PyPi.

#### Follow these steps:

- 1. In command-line window, navigate to your project directory. Issue the following command to install a package from the registry:
  - To import a Node.js package: npm install <PackageName>
  - To import a Python package: pip install <PackageName>

where <packageName> is the name of the SDK package that you want to install, such as zos-files-for-zowe-sdk.

The packages are installed. Node packages are defined in package.json in your project. Python packages are installed by default to \$PYTHONPATH/Lib/site-packages (Linux) or to the Python folder in your local /AppData folder (Windows).

- 2. **(Optional)** You might want to automatically update the SDK version when updates become available, or you might want to prevent automatic updates.
  - To define the versioning scheme for Node packages, use npm semver.
  - To define versioning for Python packages, specify versions or version ranges in a
     requirements.txt file checked-in to your project. More information, see pip documentation

## Install SDK from local package

Download and install the packages.

#### Follow these steps:

1. Navigate to Zowe.org Downloads. Select your desired programming language in the **Zowe Client SDKs** section.

The SDK is downloaded to your computer.

- 2. Unzip the SDK folder, which contains the packages for each set of functionality (such as z/OS Jobs). Copy each file that you want to install and paste them into your project directory.
- 3. Install required dependencies, which are included in the bundle. See Software requirements above for more information.
- 4. In a command-line window, navigate to your project directory. Issue one of the following commands.
  - To install a Node.js package: npm install <packageName>.tgz
  - To install a Python package: pip install <packageName>.whl

where <packageName> is the name of the package that you want to install, such as zos-files-for-zowe-sdk.

Repeat the command for each package that you need. Packages are now installed.

## Using

After you install the SDK, you can make API calls to the mainframe from within your project.

### Using - Node.js

For Node SDK usage and syntax examples, refer to the following package Readmes:

- Core libraries Use shared libraries, such as rest to access z/OSMF REST APIs, auth for connecting to token-based authentication services, and more.
- z/OS Console Perform z/OS console operations.
- z/OS Files Work with data sets on z/OS.
- z/OS Jobs Work with batch jobs on z/OS.
- z/OS Management Facility Return data about z/OSMF, such as connection status or a list of available systems.

- z/OS Provisioning Provision middleware and resources such as IBM CICS, IBM Db2, IBM MQ, and more.
- z/OS TSO Interact with TSO/E address spaces on z/OS.
- z/OS USS Work with UNIX system services (USS) files on z/OS.
- z/OS Workflows Create and manage z/OSMF workflows on z/OS.

## **Using - Python**

For information about the Python SDK, including usage and syntax examples, see the Python SDK ReadTheDocs.

## Contributing

For information about contributing to the open-source Zowe SDKs, see Developing for Zowe SDKs.

Version: v1.25.x LTS

## **Extending Zowe**

Zowe is designed as an extensible tools platform. One of the Zowe architecture goals is to provide consistent interoperability between all Zowe components including extensions. The Zowe Conformance Program defines the criteria to help accomplish the aforementioned goal. By satisfying the Zowe Conformance Program criteria, extension providers are assured that their software remains functional throughout the Zowe release cycle. For more information, see the Zowe Conformance Program.

Zowe can be extended in the following ways:

- Extend Zowe CLI
- Extend Zowe API Mediation Layer
  - Dynamic API registration
  - Static API registration
- Add a plug-in to the Zowe Desktop
- Sample extensions

**Note:** For more information on the architecture of Zowe, see Zowe Architecture.

## **Extend Zowe CLI**

Zowe CLI extenders can build plug-ins that provide new commands. Zowe CLI is built using Node.js and is typically run on a machine other than z/OS, such as a PC, where the CLI can be driven through a terminal or command prompt, or on an automation machine such as a DevOps pipeline orchestrator.

For more information about extending the Zowe CLI, see Developing a new plug-in. This article includes a sample plug-in that is provided with the tutorial; see Installing the sample plug-in.

## **Extend Zowe API Mediation Layer**

Zowe API Mediation Layer extenders can build and onboard additional API services to the API ML microservices ecosystem. REST APIs can register with the API Mediation Layer, which makes them available in the API Catalog and for routing through the API Gateway.

To register a z/OS service with the API Mediation Layer, there are two approaches:

- Dynamic API registration
- Static API registration

For information about how to onboard REST APIs, see the Onboarding Overview.

## **Dynamic API registration**

Registration of a REST API service to the API ML is performed through a call to the Discovery Service by sending registration data and metadata for the service being registered. Registration requires that the z/OS service must know the web address of the API ML Discovery Service. When Dynamic registration is performed, the service that performs the registration must periodically send heartbeat requests to the Discovery Service for each registered service instance. These heartbeat requests serve to renew the corresponding service instance registration with API ML. These requests enable the Discovery Service to monitor the availability of registered service instances. Services that are registered dynamically display the status of the service in the API Catalog after initial service registration.

For more information about how to build a service which is able to register, see the Onboarding Overview.

### **Static API registration**

For services that cannot be modified to be dynamically discoverable, it is possible onboard them to the API ML by providing the API ML a static definition file with API service details. This registration method does not require modifications to the existing API service code. For more information, see Onboard a REST API without code changes required. Unlike services that use Dynamic API registration, the status of services onboarded through Static API registration is not displayed in the API Catalog.

## Add a plug-in to the Zowe Desktop

The Zowe Desktop allows a user to interact with z/OS applications through a web browser. The Desktop is served by the Zowe Application Framework Server on z/OS, also known as Z Lightweight User Experience (ZLUX). The Zowe desktop comes with a set of default applications. You can extend it to add new applications. For more information, see Developing for Zowe Application Framework.

The Zowe Desktop is an angular application that allows native plug-ins to be built that provide for a high level of interoperability with other desktop components. The React JavaScript toolkit is also supported. Additionally, you can include an existing web application in the Zowe Desktop using an iframe.

Notes: For more information, see the following samples:

- Sample iframe App.
- Sample Angular App.
- Sample React App.

## Sample extensions

#### Sample Zowe API and API Catalog extension

The repository https://github.com/zowe/sample-node-api contains a sample Zowe extension with a node server providing sample APIs for looking at cars in a dealership. For more information, see sample-node-api.

#### Sample Zowe Desktop extension

The repository https://github.com/zowe/sample-trial-app contains a sample Zowe extension with a node server providing a web page that gives a user interface to the APIs included with the API sample above.

# Packaging z/OS extensions

You can extend Zowe in multiple ways. You may extend Zowe with "microservices", which may start a new service within Zowe. You can also create Zowe App Framework plug-ins to provide UI to users.

Before you start, review the following terms first.

- **component**: is the most generic way to describe a program which can work within Zowe. It can be a microservice, a Zowe App Framework plug-in, or even just a shared program to be used by other Zowe components. This is also the generic word when referring to both Zowe core components and extensions. In most of the cases described in this topic, this terminology doesn't include programs running on the client side, like Zowe CLI plug-in or Zowe Explorer (VSCode extension).
- **extension**: is similar to **component** but excludes Zowe core components. It is recommended that you install all Zowe extensions into a shared extension directory.

## Zowe server component package format

You can package Zowe components (extensions) into various formats. You can package them as a standalone PAX, ZIP, or TAR file. You can also bundle and ship your Zowe extension(s) within another product.

A typical component package, for example, jobs-api-package-1.0.4.zip, consists of these files and directories:

where,

- manifest.yaml: This is the Zowe component manifest file. You can find detailed definition of manifest in Zowe Component Manifest.
- apiml-static-registration.yaml.template: This is a supporting file that instructs the Zowe launch script how to register this extension service to the API Mediation Layer Discovery service. In this case, this file is referred in the manifest.yaml apimlServices.static[0].file field. This file is optional depending on the function of the component and you can change and customize the file name in the manifest file.
- bin/(configure|start|validate).sh: These are Zowe component lifecycle scripts. You may not need these files depending on the function of the component. You can find detailed definition of lifecycle scripts in Zowe component runtime lifecycle.

It is also suggested that you put the following files into the package:

- **README.md**: This file is a brief introduction to your extension in Markdown format, including how it should be installed, configured, verified, and so on.
- LICENSE : This is the full license text file.

If you decide to bundle and ship Zowe extensions within another product, you can put the whole directory structure above into your product package as subdirectories. Take the following structure as an example.

## Zowe component manifest

Note: this feature is added with Zowe v1.19.0 release.

Zowe extensions, as well as core components, can use a manifest file to describe itself. The manifest file defines the name and purpose of the component. It also provides information about how this component should be installed, configured, started, and tested. It can be named as manifest.yaml, manifest.yml, or manifest.json and should locate in the root directory of the component. Currently, only YAML or JSON format is supported.

The manifest file contains the following properties:

- name: (Required) Defines a short, computer-readable name of the component. This component name will be used as directory name after it is installed. The allowed characters in the name are alphabets, numbers, hyphen (-) and underscore (\_). For example, explorer-jes is a valid extension name.
- **id**: (Optional) Defines a long, computer-readable identifier of the component. If the component is hosted as one of the projects in Open Mainframe Project, the identifier also matches the component path in the Zowe Artifactory. For example, org.zowe.explorer-jes is a valid identifier. You can locate the component's official releases by looking into the libs-release-

local/org/zowe/explorer-jes/ directory in the Zowe Artifactory.

- **version**: (Optional but recommended) This is the current version of the component without the prefix of v. For example, 1.0.4 is a valid version value.
- title: (Optional) Defines a short human-readable name for this component. This value will also be used as the default title for API Catalog tile, or App Framework plug-in title. For example, JES Explorer is a valid title for the explorer-jes component.
- **description**: (Optional) Defines a long human-readable description of this component. There is no restriction on what you can put in the field.

- **license** : (Optional but recommended) Defines the license code of the component. For example, Zowe core components have EPL-2.0 value in this field.
- **build**: (Optional but strongly recommended) Defines the build information of the current package, including git commit hash, and so on. When Zowe core components define manifest file, these fields are left as template variables. The template will be updated when a publishable package is created. It supports the following subfields:
  - **branch** : It tells the user which branch this package is built from.
  - **number**: You may create multiple packages in the same branch. This is the sequential number of the current package.
  - commitHash: This is the commit hash of the package that can be used to match the exact source code in the repository. Zowe core components usually use git rev-parse --verify HEAD to retrieve the commit hash.
  - **timestamp**: This is the UNIX timestamp when the package is created.
- **commands**: This defines actions that should be taken when the component is installed, configured, started, or tested. You must issue this command with one or more subfields as listed below. For example, commands.install. All subfields are optional and usually should point to a USS command or script.
  - **install**: This defines extra steps when installing this component. It will be automatically executed if you install your component with the <RUNTIME\_DIR>/bin/zowe-install-component.sh utility tool.
  - configureInstance: This defines extra steps when configuring the component for a Zowe instance. It will be automatically executed if you configure your component with the <a href="https://www.executed-if-wow-configure-component.sh">k</a> utility tool.
  - **validate**: This defines extra validations that the component requires other than global validations. It is for runtime purpose, and will be automatically executed each time Zowe is started.
  - **configure** : This defines extra configuration steps before starting the component. It is for runtime purpose, and will be automatically executed each time Zowe is started.
  - **start**: This tells the Zowe launch script how to start the component. It is for runtime purpose, and will be automatically executed each time Zowe is started.
- **apimlServices**: This section defines how the component will be registered to the API Mediation Layer Discovery Service. All subfields are optional.
  - **dynamic**: Array of objects. This information will tell Zowe and users what services you will register under the Discovery service.
    - **serviceId** : This defines the service ID registered to the Discovery service.

- **static**: Array of objects. When the component is statically registered under the Discovery service, this tells Zowe where to find these static definitions. This information is for the Zowe runtime. When Zowe is started, the launch script will check this field and put the parse static definition file into the directory defined as **STATIC\_DEF\_CONFIG\_DIR** in the Zowe instance.
  - **file**: Defines the path to the static definition file. This file is supposed to be a template.
- **appfwPlugins**: Array of objects. This section defines how the component will be registered to the App Framework plug-in. All subfields are optional.
  - path: This points to the directory where App Framework pluginDefinition.json file is located. If you use the <RUNTIME\_DIR>/bin/zowe-configure-component.sh utility tool to configure this component for an instance, the script will automatically execute
     <INSTANCE\_DIR>/bin/install-app.sh with this path.
- **zisPlugins**: List of ZIS plugin objects. This section defines the ZIS plugin(s) attributes necessary for ZIS plugin installation and automation.

i.e.

Please note: All paths of directories or files mentioned above should be relative paths to the root directory where manifest is located.

## Sample manifests

There are many examples you may find across Zowe GitHub repositories, for example:

- API Catalog manifest.yaml
- Jobs API manifest.yaml
- Sample Node API and API Catalog extension manifest.yaml
- Sample Zowe App Framework extension manifest.yaml

# Install, upgrade, and configure Zowe server component

Learn how to install, upgrade, and configure the Zowe server components or extensions manually or by using the following scripts:

- zowe-install-component.sh
- zowe-upgrade-component.sh (optional)
- zowe-configure-component.sh.

**Note:** The zowe-upgrade-component.sh script is currently an alpha release feature. As such, this script could present compatibility issues between the upgraded components and other Zowe components.

# Install with zowe-install-component.sh (Technical Preview)

Technical Preview

#### Notes:

- This section is for technical preview. As such, we welcome feedback. Content in this section may be changed or improved in the future.
- This feature is added with Zowe v1.19.0 release.

From Zowe v1.19.0, Zowe ships a bin/zowe-install-component.sh tool to help you install any Zowe server component (extension). Zowe core components are also installed with this utility. In order to be compatible with the utility, we recommend components follow Zowe server component package format standard.

Execute the utility from z/OS USS. Use the following command line parameters:

#### • -o|--component-file

(Required) Defines the path to the component package or directory.

-c|--component-name

Specifies the name of the component. This parameter is optional if **NODE\_HOME** is defined and the component has the manifest file, otherwise, this parameter is required.

#### -i|--instance-dir

(Optional) Defines the path to the Zowe instance directory. When a value is defined, the script also executes bin/zowe-configure-component.sh following installation.

#### -d|--target-dir

(Optional) Defines the path to the installation target directory. For native components, the default value is \${ZOWE\_ROOT\_DIR}/components. For non-native components, the script checks the value of the ZWE\_EXTENSION\_DIR variable. If the value is also empty, the script falls back to the default target directory /global/zowe/extensions.

#### -e|--auto-encoding

(Optional) Defines whether to automatically tag the encoding of the files that are shipped with the component. The default value is **auto**, which indicates that the script determines whether the automatic tagging is needed or not.

**Note:** The automatic tagging process is opinionated about which file extensions should be in which encoding. If this does not fit in your needs, a pax format is recommended to include the tagging information into your package. This option is only applicable for z/OS. The following list presents the allowed values:

This option automatically tag the encoding of the files.

• no

Do not automatically tag encoding of the files.

° auto

Tag only when manifest is in IS08859–1 encoding.

-k|--core

<sup>•</sup> yes

This is an optional boolean. This parameter defines whether this component is bundled into the Zowe package as a core component.

-l|--logs-dir

(Optional) Specifies the path to the log directory.

-f|--log-file

(Optional) Instead of writing an independent log to a directory, you have the option to append log to this log file specified.

#### **Examples:**

The following command installs the my-zowe-component-1.2.3.pax into /global/zowe/extensions.

The following command installs my-zowe-component-1.2.3.zip into /var/zowe/my-extensions and also configures this component for the Zowe instance located at /var/zowe/instance. The installation and configuration logs writes to /var/zowe/instance/logs.

# Upgrade with zowe-upgrade-component.sh (Technical Preview)

#### Technical Preview

#### Notes:

- This section is for technical preview. As such, we welcome any feedback. Content in this section may be changed or improved in the future.
- This feature is to be added with the Zowe v1.22.0 release.

From Zowe v1.22.0, Zowe ships a bin/zowe-upgrade-component.sh utility to help you upgrade any Zowe core component to the latest version available into the Zowe Artifactory. By default, Zowe core components are not updated with this utility. To enable the upgrade functionality, set the optional boolean value ZOWE\_COMPONENTS\_UPGRADE to true as part of the installation configuration. Once the user has enabled this parameter, the zowe-install.sh install script calls the zowe-upgrade-component.sh script. The Zowe components get updated and then installed and configured using the zowe-install-component.sh and zowe-configure-component.sh scripts. In order to be compatible with this utility, we recommend components follow the Zowe server component package format standard.

The Zowe upgrade component utility can be executed from z/OS USS. You can use the following command line parameters:

• -o|--component-file

(Required) Defines the path to the component package or directory.

• -l|--logs-dir

(Optional) Specifies the path to the log directory.

-f|--log-file

(Optional) Instead of writing independent log to a directory, you have option to append log to this log file specified.

#### **Examples:**

This command upgrades my-zowe-component-1.2.3.zip to its latest version. The upgrade logs write to /var/zowe/instance/logs.

# Configure with zowe-configure-component.sh (Technical Preview)

#### **Technical Preview**

Note: This section is for technical preview and we are happy to hear any feedback. Content in this section may be changed or improved in the future.

**Note:** This feature is made available with the Zowe v1.19.0 release.

From Zowe v1.19.0, Zowe ships a bin/zowe-configure-components.sh utility to help you configure an installed Zowe server component (extension) for a Zowe instance. Zowe core components are also configured with this utility. In order to be compatible with the utility, we recommend components follow Zowe server component package format standard.

You may not need to run this script directly if you have supplied -i|--instance-dir when you run zowe-install-component.sh.

Execute this utility from z/OS USS. Use the following command line parameters:

• -c|--component-name

(Required) Specifies the name of the component.

• -i|--instance-dir

(Required) Defines the path to the Zowe instance directory.

-d|--target-dir

(Optional) Defines the directory where the component is installed. For native components, the default value is \${ZOWE\_ROOT\_DIR}/components. For non-native components, the script will check ZWE\_EXTENSION\_DIR if possible. Otherwise, it will fall back to the default target directory /global/zowe/extensions.

-k|--core

This is an optional Boolean. It defines whether this component is bundled into the Zowe package as a core component.

-l|--logs-dir

(Optional) Defines the path to the log directory.

-f|--log-file

(Optional) Instead of writing independent log to a directory, you have option to append log to this log file specified.

### Examples:

The following command configures my-zowe-component installed in /global/zowe/extensions for the Zowe instance located at /var/zowe/instance.

The following command configures my-zowe-component installed in /var/zowe/my-extensions for the Zowe instance located at /var/zowe/instance. The configuration logs write to

## Install and configure manually

#### Zowe core components

The Zowe runtime directory delivers its core components in the <RUNTIME\_DIR>/components/ directory. A typical components directory looks like this:

You can configure whether to start the Zowe core component or not with the LAUNCH\_COMPONENTS variable defined in <INSTANCE\_DIR>/instance.env. The value of this variable can be a comma-separated list of core component names.

**Note:** You can also use the full USS path to the component **bin** directory which contains lifecycle scripts, but this behavior will be deprecated in next major release.

#### **Zowe extensions**

We recommend that you install all Zowe extension runtime programs into a single location. The suggested default extension directory is /global/zowe/extensions. Each extension should be represented with the extension name in this directory, and use either a directory or a symbolic link. This location should be defined as ZWE\_EXTENSION\_DIR in <INSTANCE\_DIR>/instance.env.

The Zowe launch script reads EXTERNAL\_COMPONENTS defined in <INSTANCE\_DIR>/instance.env to determine whether to start an extension. The value of EXTERNAL\_COMPONENTS is a comma-separated list of extension names.

**Note:** You can also use the full USS path to the extension **bin** directory which contains lifecycle scripts. This behavior, however, is to be deprecated in next major release.

#### Example:

The vendor MYVENDOR has a product named MYAPP that installs into /usr/lpp/myvendor/myapp. There is one Zowe extension shipped within the product in the directory

/usr/lpp/myvendor/myapp/zowe-ext. This subdirectory is a Zowe extension so that the product can be started and stopped with Zowe and run as an address space under the ZWESVSTC started task in the Zowe USS shell.

The directory /usr/lpp/myvendor/myapp/zowe-ext should include a manifest.yaml file to describe the extension. The script /usr/lpp/myvendor/myapp/zowe-ext/bin/validate.sh checks that the environment is configured correctly and the script /usr/lpp/myvendor/myapp/zowe-ext/bin/start.sh starts the vendor application. The /usr/lpp/myvendor/myapp/zowe-ext/bin/start.sh starts the vendor application. The /usr/lpp/myvendor/myapp/zowe-ext/bin/start.sh should look like this:

Because MYAPP is shipped within another product, the installation should create a symbolic link in ZWE\_EXTENSION\_DIR directory.

Also, myapp is added into the value of the EXTERNAL\_COMPONENTS variable in <INSTANCE\_DIR>/instance.env.

You might need to manually run the script <INSTANCE\_DIR>/bin/install-app.sh if your component is a Desktop plug-in. Alternatively, you can choose to add this step to Zowe component Configure lifecycle stage.

When the Zowe instance is launched by running <INSTANCE\_DIR>/bin/zowe-start.sh, it will read manifest commands instructions and call the /usr/lpp/myvendor/myapp/zowe-ext/bin/start.sh script. The started task will create an address space under ZWESVSTC for the vendor component. When the Zowe instance is stopped, the address space is terminated.

# Verify with zowe-verify-component.sh (Technical Preview)

#### Technical Preview

Note: This section is for technical preview and we are happy to hear any feedback. Content in this section may be changed or improved in the future.

Note: This feature is added with Zowe v1.22.0 release.

From Zowe v1.22.0, Zowe ships a bin/zowe-verify-component.sh tool to help you verify an installed Zowe server component (extension) for a Zowe instance. In order to be compatible with the tool, we recommend components follow Zowe server component package format standard and define Zowe component manifest.

The zowe-verify-component.sh script checks and verifies whether a specified component is up and running. You can use it to verify both core and external Zowe components.

IMPORTANT: To successfully verify whether a component service is registered on Zowe API Mediation Layer, this utility script requires authentication with a valid system user who has proper permission granted. For more information on the required user permission, please check Protection of Service Information.

The tool can be executed from z/OS USS, and it takes these command line parameters:

- **-c -component-id** : (Required) Specifies the name of the Zowe component that you want to verify.
- **-i** | **--instance-dir** : (Required) Specifies the path to the Zowe instance directory.
- **-u -username** : (Required) Username of a specified user for the current system.
- **-p|--password**: (Required) Password of the specified user.

#### Examples

This command will verify the external-zowe-component installed in /global/zowe/extensions for the Zowe instance installed at /var/zowe/instance.

You can also run the following commands to get the same results but instead of passing in values for the -u and -p parameters, you can use the export command.

## Zowe server component runtime lifecycle

## **Zowe runtime lifecycle**

This topic describes the runtime lifecycle of Zowe core components and how an offering that provides a Zowe extension can set up runtime lifecycle for their component.

The Zowe UNIX System Services (USS) components are run as part of the started task ZWESVSTC. For more information, see Starting Zowe from a USS shell. There are two key USS directories that play different roles when launching Zowe.

- The Zowe runtime directory <RUNTIME\_DIR> that contains the executable files is an immutable set of directories and files that are replaced each time a new release is applied. The initial release or an upgrade is installed either with UNIX shell scripts (see Installing Zowe runtime from a convenience build), or SMP/E where the runtime directory is laid down initially as FMID AZWE001 and then upgraded through rollup PTF builds (see Installing Zowe SMP/E). The Zowe runtime directory is not altered during operation of Zowe, so no data is written to it and no customization is performed on its contents.
- The Zowe instance directory **<INSTANCE\_DIR>** contains information that is specific to a launch of Zowe. It contains configuration settings that determine how an instance of the Zowe server is started, such as ports that are used or paths to dependent Java and Node.js runtimes. The instance directory also contains log directory where different 'microservices' write trace data for diagnosis, as well as a workspace and shell scripts to start and stop Zowe. More than one Zowe instance directory can be created to allow multiple launches of a Zowe runtime, each one isolated from each other and starting Zowe depending on how the instance directory has been configured. For more information, see Creating and configuring the Zowe instance directory.

To start Zowe, the script <INSTANCE\_DIR>/bin/zowe-start.sh is run from a USS shell. This uses a REXX program to launch the started task ZWESVSTC, passing the instance directory path as a parameter. It is the equivalent of using the TSO command /S

ZWESVSTC, INSTANCE='<INSTANCE\_DIR>', JOBNAME='<JOBNAME>'. The ZWESVSTC PROCLIB uses the program that creates a USS process and starts the script <INSTANCE\_DIR>/bin/internal/runzowe.sh. By using BPXATSL to start the USS process, all of the address spaces started under this shell are managed by SDSF. If the zowe-start.sh run run-zowe.sh directly, the USS processes will not run as a started task and will run under the user ID of whoever ran the run-zowe.sh script rather than the Zowe user ID of ZWESVUSR, likely leading to permission errors accessing the contents of the <a href="https://www.certificate">cRUNTIME\_DIR></a> as well as the Zowe certificate. For these reasons, the zowe-start.sh script launches Zowe's USS process beneath the started task ZWESVSTC.

When run-zowe.sh is run in the USS shell that BPXBATSL creates, it executes the file <INSTANCE\_DIR>/instance.env. This file sets a number of shell variables, such as ROOT\_DIR that points to the directory with the <RUNTIME\_DIR>, variables for all of the ports used by the Zowe components, and other configuration data. For more information, see Updating the instance.env configuration file.

#### Note:

The scripts of core Zowe components and some extensions use the helper library <a>(RUNTIME\_DIR>/bin/utils</a>. Currently, these are not publicly supported. Future releases of Zowe might provide these as supported system programming interfaces (SPIs) and include their usage in the Zowe documentation.

## **Zowe component runtime lifecycle**

Each Zowe component will be installed with its own USS directory, which contains its executable files. Within each component's USS directory, a bin directory is recommended to contain scripts that are used for the lifecycle of the component. When Zowe is started, it identifies the components that are configured to launch and then execute the scripts of those components in the cycle of validate, configure, and start. All components are validated, then all are configured, and finally all are started. This technique is used as follows:

- Used for the base Zowe components that are included with the core Zowe runtime.
- Applies to extensions to allow vendor offerings to be able to have the lifecycle of their 'microservices' within the Zowe USS shell and be included as address spaces under the ZWESVSTC started task.

#### Note:

All lifecycle scripts are executed from the root directory of the component. This directory is usually the parent directory of your /bin directory.

### Validate

Each component can optionally instruct Zowe runtime to validate itself with a USS command defined in manifest commands.validate. If this is not defined, for backward compatible purpose, a call to its /bin/validate.sh script will be executed if it exists.

If present, the validate script performs tasks such as:

- Check that the shell has the correct prerequisites.
- Validate that ports are available.
- Perform other steps to ensure that the component is able to be launched successfully.

During execution of the validate script, if an error is detected, then a component should echo a message that contains information to assist a user diagnosing the problem.

## Configure

Each component can optionally instruct Zowe runtime to configure itself with a USS command defined in manifest commands.configure. If this is not defined, for backward compatible purpose, a call to its /bin/configure.sh script will be executed if it exists.

If the component has manifest defined, some configure actions will be performed automatically based on manifest definition:

• apimlServices.static: Zowe runtime will automatically parse and add your static definition to API Mediation Layer.

For backward compatible purpose, you can choose to configure component by yourself with /bin/configure.sh. An example configuration step is if a component wants to install applications into the Zowe desktop as iframes, or add API endpoints statically into the API Mediation Layer. Because a component's configure.sh script is run inside the USS shell that the instance.env has initialized, it will have all of the shell variables for prerequisites set, so the configure step can be used to query these in order to prepare the component ready for launch.

From v1.20.0 or later, you can export configuration variables from the configure step to the start step. Each component runs in separated shell space, which means that the variable of one component does not affect the same variable of another component. For example, when you run export MY\_VAR=val in /bin/configure.sh, then the variable \${MY\_VAR} will be available in your /bin/start.sh script. However, \${MY\_VAR} will not be available in other components.

## Start

Each component can optionally instruct Zowe runtime to start itself with a USS command defined in manifest commands.start. If this is not defined, for backward compatible purpose, a call to its /bin/start.sh script will be executed if it exists. If your component is not supposed to be started by itself, for example, the component is a shared library, you can skip this instruction.

It is up to each component to start itself based on how it has been written. We recommend that any variables that someone who configure Zowe may need to vary, such as timeout values, port numbers, or similar, are specified as variables in the instance.env file and then referenced as shell variables in the start.sh script to be passed into the component runtime.

## **Developing for Zowe CLI**

You can extend Zowe™ CLI by developing plug-ins and contributing code to the base Zowe CLI or existing plug-ins.

## How can I contribute?

You can contribute to Zowe CLI in the following ways:

- 1. Add new commands, options, or other improvements to the base CLI.
- 2. Develop a plug-in that users can install to Zowe CLI.

You might want to contribute to Zowe CLI to accomplish the following:

- Provide new scriptable functionality for yourself, your organization, or to a broader community.
- Make use of Zowe CLI infrastructure (profiles and programmatic APIs).
- Participate in the Zowe CLI community space.

## **Getting started**

If you want to start working with the code immediately, check out the Zowe CLI core repository and the contribution guidelines. The zowe-cli-sample-plugin GitHub repository is a sample plug-in that adheres to the guidelines for contributing to Zowe CLI projects.

## **Tutorials**

Follow these tutorials to get started working with the sample plug-in:

- 1. **Setting up** Clone the project and prepare your local environment.
- 2. Installing a plug-in Install the sample plug-in to Zowe CLI and run as-is.
- 3. Extending a plug-in Extend the sample plug-in with a new by creating a programmatic API, definition, and handler.
- 4. Creating a new plug-in Create a new CLI plug-in that uses Zowe CLI programmatic APIs and a diff package to compare two data sets.
- 5. Implementing user profiles Implement user profiles with the plug-in.

## **Plug-in Development Overview**

At a high level, a plug-in must have imperative-framework configuration (sample here). This configuration is discovered by imperative-framework through the package.json imperative key.

A Zowe CLI plug-in will minimally contain the following:

- 1. **Programmatic API** Node.js programmatic APIs to be called by your handler or other Node.js applications.
- 2. Command definition The syntax definition for your command.
- 3. **Handler implementation** To invoke your programmatic API to display information in the format that you defined in the definition.

The following guidelines and documentation will assist you during development:

### **Imperative CLI Framework Documentation**

Imperative CLI Framework documentation is a key source of information to learn about the features of Imperative CLI Framework (the code framework that you use to build plug-ins for Zowe CLI). Refer to these supplementary documents during development to learn about specific features such as:

- Auto-generated help
- JSON responses
- User profiles
- Logging, progress bars, experimental commands, and more!

### **Contribution Guidelines**

The Zowe CLI contribution guidelines contain standards and conventions for developing Zowe CLI plug-ins.

The guidelines contain critical information about working with the code, running/writing/maintaining automated tests, developing consistent syntax in your plug-in, and ensuring that your plug-in integrates with Zowe CLI properly:

For more information about	See:
General guidelines that apply to contributing to Zowe CLI and Plug-ins	Contribution Guidelines

For more information about	See:
Conventions and best practices for creating packages and plug-ins for Zowe CLI	Package and Plug-in Guidelines
Guidelines for running tests on Zowe CLI	Testing Guidelines
Guidelines for running tests on the plug-ins that you build	Plug-in Testing Guidelines
Versioning conventions for Zowe CLI and Plug-ins	Versioning Guidelines

## Setting up your development environment

Before you follow the development tutorials for creating a Zowe™ CLI plug-in, follow these steps to set up your environment.

## Prerequisites

Install Zowe CLI.

## Initial setup

To create your development space, you will clone and build zowe-cli-sample-plugin from source.

Before you clone the repository, create a local development folder named <code>zowe-tutorial</code>. You will clone and build all projects in this folder.

## Branches

There are two branches in the repository that correspond to different Zowe CLI versions. You can develop two branches of your plug-in so that users can install your plug-in into @latest or @zowe-v1-lts CLI. Developing for both versions will let you take advantage of new core features quickly and expose your plug-in to a wider range of users.

The master branch of Sample Plug-in is compatible with the @zowe-v1-lts version of core CLI (Zowe LTS release).

The master branch of Sample Plug-in is also compatible with the @latest version of core CLI (Zowe Active Development release) at this time.

For more information about the versioning scheme, see Maintainer Versioning in the Zowe CLI repository.

### Clone zowe-cli-sample-plugin and build from source

Clone the repository into your development folder to match the following structure:

Follow these steps:

- 1. cd to your zowe-tutorial folder.
- 2. git clone https://github.com/zowe/zowe-cli-sample-plugin
- 3. cd to your zowe-cli-sample-plugin folder.
- 4. git checkout master
- 5. npm install
- 6. npm run build

#### (Optional) Run the automated tests

We recommend running automated tests on all code changes. Follow these steps:

- 1. cd to the \_\_tests\_/\_\_resources\_/properties folder.
- 2. Copy example\_properties.yaml to custom\_properties.yaml.
- 3. Edit the properties within custom\_properties.yaml to contain valid system information for your site.
- 4. cd to your zowe-cli-sample-plugin folder
- 5. npm run test

## **Next steps**

After you complete your setup, follow the Installing the sample plug-in tutorial to install this sample plug-in to Zowe CLI.

```
Version: v1.25.x LTS
```

## Installing the sample plug-in

Before you begin, set up your local environment to install a plug-in.

## Overview

This tutorial covers installing and running this bundled Zowe™ CLI plugin as-is (without modification), which will display your current directory contents.

The plug-in adds a command to the CLI that lists the contents of a directory on your computer.

## Installing the sample plug-in to Zowe CLI

To begin, cd into your zowe-tutorial folder.

Issue the following commands to install the sample plug-in to Zowe CLI:

zowe plugins install ./zowe-cli-sample-plugin

## Viewing the installed plug-in

Issue zowe --help in the command line to return information for the installed zowe-cli-sample command group:

## Using the installed plug-in

To use the plug-in functionality, issue: zowe zowe-cli-sample list directory-contents:

## Testing the installed plug-in

To run automated tests against the plug-in, cd into your zowe-tutorial/zowe-cli-sample-plugin folder.

Issue the following command:

• npm run test

## Next steps

You successfully installed a plug-in to Zowe CLI! Next, try the Extending a plug-in tutorial to learn about developing new commands for this plug-in.

# **Extending a plug-in**

Before you begin, be sure to complete the Installing the sample plug-in tutorial.

## Overview

This tutorial demonstrates how to extend the plug-in that is bundled with this sample by:

- 1. Creating a new programmatic API
- 2. Creating a new command definition
- 3. Creating a new handler

```
We'll do this by using @zowe/imperative infrastructure to surface REST API data on our Zowe™ CLI plug-in.
```

Specifically, we're going to show data from this URI by Typicode. Typicode serves sample REST JSON data for testing purposes.

At the end of this tutorial, you will be able to use a new command from the Zowe CLI interface: zowe zowe-cli-sample list typicode-todos

Completed source for this tutorial can be found on the typicode-todos branch of the zowe-cli-sampleplugin repository.

## Creating a Typescript interface for the Typicode response data

First, we'll create a Typescript interface to map the response data from a server.

Within zowe-cli-sample-plugin/src/api, create a folder named doc to contain our interface (sometimes referred to as a "document" or "doc"). Within the doc folder, create a file named ITodo.ts.

The ITodo.ts file will contain the following:

#### **Creating a programmatic API**

Next, we'll create a Node.js API that our command handler uses. This API can also be used in any Node.js application, because these Node.js APIs make use of REST APIs, Node.js APIs, other NPM packages, or

custom logic to provide higher level functions than are served by any single API.

Adjacent to the existing file named zowe-cli-sample-plugin/src/api/Files.ts, create a file Typicode.ts.

Typicode.ts should contain the following:

The Typicode class provides two programmatic APIs, getTodos and getTodo, to get an array of ITodo objects or a specific ITodo respectively. The Node.js APIs use @zowe/imperative infrastructure to provide logging, parameter validation, and to call a REST API. See the Imperative CLI Framework documentation for more information.

### Exporting interface and programmatic API for other Node.js applications

Update zowe-cli-sample-plugin/src/index.ts to contain the following:

A sample invocation of your API might look similar to the following, if it were used by a separate, standalone Node.js application:

### Checkpoint

Issue **npm run build** to verify a clean compilation and confirm that no lint errors are present. At this point in this tutorial, you have a programmatic API that will be used by your handler or another Node.js application. Next you'll define the command syntax for the command that will use your programmatic Node.js APIs.

### Defining command syntax

Within Zowe CLI, the full command that we want to create is zowe zowe-cli-sample list typicodetodos. Navigate to zowe-cli-sample-plugin/src/cli/list and create a folder typicodetodos. Within this folder, create TypicodeTodos.definition.ts. Its content should be as follows:

This describes the syntax of your command.

## **Defining command handler**

Also within the typicode-todos folder, create TypicodeTodos.handler.ts. Add the following code to the new file:

The if statement checks if a user provides an --id flag. If yes, we call getTodo. Otherwise, we call getTodos. If the Typicode API throws an error, the @zowe/imperative infrastructure will automatically surface this.

## Defining command to list group

Within the file zowe-cli-sample-plugin/src/cli/list/List.definition.ts, add the following code below other import statements near the top of the file:

Then add TypicodeTodosDefinition to the children array. For example:

## Checkpoint

Issue npm run build to verify a clean compilation and confirm that no lint errors are present. You now have a handler, definition, and your command has been defined to the list group of the command.

## Using the installed plug-in

Issue the command: zowe zowe-cli-sample list typicode-todos

Refer to zowe zowe-cli-sample list typicode-todos --help for more information about your command and to see how text in the command definition is presented to the end user. You can also see how to use your optional --id flag:



## Summary

You extended an existing Zowe CLI plug-in by introducing a Node.js programmatic API, and you created a command definition with a handler. For an official plugin, you would also add JSDoc to your code and create automated tests.

## Next steps

Try the Developing a new plug-in tutorial next to create a new plug-in for Zowe CLI.

# Developing a new plug-in

Before you begin this tutorial, complete the Extending an existing plug-in tutorial.

## Overview

This tutorial demonstrates how to create a brand new Zowe™ CLI plug-in that uses Zowe CLI Node.js programmatic APIs.

At the end of this tutorial, you will have created a data set diff utility plug-in for Zowe CLI, from which you can pipe your plugin's output to a third-party utility for a side-by-side diff of data set member contents.

Completed source for this tutorial can be found on the develop-a-plugin branch of the zowe-clisample-plugin repository.

## Cloning the sample plug-in source

Clone the sample repo, delete the irrelevant source, and create a brand new plug-in. Follow these steps:

- 1. cd into your zowe-tutorial folder
- 2. git clone https://github.com/zowe/zowe-cli-sample-plugin files-util
- 3. cd files-util
- 4. Delete the .git (hidden) folder.
- 5. Delete all content within the src/api, src/cli, and docs folders.
- 6. Delete all content within the \_\_tests\_/\_\_system\_/api, \_\_tests\_/\_\_system\_/cli, \_\_tests\_/api, and \_\_tests\_/cli folders
  7. git init
  8. git add .
- 9. git commit -m "initial"

## Changing package.json

Use a unique npm name for your plugin. Change package.json name field as follows:

Issue the command npm install against the local repository.

#### Adjusting Imperative CLI Framework configuration

Change imperative.ts to contain the following:

Here we adjusted the description and other fields in the imperative JSON configuration to be relevant to this plug-in.

#### Adding third-party packages

We'll use the following packages to create a programmatic API:

- npm install --save diff
- npm install –D @types/diff

#### Creating a Node.js programmatic API

In files-util/src/api, create a file named DataSetDiff.ts. The content of DataSetDiff.ts should be the following:

### **Exporting your API**

In files-util/src, change index.ts to contain the following:

## Checkpoint

At this point, you should be able to rebuild the plug-in without errors via **npm run build**. You included third party dependencies, created a programmatic API, and customized this new plug-in project. Next, you'll define the command to invoke your programmatic API.

#### **Defining commands**

In files-util/src/cli, create a folder named diff. Within the diff folder, create a file Diff.definition.ts. Its content should be as follows:

Also within the diff folder, create a folder named data-sets. Within the data-sets folder create DataSets.definition.ts and DataSets.handler.ts.

DataSets.definition.ts should contain:

DataSets.handler.ts should contain the following:

## **Trying your command**

Be sure to build your plug-in via npm run build.

Install your plug-in into Zowe CLI via zowe plugins install.

Issue the following command. Replace the data set names with valid mainframe data set names on your system:

\$ zowe files-util diff data-sets " .cntl(iefbr14)" " .cntl(iefbr15)" | diff2html -i stdin

The raw diff output is displayed as a command response:

## **Bringing together new tools!**

The advantage of Zowe CLI and of the CLI approach in mainframe development is that it allows for combining different developer tools for new and interesting uses.

diff2html is a free tool to generate HTML side-by-side diffs to help see actual differences in diff output.

Install the diff2html CLI via npm install -g diff2html-cli. Then, pipe your Zowe CL plugin's output into diff2html to generate diff HTML and launch a web browser that contains the content in the screen shot at the top of this file.

```
    zowe files-util diff data-sets "kelda16.work.jcl(iefbr14)"
    "kelda16.work.jcl(iefbr15)" | diff2html -i stdin
```

## Next steps

Try the Implementing profiles in a plug-in tutorial to learn about using profiles with your plug-in.

## Implementing profiles in a plug-in

You can use this profile template to create a profile for your product.

The profile definition is placed in the imperative.ts file.

**someproduct** will be the profile name that you might require on various commands to have credentials loaded from a secure credential manager and retain host/port information (so that you can easily swap to different servers) from the CLI).

By default, if your plug-in is installed into Zowe<sup>™</sup> CLI that contains a profile definition like this, commands will automatically be created under zowe profiles ... to create, validate, set default, list, etc... for your profile.

## Next steps

If you completed all previous tutorials, you now understand the basics of extending and developing plug-ins for Zowe CLI. Next, we recommend reviewing the project contribution guidelines and Imperative CLI Framework documentation to learn more.

Version: v1.25.x LTS

## **Onboarding Overview**

As an API developer, you can onboard a REST API service to the Zowe<sup>™</sup> API Mediation Layer (API ML). Onboarding your REST service to the Zowe<sup>™</sup> API Mediation Layer will make your service discoverable by the API ML Discovery Service, enable routing through the API Gateway, and make service information and API documentation available through the API Catalog.

The specific method you use to onboard a REST API to the API ML depends on the programming language or framework used to build your REST service.

This Onboarding Overview article addresses the following topics:

- Prerequisites
- Service Onboarding Guides to onboard your REST service with the API ML
- Verify successful onboarding to the API ML
- Using the Sample REST API Service to learn how to onboard a REST service to the API ML

## Prerequisites

Meet the following prerequisites before you onboard your service:

• Running instance of Zowe

Note: For static onboarding, access to Zowe runtime is required to create the static service definition.

• A certificate that is trusted by Zowe and certificate(s) to trust Zowe services

Zowe uses secured communication over TLSv1.2. As such, the protocol version and the certificate is required. For more information, see API Mediation Layer security setup and Zowe API ML TLS requirements.

• A REST API-enabled service that you want to onboard

If you do not have a specific REST API service, you can use the sample service.

Your service should be documented in a valid OpenApi 2.0/3.0 Swagger JSON format.

- Access to the Zowe artifactory
- Either the Gradle or Maven build automation system

## **Service Onboarding Guides**

Services can be updated to support the API Mediation Layer natively by updating the service code. Use one of the following guides to onboard your REST service to the Zowe API Mediation Layer:

#### **Recommended guides for services using Java**

- Onboard a REST API service with the Plain Java Enabler (PJE)
- Onboard a Spring Boot based REST API Service
- Onboard a Micronaut based REST API service

#### **Recommended guides for services using Node.js**

• Onboard a Node.js based REST API Service

#### **Guides for Static Onboarding and Direct Call Onboarding**

Use one of the following guides if your service is not built with Java, or you do not want to change your codebase or use the previously mentioned libraries:

- Onboard a REST API using static definition without code changes
- Onboard a REST API directly calling Zowe Discovery Service

#### **Documentation for legacy enablers**

For legacy enabler documentation (version 1.2 and lower), refer to the previous version of the documentation:

• Zowe Docs version 1.8.x

Note: Enabler version 1.2 and previous versions are no longer supported.

**Tip**: We recommend you use the enabler version 1.3 or higher to onboard your REST API service to the Zowe API Medaition Layer.

## Verify successful onboarding to the API ML

Verifying that your service was successfully onboraded to the API ML can be done by ensuring service registration in the API ML Discovery Service or visibility of the service in the API ML Catalog.

#### Verifying service discovery through Discovery Service

Verify that your service is discovered by the Discovery Service with the following procedure.

#### Follow these steps:

1. Issue a HTTP GET request to the Discovery Service endpoint /eureka/apps to get service instance information:

**Note**: The endpoint is protected by client certificate verification. A valid trusted certificate must be provided with the HTTP GET request.

2. Check your service metadata.

#### **Response example:**

#### Tips:

- Ensure that addresses and user credentials for individual API ML components correspond to your target runtime environment.
- If you work with local installation of API ML and you use our dummy identity provider, enter user for both username and password. If API ML was installed by system administrators, ask them to provide you with actual addresses of API ML components and the respective user credentials.

#### Verifying service discovery through the API Catalog

Services may not be immediately visible in the API Catalog. We recommend you wait for 2 minutes as it may take a moment for your service to be visible in the Catalog. If your service still does not appear in the Catalog, ensure that your configuration settings are correct.

#### Follow these steps:

1. Check to see that your API service is displayed in the API Catalog UI, and that all information including API documentation is correct.

2. Ensure that you can access your API service endpoints through the Gateway.

## Sample REST API Service

To demonstrate the concepts that apply to REST API services, we use an example of a Spring Boot REST API service. This example is used in the REST API onboarding guide REST APIs without code changes required (static onboarding).

You can build this service using instructions in the source code of the Spring Boot REST API service example.

The Sample REST API Service has a base URL. When you start this service on your computer, the *service base URL* is: <a href="http://localhost:8080">http://localhost:8080</a>.

**Note:** If a service is deployed to a web application server, the base URL of the service (application) has the following format: <a href="https://application-server-hostname:port/application-name">https://application-server-hostname:port/application-name</a>.

This sample service provides one API that has the base path /v2, which is represented in the base URL of the API as http://localhost:8080/v2. In this base URL, /v2 is a qualifier of the base path that was chosen by the developer of this API. Each API has a base path depending on the particular implementation of the service.

This sample API has only one single endpoint:

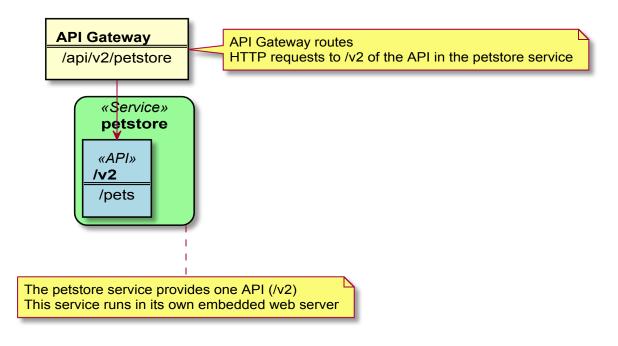
• /pets/{id} - Find pet by ID.

This endpoint in the sample service returns information about a pet when the *{id}* is between 0 and 10. If *{id}* is greater than 0 or a non-integer, an error is returned. These are conditions set in the sample service.

**Tip:** Access http://localhost:8080/v2/pets/1 to see what this REST API endpoint does. You should get the following response:

**Note:** The onboarding guides demonstrate how to add the Sample REST API Service to the API Mediation Layer to make the service available through the petstore service ID.

The following diagram shows the relations between the Sample REST API Service and its corresponding API, REST API endpoint, and API Gateway:



This sample service provides a Swagger document in JSON format at the following URL:

The Swagger document is used by the API Catalog to display API documentation.

# Onboarding a REST API service with the Plain Java Enabler (PJE)

This article is part of a series of onboarding guides, which outline the process of onboarding REST API services to the Zowe API Mediation Layer (API ML). As a service developer, you can onboard a REST service with the API ML with the Zowe API Mediation Layer using our Plain Java Enabler (PJE). This enabler is built without a dependency on Spring Cloud, Spring Boot, or SpringFramework.

Tip: For more information about onboarding API services with the API ML, see the Onboarding Overview.

## Introduction

Zowe API ML is a lightweight API management system based on the following Netflix components:

- Eureka a discovery service used for services registration and discovery
- Zuul reverse proxy / API Gateway
- Ribbon load balancer

The API ML Discovery Service component uses Netflix/Eureka as a REST services registry. Eureka endpoints are used to register a service with the API ML Discovery Service.

The API ML provides onboarding enabler libraries. The libraries are JAR artifacts available through an artifactory. Using these libraries is the recommended approach to onboard a REST service with the API ML.

The PJE library serves the needs of Java developers who are not using either Spring Boot or the Spring Framework. If Spring Boot or the Spring framework are used in the project you would like to onboard, see the Onboarding Overview for the corresponding enablers.

Additionally, this enabler is not intended for use in projects that depend on Spring Cloud Netflix components. Configuration settings in the PJE and Spring Cloud Netflix Eureka Client are different. Using the two configuration settings in combination makes the result state of the discovery registry unpredictable.

**Tip:** For more information about how to utilize another API ML enablers, see the documentation in the Onboarding Overview.

## **Onboarding your REST service with API ML**

The following steps outline the overall process to onboard a REST service with the API ML using the PJE. Each step is described in further detail in this article.

- 1. Prerequisites
- 2. Configuring your project
  - Gradle build automation system
  - Maven build automation system
- 3. Configuring your service
  - REST service identification
  - Administrative endpoints
  - API info
  - API routing information
  - API Catalog information
  - Authentication parameters
  - API Security
  - SAF Keyring configuration
  - Eureka Discovery Service
- 4. Registering your service with API ML
- 5. (Optional) Validating the discoverability of your API service by the Discovery Service
- 6. (Optional) Troubleshooting
  - Log messages during registration problems

### **Prerequisites**

Ensure that the prerequisites from the Onboarding Overview are met.

• The REST API service to onboard is written in Java

• The service is enabled to communicate with API ML Discovery Service over a TLS v1.2 secured connection

#### Notes:

- This documentation is valid for API ML version ZoweApimlVersion 1.3.0 and higher. We recommend that you check the Zowe Artifactory for latest stable versions.
- Following this guide enables REST services to be deployed on a z/OS environment. Deployment to a z/OS environment, however, is not required. As such, you can first develop on a local machine before you deploy on z/OS.
- The API Mediation Layer provides the sample application using the Plain Java Enabler in the api-layer repository

## **Configuring your project**

Use either *Gradle* or *Maven* build automation systems to configure the project with the service to be onboarded. Use the appropriate configuration procedure that corresponds to your build automation system.

**Note:** You can use either the Zowe Artifactory or an artifactory of your choice. If you decide to build the API ML from source, you are required to publish the enabler artifact to your artifactory. Publish the enabler artifact by using the *Gradle* tasks provided in the source code.

#### Gradle build automation system

Use the following procedure to use *Gradle* as your build automation system.

#### Follow these steps:

- 1. Create a gradle.properties file in the root of your project if one does not already exist.
- 2. In the gradle.properties file, set the URL of the specific artifactory containing the PJE artifact. Provide the corresponding credentials to gain access to the Maven repository.
- 3. Add the following *Gradle* code block to the repositories section of your build.gradle file:
- 4. In the same build.gradle file, add the necessary dependencies for your service. If you use the Java enabler from the Zowe Artifactory, add the following code block to your build.gradle script.

