SOLUTION PARTNER FOR **SMART TECHNOLOGY**

LENA

User Guide

LENA Support

Version 1.3.4.2

Table of Contents

Chapter 1. Overview

1.1. What is LENA?

LENA is a web middleware solution that includes all components necessary for serving JAVA J2EE Web Applications in Enterprise environments.

LENA consists of Server products that provide actual web services and a Web UI-based Manager Console for integrated management. Users can easily perform Server installation, Parameter configuration, and inter-product integration through the Manager Console, and with LENA's user-friendly UX/UI design, even users unfamiliar with web middleware solutions can quickly learn how to use them and acquire web middleware-related knowledge.

LENA provides various convenience features by consolidating years of operational know-how from web middleware operators in data center/cloud environments. Additionally, it provides Clustering with high availability and fault tolerance, and failure diagnostics/response functionality to stably process large-scale transactions and minimize service failures.

The following sections explain LENA's features in more detail.

1.2. LENA Features

Enterprise Requirements Provision

LENA Web Application Server EE (J2EE Edition) supports J2EE specifications such as EJB, JTA/XA, JMS, JAX-WS required for executing Enterprise Web Applications. Additionally, it has achieved improvements in startup performance and Application Deploy performance compared to third-party WAS, and resource usage efficiency such as CPU/Memory has also been improved. For high availability, Session Server is provided by default in Enterprise Edition for essential Session Clustering.

Open Source Compatibility Guarantee

LENA Web Server and LENA WAS are implemented on Open Source Base, ensuring perfect Open Source compatibility. Web Applications written on Open Source basis can be applied to LENA without separate modifications, greatly reducing transition effort. Additionally, using standard technologies for libraries and configuration resolves vendor dependency and strengthens users' IT ownership.

Intelligent Failure Diagnostics/Response and Service Tracing

It can perform diagnostics based on pre-defined rules for representative failure situations such as Thread Pool Full / Hang / Out of memory and take appropriate measures. Based on real-time collected monitoring data, it analyzes and prevents failure situations through Fake Page bypass or forced restart before servers lead to actual failures, or minimizes failure time even if failures occur. Simultaneously, it provides related Dumps and Reports to enable cause analysis.

Multi-Server Management and Centralized Operation

Multiple LENA Web Servers and LENA WAS can be grouped into a single Cluster, allowing control of multiple servers simultaneously through single operation. Stable application is possible through consistent configuration synchronization along with Graceful Restart or Rolling Restart. Additionally, Multi Control is supported for servers not grouped in clusters.

Cloud/Container Specialized Features

It easily responds to Auto Scaling in Cloud environments. To avoid repetitive work of updating Images every time configuration updates occur, LENA provides Server replication and

configuration synchronization functionality for VM Instances that have been scaled out. This greatly reduces the effort required for operators to configure Auto Scaling environments.

To respond to Container environments, LENA provides Base Docker Images, and these Images fully reflect various essential elements required for Container operation. Through template-based dynamic configuration deployment, there's no need to build Images every time, achieving CI/CD simplification. Additionally, various configurations can be applied to integrate with various solutions in MSA environments.

Operational Differentiation Features

Provides various convenience features for easy operation of web middleware solutions. Using template-based simple and fast Server installation and Server replication features, desired configuration sets can be built in a short time. Through Topology View, configuration and integration information between Server modules can be checked at a glance, improving visibility. Through Dashboard, Events and performance status of operating systems can be checked. Additionally, through Multi Account management, menu/resource access permission settings are possible, and operator Action Tracing, configuration update information History tracking, and Restore functionality are provided.

1.3. LENA Components and Key Concepts

LENA is provided through Binary Package and includes all necessary components. Components are broadly divided into two categories.

- Management Module for operating and managing LENA, including LENA Manager Console and LENA Node Agent.
- Server Module responsible for actual Web Service, including LENA Web Server, LENA WAS (Web Application Server), and LENA Session Server.

The following covers detailed descriptions of each component along with key concepts.

1.3.1. Management Module

LENA Manager

LENA Manager is a Web Application designed to configure and control all resources/functions of LENA through Web UI. Installation and start can be performed through scripts prepared in the LENA Package. To perform Server installation/management through LENA Manager, integration with Node Agent and Advertiser must be configured.

The following explains representative functions and concepts provided by LENA Manager. For detailed information not described below, refer to the "Operator Guide".

- **Dashboard**
  Check resource status and Events of LENA Node and Server
- **Server**
  Register LENA Node, install Web Server, WAS, Session Server, manage configuration, and control start/stop
  - **System**
    Minimum unit for managing LENA Node and Server. Multiple Nodes can be registered under one System, but one Node cannot be registered in multiple Systems.
  - **Node**
    Concept corresponding 1:1 with Node Agent. To execute commands on remote Servers from Manager, it must be done through Node Agent.

- **Cluster**
  Multi-Server management. Cluster configuration is only possible for Servers within one System, and one Server cannot belong to multiple Clusters.
  - **Server Cluster**
    Multiple LENA Web Servers and WAS can be managed as one group. Provides various convenience features such as configuration synchronization and integrated restart.
  - **Service Cluster**
    Function for responding to Container environments. Clusters can be created for LENA Web Server, LENA WAS, and LENA Session Server respectively. Through this Cluster, configuration templates can be deployed to Server Containers. The difference from Server Cluster is that while Server Cluster directly performs Server registration in LENA Manager and enables start/stop control, Service Cluster is passively registered by Server Container and start/stop control is not possible.
- **Resource**
  While not a Module provided by LENA, it defines specifications for resources that are closely integrated with LENA Server, using them as Resources. Resources can be set locally for each LENA WAS, but through the Resource menu, they can be set globally and commonly imported by WAS, avoiding duplicate work.
  - **Database**
    Defines physical specifications such as IP, Port, Driver of DBMS. Corresponds 1:1 with one DBMS.
  - **Datasource**
    Specifies JNDI Name, Url, User ID/Password for configuring DB Connection Pool in LENA WAS. Multiple Datasources can be configured under one Database.
  - **Application**
    Specifies the location and Context Path of the Application to be executed through LENA WAS.
- **Topology**
  Expresses the configuration status of LENA Web Server, LENA WAS, LENA Session Server, etc. installed and integrated on LENA Manager in Topology Diagram format. Through this function, simple Server installation and start/stop control are also possible.
- **Diagnostics**
  Equipped with resource monitoring for LENA Node and Server and various related functions.

LENA Node Agent

LENA Node Agent corresponds 1:1 with Node when registering Node in LENA Manager, is installed by default in LENA Package, and can be started through prepared scripts. Main roles are handling commands for Servers under Node when executing commands through LENA Manager, and also performing the function of transmitting monitoring and status data to LENA Manager. One Node Agent per physical server is the default, but multiple Node Agents can be configured as needed. LENA Web Server, LENA WAS, and LENA Session Server are configured under LENA Node, and LENA Node is configured under one System.

1.3.2. Server Module

LENA Web Server

LENA Web Server can transmit static content and interacts with LENA WAS in Reverse Proxy form to perform the front-end role of the Web Application service provided by LENA WAS. In addition to this, various optional additional functions can be used, with Domain/URI-based branching and Load Balancing functionality, and security layer (SSL) being representative.

LENA WAS (Web Application Server)

LENA WAS executes Java Web Application to provide Web Application services. It includes Datasource connection functionality for using DB Connection Pool and Session Server connection functionality for using Session Clustering. The following describes two types of LENA WAS.

- **LENA WAS SE (Standard Edition)**
  It consists only of Servlet Engine and JSP Engine for processing Java Class files and JSP files, and can only run WAR Type Web Applications. It has the advantage of being relatively lightweight and faster than LENA WAS EE.
- **LENA WAS EE (Enterprise Edition)**
  In addition to the Engines provided by LENA WAS SE, it supports J2EE specifications such as EJB Engine, JMS Engine, and can run WAR/EJB/EAR Type Applications. Additionally, it supports XA Datasource for 2 Phase Commit.

LENA WAS is equipped with an Advertiser Module internally, which collects monitoring results from LENA WAS's JVM through JMX and transmits them to LENA Manager.

LENA Session Server

LENA Session Server is provided to ensure high availability through Session Clustering among multiple LENA WAS. It is provided by default when using LENA Enterprise Edition, and two LENA Session Servers can be configured in Active-Active Clustering (Bidirectional Active-Standby) for Session Clustering. It is possible to implement Session Clustering by setting up a separate configuration in the Application, but it can be implemented simply by a simple configuration in LENA Manager.

However, for Session-clustering, all objects stored in HTTP Session must be serialized (Serializable).

1.4. LENA Operation Mechanism

Nodes registered in Manager are equipped with Node Agent, and Application Servers are equipped with Advertiser.

Operators control Server requests (e.g., Start, Stop, Reload, Dump, configuration changes) from Manager's UI to Node Agents, and Node Agents receive these requests and execute control.

Node Agents and Advertisers periodically transmit monitoring data to Managers, and operators can check resource status of each server through Manager's UI, such as Monitoring Dashboard. For Session Server, it directly transmits its own monitoring data to Manager.

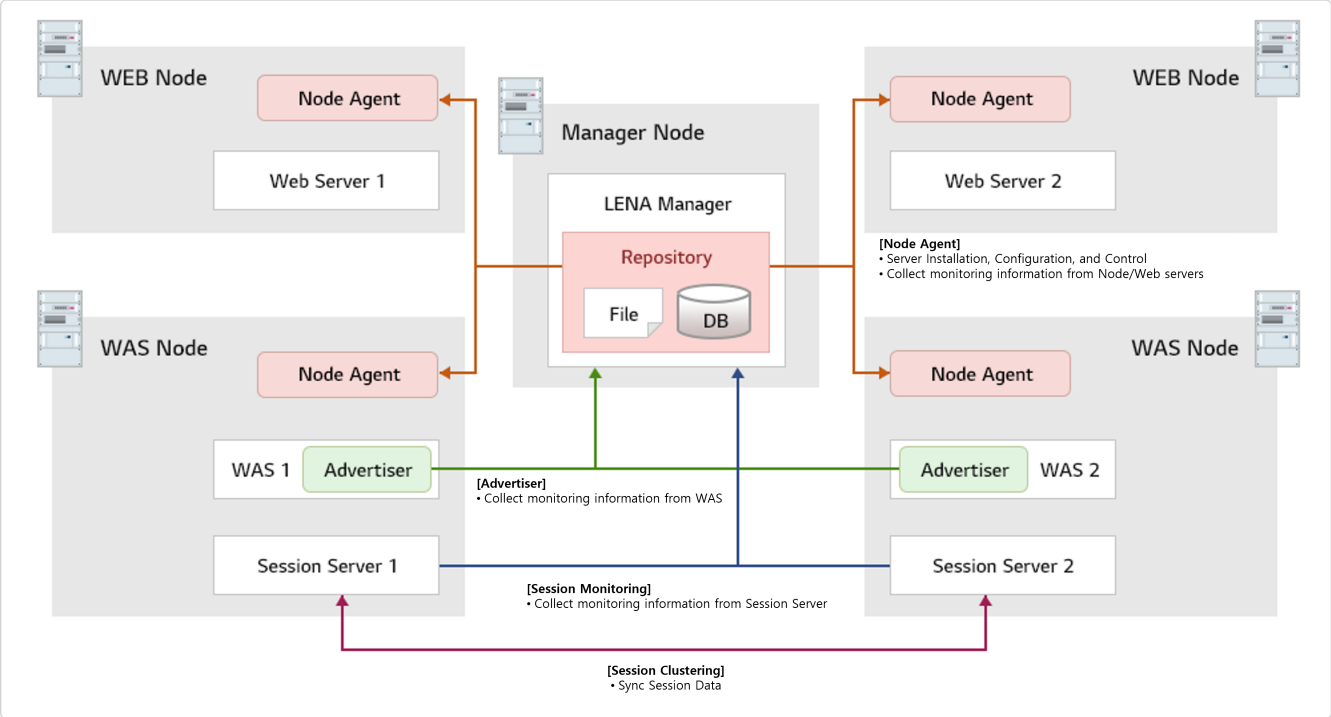


Figure 1. LENA Mechanism

Table 1. Description of LENA Components by Category

Component	Description
Manager	Provides control and monitoring functions through Agent.
Repository	Equipped with File/DB for Manager operation.
Node	Equipped with Node Agent. Server Modules are installed under Node.
Node Agent	- Server installation/replication/patch - Server start/stop control - Server configuration management - Node, Web Server, WAS, Session Server status information - Node, Web Server resource monitoring data provision
Advertiser	Provides WAS resource monitoring data.
WAS	Provides Java Web Application service.
Web Server	Interacts with WAS in Reverse Proxy form to perform the Front-end role of Web services.
Session Server	- Implements Session Clustering with WAS to ensure high availability - Provides Session Server monitoring data.

1.5. Edition-specific Spec

LENA is divided into Standard and Enterprise Editions based on the scope of functions provided by the Application Server, and a Container version is added based on Container requirements. Standard Edition supports Web Application-centric specifications, while Enterprise Edition supports JTA, JMS, EJB, etc. J2EE specifications and provides Session Clustering. The functions or specifications provided for each Edition are as follows.

Table 2. Functions and Specifications by Edition

Function/Spec (LENA-Manager basis)		Standard	Enterprise	Container
Server	Web Server	●	●	●
	WAS (SE)	●	●	●
	WAS (EE)	-	●	●
	Session Server	-	●	●
Resource	Database	●	●	●
	DataSource (General)	●	●	●
	DataSource (XA)	-	●	●
	JTA	-	●	●
	JMS	-	●	●
	Application (WAR)	●	●	●
	Application (EJB, EAR)	-	●	●
Cluster		-	●	●
Topology		●	●	●
Security		●	●	-
Diagnostics	Monitoring	●	●	●
	Diagnostics/Response	-	●	-
Patch		●	●	-

(Legend: ● Provided, - Not provided)

Chapter 2. Log In/Out

Provides functionality for logging in and out of the Manager.

2.1. Log In

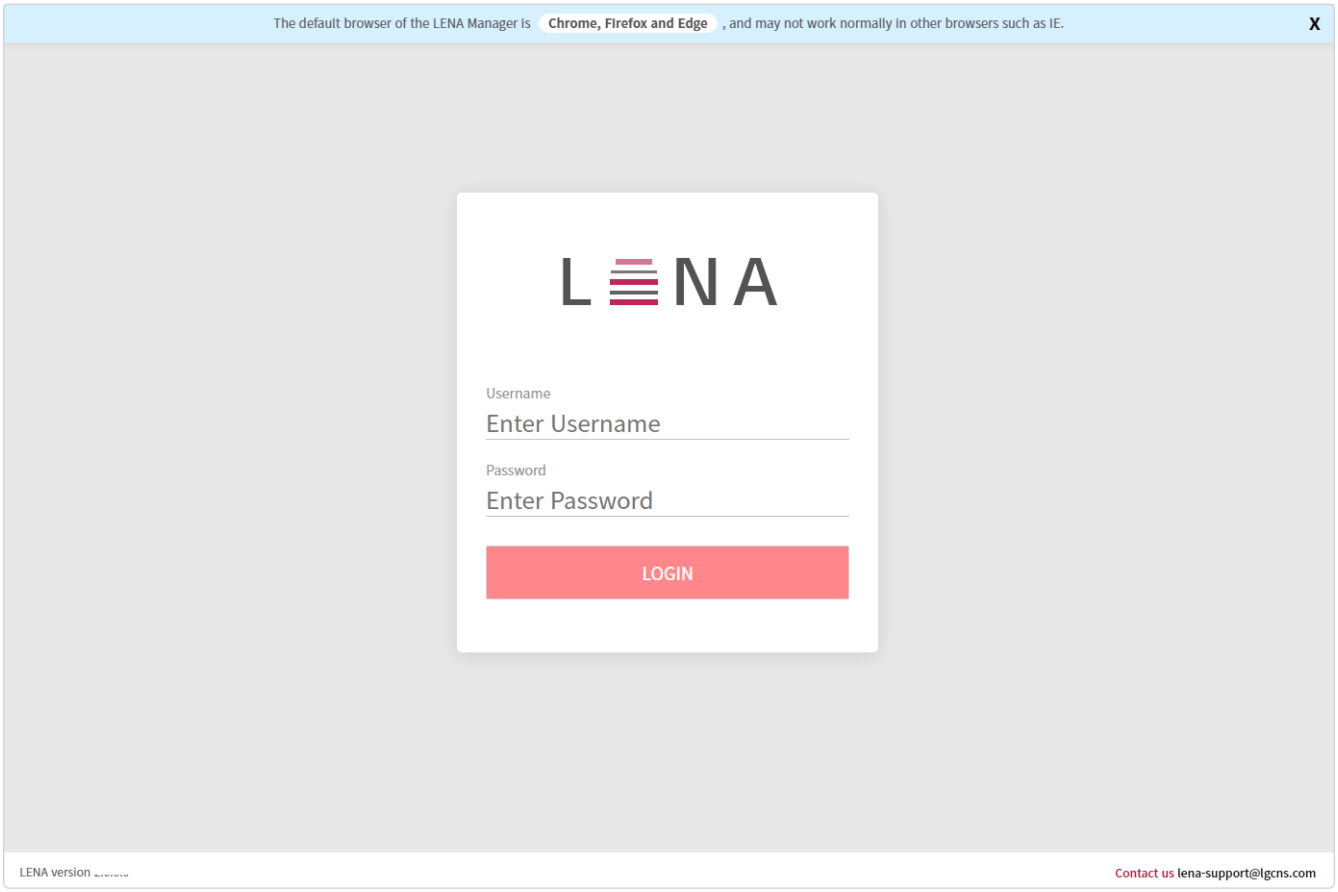


Figure 2. Manager Access Screen

You can log in by entering your user ID and password.

When attempting to log in, if there are 7 or more password errors, you cannot log in with that user. In such cases, the password must be reset through the console. (For detailed information, refer to the 'Manager admin password reset' section in the Appendix.)

2.1.1. OpenID Connect

When OpenID Connect is enabled in the Manager Environment of the Admin menu, the OpenID Connect toggle is activated on the login screen. Through the OpenID Connect toggle, you can log in via authentication providers such as Keycloak.

2.1.2. Language Settings

You can set the language to use in Manager from the Language option. (English, Korean, Chinese)

The installed version is displayed on the bottom left of the login page, and technical support contact information is displayed on the right.

2.2. Log Out

You can log out using the **door icon** on the top right of the Manager.

2.3. Theme Change

You can set the theme through the Dark Theme menu in the **gear icon** menu on the top right of the Manager. You can choose between light mode and dark mode.

Chapter 3. Dashboard

Provides a summary of system configuration information, resource monitoring, events, licenses, and other information managed by the Manager.

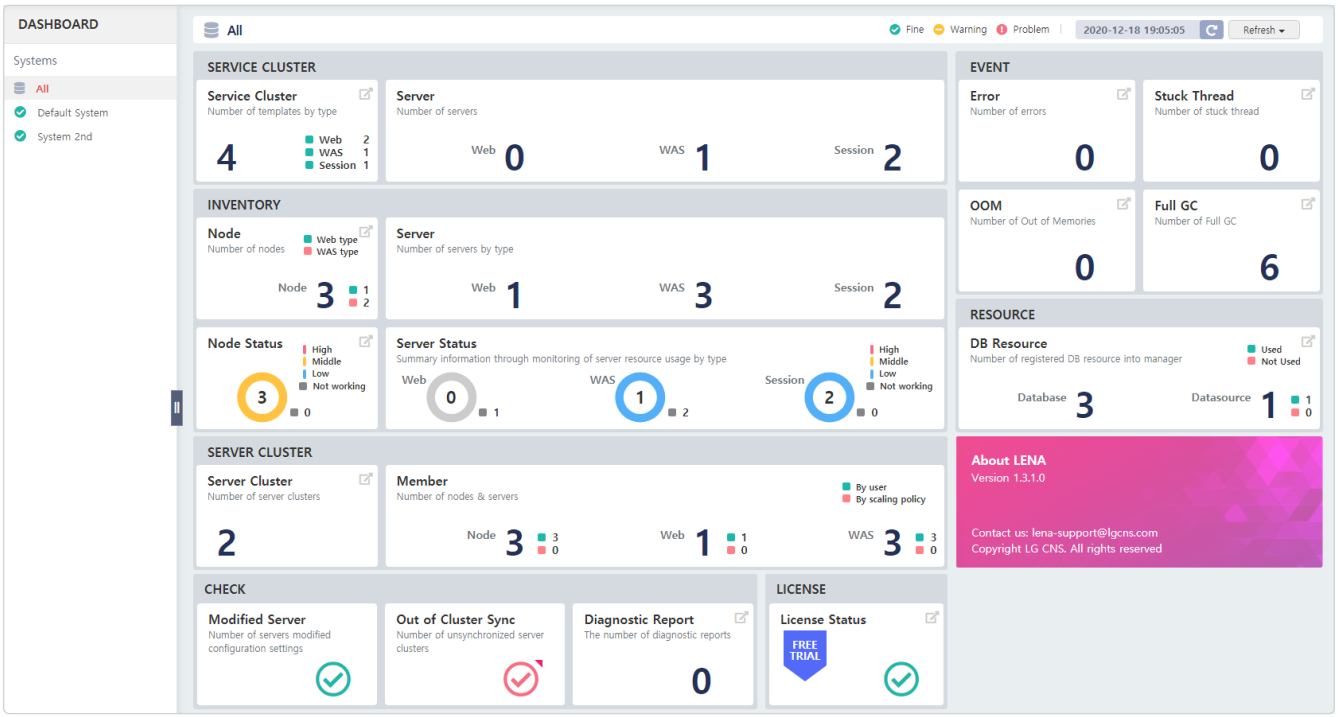


Figure 3. Dashboard

The system list on the left side of the screen provides a list of systems that the logged-in user has permissions for. All shows integrated information from all systems the user has permissions for.

Table 3. Dashboard Items

Item		Description	Notes
SERVICE CLUSTER	Service Cluster	Number of templates by type	
	Server	Total number of servers by type belonging to Service Cluster	

Item		Description	Notes
INVENTORY	Node	Number of Nodes included in the System	Legend: Count by Node type • Web type : Number of nodes where Web Server can be installed • WAS type : Number of nodes where WAS, Session Server can be installed
	Server	Count by Server type included in the System	
	Node Status	Resource usage (CPU, Memory, DISK) status of Nodes included in the System	Legend • High / Middle / Low • Not working : Number of stopped Nodes (Agent)
	Server Status	Resource usage status of Servers included in the System • Web Server : CPU, Memory, Thread check • WAS : Heap Memory, Thread Pool check • Session : Heap Memory check	Legend • High / Middle / Low • Not working : Number of stopped or hung servers
SERVER CLUSTER	Server Cluster	Number of server clusters	
	Member	Total number of servers by type belonging to server clusters	

Item		Description	Notes
CHECK	Modified Server	Whether servers requiring restart exist among Servers included in the System	
	Out of Cluster Sync	Whether Server Clusters requiring sync exist	
	Diagnostic Report	Number of reports issued after diagnostic process execution	EVENT
Exception	Number of Exceptions occurred in Servers included in the System		
Stuck Thread	Number of Stuck Threads occurred in Servers included in the System		
OOM	Number of Out Of Memory occurrences in Servers included in the System		
Full GC	Number of Full GC occurrences in Servers included in the System		RESOURCE
DB Resource	Number of Databases and Datasources registered and managed in the RESOURCE menu	Datasource legend • Used : Number of Datasources currently in use by WAS • Not Used : Number of Datasources not currently in use by WAS	LICENSE

Chapter 4. Server

Provides a screen for managing Node, WAS, Web Server, and Session Server.

You can check the number of Nodes and each Server within a specific System, and manage Node and Server status comprehensively in real-time.

4.1. System

System is a logical group that contains multiple Servers. "DefaultSystem" is provided by default, and users can create, modify, and delete Systems.

4.1.1. List

System list is provided in tree format on the left side of the screen.

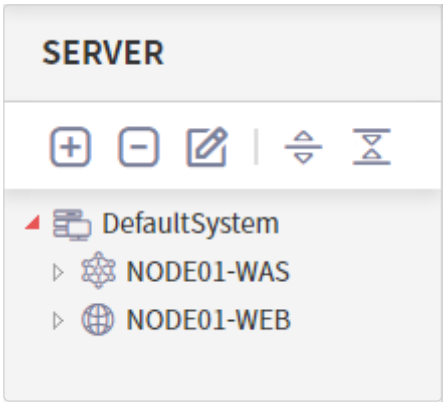


Figure 4. System List

4.1.2. Registration

1. Click the **Register(+) button** to create "Create System" in the list.
2. Enter the name of the system to create and press Enter.
3. Click the **OK button** to save.

The permissions of the currently logged-in user are mapped to that System. That is, only users with the same permissions as the logged-in user can view that System. (Same applies to Node, Server, Resource)

4.1.3. Modification

1. Select the System to modify.
2. Click the **Edit(pencil) button** to change the name of the selected System, then press Enter.
3. Click the **OK button** to save.

4.1.4. Deletion

1. Select the System to delete.
2. Click the **Delete(-) button**.

3. Click the **OK button** to save.

> Systems with Nodes underneath cannot be deleted. That is, only empty Systems can be deleted.

4.2. Node

Node is a physical Server that contains multiple WAS, Web Server, and Session Server instances.

4.2.1. List

You can manage each Node through the Node List.

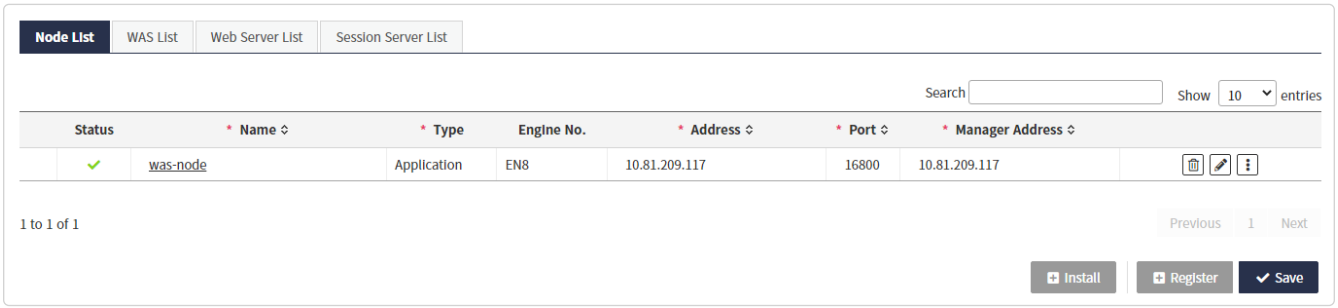


Figure 5. Node List

The properties of Node are as follows.

Table 4. Node Properties

Item (* indicates required value)	Description	Notes
Node information change status	New/Modified/Deleted status of Node data	**+ icon** - Display change status when **Register** / **Edit(pencil)** button is clicked **- icon** - Display deletion pending when **Delete(trash can)** is clicked
Status	Current status of Node	• Started(v) • Stop(□)
Name(*)	Node name	
Type(*)	Node Type	All - Can install all types of Servers Application - Can install WAS and Session Server Web - Can install Web Server MDS - Can install Cache Server

Item (* indicates required value)	Description	Notes
Engine	Engine type according to Node Type	Application - EN-7: Java EE 6 / Servlet 3.0 support - EN-8: Java EE 7 / Servlet 3.1 support - EN-9: Java EE 8 / Servlet 4.0 support - EN-10: Servlet 6.0 support Web - EN-A: JK, Proxy support - EN-N: Proxy, Net-Gateway support MDS - EN-R: Memory Cache support
Address(*)	Node IP address	
Port(*)	Node Agent port number	Default - 16800 (when Node Type is All or Application) - 16900 (when Node Type is Web) - 16700 (when Node Type is MDS)
Manager Address(*)	Manager IP address	
Button area	Displays Node information change and related function buttons	**Trash can icon** - Delete Node information **Pen icon** - Modify Node information **Terminal icon** - Provides SSH terminal functionality to the server where Node is installed **More icon** - Provides menu for JAVA Home setting and Start/Stop

4.2.2. Install

1. Click the **Install button** to prepare Node information registration.
2. Enter Node property values.
3. Click the **Save button** to save.

Table 5. Properties set during Install

Item (* indicates required value)	Description	Notes
Node Type	Node Type	Provides the following types: • Application: Can install WAS and Session Server • Web: Can install Web Server
Node Name(*)	Node name	
Node Address(*)	Node IP address	
Node Port(*)	Node Agent port number	Default : 16800 (when Node Type is All or Application), 16900 (when Node Type is Web)
User(*)	Node execution user account	For Node Type Application, cannot run with root account. For Node Type Web, use root only when Web Server Port must be 1024 or below.
Password(*)	Node execution user account password	
SSH Port	SSH port to access the corresponding Server	
LENA Home	Location where Node Agent will be installed	
JAVA Installation	Whether Java is installed	
JAVA Home	Installed Java path	

Install functionality is only supported in Linux environment.

4.2.3. Register

1. Click the **Register button** to change Node information to registrable state.
2. Enter Node's Name, Type, Address, Port, and Manager Address (default value is provided).
3. Click the **Save button** to save.

- Manager IP is automatically entered as Node's host IP.
- Depending on network configuration, automatically entered IP may differ from actual network IP.
- In this case, you must modify and enter the Manager IP.

4.2.4. Modification

1. Click the **Edit(pencil) button** to change Node information to modifiable state.
2. Modify Node properties.
3. Click the **Save button** to save.

- When Node's Address or Port needs to be changed due to port policy or firewall policy changes, modify agent.conf settings and restart Node Agent.
- At this time, modify and enter Node's Address and Port information so that Manager can also know the changed information.

When saving modified information, if 'Occured Read Timeout' message occurs, check the following cases:

- Port is being used by something other than Node Agent
- Node Agent is hung
- Network problem exists

4.2.5. Deletion

1. Click the **Trash can button** to change Node information to deletable state.
2. Click the **Save button**.

If Servers are registered under a Node, that Node cannot be deleted.

Uninstall is only supported in Linux environment, and is possible only when selecting one node to delete.

4.2.6. Start

Can start nodes that are in stopped state.

1. Select the Start menu provided when selecting the **... button** in the rightmost column of the Node list, then a popup window appears.
2. Enter User, Password, and SSH Port number, then press the **Start button**.

4.2.7. Stop

Can stop nodes that are in running state.

1. Select the Stop menu provided when selecting the **... button** in the rightmost column of the Node list, then a popup window appears.
2. Enter User, Password, and SSH Port number, then press the **Stop button**.

4.2.8. Change Java Home

Can modify JAVA Home path for Node and Servers installed on Node.

1. Modify JAVA Home Path.
   - Node Java Home Path : Edit Node Java Home Path.
   - Server Java Home Path : Edit JAVA Home path for selected servers. (Not supported in Web Node)
2. Press the **Save button**.

4.2.9. Node Terminal

Can access VM where target Node is installed through LENA Manager and use SSH terminal functionality.

To use this functionality, you must meet the following requirements:

- Node must be running and able to communicate with LENA Manager.
- OS where Node is installed must be Linux-based (Windows-based not supported).
- OS account for Node installation/execution must allow SSH access through password authentication.

This functionality reuses the connection between LENA Manager and Node, so no separate port work is necessary to use this terminal functionality.

Clicking the **terminal icon** in the Node list will show a popup screen for using the functionality, and entering the password of the OS account running Node Agent will execute the SSH terminal.

For detailed settings of Node Terminal functionality, refer to the following Manager Configuration settings.

Table 6. Manager Configuration(manager.conf) Node Terminal functionality setting options

Option key	Default value	Description
ssh.cmdCheck.mode.isWhiteList	true	- When true, controls commands using whitelist method. - When false, controls commands using blacklist method.
ssh.cmdCheck.idleTimeout	600 (second)	Disconnects connection after this time if no action is taken after terminal connection. (Minimum configurable value: 30)
ssh.cmdCheck.whitelist.view	view	Set 'view' or 'vi' commands to allow when using whitelist method, separated by ','
ssh.cmdCheck.whitelist	cd,clear,echo,ll,ls,ps,tail,exit	Set commands to allow when using whitelist method. (view, vi excluded)

Option key	Default value	Description
ssh.cmdCheck.blacklist	alias,chmod,chown,cp,dd,export,rm,mkdir,mv,kill,sed,source,sudo,touch,vi	Set commands to prohibit when using blacklist method, separated by ','

Regardless of Manager Configuration settings, the following expressions cannot be used:

```
'|' cannot be used except for '| grep' case
```

```
'&&' cannot be used
```

```
'>' or '>>' cannot be used
```

```
'()'(sub shell) and $(), and ``(backtick) cannot be used
```

4.3. WAS

Provides screens for managing WAS. Performs registration, modification, and deletion of Servers installed on Nodes, and can also install, remove, and clone Servers.

4.3.1. List

WAS can be managed through the WAS List.

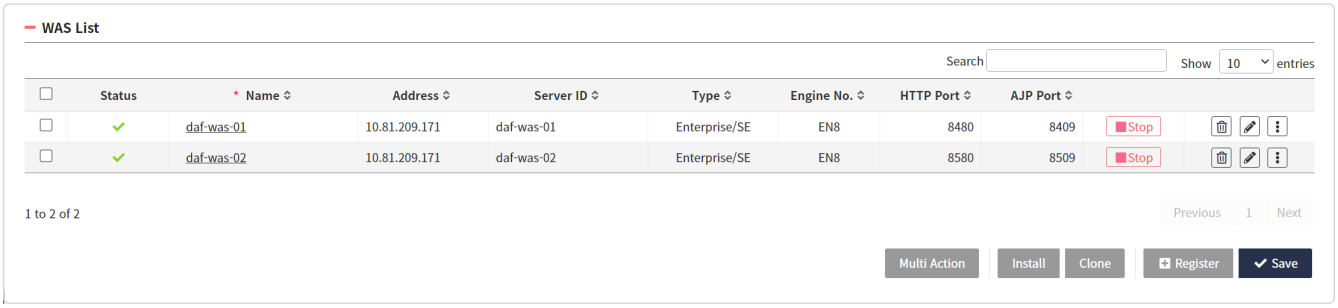


Figure 6. Web Application Server List

WAS attributes are as follows.

Table 7. WAS Attributes

Item (* indicates required values)	Description	Notes
Server information change status	WAS data new/change/delete status and CheckBox for selection	
+ icon - Displays change status when **Register** / **Edit(pencil)** button is clicked	**- icon** - Displays scheduled for deletion when **Delete(trash)** is clicked	Status
Server status	Started (v) Stop (□) Error (!)	Name(*)
Server name		Address
Server IP address		Server ID
Server ID		Type
Server type	Standard Enterprise/EE Enterprise/SE	Engine
Server engine type	Engine refers to LENA's engine type and differs by WAS Java Spec version. - EN-7: Java EE 6 / Servlet 3.0 support - EN-8: Java EE 7 / Servlet 3.1 support - EN-9: Java EE 8 / Servlet 4.0 support - EN-10: Servlet 6.0 support	HTTP Port
HTTP port number		AJP Port
AJP port number		Start/Stop button

Item (* indicates required values)	Description	Notes
Server start and stop		Button area
Displays server information change and related function buttons		**Trash icon** - Delete server information
Pen icon - Edit server information	**Log file icon** - Provides Server Log Viewer functionality	**More icon** - Provides menu for performing Start/Stop

4.3.2. Install

1. Click the **Install button** to prepare for Server installation.
2. Enter Server Type, Server ID, etc.
3. Click the **Save button** to save.

- There may be differences between Servers actually installed on Nodes and Server information managed by Manager. (when installed via console)
- If Server ID duplication error occurs, use Register function to check additional information of installed Servers.

4.3.3. Clone

1. Click the **Clone button** to prepare for Server cloning.
2. Select the Server to clone from Node List. Clone Server ID and Clone Service Port are automatically entered.
3. Modify Clone Server ID and Service Port to desired values.

   (Include External Source is available when cloning servers to other nodes and sets whether to clone application files deployed on the server to be cloned.)

4. Click the **Save button** to save.

- There may be differences between Servers actually installed on Nodes and Server information managed by Manager. (when installed via console)
- If Server ID duplication error occurs, use register function to check additional information of previously installed Servers.
- When remotely cloning WAS servers, Node's Engine No. must be the same to clone WAS servers.

4.3.4. Register

1. Click the **Register button**.
2. Select the Server to register.
3. Click the **Save button** to save.

Installation is also possible from System > Application Server List Tab. However, the Node to install must be selected from Node List.

4.3.5. Modification

1. Click the **Edit(pencil) button** to change Server information to modifiable state.
2. Modify Server attributes.
3. Click the **Save button** to save.

4.3.6. Deletion

1. Click the **Delete(trash) button** to change Server information to deletable state.
2. Click the **Save button**.
3. Press the **OK button** to display a window for selecting deletion type.
   - Deregister : Delete Server information only from Manager DB and maintain physical Server engine (can be re-registered later via **Register button**)
   - Uninstall : Delete Server information from Manager DB and also delete physical Server engine
4. When Uninstall is selected, a window asking about log directory deletion is displayed.

When deleting WAS, the corresponding Server is deleted from the target list of service control (ADMIN > Security > Rule Applying menu).

Servers bound to Server Cluster cannot be deleted.

When use Server Delete Protection value is set to true in Manager Configuration area of ADMIN > Preference > Manager Environment menu, it can prevent servers from being uninstalled from Manager.

4.3.7. Start/Stop

Single Start/Stop

1. Click the **Stop button** to stop the Server.
2. Click the **Start button** to start the Server.

- When stopping Server, WAS stops after all tasks being serviced are completed.
- If tasks are not completed even after Shutdown Timeout time in General tab, it is forcibly stopped.

When Server is started, a popup for viewing log files is executed. You can check whether Server started normally through the popup.

Start button is activated only when in startable state.

Multi Start/Stop

1. Select multiple Servers to start or stop.
2. Click the **Multi Action button** at the bottom of Server list.
3. Select Action Type in popup window and click **Action button** to perform start or stop operations for multiple Servers.

After Start / Stop commands in popup screen, the requested command is not stopped even if popup is closed.

Forced Stop/Restart

1. Click the **Additional function(...) button** at the far right of Server list.
2. Perform forced stop or forced restart.

When performing forced stop or restart, all currently serviced tasks are immediately stopped, so caution is required.

4.3.8. Configuration Information Management

Provides functionality to change Server configuration information. Select the Server name to change from Server list. For Standard Edition, General, Session, Logging, Web Configuration, Environment, Properties, Audit, Configuration Tree, History, TunA tabs are provided, and backup is performed when modifying configuration information for restoration. Enterprise Edition additionally provides Container tab.

When changing Server configuration, Server restart is required to reflect modified items

General

Manages general configuration information of Server. Port information, Connector information, and Stuck Thread related settings can be modified and saved.

Detailed contents of configuration information are as follows.

1. Server Info

Represents main configuration values of Server.

Table 8. Main Configuration

Item (* indicates required values)	Description	Notes
HTTP Port(*)	HTTP port number	
AJP Port	AJP port number	HTTP port number - 71 (auto-calculated)

Item (* indicates required values)	Description	Notes
HTTPS Port	HTTPS port number	HTTP port number + 363 (auto-calculated)
Shutdown Port	Port for receiving Shutdown command string	HTTP port number - 75 (auto-calculated)
Install Path	Server installation path	
Java Home Path	Java Home path	
Minimum Heap Size(MB)(*)	Minimum Heap size to set in WAS (Megabyte)	Default : 2048
Maximum Heap Size(MB)(*)	Maximum Heap size to set in WAS (Megabyte)	Default : 2048
AppBase	Application Base directory	Modification is possible only when Server is in stop state or when no Application is deployed in appBase.
Jvm Route	Server's Unique Identifier	Values set in System Property take priority. If not available, server.xml value is used (Generated by combination of Hostname + Port)
Auto Deploy	Whether to automatically Deploy when application changes	Default : false Detected when war file is re-uploaded to DocBase for each Application
Deploy On Startup	Whether to Deploy Application when WAS starts	Default : true
Shutdown Timeout(s)	Time to wait when tasks are running during Server shutdown (seconds)	Default : 86400

2. Connector

Represents Connector configuration values used by Server.

Table 9. Main Configuration

Item (* indicates required values)	Description	Default Value
Protocol	Protocol type	HTTP/1.1, AJP/1.3

Item (* indicates required values)	Description	Default Value
port	Port number	
Redirect Port	Redirect port	Same as HTTPS Port
Connection Timeout(ms)	Time to wait for Request URI reception after Connector allows connection (ms)	HTTP : 20000, AJP : 60000
URI Encoding	Character Encoding for converting URI bytes	UTF-8
Server	Redefines Server Header for Http Response to prevent Server information exposure	Server
Max Threads	Maximum number of Threads that Connector can create	256
Min Spare Threads	Minimum number of Threads secured when creating Connector	10
Max Queue Size	Maximum length of Request Queue	Integer.MAX_VALUE
Packet Size	AJP packet size	8192
Enable Lookups	Whether to use DNS LookUp. Not using is advantageous for performance	false
Compression	Whether to compress HTTP message Body (off, on:Text only, force:all)	off
Tcp No Delay	Send TCP packets without delay	true

3. Stuck Thread

Represents Stuck Thread configuration values.

Table 10. Main Configuration

Item (* indicates required values)	Description	Notes
Threshold(s)	Minimum time for identifying Stuck Thread (s)	
Interrupt Thread Threshold	Minimum time for interrupting Stuck Thread (s)	To terminate n seconds after Stuck Thread identification, enter "Threshold+n" value

4. Service Endpoint

Represents Endpoint Address configuration values.

Table 11. Main Configuration

Item (* indicates required values)	Description	Notes
Service Endpoint Address	Representative service domain address of WAS	

Session

Sets whether to use Session Cluster functionality.

1. Embedded Session Server mode

   Select when Session Server module is embedded in WAS and operates. When Embedded Mode is selected in Session Server Mode item, it is displayed as Embedded Type in Session Server list in Server management screen.

Table 12. Main Configuration

Item (* indicates required values)	Description	Default Value
Embedded Host	Refers to the WAS	Own IP (cannot be changed)
Embedded Port(*)	Port information for Embedded Session Server to be used in the WAS	
Secondary Server Host(*)	Slave Server host IP	
Secondary Server Port(*)	Slave Server Port	
Multi Login Control	Whether to prevent dual login	false (when true, 3 items below are provided)
Logout Page when Multi Login check(Multi Login)	Screen to provide after terminating session of user who logged in first during dual login	
Logout Message when Multi Login check(Multi Login)	Message to show after terminating session of user who logged in first during dual login	
Excepted Page When Multi Login Check(Multi Login)	Exception URL for dual login check	

2. Standalone mode

   Method of operating by connecting to separate Session Server. Select Standalone in Mode item.

   When setting Primary Server and Secondary Server in Standalone mode, Session Server must be configured in advance.

Table 13. Main Configuration

Item (* indicates required values)	Description	Default Value
Primary Server Host(*)	Primary Session Server host	Enter manually selection allows setting external session server outside system
Primary Server Port(*)	Primary Session Server port	
Secondary Server Host(*)	Secondary Session Server host Used only when connection with PrimaryServer is lost	Enter manually selection allows setting external session server outside system
Secondary Server Port(*)	Secondary Session Server port Used only when connection with PrimaryServer is lost	
External Stored Session	Store Session objects in Session Server instead of local WAS	false
Share session in applications	Share Session objects between Multi Applications Configurable only in Standalone Mode	false
Multi Login Control	Whether to prevent dual login	false (when true, 3 items below are provided)
Logout Page when Multi Login check(Multi Login)	Screen to provide after terminating session of user who logged in first during dual login	
Logout Message when Multi Login check(Multi Login)	Message to show after terminating session of user who logged in first during dual login	
Excepted Page When Multi Login Check(Multi Login)	Exception URL for dual login check	

Session functionality is provided in Enterprise Edition.

Logging

Manages Server's Logging configuration information.

1. Log Home

Table 14. Main Configuration

Item (* indicates required values)	Description	Notes
Log Home(*)	Log Home path	When default is selected, set to logs folder under server installation directory, when Enter manually is selected Log Home Prefix item allows input of log directory home path
Retention Days(*)	Maximum retention days for logs	Default : 0(unlimited)

2. Access Log

Represents configuration values for Access logs for Requests.

Table 15. Main Configuration

Item (* indicates required values)	Description	Notes
Logging Directory	Log directory	Can be specified as absolute path or relative path of
Pattern	Layout of Logging field	
Prefix	Prefix of Log file	
Suffix	Suffix of Log file	

3. Handler List

Detailed contents of Handler configuration information are as follows.

Table 16. Main Configuration

Item (* indicates required values)	Description	Notes
Name(*)	Handler class name	
Type	Handler type	ConsoleHandler and FileHandler can be selected
Level	Handler log level	
Filter	Implementation of java.util.logging.Filter	
Formatter	Implementation of java.util.logging.Formatter	Default : java.util.logging.SimpleFormatter
Encoding	Handler Character Encoding	

Item (* indicates required values)	Description	Notes
Root Handler	Whether Root Logger	

4. Logger List

Detailed contents of Logger configuration information are as follows.

Table 17. Main Configuration

Item (* indicates required values)	Description	Notes
Name(*)	Specify Logger name	
Level(*)	Logger log level	
Handler(*)	Select which Handler Logger will use	ConsoleHandler is selected by default

Server's log configuration file is ()/conf/logging.properties.

Web Configuration

Provides screen for managing Global web.xml configuration. Modify necessary items and click **Save button** at the bottom to save.

Detailed contents of configuration information are as follows.

1. Default Servlet

Table 18. Main Configuration

Item (* indicates required values)	Description	Default Value
Directory Listing	Whether to allow Directory Listing when Welcome file is not present	false
Readonly	Do not allow HTTP methods such as PUT, DELETE	true
Input Buffer Size	Input buffer size (bytes)	2048
Output Buffer Size	Output buffer size (bytes)	2048
File Encoding	File encoding	platform default
Show Server Info	Whether to display Server information when Directory Listing is allowed	true
Load On Startup(*)	Specify Servlet loading order when WAS starts	1 (negative: disable / 0: last)

2. JSP Engine

Table 19. Main Configuration

Item (* indicates required values)	Description	Default Value
Check Interval(s)	When Development is false, cycle for checking jsp changes and recompilation (s)	0 (0: disabled / positive: enabled with that cycle)
Development	Whether Development. When Development is true, changes are checked with modificationTestInterval value as cycle	true
Generate String As Character Array	Whether to generate String as Char Array	false
Modification Test Interval(s)	Cycle for jsp change check when Development is true	4 (when 0: check every access)
Trim Spaces	Remove unnecessary whitespace from response to reduce response bytes	false
Java Encoding	Encoding when generating Java source	UTF8
Load On Startup(*)	Specify Servlet loading order when WAS starts	3

3. JSP Page Encoding

Table 20. Main Configuration

Item (* indicates required values)	Description	Notes
URL Pattern	URL Pattern of JSP Page to apply Page Encoding	
JSP Page Encoding	Specify Page Encoding to apply	

4. Session

Table 21. Main Configuration

Item (* indicates required values)	Description	Notes
Session Timeout(m)	Session timeout time (minutes)	Default : 30

5. Welcome File List

Table 22. Main Configuration

Item (* indicates required values)	Description	Notes
File(*)	Specify files to service in order when Directory index is called	

Environment

Provides screen for managing JVM options, Start Shell configuration, and System Properties (provided only in Enterprise Edition). Modify through file editor and click **Save button** to save.

- JVM Env (/bin/setenv.sh): JVM options for Server execution

- Custom Env (/bin/customenv.sh): User custom environment variable configuration
- Base Env (/env.sh): Shell Script for Server startup

Do not modify JVM_ROUTE value directly here, but use **Load button** in JvmRoute item in Server Info area of General tab to modify. If modified directly here, Manager DB information is not updated, causing DB value mismatch.

- System.properties(/conf/system.properties) (This item can only be checked in Enterprise Edition)
- Catalina.properties (/conf/catalina.properties): Server's Catalina configuration

```
is WAS's default installation directory.
is originally used when creating directories to use multiple
Instances for one WAS and specifying directories for each
Instance, but in LENA, WAS and Instance have 1:1 relationship, so
is used as .
```

By default, configuration cannot be modified as it is Disabled, but if you want to modify, click **Configuration button** in ADMIN > Manager Environment > Manager Configuration item and change the following configuration to false.

```
server.environment.envshell.readonly=false
```

Properties

Provides screen for checking Server's System Properties and System Environments. Key Properties among System Properties are provided separately to check main information such as Server path, JAVA version, etc. Information can only be checked when Server is running.

Container

For Enterprise Edition, provides functionality to change EJB Container configuration. If Server is started without container configuration, EJB required container is created with default configuration. If configuration changes other than default are needed, container must be created to change configuration.

1. Basic Configuration

Table 23. Basic Configuration

Item (* indicates required values)	Description	Notes
ID(*)	Container identifier	
Type(*)	Container type	

2. CMP_ENTITY Configuration

Table 24. CMP_ENTITY Configuration

Item (* indicates required values)	Description	Notes
CmpEngineFactory	Factory class name	Default : org.apache.openejb.core.cmp.jpa.JpaCmpEngineFactory

3. BMP_ENTITY Configuration

Table 25. BMP_ENTITY Configuration

Item (* indicates required values)	Description	Notes
PoolSize	Specify Bean pool size	Default : 10

4. STATELESS Configuration

Table 26. STATELESS Configuration

Item (* indicates required values)	Description	Notes
AccessTimeOut	Wait time between invocations (Specifies the time to wait between invocations)	Default : 0 (means no timeout)
MaxSize	Maximum number of Bean pool	Default : 10
MinSize	Minimum number of Bean pool	Default : 0
StrictPooling	Specify operation method when Pool reaches maximum. StrictPooling waits without increasing pool size	Default : true
MaxAge	Maximum time until removal from Pool (h)	Default : -1
ReplaceAged	Whether to Replace when MaxAge is reached	Default : true
ReplaceFlushed	Whether to Replace when flushed from pool	Default : false
MaxAgeOffset	MaxAge usage	Default : -1
IdleTimeout	Maximum time instance can be in idle state in pool (m)	Default : 0
GarbageCollection	Whether to allow garbage collection as mechanism to reduce pool	Default : false
SweepInterval	Cycle for container to clean pool and remove expired instances (m)	Default : 5
CallbackThreads	Thread Pool size. This value is shared by all Beans deployed in container	Default : 5
CloseTimeout	Maximum time to wait until pool closes and PostConstruct method is called (m)	Default : 5

5. SINGLETON Configuration

Table 27. SINGLETON Configuration

Item (* indicates required values)	Description	Notes
AccessTimeout	Wait time between invocations (Specifies the time to wait between invocations)	Default : 0 (means no timeout)

6. STATEFUL Configuration

Table 28. STATEFUL Configuration

Item (* indicates required values)	Description	Notes
AccessTimeout	Wait time between invocations (Specifies the time to wait between invocations)	Default : 0 (means no timeout)
Cache	Cache to manage Stateful bean instances	
Default : org.apache.openejb.core.stateful.SimpleCache	Passivator	Specify Passivator class
Default : org.apache.openejb.core.stateful.SimplePassivater	TimeOut(m)	Wait time between invocations (Specifies the time to wait between invocations)
Default : 20	Frequency	Cycle for bean cache to check idle beans (s)
Default : 60	Capacity	Bean pool size for Stateful SessionBean container
Default : 1000	BulkPassivate	Number of instances to passivate at once

7. MESSAGE Configuration

Table 29. MESSAGE Configuration

Item (* indicates required values)	Description	Notes
ResourceAdapter	Specify Resource Adapter	Default : Default JMS Resource Adapter
MessageListenerInterface	Specify MessageListener	Default : Javax.jms.MessageListener

Item (* indicates required values)	Description	Notes
ActivationSpecClass	Specify Activation Spec Class	Default : org.apache.activemq.ra.ActiveMQActivationSpec
InstanceLimit	Maximum number of Instances	Default : 10

Audit

Function for collecting/managing events occurring in WAS.

Collected event information can be checked in event dashboard. For event dashboard related content, refer to Event Dashboard.

Four types of Detection Rules can be set to collect events.

Table 30. OOM Detection Rule

Item	Description	Notes
Enable	Detects Out Of Memory Error occurrence	Default : true

Table 31. Stuck Thread Detection Rule

Item	Description	Notes
Enable	Detects Stuck Thread occurrence	Default : false

LenaStuckThreadDetectionValve is basically configured in server.xml, and LenaStuckThreadDetectionValve related configuration can be done in Stuck Thread item of SERVER > Server selection > General tab screen.

When user request processing time exceeds Threshold configuration value, event occurs and is sent to Manager.

Table 32. Full GC Detection Rule

Item	Description	Notes
Enable	Detects Full GC occurrence	Default : false

Table 33. Exception Detection Rule

Item	Description	Notes
Enable	Detects Exception occurrence by pattern	Default : false
Exception Class Pattern	Specify Exception pattern to detect. Exceptions inheriting the pattern are also detected. Maximum 10 can be specified, * pattern cannot be used. ex) abc.dbc.ExampleException	
Exclude Exception Class Pattern	Specify Exception pattern to exclude from detection. Maximum 10 can be specified, * pattern cannot be used. ex) abc.dbc.ExampleException	

Item	Description	Notes
Enable Full Stack	When Exception has multiple Causes, whether to display entire content instead of summary information	Default : true
Max Line of Stack's Cause	Number of Lines to express in Exception Stack Trace. Lines are collected for each Cause by the set number. Setting too large a number can cause load in collection and storage management	Default : 3

Exception classes that can be detected are not Exceptions included in Java's own library, but Exceptions of Application or Framework. Exception patterns must be defined to prevent too many events from occurring.

Audit functionality is provided in Enterprise Edition.

Configuration Tree

Configuration files under /conf folder under WAS installation path can be managed through file editor.

User running Node Agent must have access permission to WAS configuration information files for modification. If access permission is not available, message that file cannot be edited due to no Write permission is displayed.

History

Provides backup and restore functionality for configuration information. When configuration information is modified and saved, History is managed by type. Search by entering modification date and configuration file Type.

Click **View(magnifying glass) button** to view information of selected file, and click **Restore button** to restore to that configuration file.

4.3.9. Resource Management

When Resources menu under Server menu is selected, screen for managing Resource information related to that Server is displayed. By default, information for DataSource, JMS, JTA Resources can be managed. (JMS, JTA Resources are supported only for Enterprise Server)

Methods for setting Resources in WAS are as follows.

- Add : Click **New button** to add Resource. (Datasource, JMS possible)
- Delete : Click **Delete button** to delete Resource. (Datasource, JMS possible)
- Import : Click **Import button** to import Resources registered in RESOURCE menu. (Datasource, JMS, JTA possible)

DataSource

Provides functionality to manage JNDI DataSource that can be used by WAS Applications. JNDI can be set so all Applications running on Server can share and use, or JNDI can be set for each Application for use. For Enterprise Edition, JTA is supported so additional attributes are added.

1. Server DataSource Configuration

Set DataSource shared by all Applications running on Server. List of DataSources available on Server can be queried, and DataSource registration, modification, deletion is possible.

Connection test can also be performed to check DataSource status.

DataSource attributes are as follows. Attributes not visible on initial screen are displayed when **Expand all button** is clicked.

Table 34. DataSource Attributes

Item (* indicates required values)	Description	Notes
Scope	Scope for using DataSource	Provides following scopes • Context: Datasource information is set in common context area so all Applications can share. • Global: Datasource information is set in GlobalNamingResource area, and each application individually sets and uses in DataSource Link List. • Global+ResourceLink: Datasource information is set in GlobalNamingResource area and Datasource link is set in common context area.
JNDI Name(*)	JNDI name of Global DataSource	
Databases(*)	Set information of datasource to be used commonly	
Resource Name(*)	Name of Databases	
Address(Host/Port)(*)	IP and port to be used commonly	
Driver Class Name(*)	JDBC Driver class name	
URL(*)	JDBC URL	
User Name(*)	Connection username	

Item (* indicates required values)	Description	Notes
Password(*)	Connection password	when encryption is checked, password is encrypted and stored. Encryption is recommended for security.
Encryption Level	Specify encryption scope for authentication information	Default : Password only
DefaultAutoCommit	Auto Commit status of Connections created from Pool	Default : JDBC driver default value
Auto Reconnection	Used when setting TestOnBorrow and TestWhileIdle values. When true/false, both values are set the same. When User Defined is selected, both values can be set directly by user	
InitialSize	Initial number of Pool Connections	Default : 10
MaxActive	Maximum number of Pool Connections	Default : 100
MinIdle	Minimum number of Idle Connections	Default : 10
MaxIdle	Maximum number of Idle Connections	Default : 100
MaxWait(ms)	Maximum time to wait when no available Connection in Pool (ms)	Default : 30000
MinEvictableIdleTimeMillis(ms)	Connections existing in Pool in idle state for longer than this time become removal targets (ms)	Default : 60000 (60s) (1800000 (30m) when XaDataSource = true)
ValidationQuery	Connection validity verification query	Default : null
ValidationInterval	Connection validity verification cycle (ms)	Default : 3000
TestOnBorrow	Before taking connection from Pool, perform query set in validationQuery to check connection validity	Default : default
TestOnReturn	Before returning connection to Pool, perform query set in validationQuery to check connection validity	Default : default
TestWhileIdle	For idle connections, perform query set in validationQuery to check connection validity	Default : default
LogValidationErrors	Whether to output errors when errors occur after validation query execution	Default : default(false)

Item (* indicates required values)	Description	Notes
TimeBetweenEvictionRunsMillis(ms)	Thread execution cycle for extracting unused Connections (ms)	Default : 5000
RemoveAbandoned	Whether to detect Connection loss	Default : default
RemoveAbandonedTimeout(s)	Timeout value for determining lost Connection (s)	Default : 60
LogAbandoned	Whether to log when processing Connection loss	Default : default
AbandonWhenPercentageFull	Abandon is performed only when Connection pool exceeds set occupancy rate	Default : 100
JdbcInterceptors	User-defined functionality can be added using flexible and pluggable interceptors	When setting QueryTimeout, enter QueryTimeoutInterceptor(queryTimeout=time(seconds))

When Default value is default instead of true or false, JDBC Driver's default value is used.

Additional attributes for Enterprise Edition are as follows.

Table 35. Enterprise Edition Additional Attributes

Item (* indicates required values)	Description	Notes
JtaManaged	Whether to use JTA	Default : false
XaDataSource	Whether to use XA	Default : false

- XADataSource configuration can only be used when JTA is configured, and when XADataSource is configured, validationInterval, logValidationErrors, abandonWhenPercentageFull attributes cannot be used.
- When DataSource is set to Context scope, all Applications share it.
- In EnterpriseServer, DataSource can also be set to Context scope, but Lookup is not possible in EJB. Setting to Global + ResourceLink scope is recommended for EnterpriseServer.
- Password encryption algorithm uses AES. Key value for encryption is managed as "datasource.key=keyvalue" in Manager LENA Home sub /repository/conf/manager.conf file and each WAS Home sub /conf/advertiser.conf.

2. Databases

When setting URL, register by creating Databases with information to be used commonly.

Click **Add(+) button** to create popup window.

a. Enter Resource Name to distinguish Databases.

b. Check automatically filled DriverClassName. Change if necessary.

c. Enter Address (IP and port) and save.

3. JDBC driver Upload

JDBC Driver library can be uploaded through Manager.

Click **Upload button** under DataSource detailed information to display upload screen as follows.

a. Select file to upload through Search button. File to upload is JDBC Driver library, so only JAR format files can be selected.
b. Click Upload button to upload selected file to target directory.
c. Path where JDBC Driver file is uploaded is ${SERVER_HOME}/lib/datasource.

4. Connection Test

Click **Connection Test button** in DataSource detailed screen to perform connection test for configured DataSource. When connection is successful, "JDBC Connection is successfully tested" message is displayed.

If "Driver Class[class name] does not exist." error message is displayed, check if corresponding driver class is properly uploaded and classpath is configured.

classpath is added in WAS details > Environment > JVM Settings.

Configuration Example

```
CLASSPATH="$\{CLASSPATH}:$\{CATALINA_HOME}/lib/datasource/ojdbc6.
jar"
```

JMS

For Enterprise Edition, JMS related Resources can be defined. Active MQ Resource Adapter, JMS Connection Factory, Queue, Topic configurations can be added, modified, deleted respectively.

Table 36. Main Configuration

Item (* indicates required values)	Description	Notes
ID(*)	Resource identifier	
Type(*)	Resource type	Provides following types • ActiveMQResource Adapter • JMSConnectionFactory • Queue • Topic

2. Active MQ Resource Adapter Configuration

Table 37. Main Configuration

Item (* indicates required values)	Description	Notes
BrokerXmlConfig	Broker configuration	Default : broker:(tcp://localhost:61616)?useJmx=false
ServerUrl	Broker address	Default : vm://localhost?waitForStart=20000&async=true
DataSource	Datasource for persistence messages	
StartupTimeout	Maximum startup wait time (s)	Default : 10

3. JMS Connection Factory Configuration

Table 38. Main Configuration

Item (* indicates required values)	Description	Notes
ResourceAdapter	Specify Resource Adapter to use	
TransactionSupport	Specify Global Transaction	Provides following types • XA • LOCAL • NONE
PoolMaxSize	Maximum number of physical connections to ActiveMQ broker	Default : 10
PoolMinSize	Minimum number of physical connections to ActiveMQ broker	Default : 0
ConnectionMaxWaitTime	Maximum connection wait time	Default : 5 Seconds
ConnectionMaxIdleTime	Maximum idle time before return	Default : 15 Minutes

4. Queue Configuration

Table 39. Main Configuration

Item (* indicates required values)	Description	Notes
Destination	Specify Queue name	

5. Topic Configuration

Table 40. Main Configuration

Item (* indicates required values)	Description	Notes
Destination	Specify Topic name	

JMS functionality is provided in Enterprise Edition and is available when Enterprise version WAS is installed.

JTA

For Enterprise Edition, provides functionality to change Transaction Manager configuration.

To use Transaction Manager configuration with default settings, select Auto for Managed Type. (default during installation)

To change Transaction Manager configuration, select User Defined. (When User Defined is selected, Recovery option is defaulted to "No")

1. Main Configuration

Table 41. Main Configuration

Item (* indicates required values)	Description	Notes
Managed Type	Select whether User Defined Transaction Manager	Default : Auto
ID(*)	Transaction Manager name	
Default TimeOut(min)	Specify Timeout	Default : 10 minutes
Type	JTA Type	
Recovery	Set whether to recover when Transaction error occurs	Logging configuration opens when Yes is selected

2. Transaction Recovery Logging(howl) Option

Table 42. Logging configuration for recovery when Transaction error occurs

Item (* indicates required values)	Description	Notes
Directory	Directory location to create log files	Default : txlog
File Name	Log file name	Default : howl
File Extension	Log file extension	Default : log
Max Log Files	Maximum number of log files to create	Default : 2
Max Block Per File	Maximum number of blocks per file	Default : -1
Buffer Size	Buffer size (kb)	Default : 32
Max Buffers	Maximum buffer value	Default : 0
Min Buffers	Minimum buffer value	Default : 4

Item (* indicates required values)	Description	Notes
Adler32 Checksum	When both Adler32 Checksum and Checksum Enabled settings are "Yes", calculate checksum using Adler32 algorithm	Default : Yes
Checksum Enabled	Check Buffer Contents before recording to Disk	Default : Yes
Threads Waiting	Maximum number of waiting threads	Default : -1
Flush SleepTime	Total sleep time of ForceManager	Default : 50 Milliseconds

JTA functionality is provided in Enterprise Edition and is available when Enterprise version WAS is installed.

4.3.10. Application Deployment

List

Select SERVER menu at top of screen to query Server status. Select Application of Server to deploy from left menu. Provides screen for querying list of deployed Applications.

Application list items are as follows.

Table 43. Application List Items

Item	Description	Notes
Type	Form of Application to deploy	Only Enterprise WAS Type provides following types • EJB • EAR • WAR
Base Name	Base name	
Context Path	Context path	
DocBase	Application location	
Status	Application status	Provides following statuses • Started(v) • Stop(□) • Error(!)

Item	Description	Notes
	Action button	Provides following functionalities • **Undeploy(trash) button** • **Application Start button** • **Application Stop button** • **Application Reload button**
	View button	Provides following functionalities • **web.xml View(document) button**

Deploy

Attributes for deploying Application are as follows.

Table 44. Application Deployment Attributes

Item (* indicates required values)	Description	Notes
Application Type	Form of Application to deploy	Only Enterprise WAS Type provides following types • EJB • EAR • WAR
Context Path(*)	Context path	
unpackWAR	Whether to execute after expanding WAR file. When value is false, deploy without expanding WAR file compression	Default : true
DocBase(*)	Application location	File can be uploaded through **Upload select(file) button**

Application Upload

When there is no separate deployment system, applications can be uploaded through Manager.

1. After selecting server, select Applications to move to Application screen.
2. In Application Deploy area at bottom of Applications screen, click **Upload select(file) button** at right end of DocBase item to display file system screen.
3. Select target directory (Server side Host) to upload.
4. Click **Upload button** to create popup for selecting application files.
5. Select application file to deploy and click **Upload button** to upload selected file to target directory.

Import

Click **Import button** to import and deploy Application information registered in [Resource] menu.

Configuration Information Management

When Application Name is selected from Application list query screen, Application configuration management screen can be queried. Provides configuration and management functionality for Application Descriptor and DataSource.

Application configuration changes are possible only for selected Server.

Application Settings

Manages information configured in Application Descriptor.

Click **Back(←) button** to return to Application list screen. Click **Expand all button** to configure additional Context attributes.

DocBase and ContextPath cannot be modified, and detailed information of attributes is as follows. Attributes not visible on initial screen can be checked by clicking **Expand all button**.

Table 45. Application Setting

Item (* indicates required values)	Description	Notes
DocBase(*)	Application's Document Base	
Context Path(*)	Context path	
unpackWAR	Whether to execute after expanding WAR file. When value is false, WAR file compression is not expanded, and web application is just redeployed in compressed state	Default : true
reloadable	Whether to re-reflect when Application changes (Class File)	
privileged	Whether to use Container Servlet	

Item (* indicates required values)	Description	Notes
cookies	Whether to use cookie for session identifier communication	
useHttpOnly	Whether to block access to session ID using scripts on client side	
session Cookie Domain	When set, overwrites all domains set in web application. When not set, domain distinguished by web application is used	
session Cookie Name	When set, all session cookies are created with that name	Default : JSESSIONID
session Cookie Path	When set, web application uses that path	
useNaming	Set to use JNDI InitialContext for J2EE platform	Default : true

Add Attribute button can be used to add attribute values.

DataSource Link List

Provides functionality to set Global DataSource to be used in Application.

DataSource link management attributes are as follows.

Table 46. DataSource Link Management Attributes

Item (* indicates required values)	Description
Name(*)	JNDI name to use in Application
JNDI Name(*)	JNDI name of Global DataSource
User Name	DataSource connection username
URL	JDBC URL
Description	Description of DataSource
+ icon	Click **New button**, **Edit(pencil) button** to display that selected DataSource information is being changed
- icon	Click **Delete(trash) button** to display that selected DataSource information is deleted

Click **New button** to add new configuration, and click **Save button** to save changed configuration.

Among Datasources configured in WAS, Datasources with Scope of Global or Global + ResourceLink appear as JNDI Name selection items when setting new configuration.

4.3.11. Server Log Viewer

Log Viewer button on right side of server list allows browsing log file contents under target server's Log Home path.

To use this functionality, the following must be satisfied.

- Node to which target server belongs must be running.

Click Log Viewer button in server list to check directories and files in tree structure based on target server's Log Home path.

When file is selected, file contents are queried, and when first selected, file contents from end of file up to predetermined size can be checked.

Use Load More, Load Previous buttons to query and check log file contents by predetermined size.

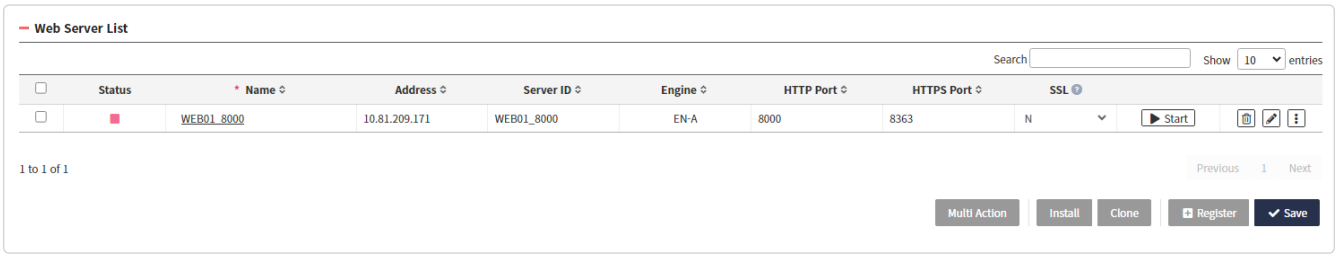
- When using Load Previous button and no more content to query (eg. beginning of file), Alert message that no more data can be read is displayed.
- When using Load More button and no more content to query (eg. end of file), message that no more data can be read is displayed at bottom of screen.

4.4. WEB

Provides screens for managing Web Servers with NODE Engine EN-A and EN-N. Registration, modification, and deletion of Web Servers installed on Nodes is possible, and start and stop operations can be performed.

4.4.1. List

Web Servers can be managed through the Web Server List.



Web Server attributes are as follows.

Table 47. Web Server Attributes

Item (* indicates required values)	Description	Notes
Status	Server status	Provides following statuses • Started(v) • Stop(□) • Error(!)

Item (* indicates required values)	Description	Notes
Name(*)	Server name	
Address	Server IP address	
Server ID	Server ID	
Engine	Node Engine type	• EN-A • EN-N
Protocol Type	Active protocol type	• HTTP • HTTPS
Port	HTTP/HTTPS port number	
Start/Stop button	Server start and stop	
Button area	Displays server information change and related function buttons	
Trash icon - Delete server information	**Pen icon** - Edit server information	**Log file icon** - Provides Server Log Viewer functionality

4.4.2. Install

1. Click the **Install button** to prepare for Server installation.
2. Enter Server ID and Service Port.
3. Click the **Save button** to save.

There may be differences between Servers actually installed on Nodes and Server information managed by Manager. (when installed via console)

If Server ID duplication error occurs, use Register function to check additional information of installed Servers.

4.4.3. Clone

1. Click the **Clone button** to prepare for Web Server cloning.

2. Select Node List to select Server to clone.
3. Enter Clone Server ID and Service Port.

   (Include External Source is available when cloning servers to other nodes and sets whether to clone files in Document Root directory of server to be cloned.)

4. Click the **Save button** to save.

There may be differences between Servers actually installed on Nodes and Server information managed by Manager. (when installed via console)

If Server ID duplication error occurs, use Register function to check additional information of installed Servers.

4.4.4. Register

1. Click the **Register button**.
2. Select the Server to register.
3. Click the **Save button** to save.

4.4.5. Modification

1. Click the **Edit(pencil) button** to change Server information to modifiable state.
2. Modify Server attributes.
3. Click the **Save button** to save.

4.4.6. Deletion

1. Click the **Delete(trash) button** to change Server information to deletable state.
2. Click the **Save button**.
3. Press the **OK button** to display a window for selecting deletion type.
   - Deregister : Delete Server information only from Manager DB and maintain physical Server engine (can be re-registered later via **Register button**)
   - Uninstall : Delete Server information from Manager DB and also delete physical Server engine
4. When Uninstall is selected, a window asking about log directory deletion is displayed.

Servers bound to Server Cluster cannot be deleted.

When use Server Delete Protection value is set to true in Manager Configuration area of ADMIN > Preference > Manager Environment menu, it can prevent servers from being uninstalled from Manager.

4.4.7. Start/Stop

Single Start/Stop

1. Click the **Stop button** to stop the Server.

2. Click the **Start button** to start the Server.

When stopping Server, shutdown method varies according to Stop Mode in General tab.

Stop : Basic shutdown option that does not guarantee currently serviced tasks.
Graceful Stop : Shuts down after completing currently serviced tasks. (Service not guaranteed on Windows)

Start button is activated only when in startable state.

Multi Server Start/Stop

1. Select multiple Servers to start or stop.
2. Click the **Multi Action button** at the bottom of Server list.
3. Select Action Type in popup window and click **Action button** to perform start or stop operations for multiple Servers.

Forced Stop/Restart

1. Click the **... button** at the far right of Server list.
2. Perform forced stop or forced restart.

4.4.8. Configuration Information Management (EN-A)

Provides functionality to change configuration information of Web Server's EN-A engine. When Server is selected from Web Server list, it moves to screen for managing configuration information.

General

General configuration values and Connection, Process information of Web Server can be edited.

Web Server's configuration information performs Validation on configuration files when saving, minimizing Server startup failures due to configuration file errors.

When configuration file error occurs, file is not saved and error message is displayed

Error message example

```
AH00526: Syntax error on line 253  Argument for 'Require all'
must be 'granted' or 'denied'
```

Detailed contents of configuration information are as follows.

1. Server Info (env.sh and /conf/httpd.conf file management)

Table 48. Server Info

Item (* indicates required values)	Description	Notes
HTTP Port(*)	HTTP Port	

Item (* indicates required values)	Description	Notes
HTTPS Port(*)	HTTPS Port	
Staging HTTP Port	Service port used when starting in Staging mode	Used during Graceful restart LENA uses basic nostage mode
Staging HTTPS Port	HTTPS port used when starting in Staging mode	Used during Graceful restart LENA uses basic nostage mode
Install Path	Server installation path	
Document Root(*)	Basic folder path where documents provided by Web Server are stored	
Welcome Page	Define which file to use as initial page document of website	
Stop Mode	Option referenced when Web Server shuts down	Stop : Basic shutdown option that does not guarantee currently serviced tasks. Graceful Stop : Shuts down after completing currently serviced tasks. (Service not guaranteed on Windows)
Directory/Path	Directory path where web documents are located to set which services and functions to allow/deny	
Directory/Options	Access control settings to apply to all files and directories under specified directory	Indexes : Prevents showing file list under Document Root when welcome page cannot be found FollowSymLinks : Prevents accessing file system other than existing web documents under Document Root via symbolic links

Item (* indicates required values)	Description	Notes
Directory/Allow Override	Set which directives to allow for resource access control configuration files for each subdirectory under Document Root (generally AccessFileName : .htaccess)	Provides following types * None : Do not allow any directives * All : All directives available * AuthConfig : Allow user authentication directives * FileInfo : Allow document type control directives * Indexes : Allow directory indexing control directives * Limit : Allow host access control directives
Directory/Require	Verify whether authenticated users perform allowed Actions	

2. Connection Info (/conf/extra/httpd-default.conf file management)

Table 49. Connection Info

Item (* indicates required values)	Description	Notes
Timeout(s)(*)	Time for Server to wait and disconnect connection when no event occurs for certain time after connection between client and Server (s)	Default : 60
Keep Alive(*)	Whether specific process continues to handle specific user's request tasks	Default : On
Max Keep Alive Requests(*)	Valid value when KeepAlive is On, process handles specific user's requests for specified number of times When this value is exceeded, that process dies and another process handles requests	Default : 100
Keep Alive Timeout(s)(*)	Valid value when KeepAlive is On, timeout to disconnect connection when no request for set time (s)	Default : 5

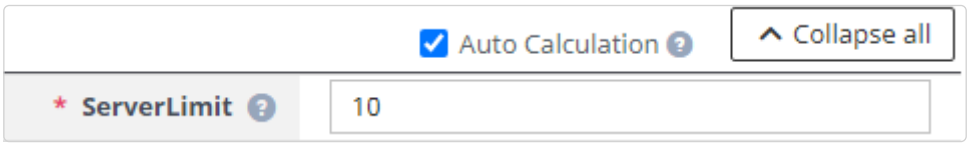
Item (* indicates required values)	Description	Notes
Request Read Timeout(s)(*)	Time to wait for receiving request header and body from user If not received within set time, sends 408 REQUEST TIME OUT error	Default : header=20-40,MinRate=500 body=20,MinRate=500

3. Process Info (/conf/extra/httpd-mpm.conf file management)

Table 50. Process Info

Item (* indicates required values)	Description	Notes
Start Servers(*)	Number of Server processes initialized when Web Server starts	Default : 2
Server Limit(*)	Maximum process value that MaxClients can create	Default : 8
Threads Per Child(*)	Number of Threads created by each child process	Default : 128
Thread Limit(*)	Maximum configurable value for ThreadsPerChild	Default : 128
Min Spare Threads(*)	When number of Idle Threads in Idle state is less than this value, Threads increase to this value and maintain	Default : 128
Max Spare Threads(*)	When number of Idle Threads in Idle state is more than this value, Threads decrease to this value and maintain	Default : 256
Max Request Workers(*)	Maximum number of Threads that all child processes can create	Default : 1024
Max Connection Per Child(*)	Maximum number of requests that child process can service. After processing this many requests, it terminates.	Default : 0 (0: unlimited)

When Web Server can use mpm event method, functionality to easily configure Process Info settings is provided.



When configuring Web Server's Process Info, checking Auto Calculation at top right provides convenient auto-calculation functionality in addition to validation of basic provided configuration values.

Rule	Validation	Auto Calculation
StartServer ServerLimit		-
ThreadsPerChild ThreadLimit		-
ThreadsPerChild + MinSpareThreads MaxSpareTheads		Auto-calculate MinSpareThreads, MaxSpareThreads when ThreadsPerChild changes
ServerLimit ThreadLimit MaxRequestWorkers		Auto-calculate MaxRequestWorkers when ServerLimit, ThreadLimit change

4. Pagespeed Info

Table 51. Pagespeed Info

Item (* indicates required values)	Description	Notes
Enabled(*)	Whether to improve site speed by performing optimization on Resources provided by Web Server by applying mod_pagespeed	Default : off Provides following options • on : Allow optimization for Resources • off : Stop additional optimization but allow access to already optimized Resources • unplugged : Stop optimization and deny access
Rewrite Level(*)	Set Level of filters that module will rewrite	

Item (* indicates required values)	Description	Notes
Default : default(CoreFilters) Provides following options * CoreFilters : Contains filters considered safe for most websites in advance * OptimizeForBandwidth : Enhanced safety, suitable for use on sites that do not recognize Pagespeed * PassThrough : Enter all filters manually	File Cache Path(*)	Path of directory where cached Files are stored
	LogDirPath(*)	Path of directory to record Logs
	Enable Filters	List of filters to use
	Disable Filters	List of filters not to use
	Allow URI	URI including wildcard(*) for Resources to allow rewrite
ex) **/**.js	Disallow URI	URI including wildcard(*) for Resources not to allow rewrite

5. SSL/TLS Security Info (/conf/extra/httpd-ssl.conf file management)

Table 52. SSL/TLS Security Info

Item (* indicates required values)	Description	Notes
Client TLS Protocol(*)	Configuration value defining protocol to use in SSL/TLS connection	Default : all -SSLv3 -TLSv1 -TLSv1.1
Client Cipher Suite(*)	Configuration value defining set of encryption algorithms to use in SSL/TLS connection	Default : HIGH:MEDIUM:!MD5:!RC4:!3DES

Item (* indicates required values)	Description	Notes
Proxy TLS Protocol(*)	Configuration defining protocol for proxy server to use in SSL/TLS connection	Default : all -SSLv3 -TLSv1 -TLSv1.1
Proxy Cipher Suite(*)	Configuration value defining set of encryption algorithms for proxy server to use in SSL/TLS connection	Default : HIGH:MEDIUM:!MD5:!RC4:!3DES

6. Enable Custom

Table 53. Custom Configuration

Item (* indicates required values)	Description	Notes
Custom Configuration	Add configurations that users want to add arbitrarily.	Stored separately in custom-httpd.conf file and managed.

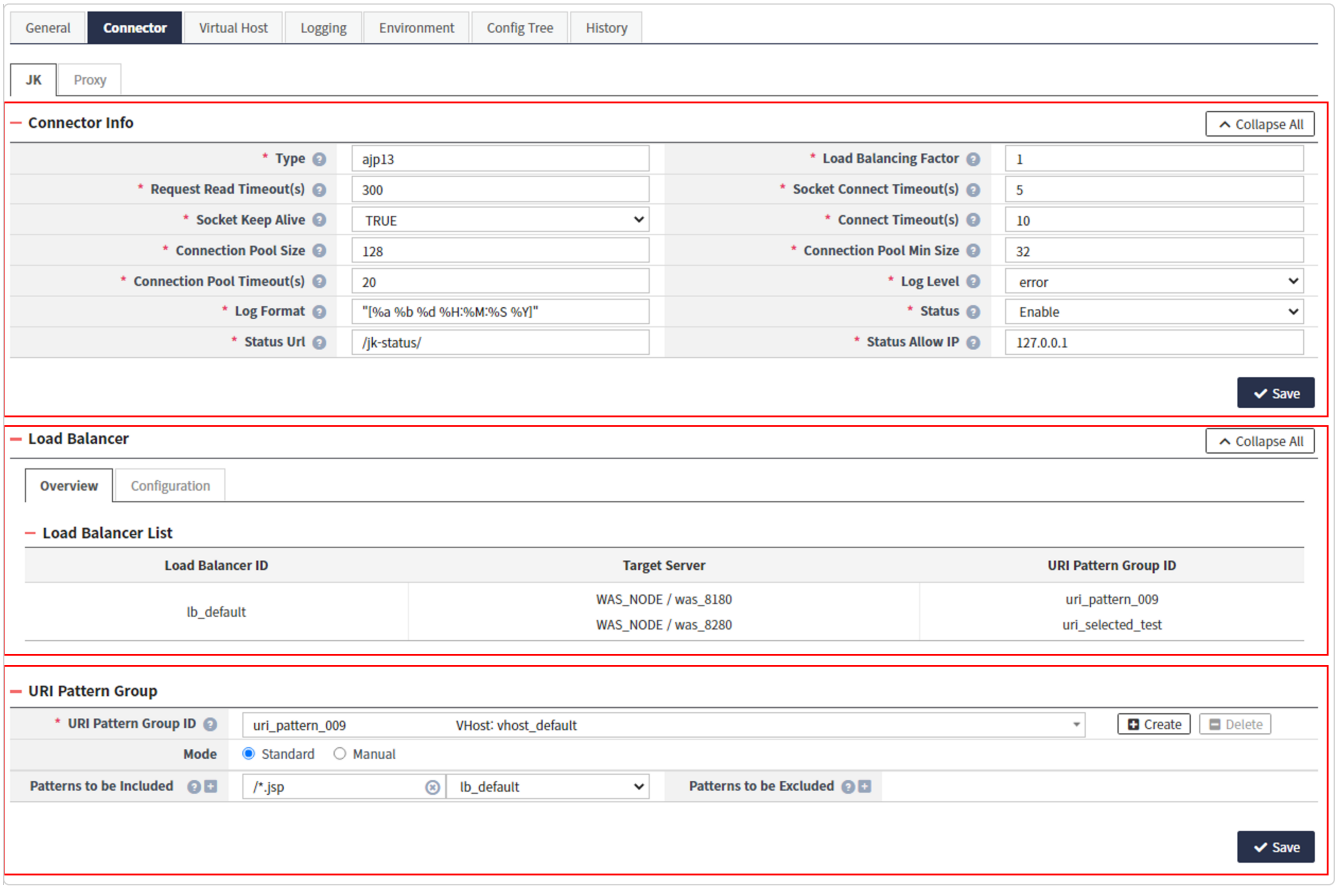
When changing configuration, Server restart is required to reflect modified items.

Connector

Manages information for linking Web Server and WAS.
Connector page is divided into JK and Proxy tabs according to linking method, and Connector configuration information according to module can be edited in each tab.

JK

Edits configuration information when using JK(mod_jk).



JK tab configuration is divided into three areas: Connector Info, Load Balancer, and URI Pattern Group as shown in the above screen.

1. Connector Info
   Manages basic configuration values of JK.

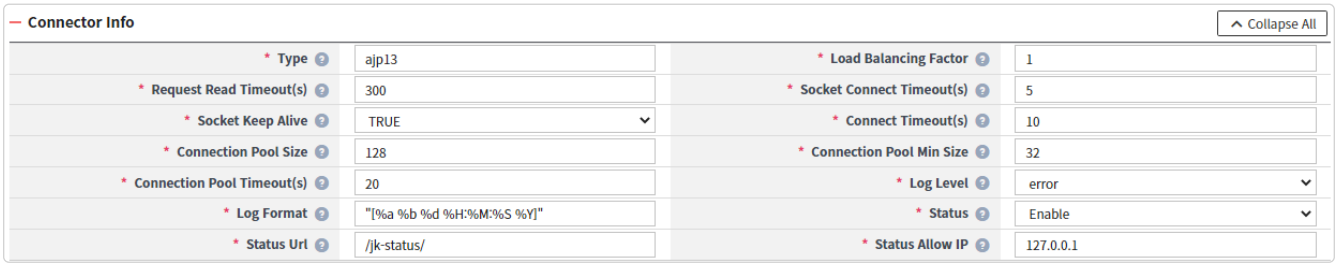


Table 54. Connector Info (JK)

Item (* indicates required values)	Description	Notes
Type(*)	Protocol used when Web Server and WAS communicate. (ajp12, ajp13, ajp14, jni, lb and status can be used, but ajp13, lb, status are recommended.)	Default: ajp13
Load Balancing Factor(*)	Load balancing index of WAS. That is, work allocation ratio.	Default: 1

Item (* indicates required values)	Description	Notes
Request Read Timeout(s)(*)	Timeout(seconds) used for communication channel between JK and remote host. If remote host does not respond within specified timeout, JK generates error and retries. When set to 0(default), JK continues to wait for response in all socket operations.	Default: 300
Socket Connect Timeout(s)(*)	Threshold for time(seconds) taken to configure socket connection between JK and remote host. If socket connection cannot be configured within specified time, JK generates error and attempts reconnection.	Default: 5
Socket Keep Alive(*)	When firewall exists between Web Server and WAS, inactive connections are discarded, but when this attribute is TRUE, sends KEEP_ALIVE message to operating system to prevent firewall from disconnecting inactive connections.	Default: TRUE
Connect Timeout(*)	connectTimeout: Wait time(s) for cpong respond to cping request in ajp13 protocol after connection between JK and WAS is completed.	Default: 10
Connection Pool Size(*)	Number of connections maintained as connection pool between JK and WAS.	Default: 128
Connection Pool Min Size(*)	Minimum number of connections maintained as connection pool between JK and WAS.	Default: 32
Connection Pool Timeout(s)(*)	Specifies time(seconds) that JK must maintain before closing inactive sockets. When set to 0, disables socket closing.	Used together with WAS's connectionTimeout option. Default: 20
Log Level(*)	Specifies log level to be recorded in log file.	Default: error
Log Format(*)	Sets format for recording logs in log file.	Default: "[%a %b %d %H:%M:%S %Y]"
Status(*)	Whether to set Server status monitoring configuration value, Status Url and Allow IP can be configured when Enable is selected.	Default: Enable
Status Url(*)	URL for Server status monitoring.	Default: /jk-status/
Status Allow IP(*)	IP that can access Server status monitoring URL.	Default: 127.0.0.1

2. Load Balancer
   Manages basic configuration and Workers of Load Balancer for load balancing.
   Load Balancer area has Overview tab and Configuration tab. Overview tab can check overall information of currently created Load Balancer, and Configuration tab can configure detailed contents of Load Balancer.

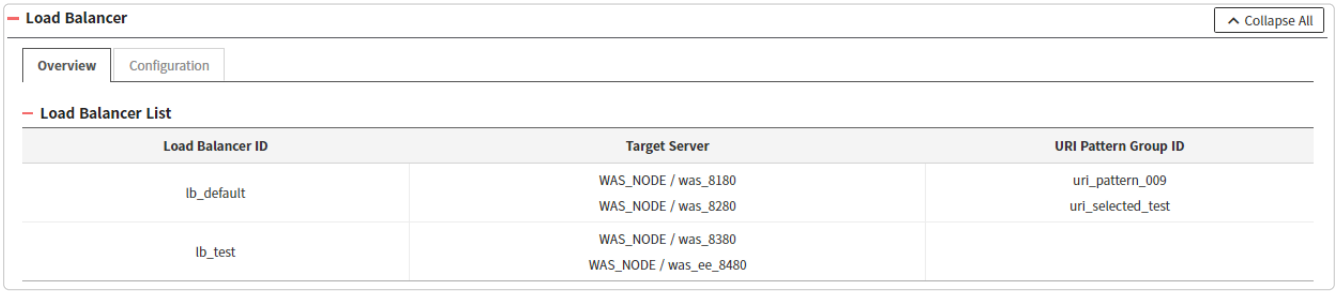


Table 55. Load Balancer Info - Overview (JK)

Item (* indicates required values)	Description	Notes
Load Balancer ID	ID of currently created Load Balancer.	
Target Server	Basic information of Workers registered in Load Balancer. Displayed in 'Node Name/Server Name' format.	
URI Pattern Group ID	When Load Balancer is specified for specific URI Pattern, URI Pattern Group ID that the URI Pattern belongs to is displayed.	

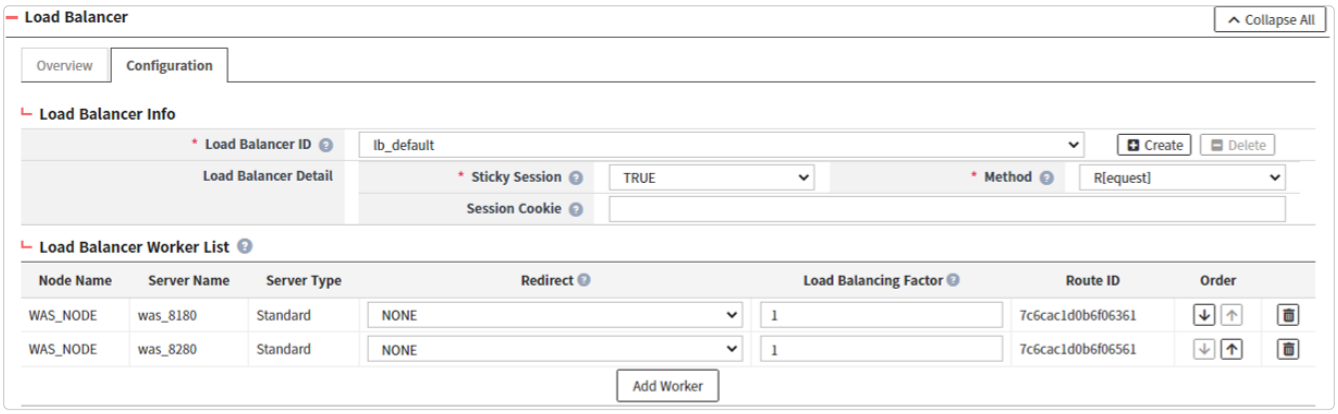


Table 56. Load Balancer Info - Configuration (JK)

Item (* indicates required values)	Description	Notes
Load Balancer ID(*)	Name of Load Balancer.	'lb_' prefix is added.
Sticky Session(*)	Whether to support routing based on Session ID.	
Method(*)	Specifies method used by Load Balancer to determine appropriate Worker for load balancing.	
* R[equest] : Selects Worker with least requests. (Default)	* S[ession] : Selects Worker with least connected sessions.	* N[ext] : Similar to S[ession] but select when fewer Sessions need to be distributed.
* T[raffic] : Selects Worker with least network traffic between JK and AJP connector.	* B[usyness] : Selects Worker with least load based on number of requests.	Session Cookie

Workers are added with Add Worker button in Load Balancer Worker List table.
When Add Worker button is pressed, window for adding Worker is displayed on screen, and users can select servers managed by LENA Manager as Workers in this window. Added Workers are managed through following information.

Table 57. Load Balancer Worker List

Item (* indicates required values)	Description	Notes
Node Name	Node name of server that Worker points to.	
Server Name	Name of server that Worker points to.	
Server Type	Type of server that Worker points to.	Standard or Enterprise is displayed as value.
Redirect	When this Worker is in error state, sets Failover Worker to handle requests received by this Worker.	Default: NONE
Load Balancing Factor	Work allocation ratio, defines how much work this Worker will do compared to other Workers.	Default: 1
Route ID	Route ID of Worker.	
Order	Can change order between Workers.	

3. URI Pattern Group
   Defines URI Mapping to pass requests coming to Web Server to WAS by checking URI patterns.

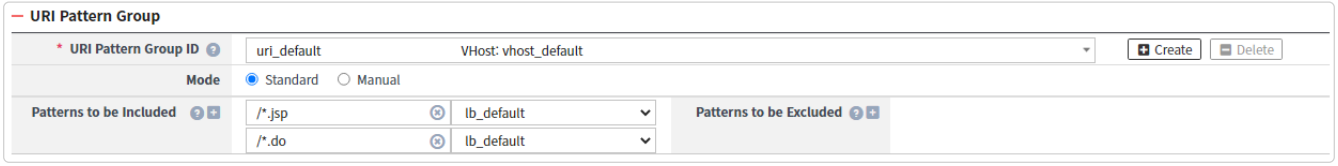


Table 58. URI Pattern Group (JK)

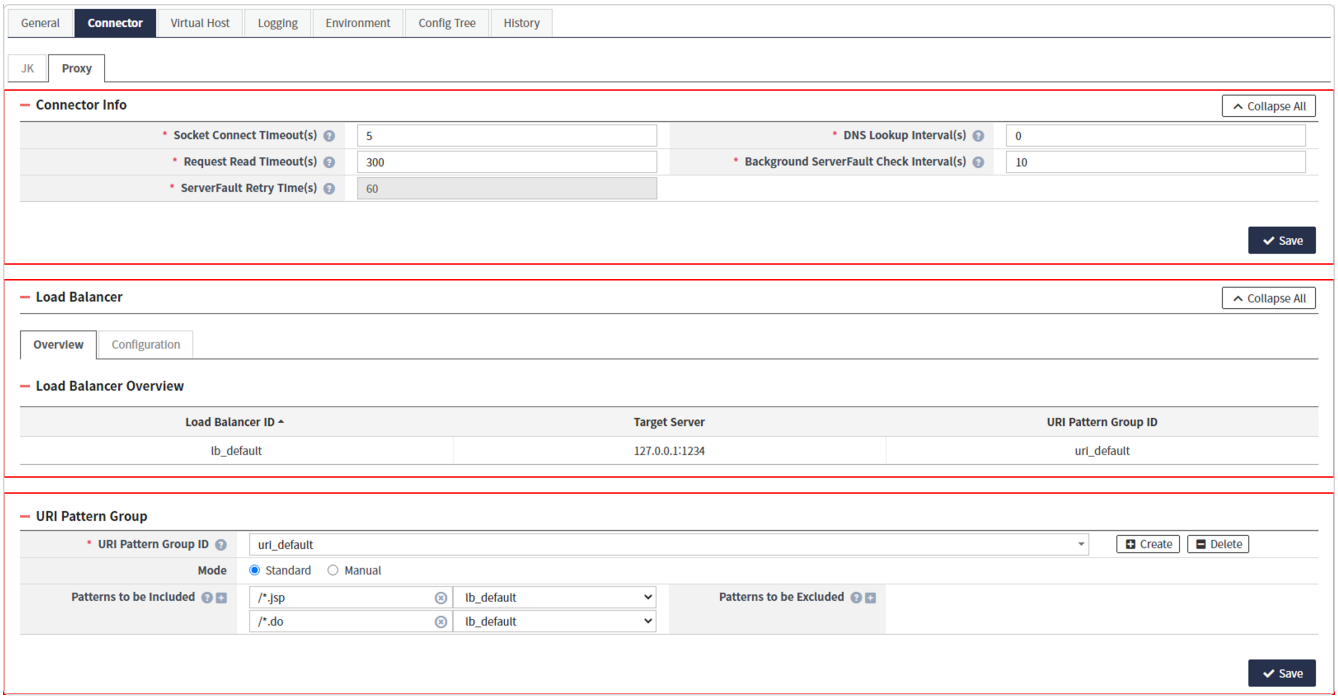
Item (* indicates required values)	Description	Notes
URI Pattern Group ID(*)	Name used for grouping and managing URI patterns. When URI Pattern Group used in Virtual Host, information about which Virtual Host is using it is displayed next to ID.	'uri_' prefix is added when Group is created.
Mode	Specifies whether to input URI patterns in format managed by LENA Manager or in user arbitrary format. Screen for inputting Patterns to be Included/Excluded or URI Patterns is displayed according to this item. If already saved pattern is in format managed by LENA Manager, it is automatically set to Standard, if in user arbitrary format, it is automatically set to Manual.	Standard: Input method according to LENA Manager URI Rule Manual: User arbitrary input method

Item (* indicates required values)	Description	Notes
Patterns to be Included	Input URI patterns to pass to WAS. Must select Load Balancer through right Select box to save. Can delete patterns through button.	Asterisk(*) meaning to allow all characters can be used, Hash(#), Equal(=) are not allowed.
Patterns to be Excluded	Input URI patterns not to pass to WAS. Can delete patterns through button.	Asterisk(*) meaning to allow all characters can be used.
URI Patterns	Used when inputting user arbitrary patterns.	

When changing configuration, Server restart is required to reflect modified items

Proxy

Edits configuration information when using Proxy(mod_proxy).



Proxy tab configuration is divided into four areas: Connector Info, Load Balancer, URI Pattern Group, and Enable Custom.

1. Connector Info
   Manages basic configuration values of Proxy.

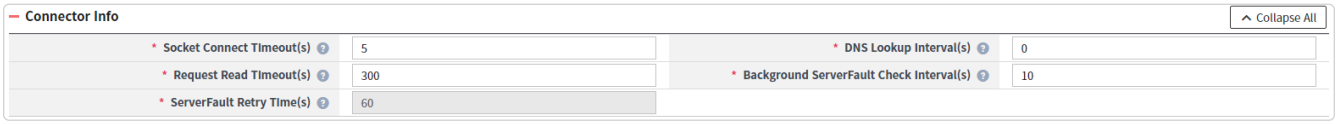


Table 59. Connector Info (Proxy)

Item (* indicates required values)	Description	Notes
Socket Connect Timeout(s)(*)	Time(s) for Apache httpd to wait until connection creation to backend is completed.	Default: 5
DNS Lookup Interval(s)(*)	DNS lookup interval. Set to 0 to disable function.	Default: 10
Request Read Timeout(s)(*)	Time(seconds) for Apache httpd to wait for transmitted data sent and received from backend.	Default: 300
Background ServerFault Check Interval(s)(*)	When Member connected to backend server is in error state, checks server at interval(seconds) set in this item and retransmits requests when server operates normally. Set to 0 to disable function.	Default: 10
ServerFault Retry Time(s)(*)	When Member connected to backend server is in error state, does not transmit any requests to that server until Apache httpd timeout(seconds) expires.	Background ServerFault Check Interval item is modifiable when 0. Default: 60

2. Load Balancer
   Manages basic configuration and Members of Load Balancer for load balancing.
   Load Balancer area has Overview tab and Configuration tab. Overview tab can check overall information of currently created Load Balancer, and Configuration tab can configure detailed contents of Load Balancer.

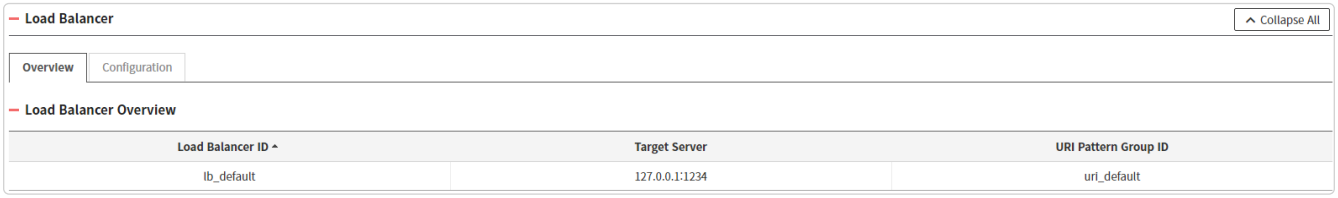


Table 60. Load Balancer Info - Overview (Proxy)

Item (* indicates required values)	Description	Notes
Load Balancer ID	ID of currently created Load Balancer.	
Target Server	Basic information of Members registered in Load Balancer. Displayed in 'Node Name/Server Name' or 'Address:Port' format.	
URI Pattern Group ID	When Load Balancer is specified for specific URI Pattern, URI Pattern Group ID that the URI Pattern belongs to is displayed.	

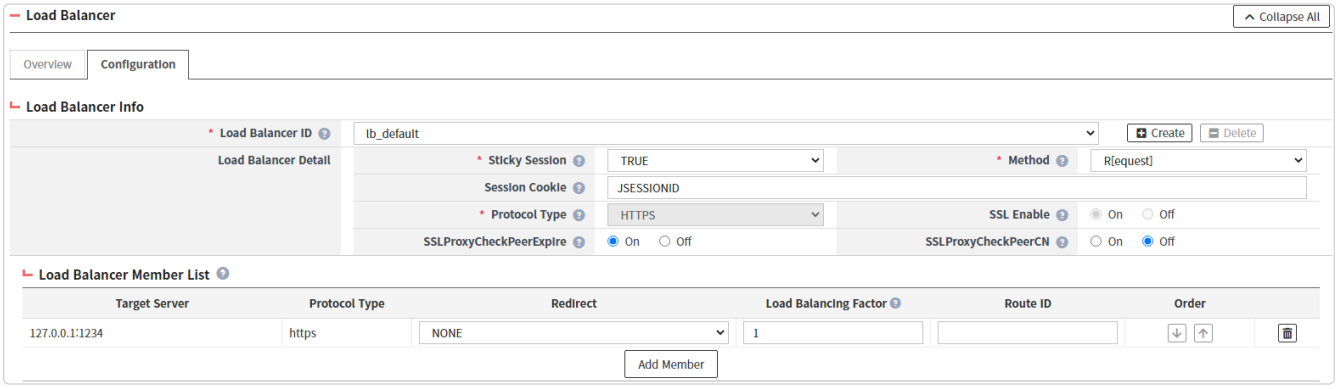


Table 61. Load Balancer Info - Configuration (Proxy)

Item (* indicates required values)	Description	Notes
Load Balancer ID(*)	Name of Load Balancer.	'lb_' prefix is added.
Sticky Session(*)	Whether to support routing based on Session ID.	
Method(*)	Specifies method used by Load Balancer to determine appropriate Member for load balancing.	
* R[equest] : Selects Member with least requests. (Default)	* T[raffic] : Selects Member with least network traffic.	* B[usyness] : Selects Member with least load based on number of requests.
Session Cookie	Set when wanting to change Session Cookie name.	
Protocol Type(*)	Specifies protocol type of Member. Can only be changed when Member is not specified.	Default: HTTP
SSL Enable	Uses SSL/TLS protocol engine for Proxy.	This option cannot be configured and operates only according to Protocol configuration. Default: Off when HTTP, On when HTTPS
SSLProxyCheckPeerExpire	Checks if remote server certificate has expired.	Default: On
SSLProxyCheckPeerCN	Checks CN field of remote server certificate.	Default: Off

Members are added with Add Member button in Load Balancer Member List table.
When Add Member button is pressed, window for adding Member is displayed on screen, and users can select servers managed by LENA Manager as Members in this window or directly input Member information to add.

Added Members are managed through following information.

Table 62. Load Balancer Member List

Item (* indicates required values)	Description	Notes
Target Server	Basic information of server that Member points to. Displayed in Node Name/Server Name format for Members managed by LENA Manager, Address:Port format for Members not managed by LENA Manager.	
Protocol Type	Protocol type used by Member.	
Redirect	When this Member is in error state, sets Failover Member to handle requests received by this Member.	Default: NONE
Load Balancing Factor	Work allocation ratio, defines how much work this Member will do compared to other Members.	Default: 1
Route ID	Route ID of Member.	Must be input when using Sticky Session.
Order	Can change order between Members.	

3. URI Pattern Group
   Defines URI Mapping to pass requests coming to Web Server to WAS by checking URI patterns.

Table 63. URI Pattern Group (Proxy)

Item (* indicates required values)	Description	Notes
URI Pattern Group ID(*)	Name used for grouping and managing URI patterns. When URI Pattern Group used in Virtual Host, information about which Virtual Host is using it is displayed next to ID.	'uri_' prefix is added when Group is created.
Mode	Specifies whether to input URI patterns in format managed by LENA Manager or in user arbitrary format. Screen for inputting Patterns to be Included/Excluded or URI Patterns is displayed according to this item. If already saved pattern is in format managed by LENA Manager, it is automatically set to Standard, if in user arbitrary format, it is automatically set to Manual.	Standard: Input method according to LENA Manager URI Rule Manual: User arbitrary input method
Patterns to be Included	Input URI patterns to pass to WAS. Must select Load Balancer through right Select box to save. Can delete patterns through button.	Asterisk(*) meaning to allow all characters can be used, Hash(#), Equal(=) are not allowed.

Item (* indicates required values)	Description	Notes
Patterns to be Excluded	Input URI patterns not to pass to WAS. Can delete patterns through button.	Asterisk(*) meaning to allow all characters can be used.
URI Patterns	Used when inputting user arbitrary patterns.	

Table 64. Enable Custom (Proxy)

Item (* indicates required values)	Description	Notes
Custom Configuration	Add configurations that users want to add arbitrarily.	Stored separately in custom-proxy.conf file and managed.

When changing configuration, Server restart is required to reflect modified items

Virtual Host

Web Server's Virtual Host information can be registered/modified/cloned/deleted.

Create button, **Delete button** can register/delete Virtual Host, **Clone button** can clone, **Rename button** can change name.

Virtual Hosts with one or more Load Balancers applied cannot be deleted. If you want to delete that Virtual Host, first change Virtual Host ID of Load Balancer to different Virtual Host ID through Connector tab.

When SSL Enabled and Rewrite Enabled are checked, detailed item areas are additionally displayed as follows.

Detailed contents of configuration information are as follows.

Managed files

- /conf/extra/vhost/{Virtual Host ID}.conf
- /conf/extra/rewrite/rewrite_{Virtual Host ID}.conf
- /conf/extra/ssl/ssl_{Virtual Host ID}.conf
- /conf/extra/vhost/custom_{Virtual Host ID}.conf

Table 65. Virtual Host Info Configuration Information

Item (* indicates required values)	Description	Notes
Virtual Host ID(*)	Virtual Host name	
Port(*)	HTTP Port used by that virtual host	

Item (* indicates required values)	Description	Notes
Document Root(*)	Homepage directory location of that virtual host	Can be specified to same or subdirectory using Server's DocumentRoot variable ${DOC_ROOT}
Domain Name(*)	Domain name to identify virtual host	
Server Alias	ServerAlias used by virtual host	Can include wildcard characters (*.example.com)
Custom Log(*)	Web log file location of virtual host	
Directory/Path	Path from DocumentRoot	
Directory/Options	Access control settings to apply to all files and directories under specified directory	-Indexes prevents showing file list under Document Root when welcome page cannot be found -FollowSymLinks prevents accessing file system other than existing web documents under Document Root via symbolic links

Item (* indicates required values)	Description	Notes
Directory/Allow Override	Set which directives to allow for resource access control configuration files for each subdirectory under Document Root (generally AccessFileName : .htaccess)	Provides following types • None : Do not allow any directives • All : All directives available • AuthConfig : Allow user authentication directives • FileInfo : Allow document type control directives • Indexes : Allow directory indexing control directives • Limit : Allow host access control directives
Directory/Require	Verify whether authenticated users perform allowed Actions	
Connector Enable	Whether to configure virtual host Connector	
Connector Type/ID	When configuring virtual host Connector, select according to Jk/Proxy type	Displays Connector list created in Connector Tab.
Rewrite Enable	Whether to use Rewrite	
Rewrite Configuration	Detailed Rewrite configuration. Rewrites according to rules set in Rewrite Rule according to specified Rewrite Condition	
Enable Custom	Add configurations that users want to add to Vhost arbitrarily	Contents are generated and stored in separate file (/conf/http/vhost/custom/custom_default.conf).
SSL Enabled	Whether to use SSL	
SSL Port(*)	HTTPS Port	

Item (* indicates required values)	Description	Notes
SSL Certificate File(*)	SSL certificate path	
SSL Certificate Key File(*)	SSL certificate Key file path	
SSL Certificate Chain File	PEM-encoded server CA certificate file path	
SSL CA Certificate File	ROOT certificate path	
SSL Password	ROOT certificate password	
Https Redirect Enabled	Whether to use Http→Https Redirect	
SSL Log Separation	Whether to use SSL Log configuration separation	
SSL Custom Log(*)	SSL Custom Log configuration	
Enable SSL/TLS Security	SSL security configuration per VirtualHost	Instead of using General SSL/TLS security configuration, SSL/TLS security configuration is applied per VirtualHost.

When changing configuration, Server restart is required to reflect modified items

Logging

Web Server's log configuration information can be edited.

Detailed contents of configuration information are as follows.

1. Log Home

Table 66. Log Home

Item (* indicates required values)	Description	Notes
Log Home(*)	Log Home path	When default is selected, set to logs folder under server installation directory, when custom is selected Log Home Prefix item allows input of log directory home path
Retention Days(*)	Maximum retention days for logs	Default : 0(unlimited)

2. Error Log

Used when Web Server records errors that occur while processing diagnostic information and requests. When problems occur during Server startup or operation, check files at location set here first.

Table 67. Error Log

Item (* indicates required values)	Description	Notes
Location(file/pipe)(*)	Specify Web Server's error log file location	
Log Level(*)	Specify how detailed to record error log file contents	

3. Log Format

Sets format to use for log files.

Table 68. Log Format

Item (* indicates required values)	Description	Notes
Format(*)	Sets format for recording logs in log file	
Nickname(*)	Name of log format to use	

4. Log Format with logio

Table 69. Log Format with logio

Item (* indicates required values)	Description	Notes
Format(*)	Sets format for recording logs in log file	Can measure bytes sent and received including request and head using %I and %O variables

Item (* indicates required values)	Description	Notes
Nickname(*)	Name of log format to use	combinedio requires mod_logio_module to be loaded

5. Log Env

Used when setting environment variables according to Request conditions.

Table 70. Log Env

Item (* indicates required values)	Description	Notes
Attribute(*)	HTTP request header (ex: Host, User-Agent, Referer, Accept-Language), one of request attributes (Remote_Host, Remote_Addr, Server_Addr, Request_Method, Request_Protocol, Request_RUI) or environment variable name associated with request	
Regex(*)	Perl compatible regular expression	
Env-variable name(*)	Variable name and value to set (optional) Varname, !varname or varname=value	
Case	Whether to distinguish case for Env-variable	With case : Distinguish case No case : No case distinction

When changing configuration, Server restart is required to reflect modified items

Environment

Provides screen for managing JVM options, Start Shell configuration, etc. Modify through file editor and click **Save button** to save.

- Custom Env (/bin/customenv.sh): User custom environment variable configuration
- Base Env (/env.sh) - Shell Script for Server startup

By default, configuration cannot be modified. If you want to modify, click **Configuration button** in ADMIN > Manager Environment > Manager Configuration item and change the following configuration to false.

```
server.environment.envshell.readonly=false
```

Configuration Tree

Web Server's ${SERVER_HOME}/conf directory sub configuration files can be managed through file editor.

User running Node Agent must have access permission to Web Server configuration information files for modification. If access permission is not available, message that file cannot be edited due to no Write permission is displayed.

History

Provides backup and restore functionality for configuration information. When configuration information is modified and saved, History is managed. Search by entering modification date.

Click **View(magnifying glass) button** to view information of selected file, and click **Restore button** to restore to that configuration file.

4.4.9. Configuration Information Management (EN-N)

Provides functionality to change engine configuration information of EN-N type Web Server. When Server is selected from Web Server list, it moves to screen for managing configuration information.

General

General configuration values and Connection, Process information of Web Server can be edited.

Web Server's configuration information performs Validation on configuration files when saving, minimizing Server startup failures due to configuration file errors.

When configuration file error occurs, file is not saved and error message is displayed

Error message example

```
AH00526: Syntax error on line 253  Argument for 'Require all'
must be 'granted' or 'denied'
```

Detailed contents of configuration information are as follows.

1. Server Info (/var/common_value.env file management)

Table 71. Server Info

Item (* indicates required values)	Description	Notes
Install Path	Server installation path	
Base Port(*)	Port Type information and Port Number set during installation	Port Type cannot be changed, Port Number can be changed
Welcome Page	Define which file to use as initial page document of website	
Stop Mode	Server stop Mode	• Stop • Graceful Stop
Directory Root Path	Basic folder path where documents provided by Web Server are stored	
Disable Symbolic Links	Whether to not use Symbolic Link	Default : on (not used)
Diasble Auto Index	Enable or disable directory listing output.	Default : on (disabled)

2. Additional Port Info (/var/tcp_port.env, /var/udp_port.env file management)

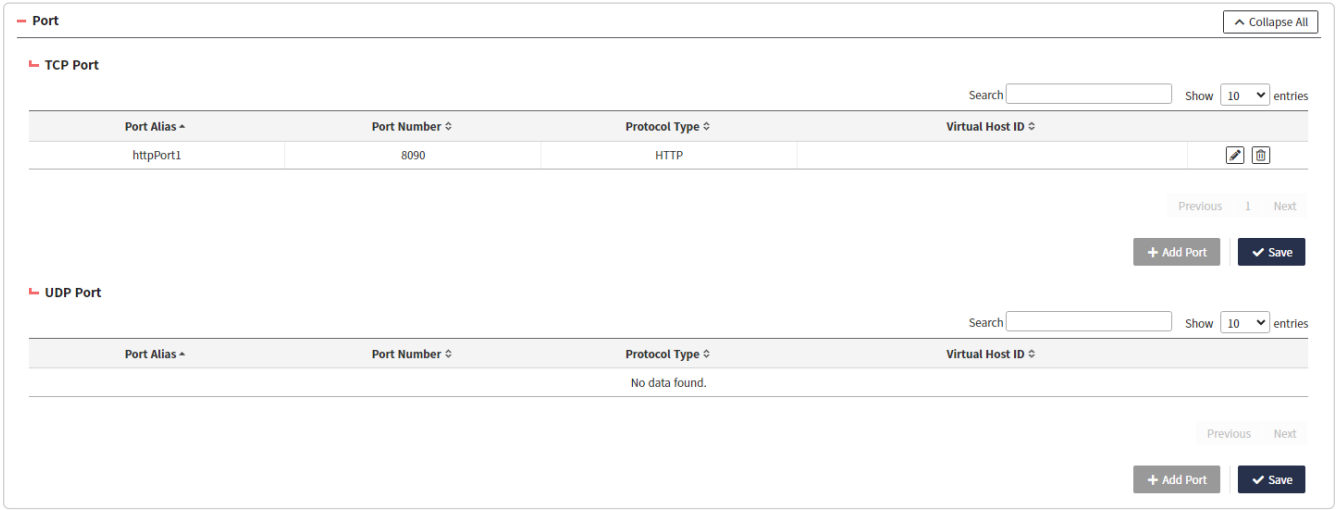


Table 72. TCP Port

Item (* indicates required values)	Description	Notes
Port Alias(*)	Set Alias of port.	
Port Number	Specify port number.	
Protocol Type	Select protocol type.	

Item (* indicates required values)	Description	Notes
Virtual Host ID	Display Virtual Host ID using that Port.	Cannot change Port Alias when specific Virtual Host is using that Port.

TCP Protocol dedicated usage ports (Proxy(HTTP, HTTPS), Net Gateway(TCP))

Table 73. UDP Port

Item (* indicates required values)	Description	Notes
Port Alias(*)	Set Alias of port.	
Port Number	Specify port number.	
Protocol Type	Select protocol type.	
Virtual Host ID	Display Virtual Host ID using that Port.	Cannot change Port Alias when specific Virtual Host is using that Port.

UDP Protocol dedicated usage ports (Net Gateway)

3. Connection Info (/var/common_value.env file management - related file /conf/http/lenan-http.conf)

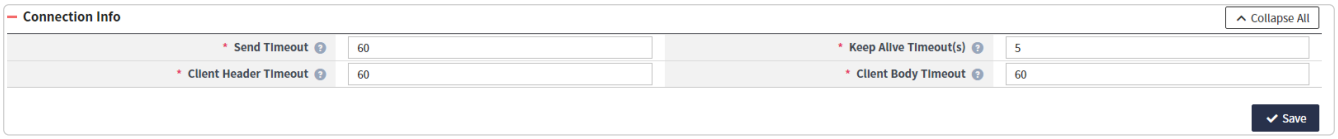


Table 74. Connection Info

Item (* indicates required values)	Description	Notes
Send Timeout(*)	Timeout time set for sending response to client. **This is timeout time between two consecutive write operations, not total response transmission timeout time.** If client receives nothing within time specified in send_timeout, connection is closed.	Default : 60
Keep Alive Timeout(s) (*)	Timeout time set for keeping connection between server and client open.	Default : 5

Item (* indicates required values)	Description	Notes
Client Header Timeout(*)	Time to read request header information, if **client does not send header within specified time**, request ends with 408(Request Time-out).	Default: 60
Client Body Timeout(*)	Time to read request body information, **this is timeout time between two consecutive read operations, not total request body transmission timeout time.** If client sends nothing within time specified in client_body_timeout, request ends with 408(Request Time-out).	Default: 60

4. Process Info (/var/common_value.env file management - related file /conf/lenan.conf)

Table 75. Process Info

Item (* indicates required values)	Description	Notes
Worker Process(*)	Define number of worker processes.	Default : 2
Worker Connection(*)	Set maximum number of simultaneous connections.	Maximum Request allowance: worker_processes * worker_connections

When changing configuration, Server restart is required to reflect modified items.

5. Enable Custom (/conf/custom/custom.conf file management - related file /conf/lenan.conf)

[server 5 general enableCustom] | manual/server_5_general_enableCustom.png

Table 76. Enable Custom

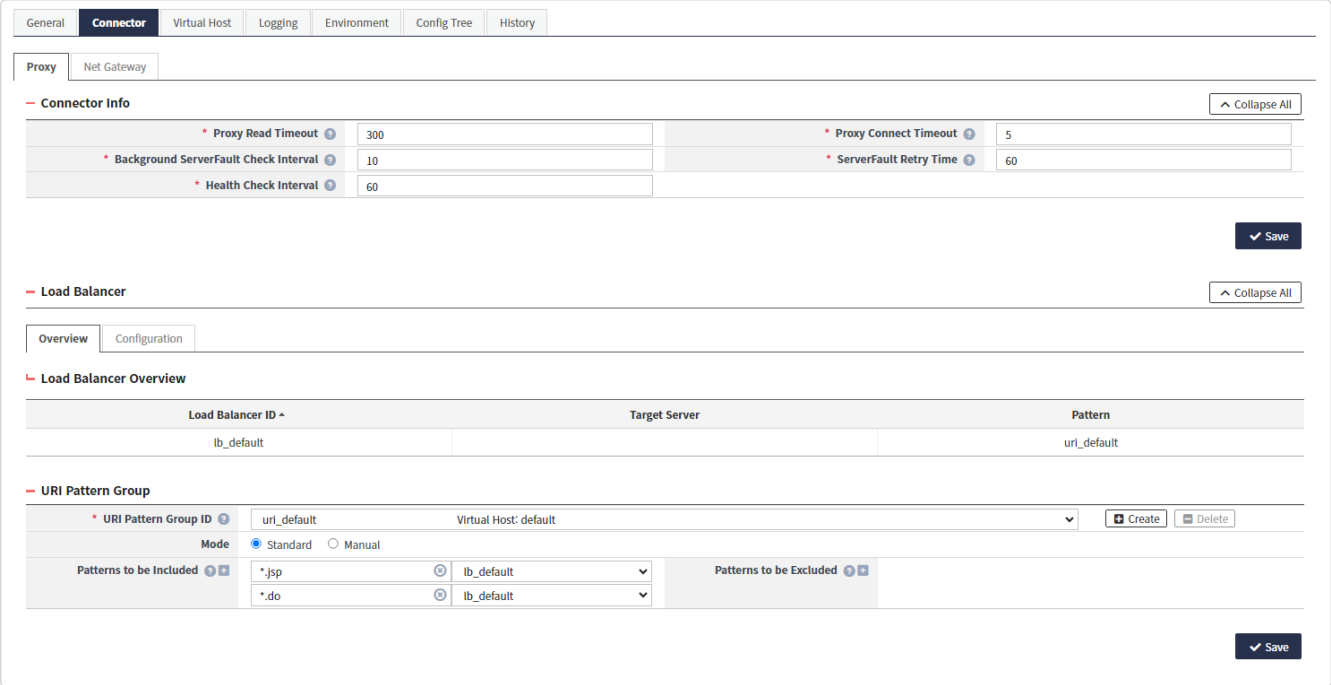
Item (* indicates required values)	Description	Notes
Custom Configuration	Input content that users can freely insert through custom.conf included in lenan.conf.	

Connector

Manages information for linking Web Server and WAS(Backend).
Connector page is divided into Proxy and Net Gateway tabs according to protocol, and Connector configuration information according to module can be edited in each tab.

Proxy

Edits configuration information when using Proxy(ngx_http_upstream_module).



Proxy tab configuration is divided into three areas: Connector Info, Load Balancer, and URI Pattern Group as shown in the above screen.

1. Connector Info
   Manages basic configuration values of Proxy.

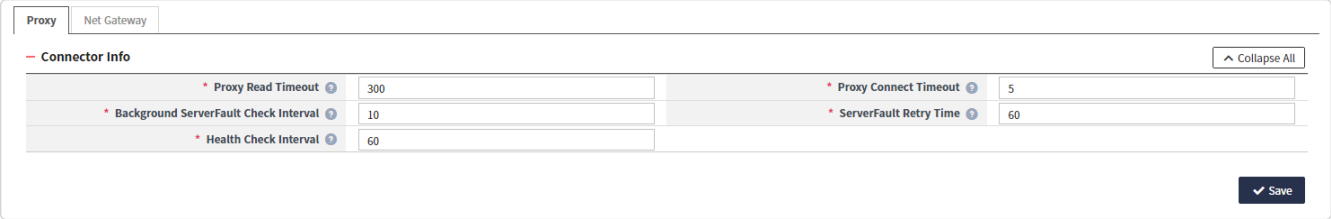


Table 77. Connector Info (Proxy)

Item (* indicates required values)	Description	Notes
Proxy Read Timeout(*)	Timeout time set for reading response from backend server. This is timeout time between two consecutive read operations, not total response transmission timeout time. If backend server sends nothing within time specified in proxy_read_timeout, connection is closed.	Default: 300
Proxy Connect Timeout(*)	Define time limit for establishing connection with backend server. This time limit generally cannot exceed 75 seconds.	Default: 5

Item (* indicates required values)	Description	Notes
Background ServerFault Check Interval(*)	When Member connected to backend server is in error state, checks server at interval(seconds) set in this item and retransmits requests when server operates normally. Set to 0 to disable function.	Default: 10
Server Fault Retry Time(*)	When Member connected to backend server is in error state, does not transmit any requests to that server until timeout(seconds) expires.	Default: 60
Health Check Interval(*)	Checks server at interval(seconds) set for checking backend server status. Set to 0 to disable function.	Default: 60
DNS Lookup Interval(*)	DNS lookup interval. Set to 0 to disable function.	Default: 10

When Background ServerFault Check Interval and Health Check Interval are saved as 0
All LoadBalancer's Auto Server Fault Recovery values change to off, and new creation values are also fixed to off.