The published artifact from the Zowe Artifactory also contains the enabler dependencies from other software packages. If you are using an artifactory other than Zowe, add also the following dependencies in your service build.gradle script:

#### Notes:

- You may need to add more dependencies as required by your service implementation.
- The information provided in this file is valid for ZoweApimlVersion 1.3.0 and higher.
- 5. In your project home directory, run the gradle clean build command to build your project. Alternatively, you can run gradlew to use the specific gradle version that is working with your project.

#### Maven build automation system

Use the following procedure if you use Maven as your build automation system.

#### Follow these steps:

1. Add the following XML tags within the newly created pom.xml file:

**Tip:** If you want to use snapshot version, replace <code>libs-release</code> with <code>libs-snapshot</code> in the repository url and change snapshots->enabled to <code>true</code>.

- 2. Add the proper dependencies:
- 3. In the directory of your project, run the mvn clean package command to build the project.

## **Configuring your service**

To configure your service, create the configuration file service-configuration.yml in your service source tree resources directory. The default path for a java application is src/main/resources. The service-configuration.yml file is used to set the application properties and eureka metadata. Application properties are for your service runtime. For example, the ssl section specifies the keystore and trustore. The eureka metadata is used for registration with API Mediation Layer.

**Note:** To externalize service onboarding configuration, see: Externalizing onboarding configuration.

The following code snippet shows an example of service-configuration.yml. Some parameters which are specific for your service deployment are in *\${parameterValue}* format. For your service configuration file, provide actual values or externalize your onboarding configuration.

#### Example:

#### **Optional metadata section**

The following snippet presents additional optional metadata that can be added.

#### Example:

The onboarding configuration parameters are broken down into the following groups:

- REST service identification
- Administrative endpoints
- API info
- API routing information
- API catalog information
- Authentication parameters
- API security
- SAF Keyring configuration
- Eureka Discovery Service
- Custom Metadata
- Connection Timeout

#### **REST service identification**

• serviceId

The serviceId uniquely identifies one or more instance of a microservice in the API ML and is used as part of the service URL path in the API ML Gateway address space. Additionally, the API ML Gateway uses the serviceId for routing to the API service instances. When two API services use the same serviceId, the API Gateway considers the services as clones of each other. An incoming API request can be routed to either of them through utilized load balancing mechanism.

**Important!** Ensure that the serviceId is set properly with the following considerations:

- The same servicedId should only be set for multiple API service instances for API scalability.
- The servicedId value must only contain lowercase alphanumeric characters.
- The servicedId cannot contain more than 40 characters.

#### Example:

• If the serviceId is sampleservice, the service URL in the API ML Gateway address space appears as the following path:

#### • title

This parameter specifies the human readable name of the API service instance. This value is displayed in the API Catalog when a specific API service instance is selected. This parameter can be externalized and set by the customer system administrator.

**Tip:** We recommend that service developer provides a default value of the **title**. Use a title that describes the service instance so that the end user knows the specific purpose of the service instance.

#### • description

This parameter is a short description of the API service. This value is displayed in the API Catalog when a specific API service instance is selected. This parameter can be externalized and set by the customer system administrator.

**Tip:** Describe the service so that the end user understands the function of the service.

#### baseUrl

This parameter specifies the base URL for the following administrative endpoints:

- homePageRelativeUrl
- statusPageRelativeUrl

#### • healthCheckRelativeUrl

Use the following format to include your service name in the URL path:

protocol://host:port/servicename

**Note:** Ensure that the baseUrl does not end with a trailing /. Inclusion of / causes a malformed URL if any of the above administrative endpoints begin with a /. It is expected that each administrative endpoint begins with a /. Warnings will be logged if this recommendation is not followed.

• servicelpAddress (Optional)

This parameter specifies the service IP address and can be provided by a system administrator in the externalized service configuration. If this parameter is not present in the configuration file or is not set as a service context parameter, it is resolved from the hostname part of the baseUrl.

• preferIpAddress (Optional)

Set the value of this parameter to true to advertise a service IP address instead of its hostname.

#### Administrative endpoints

The following snippet presents the format of the administrative endpoint properties:

where:

#### homePageRelativeUrl

specifies the relative path to the home page of your service.

Start this path with 7. If your service has no home page, leave this parameter blank.

#### **Examples:**

- homePageRelativeUrl: This service has no home page
- homePageRelativeUrl: / This service has a home page with URL \${baseUrl}/

#### • statusPageRelativeUrl

specifies the relative path to the status page of your service.

Start this path with /.

#### **Example:**

#### statusPageRelativeUrl: /application/info

This results in the URL: \${baseUrl}/application/info

#### healthCheckRelativeUrl

specifies the relative path to the health check endpoint of your service.

Start this path with /.

#### **Example:**

healthCheckRelativeUrl: /application/health

This results in the URL: \${baseUrl}/application/health

#### **API info**

REST services can provide multiple APIs. Add API info parameters for each API that your service wants to expose on the API ML.

The following snippet presents the information properties of a single API:

where:

#### • apilnfo.apild

specifies the API identifier that is registered in the API ML installation. The API ID uniquely identifies the API in the API ML. The apiId can be used to locate the same APIs that are provided by different service instances. The API developer defines this ID. The apiId must be a string of up to 64 characters that uses lowercase alphanumeric characters and a dot: .

#### • apilnfo.version

specifies the api version. This parameter is used to correctly retrieve the API documentation according to requested version of the API.

#### • apilnfo.gatewayUrl

specifies the base path at the API Gateway where the API is available. Ensure that this value is the same path as the gatewayUrl value in the routes sections that apply to this API.

• apiInfo.swaggerUrl (Optional)

specifies the Http or Https address where the Swagger JSON document is available.

• apilnfo.documentationUrl (Optional)

specifies the link to the external documentation. A link to the external documentation can be included along with the Swagger documentation.

• apiInfo.defaultApi (Optional)

specifies that this API is the default one shown in the API Catalog. If no apilnfo fields have defaultApi set to true, the default API is the one with the highest API version.

#### **API routing information**

The API routing group provides the required routing information used by the API ML Gateway when routing incoming requests to the corresponding REST API service. A single route can be used to direct REST calls to multiple resources or API endpoints. The route definition provides rules used by the API ML Gateway to rewrite the URL in the Gateway address space. Currently, the routing information consists of two parameters per route: The gatewayUrl and serviceUrl. These two parameters together specify a rule for how the API service endpoints are mapped to the API Gateway endpoints.

The following snippet is an example of the API routing information properties.

#### Example:

where:

routes

specifies the container element for the route.

#### • routes.gatewayUrl

The gatewayUrl parameter specifies the portion of the gateway URL which is replaced by the serviceUrl path part.

#### routes.serviceUrl

The serviceUrl parameter provides a portion of the service instance URL path which replaces the gatewayUrl part.

#### Examples:

- is routed to:
- API major version 1:

is routed to:

• APIs docs major version 1:

is routed to:

#### **API Catalog information**

The API ML Catalog UI displays information about discoverable REST services registered with the API ML Discovery Service. Information displayed in the Catalog is defined by the metadata provided by your service during registration. The following image is an example of a tile in the API Catalog:

The Catalog groups correlated services in the same tile if these services are configured with the same catalog.tile.id metadata parameter.

The following code block is an example of configuration of a service tile in the Catalog:

#### Example:

where:

• catalog.tile.id

specifies the unique identifier for the product family of API services. This is a value used by the API ML to group multiple API services into a single tile. Each unique identifier represents a single API dashboard tile in the Catalog.

**Tip:** Specify a value that does not interfere with API services from other products. We recommend that you use your company and product name as part of the ID.

• catalog.tile.title

specifies the title of the product family of the API service. This value is displayed in the API Catalog dashboard as the tile title.

#### • catalog.tile.description

is the detailed description of the API services product family. This value is displayed in the API Catalog UI dashboard as the tile description.

#### catalog.tile.version

specifies the semantic version of this API Catalog tile.

**Note:** Ensure that you increase the version number when you introduce changes to the API service product family details.

#### **Authentication parameters**

These parameters are not required. Parameters that are not specified results in the use of the default values.

Authentication parameters enables a service to accept the Zowe JWT. The API Gateway translates the token to an authentication method supported by a service.

The following example shows the parameters that define the service authentication method:

#### Example:

where:

#### • authentication.scheme

specifies a service authentication scheme. The following schemes are supported by the API Gateway:

#### • bypass

This value specifies the token is passed unchanged to service.

Note: This is the default scheme when no authentication parameters are specified.

• zoweJwt

This value specifies that a service accepts the Zowe JWT. No additional processing is done by the API Gateway.

#### • httpBasicPassTicket

This value specifies that a service accepts PassTickets in the Authorization header of the HTTP requests using the basic authentication scheme. It is necessary to provide a service APPLID in authentication.applid parameter.

For more information, see Enabling PassTicket creation for API Services that Accept PassTickets

#### • zosmf

This value specifies that a service accepts z/OSMF LTPA (Lightweight Third-Party Authentication). This scheme should be used only for a z/OSMF service used by the API Gateway Authentication Service and other z/OSMF services that use the same LTPA key.

For more information about z/OSMF Single Sign-on, see Establishing a single sign-on environment

#### • **x509**

This value specifies that a service accepts client certificates forwarded in the HTTP header. The Gateway service extracts information from a valid client certificate. For validation, the certificate needs to be trusted by API Mediation Layer, and needs to contain a Client Authentication (1.3.6.1.5.5.7.3.2) entry in Extended Key Usage. To use this scheme, it is also necessary to specify which headers to include. Specify these parameters in headers.

#### • headers

When the x509 scheme is specified, use the headers parameter to select which values to send to a service. Use one of the following values:

X-Certificate-Public

The public part of client certificate base64 encoded

X-Certificate-DistinguishedName

The distinguished name from client certificate

X-Certificate-CommonName

The common name from the client certificate

#### • authentication.applid

This parameter specifies a service APPLID. This parameter is valid only for the httpBasicPassTicket authentication scheme.

#### **API Security**

REST services onboarded with the API ML act as both a client and a server. When communicating to API ML Discovery service, a REST service acts as a client. When the API ML Gateway is routing requests to a service, the REST service acts as a server. These two roles have different requirements. The Zowe API ML Discovery Service communicates with its clients in secure Https mode. As such, TLS/SSL configuration setup is required when a service is acting as a server. In this case, the system administrator decides if the service will communicate with its clients securely or not.

Client services need to configure several TLS/SSL parameters in order to communicate with the API ML Discovery service. When an enabler is used to onboard a service, the configuration is provided in the ssl section/group in the same *YAML* file that is used to configure the Eureka parameters and the service metadata.

For more information about API ML security, see API ML security.

TLS/SSL configuration consists of the following parameters:

#### verifySslCertificatesOfServices

This parameter makes it possible to prevent server certificate validation.

**Important!** Ensure that this parameter is set to true in production environments. Setting this parameter to false in production environments significantly degrades the overall security of the system.

#### protocol

This parameter specifies the TLS protocol version currently used by Zowe API ML Discovery Service.

Tip: We recommend you use TLSv1.2 as your security protocol

keyAlias

This parameter specifies the alias used to address the private key in the keystore.

#### keyPassword

This parameter specifies the password associated with the private key.

#### keyStore

This parameter specifies the keystore file used to store the private key. When using keyring, the value should be set to the SAF keyring location. For information about required certificates, see Zowe API ML TLS requirements.

If you have an issue with loading the keystore file in your environment, try to provide the absolute path to the keystore file. The sample keystore file for local deployment is in api-layer repository

#### keyStorePassword

This parameter specifies the password used to unlock the keystore.

#### keyStoreType

This parameter specifies the type of the keystore.

#### trustStore

This parameter specifies the truststore file used to keep other parties public keys and certificates. When using keyring, this value should be set to the SAF keyring location. For information about required certificates, see Zowe API ML TLS requirements.

If you have an issue with loading the truststore file in your environment, try to provide the absolute path to the truststore file. The sample truststore file for local deployment is in api-layer repository

#### trustStorePassword: password

This parameter specifies the password used to unlock the truststore.

#### • trustStoreType: PKCS12

This parameter specifies the truststore type. The default for this parameter is PKCS12.

#### Notes:

• Ensure that you define both the key store and the trust store even if your server is not using an Https port.

#### **SAF Keyring configuration**

You can choose to use SAF keyring instead of keystore and truststore for storing certificates. For information about required certificates, see Zowe API ML TLS requirements. For information about running Java on z/OS with keyring, see SAF Keyring. Make sure that the enabler can access and read the keyring. Please refer to documentation of your security system for details.

The following example shows enabler configuration with keyrings:

#### **Eureka Discovery Service**

The Eureka Discovery Service parameters group contains a single parameter used to address Eureka Discovery Service location. An example is presented in the following snippet:

#### Example:

where:

#### • discoveryServiceUrls

Specifies the public URL of the Discovery Service. The system administrator at the customer site defines this parameter. It is possible to provide multiple values in order to utilize fail over and/or load balancing mechanisms.

#### **Custom Metadata**

Custom metadata are described here.

## **Registering your service with API ML**

The following steps outline the process of registering your service with API ML. Each step is described in detail in this article. The process describes the integration with the usage of the Java application server. The guideline is tested with the Tomcat application server. The specific steps that apply for other application servers may differ.

1. Add a web application context listener class

- 2. Register a web application context listener
- 3. Load service configuration
- 4. Register with Eureka discovery service
- 5. Unregister your service

#### Follow these steps:

1. Implement and add a web application context listener class

implements javax.servlet.ServletContextListener

The web application context listener implements two methods to perform necessary actions at application start-up time as well as when the application context is destroyed:

- The contextInitialized method invokes the apiMediationClient.register(config) method to register the application with API Mediation Layer when the application starts.
- The contextDestroyed method invokes the apiMediationClient.unregister() method when the application shuts down. This unregisters the application from the API Mediation Layer.
- 2. Register a web application context listener.

Add the following code block to the deployment descriptor web.xml to register a context listener:

3. Load the service configuration.

Load your service configuration from a file service-configuration.yml file. The configuration parameters are described in the preceding section, Configuring your service.

Use the following code as an example of how to load the service configuration.

#### Example:

**Note:** The ApiMediationServiceConfigReader class also provides other methods for loading the configuration from two files, java.util.Map instances, or directly from a string. Check the ApiMediationServiceConfigReader class JavaDoc for details.

4. Register with Eureka Discovery Service.

Use the following call to register your service instance with Eureka Discovery Service:

#### Example:

5. Unregister your service.

Use the **contextDestroyed** method to unregister your service instance from Eureka Discovery Service in the following format:

#### Example:

The following code block is a full example of a context listener class implementation.

#### **Example:**

## Validating the discoverability of your API service by the Discovery Service

Once you are able to build and start your service successfully, you can use the option of validating that your service is registered correctly with the API ML Discovery Service.

#### Follow these steps:

- 1. Validate successful onboarding
- 2. Check that you can access your API service endpoints through the Gateway.
- 3. (Optional) Check that you can access your API service endpoints directly outside of the Gateway.

Specific addresses and user credentials for the individual API ML components depend on your target runtime environment.

**Note:** If you are working with local installation of API ML and you are using our dummy identity provider, enter user for both username and password. If API ML was installed by system administrators, ask them to provide you with actual addresses of API ML components and the respective user credentials.

**Tip:** Wait for the Discovery Service to discover your service. This process may take a few minutes after your service was successfully started.

## Troubleshooting

#### Log messages during registration problems

When an Enabler connects to the Discovery service and fails, an error message prints to the Enabler log. The default setting does not suppress these messages as they are useful to resolve problems during the Enabler registration. Possible reasons for failure include the location of Discovery service is not correct, the Discovery Service is down, or the TLS certificate is invalid.

These messages continue to print to the Enabler log, while the Enabler retries to connect to the Discovery Service. To fully suppress these messages in your logging framework, set the log levels to **OFF** on the following loggers:

Some logging frameworks provide other tools to suppress repeated messages. Consult the documentation of the logging framework you use to find out what tools are available. The following example demonstrates how the Logback framework can be used to suppress repeated messages.

#### Example:

The Logback framework provides a filter tool, DuplicateMessageFilter.

Add the following code to your configuration file if you use XML configuration:

**Note:** For more information, see the full configuration used in the Core Services in GitHub.

Version: v1.25.x LTS

## API Mediation Layer onboarding configuration

This article describes the process of configuring a REST service to onboard with the Zowe API Mediation Layer using the API ML Plain Java Enabler. As a service developer, you can provide basic configuration of a service to onboard to the API ML. You can also externalize configuration parameters for subsequent customization by a systems administrator.

- Introduction
- Configuring a REST service for API ML onboarding
- Plain Java Enabler service onboarding
  - Automatic initialization of the onboarding configuration by a single method call
- Validating successful onboarding with the API Mediation Layer
- Loading YAML configuration files
  - Loading a single YAML configuration file
  - Loading and merging two YAML configuration files

## Introduction

The API ML Plain Java Enabler (PJE) is a library which helps to simplify the process of onboarding a REST service with the API ML. This article describes how to provide and externalize the Zowe API ML onboarding configuration of your REST service using the PJE.

**Note:** For more information about specific configuration parameters and their possible values, and the service registration process, see the specific documentation of the onboarding approach you are using for your project:

- Direct REST call registration (No enabler)
- Plain Java Enabler

The PJE is the most universal Zowe API ML enabler. This enabler uses only Java, and does not use advanced Inversion of Control (*IoC*) or Dependency Injection (*DI*) technologies. The PJE enables you to onboard any REST service implemented in Java, avoiding dependencies, versions collisions, unexpected application behavior, and unnecessarily large service executables. Service developers provide onboarding configuration as part of the service source code. While this configuration is valid for the development system environment, it is likely to be different for an automated integration environment. Typically, system administrators need to deploy a service on multiple sites that have different system environments and requirements such as security.

The PJE supports both the service developer and the system administrator with the functionality of externalizing the service onboarding configuration.

The PJE provides a mechanism to load API ML onboarding service configuration from one or two YAML files.

## **Configuring a REST service for API ML onboarding**

In most cases, the API ML Discovery Service, Gateway, and service endpoint addresses are not known at the time of building the service executables. Similarly, security material such as certificates, private/public keys, and their corresponding passwords depend on the specific deployment environment, and are not intended to be publicly accessible. Therefore, to provide a higher level of flexibility, the PJE implements routines to build service onboarding configuration by locating and loading one or two *YAML* file sources:

#### • internal service-configuration.yml

The first configuration file is typically internal to the service deployment artifact. This file must be accessible on the service classpath. This file contains basic API ML configuration based on values known at development time. Usually, this basic API ML configuration is provided by the service developer and is located in the /resources folder of the Java project source tree. This file is usually found in the deployment artifacts under /WEB-INF/classes. The configuration contained in this file is provided by the service developer or builder. As such, it will not match every possible production environment and its corresponding requirements.

#### • external or additional service-configuration.yml

The second configuration file is used to externalize the configuration. This file can be stored anywhere on the local file system, as long as that the service has access to that location. This file is provided by the service deployer/system administrator and contains the correct parameter values for the specific production environment.

At service start-up time, both *YAML* configuration files are merged, where the externalized configuration (if provided) has higher priority.

The values of parameters in both files can be rewritten by Java system properties or servlet context parameters that were defined during service installation/configuration, or at start-up time.

In the YAML file, standard rewriting placeholders for parameter values use the following format:

#### \${apiml.parameter.key}

The actual values are taken from [key, value] pairs defined as Java system properties or servlet context parameters. The system properties can be provided directly on a command line. The servlet context parameters can be provided in the service web.xml or in an external file.

The specific approach of how to provide the servlet context to the user service application depends on the application loading mechanism and the specific Java servlet container environment.

#### Example:

If the service is deployed in a Tomcat servlet container, you can configure the context by placing an *XML* file with the same name as the application deployment unit into

\_\$CATALINA\_BASE/conf/[enginename]/[hostname]/\_.

Other containers provide different mechanisms for the same purpose.

## Plain Java Enabler service onboarding API

You can initialize your service onboarding configuration using different methods of the Plain Java Enabler class ApiMediationServiceConfigReader:

#### Automatic initialization of the onboarding configuration by a single method call

The following code block shows automatic initialization of the onboarding configuration by a single method call:

This method receives the ServletContext parameter, which holds a map of parameters that provide all necessary information for building the onboarding configuration. The following code block is an example of Java Servlet context configuration.

#### Example:

Where the two parameters corresponding to the location of the configuration files are:

• apiml.config.location

This parameter describes the location of the basic configuration file.

apiml.config.additional-location

This parameter describes the location of the external configuration file.

The method in this example uses the provided configuration file names in order to load them as *YAML* files into the internal Java configuration object of type *ApiMediationServiceConfig*.

The other context parameters with the *apiml* prefix are used to rewrite values of properties in the configuration files.

## Validating successful onboarding with the API Mediation Layer

Ensure that you successfully onboarded a service with the API Mediation Layer.

#### Follow these steps:

- 1. Validate successful onboarding
- 2. Check that you can access your API service endpoints through the Gateway.
- 3. (Optional) Check that you can access your API service endpoints directly outside of the Gateway.

## Loading YAML configuration files

YAML configuration files can be loaded either as a single YAML file, or by merging two YAML files. Use the loadConfiguration method described later in this article that corresponds to your service requirements.

After successfully loading a configuration file, the loading method loadConfiguration uses Java system properties to substitute corresponding configuration properties.

#### Loading a single YAML configuration file

To build your configuration from multiple sources, load a single configuration file, and then rewrite parameters as needed using values from another configuration source. See: Loading and merging two YAML configuration files described later in this article.

Use the following method to load a single YAML configuration file:

This method receives a single *String* parameter and can be used to load an internal or an external configuration file.

**Note:** This method first attempts to load the configuration as a Java resource. If the file is not found, the method attempts to resolve the file name as an absolute. If the file name still cannot be found, this method attempts to resolve the file as a relative path. When the file is found, the method loads the contents of the file and maps them to internal data classes. After loading the configuration file, the method attempts to substitute/rewrite configuration property values with corresponding Java System properties.

#### Loading and merging two YAML configuration files

To load and merge two configuration files, use the following method:

where:

#### String internalConfigurationFileName

references the basic configuration file name.

#### String externalizedConfigurationFileName

references the external configuration file name.

**Note:** The external configuration file takes precedence over the basic configuration file in order to match the target deployment environment. After loading and before merging, each configuration will be separately patched using Java System properties.

The following code block presents an example of how to load and merge onboarding configuration from *YAML* files.

#### Example:

## Onboarding a service with the Zowe API Meditation Layer without an onboarding enabler

This article is part of a series of guides to onboard a REST service with the Zowe API Mediation Layer (API ML). Onboarding with API ML makes services accessible through the API Gateway and visible in the API Catalog. Once a service is successfully onboarded, users can see if the service is currently available and accepting requests.

This guide describes how a REST service can be onboarded with the Zowe API ML independent of the language used to write the service. As such, this guide does not describe how to onboard a service with a specific enabler. Similarly, various Eureka client implementations are not used in this onboarding method.

**Tip:** If possible, we recommend that you onboard your service using the API ML enabler libraries. The approach described in this article should only be used if other methods to onboard your service are not suitable.

For more information about how to onboard a REST service, see the following links:

- API ML onboarding overview
- python-eureka-client
- eureka-js-client
- Rest API developed based on Java

This article outlines a process to make an API service available in the API Mediation Layer by making a direct call to the Eureka Discovery Service.

- Introduction
- Registering with the Discovery Service
  - API Mediation Layer Service onboarding metadata
    - Catalog parameters
    - Service parameters
    - Routing parameters
    - API Info Parameters
- Sending a heartbeat to API Mediation Layer Discovery Service

- Validating successful onboarding with the API Mediation Layer
- External Resources

## Introduction

The API ML Discovery Service uses Netflix/Eureka as a REST services registry. Eureka is a REST-based service that is primarily used to locate services.

Eureka endpoints are used to register a service with the API ML Discovery Service. Endpoints are also used to send a periodic heartbeat to the Discovery Service to indicate that the onboarded service is available.

Note: Required parameters should be defined and sent at registration time.

## **Registering with the Discovery Service**

Begin the onboarding process by registering your service with the API ML Discovery Service.

Use the **POST** Http call to the Eureka server together with the registration configuration in the following format:

The following code block shows the format of the parameters in your **POST** call, which are sent to the Eureka registry at the time of registration.

where:

• app

uniquely identifies one or more instances of a microservice in the API ML.

The API ML Gateway uses the serviceId for routing to the API service instances. As such, the serviceId is part of the service URL path in the API ML Gateway address space.

Important! Ensure that the service ID is set properly with the following considerations:

- The service ID value contains only lowercase alphanumeric characters.
- The service ID does not contain more than 40 characters.

• The same service ID is only set for multiple API service instances to support API scalability. When two API services use the same service ID, the API Gateway considers the services as clones of each other. An incoming API request can be routed to either instance through load balancing.

#### Example:

• If the serviceId is sampleservice, the service URL in the API ML Gateway address space appears as:

#### • ipAddr

specifies the IP address of this specific service instance.

#### • port

specifies the port of the instance when you use Http. For Http, set enabled to true.

#### securePort

specifies the port of the instance for when you use Https. For Https, set enabled to true.

#### hostname

specifies the hostname of the instance.

#### vipAddress

specifies the serviceId when you use Http.

**Important!** Ensure that the value of vipAddress is the same as the value of app. Furthermore, be sure not to omit vipAddress, even if you provided secureVipAddress. Due to a current limitation in Spring Cloud Netflix, routes are created only for instances in which vipAddress is defined.

#### • secureVipAddress

specifies the serviceId when you use Https.

Important! Ensure that the value of secureVipAddress is the same as the value of app.

• instanceld

specifies a unique id for the instance. Define a unique value for the **instanceId** in the following format:

```
{hostname}:{serviceId}:{port}
```

• metadata

specifies the set of parameters described in the following section addressing API ML service metadata.

#### **API Mediation Layer Service onboarding metadata**

At registration time, provide metadata in the following format. Metadata parameters contained in this code block are described in the following section.

Metadata parameters are broken down into the following categories:

- Catalog parameters
- Service parameters
- Routing parameters
- Authentication parameters
- API Info parameters

#### **Catalog parameters**

Catalog parameters are grouped under the prefix: apiml.catalog.tile.

The API ML Catalog displays information about services registered with the API ML Discovery Service. Information displayed in the Catalog is defined in the metadata provided by your service during registration. The Catalog groups correlated services in the same tile when these services are configured with the same catalog.tile.id metadata parameter.

The following parameters are used to populate the API Catalog:

#### • apiml.catalog.tile.id

This parameter specifies the specific identifier for the product family of API services. This is a value used by the API ML to group multiple API services into a single tile. Each identifier represents a single API dashboard tile in the Catalog.

**Important!** Specify a value that does not interfere with API services from other products. We recommend that you use your company and product name as part of the ID.

#### • apiml.catalog.tile.title

This parameter specifies the title of the API services product family. This value is displayed in the API Catalog dashboard as the tile title.

#### • apiml.catalog.tile.description

This parameter is the detailed description of the API services product family. This value is displayed in the API Catalog UI dashboard as the tile description.

#### • apiml.catalog.tile.version

This parameter specifies the semantic version of this API Catalog tile.

**Note:** Ensure that you increase the version number when you introduce changes to the API service product family details.

#### Service parameters

Service parameters are grouped under the prefix: apiml.service

The following parameters define service information for the API Catalog:

#### • apiml.service.title

This parameter specifies the human-readable name of the API service instance.

This value is displayed in the API Catalog when a specific API service instance is selected.

#### • apiml.service.description

This parameter specifies a short description of the API service.

This value is displayed in the API Catalog when a specific API service instance is selected.

#### • apiml.enableUrlEncodedCharacters

When this parameter is set to true, the Gateway allows encoded characters to be part of URL requests redirected through the Gateway. The default setting of false is the recommended setting.

Change this setting to true only if you expect certain encoded characters in your application's requests.

**Important!** When the expected encoded character is an encoded slash or backslash (%2F, %5C), make sure the Gateway is also configured to allow encoded slashes. For more info see Installing the Zowe runtime on z/OS.

#### • apiml.connectTimeout

The value in milliseconds that specifies a period in which API ML should establish a single, nonmanaged connection with this service. If omitted, the default value specified in the API ML Gateway service configuration is used.

#### • apiml.readTimeout

The value in milliseconds that specifies maximum time of inactivity between two packets in response from this service to API ML. If omitted, the default value specified in the API ML Gateway service configuration is used.

#### • apiml.connectionManagerTimeout

HttpClient employs a special entity to manage access to HTTP connections called by HTTP connection manager. The purpose of an HTTP connection manager is to serve as a factory for new HTTP connections, to manage the life cycle of persistent connections, and to synchronize access to persistent connections. Internally, an HTTP connection manager works with managed connections, which serve as proxies for real connections. **ConnectionManagerTimeout** specifies a period in which managed connections with API ML should be established. The value is in milliseconds. If omitted, the default value specified in the API ML Gateway service configuration is used.

#### • apiml.okToRetryOnAllOperations

Specifies whether all operations can be retried for this service. The default value is false. The false value allows retries for only GET requests if a response code of 503 is returned. Setting this value to true enables retry requests for all methods, which return a 503 response code. Enabling retry can impact server resources resulting from buffering of the request body.

#### • apiml.service.corsEnabled

When this parameter is set to true, CORS is enabled on the service level for all service routes. The same parameter can also be set on the service level, by providing the parameter as customMetadata

as shown in the custom metadata.md.

#### • apiml.response.compress

When this parameter is set to true, API ML compresses content for all responses from these services using GZIP. API ML also adds the Content-Encoding header with the value gzip to responses.

#### customMetadata.apiml.response.compressRoutes

When the customMetadata.apiml.response.compress parameter is set to true, this parameter allows the services to further limit the compressed routes. The parameter accepts ant style routes deliminated by , . The expectation is to provide the absolute paths. If relative paths are provided, the starting / is added. If the beginning of the pattern does not require specification, use \*\*/{pathYouAreInterestedIn}

#### Examples

o /service/\*\*

Compresses all paths starting with /service/

o /service/api/v1/compress,/service/api/v1/custom-compress

Compresses the specific two routes

/\\*\\*/compress/\\*\\*

Compresses all paths that contain compress as a specific path

#### **Routing parameters**

Routing parameters are grouped under the prefix: apiml.routes

The API routing group provides necessary routing information used by the API ML Gateway when routing incoming requests to the corresponding service. A single route can be used to make direct REST calls to multiple resources or API endpoints. The route definition provides rules used by the API ML Gateway to rewrite the URL in the Gateway address space.

Routing information consists of two parameters per route:

gatewayUrl

serviceUrl

These two parameters together specify a rule of how the API service endpoints are mapped to the API Gateway endpoints.

The following snippet is an example of the API routing information properties.

#### Example:

where:

#### • apiml.routes.{route-prefix}.gatewayUrl

The gatewayUrl parameter specifies the portion of the gateway URL which is replaced by the serviceUrl path.

#### • apiml.routes.{route-prefix}.serviceUrl

The serviceUrl parameter provides a portion of the service instance URL path which replaces the gatewayUrl part.

**Note:** The routes configuration used for a direct REST call to register a service must also contain a prefix before the gatewayUrl and serviceUrl. This prefix is used to differentiate the routes. This prefix must be provided manually when *XML* configuration is used.

For more information about API ML routing, see API Gateway Routing.

#### **Authentication parameters**

Authentication parameters are grouped under the prefix: apiml.authentication. When unspecified, the default values are used.

This parameter enables a service to accept the Zowe JWT token. The API Gateway translates the token to an authentication method supported by a service.

The following parameters define the service authentication method:

#### • apiml.authentication.scheme

This parameter specifies a service authentication scheme. The following schemes are supported by the API Gateway:

#### • bypass

This value specifies that the token is passed unchanged to the service.

Note: This is the default scheme when no authentication parameters are specified.

#### • zoweJwt

This value specifies that a service accepts the Zowe JWT token. No additional processing is done by the API Gateway.

#### • httpBasicPassTicket

This value specifies that a service accepts PassTickets in the Authorization header of the HTTP requests using the basic authentication scheme. It is necessary to provide a service APPLID in the apiml.authentication.applid parameter.

**Tip:** For more information, see Enabling PassTicket creation for API Services that Accept PassTickets.

#### • zosmf

This value specifies that a service accepts z/OSMF LTPA (Lightweight Third-Party Authentication). This scheme should only be used for a z/OSMF service used by the API Gateway Authentication Service, and other z/OSMF services that are using the same LTPA key.

**Tip:** For more information about z/OSMF Single Sign-on, see Establishing a single sign-on environment.

#### • apiml.authentication.applid

This parameter specifies a service APPLID. This parameter is valid only for the httpBasicPassTicket authentication scheme.

#### **API Info parameters**

API Info parameters are grouped under the prefix: apiml.apiInfo.

REST services can provide multiple APIs. Add API info parameters for each API that your service wants to expose on the API ML. These parameters provide information for API (Swagger) documentation that is displayed in the API Catalog.

The following parameters provide the information properties of a single API:

#### • apiml.apiInfo.{api-index}.apiId

The API ID uniquely identifies the API in the API ML. Multiple services can provide the same API. The API ID can be used to locate the same APIs that are provided by different services. The creator of the API defines this ID. The API ID needs to be a string of up to 64 characters that uses lowercase alphanumeric characters and a dot: .

Tip: We recommend that you use your organization as the prefix.

#### • apiml.apiInfo.{api-index}.version

This parameter specifies the API version. This parameter is used to correctly retrieve the API documentation according to the requested version of the API.

#### • apiml.apiInfo.{api-index}.gatewayUrl

This parameter specifies the base path at the API Gateway where the API is available. Ensure that this value is the same path as the gatewayUrl value in the routes sections for the routes, which belong to this API.

#### • apiml.apiInfo.{api-index}.swaggerUrl

(Optional) This parameter specifies the Http or Https address where the Swagger JSON document is available.

#### • apiml.apiInfo.{api-index}.documentationUrl

(Optional) This parameter specifies the link to the external documentation. A link to the external documentation can be included along with the Swagger documentation.

#### • apiml.apiInfo.{api-index}.defaultApi

(Optional) This parameter specifies if the API is the default one shown in the API Catalog. If no API has this parameter set to true, or multiple APIs have it set to true, then the default API becomes the API with the highest major version seen in apiml.apiInfo.{api-index}.version.

**Note:** The {api-index} is used to differentiate the service APIs. This index must be provided manually when *XML* configuration is used. In the following example, **0** represents the api-index.

## Sending a heartbeat to API Mediation Layer Discovery Service

After registration, a service must send a heartbeat periodically to the Discovery Service to indicate that the service is available. When the Discovery Service does not receive a heartbeat, the service instance is deleted from the Discovery Service.

If the server does not receive a renewal in 90 seconds, it removes the instance from its registry.

Note: We recommend that the interval for the heartbeat is no more than 30 seconds.

Use the Http PUT method in the following format to tell the Discovery Service that your service is available:

https://{eureka\_hostname}:{eureka\_port}/eureka/apps/{serviceId}/{instanceId}

## Validating successful onboarding with the API Mediation Layer

Ensure that you successfully onboarded a service with the API Mediation Layer.

#### Follow these steps:

- 1. Validate successful onboarding
- 2. Check that you can access your API service endpoints through the Gateway.
- 3. (Optional) Check that you can access your API service endpoints directly outside of the Gateway.

## **External Resources**

- https://blog.asarkar.org/technical/netflix-eureka/
- https://medium.com/@fahimfarookme/the-mystery-of-eureka-health-monitoring-5305e3beb6e9
- https://github.com/Netflix/eureka/wiki/Eureka-REST-operations

## Onboarding a Spring Boot based REST API Service

This guide is part of a series of guides to onboard a REST API service with the Zowe API Mediation Layer. As an API developer, you can onboard your REST API service built with the Spring Boot framework with the Zowe API Mediation Layer.

**Note:** Before API ML version 1.2, the API ML provided an integration enabler based on Spring Cloud Netflix components. From version 1.3 and later, the API ML uses a new implementation based on the Plain Java Enabler (PJE) that is not backwards compatible with the previous enabler versions. API ML core services (Discovery Service, Gateway, and API Catalog) support both the old and new enabler versions.

Tip: For more information about how to utilize another onboarding method, see:

- Onboard a REST API service with the Plain Java Enabler (PJE)
- Onboard a REST service directly calling eureka with xml configuration
- Onboard an existing REST API service without code changes

## **Outline of onboarding a REST service using Spring Boot**

The following steps outline the overall process to onboard a REST service with the API ML using a Spring Boot enabler. Each step is described in further detail in this article.

- 1. Selecting a Spring Boot Enabler
- 2. Configuring your project
  - Gradle build automation system
  - Maven build automation system
- 3. Configuring your Spring Boot based service to onboard with API ML
  - Sample API ML Onboarding Configuration
  - SAF Keyring configuration
  - Custom Metadata
  - Api Mediation Layer specific metadata

- 4. Registering and unregistering your service with API ML
  - Unregistering your service with API ML
  - Basic routing
- 5. Adding API documentation
- 6. (Optional) Validating your API service discoverability
- 7. (Optional) Troubleshooting
  - Log messages during registration problems

## **Selecting a Spring Boot Enabler**

Add a dependency on the Spring Enabler version to your project build configuration that corresponds to the Spring Boot version that you use for the whole project:

- onboarding-enabler-spring-v1
- onboarding-enabler-spring-v2

**Note:** The process of onboarding an API service is the same for both Spring Boot enabler versions.

## **Configuring your project**

Use either Gradle or Maven as your build automation system to manage your project builds.

**Note:** You can download the selected enabler artifact from the Zowe Artifactory for latest stable versions.. Alternatively, if you decide to build the API ML from source, it is necessary to publish the enabler artifact to your Artifactory. Publish the enabler artifact by using the *Gradle* tasks provided in the source code.

#### Gradle build automation system

Use the following procedure to use *Gradle* as your build automation system.

#### Follow these steps:

1. Create a gradle.properties file in the root of your project if one does not already exist.

- 2. In the gradle.properties file, set the URL of the specific Artifactory containing the SpringEnabler artifact.
- 3. Add the following *Gradle* code block to the repositories section of your build.gradle file:
- 4. In the same build.gradle file, add the necessary dependencies for your service. If you use the *SpringEnabler* from the Zowe Artifactory, add the following code block to your build.gradle script:

Use the corresponding artifact according to the Zowe APIML version you are using.

- For Zowe APIML versions greater than 1.23.5 use the following artifact:
- For Zowe APIML version 1.23.5 use the following artifact:
- For Zowe APIML versions 1.22.3, 1.22.4, and 1.23.0 1.23.4 use the following artifact:
- For Zowe APIML versions 1.21.6 1.21.13 and 1.22.0 1.22.2 use the following artifact:
- For Zowe APIML versions earlier than 1.21.6 that use Spring 2.1.1 use the following artifact:
- For Zowe APIML versions earlier than 1.21.6 that use Spring 1.5.9 use the following artifact:

#### Notes:

- You may need to add additional dependencies as required by your service implementation.
- The information provided in this file is valid for ZoweApimlVersion 1.3.0 and above.
- 5. In your project home directory, run the gradle clean build command to build your project. Alternatively, you can run gradlew to use the specific gradle version that is working with your project.

#### Maven build automation system

Use the following procedure if you use Maven as your build automation system.

#### Follow these steps:

1. Add the following XML tags within the newly created pom.xml file:

**Tip:** If you want to use snapshot version, replace libs-release with libs-snapshot in the repository url and change snapshots->enabled to true.

- For Zowe APIML versions greater than 1.23.5 use the following artifact:
- For Zowe APIML version 1.23.5 use the following artifact:
- For Zowe APIML versions 1.22.3, 1.22.4, and 1.23.0 1.23.4 use the following artifact:
- For Zowe APIML versions 1.21.6 1.21.13 and 1.22.0 1.22.2 use the following artifact:
- For Zowe APIML versions earlier than 1.21.6 that use Spring 2.1.1 use the following artifact:
- For Zowe APIML versions earlier than 1.21.6 that use Spring 1.5.9 use the following artifact:
- 3. In the directory of your project, run the mvn clean package command to build the project.

## Configuring your Spring Boot based service to onboard with API ML

To configure a Spring Boot based service, it is useful to first understand how API ML enabled service Spring Boot based configuration relates to configuration using the Plain Java Enabler.

Spring Boot expects to find the default configuration of an application in an application.yml file that is placed on the classpath. Typically application.yml contains Spring Boot specific properties such as properties that are used to start a web application container including TLS security, different spring configuration profiles definitions, and other properties. This application.yml must contain the Plain Java Enabler API ML service configuration under the apiml.service prefix. The API ML configuration under this prefix is necessary to synchronize the configuration of apiml.service with the spring server configuration.

Configuration properties belong to two categories:

- Service related properties which include endpoints, relative paths, or API documentation definitions.
- Environment related properties which include host names, ports, context etc.

Execution environment related properties should be provided by additional configuration mechanisms that are specific to the target execution environment. Execution environment related properties for development deployments on a local machine differ with those properties on a mainframe system.

- In a development environment, provide execution environment related properties in an additional YAML file with the system property in the following format:
- On the mainframe system, provide additional configuration properties and values for existing configuration properties through Java system properties.

Execution environments for local development deployments and mainframe deployment are described in detail later in this article.

#### Follow these steps:

- 1. Provide a configuration section for onboarding with API ML in the application.yml file.
  - If you have already onboarded your service with API ML, copy and paste the contents of your existing API ML onboarding configuration file. The default of the API ML onboarding configuration file is the service-configuration.yml in the application.yml file under the apiml.service prefix.
  - If you have not yet onboarded your REST service with API ML, use the Sample API Onboarding Configuration to get started.
- 2. If you are reusing your existing API ML onboarding configuration, modify the API ML related properties of the application.yml file.

a) Remove certain properties under the apiml.service section, which must be externalized. Properties for removal are described in the following sample of API ML onboarding configuration.

b) Provide the following additional properties under the apiml section:

These additional properties are contained in the following sample.

#### Sample API ML Onboarding Configuration

In the following sample API ML onboarding configuration, properties prefixed with **###** (3 hashtags) indicate that their value must be provided as **\_Dsystem.property.key=PROPERTY\_VALUE** defined in the mainframe execution environment. The **\_Dsystem.property.key** must be the same as the flattened path of the YAML property which is commented out with **###**. These properties must not be defined (uncommented) in your default service YAML configuration file.

#### Example:

In this example from the YAML configuration file, when the application service is run on the mainframe, provide your mainframe hostname value on the Java execution command line in the following format:

Since this value is provided in the Java execution command line, leave the property commented out in the application.yml.

For development purposes, you can replace or add any property by providing the same configuration structure in an external YAML configuration file. When running your application, provide the name of the external/additional configuration file on the command line in the following format:

A property notation provided in the format -Dproperty.key=PROPERTY\_VALUE can be used for two purposes:

To provide a runtime value for any YAML property if \${property.key} is used as its value (after
in the YAML configuration file

#### Example:

• To add a property to configuration if the property does not already exist

#### Example:

**Note**: System properties provided with –D notation on the command line will not replace properties defined in any of the YAML configuration files.

#### **API ML Onboarding Configuration Sample**

Some parameters which are specific for your service deployment are written in \${fill.your.parameterValue} format. For your service configuration file, provide actual values or externalize your configuration using -D java commandline parameters.

**Tip:** To determine if your configuration is complete, set the logging level to **debug** and run your application. Setting the logging level to 'debug' enables you to troubleshoot issues with certificates for HTTPS and connections with other services.

3. Provide the suitable parameter corresponding to your runtime environment:

• For a local machine runtime environment, provide the following parameter on your command line:

At runtime, Spring will merge the two YAML configuration files, whereby the properties in the external file have higher priority.

• For a mainframe execution environment, provide environment specific configuration properties. Define these configuration properties and provide them using Java System Properties on the application execution command line.

**Important!** Ensure that the default configuration contains only properties which are not dependent on the deployment environment. Do not include security sensitive data in the default configuration.

**Note:** For details about the configuration properties, see Configuring your service in the article *Onboarding a REST API service with the Plain Java Enabler (PJE)*.

#### SAF Keyring configuration

You can choose to use a SAF keyring instead of keystore and truststore for storing certificates. For information about required certificates, see Zowe API ML TLS requirements. For information about running Java on z/OS with a keyring, see SAF Keyring. Make sure that the enabler can access and read the keyring. Please refer to documentation of your security system for details.

The following example shows enabler configuration with keyrings:

#### **Custom Metadata**

Custom metadata are described here.

## Registering and unregistering your service with API ML

Onboarding a REST service to the API ML means registering the service with the API ML Discovery Service. The registration is triggered automatically by Spring after the service application context is fully initialized by firing a ContextRefreshed event.

To register your REST service with API ML using a Spring Boot enabler, annotate your application main class with @EnableApiDiscovery.

#### Unregistering your service with API ML

Unregistering a service onboarded with API ML is done automatically at the end of the service application shutdown process in which Spring fires a **ContextClosed** event. The Spring onboarding enabler listens for this event and issues an **unregister** REST call to the API ML Discovery Service.

#### **Basic routing**

See API ML Basic Routing for more information about basic routing in the API ML.

## **Adding API documentation**

Use the following procedure to add Swagger API documentation to your project.

#### Follow these steps:

- 1. Add a SpringFox Swagger dependency.
  - For *Gradle*, add the following dependency in build.gradle:
  - For *Maven*, add the following dependency in pom.xml:
- 2. Add a Spring configuration class to your project.

#### Example:

3. Customize this configuration according to your specifications. For more information about customization properties, see Springfox documentation.

**Note:** The current SpringFox Version 2.9.2 does not support OpenAPI 3.0. For more information about the open feature request see this issue.

## Validating the discoverability of your API service by the Discovery Service

Once you build and start your service successfully, you can use the option of validating that your service is registered correctly with the API ML Discovery Service.

#### Follow these steps:

1. Validate successful onboarding

- 2. Check that you can access your API service endpoints through the Gateway.
- 3. (Optional) Check that you can access your API service endpoints directly outside of the Gateway.

Specific addresses and user credentials for the individual API ML components depend on your target runtime environment.

**Note:** If you are working with local installation of API ML and you are using our dummy identity provider, enter user for both username and password. If API ML was installed by system administrators, ask them to provide you with actual addresses of API ML components and the respective user credentials.

**Tip:** Wait for the Discovery Service to fully register your service. This process may take a few minutes after your service was successfully started.

## Troubleshooting

#### Log messages during registration problems

When an Enabler connects to the Discovery Service and fails, an error message prints to the Enabler log. The default setting does not suppress these messages as they are useful to resolve problems during the Enabler registration. Possible reasons for failure include the location of Discovery Service is not correct, the Discovery Service is down, or the TLS certificate is invalid. These messages continue to print to the Enabler log, while the Enabler retries to connect to the Discovery Service.

To fully suppress these messages in your logging framework, set the log levels to **OFF** on the following loggers:

Some logging frameworks provide other tools to suppress repeated messages. Consult the documentation of the logging framework you use to find out what tools are available. The following example demonstrates how the Logback framework can be used to suppress repeated messages.

#### Example:

The Logback framework provides a filter tool, DuplicateMessageFilter.

Add the following code to your configuration file if you use XML configuration:

**Note:** For more information, see the full configuration used in the Core Services in GitHub.

Version: v1.25.x LTS

# Onboarding a Micronaut based REST API service

As an API developer, you can onboard a REST service to the Zowe API Mediation Layer using the Micronaut framework. While using the Spring framework to develop a JVM-based service to register to the API ML is the recommended method, you can use the procedure described in this article to onboard a service using the Micronaut framework.

Note: For more information about onboarding API services with the API ML, see the Onboarding Overview.

For Micronaut-related documentation, see the Micronaut website.

- Set up your build automation system
  - Specify the main class
  - Define the output jar file
  - (Optional) Create a shadow jar
  - Start the application
- Configure the Micronaut application
  - Add API ML configuration
  - Add Micronaut configuration
  - Set up logging configuration
- Validate successful registration

## Set up your build automation system

Currently, the only build automation system for use with onboarding a Micronaut based service is Gradle.

#### Follow these steps:

- 1. Create a gradle.properties file in the root of your project if one does not already exist.
- 2. In the gradle.properties file, set the URL of the specific Artifactory containing the SpringEnabler artifact.
- 3. Add the following *Gradle* code block to the repositories section of your build.gradle file:

4. In the build.gradle file, add the micronaut enabler as a dependency:

- 5. (Optional) Add a shadow plug-in to create a runnable jar file. Update the gradle.build file with a plugin:
- 6. Specify the main class with the following script:
- 7. Define the output jar file.

Add the following script to define the output of the jar file:

The following example shows a sample gradle.build file:

#### Example:

8. (Optional) Create a shadow jar.

To create a shadow jar, execute the gradle shadowJar task. For this sample, the plugin produces the jar micronaut-enabler-1.0.jar in build/libs directory.

You can now run your application with the command java -jar micronaut-enabler-1.0.jar.

9. Start the application.

From the root directory of your project, start the application with the **gradle run** command.

## **Configure the Micronaut application**

Use a yaml file to configure your Micronaut application. Create the following two sections in your yaml file:

- apiml for API ML configuration
- micronaut for micronaut configuration

#### Add API ML configuration

Use the following procedure to add API ML configuration to the application.yaml.

#### Follow these steps:

1. Add the following configuration to the apiml section in the yaml file:

where:

#### o fill.your.service

specifies the ID of your service

2. Add SSL-resolving properties as shown in the following example. Ensure that you structure the nested objects within apiml.service as arrays. Be sure to include – (hyphen) before enabled thereby indicating the first element of the array.

#### Example:

**Note:** For a sample of this configuration, see API ML Onboarding Configuration Sample.

The yaml now contains configuration to register to the API Mediation Layer.

#### Add Micronaut configuration

Once you complete API ML configuration, add configuration to provide correct mapping between API ML and micronaut parameters.

#### Follow these steps:

1. Add the following yaml snippet with the micronaut configuration parameters:

where:

o apiml.service.serviceId

specifies the ID of your service

o apiml.service.port

specifies the port on which the service listens

apiml.service.ssl[0].keyPassword

specifies the password that protects the key in keystore

apiml.service.ssl[0].keyStoreType

specifies the type of the keystore, (Example: PKCS12)

#### o apiml.service.ssl[0].keyStore

specifies the location of the keystore

#### apiml.service.ssl[0].keyAlias

specifies the alias under which the key is stored in the keystore

#### o apiml.service.ssl[0].trustStorePassword

specifies the password that protects the certificates in the truststore

#### o apiml.service.ssl[0].trustStore

specifies the location of the truststore

#### o apiml.service.ssl[0].trustStoreType

specifies the type of the truststore, (Example: PKCS12)

#### apiml.service.ssl[0].ciphers

specifies the list of ciphers that user wants to enable for TLS communication

#### apiml.service.ssl[0].protocol

specifies the type of SSL/TLS protocol (Example: TLSv1.2)

#### (Optional) Set up logging configuration

Set up custom logging configuration to have more structured output and better control of logs.

Create a logback.xml file in the resources folder and include the application.yml. Update the logback.xml file with the following configuration:

## Validate successful registration

After you complete the configuration, ensure that your application is visible within Zowe API ML. For more information, see the article validating the discoverability of your API service by teh Discovery Service, which describes the validation procedure common for all enablers.

Version: v1.25.x LTS

## Onboarding a Node.js based REST API service

This article is part of a series of onboarding articles, which outline the process of onboarding REST API services to the Zowe API Mediation Layer (API ML). As a service developer, you can onboard a REST service based on NodeJS with the API ML with the Zowe API Mediation Layer using our Node.js Enabler.