2. Load Balancer
   Manages basic configuration and Members of Load Balancer for load balancing.
   Load Balancer area has Overview tab and Configuration tab. Overview tab can check overall information of currently created Load Balancer, and Configuration tab can configure detailed contents of Load Balancer.

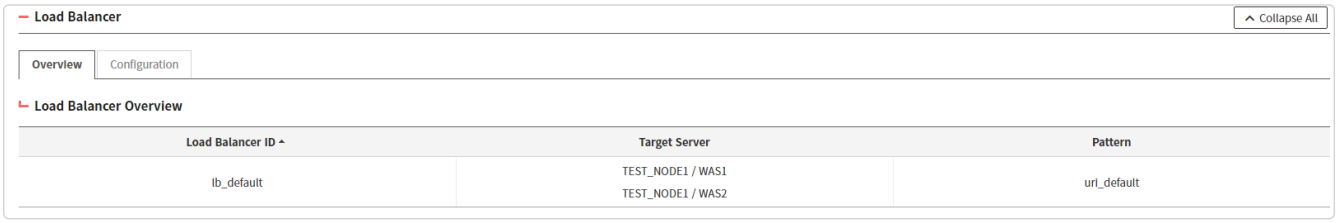


Table 78. Load Balancer Info - Overview (Proxy)

Item (* indicates required values)	Description	Notes
Load Balancer ID	ID of currently created Load Balancer.	
Target Server	Basic information of Workers registered in Load Balancer. Displayed in 'Node Name/Server Name' format.	
Pattern	When Load Balancer is specified for specific URI Pattern, URI Pattern Group ID that the URI Pattern belongs to is displayed.	

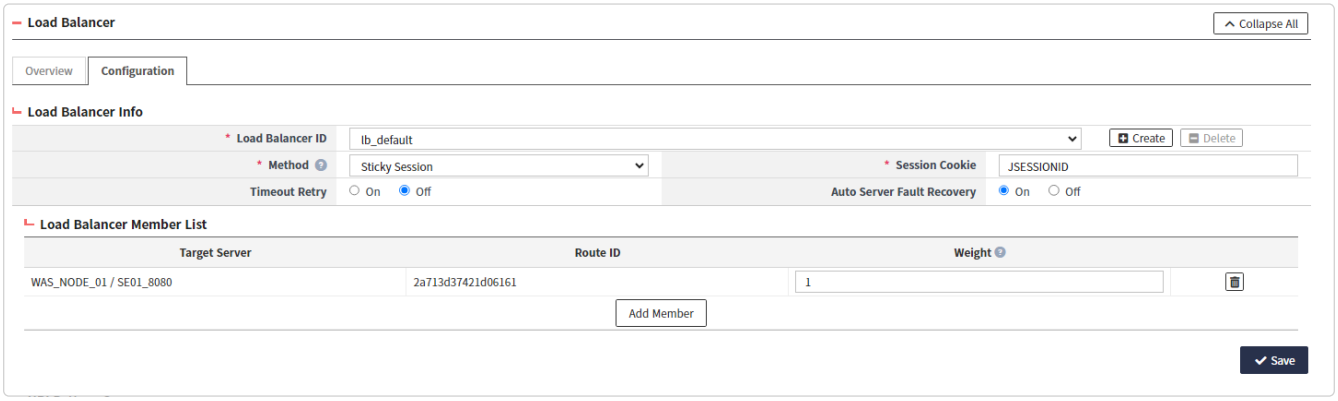


Table 79. Load Balancer Info - Configuration (Proxy)

Item (* indicates required values)	Description	Notes
Load Balancer ID(*)	Name of Load Balancer.	'lb_' prefix is added.
Method(*)	Specifies method used by Load Balancer to determine appropriate Worker for load balancing.	
* Sticky Session : Route based on Session Cookie	* RoundRobin : Route in order of registered members	• IP Hash : Route based on Client's IP
* Least Connection : Route to side with fewer connections	Session Cookie(*)	Set when wanting to change Session Cookie name.
Default: JSESSIONID	Timeout Retry	Set when wanting to change Session Cookie name.
Default:Off When On is set, retransmits when Gateway Timeout occurs.	Auto Server Fault Recovery	Whether to use fox Directive

Members are added with Add Member button in Load Balancer MemberList table.
When Add Member button is pressed, window for adding Member is displayed on screen, and users can select servers managed by LENA Manager as Members in this window. Added Members are managed through following information.

Table 80. Load Balancer Member List

Item (* indicates required values)	Description	Notes
Target Server	Node name and server name of server that Member points to.	
Route ID	Route ID of Member	

Item (* indicates required values)	Description	Notes
Weight	Work allocation ratio, defines how much work this Worker will do compared to other Workers.	Default: 1

3. URI Pattern Group
   Defines URI Mapping to pass requests coming to Web Server to WAS by checking URI patterns.

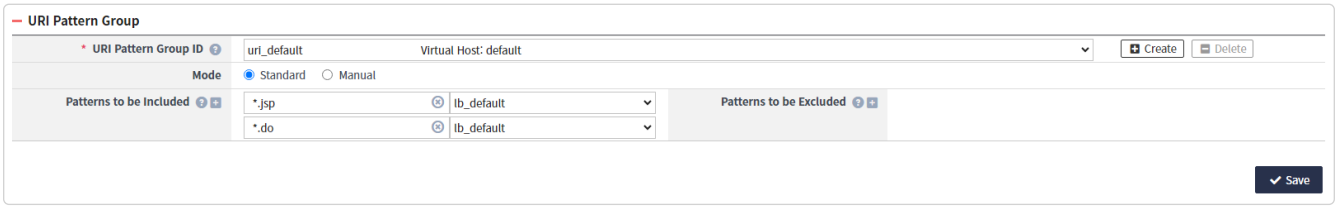


Table 81. URI Pattern Group (Proxy)

Item (* indicates required values)	Description	Notes
URI Pattern Group ID(*)	Name used for grouping and managing URI patterns. When URI Pattern Group used in Virtual Host, information about which Virtual Host is using it is displayed next to ID.	Group creation adds 'uri_' prefix.
Mode	Specifies whether to input URI patterns in format managed by LENA Manager or in user arbitrary format. Screen for inputting Patterns to be Included/Excluded or URI Patterns is displayed according to this item. If already saved pattern is in format managed by LENA Manager, it is automatically set to Standard, if in user arbitrary format, it is automatically set to Manual.	• Standard: Input method according to LENA Manager URI Rule • Manual: User arbitrary input method
Patterns to be Included	Input URI patterns to pass to WAS. Must select Load Balancer through right Select box to save. Can delete patterns through button.	Asterisk(*) meaning to allow all characters can be used, Hash(#), Equal(=) are not allowed.
Patterns to be Excluded	Input URI patterns not to pass to WAS. Can delete patterns through button.	Asterisk(*) meaning to allow all characters can be used.
URI Patterns	Used when inputting user arbitrary patterns.	

4. Enable Custom
   /conf/http/custom/custom_http.conf file management - related file /conf/http/lenan-http.conf)

[server 5 web server proxy enable custom] | manual/server_5_web_server_proxy_enable_custom.png

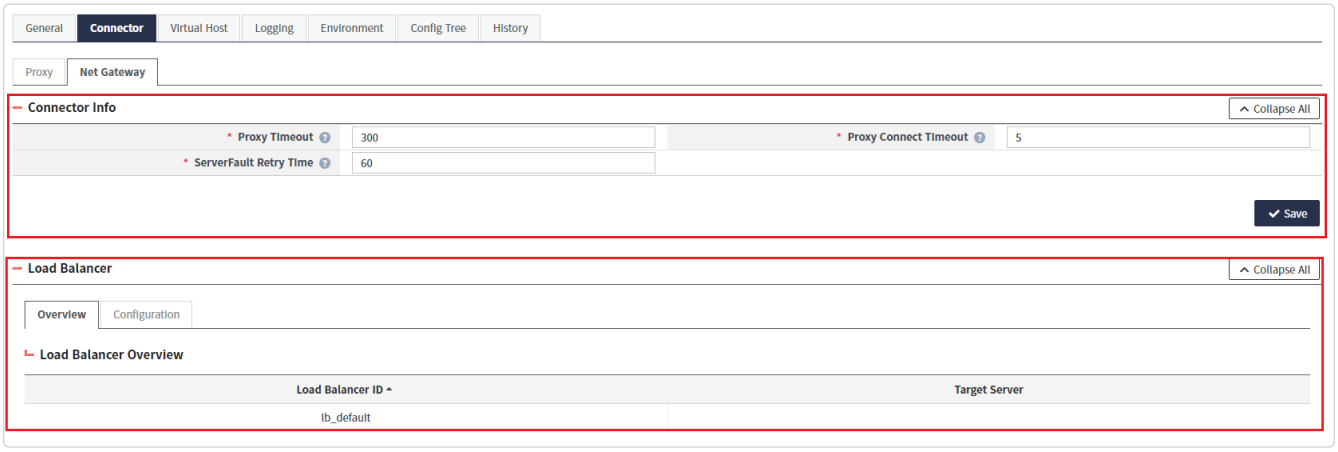
Table 82. Enable Custom (Proxy)

Item (* indicates required values)	Description	Notes
Custom Configuration	Input content that users can freely insert through custom_http.conf included in lenan-http.conf.	

When changing configuration, Server restart is required to reflect modified items

Net Gateway

Edits configuration information when using Net Gateway(ngx_stream_upstream_module).



Net Gateway tab configuration is divided into two areas: Connector Info and Load Balancer.

1. Connector Info
   Manages basic configuration values of Net Gateway.

Table 83. Connector Info (Net Gateway)

Item (* indicates required values)	Description	Notes
Proxy Timeout(s)(*)	Set time limit between two consecutive read or write operations in client or proxy server connection. If data is not transmitted within this time, connection is closed.	Default: 5
Proxy Connect Timeout(s)(*)	Define timeout for establishing connection with proxy server	Default: 10
ServerFault Retry Time(s)(*)	Time period during which server is considered unavailable after specified number of server communication failures occur, period during which server is considered unavailable.	Default: 60

2. Load Balancer
   Manages basic configuration and Members of Load Balancer for load balancing.
   Load Balancer area has Overview tab and Configuration tab. Overview tab can check overall information of currently created Load Balancer, and Configuration tab can configure detailed

contents of Load Balancer.

Table 84. Load Balancer Info - Overview (Net Gateway)

Item (* indicates required values)	Description	Notes
Load Balancer ID	ID of currently created Load Balancer.	
Target Server	Basic information of Members registered in Load Balancer. Displayed in 'Address:Port' format.	

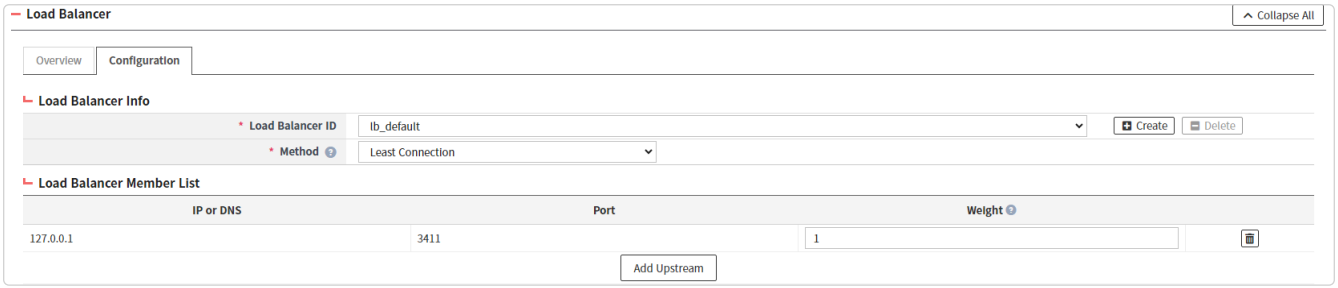


Table 85. Load Balancer Info - Configuration (Net Gateway)

Item (* indicates required values)	Description	Notes
Load Balancer ID(*)	Name of Load Balancer.	'lb_' prefix is added.
Method(*)	Specifies method used by Load Balancer to determine appropriate Member for load balancing.	
* Round Robin : Route sequentially through registered member list	* IP Hash : Route based on Client IP	• Least Connection : Route to side with fewer connections based on Connection

Members are added with Add Upstream button in Load Balancer Member List table.
When Add Upstream button is pressed, window for adding Upstream is displayed on screen, and users can directly input Upstream information to add in this window.

Added Upstreams are managed through following information.

Table 86. Load Balancer Member List

Item (* indicates required values)	Description	Notes
IP or DNS	Basic information of server that Upstream points to. Basically displayed in Address:Port format.	DNS can also be input.

Item (* indicates required values)	Description	Notes
Port	Port information used by Upstream.	
Weight	Work allocation ratio, defines how much work this Upstream will do compared to other Upstreams.	Default: 1 Cannot input 0 for work allocation (changes to default 1)

3. Enable Custom /conf/stream/custom/custom_stream.conf file management - related file /conf/stream/lenan-stream.conf)

[server 5 web server stream enable custom] |

manual/server_5_web_server_stream_enable_custom.png

Table 87. Enable Custom (Net Gateway)

Item (* indicates required values)	Description	Notes
Custom Configuration	Input content that users can freely insert through custom_stream.conf included in lenan-stream.conf.	

When changing configuration, Server restart is required to reflect modified items

Virtual Host

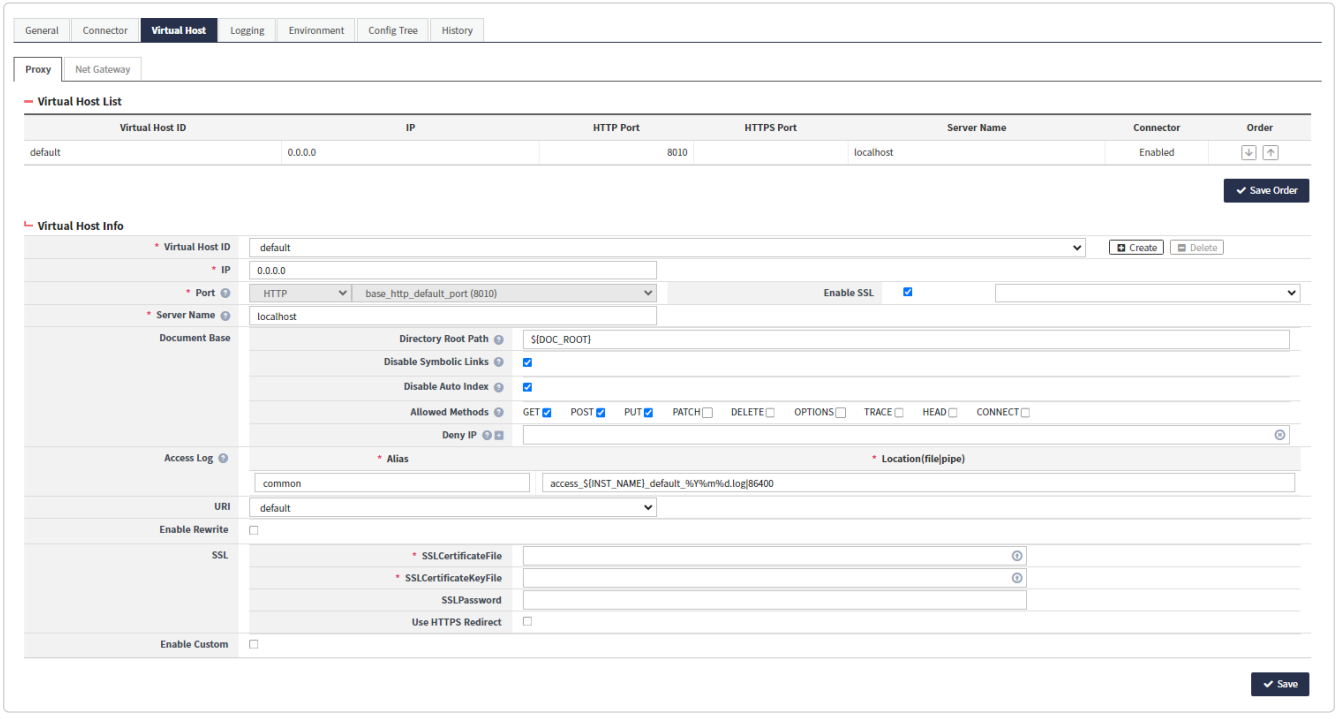
Proxy

Proxy Web Server's Virtual Host information can be registered/modified/cloned/deleted.

Create button, **Delete button** can register/delete Virtual Host, **Clone button** can clone, **Rename button** can change name.

Virtual Hosts with one or more Load Balancers applied cannot be deleted. If you want to delete that Virtual Host, first change Virtual Host ID of Load Balancer to different Virtual Host ID through Connector tab.

When Enable SSL and Enable Rewrite and Enable Custom are checked, detailed item areas are additionally displayed.



Detailed contents of configuration information are as follows.

Managed files

- /conf/http/vhost/vhost_{Virtual Host ID}.conf
- /conf/http/vhost/vhost.list
- /conf/http/vhost/rewrite/rewrite_{Virtual Host ID}.conf

- /conf/http/vhost/custom/custom_{Virtual Host ID}.conf

Table 88. Virtual Host Info Configuration Information

Item (* indicates required values)	Description	Notes
Virtual Host ID(*)	Virtual Host name	
Domain Name	Domain name to identify virtual host	
IP(*)	Select protocol to be used by that virtual host (HTTP, HTTPS) IP used by that virtual host	
Port(*)	Port used by that virtual host	
SSL Enable	Whether to additionally use SSL, HTTPS service port to be used by that virtual host	When checked, need to use port from combo box for HTTPS service port (port information to use must be pre-registered as HTTPS port in General tab's Port Info)
SSL/SSLCertificateFile	SSL certificate path	
SSL/SSLCertificateKeyFile	SSL certificate Key file path	
SSL/SSLPassword	SSL Password	When password is input, managed through AES256 encryption
SSL/Use HTTPS Redirect	Whether to use HttpHttps Redirect	
Document base/Directory Root Path	Homepage directory location of that virtual host	Can be specified to same or subdirectory using Server's DocumentRoot variable ${DOC_ROOT}
Document base/Disable Symbolic Links	Prevent accessing file system other than existing web documents under Document Root via symbolic links	
Document base/Disable Auto Index	Prevent showing file list under Document Root when welcome page cannot be found	

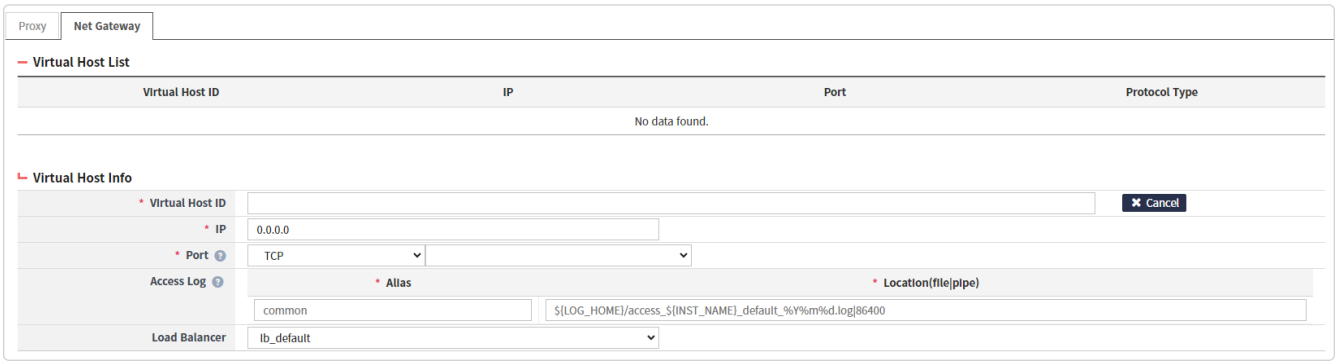
Item (* indicates required values)	Description	Notes
Document base/Allowed Methods	Allow access for specified http methods	
Document base/Deny IP	Deny access for specified networks or addresses	
Access Log/Alias	Set format for recording logs in log file	
Access Log/Location	Set location and name for log files	
URI	Select URI Pattern Group set in Connector Proxy Tab	Not required selection
Enable Rewrite	Whether to use Rewrite function, creates input window below when checked	Input content is generated and stored in separate file
Enable Custom	Whether to use Custom Configuration, creates input window below when checked	Input content is generated and stored in separate file (/conf/http/vhost/custom/custom_default.conf)

Net Gateway

Net Gateway Web Server's Virtual Host information can be registered/modified/cloned/deleted.

Create button, **Delete button** can register/delete Virtual Host, **Clone button** can clone, **Rename button** can change name.

Virtual Hosts with one or more Load Balancers applied cannot be deleted. If you want to delete that Virtual Host, first change Virtual Host ID of Load Balancer to different Virtual Host ID through Connector tab.



Detailed contents of configuration information are as follows.

Managed files

- /conf/stream/vhost/vhost_{Virtual Host ID}.conf

- /conf/stream/vhost/vhost.list
- /conf/stream/vhost/custom_{Virtual Host ID}.conf

Table 89. Virtual Host Info Configuration Information

Item (* indicates required values)	Description	Notes
Virtual Host ID(*)	Virtual Host name	
IP(*)	Select protocol to be used by that virtual host (HTTP, HTTPS) IP used by that virtual host	
Port(*)	Port used by that virtual host	
Access Log/Alias	Set format for recording logs in log file	
Access Log/Location	Set location and name for log files	
Load Balancer	Select Load Balancer Group set in Connector Net Gateway Tab	
Enable Custom	Whether to use Custom Configuration, creates input window below when checked	Input content is generated and stored in separate file (/conf/stream/vhost/custom/custom_default.conf)

Logging

Web Server's log configuration information can be edited.

Detailed contents of configuration information are as follows.

1. Log Home

Table 90. Log Home

Item (* indicates required values)	Description	Notes
Log Home(*)	Log Home path	When default is selected, set to logs folder under server installation directory, when custom is selected Log Home Prefix item allows input of log directory home path
Retention Days(*)	Maximum retention days for logs	Default : 0(unlimited)

2. Error Log

Used when Web Server records errors that occur while processing diagnostic information and requests. When problems occur during Server startup or operation, check files at location set here first.

Table 91. Error Log

Item (* indicates required values)	Description	Notes
Location(file/pipe)(*)	Specify Web Server's error log file location	
Log Level(*)	Specify how detailed to record error log file contents	

3. Log Format : Proxy

Sets format to use for Proxy log files.

Table 92. Log Format : Proxy

Item (* indicates required values)	Description	Notes
Alias(*)	Name of log format to use	
Format(*)	Sets format for recording logs in log file	

4. Log Format : Net Gateway

Sets format to use for Net Gateway log files.

Table 93. Log Format : Net Gateway

Item (* indicates required values)	Description	Notes
Alias(*)	Name of log format to use	
Format(*)	Sets format for recording logs in log file	

When changing configuration, Server restart is required to reflect modified items

Environment

Provides screen for managing JVM options, Start Shell configuration, etc. Modify through file editor and click **Save button** to save.

- Custom Env (/bin/customenv.sh): User custom environment variable configuration
- Base Env (/env.sh) - Shell Script for Server startup

By default, configuration cannot be modified. If you want to modify, click **Configuration button** in ADMIN > Manager Environment > Manager Configuration item and change the following configuration to false.

```
server.environment.envshell.readonly=false
```

Configuration Tree

Web Server's ${SERVER_HOME}/conf directory sub configuration files can be managed through file editor.

User running Node Agent must have access permission to Web Server configuration information files for modification. If access permission is not available, message that file cannot be edited due to no Write permission is displayed.

History

Provides backup and restore functionality for configuration information. When configuration information is modified and saved, History is managed. Search by entering modification date.

Click **View(magnifying glass) button** to view information of selected file, and click **Restore button** to restore to that configuration file.

4.4.10. Server Log Viewer

Log Viewer button on right side of server list allows browsing log file contents under target server's Log Home path.

To use this functionality, the following must be satisfied.

- Node to which target server belongs must be running.

Click Log Viewer button in server list to check directories and files in tree structure based on target server's Log Home path.

When file is selected, file contents are queried, and when first selected, file contents from end of file up to predetermined size can be checked.

Use Load More, Load Previous buttons to query and check log file contents by predetermined size.

- When using Load Previous button and no more content to query (eg. beginning of file), Alert message that no more data can be read is displayed.

- When using Load More button and no more content to query (eg. end of file), message that no more data can be read is displayed at bottom of screen.

4.5. Session Server

Provides a screen for managing Session Server. You can register, modify, and delete Session Servers installed on Nodes, and execute start and stop shells.

4.5.1. List

You can manage each WAS through the Session Server List.

Figure 7. Session Server List

The properties of Session Server are as follows.

Table 94. Session Server Properties

Item (* indicates required value)	Description	Notes
Status	Session Server status	• Started(v) • Stop(□) • Error(!)
Name(*)	Session Server name	
Address	Session Server IP address	
Server ID	Server ID	
Type	Session Server type	• Standalone • Embedded
Port	Service port number	
Start/Stop button	Server start and stop	

Item (* indicates required value)	Description	Notes
Button area	Displays server information change and related function buttons	**Trash can icon** - Delete server information **Pen icon** - Modify server information **Log file icon** - Provides Server Log Viewer functionality **More icon** - Provides menu for performing Start/Stop

Session Server is a functionality provided by Enterprise Edition and is available when installing Enterprise version WAS.

4.5.2. Install

1. Click the **Install button**.
2. Enter Server ID, Service Port, and Mirror Server IP/Port.
3. Click the **Save button** to save.

There may be differences between the information of Servers actually installed on Nodes and Servers managed by Manager. (When installing via console)

If a Server ID duplication error occurs, use the Register function to check previously installed Server information.

4.5.3. Register

1. Click the **Register button**.
2. Click on the Server to register.
3. Click the **Save button** to save.

4.5.4. Modification

1. Click the **Edit(pencil) button** to change Server information to modifiable state.
2. Modify Server properties.
3. Click the **Save button** to save.

4.5.5. Deletion

1. Click the **Delete(trash can) button** to change Server information to deletable state.
2. Click the **Save button**.
3. Press the **OK button** to display a window for selecting deletion type.
    - Deregister : Delete Server information only from Manager DB and maintain physical Server engine (can be re-registered later via **Register button**)

- Uninstall : Delete Server information from Manager DB and also delete physical Server engine

4. Uninstall selection, a window asking to delete the log directory is displayed.

Servers linked to a Server Cluster cannot be deleted.

When the use Server Delete Protection value in the Manager Environment menu of ADMIN > Preference > Manager Environment is set to true, Manager can prevent the server from being uninstalled.

4.5.6. Start/Stop

1. Click the **Stop button** to stop the Server.
2. Click the **Start button** to start the Server.

Only when the Server is in a state where it can be started, the **Start button** is activated.

4.5.7. Setting Information Management

General

Provides functionality to change Server settings. When you select a Server in the Session Server list, you will be taken to a screen to manage the settings.

The properties that can be changed in the environment settings are as follows.

1. Configuration

Table 95. Configuration

Item (* indicates required value)	Description	Notes
Host(*)	Server's Service Host (IP)	
Port(*)	Server's Service Port	
Mirror Server Host(*)	Pair Server's Host (IP)	
Mirror Serror Port(*)	Pair Server's Service Port	
Share session in applications	Setting for sharing Session between Multi Applications.	You must process this item with the same value in WAS. Only available in standalone.

2. Connected WAS List

Refresh button to refresh the list.

Table 96. Connected WAS List

Item (* indicates required value)	Description	Notes
Server ID	WAS ID	
Host	Host name where WAS is installed	

3. Status (Provides Session Server status information)

Refresh button to refresh the list.

Table 97. Status

Item (* indicates required value)	Description
Session Count	Current number of Sessions
Logout Count	Number of Sessions logged out due to Logout request
Session Max Count	Maximum number of Sessions stored
Session Timeout	Session timeout time (ms)
Request Getnew Logout	Number of Logout responses for GET_FRESH Request received from WAS
Data From Nodes	Number of Sessions received from WAS
Request Getnew Nodata	Number of NODATA responses for GET_FRESH Request received from WAS
Request Getnew	Number of times increased when GET_SESSION Request was made from WAS
Pid	Process ID when Session is standalone
Request Getfresh Data	Number of times increased when GET_FRESH Request was received from WAS and the corresponding Session existed
Request Getfresh Logout	Number of times increased when GET_FRESH Request was received from WAS and the corresponding Session was Logout
Session Recv Lost	Number of Session receive losses
Logout From Nodes	Number of Logouts received from other WASs
Session Expired	Number of Sessions expired due to Session Time Out
Request Getfresh Nodata	Number of times increased when GET_FRESH_SESSION request was made from WAS and no data was found
Data From Secondary	Number of Data received from Slave server
Request Getfresh	Number of GET_FRESH Request requests from WAS

Item (* indicates required value)	Description
Logout From Secondary	Number of Logout requests received from Slave Server
Req Lost	Number of Request losses
Request Getfresh Secondary	Number of GET_FRESH Request requests from Slave Server
Resp Lost	Number of Response losses due to size of Response Queue exceeding
Request Getfresh Not New	Number of NOT_NEW responses for GET_FRESH Request received from WAS
Request Getnew Secondary	Number of times increased when GET_SESSION request was made from Slave Server

Logging

You can edit the Session Server log settings.

The detailed contents of the settings are as follows.

1. Log Home

Table 98. Log Home

Item (* indicates required value)	Description	Notes
Log Home(*)	Log Home path	When default is selected, it is set to the logs folder under the server installation directory, and when manually selected, you can enter the log directory home path in the Log Home Prefix field
Retention Days(*)	Maximum retention days for logs	Default: 0 (unlimited)

Environment

Provides a screen for managing Start Shell settings. Modify using a file editor and click the **Save button** to save.

- Base Env ($CATALINA_HOME/env.sh) - Shell Script for starting Server

By default, settings are disabled for modification, but if you want to modify them, click **Settings button** in ADMIN > Manager Environment > Manager Configuration to change the following settings to false.

```
server.environment.envshell.readonly=false
```

4.5.8. Server Log Viewer

You can search for log file contents under the Log Home path of the target Server via the Log Viewer button on the right side of the Server list.

To use this functionality, you must meet the following requirements.

- The Node to which the target Server belongs must be running.

Clicking the Log Viewer button on the Server list will allow you to check the directory and files based on the Log Home path of the target Server in a tree structure.

Selecting a file will allow you to view the file content, and when you first select it, you can check the file content up to a predetermined size from the end.

You can view and check the content of log files in a predetermined size using Load More and Load Previous buttons.

- When there is no more content to search (e.g., at the beginning of the file), a message "No more data to read" will be displayed in Alert.
- If you use Load More and there is no more content to search (e.g., at the end of the file), a message "No more data to read" will be displayed at the bottom of the screen.

Chapter 5. Cluster

5.1. Server Cluster

Server Cluster is a group of Application Servers and Web Servers that run with the same configuration to provide the same service.

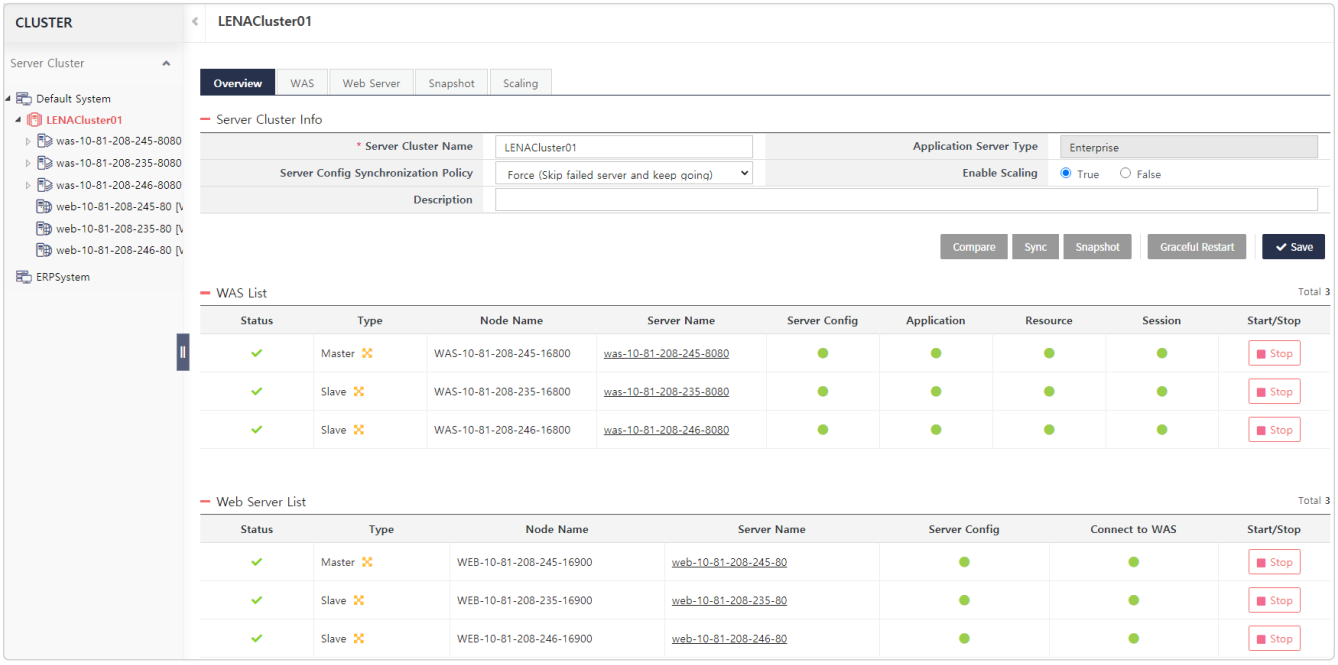


Figure 8. Server Cluster Screen

5.1.1. Server Cluster List

You can check the list of Server Clusters registered in the manager by selecting Server Cluster from the left menu.

The properties provided in the Server Cluster List table are as follows.

Table 99. Server Cluster Properties

Item	Description	Remarks
Select	Combo box for deletion	
Server Cluster Name	Cluster name	
Servers	Number of each Server that constitutes the Server Cluster 1. Application Server 2. Web Servers	

5.1.2. Server Cluster Creation

In Server Cluster creation, you select the Application Server list and Web Server list to configure the

Server Cluster.

1. Select the Server Cluster Group and click the **+New button** at the bottom of the Server Cluster list to display the new registration screen.
2. Enter the basic information of the Server Cluster.
   - Server Cluster Name: Enter the Server Cluster name.
   - Application Server Type: Select the Application Type to be used as a member of the Server Cluster. There are two types: Standard and Enterprise.
   - Enable Scaling: Select whether to use Auto Scaling functionality. This option cannot be changed after server cluster creation. (This functionality is only supported in Container Edition, and to use it, set scaling.enable to true in manager.conf.)
   - Description: Enter necessary descriptions related to the Server Cluster.
3. The server list corresponding to the selected Application Server Type is displayed in the Application server in server cluster area below. Click the desired server in Selectable Servers and press the **>> button** to move it to the Selected Servers area. Similarly in the Web Servers in server cluster area, click the desired server in Selectable Servers and press the **>> button** to move it to the Selected Servers area.

One Server can only be assigned to one Server Cluster, so only Application Servers and Web Servers that are not mapped to other Server Clusters are displayed in the Selectable Servers list.

4. Click the **V Save button** to save.
5. You can confirm that the menu with the entered server cluster name has been added to the left tree.

5.1.3. Server Cluster Deletion

1. Select the Server Cluster Group from the left Server Cluster tree menu.
2. Check the checkbox in the Select column of the Server Cluster to be deleted in the Server Cluster List.
3. Click the **- Delete button** to delete.

5.1.4. Server Cluster Details

Overview

When you select a Server Cluster from the left menu or Server Cluster Group details, the Overview screen for the Server Cluster is displayed.

The items and buttons in the Server Cluster details area provide the following functions.

Table 100. Server Cluster Details Area Items and Buttons

Item or Button Name	Function
Server Cluster Name	Server Cluster name
Application Server Type	Application Server type configured in the Server Cluster (cannot be changed)

Item or Button Name	Function
Server Configuration Synchronization Policy	Policy for handling errors during Server Cluster synchronization (**Sync button** selection) Server Configuration Synchronization Policy options are as follows. (Default: Stop) 1. Stop : Stop immediately when an error occurs during configuration synchronization 2. Rollback : Perform full rollback when an error occurs during configuration synchronization 3. Force : Skip the corresponding Server and proceed to the next when an error occurs during configuration synchronization
Enable Scaling	Whether to use Auto Scaling functionality for Server Cluster (cannot be changed)
Description	Description of the Server Cluster
Compare button	Compares the synchronization status of Application Servers, Web Servers, and Session Servers within the Server Cluster. The comparison items by Server type are as follows, and these are displayed in the respective columns of each Server list area below. Server Configuration, Application, Resource, and Session comparisons are based on the Master Server of each Server type. **Application Server** • Server Configuration : Whether Application Server configuration information is identical • Application : Whether Applications deployed on each Application Server are identical • Resource : Whether Resource configuration is identical • Session : Whether Session Server configuration for Session Clustering is identical **Web Server** • Server Configuration : Whether Web Server configuration information is identical • Connect to WAS : Whether it is connected to all Application Servers within the Server Cluster
Sync button	Synchronizes Server Configuration, Application, Resource, and Session information of Application Servers within the Server Cluster. Synchronizes Server Configuration and WAS connection information of Web Servers within the Server Cluster.

Item or Button Name	Function
Snapshot button	Saves the current status as a Snapshot for the synchronized Server Cluster. Generated Snapshots can be checked in the Snapshot tab. Snapshots include Application Source. Therefore, creating Snapshots excessively can occupy a lot of system disk space, so create them only when necessary and delete unnecessary Snapshots through the Snapshot tab.
WAS Scaling Template button	Creates a Scaling Template that can be used in Sync mode Scaling by copying files from the WAS Master Server. Target files are the same as those set in the Configuration function of the WAS tab, and this button is only visible when Scaling is active and Scaling Mode is sync.
Web Scaling Template button	Creates a Scaling Template that can be used in Sync mode Scaling by copying files from the Web Master Server. Target files are the same as those set in the Configuration function of the Web Server tab, and this button is only visible when Scaling is active and Scaling Mode is sync.
Graceful Restart button	Sequentially restarts Web Servers and Application Servers within the Server Cluster. Since Graceful Stop is performed, the Server stops after all services being processed are terminated. The processing order is as follows. Procedures expressed in () are optional. 1. Web Server Stop 2. Application Stop 3. (Application Source upload) 4. Application Server Start 5. (Start Web Server in staging port for testing with separate port) 6. Web Server Start
V Save button	Saves the changed Server Cluster details configuration.

Synchronization Status Check

You can check the synchronization status of the Server Cluster by selecting the **Compare button** and then checking the results through the columns below each Server list.

When the status is identical or valid, it is displayed as **green circle icon**.

When the Server status is not identical, it appears as **red circle icon**, and clicking the corresponding icon displays a separate popup window where you can check detailed information by Server.

Also, clicking on the Server Name in each Server list allows you to navigate to the corresponding Server details screen.

- Application Server Server Configuration Details

  The comparison results of configuration files are displayed. In the popup window, clicking the

magnifying glass button next to the Detail item allows you to see the comparison results (last modification date, configuration file content) of the current configuration file compared to the Master server in detail.

- Application Server Application Details

  The comparison results of Application deployment status are displayed.

- Application Server Resource Details

  The comparison results of Application Server Resources are displayed.

- Application Server Session Details

  The comparison results of Application Server Session configuration are displayed. The popup window provides session information configured on the Master Server.

- Web Server Server Configuration

  The comparison results of configuration files are displayed. In the popup window, clicking the **magnifying glass button** next to the Detail item allows you to see the comparison results (last modification date, configuration file content) of the current configuration file compared to the Master server in detail.

- Web Server Connect to WAS

  When the corresponding Web Server is only connected to all Application Servers belonging to the Server Cluster, it is displayed as **green circle icon** status, otherwise it is displayed as **red circle icon**. Clicking on **red circle icon** displays a separate popup window where you can check detailed information.

  The popup window displays detailed information about whether all Application Servers connected to the Web Server are registered Servers in the Server Cluster (Web Server Status). Also, it displays detailed information about whether all Application Servers registered in the Server Cluster are connected to the corresponding Web Server (Application Server Status).

Status Synchronization Execution

Server Cluster synchronization execution proceeds by selecting the **Sync button**. The results can be checked through the columns below each Server list.

Graceful Restart

Graceful Restart functionality is used when performing restart of all servers within the Server Cluster while ensuring the completion of ongoing tasks. When executed, it proceeds through the following procedures. (Applied to all servers within the Server Cluster)

1. Before Graceful Restart starts

   Clicking the Start Process button starts the Graceful Restart operation.

2. Web Server Stop phase

   Performs Stop for Web Server. Web Server stops after all executing threads are terminated.

3. Application Server Stop phase

   Performs Stop for Application Server. This phase is activated after all Web Servers are terminated.

4. Source deployment (optional) phase

   Performs source deployment for Application Server. This phase can be omitted if there is a separate deployment system.

5. Application Server Start phase

   Performs Start for Application Server. You can also check the start logs.

6. Start Web Server in Staging mode (optional) phase

   Starts Web Server in Staging mode. (This phase is optional.) Through this, you can perform business testing with staging port in the same environment as production before opening to general users.

7. Web Server Start phase

   Starts Web Server in Staging mode. (This phase is optional.) Through this, you can perform business testing with staging port in the same environment as production before opening to general users.

8. Graceful Restart completion

Application Server

This is a tab that manages the list and synchronization target information of Application Servers within the Server Cluster.

The detailed information of the server list at the top of the tab is the same as Overview.

Synchronization Target Items

Server Configuration File Management

Selecting the **Configuration button** provides a popup window where you can set the Master Server selection for Application Server, specify configuration files to synchronize, and set whether to synchronize JDBC Drivers.

- Master Server

  Specifies the Master Server among Application Servers within the Server Cluster.

- Server Configs for Synchronization

  This is the list of files to be maintained with identical content in Application Servers within the Server Cluster. Basic file lists are registered when creating the Server Cluster, and you can add/delete files according to project circumstances. The file path is a relative path under the Application Server's Home.

- Sync JDBC Drivers

  Selects whether to include all jar files under the Manager Repository path/lib/datasource/ folder in the synchronization target.

JDBC Drivers are only synchronized when the corresponding JDBC Driver does not exist on the target server to prevent errors due to Jar file replacement during Runtime.

Application Management

When selecting a server from the Application Server list, you can check the Application detailed information of the selected server through the Application tab below. The provided screen and functionality are identical to those described in Application. Therefore, detailed explanations of functionality are omitted in this chapter.

Resource Management

When selecting a server from the Application Server list, you can check the detailed information of DataSource, JMS, and JTA of the selected server through the DataSource, JMS, and JTA tabs below. The provided screen and functionality are identical to those described in Datasource, JMS, JTA. Therefore, detailed explanations of functionality are omitted in this chapter.

Session Management

When selecting a server from the Application Server list, you can check the Session detailed information of the selected server through the Session tab below. The provided screen and functionality are identical to those described in Session. Therefore, detailed explanations of functionality are omitted in this chapter.

WAS List Management

You can include or exclude Application Servers in the Server Cluster using the **Clone button**, **Join button**, or **Unjoin button**.

- Clone

  Clicking the **Clone button** allows you to install a new server with the same configuration as the Master server and register it in the Server Cluster.

Table 101. Clone Popup Window Item Description

Item Name	Function
Post Processing Options	• Cloned Server Start: Check whether to start server after cloning • All Web Server Sync: Synchronize with Web Server after cloning • All Web Server Graceful Restart : Whether to restart Web Server after cloning
Node List	Node to install the server to be cloned
Server ID / Clone Service Port	Enter the ID and Service Port of the Server to be cloned
Include External Source	Select Y if you want to clone the source as well when the application source of the server to be cloned is outside the server

- Join

Clicking the **Join button** adds an available Server among already created Application Servers to the Server Cluster.

- Unjoin

  Clicking the **Unjoin button** deletes the Server registered in the Cluster from the Cluster list.

Application Server Synchronization and Comparison

- Compare

  Clicking the **Compare button** compares the synchronization status of Application Servers within the Server Cluster.

- Sync

  Clicking the **Sync button** synchronizes Server Configuration, Application, Resource, and Session configurations of Application Servers within the Server Cluster.

Scaling Template

Clicking the **Scaling Template button** creates a Scaling Template that can be used in Sync mode Scaling by copying files from the WAS Master Server. The copied target files are the same as those set in the Sync target files in Configuration, and this button is only visible when Scaling is active and Scaling Mode is sync.

Rolling Restart

Rolling Restart is used when sequentially restarting Application Servers within the Server Cluster.

This is a function performed on servers to be restarted, so stopped servers are excluded. After selecting target servers from the server list, clicking the **Rolling Restart button** provides the Rolling Restart popup window.

In the popup window, users can set the start interval between servers and whether to Force Stop in the Execution option area before starting Rolling Restart. In the Rolling Restart area, you can check the status of selected servers performing sequential restart.

Table 102. Rolling Restart Popup Window Item Description

Node	Node name where the server is installed
Server	Server name
Server Status	Current start status of the server
Stop Status	Server stop operation status
Start Status	Server start operation status
Action	**Force Restart button** and **Next button** are provided for servers being restarted.
Interval	Remaining processing time for the server. After starting from the value set in the Interval of the Execution Option area and counting down to 0, the next server's restart is performed.
Elapsed time	Restart processing time

Table 103. Rolling Restart Popup Window Button Description

Button Name	Function
Start	Starts the restart of target servers shown in the popup window. It proceeds sequentially from the top of the table.
Pause	Temporarily pauses the restart operation. If stop/start is being performed, the executing command is not interrupted, but the next operation waits.
Resume	Resumes the restart operation. It starts from after the work completed before Pause.
Force Restart	When stop is not working normally, you can force stop and then start through this button. It is only shown on screen until the server being restarted completes stopping.
Next	When you want to proceed with the next server's restart operation immediately before the current server's restart operation is completed, you can perform the next server's restart through the Next button. Even if Next is performed, the restart operations of previous servers continue.

Web Server

This is a tab that manages the list and synchronization target information of Web Servers within the Server Cluster.

The detailed information of the server list at the top of the tab is the same as Overview.

Synchronization Target Items

Server Configuration File Management

Selecting the **Configuration button** provides a popup window where you can set the Master Server selection for Web Server and specify the list of configuration files to synchronize.

- Master Server :

  Specifies the Master Server among Web Servers within the Server Cluster.

- Server Configs for Synchronization :

  This is the list of files to be maintained with identical content in Web Servers within the Server Cluster. Basic file lists are registered when creating the Server Cluster, and you can add/delete files according to project circumstances. The file path is a relative path under the Web Server's Home.

Connector

You can check and modify detailed connector information of the Web Server.

When selecting a server from the Web Server list, you can check the Connector detailed information of the selected server through the Connector tab below. The provided screen and functionality are identical to those described in Connector. Therefore, detailed explanations of functionality are omitted

in this chapter.

Web Server List Management

You can include or exclude Web Servers in the Server Cluster using the **Clone button**, **Join button**, or **Unjoin button**.

- Clone

  Clicking the **Clone button** allows you to install a new server with the same configuration as the Master server and register it in the Server Cluster.

Table 104. Clone Popup Window Item Description

Item Name	Function
Post Processing Options	• Cloned Server Start: Check whether to start server after cloning
Node List	Node to install the server to be cloned
Server ID / Clone Service Port	Enter the ID and Service Port of the Server to be cloned
Include External Source	Select Y if you want to clone the source as well when the source of the server to be cloned is outside the server

- Join

  Clicking the **Join button** adds an available Server among already created Web Servers to the Server Cluster.

- Unjoin

  Clicking the **Unjoin button** deletes the Server registered in the Cluster from the Cluster list.

Web Server Synchronization and Comparison

- Compare

  Clicking the **Compare button** compares the synchronization status of Web Servers within the Server Cluster.

- Sync

  Clicking the **Sync button** synchronizes Server Configuration and Connect WAS of Web Servers within the Server Cluster.

When clicking the Web Server's Sync button, Web Server configuration synchronization and all Web Servers and WAS included in the Server Cluster are interconnected in a Full Mesh structure.
If you want to synchronize only configurations without changing to Full Mesh structure, it is recommended to configure Web Server and WAS each as separate Server Clusters.

Scaling Template

Clicking the **Scaling Template button** creates a Scaling Template that can be used in Sync mode Scaling by copying files from the Web Master Server. The copied target files are the same as those set in the Sync target files in Configuration, and this button is only visible when Scaling is active and Scaling Mode is sync.

Rolling Restart

Rolling Restart is used when sequentially restarting Web Servers within the Server Cluster.

This is a function performed on servers to be restarted, so stopped servers are excluded. After selecting target servers from the server list, clicking the **Rolling Restart button** provides the Rolling Restart popup window.

In the popup window, users can set the start interval between servers and whether to Force Stop in the Execution option area before starting Rolling Restart. In the Rolling Restart area, you can check the status of selected servers performing sequential restart.

Table 105. Rolling Restart Popup Window Item Description

Node	Node name where the server is installed
Server	Server name
Server Status	Current start status of the server
Stop Status	Server stop operation status
Start Status	Server start operation status
Action	**Force Restart button** and **Skip button** are provided for servers being restarted.
Interval	Remaining processing time for the server. After starting from the value set in the Interval of the Execution Option area and counting down to 0, the next server's restart is performed.
Elapsed time	Restart processing time

Snapshot

Clicking the Snapshot button in the Overview Tab displays a window for Snapshot creation, and clicking the OK button creates a Snapshot of the Server Cluster.

Snapshots can only be created when the Server Cluster is in a synchronized state.

The Snapshot tab provides a screen for managing the Snapshot list. It receives a date input to search Snapshot history. You can check detailed information about Snapshot history, and it also provides functionality to restore to a desired point in time.

Clicking the **list button** in the Detail item of the Snapshot list allows you to check detailed information about the corresponding snapshot.

Snapshot information is managed by each server, so servers added to the Cluster after creating a specific Snapshot are excluded from restoration to that Snapshot. (In this case, after Snapshot restoration, you need to perform Sync again for all servers to have the same configuration.) Also, if a specific server is deleted from the Cluster after Snapshot creation, all Snapshot information for that server is deleted. When creating Snapshots, source code is not copied to the Snapshot, and only basic

configuration files, application configuration files, and enterprise.xml are included in the Snapshot.

When creating Snapshots, be careful as they can put a load on disk capacity. Also, generated Snapshots are not automatically deleted and must be manually deleted by users. Therefore, it is recommended to delete unnecessary Snapshots at appropriate times.

5.1.5. Scaling

When Enable Scaling option is set to True during Server Cluster creation, it supports service scaling according to Auto-Scaling (Infra Scaling) provided by CSP or Cloud platforms. This functionality is only supported in environments where the VM OS is Linux and Init-Script (e.g., UserData for AWS EC2) is provided during VM Instance creation.

In Cloud environments, Scaling is generally performed through the following procedures:

1. VM Image creation (including LENA Node, LENA Server, and Application)
2. VM Init-Script writing
3. LENA Manager Scaling Policy configuration
4. When pre-configured Scaling Trigger conditions (Resource threshold conditions) occur, VM Auto-Scaling Out is performed (CSP, Cloud platform area)
5. During VM Scale-Out, LENA Node Agent and Server registration, configuration synchronization, and License issuance are performed according to Cloud Init-Script (LENA area)
6. When Resource thresholds normalize, VM Scale-in is performed (CSP, Cloud platform area)
7. After VM Scale-in, if Node Agent Alive check failures occur as many times as configured in LENA Manager, the corresponding Node and Server are removed from LENA Manager (LENA area)

The following explains the Scaling Policy configuration, VM Init-Script related parts, and LENA Node Agent/Server registration related content among the above procedures related to LENA's Scaling support area.

Scaling functionality is executed by setting necessary environment variables in Init-Script that runs during Infra Scaling and calling the LENA Scaling execution command scale.sh, which triggers Scale-Out. Scale-In is executed when Node Agent communication failure is recognized according to Rules configured in Manager, or when stop-agent.sh is explicitly called with option settings during VM destruction.

- Scale Out

Scale Out is performed by setting environment variables and calling scale.sh. For AWS, this script is written in UserData in the launch template of the AutoScaling group and executed. Scaling License must be pre-deployed in Manager for the server to start normally by downloading the Scaling License.

- Init-Script Init-Script contains procedures for setting necessary environment variables and calling scale.sh. The environment variables referenced by scale.sh for Scale Out are as follows.

Table 106. scale.sh referenced environment variables

Environment Variable	Description
LENA_MANAGER_ADDRESS	• Required option, LENA Manager service address for performing Scaling processing on Node and Server, format is {IP address}:{HttpPort} • This environment variable can be used to configure Fail-Over for redundant Managers. When Manager addresses are separated by commas (","), if connection to the first Manager fails, it attempts to connect to the second Manager. This process is repeated until connection to Manager succeeds within the specified time (default 10 minutes).
JAVA_HOME	• Installation location of Java to be used by Node Agent and Server
LENA_CLUSTER_NAME	• Server Cluster name, target Server Cluster name where the scaled Server will be registered. Only existing Server Cluster names can be entered for normal Scaling execution.
LENA_USER, LENA_GROUP	• OS user and group to start Node Agent and Server
LENA_WAS_SCALING	• Whether to perform WAS server Scaling
LENA_WAS_HOME	• WAS server installation location
LENA_WAS_AGENT_PORT	• WAS server Node Agent service port
LENA_WEB_SCALING	• Whether to execute Web server Scaling
LENA_WEB_HOME	• Web server installation location
LENA_WEB_AGENT_PORT	• Web server Node Agent service port
LENA_WEB_OPENSSL_VER	• OpenSSL version installed on OS, required for Web server startup • Supported versions are 1.0.1, 1.0.2, 1.1.1, default value is 1.0.2
LENA_IMAGE_TYPE	• VM Image type, there are 'base' with only LENA package installed and 'golden' with Server installed. 'base' corresponds to 'clone' in Scaling Mode, and 'golden' corresponds to 'sync'/'nosync' in Scaling Mode.
WAS_CONFIG_DATA	• Individual WAS configuration information defined in Json format. Session Cluster information and Datasource information can be configured, which changes the actual configuration information of the configured Server.

Environment variable application and scale.sh call example (Init-Script)

```
export LENA_MANAGER_ADDRESS=10.200.30.213:7700,10.200.30.214:7700
export LENA_CLUSTER_NAME=cust-g3r
export LENA_USER=lena
export LENA_GROUP=lena

export LENA_WAS_SCALING=Y
export LENA_WAS_HOME=/engn001/lena/1.5.0
export LENA_WAS_AGENT_PORT=16800

export LENA_WEB_SCALING=Y
export LENA_WEB_HOME=/engn001/lenaw/1.5.0
export LENA_WEB_AGENT_PORT=16900
export LENA_WEB_OPENSSL_VER=1.0.2

export LENA_IMAGE_TYPE=base

export WAS_CONFIG_DATA='[
     {
         "server_id": "comm_core_was-8980",
         "session_cluster": {
             "primary_port": "5480",
             "secondary_port": "5480"
         },
         "datasource": [
             {
                 "jndi_name": "jdbc/petclinic",
                 "url": "jdbc:mysql://10.200.30.7:63306/petclinic"
             }
         ]
     }
 ]'

if [ "$LENA_WAS_SCALING" = "Y" ]; then $LENA_WAS_HOME/bin/scale.sh; fi
if [ "$LENA_WEB_SCALING" = "Y" ]; then $LENA_WEB_HOME/bin/scale.sh; fi
```

- Scale-in

Scale-in is the process of deregistering Node and Server registered through Scale-Out process, which can be executed by 1) automatically deregistering Node and Server installed on that Node when Node Agent response failure occurs as many times as configured in Manager's Scheduler, or 2) explicitly executing by directly calling stop-agent.sh with options added. The option information for stop-agent.sh is as follows.

Table 107. stop-agent.sh option information

Option	Description
-ur${Manager Address(IP:Port)}	• Required option, deregisters (*Ur*egister) Node or Server • Input parameter is Manager address, format is ${IP address}:${HttpPort} • This option supports Fail-Over processing for Manager. When Manager addresses are separated by commas (","), if connection to the first Manager fails, it attempts to connect to the second Manager.
-f	• Force deregistration, optional • When -f option is set, it is deregistered from Server Cluster
-rt ${time - milliseconds}	• "Retry Time", Optional • Retries for that time. Retry cycle is 3 seconds, default Retry Time is 10 seconds

Option usage example

```
# Remove all Node / Server information from Manager
# Manager License usage calculation stops for that server
stop-agent.sh -ur 10.80.44.55:78700 -f
```

Scaling Overview

When selecting the Scaling tab, the table at the top of the provided screen shows current Scaling status by Node type.

- Initial Node : Number of nodes currently included in the Server Cluster
- Scaled Node : Number of nodes created according to Scaling policy
- Today Event : Number of Scaling events that occurred today
- Latest Event : Time when the most recent Scaling event occurred

Policy

Policy information such as Naming Rules applied during Scaling can be defined.

Common Policy

- System : System name where Scaling is applied
- Sync Button Enabled : Whether to enable Sync button of Server Cluster functionality
- Scaling Mode : Server Scaling type
  - nosync : Register Node and Server and add to Cluster
  - sync : Register Node and Server and add to Cluster, then perform Cluster Configuration-based Sync, Sync is performed only for newly scaled Servers
  - clone : Register Node and add to Cluster, then install Server by cloning Master Server and add to Cluster, and perform Web/WAS Sync
- Web-WAS Connection Scope : Web-WAS connection method

- none (Using Proxy) : Do not perform separate Web-WAS connection
- JK Mesh - Cluster Servers : Perform connection between servers in Cluster, for Web, connect newly registered Web servers with servers in Cluster, for WAS, connect newly registered WAS servers with Web servers in Cluster, in nosync Mode, do not synchronize LoadBalancer set in Web servers and connect each LoadBalancer with WAS in Cluster to support Blue-Green deployment method
- JK Mesh - Servers on same machine : Perform connection only for Web-WAS on the same VM

WAS Node

- Node Naming Rule : WAS node naming rule
- Server Naming Rule : WAS naming rule
- Wait For WAS Start Up : Whether to wait for WAS startup when scaled out. If 'Y', proceed to next procedure (e.g., WEB server restart) after startup
- Wait Time for WAS Start Up : Maximum WAS startup wait time. Even if Wait For WAS Start Up is 'Y', proceed to next procedure when that time passes

WEB Node

- Node Naming Rule : WEB node naming rule
- Server Naming Rule : Web server naming rule

The Conventions (reserved words) used in naming rules are as follows.

- #{IP} : Node or Server IP address with each unit separated by '-'
- #{IP[4]} : 4th number in Node or Server IP address
- #{PORT} : HTTP service address of Node Agent or Server
- #{MASTER_NAME} : Master Server name
- #{HOSTNAME} : Host name of VM where Node or Server is installed
- #{HOSTNAME[R4]} : Rightmost 4 characters of VM Host name

After saving the information for the corresponding items, click the **Save button** to save.

WAS Scaling Template / Web Scaling Template

You can view the list and content of files synchronized during Sync mode Scaling. The displayed File list is manually copied from the Master Server of the corresponding Server Cluster. Clicking the **Create button** on the screen manually generates files. Click the **magnifying glass button** to view detailed file content and check comparison results with current Master Server configuration files.

History

You can search Scaling event history based on date and time. Select the date when Scaling occurred and enter the time, then click the **Search button** to search for Scaling Events that occurred at that time.

Scaling functionality is only provided in Enterprise Edition.

5.2. Service Cluster

Service Cluster is a logical grouping for managing Containers. It is registered under System and can be created by selecting Standard Application Server, Web Server, or Session Server. You can view information about currently running Containers and history of terminated Containers. Additionally, Standard Application Server and Web Server provide Template management functionality. Through Templates, you can manage configuration information for Standard Application Server and Web Server, and create and manage Revisions. When creating/starting Container Images, you can download Templates and apply the information configured in Service Cluster to Containers.

Service Cluster functionality can only be used when both Manager and Container Server are running Linux OS.

5.2.1. Service Cluster Creation

1. Select a System and click the **New button** below the Service cluster list to display the new registration screen as shown below.