Note: For more information about onboarding API services with the API ML, see the Onboarding Overview.

## Introduction

The API ML onboarding Node.js enabler is an NPM package which helps to simplify the process of onboarding a REST service written in Node.js with the API ML.

For more information about how to utilize another API ML enablers, see the Onboarding Overview.

## **Onboarding your Node.js service with API ML**

The following steps outline the overall process to onboard a REST service with the API ML using the onboarding Node.js enabler. Each step is described in further detail in this article.

- 1. Prerequisites
- 2. Install the npm dependency
- 3. Configure your service
- 4. Register your service with API ML
- 5. (Optional) Validate the discoverability of your API service by the Discovery Service

### Prerequisites

Ensure that you meet the following prerequisites:

- You satisfy the prerequisites from the Onboarding Overview.
- The REST API service to onboard is written in Node.js.
- The service is enabled to communicate with API ML Discovery Service over a TLS v1.2 secured connection.

### Installing the npm dependency

Install the onboarding Node.js enabler package as a dependency of your service. Run the following npm command from your project directory:

**Note:** If you have a multi-module project, you have to run the npm command from the submodule where your Node.js project is located.

## **Configuring your service**

Create a yaml file named service-configuration.yml inside a /config directory at the same level of your index.js, and add the following configuration properties.

The following example shows a sample configuration.

#### **Example:**

## **Registering your service with API ML**

To register your service with API ML, use the following procedure.

#### Follow these steps:

- 1. Inside your Node.js service index.js, add the following code block to register your service with Eureka:
- 2. Start your Node.js service and verify that the service is registered to the Zowe API Mediation Layer.

## Validating the discoverability of your API service by the Discovery Service

Once you build and start your service successfully, you can use the option of validating that your service is registered correctly with the API ML Discovery Service.

#### Follow these steps:

- 1. Validate successful onboarding
- 2. Check that you can access your API service endpoints through the Gateway.
- 3. (Optional) Check that you can access your API service endpoints directly outside of the Gateway.

Specific addresses and user credentials for the individual API ML components depend on your target runtime environment.

**Note:** If you are working with a local installation of API ML, and you are using our dummy identity provider, enter user for both username and password. If API ML was installed by system administrators, ask them to provide you with actual addresses of API ML components and the respective user credentials.

**Note:** Wait for the Discovery Service to fully register your service. This process may take a few minutes after your service starts successfully.

# Onboard a REST API without code changes required

As a user of Zowe<sup>™</sup>, onboard an existing REST API service to the Zowe<sup>™</sup> API Mediation Layer without changing the code of the API service. This form of onboarding is also refered to as, "static onboarding".

**Note:** When developing a new service, it is not recommended to onboard a REST service using this method, as this method is non-native to the API Mediation Layer. For a complete list of methods to onboard a REST service natively to the API Mediation Layer, see the Onboarding Overview.

The following procedure outlines the steps to onboard an API service through the API Gateway in the API Mediation Layer without requiring code changes.

- Identify the API that you want to expose
- Define your service and API in YAML format
- Route your API
- Customize configuration parameters
- Add and validate the definition in the API Mediation Layer running on your machine
- Add a definition in the API Mediation Layer in the Zowe runtime
- (Optional) Check the log of the API Mediation Layer
- (Optional) Reload the services definition after the update when the API Mediation Layer is already started

**Tip:** For more information about the structure of APIs and which APIs to expose in the Zowe API Mediation Layer, see the Onboarding Overview.

### Identify the APIs that you want to expose

The first step in API service onboarding is to identify the APIs that you want to expose.

#### Follow these steps:

- 1. Identify the following parameters of your API service:
  - Hostname

- Port
- (Optional) base path where the service is available. This URL is called the base URL of the service.

#### Example:

In the sample service described in the Onboarding Overview, the URL of the service is: http://localhost:8080.

2. Identify the API of the service that you want to expose through the API Gateway.

#### Example:

The API provided by the sample service is a second version of the Pet Store API. All the endpoints to be onboarded are available through http://localhost:8080/v2/ URL. This REST API is therefore available at the path /v2 relative to base URL of the service. There is no version 1 in this case.

3. Choose the service ID of your service. The service ID identifies the service uniquely in the API Gateway. The service ID is an alphanumeric string in lowercase ASCII.

#### Example:

In the sample service, the service ID is petstore.

4. Decide which URL to use to make this API available in the API Gateway. This URL is referred to as the gateway URL and is composed of the API type and the major version. The usually used types are: api, ui and ws but you can use any valid URL element you want.

#### Example:

In the sample service, we provide a REST API. The first segment is /api as the service provides only one REST API. To indicate that this is version 2, the second segment is /v2. This version is required by the Gateway. If your service does not have a version, use v1 on the Gateway.

### Define your service and API in YAML format

After you identify the APIs you want to expose, you need to define your service and API in YAML format as presented in the following sample petstore service example.

#### **Example:**

To define your service in YAML format, provide the following definition in a YAML file as in the following sample **petstore** service. This configuration is the minimal configuration necessary for the Gateway to properly route the requests to the application and to show the Service in the Catalog UI.

**Note:** For more details about configuration, see Customize configuration parameters.

In this example, a suitable name for the file is petstore.yml.

#### Notes:

- The filename does not need to follow specific naming conventions but it requires the .yml extension.
- The file can contain one or more services defined under the services: node.
- Each service has a service ID. In this example, the service ID is **petstore**. The service id is used as a part of the request URL towards the Gateway. It is removed by the Gateway when forwarding the request to the service.
- The service can have one or more instances. In this case, only one instance http://localhost:8080 is used.
- One API is provided and the requests with the relative base path api/v2 at the API Gateway (full gateway URL: https://gateway:port/api/v2/serviceId/...) are routed to the relative base path /v2 at the full URL of the service (http://localhost:8080/v2/...).
- The file on USS should be encoded in ASCII to be read correctly by the API Mediation Layer.

#### Tips:

- There are more examples of API definitions at this link.
- For more details about how to use YAML format, see this link.

## **Route your API**

Routing is the process of sending requests from the API Gateway to a specific API service. Route your API by using the same format as in the following petstore example. The configuration parameters are explained in Customize configuration parameters. Gateway URL format:

Note: The API Gateway differentiates major versions of an API.

#### Example:

When the configuration parameters are:

To access API version 2 of the service petstore, gateway URL will be:

It will be routed to:

To access resource pets of the petstore version 2 API, gateway URL will be:

It will be routed to:

**Note:** This method enables you to access the service through a stable URL, and move the service to another machine without changing the gateway URL. Accessing a service through the API Gateway also enables you to have multiple instances of the service running on different machines to achieve high-availability.

### **Customize configuration parameters**

This part contains a more complex example of the configuration and an explanation of all the possible parameters:

#### • serviceId

This parameter specifies the service instance identifier that is registered in the API Mediation Layer installation. The service ID is used in the URL for routing to the API service through the Gateway. The service ID uniquely identifies the service in the API Mediation Layer. The system administrator at the customer site defines this parameter.

Important! Ensure that the service ID is set properly with the following considerations:

- When two API services use the same service ID, the API Gateway considers the services to be clones (i.e. two instances for the same service). An incoming API request can be routed to either of them.
- The same service ID should be set only for multiple API service instances for API scalability.
- The service ID value must contain only lowercase alphanumeric characters.
- The service ID cannot contain more than 40 characters.

• The service ID is linked to security resources. Changes to the service ID require an update of security resources.

#### Examples:

- If the customer system administrator sets the service ID to monitoringpr1, the API URL in the API Gateway appears as the following URL:
- If customer system administrator sets the service ID to authenticationprod1, the API URL in the API Gateway appears as the following URL:

#### • title

This parameter specifies the human readable name of the API service instance (for example, Monitoring Prod or systemInfo LPAR1). This value is displayed in the API catalog when a specific API service instance is selected. This parameter is externalized and set by the customer system administrator.

**Tip:** We recommend that you provide a specific default value of the title. Use a title that describes the service instance so that the end user knows the specific purpose of the service instance.

#### description

This parameter specifies a short description of the API service.

#### Examples:

- Monitoring Service Production Instance
- System Info Service running on LPAR1

This value is displayed in the API Catalog when a specific API service instance is selected. This parameter is externalized and set by the customer system administrator.

Tip: Describe the service so that the end user knows the function of the service.

#### • instanceBaseUrls

This parameter specifies a list of base URLs to your service's REST resource. It will be the prefix for the following URLs:

- homePageRelativeUrl
- statusPageRelativeUrl
- healthCheckRelativeUrl

#### **Examples:**

- http://host:port/ftpservice for an HTTP service
- - https://host:port/source-code-mngmnt for an HTTPS service

You can provide one URL if your service has one instance. If your service provides multiple instances for the high-availability then you can provide URLs to these instances.

#### **Examples:**

- https://host1:port1/source-code-mngmnt
- o https://host2:port2/source-code-mngmnt

#### homePageRelativeUrl

This parameter specifies the relative path to the homepage of your service. The path should start with /. If your service has no homepage, omit this parameter. The path is relative to the instanceBaseUrls.

#### Examples:

- homePageRelativeUrl: / The service has homepage with URL \${baseUrl}/
- homePageRelativeUrl: /ui/ The service has homepage with URL \${baseUrl}/ui/
- o homePageRelativeUrl: The service has homepage with URL \${baseUrl}

#### • statusPageRelativeUrl

This parameter specifies the relative path to the status page of your service. Start this path with  $\bigcirc$ . If you service doesn't have a status page, omit this parameter. The path is relative to the instanceBaseUrls.

#### Example:

the result URL will be:

#### \${baseUrl}/application/info

#### healthCheckRelativeUrl

This parameter specifies the relative path to the health check endpoint of your service. Start this URL with  $\checkmark$ . If your service does not have a health check endpoint, omit this parameter. The path is relative to the instanceBaseUrls.

#### Example:

healthCheckRelativeUrl: /application/health

This results in the URL:

\${baseUrl}/application/health

#### routes

The following parameters specify the routing rules between the Gateway service and your service. Both specify how the API endpoints are mapped to the API Gateway endpoints.

#### routes.gatewayUrl

The *gatewayUrl* parameter sets the target endpoint on the Gateway. This is the portion of the final URL that is Gateway specific.

#### Example:

For the petstore example, the full Gateway URL would be:

https://gatewayUrl:1345/api/v2/petstore/pets/1

In this case, the URL that will be called on the service is:

http://localhost:8080/v2/pets/1

#### • routes.serviceRelativeUrl

The *serviceRelativeUrl* parameter points to the target endpoint on the service. This is the base path on the service called through the Gateway.

#### • authentication

Parameters under this grouping allow a service to accept the Zowe JWT token. The API Gateway translates the token to an authentication method supported by a service.

#### • authentication.scheme

This parameter specifies a service authentication scheme. The following schemes are supported by the API Gateway:

#### bypass

This value specifies that the token is passed unchanged to the service. This is the default scheme when no authentication parameters are specified.

#### zoweJwt

This value specifies that a service accepts the Zowe JWT token. No additional processing is done by the API Gateway.

#### httpBasicPassTicket

This value specifies that a service accepts PassTickets in the Authorization header of the HTTP requests using the basic authentication scheme. It is necessary to provide a service APPLID in the apiml.authentication.applid parameter.

**Tip:** For more information, see Enabling PassTicket creation for API Services that accept PassTickets.

#### zosmf

This value specifies that a service accepts z/OSMF LTPA (Lightweight Third-Party Authentication). This scheme should only be used for a z/OSMF service used by the API Gateway Authentication Service, and other z/OSMF services that are using the same LTPA key.

**Tip:** For more information about z/OSMF Single Sign-on, see Establishing a single sign-on environment.

#### • authentication.applid

This parameter specifies a service APPLID. This parameter is only valid for the httpBasicPassTicket authentication scheme.

#### • apilnfo

This section defines APIs that are provided by the service. Currently, only one API is supported.

#### • apilnfo.apild

that uses lowercase alphanumeric characters and a dot: .

#### • apilnfo.gatewayUrl

This parameter specifies the base path at the API Gateway where the API is available. Ensure that this path is the same as the *gatewayUrl* value in the *routes* sections.

#### • apilnfo.swaggerUrl

(Optional) This parameter specifies the HTTP or HTTPS address where the Swagger JSON document is available.

#### • apiInfo.documentationUrl

(Optional) This parameter specifies a URL to a website where external documentation is provided. This can be used when *swaggerUrl* is not provided.

#### • apilnfo.version

(Optional) This parameter specifies the actual version of the API in semantic versioning format. This can be used when *swaggerUrl* is not provided.

#### • apiInfo.defaultApi

(Optional) This parameter specifics that the API is the default one to show in the API Catalog. If this not set to true for any API, or multiple APIs have it set to true, then the default API becomes the API with the highest major version as seen in apiInfo.version.

#### customMetadata

Custom metadata are described here.

#### catalogUiTileId

This parameter specifies the unique identifier for the API services group. This is the grouping value used by the API Mediation Layer to group multiple API services together into "tiles". Each unique identifier represents a single API Catalog UI dashboard tile. Specify the value based on the ID of the defined tile.

#### • catalogUiTile

This section contains definitions of tiles. Each tile is defined in a section that has its tile ID as a key. A tile can be used by multiple services.

#### • catalogUiTile.{tileId}.title

This parameter specifies the title of the API services product family. This value is displayed in the API Catalog UI dashboard as the tile title.

#### • catalogUiTile.{tileId}.description

This parameter specifies the detailed description of the API Catalog UI dashboard tile. This value is displayed in the API Catalog UI dashboard as the tile description.

#### • additionalServiceMetadata

This section contains a list of changes that allows adding or modifying metadata parameters for the corresponding service.

#### • additionalServiceMetadata.serviceId

This parameter specifies the service identifier for which metadata is updated.

#### • additionalServiceMetadata.mode

This parameter specifies how the metadata are updated. The following modes are available:

#### UPDATE

Only missing parameters are added. Already existing parameters are ignored.

#### FORCE\_UPDATE

All changes are applied. Existing parameters are overwritten.

#### • additionalServiceMetadata.{updatedParameter}

This parameter specifies any metadata parameters that are updated.

## Add and validate the definition in the API Mediation Layer running on your machine

After you define the service in YAML format, you are ready to add your service definition to the API Mediation Layer ecosystem.

The following procedure describes how to add your service to the API Mediation Layer on your local machine.

#### Follow these steps:

- 1. Copy or move your YAML file to the config/local/api-defs directory in the directory with API Mediation Layer.
- 2. Start the API Mediation Layer services.

**Tip:** For more information about how to run the API Mediation Layer locally, see Running the API Mediation Layer on Local Machine.

3. Run your Java application.

Tip: Wait for the services to be ready. This process may take a few minutes.

4. Validate successful onboarding

You successfully defined your Java application if your service is running and you can access the service endpoints. The following example is the service endpoint for the sample application:

https://localhost:10010/api/v2/petstore/pets/1

## Add a definition in the API Mediation Layer in the Zowe runtime

After you define and validate the service in YAML format, you are ready to add your service definition to the API Mediation Layer running as part of the Zowe runtime installation on z/OS.

#### Follow these steps:

 Locate the Zowe instance directory. The Zowe instance directory is the directory from which Zowe was launched, or else was passed as an argument to the SDSF command used to start Zowe. If you are unsure which instance directory a particular Zowe job is using, open the JESJCL spool file and navigate to the line that contains STARTING EXEC ZWESVSTC, INSTANCE=. This is the fully qualified path to the instance directory.

Tip: For more information, see Creating and configuring the Zowe instance directory.

**Note:** We use the \${zoweInstanceDir} symbol in following instructions.

- 2. Add the fully qualified zFS path of your YAML file to instance.env.
  - To hold your YAML file outside of the instance directory, append the fully qualified zFS path of the YAML file to the ZWEAD\_EXTERNAL\_STATIC\_DEF\_DIRECTORIES variable in the instance.env file. This variable contains a semicolon separated list of static API extension YAML files.
  - To place your YAML file within the instance directory, copy your YAML file to the \${zoweInstanceDir}/workspace/api-mediation/api-defs directory.

#### Notes:

- The \${zoweInstanceDir}/workspace/api-mediation/api-defs directory is created the first time that Zowe starts. If you have not yet started Zowe, this directory might be missing.
- The user ID ZWESVUSR that runs the Zowe started task must have permission to read the YAML file.
- 3. Ensure that your application that provides the endpoints described in the YAML file is running.
- 4. Restart Zowe runtime or follow steps in section (Optional) Reload the services definition after the update when the API Mediation Layer is already started which allows you to add your static API service to an already running Zowe.

#### 5. Validate successful onboarding

You successfully defined your Java application if your service is running and you can access its endpoints. The endpoint displayed for the sample application is:

## (Optional) Check the log of the API Mediation Layer

The API Mediation Layer log can contain messages based on the API ML configuration. The API ML prints the following messages to its log when the API definitions are processed:

Note: If these messages are not displayed in the log, ensure that the API ML debug mode is active.

## (Optional) Reload the services definition after the update when the API Mediation Layer is already started

The following procedure enables you to refresh the API definitions after you change the definitions when the API Mediation Layer is already running.

#### Follow these steps:

1. Use a REST API client to issue a **POST** request to the Discovery Service (port 10011):

#### http://localhost:10011/discovery/api/v1/staticApi

The Discovery Service requires authentication by a client certificate. If the API Mediation Layer is running on your local machine, the certificate is stored at keystore/localhost/localhost.pem.

This example uses the HTTPie command-line HTTP client and is run with Python 3 installed:

Alternatively, it is possible to use curl to issue the POST call if it is installed on your system:

2. Check if your updated definition is effective.

Note: It can take up to 30 seconds for the API Gateway to pick up the new routing.

## Zowe API Mediation Layer Single-Sign-On Overview

You can extend Zowe and utilize Zowe Single-Sign-On (SSO) provided by Zowe API Mediation Layer (API ML) to enhance system security and improve the user experience.

This article provides an overview of the API ML single-sign-on feature, the principle participants in the SSO process, and links to detailed Zowe SSO documentation. Zowe Single-Sign-On is based on single-user authentication which produces an access token that represents the user in communication with z/OS services accessible through the API Mediation Layer. The access token is issued by the Zowe Authentication and Authorization Service (ZAAS), which is part of API ML. ZAAS issues an access token based on valid z/OS credentials. This token can be validated by any component participating in SSO.

Note: Currently, API ML can provide SSO only in a single security domain.

- Zowe API ML client
- API service accessed via Zowe API ML
- Existing services that cannot be modified

The following diagram describes the interactions between the general participants in the single-sign-on process.

There are two main types of components that participate in Zowe SSO through API ML:

- Zowe API ML client
  - This type of component is user-facing and can obtain user credentials through a user interface (web, CLI, desktop).
  - API ML clients can be confidential or public.
  - A Zowe API ML client calls API services through the API ML.
  - An example of such clients are Zowe CLI or Zowe Desktop.
- An API service accessed through Zowe API ML
  - A service that is registered to API ML and is accessed through the API Gateway.

- Services are protected by an access token or PassTicket.
- The access token or PassTicket can be validated by the called API service.

The following sections describe what is necessary to utilize SSO for both types of components.

#### **Zowe API ML client**

- The Zowe API ML client needs to obtain an access token via the /login endpoint of ZAAS by providing z/OS credentials.
- A client can call the ZAAS /query endpoint to validate the token and get information from the token.
   This is useful when the API client has the token but does not store the associated data such as the user ID.
- The API client needs to provide the access token to API services in the form of a Secure HttpOnly cookie with the name apimlAuthenticationToken, or in the Authorization: Bearer HTTP header as described in Authenticated Request.

#### API service accessed via Zowe API ML

This section describes the requirements that an API service needs to satisfy to adopt a Zowe SSO access token.

- The token received by the Gateway is first validated and then may be passed directly to the service. Alternatively, the Gateway can exchange the token for a PassTicket if the API service is configured to expect a PassTicket.
- The API service can validate the token and extract information about the user ID by calling the ZAAS /query endpoint.
- The alternative is to validate the signature of the JWT token using the public key of the token issuer (e.g. the API ML Gateway). The API service needs to have the API ML Gateway certificate along with the full CA certification chain in the API service truststore.

Note: The REST API of ZAAS can easily be called from a Java application using the ZAAS Client.

#### Existing services that cannot be modified

If you have a service that cannot be changed to adopt the Zowe authentication token, the service can utilize Zowe SSO if the API service is able to handle PassTickets.

**Note:** For more information, see Enabling PassTicket creation for API Services that Accept PassTickets for more details.

# **Further resources**

- Authentication Methods
- User guide for SSO in Zowe CLI
- System requirements for using web tokens for SSO in Zlux and ZSS
- Certificate configuration for the usage of web tokens for SSO in Zlux and ZSS

# **Obtaining Information about API Services**

As an API Mediation Layer user, information about API services can be obtained for various purposes. The following list presents some of the use cases for using the API Mediation Layer:

- To display available services based on a particular criterion (API ID, hostname, or custom metadata)
- To locate a specific API service based on one or more specific criteria (for example the API ID)
- To obtain information that permits routing through the API Gateway such as baseUrl or basePath
- To obtain information about an API service, the service APIs, or instances of the service

This article provides further detail about each of these use cases.

- API ID in the API Mediation Layer
- Protection of Service Information
- API Endpoints
  - Obtain Information about a Specific Service
  - Obtain Information about All Services
  - Obtain Information about All Services with a Specific API ID

# **API ID in the API Mediation Layer**

The API ID uniquely identifies the API in the API ML. The API ID can be used to locate the same APIs that are provided by different service instances. The API developer defines this ID.

For more information about *baseUrl* or *basePath*, see Components of URL.

# **Protection of Service Information**

Information about API services is considered sensitive as it contains partial information about the internal topology of the mainframe system. As such, this information should be made accessible only by authorized users and services.

Access to this information requires authentication using mainframe credentials, and a SAF resource check is done. The resource class and resource is defined in the ZWESECUR job. You can find more details about the ZWESECUR job in Configuring the z/OS system for Zowe.

The security administrator needs to permit READ access to the APIML.SERVICES resource in the ZOWE resource class to the your that can access the information about API services.

In IBM RACF, the access to the service information can be given by:

In Top Secret:

In ACF2:

API Gateway can be configured to check for SAF resource authorization in several ways. For details, see SAF Resource Checking

# **API Endpoints**

## **Obtain Information about a Specific Service**

Use the following method to get information about a specific service:

GET /gateway/api/v1/services/{serviceId}

where:

• **{serviceId}** is the service ID of the API service (Example: apicatalog)

This method returns a JSON response that describes the service. For more information, see Response Format.

## **Obtain Information about All Services**

Use the following method to get information about all services:

## GET /gateway/api/v1/services

This method returns a JSON response with a list of all services. For more information, see Response Format.

## Obtain Information about All Services with a Specific API ID

Use the following method to get information about all services with a specific API ID:

## GET /gateway/api/v1/services?apiId={apiId}

where:

• {apild} is the API ID that represents required API (e.g. zowe.apiml.apicatalog)

This method returns a JSON response with a list of services provided by a specified API ID. For more information, see Response Format.

## **Response Format**

This section provides basic information about the structure of the response. The full reference on the field in the response is presented in the API Catalog.

The apiml section provides information about the following points:

- The service in the service subsection is displayed.
- The APIs that are provided by the service in the apiInfo section. This section presents each major API version that is provided by at least one instance. For each major version, the lowest minor version is displayed.
- The authentication methods that are supported by all instances are displayed.

API clients can use this information to locate the API based on API ID. baseUrl or basePath are used to access the API through the API Gateway.

The instances section contains more details about the instances of the service. An API service can provide more application specific details in customMetadata that can be used by API clients. Do not use information in this section for use cases that API Gateway supports, such as routing or load balancing.

## Example:

# API Mediation Layer Message Service Component

The API ML Message Service component unifies and stores REST API error messages and log messages in a single file. The Message Service component enables users to mitigate the problem of message definition redundancy which helps to optimize the development process.

- Message Definition
- Creating a message
- Mapping a message
- API ML Logger

# **Message Definition**

API ML uses a customizable infrastructure to format both REST API error messages and log messages. yaml files make it possible to centralize both API error messages and log messages. Messages have the following definitions:

• Message key - a unique ID in the form of a dot-delimited string that describes the reason for the message. The key enables the UI or the console to show a meaningful and localized message.

#### **Tips:**

- We recommend using the format org.zowe.sample.apiservice.{TYPE}.greeting.empty to define the message key. {TYPE} can be the api or log keyword.
- Use the message key and not the message number. The message number makes the code less readable, and increases the possibility of errors when renumbering values inside the number.
- Message number a typical mainframe message ID (excluding the severity code)
- Message type There are two Massage types:
  - REST API error messages: ERROR
  - Log messages: ERROR , WARNING , INFO , DEBUG , or TRACE

• Message text - a description of the issue

The following example shows the message definition.

Example:

## **Creating a message**

Use the following classes when you create a message:

- org.zowe.apiml.message.core.MessageService lets you create a message from a file.
- org.zowe.apiml.message.yaml.YamlMessageService implements

org.zowe.apiml.message.core.MessageService so that

org.zowe.apiml.message.yaml.YamlMessageService can read message information from a

yaml file, and create a message with message parameters.

Use the following process to create a message.

#### Follow these steps:

1. Load messages from the yaml file.

#### Example:

 Use the Message createMessage(String key, Object... parameters); method to create a message.

Example:

# Mapping a message

You can map the Message either to a REST API response or to a log message.

When you map a REST API response, use the following methods:

- mapToView returns a UI model as a list of API Message, and can be used for Rest API error messages
- mapToApiMessage returns a UI model as a single API Message

The following example is a result of using the mapToView method.

## Example:

The following example is the result of using the mapToApiMessage method.

## Example:

## **API ML Logger**

The org.zowe.apiml.message.log.ApimLogger component controls messages through the Message Service component.

The following example uses the log message definition in a yaml file.

## Example:

When you map a log message, use mapToLogMessage to return a log message as text. The following example is the output of the mapToLogMessage.

## Example:

Use the ApimlLogger to log messages which are defined in the yaml file.

## Example:

The following example shows the output of a successful ApimlLogger usage.

## Example:

# **Zowe API Mediation Layer Security**

- Zowe API Mediation Layer Security
  - Zowe API Mediation Layer Single-Sign-On Overview
  - How API ML transport security works
    - Transport layer security
    - Authentication
    - Zowe API ML services
    - Zowe API ML TLS requirements
    - Authentication for API ML services
      - Authentication endpoints
      - Authentication providers
        - z/OSMF Authentication Provider
        - Dummy Authentication Provider
    - Authorization
    - JWT Token
    - z/OSMF JSON Web Tokens Support
    - API ML truststore and keystore
    - API ML SAF Keyring
    - Discovery Service authentication
    - Setting ciphers for API ML services
  - ZAAS Client
    - Pre-requisites
    - API Documentation
      - Obtain a JWT token (login)
      - Validate and get details from the token (query)
      - Invalidate a JWT token (logout)
      - Obtain a PassTicket (passTicket)
    - Getting Started (Step by Step Instructions)
  - Certificate management in Zowe API Mediation Layer
    - Running on localhost
      - How to start API ML on localhost with full HTTPS

- Certificate management script
- Generate certificates for localhost
- Generate a certificate for a new service on localhost
- Add a service with an existing certificate to API ML on localhost
- Service registration to Discovery Service on localhost
- Zowe runtime on z/OS
  - Import the local CA certificate to your browser
  - Generate a keystore and truststore for a new service on z/OS
  - Add a service with an existing certificate to API ML on z/OS
  - Procedure if the service is not trusted

# How API ML transport security works

Security within the API Mediation Layer (API ML) is performed on several levels. This article describes how API ML uses Transport Layer Security (TLS). As a system administrator or API developer, use this guide to familiarize yourself with the following security concepts:

## Transport layer security

The TLS protocol should be used to ensure secure data-transport for all connections to API Mediation Layer services. While it is possible to disable the TLS protocol for debugging purposes or other use-cases, the enabled TLS protocol is the default mode.

## Authentication

Authentication is how an entity, whether it be a user (API Client), or an application (API Service), proves its true identity.

API ML uses the following authentication methods:

## User ID and password

- The user ID and password are used to retrieve authentication tokens
- Requests originate from a user
- The user ID and password are validated by a z/OS security manager whereby a token is issued that is then used to access the API service

## • TLS client certificates

· Certificates are used for service-only requests

## **Zowe API ML services**

The following range of service types apply to the Zowe<sup>™</sup> API ML:

- Zowe API ML services
  - Gateway Service (GW) The Gateway is the access point for API clients that require access to API services. API services can be accessed through the Gateway by API Clients. The Gateway receives information about an API Service from the Discovery Service.
  - Discovery Service (DS) The Discovery Service collects information about API services and provides this information to the Gateway and other services. API ML internal services also register to the Discovery Service.
  - **API Catalog (AC)** The Catalog displays information about API services through a web UI. The Catalog receives information about an API service from the Discovery Service.

## • Authentication and Authorization Service (AAS)

AAS provides authentication and authorization functionality to check user access to resources on z/OS. The API ML uses z/OSMF API for authentication. For more information, see the API ML wiki

## API Clients

API Clients are external applications, users, or other API services that access API services through the API Gateway

## API Services

API services are applications that are accessed through the API Gateway. API services register themselves to the Discovery Service and can access other services through the Gateway. If an API service is installed so that direct access is possible, API services can access other services without the Gateway. When APIs access other services, they can also function as API clients.

## **Zowe API ML TLS requirements**

The API ML TLS requires servers to provide HTTPS ports. Each API ML service has the following specific requirements:

## • API Client

- The API Client is not a server
- Requires trust of the API Gateway
- Has a truststore or SAF keyring that contains certificates required to trust the Gateway

## Gateway Service

- Provides an HTTPS port
- Has a keystore or SAF keyring with a server certificate
  - The certificate needs to be trusted by API Clients
  - This certificate should be trusted by web browsers because the API Gateway can be used to display web UIs
- Has a truststore or SAF keyring that contains certificates needed to trust API Services

## API Catalog

- Provides an HTTPS port
- Has a keystore or SAF keyring with a server certificate
  - The certificate needs to be trusted by the API Gateway
  - This certificate does not need to be trusted by anyone else

## • Discovery Service

- Provides an HTTPS port
- Has a keystore or SAF keyring with a server certificate
- Has a truststore or SAF keyring that contains certificates needed to trust API services

## • API Service

- Provides an HTTPS port
- Has a keystore or SAF keyring with a server and client certificate
  - The server certificate needs to be trusted by the Gateway
  - The client certificate needs to be trusted by the Discovery Service
  - The client and server certificates can be the same
  - These certificates do not need to be trusted by anyone else

 Has a truststore or SAF keyring that contains one or more certificates that are required to trust the Gateway and Discovery Service

## Authentication for API ML services

- API Gateway
  - The API Gateway handles authentication
  - There are two authentication endpoints that allow authentication of the resource by providers
  - Diagnostic endpoints https://{gatewayUrl}:{gatewayPort}/application/\*\* in API
     Gateway are protected by basic authentication or a Zowe JWT token

## API Catalog

- API Catalog is accessed by users and requires a login
- Protected access is performed by the Authentication and Authorization Service

## • Discovery Service

- Discovery Service is accessed by API Services
- This access (reading information and registration) requires protection by means of a client certificate
- (Optional) Access can be granted to users (administrators)
- Diagnostic endpoints https://{gatewayUrl}:{gatewayPort}/application/\*\* in
   Discovery Service are protected by basic authentication or Zowe JWT token

## • API Services

- Authentication is service-dependent
- It is recommended to use the Authentication and Authorization Service for authentication

## **Authentication endpoints**

The API Gateway contains the following REST API authentication endpoints:

auth/login

The full path of the auth/login endpoint appears as <a href="https://fatewayUrl">https://fatewayUrl</a> : <a href="https://fatewayPort/gateway/api/v1/auth/login">fatewayPort/gateway/api/v1/auth/login</a> (preferred option) or <a href="https://fatewayPort/gateway/api/v1/auth/login">https://fatewayUrl</a> :

The auth/login endpoint authenticates mainframe user credentials and returns an authentication token. The login request requires user credentials though one of the following methods:

- Basic access authentication
- JSON with user credentials
- Client certificate

When authentication is successful, the response to the request is an empty body and a token is contained in a secure HttpOnly cookie named apimlAuthenticationToken. When authentication fails, the user receives a 401 status code.

auth/query

The full path of the auth/query endpoint appear as <a href="https://gatewayUrl">https://gatewayUrl</a>: {gatewayPort}/gateway/api/v1/auth/query (preferred option) or <a href="https://gatewayUrl">https://gatewayUrl</a>: {gatewayPort}/api/v1/gateway/auth/query.

The auth/query endpoint validates the token and retrieves the information associated with the token. The query request requires the token through one of the following methods:

- A cookie named apimlAuthenticationToken
- Bearer authentication

When authentication is successful, the response to the request is a JSON object which contains information associated with the token. When authentication fails, the user receives a 401 status code.

auth/ticket

The auth/ticket endpoint generates a PassTicket for the user associated with a token. The full path of the auth/ticket endpoint appears as https://{gatewayUrl}: {gatewayPort}/gateway/api/v1/auth/ticket (preferred option) or https://{gatewayUrl}:{gatewayPort}/api/v1/gateway/auth/ticket.

This endpoint is protected by a client certificate. The ticket request requires the token in one of the following formats:

- Cookie named apimlAuthenticationToken.
- Bearer authentication

The request takes the applicationName parameter, which is the name of the application for which the PassTicket should be generated. Supply this parameter.

The response is a JSON object, which contains information associated with the ticket.

## auth/refresh

## Notes:

- The endpoint is disabled by default. [Jwt token refresh endpoint enablement](../../user-guide/apimediation/api-gateway-configuration. md#jwt-token-refresh-endpoint-enablement)
- The endpoint is protected by a client certificate.

The auth/refresh endpoint generates a new token for the user based on valid jwt token. The full path of the auth/refresh endpoint appears as https://{gatewayUrl}: {gatewayPort}/gateway/api/v1/auth/refresh (preferred option) or https://{gatewayUrl}:{gatewayUrl}:{gatewayVort}/api/v1/gateway/auth/refresh. The new token overwrites the old cookie with a Set-Cookie header. As part of the process, the old token gets invalidated and is not usable anymore.

The refresh request requires the token in one of the following formats:

- Cookie named apimlAuthenticationToken.
- Bearer authentication

For more information, see the OpenAPI documentation of the API Mediation Layer in the API Catalog.

## Supported authentication methods

The API Mediation Layer provides multiple methods which clients can use to authenticate. When the API ML is run as part of Zowe, all of the following methods are enabled and supported. All methods are supported at least to some extent with each authentication provider.

## Username/Password

The client can authenticate via Username and password. There are multiple methods which can be used to deliver

credentials. For more details, see the ZAAS Client documentation.

#### **Client certificate**

## Note:

Beginning with release 1.19 LTS, it is possible to perform authentication with client certificates. This feature is functional and tested, but automated testing on various security systems is not yet complete. As such, the feature is provided as a beta release for early preview. If you would like to offer feedback using client certificate authentication, please create an issue against the api-layer repository. Client Certificate authentication will move out of Beta once test automation is fully implemented across different security systems.

If the keyring or a truststore contains at least one valid certificate authority (CA) other than the CA of the API ML, it is possible to use the client certificates issued by this CA to authenticate to the API ML. This feature is not enabled by default and needs to be configured.

When providing credentials in any form together with client certificate on the same login request, the credentials take precedence and client certificate is ignored.

## Authentication is performed in the following ways:

- The client calls the API ML Gateway login endpoint with the client certificate.
- The client certificate and private key are checked as a valid TLS client certificate against the Gateway's trusted CAs.
- The public part of the provided client certificate is checked against SAF, and SAF subsequently returns a user ID that owns this certificate. ZSS provides this API for the Mediation Layer.
- The Gateway performs the login of the mapped user and returns a valid JWT token.

## **Prerequisites:**

 Alter the Zowe runtime user and set protection by password. The user is created with the NOPASSWORD parameter by the Zowe installer. It is necessary to change this password. For RACF, issue the following TSO command:

For other security systems, please refer to the documentation for an equivalent command.

- Ensure that the Zowe runtime user is allowed to log in to z/OSMF (For example user is member of the default IZUUSER group)
- Ensure that you have an external Certificate Authority and signed client certificates, or generate these certificates in SAF. The client certificate has to have correct Extended Key Usage metadata to allow being used for TLS client authentication. (OID: 1.3.6.1.5.5.7.3.2)
- Import the client certificates to SAF, or add them to a user profile. (Examples: RACDCERT ADD or RACDCERT GENCERT). For more information, see your security system documentation.
- Import the external CA to the truststore or keyring of the API Mediation Layer.
- Configure Gateway for client certificate authentication.
- To upgrade from Zowe 1.18 or lower, see the Additional security rights that need to be granted.
- PassTicket generation must be enabled for the Zowe runtime user. The user has to be able to generate PassTicket for itself and for the APPLID of z/OSMF. For more information, see Configure Passticket.
- The Zowe runtime user has to be enabled to perform identity mapping in SAF. For more information, see Additional security rights that need to be granted.
- ZSS has to be configured to participate in Zowe SSO. For more information, see Using web tokens for sso on Zlux and ZSS.
- •

## JWT Token

When the client authenticates with the API ML, the client receives the JWT token in exchange. This token can be used for further authentication. If z/OSMF is configured as the authentication provider and the client already received a JWT token produced by z/OSMF, it is possible to reuse this token within API ML for authentication.

## Authentication providers

API ML contains the following providers to handle authentication for the API Gateway:

- z/OSMF Authentication Provider
- SAF Authentication Provider

• Dummy Authentication Provider

#### z/OSMF Authentication Provider

The z/OSMF Authentication Provider allows the API Gateway to authenticate with the z/OSMF service. The user needs z/OSMF access in order to authenticate.

Use the following properties of the API Gateway to enable the z/OSMF Authentication Provider:

#### **SAF Authentication Provider**

The SAF Authentication Provider allows the API Gateway to authenticate directly with the z/OS SAF provider that is installed on the system. The user needs a SAF account to authenticate.

Use the following property of the API Gateway to enable the SAF Authentication Provider :

#### **Dummy Authentication Provider**

The Dummy Authentication Provider implements simple authentication for development purpose using dummy credentials (username: user, password user). The Dummy Authentication Provider makes it possible for the API Gateway to run without authenticating with the z/OSMF service.

Use the following property of API Gateway to enable the Dummy Authentication Provider :

## Authorization

Authorization is a method used to determine access rights of an entity.

In the API ML, authorization is performed by the z/OS security manager (ACF2, IBM RACF, Top Secret). An authentication token is used as proof of valid authentication. The authorization checks, however, are always performed by the z/OS security manager.

## **JWT Token**

The JWT secret that signs the JWT Token is an asymmetric private key that is generated during Zowe keystore configuration. The JWT token is signed with the RS256 signature algorithm.

You can find the JWT secret, alias jwtsecret, in the PKCS12 keystore that is stored in \${KEYSTORE\_DIRECTORY}/localhost/localhost.keystore.p12. The public key necessary to validate the JWT signature is read from the keystore. \${KEYSTORE\_DIRECTORY}/localhost/localhost.keystore.jwtsecret.pem file.

You can also use the /api/v1/gateway/auth/keys/public/all endpoint to obtain all public keys that can be used to verify JWT tokens signature in standard JWK format.

## z/OSMF JSON Web Tokens Support

Your z/OSMF instance can be enabled to support JWT tokens as described at Enabling JSON Web Token support. In this case, the Zowe API ML uses this JWT token and does not generate its own Zowe JWT token. All authentication APIs, such as /api/v1/gateway/login and /api/v1/gateway/check function in the same way as without z/OSMF JWT. The zowe-setup-certificates.sh stores the z/OSMF JWT public key to the localhost.keystore.jwtsecret.pem that can be used for JWT signature validation.

## API ML truststore and keystore

A *keystore* is a repository of security certificates consisting of either authorization certificates or public key certificates with corresponding private keys (PK), used in TLS encryption. A *keystore* can be stored in Java specific format (JKS) or use the standard format (PKCS12). The Zowe API ML uses PKCS12 to enable the keystores to be used by other technologies in Zowe (Node.js).

## **API ML SAF Keyring**

As an alternative to using a keystore and truststore, API ML can read certificates from a SAF keyring. The user running the API ML must have rights to access the keyring. From the java perspective, the keyring behaves as the JCERACFKS keystore. The path to the keyring is specified as safkeyring:///user\_id/key\_ring\_id. The content of SAF keyring is equivalent to the combined contents of the keystore and the truststore.

**Note:** When using JCERACFKS as the keystore type, ensure that you define the class to handle the RACF keyring using the -D options to specify the java.protocol.handler.pkgs property:

The elements in the following list, which apply to the API ML SAF Keyring, have these corresponding characteristics:

## The API ML local certificate authority (CA)

- The API ML local CA contains a local CA certificate and a private key that needs to be securely stored.
- The API ML local certificate authority is used to sign certificates of services.

• The API ML local CA certificate is trusted by API services and clients.

## The API ML keystore or API ML SAF Keyring

- Server certificate of the Gateway (with PK). This can be signed by the local CA or an external CA.
- Server certificate of the Discovery Service (with PK). This can be signed by the local CA.
- Server certificate of the Catalog (with PK). This can be signed by the local CA.
- Private asymmetric key for the JWT token, alias jwtsecret. The public key is exported to the localhost.keystore.jwtsecret.cer directory.
- The API ML keystore is used by API ML services.

## The API ML truststore or API ML SAF Keyring

- Local CA public certificate
- External CA public certificate (optional)
- Can contain self-signed certificates of API Services that are not signed by the local or external CA
- Used by API ML services

## Zowe core services

- Services can use the same keystore and truststore or the same keyring as APIML for simpler installation and management.
- When using a keystore and truststore, services have to have rights to access and read them on the filesystem.
- When using a keyring, the user of the service must have authorization to read the keyring from the security system.
- Alternatively, services can have individual stores for higher security.

## API service keystore or SAF keyring (for each service)

• The API service keystore contains a server and client certificate signed by the local CA.

## API service truststore or SAF keyring (for each service)

• (Optional) The API service truststore contains a local CA and external CA certificates.

## **Client certificates**

 A client certificate is a certificate that is used for validation of the HTTPS client. The client certificate of a Discovery Service client can be the same certificate as the server certificate of the services which the Discovery Service client uses.

## **Discovery Service authentication**

There are several authentication mechanisms, depending on the desired endpoint, as described by the following matrix:

Endpoint	Authentication method	Note
UI (eureka homepage)	basic auth(MF), token	see note about mainframe authentication
application/**	basic auth(MF), token	see note about mainframe authentication
application/health, application/info	none	
eureka/**	client certificate	Allows for the other services to register without mainframe credentials or token. API ML's certificate can be used. It is stored in the keystore/localhost/localhost.keystore.p12 keystore or in the SAF keyring. It is exported to .pem format for convenience. Any other certificate which is valid and trusted by Discovery service can be used.
discovery/**	certificate, basic auth(MF), token	see note about mainframe authentication

**Note:** Some endpoints are protected by mainframe authentication. The authentication function is provided by the API Gateway. This functionality is not available until the Gateway registers itself to the Discovery Service.

Since the Discovery Service uses HTTPS, your client also requires verification of the validity of its certificate. Verification is performed by validating the client certificate against certificates stored in the truststore or SAF keyring.

Some utilities including HTTPie require the certificate to be in PEM format. The exported certificate in .pem format is located here: keystore/localhost/localhost.pem.

The following example shows the HTTPie command to access the Discovery Service endpoint for listing registered services and provides the client certificate:

## Setting ciphers for API ML services

You can override ciphers that are used by the HTTPS servers in API ML services by configuring properties of the Gateway, Discovery Service, and API Catalog.

Note: You do not need to rebuild JAR files when you override the default values in shell scripts.

The *application.yml* file contains the default value for each service, and can be found here. The default configuration is packed in .jar files. On z/OS, you can override the default configuration in <a href="https://www.components/component

On localhost, you can override the default configuration in config/local/gateway-service.yml (including other YAML files for development purposes).

The following list shows the default ciphers. API ML services use the following cipher order:

**Note:** Ensure that the version of Java you use is compatible with the default cipherset.

Only IANA ciphers names are supported. For more information, see Cipher Suites or List of Ciphers.

# **ZAAS** Client

The ZAAS client is a plain Java library that provides authentication through a simple unified interface without the need for detailed knowledge of the REST API calls presented in this section. The Client function has only a few dependencies including Apache HTTP Client, Lombok, and their associated dependencies. The client contains methods to perform the following actions:

• To obtain a JWT token

- To validate and get details from a JWT token
- To invalidate the JWT token
- To obtain a PassTicket

## **Pre-requisites**

- Java SDK version 1.8.
- An active instance of the API ML Gateway Service.
- A property file which defines the keystore or truststore certificates.

## **API Documentation**

The plain java library provides the ZaasClient interface with following public methods:

This Java code enables your application to add the following functions:

- Obtain a JWT token (login)
- Validate and get details from the token (query)
- Invalidate a JWT token (logout)
- Obtain a PassTicket (passTicket)

## Obtain a JWT token (login)

To integrate login, call one of the following methods for login in the ZaasClient interface:

- If the user provides credentials in the request body, call the following method from your API:
- If the user provides credentials as Basic Auth, use the following method:

These methods return the JWT token as a String. This token can then be used to authenticate the user in subsequent APIs.

**Note:** Both methods automatically use the truststore file to add a security layer, which requires configuration in the **ConfigProperties** class.

## Validate and get details from the token (query)

Use the **query** method to get the details embedded in the token. These details include creation time of the token, expiration time of the token, and the user who the token is issued to.

Call the query method from your API in the following format:

In return, you receive the ZaasToken Object in JSON format.

This method automatically uses the truststore file to add a security layer, which you configured in the ConfigProperties class.

The query method is overloaded, so you can provide the HttpServletRequest object that contains the token in the apimlAuthenticationToken cookie or in an Authorization header. You then receive the ZaasToken Object in JSON format.

## Invalidate a JWT token (logout)

The logout method is used to invalidate the JWT token. The token must be provided in the Cookie header and must follow the format accepted by the API ML.

Call the logout method from your API in the following format:

If the token is successfully invalidated, you receive a 204 HTTP status code in return.

## Obtain a PassTicket (passTicket)

The passTicket method has an added layer of protection. To use this method, call the method of the interface, and provide a valid APPLID of the application and JWT token as input.

The APPLID is the name of the application (up to 8 characters) that is used by security products to differentiate certain security operations (like PassTickets) between applications.

This method has an added layer of security, whereby you do not have to provide an input to the method since you already initialized the ConfigProperties class. As such, this method automatically fetches the truststore and keystore files as an input.

In return, this method provides a valid pass ticket as a String to the authorized user.

**Tip:** For additional information about PassTickets in API ML see Enabling PassTicket creation for API Services that Accept PassTickets.

## **Getting Started (Step by Step Instructions)**

To use this library, use the procedure described in this section.

#### Follow these steps:

1. Add zaas-client as a dependency in your project.

You will need to specify the version of the zaas-client you want. zaas-client versioning following the semantic versioning format of major.minor.patch. For example, 1.22.0.

Gradle:

- i. Create a gradle.properties file in the root of your project if one does not already exist.
- ii. In the gradle.properties file, set the URL of the specific Artifactory containing the *SpringEnabler* artifact.
- iii. Add the following *Gradle* code block to the repositories section of your build.gradle file:
- iv. Add the following Gradle dependency:

Maven:

i. Add the following *XML* tags within the newly created pom.xml file:

**Tip:** If you want to use snapshot version, replace libs-release with libs-snapshot in the repository url and change snapshots->enabled to true.

- ii. Then add the following *Maven* dependency:
- 2. In your application, create your Java class which will be used to create an instance of ZaasClient, which enables you to use its method to login, query, and to issue a PassTicket.
- 3. To use zaas-client , provide a property file for configuration.

**Tip:** Check org.zowe.apiml.zaasclient.config.ConfigProperites to see which properties are required in the property file.

## **Configuration Properties:**

**Note:** If httpOnly property is set to true, the ZAAS Client will access the API ML via HTTP protocol without TLS. This meant for z/OS configuration with AT-TLS that will ensure that TLS and the required client certificates are used.

4. Create an instance of ZaasClient in your class and provide the configProperties object.

#### Example:

You can now use any method from ZaasClient in your class.

#### Example:

For login, use the following code snippet:

The following codeblock is an example of a SampleZaasClientImplementation.

## Example:

## **Certificate management in Zowe API Mediation Layer**

## **Running on localhost**

## How to start API ML on localhost with full HTTPS

The https://github.com/zowe/api-layer repository already contains pre-generated certificates that can be used to start API ML with HTTPS on your computer. The certificates are not trusted by your browser so you can either ignore the security warning or generate your own certificates and add them to the truststore of your browser or system.

The certificates are described in more detail in the TLS Certificates for localhost.

Note: When running on localhost, only the combination of using a keystore and truststore is supported.

#### Certificate management script

Zowe API Mediation Layer provides a script that can be used on Windows, Mac, Linux, and z/OS to generate a certificate and keystore for the local CA, API Mediation Layer, and services.

This script is stored in <a href="mailto:zowe-install-packaging">zowe-install-packaging</a> repository <a href="mailto:bin/apiml\_cm.sh">bin/apiml\_cm.sh</a>. It is a UNIX shell script that can be executed by Bash or z/OS Shell. For Windows, install Bash by going to the following link: <a href="mailto:cmder.cmder">cmder</a>.

#### **Generate certificates for localhost**

#### Follow these steps:

- 1. Clone the zowe-install-packaging repository to your local machine.
- 2. Place the bin/apiml\_cm.sh scripts directory in your API Mediation Layer repository folder
- 3. Use the following script in the root of the api-layer repository to generate certificates for localhost:

#### scripts/apiml\_cm.sh --action setup

This script creates the certificates and keystore for the API Mediation Layer in your current workspace.

#### Generate a certificate for a new service on localhost

To generate a certificate for a new service on localhost, see Generating certificate for a new service on localhost.

## Add a service with an existing certificate to API ML on localhost

For more information about adding a service with an existing certificate to API ML on localhost, see Trust certificates of other services.

## Service registration to Discovery Service on localhost

To register a new service to the Discovery Service using HTTPS, provide a valid client certificate that is trusted by the Discovery Service.

## Zowe runtime on z/OS

Certificates for the API ML local CA and API ML service are managed by installing the Zowe runtime on z/OS. Follow the instructions in Installing the Zowe runtime on z/OS.

There are two ways to set up certificates on a z/OS machine:

- Certificates in SAF keyring
- Certificates in UNIX files (keystore and truststore)

The Configuring Zowe certificates contains instructions about how to set up certificates during installation. Follow the procedure in the applicable section described in this article during installation.

#### Import the local CA certificate to your browser

Trust in the API ML server is a necessary precondition for secure communication between Browser or API Client application. Ensure this trust through the installation of a Certificate Authority (CA) public certificate. By default, API ML creates a local CA. Import the CA public certificate to the truststore for REST API clients and to your browser. You can also import the certificate to your root certificate store.

## Notes:

- If a SAF keyring is being used and set up with ZWEKRING JCL, the procedure to obtain the certificate does not apply. It is recommended that you work with your security system administrator to obtain the certificate. Start the procedure at step 2.
- The public certificate in the PEM format is stored at

   <KEYSTORE\_DIRECTORY>/local\_ca/localca.cer
   where <KEYSTORE\_DIRECTORY> is defined
   in a customized <RUNTIME\_DIR>/bin/zowe-setup-certificates.env
   file during the installation
   step that generates Zowe certificates. The certificate is stored in UTF-8 encoding so you need to
   transfer it as a binary file. Since this is the certificate to be trusted by your browser, it is recommended
   to use a secure connection for transfer.