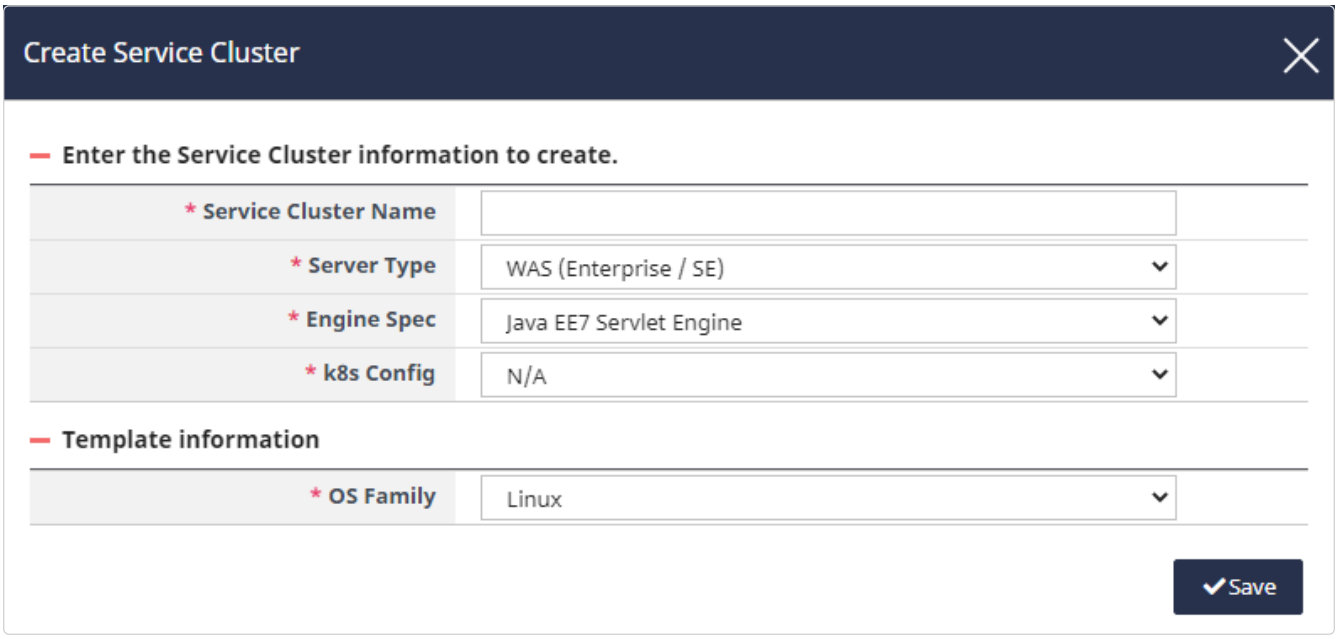


Figure 9. Service Cluster Creation Popup

2. Enter the Service Cluster Name.
3. Select the Server Type. (WEB Server, Application Server, Session Server)
4. Select the k8s Config. You can select k8s Config registered in Resources, or select N/A if no Configuration exists.
5. Select the OS Family. The Server Template type is selected based on your choice, with Linux being the default.

5.2.2. Service Cluster Deletion

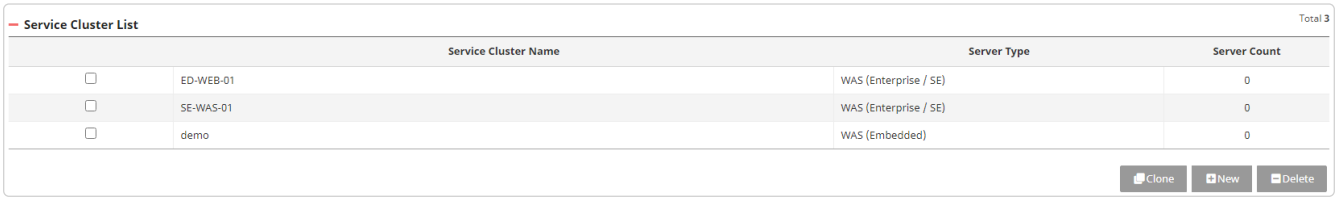


Figure 10. Service Cluster List

1. Check the combo box of the Service Cluster to be deleted from the Service Cluster list.
2. Click the **Delete button** to delete it.

5.2.3. Service Cluster Clone

1. Select a System and click the **Clone button** below the Service cluster list to display the screen as shown below.

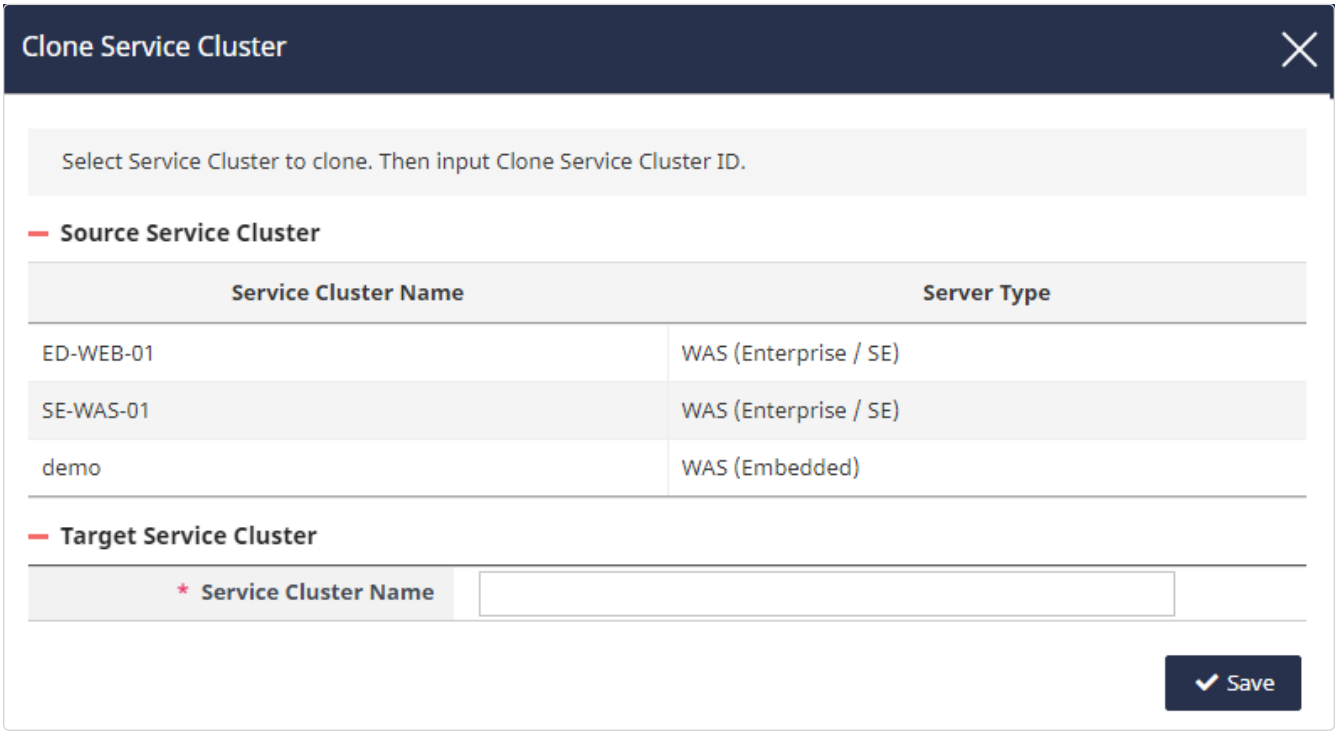


Figure 11. Service Cluster Clone Popup

2. Select the target Service Cluster to clone, enter the name for the newly created Service Cluster, then click the 'Save' button to create a Service Cluster by cloning the Default Revision of the selected Service Cluster.

If the target Service Cluster for cloning has no Default Revision, Configuration files are created using the default Template.

5.2.4. Service Cluster Overview

1. Select a Service Cluster from the left menu or Service Cluster Group details to display the Overview screen for the Service Cluster.

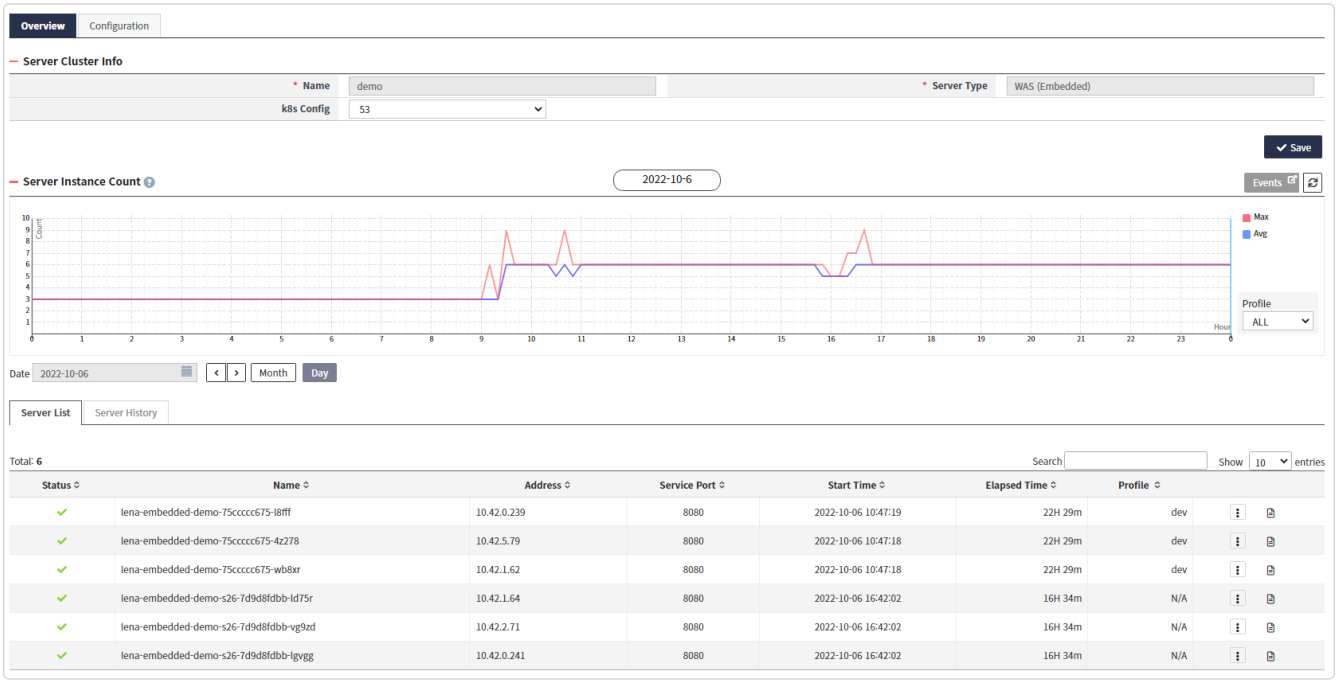


Figure 12. Service Cluster Overview

Service Cluster Info

View and modify basic information of the Service Cluster.

Item	Description
Name	Service Cluster name
Server Type	Type of Server supported by the Service Cluster
Service Endpoint	Service endpoint address. Session servers have 2 endpoints configured as they use redundancy by default.
k8s Config	Kubernetes Config information referenced by the Service Cluster. Used when using Log / Terminal functionality. Kubernetes Config is managed in Resources.

Service Instance Count

Shows the number of running Containers in a graph based on Month/Day. When using Month as the basis, it shows the cumulative number of Servers by date in a graph. When using Day as the basis, it shows the cumulative number of Servers by hour in a graph.

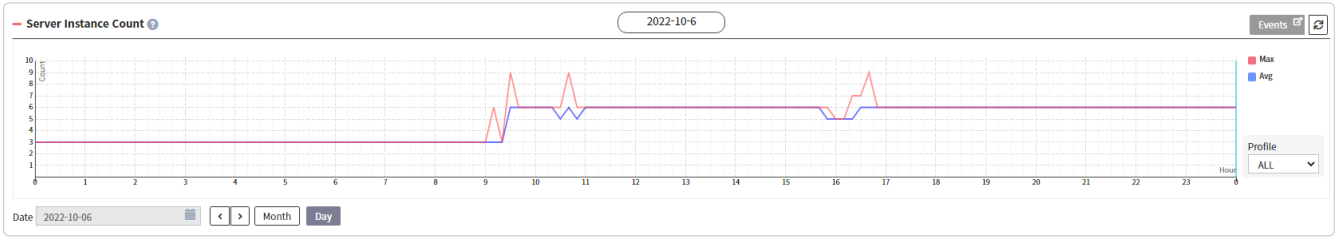


Figure 13. Server Instance Graph

Button Name	Description
Events	Moves to the Event Dashboard screen of the current Server Cluster.

Button Name	Description
Server List	Queries running Containers based on the Server Cluster.
Server History	Queries terminated Containers based on the Server Cluster.

Server List

Shows a list of currently running Servers. Through the ⋮ button, you can view Server logs and connect to Terminal.

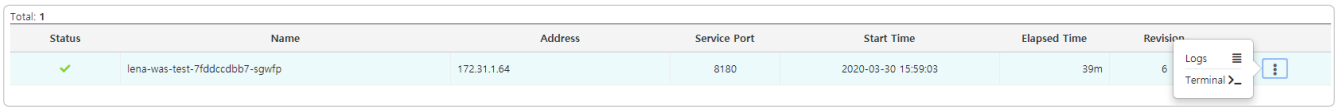


Figure 14. Server List

Log / Terminal functionality can only be used in Service Clusters where k8s Config is configured.

Server History

Shows a list of Server history. Displays start/stop times, address information, and referenced Revision information.

Figure 15. Server History

The Container start time is the Server start time, and the stop time refers to when the monitoring information communication (UDP communication) with the Manager was disconnected.

5.2.5. Application Server Template Management

Modifies the configuration information Template for Application Server and creates Revisions. Once a Revision is created, the Template configuration information can be applied to Containers.

Unlike general VM/HOST-based methods, after Server configuration, the Template must be downloaded during the Container redeployment process for the configuration to be applied.

Server Template Overview

Select a Service Cluster from the left menu or Service Cluster Group details and click the Template tab to display the Service Template Overview screen. Shows OS Family information and current Revision information.

Server Template Configuration Management

Provides functionality to change Web Server configuration information. When you select a Server from the Web Server list, it moves to a screen for managing configuration information.

Summary

Click the Summary tab at the bottom of the Template tab in Service Cluster to display the screen.

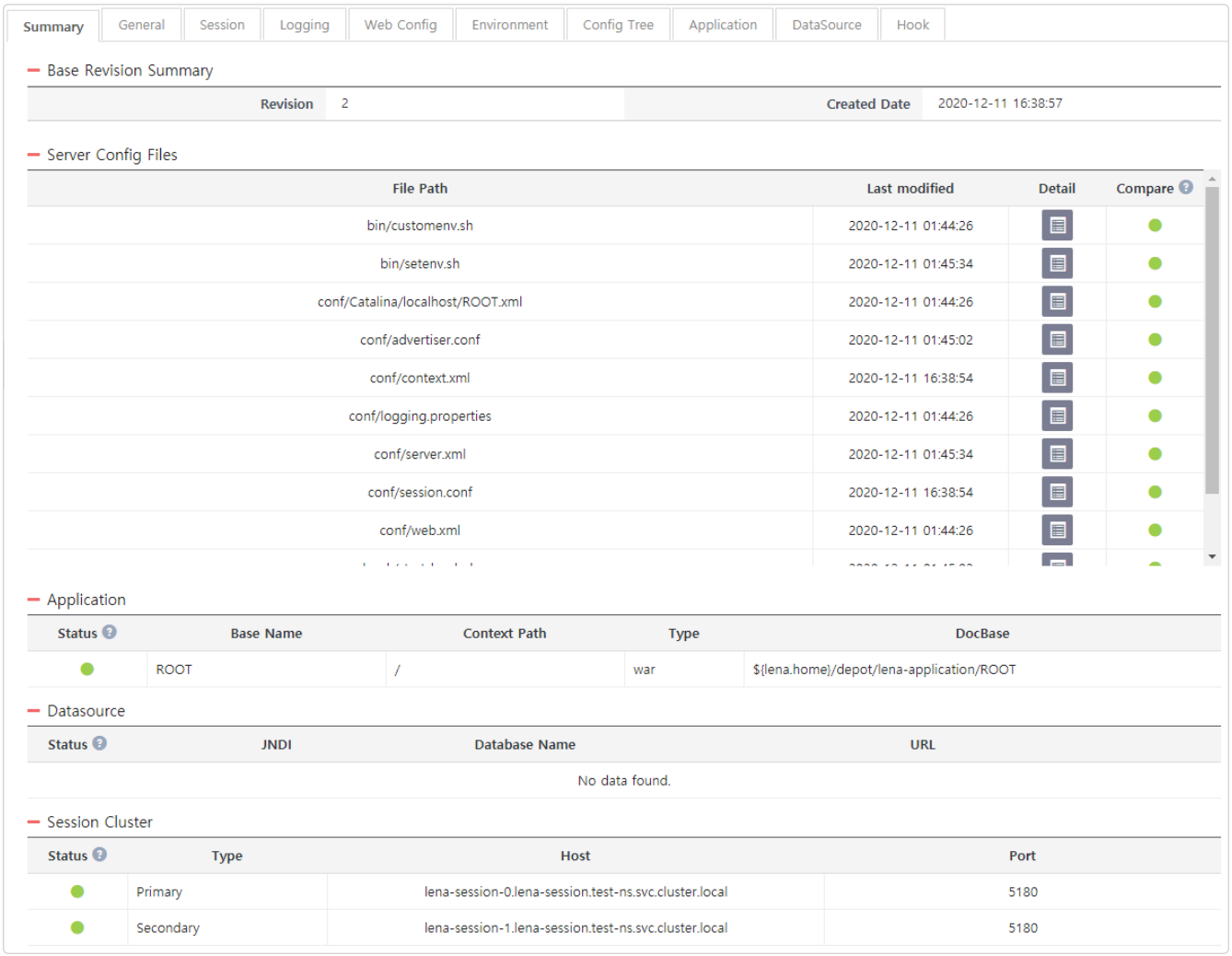


Figure 16. WAS Server Template Summary Tab

1. Base Revision Summary shows the currently loaded Revision number and creation date of the Revision.
2. Server Configuration Files shows a list of Files that make up the currently loaded Revision. Content can be viewed by file, and modified configuration files can be checked and compared through the Compare functionality. If there are no changes, a **green icon** is displayed, and if configuration files are changed, a **red X icon** is displayed. Clicking the **red X icon** shows the differences between the original file and modified file of the loaded Revision in a popup.
3. Application shows Application information configured in the currently loaded Revision. If there are no changes, a **green icon** is displayed, and if Application information is changed, added, or deleted, a **red X icon** is displayed.
4. Database shows Database information configured in the currently loaded Revision. If there are no changes, a **green icon** is displayed, and if Database information is changed, added, or deleted, a **red X icon** is displayed.
5. Session Cluster shows Session Cluster information configured in the currently loaded Revision. If there are no changes, a **green icon** is displayed, and if Session Cluster information is changed, added, or deleted, a **red X icon** is displayed. If the Session Cluster is not running, a **red ! icon** is displayed.

General

Manages general configuration information for the Server. You can modify and save Port information, Connector, Access Log, and Session Cluster related settings.

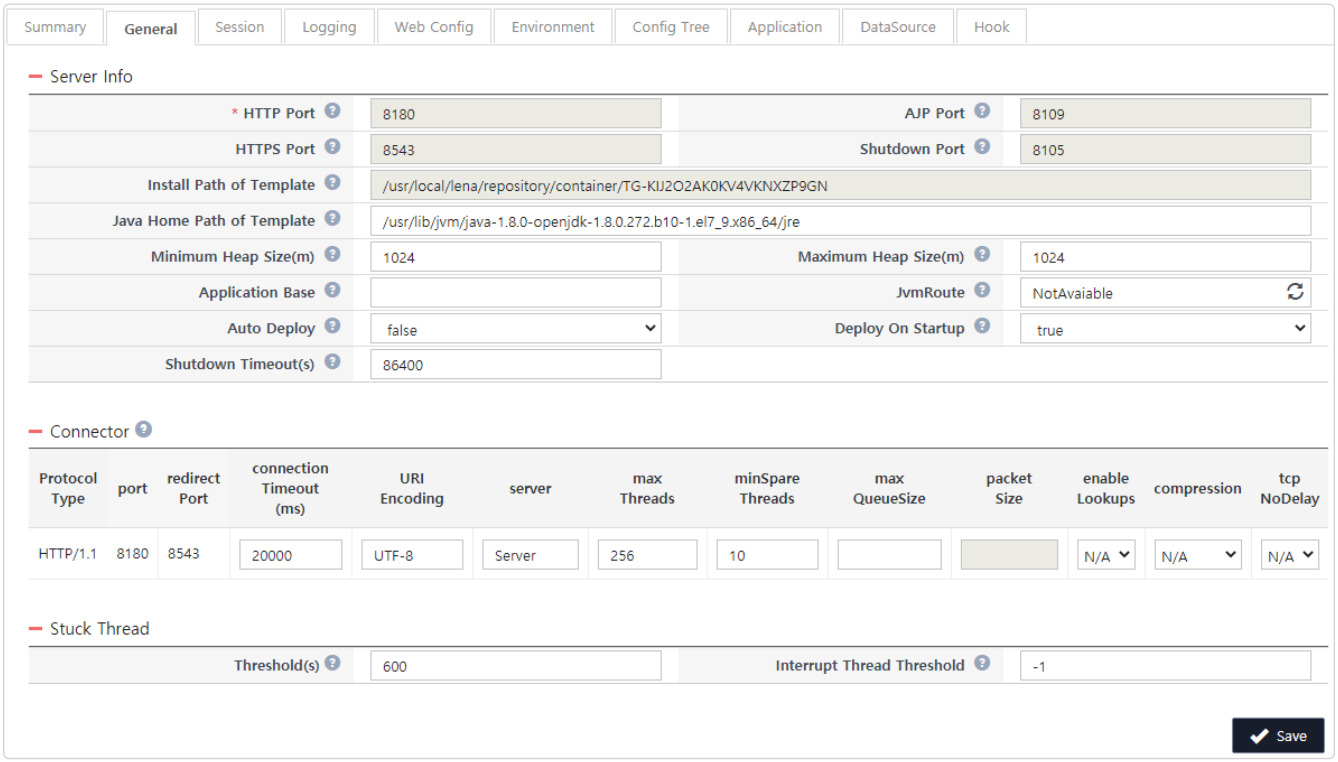


Figure 17. WAS Server Template General Tab

1. Server Info consists of the main attribute values of the Application Server.

Item	Description	Notes
HTTP Port	HTTP port number	Default : 8180
AJP Port	AJP port number	HTTP port number - 71 (auto-calculated)
HTTPS Port	HTTPS port number	HTTP port number + 363 (auto-calculated)
Shutdown Port	Port for receiving shutdown command string	HTTP port number - 75 (auto-calculated)
Application Base	Application's base directory	Can only be modified when the Server is in stop state or when there are no Applications deployed in appBase.
jvmRoute	Server's unique identifier	Prioritizes values set in System Properties. If not available, uses values from server.xml (generated as Hostname + Port combination)
Auto Deploy	Whether to automatically deploy when applications change	Default : false Detected when war files are re-uploaded to Application-specific DocBase

Item	Description	Notes
Deploy On Startup	Whether to deploy Applications when WAS starts	Default : true
Shutdown Timeout	Time to wait (seconds) when running Threads exist during server shutdown	Default : 30

2. Connector represents configuration values for Application Server to communicate with external systems.

Item	Description	Notes
Protocol Type(*)	Protocol type	Default : HTTP/1.1, AJP/1.3
port(*)	Port number	
redirect Port	Redirect port	Same as HTTPS Port
connection Timeout	Connection timeout (ms)	Default : HTTP : 20000, AJP : 60000
URIEncoding	Character encoding for converting URI bytes	Default : UTF-8
server	Redefines Server Header for HTTP Response to prevent server information exposure	Default : Server
maxThreads	Maximum number of Threads that Connector can create	Default : 256
minSpareThreads	Minimum number of Threads to secure when creating Connector	Default : 10
maxQueueSize	Maximum length of Request Queue	Default : Integer.MAX_VALUE
packetSize	AJP packet size	Default : 8192
enableLookups	Whether to use DNS LookUp. Not using it is beneficial for performance	Default : false
compression	HTTP message Body compression (off, on:Text only, force:all)	Default : off
tcpNoDelay	Send TCP packets without delay	Default : true

In Container-based Application Servers, AJP Connector is disabled by default.

3. Stuck Thread is a configuration for identifying tasks that occupy Threads for extended periods.

Item	Description	Notes
Threadshold	Minimum time to identify Stuck Thread	Unit: seconds

Item	Description	Notes
InterruptThreadThreshold	Minimum time to interrupt Stuck Thread	Unit: seconds (To terminate n seconds after Stuck Thread identification, enter "Threshold+n" value)

Session

Provides a screen for managing Session Cluster configuration.

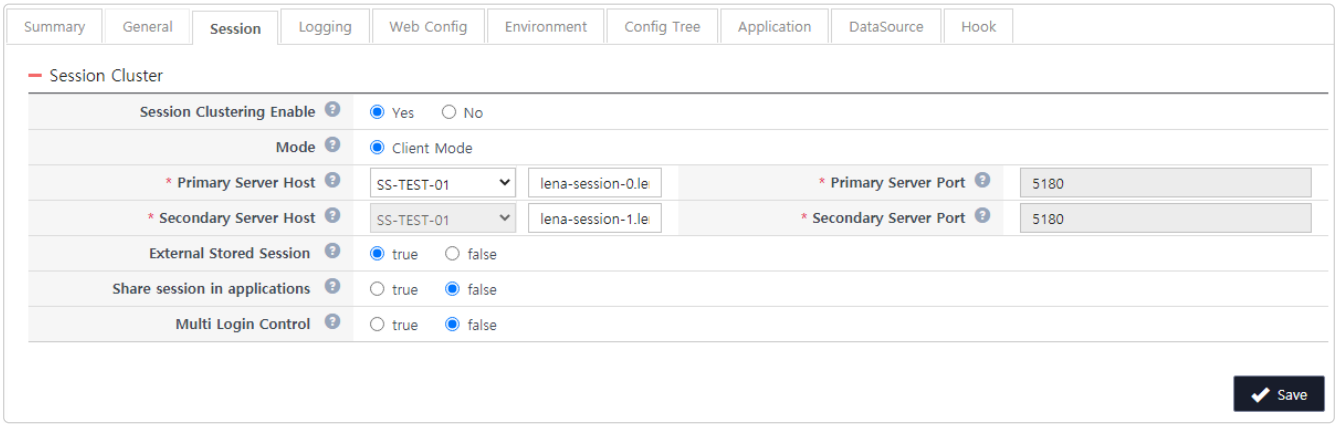


Figure 18. WAS Server Template Session Tab

Item	Description	Default Value
Setting Selection	Whether to use Session Cluster	No
Primary Server Host	Primary Session Server host	
Primary Server Port	Primary Session Server port	
Secondary Server Host	Secondary Session Server host Used only when connection to Primary server is lost	
Secondary Server Port	Secondary Session Server port Used only when connection to Primary server is lost	
External Stored Session	Whether to use External Stored Session When used, Session information is not stored in Application Server.	true
Share session in applications	Share Session objects between Multi Applications Can only be configured in Standalone Mode	false
Multi Login Control	Whether to prevent duplicate login	false

In Container environments, Embedded Mode is not supported due to the environmental characteristics where Server state maintenance is not guaranteed.

Logging

Provides a screen for managing log configuration. You can configure log output types, Handler lists, Handler details, Logger lists, etc. After modifying configuration files, click the **Save button** to update the server's log configuration.

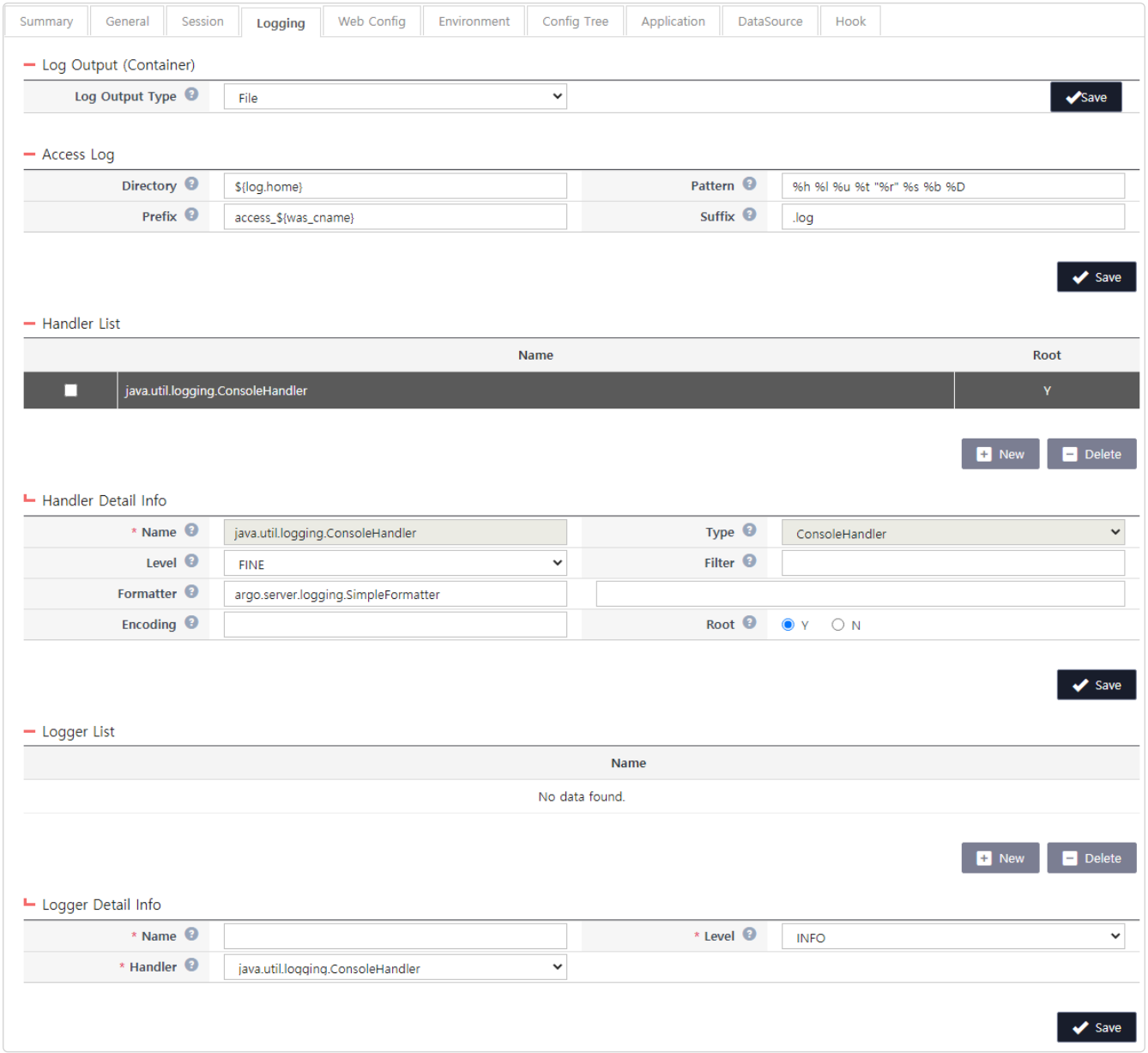


Figure 19. WAS Server Template Logging Tab

1. The details of Log Output (Container) are as follows.

Item	Description	Notes
Log Output Type	Output type of GC log and Engine log	Select from File, Console - File : Single file output and log-rotate execution - Console : Standard out/err output

2. Access Log represents configuration values for Access logs for Requests.

Item	Description	Notes
Output Type	Log output type	File / Console

Item	Description	Notes
Directory	Log directory	Can be specified as absolute path or relative path of
Pattern	Layout of Logging field	
Prefix	Prefix of Log file	
Suffix	Suffix of Log file	

3. Detailed contents of Handler configuration information are as follows.

Item	Description	Notes
Name	Handler class name	
Type	Handler type	ConsoleHandler and FileHandler can be selected.
Level	Handler log level	
Filter	Implementation of java.util.logging.Filter	
Formatter	Implementation of java.util.logging.Formatter	Default value: java.util.logging.SimpleFormatter
Encoding	Handler Character Encoding	
Root	Whether Root Logger	

4. Detailed contents of Logger configuration information are as follows.

Item	Description	Notes
Name	Specify Logger name	
Level	Logger log level	
Handler	Select which Handler Logger will use	ConsoleHandler is selected by default

Server's log configuration file is ()/conf/logging.properties.

Web Configuration

Provides screen for managing Global web.xml configuration. Modify necessary items and click **Save button** to save.

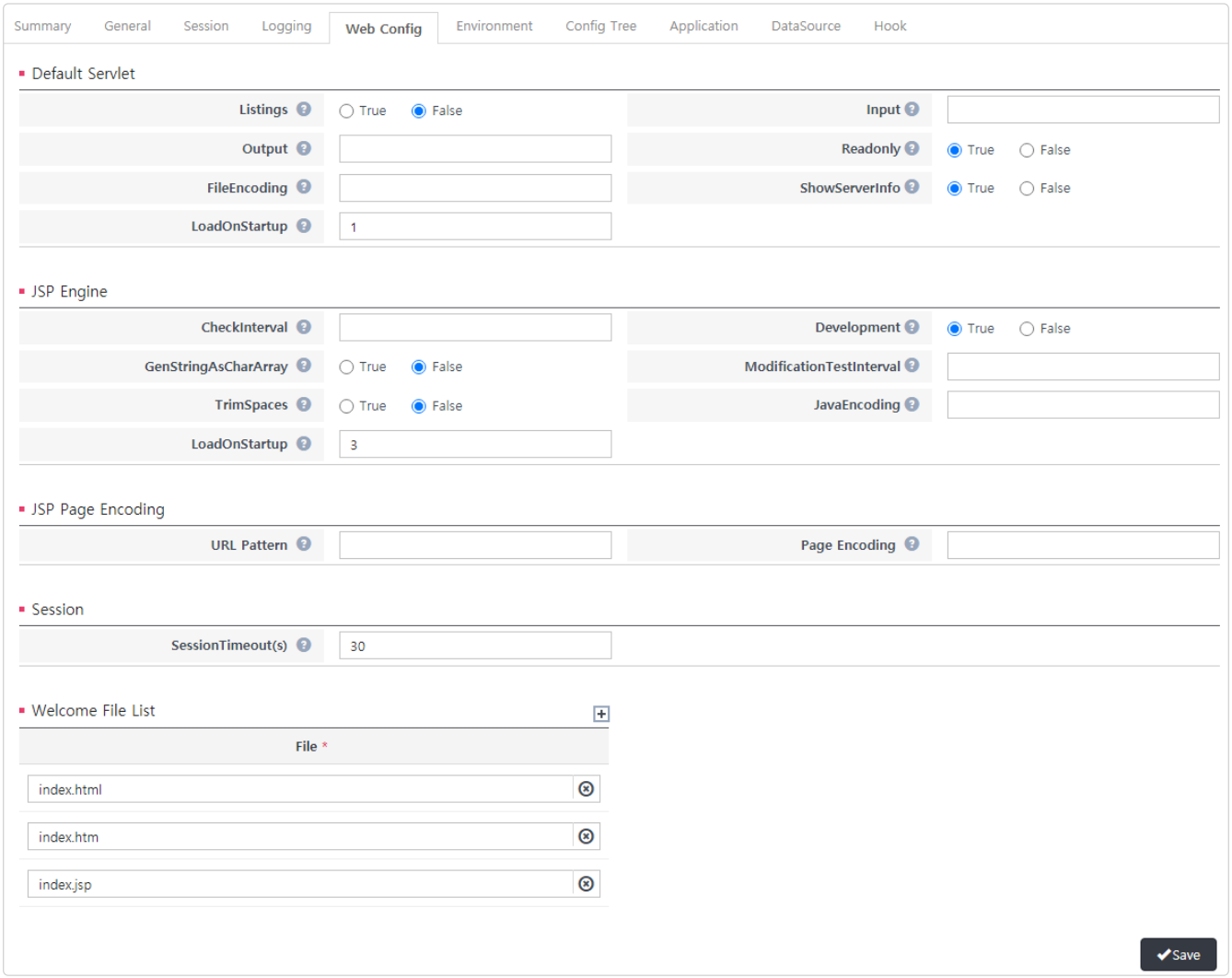


Figure 20. WAS Server Template Web Configuration Tab

1. Default Servlet

Item	Description	Default Value
Listings	Whether to allow Directory Listing when Welcome file is not present	false
Input	Input buffer size (bytes)	2048
Output	Output buffer size (bytes)	2048
Readonly	Do not allow HTTP methods such as PUT, DELETE	true
FileEncoding	File encoding	platform default
ShowServerInfo	Whether to display Server information when Directory Listing is allowed	true
LoadOnStartup	Specify Servlet loading order when WAS starts	1(negative: disable / 0: last)

2. JSP Engine

Item	Description	Default Value
CheckInterval	When Development is false, cycle for checking jsp changes and recompilation (seconds)	0 (0: disabled / positive: enabled with that cycle)
Development	Whether Development. When Development is true, changes are checked with modificationTestInterval value as cycle	true (0: check every access)
GenStringAsCharArray	Whether to generate String as Char Array	false
ModificationTestInterval	Cycle for jsp change check when Development is true	4
TrimSpaces	Remove unnecessary whitespace from response to reduce response bytes	false
JavaEncoding	Encoding when generating Java source	UTF8
LoadOnStartup	Specify Servlet loading order when WAS starts	3

3. Welcome File List

Item	Description	Notes
File	Specify files to service in order when Directory index is called	

4. Session Timeout

Item	Description	Notes
SessionTimeout	Session timeout time (minutes)	Default: 30

Environment

Provides screen for managing JVM options. Modify through editor and click **Save button** to save.

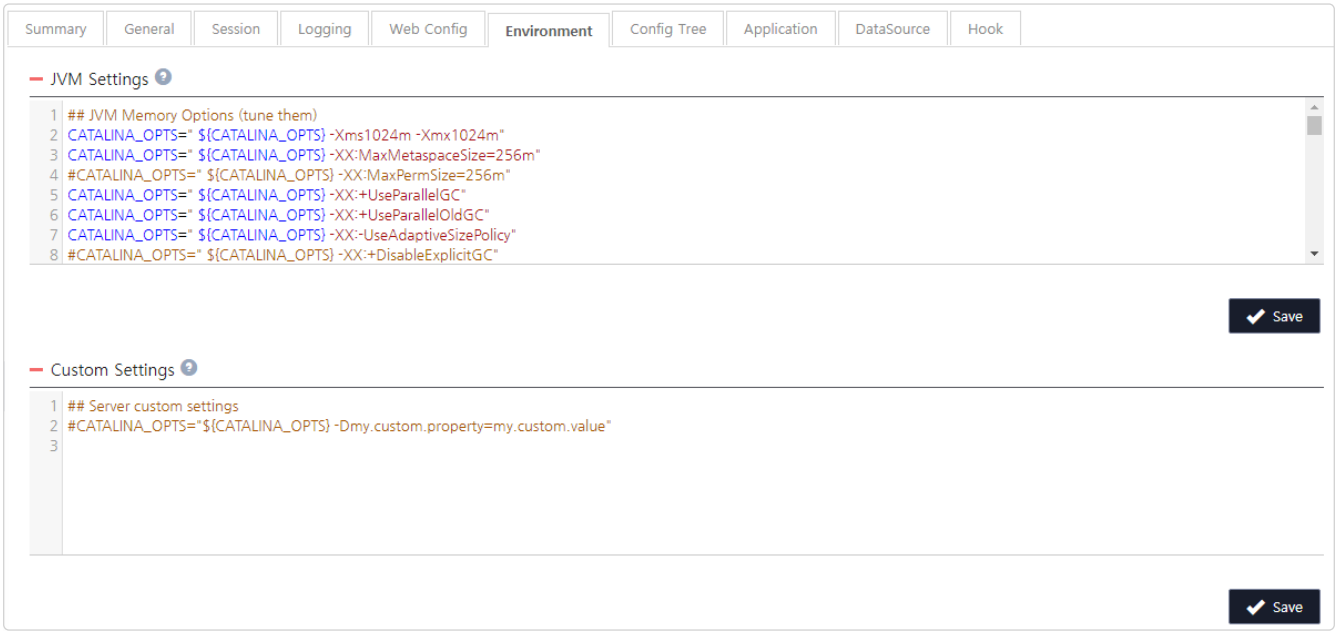


Figure 21. WAS Server Template Environment Tab

Configuration Tree

Application Server's /conf folder sub configuration files under installation path can be managed through file editor.

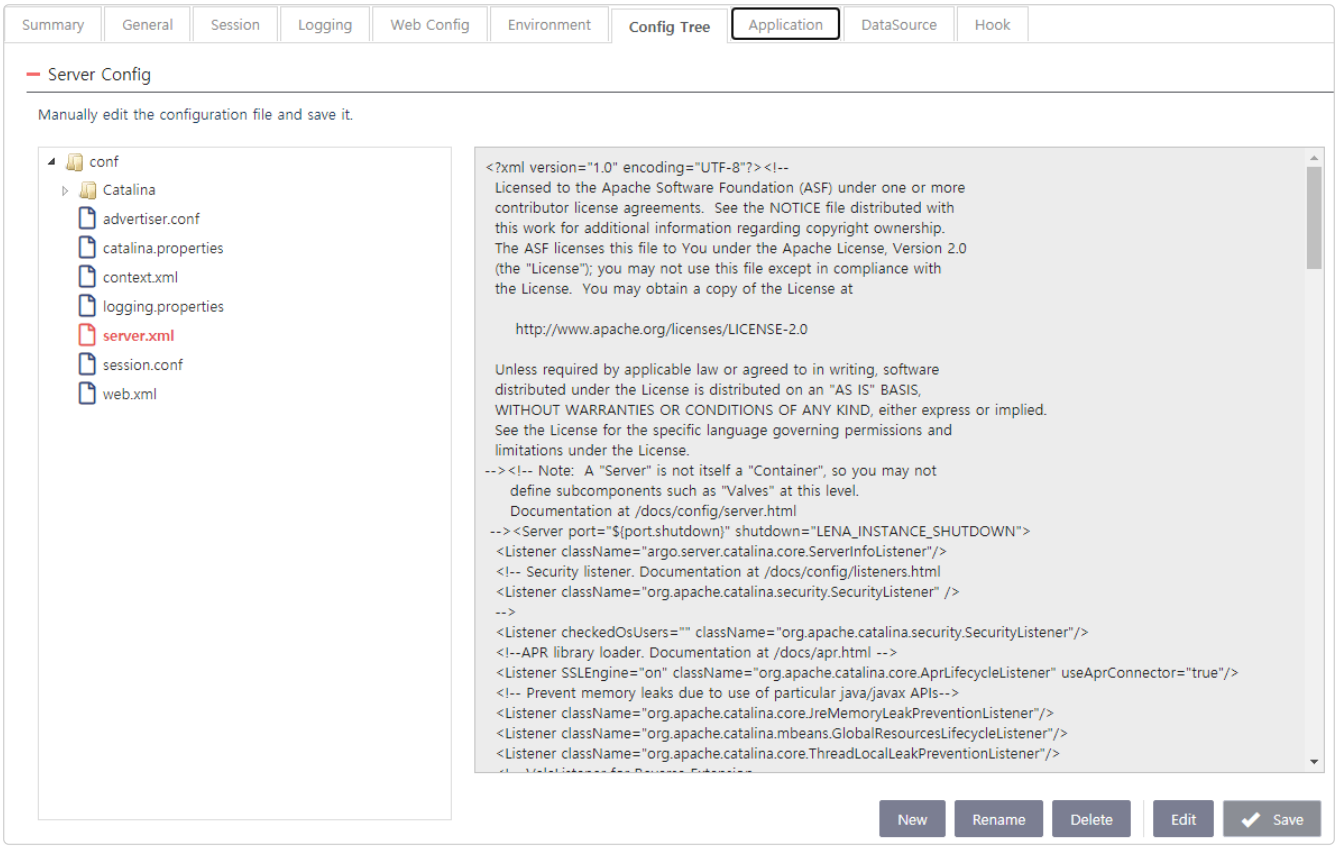


Figure 22. WAS Server Template Configuration Tree Tab

Application

Provides screen for adding/querying Application list.

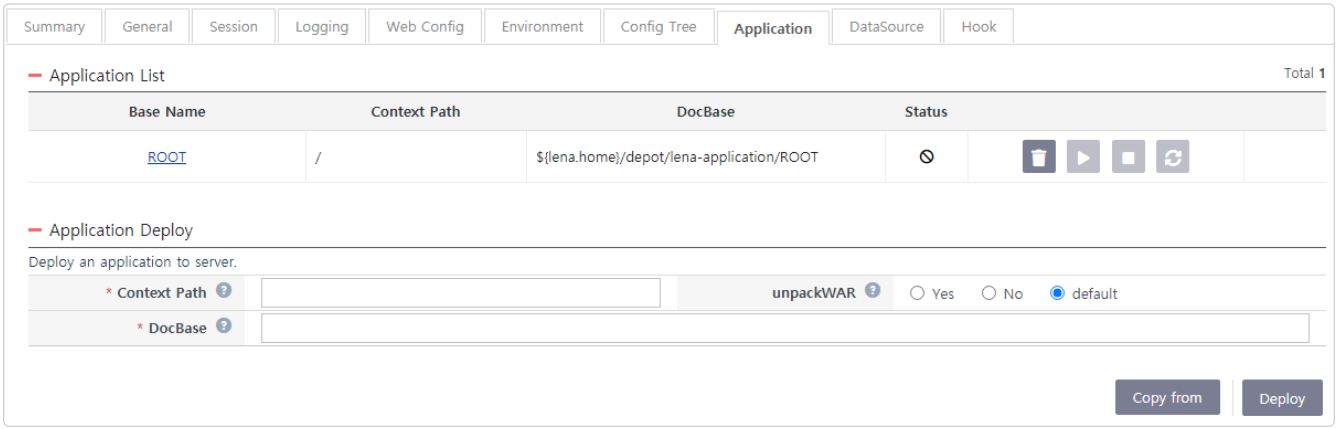


Figure 23. WAS Server Template Application Tab

1. Application List
   Click **trash button** in query screen to Undeploy that Application. When performing Undeploy for WAS, all of the following operations are performed regardless of application's DocBase. Be careful when performing Undeploy if source is located in appBase.
   a. Delete {contextPath}.xml under /conf/Catalina/localhost (basic management method)
   b. Delete {contextPath}.war under appBase
   c. Delete {contextPath} directory under appBase
2. Application Deploy

Item	Description	Notes
Context Path	Context path	Input only when Application Type is selected as WAR
unpackWAR	Whether to execute after expanding WAR file. When value is false, WAR file compression is not expanded, and web application is just redeployed in compressed state	(default: true) Input only when Application Type is selected as WAR
DocBase	Application location	

Two methods can be used to deploy Applications. First is clicking **Copy from button** to import application information registered in resources. Only settings of applications registered in resources are copied, application source is not cloned. Second is directly inputting information. When specifying DocBase, directly input application path or click **Browser button** to get path where that source is located. Then click **Deploy button** to Deploy Application.

When deploying WAS, {contextPath}.xml file is created under /conf/Catalina/localhost.

Even if Application in resources is changed, it is not applied to Service Cluster that cloned that Resource.

DataSource

Provides functionality to manage JNDI DataSource that can be used by Application Server's Applications. JNDI can be set so all Applications running on Server can share and use, or JNDI can be

set for each Application for use. For Enterprise Edition, JTA is supported so additional attributes are added.

1. Server DataSource Configuration Set DataSource shared by all Applications running on Server. List of DataSources available on Server can be queried, and DataSource registration, modification, deletion is possible.

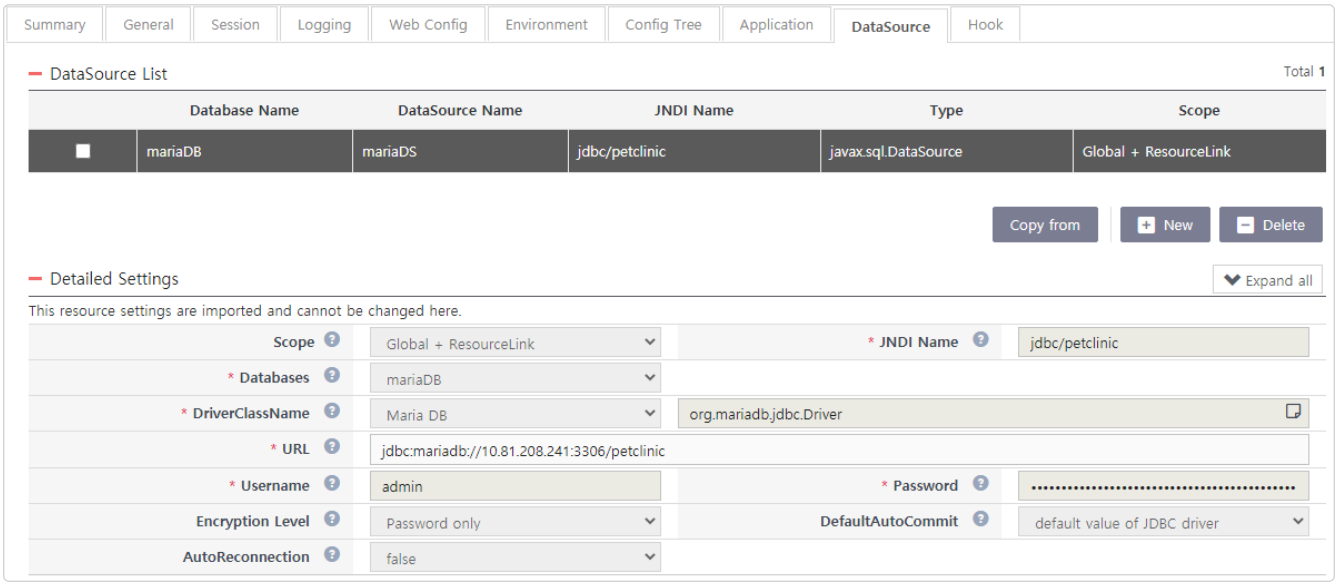


Figure 24. WAS Server Template Datasource Tab

DataSource attributes are as follows. Attributes not visible on initial screen are displayed when **Expand all** button is clicked.

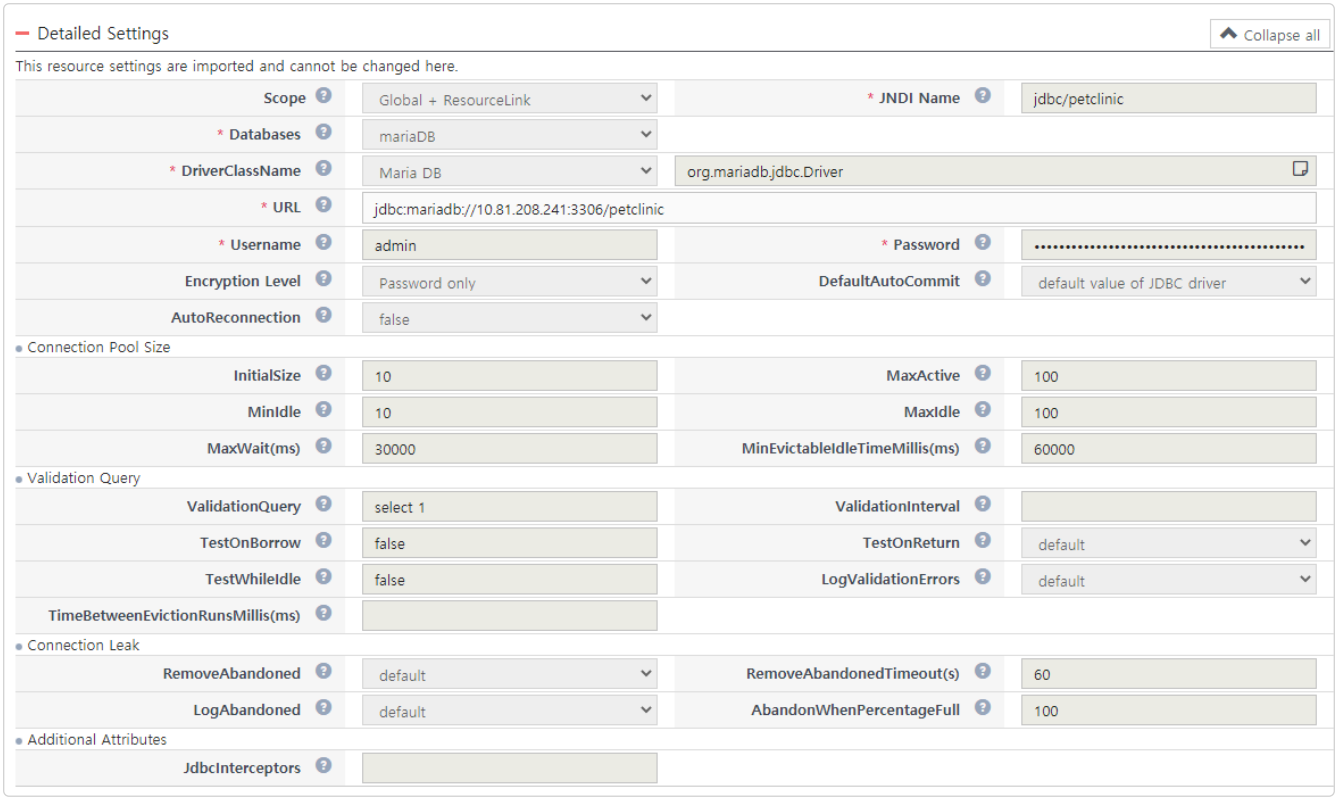


Figure 25. WAS Server Template Datasource Detail

Item	Description	Notes
Scope(*)	Scope for using DataSource	- Context: Datasource information is set in common context area so all Applications can share. - Global: Datasource information is set in GlobalNamingResource area, and each application individually sets and uses in DataSource link management. - Global+ResourceLink: Datasource information is set in GlobalNamingResource area and Datasource link is set in common context area.
JNDI Name(*)	JNDI name of Global DataSource	
Databases	Set information of datasource to be used commonly	
Resource Name	Name of Databases	
Address(Host/Port)	IP and port to be used commonly	
DriverClass Name	JDBC Driver class name	
URL(*)	JDBC URL	
Username(*)	Connection username	
Password(*)	Connection password	when encryption is checked, password is encrypted and stored. Encryption is recommended for security.
Auth(*)	JNDI authority	Default : "Container"
Description	Description of Datasource	
Encryption Level	Specify encryption scope for authentication information	Default : Password only
InitialSize	Initial number of Pool Connections	Default : 10
MaxActive	Maximum number of Pool Connections	Default : 100
MinIdle	Minimum number of Idle Connections	Default : 10
MaxIdle	Maximum number of Idle Connections	Default : 100
MaxWait	Maximum time to wait when no available Connection in Pool (ms)	Default : 30000

Item	Description	Notes
TimeBetweenEvictionRunsMills	Thread execution cycle for extracting unused Connections (ms)	Default : 5000
MinEvictableIdleTimeMillis	Connections existing in Pool in idle state for longer than this time become removal targets (ms)	Default : 60000 (60 seconds) (1800000 (30 minutes) when XaDataSource = true)
DefaultAutoCommit	Auto Commit status of Connections created from Pool	Default : JDBC driver's default value
ValidationQuery	Connection validity verification query	Default : null
ValidationInterval	Connection validity verification cycle (ms)	Default : 3000
TestOnBorrow	Before taking connection from Pool, perform query set in validationQuery to check connection validity	Default : default(false)
TestOnReturn	Before returning connection to Pool, perform query set in validationQuery to check connection validity	Default : default(false)
TestWhileIdle	For idle connections, perform query set in validationQuery to check connection validity	Default : default(false)
LogValidationErrors	Whether to output errors when errors occur after validation query execution	Default : default(false)
RemoveAbandoned	Whether to detect Connection loss	Default : default(false)
RemoveAbandonedTimeout	Timeout value for determining lost Connection (unit: seconds)	Default : 60
LogAbandoned	Whether to log when processing Connection loss	Default : default(false)
AbandonWhenPercentageFull	Connection pool must exceed set occupancy rate to perform abandon	Default : 0
JdbcInterceptors	User-defined functionality can be added using flexible and pluggable interceptors	When setting QueryTimeout, enter QueryTimeoutInterceptor(queryTimeout=time(seconds))

Additional attributes for Enterprise Edition are as follows.

Item	Description	Notes
JtaManaged	Whether to use JTA	Default "false"
XaDataSource	Whether to use XA	Default "false"

XADataSource configuration can only be used when JTA is configured, and when XADataSource is configured, validationInterval, logValidationErrors, abandonWhenPercentageFull attributes cannot be used.

When DataSource is set to Context scope, all Applications share it.

In Enterprise servers, DataSource can also be set to Context scope, but Lookup is not possible in EJB. Setting to Global + ResourceLink scope is recommended for Enterprise servers.

Password encryption algorithm uses AES. Key value for encryption is managed as "datasource.key=keyvalue" in Manager LENA Home sub /conf/manager.conf file and each Application Server Home sub /conf/advertiser.conf.

2. Databases
   When setting URL, register by creating Databases with information to be used commonly. **+ button** creates popup window when clicked.
   a. Enter Resource Name to distinguish Databases.
   b. Check automatically filled DriverClassName. Change if necessary.
   c. Enter Address (IP and port) and save.

3. JDBC driver Upload
   JDBC Driver library can be uploaded through Manager. Click **Upload button** under DataSource detailed information to display upload screen as follows.

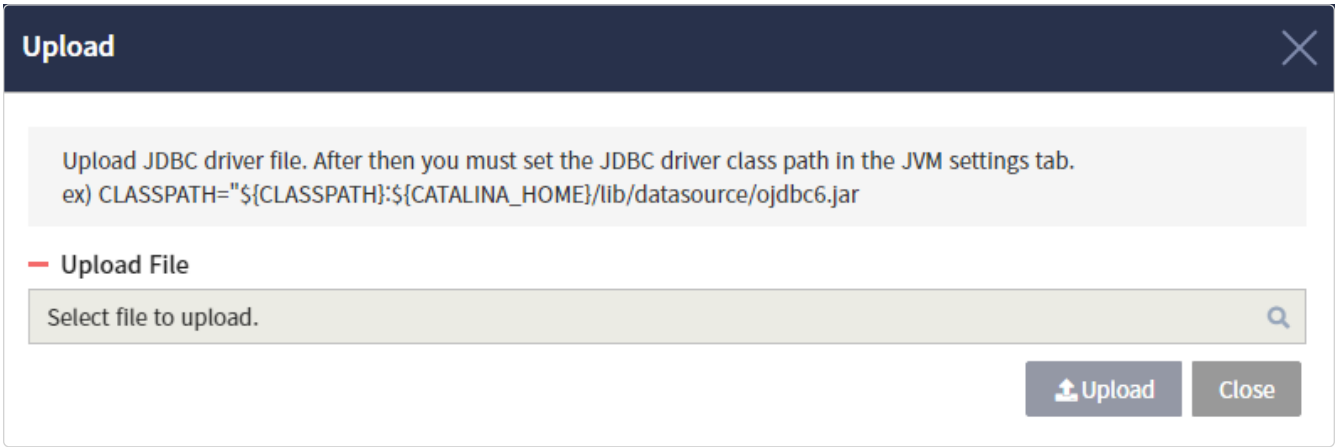


Figure 26. JDBC driver upload popup

a. Select file to upload through Search button. File to upload is JDBC Driver library, so only JAR format files can be selected.
b. Click Upload button to upload selected file to target directory.
c. Path where JDBC Driver file is uploaded is ${SERVER_HOME}/lib/datasource.

4) Connection Test
Click **Connection Test button** in DataSource detailed screen to perform connection test for configured DataSource. When connection is successful, "JDBC Connection is successfully tested" message is displayed as follows. If "Driver Class[class name] does not exist." error message is displayed, check if corresponding driver class is properly uploaded and classpath is configured. classpath is added in Application Server details > JVM Env > JVM Settings. Configuration example is as follows.
ex) CLASSPATH="${CLASSPATH}:${CATALINA_HOME}/lib/datasource/ojdbc6.jar"

When Resources menu under Server menu is selected, screen for managing Resource information related to that Server is displayed. By default, information for DataSource, JMS, JTA Resources can be managed. (JMS, JTA Resources are supported only for Enterprise Server)

5. Resource Configuration Clone

Click **Copy from button** to clone DataSource settings and driver files registered in resources.

Even if DataSource in resources is changed, it is not applied to Service Cluster that cloned that Resource.

Hook

Allows execution of user-defined Shell Script before Application Server startup and after shutdown in Container.

- Start Hook Script : This Script is executed before starting Application Server during Container startup.
- Stop Hook Script : This Script is executed after stopping Application Server during Container shutdown.