## Follow these steps:

- 1. Download the local CA certificate to your computer. Use one of the following methods to download the local CA certificate to your computer:
  - Use Zowe CLI (Recommended) Issue the following command:

```
zowe zos-files download uss-file --binary
$KEYSTORE_DIRECTORY/local_ca/localca.cer
```

• **Use sftp** Issue the following command:

To verify that the file has been transferred correctly, open the file. The following heading and closing should appear:

- 2. Import the certificate to your root certificate store and trust it.
  - For Windows, run the following command:

certutil -enterprise -f -v -AddStore "Root" localca.cer

**Note:** Ensure that you open the terminal as **administrator**. This will install the certificate to the Trusted Root Certification Authorities.

• **For macOS**, run the following command:

\$ sudo security add-trusted-cert -d -r trustRoot -k
/Library/Keychains/System.keychain localca.cer

• For Firefox, manually import your root certificate via the Firefox settings, or force Firefox to use the Windows truststore.

**Note:** Firefox uses its own certificate truststore.

Create a new Javascript file firefox-windows-truststore.js at C:\Program Files (x86)\Mozilla Firefox\defaults\pref with the following content:

## Generate a keystore and truststore for a new service on z/OS

**Note:** This procedure applies to UNIX file keystore and truststore only. For the SAF keyring option, it is recommended that you perform the actions manually using your security system commands.

You can generate a keystore and truststore for a new service by calling the apiml\_cm.sh script in the directory with API Mediation Layer:

Call the apiml\_cm.sh script in the directory with the API Mediation Layer as in the following example.

## Example:

where:

• service-alias

is a unique string to identify the key entry. All keystore entries (key and trusted certificate entries) are accessed via unique aliases. Since the keystore has only one certificate, you can omit this parameter and use the default value localhost.

## service-keystore

Specifies repository of security certificates plus corresponding private keys. The <keystore\_path> is the path excluding the extension to the keystore that is generated. It can be an absolute path or a path relative to the current working directory. The key store is generated in PKCS12 format with the

.p12 extension. Ensure that the path is in an existing directory where your service expects the keystore.

## Example: /opt/myservice/keystore/service.keystore.

## service-truststore

Contains certificates from other parties that you expect to communicate with, or from Certificate Authorities that you trust to identify other parties. The <truststore\_path> is the path excluding the extension to the trust store that is generated. It can be an absolute path or a path relative to the current working directory. The truststore is generated in PKCS12 format.

#### service-ext

Specifies the X.509 extension that should be the Subject Alternate Name (SAN). The SAN contains host names that are used to access the service. You need to specify the same hostname that is used by the service during API Mediation Layer registration.

Example: "SAN=dns:localhost.localdomain,dns:localhost,ip:127.0.0.1"

**Note:** For more information about SAN, see *SAN or SubjectAlternativeName* at Java Keytool - Common Options.

#### service-dname

Specifies the X.509 Distinguished Name and is used to identify entities, such as those which are named by the subject and issuer (signer) fields of X.509 certificates.

```
Example: "CN=Zowe Service, OU=API Mediation Layer, O=Zowe Sample, L=Prague, S=Prague, C=CZ"
```

#### service-validity

Specifies the number of days until the certificate expires.

#### service-password

Specifies the keystore password. The purpose of the password is the integrity check. The access protection for the keystore and keystore need to be achieved by making them accessible only by the ZOVESVR user ID and the system administrator.

The local-ca-filename is the path to the keystore that is used to sign your new certificate with the local CA private key. It should point to the \$KEYSTORE\_DIRECTORY/local\_ca/localca where \$KEYSTORE\_DIRECTORY is defined in a customized \$ZOWE\_ROOT\_DIR/bin/zowe-setup-certificates.env file during the installation step that generates Zowe certificates.

## Add a service with an existing certificate to API ML on z/OS

**Note:** This procedure applies only to UNIX file keystore/truststore. For the SAF keyring option, we recommend to perform the actions manually using your security system commands.

The API Mediation Layer requires validation of the certificate of each service that it accessed by the API Mediation Layer. The API Mediation Layer requires validation of the full certificate chain. Use one of the following methods:

- Import the public certificate of the root CA that has signed the certificate of the service to the APIML truststore.
- Ensure that your service has its own certificate. If it was signed by intermediate CA, ensure that all intermediate CA certificates are contained in the service's keystore.

**Note:** If the service does not provide an intermediate CA certificates to the API ML, then validation fails. This can be circumvented by importing the intermediate CA certificates to the API ML truststore.

The following path is an example of importing a public certificate to the API ML truststore by calling in the directory with API Mediation Layer.

## Example:

## Procedure if the service is not trusted

If your service is not trusted, you may receive a response with the HTTP status code 502 Bad Gateway and a JSON response in the standardized format for error messages. The following request is an example of when this error response may occur.

## Example:

http --verify=\$KEYSTORE\_DIRECTORY/local\_ca/localca.cer GET https://<gatewayHost>:
<port></port>/api/v1/<untrustedService>/greeting

In this example, you receive a similar response:

The message has the key apiml.common.tlsError, and the message number AML0105, and content that explains details about the message.

If you receive this message, import the certificate of your service or the CA that signed it to the truststore of the API Mediation Layer as described previously.

# **API Mediation Layer routing**

As an application developer, you can route your service through the Gateway using the API Mediation Layer to consume a specific resource.

There are two ways to route your service to the API Mediation Layer:

- Basic Routing (using Service ID and version)
- Basic Routing (using only the service ID)

# Terminology

• Service

A service provides one or more APIs, and is identified by a service ID. Note that sometimes the term "service name" is used to mean service ID.

The default service ID is provided by the service developer in the service configuration file.

A system administrator can replace the service ID with a deployment environment specific name using additional configuration that is external to the service deployment unit. Most often, this is configured in a JAR or WAR file.

Services are deployed using one or more service instances, which share the same service ID and implementation.

## • URI (Uniform Resource Identifier)

A string of characters used to identify a resource. Each URI must point to a single corresponding resource that does not require any additional information, such as HTTP headers.

# **APIML Basic Routing (using Service ID and version)**

This method of basic routing is based on the service ID that identifies the service. The specific instance is selected by the API Gateway. All instances require an identical response. Eureka and Zuul expect this type of routing.

The URI identifies the resource, but does not identify the instance of the service as unique when multiple instances of the same service are provided. For example, when a service is running in high-availability (HA) mode.

Services of the same product that provide different resources, such as CA SYSVIEW on one system and CA SYSVIEW in a different sysplex, cannot have the same service ID (the same URI cannot have two different meanings).

In addition to the basic Zuul routing, the Zowe API Gateway supports versioning in which you can specify a major version. The Gateway routes a request only to an instance that provides the specified major version of the API.

The /api/ prefix is used for REST APIs. The prefix /ui/ applies to web UIs and the prefix /ws/ applies to WebSockets.

You can implement additional routing using a Zuul pre-filter. For more information about how to implement a Zuul filter, see Router and Filter: Zuul

The URL format expected by the API Gateway is:

https://{gatewayHost}:{port}/api/v{majorVersion}/{serviceId}/{resource}

#### Example:

The following address shows the original URL of a resource exposed by a service:

The following address shows the API Gateway URL of the resource:

The following diagram illustrates how basic routing works:

## **Implementation Details**

Service instances provide information about routing to the API Gateway via Eureka metadata.

## Example:

In this example, the service has a service ID of helloworldservice that exposes the following endpoints:

- UI https://gateway/ui/v1/helloworldservice routed to https://hwServiceHost:port/helloworld/
- API major version 1 https://gateway/api/v1/helloworldservice routed to https://hwServiceHost:port/helloworld/v1
- API major version 2 https://gateway/api/v2/helloworldservice routed to https://hwServiceHost:port/helloworld/v2

where:

- The gatewayUrl is matched against the prefix of the URL path used at the Gateway https://gateway/urlPath, where urlPath is prefix/serviceId/resourcePath.
- The service ID is used to find the service host and port.
- The serviceUrl is used to prefix the resourcePath at the service host.

**Note:** The service ID is not included in the routing metadata, but the service ID is in the basic Eureka metadata.

# Basic Routing (using only the service ID)

This method of routing is similar to the previous method, but does not use the version part of the URL. This approach is useful for services that handle versioning themselves with different granularity.

One example that only uses a service ID is z/OSMF.

## Example:

z/OSMF URL through the Gateway: <a href="https://gateway:10010/api/zosmf/restjobs/jobs/...">https://gateway:10010/api/zosmf/restjobs/jobs/...</a>

where:

- zosmf is the service ID.
- /restjobs/1.0/... is the rest of the endpoint segment.

Note that no version is specified in this URL.

# Enabling PassTicket creation for API Services that Accept PassTickets

As system programmer, you can configure Zowe to use PassTickets for API services that are compatible to accept them to authenticate your service with the API Mediation Layer.

# Overview

API clients can use a Zowe JWT token to access an API service even if the API service itself does not support the JWT token. The Zowe JWT token is available through the API Gateway authentication endpoint.

When an API client provides a valid Zowe JWT token to the API ML, the API Gateway then generates a valid PassTicket for any API service that supports PassTickets. The API Gateway then uses the PassTicket to access that API service. The API Gateway provides the user ID and password in the Authorization header of the HTTP requests using the Basic authentication scheme.

- Outline for enabling PassTicket support
- Security configuration that allows the Zowe API Gateway to generate PassTickets for an API service
  - ACF2
  - Top Secret
  - RACF
- API services that support PassTickets
  - API Services that register dynamically with API ML that provide authentication information
  - API Services that register dynamically with API ML but do not provide metadata
  - API services that are defined using a static YAML definition
- Adding YAML configuration to API services that register dynamically with API ML

# **Outline for enabling PassTicket support**

The following steps outline the procedure for enabling PassTicket Support:

- 1. Follow the API service documentation that explains how to activate support for PassTickets.
  - The PassTickets for the API service must have the replay protection switched off. The PassTickets are exchanged between Zowe API Gateway and the API Service in a secure mainframe

environment.

- 2. Record the value of the APPLID of the API service.
- 3. Enable the Zowe started task user ID to generate PassTickets for the API service.
- 4. Enable PassTicket support in the API Gateway for your API service.

**Note:** PassTickets must be enabled for every user who requires access to the API service.

# Security configuration that allows the Zowe API Gateway to generate PassTickets for an API service

Consult with your security administrator to issue security commands to allow the Zowe started task user ID to generate PassTickets for the API service.

Use the following variables to generate PassTickets for the API service to enable the Zowe started task user ID:

- <applid> is the APPLID value used by the API service for PassTicket support (e.g. OMVSAPPL)
- <zowesrv> is Zowe started task user ID used during the Zowe installation

Replace the variables in the following examples with actual values.

## ACF2

Grant the Zowe started task user ID permission to generate PassTickets for users of that API service. The following code is an example of security commands that need to be issued.

## Example:

## **Top Secret**

Grant the Zowe started task user ID permission to generate PassTickets for users of that API service.

## Example:

## RACF

To enable PassTicket creation for API service users, define the profile IRRPTAUTH.<applid>.\* in the PTKTDATA class and set the universal access authority to NONE.

Grant the Zowe started task user ID permission to generate PassTickets for users of that API service.

#### Example:

# **API services that support PassTickets**

The following types of API services support PassTickets:

- API Services that register dynamically with API ML that provide authentication information
- API Services that register dynamically with API ML but do not provide metadata
- API services that are defined using a static YAML definition

# API Services that register dynamically with API ML that provide authentication information

API services that support Zowe API Mediation Layer and use dynamic registration to the Discovery Service already provide metadata that enables PassTicket support.

As a system programmer, you are not required to do anything in this case. All required information is provided by the API service automatically.

#### API Services that register dynamically with API ML but do not provide metadata

Some services can use PassTickets but the API ML does not recognize that the service can accept PassTickets. For such services, you can provide additional service metadata externally in the same file that contains the static YAML definiton. The static YAML definitions are described in REST APIs without code changes required.

Add the following section to the YAML file with a static definition:

where:

• <serviceId>

is the service ID of the service to which you want to add metadata.

#### API services that are defined using a static YAML definition

Add the following metadata to the same level as the serviceId:

#### Example:

**Note:** The fields in this example are explained later in this article.

# Adding YAML configuration to API services that register dynamically with API ML

As a developer of an API service that registers dynamically with the API ML, you need to provide additional metadata to tell the API Gateway to use PassTickets. Additional metadata tells the API Gateway how to generate them. The following code shows an example of the YAML configuration that contains this metadata.

#### Example:

where:

httpBasicPassTicket

is the value that indicates that the HTTP Basic authentication scheme is used with PassTickets.

• <applid>

is the APPLID value that is used by the API service for PassTicket support (e.g. OMVSAPPL).

# **Custom Metadata**

(Optional) Additional metadata can be added to the instance information that is registered in the Discovery Service in the customMetadata section. This information is propagated from the Discovery Service to the onboarded services (clients). In general, additional metadata do not change the behavior of the client. Some specific metadata can configure the functionality of the API Mediation Layer. Such metadata are generally prefixed with the apiml. qualifier. We recommend you define your own qualifier, and group all metadata you wish to publish under this qualifier. If you use the Spring enabler, ensure that you include the prefix apiml.service before the parameter name.

#### customMetadata.apiml.enableUrlEncodedCharacters

When this parameter is set to true, the Gateway allows encoded characters to be part of URL requests redirected through the Gateway. The default setting of false is the recommended setting. Change this setting to true only if you expect certain encoded characters in your application's requests.

**Important!** When the expected encoded character is an encoded slash or backslash (%2F, %5C), make sure the Gateway is also configured to allow encoded slashes. For more information, see Installing the Zowe runtime on z/OS.

Note: If you use the Spring enabler, use the following parameter name:

#### apiml.service.customMetadata.apiml.enableUrlEncodedCharacters

#### customMetadata.apiml.connectTimeout

The value in milliseconds that specifies a period in which API ML should establish a single, nonmanaged connection with this service. If omitted, the default value specified in the API ML Gateway service configuration is used.

**Note:** If you use the Spring enabler, use the following parameter name:

apiml.service.customMetadata.apiml.connectTimeout

customMetadata.apiml.readTimeout

The value in milliseconds that specifies the time of inactivity between two packets in response from this service to API ML. If omitted, the default value specified in the API MLGateway service configuration is used.

**Note:** If you use the Spring enabler, use the following parameter name:

apiml.service.customMetadata.apiml.readTimeout

#### customMetadata.apiml.connectionManagerTimeout

HttpClient employs a special entity to manage access to HTTP connections called by the HTTP connection manager. The purpose of an HTTP connection manager is to serve as a factory for new HTTP connections, to manage the life cycle of persistent connections, and to synchronize access to persistent connections. Internally, it works with managed connections which serve as proxies for real connections. **connectionManagerTimeout** specifies a period in which managed connections with API ML should be established. The value is in milliseconds. If omitted, the default value specified in the API ML Gateway service configuration is used.

**Note:** If you use the Spring enabler, use the following parameter name:

apiml.service.customMetadata.apiml.connectionManagerTimeout

#### customMetadata.apiml.okToRetryOnAllOperations

Specifies whether all operations can be retried for this service. The default value is false. The false value allows retries for only GET requests if a response code of 503 is returned. Setting this value to true enables retry requests for all methods, which return a 503 response code. Enabling retry can impact server resources resulting from buffering of the request body.

**Note:** If you use the Spring enabler, use the following parameter name:

#### apiml.service.customMetadata.apiml.okToRetryOnAllOperations

#### customMetadata.apiml.corsEnabled

When this parameter is set to true, CORS handling by the Gateway is enabled on the service level for all service routes. For more information, see Cross-Origin Resource Sharing (CORS).

**Note:** If you use the Spring enabler, use the following parameter name:

#### customMetadata.apiml.corsAllowedOrigins

Optionally, service can specify which origins will be accepted by Gateway during the CORS handling. When this parameter is not set, the accepted origins are  $\ast$  by default. You can provide a coma separated list of values to explicitly limit the accepted origins.

**Note:** If you use the Spring enabler, use the following parameter name:

apiml.service.customMetadata.apiml.corsAllowedOrigins

#### customMetadata.apiml.lb.type

This parameter is part of the load balancing configuration for the Deterministic Routing capability. Through this parameter, the service can specify which load balancing schema the service requires. If this parameter is not specified, the service is routed using the basic round robin schema. This parameter can be set to the following values:

#### • headerRequest

This value applies the Header Request load balancing schema. Clients can call the API Gateway and provide a special header with the value of the requested instanceld. The Gateway understands this as a request from the client for routing to a specific instance. Clients have several possibilities for understanding the topology of service instances, such as via the /eureka/apps endpoint on the Discovery service, or the /gateway/services endpoint on the Gateway. In either case, the information is provided. The client can then request a specific instance by using the special header described below.

The header name is X-InstanceId, and the sample value is discoverableclient:discoverableclient:10012. This is identical to instanceId property in the registration of the Discovery service.

In combination with enabling Routed instance header, the client can achieve sticky session functionality. (The term, 'sticky session' refers to the feature of many load balancing solutions to route the requests for a particular session to the same physical machine that serviced the first request for that session). The benefit of this approach is that there is no session on the Gateway, and the client ultimately decides whether or not to go to a specific instance. This method uses the following sequence:

- a. The client calls API Gateway and gets routed to a service.
- b. The client reads the X-InstanceId header value from the response to understand the service was routed to.
- c. For all subsequent requests, the client provides the X-InstanceId header with previously read value to get routed to the same instance of the service.

#### • authentication

This value applies the Authentication load balancing schema. This is a sticky session functionality based on the ID of the user. The user ID is understood from the Zowe SSO token on the client's request. Requests without the token are routed in a round robin fashion. The user is first routed in a round robin fashion, and then the routed instance Id is cached. The instance information is used for subsequent requests to route the client to the cached target service instance. This session's default expiration time is 8 hours. After the session expires, the process initiates again.

In default configuration, this cache is stored on each Gateway instance. You can choose to distribute this cache between the Gateway's instances. To do so, follow the steps described in Distributed load balancer cache.

#### customMetadata.apiml.lb.cacheRecordExpirationTimeInHours

When the property customMetadata.apiml.lb.type is set to authentication, the user can also define the expiration time for the selected instance information that is cached. This property aims to prevent any discrepancy which might occur if the required target server is no longer available. The default value is 8 hours.

#### customMetadata.apiml.response.compress

When this parameter is set to true, API ML compresses content for all responses from this services using GZIP. API ML also adds the Content-Encoding header with value gzip to responses.

#### customMetadata.apiml.response.compressRoutes

When the customMetadata.apiml.response.compress parameter is set to true, this parameter allows services to further limit the compressed routes. The parameter accepts ant style routes deliminated by , . The expectation is to provide the absolute paths.

If relative paths are provided, the starting / is added. If the beginning of the pattern does not need to be specifically defined, use **\*\***/{pathYouAreInterestedIn}

#### **Examples:**

o /service/\*\*

Compresses all paths starting with /service/

o /service/api/v1/compress,/service/api/v1/custom-compress

Compresses the specific two routes

/\\*\\*/compress/\\*\\*

Compresses all paths that contain compress as a specific path

#### customMetadata.apiml.response.headers

(Optional) A service can specify headers that are added to the response by the Gateway. When this parameter is not set or is empty, no headers are added. Header names and header values are separated by :. Multiple headers can be added, delimited by ,. If a header with the same name already exists in the response, the Gateway overwrites the value of the header.

#### **Examples:**

Strict-Transport-Security:max-age=1234; includeSubDomains

Sets a header with name Strict-Transport-Security and value max-age=1234; includeSubDomains.

#### Strict-Transport-Security:max-age=1234; includeSubDomains, X-Frame-Options:SAMEORIGIN

Sets two headers:

1) Header with name Strict-Transport-Security and value max-age=1234; includeSubDomains . 2) Header with name X-Frame-Options and value `SAMEORIGIN.

#### customMetadata.apiml.headersTolgnore

(Optional) A service can specify headers that are removed from the request to the southbound service by the Gateway. When this parameter is not set or is empty, no headers are removed. Multiple headers can be removed, delimited by ,. Version: v1.25.x LTS

# **Using the Caching Service**

As an API developer, you can use the Caching Service as a storage solution to enable resource sharing between service instances, thereby ensuring High Availability of services. The Caching Service makes it possible to store, retrieve, and delete data associated with keys. The Caching Service is designed to make resource sharing possible for services that cannot be made stateless in two ways:

- Using VSAM to store key/value pairs for production
- Using InMemory

**Note:** In the current implementation of the Caching service, VSAM is required for the storage of key/value pairs for production, as VSAM is a native z/OS solution for storing key/value pairs.

The Caching service is available only for internal Zowe applications, and is not exposed to the internet. The Caching service supports a hot-reload scenario in which a client service requests all available service data.

- Architecture
- Storage methods
  - VSAM
  - Redis
  - InMemory
- How to start the service
- Methods to use the Caching service API
- Configuration properties
- Authentication

# Architecture

A precondition to provide for High Availability of all components within Zowe is the requirement for these components to be either stateless, or for the resources of the service to be offloaded to a location accessible by all instances of the service. This condition also applies to recently started instances. Some services, however, are not, and cannot be stateless. The Caching Service is designed for these types of services.

REST APIs make it possible to create, delete, and update key-value pairs in the cache. Other APIs read a specific key-value pair or all key-value pairs in the cache.

Information from cached APIs is stored as a JSON in the following format:

# Storage methods

The Caching Service supports the following storage solutions, which provide the option to add custom implementation.

#### VSAM

VSAM can be used to organize records into four types of data sets: key-sequenced, entry-sequenced, linear, or relative record. Use VSAM as the storage solution for production. VSAM is used primarily for applications and is not used for source programs, JCL, or executable modules. ISPF cannot be used to display or edit VSAM files.

For more information about the VSAM storage access method, see Using VSAM as a storage solution through the Caching service.

#### Redis

Redis is a common storage solution that runs outside of the z/OS platform. It can store data structures in key-value pairs, has high-availability support, and is highly performant.

For more information about the Redis storage access method, see Using Redis as a storage solution through the Caching service.

#### InMemory

TODO (add in memory procedure) The InMemory storage method is a method suitable for testing and integration verification. Be sure not to use InMemory storage in production. The key/value pairs are stored only in the memory of a single instance of the service. As such, the key/value pairs do not persist.

## How to start the service

By default, the Caching service starts along with the other Zowe components. To prevent the Caching service from starting, set the following parameter to false:

```
zowe_apiml_caching_service_start
```

This parameter is defined in the ansible playbooks.

When this parameter is set to false, the parameter appends to the instance.env configuration file, which is used at Zowe start time.

### Methods to use the Caching service API

To apply a method to the Caching service, use the following API path:

/cachingservice/api/v1/cache/\${path-params-as-needed}

Use the following methods with the Caching Service API:

• POST /cache

Creates a new key in the Cache

• GET /cache

Returns all key/value pairs for specific service

PUT /cache/{key}

Updates the existing value for the given key

• GET /cache/{key}

Returns the existing value for the given key

• DELETE /cache/{key}

Deletes a key/value pair

### **Configuration properties**

The Caching Service uses the standard application.yml structure for configuration. The service is built on top of the Spring enabler. As such, it dynamically registers to the API Mediation Layer. The service appears in the API Catalog under the tile, "Zowe Applications".

#### caching.storage.size

This property limits the size of the Caching Service. In the VSAM and InMemory implementations, this property represents the number of records stored before the eviction strategy is initiated. The default value is 100.

Note: Different implementations may implement this property differently.

#### caching.storage.evictionStrategy

This parameter specifies service behavior when the limit of records is reached. The default value is Reject.

where:

#### • reject

rejects the new item with the HTTP status code 507 when the service reaches the configured maximum number

#### • removeOldest

removes the oldest item in the cache when the service reaches the configured maximum number

#### Notes:

- For more information about how to configure the Caching Service in the application.yml, see: Add API Onboarding Configuration.
- When using VSAM, ensure that you set the additional configuration parameters. For more information about setting these parameters, see Using VSAM as a storage solution through the Caching service.

# Authentication

#### **Direct calls**

Caching service requires TLS mutual authentication. This verifies authenticity of client. Calls without valid client certificate generate 403 response code: Forbidden. This requirement is disabled when

Call must have a header X-Certificate-DistinguishedName containing information about certificate's distinguished name. This header is added by API Gateway. It needs to be added manually for direct call. Calls without this header produce 401 response code: Unauthorized.

#### **Routed calls through API Gateway**

Caching service registers with the following authentication scheme to Discovery service:

which makes Gateway to attempt mutual authentication with Client and if succesfull, propagate the Client's certificate information to X-Certificate- headers. With this scheme, Gateway will use it's server/client certificate for the routed call to caching service.

Version: v1.25.x LTS

# Using VSAM as a storage solution through the Caching service

As an API developer, you can configure VSAM as a storage solution through the Caching service. The procedure in this article describes how to configure your storage solution for VSAM. Configuring VSAM ensures that you do not lose data if you need to restart. Configuring VSAM also makes it possible to leverage multiple caching services concurrently, whereby clients can retreive data through VSAM.

- Understanding VSAM
- VSAM configuration

# **Understanding VSAM**

Virtual Storage Access Method (VSAM) is both a data set type, and a method for accessing various user data types. Using VSAM as an access method makes it possible to maintain disk records in a unique format that is not understandable by other access methods. VSAM is used primarily for applications, and is not used for source programs, JCL, or executable modules. ISPF cannot be used to display or edit VSAM files. VSAM can be used to organize records into four types of data sets: key-sequenced, entry-sequenced, linear, or relative record. The API Caching service supports VSAM as a storage method to cache APIs, and uses the Key Sequence Data Set (KSDS) dataset. Each record has one or more key fields, and a record can be retrieved (or inserted) by the key value, thereby providing random access to data. Records are of variable length. IMS<sup>™</sup> uses KDSDs.

For more information about VSAM, see the IBM documentation.

#### **VSAM** configuration

Configure VSAM as a storage solution through the Caching service by modifying the following configuration parameters in the service application.yml.

#### caching.storage.vsam.name

The ZFile filename. The ZFile is a wrapper around a z/OS file based on the supplied name and options. This method calls the fopen() and fldata() C-library routines. The ZFile filename should follow the specific naming convention // 'DATASET.NAME'.

#### caching.storage.vsam.keyLength

The VsamKey length. The default value is 32 bytes.

#### • caching.storage.vsam.recordLength

The record length. The default value is 512 bytes.

#### • caching.storage.vsam.encoding

The character encoding. The default value is IBM-1047.

Version: v1.25.x LTS

# Using Redis as a storage solution through the Caching service

As an API developer, you can configure Redis as a storage solution through the Caching service. This article describes how to configure your storage solution for Redis. You can configure Redis for high availability as well as to replicate data to provide data durability and availability.

- Understanding Redis
- Redis configuration

## **Understanding Redis**

Redis is an off-Z storage solution that stores data structures in key-value pairs. The API Caching service uses hash sets, where each service storing data via the Caching service has its own hash, and each data entry is a key-value entry within that service's Redis hash set.

For more information on Redis, see the official Redis documentation.

#### **Redis replica instances**

Redis can be used with one standalone instance. For data durability, however, a master/replica configuration is recommended. Redis replicas automatically connect, and re-connect when necessary, to the master Redis instance and attempt to be an exact copy of the master.

For more information on Redis replication and how to configure a replica instance, see the official Redis Replication documentation.

#### **Redis Sentinel**

Redis Sentinel is a configuration that provides high availability for Redis master/replica instances. Sentinel instances are used to monitor the master instance and use a quorum to automatically determine if a failover procedure needs to occur from a master instance to one of its replicas.

For more information on Redis Sentinel and how to configure Sentinel instances with master/replica instances, see the official Redis Sentinel documentation.

#### **Redis SSL/TLS**

Redis supports SSL/TLS starting in version 6. For information on enabled SSL/TLS with Redis, see the official Redis TLS Support documentation.

#### **Redis and Lettuce**

The Lettuce library is used to connect to Redis. Lettuce uses Master or Sentinel node registration information to automatically discover other instances. The IP address used to register between nodes is therefore what Lettuce uses to connect to downstream replica instances. This means the IP address of replica instances, or the IP address of both master and replica instances in the case of Sentinel topology, must be accessible to the Caching service. For example, in a master/replica topology running in separate Docker containers, the replica container's IP address needs to be accessible to the Caching service, rather than only exposing a port.

# **Redis configuration**

Configure Redis as a storage solution through the Caching service by setting the following environment variables. Environment variables can be set by adding them to instance.env.

#### CACHING\_STORAGE\_REDIS\_MASTERNODEURI

The URI used to connect to the Redis master instance in the form username: password@host:port.

- The host section of the URI is mandatory
- The port section is optional and if not included defaults to 6379.
- The username section is optional and if not included defaults to the Redis default username default.
- The password section is optional, but must be included if a username is included. If the password is not set a username cannot be set.

#### • CACHING\_STORAGE\_REDIS\_TIMEOUT

The timeout duration in seconds for the Caching service when first connecting to Redis. Defaults to 60 seconds.

• CACHING\_STORAGE\_REDIS\_SENTINEL\_MASTERINSTANCE

The Redis master instance ID used by the Redis Sentinel instances. Required if Redis Sentinel is being used.

#### CACHING\_STORAGE\_REDIS\_SENTINEL\_NODES

The URI used to connect to a Redis Sentinel instance in the form username:password@host:port.

- The host section of the URI is mandatory
- The port section is optional and if not included defaults to 6379.
- The password section is optional and defaults to no password.

To supply multiple Redis Sentinel URIs, concatenate the URIs with a comma ,.

#### • CACHING\_STORAGE\_REDIS\_SSL\_ENABLED

A flag indicating if Redis is being used with SSL/TLS support. Defaults to true.

#### • CACHING\_STORAGE\_REDIS\_SSL\_KEYSTORE

The keystore file used to store the private key. Defaults to the Caching Service's keystore.

#### CACHING\_STORAGE\_REDIS\_SSL\_KEYSTOREPASSWORD

The password used to unlock the keystore. Defaults to the Caching Service's keystore password.

#### CACHING\_STORAGE\_REDIS\_SSL\_TRUSTSTORE

The truststore file used to keep other parties public keys and certificates. Defaults to the Caching Service's truststore.

#### • CACHING\_STORAGE\_REDIS\_SSL\_TRUSTSTOREPASSWORD

The password used to unlock the truststore. Defaults to the Caching Service's truststore password.

Version: v1.25.x LTS

# **Overview**

You can create application plug-ins to extend the capabilities of the Zowe™ Application Framework. An application plug-in is an installable set of files that present resources in a web-based user interface, as a set of RESTful services, or in a web-based user interface and as a set of RESTful services.

Read the following topics to get started with extending the Zowe Application Framework.

## **How Zowe Application Framework works**

Read the following topics to learn how Zowe Application Framework works:

- Creating application plug-ins
- Plug-ins definition and structure
- Dataservices
- Zowe Desktop and window management
- Configuration Dataservice
- URI Broker
- Application-to-application communication
- Error reporting UI
- Logging utility

# **Tutorials**

The following tutorials are available in Github.

• Stand up a local version of the Example Zowe Application Server



User Browser Workshop App

#### **GITHUB REPO:**

User Browser Workshop App

• Internationalization in Angular Templates in Zowe Application Server

#### $\bigcirc$ GITHUB SAMPLE REPO:

sample-angular-app (Internationalization)

• App to app communication

GITHUB SAMPLE REPO :

sample-angular-app (App to app communication).

• Using the Widgets Library

 $\bigcirc$  GITHUB SAMPLE REPO:

sample-angular-app (Widgets)

• Configuring user preferences (configuration dataservice)

○ GITHUB SAMPLE REPO:

sample-angular-app (configuration dataservice)

### Samples

Zowe allows extensions to be written in any UI framework through the use of an Iframe, or Angular and React natively. In this section, code samples of various use-cases will be provided with install instructions.

**TROUBLESHOOTING SUGGESTIONS:** If you are running into issues, try these suggestions:

- Restart the Zowe Server/ VM.
- Double check that the name in the plugins folder matches your identifier in pluginsDefinition.json located in the Zowe root.
- After logging into the Zowe desktop, use the Chrome or Firefox developer tools and navigate to the "network" tab to see what errors you are getting.
- Check each file with cat <filename> to be sure it wasn't corrupted while uploading. If files were corrupted, try uploading using a different method like SCP or SFTP.

#### Sample Iframe App

 $\bigcirc$  GITHUB SAMPLE REPO:

sample-iframe-app

#### Sample Angular App

**GITHUB SAMPLE REPO:** 

sample-angular-app

#### Sample React App

**GITHUB SAMPLE REPO:** 

<u>sample-react-app</u>

#### **User Browser Workshop Starter App**

#### **GITHUB SAMPLE REPO:**

workshop-starter-app

This sample is included as the first part of a tutorial detailing communication between separate Zowe apps.

It should be installed on your system before starting the User Browser Workshop App Tutorial

The App's scenario is that it has been opened to submit a task report to a set of users who can handle the task. In this case, it is a bug report. We want to find engineers who can fix this bug, but this App does not contain a directory listing for engineers in the company, so we need to communicate with some App that does provide this information. In this tutorial, you must build an App which is called by this App in order to list engineers, is able to be filtered by the office that they work from, and is able to submit a list of engineers which would be able to handle the task.

After installing this app on your system, follow directions in the User Browser Workshop App Tutorial to enable app-to-app communication.

# **Plug-ins definition and structure**

The Zowe<sup>TM</sup> Application Server (zlux-server-framework) enables extensibility with application plug-ins. Application plug-ins are a subcategory of the unit of extensibility in the server called a *plug-in*.

The files that define a plug-in are located in the pluginsDir directory.

# **Application plug-in filesystem structure**

An application plug-in can be loaded from a filesystem that is accessible to the Zowe Application Server, or it can be loaded dynamically at runtime. When accessed from a filesystem, there are important considerations for the developer and the user as to where to place the files for proper build, packaging, and operation.

#### **Root files and directories**

The root of an application plug-in directory contains the following files and directories.

#### pluginDefinition.json

This file describes an application plug-in to the Zowe Application Server. (A plug-in is the unit of extensibility for the Zowe Application Server. An application plug-in is a plug-in of the type "Application", the most common and visible type of plug-in.) A definition file informs the server whether the application plug-in has server-side dataservices, client-side web content, or both. The attributes of this file and how it is found by the server are described in the Plugin Definition article.

#### Dev and source content

Aside from demonstration or open source application plug-ins, the following directories should not be visible on a deployed server because the directories are used to build content and are not read by the server.

#### nodeServer

When an application plug-in has router-type dataservices, they are interpreted by the Zowe Application Server by attaching them as ExpressJS routers. It is recommended that you write application plug-ins using Typescript, because it facilitates well-structured code. Use of Typescript results in build steps because the pre-transpilation Typescript content is not to be consumed by NodeJS. Therefore, keep server-side source code in the nodeServer directory. At runtime, the server loads router dataservices from the lib directory.

#### webClient

When an application plug-in has the *webContent* attribute in its definition, the server serves static content for a client. To optimize loading of the application plug-in to the user, use Typescript to write the application plug-in and then package it using Webpack. Use of Typescript and Webpack result in build steps because the pre-transpilation Typescript and the pre-webpack content are not to be consumed by the browser. Therefore, separate the source code from the served content by placing source code in the webClient directory.

#### **Runtime content**

At runtime, the following set of directories are used by the server and client.

#### lib

The lib directory is where router-type dataservices are loaded by use in the Zowe Application Server. If the JS files that are loaded from the lib directory require NodeJS modules, which are not provided by the server base (the modules <code>zlux-server-framework</code> requires are added to <code>NODE\_PATH</code> at runtime), then you must include these modules in <code>lib/node\_modules</code> for local directory lookup or ensure that they are found on the <code>NODE\_PATH</code> environment variable. <code>nodeServer/node\_modules</code> is not automatically accessed at runtime because it is a dev and build directory.

#### web

The web directory is where the server serves static content for an application plug-in that includes the *webContent* attribute in its definition. Typically, this directory contains the output of a webpack build. Anything you place in this directory can be accessed by a client, so only include content that is intended to be consumed by clients.

#### Packaging applications as compressed files

Application plug-in files can be served to browsers as compressed files in brotli (.br) or gzip (.gz) format. The file must be below the application's /web directory, and the browser must support the compression method. If there are multiple compressed files in the /web directory, the Zowe Application Server and browser perform runtime negotiation to decide which file to use.

#### **Default user configuration**

Configuration Dataservice default settings for users can be packaged within a plugin.

This is done by putting content within the /config/storageDefaults folder, and more on that subject can be found here

#### **App-to-App Communication**

App-to-App communication behaviors can be statically defined or dynamically created at runtime. Static definitions help as a form of documentation and to be able to depend upon them, so it is recommended that these be packaged with a plugin if you wish other's to be able to use App-to-App communication on your App.

This page describes the subject in more detail.

In summary, App-to-App Actions and Recognizers can be stored within an App's /config/actions and /config/recognizers folders, respectively, where the filenames much match the identifiers of Apps.

#### Documentation

In order for Zowe servers to pick up documentation to present to UIs, they must be in a uniform place.

The **/doc** folder of any Plugin can contain at its root any READMEs or documents that an administrator or developer may care about when working with a Plugin for the first time.

The **/doc/swagger** folder on the other hand, will be used to store .yaml extension Swagger 2.0 files that document the APIs of a Plugin's dataservices if they exist.

Other folders may exist, such as **/doc/ui** to document help behavior that may be shown in a UI, but is not implemented at this time.

# Location of plug-in files

The files that define a plug-in are located in the plugins directory.

#### pluginsDir directory

At startup, the server reads from the plugins directory. The server loads the valid plug-ins that are found by the information that is provided in the JSON files.

Within the pluginsDir directory are a collection of JSON files. Each file has two attributes, which serve to locate a plug-in on disk:

**location**: This is a directory path that is relative to the server's executable (such as zlux-app-server/bin/nodeServer.sh) at which a pluginDefinition.json file is expected to be found.

**identifier**: The unique string (commonly styled as a Java resource) of a plug-in, which must match what is in the pluginDefinition.json file.

# **Plug-in definition file**

pluginDefinition.json is a file that describes a plug-in. Each plug-in requires this file, because it defines how the server will register and use the backend of an application plug-in (called a *plug-in* in the terminology of the proxy server). The attributes in each file are dependent upon the pluginType attribute. Consider the following pluginDefinition.json file from sample-app:

# **Plug-in attributes**

There are two categories of attributes: General and Application.

#### **General attributes**

#### identifier

Every application plug-in must have a unique string ID that associates it with a URL space on the server.

#### apiVersion

The version number for the pluginDefinition scheme and application plug-in or dataservice requirements. The default is 1.0.0.

#### pluginVersion

The version number of the individual plug-in.

#### pluginType

A string that specifies the type of plug-in. The type of plug-in determines the other attributes that are valid in the definition.

- application: Defines the plug-in as an application plug-in. Application plug-ins are composed of a
  collection of web content for presentation in the Zowe web component (such as the Zowe Desktop), or
  a collection of dataservices (REST and websocket), or both.
- **library**: Defines the plug-in as a library that serves static content at a known URL space.
- nodeAuthentication: Authentication and Authorization handlers for the Zowe Application Server.

#### requirements (optional)

Describes the environmental requirements that a plugin may have.

- **components**: Houses the list of any component requirements for that plugin.
- id: Defines the component requirement. This is a growing list of support: app-server, zss
- •
- •

#### **Application attributes**

When a plug-in is of *pluginType* application, the following attributes are valid:

#### webContent

An object that defines several attributes about the content that is shown in a web UI.

#### dataServices

An array of objects that describe REST or websocket dataservices.

#### configurationData

An object that describes the resource structure that the application plug-in uses for storing user, group, and server data.

#### **Application web content attributes**

An application that has the *webContent* attribute defined provides content that is displayed in a Zowe web UI.

The following attributes determine some of this behavior:

#### framework

States the type of web framework that is used, which determines the other attributes that are valid in *webContent*.

- **angular2**: (or **angular**) Defines the application as having an Angular (2+) web framework component. This is the standard for a "native" framework Zowe application.
- **react**: Defines this App as having a React web framework component.
- **iframe**: Defines the application as being external to the native Zowe web application environment, but instead embedded in an iframe wrapper.

#### launchDefinition

An object that details several attributes for presenting the application in a web UI.

- **pluginShortNameDefault**: A string that gives a name to the application when i18n is not present. When i18n is present, i18n is applied by using the *pluginShortNameKey*.
- **descriptionDefault**: A longer string that specifies a description of the application within a UI. The description is seen when i18n is not present. When i18n is present, i18n is applied by using the *descriptionKey*.
- **imageSrc**: The relative path (from /web) to a small image file that represents the application icon.

#### defaultWindowStyle

An object that details the placement of a default window for the application in a web UI.

- width: The default width of the application plug-in window, in pixels.
- **height**: The default height of the application plug-in window, in pixels.

#### **IFrame application web content**

In addition to the general web content attributes, when the framework of an application is "iframe", you must specify the page that is being embedded in the iframe. To do so, include the attribute *startingPage* within *webContent*. *startingPage* is relative to the application's //web directory.

Specify *startingPage* as a relative path rather than an absolute path because the pluginDefinition.json file is intended to be read-only, and therefore would not work well when the hostname of a page changes.

Within an IFrame, the application plug-in still has access to the globals that are used by Zowe for application-to-application communication; simply access *window.parent.ZoweZLUX*.

#### **Plugin Definition Schema Revision Notes**

The initial Plugin Definition Schema is version 1.0.0, since then, the following updates have been made

- 1.0.1
  - Added webContent.hasComponents which instructs the App code as to if it needs to load
     Zowe App Component logic from a components.js file, rather than the main.js webpack
     file, for non-iframe Apps.
  - Added os as an object and os.platform, and os.type as arrays of strings to be able to know if a Plugin should be loaded dependent upon the host OS.
- 1.1.0
  - Added "binary" as a property of configuration dataservice resources.
- 1.15.0
  - Added "pluginReqs" as an optional section to state plugin environmental & other requirements.

#### **Application Dataservices**

See Dataservices

#### **Application Configuration Data**

The App server has a component for managing an App's configuration & user data, organized by scope such as user, group, and server instance. For more information, see Configuration Dataservice Documentation.

# **Building plugin apps**

You can build a plugin app by using the following steps as a model. Alternatively, you can follow the Sample Angular App tutorial.

Plugins can have any build process desired as long as it doesn't conflict with the packaging structure. The basic requirement for a plugin app is that static web content must be in a /web directory, and server and other backend files must be in a /lib directory.

Before you can build a plugin app you must install all prerequisites.

# **Building web content**

1. On the computer where the virtual desktop is installed, use the the following command to specify a value for the MVD\_DESKTOP\_DIR environment variable:

Where <path> is the install location of the virtual desktop.

- 2. Navigate to /<plugin\_dir>/webClient. If there is no /webClient directory, proceed to the **Building server content** section below.
- 3. Run the npm install command to install any application dependencies. Check for successful return code.
- 4. Run one of the following commands to build the application code:
  - Run the npm run build command to generate static content in the /web directory. (You can ignore warnings as long as the build is successful.)
  - Run the npm run start command to compile in real-time. Until you stop the script, it compiles code changes as you make them.

# **Building app server content**

1. Navigate to the plugin directory. If there is no **/nodeServer** directory in the plugin directory, proceed to the **Building Javascript content (\*.js files)** section below.

- 2. Run the npm install command to install any application dependencies. Check for successful return code.
- 3. Run one of the following commands to build the application code:
  - Run the npm run build command to generate static content in the /lib directory.
  - Run the npm run start command to compile in real-time. Until you stop the script, it compiles code changes as you make them.

## **Building zss server content**

- 1. Clone the zss repository and its submodule zowe-common-c.
- 2. Make a build script that compiles your C code with -Wc,dll and -Wl,dll, and other flags as seen in this zowe example
- 3. Include a ZSS .x file to link zss server APIs to your plugin, as seen in this zowe example
- 4. Ensure that the build output ends up in the /lib folder as a .so file that has the z/OS program control (+p) extended attribute.

# Tagging plugin files on z/OS

When Zowe App Framework is installed on z/OS developers should tag their plugin files according to the file content. Tagging files helps programs on z/OS understand how to interpret those files, most importantly to know whether a file is encoded using EBCDIC (Extended Binary Coded Decimal Interchange Code). If you are unsure if a plugin you are using is tagged, it can be checked and set using the <a href="https://chtag.command.lf">chtag</a> command. If you want to set the tags, it can be done in bulk with the help of these programs:

- Autotag: This free, open-source application is not part of Zowe. You can download the binary from here for example https://anaconda.org/izoda/autotag. Source: https://github.com/RocketSoftware/autotag
- The Zowe tagging script: This script tags by file extension. It might not work for all cases, but can be altered to suit your needs. Source: https://github.com/zowe/zowe-installpackaging/blob/master/scripts/tag-files.sh

# **Building Javascript content (\*.js files)**

Unlike Typescript, Javascript is an interpreted language and does not need to be built. In most cases, reloading the page should build new code changes. For Iframes or other JS-based apps, close and open the app.

# Installing

Follow the steps described in Installing plugins to add your built plugin to the Zowe desktop.

# Packaging

For more information on how to package your Zowe app, developers can see Plugins definition and structure.

Version: v1.25.x LTS

# **Installing Plugins**

Plugins can be added or removed from the Zowe App Server, as well as upgraded. There are two ways to do these actions: By REST API or by filesystem. The instructions below assume you have administrative permissions either to access the correct REST APIs or to have the necessary permissions to update server directories & files.

NOTE: Plugins must be pre-built, and follow the directory structure, and have all dependencies met to be successfully installed. Read the server log in <INSTANCE\_DIR>/log/install-app.log, (ex ~/.zowe/log/install-app.log) if a plugin does not show in the Zowe desktop, but has been installed successfully.

# By filesystem

The App server uses directories of JSON files, described in the wiki. Defaults are located in the folder zlux-app-server/defaults/plugins, but the server reads the list of plugins instead from the instance directory, at <INSTANCE\_DIR>/workspace/app-server/plugins (for example, ~/.zowe/workspace/app-server/plugins) (Or in prior releases, the Old plugins folder) which includes JSON files describing where to find a plugin. Adding or removing JSONs from this folder will add or remove plugins upon server restart, or you can use REST APIs and cluster mode to add or remove plugins without restarting).

### Adding/Installing

To add or install a plugin, run the script <INSTANCE\_DIR>/workspace/bin/install-app.sh providing the location to a plugin folder. For example:

```
./install-app.sh /home/john/zowe/sample-angular-app
```

This will generate a JSON file <INSTANCE\_DIR>/workspace/app-

server/plugins/org.zowe.zlux.sample.angular.json that contains the plugin's ID and its location on disk. These JSON files tell the Desktop where to find apps and are the glue between the Zowe instance's desktop and the plugin code itself held in its directory.

. For example, if we were to install the sample angular-app in the folder /home/john/zowe/sampleangular-app , then the JSON would be:

#### Removing

To remove a plugin, locate the server's instance plugin directory <INSTANCE\_DIR>/workspace/appserver/plugins (for example, ~/.zowe/workspace/app-server/plugins) and remove the locator JSON that is associated with that plugin. Remove the plugin's content by deleting it from the file system if applicable.

#### Upgrading

Currently, only one version of a plugin can exist per server. So, to upgrade, you either upgrade the plugin within its pre-existing directory by rebuilding it (with more up to date code), or you alter the locator JSON of that app to point to the content of the upgraded version.

#### Modifying without server restart (Exercise to the reader)

The server's reading of the locator JSONs and initializing of plugins only happens during bootstrapping at startup. However, in cluster mode the bootstrapping happens once per worker process. Therefore, it is possible to manage plugins without a server restart by killing & respawning all worker processes without killing the cluster master process. This is what the REST API does, internally. To do this without the REST API, it may be possible to script knowing the parent process ID, and running a kill command on all child processes of the App server cluster process.

# **By REST API**

The server REST APIs allow plugin management without restarting the server - you can add, remove, and upgrade plugins in real-time. However, removal or upgrade must be done carefully as it can disrupt users of those plugins.

#### This swagger file documents the REST API for plugin management

The API only works when RBAC is configured, and an RBAC-compatible security plugin is being used. An example of this is zss-auth, and use of RBAC is described in this documentation and in the wiki.

*NOTE:* If you do not see your plugin in the Zowe desktop check the server log in the (INSTANCE\_DIR>/log/install-app.log) directory to troubleshoot the problem. If you are building your own desktop extension then you need to pre-build your plugin with the correct directory structure, and meet all dependencies.

#### **Old plugins folder**

Prior to the start of Zowe Long Term Support for v1 (that began with Zowe 1.9.0) the location of the default and instance plugins directory were located within <code>zlux-app-server</code> folder (unless otherwise customized). Zowe v1 releases (1.9.0 and later) have backwards compatibility for the existence of these directories, but they can and should be migrated to take advantage of future enhancements.

Folder	New Location	Old Location	Note
Default plugins	<pre>zlux-app- server/defaults/plugins</pre>	<pre>zlux-app-server/plugins</pre>	
Instance plugins	<instance_dir>/workspace/app- server/plugins</instance_dir>	<pre>zlux-app- server/instance/ZLUX/plugins</pre>	INSTANCE is ~/.zowe not otherv defined

# **Embedding plugins**

Add these imports to a component where you want to embed another plugin:

Inject Angular2PluginEmbedActions into your component constructor:

In the component template prepare a container where you want to embed the plugin:

In the component class add a reference to the container:

In the component class add a reference to the embedded instance:

Everything is ready to start embedding, you just need to know the pluginld that you want to embed:

### How to interact with embedded plugin

If the main component of embedded plugin declares Input and Output properties then you can interact with it. ApplicationManager provides methods to set Input properties and get Output properties of the embedded plugin. Suppose, that the embedded plugin declares Input and Output properties like this:

Obtain a reference to ApplicationManager in your component constructor:

*Note:* We are unable to inject ApplicationManager with @Inject() until an AoT-compiler issue with namespaces is resolved: angular/angular#15613

Now you can set sampleInput property, obtain sampleOutput property and subscribe to it:

## How to destroy embedded plugin

There is no special API to destroy embedded plugin. If you want to destroy the embedded plugin just clear the container for the embedded plugin and set embeddedInstance to null:

### How to style a container for the embedded plugin

It is hard to give a universal recipe for a container style. At least, the container needs **position:** "relative" because the embedded plugin may have absolutely positioned elements. Here is sample styles you can start with if your component utilizes flexbox layout:

# Applications that use embedding

Workflow app demonstrates advanced usage.

# Dataservices

Dataservices are dynamic backend components of Zowe<sup>™</sup> plug-in applications. You can optionally add them to your applications to make the application do more than receive static content from the proxy server. Each dataservice defines a URL space that the server can use to run extensible code from the application. Dataservices are mainly intended to create REST APIs and WebSocket channels.

# **Defining dataservices**

You define dataservices in the application's pluginDefinition.json file. Each application requires a definition file to specify how the server registers and uses the application's backend. You can see an example of a pluginDefinition.json file in the top directory of the sample-angular-app.

In the definition file is a top level attribute called dataServices, for example:

To define your dataservice, create a set of keys and values for your dataservice in the dataservices array. The following values are valid:

#### type

Specify one of the following values:

- **router**: Router dataservices run under the proxy server and use ExpressJS Routers for attaching actions to URLs and methods.
- **service**: Service dataservices run under ZSS and utilize the API of ZSS dataservices for attaching actions to URLs and methods.
- **java-war**: See the topic *Defining Java dataservices* below.
- **external**: Used to set up an endpoint in your plugin's namespace as a proxy for an endpoint on another server. External services have the following values to state how to proxy.