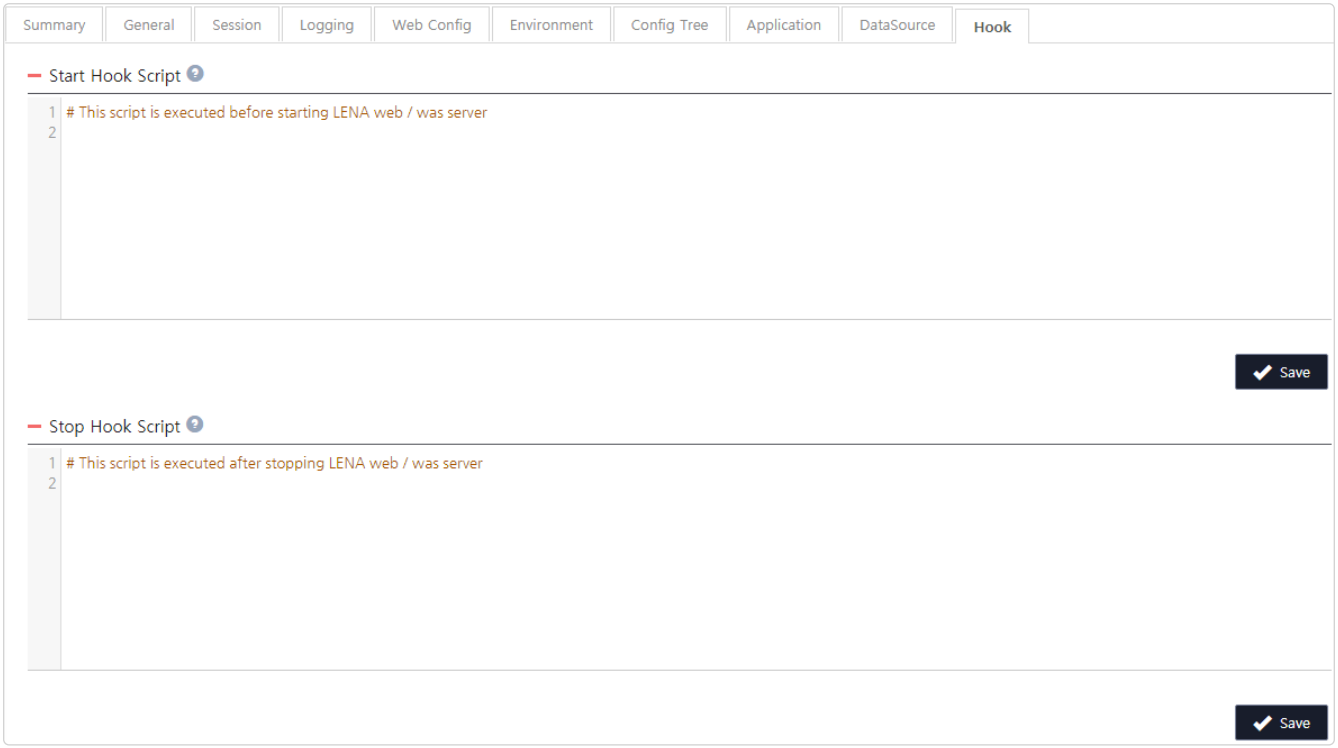


Figure 27. WAS Server Template Hook Tab

TunA

Easily integrates Container environment with TunA APM to conveniently monitor user application performance. TunA Agent file is located under /lib/tuna/ for use. Based on LENA v1.3.4.2, TunA v2.7.0 or higher, can be used on Linux/Unix OS.

- Enable TunA : Whether to use TunA. When checked, System Group and Configuration fields are displayed on screen, when unchecked, those items are not visible on screen.
- System Group : Select TunA System Group that server will belong to.
- Configuration : Provides functionality to check and modify Agent configuration.

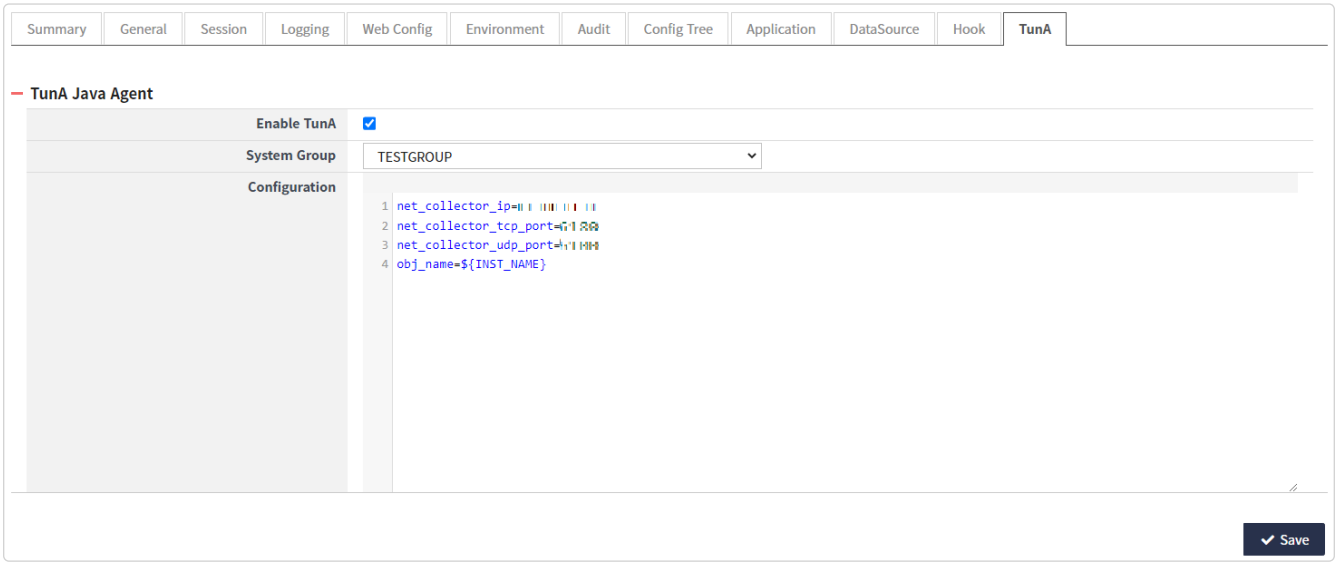


Figure 28. TunA Tab

Revision Creation

Click **New Revision button** in Template tab to create new Revision. Modify WAS, WEB server configuration files through tabs at bottom of System Template Overview and click Save to temporarily save. After all configuration file modifications are complete, click New Revision button to create new Revision and generate Template compressed file. Created Revision can be checked in Revision tab.

Even after modifying and saving WAS, WEB server configuration files, if new Revision is not created, screen returns to Default Revision when re-entering. Configuration

Configuration

Click **Configuration button** in Template tab to display Configuration screen.

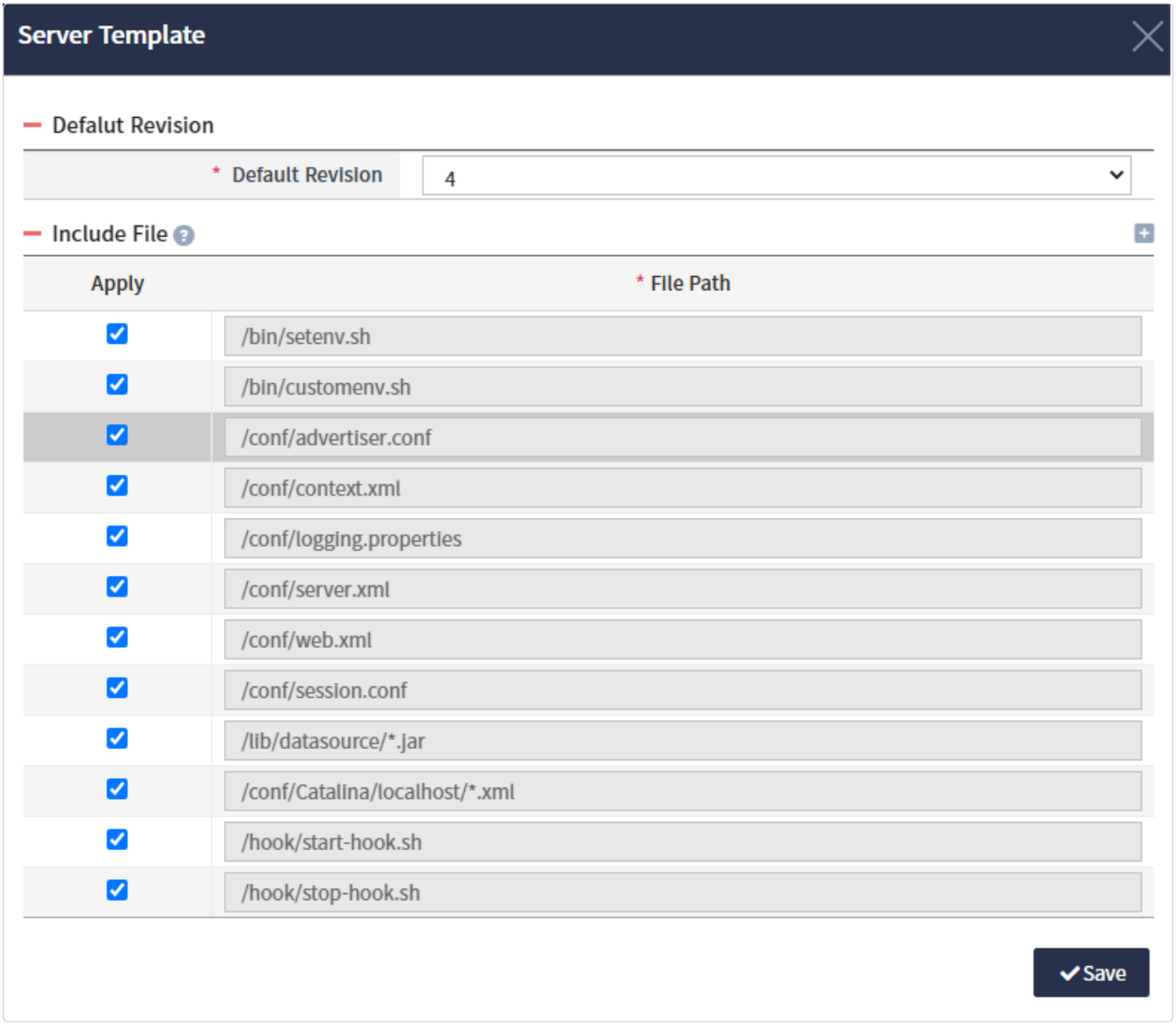


Figure 29. WAS Server Template Configuration Popup

Default Revision and Include Files to be included in Template compressed file can be specified. Basic file list for Template configuration is automatically generated, and users can add desired files. Only files with Apply checkbox activated are included in Template compressed file.

Export

Click **Export button** in Template tab to display Template Export screen. Download Template compressed file to local computer or upload to AWS S3, GCP Storage, Filesystem.

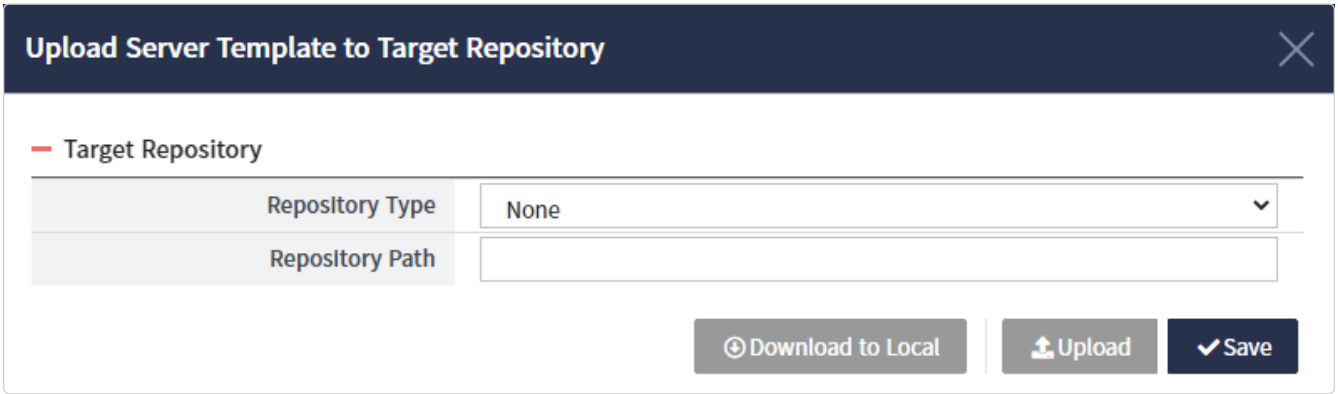


Figure 30. WAS Server Template Export Popup

Copy Configurations

Click **Copy Configurations button** in Template tab to display Copy Configurations screen.

[service cluster template copy configs] | manual/container/service_cluster_template_copy_configs.png

Figure 31. WAS Server Template Copy Configurations Popup

Guides environment variables needed when using Template in Container. 'Key-value' pairs defined on screen are used as container environment variables for Pods. Click right button of each row to copy that value to clipboard, click Copy All to Clipboard button at bottom to copy in 'key-value' format to clipboard.

5.2.6. Web Server Template Management (EN-A)

Server Template Overview

Select Service Cluster from left menu or Service Cluster Group details and click Template tab to display Service Template Overview screen. Shows OS Family information and current Revision information.

Server Template Configuration Management

Provides functionality to change Web Server configuration information. After changing configuration information and clicking New Revision button, new Revision is created. Changed configuration information is managed through created Revision.

Summary

Click Summary tab at bottom of Template tab in Service Cluster to display screen.

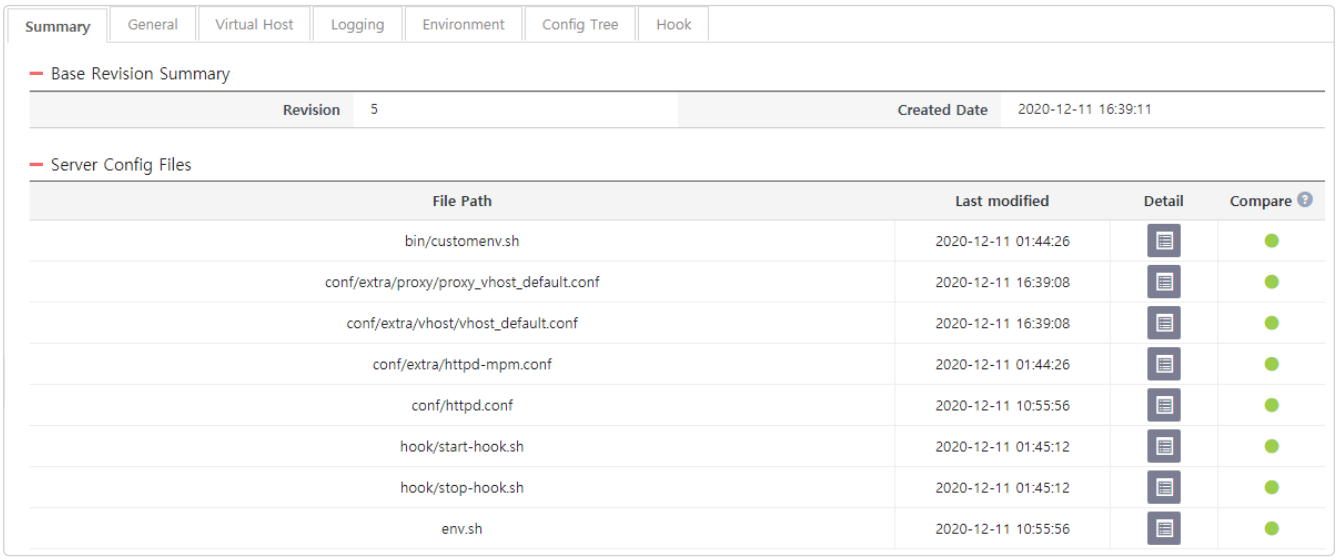


Figure 32. Web Server Template Summary Tab (EN-A)

1. Base Revision Summary shows currently loaded Revision number and Revision creation date.
2. Server Configuration Files shows file list that makes up currently loaded Revision. Content can be checked by file, and modified configuration files can be checked/compared through Compare functionality. If there are no changes, **green icon** is displayed, and if configuration files are modified, **red X icon** is displayed. Click **red X icon** to show differences between original file and modified file of loaded Revision in popup.

General

General configuration values and Connection, Process information of Web Server can be edited. Web Server's configuration information performs Validation on configuration files when saving, minimizing Server startup failures due to configuration file errors.

When configuration file error occurs, file is not saved and error message is displayed
ex) AH00526: Syntax error on line 253 Argument for 'Require all' must be 'granted' or 'denied'

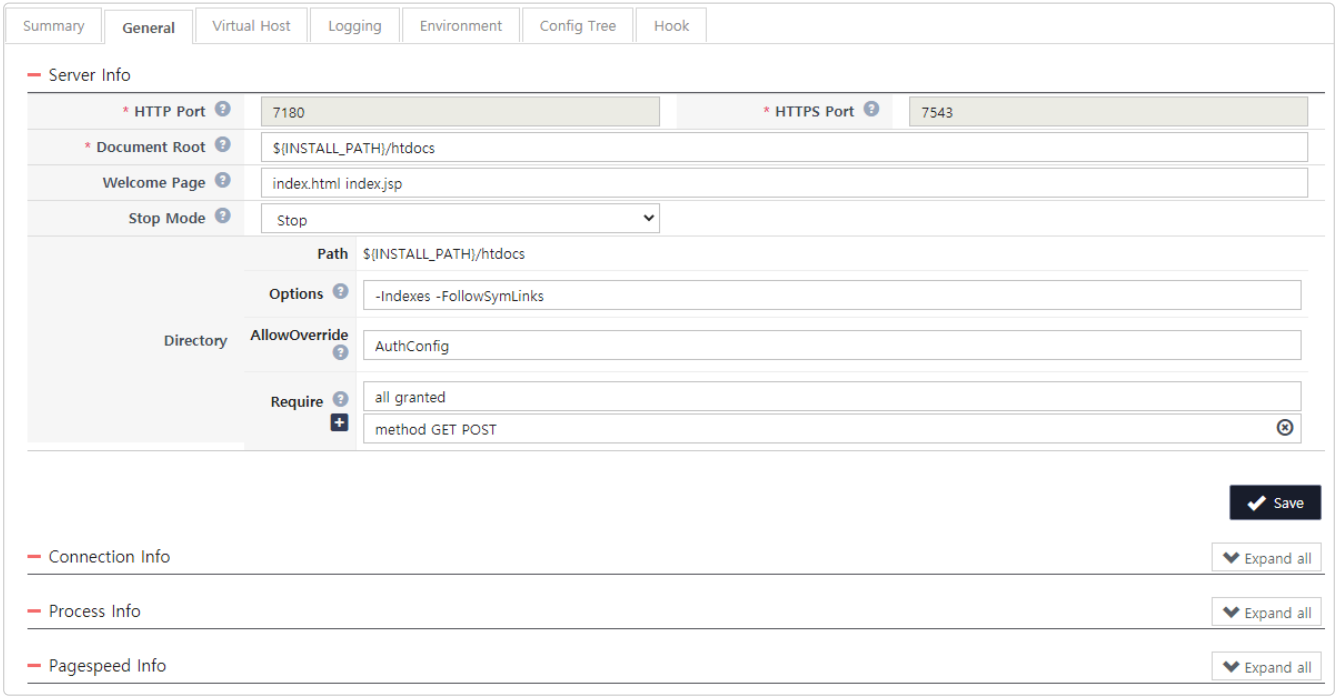


Figure 33. Web Server(EN-A) Template General Tab

1. Server Info (env.sh and /conf/httpd.conf file management)

Item	Description	Notes
Http Port(*)	HTTP Port	Fixed at 7180
Https Port(*)	HTTPS Port	Fixed at 7543
Staging HTTP Port	Service port used when starting in Staging mode	Used during Graceful restart LENA uses basic nostage mode
Staging HTTPS Port	HTTPS port used when starting in Staging mode	Used during Graceful restart LENA uses basic nostage mode
Document Root(*)	Basic folder path where documents provided by Web Server are stored	
Log Home(*)	Folder path containing Web Server's log information	
Welcome Page	Define which file to use as initial page document of website	
Directory/Path	Directory path where web documents are located to set which services and functions to allow/deny	

Item	Description	Notes
Directory/Options	Access control settings to apply to all files and directories under specified directory	-Indexes prevents showing file list under Document Root when welcome page cannot be found -FollowSymLinks prevents accessing file system other than existing web documents under Document Root via symbolic links
Directory /AllowOverride	Set which directives to allow for resource access control configuration files for each subdirectory under Document Root (generally AccessFileName : .htaccess)	-None : Do not allow any directives -All : All directives available -AuthConfig : Allow user authentication directives -FileInfo : Allow document type control directives -Indexes : Allow directory indexing control directives -Limit : Allow host access control directives
Directory/Require	Verify whether authenticated users perform allowed Actions	

2. Connection Info (/conf/extra/httpd-default.conf file management)

Item	Description	Notes
Timeout(*)	Time for Server to wait and disconnect connection when no event occurs for certain time after connection between client and server	Default : 60(sec)
KeepAlive(*)	Whether specific process continues to handle specific user's request tasks	Default : On
MaxKeepAlive Requests(*)	Valid value when KeepAlive is On, process handles specific user's requests for specified number of times When this value is exceeded, that process dies and another process handles requests	Default : 100
KeepAliveTimeout(*)	Valid value when KeepAlive is On, timeout to disconnect connection when no request for set time	Default : 5(sec)
RequestReadTimeout(*)	Time to wait for receiving request header and body from user, if not received within set time, sends 408 REQUEST TIME OUT error	Default : header=20-40,MinRate=500 body=20,MinRate=500

3. Process Info (/conf/extra/httpd-mpm.conf file management)

Item	Description	Notes
StartServers(*)	Number of server processes initialized when Web Server starts	Default : 4

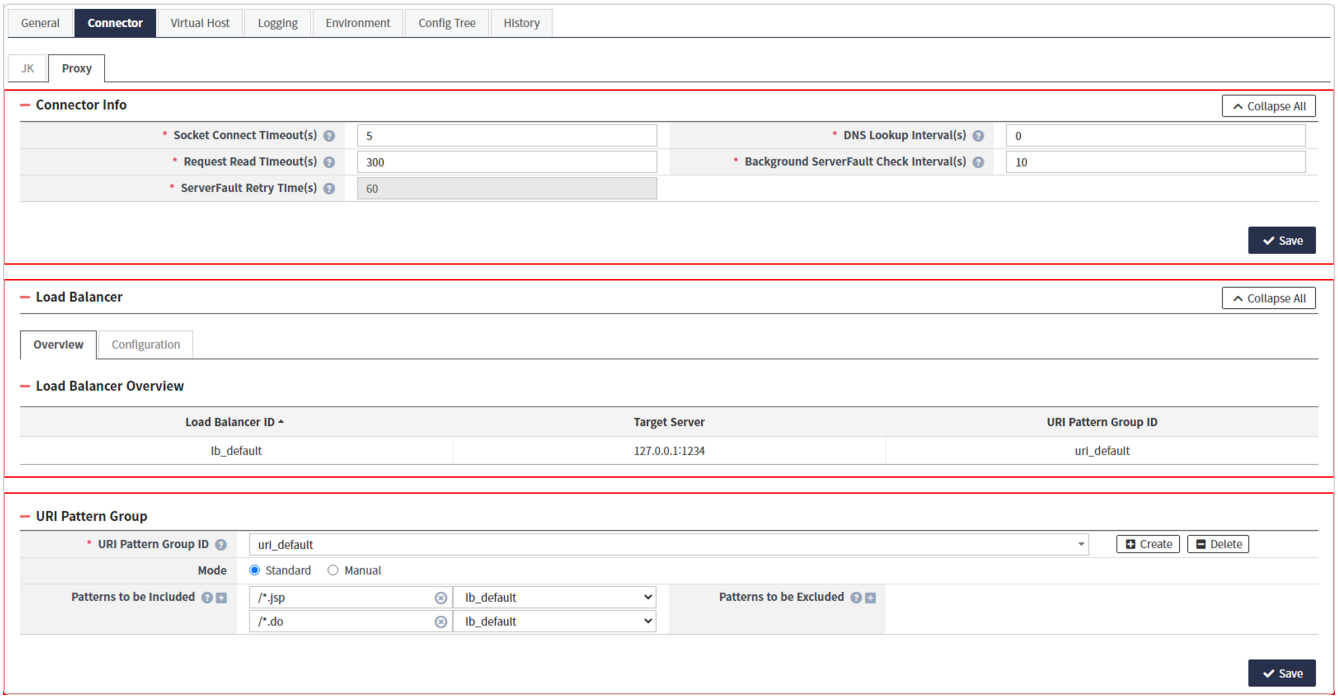
Item	Description	Notes
ServerLimit(*)	Maximum process value that MaxClients can create	Default : 32
ThreadLimit(*)	Maximum configurable value for ThreadPerChild	Default : 128
MinSpareThreads(*)	When number of Idle Threads in Idle state is less than this value, Threads increase to this value and maintain	Default : 128
MaxSpareThreads(*)	When number of Idle Threads in Idle state is more than this value, Threads decrease to this value and maintain	Default : 256
ThreadPerChild(*)	Number of Threads created by each child process	Default : 128
MaxRequestWorkers(*)	Maximum number of Threads that all child processes can create	Default : 1024
MaxConnectionPerChild(*)	Maximum number of requests that child process can service After processing this many requests, it terminates.	Default : 0 (0: unlimited)

Connector

Manages information for linking Web Server and WAS.

Proxy

Edits configuration information when using Proxy(mod_proxy).



Proxy tab configuration is divided into three areas: Connector Info, Load Balancer, and URI Pattern Group.

1. Connector Info
   Manages basic configuration values of Proxy.

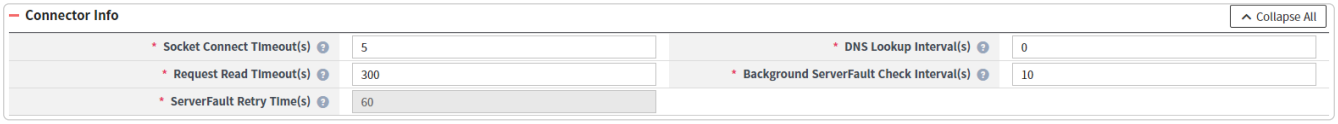


Table 108. Connector Info (Proxy)

Item (* indicates required values)	Description	Notes
Socket Connect Timeout(s)(*)	Time(s) for Apache httpd to wait until connection creation to backend is completed.	Default: 5
DNS Lookup Interval(s)(*)	DNS lookup interval. Set to 0 to disable function.	Default: 10
Request Read Timeout(s)(*)	Time(seconds) for Apache httpd to wait for transmitted data sent and received from backend.	Default: 300
Background ServerFault Check Interval(s)(*)	When Member connected to backend server is in error state, checks server at interval(seconds) set in this item and retransmits requests when server operates normally. Set to 0 to disable function.	Default: 10
ServerFault Retry Time(s)(*)	When Member connected to backend server is in error state, does not transmit any requests to that server until Apache httpd timeout(seconds) expires.	Background ServerFault Check Interval item is modifiable when 0. Default: 60

2. Load Balancer
   Manages basic configuration and Members of Load Balancer for load balancing.
   Load Balancer area has Overview tab and Configuration tab. Overview tab can check overall information of currently created Load Balancer, and Configuration tab can configure detailed contents of Load Balancer.

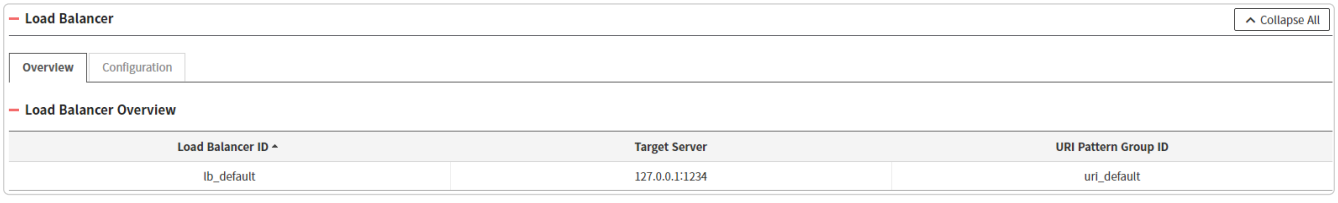


Table 109. Load Balancer Info - Overview (Proxy)

Item (* indicates required values)	Description	Notes
Load Balancer ID	ID of currently created Load Balancer.	
Target Server	Basic information of Members registered in Load Balancer. Displayed in 'Node Name/Server Name' or 'Address:Port' format.	

Item (* indicates required values)	Description	Notes
URI Pattern Group ID	When Load Balancer is specified for specific URI Pattern, URI Pattern Group ID that the URI Pattern belongs to is displayed.	

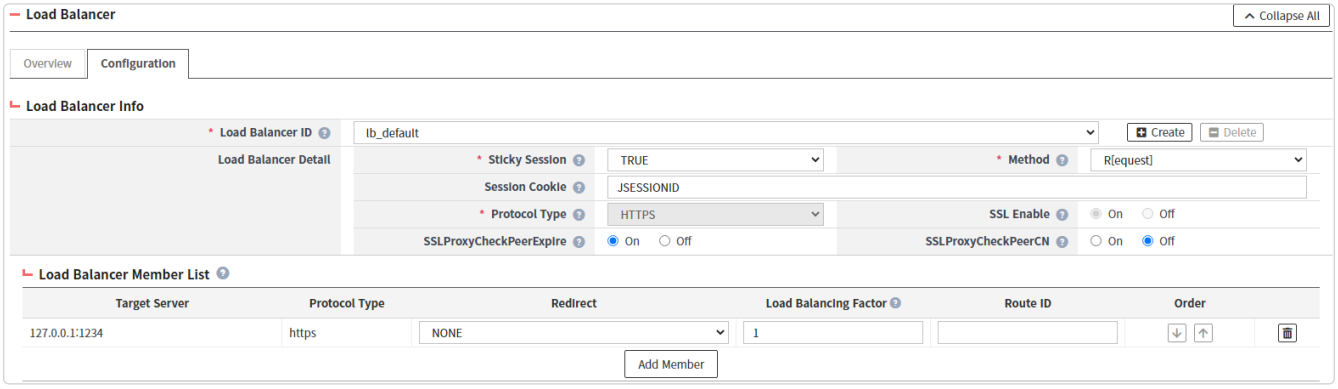


Table 110. Load Balancer Info - Configuration (Proxy)

Item (* indicates required values)	Description	Notes
Load Balancer ID(*)	Name of Load Balancer.	'lb_' prefix is added.
Sticky Session(*)	Whether to support routing based on Session ID.	
Method(*)	Specifies method used by Load Balancer to determine appropriate Member for load balancing.	
* R[equest] : Selects Member with least requests. (Default)	* T[raffic] : Selects Member with least network traffic.	* B[usyness] : Selects Member with least load based on number of requests.
Session Cookie	Set when wanting to change Session Cookie name.	
Protocol Type(*)	Specifies protocol type of Member. Can only be changed when Member is not specified.	Default: HTTP
SSL Enable	Uses SSL/TLS protocol engine for Proxy.	This option cannot be configured and operates only according to Protocol configuration. Default: Off when HTTP, On when HTTPS
SSLProxyCheckPeerExpire	Checks if remote server certificate has expired.	Default: On
SSLProxyCheckPeerCN	Checks CN field of remote server certificate.	Default: Off

Members are added with Add Member button in Load Balancer Member List table.
When Add Member button is pressed, window for adding Member is displayed on screen, and users can select servers managed by LENA Manager as Members in this window or directly input Member

information to add.

Added Members are managed through following information.

Table 111. Load Balancer Member List

Item (* indicates required values)	Description	Notes
Target Server	Basic information of server that Member points to. Displayed in Node Name/Server Name format for Members managed by LENA Manager, Address:Port format for Members not managed by LENA Manager.	
Protocol Type	Protocol type used by Member.	
Redirect	When this Member is in error state, sets Failover Member to handle requests received by this Member.	Default: NONE
Load Balancing Factor	Work allocation ratio, defines how much work this Member will do compared to other Members.	Default: 1
Route ID	Route ID of Member.	Must be input when using Sticky Session.
Order	Can change order between Members.	

3. URI Pattern Group
   Defines URI Mapping to pass requests coming to Web Server to WAS by checking URI patterns.

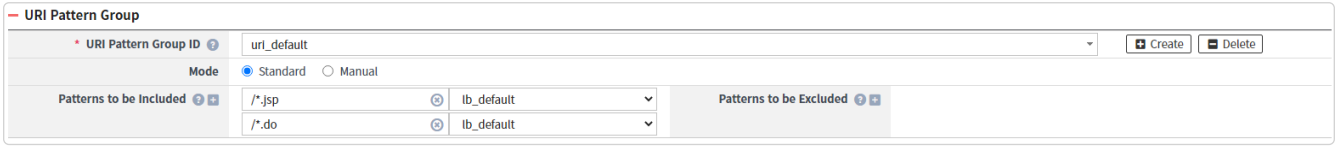


Table 112. URI Pattern Group (Proxy)

Item (* indicates required values)	Description	Notes
URI Pattern Group ID(*)	Name used for grouping and managing URI patterns. When URI Pattern Group used in Virtual Host, information about which Virtual Host is using it is displayed next to ID.	'uri_' prefix is added when Group is created.
Mode	Specifies whether to input URI patterns in format managed by LENA Manager or in user arbitrary format. Screen for inputting Patterns to be Included/Excluded or URI Patterns is displayed according to this item. If already saved pattern is in format managed by LENA Manager, it is automatically set to Standard, if in user arbitrary format, it is automatically set to Manual.	Standard: Input method according to LENA Manager URI Rule Manual: User arbitrary input method

Item (* indicates required values)	Description	Notes
Patterns to be Included	Input URI patterns to pass to WAS. Must select Load Balancer through right Select box to save. Can delete patterns through button.	Asterisk(*) meaning to allow all characters can be used, Hash(#), Equal(=) are not allowed.
Patterns to be Excluded	Input URI patterns not to pass to WAS. Can delete patterns through button.	Asterisk(*) meaning to allow all characters can be used.
URI Patterns	Used when inputting user arbitrary patterns.	

When changing configuration, New Revision creation and Server restart are required to reflect modified items

Virtual Host

Web Server's Virtual Host information can be registered/modified/deleted.

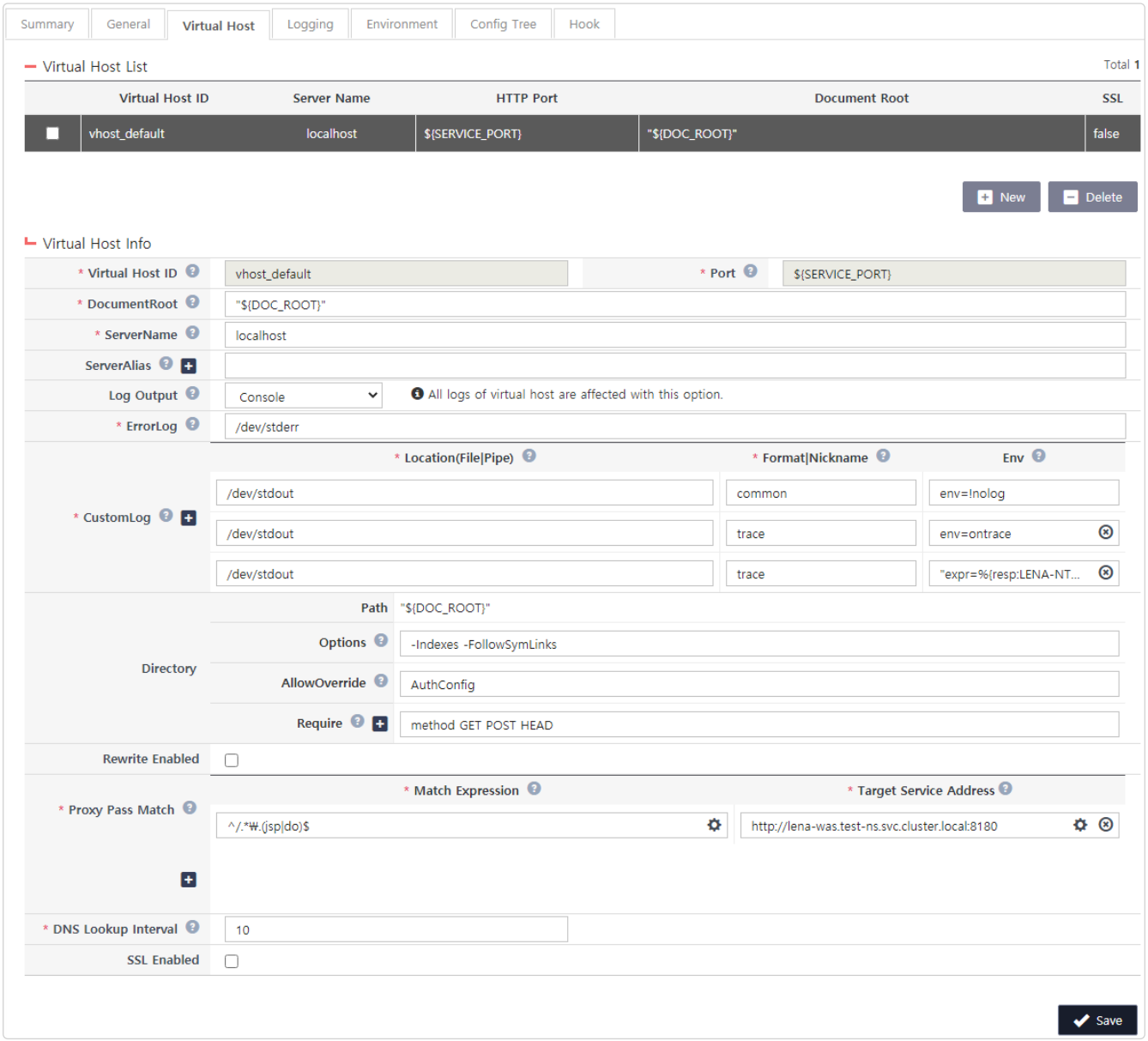


Figure 34. Web Server(EN-A) Template Virtual Host Tab

New / **Delete button** can register/delete Virtual Host. Virtual Hosts with one or more Load Balancers applied cannot be deleted. If you want to delete that Virtual Host, first change Virtual Host ID of Load Balancer to different Virtual Host ID through Connector tab. When SSL Enabled and Rewrite Enabled are checked, detailed item areas are additionally displayed as follows.

Figure 35. Web Server(EN-A) Template Virtual Host Rewrite Detail

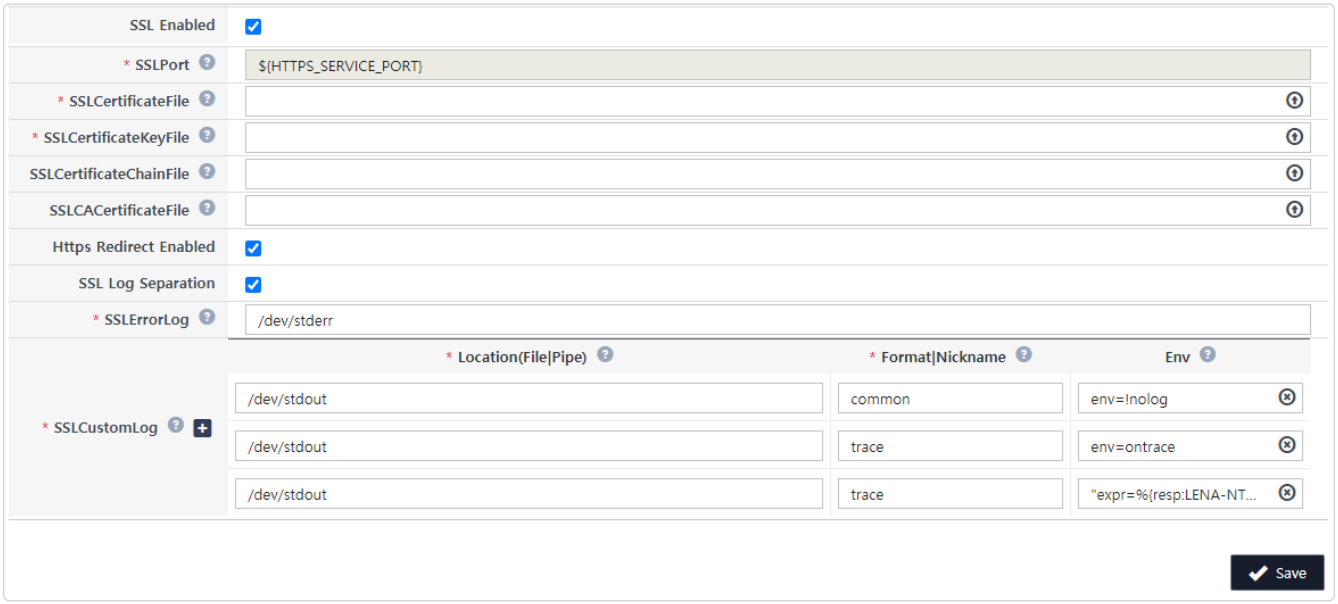


Figure 36. Web Server(EN-A) Template Virtual Host SSL Detail

Detailed contents of configuration information are as follows.

Managed files

- /conf/extra/vhost/{Virtual Host ID}.conf
- /conf/extra/rewrite/rewrite_{Virtual Host ID}.conf
- /conf/extra/ssl/ssl_{Virtual Host ID}.conf
- /conf/extra/vhost/custom_{Virtual Host ID}.conf

Item	Description	Notes
Virtual Host ID(*)	Virtual Host name	
Port(*)	HTTP Port used by that virtual host	
DocumentRoot(*)	Homepage directory location of that virtual host Can be specified to same or subdirectory using Server's DocumentRoot variable ${DOC_ROOT}	
Domain Name(*)	Domain name of that virtual host	
ServerAlias	ServerAlias used by that virtual host Can include wildcard characters (*.example.com)	
Log Output	Set log output type. ErrorLog, CustomLog settings are automatically changed according to selection.	
ErrorLog(*)	Web error log file location of that virtual host	
CustomLog(*)	Web log file location of that virtual host	

Item	Description	Notes
Directory/Path	Path from DocumentRoot	
Directory/Options	Access control settings to apply to all files and directories under specified directory	-Indexes prevents showing file list under Document Root when welcome page cannot be found
-FollowSymLinks prevents accessing file system other than existing web documents under Document Root via symbolic links	Directory/AllowOverride	Set which directives to allow for resource access control configuration files for each subdirectory under Document Root (generally AccessFileName : .htaccess)
-None : Do not allow any directives -All : All directives available -AuthConfig : Allow user authentication directives -FileInfo : Allow document type control directives -Indexes : Allow directory indexing control directives -Limit : Allow host access control directives	Directory/Require	Verify whether authenticated users perform allowed Actions
	SSL Enabled	Whether to use SSL
	SSLPort(*)	HTTPS Port
	SSLCertificateFile(*)	SSL certificate path
	SSLCertificateKeyFile(*)	SSL certificate Key file path

Item	Description	Notes
	SSLCertificateChainFile	File of PEM-encoded Server CA Certificate(optional)
	SSLCACertificateFile	ROOT certificate path(optional)
	Rewirte Enabled	Whether to use Rewrite
	Rewirte Conf	Detailed Rewrite configuration Rewrite according to rules set in Rewrite Rule according to specified Rewrite Condition https://httpd.apache.org/docs/2.4/mod/mod_rewrite.html reference
	Enable Custom	Add configurations that users want to add to Vhost arbitrarily.
Contents are generated and stored in separate file (custom_{Virtual Host ID}.conf).	Proxy Pass Match(*)	Match Expression : Request URL pattern to connect to Proxy Service Target Service Address : Target Proxy Service address to connect
Regular expression	DNS Lookup interval(*)	Domain Address Cache update cycle

Match Expression value of Proxy Pass Match must input URL pattern as regular expression, and can be input directly or by clicking **gear button**.

Figure 37. Web Server Template Virtual Host Proxy Configuration Popup

Match Rules area in above screen shows regular expressions decomposed by '()' units as list. To add unit Rule, click **+ button** at top and input regular expression. To delete unnecessary Rule, click **X button**. Rule Matching Test area is functionality to test whether Match Rules input regular expressions match. Input URL in Path field and click **Test button** to display regular expression matching result at bottom. In above screen, select Service Endpoint and click **Apply button** to close popup window and input value in Target Match Expression field.

Target Service Address of Proxy Pass Match can be input directly or click **gear button** to select Application Server type Service Cluster's Service Endpoint from displayed popup.

Logging

Web Server's log configuration information can be edited.

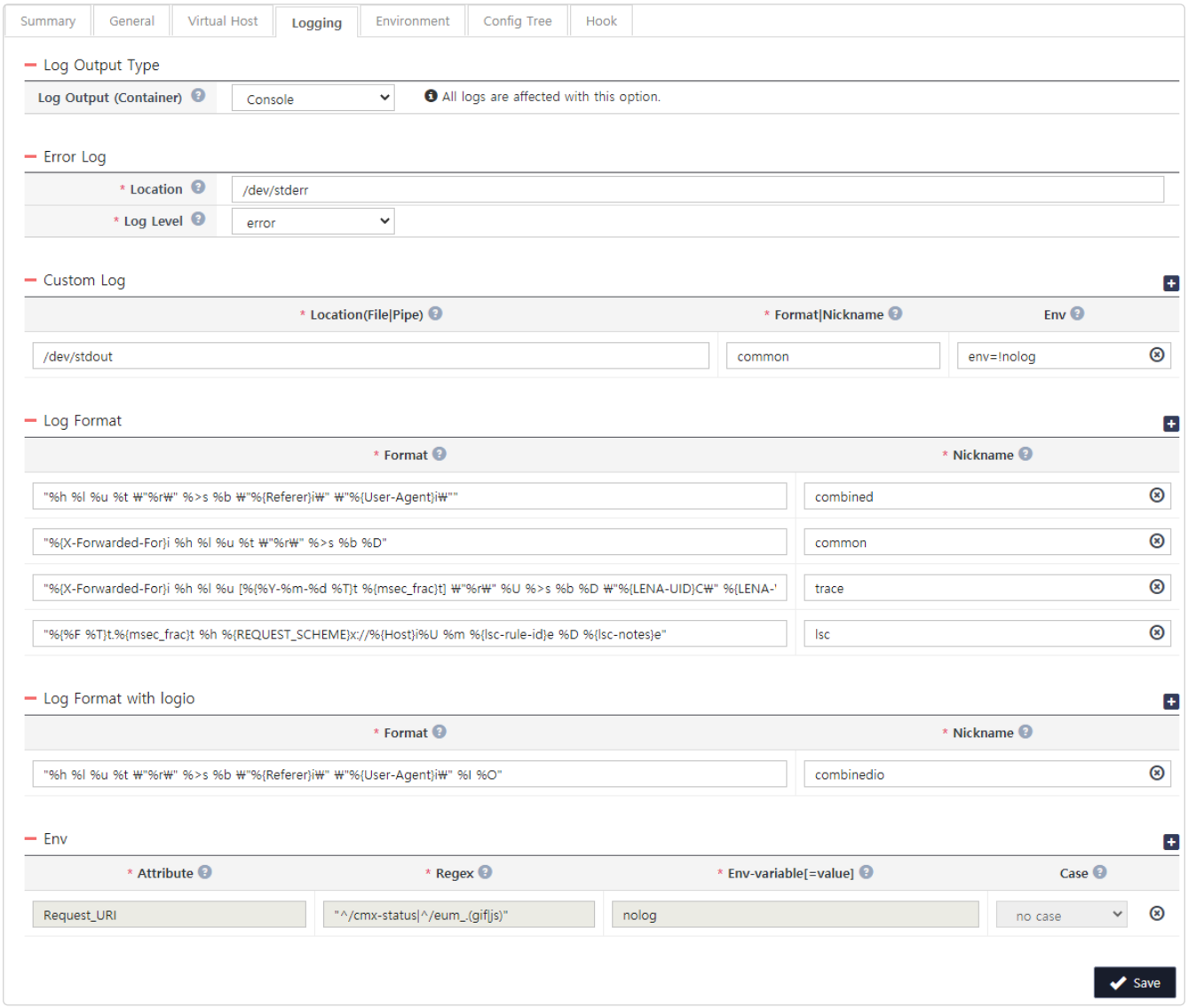


Figure 38. Web Server Template Logging Tab

1. Log Output Type

Select log output type for Web server. Error Log, Custom Log settings are changed according to selection.

Item	Description	Notes
Console	Output Log to standard output / error.	
File	Output Log to single file.	
Rotate pipe	Output Log to file and divide files by date.	
Manually Input	Output Log according to user definition.	

2. Error Log

Used when Web server records errors that occur while processing diagnostic information and requests. When problems occur during Server startup or operation, check files at location set here first.

(*) indicates required values

Item	Description	Notes
Location(*)	Specify Web server's error log file location	
Log Level(*)	Specify how detailed to record error log file contents	

3. Log Format

Sets format to use for log files.

Item	Description	Notes
Format(*)	Sets format for recording logs in log file	
Nickname(*)	Log format name to use in CustomLog	

4. Log Format with logio

Item	Description	Notes
Format(*)	Sets format for recording logs in log file Can measure bytes sent and received including request and head using %I and %O variables	
Nickname(*)	Log format name to use in CustomLog combinedio requires mod_logio_module to be loaded	

5. Custom Log

Sets log file name and format. Can selectively record logs according to request characteristics using environment variables.

Item	Description	Notes
Location(File	Pipe)(*)	File: Error log file location Pipe: Program path to receive log information as standard input after pipe character '
'		Format
Nickname(*)	Content to record in log file Use nickname defined in Log Format or write log format directly	
Env	Write whether to record logs according to server environment variable presence	(optional)

ex) When wanting to record requests from English users and non-English users in different log files
Location Format Env
logs/english_log common english

logs/non_english_log common !english

6. Env

Used when setting environment variables according to Request conditions.

Item	Description	Notes
Attribute(*)	HTTP request header (ex: Host, User-Agent, Referer, Accept-Language), one of request attributes (Remote_Host, Remote_Addr, Server_Addr, Request_Method, Request_Protocol, Request_RUI) or environment variable name associated with request	
Regex(*)	Perl compatible regular expression	
Env-variable[=value]	Variable name and value to set (optional) Varname, !varname or varname=value	
Case	Whether to distinguish case for Env-variable	With case : Distinguish case No case : No case distinction

Configuration Tree

Web Server's ${SERVER_HOME}/conf directory sub configuration files can be managed through file editor.

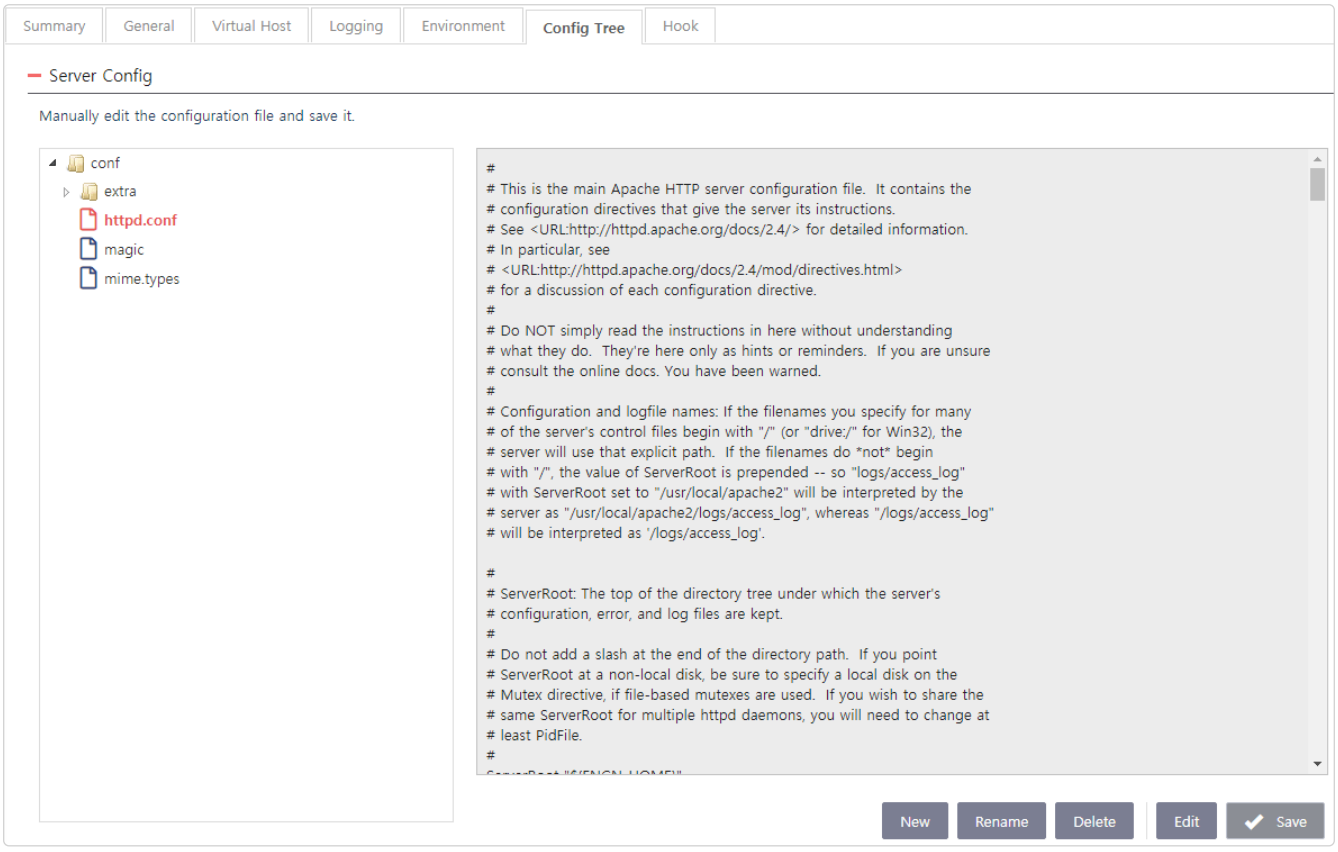


Figure 39. Web Server Template Configuration Tree Tab

Hook

Allows execution of user-defined Shell Script before Application Server startup and after shutdown in Container.

- Start Hook Script : This Script is executed before starting Application Server during Container startup.
- Stop Hook Script : This Script is executed after stopping Application Server during Container shutdown.

Revision Creation

Click **New Revision button** in Template tab to create new Revision. Modify WAS, WEB server configuration files through tabs at bottom of System Template Overview and click Save to temporarily save. After all configuration file modifications are complete, click New Revision button to create new Revision and generate Template compressed file. Created Revision can be checked in Revision tab.

Even after modifying and saving WAS, WEB server configuration files, if new Revision is not created, screen returns to Default Revision when re-entering.

Configuration

Click **Configuration button** in Template tab to display configuration screen.

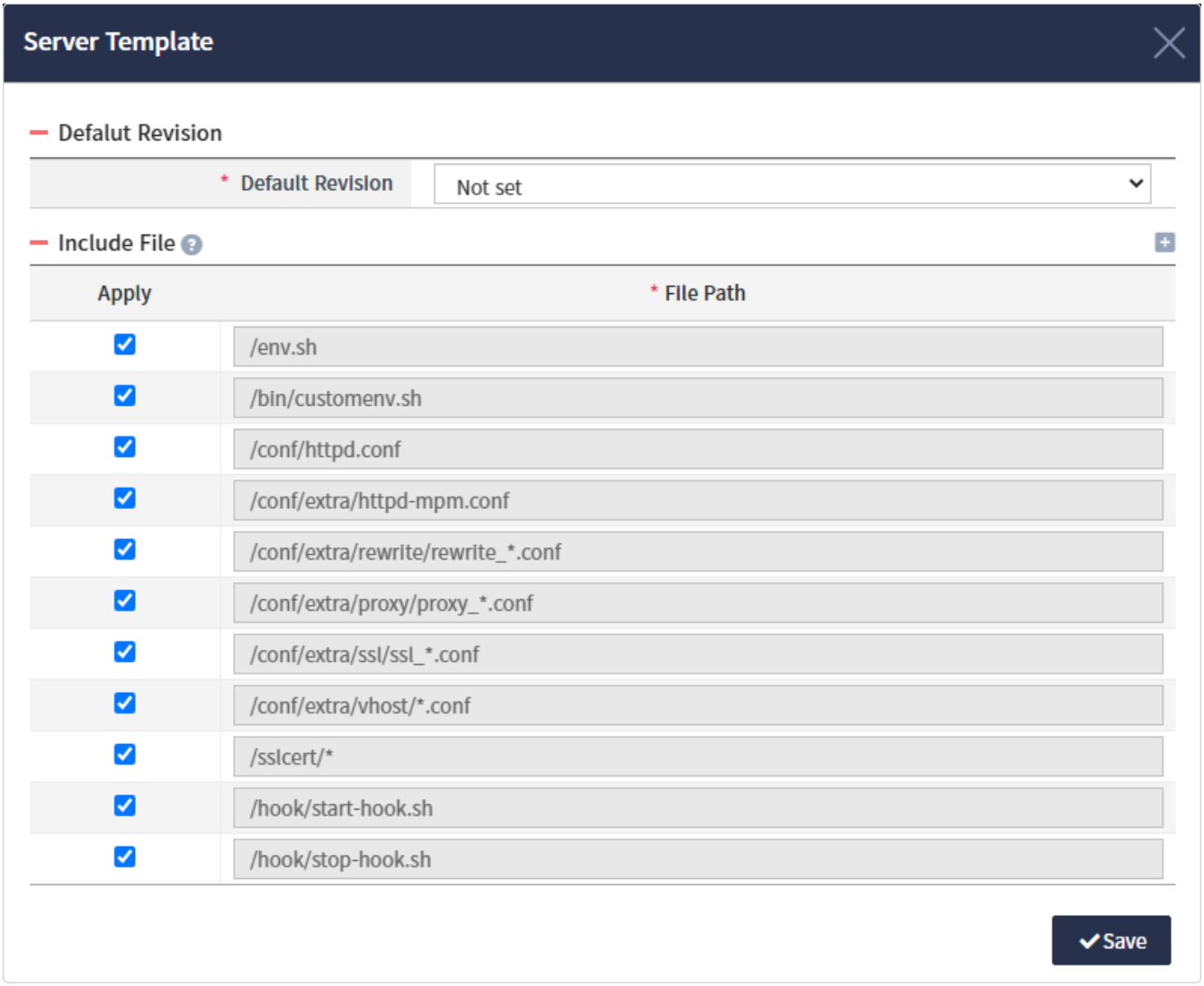


Figure 40. Web Server Template Configuration Popup

Default Revision and Include Files to be included in Template compressed file can be specified. Basic file list for Template configuration is automatically generated, and users can add desired files. Only files with Apply checkbox activated are included in Template compressed file.

Export

For detailed content related to Export, refer to Export in this document.

Copy Configurations

For detailed content related to User Guide, refer to Copy Configurations in this document.

5.2.7. Web Server Template Management (EN-N)

Server Template Overview

Select Service Cluster from left menu or Service Cluster Group details and click Template tab to display Service Template Overview screen. Shows OS Family information and current Revision information.

Server Template Configuration Management

Provides functionality to change Web Server configuration information. After changing configuration information and clicking New Revision button, new Revision is created. Changed configuration information is managed through created Revision.

Summary

Click Summary tab at bottom of Template tab in Service Cluster to display screen.

[service cluster webn template summary] |

manual/container/service_cluster_webn_template_summary.png

Figure 41. Web Server Template Summary Tab (EN-N)

1. Base Revision Summary shows currently loaded Revision number and Revision creation date.
2. Server Configuration Files shows file list that makes up currently loaded Revision. Content can be checked by file, and modified configuration files can be checked/compared through Compare functionality. If there are no changes, **green icon** is displayed, and if configuration files are modified, **red X icon** is displayed. Click **red X icon** to show differences between original file and modified file of loaded Revision in popup.

General

General configuration values and Connection, Process information of Web Server can be edited.

Web Server's configuration information performs Validation on configuration files when saving, minimizing Server startup failures due to configuration file errors.

When configuration file error occurs, file is not saved and error message is displayed

Error message example

```
AH00526: Syntax error on line 253  Argument for 'Require all'
must be 'granted' or 'denied'
```

Detailed contents of configuration information are as follows.

1. Server Info (/var/common_value.env file management)

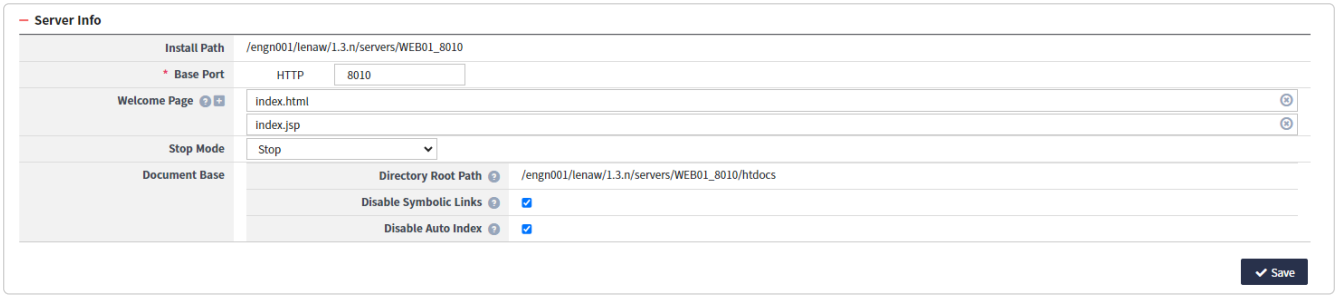


Table 113. Server Info

Item (* indicates required values)	Description	Notes
Install Path	Server installation path	
Base Port(*)	Port Type information and Port Number set during installation	Port Type cannot be changed, Port Number can be changed
Welcome Page	Define which file to use as initial page document of website	

Item (* indicates required values)	Description	Notes
Stop Mode	Server stop Mode	• Stop • Graceful Stop
Directory Root Path	Basic folder path where documents provided by Web Server are stored	
Disable Symbolic Links	Whether to not use Symbolic Link	Default : on (not used)
Diasble Auto Index	Enable or disable directory listing output.	Default : on (disabled)

2. Additional Port Info (/var/tcp_port.env file management)

[service cluster webn general portInfo] | manual/container/service_cluster_webn_general_portInfo.png

Table 114. TCP Port

Item (* indicates required values)	Description	Notes
Port Alias(*)	Set Alias of port.	
Port Number	Specify port number.	
Protocol Type	Select protocol type.	
Virtual Host ID	Display Virtual Host ID using that Port.	Cannot change Port Alias when specific Virtual Host is using that Port.

TCP Protocol dedicated usage ports (Proxy(HTTP, HTTPS), Net Gateway(TCP))

3. Connection Info (/var/common_value.env file management - related file /conf/http/lenan-http.conf)

Table 115. Connection Info

Item (* indicates required values)	Description	Notes
Send Timeout(*)	Timeout time set for sending response to client. **This is timeout time between two consecutive write operations, not total response transmission timeout time.** If client receives nothing within time specified in send_timeout, connection is closed.	Default : 60
Keep Alive Timeout(s)(*)	Timeout time set for keeping connection between server and client open.	Default : 5
Client Header Timeout(*)	Time to read request header information, if **client does not send header within specified time**, request ends with 408(Request Time-out).	Default: 60
Client Body Timeout(*)	Time to read request body information, **this is timeout time between two consecutive read operations, not total request body transmission timeout time.** If client sends nothing within time specified in client_body_timeout, request ends with 408(Request Time-out).	Default: 60

4. Process Info (/var/common_value.env file management - related file /conf/lenan.conf)

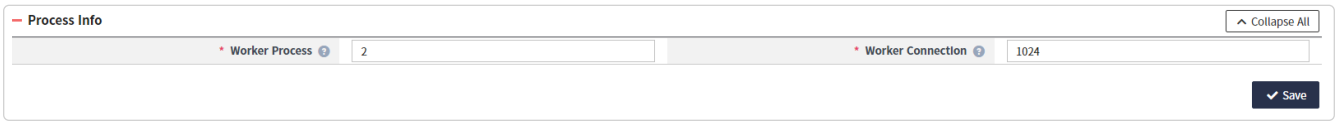


Table 116. Process Info

Item (* indicates required values)	Description	Notes
Worker Process(*)	Define number of worker processes.	Default : 2
Worker Connection(*)	Set maximum number of simultaneous connections.	Maximum Request allowance: worker_processes * worker_connections

When changing configuration, Server restart is required to reflect modified items.

5. Enable Custom (/conf/custom/custom.conf file management - related file /conf/lenan.conf)

[server 5 general enableCustom] | manual/server_5_general_enableCustom.png

Table 117. Enable Custom

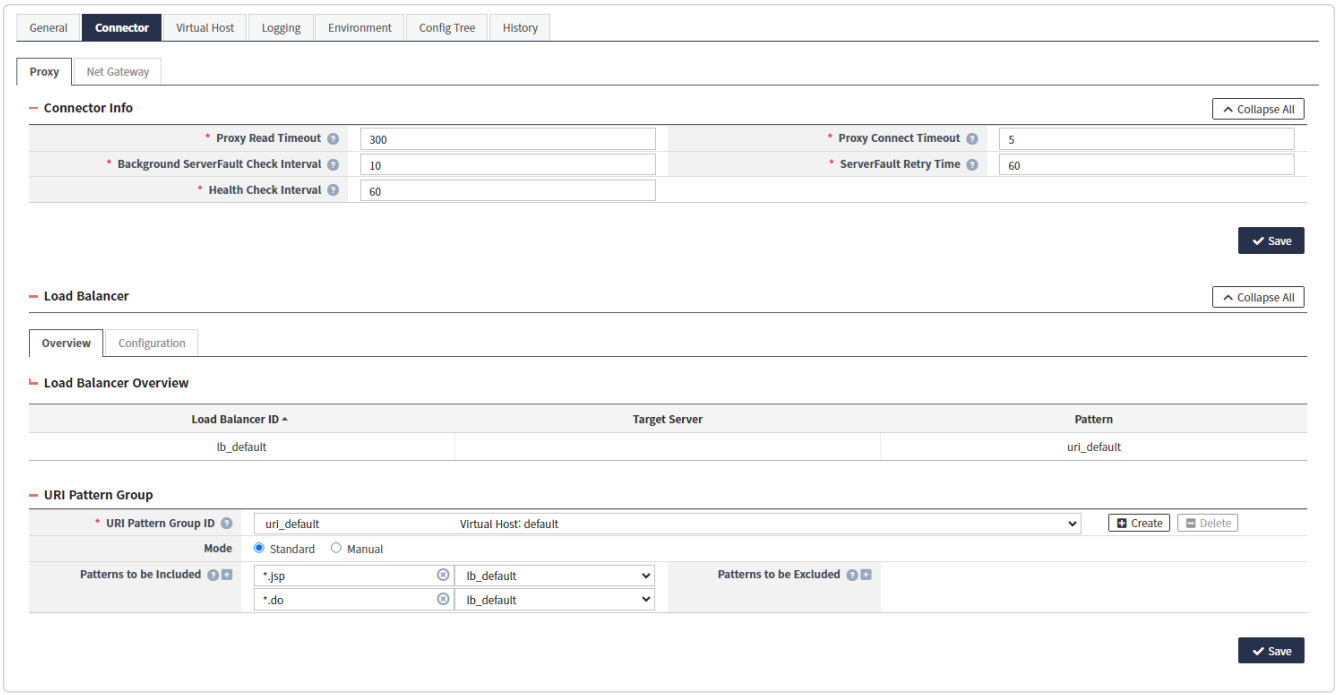
Item (* indicates required values)	Description	Notes
Custom Configuration	Input content that users can freely insert through custom.conf included in lenan.conf.	

Connector

Manages information for linking Web Server and WAS(Backend).
Connector page is divided into Proxy and Net Gateway tabs according to protocol, and Connector configuration information according to module can be edited in each tab.

Proxy

Edits configuration information when using Proxy(ngx_http_upstream_module).



Proxy tab configuration is divided into three areas: Connector Info, Load Balancer, and URI Pattern Group as shown in the above screen.

1. Connector Info
   Manages basic configuration values of Proxy.

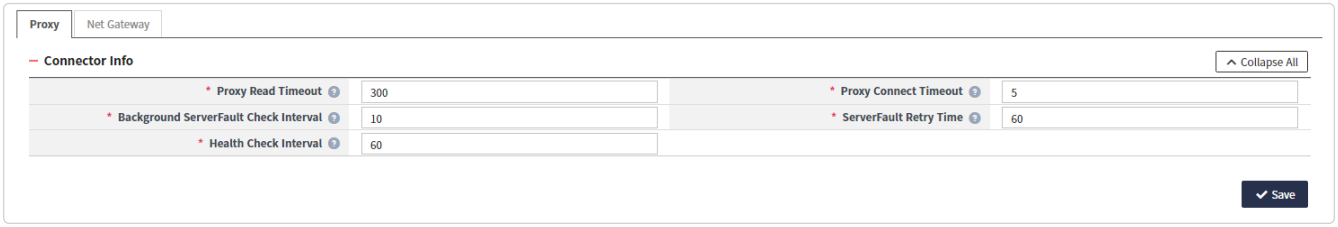


Table 118. Connector Info (Proxy)

Item (* indicates required values)	Description	Notes
Proxy Read Timeout(*)	Timeout time set for reading response from backend server. This is timeout time between two consecutive read operations, not total response transmission timeout time. If backend server sends nothing within time specified in proxy_read_timeout, connection is closed.	Default: 300
Proxy Connect Timeout(*)	Define time limit for establishing connection with backend server. This time limit generally cannot exceed 75 seconds.	Default: 5
Background ServerFault Check Interval(*)	When Member connected to backend server is in error state, checks server at interval(seconds) set in this item and retransmits requests when server operates normally. Set to 0 to disable function.	Default: 10
Server Fault Retry Time(*)	When Member connected to backend server is in error state, does not transmit any requests to that server until timeout(seconds) expires.	Default: 60
Health Check Interval(*)	Checks server at interval(seconds) set for checking backend server status. Set to 0 to disable function.	Default: 60
DNS Lookup Interval(*)	DNS lookup interval. Set to 0 to disable function.	Default: 10

When Background ServerFault Check Interval and Health Check Interval are saved as 0
All LoadBalancer's Auto Server Fault Recovery values change to off, and new creation values are also fixed to off.

2. Load Balancer
   Manages basic configuration and Members of Load Balancer for load balancing.
   Load Balancer area has Overview tab and Configuration tab. Overview tab can check overall information of currently created Load Balancer, and Configuration tab can configure detailed contents of Load Balancer.

[service cluster webn server proxy lb overview] |

manual/container/service_cluster_webn_server_proxy_lb_overview.png

Table 119. Load Balancer Info - Overview (Proxy)

Item (* indicates required values)	Description	Notes
Load Balancer ID	ID of currently created Load Balancer.	
Target Server	Basic information of Workers registered in Load Balancer. Displayed as Service Endpoint.	
Pattern	When Load Balancer is specified for specific URI Pattern, URI Pattern Group ID that the URI Pattern belongs to is displayed.	

[service cluster webn server proxy lb config] |

manual/container/service_cluster_webn_server_proxy_lb_config.png

Table 120. Load Balancer Info - Configuration (Proxy)

Item (* indicates required values)	Description	Notes
Load Balancer ID(*)	Name of Load Balancer.	'lb_' prefix is added.
Method(*)	Specifies method used by Load Balancer to determine appropriate Worker for load balancing.	
* Sticky Session : Route based on Session Cookie	* RoundRobin : Route in order of registered members	• IP Hash : Route based on Client's IP
* Least Connection : Route to side with fewer connections	Session Cookie(*)	Set when wanting to change Session Cookie name.
Default: JSESSIONID	Timeout Retry	Set when wanting to change Session Cookie name.
Default:Off When On is set, retransmits when Gateway Timeout occurs.	Auto Server Fault Recovery	Whether to use fox Directive

Members are added with Add Member button in Load Balancer MemberList table.
When Add Member button is pressed, window for adding Member is displayed on screen, and users can select servers managed by LENA Manager as Members in this window. Added Members are managed through following information.

Table 121. Load Balancer Member List

Item (* indicates required values)	Description	Notes
Target Server	Service Endpoint that Member points to.	
Route ID	Route ID of Member	
Weight	Work allocation ratio, defines how much work this Worker will do compared to other Workers.	Default: 1

3. URI Pattern Group
   Defines URI Mapping to pass requests coming to Web Server to WAS by checking URI patterns.

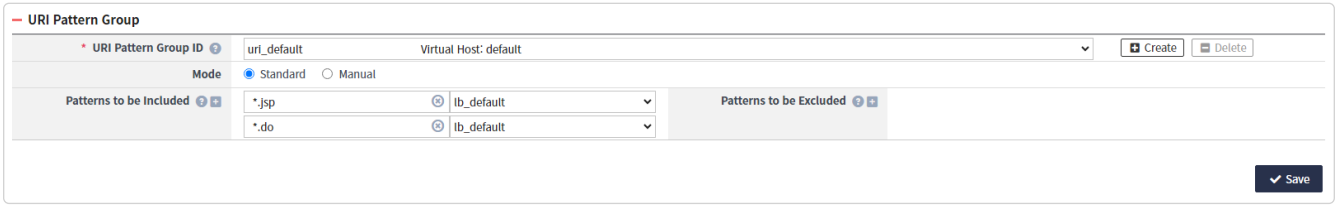


Table 122. URI Pattern Group (Proxy)

Item (* indicates required values)	Description	Notes
URI Pattern Group ID(*)	Name used for grouping and managing URI patterns. When URI Pattern Group used in Virtual Host, information about which Virtual Host is using it is displayed next to ID.	Group creation adds 'uri_' prefix.
Mode	Specifies whether to input URI patterns in format managed by LENA Manager or in user arbitrary format. Screen for inputting Patterns to be Included/Excluded or URI Patterns is displayed according to this item. If already saved pattern is in format managed by LENA Manager, it is automatically set to Standard, if in user arbitrary format, it is automatically set to Manual.	• Standard: Input method according to LENA Manager URI Rule • Manual: User arbitrary input method
Patterns to be Included	Input URI patterns to pass to WAS. Must select Load Balancer through right Select box to save. Can delete patterns through button.	Asterisk(*) meaning to allow all characters can be used, Hash(#), Equal(=) are not allowed.
Patterns to be Excluded	Input URI patterns not to pass to WAS. Can delete patterns through button.	Asterisk(*) meaning to allow all characters can be used.
URI Patterns	Used when inputting user arbitrary patterns.	

4. Enable Custom /conf/http/custom/custom_http.conf file management - related file /conf/http/lenan-http.conf)

[server 5 web server proxy enable custom] | manual/server_5_web_server_proxy_enable_custom.png

Table 123. Enable Custom (Proxy)

Item (* indicates required values)	Description	Notes
Custom Configuration	Input content that users can freely insert through custom_http.conf included in lenan-http.conf.	

When changing configuration, Server restart is required to reflect modified items

Virtual Host

Proxy

Proxy Web Server's Virtual Host information can be registered/modified/deleted.

New button, **Delete button** can register/delete Virtual Host.

Virtual Hosts with one or more Load Balancers applied cannot be deleted. If you want to delete that Virtual Host, first change Virtual Host ID of Load Balancer to different Virtual Host ID through Connector tab.

When Enable SSL and Enable Rewrite and Enable Custom are checked, detailed item areas are additionally displayed.

[service cluster webn server proxy vhost] |

manual/container/service_cluster_webn_server_proxy_vhost.png

Detailed contents of configuration information are as follows.

Managed files

- /conf/http/vhost/vhost_{Virtual Host ID}.conf
- /conf/http/vhost/vhost.list
- /conf/http/vhost/rewrite/rewrite_{Virtual Host ID}.conf
- /conf/http/vhost/custom/custom_{Virtual Host ID}.conf

Table 124. Virtual Host Info Configuration Information

Item (* indicates required values)	Description	Notes
Virtual Host ID(*)	Virtual Host name	
Domain Name	Domain name to identify virtual host	
IP(*)	Select protocol to be used by that virtual host (HTTP, HTTPS) IP used by that virtual host	
Port(*)	Port used by that virtual host	
SSL Enable	Whether to additionally use SSL, HTTPS service port to be used by that virtual host	When checked, need to use port from combo box for HTTPS service port (port information to use must be pre-registered as HTTPS port in General tab's Port Info)
SSL/SSLCertificateFile	SSL certificate path	
SSL/SSLCertificateKeyFile	SSL certificate Key file path	
SSL/SSLPassword	SSL Password	When password is input, managed through AES256 encryption
SSL/Use HTTPS Redirect	Whether to use HttpHttps Redirect	

Item (* indicates required values)	Description	Notes
Document base/Directory Root Path	Homepage directory location of that virtual host	Can be specified to same or subdirectory using Server's DocumentRoot variable ${DOC_ROOT}
Document base/Disable Symbolic Links	Prevent accessing file system other than existing web documents under Document Root via symbolic links	
Document base/Disable Auto Index	Prevent showing file list under Document Root when welcome page cannot be found	
Document base/Allowed Methods	Allow access for specified http methods	
Document base/Deny IP	Deny access for specified networks or addresses	
Access Log/Alias	Set format for recording logs in log file	
Access Log/Location	Set location and name for log files	
URI	Select URI Pattern Group set in Connector Proxy Tab	Not required selection
Enable Rewrite	Whether to use Rewrite function, creates input window below when checked	Input content is generated and stored in separate file
Enable Custom	Whether to use Custom Configuration, creates input window below when checked	Input content is generated and stored in separate file (/conf/http/vhost/custom/custom_default.conf)

Logging

Web Server's log configuration information can be edited.

[service cluster webn server log] | manual/container/service_cluster_webn_server_log.png

Detailed contents of configuration information are as follows.

1. Error Log

Used when Web Server records errors that occur while processing diagnostic information and

requests. When problems occur during Server startup or operation, check files at location set here first.

Table 125. Error Log

Item (* indicates required values)	Description	Notes
Location(file/pipe)(*)	Specify Web Server's error log file location	
Log Level(*)	Specify how detailed to record error log file contents	

2. Log Format : Proxy

Sets format to use for Proxy log files.

Table 126. Log Format : Proxy

Item (* indicates required values)	Description	Notes
Alias(*)	Name of log format to use	
Format(*)	Sets format for recording logs in log file	

When changing configuration, New Revision creation and Server restart are required to reflect modified items

Environment

Provides screen for managing JVM options, Start Shell configuration, etc. Modify through file editor and click **Save button** to save.

- Custom Env (/bin/customenv.sh): User custom environment variable configuration
- Base Env (/env.sh) - Shell Script for Server startup

By default, configuration cannot be modified. If you want to modify, click **Configuration button** in ADMIN > Manager Environment > Manager Configuration item and change the following configuration to false.

```
server.environment.envshell.readonly=false
```

Configuration Tree

Web Server's ${SERVER_HOME}/conf directory sub configuration files can be managed through file editor.

User must have access permission to Web Server configuration information files for modification. If access permission is not available, message that file cannot be edited due to no Write permission is displayed.

Hook

Allows execution of user-defined Shell Script before Web Server startup and after shutdown in Container.

- Start Hook Script : This Script is executed before starting Web Server during Container startup.
- Stop Hook Script : This Script is executed after stopping Web Server during Container shutdown.

Revision Creation

Click **New Revision button** in Template tab to create new Revision. Modify WAS, WEB server configuration files through tabs at bottom of System Template Overview and click Save to temporarily save. After all configuration file modifications are complete, click New Revision button to create new Revision and generate Template compressed file. Created Revision can be checked in Revision tab.

Even after modifying and saving WAS, WEB server configuration files, if new Revision is not created, screen returns to Default Revision when re-entering.

Configuration

Click **Configuration button** in Template tab to display configuration screen.

[service cluster webn template config] | manual/container/service_cluster_webn_template_config.png

Figure 42. Web Server Template Configuration Popup

Default Revision and Include Files to be included in Template compressed file can be specified. Basic file list for Template configuration is automatically generated, and users can add desired files. Only files with Apply checkbox activated are included in Template compressed file.

Export

For detailed content related to Export, refer to Export in this document.

Copy Configurations

For detailed content related to User Guide, refer to Copy Configurations in this document.

5.2.8. Embedded WAS Configuration Management

Embedded WAS sets Server configuration in Application internal files. For Spring Boot based Applications, default configuration is done in application.properties file or application.yml file. LENA configuration should also be set in those files.

Embedded WAS requires dependency to be added to Spring Boot Application to be usable. For example, when using maven, declare as follows in pom.xml.

```
<dependency>
    <groupId>lena</groupId>
    <artifactId>spring-boot-starter-lena</artifactId>
    <version>1.3.1.4</version>
</dependency>
```

Embedded WAS Overview

Overview content refers to Service Cluster Overview.

Server List

For Embedded WAS, some items are displayed differently in Server List.

Item	Description	Notes
Profile	Application's Profile	
Note icon	Query Audit configuration, MBean Attributes, System Properties of that Instance	

Embedded WAS Configuration

Basically, Embedded WAS configuration information is inside each Application. Configuration information managed by Manager is not items directly applied to Applications with Embedded WAS. 'Application Properties' can be used when separating configuration information from deployment package, and 'Audit' helps easily apply WAS event collection settings to Applications.

Application Properties

When separating Application's environment configuration information from deployment package, Spring Cloud Config can be used to read and apply configuration information from remote server. LENA Manager acts as Spring Cloud Config Server to read configuration files uploaded to Git Repository and deliver to Applications. LENA Manager can specify Git Repository by Application&Profile unit.

Item	Description	Notes
Profile	Application's Profile	
Application Name	Application Name. Same as Service Cluster Name. Must input according to {Application Name}-{Profile} pattern since it's retrieved from Git Repository.	
Type	Remote type to receive configuration information.	Currently only Git is supported.
defaultLabel	Git branch name	default: master
URI	Git URI	
username	Username for Git Repository authentication.	Required depending on authentication method.
password	Password for Git Repository authentication.	Required depending on authentication method.

Item	Description	Notes
ignoreLocalSshSettings	Whether to set SSH configuration using JAVA properties when accessing Local SSH configuration files is difficult.	default: false
hostKey	Host key of Git repository server, should not include algorithm prefix included in host-key-algorithm.	
hostKeyAlgorithm	Host key algorithm should be ssh-dss, ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 or ecdsa-sha2-nistp521 (required only when host-key exists)	
strictHostKeyChecking	Whether Config server instance fails to start when using private host-key.	default: true
privateKey	privateKey for git repository authentication.	
knownHostsFile	Input location of .known_hosts file.	
preferredAuthentications	Override server authentication method order.	

Applications must configure whether to use Spring Cloud Config functionality. (Default setting value is not used.) Must input usage and manager information in boostrap.properties (or yml).

```
server.lena.config.enabled=true
server.lena.config.uri=http://Manager address/lena-embed-manager/config
spring.application.name=
```

spring.application.name, LENA Manager's Application Name, and file pattern stored in Git Repository must match to read configuration files.

Audit

Screen for configuring WAS event collection. Adding configuration information to Application's startup options allows collected event information to be checked in Event Dashboard. For Event Dashboard related content, refer to Event Dashboard.
For event configuration content, refer to Audit. Click **Generate button** to display configuration information script in popup window. Click **Copy to Clipboard button** to easily add to JVM Option. Click **Download oom.sh button** to download execution script file that delivers OOM information to Manager when OOM occurs.

For StuckThread event Valve configuration, refer to Valve Configuration.

oom.sh file can be downloaded as oom.bat file when OS is WINDOWS.
After placing downloaded oom.sh file in specific location, write -XX:OnOutOfMemoryError=.
Refer to [JVM-Option-Setting].

Encryption

Functionality to encrypt information that should not be exposed externally in Application configuration files (application.properties, application.yml, etc.).

Item	Description	Notes
Use Provided Key	Encryption/Decryption Key	TRUE:LENA provided Key
ENcrypt Target String	Plain Text to encrypt	
Key	Encryption/Decryption Key	Activated when Use Provided Key is false
Encrypt Result	Encryption result	Value changes each time Encrypt button is pressed

Configuration method

```
jasypt.encryptor.bean=lenaStringEncryptor
jasypt.encryptor.password=ENC(Os3OQ2CdW0M5xGf9pfdklT2Ce2vj4ti+S1pgI3Rr4B8=)
```

Put Encrypt Result value inside ENC() of jasypt.encryptor.password and start.

Check Configuration

Pre-defines conditional expressions for WAS Configuration Properties values and displays alarm when started WAS does not meet those conditions.

Item	Description	Notes
Name	Name	
Key	Key value to compare	Example) server.lena.stuckThread.threadhold
Value	Reference value	
Condition	Condition	
Description	Description	

```
 When Key value contains dashes, modify to CamelCase and write. +
When started WAS does not meet above conditions, exclamation mark(!) alarm
appears in ETC-INFO item at bottom of Overview tab's ServerList and
clicking exclamation mark allows checking which values did not meet
conditions.
```

Embedded WAS Configuration Items

Spring Boot's Server configuration is as follows.
https://docs.spring.io/spring-boot/docs/current/reference/html/appendix-application-properties.html#common-application-properties-server

Embedded WAS can use Server configuration provided by Spring Boot as is.
However, Spring Boot's tomcat configuration must be changed to lena for use.
ex) Use server.lena.accesslog.enabled= true instead of server.tomcat.accesslog.enabled= true.

Connector Configuration

Additional connector attribute items configurable in LENA are as follows.

Item	Default Value	Description
server.lena.connector.max-cookie-count	200	Maximum number of Cookies allowed in Request
server.lena.connector.max-parameter-count	10000	Maximum number of parameters that can be automatically parsed. Parameter values exceeding this limit are ignored. Negative values mean no limit
server.lena.connector.max-post-size	2097152	Maximum size of POST to be processed by Form URL parameter parsing (Byte)
server.lena.connector.uri-encoding	UTF-8	URI Encoding method
server.lena.connector.use-body-encoding-for-uri	false	Whether to use encoding specified in 'content-type' for URI query parameters instead of uriEncoding

Session Clustering Configuration

Session Clustering using LENA Session Server is configured as follows.

Item	Default Value	Description
server.lena.session.enabled	false	Whether to use Session Clustering with LENA Session Server
server.lena.session.config-file		File path when setting session clustering configuration in separate conf file.
server.lena.session.primary-host		LENA Session Server's Host(Primary)
server.lena.session.primary-port		LENA Session Server's Port(Primary)
server.lena.session.secondary-host		LENA Session Server's Host(Secondary)
server.lena.session.secondary-port		LENA Session Server's Port(Secondary)

Valve Configuration

LENA basically has LenaStuckThreadDetectionValve configured. Default configuration is threshold = 600, interruptThreadThreshold = -1. To change, modify as follows.

Item	Default Value	Description
server.lena.stuckThread.threshold	600	Minimum execution time(sec) for Thread to be considered Stuck. Setting to 0 disables.
server.lena.stuckThread.interruptThreadThreshold	-1	Minimum execution time for releasing StuckThread (release not guaranteed). Setting to -1 disables. Must be larger than threshold value to use this functionality.

When additional Valve is needed in LENA, it's possible with following configuration. Valve and Valve's attributes must be declared as arrays.

Item	Default Value	Description
server.lena.valve.className		Valve's ClassName (including package)
server.lena.valve.attribute.name		Valve's attribute name
server.lena.valve.attribute.value		Valve's attribute value

Valve configuration example is as follows.

```
server.lena.valve[0].className=org.apache.catalina.valves.StuckThreadDetection
Valve
server.lena.valve[0].attribute[0].name=threshold
server.lena.valve[0].attribute[0].value=100
server.lena.valve[0].attribute[1].name=interruptThreadThreshold
server.lena.valve[0].attribute[1].value=10
```

Existing Application's Port information was defined as server.port.
For management convenience in Embedded LENA, define in startup options.
-Dspring.application.json={"server.port":8080}
In this case, even if server.port is defined in application.properties, priority causes startup with port value defined in startup options.

Startup Configuration

When building and starting Spring Boot Application as jar, following configuration is needed to use Management functionality through LENA Manager.
LENA's Docker Base Image Build method is checked through [Embedded-WAS-Deploy].

- Prepare agent library and conf file
  : Agent library and environment configuration conf file are needed to send monitoring information to LENA Manager.
  Prepare lena-advertiser-1.3.1c.jar file and advertiser.conf file in specific location.
  Basic configuration of advertiser.conf can be modified as follows.

```
# Manager Server address
advertiser.server.addr=127.0.0.1

# Manager Server UDP Port (value entered during Manager Server installation)
advertiser.server.port=16100

# Service Cluster Name.
container.group.name=ApplicationName

# Whether to make TCP connection with Manager (set true if wanting to generate
ThreadDump remotely through Manager)
advertiser.enable.reverse.tcp.connection=true
```

- JVM Option Configuration
  : Library and conf file paths and service port information must be added to JAVA Option during startup.
  To check monitoring information, also change mbean configuration to true by default.
  Following script can be used for easy configuration.

```
#!/bin/sh

# Environment variables for LENA Manager integration
export AGENT_LIB_HOME= # lena-advertiser.jar file path
export AGENT_CONF_HOME= # advertiser.conf file path
export HTTP_PORT= # application service port
export PROFILE=
export
SPRING_OPTION="{\"server.port\":\"\",\"spring.datasource.hikari.register-
mbeans\":true,\"spring.jmx.enabled\":true,\"server.lena.mbeanregistry.enabled\
":true}"
export LENA_VERSION=1.3.1c
export BIN_DIR= # oom.sh file path (oom event option)

# Some options that must be added per project. Must be modified according to
project.
export JVM_HEAP_SIZE=
export JVM_METASPACE_SIZE=
export DUMP_OUTPUT_DIR=
export LOG_OUTPUT_DIR=
export HOSTNAME=LCSKVM06827

# JVM_Option value configuration for LENA Manager integration (required)
JVM_OPTS="-javaagent:/lena-advertiser-.jar"
JVM_OPTS=" -Dport.http="
JVM_OPTS=" -Dlena.config=/advertiser.conf"
JVM_OPTS=" -Dspring.application.json="
JVM_OPTS="
```

```
-
Dspring.profiles.active=C:\Users\76882\Documents\WindowsPowerShell\Microsoft.P
owerShell_profile.ps1"
JVM_OPTS=" -Dlena.name=LENA_Application"

# Event configuration (value created in Manager)
JVM_OPTS=" -XX:+HeapDumpOnOutOfMemoryError"
JVM_OPTS=" -XX:HeapDumpPath=/hdump"
JVM_OPTS=" -Devent.oom.enable=true"
JVM_OPTS=" -Devent.stuckthread.enable=true"
JVM_OPTS=" -Devent.fullgc.enable=false"
JVM_OPTS=" -Devent.exception.enable=false"
JVM_OPTS=" -Devent.exception.pattern="
JVM_OPTS=" -Devent.exception.exclude.pattern="
JVM_OPTS=" -Devent.exception.fullstack.enable=true"
JVM_OPTS=" -Devent.exception.fullstack.maxline=3"

# Additional configuration (set according to project)
JVM_OPTS=" -Xmsm -Xmxm"
JVM_OPTS=" -XX:MaxMetaspaceSize=m"
JVM_OPTS=" -XX:+UseParallelGC"
JVM_OPTS=" -XX:+UseParallelOldGC"
JVM_OPTS=" -XX:-UseAdaptiveSizePolicy"
JVM_OPTS=" -XX:+ExplicitGCInvokesConcurrent"
JVM_OPTS=" -Xloggc:/gc_embeddedServer_.log"
JVM_OPTS=" -verbose:gc"
JVM_OPTS=" -XX:+PrintGCDetails"
JVM_OPTS=" -XX:+PrintGCDateStamps"


# Startup method should also be changed according to project.
(XX:OnOutOfMemoryError configuration is needed to collect oom event.)
java -jar  \
-XX:OnOutOfMemoryError="/oom.sh %p /lena-advertiser-.jar /advertiser.conf
/hdump  true" \
application.jar
```

Chapter 6. Resource

6.1. Database

When you select Database from the left menu, the Database Resource list is displayed.

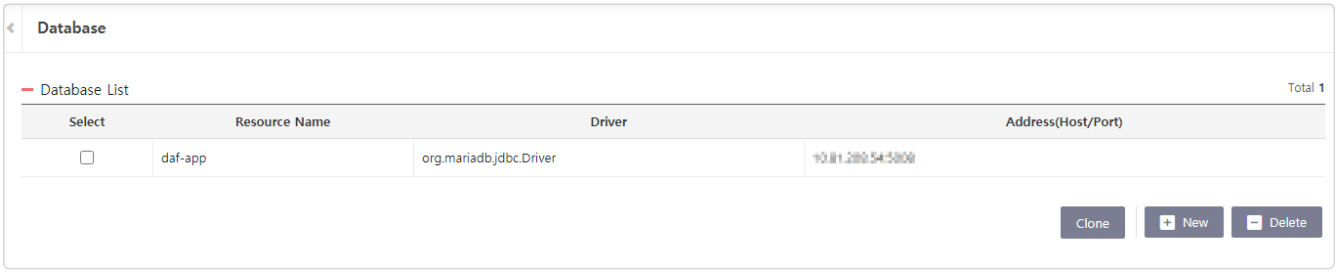


Figure 43. Database List Screen

6.1.1. Database Registration

1. Click the **New button** in the Database Resource list to display the new registration screen.
2. Enter the input fields.
   - Enter the Resource Name.
   - Check the DriverClassName and select the driver for your desired vendor.
   - Enter the Address (host/Port) information.
3. Click the **Save button** to save.

6.1.2. Database Modification

1. Select the checkbox of the Database Resource you want to modify from the Database Resource list.
2. Modify the Database Resource items and save.

When content is modified, it propagates to the DataSource Resource and WAS configuration connected to that Database Resource, so if there are DataSource Resources connected under that Database Resource, the input fields are disabled by default. Click the **Edit button** to enable modification.

6.2. DataSource

When you select DataSource from the left menu, the DataSource Resource list is displayed.

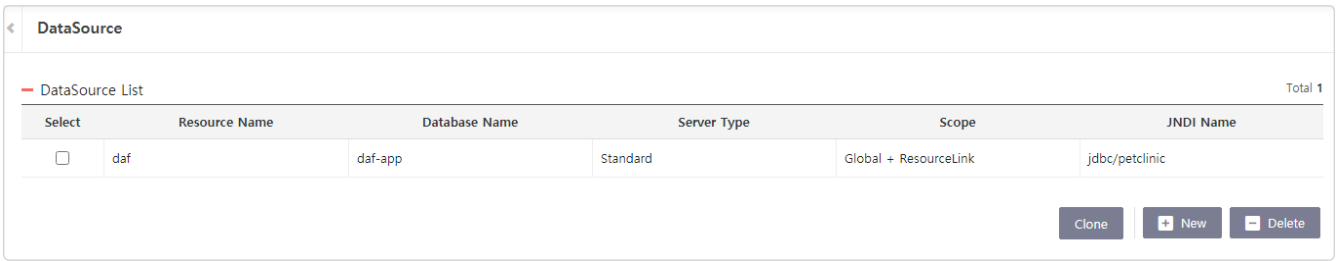


Figure 44. DataSource List Screen

6.2.1. DataSource Registration

1. Click the **New button** in the DataSource Resource list to display the new registration screen.
2. Enter a logical name in the Resource Name field.
3. Set the Server Type. Server Type must be selected from Standard or Enterprise, and thereafter it can only be imported and used on servers of the same type.
4. Configure the detailed settings for DataSource (refer to the detailed item descriptions in [Server DataSource Settings])
5. Click the **Upload button** to register the Driver for that DataSource on the Manager server. Pre-registered Drivers are transmitted to the corresponding server when operators import them to the server.
6. Click the **Save button** to save.

JDBC Drivers uploaded to the Manager are transmitted to the corresponding server when operators import that DataSource Resource to the server. Transmitted JDBC Drivers are located in the {server home path}/lib/datasource directory and are automatically registered in the Classpath.

6.2.2. DataSource Modification

1. When you select a row you want to modify from the DataSource Resource list, the DataSource Resource modification screen is displayed.
2. Change the configuration you want to modify.
3. Click the **Save button** to save.

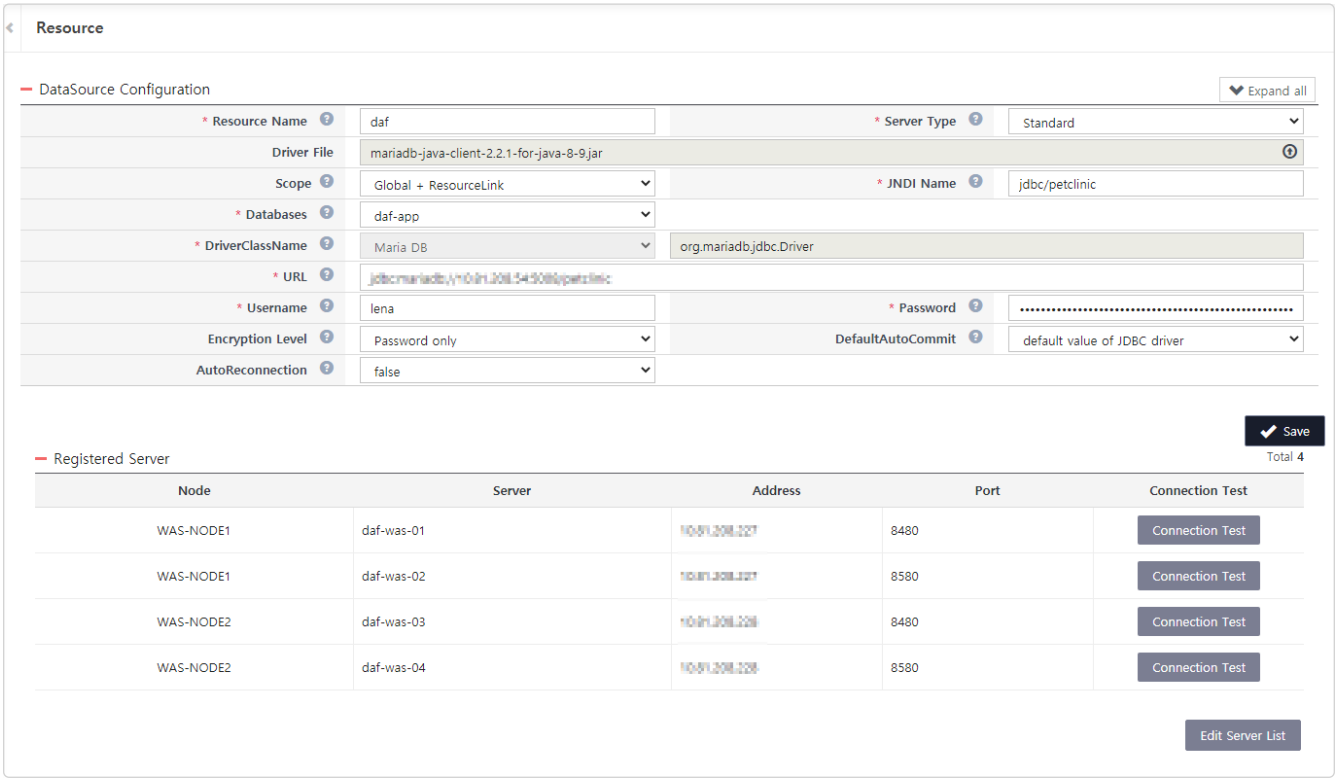


Figure 45. DataSource Detail Information Screen

When you save after modifying DataSource Resource information, the changed configuration propagates to the server where that DataSource Resource is used. When you restart the server where the configuration has propagated, that configuration is applied.

After importing a DataSource Resource set to Standard Type to a Standard server, the Server Type cannot be changed to Enterprise.

Note that when deleting a DataSource Resource after Classpath registration, the Classpath is not deleted.

6.2.3. DataSource Deletion

1. Select the checkbox of the DataSource Resource you want to delete from the DataSource Resource list.
2. Click the **Delete button** to delete.

If there are Registered Servers or Registered Applications that have imported from the Server or Application, that DataSource Resource cannot be deleted.

6.2.4. JDBC Driver Upload

1. Click the **Upload button** in the DataSource Resource registration or edit screen to display a screen where you can upload Driver Files.
2. Click the **File Selection button** to select the Driver File you want to upload from your local PC.
3. Click the **Upload button** to upload the Driver File to the Manager.

6.2.5. DataSource Import

The list of Servers using the created DataSource Resource by importing it (when Scope is Context, Global, Global + Link) or the list of Applications (when Scope is Application) is displayed in the lower area when viewing DataSource Resource details.

Importing DataSource from DataSource Detail Screen

DataSource Resources with Scope Context, Global, or Global + Link can register servers that import them.

1. In the DataSource management screen, select a specific DataSource Resource to navigate to the detail information screen.
2. Click the **Edit Server List button** to display a window where you can register and manage servers.
3. Specify the server to import that DataSource and move it to the right area.
4. Click the **Save button** to import the DataSource Resource to that server.

To delete an imported DataSource Resource from a server, move the target server to the left area and click the **Save button**.

Importing DataSource from Individual Server

1. Select the Servers menu from the top of LENA Manager.
2. Click on the left side: Individual Web Application Server > Resources > DataSource tab to display a screen where you can view the DataSource Resource list for that server and add DataSource Resources.
3. Click the **Import button** to display a list of predefined DataSource Resources in a popup window.
4. Select the DataSource Resource you want to import.
5. Click the **OK button** to import that DataSource Resource.

When you import a DataSource Resource, connection information between that DataSource Resource and the server is internally created. Based on this connection information, configuration updates are delivered to that server when the DataSource Resource is modified.

Standard Servers cannot import Enterprise Type DataSource Resources. (They are not displayed in the list)

Imported DataSource Resource settings cannot be edited in Server settings. (Configuration information can be viewed but not modified) To change the configuration, go to the Resource > DataSource screen to make changes.

6.3. JTA

When you select JTA from the left menu, the JTA Resource list is displayed.

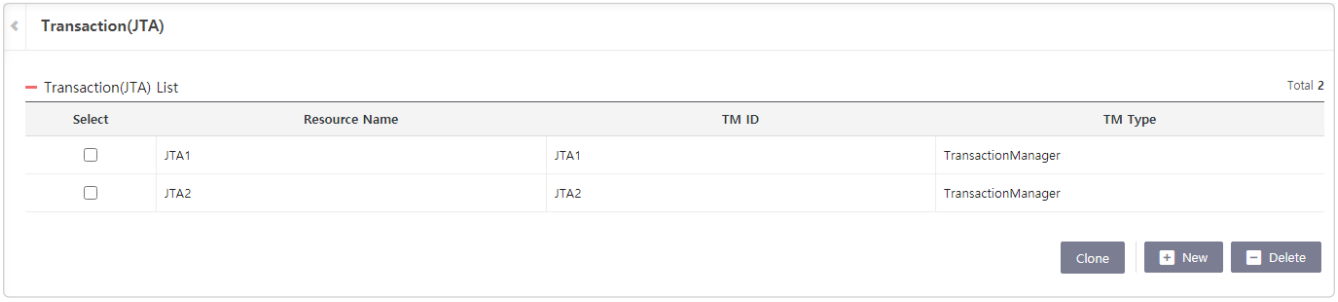


Figure 46. JTA List Screen

6.3.1. JTA Registration

1. Click the **New button** in the JTA list to display the new registration screen.
2. Enter the values you want to configure. (For detailed settings, refer to "4.3.7 Server Configuration Information Management")
3. Click the **Save button** to save.

6.3.2. JTA Modification

1. When you select a row you want to modify from the JTA Resource list, the modification screen is displayed.
2. Enter the configuration you want to change.
3. Click the **Save button** to save.

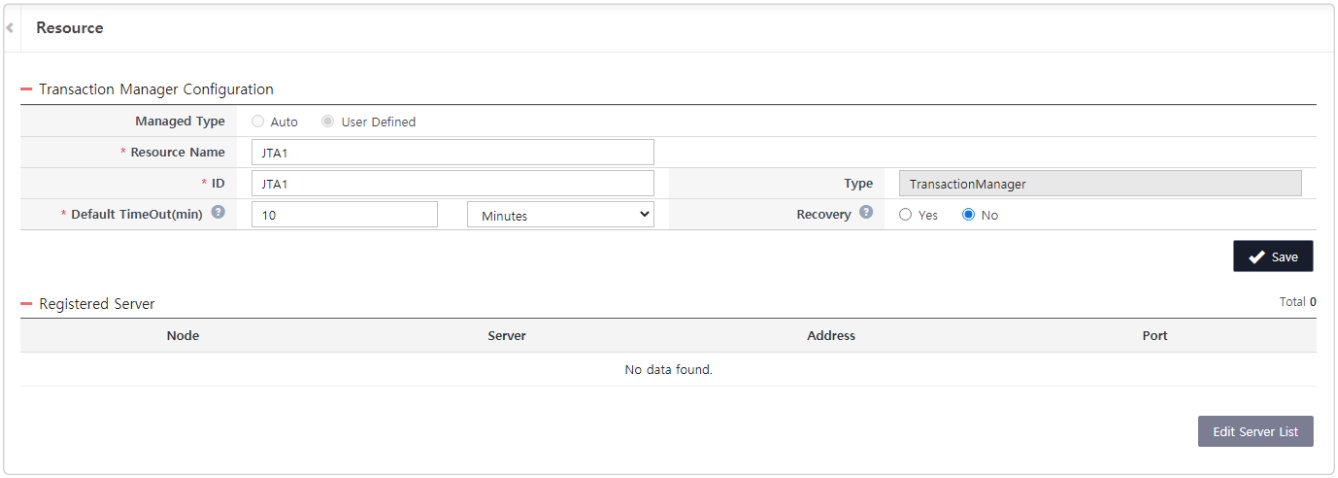


Figure 47. JTA Detail Information Screen

When you save after modifying JTA Resource information, the changed configuration propagates to the server where that JTA Resource is used. When you restart the server where the configuration has propagated, that configuration is applied.

6.3.3. JTA Deletion

1. Select the checkbox of the JTA Resource you want to delete from the JTA list.
2. Click the **Delete button** to delete.

If there are Registered Servers that have imported from the server, that JTA Resource cannot be deleted.

6.3.4. JTA Import

The list of servers using the created JTA Resource by importing it is displayed in the lower area when viewing JTA Resource details.

Importing JTA from JTA Detail Screen

In the JTA detail screen, you can modify the list of servers that are importing and using it.

1. In the JTA management screen, select a specific JTA Resource to navigate to the detail information screen.
2. Click the **Edit Server List button** to display a window where you can register and manage servers.
3. Specify the server to import that JTA Resource and move it to the right area.
4. Click the **Save button** to import the JTA Resource to that server.

To delete an imported JTA Resource from a server, move the target server to the left area and click the **Save button**.

Importing JTA from Individual Server

1. Select the Servers menu from the top of LENA Manager.
2. Click on the left side: Individual Web Application Server > Resources > JTA tab to display a screen where you can view the JTA Resource list for that server and add JTA Resources.
3. Click the **Import button** to display a list of predefined JTA Resources in a popup window.

4. Select the JTA Resource you want to import.
5. Click the **OK button** to import that JTA Resource.

When you import a JTA Resource, connection information between that JTA Resource and the server is internally created. Based on this connection information, configuration updates are delivered to that server when the JTA Resource is modified. Connection information can be viewed in the Resource > JTA screen.

Imported JTA Resource settings cannot be edited in server settings. (Configuration information can be viewed but not modified) To change the configuration, go to the Resource > JTA screen to make changes.

6.4. JMS

When you select JMS from the left menu, the JMS Resource list is displayed.

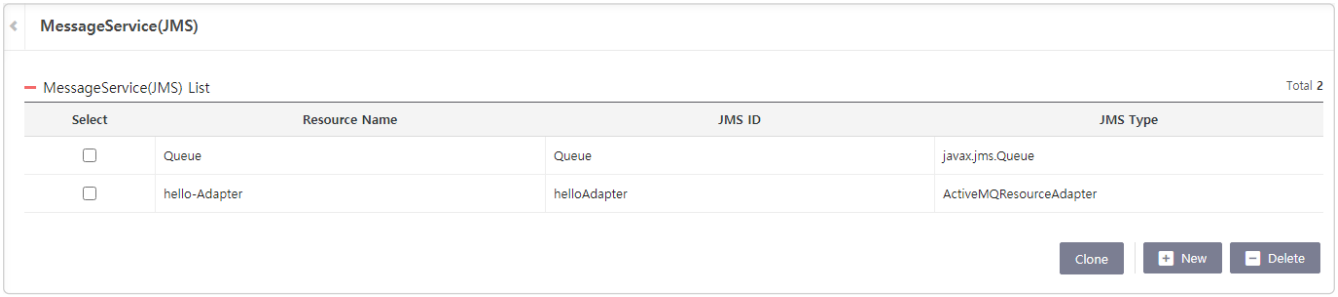


Figure 48. JMS List Screen

6.4.1. JMS Registration

1. Click the **New button** in the JMS list to display the new registration screen.
2. When you select the type of JMS Resource to register, configuration information appropriate for the selected type is displayed below.
3. Enter the values you want to configure. (For detailed settings, refer to "4.3.7 Server Configuration Information Management")
4. Click the **Save button** to save.

6.4.2. JMS Modification

1. When you select a row you want to modify from the JMS Resource list, the modification screen is displayed.
2. Enter the configuration you want to change.
3. Click the **Save button** to save.

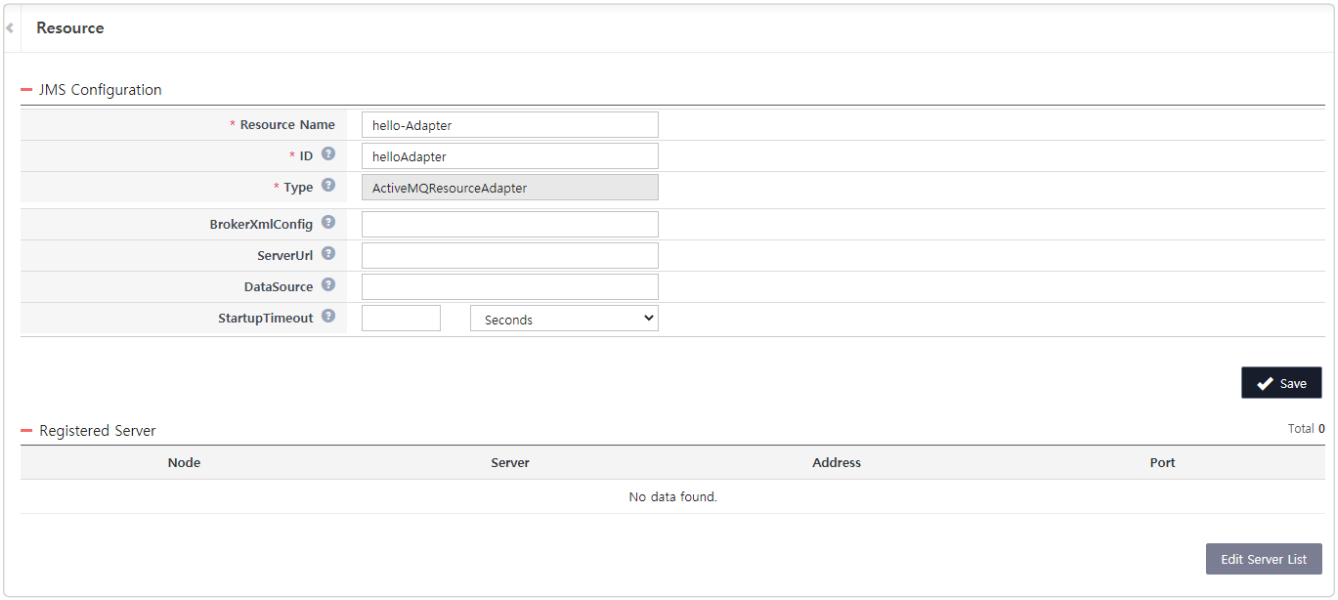


Figure 49. JMS Detail Information Screen

When you save after modifying JMS Resource information, the changed configuration propagates to the server where that JMS Resource is used. When you restart the server where the configuration has propagated, that configuration is applied.

6.4.3. JMS Deletion

1. Select the checkbox of the JMS Resource you want to delete from the JMS list.
2. Click the **Delete button** to delete.

If there are Registered Servers that have imported from the server, that JMS Resource cannot be deleted.

6.4.4. JMS Import

The list of servers using the created JMS Resource by importing it is displayed in the lower area when viewing JMS Resource details.

Importing JMS from JMS Detail Screen

In the JMS detail screen, you can modify the list of servers that are importing and using it.

1. In the JMS management screen, select a specific JMS Resource to navigate to the detail information screen.
2. Click the **Edit Server List button** to display a window where you can register and manage servers.
3. Specify the server to import that JMS and move it to the right area.
4. Click the **Save button** to import the JMS Resource to that server.

To delete an imported JMS Resource from a server, move the target server to the left area and click the **Save button**.

Importing JMS from Individual Server

1. Select the Servers menu from the top of LENA Manager.
2. Click on the left side: Individual Web Application Server > Resources > JMS tab to display a screen where you can view the JMS Resource list for that server and add JMS Resources.
3. Click the **Import button** to display a list of predefined JMS Resources in a popup window.
4. Select the JMS Resource you want to import.
5. Click the **OK button** to import that JMS Resource.

When you import a JMS Resource, connection information between that JMS Resource and the server is internally created. Based on this connection information, configuration updates are delivered to that server when the JMS Resource is modified. Connection information can be viewed in the Resource > JMS screen.

Imported JMS Resource settings cannot be edited in server settings. (Configuration information can be viewed but not modified) To change the configuration, go to the Resource > JMS screen to make changes.

6.5. Application

When you select Application from the left menu, the Application Resource list is displayed.

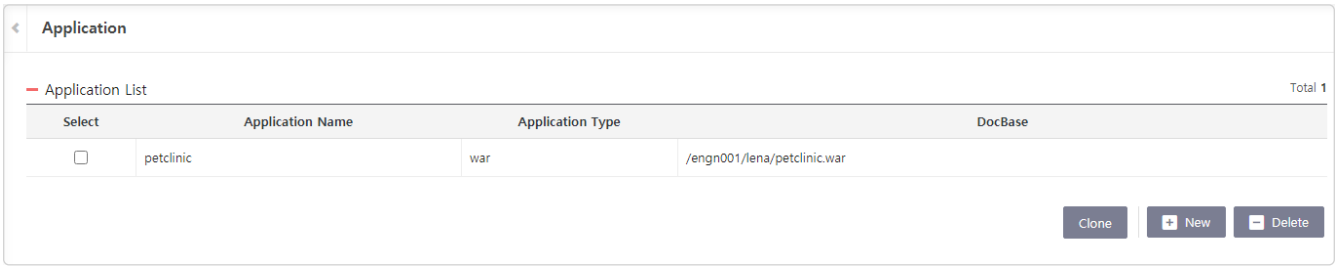


Figure 50. Application List Screen

6.5.1. Application Registration

1. Click the **New button** in the Application list to display the new registration screen.
2. Enter the values you want to configure.
   - If Application Type is WAR, additional configurable items are displayed. (For detailed settings, refer to Application Settings)
3. Click the **Save button** to save.

6.5.2. Application Modification

1. When you select a row you want to modify from the Application Resource list, the modification screen is displayed.
2. Enter the configuration you want to change.
3. Click the **Save button** to save.

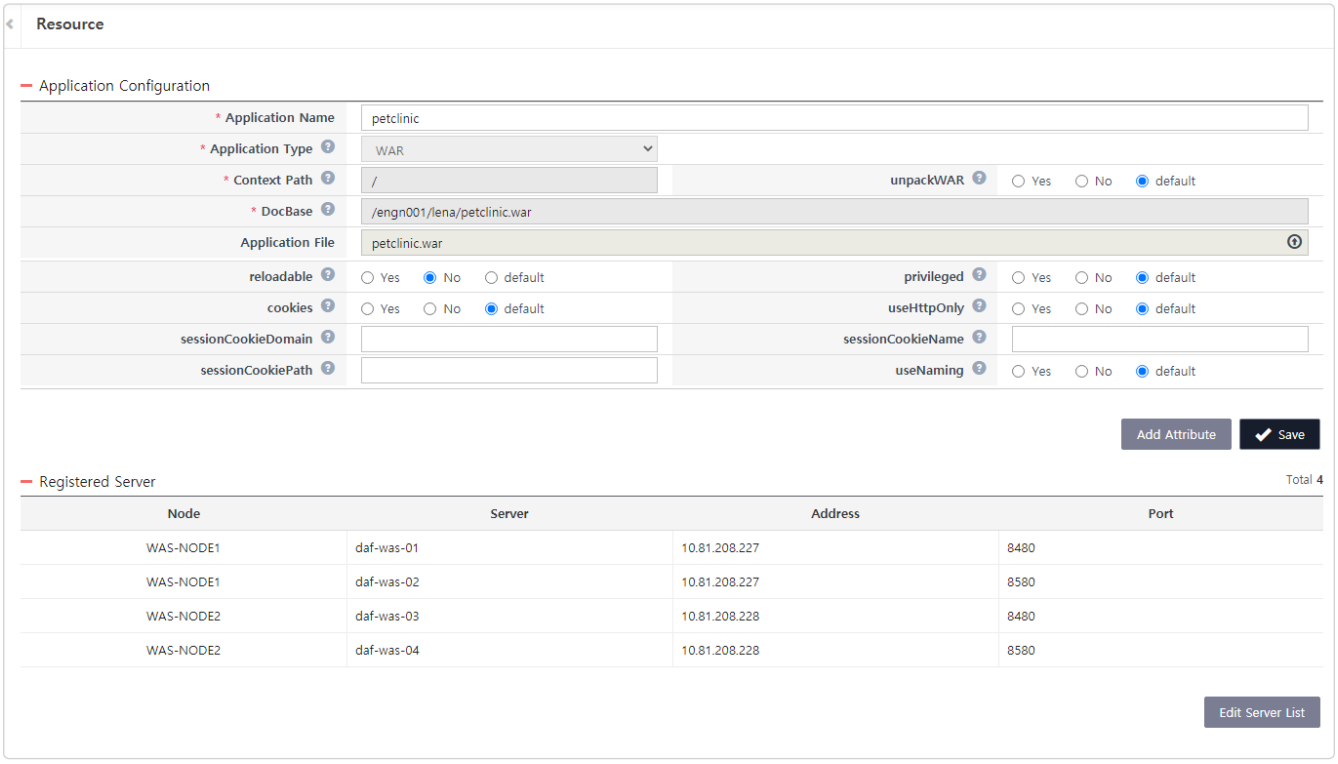


Figure 51. Application Detail Information Screen

When you save after modifying Application Resource information, the changed configuration propagates to the Server where that Resource is used. The Server where the configuration has propagated will apply that configuration when restarted.

6.5.3. Application Deletion

1. Select the checkbox of the Application Resource you want to delete from the Application list.
2. Click the **Delete button** to delete.

If there are Registered Servers that have imported from the Server, that Application Resource cannot be deleted.

6.5.4. Application Upload

1. Click the **Upload button** in the Application Resource registration or edit screen to display a screen where you can upload Application Files.
2. Click the **File Selection button** to select the Application File you want to upload from your local PC.
3. Click the **Upload button** to upload the Application File to the Manager.

Application Import

The list of Servers that are using the created Application Resource by importing it is displayed in the lower area of the Application Resource detail view.

Importing Application from Application Detail Screen

In the Application detail screen, you can modify the list of Servers that are importing and using it.

1. In the Application management screen, select a specific Application Resource to navigate to the

detail information screen.

2. Click the **Edit Server List button** to display a window where you can register and manage Servers.
3. Specify the Server to import that Application and move it to the right area.
4. Click the **Save button** to import the Application Resource to that Server.

To delete an imported Application Resource from a Server, move the target Server to the left area and click the **Save button**.

Importing Application from Individual Server

1. Select the Servers menu from the top of LENA Manager.
2. Click on the left side: Individual Web Application Server > Applications menu to display a screen where you can view the Application Resource list for that Server and add Application Resources.
3. Click the **Import button** to display a list of predefined Application Resources in a popup window.
4. Select the Application Resource you want to import.
5. Click the **OK button** to import that Application Resource.

When you import an Application Resource, connection information between that Application Resource and the Server is internally created. Based on this connection information, configuration updates are delivered to that Server when the Application Resource is modified. Connection information can be viewed in the Resource > Application screen.

Imported Application Resource settings cannot be edited in Server settings. (Configuration information can be viewed but not modified) To change the configuration, go to the Resource > Application screen to make changes.

6.6. k8s Config

6.6.1. k8s Config Registration

1. Click on k8s Config and click the **New button** to display the new registration screen as shown below.

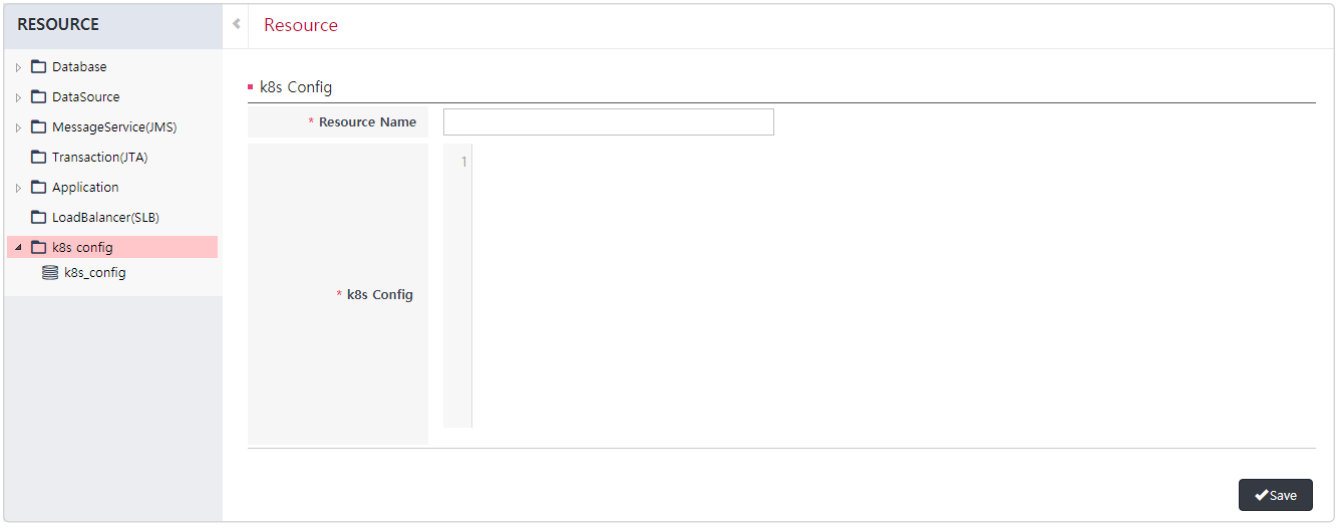


Figure 52. k8s Config Registration Screen

2. Enter the Resource Name.
3. Copy the kubernetes cluster config file content to k8s Config and save.

After setting up k8s Config, each Service Cluster can share and use it. When using Log / Terminal functionality in Service Cluster, the API is called by referencing the information entered above.