#### name

The name of the service. Names must be unique within each pluginDefinition.json file. The name is used to reference the dataservice during logging and to construct the URL space that the dataservice

occupies.

#### version

A semver version string. More than one version of the same service can be present within a plugin, but versions must be declared to track dependencies.

#### initializerLookupMethod

Specify external unless otherwise instructed.

#### fileName

The name of the file that is the entry point for construction of the dataservice, relative to the application's /lib directory. For example, for the sample-app the fileName value is "helloWorld.js" - without a path. So its typescript code is transpiled to JavaScript files that are placed directly into the /lib directory.

#### dependenciesIncluded

Specify true for anything in the pluginDefinition.json file. Only specify false when you are adding dataservices to the server dynamically.

### Router-type specific attributes

#### routerFactory (Optional)

When you use a router dataservice, the dataservice is included in the proxy server through a require() statement. If the dataservice's exports are defined such that the router is provided through a factory of a specific name, you must state the name of the exported factory using this attribute.

### Import-type specific attributes

#### sourcePlugin

The ID of the plugin where the service can be found for an **import** type dataservice.

#### sourceName

The name of the dataservice to be found in the source plugin when using an **import** type dataservice.

#### localName

The name of the dataservice within your plugin's namespace when using an **import** type dataservice.

#### versionRange

A semver string plus range modifiers such as "^" to denote what range of versions would satisfy the import.

Note: Import-type dataservices cannot at this time override the attributes of the imported dataservice. For example, if the original dataservice had <a href="httpCaching:false">httpCaching:false</a>, and the import used <a href="httpCaching:true">httpCaching:true</a>, the import's value is ignored and the original value used instead.

### **External-type specific attributes**

#### urlPrefix

The prefix to be prepended when making the proxy connection to the external source. For example, if the user tried to access <your external service>/foo, but your urlPrefix was /bar, then the proxy would make a connection to <your external destination>/bar/foo.

#### isHttps

Boolean used to tell the server whether to proxy to a destination that is or is not using https instead of http.

Note: External-type dataservices also require specification of the proxied host & port. This is accomplished via making a JSON file, remote.json, with attributes host and port, and placing it within the internal configuration storage for that dataservice. See more about that storage here: https://github.com/zowe/zlux/wiki/Configuration-Dataservice#internal--bootstrapping-use

# **Defining Java dataservices**

In addition to other types of dataservice, you can use Java (also called java-war) dataservices in your applications. Java dataservices are powered by Java Servlets.

To use a Java dataservice you must meet the prerequisites, define the dataservice in your plug-in definition, and define the Java Application Server library to the Zowe Application Server.

### **Prerequisites**

- Install a Java Application Server library. In this release, Tomcat is the only supported library.
- Make sure your plug-in's compiled Java program is in the application's /lib directory, in either a

   war archive file or a directory extracted from a .war archive file. Extracting your file is
   recommended for faster start-up time.

### **Defining Java dataservices**

To define the dataservice in the pluginDefinition.json file, specify the type as java-war, for example:

To access the service at runtime, the plug-in can use the Zowe dataservice URL standard: /ZLUX/plugins/[PLUGINID]/services/[SERVICENAME]/[VERSIONNUMBER]

Using the example above, a request to get users might be: /ZLUX/plugins/[PLUGINID]/services/javaservlet/1.0.0/users

**Note:** If you extracted your servlet contents from a .war file to a directory, the directory must have the same name as the file would have had. Using the example above, javaservlet.war must be extracted to a directory named \javaservlet.

### **Defining Java Application Server libraries**

In the zlux-app-server/zluxserver.json file, use the example below to specify Java Application Server library parameters:

Specify the following parameters in the languages.java object:

- **runtimes** (object) The name and location of a Java runtime that can be used by one or more services. Used to load a Tomcat instance.
  - name (object) The name of the runtime.
    - home (string) The path to the runtime root. Must include /bin and /lib directories.
- ports (array <number>)(Optional) An array of port numbers that can be used by instances of Java Application Servers or microservices. Must contain as many ports as distinct servers that will be spawned, which is defined by other configuration values within languages.java. Either ports or portRange is required, but portRange has a higher priority.
- portRange (array <number>)(Optional) An array of length 2, which contains a start number and end number to define a range of ports to be used by instances of application servers or microservices. You will need as many ports as distinct servers that will be spawned, which is defined by other

configuration values within languages.java. Either ports or portRange is required, but portRange has a higher priority.

- war (object) Defines how the Zowe Application Server should handle java-war dataservices.
  - defaultGrouping (string)(Optional) Defines how services should be grouped into instances of Java Application Servers. Valid values: appserver or microservice. Default: appserver.
     appserver means 1 server instance for all services. microservice means one server instance per service.
  - pluginGrouping (array <object>)(Optional) Defines groups of plug-ins to have their javawar services put within a single Java Application Server instance.
    - plugins (Array <string>) Lists the plugins by identifier which should be put into this group. Plug-ins with no java-war services are skipped. Being in a group excludes a plugin from being handled by defaultGrouping.
    - runtime (string)(Optional) States the runtime to be used by the Tomcat server instance, as defined in languages.java.runtimes.
  - **javaAppServer** (object) Java Application Server properties.
    - **type** (string) Type of server. In this release, tomcat is the only valid value.
    - path (string) Path of the server root, relative to zlux-app-server/lib. Must include
       /bin and /lib directories.
    - **config** (string) Path of the server configuration file, relative to zlux-app-server/lib.
    - https (object) HTTPS parameters.
      - key (string) Path of a private key, relative to zlux-app-server/lib.
      - certificate (string) Path of an HTTPS certificate, relative to zlux-app-server/lib.

## Java dataservice logging

The Zowe Application Server creates the Java Application Server instances required for the java-war dataservices, so it logs the stdout and stderr streams for those processes in its log file. Java Application Server logging is not managed by Zowe at this time.

## Java dataservice limitations

Using Java dataservices with a Zowe Application Server installed on a Windows computer, the source and Java dataservice code must be located on the same storage volume.

To create multiple instances of Tomcat on non-Windows computers, the Zowe Application Server establishes symbolic links to the service logic. On Windows computers, symbolic links require administrative privilege, so the server establishes junctions instead. Junctions only work when the source and destination reside on the same volume.

# **Using dataservices with RBAC**

If your administrator configures the Zowe Application Framework to use role-based access control (RBAC), then when you create a dataservice you must consider the length of its paths.

To control access to dataservices, administrators can enable RBAC, then use a z/OS security product such as RACF to map roles and authorities to a System Authorization Facility (SAF) profile. For information on RBAC, see Applying role-based access control to dataservices.

SAF profiles have the following format:

```
<product>.<instance id>.SVC.<pluginid_with_underscores>.<service>.<HTTP method>.<dataservice path with forward slashes '/' replaced by periods '.'>
```

For example, to access this dataservice endpoint:

/ZLUX/plugins/org.zowe.foo/services/baz/\_current/users/fred

Users must have READ access to the following profile:

ZLUX.DEFAULT.SVC.ORG\_ZOWE\_F00.BAZ.POST.USERS.FRED

Profiles cannot contain more than 246 characters. If the path section of an endpoint URL makes the profile name exceed limit, the path is trimmed to only include elements that do not exceed the limit. For example, imagine that each path section in this endpoint URL contains 64 characters:

/ZLUX/plugins/org.zowe.zossystem.subsystems/services/data/\_current/aa..a/bb..b/cc ..c/dd..d

So aa..a is 64 "a" characters, bb..b is 64 "b" characters, and so on. The URL could then map to the following example profile:

ZLUX.DEFAULT.SVC.ORG\_ZOWE\_ZOSSYSTEM\_SUBSYSTEMS.DATA.GET.AA..A.BB..B

The profile ends at the BB..B section because adding CC..C would put it over 246 characters. So in this example, all dataservice endpoints with paths that start with AA..A.BB..B are controlled by this one

profile.

To avoid this issue, we recommend that you maintain relatively short endpoint URL paths.

# **Dataservice APIs**

Dataservice APIs can be categorized as Router-based or ZSS-based, and either WebSocket or not.

### **Router-based dataservices**

Each Router dataservice can safely import Express, express-ws, and bluebird without requiring the modules to be present, because these modules exist in the proxy server's directory and the *NODE\_MODULES* environment variable can include this directory.

#### HTTP/REST Router dataservices

Router-based dataservices must return a (bluebird) Promise that resolves to an ExpressJS router upon success. For more information, see the ExpressJS guide on use of Router middleware: Using Router Middleware.

Because of the nature of Router middleware, the dataservice need only specify URLs that stem from a root '/' path, as the paths specified in the router are later prepended with the unique URL space of the dataservice.

The Promise for the Router can be within a Factory export function, as mentioned in the pluginDefinition specification for *routerFactory* above, or by the module constructor.

An example is available in the Sample Angular App.

#### WebSocket Router dataservices

ExpressJS routers are fairly flexible, so the contract to create the Router for WebSockets is not significantly different.

Here, the express-ws package is used, which adds WebSockets through the ws package to ExpressJS. The two changes between a WebSocket-based router and a normal router are that the method is 'ws', as in router.ws(<url>,<callback>), and the callback provides the WebSocket on which you must define event listeners.

See the ws and express-ws topics on www.npmjs.com for more information about how they work, as the API for WebSocket router dataservices is primarily provided in these packages.

```
An example is available in zlux-server-framework/plugins/terminal-
proxy/lib/terminalProxy.js
```

#### Router dataservice context

Every router-based dataservice is provided with a **Context** object upon creation that provides definitions of its surroundings and the functions that are helpful. The following items are present in the **Context** object:

### serviceDefinition

The dataservice definition, originally from the pluginDefinition.json file within a plug-in.

### serviceConfiguration

An object that contains the contents of configuration files, if present.

#### logger

An instance of a Zowe Logger, which has its component name as the unique name of the dataservice within a plug-in.

#### makeSublogger

A function to create a Zowe Logger with a new name, which is appended to the unique name of the dataservice.

### addBodyParseMiddleware

A function that provides common body parsers for HTTP bodies, such as JSON and plaintext.

### plugin

An object that contains more context from the plug-in scope, including:

- **pluginDef**: The contents of the pluginDefinition.json file that contains this dataservice.
- **server**: An object that contains information about the server's configuration such as:

- **app**: Information about the product, which includes the *productCode* (for example: ZLUX).
- **user**: Configuration information of the server, such as the port on which it is listening.

### Router storage API

## **ZSS based dataservices**

ZSS dataservices much like zlux router services can be used to implement REST or websocket APIs. Each service is associated with a URL which when requested will call a function to handle the request or websocket message event.

### HTTP/REST ZSS dataservices

ZSS REST dataservices are registered into ZSS with a service installer function, where initializerName is the function name located in the dll libraryName. The methods list what HTTP methods are expected of this dataservice. Example:

The service installer is given DataService, which includes context such as the above definition plus a loggingIdentifier. The service is also given HttpServer, a reference to ZSS and its configuration. To register the dataservice, you must make an HttpService object like

Then you must assign properties to the dataservice, such as

- authType: What type of authentication and authorization checks should be done before calling this service. values such as SERVICE\_AUTH\_NONE when the service does not need securty or SERVICE\_AUTH\_NATIVE\_WITH\_SESSION\_TOKEN when the service should be protected by ZSS's cookie are valid.
- serviceFunction: The function within this dataservice that will be called whenever a request is received.
- runInSubtask: (TRUE/FALSE) Whether to run the service function in a subtask or not whenever a request is received.
- doImpersonation: (TRUE/FALSE) When true, the service function will be ran as the authenticated user, rather than the server user. This is recommended whenever possible to keep permissions management in line with the users own permissions.

Example of service installer:

When a request is received, the service function is called with the HttpService and HttpResponse objects. HttpService is used to store and retrieve cached data and access the storage API.

HttpRequest is a pointer within the response object, and utilities exist to help with parsing it.

Example of request handling:

#### **ZSS dataservice context and structs**

Headers to important dataservice structs include

- HttpResponse
- HttpRequest
- HttpService
- HttpServer
- Json handling
- DataService context
- Utilities
- Data structures

#### ZSS storage API

The DataService struct contains two Storage structs, localStorage and remoteStorage. They implement the same API for getting, setting, and removing data, but manage the data in different locations. localStorage stores data within the ZSS server, for high speed access. remoteStorage stores data in the Caching Service, for high availability state storage.

Usage example: Sample angular app storage test api: https://github.com/zowe/sample-angularapp/blob/v1.23.0-RC1/zssServer/src/storage.c

# **Documenting dataservices**

It is recommended that you document your RESTful application dataservices in OpenAPI (Swagger) specification documents. The Zowe Application Server hosts Swagger files for users to view at runtime.

To document a dataservice, take the following steps:

1. Create a .yaml or .json file that describes the dataservice in valid Swagger 2.0 format. Zowe validates the file at runtime.

- 2. Name the file with the same name as the dataservice. Optionally, you can include the dataservice version number in the format: <name>\_<number>. For example, a Swagger file for a dataservice named user must be named either users.yaml or users\_1.1.0.yaml.
- 3. Place the Swagger file in the /doc/swagger directory below your application plug-in directory, for example:

/sample-angular-app/doc/swagger/hello.yaml

At runtime, the Zowe Application Server does the following:

- Dynamically substitutes known values in the files, such as the hostname and whether the endpoint is accessible using HTTP or HTTPS.
- Builds documentation for each dataservice and for each application plug-in, in the following locations:
  - Dataservice documentation:
     /ZLUX/plugins/<app\_name>/catalogs/swagger/servicename
  - Application plug-in documentation: /ZLUX/plugins/<app\_name>/catalogs/swagger
- In application plug-in documentation, displays only stubs for undocumented dataservices, stating that the dataservice exists but showing no details. Undocumented dataservices include non-REST dataservices such as WebSocket services.

Version: v1.25.x LTS

# **Authentication API**

This topic describes the web service API for user authentication.

The authentication mechanism of the ZLUX server allows for an administrator to gate access to services by a given auth handler, while on the user side the authentication structure allows for a user to login to one or more endpoints at once provided they share the same credentials given.

# Handlers

The auth handlers are a type of zlux server plugin (type=nodeAuthentication) which are categorized by which kind of authentication they can provide. Whether it's to z/OS via type=saf or theoretical authentication such as Facebook or Amazon cloud, the handler API is abstract to handle different types of security needs.

## Handler installation

Auth handler plugins are installed like any other plugin.

# Handler configuration

The server top-level configuration attribute dataserviceAuthentication states properties about which plugins to use and how to use them.

For example,

The dataserviceAuthentication attribute has the following properties:

- defaultAuthentication: Which authentication category to choose by default, in case multiple are installed.
- rbac: Whether or not the server should do authority checks in addition to authentication checks when requesting a dataservice.

## Handler context

These plugins are given an object, context, in the constructor. Context has attributes to help the plugin know about the server configuration, provide a named logger, and more. The parameters include:

- pluginDefinition: The object describing the plugin's definition file
- pluginConf: An object that gives the plugin it's configuration from the Config Service internal storage
- serverConfiguration: The object describing the server's current configuration
- context: An object holding contextual objects
  - logger: A logger with the name of the plugin's ID

# Handler capabilities

A handler's constructor should return a capabilities object that states which capabilities the plugin has. If a capabilities object is not returned, it is assumed that only the authenticate and authorize functions are implemented, for backward compatibility support. The capabilities object should include:

- canGetCategories: (true/false) If the getCategories() function exists, which returns a string array of categories of auth the plugin can support given the server context. This is useful if the plugin can support multiple categories conditionally.
- canLogout: (true/false) If the logout(request, sessionState) function exists. Used to clear state and cookies when a session should be ended.
- canGetStatus: (true/false) If the getStatus(sessionState) function exists
- canRefresh: (true/false) If the refreshStatus(request, sessionState) function exists, which is used to renew a session that has an expiration limit.
- canAuthenticate: (true/false) If the authenticate(request, sessionState):Promise function exists (Required, assumed)
- canAuthorized: (true/false) If the \*authorized(request, sessionState, options) function exists (Required, assumed)
- haCompatible: (true/false) Used to be sure that a plugin has no state that would be lost in a high availability environment.
- canGenerateHaSessionId: (true/false) If generateHaSessionId(request) exists, which is used to set the value used for an app-server session for a user. When not in a high availability environment, the appserver generates its own session ID.
- canResetPassword: (true/false) If passwordRest(request, sessionState) exists
- proxyAuthorizations: (true/false) If the addProxyAuthorizations(req1, req2Options, sessionState) function exists

# Examples

sso-auth, which conditionally implements the saf, zss, and apiml security types: https://github.com/zowe/zlux-server-framework/tree/v1.23.0-RC1/plugins/sso-auth

# High availability (HA)

Some auth handlers are not capable of working in a high availability environment. In these environments, there can be multiple zlux servers and there may not be a safe and secure way to share session state data. This extends to the zlux server cookie as well, which is not sharable between multiple servers by default. Therefore, high availability has the following two requirements from an auth handler plugin: 1) The plugin must state that it is HA capable by setting the capability flag haCompatible=true, usually indicating that the plugin has no state data. 2) A plugin must have capability canGenerateHaSessionId=true so that the zlux server cookie is sharable between multiple zlux servers.

# **REST API**

## **Check status**

Returns the current authentication status of the user to the caller.

Response example:

Every key in the response object is a registered auth type. The value object is guaranteed to have a Boolean field named "authenticated" which indicates that at least one plugin in the category was able to authenticate the user.

Each item also has a field called "plugins", where every property value is a plugin-specific object.

# Authenticate

Authenticates the user against authentication back-ends.

Request body example:

The categories parameter is optional. If omitted, all auth plugins are invoked with the username and password Response example:

First-level keys are authentication categories or types. "success" means that all of the types requested have been successful. For example typeA successful AND typeB successful AND ...

Second-level keys are auth plugin IDs. "success" on this level means that there's at least one successful result in that auth type. For example, pluginA successful OR pluginB successful OR ...

# User not authenticated or not authorized

The response received by the browser when calling any service, when the user is either not authenticated or not allowed to access the service.

## Not authenticated

The client is supposed to address this by showing the user a login form which will later invoke the login service for the plugin mentioned and repeat the request.

## Not authorized

There's no general way for the client to address this, except than show the user an error message.

## **Refresh status**

If you have an active session, some auth plugins may be able to renew the session. Not all plugins support this action, so while the call may return successful, if there is an associated expiration time you may notice that the expiration time has not changed or been reset.

{ "success": true, "categories": { "saf": { "success": true, "plugins": { "org.zowe.zlux.auth.safsso": {
 "success": true "username":"foo", "expms": 60000 } } } }

## Logout

When you have an active session, you can terminate it early with a logout. This should remove cookies and tell the server to clear any cache it had about a session.

## **Password changes**

Some auth plugins will allow you to change your password. Depending on the backing security (such as SAF), you may need to provide your current password to change it.

Version: v1.25.x LTS

# Internationalizing applications

You can internationalize Zowe™ application plug-ins using Angular and React frameworks. Internationalized applications display in translated languages and include structures for ongoing translation updates.

The steps below use the Zowe Sample Angular Application and Zowe Sample React Application as examples. Your applications might have slightly different requirements, for example the React Sample Application requires the react-i18next library, but your application might require a different React library.

For detailed information on Angular or React, see their documentation. For detailed information on specific internationalization libraries, see their documentation. You can also reference the Sample Angular Application internationalization tutorial, and watch a video on how to internationalize your Angular application.

After you internationalize your application, you can view it by following steps in Changing the desktop language.

# Internationalizing Angular applications

Zowe applications that use the Angular framework depend on **.**xlf formatted files to store static translated content and **.**json files to store dynamic translated content. These files must be in the application's web/assets/i18n folder at runtime. Each translated language will have its own file.

To internationalize an application, you must install Angular-compatible internationalization libraries. Be aware that libraries can be better suited to either static or dynamic HTML elements. The examples in this task use the ngx-i18nsupport library for static content and angular-l10n for dynamic content.

To internationalize Zowe Angular applications, take the following steps:

1. To install internationalization libraries, use the **npm** command, for example:

**Note** --save-dev commits the library to the application's required libraries list for future use.

2. To support the CLI tools and to control output, create a webClient/tsconfig.i18n.json typescript file and add the following content:

For example, see this file in the Sample Angular Application.

3. In the static elements in your HTML files, tag translatable content with the i18n attribute within an Angular template, for example:

The attribute should include a message ID, for example the @@welcome above.

4. To configure static translation builds, take the following steps:

a. In the webClient/package.json script, add the following line:

b. In the in webClient directory, create a xliffmerge.json file, add the following content, and specify the codes for each language you will translate in the languages parameter:

When you run the i18n script, it reads this file and generates a messages. [lang].xlf file in the src/assets/i18n directory for each language specified in the languages parameter. Each file contains the untranslated text from the i18n-tagged HTML elements.

5. Run the following command to run the i18n script and extract i18n tagged HTML elements to .xlf files:

**Note** If you change static translated content, you must run the npm run build command to build the application, and then re-run the npm run i18n command to extract the tagged content again.

- 6. In each .xlf file, replace target element strings with translated versions of the source element strings. For example:
- 7. Run the following command to rebuild the application:

When you switch the Zowe Desktop to one of the application's translated languages, the application displays the translated strings.

8. For dynamic translated content, follow these steps:

a. Import and utilize angular-I10n objects within an Angular component, for example:

b. In the related Angular template, you can implement **myDynamicMessage** as an ordinary substitutable string, for example:

9. Create logic to copy the translation files to the web/assets directory during the webpack process, for example in the sample application, the following JavaScript in the copy-webpack-plugin file copies the files:

**Note:** Do not edit files in the web/assets/i18n directory. They are overwritten by each build.

# **Internationalizing React applications**

To internationalize Zowe applications using the React framework, take the following steps:

**Note:** These examples use the recommended react-i18next library, which does not differentiate between dynamic and static content, and unlike the Angular steps above does not require a separate build process.

1. To install the React library, run the following command:

npm install --save-dev react-i18next

- 2. In the directory that contains your index.js file, create an i18n.js file and add the translated content, for example:
- 3. Import the i18n file from the previous step into index.js file so that you can use it elsewhere, for example:
- 4. To internationalize a component, include the useTranslation hook and reference it to substitute translation keys with their translated values. For example:

# Internationalizing application desktop titles

To display the translated application name and description in the Desktop, take the following steps:

- 1. For each language, create a pluginDefinition.i18n.<lang\_code>.json file. For example, for German create a pluginDefinition.i18n.de.json file.
- 2. Place the .json files in the web/assets/i18n directory.
- 3. Translate the pluginShortNameKey and descriptionKey values in the application's pluginDefinition.json file. For example, for the file below you would translate the values "sampleangular" and "sampleangulardescription":
- 4. Add the translated values to the translation file. For example, the German translation file example, pluginDefinition.i18n.de.json, would look like this:

5. Create logic to copy the translation files to the web/assets directory during the webpack process. For example, in the Sample Angular Application the following JavaScript in the webClient/webpack.config.js file copies files to the web/assets directory:

# **Zowe Desktop and window management**

The Zowe<sup>™</sup> Desktop is a web component of Zowe, which is an implementation of MVDWindowManagement, the interface that is used to create a window manager.

The code for this software is in the zlux-app-manager repository.

The interface for building an alternative window manager is in the <code>zlux-platform</code> repository.

Window Management acts upon Windows, which are visualizations of an instance of an application plug-in. Application plug-ins are plug-ins of the type "application", and therefore the Zowe Desktop operates around a collection of plug-ins.

**Note:** Other objects and frameworks that can be utilized by application plug-ins, but not related to window management, such as application-to-application communication, Logging, URI lookup, and Auth are not described here.

# Loading and presenting application plug-ins

Upon loading the Zowe Desktop, a GET call is made to /plugins?type=application. The GET call returns a JSON list of all application plug-ins that are on the server, which can be accessed by the user. Application plug-ins can be composed of dataservices, web content, or both. Application plug-ins that have web content are presented in the Zowe Desktop UI.

The Zowe Desktop has a taskbar at the bottom of the page, where it displays each application plug-in as an icon with a description. The icon that is used, and the description that is presented are based on the application plug-in's PluginDefinition's webContent attributes.

# **Plug-in management**

Application plug-ins can gain insight into the environment in which they were spawned through the Plugin Manager. Use the Plugin Manager to determine whether a plug-in is present before you act upon the existence of that plug-in. When the Zowe Desktop is running, you can access the Plugin Manager through ZoweZLUX.PluginManager

The following are the functions you can use on the Plugin Manager:

- getPlugin(pluginID: string)
  - Accepts a string of a unique plug-in ID, and returns the Plugin Definition Object (DesktopPluginDefinition) that is associated with it, if found.

# **Application management**

Application plug-ins within a Window Manager are created and acted upon in part by an Application Manager. The Application Manager can facilitate communication between application plug-ins, but formal application-to-application communication should be performed by calls to the Dispatcher. The Application Manager is not normally directly accessible by application plug-ins, instead used by the Window Manager.

The following are functions of an Application Manager:

Function	Description
<pre>spawnApplication(plugin: DesktopPluginDefinition, launchMetadata: any): Promise<mvdhosting.instanceid>;</mvdhosting.instanceid></pre>	Opens an application instance into the Window Manager, with or without context on what actions it should perform after creation.
<pre>killApplication(plugin:ZLUX.Plugin, appId:MVDHosting.InstanceId): void;</pre>	Removes an application instance from the Window Manager.
<pre>showApplicationWindow(plugin: DesktopPluginDefinitionImpl): void;</pre>	Makes an open application instance visible within the Window Manager.
<pre>isApplicationRunning(plugin: DesktopPluginDefinitionImpl): boolean;</pre>	Determines if any instances of the application are open in the Window Manager.

# **Windows and Viewports**

When a user clicks an application plug-in's icon on the taskbar, an instance of the application plug-in is started and presented within a Viewport, which is encapsulated in a Window within the Zowe Desktop. Every instance of an application plug-in's web content within Zowe is given context and can listen on events about the Viewport and Window it exists within, regardless of whether the Window Manager implementation

utilizes these constructs visually. It is possible to create a Window Manager that only displays one application plug-in at a time, or to have a drawer-and-panel UI rather than a true windowed UI.

When the Window is created, the application plug-in's web content is encapsulated dependent upon its framework type. The following are valid framework types:

- "angular2": The web content is written in Angular, and packaged with Webpack. Application plug-in framework objects are given through @injectables and imports.
- *"iframe"*: The web content can be written using any framework, but is included through an iframe tag. Application plug-ins within an iframe can access framework objects through *parent.RocketMVD* and callbacks.
- *"react"*: The web content is written in React, Typescript, and packaged with Webpack. App framework objects are provided via the ReactMVDResources object

In the case of the Zowe Desktop, this framework-specific wrapping is handled by the Plugin Manager.

# Viewport Manager

Viewports encapsulate an instance of an application plug-in's web content, but otherwise do not add to the UI (they do not present Chrome as a Window does). Each instance of an application plug-in is associated with a viewport, and operations to act upon a particular application plug-in instance should be done by specifying a viewport for an application plug-in, to differentiate which instance is the target of an action. Actions performed against viewports should be performed through the Viewport Manager.

The following are functions of the Viewport Manager:

Function	Description
<pre>createViewport(providers: ResolvedReflectiveProvider[]): MVDHosting.ViewportId;</pre>	Creates a viewport into which an application plug-in's webcontent can be embedded.
<pre>registerViewport(viewportId: MVDHosting.ViewportId, instanceId: MVDHosting.InstanceId): void;</pre>	Registers a previously created viewport to an application plug-in instance.

Function	Description
<pre>destroyViewport(viewportId: MVDHosting.ViewportId): void;</pre>	Removes a viewport from the Window Manager.
`getApplicationInstanceId(viewportId: MVDHosting.ViewportId): MVDHosting.InstanceId	null;`

# **Injection Manager**

When you create Angular application plug-ins, they can use injectables to be informed of when an action occurs. iframe application plug-ins indirectly benefit from some of these hooks due to the wrapper acting upon them, but Angular application plug-ins have direct access.

The following topics describe injectables that application plug-ins can use.

## **Plug-in definition**

Provides the plug-in definition that is associated with this application plug-in. This injectable can be used to gain context about the application plug-in. It can also be used by the application plug-in with other application plug-in framework objects to perform a contextual action.

## Logger

Provides a logger that is named after the application plug-in's plugin definition ID.

# Launch Metadata

If present, this variable requests the application plug-in instance to initialize with some context, rather than the default view.

# **Viewport Events**

Presents hooks that can be subscribed to for event listening. Events include:

resized: Subject<{width: number, height: number}>

Fires when the viewport's size has changed.

# **Window Events**

Presents hooks that can be subscribed to for event listening. The events include:

Event	Description
<pre>maximized: Subject<void></void></pre>	Fires when the Window is maximized.
<pre>minimized: Subject<void></void></pre>	Fires when the Window is minimized.
<pre>restored: Subject<void></void></pre>	Fires when the Window is restored from a minimized state.
<pre>moved: Subject&lt;{top: number, left: number}&gt;</pre>	Fires when the Window is moved.
<pre>resized: Subject&lt;{width: number, height: number}&gt;</pre>	Fires when the Window is resized.
<pre>titleChanged: Subject<string></string></pre>	Fires when the Window's title changes.

# Window Actions

An application plug-in can request actions to be performed on the Window through the following:

Item	Description
<pre>close(): void</pre>	Closes the Window of the application plug-in instance.
<pre>maximize(): void</pre>	Maximizes the Window of the application plug- in instance.

Item	Description
<pre>minimize(): void</pre>	Minimizes the Window of the application plug-in instance.
<pre>restore(): void</pre>	Restores the Window of the application plug-in instance from a minimized state.
<pre>setTitle(title: string):void</pre>	Sets the title of the Window.
<pre>setPosition(pos: {top: number, left: number, width: number, height: number}): void</pre>	Sets the position of the Window on the page and the size of the window.
<pre>spawnContextMenu(xPos: number, yPos: number, items: ContextMenuItem[]): void</pre>	Opens a context menu on the application plug- in instance, which uses the Context Menu framework.
<pre>registerCloseHandler(handler: () =&gt; Promise<void>): void</void></pre>	Registers a handler, which is called when the Window and application plug-in instance are closed.

# **Framework API examples**

The following are examples of how you would access the Window Actions API to begin an App in maximized mode upon start-up.

### Angular

- 1. Import Angular2InjectionTokens from 'pluginlib/inject-resources'
- 2. Within the constructor of your App, in the arguments, do @Optional()

@Inject(Angular2InjectionTokens.WINDOW\_ACTIONS) private windowActions: Angular2PluginWindowActions

3. Then inside the constructor, check that window actions exist and then execute the action if (this.windowActions) { this.windowActions.maximize(); }

4. Depending on your App layout, certain UI elements may not have loaded so to wait for them to load, one may want to use something like Angular's NgOnInit directive.

### React

- 1. Similar to how we do things in Angular, except the Window Actions (& other Zowe resources) are located in the resources object. So if we were using a React.Component, we could have a constructor with constructor(props){ super(props); ... }
- 2. Then accessing Window Actions would be as simple as this.props.resources.windowActions

### IFrames

 Iframes are similar to Angular & React, but require a different import step. Instead to use Window Actions (& other Zowe resources), we have to import the Iframe adapter. The Iframe adapter is located in zlux-app-manager/bootstrap/web/iframe-adapter.js so something like a relative path in my JS code will suffice,

```
<script type="text/javascript" src="../../org.zowe.zlux.bootstrap/web/iframe-
adapter.js"></script>
```

2. Then to use Window Actions would be as simple as await windowActions.minimize();

NOTE: The Iframe adapter is not yet feature-complete. If you are attempting to use an event supported by Angular or React, but not yet supported in Iframes, try to use the window.parent.ZoweZLUX object instead.

Version: v1.25.x LTS

# **Configuration Dataservice**

The Configuration Dataservice is an essential component of the Zowe™ Application Framework, which acts as a JSON resource storage service, and is accessible externally by REST API and internally to the server by dataservices.

The Configuration Dataservice allows for saving preferences of applications, management of defaults and privileges within a Zowe ecosystem, and bootstrapping configuration of the server's dataservices.

The fundamental element of extensibility of the Zowe Application Framework is a *plug-in*. The Configuration Dataservice works with data for plug-ins. Every resource that is stored in the Configuration Service is stored for a particular plug-in, and valid resources to be accessed are determined by the definition of each plug-in in how it uses the Configuration Dataservice.

The behavior of the Configuration Dataservice is dependent upon the Resource structure for a plug-in. Each plug-in lists the valid resources, and the administrators can set permissions for the users who can view or modify these resources.

1. Resource Scope

### 2. REST API

- i. REST Query Parameters
- ii. REST HTTP Methods
  - a. GET

b. PUT

- c. DELETE
- iii. Administrative Access & Group
- 3. App API
- 4. Internal & Bootstrapping Use
- 5. Packaging Defaults
- 6. Plugin Definition
- 7. Aggregation Policies
- 8. Relevant Source Code

# **Resource Scope**

Data is stored within the Configuration Dataservice according to the selected *Scope*. The intent of *Scope* within the Dataservice is to facilitate company-wide administration and privilege management of Zowe data.

When a user requests a resource, the resource that is retrieved is an override or an aggregation of the broader scopes that encompass the *Scope* from which they are viewing the data.

When a user stores a resource, the resource is stored within a *Scope* but only if the user has access privilege to update within that *Scope*.

Scope is one of the following:

#### Plugin

Configuration defaults that come with a plugin. Cannot be modified.

#### Product

Configuration defaults that come with the product. Cannot be modified.

#### Site

Data that can be used between multiple instances of the Zowe Application Server.

#### Instance

Data within an individual Zowe Application Server.

#### Group

Data that is shared between multiple users in a group.(Pending)

#### User

Data for an individual user. (Pending)

**Note:** While Authorization tuning can allow for settings such as GET from Instance to work without login, *User* and *Group* scope queries will be rejected if not logged in due to the requirement to pull resources from a specific user. Because of this, *User* and *Group* scopes will not be functional until the Security Framework is merged into the mainline.

Where *Plugin* is the broadest scope and *User* is the narrowest scope.

When you specify *Scope User*, the service manages configuration for your particular username, using the authentication of the session. This way, the *User* scope is always mapped to your current username.

Consider a case where a user wants to access preferences for their text editor. One way they could do this is to use the REST API to retrieve the settings resource from the *Instance* scope.

The *Instance* scope might contain editor defaults set by the administrator. But, if there are no defaults in *Instance*, then the data in *Group* and *User* would be checked.

Therefore, the data the user receives would be no broader than what is stored in the *Instance* scope, but might have only been the settings they saved within their own *User* scope (if the broader scopes do not have data for the resource).

Later, the user might want to save changes, and they try to save them in the *Instance* scope. Most likely, this action will be rejected because of the preferences set by the administrator to disallow changes to the *Instance* scope by ordinary users.

# **REST API**

When you reach the Configuration Service through a REST API, HTTP methods are used to perform the desired operation.

The HTTP URL scheme for the configuration dataservice is:

```
<Server>/plugins/com.rs.configjs/services/data/<plugin
ID>/<Scope>/<resource>/<optional subresources>?<query>
```

Where the resources are one or more levels deep, using as many layers of subresources as needed.

Think of a resource as a collection of elements, or a directory. To access a single element, you must use the query parameter "name="

### **REST query parameters**

Name (string)

Get or put a single element rather than a collection.

```
Recursive (boolean)
```

When performing a DELETE, specifies whether to delete subresources too.

Listing (boolean)

When performing a GET against a resource with content subresources, <code>listing=true</code> will provide the names of the subresources rather than both the names and contents.

## **REST HTTP methods**

Below is an explanation of each type of REST call.

Each API call includes an example request and response against a hypothetical application called the "code editor".

### GET

GET /plugins/com.rs.configjs/services/data/<plugin>/<scope>/<resource>?name= <element>

• This returns JSON with the attribute "content" being a JSON resource that is the entire configuration that was requested. For example:

/plugins/com.rs.configjs/services/data/org.openmainframe.zowe.codeeditor/user
/sessions/default?name=tabs

The parts of the URL are:

- Plugin: org.openmainframe.zowe.codeeditor
- Scope: user
- Resource: sessions
- Subresource: default
- Element = tabs

The response body is a JSON config:

### GET /plugins/com.rs.configjs/services/data/<plugin>/<scope>/<resource>

This returns JSON with the attribute **content** being a JSON object that has each attribute being another JSON object, which is a single configuration element.

GET /plugins/com.rs.configjs/services/data/<plugin>/<scope>/<resource>

(When subresources exist.)

This returns a listing of subresources that can, in turn, be queried.

### PUT

PUT /plugins/com.rs.configjs/services/data/<plugin>/<scope>/<resource>?name= <element>

Stores a single element (must be a JSON object {...}) within the requested scope, ignoring aggregation policies, depending on the user privilege. For example:

/plugins/com.rs.configjs/services/data/org.openmainframe.zowe.codeeditor/user/ses
sions/default?name=tabs

Body:

Response:

#### DELETE

DELETE /plugins/com.rs.configjs/services/data/<plugin>/<scope>/<resource>?
recursive=true

Deletes all files in all leaf resources below the resource specified.

DELETE /plugins/com.rs.configjs/services/data/<plugin>/<scope>/<resource>?name= <element>

Deletes a single file in a leaf resource.

DELETE /plugins/com.rs.configjs/services/data/<plugin>/<scope>/<resource>

- Deletes all files in a leaf resource.
- Does not delete the directory on disk.

# Administrative access and group

By means not discussed here, but instead handled by the server's authentication and authorization code, a user might be privileged to access or modify items that they do not own.

In the simplest case, it might mean that the user is able to do a PUT, POST, or DELETE to a level above User, such as *Instance*.

The more interesting case is in accessing another user's contents. In this case, the shape of the URL is different. Compare the following two commands:

GET /plugins/com.rs.configjs/services/data/<plugin>/user/<resource>

Gets the content for the current user.

GET /plugins/com.rs.configjs/services/data/<plugin>/users/<username>/<resource>

Gets the content for a specific user if authorized.

This is the same structure that is used for the *Group* scope. When requesting content from the *Group* scope, the user is checked to see if they are authorized to make the request for the specific group. For example:

GET /plugins/com.rs.configjs/services/data/<plugin>/group/<groupname>/<resource>

Gets the content for the given group, if the user is authorized.

# **Application API**

Retrieves and stores configuration information from specific scopes.

**Note:** This API should only be used for configuration administration user interfaces.

```
ZLUX.UriBroker.pluginConfigForScopeUri(pluginDefinition: ZLUX.Plugin, scope:
string, resourcePath:string, resourceName:string): string;
```

A shortcut for the preceding method, and the preferred method when you are retrieving configuration information, is simply to "consume" it. It "asks" for configurations using the *User* scope, and allows the configuration service to decide which configuration information to retrieve and how to aggregate it. (See below on how the configuration service evaluates what to return for this type of request).

ZLUX.UriBroker.pluginConfigUri(pluginDefinition: ZLUX.Plugin, resourcePath:string, resourceName:string): string;

# Internal and bootstrapping

Some dataservices within plug-ins can take configuration that affects their behavior. This configuration is stored within the Configuration Dataservice structure, but it is not accessible through the REST API.

Within the instance configuration directory of a zLUX installation, each plugin may optionally have an **\_\_internal** directory. An example of such a path would be:

~/.zowe/workspace/app-server/ZLUX/pluginStorage/<pluginName>/\_internal

Within each \_\_internal directory, the following directories might exist:

- services/<servicename>: Configuration resources for the specific service.
- plugin : Configuration resources that are visible to all services in the plug-in.

The JSON contents within these directories are provided as Objects to dataservices through the dataservice context Object.

# **Packaging Defaults**

The best way to provide default settings for a plugin is to include it as part of the plugin's package. It's easy to distribute to users, requires no configuration steps, and is read-only from the server. To package, all content must be stored within the /config/storageDefaults directory of your plugin. Within, non-leaf resources are folders, and leaf resources are files, regardless of JSON or binary. The \_internal folder and content is also permitted.

# **Plug-in definition**

Because the Configuration Dataservices stores data on a per-plug-in basis, each plug-in must define their resource structure to make use of the Configuration Dataservice. The resource structure definition is included in the plug-in's pluginDefinition.json file.

For each resource and subresource, you can define an aggregationPolicy to control how the data of a broader scope alters the resource data that is returned to a user when requesting a resource from a narrower Scope.

For example:

# **Aggregation policies**

Aggregation policies determine how the Configuration Dataservice aggregates JSON objects from different Scopes together when a user requests a resource. If the user requests a resource from the *User* scope, the data from the User scope might replace or be merged with the data from a broader scope such as *Instance*, to make a combined resource object that is returned to the user.

Aggregation policies are defined by a plug-in developer in the plug-in's definition for the Configuration Service, as the attribute aggregationPolicy within a resource.

The following policies are currently implemented:

- **NONE**: If the Configuration Dataservice is called for *Scope User*, only user-saved settings are sent, unless there are no user-saved settings for the query, in which case the dataservice attempts to send data that is found at a broader scope.
- **OVERRIDE**: The Configuration Dataservice obtains data for the resource that is requested at the broadest level found, and joins the resource's properties from narrower scopes, overriding broader attributes with narrower ones, when found.

# Examples

zlux-app-manager VT Terminal App

# **URI Broker**

The URI Broker is an object in the application plug-in web framework, which facilitates calls to the Zowe™ Application Server by constructing URIs that use the context from the calling application plug-in.

- 1. Accessing the URI Broker
  - i. Natively
  - ii. In an iframe
- 2. Functions
  - i. Accessing App's Dataservices
    - a. HTTP Dataservice URI
    - b. Websocket Dataservice URI
  - ii. Accessing App's Configuration Resources
    - a. Standard Configuration Access
    - b. Scoped Configuration Access
  - iii. Accessing Static Content
  - iv. Accessing the App's Root
  - v. Server Queries
    - a. Accessing List of Plugins

# Accessing the URI Broker

The URI Broker is accessible independent of other frameworks involved such as Angular, and is also accessible through iframe. This is because it is attached to a global when within the Zowe Desktop. For more information, see Zowe Desktop and window management. Access the URI Broker through one of two locations:

Natively:

window.ZoweZLUX.uriBroker

In an iframe:

window.parent.ZoweZLUX.uriBroker
----------------------------------

# Functions

The URI Broker builds the following categories of URIs depending upon what the application plug-in is designed to call.

### Accessing an application plug-in's dataservices

Dataservices can be based on HTTP (REST) or Websocket. For more information, see Dataservices.

#### **HTTP Dataservice URI**

pluginRESTUri(plugin:ZLUX.Plugin, serviceName: string, relativePath:string):
string

Returns: A URI for making an HTTP service request.

### Websocket Dataservice URI

pluginWSUri(plugin: ZLUX.Plugin, serviceName:string, relativePath:string):
string

Returns: A URI for making a Websocket connection to the service.

### Accessing application plug-in's configuration resources

Defaults and user storage might exist for an application plug-in such that they can be retrieved through the Configuration Dataservice.

There are different scopes and actions to take with this service, and therefore there are a few URIs that can be built:

#### Standard configuration access

```
pluginConfigUri(pluginDefinition: ZLUX.Plugin, resourcePath:string,
resourceName?:string): string
```

Returns: A URI for accessing the requested resource under the user's storage.

### **Scoped configuration access**

pluginConfigForScopeUri(pluginDefinition: ZLUX.Plugin, scope: string, resourcePath:string, resourceName?:string): string

Returns: A URI for accessing a specific scope for a given resource.

#### Accessing static content

Content under an application plug-in's web directory is static content accessible by a browser. This can be accessed through:

pluginResourceUri(pluginDefinition: ZLUX.Plugin, relativePath: string): string

Returns: A URI for getting static content.

For more information about the web directory, see Application plug-in filesystem structure.

## Accessing the application plug-in's root

Static content and services are accessed off of the root URI of an application plug-in. If there are other points that you must access on that application plug-in, you can get the root:

pluginRootUri(pluginDefinition: ZLUX.Plugin): string

Returns: A URI to the root of the application plug-in.

#### Server queries

A client can find different information about a server's configuration or the configuration as seen by the current user by accessing specific APIs.

#### Accessing a list of plug-ins

```
pluginListUri(pluginType: ZLUX.PluginType): string
```

Returns: A URI, which when accessed returns the list of existing plug-ins on the server by type, such as "Application" or "all".

# **Application-to-application communication**

Zowe<sup>™</sup> application plug-ins can opt-in to various application framework abilities, such as the ability to have a Logger, the ability to use a URI builder utility, and more.

The ability for one appliccation plug-in to communicate with another is an ability that is unique to Zowe environments with multiple application plug-ins. The application framework provides constructs that facilitate this ability.

The constructs are: the Dispatcher, Actions, Recognizers, Registry, and the features that utilize them such as the framework's Context menu.

- 1. Why use application-to-application communication?
- 2. Actions
- 3. Recognizers
- 4. Dispatcher
- 5. URI Parameters

## Why use application-to-application communication?

When working with computers, people often use multiple applications to accomplish a task. For example, a person might check their email before opening a bank statement in a browser. In many environments, the relationship between one application and another is not well defined. For example, you may open one program to learn of a situation, which is then resolved by opening a different program and typing in content. The application framework attempts to solve this problem by creating structured messages that can be sent from one application plug-in to another.

An application plug-in has a context of the information that it contains. This context can be used to invoke an action on another application plug-in that is better suited to handle some of the information discovered in the first application plug-in. Well-structured messages facilitate the process of determining which application plug-in is best suited to handle a given situation, while also explaining, in detail, what that application plug-in should do.

This way, rather than finding out that an attachment with the extension ".dat" was not meant for a text editor, but rather for an email client, one application plug-in may be able to invoke an action on an application plugin that is capable of opening of an email.

## Actions

To manage communication from one application plug-in to another, a specific structure is needed. In the application framework, the unit of application-to-application communication is an Action. The typescript definition of an Action is as follows:

An Action has a specific structure of data that is passed, to be filled in with the context at runtime, and a specific target to receive the data.

The Action is dispatched to the target in one of several modes, for example: to target a specific instance of an application plug-in, an instance, or to create a new instance.

The Action can be less detailed than a message. It can be a request to minimize, maximize, close, launch, and more. Finally, all of this information is related to a unique ID and localization string such that it can be managed by the framework.

#### Action target modes

When you request an Action on an application plug-in, the behavior is dependent on the instance of the application plug-in you are targeting. You can instruct the framework to target the application plug-in with a target mode from the ActionTargetMode enum:

## **Action types**

The application framework performs different operations on application plug-ins depending on the type of an Action. The behavior can be quite different, from simple messaging to requesting that an application plug-in be minimized. The types are defined by an enum :

## **Loading actions**

Actions can be created dynamically at runtime, or saved and loaded by the system at login.

## App2App via URL

Another way the Zowe Application Framework invokes Actions is via URL Query Parameters, with parameters formatted in JSON. This feature enables users to bookmark a set of application-to-application communication actions (in the form of a URL) that will be executed when opening the webpage. Developers creating separate web apps can build a link that will open the Zowe Desktop and do specific actions in Apps, for example, opening a file in the Editor.

The App2App via URL feature allows you to:

- 1. Specify one or more actions that will be executed upon login, allowing you to bookmark a series of actions that you can share with someone else.
- 2. Specify actions that are declared by plugins (when formatter is equal to a known action ID) or actions that you have custom-made (when formatter = 'data').
- 3. Customize the action type, mode, and target plugin (when the formatter is equal to an existing action ID).

#### Samples

Query parameter format:

?app2app={pluginId}:{actionType}:{actionMode}:{formatter}:{contextData}&app2app=
{pluginId}:{actionType}:{actionMode}:{formatter}:{contextData}

- pluginId application identifier, e.g. 'org.zowe.zlux.ng2desktop.webbrowser'
- actionType 'launch' | 'message'
- actionMode 'create' | 'system'
- formatter 'data' | actionId
- contextData context data in form of JSON
- windowManager 'MVD' | undefined : (Optional) While in standalone mode, controls whether to use the Zowe (MVD) window manager or the deprecated simple window manager. Default is MVD.
- showLogin true | false : (Optional) While in standalone mode, controls whether to show Zowe's login page if credentials are not retrieved from a previous Desktop session, or if to disable it and load the application anyway (ideal solution for apps with their own login experiences). Default is true.

Note that some of these parameters are shared with single app mode, therefore, you may need to adjust pluginId and app2app parameters as follows

(desktop mode)

(single app mode)

## Dynamically

You can create Actions by calling the following Dispatcher method: makeAction(id: string,
defaultName: string, targetMode: ActionTargetMode, type: ActionType,
targetPluginID: string, primaryArgument: any):Action

#### Saved on system

Actions can be stored in JSON files that are loaded at login. The JSON structure is as follows:

## Recognizers

Actions are meant to be invoked when certain conditions are met. For example, you do not need to open a messaging window if you have no one to message. Recognizers are objects within the application framework that use the context that the application plug-in provides to determine if there is a condition for which it makes sense to execute an Action. Each recognizer has statements about what condition to recognize, and when that statement is met, which Action can be executed at that time. The invocation of the Action is not handled by the Recognizer; it simply detects that an Action can be taken.

#### **Recognition clauses**

Recognizers associate a clause of recognition with an action, as you can see from the following class:

A clause, in turn, is associated with an operation, and the subclauses upon which the operation acts. The following operations are supported:

## Loading Recognizers at runtime

You can add a Recognizer to the application plug-in environment in one of two ways: by loading from Recognizers saved on the system, or by adding them dynamically.

#### Dynamically

You can call the Dispatcher method, addRecognizer(predicate:RecognitionClause,
actionID:string):void

#### Saved on system

Recognizers can be stored in JSON files that are loaded at login. The JSON structure is as follows:

clause can take on one of two shapes:

Or,

Where this one can again, have subclauses.

#### **Recognizer example**

Recognizers can be as simple or complex as you write them to be, but here is an example to illustrate the mechanism:

In this case, the Recognizer detects whether it is possible to run the **org.zowe.explorer.openmember** Action when the TN3270 Terminal application plug-in is on the screen ISRUDSM (an ISPF panel for browsing PDS members).

## Dispatcher

The dispatcher is a core component of the application framework that is accessible through the Global ZLUX Object at runtime. The Dispatcher interprets Recognizers and Actions that are added to it at runtime. You can register Actions and Recognizers on it, and later, invoke an Action through it. The dispatcher handles how the Action's effects should be carried out, acting in combination with the Window Manager and application plug-ins to provide a channel of communication.

## Registry

The Registry is a core component of the application framework, which is accessible through the Global **ZLUX** Object at runtime. It contains information about which application plug-ins are present in the environment, and the abilities of each application plug-in. This is important to application-to-application communication, because a target might not be a specific application plug-in, but rather an application plug-in of a specific category, or with a specific featureset, capable of responding to the type of Action requested.

## Pulling it all together in an example

The standard way to make use of application-to-application communication is by having Actions and Recognizers that are saved on the system. Actions and Recognizers are loaded at login, and then later, through a form of automation or by a user action, Recognizers can be polled to determine if there is an Action that can be executed. All of this is handled by the Dispatcher, but the description of the behavior lies in the Action and Recognizer that are used. In the Action and Recognizer descriptions above, there are two

JSON definitions: One is a Recognizer that recognizes when the Terminal application plug-in is in a certain state, and another is an Action that instructs the MVS Explorer to load a PDS member for editing. When you put the two together, a practical application is that you can launch the MVS Explorer to edit a PDS member that you have selected within the Terminal application plug-in.