6.6.2. k8s Config Modification

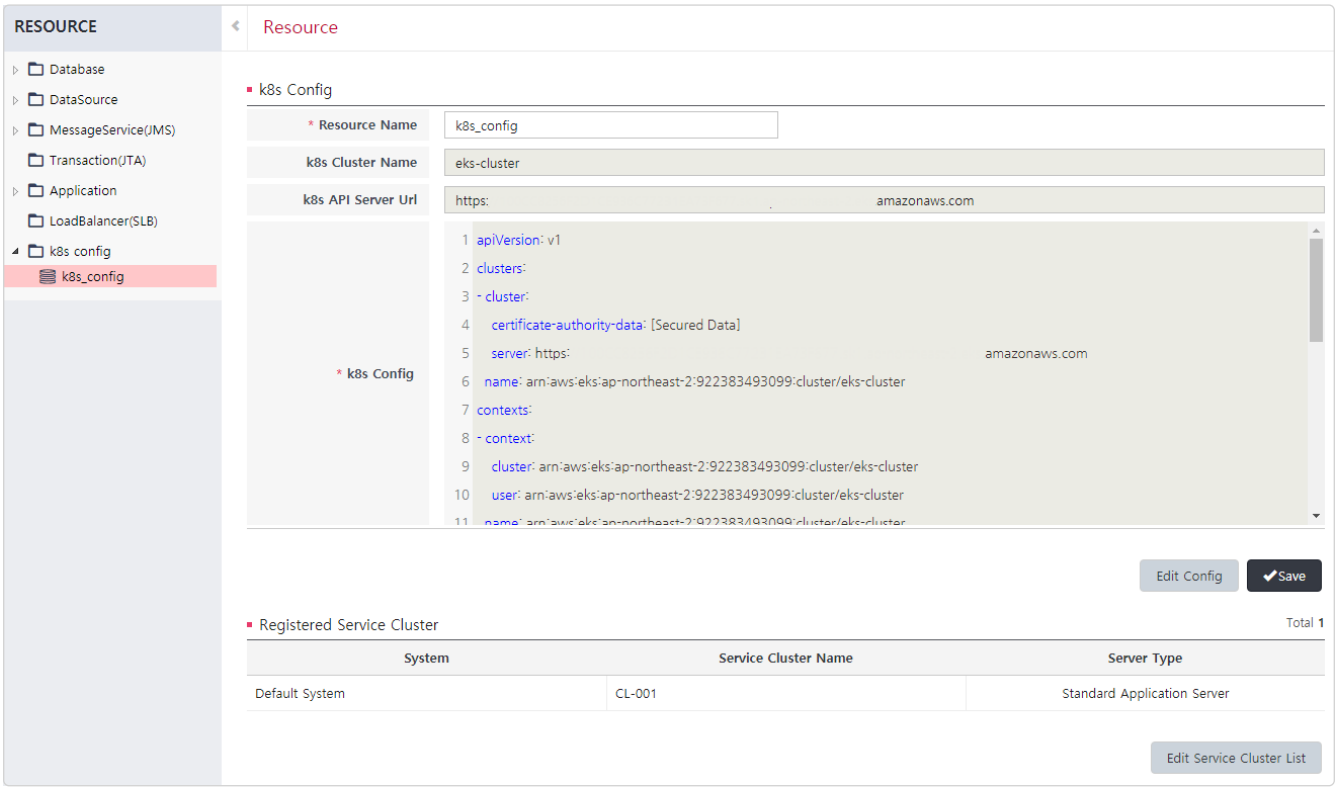


Figure 53. k8s Config Modification Screen

1. Modify the Resource Name and k8s Config content and save.
2. Click the **Edit Configuration button** to modify the k8s Config content.
3. Click the **Edit Service Cluster List button** in Registered Service Cluster to modify the list of Service Clusters mapped to k8s Config.

6.6.3. k8s Config Deletion

1. Click on k8s Config and check the Resource List.
2. Check the k8s Config you want to delete in Select, then click the **Delete button** to delete. If there are Service Clusters mapped to k8s Config, deletion is not possible.

6.6.4. k8s Config Clone

1. Click on k8s Config and check the Resource List. Select the item and click the **Clone button** to clone the k8s Config.
2. Enter values to register a new k8s Config.

Chapter 7. Diagnostics

7.1. Monitoring Dashboard

7.1.1. Status Summary

The Monitoring Dashboard screen provides 3 tabs at the bottom, and the summary information provided at the top changes according to the selected tab.

The information provided by each tab is as follows.

Node Tab

Provides Server monitoring information by registered Node

Server Cluster Tab

Provides Server monitoring information by Server Cluster group

Service Cluster Tab

Provides Container monitoring information by Service Cluster group

You can set the query cycle for each piece of information, and for WAS, clicking the **popup button** in the Function column allows you to navigate to the detailed monitoring screen.

The Monitoring Dashboard screen is as follows.

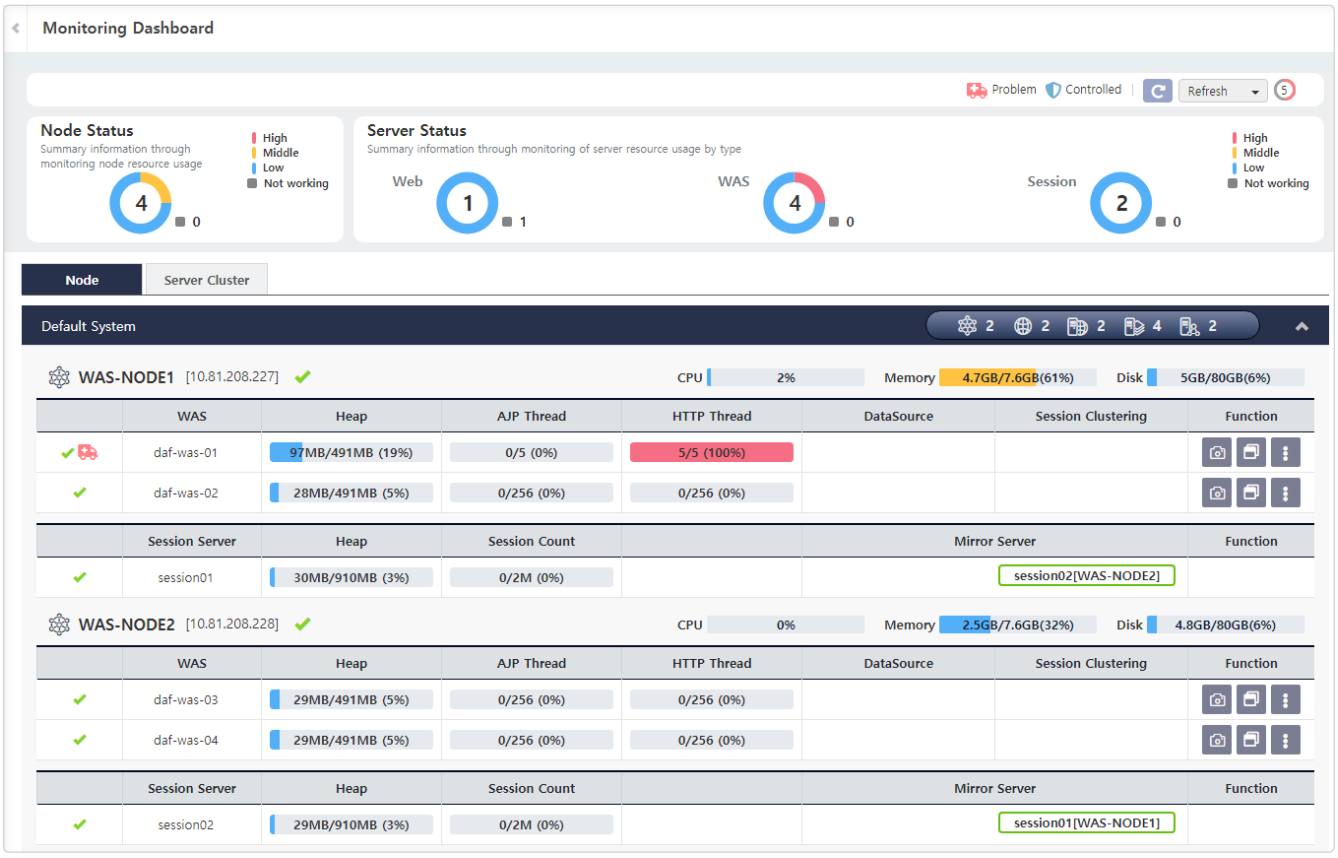


Figure 54. Monitoring Dashboard Node Tab Screen (1/2)

[diagnostics monitoring dashboard node tab mcr] |

manual/diagnostics_monitoring_dashboard_node_tab_mcr.png

Figure 55. Monitoring Dashboard Node Tab Screen (2/2)

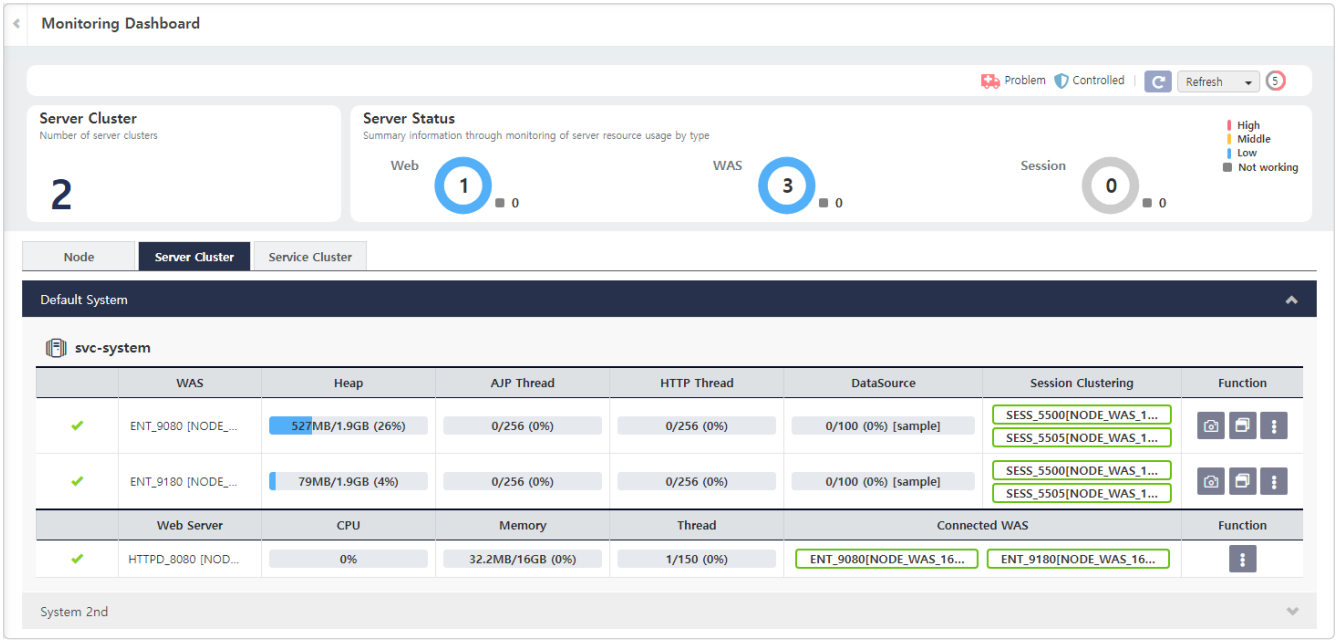


Figure 56. Monitoring Dashboard Server Cluster Tab Screen

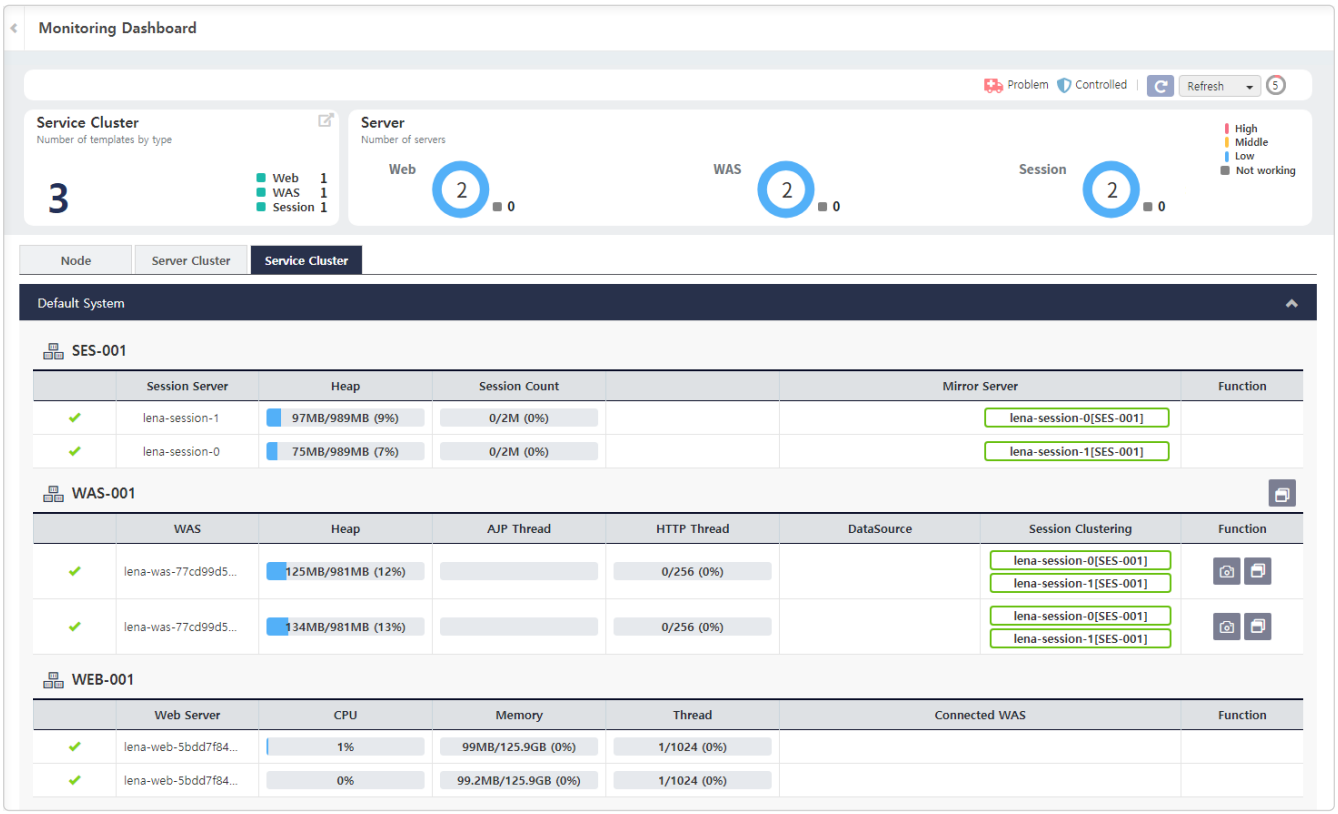


Figure 57. Monitoring Dashboard Service Cluster Tab Screen

The Service Cluster tab is a functionality provided in the Container Edition.

The attributes used in the Monitoring Dashboard screen are as follows. The colors of information provided in usage form can be changed using the Status Range attribute. (Refer to the monitoring basic settings subsection of this chapter)

Table 127. Node Status

Item	Description	Notes
CPU	Node CPU usage	Default setting is Low when below 60%, High when 80% or above.
Memory	Node Memory usage	Default setting is Low when below 60%, High when 80% or above.
Disk	Node Disk usage	This is the usage of the Disk where the Engine is installed, with default setting being Low when below 60%, High when 80% or above.

Table 128. Application Server Status

Item	Description	Notes
Status	Server start status, diagnostic result issuance status (**ambulance icon**), and automatic response execution status (**shield icon**)	Unknown status is displayed when server status cannot be retrieved through Node Agent
Server Name	Server name	
Heap Memory	Heap Memory usage used in Application Server	
Thread Pool	Displays Request Thread usage managed by Application Server as a Pool by Connector (Ajp, Http)	
DataSource	Datasource Connection usage rate managed by Application Server as a Pool	
Session Clustering	Information about Session Server configured in Application Server and start status	Red means stopped state, green means running state, black means server existing outside the system

Table 129. Web Server Status

Item	Description	Notes
Status	Server start status	Unknown status is displayed when server status cannot be retrieved through Node Agent
Server Name	Server name	
CPU	Web Server process CPU usage	
Memory	Web Server process Memory usage	

Item	Description	Notes
Thread	Web Server Thread count (Active / Max)	
Connected WAS	Information about WAS connected to Web Server and start status	Red means stopped state, green means running state, black means server existing outside the system

Table 130. Session Server Status

Item	Description	Notes
Status	Server start status	Unknown status is displayed when server status cannot be retrieved through Node Agent
Server Name	Server name	
Heap	Heap Memory usage used in Session Server	
Session Count	Ratio of active Sessions	
Mirror Server	Information about Mirror Server and start status	Red means stopped state, green means running state, black means server existing outside the system

Table 131. Memory Cache Server Status

Item	Description	Notes
Status	Server start status, diagnostic result issuance status (**ambulance icon**), and automatic response execution status (**shield icon**)	Unknown status is displayed when server status cannot be retrieved through Node Agent
Server Name	Server name	
CPU	CPU usage used in the server	
Memory	Memory usage used in the server	
Connection	Number of Connections currently connected from clients	
Replicas	Replicas connected to the server	

The following functionality is provided together to immediately control each server.

Table 132. Application Server Control Functions

Item	Description	Notes
Thread Dump	Generate Thread Dump	**Left button (Server Snapshot(dump))** > Select Dump List menu > Dump file can be downloaded
Active Service Dump	Create Active Service Dump	**Left button (Server Snapshot(dump))** > Select Dump List menu > Download Dump file
Heap Dump	Create Heap Dump	**Left button (Server Snapshot(dump))** > Select Dump List menu > Download Dump file
Forced Stop	Force server to stop	Forced to stop immediately without waiting
Forced Restart	Force server to restart	Forced to restart immediately without waiting
All Diagnostics Disable	Disable all diagnostic/response functions applied to the server	

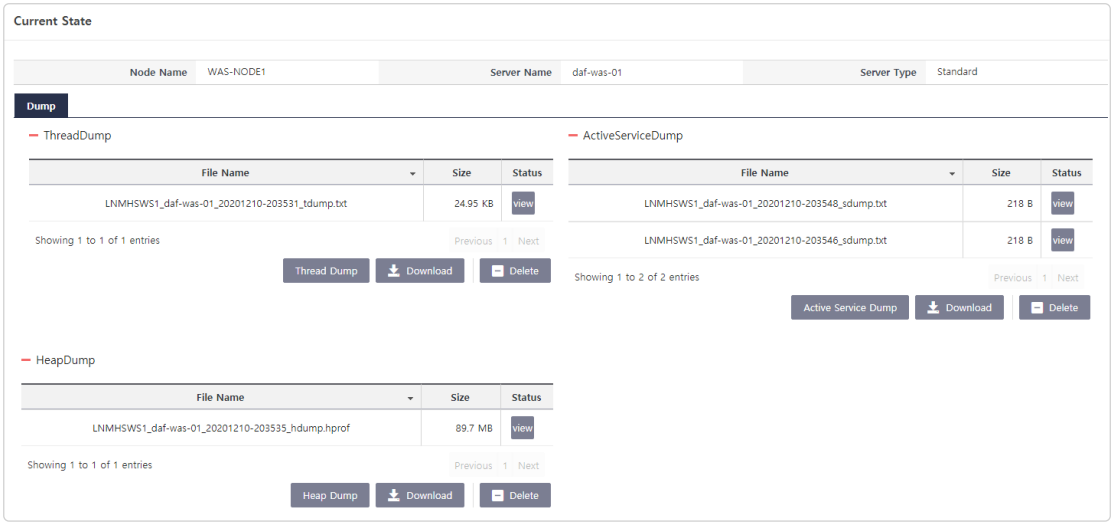


Figure 58. Dump window

You can generate and download Heap Dump, Thread Dump, Active Service Dump. Generally, Dump is generated to investigate the cause of errors such as Out Of Memory in the server, excessive use of Thread Pool, or service delay.

Depending on the Dump type you want to generate, click **Thread Dump button** , **Active Service Dump button** , **Heap Dump button** to generate Dump. Generated Dump is stored in the Host where Web Application Server exists, Thread Dump in {log_home}/logs/tdump, Active Service Dump in {log_home}/logs/sdump, HeapDump file in {log_home}/logs/hdump path.

Delete button can be clicked to delete Dump files. **Download button** can be clicked to download Dump files, and when downloading, the corresponding Dump file is also downloaded in zip format together with the system status Dump file.

The items in the Dump management screen are as follows.

Table 133. Dump screen items

Item	Description	Notes
File Name	Generated file name	Automatically generated with date string
Size	Size of generated file	
Status	System and Server status at the time of Dump execution	System's CPU, Memory information and key resource usage information of Web Application Server are also generated together at the time of Dump generation. **View button** can be clicked to check the generated Status value.

Table 134. Web Server Control Functions

Item	Description	Notes
Forced Stop	Server forced shutdown	No waiting time, immediate forced shutdown
Graceful Stop	Server graceful shutdown	

If Monitoring information is not displayed, check if the registered Node/Server actually exists and if communication with Node/Server is in a good state.

Table 135. Memory Cache Server Control Functions

Item	Description	Notes
Start	Server start	
Stop	Server shutdown	

7.1.2. Detailed Status Monitoring

When you select **the middle button (View Detail Chart)** in the Function column of the Monitoring Dashboard, you can monitor detailed Thread, Memory, and service information.

System Window

You can check Memory, Thread, and Service information of Web Application Server.

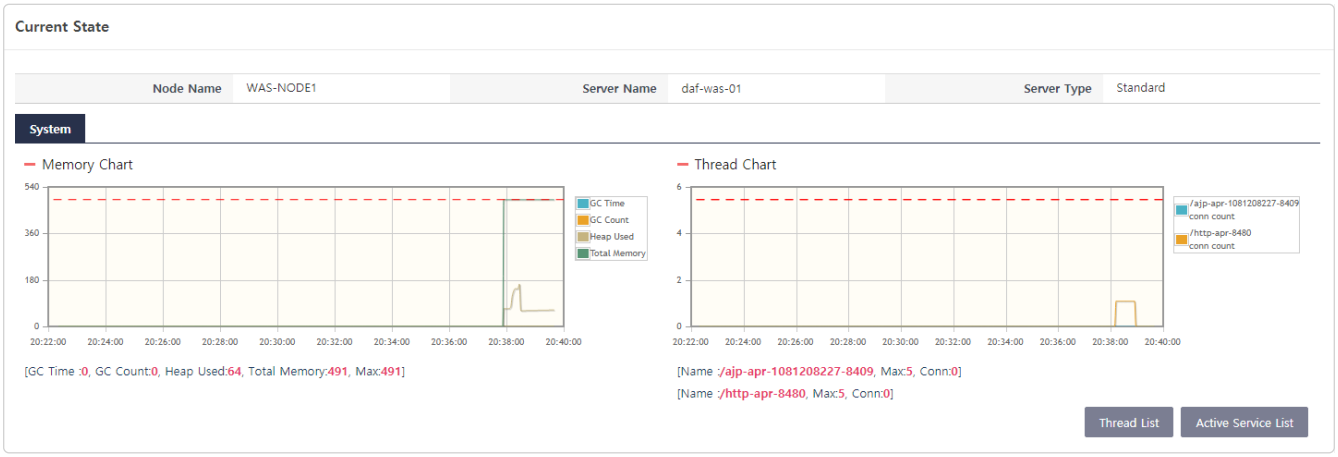


Figure 59. System Tab

Memory Chart

Real-time Memory usage information is displayed. The information provided includes GC Time (Garbage Collection time), GC Count, Heap Used (Total Memory - Free Memory), Total Memory (total memory used on the server), and Peak Memory (maximum memory used). The red dotted line in the chart means the maximum available Heap Memory. Therefore, if the chart shows Heap Memory usage for a long time continuously close to the red dotted line, it should be noted.

The maximum value of Request Thread can be changed through the maxThreads property of the corresponding Web Application Server in the Server menu.

Thread Chart

It is a Line Chart showing the usage of Request Thread managed by Web Application Server for processing user requests. The red dotted line in the chart means the maximum available Request Thread. Therefore, if the chart shows Request Thread count close to the red dotted line, it should be noted.

The maximum value of Request Thread can be changed through the maxThreads property of the corresponding Web Application Server in the Server menu.

Thread List

You can check all Threads of Web Application Server. You can filter based on the Thread name or Thread status. The items in the Thread List are as follows.

Table 136. Thread List Items

Item	Description	Notes
Thread ID	Unique Thread ID	
Name	Thread name	
Stat	Thread status	There are three states in total • RUNNABLE: Available Thread • WAITING: Thread waiting for a specific Action from another Thread • TIMED_WAITING: Thread with a specified waiting time
CPU	CPU usage for the specified Thread	
Elapsed	Time taken for the Thread to execute	
Service Name	Service name executed by the Thread	

+ button can be clicked to view detailed information as follows.

Table 137. Thread detailed information items

Item	Description	Notes
threadId	Unique Thread ID	
threadName	Thread name	

Item	Description	Notes
state	Thread status	There are three states in total • RUNNABLE: Available Thread • WAITING: Thread waiting for a specific Action from another Thread • TIMED_WAITING: Thread with a specified waiting time
threadCpuTime	CPU time for the current Thread and all Threads	
threadUserTime	CPU time for the current Thread	
blockedCount	Total blocked	
blockedTime	Accumulated blocked time	
waitedCount	Total waited Threads	
waitedTime	Accumulated waited time	
lockOwnerId	ID of the Thread owning the locked Object	
lockName	Name of the locked Object	
lockOwnerName	Name of the Thread owning the locked Object	
stackTrace	stackTrace	

Active Service List

You can check service information and Thread information for the service that is currently processing. The items in the Active Service List are similar to those in the Thread List, with the following additional items.

Table 138. Active Service List Items

Item	Description	Notes
Sql	Current SQL statement being executed	

DataSource Window

You can check DataSource information configured in Application Server.

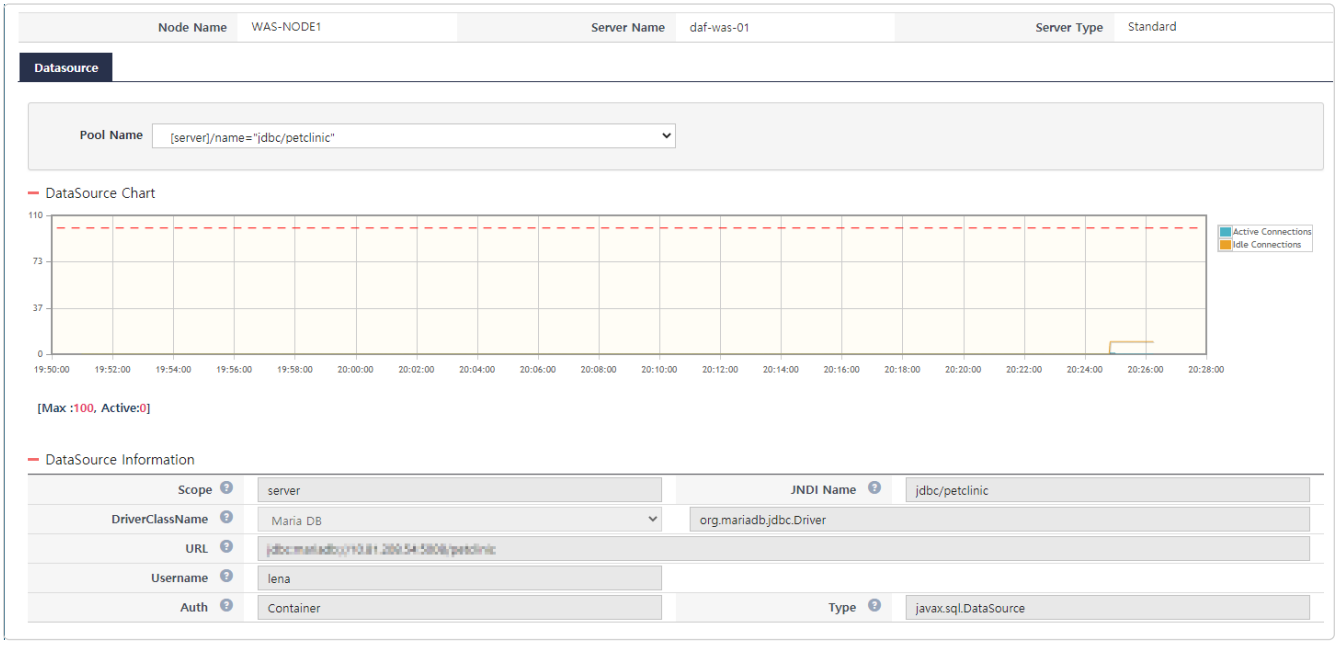


Figure 60. DataSource Tab Screen

DataSource Chart

Active Connection count and Idle Connection count are displayed in real-time in the chart. The red dotted line in the chart means the maximum set Connection count. When Active Connections are close to the red dotted line, it should be noted. You can select DataSource in the combo box to monitor other DataSources.

The maximum Connection count can be changed through the maxConnection property in the DataSource registration screen.

DataSource Information

You can check the configured settings of the specified Datasource.

7.1.3. Memory Cache Server

When you select **the left button (System)** in the Function column of the Monitoring Dashboard, you can monitor detailed service information.

System Window

You can check Memory, CPU, and Service information of Memory Cache Server.

[diagnostics memory cache system 01] | manual/diagnostics_memory_cache_system_01.png

[diagnostics memory cache system 02] | manual/diagnostics_memory_cache_system_02.png

CPU Chart

You can check CPU usage of Memory Cache Server over time.

Command Processing

You can monitor CPU usage of commands that Memory Cache Server is processing in real-time.

Memory Chart

You can check Memory usage of Memory Cache Server over time. The items that can be monitored for Memory include Peak Memory (maximum memory used), Max Memory (maximum available memory), current memory usage, physical memory (RSS Memory), and physical memory usage relative to actual memory (RSS Ratio).

Network Input/Output

You can monitor Network packet size that enters and leaves Memory Cache Server in real-time.

Hit Ratio

It shows the success rate of data retrieval commands requested by clients.

Key

You can check the total number of Keys for each DB in Memory Cache Server, and you can check the number of keys evicted and the time of the last eviction.

Connected Client

You can check the number of Connections currently connected to clients over time, and you can also monitor the maximum number of simultaneous Connections and the number of Rejected Connections.

Connected Client List

By clicking the Retrieve button, you can find the list of currently connected Clients, the last successful command, the time taken, Idle time, etc.

Slog Log

You can view commands executed beyond the pre-defined time.

7.1.4. Monitoring Settings

You can set monitoring basic settings in the DIAGNOSTICS > Policy > Common Rule Setting menu. The settings are as follows.

Table 139. Monitoring related basic settings items

Item	Description	Default Value
Status Range	Sets the Low, Middle, High criteria for Resources in the Monitoring Dashboard.	60% or less means Low, 60% or more means Middle, 80% or more means High.
Diagnostics Interval	Sets the diagnostic cycle.	10000(ms)
Dump Limit	Limits the number of Dumps (Thread/ActiveService/Heap) per server directory (0 means unlimited)	200(items)

7.2. Analysis Dashboard

The Analysis Dashboard provides real-time failure analysis status information by system unit. The types of information provided are as follows.

- Performance Map
- Analysis Summary
- Instance Map

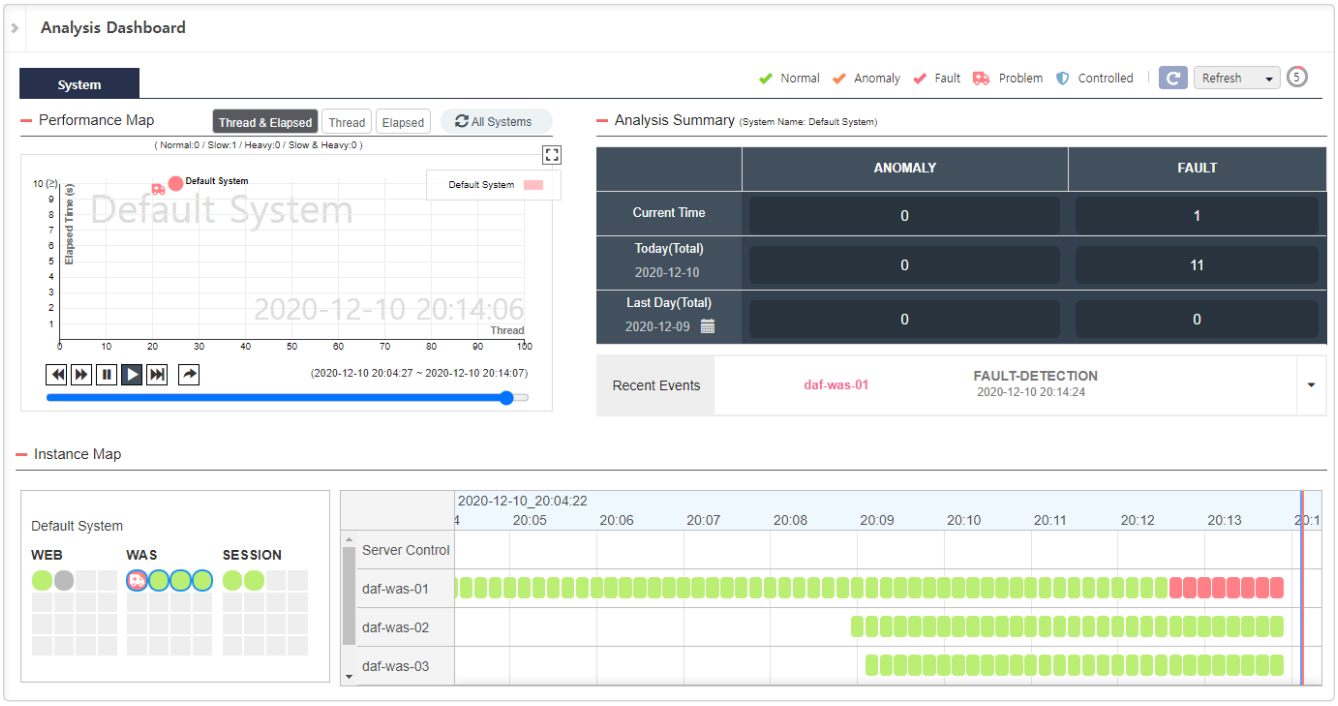


Figure 61. Analysis Dashboard

7.2.1. Performance Map

The Performance Map shown in the top left of the Analysis Dashboard provides system status information based on "Thread & Elapsed", "Thread", and "Elapsed" criteria respectively. Each system is displayed as a colored circle on the Chart. The colors by system status are as follows.

- Normal: Green
- Anomaly: Orange (Anomaly situation detected by diagnostic results)
- Fault: Red (Fault situation detected by diagnostic results)

The meanings of the X-axis and Y-axis in the Chart are as follows.

Table 140. Performance Map Chart X, Y-axis Meanings

Item	Description	Notes
Thread & Elapsed Chart	X-axis: Average Thread usage of Web Application Server within the system Y-axis: Average response time of services performed in Web Application Server within the system	

Item	Description	Notes
Thread Chart	X-axis: 10-minute Time Line Y-axis: Average Thread usage of Web Application Server within the system	
Elapsed Chart	X-axis: 10-minute Time Line Y-axis: Average response time of services performed in Web Application Server within the system	

The System status summary information displayed at the top of the Chart is as follows.

Table 141. System Status Summary Information Items

Item	Description	Notes
Normal	Number of normal Systems	
Slow	Number of Systems with long response times	
Heavy	Number of Systems with high Thread pool usage	
Slow & Heavy	Number of Systems that are both Slow and Heavy	

You can view previous status information by manipulating the slide bar at the bottom of the Chart, and you can move through time by clicking **Previous 10 minutes icon**, **Next 10 minutes icon**, **Pause icon**, **Play icon**, **Move to current time icon**. When first entering the Dashboard, all systems are displayed, and you can select specific systems by clicking on systems or legends displayed in the Chart. To view all systems again, click the **All System icon** in the top right.

Right-clicking on a system icon allows you to perform the following functions.

Table 142. Functions Available When Right-clicking on System Icon

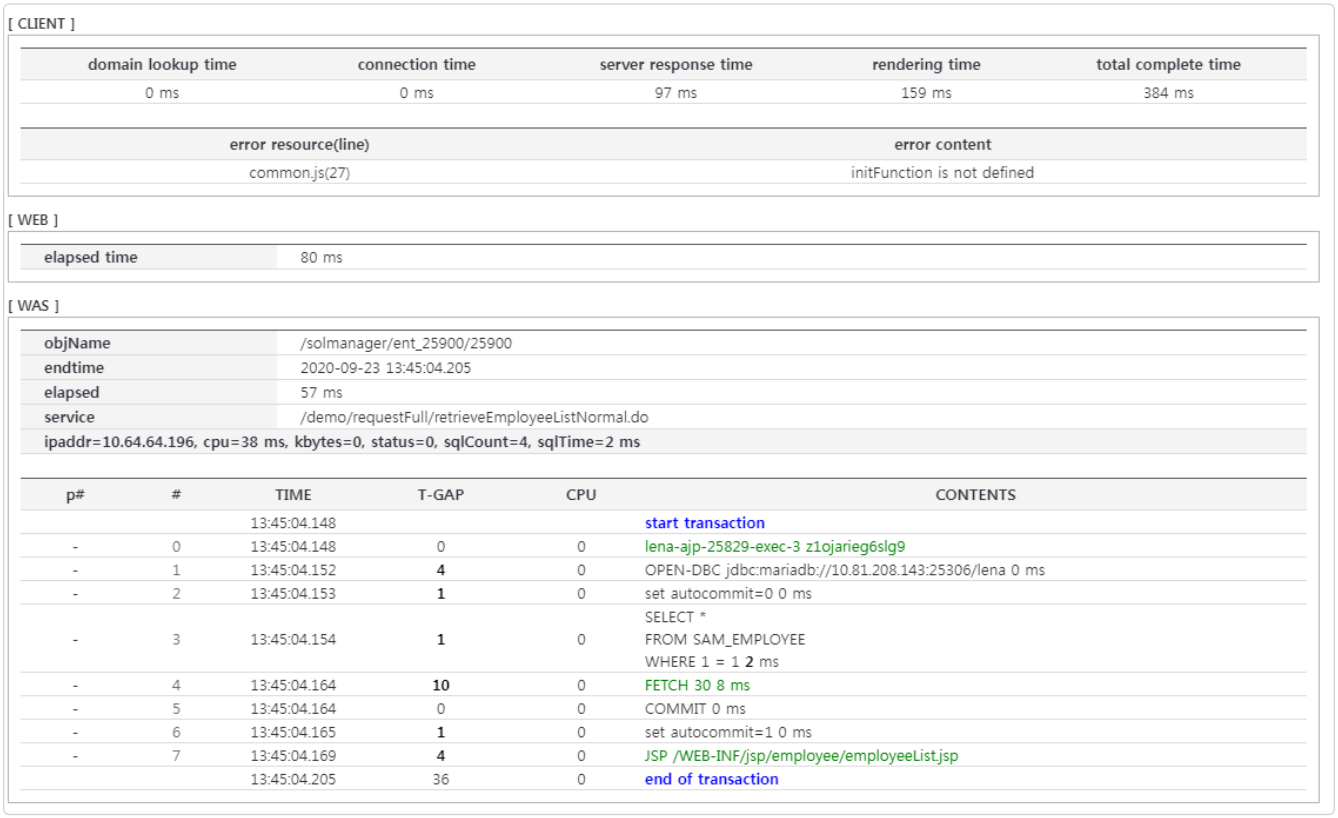
Item	Description	Notes
Topology View	Move to Topology View screen	
Service Analysis	Display System Detail popup window	
Monitoring	Move to Monitoring Dashboard screen	
Statistics	Move to Statistics screen	

The popup window displayed when clicking Service Analysis among the system right-click functions is as follows. The current status of Web Server, WAS, and Session Server is displayed on the left. On the right, you can see the Transaction Heat Map Chart, and you can check detailed information by dragging an area.

Figure 62. System Detail Screen

Transaction information only remains when collected through the Service Trace functionality in LENA Dashboard.

The following is the detailed information screen that can be viewed when selecting a specific Transaction from the Transaction list displayed after dragging the desired area in the Transaction Heat Map Chart.



[CLIENT]

domain lookup time	connection time	server response time	rendering time	total complete time
0 ms	0 ms	97 ms	159 ms	384 ms

error resource(line)	error content
common.js(27)	initFunction is not defined

[WEB]

elapsed time	80 ms

[WAS]

objName	/solmanager/ent_25900/25900
endtime	2020-09-23 13:45:04.205
elapsed	57 ms
service	/demo/requestFull/retrieveEmployeeListNormal.do
ipaddr=10.64.64.196, cpu=38 ms, kbytes=0, status=0, sqlCount=4, sqlTime=2 ms	

p#	#	TIME	T-GAP	CPU	CONTENTS
		13:45:04.148			start transaction
-	0	13:45:04.148	0	0	lena-ajp-25829-exec-3 z1ojarieg6slg9
-	1	13:45:04.152	4	0	OPEN-DBC jdbc:mariadb://10.81.208.143:25306/lena 0 ms
-	2	13:45:04.153	1	0	set autocommit=0 0 ms
-	3	13:45:04.154	1	0	SELECT * FROM SAM_EMPLOYEE WHERE 1 = 1 2 ms
-	4	13:45:04.164	10	0	FETCH 30 8 ms
-	5	13:45:04.164	0	0	COMMIT 0 ms
-	6	13:45:04.165	1	0	set autocommit=1 0 ms
-	7	13:45:04.169	4	0	JSP /WEB-INF/jsp/employee/employeeList.jsp
		13:45:04.205	36	0	end of transaction

Figure 63. Transaction Detail Information Screen

The detailed information consists of data from CLIENT (user browser related), WEB (LENA Web Server related), and WAS (LENA Web Application Server related) perspectives. The items that can be viewed in each type of information are as follows.

Table 143. CLIENT Related Data Items

Item	Description	Notes
domain lookup time	Time for browser to perform domain lookup to connect to server	

Item	Description	Notes
connection time	Time for browser to establish connection with server	
server response time	Total time for browser to send request to server and receive response	
rendering time	Browser screen rendering time	
total complete time	Total time processed in browser	
error resource(line)	When script error occurs, the line where the error occurred	
error content	When script error occurs, the content of the error that occurred	

Table 144. WEB Related Data Items

Item	Description	Notes
elapsed time	Processing time performed in WEB	

WAS Related Data Items

- Basic Information

Table 145. Basic Information

Item	Description	Notes
objName	Name of server that processed the request	
endtime	Request processing completion time	
elapsed	Request processing execution time	
service	Request service name	
ipaddr	IP information of the caller	
cpu	CPU usage time	
sqlCount	Number of queries executed	
sqlTime	Query execution time	

- Profile Information

Table 146. Profile Information

Item	Description	Notes
#	Index indicating the order of profile steps	
p#	Parent index if it's an internal step	
TIME	Time when the step started	
T-GAP	Difference between current step start time and previous step start time	

Item	Description	Notes
CPU	CPU usage time	
CONTENTS	Content of each step	

CLIENT and WEB related information is only collected when the E2E functionality is ON. It is OFF by default to minimize load.

Profile information is only collected when profile settings are ON in WAS. It is OFF by default to minimize load.

7.2.2. Analysis Summary

Shows summary information of currently detected diagnostic result counts, total diagnostic result counts that occurred today, and diagnostic result counts that occurred on previous days (Default: 1 day ago).

Table 147. Analysis Summary Information Items

Item	Description	Notes
Anomaly	Number of diagnostic results that are not in Fault status but need careful attention	
Fault	Number of diagnostic results diagnosed as Fault status	

Recent Events shows the most recently occurred diagnostic results, and clicking on an item allows you to check Report information.

7.2.3. Instance Map

When a specific system is selected in the Performance Map, you can see a Time Line Chart at the bottom of the screen showing server information within the system and diagnostic results. Servers are displayed in different colors according to their status, and you can toggle specific servers to show or hide them in the right Time Line Chart. After diagnosis, if Anomaly or Fault situations are detected, they are displayed in orange (Anomaly situation) or red (Fault) on the Time Line, and double-clicking on the area allows you to check the Report.

7.3. Event Dashboard

The Event Dashboard provides event status information that occurred in WAS.

Event information is generated in WAS and transmitted to the Manager via UDP. Event information sent by WAS is stored in the Manager's DB for a certain period (3 months), and detailed SQL and Exception Trace information for that event is stored for only 7 days due to large data size.

7.3.1. Event Types

There are 4 types of events as follows.

- Out Of Memory Error occurrence event in WAS
- Full GC occurrence event in WAS

- Stuck Thread occurrence event in WAS
- Exception occurrence event in WAS

WAS Exception events are generated and transmitted to the Manager in the following two situations.

- When an Exception is thrown outside the Servlet's service method for a user request
- When an Exception of a type configured by the user occurs

7.3.2. Event Management through Event Dashboard

You can manage Events collected in the Event Dashboard of LENA Manager.

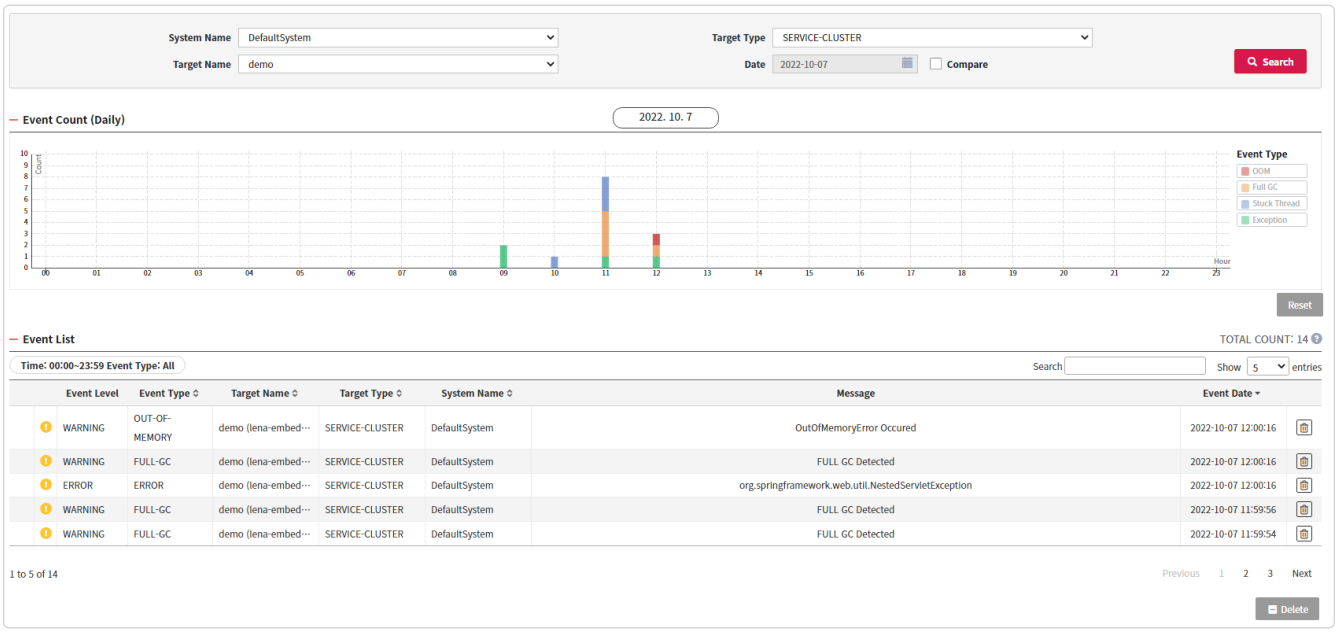


Figure 64. Event Dashboard

You can check event occurrence trends in daily bar charts. You can view all Systems or specify specific Systems or Servers for queries. Click the **Calendar button** to change the date.

The items in the event list are as follows.

Table 148. Event List Items

Item	Description	Notes
Event Level	Event level	The following types exist. The 4 events are WARNING by default and can be changed. • INFO • WARNING(DEFAULT) • ERROR • CRITICAL

Item	Description	Notes
Event Type	Event type	The following types exist • OUT-OF-MEMORY • FULL-GC • STUCK-THREAD • ERROR
Target Name	Target server name	WAS name or Service Cluster name
System Name	System name	
Message	Event message	Error events leave the name of the occurred Exception, and Stuck Thread events leave a message indicating that a Stuck Thread occurred
Event Date	Event occurrence time	
(**Delete button**)	Button to select when deleting an event	

Clicking on an individual event row allows you to check the following Event detailed information.

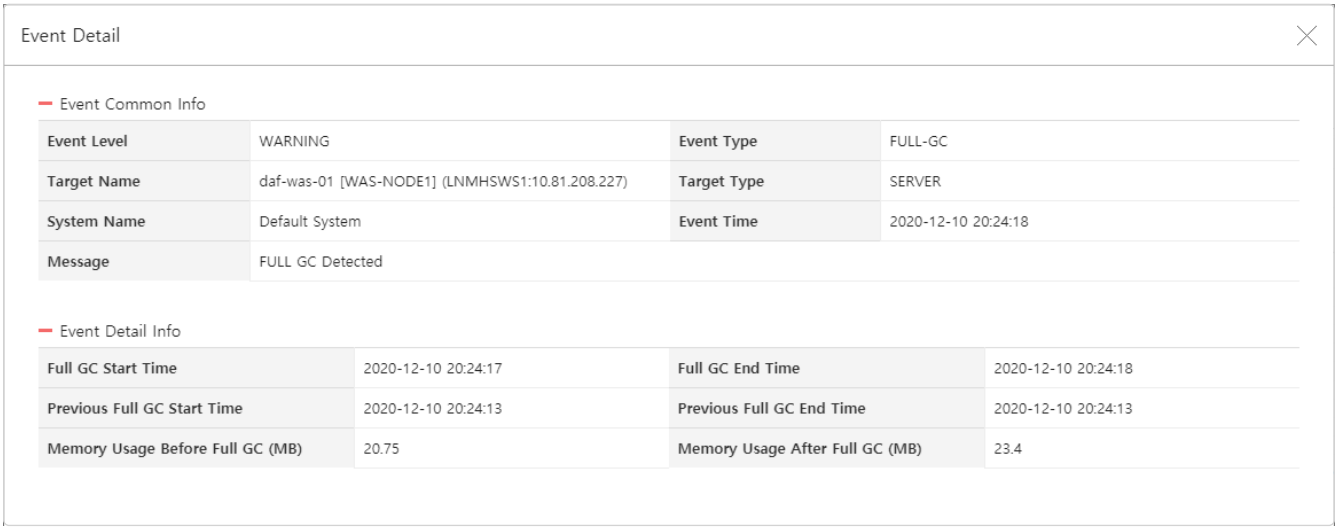


Figure 65. Event Detail Information Screen

The common items in Event detailed information are as follows.

Table 149. Common Items in Event Detailed Information (Event Common Info)

Item	Description	Notes
Event Level	Event level	The following types exist. • WARNING • INFO • ERROR • CRITICAL
Event Type	Event type	The following types exist • OUT-OF-MEMORY • FULL-GC • STUCK-THREAD • ERROR
Target Name	Target server name	WAS name or Service Cluster name
Target Type	Target server type	The following types exist • WAS • SERVICE-CLUSTER
System Name	System name	
Event Date	Event occurrence time	

The detailed information items that differ by Event are as follows.

Table 150. Out Of Memory Event Detailed Information Items (Event Detail Info)

Item	Description	Notes
Heap Dump File Name	Name of the Heap Dump file automatically generated when Out Of Memory Error occurs	

Table 151. Full GC Event Detailed Information Items (Event Detail Info)

Item	Description	Notes
Full GC Start Time	Full GC start time	
Full GC End Time	Full GC end time	
Previous Full GC Start Time	Start time of the immediately previous Full GC	
Previous Full GC End Time	End time of the immediately previous Full GC	

Item	Description	Notes
Memory Usage Before Full GC (MB)	Memory usage before Full GC execution	
Memory Usage After Full GC (MB)	Memory usage after Full GC execution	

Table 152. Stuck Thread Event Detailed Information Items (Event Detail Info)

Item	Description	Notes
Service	Service URL	
Http Query	get parameters of the service URL	post data is not visible get parameter keys are displayed but values are masked
Threshold(ms)	Threshold value set in LenaStuckThreadDetectionValve	
Active Time(ms)	Processing time of the service when Stuck Thread is detected	
Stack Trace	Stack Trace at the time of Stuck Thread detection	

Table 153. Error Event Detailed Information Items (Event Detail Info)

Item	Description	Notes
Service	Service URL	
Http Query	get parameters of the service URL	post data is not visible get parameter keys are displayed but values are masked
Remote Addr	Client remote address	
Custom Info	User-defined code information	Key, Value specified by the user using custom Servlet Filter
Exception Trace	Trace of the occurred Exception	

7.4. Statistics

7.4.1. Annual Diagnostics/Response Statistics

The DIAGNOSTICS > Analysis > Diagnostics Trend menu provides annual diagnostic results by server through charts.

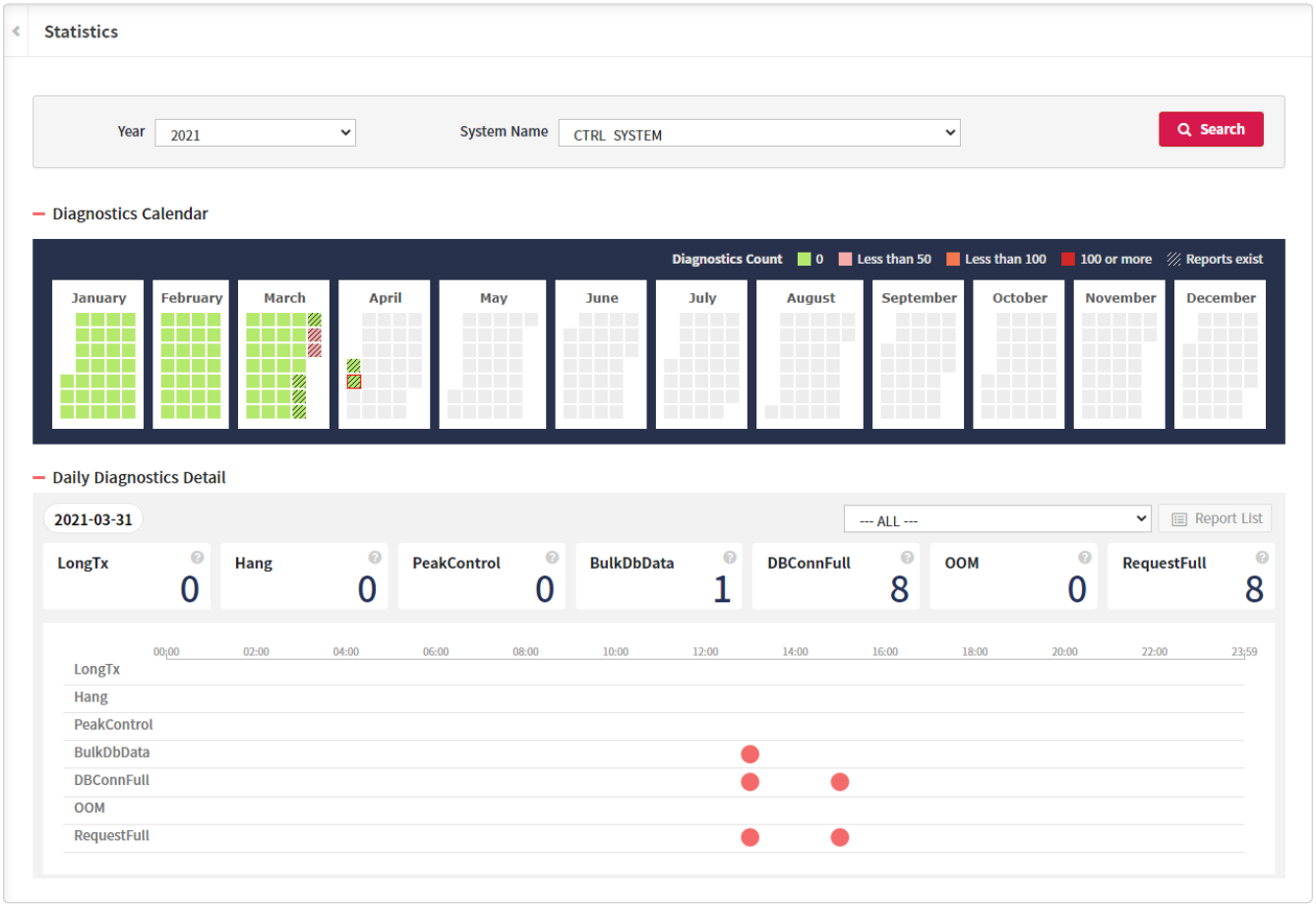


Figure 66. Statistics Screen

The following content can be checked in the above screen.

- Diagnostics Calendar
  - Each cell represents one day, and you can check the number of diagnostics that occurred on that day by hovering over a date in the annual statistics chart.
- Daily Diagnostics Detail
  - When you click on a specific date in the Diagnostics Calendar, a time-based diagnostic occurrence graph for the selected date is displayed at the bottom of the screen.

7.4.2. Reports

When diagnostics and response functionality is performed, Reports are automatically generated. Reports are stored for 7 days, and old Reports are automatically deleted.

Diagnostics/Response Report List

In the DIAGNOSTICS > Analysis > Diagnostics Trend screen, after selecting a specific server, click the **Report List button** to view the diagnostics/response report list screen. The diagnostics/response report list screen is as follows.

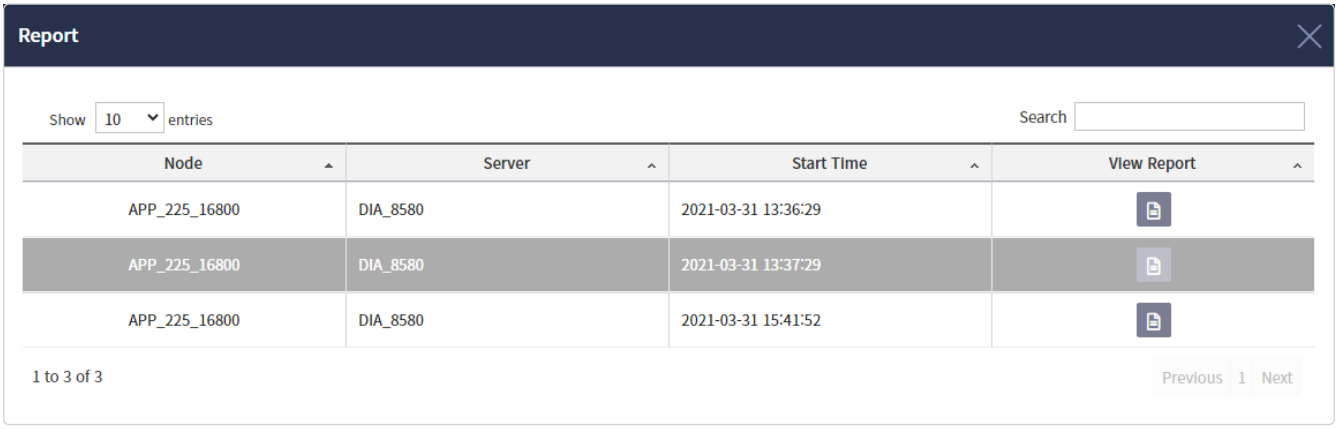


Figure 67. Diagnostics/Response Report List Screen

You can check the Report by selecting the **View button**.

Report Common Information

The content of Reports is displayed differently according to diagnostic results, but they have the following common information.