# **Configuring IFrame communication**

The Zowe Application Framework provides the following shared resource functions through a ZoweZLUX object: pluginManager, uriBroker, dispatcher, logger, registry, notificationManager, and globalization

Like REACT and Angular apps, IFrame apps can use the ZoweZLUX object to communicate with the framework and other apps. To enable communication in an IFrame app, you must add the following javascript to your app, for example in your index.html file:

logger.js is the javascript version of logger.ts and is capable of the same functions, including access to the Logger and ComponentLogger classes. The Logger class determines the behavior of all the ComponentLoggers created from it. ComponentLoggers are what the user implements to perform logging.

If rame-adapter.js is designed to mimic the ZoweZLUX object that is available to apps within the virtual-desktop, and serves as the middle-man for communication between IFrame apps and the Zowe desktop.

You can see an implementation of this functionality in the sample IFrame app.

The version of ZoweZLUX adapted for IFrame apps is not complete and only implements the functions needed to allow the Sample IFrame App to function. The notificationManager, logger, globalization, dispatcher, windowActions, windowEvents, and viewportEvents are fully implemented. The pluginManager and uriBroker are only partially implemented. The registry is not implemented.

Unlike REACT and Angular apps, in IFrame apps the ZoweZLUX and initialization objects communicate with Zowe using the browser's onmessage and postmessage APIs. That means that communication operations are asynchronous, and you must account for this in your app, for example by using Promise objects and await or then functions.

Version: v1.25.x LTS

## **Error reporting UI**

The **zLUX Widgets** repository contains shared widget-like components of the Zowe<sup>™</sup> Desktop, including Button, Checkbox, Paginator, various pop-ups, and others. To maintain consistency in desktop styling across all applications, use, reuse, and customize existing widgets to suit the purpose of the application's function and look.

Ideally, a program should have little to no logic errors. Once in a while a few occur, but more commonly an error occurs from misconfigured user settings. A user might request an action or command that requires certain prerequisites, for example: a proper ZSS-Server configuration. If the program or method fails, the program should notify the user through the UI about the error and how to fix it. For the purposes of this discussion, we will use the Workflow application plug-in in the <code>zlux-workflow</code> repository.

## ZluxPopupManagerService

The ZluxPopupManagerService is a standard popup widget that can, through its reportError() method, be used to display errors with attributes that specify the title or error code, severity, text, whether it should block the user from proceeding, whether it should output to the logger, and other options you want to add to the error dialog. ZluxPopupManagerService uses both ZluxErrorSeverity and ErrorReportStruct.

## ZluxErrorSeverity

ZluxErrorSeverity classifies the type of report. Under the popup-manager, there are the following types: error, warning, and information. Each type has its own visual style. To accurately indicate the type of issue to the user, the error or pop-up should be classified accordingly.

## ErrorReportStruct

ErrorReportStruct contains the main interface that brings the specified parameters of reportError() together.

## Implementation

Import ZluxPopupManagerService and ZluxErrorSeverity from widgets. If you are using additional services with your error prompt, import those too (for example, LoggerService to print to the logger or GlobalVeilService to create a visible semi-transparent gray veil over the program and pause background tasks). Here, widgets is imported from node\_modules\@zlux\ so you must ensure zLUX widgets is used in your package-lock.json or package.json and you have run npm install.

import { ZluxPopupManagerService, ZluxErrorSeverity } from '@zlux/widgets';

#### Declaration

Create a member variable within the constructor of the class you want to use it for. For example, in the Workflow application plug-in under \zlux-workflow\src\app\app\zosmf-serverconfig.component.ts is a ZosmfServerConfigComponent class with the pop-up manager service variable. To automatically report the error to the console, you must set a logger.

#### Usage

Now that you have declared your variable within the scope of your program's class, you are ready to use the method. The following example describes an instance of the reload() method in Workflow that catches an error when the program attempts to retrieve a configuration from a configService and set it to the program's this.config. This method fails when the user has a faulty zss-Server configuration and the error is caught and then sent to the class' popupManager variable from the constructor above.

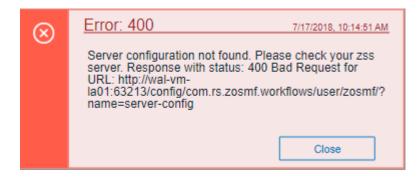
Here, the errorMessage clearly describes the error with a small degree of ambiguity as to account for all types of errors that might occur from that method. The specifics of the error are then generated dynamically and are printed with the err.toString(), which contains the more specific information that is used to pinpoint the problem. The this.popupManager.report() method triggers the error prompt to display. The error severity is set with ZluxErrorSeverity.ERROR and the err.status.toString() describes the status of the error (often classified by a code, for example: 404). The optional parameters in options specify that this error will block the user from interacting with the application plug-in until the error is closed or it until goes away on its own. globalVeilService is optional and is used to create a gray veil on the outside of the program when the error is caused. You must import globalVeilService separately (see the zlux-workflow repository for more information).

## HTML

The final step is to have the recently created error dialog display in the application plug-in. If you do this.popupManager.report() without adding the component to your template, the error will not be displayed. Navigate to your component's .html file. On the Workflow application plug-in, this file will be in \zlux-workflow\src\app\app\zosmf-server-config.component.html and the only item left is to add the popup manager component alongside your other classes.

```
<zlux-popup-manager></zlux-popup-manager>
```

So now when the error is called, the new UI element should resemble the following:



The order in which you place the pop-up manager determines how the error dialog will overlap in your UI. If you want the error dialog to overlap other UI elements, place it at the end of the .html file. You can also create custom styling through a CSS template, and add it within the scope of your application plug-in.

# Logging utility

The zlux-shared repository provides a logging utility for use by dataservices and web content for an application plug-in.

- 1. Logging Objects
- 2. Logger IDs
- 3. Accessing Logger Objects
  - i. Logger
    - a. App Server
    - b. Web
  - ii. Component Logger
    - a. App Server
    - b. Web
- 4. Logger API
- 5. Component Logger API
- 6. Log Levels
- 7. Logging Verbosity
  - i. Configuring Logging Verbosity
    - a. Server Startup Logging Configuration
- 8. Using log message IDs

## Logging objects

The logging utility is based on the following objects:

- **Component Loggers**: Objects that log messages for an individual component of the environment, such as a REST API for an application plug-in or to log user access.
- **Destinations**: Objects that are called when a component logger requests a message to be logged. Destinations determine how something is logged, for example, to a file or to a console, and what formatting is applied.
- Logger: Central logging object, which can spawn component loggers and attach destinations.

## Logger IDs

Because Zowe<sup>™</sup> application plug-ins have unique identifiers, both dataservices and an application plug-in's web content are provided with a component logger that knows this unique ID such that messages that are logged can be prefixed with the ID. With the association of logging to IDs, you can control verbosity of logs by setting log verbosity by ID.

## Accessing logger objects

#### Logger

The core logger object is attached as a global for low-level access.

#### App Server

NodeJS uses global as its global object, so the logger is attached to: global.COM\_RS\_COMMON\_LOGGER

#### Web

Browsers use window as the global object, so the logger is attached to: window.COM\_RS\_COMMON\_LOGGER

## **Component logger**

Component loggers are created from the core logger object, but when working with an application plug-in, allow the application plug-in framework to create these loggers for you. An application plug-in's component logger is presented to dataservices or web content as follows.

#### App Server

See Router Dataservice Context in the topic Dataservices.

#### Web

(Angular App Instance Injectible). See Logger in Zowe Desktop and window management.

## Logger API

The following constants and functions are available on the central logging object.

Attribute	Туре	Description	Arguments
makeComponentLogger	function	Returns an existing logger of this name, or creates a new component logger if no logger of the specified name exists - Automatically done by the application framework for dataservices and web content	componentIDString
setLogLevelForComponentName	function	Sets the verbosity of an existing component logger	<pre>componentIDString, logLevel</pre>

## **Component Logger API**

The following constants and functions are available to each component logger.

Attribute	Туре	Description	Arguments
CRITICAL	const	Is a const for logLevel	
SEVERE	const	Is a const for logLevel	
WARN	const	Is a const for logLevel	
WARNING	const	Is a const for logLevel	
INFO	const	Is a const for logLevel	

Attribute	Туре	Description	Arguments
DEBUG	const	Is a const for logLevel	
FINE	const	Is a const for logLevel	
FINER	const	Is a const for logLevel	
TRACE	const	Is a const for logLevel	
FINEST	const	Is a const for logLevel	
log	function	Used to write a log, specifying the log level	logLevel, messageString
critical	function	Used to write a CRITICAL log.	messageString
severe	function	Used to write a SEVERE log.	messageString
warn	function	Used to write a WARNING log.	messageString
info	function	Used to write an INFO log.	messageString
debug	function	Used to write a FINE log.	messageString
trace	function	Used to write a TRACE log.	messageString
makeSublogger	function	Creates a new component logger with an ID appended by the string given	componentNameSuffix

## Log Levels

An enum, LogLevel, exists for specifying the verbosity level of a logger. The mapping is:

Level Number

Level	Number	
CRITICAL	0	
WARNING	1	
INFO	2	
DEBUG	3	
FINER	4	
TRACE	5	

Note: The default log level for a logger is INFO.

## Logging verbosity

Using the component logger API, loggers can dictate at which level of verbosity a log message should be visible. You can configure the server or client to show more or less verbose messages by using the core logger's API objects.

Example: You want to set the verbosity of the org.zowe.foo application plug-in's dataservice, bar to show debugging information.

```
logger.setLogLevelForComponentName('org.zowe.foo.bar',LogLevel.DEBUG)
```

#### **Configuring logging verbosity**

The application plug-in framework provides ways to specify what component loggers you would like to set default verbosity for, such that you can easily turn logging on or off.

#### Server startup logging configuration

The server configuration file allows for specification of default log levels, as a top-level attribute logLevel, which takes key-value pairs where the key is a regex pattern for component IDs, and the value is an integer for the log levels.

For example:

For more information about the server configuration file, see Zowe Application Framework (zLUX) configuration.

## Using log message IDs

To make technical support for your application easier, create IDs for common log messages and use substitution to generate them. When you use IDs, people fielding support calls can identify and solve problems more quickly. IDs are particularly helpful if your application is translated, because it avoids users having to explain problems using language that the tech support person might not understand.

To use log message IDs, take the following steps:

- 1. Depending on how your application is structured, create message files in the following locations:
  - Web log messages: {plugin}/web/assets/i18n/log/messages\_{language}.json
  - App server log messages: {plugin}/lib/assets/i18n/log/messages\_{language}.json
- 2. In the files, create ID-message pairs using the following format:

Where "id#" is the message ID and "value#" is the text. For example:

3. Reference the IDs in your code, for example:

Which compiles to:

Or in another supported language, such as Russian:

#### Message ID logging examples

Server core: https://github.com/zowe/zlux-serverframework/blob/master/plugins/config/lib/assets/i18n/log/messages\_en.json

# Using Conda to make and manage packages of Application Framework Plugins

As Zowe is composed of components which can be extended by Plugins, a standardized and simple way to find, install, upgrade, and list Plugins in your Zowe environment is important to make it easy to get the most out of Zowe.

Package management as a concept generally provides a way to find packages such as plugins, check and possible co-install dependencies the package has, and ultimately install the desired package. Post-install, management tasks such as upgrading and uninstalling are common.

Conda is one such package manager, and if you are familiar with apt, yum, or npm, you will find that using Conda is very similar. But, there are some important abilities that make Conda stand out:

- Very cross platform: Conda is available, and acts very similar on z/OS, Windows, Linux, macOS, and various Unix. Packages can state which platforms they support, so it easy to know what packages you can install.
- Tagging: On z/OS, Conda packages can contain tagging information, to avoid issues around the difference between EBCDIC & ASCII.
- Software neutrality: Language-specific package managers are becoming popular, but Conda does not assume the purpose of the package, so you can install almost anything.
- Environments: If desired, every user can have a different set of packages, because Conda can install & manage packages in personal folders instead of system ones. A user can even have multiple such environments, and switch between them rapidly to work with different sets of related software without conflict.

## **Initial Conda setup**

If you have not installed Conda yet, it can be downloaded as an all-in-one package that has no extra dependencies, known as "miniconda". For Linux, Unix, macOS, and Windows, this can be downloaded at https://docs.conda.io/en/latest/miniconda.html For z/OS, Conda can be downloaded from Rocket Software at https://www.rocketsoftware.com/zos-open-source

Conda will prompt during the install for certain setup options, and ultimately you'll want to put some Conda initialization content into your startup script so that whenever you open your terminal, Conda will be ready

for your use.

Once you have Conda downloaded and installed, you'll want to create your first Conda "environment" this can be done by providing a path or a nickname

conda create --prefix PATH conda create --name ENVIRONMENT

Either will work, but path helps you better separate your content from content others use by placing it in a folder that you can have stricter permissions on.

If you need to know more about certain commands, you can use the help command for any.

conda create --help

Or, check the official documentation: https://docs.conda.io/en/latest/index.html

Once you have an environment, you should activate it so that the actions you do are on that environment, as opposed to the base one.

#### conda activate PATH\_OR\_NAME

Conda will detect whether the parameter is a path or a nickname, so this command works for both.

Finally, you can view the Conda environment and other information by checking "info"

conda info

## **Managing Conda channels**

When downloading a package, such as a Zowe Plugin, the place that you download from is configurable. These are called "Channels", but are very similar to "Repositories" seen in other package managers. With Conda, you can install from:

- A network channel (Internet or company internal)
- A local channel (Collection of plugins on your computer)
- Just an individual package, without a channel

You can have multiple of each, and if a package is present in more than one location, you can specify which one to use.

## **Searching for packages**

Conda has a search utility that searches for all Channels,

```
conda search anything_you_want
```

but it's important to note that because any type of software can be installed through Conda, you probably want to search through a detailed view to help identify which ones are meant for Zowe, or use Channels that are distinctly for Zowe so that you can get packages that are strictly for Zowe.

conda search --info anything\_you\_want

## **Using Conda with Zowe**

Zowe is not yet available in the form of Conda packages yet, so it must be installed separately. If you have Zowe installed on the same system as Conda, some Zowe Plugins installed through Conda will automatically register into Zowe. In order to do this, the Plugins must be able to find Zowe. You should set environment variables before trying to install the Plugins:

## Setting environment variables temporarily:

z/OS, Linux, Unix:

Windows cmd.exe:

**INSTANCE\_DIR** and **R00T\_DIR** are also supported, but the **Z0WE\_** prefix helps distinguish its purpose.

#### Setting environment variables persistently

z/OS, Linux, Unix: You can put the export statements into the .profile file in your home directory to have them apply on login.

Windows: There is a UI to set variables, but it varies depending on Windows version. Try typing 'environment variable' into the Windows search bar to get to the relevant menu.

#### Installing a Zowe plugin

A Conda package could contain one or more Zowe Plugins, and a Conda package could contain non-Zowe code alongside Zowe Plugins. This is left up to the program vendor and regardless the install process is the

same:

conda install package\_name

If the Zowe environment variables are set, such a package may automatically register Plugins into the Zowe instance of your choice.

#### Zowe plugin configuration

Aside from possible automation during install and uninstall, Conda does not manage Zowe, its configuration, or configuration of the Plugins. However, Conda does manage the package files, and therefore you can do additional Zowe tasks on the Plugins by going into the Conda environment. Zowe Plugins are intended to be found in a standardized location in the Conda environment,

#### /opt/zowe/plugins

This folder contains Plugins, which in turn contain sub-folders that are the Zowe components that they utilize. If a plugin uses multiple Zowe components, its contents could be found within multiple component folders.

/opt/zowe/plugins/my\_plugin/app-server /opt/zowe/plugins/my\_plugin/cli

#### Zowe package structure

Zowe Plugins packaged into Conda follow the structure outlined here: https://github.com/zowe/zowe-installpackaging/issues/1569 This structure allows for plugin to have content meant for one or more Zowe components. The Conda packages extend this by allowing for more than one Plugin, or a mix of Zowe Plugins and other software to be within a single package.

## **Building Conda packages for Zowe**

This document is intended to be provided with example scripts by the Zowe community, which shows you how you can build a simple Zowe plugin into a Conda package. You can find the example scripts on the Zowe zlux-build github repository. This is not intended to be a one-size-fits-all set of scripts. If you have more advanced needs, you can use these scripts as a basis for writing your own scripts.

To make a Conda package, you need conda-build, which you can install into a Conda environment:

Once you have it, you can build a package via

conda build path/to/build/scripts

However, first you must set up the build information.

#### **Defining package properties**

Conda needs a metadata file, meta.yaml to state information about the package, such as dependencies, what OS it supports, its name and version. This information can be programmatically found, and Zowe provides examples of how to do this by reading Zowe's own metadata files into this one.

#### **Creating build step**

It's recommended not to build your code from scratch to put into Conda. Rather, build your code however you want, and then just copy the contents into a Conda package. This keeps the Conda scripting small and simple.

In the same folder as meta.yaml, Conda requires build.sh for building on Unix, Linux, or z/OS and build.bat for Windows. Except for z/OS, this script does not determine where your package can be used, it's just about where you are building it. z/OS is the exception because when you build on z/OS, unix file tagging information is preserved. So, it's highly recommended that you tag your files so that users do not have to deal with encoding issues. For code that works equally well on all platforms, a simple way to build for all is:

- 1. Build your code on Linux
- 2. Transfer the output to z/OS
- 3. Run a Conda build on the output on Linux
- 4. Run a Conda build on the output on z/OS
- 5. Deliver the Linux package as 'noarch' content, and the z/OS package as 'zos-z' content.

#### Lifecycle scripts

When a Conda package is installed or uninstalled, a script from the package can be run. For Zowe, the scripts post-link.sh and pre-unlink.sh can be important, and you must put them into the same folder as meta.yaml for building.

#### Install automation

post-link.sh runs at install, after Conda has put the package content onto the system. At this time, registration into Zowe is recommended if the Plugin does not require any information from the user for configuration. If the Plugin is okay to be automatically installed, we recommend putting a script into the package folder named autoinstall.sh Zowe's provided Conda examples will utilize autoinstall.sh to do any install steps your package needs, and provides Zowe information to make install simple. However, it's possible to do what you want in your own post-link.sh script instead.

#### **Uninstall automation**

pre-unlink.sh is the opposite of post-link.sh. It allows you to do anything you need to before the package is removed from the system. This is a good time to remove any package information from Zowe, but you should be careful because users may uninstall and later re-install, so you should not remove configuration information without consent.

#### Adding configuration to Conda packages

As a package manager, Conda is not responsible for configuration. Your packages can include defaults to utilize, but if configuration is needed you should alert the user to perform a post-install task. post-link.sh could be used to print such an alert.

# Creating and adding Zowe extension containers

Zowe extensions such as services and plug-ins that use Zowe component packaging can be used within a Zowe container environment. To do this, the extension component must be delivered as a container image that is compatible with Zowe containers. Following Zowe's container conformance criteria is recommended to make compatibility easy to accomplish and understand.

You can add extension component containers to a Zowe container environment the same way as Zowe's own components.

- 1. Build and publish a component image to a registry.
- 2. Define a deployment object
- 3. Start the component from the deployment.

## 1. Build and publish a component image to a registry

An extension component must have a container image to run in a Zowe container environment.

You can use a Dockerfile to create such images, and can follow some examples of how the Zowe core components are built. The core components define component Dockerfiles and use GitHub Actions to build images. For example, explorer-jes component has a Dockerfile defined at https://github.com/zowe/explorer-jes/blob/master/container/Dockerfile and defines a GitHub Actions workflow https://github.com/zowe/explorer-jes/blob/master/.github/workflows/explorer-jes-images.yml to build the image.

The following are Actions used by the core components to build conformant images. They may not be completely reusable for extenders, but are provided as an example.

- zowe-actions/shared-actions/docker-prepare will prepare required environment variables used by following steps.
- zowe-actions/shared-actions/docker-build-local can build docker image directory on GitHub Actions virtual machine. By default it will be ubuntu-latest. This action can be used to build image for amd64 CPU architecture.

- zowe-actions/shared-actions/docker-build-zlinux can build docker image on a Linux on Z virtual machine. This is useful if you want to build image for s390x CPU architecture.
- zowe-actions/shared-actions/docker-manifest can collect all related images and define them as docker manifests. This is useful for end user to automatically pull the correct image based on cluster node CPU architecture, and also pull images based on popular tags like latest and latest-ubuntu.

Once a component image is built, you must publish it to a container registry before it can be added to the Zowe container environment.

## 2. Define Deployment object

To start your component in Kubernetes, you need to define a Deployment object. To define Deployment for your component, you can copy from samples/sample-deployment.yaml and modify all occurrences of the following variables:

- <my-component-name> : this is your component name. For example, sample-node-api.
- <my-component-image>: this is your component image described in the above section. For example, zowe-docker-release.jfrog.io/ompzowe/sample-node-api:latest-ubuntu.
- <my-component-port> : this is the port of your service. For example, 8080.

Continue to customize the specification to fit in your component requirements:

- spec.replicas : defines how many pods you want to start for your component,
- spec.template.spec.containers[0].resources : defines the memory and CPU resource required to start the container,
- metadata.annotations, spec.template.spec.volumes and spec.template.spec.securityContext and so on.

## 3. Start your component

After you define your component Deployment object, you can run kubectl apply -f /path/to/your/component-deployment.yaml to apply it to Kubernetes cluster that runs Zowe.

Now you can follow common Kubernetes practice to manage your component workload.

# **Extending Zowe Explorer**

You can extend the possibilities of Zowe Explorer by creating you own extensions. For more information on how to create your own Zowe Explorer extension, see Extensions for Zowe Explorer.

# **Developing for Zowe SDKs**

The Zowe SDKs are open source. You can contribute to add features, enhancements, and bug fixes to the source code.

The functionality is currently limited to the interfaces provided by IBM z/OSMF. As a plug-in developer, you can enhance the SDK by creating a packages that exposes programmatic APIs for your service.

For detailed contribution guidelines, see the following documents:

- Node.js SDK guidelines
- Coming soon! Python SDK guidelines

Version: v1.25.x LTS

# **Zowe Conformance Program**

## Introduction

Administered by the Open Mainframe Project, the Zowe™ Conformance Program aims to give users the confidence that when they use a product, app, or distribution that leverages Zowe, they can expect a high level of common functionality, interoperability, and user experience.

Conformance provides Independent Software Vendors (ISVs), System Integrators (SIs), and end users greater confidence that their software will behave as expected. Just like Zowe, the Zowe Conformance Program will continue to evolve and is being developed by committers and contributors in the Zowe community.

As vendors, you are invited to submit conformance testing results for review and approval by the Open Mainframe Project. If your company provides software based on Zowe, you are encouraged to get certified today.

## How to participate

To participate in the Zowe Conformance Program, follow the process on the Zowe Conformance Program website. You can also find a list of products that have earned Zowe Conformant status.

To learn the criteria of achieving Zowe conformance for an offering, see Zowe Conformance Criteria.

# How to suggest updates to the Zowe conformance program

The Zowe conformance criteria is available as a table in a Markdown file in the Open Mainframe Project's GitHub repo. If you find a mistake with the Zowe conformance documents, or you are a Zowe squad lead and want to make an amendment to the criteria, you can update that Markdown file. The same information is also held in another document Zowe Conformance Test Evaluation Guide that has history going back to Zowe 2019 conformance and allows easy change history comparison.

To submit a proposal to update the conformance criteria, fork the OMP's foundation repository at https://github.com/openmainframeproject/foundation and make a pull request. Flag the Pull Request to the attention of GitHub user ID @mertic, and also reach out to the Zowe onboarding squad in the #zowe-onboarding Slack channel. If you are not already signed up to Zowe Slack community, you can sign up at https://slack.openmainframeproject.org first.

## Troubleshooting

To isolate and resolve Zowe™ problems, you can use the troubleshooting and support information.

## **Known problems and solutions**

Some common problems with Zowe are documented, along with their solutions or workarounds. If you have a problem with Zowe installation and components, review the problem-solution topics to determine whether a solution is available to the problem that you are experiencing.

You can also find error messages and codes, must-gathers, and information about how to get community support in these topics.

- Troubleshooting Zowe z/OS component installation
- Troubleshooting API Mediation Layer
- Troubleshooting Zowe Application Framework
- Troubleshooting z/OS Services
- Troubleshooting Zowe CLI
- Troubleshooting Zowe Launcher

## **Collecting data for Zowe problems**

Sometimes you cannot solve a problem by troubleshooting the symptoms. In such cases, you must collect diagnostic data. To collect diagnostic data about Zowe, see Capturing diagnostics to assist problem determination.

## Verifying a Zowe release's integrity

Following a successful install of a Zowe release, the Zowe runtime directory should contain the code needed to launch and run Zowe. If the contents of the Zowe runtime directory have been modified then this may result in unpredictable behavior. To assist with this Zowe provides the ability to validate the integrity of a Zowe runtime directory, see Verify Zowe runtime directory

## **Understanding the Zowe release**

Knowing which version of Zowe you are running might help you isolate the problem. Also, the Zowe community who helps you will need to know this information. For more information, see Understanding the Zowe release.

Version: v1.25.x LTS

# **Understanding the Zowe release**

## **Zowe releases**

Zowe uses semantic versioning for its releases, also known as SemVer. Each release has a unique ID made up of three numbers that are separated by periods.

Each time a new release is created, the release ID is incremented. Each number represents the content change since the previous release. For example,

- **1.5.0** represents the fifth minor release since the first major release.
- 1.5.1 represents the first patch to the 1.5.0 release.
- 1.6.0 is the first minor release to be created after 1.5.1.

## Patch

A patch is usually reserved for a bug fix to a minor release.

#### **Minor release**

A minor release indicates that new functionality is added but the code is compatible with an earlier version. The Zowe community works on two-week sprints and creates a minor release at the end of these, typically once per month although the frequency might vary.

#### **Major release**

A major release is required if changes are made to the public API and the code is no longer compatible with an earlier version.

When Zowe is version one, it is associated with the Zowe v1 conformance program. Offerings that extend Zowe and achieve the Zowe v1 conformance badge will remain compatible with Zowe throughout its version 1 lifetime. A major release increment because of incompatibility is sometimes referred to as a "breaking" change.

The first SMP/E build for Zowe v1 has a Functional Module ID (FMID) of AZWE001, which was created with content from the 1.9.0 release. Each major release will be its own SMP/E FMID where the last digit is updated, for example AZWE00V where V represents the major version.

Subsequent minor and patch releases to V1 are delivered as SMP/E PTF SYSMODs. Because of the size of the content, two co-requisite PTFs are created for each Zowe release.

While Major releases are required for a "breaking" change, they also can be used to indicate to the community a significant content update over and above what would be included in a minor release.

## Check the Zowe release number

To see the release number of Zowe, look at the manifest.json file. This is included in the top-level directory of where a Zowe convenience build is expanded to, the top-level directory of a Zowe runtime <RUNTIME\_DIR>, and the Zowe instance directory <INSTANCE\_DIR>/workspace.

To see the version of a Zowe release, use the Unix grep command in a directory that contains a manifest.json file.

will return a single line with the Zowe release number. For example,

# Capturing diagnostics to assist problem determination

To help Zowe<sup>™</sup> Open Community effectively troubleshoot Zowe, a shell script zowe-support.sh captures diagnostics data that is required for successful problem determination. By running the shell script on your z/OS environment, you receive a set of output files, which contain all relevant diagnostics data necessary to start a troubleshooting process. You can find the zowe-support.sh script in the <INSTANCE\_DIRECTORY>/bin directory. To determine the <INSTANCE\_DIRECTORY> for a Zowe started task, open the JESJCL step in the ZWESVSTC task and navigate to the line including //STARTING EXEC ZWESVSTC, INSTANCE=. The <INSTANCE\_DIRECTORY>/bin/zowe-support.sh script captures the following data:

- Started task output
  - Zowe server started task
  - Zowe Cross Memory started task (STC)

**Note:** You will need to install the TSO exit IKJEFF53 to permit the TSO OUTPUT command to collect the Zowe started task output. If this exit is not enabled, you will see an error message when you run zowe-support.sh:

For how to correct this error, see the TSO/E installation exit IKJEFF53 topic in IBM Knowledge Center.

The above is the authoritative description, and will be the first to reflect changes. To assist you, a summary of the situation and actions you could take to allow TSO OUTPUT to work in your installation are provided in IKJ56328I JOB job name REJECTED.

- Zowe Install log
- Scripts that are called from run-zowe.sh
- Versions:
  - manifest.json
  - z/OS version
  - Java version
  - Node version

- Additional logs
  - Zowe app server
  - zLUX app server
- Process list with CPU info with the following data points:
  - Running command and all arguments of the command
  - Real time that has elapsed since the process started
  - Job name
  - Process ID as a decimal number
  - Parent process ID as a decimal number
  - Processor time that the process used
  - Process user ID (in a form of user name if possible, or as a decimal user ID if not possible)

## Running the diagnostic support script

To run the zowe-support.sh script, issue the following commands:

where the -l optional parameter points to the custom directory supplied during the installation and setup scripts (zowe-install.sh, zowe-setup-certificates.sh, zowe-install-xmem.sh, zowe-install-proc.sh) if applicable.

## Problems that may occur running the diagnostic script

## IKJ56328I JOB job name REJECTED

**Audience:** Zowe users or the personnel who collects support logs. These individuals should also inform their z/OS system programmer.

The zowe-support.sh script collects logs that your support team needs to assist you with problem determination. One of the logs it collects is the JES job log for Zowe tasks. The zowe-support.sh script uses the TSO OUTPUT command to collect these logs. On an unmodified z/OS system, the TSO OUTPUT command is restricted to jobs starting with your user ID, and the Zowe tasks will typically have a different job name. You will know that the TSO OUTPUT command is restricted if you see the following message when you issue the TSO OUTPUT command for a job whose job name does not start with your user ID.

Job name filtering is controlled by an exit that is called by the TSO OUTPUT command. The exit is named IKJEFF53. IBM provides the source code for a replacement exit that can remove this restriction in

SYS1.SAMPLIB(IKJEFF53) which you can tailor and use instead. Review this exit and if it meets your needs, assemble it and replace it in your LINKLIB concatenation.

**Warning:** You are strongly advised to take great care before attempting to modify LINKLIB directly. You could easily corrupt your entire z/OS system and require an IPL or reinstallation of z/OS. Consult your system programmer before you continue. You should also read the TSO/E installation exit IKJEFF53 topic in the IBM Knowledge Center.

The original exit load module has the following attributes:

The replacement exit load module has the following attributes when assembled and linked:

It is safer to add a module to a private dataset further down the LINKLIST concatenation than to modify SYS1.LINKLIB directly. You can display the LINKLIST with this command at the operator console

The private dataset or the exit itself does not have to be APF-authorized.

Whichever library you choose, rename IKJEFF53 in SYS1.LINKLIB (or its first occurrence in the LINKLIST concatenation) and add the assembled load module IKJEFF53 to your chosen library.

To activate your changes, refresh the link-list lookaside list with this command

Now your TSO OUTPUT command will work as described in SYS1.SAMPLIB(IKJEFF53).

Note that this change will affect all users of the TSO OUTPUT command on LPARS sharing the SYS1.LINKLIB dataset. It is not limited to Zowe users. Consult your system programmer to ensure that this change does not impact your site rules about the OUTPUT command, because the specified jobs will be PURGED from the JES output queue if this exit is implemented as described above.

# Verify Zowe runtime directory

The Zowe runtime directory **RUNTIME\_DIR** contains the code modules that make up Zowe. If these code modules are altered in any way, the behavior of Zowe is unpredictable. To check if the **RUNTIME\_DIR** has been altered, Zowe provides a verify tool that comprises a script file <code>zowe-verify-authenticity.sh</code> and the files it needs to check the release contents.

You can use this verify tool on Zowe version 1.9 and later.

- If you use Zowe version 1.14 or later, the verify tool is delivered with Zowe, so you can skip Step 1 below, but you can still download the verify tool if required.
- If you use Zowe version 1.9, 1.10, 1.11, 1.12, and 1.13, you must obtain the verify tool separately and use it to verify the **RUNTIME\_DIR**.

#### **Contents in this topic**

- Step 1: Obtain the verify tool (Required for versions before v1.14)
- Step 2: Verify your runtime directory
- Step 3: Review results
  - Mismatch
  - Match
- zowe-verify-authenticity.sh parameters
- Use of zowe-verify-authenticity.sh by zowe-support.sh

# Step 1: Obtain the verify tool (Required for versions before v1.14)

- 1. Start a USS terminal session with the z/OS system where Zowe is installed.
- 2. Create a new, writable, local directory, for example, /u/username/hash.
- 3. Go to the download link to download the fingerprint.pax PAX file.
- 4. Upload the downloaded file to a temporary directory such as **/tmp** on your z/OS USS file system by using SFTP or a similar file transfer utility. When you transfer the PAX file between systems, you must

use binary transfer mode.

- 5. Extract the PAX file from inside the local directory you created (in this example, it is /u/username/hash) using commands like the following one:
- 6. When the PAX file is extracted, you will see the following files in your /u/username/hash directory:
  - HashFiles.class (binary)
  - RefRuntimeHash-1.9.0.txt (text)
  - RefRuntimeHash-1.10.0.txt (text)
  - RefRuntimeHash-1.11.0.txt (text)
  - RefRuntimeHash-1.12.0.txt (text)
  - RefRuntimeHash-1.13.0.txt (text)
  - zowe-verify-authenticity.sh (text)

Each RefRuntimeHash-V.v.p.txt file is specific to a Zowe release, where V.v.p is your Zowe release number, for example, 1.9.0. This list of files is updated to include new Zowe releases as they become available. For example, if you use Zowe version 1.14, you will see RefRuntimeHash-1.14.0.txt in the list.

# Step 2: Verify your runtime directory

Now you are ready to verify your runtime directory **RUNTIME\_DIR**, for example,

/usr/lpp/zowe/v1.14, which contains the following files. You can show these files by using the ls command.

Note that you will not have a fingerprint directory in releases prior to v1.14.0.

- 1. Change to the runtime directory.
- 2. Run the zowe-verify-authenticity.sh script.

The script will automatically choose the correct **RefRuntimeHash-V.v.p.txt** file that matches the release found in your runtime directory.

#### For Zowe v1.14 and later

Issue the following command. You do not need to specify any parameters to this script.

If you suspect that the versions of the files in RUNTIME\_DIR have been altered since this version of Zowe was installed, you might want to use the verify tool's script or files which you downloaded instead of the ones in your runtime directory. In this case, you can call the downloaded script and specify the options -f and -h in the following way:

To display a list of parameters, enter this command

### For Zowe releases prior to v1.14

Issue commands similar to the following. In this example, you use Zowe v1.9.

```
The zowe-verify-authenticity.sh script creates a CustRuntimeHash.txt file, which it compares with the RefRuntimeHash-V.v.p.txt file.
```

# **Step 3: Review results**

You will get one of the following results.

- Mismatch
- Match

# Mismatch

When files don't match, you see output similar to the following.

#### **Troubleshooting and hints**

This is a worst-case scenario of a bad mismatch. To find out what the problem is, you could, for example, start by referring to the manifest.json file to see whether one of the components is from the wrong release.

If you have many files different but none missing or extra, you might have a file tagging or code-page problem. Check that the environment variables are set as required according to zowe-set-env.sh.

The hash files mentioned above are left in the /u/username/hash directory in case you want to use a GUI tool to perform a better file comparison.

# Match

When files match, you see output similar to the following.

# zowe-verify-authenticity.sh parameters

Usage:

- All parameters are optional
- You can use dot (.) and tilde (~) in the parameters

Description of parameters:

–r <runtime-dir>

Root directory of the executables used by Zowe at run time. The typical value is /usr/lpp/zowe. The default value is the parent directory of the bin folder where this script is located.

-h <HashPgm-dir>

Directory of the hash key program. The typical value is /usr/lpp/zowe/fingerprint. The default value is the fingerprint directory of the parent folder where this script is located.

–f <HashRef-dir>

Directory of the reference hash key file RefRuntimeHash-V.v.p.txt. The typical value and default value are the same as that of the -h parameter. The values specified for -h and -f can be the same or different.

-l <output-dir>

Output directory where the following log and output files will be written.

The typical value is ~/zowe/fingerprint. The directory will be created if you specify it but it does not exist.

The following defaults will be tried in the listed order:

# Use of zowe-verify-authenticity.sh by zowe-support.sh

Starting in Zowe v1.14, the zowe-verify-authenticity.sh script is automatically called, with no parameters, by zowe-support.sh.

# Troubleshooting installation and startup of Zowe z/OS components

The following topics contain information that can help you troubleshoot problems when you encounter unexpected behavior installing Zowe z/OS components or starting Zowe's ZWESVSTC started task.

# How to check if ZWESVSTC startup is successful

The ZWESVSTC started task on z/OS brings up a number of address spaces. There is no single **Zowe has launched and is ready to run** message as the sequence of address spaces initialization is environmentdependent, although the message ID ZWED0021I is typically the last one that is logged. More details on each subsystem and their startup messages are described in the following sections.

- Check the startup of API Mediation Layer
- Check the startup of Zowe Desktop
- Check the startup of Zowe File and Jobs API servers
- Check the startup of Zowe Secure Services

To check that Zowe has started successfully, the most complete way is to check that each component successfully completed its initialization. Each component writes messages to the JES **STDOUT** and writes severe errors to the **STDERR** job spool file.

To learn more about the Zowe components and their role, see Zowe Architecture. It is possible to configure Zowe to bring up only a subset of its components by using the LAUNCH\_COMPONENT\_GROUPS variable in the instance.env file. See Component Groups for more information.

To monitor **ZWESVSTC** to check whether each component has launched successfully, you can use one of the following ways:

- A good approach is to look at the active address spaces by using a command such as DA in SDSF.
   Each address space is named to identify its component, see Address space names.
- You can also look for particular messages in the STDOUT Job spool file.

# Check the startup of API Mediation Layer

The API Mediation Layer has three address spaces: API Catalog ZWE1AC, API Gateway ZWE1AG, and API Discovery ZWE1AD. These might have been changed from their defaults. For more information, see Address space names.

To check whether the API mediation layer is fully initialized, you can look for the ZWEAM000I message. Each component writes a successful startup message ZWEAM000I to the JES as shown below. The message also indicates the CPU of seconds spent. Check that each address space has written this message.

As well as looking for ZWEAM001 in the JES log, you can also log in to the gateway homepage and check the service status indicator. If there is a red or yellow tick beside one of its three services, the components are still starting.

When all services are fully initialized, there will be three green ticks.

# Check the startup of Zowe Desktop

The Zowe Desktop address space is named ZWE1DS1. During its initialization process, the desktop loads its plug-ins and writes a message ZWED00311 when it is completed.

The ZWED00311 message includes a count of the number of loaded plug-ins as well as the total number of plug-ins, for example Plugins successfully loaded: 100% (21/21). A failed plug-in load will not abort the launch of the desktop.

In the preceding message example, it indicates that 21 plug-ins have loaded successfully. Each of these plug-ins writes its individual message ZWED0290I, so ZWED0031I indicates 21 plug-ins have loaded and there will be 21 instances of ZWED0290I, for example:

Messages for ZWED0290I will be written when the JES Explorer org.zowe.explorer-jes, the MVS Explorer org.zowe.explorer-mvs, and the USS Explorer org.zowe.explorer-uss are loaded.

When the Zowe desktop and the API Gateway are both started in a launch configuration, it will register itself with the API Gateway after the Zowe desktop has started. This step must be completed before a user is able to successfully log in, as the API Mediation layer is used as the backing authentication service. The message that is written to indicate that the registration has been successful is ZWED00211, for example

If you try to log into the Zowe desktop too early before the Eureka client registration has occurred you may get an **Authentication failed** message on the login page because the APIML handshake is incomplete. If this occurs wait for the registration to be complete as indiciated by the **ZWED0021I** message.

# Check the startup of Zowe File and Jobs API servers

Zowe has two servers that are used to provide API services for jobs and files. The Jobs API server address space is named ZWE1EF and the Files API server address space is named ZWE1EJ. When these have successfully started, a message Started <name> in <nn> seconds (JVM running for <nn>) is written to the log, for example:

# Check the startup of Zowe Secure Services

The zssServer is used for secure services for the Zowe desktop.

The zssServer will register itself with the cross memory server running under the address space ZWESISTC. You can use the attach message ID ZWES1014I to check that this has occurred successfully. If this message contains a nonzero return code in the cmsRC= value, then a failure occurred. For more information on how to diagnose these, see ZSS server unable to communicate with X-MEM.

# Unable to launch Zowe with { FSUM7351 }

When you run zowe-start.sh from a unix shell path <zowe-instance-directory>/bin, you encounter the following error:

This can be because the value of ROOT\_DIR in the <zowe-instance-directory>/instance.env file is pointing to an invalid Zowe runtime. This can occur in scenarios where the Zowe runtime directory was removed during an upgrade of a convenience build, and the instance.env file's ROOT\_DIR value was not updated to point to the new fully qualified path for the new Zowe runtime.

This errors can also occur if the user ID running <code>zowe-start.sh</code> does not have read and traverse access to the directory tree ancestors of the <code>ROOT\_DIR</code> itself. For example, if <code>ROOT\_DIR</code> is set to <code>/usr/lpp/zowe</code> then the TSO user executing <code>zowe-start.sh</code> must have <code>rx</code> access to the directories <code>usr/lpp/zowe</code>, <code>usr/lpp</code> and <code>usr</code>. To see the access for a directory issue the unix command <code>ls -alT</code>. If you do not wish to open up <code>rx</code> access to the directory tree ancestors of the <code>ROOT\_DIR</code> then Zowe can still be launched using a TSO command, see Starting Zowe with a /S TSO command.

# **Unable to create BPXAS instances**

#### Symptom:

When you start ZWESVSTC started task, either by running the zowe-start.sh script or by launching the started task directly, you encounter the following error in the log:

You will also encounter the following messages in the SYSLOG:

### Solution:

This problem occurs when the maximum number of BPXAS instances have been reached.

This may be because when the Zowe instance directory was created, it was generated in the same location as the Zowe root directory. The Zowe instance directory is created by using the script <a href="mailto:<RUNTIME\_DIR>/bin/zowe-configure-instance.sh-c">C <PATH\_T0\_INSTANCE\_DIR></a>. See Creating an instance directory. The Zowe runtime directory is replaced when new PTFs are applied and should be considered as a read-only set of files. Zowe instance directories are designed to live outside the directory structure and are used to start a Zowe runtime.

This problem will only occur with Zowe drivers prior to v1.10 and has been resolved in v1.10 where the zowe-configure-instance.sh script will report error if it detects the -c argument because the installation directory location is an existing Zowe runtime directory.

# Errors caused when running the Zowe desktop with node 8.16.1

## Symptom:

When you start the ZWESVSTC started task, you encounter the following error messages:

# Solution:

This problem occurs when you use Node.js v8.16.1 which is not supported on Zowe. There is a known issue with node.js v8.16.1 and Zowe desktop encoding. Use a supported version of Node.js instead. For more information, see Supported Node.js versions.

# Cannot start Zowe and UNIX commands not found with FSUM7351

#### Symptom:

When you start the ZWESVSTC started task, you might encounter the following error message:

#### Solution:

Check that /bin is part on your PATH. Do echo \$PATH to check. If it is missing, make sure that it is appended to PATH in your profile, for example, in /etc/profile/.

# Various warnings show when connecting Zowe with another domain

#### Symptoms:

When you configure the Zowe environment variable ZOWE\_EXPLORER\_HOST in instance.env with a domain (for example, domain-a.com), and access Zowe with another domain (for example, domain-b.com), you may see the following errors:

- Certificate warnings similar to the following one:
- No pinned applications show in Zowe Desktop.
- JES Explorer, MVS Explorer, USS Explorer may show errors similar to the following one if you ignore the certificate error.

The above warnings and errors will also show when you plan to use Zowe with multiple domain names.

#### Solutions:

You can take the following steps:

• When you prepare the bin/zowe-setup-certificates.env file, specify the HOSTNAME= and IPADDRESS= parameters to accept multiple domains separated by comma (from Zowe v1.14.0). The following configuration is an example:

Then you can proceed to run the bin/zowe-setup-certificates.sh script.

- After you run the bin/zowe-configure-instance.sh script, modify the instance.env file located in the instance directory in the following ways to reflect the multiple domains you plan to use.
  - Add a line of ZWE\_EXTERNAL\_HOSTS. For example, ZWE\_EXTERNAL\_HOSTS=domaina.com,domain-b.com.
  - Add a line of ZWE\_REFERRER\_HOSTS. For example, ZWE\_REFERRER\_HOSTS=domaina.com,domain-b.com.
  - Find the line that starts with ZOWE\_EXPLORER\_FRAME\_ANCESTORS and modify its values to ZOWE\_EXPLORER\_FRAME\_ANCESTORS="\${ZOWE\_EXPLORER\_HOST}:\*,domaina.com:\*,domain-b.com:\*,\${ZOWE\_IP\_ADDRESS}:\*".

#### Drawback:

With this change, you must use the API Mediation Layer Gateway port (default is 7554) to access Zowe Desktop, for example, <a href="https://domain-a.com:7554/ui/v1/zlux">https://domain-a.com:7554/ui/v1/zlux</a> or <a href="https://domain-b.com:8544/">https://domain-a.com:7554/ui/v1/zlux</a> or <a href="https://domain-b.com:8544/">https://domain-a.com:7554/ui/v1/zlux</a> or <a href="https://domain-b.com:8544/">https://domain-a.com:7554/ui/v1/zlux</a> or <a href="https://domain-b.com:8544/">https://domain-a.com:7554/ui/v1/zlux</a> or <a href="https://domain-b.com:8544/">https://domain-b.com:8544/</a>

is not supported.

# **Troubleshooting Kubernetes environments**

The following topics contain information that can help you troubleshoot problems when you encounter unexpected behavior installing and using Zowe™ containers in a Kubernetes environment.

# ISSUE: /tmp directory is not writable

#### **Problem:**

readOnlyRootFilesystem SecurityContext is enabled by default in Deployment object definition. As a result, /tmp is read-only and not writable to zowe runtime user.

#### **Recommended solution:**

Adjust your component to check the TMPDIR or TMP environment variable to determine location of the temporary directory. Zowe runtime customizes those variables and points them to /home/zowe/instance/tmp directory, which is writable.

#### Alternative solution:

Disabling readOnlyRootFilesystem SecurityContext is not recommended. But you can make /tmp writable by replacing it with a new mounted volume. Here is an example of defining the /tmp volume.

With this added to your Deployment, your component should be able to write to /tmp directory.

# ISSUE: Permission denied showing in pod log

#### **Problem:**

You see error messages similar to the following one in your pod log.

It means zowe user (UID 20000) does not have write permission to your persistent volume. It's very likely the persistent volume is mounted as root user.

#### Solution:

To solve this issue, you can modify workload files with extra initContainers step like this:

# ISSUE: Deployment and ReplicaSet failed to create pod

#### Problem:

If you are using OpenShift and see these error messages in ReplicaSet Events:

That means the Zowe ServiceAccount zowe-sa doesn't have any SecurityContextConstraint attached.

#### Solution:

You can run this command to grant certain level of permission, for example privileged, to zowe-sa ServiceAccount:

### **ISSUE:** Failed to create services

#### Problem:

If you are using OpenShift and apply services, you may see this error:

#### Solution:

To fix this issue, you can simply find and comment out this line in the Service definition files:

With OpenShift, you can define a PassThrough Route to let Zowe handle TLS connections.

# **Troubleshooting API ML**

As an API Mediation Layer user, you may encounter problems with how the API ML functions. This article presents known API ML issues and their solutions.

# **Enable API ML Debug Mode**

Use debug mode to activate the following functions:

- Display additional debug messages for API ML
- Enable changing log level for individual code components

**Important:** We highly recommend that you enable debug mode only when you want to troubleshoot issues. Disable debug mode when you are not troubleshooting. Running in debug mode while operating API ML can adversely affect its performance and create large log files that consume a large volume of disk space.

#### Follow these steps:

- 1. Open the file instance.env.
- 2. Find the line that contains the APIML\_DEBUG\_MODE\_ENABLED= parameter and set the value to true :

By default debug mode is disabled, so the APIML\_DEBUG\_MODE\_ENABLED is set to false.

3. Restart Zowe™.

You enabled debug mode for the API ML core services (API Catalog, API Gateway and Discovery Service).

4. (Optional) Reproduce a bug that causes issues and review debug messages. If you are unable to resolve the issue, create an issue here.

# Change the Log Level of Individual Code Components

You can change the log level of a particular code component of the API ML internal service at run time.

#### Follow these steps:

- 1. Enable API ML Debug Mode as described in Enable API ML Debug Mode. This activates the application/loggers endpoints in each API ML internal service (Gateway, Discovery Service, and Catalog).
- 2. List the available loggers of a service by issuing the GET request for the given service URL:

#### • scheme

Specifies the API ML service scheme (http or https)

#### • hostname

Specifies the API ML service hostname

#### • port

MFS\_DS\_PORT for the Discovery Service (by default, set to gateway port + 1), and MFS\_AC\_PORT for the Catalog (by default, set to gateway port + 2).

**Note:** For the Catalog you can list the available loggers by issuing a GET request for the given service URL in the following format:

**Tip:** One way to issue REST calls is to use the http command in the free HTTPie tool: https://httpie.org/.

#### Example:

- 3. Alternatively, you extract the configuration of a specific logger using the extended **GET** request:
  - {name}

Specifies the logger name

4. Change the log level of the given component of the API ML internal service. Use the POST request for the given service URL:

The POST request requires a new log level parameter value that is provided in the request body:

• level

Specifies the new log level: OFF, ERROR, WARN, INFO, DEBUG, TRACE

Example:

# **Known Issues**

# API ML stops accepting connections after z/OS TCP/IP stack is recycled

#### Symptom:

When z/OS TCP/IP stack is restarted, it is possible that the internal services of API Mediation Layer (Gateway, Catalog, and Discovery Service) stop accepting all incoming connections, go into a continuous loop, and write a numerous error messages in the log.

#### Sample message:

The following message is a typical error message displayed in STDOUT:

#### Solution:

Restart API Mediation Layer.

**Tip:** To prevent this issue from occurring, it is strongly recommended not to restart the TCP/IP stack while API ML is running.

# SEC0002 error when logging in to API Catalog

SEC0002 error typically appears when users fail to log in to API Catalog. The following image shows the API Catalog login page with the SEC0002 error.

The error is caused by failed z/OSMF authentication. To determine the reason authentication failed, open the ZWESVSTC joblog and look for a message that contains ZosmfAuthenticationProvider. The following is an example of the message that contains ZosmfAuthenticationProvider :

Check the rest of the message, and identify the cause of the problem. The following list provides the possible reasons and solutions for the z/OSMF authentication issue:

- Connection refused
- Missing z/OSMF host name in subject alternative names
- Invalid z/OSMF host name in subject alternative names

#### **Connection refused**

In the following message, failure to connect to API Catalog occurs when connection is refused:

The reason for the refused connection message is either invalid z/OSMF configuration or z/OSMF being unavailable. The preceding message indicates that z/OSMF is not on the 127.0.0.1:1443 interface.

#### Solution:

#### Configure z/OSMF

Make sure that z/OSMF is running and is on 127.0.0.1:1443 interface, and try to log in to API Catalog again. If you get the same error message, change z/OSMF configuration.

#### Follow these steps:

1. Locate the z/OSMF PARMLIB member IZUPRMxx.

For example, locate IZUPRM00 member in SYS1.PARMLIB.

- 2. Change the current HOSTNAME configuration to HOSTNAME('\*').
- 3. Change the current HTTP\_SSL\_PORT configuration to HTTP\_SSL\_PORT('1443').

**Important!** If you change the port in the z/OSMF configuration file, all your applications lose connection to z/OSMF.

For more information, see Syntax rules for IZUPRMxx.

If changing the z/OSMF configuration does not fix the issue, reconfigure Zowe.

#### Follow these steps:

- 1. Open .zowe\_profile in the home directory of the user who installed Zowe.
- 2. Modify the value of the ZOWE\_ZOSMF\_PORT variable.
- 3. Reinstall Zowe.

#### Missing z/OSMF host name in subject alternative names

In following message, failure to connect to API Catalog is caused by a missing z/OSMF host name in the subject alternative names:

#### Solutions:

Fix the missing z/OSMF host name in subject alternative names using the following methods:

**Note:** Apply the insecure fix only if you use API Catalog for testing purposes.

- Secure fix
- Insecure fix

#### Secure fix

#### Follow these steps:

- 1. Obtain a valid certificate for z/OSMF and place it in the z/OSMF keyring. For more information, see Configure the z/OSMF Keyring and Certificate.
- 2. Re-create the Zowe keystore by deleting it and re-creating it. For more information, see Configuring Zowe certificates. The Zowe keystore directory is the value of the KEYSTORE\_DIRECTORY variable in the instance.env file in the instance directory that is used to launch Zowe. See Creating and configuring the Zowe instance directory for more information.

#### Insecure fix

#### Follow these steps:

 Re-create the Zowe keystore by deleting it and re-creating it. For more information, see Configuring Zowe certificates. In the zowe-setup-certificates.env file that is used to generate the keystore, ensure that the property VERIFY\_CERTIFICATES and NONSTRICT\_VERIFY\_CERTIFICATES are set to false.

**Important!** Disabling VERIFY\_CERTIFICATES or NONSTRICT\_VERIFY\_CERTIFICATES may expose your server to security risks. Ensure that you contact your system administrator before you do so and use these options only for troubleshooting purpose.

#### Invalid z/OSMF host name in subject alternative names

In the following message, failure to connect to API Catalog is caused by an invalid z/OSMF host name in the subject alternative names:

#### Solutions:

Fix the invalid z/OSMF host name in the subject alternative names using the following methods:

- Request a new certificate
- Re-create the Zowe keystore

#### Request a new certificate

Request a new certificate that contains a valid z/OSMF host name in the subject alternative names.

#### **Re-create the Zowe keystore**

Re-create the Zowe keystore by deleting it and re-creating it. For more information, see Configuring Zowe certificates. The Zowe keystore directory is the value of the KEYSTORE\_DIRECTORY variable in the instance directory that is used to launch Zowe. See Creating and configuring the Zowe instance directory.

## API ML throws I/O error on GET request and cannot connect to other services

#### Symptom:

The API ML services are running but they are in DOWN state and not working properly. The following exceptions can be found in the log: java.net.UnknownHostException and java.net.NoRouteToHostException.

#### Sample message:

See the following message for full exceptions.

#### Solution:

The Zowe started task needs to run under the same user ID as z/OSMF (typically IZUSVR). This is stated in the installation documentation.

The hostname that is displayed in the details of the exception is a valid hostname. You can validate that the hostname is valid by using ping command on the same mainframe system. For example, ping USILCA32.lvn.broadcom.net. If it is valid, then the problem can be caused by insufficient privileges of your started task that is not allowed to do network access.

You can fix it by setting up the security environment as described in the Zowe documentation.

# Certificate error when using both an external certificate and Single Sign-On to deploy Zowe

#### Symptom:

You used an external certificate and Single Sign-On to deploy Zowe. When you log in to the Zowe Desktop, you encounter an error similar to the following:

#### Solution:

This issue might occur when you use a Zowe version of 1.12.0 or later. To resolve the issue, you can download your external root certificate and intermediate certificates in PEM format. Then, add the following parameter in the Zowe instance.env file.

```
ZWED_node_https_certificateAuthorities="/path/to/zowe/keystore/local_ca/localca.c
er-ebcdic","/path/to/carootcert.pem","/path/to/caintermediatecert.pem"
```

Recycle your Zowe server. You should be able to log in to the Zowe Desktop successfully now.

## Browser unable to connect due to a CIPHER error

#### Symptom:

When connecting to the API Mediation Layer, the web browser throws an error saying that the site is unable to provide a secure connection because of an error with ciphers.

The error shown varies depending on the browser. For example,

- For Google Chrome:
- For Mozilla Firefox:

#### Solution:

Remove GCM as a disabled TLS algorithm from the Java runtime being used by Zowe.

To do this, first locate the \$JAVA\_HOME/lib/security/java.security file. You can find the value of \$JAVA\_HOME in one of the following ways.

• Method 1: By looking at the JAVA\_HOME= value in the instance.env file used to start Zowe.

For example, if the instance.env file contains the following line,

then, the \$JAVA\_HOME/lib/security/java.security file will be
/usr/lpp/java/J8.0\_64/lib/security/java.security.

• Method 2: By inspecting the STDOUT JES spool file for the ZWESVSTC started task that launches the API Mediation Layer.

In the java.security file, there is a parameter value for jdk.tls.disabledAlgorithms, for example,

**Note:** This line may have a continuation character N and be split across two lines due to its length.

Edit the parameter value for jdk.tls.disabledAlgorithms to remove GCM. If as shown above the line ends <224, GCM, remove the preceding comma so the values remain a well-formed list of comma-separated algorithms:

**Note:** The file permissions of java.security might be restricted for privileged users at most z/OS sites.

After you remove GCM, restart the ZWESVSTC started task for the change to take effect.

# API Components unable to handshake

#### Symptom:

The API Mediation Layer address spaces ZWE1AG, ZWE1AC and ZWE1AD start successfully and are visible in SDSF, however they are unable to communicate with each other.

Externally the status of the API Gateway homepage will show ! icons against the API Catalog, Discovery Service and Authentication Service (shown on the left side image below) which do not progress to green tick icons as normally occurs during successful startup (shown on the right side image below).

The Zowe desktop is able to start but logon fails.

The log contains messages to indicate that connections are being reset. For example, the message below shows that the API Gateway ZWEAG is unable to connect to the API Discovery service, by default 7553.

The Zowe desktop is able to be displayed in a browser but fails to logon.

#### Solution:

Check that the Zowe certificate has been configured as a client certificate, and not just as a server certificate. More detail can be found in Configuring certificates.

# Java z/OS components of Zowe unable to read certificates from keyring

#### Symptom:

Java z/OS components of Zowe are unable to read certificates from a keyring. This problem may appear as an error as in teh following example where Java treats the SAF keyring as a file.

#### Example:

#### Solution:

Apply the following APAR to address this issue:

• APAR IJ31756

# **Error Message Codes**

The following error message codes may appear on logs or API responses. Use the following message code references and the corresponding reasons and actions to help troubleshoot issues.

# **API mediation utility messages**

# ZWEAM000I

%s started in %s seconds

Reason:

The service started.

#### Action:

No action required.

# **API mediation common messages**

# ZWEAO102E

Gateway not yet discovered. The Transform service cannot perform the request

#### Reason:

The Transform service was requested to transform a url, but the Gateway instance was not discovered.

#### Action:

Do not begin performing requests until the API Mediation Layer fully initializes after startup. Check that your Discovery service is running and that all services (especially the Gateway) are discovered correctly.

# ZWEAO104W

GatewayInstanceInitializer has been stopped due to exception: %s

#### Reason:

An unexpected exception occurred while retrieving the Gateway service instance from the Discovery Service.

#### Action:

Check that both the service and the Gateway can register with Discovery. If the services are not registering, investigate the reason why. If no cause can be determined, create an issue.

# ZWEAO105W

Gateway HTTP Client per-route connection limit (maxConnectionsPerRoute) of %s has been reached for the '%s' route.

#### Reason:

Too many concurrent connection requests were made to the same route.

#### Action:

Further connections will be queued until there is room in the connection pool. You may also increase the perroute connection limit via the gateway start-up script by setting the Gateway configuration for maxConnectionsPerRoute.

# ZWEAO106W

Gateway HTTP Client total connection limit (maxTotalConnections) of %s has been reached.

#### Reason:

Too many concurrent connection requests were made.

#### Action:

Further connections will be queued until there is room in the connection pool. You may also increase the total connection limit via the gateway start-up script by setting the Gateway configuration for maxTotalConnections.

# ZWEAO401E

Unknown error in HTTPS configuration: '%s'

#### Reason:

An Unknown error occurred while setting up an HTTP client during service initialization, followed by a system exit.

#### Action:

Start the service again in debug mode to get a more descriptive message. This error indicates it is not a configuration issue.

# **Common service core messages**

# ZWEAM100E

Could not read properties from: '%s'

#### Reason:

The Build Info properties file is empty or null.

#### Action:

The jar file is not packaged correctly. Please submit an issue.

# ZWEAM101E

I/O Error reading properties from: '%s' Details: '%s'

#### Reason:

I/O error reading META-INF/build-info.properties or META-INF/git.properties.

#### Action:

The jar file is not packaged correctly. Please submit an issue.

# ZWEAM102E

Internal error: Invalid message key '%s' is provided. Please create an issue with this message.

#### Reason:

Message service is requested to create a message with an invalid key.

#### Action:

Create an issue with this message.

## ZWEAM103E

Internal error: Invalid message text format. Please create an issue with this message.

#### Reason:

Message service is requested to create a message with an invalid text format.

#### Action:

Create an issue with this message.

# ZWEAM104E

The endpoint you are looking for '%s' could not be located

#### Reason:

The endpoint you are looking for could not be located.

#### Action:

Verify that the URL of the endpoint you are trying to reach is correct.

# ZWEAM400E

Error initializing SSL Context: '%s'

#### **Reason:**

An error occurred while initializing the SSL Context.

#### Action:

Refer to the specific message to identify the exact problem. Possible causes include:

- Incorrect security algorithm
- The keystore is invalid or corrupted
- The certificate is invalid or corrupted

# ZWEAM500W

The service is not verifying the TLS/SSL certificates of the services

#### Reason:

This is a warning that the SSL Context will be created without verifying certificates.

## Action:

Stop the service and set the verifySslCertificatesOfServices parameter to true, and then restart the service. Do not use this option in a production environment.

# ZWEAM501W

Service is connecting to Discovery service using the non-secure HTTP protocol.

## Reason:

The service is connecting to the Discovery Service using the non-secure HTTP protocol.

## Action:

For production use, start the Discovery Service in HTTPS mode and configure the services accordingly.

# ZWEAM502E

Error reading secret key: '%s'

#### Reason:

A key with the specified alias cannot be loaded from the keystore.

#### Action:

Ensure that the configured key is present, in the correct format, and not corrupt.

# ZWEAM503E

Error reading secret key: '%s'

#### Reason:

Error reading secret key.

#### Action:

Refer to the specific message to identify the exact problem. Possible causes include:

- An incorrect security algorithm
- The keystore is invalid or corrupted
- The certificate is invalid or corrupted

# ZWEAM504E

Error reading public key: '%s'

#### Reason:

Error reading secret key.

#### Action:

Refer to the specific message to identify the exact problem. Possible causes include:

- An incorrect security algorithm
- The keystore is invalid or corrupted
- The certificate is invalid or corrupted

# ZWEAM505E

Error initializing SSL/TLS context: '%s'

#### Reason:

Error initializing SSL/TLS context.

#### Action:

Refer to the specific message to identify the exact problem. Possible causes include:

- An incorrect security algorithm
- The keystore is invalid or corrupted
- The certificate is invalid or corrupted

# ZWEAM506E

Truststore Password configuration parameter is not defined

#### Reason:

Your truststore password was not set in the configuration.

#### Action:

Ensure that the parameter server.ssl.trustStorePassword contains the correct password for your truststore.

# ZWEAM507E

Truststore configuration parameter is not defined but it is required

#### Reason:

The truststore usage is mandatory, but the truststore location is not provided.

#### Action:

If a truststore is required, define the truststore configuration parameter by editing the server.ssl.truststore, server.ssl.truststorePassword and server.ssl.truststoreType parameters with valid data. If you do not require a truststore, change the trustStoreRequired boolean parameter to false.

# ZWEAM508E

Keystore not found, server.ssl.keyStore configuration parameter is not defined

#### Reason:

Your keystore path was not set in the configuration.

#### Action:

Ensure that the correct path to your keystore is contained in the parameter server.ssl.keyStore in the properties or yaml file of your service.

### ZWEAM509E

Keystore password not found, server.ssl.keyStorePassword configuration parameter is not defined

#### Reason:

Your keystore password was not set in the configuration.

#### Action:

Ensure that the correct password to your keystore in the parameter server.ssl.keyStorePassword is contained in the properties or yaml file of your service.

## ZWEAM510E

Invalid key alias '%s'

#### Reason:

The key alias was not found.

#### Action:

Ensure that the key alias provided for the key exists in the provided keystore.

## ZWEAM511E

The certificate of the service accessed using URL '%s' is not trusted by the API Gateway: %s

#### Reason:

The Gateway does not trust the requested service and refuses to communicate with it.

#### Action:

Possible actions regarding to message content:

- Message: Certificate does not match any of the subject alternative names. Action: Verify that the hostname which the certificate is issued for matches the hostname of the service.
- Message: Unable to find the valid certification path to the requested target. Action: Import the root CA that issued services's certificate to API Gateway truststore

## ZWEAM600W

Invalid parameter in metadata: '%s'

#### Reason:

An invalid apilnfo parameter was found while parsing the service metadata.

#### Action:

Remove or fix the referenced metadata parameter.

## ZWEAM700E

No response received within the allowed time: %s

#### Reason:

No response was received within the allowed time.

#### Action:

Verify that the URL you are trying to reach is correct and all services are running.

# ZWEAM701E

The request to the URL '%s' has failed: %s caused by: %s

#### Reason:

The request failed because of an internal error.

#### Action:

Refer to specific exception details for troubleshooting. Create an issue with this message.

# Security common messages

## ZWEAT100E

Token is expired for URL '%s'

#### Reason:

The validity of the token is expired.

#### Action:

Obtain a new token by performing an authentication request.

## ZWEAT103E

Could not write response: %s

#### Reason:

A message could not be written to the response.

#### Action:

Please submit an issue with this message.

# ZWEAT403E

The user is not authorized to the target resource: %s

#### **Reason:**

The service has accepted the authentication of the user but the user does not have access rights to the resource.

#### Action:

Contact your security administrator to give you access.

# ZWEAT409E

The platform returned error: %s

#### Reason:

The platform responded with unknown errno code.

#### Action:

Please submit an issue with this message.

# ZWEAT410E

The platform returned error: %s

#### Reason:

The specified password is incorrect.

#### Action:

Provide correct password.

#### ZWEAT411E

The platform returned error: %s

#### Reason:

The platform returned error, specified in the error message.

#### Action:

Contact your security administrator with the message.

# ZWEAT412E

The platform returned error: %s

#### Reason:

The specified password is expired.

#### Action:

Contact your security administrator to reset your password.

## ZWEAT413E

The platform returned error: %s

#### Reason:

The new password is not valid.

#### Action:

Provide valid password.

## ZWEAT414E

The platform returned error: %s

#### Reason:

The user name access has been revoked.

#### Action:

Contact your security administrator to unsuspend your account.

## ZWEAT415E

The platform returned error: %s

#### Reason:

The user name does not exist in the system.

#### Action:

Provide correct user name.

## ZWEAT416E

The platform returned error: %s

#### Reason:

The specified user name or password is invalid.

#### Action:

Provide correct user name or password.

## ZWEAT601E

z/OSMF service name not found. Set parameter apiml.security.auth.zosmf.serviceId to your service ID.

#### Reason:

The parameter zosmfserviceld was not configured correctly and could not be validated.

#### Action:

Ensure that the parameter apiml.security.auth.zosmf.serviceId is correctly entered with a valid z/OSMF service ID.

# ZWEAT602E

The SAF provider endpoint supports only the resource class 'ZOWE', but the current one is '%s'

#### Reason:

The parameter apiml.security.authorization.provider is set to endpoint

#### Action:

Change the SAF provider to another one to use this endpoint

# ZWEAT603E

Endpoint %s is not properly configured

#### Reason:

The application cannot call the endpoint to check the SAF resource of the user

#### Action:

Verify the state of ZSS and IZS, then check if parameters apiml.security.authorization.endpoint.\* are matching.

# Security client messages

# ZWEAS100E

Authentication exception: '%s' for URL '%s'

#### Reason:

A generic failure occurred while authenticating.

#### Action:

Refer to the specific message to troubleshoot.

# ZWEAS101E

Authentication method '%s' is not supported for URL '%s'

#### Reason:

The HTTP request method is not supported for the URL.

#### Action:

Use the correct HTTP request method that is supported for the URL.

# ZWEAS103E

API Gateway Service is not available by URL '%s' (API Gateway is required because it provides the authentication functionality)

#### Reason:

The security client cannot find a Gateway instance to perform authentication. The API Gateway is required because it provides the authentication functionality.

#### Action:

Check that both the service and Gateway are correctly registered in the Discovery service. Allow some time after the services are discovered for the information to propagate to individual services.

# ZWEAS104E

Authentication service is not available by URL '%s'

#### Reason:

The Authentication service is not available.

#### Action:

Make sure that the Authentication service is running and is accessible by the URL provided in the message.

## ZWEAS105E

Authentication is required for URL '%s'

#### Reason:

Authentication is required.

#### Action:

Provide valid authentication.

# ZWEAS120E

Invalid username or password for URL '%s'

#### Reason:

The username or password is invalid.

#### Action:

Provide a valid username and password.

# ZWEAS121E

Authorization header is missing, or the request body is missing or invalid for URL '%s'

#### Reason:

The authorization header is missing, or the request body is missing or invalid.

#### Action:

Provide valid authentication.

# ZWEAS130E

Token is not valid for URL '%s'

#### Reason:

The token is not valid.

#### Action:

Provide a valid token.

# ZWEAS131E

No authorization token provided for URL '%s'

#### Reason:

No authorization token is provided.

#### Action:

Provide a valid authorization token.

# ZAAS client messages

# ZWEAS100E

Token is expired for URL

#### Reason:

The application using the token kept it for longer than the expiration time

#### Action:

When this error occurs it is necessary to get a new JWT token.

# ZWEAS120E

Invalid username or password

#### Reason:

Provided credentials weren't recognized

## Action:

Try with different credentials

# ZWEAS121E

Empty or null username or password values provided

## Reason:

One of the credentials was null or empty

#### Action:

Try with full set of credentials

# ZWEAS122E

Empty or null authorization header provided

#### Reason:

The authorization header was empty or null

#### Action:

Try again with a valid authorization header

# ZWEAS170E

An exception occurred while trying to get the token

#### Reason:

General exception. There are more pieces of information in the message

#### Action:

Log the message from the exception and then handle the exception based on the information provided there.

# **ZWEAS400E**

Unable to generate PassTicket. Verify that the secured signon (PassTicket) function and application ID is configured properly by referring to Using PassTickets in the guide for your security provider

#### Reason:

Unable to generate PassTicket.

#### Action:

Verify that the secured signon (PassTicket) function and application ID is configured properly by referring to Using PassTickets in the guide for your security provider

# ZWEAS401E

Token is not provided

### Reason:

There was no JWT token provided for the generation of the PassTicket

## Action:

Ensure that you are passing JWT token for PassTicker generation

# ZWEAS404E

Gateway service is unavailable

#### Reason:

Gateway service does not respond.

#### Action:

Ensure that the Gateway service is up and that the path to the gateway service is properly set.

# ZWEAS417E

The application name was not found

#### Reason:

The application id provided for the generation of the PassTicket was not recognized by the security provider

#### Action:

Ensure that the security provider recognized the application id.

# ZWEAS130E

Invalid token provided

#### Reason:

The JWT token is not valid

#### Action:

Provide a valid token.

## ZWEAS500E

There was no path to the trust store.

#### Reason:

The Zaas Client configuration does not contain the path to the trust store

#### Action:

Ensure that the configuration contains the trustStorePath and that it points to valid trust store.

#### ZWEAS501E

There was no path to the key store.

#### Reason:

The Zaas Client configuration does not contain the path to the key store

#### Action:

Ensure that the configuration contains the keyStorePath and that it points to valid key store.

#### ZWEAS502E

The configuration provided for SSL is invalid.

#### Reason:

The type of the keystore, truststore or the included keys/certs aren't considered valid

#### Action:

Ensure that the combination of the configuration is cryptographically valid.

# ZWEAS503E

The SSL configuration contained invalid path.

#### Reason:

There was an invalid path to either trust store or keystore

#### Action:

Ensure that both provided paths are resolved to valid trust store and valid key store

# **Discovery service messages**

# ZWEAD400E

Cannot notify Gateway on '%s' about new instance '%s'

#### Reason:

The Discovery Service tried to notify the Gateway about an instance update, but the REST call failed. The purpose of this call is to update the Gateway caches. The Gateway might be down or a network problem occurred.

#### Action:

Ensure that there are no network issues and that the Gateway was not restarted. If the problem reoccurs, contact Broadcom support.

## ZWEAD401E

Cannot notify Gateway on '%s' about cancelled registration

#### Reason:

The Discovery Service tried to notify the Gateway about service un-registration, but the REST call failed. The purpose of this call is to update the Gateway caches. The Gateway might be down or a network problem occurred.

#### Action:

Ensure that there are no network issues and that the Gateway was not restarted. If the problem reoccurs, contact Broadcom support.

# ZWEAD700W

Static API definition directory '%s' is not a directory or does not exist

#### Reason:

One of the specified static API definition directories does not exist or is not a directory.

#### Action:

Review the static API definition directories and their setup. The static definition directories are specified as a launch parameter to a Discovery service jar. The property key is: apiml.discovery.staticApiDefinitionsDirectories

# ZWEAD701E

Error loading static API definition file '%s'

#### Reason:

A problem occurred while reading (IO operation) of a specific static API definition file.

#### Action:

Ensure that the file data is not corrupted or incorrectly encoded.

# ZWEAD702W

Unable to process static API definition data: '%s' - '%s'

#### Reason:

A problem occurred while parsing a static API definition file.

#### Action:

Review the mentioned static API definition file for errors. Refer to the specific log message to determine the exact cause of the problem:

- Serviceld is not defined in the file '%s'. The instance will not be created. Make sure to specify the Serviceld.
- The instanceBaseUrls parameter of %s is not defined. The instance will not be created. Make sure to specify the InstanceBaseUrl property.
- The API Catalog UI tile ID %s is invalid. The service %s will not have an API Catalog UI tile. Specify the correct catalog title ID.
- One of the instanceBaseUrl of %s is not defined. The instance will not be created. Make sure to specify the InstanceBaseUrl property.
- The URL %s does not contain a hostname. The instance of %s will not be created. The specified URL is malformed. Make sure to specify valid URL.
- The URL %s does not contain a port number. The instance of %s will not be created.
- The specified URL is missing a port number. Make sure to specify a valid URL.
- The URL %s is malformed. The instance of %s will not be created: The Specified URL is malformed. Make sure to specify a valid URL.
- The hostname of URL %s is unknown. The instance of %s will not be created: The specified hostname of the URL is invalid. Make sure to specify a valid hostname.
- Invalid protocol. The specified protocol of the URL is invalid. Make sure to specify valid protocol.
- Additional service metadata of %s in processing file %s could not be created: %s

# ZWEAD703E

A problem occurred during reading the static API definition directory: '%s'

## Reason:

There are three possible causes of this error:

- The specified static API definition folder is empty.
- The definition does not denote a directory.

• An I/O error occurred while attempting to read the static API definition directory.

#### Action:

Review the static API definition directory definition and its contents on the storage. The static definition directories are specified as a parameter to launch a Discovery Service jar. The property key is: apiml.discovery.staticApiDefinitionsDirectories

# ZWEAD704E

Gateway Service is not available so it cannot be notified about changes in Discovery Service

#### Reason:

Gateway Service is probably mis-configured or failed to start from another reason.

#### Action:

Review the log of Gateway Service and its configuration.

# Gateway service messages

# ZWEAG500E

Client certificate is missing in request.

#### Reason:

No client certificate is present in the HTTPS request.

#### Action:

Properly configure client to send client certificate.

# ZWEAG700E

No instance of the service '%s' found. Routing will not be available.

#### Reason:

The Gateway could not find an instance of the service from the Discovery Service.

#### Action:

Check that the service was successfully registered to the Discovery Service and wait for Spring Cloud to refresh the routes definitions.

# ZWEAG701E

Service '%s' does not allow encoded characters in the request path: '%s'.

#### Reason:

The request that was issued to the Gateway contains an encoded character in the URL path. The service that the request was addressing does not allow this pattern.

#### Action:

Contact the system administrator and request enablement of encoded characters in the service.

# ZWEAG702E

Gateway does not allow encoded slashes in request: '%s'.

#### Reason:

The request that was issued to the Gateway contains an encoded slash in the URL path. Gateway configuration does not allow this encoding in the URL.

#### Action:

Contact the system administrator and request enablement of encoded slashes in the Gateway.

# ZWEAG704E

Configuration error '%s' when trying to read jwt secret: %s

#### Reason:

A problem occurred while trying to read the jwt secret key from the keystore.

#### Action:

Review the mandatory fields used in the configuration such as the keystore location path, the keystore and key password, and the keystore type.

## ZWEAG705E

Failed to load public or private key from key with alias '%s' in the keystore '%s'. Gateway is shutting down.

#### Reason:

Failed to load a public or private key from the keystore during JWT Token initialization.

#### Action:

Check that the key alias is specified and correct. Verify that the keys are present in the keystore.

## ZWEAG706E

RequestContext is not prepared for load balancing.

#### Reason:

Custom Ribbon load balancing is not in place before calling Ribbon.

#### Action:

Contact Broadcom support.

## ZWEAG707E

The request to the URL '%s' aborted without retrying on another instance. Caused by: %s

#### Reason:

Request to the server instance failed and will not be retried on another instance.

#### Action:

Refer to Caused by details for troubleshooting.

# ZWEAG708E

The request to the URL '%s' failed after retrying on all known service instances. Caused by: %s

#### Reason:

Request to the server instance could not be executed on any known service instance.

#### Action:

Verify the status of the requested instance.

## ZWEAG709E

Service is not available at URL '%s'. Error returned: '%s'

#### Reason:

The service is not available.

#### Action:

Make sure that the service is running and is accessible by the URL provided in the message.

# ZWEAG710E

Load balancer does not have available server for client: %s

#### Reason:

The service is not available. It might be removed by the Circuit Breaker or by requesting specific instance that is not available

#### Action:

Try the request later or remove the request for specific instance.

# ZWEAG711E

The principal '%s' is missing queried authorization.

#### Reason:

The principal does not have the queried access to resource name within resource class.

#### Action:

No action needed.

# ZWEAG712E

The URI '%s' is an invalid format

#### Reason:

The URI did not follow the format /{serviceld}/{type}/{version}/{endpoint} or /{type}/{version}/{serviceld}/{endpoint}.

#### Action:

Use a properly formatted URI.

# ZWEAG100E

Authentication exception: '%s' for URL '%s'

#### Reason:

A generic failure occurred during authentication.

#### Action:

Refer to the specific authentication exception details for troubleshooting.

# ZWEAG101E

Authentication method '%s' is not supported for URL '%s'

#### Reason:

The HTTP request method is not supported by the URL.

#### Action:

Use the correct HTTP request method supported by the URL.

# ZWEAG102E

Token is not valid

#### Reason:

The JWT token is not valid.

#### Action:

Provide a valid token.

# ZWEAG103E

The token has expired

#### Reason:

The JWT token has expired.

#### Action:

Obtain new token by performing an authentication request.

# ZWEAG104E

Authentication service is not available at URL '%s'. Error returned: '%s'

#### Reason:

The authentication service is not available.

#### Action:

Make sure that the authentication service is running and is accessible by the URL provided in the message.

# ZWEAG105E

Authentication is required for URL '%s'

#### Reason:

Authentication is required.

#### Action:

Provide valid authentication.

# ZWEAG106W

Login endpoint is running in dummy mode. Use credentials '%s'/'%s' to log in. Do not use this option in the production environment.

#### Reason:

The authentication is running in dummy mode.

#### Action:

Ensure that this option is not being used in a production environment.

# ZWEAG107W

Incorrect value: apiml.security.auth.provider = '%s'. The authentication provider is not set correctly. The default 'zosmf' authentication provider is being used.

#### Reason:

An incorrect value of the apiml.security.auth.provider parameter is set in the configuration.

#### Action:

Ensure that the value of apiml.security.auth.provider is set either to 'dummy' if you want to use dummy mode, or to 'zosmf' if you want to use the z/OSMF authentication provider.

## ZWEAG108E

z/OSMF instance '%s' not found or incorrectly configured. Gateway is shutting down.

#### Reason:

The Gateway could not find the z/OSMF instance from the Discovery Service or it could not communicate with the provided z/OSMF instance.

#### Action:

Ensure that the z/OSMF instance is configured correctly and that it is successfully registered to the Discovery Service and that the API Mediation Layer can communicate with provided z/OSMF instance. The default timeout is 5 minutes. On slower system, add APIML\_SECURITY\_JWTINITIALIZERTIMEOUT=... variable and value in minutes into Zowe's configuration to override this value.

# ZWEAG109E

z/OSMF response does not contain field '%s'.

#### Reason:

The z/OSMF domain cannot be read.

#### Action:

Review the z/OSMF domain value contained in the response received from the 'zosmf/info' REST endpoint.

# ZWEAG110E

Error parsing z/OSMF response. Error returned: '%s

#### Reason:

An error occurred while parsing the z/OSMF JSON response.

#### Action:

Check the JSON response received from the 'zosmf/info' REST endpoint.

## ZWEAG120E

Invalid username or password for URL '%s'

#### **Reason:**

The username and/or password are invalid.

#### Action:

Provide a valid username and password.

# ZWEAG121E

Authorization header is missing, or the request body is missing or invalid for URL '%s'

#### Reason:

The authorization header is missing, or the request body is missing or invalid.

#### Action:

Provide valid authentication.

# ZWEAG130E

Token is not valid for URL '%s'

#### Reason:

The token is not valid.

#### Action:

Provide a valid token.

# ZWEAG131E

No authorization token provided for URL '%s'

#### Reason:

No authorization token is provided.

#### Action:

Provide a valid authorization token.

# ZWEAG140E

The 'applicationName' parameter name is missing.

#### Reason:

The application name is not provided.

#### Action:

Provide the 'applicationName' parameter.

## ZWEAG141E

The generation of the PassTicket failed. Reason: %s

#### Reason:

An error occurred in the SAF Auth Service. Review the reason in the error message.

#### Action:

Supply a valid user and application name, and check that corresponding permissions have been set up.

# **API Catalog messages**

# ZWEAC100W

Could not retrieve all service info from discovery -- %s -- %s -- %s

#### Reason:

The response from The Discovery Service about the registered instances returned an error or empty body.

#### Action:

Make sure the Discovery Service is up and running. If the http response error code refers to a security issue, check that both the Discovery Service and Catalog are running with the https scheme and that security is configured properly.

# ZWEAC101E

Could not parse service info from discovery -- %s

#### Reason:

The response from the Discovery Service about the registered instances could not be parsed to extract applications.

#### Action:

Run debug mode and look at the Discovery Service potential issues while creating a response. If the Discovery Service does not indicate any error, create an issue.

## ZWEAC102E

Could not retrieve containers. Status: %s

#### Reason:

One or more containers could not be retrieved.

#### Action:

Check the status of the message for more information and the health of the Discovery Service.

## ZWEAC103E

API Documentation not retrieved, %s

#### Reason:

API documentation was not found.

#### Action:

Make sure the service documentation is configured correctly.

## ZWEAC104E

Could not retrieve container statuses, %s

#### Reason:

The status of one or more containers could not be retrieved.

#### Action:

Check the status of the message for more information and the health of the Discovery Service.

# ZWEAC700E

Failed to update cache with discovered services: '%s'

#### Reason:

Cache could not be updated.

#### Action:

Check the status of the Discovery Service.

# ZWEAC701W

API Catalog Instance not retrieved from Discovery service

#### Reason:

An error occurred while fetching containers information.

#### Action:

The jar file is not packaged correctly. Please submit an issue.

# ZWEAC702E

An unexpected exception occurred when trying to retrieve an API Catalog instance from the Discovery Service: %s

#### Reason:

An unexpected error occurred during API Catalog initialization. The API Catalog was trying to locate an instance of itself in the Discovery Service.

#### Action:

Review the specific message for more information. Verify if the Discovery Service and service registration work as expected.

# ZWEAC703E

Failed to initialize API Catalog with discovered services

#### Reason:

The API Catalog could not initialize running services after several retries.

#### Action:

Ensure services are started and discovered properly.

## ZWEAC704E

ApiDoc retrieval problem for '%s' service. %s

#### Reason:

ApiDoc for service could not be retrieved.

#### Action:

Verify that the service provides a valid ApiDoc.

## ZWEAC705W

The home page url for service %s was not transformed. %s

#### Reason:

The home page url for service was not transformed. The original url will be used.

#### Action:

Refer to the specific printed message. Possible causes include:

- The Gateway was not found. The Transform service cannot perform the request. Wait for the Gateway to be discovered.
- The URI is not valid. Ensure the service is providing a valid URL.
- Not able to select a route for the URL of the specific service. The original URL is used. If necessary, check the routing metadata of the service.
- The path of the service URL is not valid. Ensure the service is providing the correct path.

# ZWEAC706E

Service not located, %s

#### Reason:

The service could not be found.

#### Action:

Check if the service is up and registered. If it is not registered, review the onboarding guide to ensure that all steps were completed.

# ZWEAC707E

Static API refresh failed, caused by exception: %s

#### Reason:

The Static API refresh could not be performed because of exception.

#### Action:

Check the specific exception for troubleshooting.

# ZWEAC708E

The API base path for service %s was not retrieved. %s

#### Reason:

The API base path for service was not retrieved. An empty path will be used.

#### Action:

Refer to the specific printed message. Possible causes include:

- The URI is not valid. Ensure the service is providing a valid URL.
- Not able to select a route for the URL of the specific service. The original URL is used. If necessary, check the routing metadata of the service.
- The path of the service URL is not valid. Ensure the service is providing the correct path.

# ZWEAC709E

Static definition generation failed, caused by exception: %s

#### Reason:

The Static definition generation could not be performed because of exception.

#### Action:

Check the specific exception for troubleshooting.

# Troubleshooting Zowe Application Framework

The following topics contain information that can help you troubleshoot problems when you encounter unexpected behavior installing and using Zowe™ Application Framework which includes the Zowe Desktop.

Most of the solutions below identify issues by referring to the Zowe logs. To identify and resolve issues, you should be familiar with their names and locations.

The Zowe Application Framework manages issues in GitHub. When you troubleshoot a problem, you can check whether a GitHub issue (open or closed) that covers the problem already exists. For a list of issues, see the zlux repo.

# Desktop apps fail to load

#### Symptom:

When you open apps in the Zowe desktop, a page is displayed with the message "The plugin failed to load."

#### Solution:

This problem might occur when you use Node.js v8.16.1, which performs auto-encoding in a way that breaks Zowe apps. See https://github.com/ibmruntimes/node/issues/142 for details.

To solve the problem, use a different version of Node.js v8, such as v8.17.0, or use Node.js v12. You can obtain them from the Node.js marketplace. Download the ibm-trial-node-v8.17.0-os390-s390x.pax.Z file.

# **NODEJSAPP** disables immediately

#### Symptom:

You receive the message CEE5207E The signal SIGABRT was received in stderr.

#### Solution:

You might have reached the limit for shared message queues on your LPAR. When Node.js applications are terminated by a SIGKILL signal, shared message queues might not be deallocated. For more information, see the **If the NODEJSAPP disables immediately** section in the Troubleshooting Node.js applications topic on IBM Knowledge Center.

# Cannot log in to the Zowe Desktop

## Symptom:

When you attempt to log in to the Zowe Desktop, you receive the following error message that is displayed beneath the **Username** and **Password** fields.

The Zowe desktop attempts to authenticate the credentials using the types that have been configured, by default the three above of ["saf", "apiml", "zss"]. If Zowe has been configured with the LAUNCH\_COMPONENT\_GROUPS=DESKTOP where GATEWAY is not a launch group, then the message will just include the types ["saf", "zss"].

#### Solution:

This error may simply mean your password is not correct. If that's not the case, please continue on following troubleshooting guidance.

For the Zowe Desktop to work, the node server that runs under the ZWESVSTC started task must be able to make cross memory calls to the ZWESIS01 load module running under the ZWESISTC started task. If this communication fails, you see the authentication error.

There are three known problems that might cause this error. The Zowe architecture diagram shows the following connections. One of these three connections likely failed.

- 1. The zssServer connection to the ZWESISTC started task using cross memory communication. If this fails, see zssServer unable to communicate with X-MEM. The architecture diagram below has been annotated with a (1) to show this connection.
- 2. The Zowe Desktop ZLUX server connection to the zssServer across the default port 8542. If this fails, see ZLUX unable to communicate with zssServer. The architecture diagram below has been annotated with a (2) to show this connection.
- 3. The Zowe Desktop ZLUX server cannot connect to API Mediation Layer for authentication. If this fails, see ZLUX unable to communicate with API Mediation Layer.

# ZSS server unable to communicate with X-MEM

- Open the log file **\$INSTANCE\_DIR**/logs/zssServer-yyyy-mm-dd-hh-ss.log. This file is created each time ZWESVSTC is started and only the last five files are kept.
- Look for the message that starts with ZIS status.
- If the communication works, the message includes **0k**. For example:

If the communication works, the problem is likely that the ZLUX server is unable to communicate to the zssServer. For more information, see ZLUX unable to communicate with zssServer.

• If the communication is not working, the message includes Failure. For example:

or

or

In this case, check that the ZWESISTC started task is running. If not, start it with the TSO command /S ZWESISTC

- If the problem cannot be easily fixed (such as the ZWESISTC task not running), then it is likely that the cross memory server is not running. To check whether the cross memory is running, check the started task ZWESISTC log for any errors.
- If the cross memory server ZWESISTC started task is running, check that the program name of the cross memory procedure matches between the ZWESISTC PROBLIB member and the instance.env file used to launch Zowe.

By default the proc value is ZWESIS\_STD, and if a new name is chosen then both files need to be updated for the handshake to be successful.

The line in the ZWESISTC problib that defines the procedure name that cross memory will use is

The line in the instance.env that specifies the cross memory procedure that the zssServer will try to attach to is

 If this is the first time you set up Zowe, it is possible that the cross memory server configuration did not complete successfully. To set up and configure the cross memory server, follow steps as described in the topic Installing and configuring the Zowe cross memory server (ZWESISTC). Once ZWESISTC is started, if problems persist, check its log to ensure it has been able to correctly locate its load module ZWESIS01 as well as the parmlib ZWESIP00.

• If there is an authorization problem, the message might include **Permission Denied**. For example:

Check that the user ID of the ZWESVSTC started task is authorized to access the load module. Only authorized code can call ZWESIS01 because it is an APF-authorized load module.

**Note:** If you are using RACF security manager, a common reason for seeing **Permission Denied** is that the user running the started task ZWESVSTC (typically ZWESVUSR) does not have READ access to the FACILITY class ZWES.IS.

If the message includes the following text, the configuration of the Application Framework server may be incomplete:

If you are using AT/TLS, then the "attls" : true statement might be missing from the zluxserver.json file. For more information, see Configuring Zowe App Server for HTTPS communication with ZSS.

## ZLUX unable to communicate with zssServer

Follow these steps:

- Open the log file **\$INSTANCE\_DIR**/logs/appServer-yyyy-mm-dd-hh-ss.log. This file is created each time ZWESVSTC is started and only the last five files are kept.
- Look for the message that starts with GetAddrInfoReqWrap.onlookup and the log messages below.

These messages show that the host name localhost cannot be reached between the Zowe desktop server and the zssServer because localhost has not been mapped to an IP address.

• Map localhost to port 127.0.0.1.

Create an entry in the file /etc/hosts that contains the line

• Restart the ZWESVSTC address space.

## ZLUX unable to communicate with API Mediation Layer

Follow these steps:

- Verify whether API Mediation Layer is started or not. If it is started, you can see a service status page with all green check marks by visiting <a href="https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host>:<gateway-port>">https://syour-zowe-host</a>
- You may need to wait a little longer to allow API Mediation Layer Gateway to complete the environment test. This could be more noticeable with certain z/OSMF level and Zowe v1.20.0 release and later.

# Server startup problem ret=1115

**Symptom:** When ZWESVSTC is restarted, the following message is returned in the output of the ZSS server log file, **\$INSTANCE\_DIR**/logs/zssServer-yyyy-mm-dd-hh-ss.log:

**Solution:** This message means that some other process is already listening on port 7542, either at address 127.0.0.1 (localhost) or at 0.0.0.0 (all addresses). This prevents the ZSS server from starting.

One possibility is that a previously running ZSS server did not shut down correctly, and either the operating system has not released the socket after the ZSS server shut down, or the ZSS server is still running.

# Application plug-in not in Zowe Desktop

#### Symptom:

An application plug-in is not appearing in the Zowe Desktop.

#### Solution:

To check whether the plug-in loaded successfully, enter the following URL in a browser to display all successfully loaded Zowe plug-ins:

#### https://my.mainframe.com:8544/plugins?type=application

You can also search the node server logs for the plug-in identifier, for example org.zowe.sample.app. If the plug-in loaded successfully, you will find the following message:

If the plug-in did not load successfully, you will find the following message:

If the identifier is not in the logs, make sure the plug-in's locator file is in the /zlux-appserver/deploy/instance/ZLUX/plugins/ directory. The plug-in locator is a .json file, usually with same name as the identifier, for example org.zowe.sampleapp.json. Open the file and make sure that the path that is defined with the pluginLocation attribute is correct. If the path is relative, make sure it is relative to the zlux-app-server/bin directory.

For more information on loading plug-ins to the Desktop, see Adding Your App to the Desktop.

# Error: You must specify MVD\_DESKTOP\_DIR in your environment

#### Symptom:

A plug-in that is built in your local environment using npm run start or npm run build failed with an error message about a missing MVD\_DESKTOP\_DIR environment variable.

#### Solution:

Add the Zowe Desktop directory path to the MVD\_DESKTOP\_DIR environment variable. To specify the path, run the following commands in your Windows console or Linux bash shell:

- Windows
- Mac Os/Linux

# Error: Zowe Desktop address space fails to start { ZWED0115E }

After launching the started task ZWESVSTC there are no Zowe desktop ZWE1DS address space(s).

#### Symptom: Check the log for the message

The timeout value was increased to be 30000 in 1.11.0 release. To check which release of Zowe you are running, see Determining the Zowe release number. To further increase this, or update the value on a previous release you can add an entry to your \$INSTANCE\_DIR/instance.env.

where the timeout value is in milliseconds.

# Warning: Problem making eureka request { Error: connect ECONNREFUSED }

Symptom: The Zowe started task ZWESVSTC log contains error messages reporting problems connecting

#### Solution:

You can ignore these messages. These messages are timing-related where different Eureka servers come up, try to connect to each other, and warn that the endpoint they are trying to perform a handshake with is not available. When all of the Eurka services have started, these errors will stop being logged.

# Warning: ZWED0159W - Plugin (org.zowe.zlux.proxy.zosmf) loading failed.

Symptom: The Zowe started task ZWESVSTC log contains messages

#### Solution:

You can ignore these messages which should not occur in 1.11 or later releases. To check which release of Zowe you are running, see Determining the Zowe release number.

# Warning: ZWED0050W - Could not read swagger doc folder (..)

Symptom: The Zowe started task ZWESVSTC log contains messages ending

#### Solution:

You can ignore these messages.

# Warning: ZWED0047W - Swagger file for server (...) not found

#### Symptom:

The Zowe started task ZWESVSTC log contains messages ending

#### Solution:

You can ignore these messages.

# Unable to log in to the explorers when using Zowe V1.13 or V1.14

#### Symptom:

You installed Zowe V1.13 or V1.14. When you start the Zowe server, you see the following error message in the appServer log.

When you log in to the Zowe Desktop, you cannot open the JES, MVS, or USS Explorers. You receive the following error message:

#### Solution:

A new property ZOWE\_EXPLORER\_FRAME\_ANCESTORS was introduced in V1.12. This property is required to be present in the instance.env file with some valid value. When undefined, it is treated as Boolean, which breaks the string split function. To resolve the issue, define the value for this property in the instance.env file.

# Gathering information to troubleshoot Zowe Application Framework

Gather the following information to troubleshoot Zowe™ Application Framework issues:

- z/OS release level
- Zowe version and release level
- Log output from the Zowe Application Server
- Error message codes
- JavaScript console output (Web Developer toolkit accessible by pressing F12)
- Screen captures (if applicable)

# z/OS release level

To find the z/OS release level, issue the following command in SDSF:

Check the output for the release level, for example:

# Zowe version and release level

#### Output:

Displays zowe version

# Log output from the Zowe Application Server

There are two major components of Zowe application server: ZLUX and ZSS. They log to different files.

The default location for logs for both zlux and zss is folder **\$INSTANCE\_DIR/logs**, but can customize the log locations by using environment variables in **\$INSTANCE\_DIR/instance.env** 

Read more about controlling the log location here.

#### **Output:**

List of files by most recent timestamp for both app-server as well ZSS.

# **Error message codes**

It is advisable to look into log files for capturing error codes. Warning messages contain the word "WARN", and errors contain "CRITICAL"

# Javascript console output

When the web UI such as the Zowe Desktop or Apps inside it have an issue, the root problem may originate from either server-side or browser-side behavior. In addition to the server logs, the browser logs should be gathered. They can be accessed by opening a browser's web developer toolkit. Most browsers allow this via pressing F12.

Read more about it here.

# Screen captures

If possible, add a screen capture of the issue.

# Raising a Zowe Application Framework issue on GitHub

When necessary, you can raise GitHub issues against the Zowe™ zlux core repository here. It is suggested that you use either the bug or enhancement template.

For issues with particular applications, such as Code Editor or JES Explorer, create the issue in the application's project.

# Raising a bug report

Please provide as much of the information listed on Troubleshooting Zowe Application Framework as possible. Anyone working on the issue might need to request this and other information if it is not supplied initially. A description of the error and how it can be reproduced is the most important information.

# **Raising an enhancement report**

Enhancement reports are just as important to the Zowe project as bug reports. Enhancement reports should be clear and detailed requirements for a potential enhancement.

# **Troubleshooting z/OS Services**

The following topics contain information that can help you troubleshoot problems when you encounter unexpected behavior installing and using Zowe™ z/OS Services.

# z/OSMF JVM cache corruption

#### Symptom:

When you work with Zowe, there are situations when z/OSMF abends.

The following is a snippet from the Java core dump.

#### Solution:

The error occurs when the Java runtime being used by the z/OSMF Liberty server and the Java runtimes being used by Zowe share a user ID of IZUSVR1, which results in a collision. To resolve this issue, review the following steps.

- 1. Isolate the started task user IDs
- 2. Update z/OSMF to not use JVM class caching

# Isolate the started task user IDs

The z/OSMF started task IZUSVR1 runs under the user ID of IZUUSER. Before version 1.9 of Zowe, its started task ZWESVSTC also ran under the same user ID. With Zowe 1.9, the default configuration changed to use a new user ID of ZWESVUSR and group of ZWEADMIN.

If your started task ZWESVSTC is configured to run under the user ID IZUUSER, change it to run under user ID ZWESVUSR. For more information, see Configuring the z/OS System for Zowe.

# Update z/OSMF to not use JVM class caching

If you need to run ZWESVSTC under the same user ID as z/OSMF for your environment, you can update the z/OSMF configuration to switch off shared class caching which stops the crash from occurring. Disabling

shared class caching reduces the performance of z/OSMF so the preferred fix is to change the user ID of ZWESVSTC away from IZUUSER to ZWESVUSR as described above.

Navigate to the file /var/zosmf/configuration/local\_override.cfg. This contains the startup arguments for the Java runtime used by z/OSMF. Add the following line:

You will need to recycle the z/OSMF server running, which by default will be running under the started task IZUSVR1.

For more information on the effect that disabling a shared class cache has on a Java runtime, see Class data sharing in the IBM Knowledge Center.

# Unable to generate unique CeaTso APPTAG

#### Symptom:

When you request a Zowe data set or z/OS Files API, you receive a response code 500 - 'Internal Server Error', with a message "Unable to generate unique CeaTso APPTAG".

#### Solution:

Check z/OSMF settings of REST API of file. You must define **RESTAPI\_FILE** in IZUPRMxx by the following statement:

RESTAPI\_FILE ACCT(IZUACCT) REGION(32768) PROC(IZUFPROC)

The default IZUFPROC can be found in SYS1.PPROCLIB. And the proper authorization is needed to get IZUFPROC work successfully.

# z/OS Services are unavailable

If the z/OS Services are unavailable, take the following corrective actions.

 Ensure that the z/OSMF REST API services are working. Check the z/OSMF IZUSVR1 task output for errors and confirm that the z/OSMF RESTFILES services are started successfully. If no errors occur, you can see the following message in the IZUSVR1 job output:

To test z/OSMF REST APIs you can run curl scripts from your workstation.

where the *securezosmfport* is 443 by default. You can verify the port number by checking the *izu.https.port* variable assignment in the z/OSMF bootstrap.properties file.

If z/OSMF returns jobs correctly, you can test whether it is able to returns files by using the following curl scripts:

If the restfiles curl statement returns a TSO SERVLET EXCEPTION error, check that the the z/OSMF installation step of creating a valid IZUFPROC procedure in your system PROCLIB has been completed. For more information, see the z/OSMF Configuration Guide.

The IZUFPROC member resides in your system PROCLIB, which is similar to the following sample:

Note: You might need to change paths and data sets names to match your installation.

A known issue and workaround for RESTFILES API can be found at TSO SERVLET EXCEPTION ATTEMPTING TO USE RESTFILE INTERFACE.

• Check your system console log for related error messages and respond to them.

Version: v1.25.x LTS

# **Troubleshooting Zowe CLI**

# Problem

Zowe™ CLI is experiencing a problem. You need to collect information that will help you resolve the issue.

#### Environment

These instructions apply to Zowe CLI installed on Windows, Mac OS X, and Linux systems as a standalone installation via a Zowe download or an NPM registry.

# Before reaching out for support

- 1. Is there already a GitHub issue (open or closed) that covers the problem? Check CLI Issues.
- 2. Review the current list of Known issues in documentation. Also try searching using the Zowe Docs search bar.

# **Resolving the problem**

Collect the following information to help diagnose the issue:

- Zowe CLI version installed.
- List of plug-ins installed and their version numbers.
- Node.js and NPM versions installed.
- List of environment variables in use.

For instructions on how to collect the information, see Gathering information for Zowe CLI.

The following information is also useful to collect:

- If you are experiencing HTTP errors, see z/OSMF troubleshooting for information to collect.
- Is the CLI part of another Node application, such as VSCode, or is it a general installation?
- Which operating system version are you running on?

- What shell/terminal are you using (bash, cmd, powershell, etc...)?
- Which queue managers are you trying to administer, and on what systems are they located?
- Are the relevant API endpoints online and valid?

# Gathering information to troubleshoot Zowe CLI

Follow these instructions to gather specific pieces of information to help troubleshoot Zowe™ CLI issues.

[[toc]]

# Identify the currently installed CLI version

Issue the following command:

The exact Zowe CLI version may vary depending upon if the @latest or @zowe-v1-lts, or @ltsincremental version is installed.

For the @zowe-v1-lts and the @latest (forward-development) version tags:

For the @lts-incremental version tag:

More information regarding versioning conventions for Zowe CLI and plug-ins is located in Versioning Guidelines.

# Identify the currently installed versions of plug-ins

Issue the following command:

The output describes version and the registry information.

# **Environment variables**

The following settings are configurable via environment variables:

#### Log levels

Environment variables are available to specify logging level and the CLI home directory.

**Important!** Setting the log level to TRACE or ALL might result in "sensitive" data being logged. For example, command line arguments will be logged when TRACE is set.

Environment Variable	Description	Values	Default
ZOWE_APP_LOG_LEVEL	Zowe CLI logging level	Log4JS log levels (OFF, TRACE, DEBUG, INFO, WARN, ERROR, FATAL)	DEBUG
ZOWE_IMPERATIVE_LOG_LEVEL	Imperative CLI Framework logging level	Log4JS log levels (OFF, TRACE, DEBUG, INFO, WARN, ERROR, FATAL)	DEBUG

#### **Home directory**

You can set the location on your computer for the Zowe CLI home directory, which contains log files, profiles, and plug-ins for the product.

**Tip!** The default . zowe folder is created when you issue your first Zowe CLI command. If you change the location of the folder, you must reinstall plug-ins and recreate or move profiles and log files that you want to retain. In some cases, you might want to maintain a different set of profiles in multiple folders, then switch between them using the environment variable.

Environment Variable	Description	Values	Default
ZOWE_CLI_HOME	Zowe CLI home directory location	Any valid path on your computer	C:\Users\ <username>\.zowe</username>

The values for these variables can be **echo**ed.

### Home directory structure

There are two sets of logs to be aware of:

- Imperative CLI Framework log, which generally contains installation and configuration information.
- Zowe CLI log, which contains information about interaction between CLI and the server endpoints.

Analyze these logs for any information relevant to your issue.

#### **Profile configuration**

The profiles folder stores connection information.

**Important!** The profile directory might contain "sensitive" information, such as your mainframe password. You should obfuscate any sensitive references before providing configuration files.

# Node.js and npm

Zowe CLI is compatible with the currently supported Node.js LTS versions. For an up-to-date list of supported LTS versions, see Node.js.org.

To gather the Node.js and npm versions installed on your computer, issue the following commands:

#### npm configuration

If you are having trouble installing Zowe CLI from an npm registry, gather your npm configuration to help identify issues with registry settings, global install paths, proxy settings, etc...

#### npm log files

In case of errors, npm creates log files in the npm\_cache\\_logs location. To get the npm\_cache location for a specific OS, run the following command:

By default, npm keeps only 10 log files, but sometimes more are needed. Increase the log count by issuing the following command:

This command increases the log count to 50, so that more log files will be stored on the system. Now you can run tests multiple times and not lose the log files. The logs can be passed to Support for analysis.

As the log files are created only when an npm command fails, but you are interested to see what is executed, you can increase the log level of npm. Issue the following command:

- With this change, you can see all actions taken by npm on the stdout. If the command is successful, it still does not generate a log file.
- The available log levels are: "silent", "error", "warn", "notice", "http", "timing", "info", "verbose", "silly", and "notice". "Notice" is the default.
- Alternatively, you can pass --loglevel verbose on the command line, but this only works with npm related commands. By setting log level in the config, it also works when you issue some zowe commands that use npm (for example, zowe plugins install @zowe/cics).

# z/OSMF troubleshooting

The core command groups use the z/OSMF REST APIs which can experience any number of problems.

If you encounter HTTP 500 errors with the CLI, consider gathering the following information:

- 1. The IZU\* (IZUSVR and IZUANG) joblogs (z/OSMF server)
- 2. z/OSMF USS logs (default location: /global/zosmf/data/logs but may change depending on installation)

If you encounter HTTP 401 errors with the CLI, consider gathering the following information:

1. Any security violations for the TSO user in SYSLOG

# Alternate methods

At times, it may be beneficial to test z/OSMF outside of the CLI. You can use the CLI tool **curl** or a REST tool such as "Postman" to isolate areas where the problem might be occurring (CLI configuration, server-side, etc.).

Example curl command to GET /zosmf/info:

# **Known Zowe CLI issues**

The following topics contain information that can help you troubleshoot problems when you encounter unexpected behavior installing and using Zowe™ CLI.

# EACCESS error when issing npm install command

Valid on Windows, Mac, or Linux

#### Symptom:

An EACCESS error is returned when you issue the npm install -g command to install a package from Zowe.org or npm.

#### Solution:

To resolve the issue, follow the steps described in Resolving EACCESS permissions errors when installing packages globally in the npm documentation.

# Command not found message displays when issuing npm install commands

#### Valid on all supported platforms

#### Symptom:

When you issue NPM commands to install the CLI, the message *command not found* displays. The message indicates that Node.js and NPM are not installed on your computer, or that PATH does not contain the correct path to the NodeJS folder.

#### Solution:

To correct this behavior, verify the following:

- Node.js and NPM are installed.
- PATH contains the correct path to the NodeJS folder.

### npm install -g Command Fails Due to an EPERM Error

#### Valid on Windows

#### Symptom:

This behavior is due to a problem with Node Package Manager (npm). There is an open issue on the npm GitHub repository to fix the defect.

#### Solution:

If you encounter this problem, some users report that repeatedly attempting to install Zowe CLI yields success. Some users also report success using the following workarounds:

- Issue the npm cache clean command.
- Uninstall and reinstall Zowe CLI. For more information, see Install Zowe CLI.
- Add the --no-optional flag to the end of the npm install command.

# Sudo syntax required to complete some installations

#### Valid on Linux and macOS

#### Symptom:

The installation fails on Linux or macOS.

#### Solution:

Depending on how you configured Node.js on Linux or macOS, you might need to add the prefix sudo before the npm install -g command or the npm uninstall -g command. This step gives Node.js write access to the installation directory.

# npm install -g command fails due to npm ERR! Cannot read property 'pause' of undefined error

#### Valid on Windows or Linux

#### Symptom:

You receive the error message npm ERR! Cannot read property 'pause' of undefined when you attempt to install the product.

#### Solution:

This behavior is due to a problem with Node Package Manager (npm). If you encounter this problem, revert to a previous version of npm that does not contain this defect. To revert to a previous version of npm, issue the following command:

### Node.js commands do not respond as expected

#### Valid on Windows or Linux

#### Symptom:

You attempt to issue node.js commands and you do not receive the expected output.

#### Solution:

There might be a program that is named *node* on your path. The Node.js installer automatically adds a program that is named *node* to your path. When there are pre-existing programs that are named *node* on your computer, the program that appears first in the path is used. To correct this behavior, change the order of the programs in the path so that Node.js appears first.

### **Installation fails on Oracle Linux 6**

#### Valid on Oracle Linux 6

#### Symptom:

You receive error messages when you attempt to install the product on an Oracle Linux 6 operating system.

#### Solution:

Install the product on Oracle Linux 7 or another Linux or Windows OS. Zowe CLI is not compatible with Oracle Linux 6.

# **Raising a CLI issue on GitHub**

When necessary, you can raise GitHub issues against the Zowe™ CLI repository here. It is suggested that you use either the bug or enhancement template.

# **Raising a bug report**

Please provide as much of the information listed on Troubleshooting CLI as is reasonable. Anyone working on the issue might need to request this and other information if it is not supplied initially. A description of the error and how it can be reproduced is the most important information.

# **Raising an enhancement report**

Enhancement reports are just as important to the Zowe project as bug reports. Enhancement reports should be clear and detailed requirements for a potential enhancement.

# **Troubleshooting Zowe Explorer**

As a Zowe Explorer user, you may encounter problems with how the VS Code extension functions. This article presents known Zowe Explorer issues and their solutions.

# Before reaching out for support

- 1. Is there already a GitHub issue (open or closed) that covers the problem? Check Zowe Explorer Issues.
- 2. Review the current list of Known issues in documentation. Also, try searching using the Zowe Docs search bar.
- 3. Collect the following information to help diagnose the issue:
- Zowe Explorer and VS Code version installed.
- Node.js and NPM versions installed.
- Whether you have Zowe CLI and the Secure Credential Store Zowe CLI plug-in installed.
- Your operating system.
- Zowe Logs.

Usually, can be found in C:\Users\userID\.zowe\zowe\logs.

Use the Slack channel to reach the Zowe Explorer community for assistance.

# **Known Zowe Explorer issues**

The following topics contain information that can help you troubleshoot problems when you encounter unexpected behavior, using Zowe Explorer.

# **Data Set Creation Error**

#### Symptom:

Data set creation fails.

#### Sample message:

Error running command zowe.createDataset: z/OSMF REST API Error: http(s) request error event called Error: self signed certificate in certificate chain. This is likely caused by the extension that contributes zowe.createDataset.

#### Solution:

Set the value of the Reject-Unauthorized parameter to false. Use the profile edit function to change profile's parameters.

# **Opening Binary Files Error**

#### Symptom:

When opening a binary file, an error message pops up.

#### Sample message:

Cannot open file:///Users/userID/.vscode/extensions/zowe-vs.code-extension-for-zowe-1.8.0/resources/temp/binaryfilename. Detail: File seems to be binary and cannot be opened as text

Error running command zowe.editMember: cannot open file:///Users/userID/.vscode/extensions/zowevs.code-extension-for-zowe-1.8.0/resources/temp/binaryfilename. Detail: File seems to be binary and cannot be opened as text. This is likely caused by the extension that contributes zowe.editMember. Solution:

# **Raising a Zowe Explorer issue on GitHub**

You can raise GitHub issues against the Zowe Explorer repository. It is suggested that you use either the bug or feature request.

# **Raising a bug report**

Please provide as much of the information listed on Troubleshooting Zowe Explorer as is reasonable. Anyone working on the issue might need to request this and other information if it is not supplied initially. A description of the error and how it can be reproduced is the most important information.

# Submitting a feature request

Feature requests are just as important to the Zowe project as bug reports. Feature requests should contain clearly formulated ideas that can improve user experience.

```
Version: v1.25.x LTS
```

# **Troubleshooting Zowe Launcher**

The following topics contain information that can help you troubleshoot problems when you encounter unexpected behavior using Zowe™ Launcher.

Issues and development of the Zowe Launcher is managed in GitHub. When you troubleshoot a problem, you can check whether a GitHub issue (open or closed) that covers the problem already exists. For a list of issues, see the launcher repo.

#### **Error Message Codes**

### **Enable Zowe Launcher Debug Mode**

Use debug mode to display additional debug messages for Zowe Launcher.

**Important:** We highly recommend that you enable debug mode only when you want to troubleshoot issues. Disable debug mode when you are not troubleshooting. Running Zowe Launcher in debug mode can adversely affect its performance and consume a large amount of spool space.

#### Follow these steps:

- 1. Open the PROCLIB member ZWESLSTC
- 2. Find STDENV DD inline statements
- 3. Add a new line

By default debug mode is disabled, so the ZLDEBUG is set to OFF. To disable debug mode remove the line or set ZLDEBUG to OFF.

4. Restart ZWESLSTC Started Task.

# **Error Message Codes**

The following error message codes may appear on Zowe Launcher SYSPRINT. Use the following message code references and the corresponding reasons and actions to help troubleshoot issues.

# **Zowe Launcher informational messages**

#### ZWEL0001I

component %s started

Reason:

Component <component-name> started.

#### Action:

No action required.

#### ZWEL0002I

component %s stopped

#### Reason:

Component <component-name> stopped.

#### Action:

No action required.

#### ZWEL0003I

new component initialized %s, restart\_cnt=%d, min\_uptime=%d seconds, share\_as=%s

#### **Reason:**

Component <component-name> initialized.

- restart\_cnt Number of attempts to restart the component in case of failure
- min\_uptime Minimum uptime that the component can be considered as successfully started
- share\_as One of <yes | no | must> which indicates whether child processes of the component start in the same address space. See documentation for \_BPX\_SHAREAS for details.

#### Action:

No action required.

#### ZWEL0004I

component %s(%d) terminated, status = %d

#### **Reason:**

Component <component-name> (<pid>) terminated with status <code>.

#### Action:

No action required.

#### ZWEL0005I

next attempt to restart component %s in %d seconds

#### Reason:

Component failure detected.

#### Action:

No action required. The component <component-name> will be restarted in <n> seconds.

### Zowe Launcher error messages

#### ZWEL0030E

failed to prepare Zowe instance

#### Reason:

Failed to prepare the Zowe high availability (HA) instance.

#### Action:

Check previous messages in the Zowe Launcher SYSPRINT to find the reason and correct it.

#### ZWEL0038E

failed to restart component %s, max retries reached

#### Reason:

Maximum retries reached for restarting component <component-name >.

#### Action:

Check <component-name> configuration and correct the maximum restart count via configuration attribute restartIntervals if needed, then restart the component by using z/OS MODIFY command F ZWESLSTC, APPL=STOP(<component-name>)

#### ZWEL0040E

failed to start component %s

#### Reason:

Failed to start component <component-name>.

#### Action:

Check <component-name> configuration and correct if needed, then either 1) start the component manually by using z/OS MODIFY command F ZWESLSTC, APPL=STOP(<component-name>) or 2) restart the entire HA instance

# **Contribute to Zowe**

You are welcome to contribute to Zowe in many forms and help make this project better! We want to make it as easy as possible for you to become a Zowe contributor. This topic outlines the different ways that you can get involved and provides some of the resources that are available to help you get started. All feedback is welcome.

- Report bugs and enhancements
- Fix issues
- Send a Pull Request
- Report security issues
- Contribution guidelines
- Promote Zowe
- Helpful resources

### **Report bugs and enhancements**

- Report bugs: Download and try one of the latest Zowe builds. Report any bugs you find by creating a Zowe bug report in GitHub.
- Report enhancements: Got an idea for a feature? Or something you're already using could be improved?
   Post an enhancement request in GitHub!

If you have an issue that is specific to a sub-project or community team, feel free to submit an issue against a specific repo.

# **Fix issues**

- There are many issues and bugs with the label Good first issue in the Zowe GitHub repositories to help you get familiar with the contribution process. Check out the following list of GitHub repos to make your contribution!
  - Zowe sub-projects repositories
  - Zowe operations squads repositories

When you decide to work on an issue, check the comments on that issue to ensure that it's not taken by anyone. If nobody is working on it, comment on that issue to let others know that you want to work on it to avoid duplicate work. The squad can assign that issue to you and provide guidance as well.

• You can also reach out to the Zowe squads on Slack to check with the squads if there is any good starter issue that you can work on.

### **Send a Pull Request**

All code in Zowe aligns with the established licensing and copyright notice guidelines.

Before submitting a Pull Request, review the general Zowe Pull Request Guidelines and make sure that you provide the information that is required in the Pull Request template in that specific repo.

All Zowe commits need to be signed by using the Developer's Certificate of Origin 1.1 (DCO), which is the same mechanism that the Linux® Kernel and many other communities use to manage code contributions. You need to add a Signed-off-by line as a part of the commit message. Here is an example Signed-off-by line, which indicates that the submitter accepts the DCO:

Signed-off-by: John Doe <john.doe@hisdomain.com>

You can find more information about DCO signoff in the zlc repo.

### **Report security issues**

Please direct all security issues to zowe-security@lists.openmainframeproject.org. A member of the security team will reply to acknowledge receipt of the vulnerability and coordinate remediation with the affected project.

# **Contribution guidelines**

Check out the contribution guidelines for different components and squads to learn how to participate.

- Zowe CLI
- Zowe API Mediation Layer
- Zowe Application Framework
- Zowe Explorer

- Zowe Client SDKs
- Zowe Docs

### **Promote Zowe**

- Contribute a blog about Zowe. Read the Zowe blog guidelines to get started.
- Present Zowe on conferences and social channels

# **Helpful resources**

- General code guidelines
- UI guidelines
- Zowe learning resources

# **Code categories**

The Zowe™ codebase consists of a few key areas, with both unique and shared guidelines that define how to write new code. A few such areas are:

- Server Core
- Server Security
- Microservices
- Zowe Desktop Applications
- Zowe Application Framework
- Zowe CLI and CLI Plug-ins
- Imperative CLI Framework

# **Programming languages**

For each area of the codebase, there are established and favored programming languages. Each repository in Github identifies the primary language used. Some of the basic skills needed to contribute to the project include:

- CLI Node.js, TypeScript
- Desktop UI Node.js, JavaScript
- APIs C, Assembler, Java, Spring
- API Mediation Layer Java, Spring

Note: JavaScript is not recommended and should be avoided in favor of Typescript to utilize typing.

# **Component-specific guidelines and tutorials**

This "Code Guidelines" section provides high-level best practices. Each component may have more specific contribution guidelines. Look for a CONTRIBUTING.md file in the component's GitHub repository for specific details.

To learn more about how to develop Zowe applications and plug-ins or extending Zowe with APIs, see Extending.

# **General code style guidelines**

All code written in the languages described in Code categories should adhere to the following guidelines to facilitate collaboration and understanding.

**Note:** Uncertainties, unimplemented but known future action-items, and odd/specific constants should all be accompanied with a short comment to make others aware of the reasoning that went into the code.

### Whitespaces

Do not use tabs for whitespace. Use 2 spaces per tab instead.

# **Naming Conventions**

Self-documenting code reduces the need for extended code comments. It is encouraged to use names as long as necessary to describe what is occurring.

#### **Functions and methods**

Methods should be named as verbs (for example, get or set), while Objects/Classes should be nouns.

Objects and functions should be CamelCase. Methods on Objects should be dromedaryCase.

#### Variables

Constants should be CAPITALIZED\_AND\_UNDERSCORED for clarity, while variables can remain dromedaryCase.

Avoid non-descriptive variable names such as single letters (except for iteration in loops such as i or j) and variable names that have been arbitrarily shortened (Don't strip vowels; long variable names are OK).

# **Pull requests guidelines**

The Zowe<sup>™</sup> source code is stored in GitHub repositories under the Zowe GitHub project. You contribute to the project through Pull Requests in GitHub.

Each pull request is made against a repository that has assigned "maintainers". Pull requests cannot be merged without the approval of at least one maintainer, who will review Pull Requests to ensure that they meet the following criteria:

- The code in the pull request must adhere to the General Code Style Guidelines.
- The code must compile/transpile (where applicable) and pass a smoke-test such that the code is not known to break the current state of Zowe.
- The pull request must describe the purpose and implementation to the extent that the maintainer understands what is being accomplished. Some pull requests need less details than others.
- The pull request must state how to test this change, if applicable, such that the maintainer or a QA team can check correctness. The explanation may simply be to run included test code.
- If a pull request depends upon a pull request from the same/another repository that is pending, this must be stated such that maintainers know in which order to merge open pull requests.

Version: v1.25.x LTS

# **Documentation Guidelines**

Documentation of Zowe<sup>™</sup> comes in various forms depending on the subject being detailed. In general, consider how you can help end users and contributors through external documentation, in-product help, error messages, etc... and open an issue in zowe/docs-site if you need assistance.

### **Contributing to external documentation**

The external documentation for the Zowe project, Zowe Docs, is completely open-source. See How to contribute for more information about contributing to the documentation.

Consider: Release Notes, Install/Config/User Guides, Developer Tutorials, etc...

# **Component Categories**

Provide the following documentation depending on the component that you contribute to:

#### Server Core

Principles of operation and end-user guides (configuration, troubleshooting) should be documented on Zowe Docs site. Code documentation follows language-specific formats.

#### **Server Security**

Principles of operation and end-user guides (configuration, troubleshooting) should be documented on Zowe Docs site. Code documentation follows language-specific formats.

#### Microservices

Microservices implement a web API, and therefore must be documented for understanding and testing. These web APIs must be accompanied with documentation in the Swagger (https://swagger.io/) format. These documents must be Swagger 2.0, .yaml extension files. Zowe Application Framework plug-ins that implement microservices should store these files within the /doc/swagger folder.

#### **Zowe Desktop Applications**

Zowe Desktop applications should include documentation that explains how to use them, such that this documentation can integrate with a Zowe Desktop documentation reader. This is not strictly API documentation, but rather user guides that can display within the Desktop GUI. The preferred documentation format is a .md extension file that exists in the /doc/guide folder of an App.

#### Web Framework

Principles of operation and end-user guides (configuration, troubleshooting) should be documented on Zowe Docs site. Code documentation follows language-specific formats.

#### **CLI Plugins**

Provide a readme.md file for developers (overview, build, test) as well as end-user documentation for your plug-in on Zowe Docs site.

For more information, see the CLI documentation contribution guidelines.

#### **Core CLI Imperative CLI Framework**

Contributions that affect end users of the CLI should be documented on Zowe Docs site.

Contributions that affect the underlying Imperative CLI Framework should be documented in the GitHub Wiki for future developers using the framework.

Code documentation follows language-specific formats.

### **Programming Languages**

Each of the common languages in Zowe have code-documentation-generation tools, each with their own incode comment style requirements to adhere to in order to generate readable API references. Objects and functions of interest should be commented in accordance to the language-specific tools to result in output that serves as the first point of documentation for APIs.

#### Typescript

When writing TypeScript code, comment objects and functions in compliance with JSDoc. If you are writing in an area of the codebase that does not yet have a definition file for JSDoc, define a configuration file that can be used for future documentation of that code.

#### Java

When writing TypeScript code, comment objects and functions in the Javadoc format.

#### С

When writing C code, comment functions and structures in compliance with Doxygen.

# Version: v1.25.x LTS

This style guide is the visual language that represents Zowe™. It is a living document that will be updated based on the needs of our users and software requirements.

# Clear

Our users rely on our software to help them be efficient in their work. The interfaces and experiences that we design should be clear so that there is never confusion about where to click or how to take the next step. Users should always feel confident in their actions.

# Consistent

Users should be able to look at Zowe software products and know that they are in a family. Each software product is different, but should use similar patterns, icons, and interactions. If a user switches to a new product within Zowe, it should feel familiar.

# Smart

Our users are intelligent, and they need smart software. Zowe design patterns should always compliment the user's intelligence and reflect the user's complex work environment. Designs should align with the Zowe design language by putting the human needs of the user first.

# Colors

Color brings a design to life. Color is versatile; it's used to express emotion and tone, as well as place emphasis and create associations. Color should always be used in meaningful and intentional ways to create patterns and visual cues.

# **Color palette**

The Zowe<sup>™</sup> color palette is designed and implemented in a theme-able manner. The universal color variables are determined by common roles and usage; it is not based singularly on a color value (i.e. unique hex code). The same color value might be assigned to multiple variables in a theme's palette when the values have distinctly different roles.

A universal variable can also have multiple associated roles when the color is consistently used across those roles. This allows for uniform color application across themes, while giving each theme the freedom to express its own individuality at a more detailed level.

#### **Light theme**

#### **Dark theme**

### Color contrast | WCAG AA standards

• Type colors

All type color combinations on Zowe must pass WCAG AA standards of 4.5:1 for normal text and 3:1 for large text. For larger text, if the font weight is light (300) or normal (400) the text should be no smaller than 24px. If the font weight is Semi-Bold (600) then the large text should be no smaller than 19px.

• Body Text (4.5:1)

• Large Text (3:1): at least 24px / 19px semi-bold

WCAG guidelines: https://www.w3.org/WAI/standards-guidelines/wcag/

Contrast Checker Tool: https://webaim.org/resources/contrastchecker/

Version: v1.25.x LTS

# Typography

Typography is used to create clear hierarchies, useful organizations, and purposeful alignments that guide users through the product and experience. It is the core structure of any well designed interface.

# Typeface

Title typeface: Roboto Condensed

Body typeface: Roboto

Sample:

# Font weight

Font weight is an important typographic style that can add emphasis and is used to differentiate content hierarchy. Font weight and size pairings must be carefully balanced. A bold weight will always have more emphasis than a lighter weight font of the same size. However, a lighter weight font can rank hierarchically higher than a bold font if the lighter weight type size is significantly larger than the bold.

Roboto font family provides a wide range of weights. However, only SemiBold, Regular, Light should be used for product design.

• Font-weight: 300 / Light

# Light

Should only be used at sizes greater than or equal to 18px / 1.125rem

• Font-weight: 400 / Normal

# Regular

• Font-weight: 500 / Semi-bold

# Semi-Bold

# Body copy

We recommended that you use two sizes for body copy. The first size is UI specific. To maximize screen real estate we chose a smaller 14px / 0.875rem body copy size for the standard UI console. However, for areas that have prolonged reading, such as Documentation, we use a larger body copy size of 16px / 1rem to enhance readability.

# Line scale

- 1.333 Perfect Fourth-type scale desktop
- 1.2 Minor Third type-scale mobile

# Line-height

Line-height, traditionally known as leading, is one of several factors that directly contribute to readability and pacing of copy. Line-heights are based on the size of the font itself. Ideal line-heights for standard copy have a ratio of 1:1.5 (typesize : line-height). For example, a type at 16px / 1rem would have a line-height of 1.5rem / 24px (16 x 1.5). The exception to this rule are headings, which need less spacing and therefore have a line-height ratio of 1:1.25.

# **Embed font**

To embed your selected fonts into a web page, copy the following code into the <head> of your HTML document:

# Import font

### Specify in CSS

Use the following CSS rules to specify these families:

# Grid

Grid systems are used for creating page layouts through a series of rows and columns that house your content. Zowe<sup>™</sup> uses a responsive, mobile-first, fluid grid system that appropriately scales up to 12 columns as the device or view port size increases.

### 12 column grid

A 12 column grid is recommended. 12 is a well-distributed division that provides a good range of widths to assign to content. It is dividable by 2, 3, 4 and 6, which allows flexibility. Many frameworks, such as Bootstrap and Pure, use a 12 column grid by default. Other grid systems like a 5 column grid can reduce flexibility, balance, and consistency.

### **Gutters**

Columns create gutters (gaps between column content) through padding. For devices with a screen width greater than 768px, the column padding is 20px. For devices with a screen width less than 768px, the column padding is 10px.

Screen width  $\geq$  768px = 20px gutters

Screen width 768px = 10px gutters

### Columns

Zowe designs should be limited to 12 columns. If designers feel that they need fewer columns in their grid, they can specify the number of 12 available columns they wish to span.

This can translate to percentages of the twelve columns. Using this method, a designer can create a folded, less granular grid. For example, if your component spans three equal columns, that is equal to 25% of twelve columns.

Column count: 12

### Margins

The 12 column grid does not have a maximum width. It has a width of 100%, with built in margins that create padding between column count and the edges of the viewport.

In devices with a screen width greater than 768px, the margins are **5%** on the left, and **5%** on the right.

In devices with a screen width less than 768px, the margins are **3%** on the left, and **3%** on the right.

Example: Screen Width > 768px

Example: Screen Width 320px

Version: v1.25.x LTS

# Iconography

Icons are key component for a successful UI design because they are a visual way to help add meaning to elements.

Font Awesome is a robust icon library that allows for an easy addition to any web project. Scalable vector icons that can instantly be customized — size, color, drop shadow, and anything that can be done with the power of CSS.

- One Font, Hundreds of Icons In a single collection, Font Awesome is a pictographic language of web-related actions.
- **No JavaScript Required** Fewer compatibility concerns because Font Awesome doesn't require JavaScript.
- Infinite Scalability Scalable vector graphics means every icon looks awesome at any size.
- Free, as in Speech Font Awesome is completely free for commercial use. Check out the license.
- **CSS Control** Easily style icon color, size, shadow, and anything that's possible with CSS.
- **Perfect on Retina Displays** Font Awesome icons are vectors, which mean they're gorgeous on high-resolution displays.
- Plays Well with Others Originally designed for Bootstrap, Font Awesome works great with all frameworks.
- **Desktop Friendly** To use on the desktop or for a complete set of vectors, check out the cheatsheet.
- Accessibility-minded Font Awesome loves screen readers and helps make your icons accessible on the web.

To learn more or download the library go to www.fontawesome.com

# Version: v1.25.x LTS Application icon

### **General rules**

**Embrace simplicity.** Use a simple, unique shape or element that represents the essence of the application. Avoid excessive details and redundant shading.

**Use the Zowe™ color palette.** Avoid using a monochromatic palette for your icons. Use the Zowe color palette to ensure that the icons have a consistent look.

**Use unique shapes and design elements.** Avoid using single commonly used design elements, such as the gear, document, or folder. These elements can reduce recognizability. Do not use photos and screenshots. Keep icons simple and abstract.

**Avoid labels and text.** Short, commonly used abbreviations are acceptable, if necessary. Remember that all icons have center-aligned labels beneath them.

**Use brand identity.** If your Zowe application has a brand identity element such as a logo, you can use it. Remember to include the copyright symbol.

### Shape, size, and composition

**Use a flat design style.** Flat design focuses on open space, bright colors, and flat graphics or illustrations. Our minimalistic design approach puts the emphasis on usability.

A flat icon has clean, crisp edges and a flat dimensional layout.

**Use solid fill shapes.** Most Zowe App icons have solid fill shapes, which are more readable on dark backgrounds.

Use the circle shape for the background application icons. Set the outer corners to 100% opacity. Create an image file that is 87x87 pixels, and save the file in PNG format.

#### Maintain consistent visual proportions.

### **Colors and shades**

#### Verify the contrast

Verify that the background color of the icon provides enough contrast against the desktop.

#### Use the Zowe palette

To ensure that your app icons are clear and consistent, use the Zowe color palette. If you need to use wellestablished brand identity elements, you can use the colors that are associated with the brand.

#### **Layer Shadows**

Use smooth shadows to represent that some elements are on different layers and should be visually separated. Avoid using too many layers because they can overcomplicate the icon.



#### Use the long shadow for consistency.

Although the long shadow effect does not have any semantic meaning, it adds focus to the main icon shape and identifies the central, most meaningful element.

Use the gradient shadow settings shown in the following image, or use a flat non-gradient shadow with 20% opacity and #000000 color.

# **Contributing to Zowe Documentation**

- Contributing to Zowe Documentation
  - Before You Get Started
  - Getting Started Checklist
  - The Zowe Documentation Repository
  - Sending a GitHub Pull Request
  - Opening An Issue for Zowe Documentation
  - Documentation Style guide
    - Headings and titles
    - Technical elements
    - Tone
    - Word usage
    - Graphics
    - Abbreviations
    - Structure and format
    - Word usage

### **Before You Get Started**

You are welcome to contribute to the Zowe<sup>™</sup> documentation repository. Anyone can open an issue about documentation, or contribute a change with a pull request (PR) to the zowe/docs-site GitHub repository. However, before contributing a documentation change to the repository, you should be familiar with:

- Git and Github: To learn about git and GitHub, refer to the Github Guides.
- Slack: The Zowe Documentation team communicates using the Slack application. To learn about Slack, refer to the Slack Help Center. The Zowe team is part of the Open Mainframe Project channel.
- Markdown Language: The Zowe documentation is written in Markdown language. To learn about Markdown, refer to The Markdown Guide

In addition to being familiar with the Zowe community and how we work together, you will need to sign the CNCF Contributor License Agreement. The Contributor License Agreement defines the terms under which you contribute to Zowe documentation. Contributions to Zowe documentation are reviewed before being committed to the repository. Committing changes to the Zowe repository requires additional access rights.

See https://github.com/zowe/community/blob/master/COMMITTERS.md. Also see Participating in Zowe Documentation for more details about roles and permissions.

### **Getting Started Checklist**

If you are ready to get started contributing to the Zowe Documentation repository:

- Verify that you are familiar with the concepts in Before You Get Started.
- Familiarize yourself with the Zowe documentation repository
- Verify that you can open a pull request and review changes
- Open an issue for Zowe documentation if you find a problem
- Read the documentation style guide

### **The Zowe Documentation Repository**

The Zowe documentation is managed in a GitHub repository.

- Review the site's overall organization and structure
- Review the help files related to your planned changes or addition

### Sending a GitHub Pull Request

You can provide suggested edit to any documentation page by using the **Propose content change in GitHub** link on each page. After you make the changes, you submit updates in a pull request for the Zowe content team to review and merge.

Follow these steps:

- 1. Click **Propose content change in GitHub** on the page that you want to update.
- 2. Make the changes to the file.
- 3. Scroll to the end of the page and enter a brief description about your change.
- 4. Optional: Enter an extended description.
- 5. Select **Propose file change**.
- 6. Select Create pull request.

### **Opening An Issue for Zowe Documentation**

You can request the documentation to be improved or clarified, report an error, or submit suggestions and ideas by opening an issue in GitHub for the Zowe content team to address. The content team tracks the issues and works to address your feedback.

Follow these steps:

- 1. Click the **GitHub** link at the top of the page.
- 2. Select Issues.
- 3. Click New issue.
- 4. Enter a title and description for the issue.
- 5. Click **Submit new issue**.

### **Documentation Style guide**

This section gives writing style guidelines for the Zowe documentation.

- Headings and titles
- Technical elements
- Tone
- Word usage
- Graphics
- Abbreviations
- Structure and format

#### **Headings and titles**

#### Use sentence-style capitalization for headings

Capitalize only the initial letter of the first word in the text and other words that require capitalization, such as proper nouns. Examples of proper nouns include the names of specific people, places, companies, languages, protocols, and products.

Example: Verifying that your system meets the software requirements.

#### For tasks and procedures, use gerunds for headings.

Example:

- Building an API response
- Setting the active build configuration

#### For conceptual and reference information, use noun phrases for headings.

Example:

- Query language
- Platform and application integration

#### Use headline-style capitalization for only these items:

Titles of books, CDs, videos, and stand-alone information units.

#### Example:

- Installation and User's Guide
- Quick Start Guides or discrete sets of product documentation

#### Make headings brief, descriptive, grammatically parallel, and, if possible, task oriented.

If the subject is a functional overview, begin a heading with words such as Introduction or Overview rather than contriving a pseudo-task-oriented heading that begins with Understanding, Using, Introducing, or Learning.

#### **Technical elements**

#### Variables

Style:

• Italic when used outside of code examples,

Example: myHost

• If wrap using angle brackets <> within code examples, italic font is not supported.

Example:

- put <pax-file-name>.pax
- Where *pax-file-name* is a variable that indicates the full name of the PAX file you download. For example, zoe-0.8.1.pax.

#### Message text and prompts to the user

Style: Put messages in quotation marks.

Example: "The file does not exist."

#### Code and code examples

Style: Monospace

Example: java -version

#### Command names, and names of macros, programs, and utilities that you can type as commands

Style: Monospace

Example: Use the **BROWSE** command.

#### Interface controls

Categories: check boxes, containers, fields, folders, icons, items inside list boxes, labels (such as **Note:**), links, list boxes, menu choices, menu names, multicolumn lists, property sheets, push buttons, radio buttons, spin buttons, and Tabs

#### Style: Bold

Example: From the **Language** menu, click the language that you want to use. The default selection is **English**.

#### **Directory names**

Style: Monospace

Example: Move the install.exe file into the newuser directory.

#### File names, file extensions, and script names

#### Style: Monospace

#### Example:

- Run the install.exe file.
- Extract all the data from the .zip file.

#### Search or query terms

Style: Monospace

Example: In the Search field, enter Zowe.

#### Citations that are not links

Categories: Chapter titles and section titles, entries within a blog, references to industry standards, and topic titles in IBM Knowledge Center

Style: Double quotation marks

Example:

- See the "Measuring the true performance of a cloud" entry in the Thoughts on Cloud blog.
- See "XML Encryption Syntax and Processing" on the W3C website.
- For installation information, see "Installing the product" in IBM Knowledge Center.

#### Tone

#### Use simple present tense rather than future or past tense, as much as possible.

#### Example:

 $\checkmark$  The API returns a promise.

X The API will return a promise.

#### Use simple past tense if past tense is needed.

#### Example:

 $\checkmark$  The limit was exceeded.

X The limit has been exceeded.

#### Use active voice as much as possible

Example:

 $\checkmark$  In the Limits window, specify the minimum and maximum values.

X The Limits window is used to specify the minimum and maximum values.

Exceptions: Passive voice is acceptable when any of these conditions are true:

- The system performs the action.
- It is more appropriate to focus on the receiver of the action.
- You want to avoid blaming the user for an error, such as in an error message.
- The information is clearer in passive voice.

Example:

- $\checkmark$  The file was deleted.
- X You deleted the file.

#### Using second person such as "you" instead of first person such as "we" and "our".

In most cases, use second person ("you") to speak directly to the reader.

#### End sentences with prepositions selectively

Use a preposition at the end of a sentence to avoid an awkward or stilted construction.

Example:

- $\checkmark$  Click the item that you want to search for.
- X Click the item for which you want to search.

#### Avoid using "Please", "thank you"

In technical information, avoid terms of politeness such as "please" and "thank you". "Please" is allowed in UI only when the user is being inconvenienced.

Example: Indexing might take a few minutes. Please wait.

#### Avoid anthropomorphism.

Focus technical information on users and their actions, not on a product and its actions.

Example:

✓ User focus: On the Replicator page, you can synchronize your local database with replica databases.

X Product focus: The Replicator page lets you synchronize your local database with replica databases.

Avoid complex sentences that overuse punctuation such as commas and semicolons.

#### Word usage

Note headings such as Note, Important, and Tip should be formatted using the lower case and bold format.

Example:

- Note:
- Important!
- Tip:

#### Use of "following"

For whatever list or steps we are introducing, the word "following" should precede a noun.

Example:

- Before a procedure, use "Follow these steps:"
- The <component\_name> supports the following use cases:
- Before you install Zowe, review the following prerequisite installation tasks:

Avoid ending the sentence with "following".

Example:

#### $\mathbf{X}$ Complete the following.

 $\checkmark$  Complete the following tasks.

#### Use a consistent style for referring to version numbers.

When talking about a specific version, capitalize the first letter of Version.

Example:

✓ Java Version 8.1 or Java V8.1

X Java version 8.1, Java 8.1, or Java v8.1

When just talking about version, use "version" in lower case.

Example: Use the latest version of Java.

#### Avoid "may"

Use "can" to indicate ability, or use "might" to indicate possibility.

#### Example:

- Indicating ability:
  - ✓ You can use the command line interface to update your application."
  - X "You may use the command line interface to update your application."
- Indicating possibility:
  - $\checkmark$  "You might need more advanced features when you are integrating with another application."
  - X "You may need more advanced features when you are integrating with another application."

#### Use "issue" when you want to say "run/enter" a command.

Example: At a command prompt, type the following command:

#### Graphics

• Use graphics sparingly.

Use graphics only when text cannot adequately convey information or when the graphic enhances the meaning of the text.

• When the graphic contains translatable text, ensure you include the source file for the graphic to the doc repository for future translation considerations.

#### **Abbreviations**

Do not use an abbreviation as a noun unless the sentence makes sense when you substitute the spelled-out form of the term.

Example:

- X The tutorials are available as PDFs. [portable document formats]
- $\checkmark$  The tutorials are available as PDF files.

#### Do not use abbreviations as verbs.

Example:

- $\mathbf{X}$  You can FTP the files to the server.
- $\checkmark$  You can use the FTP command to send the files to the server.

#### Do not use Latin abbreviations.

Use their English equivalents instead. Latin abbreviations are sometimes misunderstood.

Latin	English equivalent
e.g.	for example
etc.	and so on. When you list a clear sequence of elements such as "1, 2, 3, and so on" and "Monday, Tuesday, Wednesday, and so on." Otherwise, rewrite the sentence to replace "etc." with something more descriptive such as "and other output."

Latin	English equivalent
i.e.	that is

Spell out the full name and its abbreviation when the word appears for the first time. Use abbreviations in the texts that follow.

Example: Mainframe Virtual Desktop (MVD)

#### **Structure and format**

Add "More information" to link to useful resources or related topics at the end of topics where necessary.

#### Word usage

The following table alphabetically lists the common used words and their usage guidelines.

Do	Don't
API Mediation Layer	
application	арр
Capitalize "Server" when it's part of the product name	
data set	dataset
Java	java
IBM z/OS Management Facility (z/OSMF) z/OSMF	zosmf (unless used in syntax)
ID	id
PAX	рах

Do	Don't
personal computer PC server	machine
later	higher Do not use to describe versions of software or fix packs.
macOS	MacOS
Node.js	node.js Nodejs
plug-in	plugin
REXX	Rexx
UNIX System Services z/OS UNIX System Services	USS
zLUX	ZLUX zLux
Zowe CLI	

# Zowe CLI command reference guide

View detailed documentation on commands, actions, and options in Zowe CLI. The reference document is based on the @zowe-v1-lts version of the CLI. You can read an interactive online version, download a PDF document, or download a ZIP file containing the HTML for the online version:

- Browse online
- Download CLI reference in PDF format
- Download CLI reference in ZIP format

## **Zowe API reference**

Find and learn about the Zowe APIs that you can use.

- REST API for the Data sets and z/OS Unix Files Services
- **REST API for the API Gateway service**
- REST API for the JES Jobs Service
- REST API for ZLUX Plug-in

Version: v1.25.x LTS

# **Zowe Binaries - Bill of Materials**

The following materials are distributed with Zowe<sup>™</sup> binaries:

### **Zowe PAX**

File Path	Description	Source Location	Build Script(s)
zowe-x.y.z.pax	Root PAX file containing all Zowe z/OS Components	Multiple open source repositories within zowe, detailed below.	Zowe Install/Packaging Pipeline
manifest.json	Zowe PAX Manifest	zowe-install- packaging	Zowe Install/Packaging Pipeline
bin/apiml_cm.sh	APIML Certificate Management Script	zowe-install- packaging	Zowe Install/Packaging Pipeline
bin/zowe-support.sh	In development script to gather Zowe z/OS diagnostics.	zowe-install- packaging	Zowe Install/Packaging Pipeline
bin/internal/run-zowe.sh	Zowe entrypoint script, executed from the Zowe STC	zowe-install- packaging	Zowe Install/Packaging Pipeline
bin/internal/zowe-set-env.sh	Sets ENVs for Zowe install and runtime	zowe-install- packaging	Zowe Install/Packaging Pipeline
bin/zowe-setup-certificates.sh	Script to generate Zowe TLS certificates	zowe-install- packaging	Zowe Install/Packaging Pipeline

File Path	Description	Source Location	Build Script(s)
bin/utils/zowe-install-iframe- plugin.sh	Script to install default Zowe Application Framework plugins	zowe-install- packaging	Zowe Install/Packaging Pipeline
bin/zowe-init.sh	Script to initialize Zowe installation	zowe-install- packaging	Zowe Install/Packaging Pipeline
bin/zowe-setup-certificates.env	Environment configurations for certificate management	zowe-install- packaging	Zowe Install/Packaging Pipeline
bin/zowe-configure-instance.sh	Script which configures installed instance of Zowe	zowe-install- packaging	Zowe Install/Packaging Pipeline
licenses/zowe_licenses_full.zip	License archive for Zowe third party dependencies	N/A	Zowe License Scan Pipeline
files/zlux/sample-iframe-app.pax	Sample iFrame ZAF App	sample-iframe-app	N/A
files/zlux/sample-react-app.pax	Sample React ZAF App	sample-react-app	N/A
files/zlux/tn3270-ng2.pax	TN3270 ZAF App	tn3270-ng2	N/A
files/zlux/vt-ng2.pax	USS/VT Terminal Emulator ZAF App	vt-ng2	N/A

File Path	Description	Source Location	Build Script(s)
files/zlux/config/zluxserver.json	Zowe Application Framework Config JSON	zowe-install- packaging	Zowe Install/Packaging Pipeline
files/zlux/config/plugins/*.json	Zowe Application Framework JSON Configuration Files	zowe-install- packaging	Zowe Install/Packaging Pipeline
files/zlux/zlux-workflow.pax	Workflow ZAF App	zlux-workflow	N/A
files/zlux/zlux-editor.pax	Editor ZAF App	zlux-editor	N/A
files/zlux/zlux-core.pax	Zowe Application Framework Core Components	zlux	N/A
files/zlux/sample-angular- app.pax	Sample Angular ZAF App	sample-angular-app	N/A
files/zlux/zosmf-auth.pax	z/OSMF Authentication ZAF App	zosmf-auth	N/A
files/zlux/zss-auth.pax	zSS Authentication ZAF App	zss-auth	N/A
files/jcl/ZWESECUR.jcl	JCL to define Zowe z/OS security definitions	zowe-install- packaging	Zowe Install/Packaging Pipeline
files/jcl/ZWENOSEC.jcl	JCL to remove Zowe z/OS Security definitions	zowe-install- packaging	Zowe Install/Packaging Pipeline

File Path	Description	Source Location	Build Script(s)
files/jcl/ZWESVSTC.jcl	JCL to start Zowe (Zowe STC)	zowe-install- packaging	Zowe Install/Packaging Pipeline
files/jobs-api-server-*-boot.jar	Java binaries - Zowe Jobs REST API Server	jobs sources	Jobs Pipeline
files/workflows/ZWEWRF02.xml	Zowe Install Workflow Definition	zowe-install- packaging	Zowe Install/Packaging Pipeline
files/workflows/ZWEYML02.yml	Zowe Install Workflow Configuration Variables	zowe-install- packaging	Zowe Install/Packaging Pipeline
files/api-mediation-package- *.pax	PAX Archive containing Zowe API Mediation Layer Components	api layer	api-layer pipeline
files/explorer-uss-*.pax	PAX Archive containing Zowe Desktop USS Plugin	explorer-uss	explorer-uss pipeline
files/explorer-jes-*.pax	PAX Archive containing Zowe Desktop JES Plugin	explorer-jes	explorer-jes pipeline
files/data-sets-api-server-*- boot.jar	Java binaries - Zowe Data-Sets REST API Server	data-sets	Data-Sets pipeline
files/scripts/files-api-start.sh	Script to start the Data-Sets Server	data-sets	Data-Sets Pipeline

File Path	Description	Source Location	Build Script(s)
files/scripts/files-api-validate.sh	Script to validate the Data-Sets Server Configuration	data-sets	Data-Sets Pipeline
files/scripts/files-api- configure.sh	Script to configure the Data-Sets Server Configuration	data-sets	Data-Sets Pipeline
files/scripts/jobs-api-validate.sh	Script to validate the Jobs Server Configuration	jobs	Jobs Pipeline
files/scripts/jobs-api-start.sh	Script to start the Jobs server	jobs	Jobs Pipeline
files/scripts/jobs-api- configure.sh	Script to configure the Jobs Server Configuration	jobs	Jobs Pipeline
files/explorer-mvs-*.pax	PAX Archive containing Zowe Desktop MVS Plugin	explorer-mvs sources	Explorer MVS Pipeline
files/zss.pax	Zowe ZSS Cross- Memory Server	ZSS	zss build scripts
install/zowe-check-prereqs.sh	Script to check required environment configuration(s)	zowe-install- packaging	Zowe Install/Packaging Pipeline
install/zowe-install.sh	Script to initiate Zowe automated installation	zowe-install- packaging/install	Zowe Install/Packaging Pipeline

File Path	Description	Source Location	Build Script(s)
scripts/allocate-dataset.sh	Script to allocate a dataset	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/check-dataset-dcb.sh	Script to check Database DCB property	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/check-dataset-exist.sh	Script to check if a dataset exists	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/instance.template.env	Zowe Instance Template ENV Configuration	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/ocopyshr.clist	A CList to copy a USS file to a PDS member	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/ocopyshr.sh	Script to copy a uss JCL file to a shared PDS	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/opercmd	REXX file to issue z/OS console commands	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/opercmd.rex	REXX script to issue an operator command and trap output	zowe-install- packaging	Zowe Install/Packaging Pipeline

File Path	Description	Source Location	Build Script(s)
scripts/tag-files.sh	Script to change USS file tags	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/utils/configure-java.sh	Script to configure Java Home ENV variable	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/utils/configure-node.sh	Script to configure Node Home ENV variable	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/utils/error.sh	Script to track and handle errors	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/utils/mcopyshr.clist	CLIST to copy PDS member to another PDS	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/utils/validate-apiml- variables.sh	Validate APIML Configuration Variables	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/utils/validate-directory- is-accessible.sh	Validate user can access directory	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/utils/validate-directory- is-writable.sh	Validate user can write to directory	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/utils/validate-java.sh	Validate Java version and PATH	zowe-install- packaging	Zowe Install/Packaging Pipeline

File Path	Description	Source Location	Build Script(s)
scripts/utils/validate-keystore- directory.sh	Validate Keystore Directory	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/utils/validate-node.sh	Validate Node Version and PATH	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/utils/validate-port- available.sh	Validate a port is available	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/utils/validate-static- definition-directory.sh	Validate APIML Static Definition Dir	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/utils/validate-zosmf- host-and-port.sh	Validate z/OSMF Configuration	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/utils/validate-zowe- prefix.sh	Validate configured Zowe prefix	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/utils/zosmfHttpRequest.js	Node.js script to validate z/OSMF info	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/utils/zowe-copy-to- JES.sh	Copy SAMPLIB member into JES PROCLIB concatenation	zowe-install- packaging	Zowe Install/Packaging Pipeline

File Path	Description	Source Location	Build Script(s)
scripts/utils/zowe-install-proc.sh	Copy Zowe server PROC to JES concatenation	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/utils/zowe-install- xmem.sh	Copy cross-memory server artifacts to destination	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/wait-for-job.sh	Script to submit job and wait for completion	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/zowe-install-MVS.sh	Script which installs Zowe datasets, such as LOADLIB	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/zowe-install-api- mediation.sh	Script which installs Zowe API Mediation Layer	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/zowe-install-explorer- api.sh	Script which installs Explorer API Server	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/zowe-install-explorer- ui.sh	Script which installs Explorer UI App	zowe-install- packaging	Zowe Install/Packaging Pipeline
scripts/zowe-install-zlux.sh	Script which extracts and install Zowe Desktop	zowe-install- packaging	Zowe Install/Packaging Pipeline

### Zowe CLI Package

File Path	Description	Source Location	Build Script(s)
zowe-cli-package-1.9.0.zip	Zowe CLI Package containing the core Zowe CLI and SCS plugin	Multiple open source repositories within zowe	zowe-cli- standalone- package pipeline
licenses/zowe_licenses_full.zip	License archive for Zowe third party dependencies	N/A	Zowe License Scan Pipeline
zowe-cli.tgz	Zowe CLI	zowe-cli	zowe-cli pipeline
secure-credential-store-for- zowe-cli.tgz	Secure Credential Store for Zowe CLI	zowe-cli-scs- plugin	zowe-cli-scs- plugin pipeline

### **Zowe CLI Plugins**

File Path	Description	Source Location	Build Script(s)
zowe-cli-plugins-1.9.0.zip	Zowe CLI Package containing Zowe CLI Plugins	Multiple open source repositories within zowe	zowe-cli- standalone- package pipeline
licenses/zowe_licenses_full.zip	License archive for Zowe third party dependencies	N/A	Zowe License Scan Pipeline
cics-for-zowe-cli.tgz	IBM® CICS® Plug-in for Zowe CLI	zowe-cli-cics-plugin	zowe-cli-cics- plugin pipeline
db2-for-zowe-cli.tgz	IBM® Db2® for z/OS® Plug-in for Zowe CLI	zowe-cli-db2-plugin	zowe-cli-db2- plugin pipeline

File Path	Description	Source Location	Build Script(s)
zos-ftp-for-zowe-cli.tgz	IBM® z/OS FTP Plug-in for Zowe CLI	zowe-cli-ftp-plugin	zowe-cli-ftp- plugin pipeline
ims-for-zowe-cli.tgz	IBM® IMS™ Plug-in for Zowe CLI	zowe-cli-ims-plugin	zowe-cli-ims- plugin pipeline
mq-for-zowe-cli.tgz	IBM® MQ Plug-in for Zowe CLI	zowe-cli-mq-plugin	zowe-cli-mq- plugin pipeline