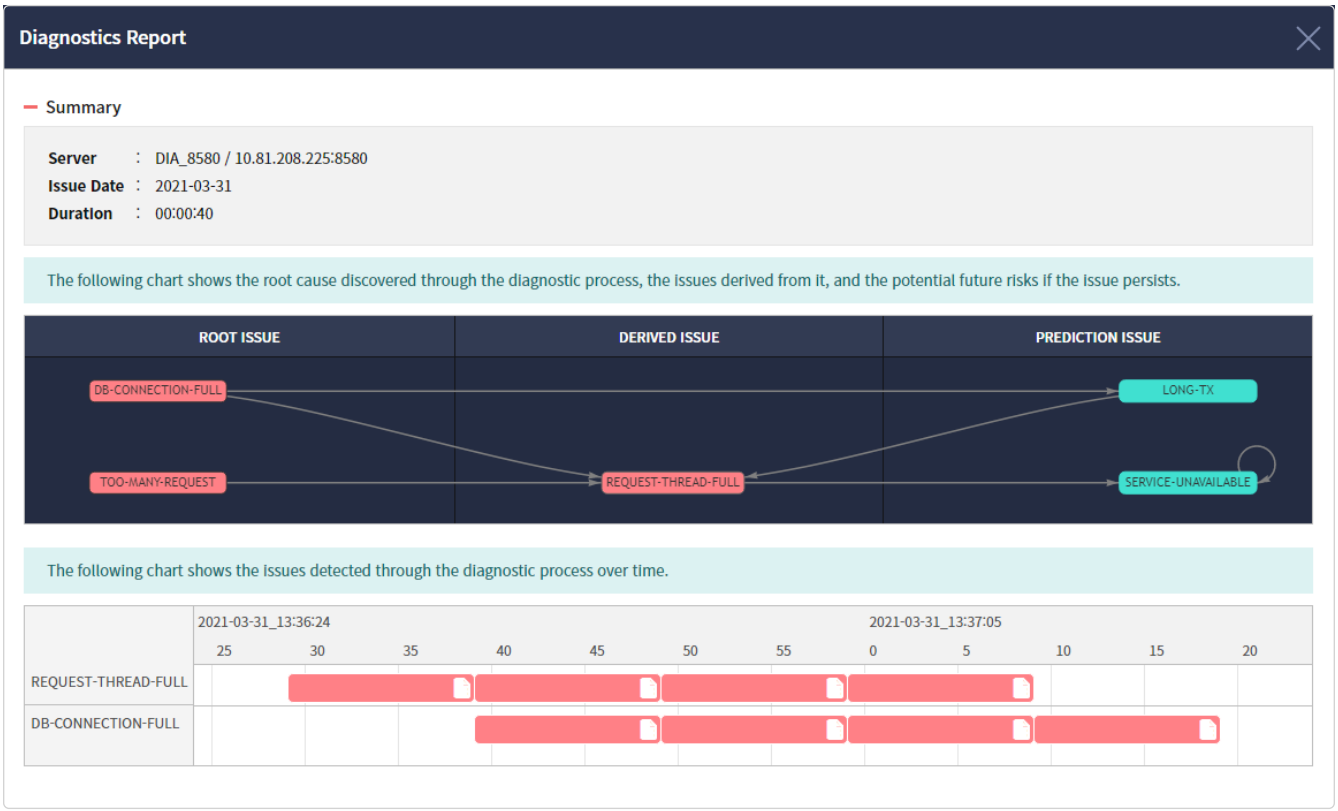


Figure 68. Diagnostics/Response Report Screen

As shown above, it provides a diagram of the causal relationship between diagnostic results detected during the period when abnormal phenomena persisted, and at the bottom of the screen, it shows when each diagnostic result was generated.

Anomaly situations mean situations where only some of the configured content in diagnostic/response Rules are satisfied and are displayed in orange, while Fault situations mean situations where all configured content in diagnostic/response Rules are satisfied and are displayed in red.

Report Detailed Information

In the Time Line at the bottom of the Report, clicking on a specific diagnostic type at a specific time allows you to check detailed information as follows.

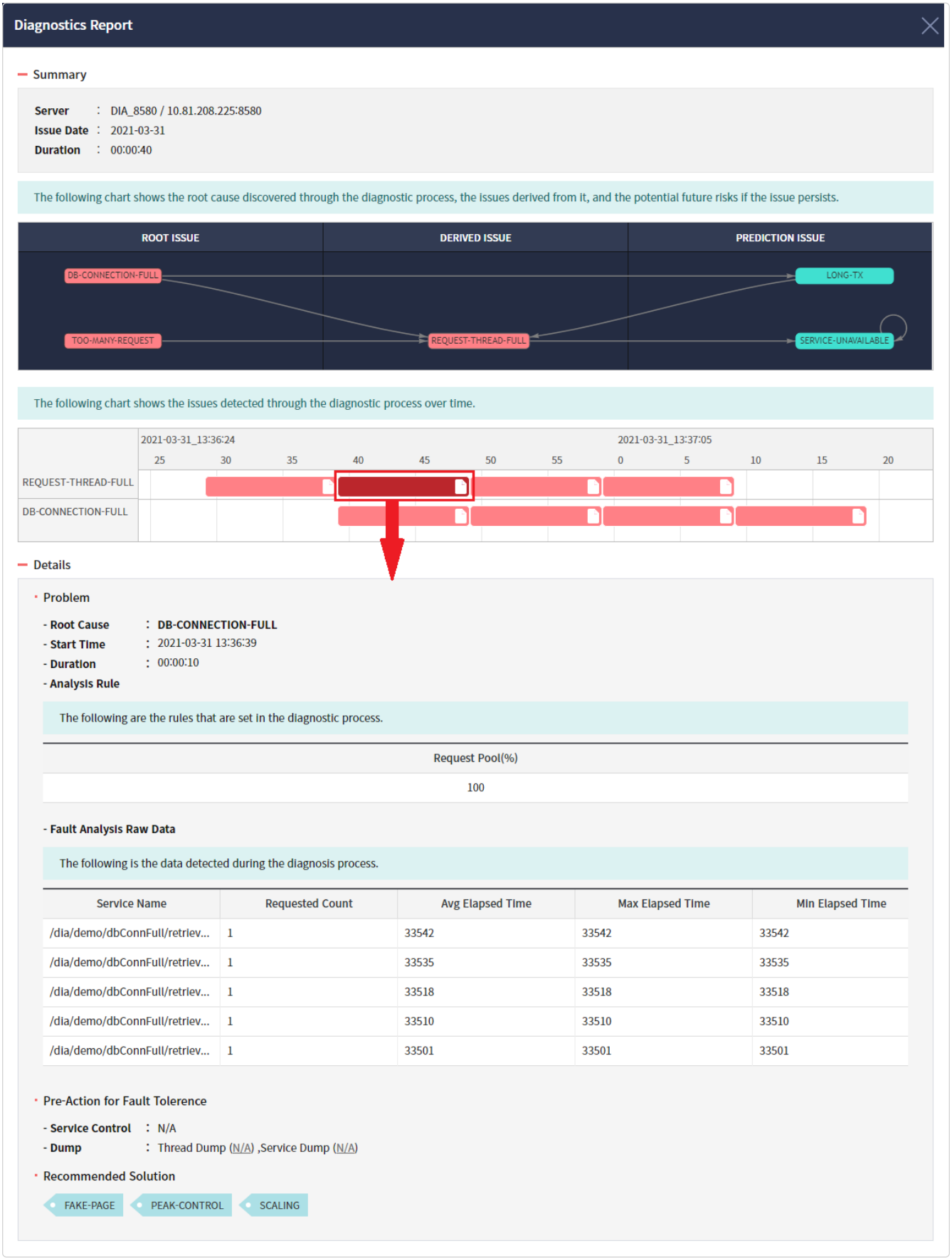


Figure 69. Diagnostics/Response Report Detailed Information

The items in the Report detailed information are as follows.

Table 154. Report Detailed Information Items

Item	Description	Notes
Root Cause	Diagnostic item that is the cause	Refers to the diagnostic item that caused the diagnostic result, and if there is another diagnostic item that caused the diagnostic result, the other diagnostic item is displayed
Analysis Rule	Threshold set in diagnostic/response Rule	
Fault Analysis Raw Data	Back Data that serves as the basis for diagnosis	
Pre-Action for Fault Tolerance	Performed Action and Dump file names	
Recommended Solution	Actionable solutions	

The Back Data items by diagnostic/response type are as follows.

The Back Data for Request Full diagnostic Reports consists of information about the 5 most frequently called services.

Table 155. Back Data Items for Request Full Diagnostic Reports

Item	Description	Notes
Service Name	Service name	
Requested Count	Number of requests for that service	
Avg. Elapsed Time	Average response time for that service	
Max Elapsed Time	Response time of the service that took the longest among that service	
Min Elapsed Time	Response time of the service that took the shortest among that service	

The Back Data for bulk DB Data request diagnostic Reports consists of information about the 5 services that made the most bulk DB Data requests.

Table 156. Back Data Items for Bulk DB Data Request Diagnostic Reports

Item	Description	Notes
Service Name	Service name	
Count	Number of requests for that service	
Blocked Count	Number of blocked DB data queries	

The Back Data for DB Conn Full diagnostic Reports consists of information about the excessively

occupied DataSource Connection Pool.

Table 157. Back Data Items for DB Conn Full Diagnostic Reports

Item	Description	Notes
DataSource Name	DataSource name	
DB Connection Pool Usage Rate	DB Connection Pool usage rate	

Long Transaction diagnostic Report's Back Data consists of the 5 services that took the longest among the diagnostic target services.

Table 158. Back Data Items for Long Transaction Diagnostic Reports

Item	Description	Notes
Service Name	Service name	
Requested Count	Number of requests for that service	
Avg. Elapsed Time	Average response time for that service	
Max Elapsed Time	Response time of the service that took the longest among that service	
Min Elapsed Time	Response time of the service that took the shortest among that service	

Peak Control diagnostic Report's Back Data consists of the 5 services that took the longest among the diagnostic target services.

Table 159. Back Data Items for Peak Control Diagnostic Reports

Item	Description	Notes
Service Name	Service name	
Requested Count	Number of requests for that service	
Avg. Elapsed Time	Average response time for that service	
Max Elapsed Time	Response time of the service that took the longest among that service	
Min Elapsed Time	Response time of the service that took the shortest among that service	

OOM diagnostic Report's Back Data consists of OOM occurrence status and memory usage information.

Table 160. Back Data Items for OOM Diagnostic Reports

Item	Description	Notes
OOM Occurred	OOM occurred	
Heap Usage Rate	Heap Memory usage rate	
Full GC Count	Full GC count	

Item	Description	Notes
Memory Leak	Memory Leak occurred	
Heap Dump	File name if Heap Dump was generated	

Hang diagnostic Report's Back Data consists of server status and system resource information.

Table 161. Back Data Items for Hang Diagnostic Reports

Item	Description	Notes
Node CPU Rate	CPU usage rate of the system measured by Node Agent	
Node Memory Rate	Memory usage rate of the system measured by Node Agent	
Process CPU Rate	CPU usage rate of the server	
Full GC Count	Full GC count of the server	

7.4.3. Alerts

When Reports are generated through diagnostics/response, they can be checked through the **bell icon** in the top right of LENA Manager as follows.

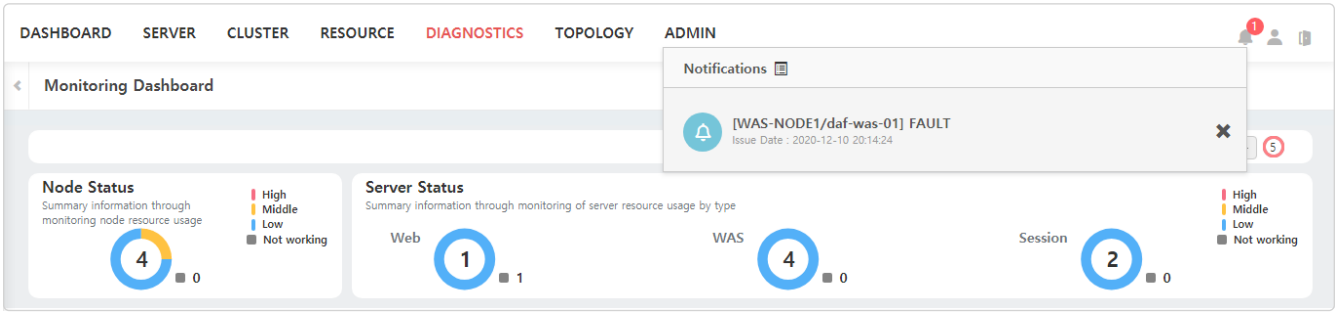


Figure 70. Diagnostics/Response Result Alert

When you select the alert content, you can immediately check the generated Report, and if you want to check the alert content and no longer display it, click the **x button**. When there are many alerts, you can select the **bell icon** in the top right of the Manager and then check them all at once in the Notifications screen.

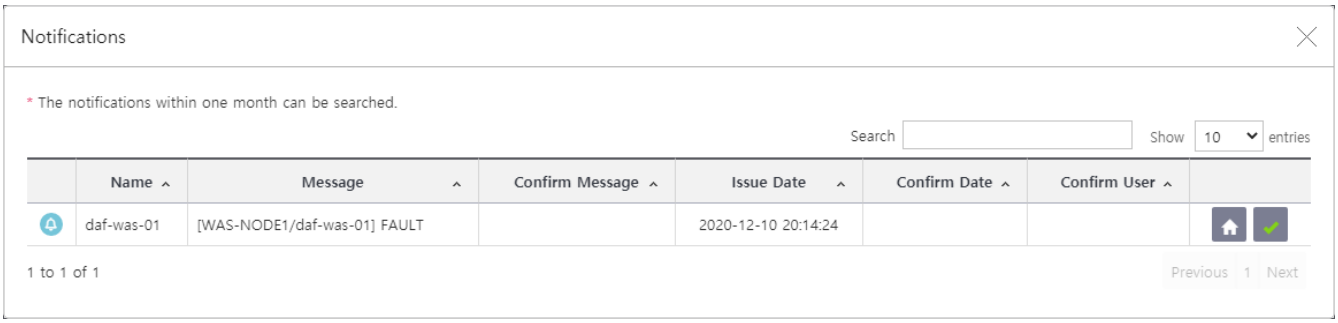


Figure 71. Bulk Check of Diagnostics/Response Result Alert List

Clicking the **Home icon** navigates to the diagnostic history screen for the selected alert. Clicking the **V icon** means that the selected alert has been checked, and alerts clicked this way will no longer be displayed in the **bell icon** in the top right of the Manager.

In the Notifications screen, you can check the history of past alerts within 1 month. Data older than 1 month is automatically deleted.

7.4.4. Thread Dump Analysis

Analyze thread dumps generated through LENA Manager and present them in an easily understandable format for users.

Prerequisites require a thread dump file within the server or service cluster.

Report

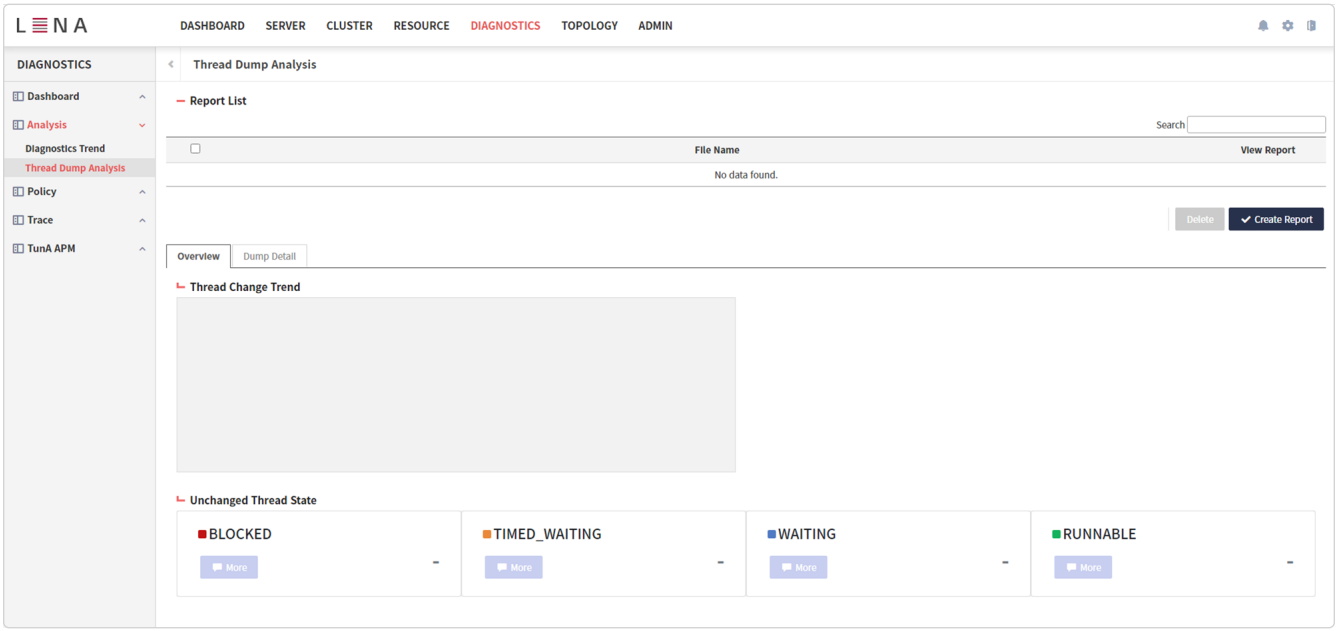


Figure 72. Thread Dump Analysis Initial Screen

Select the 'DIAGNOSTICS' menu at the top of LENA Manager and click Thread Dump Analysis in Analysis on the left.

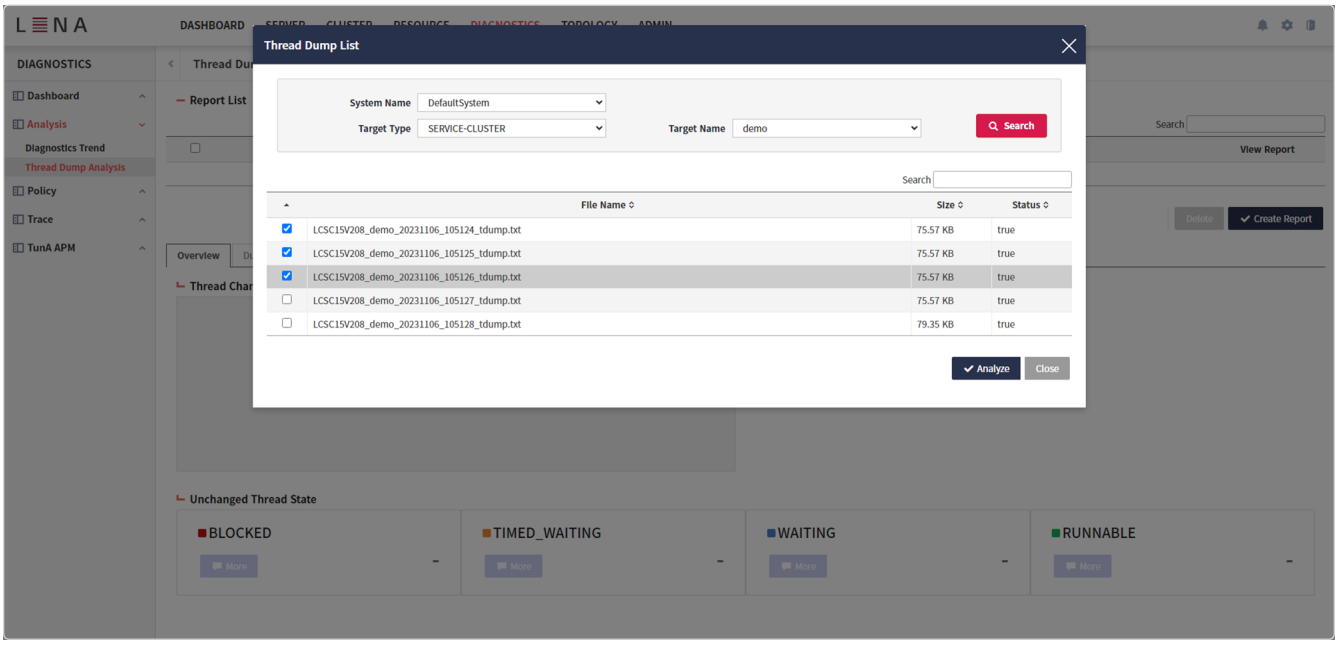


Figure 73. Modal window to select the Thread Dump to analyze and generate the Report

Create Report button to confirm the modal window.

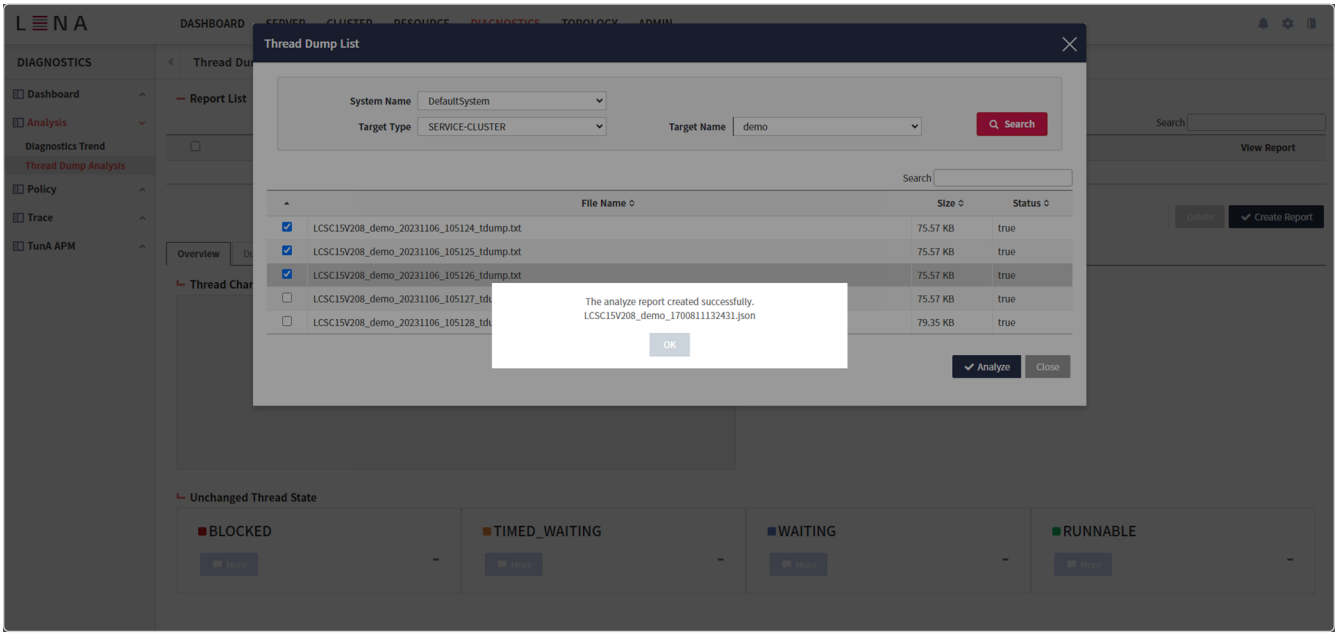


Figure 74. Screen showing successful Report generation after analyzing the Thread Dump file

Select System Name, Target Type, Target Name in order and click Search button to check the list of available Thread Dump files.
Select the Thread Dump file to analyze and click Analyze button to generate the Report.
The path of the generated Report is as follows.

- (LENA-Manager installation path)/repository/monitoringDB/report

(You need to select 3-5 Thread Dump files for analysis.)

Overview

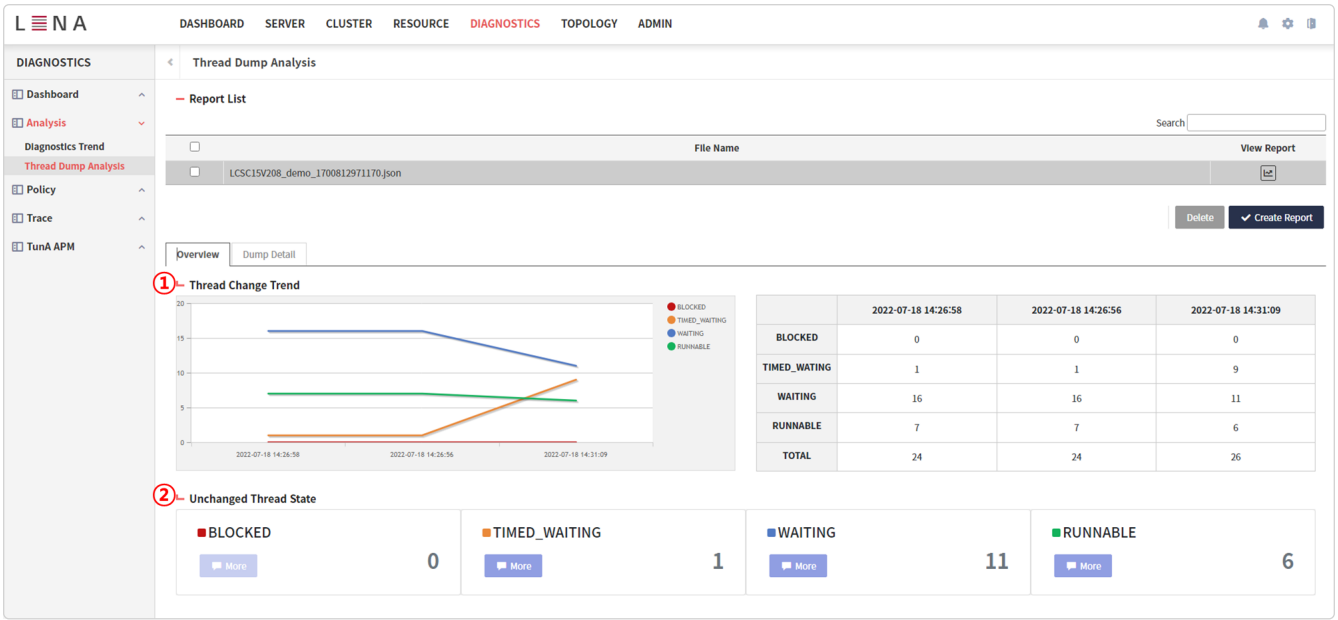


Figure 75. Screen showing the analyzed Report file

1. Thread Change Thrend
   You can check the state (State) change trend of Threads by graph and specific count by table.
2. Unchanged Thread State
   Check the number of Threads that did not change in all analyzed Thread Dump files and click 'More' button to check detailed information.

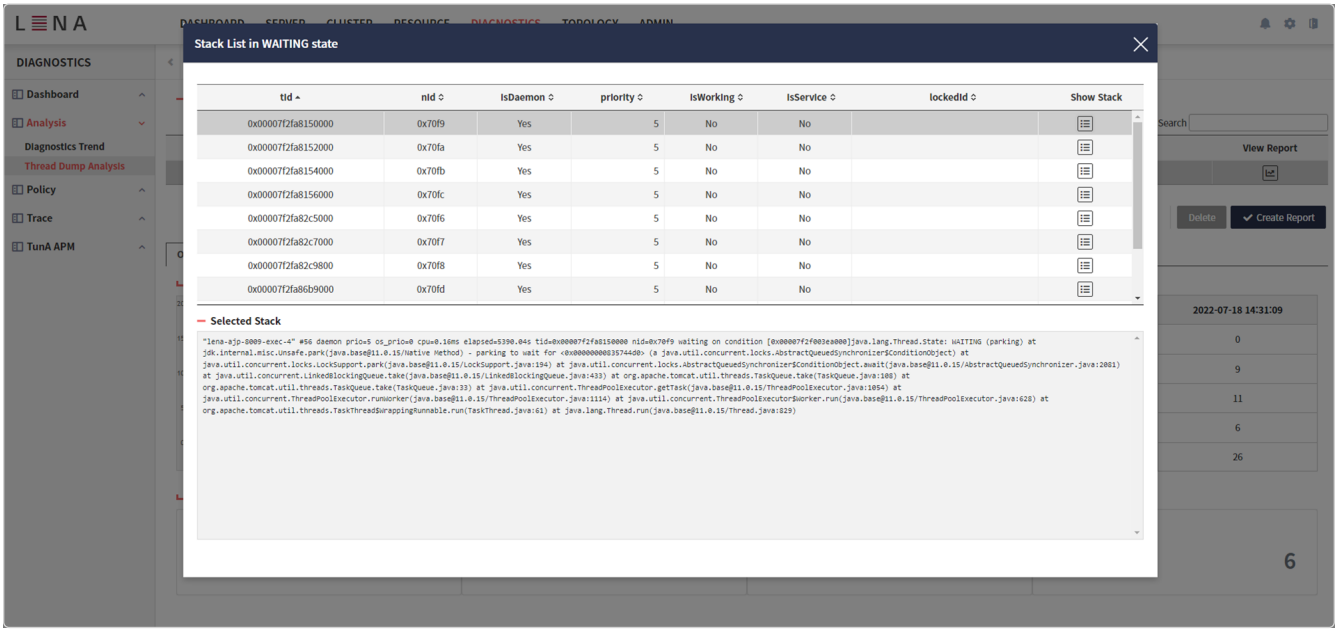


Figure 76. Information about Threads by state

Dump Detail

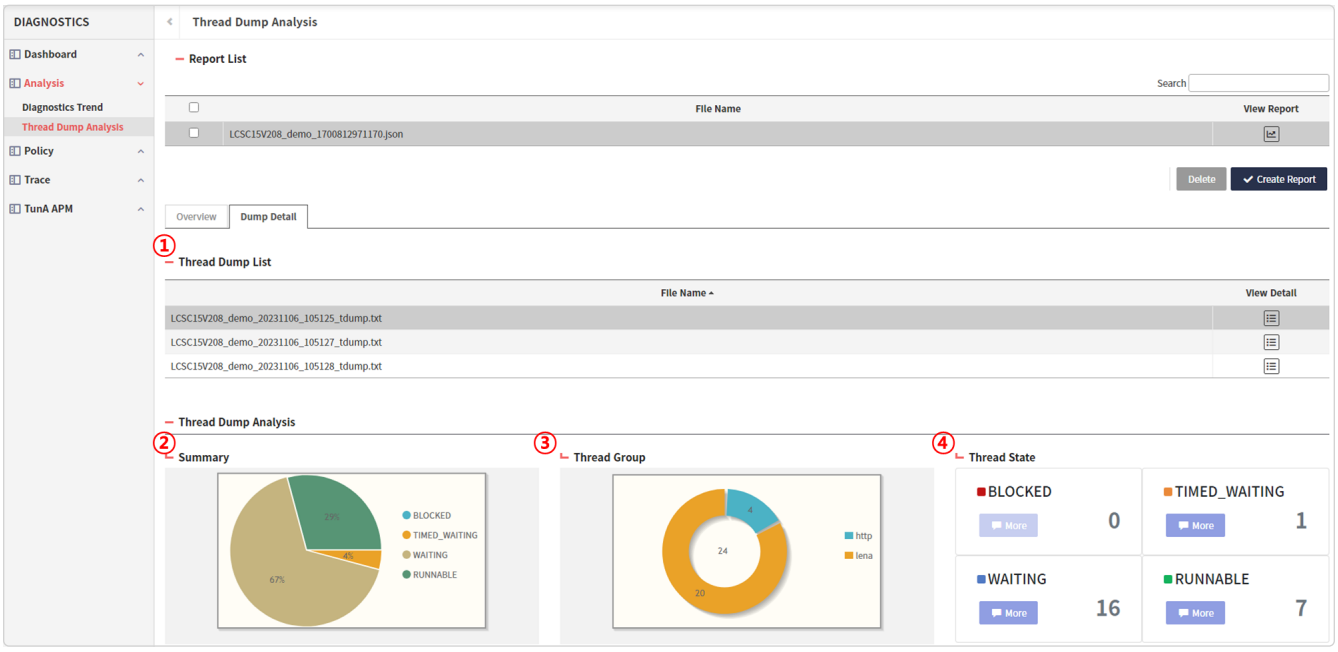


Figure 77. Screen showing Thread information for each analyzed Dump file

1. Thread Dump List
   List of analyzed Thread Dump files
2. Summary
   Thread state distribution of the corresponding Thread Dump
3. Thread Group
   Number of Threads grouped by workerThread defined in the Rule file
   - Rule file path: (LENA-Manager installation path)/repository/conf/diagnostics/basic-parser.json
4. Thread State
   You can check detailed information by clicking 'More' button.

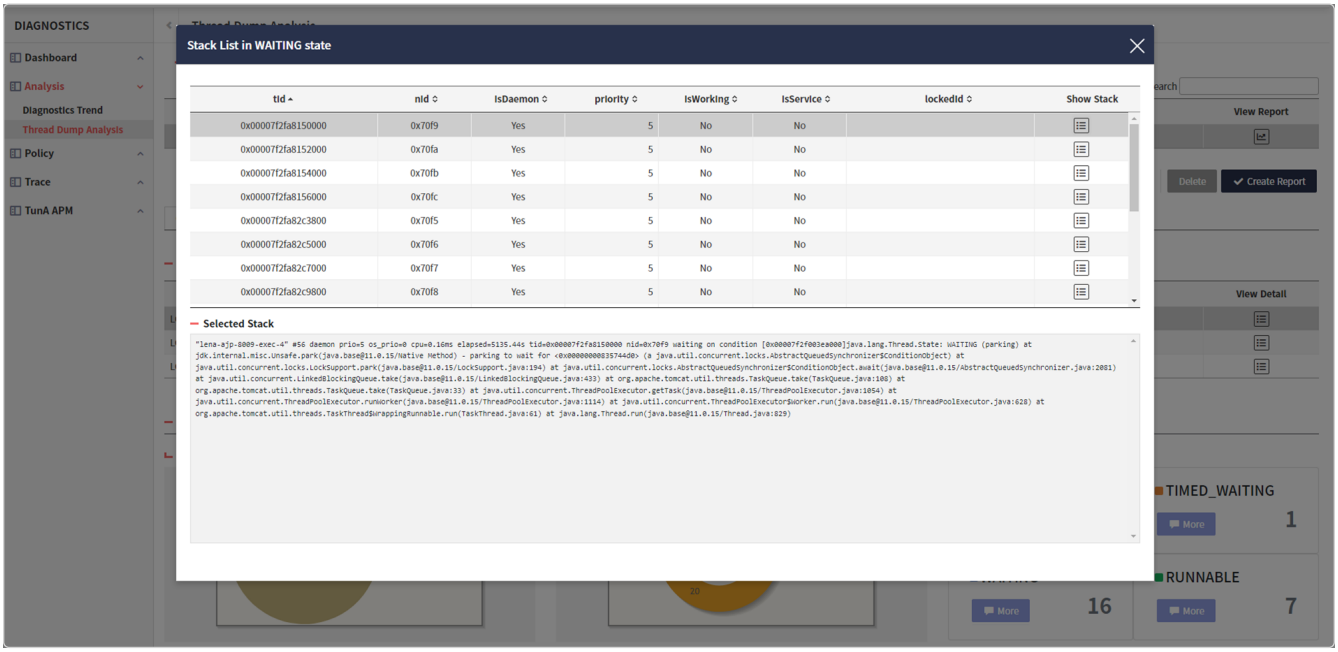


Figure 78. Thread information for the selected Thread Dump file

7.4.5. Diagnostics Pipeline

LENA Manager automatically analyzes Thread Dump and generates a Thread Dump Analysis Report and shares the abnormal phenomenon with users through alerts.

Prerequisites

- Server Rule Setting Diagnostics Rule applied (for Thread Dump generation)
- Configure settings in `manager.conf`
  - `diagnostics.pipeline.enable=true` (default: false)
  - `diagnostics.pipeline.dump.count=5` (default: 5, range: 3-5)
  - `diagnostics.pipeline.interval=300` (default: 300, sec)

Operation Sequence

1. Server overload causes Thread Dump
2. Automatic generation of Thread Dump Analysis Report and alert
3. Click the alert to navigate to the Thread Dump Analysis screen
4. Analyze the abnormal phenomenon

[diagnostics dump reportAlarm] | manual/diagnostics_dump_reportAlarm.png

Figure 79. Thread Dump Analysis Report generation alert

7.5. Diagnostics and Response

By using the diagnostics and response functionality, you can diagnose potential failures in advance and automatically perform appropriate responses to improve Server stability.

- The diagnostics function is a rule-based function that automatically determines the possibility of Server failure (or failure situations).
- The response function is a function that supports overcoming failure situations and providing

stable services through appropriate Server control based on diagnostic results.

The types of diagnostic targets are as follows.

- Excessive use of Request Pool (Request Full)
  - When all available Request Threads of the Server are exhausted due to excessive service requests, service requests may be delayed or fall into a service unavailable state. Based on Request Thread usage, it identifies whether there are excessive service requests, and automatically redirects those requests to a temporary page to maintain the Server in a stable state.
- Bulk DB Data Request
  - When a service processes large amounts of DB data, it may cause OOM phenomena, frequent Full GC causing server hang phenomena, etc., while using memory excessively. It identifies whether the service is making bulk DB data requests, and forcibly terminates that service to maintain the Server in a stable state.
- Excessive use of DB Connection Pool (Db Conn Full)
  - When DB Connections are excessively occupied due to DB processing time delays, WAS-DB network delays, DB locks, etc., services are delayed until they are allocated available DB Connections. When services waiting for DB Connection allocation accumulate and excessively occupy the Request Thread Pool, service failure states may occur. When all DB Connections of a specific DataSource are exhausted, it maintains the Server in a stable state by isolating failures through methods that reduce allocation wait times.
- Long-running Services (Long Transaction)
  - When services are delayed due to temporary network or inter-system problems, or when services that originally take a long time to execute exist, those services may excessively occupy the Server's available Request Threads, causing interference with other service execution. It ensures QoS for other services by limiting the Request Thread usage rate of long-running services.
- Server Operation Failure (Hang)
  - When the Server becomes in a Hang state where it cannot operate, not only are all tasks performed on the Server interrupted, but it may also affect the entire system where the Server is installed. When a Hang state is detected, it immediately restarts to resolve the Server's failure situation and prevent system-wide failure occurrence.
- Out of Memory Error Occurrence (OOM)
  - Out of Memory (OOM) errors may occur due to service logic errors or excessive Memory usage. When OOM occurs, the Server's normal operation cannot be guaranteed, so it quickly identifies OOM occurrence and automatically restarts promptly to overcome the Server's failure situation.
- User Surge (Peak Control)
  - When there are many user requests that exceed the Server's processing limits, service delays or failure states may occur. If user requests are concentrated on specific services only, controlling requests to enter in order can provide stable services while preventing user churn. It can also ensure QoS for other services.

7.5.1. Diagnostics/Response Rule Setting

You can set diagnostics/response rules in the DIAGNOSTICS > Policy > Diagnostics Rule Setting menu.

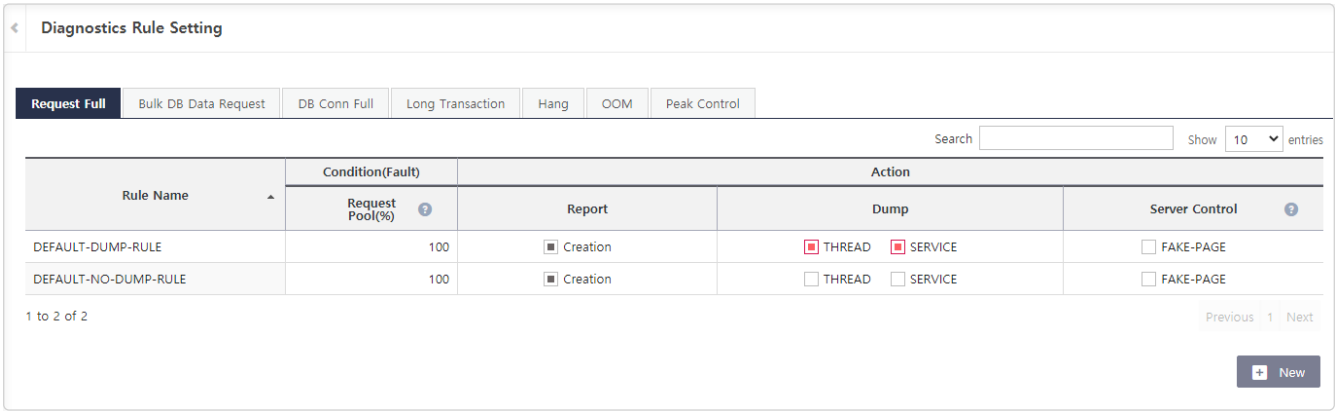


Figure 80. Diagnostics Rule Setting Screen

It is organized by tabs for each diagnostics/response type, and basic Default Rules are provided. Click the **New button** to create a new rule, or select an existing rule to modify or delete it.

Two Default Rules are provided for each diagnostic item as follows.

- Rule that only generates reports after diagnosis
- Rule that generates reports and dumps after diagnosis (Action is provided disabled)

The rule setting items for each diagnostic type are as follows.

Table 162. Request Full Diagnostic Rule

Item	Description	Default Value
Rule Name	Rule name	
Request Pool(%)	Request Pool usage threshold	100
Report	Report generation (always Enable)	Enable
Dump	Dump type to generate when abnormality is detected • THREAD: Thread Dump • SERVICE: Active Service Dump	Enable
Server Control	Action to perform when abnormality is detected • NONE: Do not perform • FAKE-PAGE: Redirect requests to temporary page (redirect page can be specified)	NONE

Table 163. Bulk DB Data Request Diagnostic Rule

Item	Description	Default Value
Rule Name	Rule name	
RS Count	Threshold for number of DB Data records requested within service	10000

Item	Description	Default Value
Exceptional URI	Service URI to exclude from diagnosis	
Report	Report generation (always Enable)	Enable
Dump	Dump type to generate when abnormality is detected • THREAD: Thread Dump • SERVICE: Active Service Dump	Enable
Server Control	Action to perform when abnormality is detected • NONE: Do not perform • THROW-EXCEPTION: Generate exception to forcibly terminate service	NONE

Table 164. DB Conn Full Diagnostic Rule

Item	Description	Default Value
Rule Name	Rule name	
DB Connection Pool(%)	DB Connection Pool usage threshold	100
Report	Report generation (always Enable)	Enable
Dump	Dump type to generate when abnormality is detected • THREAD: Thread Dump • SERVICE: Active Service Dump	Enable
Server Control	Action to perform when abnormality is detected • NONE: Do not perform • DB-CONN-CONTROL: Dynamically change Datasource Connection allocation wait time (wait time can be set)	NONE

Table 165. Long Transaction Diagnostic Rule

Item	Description	Default Value
Rule Name	Rule name	
Elapsed Time(s)	Execution time threshold for diagnostic target service	300
Service Allow Rate(%)	Request Thread usage rate threshold allowed for diagnostic target service	50
Target URI	Target service URI	

Item	Description	Default Value
Report	Report generation (always Enable)	Enable
Dump	Dump type to generate when abnormality is detected • THREAD: Thread Dump • SERVICE: Active Service Dump	Enable
Server Control	Action to perform when abnormality is detected • NONE: Do not perform • SERVICE-CONTROL: Redirect requests to temporary page (redirect page can be specified)	NONE

Table 166. Hang Diagnostic Rule

Item	Description	Default Value
Rule Name	Rule name	
Timeout(ms)	Response wait time threshold after Health Check attempt to server	3000(ms)
Retry Count	Number of retries when Health Check fails on server	3
FullGC Duration(s)	Time interval to check Full GC count	60
FullGC Count	Full GC count	2
Report	Report generation (always Enable)	Enable
Dump	Dump type to generate when abnormality is detected • THREAD: Thread Dump	Enable
Server Control	Action to perform when abnormality is detected • NONE: Do not perform • SHUTDOWN: Server shutdown • RESTART: Server restart	NONE

The relationship between Hang diagnostic setting items is as follows.

- Fault condition: When a situation where there is no response for Timeout(s) after Health Check attempt due to server Hang is repeated Retry Count times, it is judged as a Fault situation and Action is performed
- Anomaly condition: If Full GC occurs FullGC Count times within FullGC Duration(s) interval, it is judged as an Anomaly situation and only a Warning report is generated without Action

Table 167. OOM Diagnostic Rule

Item	Description	Default Value
Rule Name	Rule name	
OUT OF MEMORY	OOM occurrence (judged as Fault situation)	Detection of occurrence without separate setting
Memory Leak	Memory Leak occurrence (judged as Anomaly situation)	Detection of occurrence without separate setting
Report	Report generation (always Enable)	Enable
Dump	Dump type to generate when abnormality is detected • THREAD: Thread Dump • SERVICE: Active Service Dump	Enable
Server Control	Action to perform when abnormality is detected • NONE: Do not perform • SHUTDOWN: Server shutdown • RESTART: Server restart	NONE

Table 168. Peak Control Diagnostic Rule

Item	Description	Default Value
Rule Name	Rule name	
Target URI	Peak Control target service URI	
Service Allow Rate(%)	Request Thread usage rate threshold allowed for diagnostic target service	50
Release Rate(%)	Request Thread usage rate threshold that becomes the condition for releasing abnormal situation	10
Report	Report generation (always Enable)	Enable

Item	Description	Default Value
Dump	Dump type to generate when abnormality is detected • THREAD: Thread Dump • SERVICE: Active Service Dump	Enable
Server Control	Action to perform when abnormality is detected • NONE: Do not perform • PEAK-CONTROL: Redirect requests to temporary page (redirect page can be specified)	NONE

7.5.2. Server Rule Setting

You can map diagnostics/response rules to servers and enable/disable them in the DIAGNOSTICS > Policy > Server Rule Setting menu.

Initially, no diagnostic rules are mapped, so you must first map diagnostics/response rules before performing enable/disable functions. You can map diagnostics/response rules to servers by clicking on each server's row as follows.

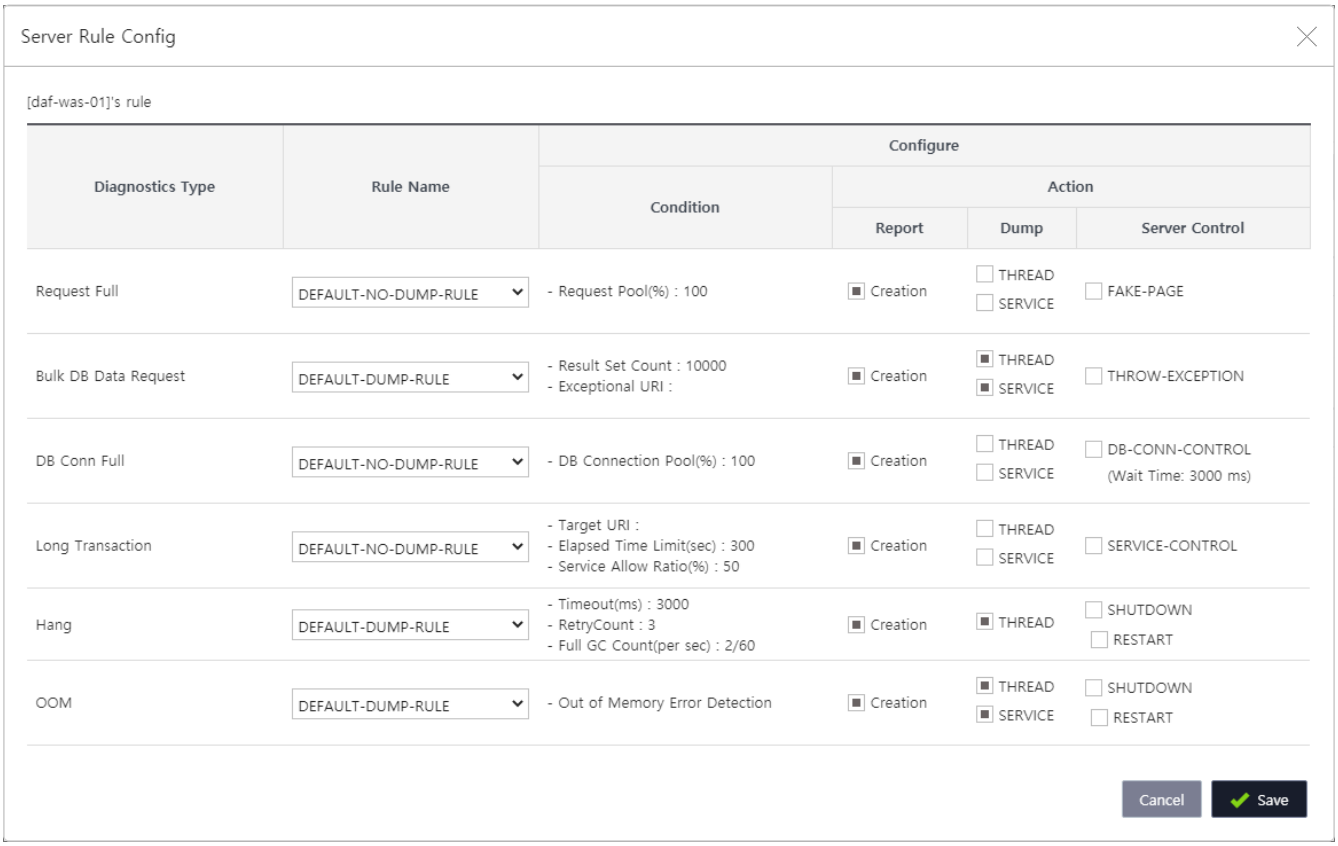


Figure 81. Diagnostics Rule Mapping Screen

After diagnostics/response rules are mapped, you can enable/disable rules in the Server Rule Setting screen as follows.

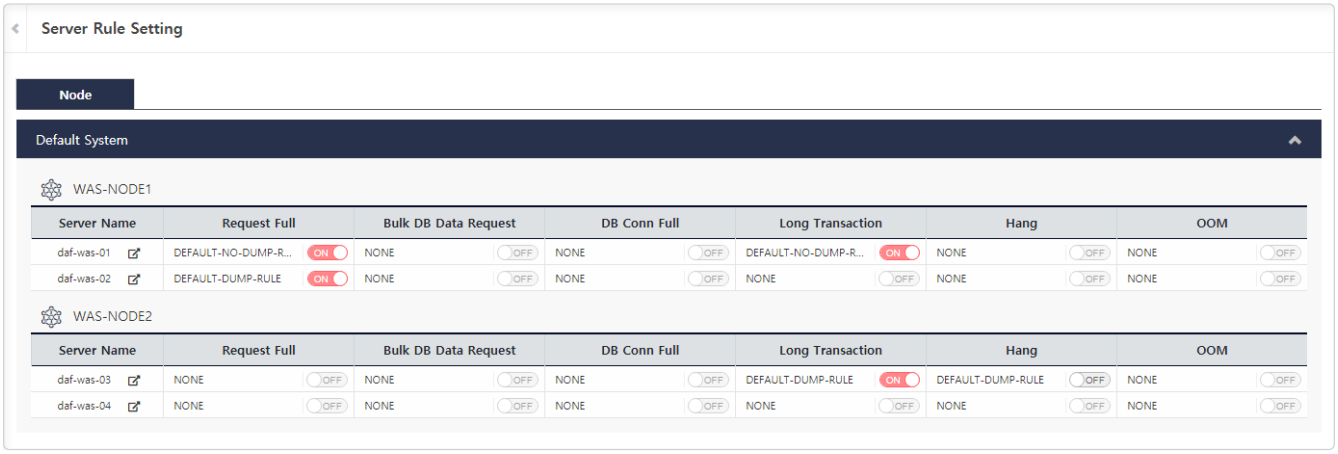


Figure 82. Server Rule Setting Screen

Peak Control diagnostic rules are only set in the DIAGNOSTICS > Policy > Peak Control Rule Setting menu.

7.6. Diagnostics and Response (Container & Embedded LENA)

Using the diagnostics and response functionality, you can diagnose potential failures in advance and automatically perform appropriate responses to improve Server stability.

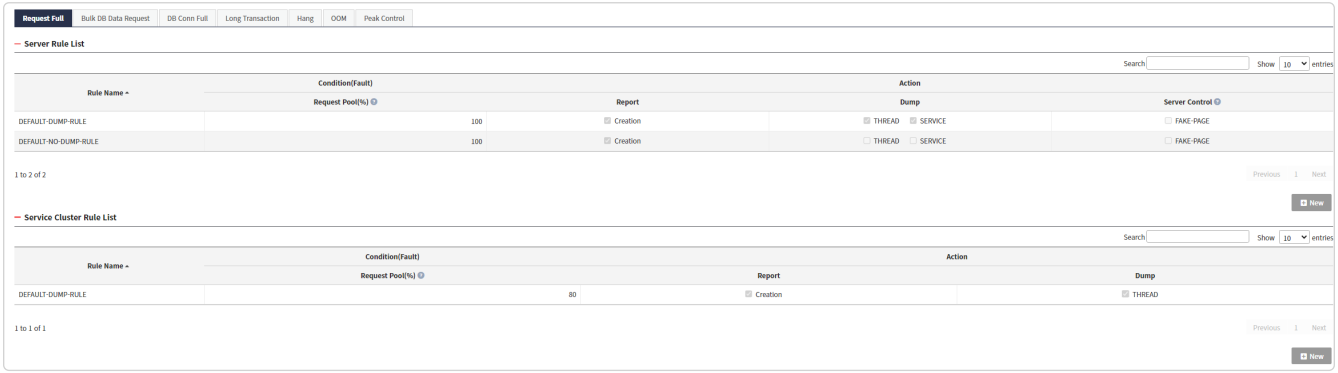
- Diagnostics functionality is a Rule-based function that automatically determines the potential failure (or failure situation) of a Server.
- Response functionality is a function that supports overcoming failure situations and providing stable services through appropriate Server control based on diagnostic results.

The types of diagnostic targets are as follows.

- Excessive use of Request Pool (Request Full)
  - When excessive service requests exhaust all available Request Threads in the Server, service requests may be delayed or fall into a service unavailable state.
    Based on Request Thread usage, it identifies whether there are excessive service requests, and can manage History based on Reports.
- Bulk DB Data Request
  - When services process large amounts of DB data, phenomena such as OOM due to excessive memory usage, server hang due to frequent Full GC, etc. may occur. It identifies whether there are bulk DB data requests in the service, and can manage History based on Reports.
- Excessive use of DB Connection Pool (DB Conn Full)
  - When DB Connections are excessively occupied due to DB processing time delays, network delays between WAS-DB, DB locks, etc., services are delayed until they receive an available DB Connection. When services waiting for DB Connection allocation accumulate and excessively occupy the Request Thread Pool, service failure states may occur. When all DB Connections of a specific DataSource are exhausted, etc., History can be managed based on Reports.
- Out of Memory Error (OOM)
  - Out of Memory (OOM) errors may occur due to service logic errors or excessive Memory usage. When OOM occurs, normal Server operation cannot be guaranteed, so it quickly identifies OOM occurrence and can manage History based on Reports.

7.6.1. Diagnostic/Response Rule Configuration

You can configure diagnostic/response Rules for Embedded LENA and Container Server in the Service Cluster Rule List of the DIAGNOSTICS > Policy > Diagnostics Rule Setting menu.



It is organized into tabs by diagnostic/response type, and basic Default Rules are provided. Click the New button to create a new Rule, or select an existing Rule to modify or delete it.

Table 169. Request Full Diagnostic Rule

Item	Description	Default Value
Rule Name	Rule name	
Request Pool(%)	Request Pool usage threshold	100
Report	Whether to generate Report (always Enable)	Enable
Dump	Dump type to generate when judged as abnormal • THREAD: Thread Dump • SERVICE: Active Service Dump	Enable

Table 170. Bulk DB Data Request Diagnostic Rule

Item	Description	Default Value
Rule Name	Rule name	
RS Count	Threshold for DB Data count requested within service	10000
Report	Whether to generate Report (always Enable)	Enable
Dump	Dump type to generate when judged as abnormal • THREAD: Thread Dump	Enable

Table 171. DB Conn Full Diagnostic Rule

Item	Description	Default Value
Rule Name	Rule name	

Item	Description	Default Value
DB Connection Pool(%)	DB Connection Pool usage threshold	100
Report	Whether to generate Report (always Enable)	Enable
Dump	Dump type to generate when judged as abnormal • THREAD: Thread Dump	Enable

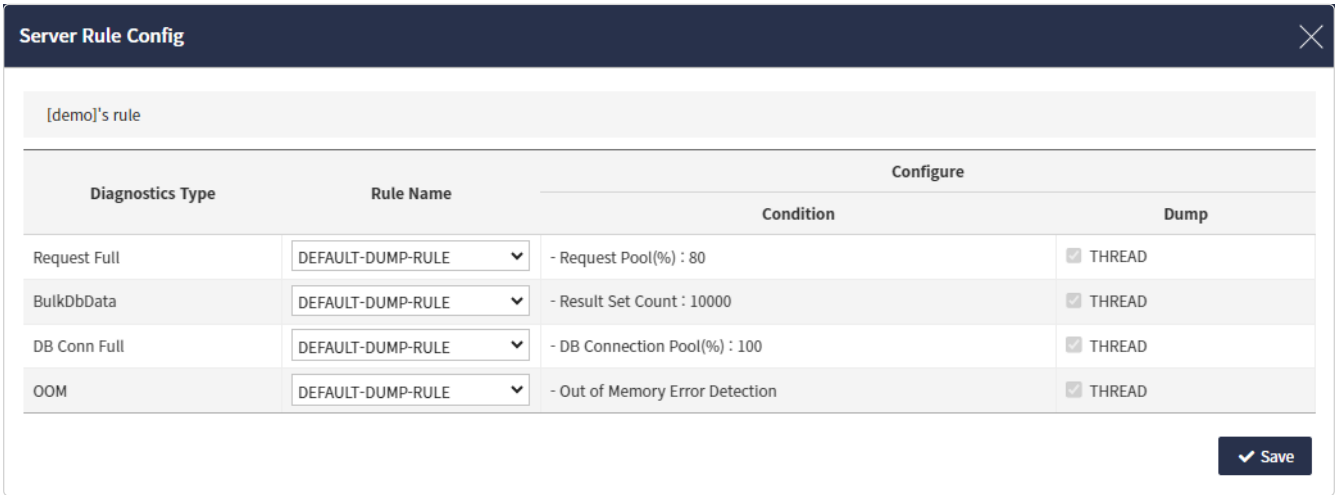
Table 172. OOM Diagnostic Rule

Item	Description	Default Value
Rule Name	Rule name	
OUT OF MEMORY	OOM occurred (judged as Fault situation)	Detected without separate settings
Memory Leak	Memory Leak occurred (judged as Anomaly situation)	Detected without separate settings
Report	Whether to generate Report (always Enable)	Enable
Dump	Dump type to generate when judged as abnormal • THREAD: Thread Dump	Enable

7.6.2. Server Rule Configuration

You can map diagnostic/response Rules to Service Cluster and Enable/Disable them in the DIAGNOSTICS > Policy > Server Rule Setting menu.

Initially, no diagnostic Rules are mapped, so diagnostic/response Rules must be mapped first before performing Enable/Disable functionality. Click on each Service Cluster row to map diagnostic/response Rules to the server as follows.



After diagnostic/response Rules are mapped, you can Enable/Disable Rules in the Server Rule Setting screen as follows.

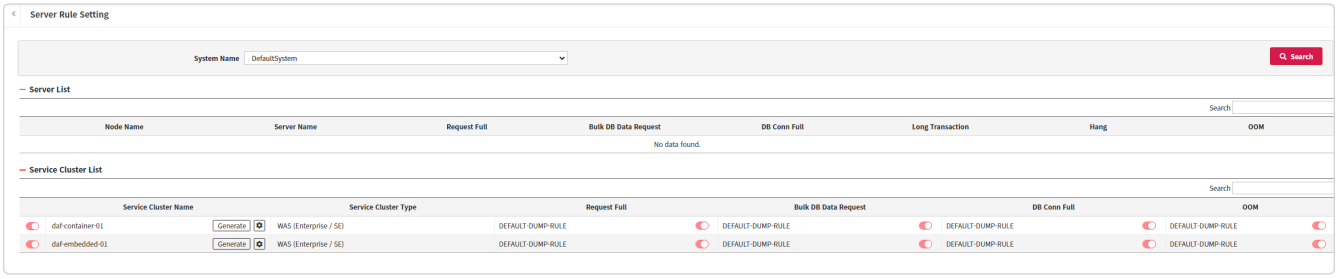


Figure 83. Server Rule Setting Screen

7.7. Trace

Trace records the movement path and time of a Request between LENA Servers to diagnose the cause for failure diagnosis. The Trace types provided by LENA are as follows.

- Session Trace
- Event Trace

You can use various functions through the sub-menus of the DIAGNOSTICS > Trace menu.

7.7.1. Session ID Search

You can check Session Trace information (which Server the Session exists in). To find a Session, the clustered Session Server must be running.

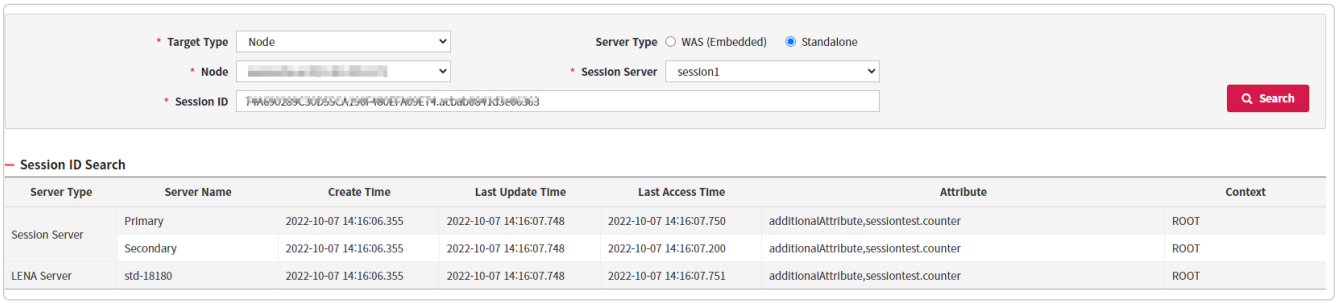


Figure 84. Session Trace Screen

The query result items are as follows.

Table 173. Session Trace Query Result Items

Item	Description	Notes
Server Type	Server type	Session Server: LENA Session Server LENA Server: LENA Application Server
Server Name	Server name	For Session Server, the search target Server is Primary and the Slave Server of the search target server is Secondary
Create Time	Session creation time	

Item	Description	Notes
Last Update Time	Time when Session was last modified	
Last Access Time	Time when the Session was last called on the Server	
Attribute	Session Attribute	
Context	Application Context of the Session	

7.7.2. Event Trace

When an event judged as a failure occurs, you can check the Trace information of that Request.

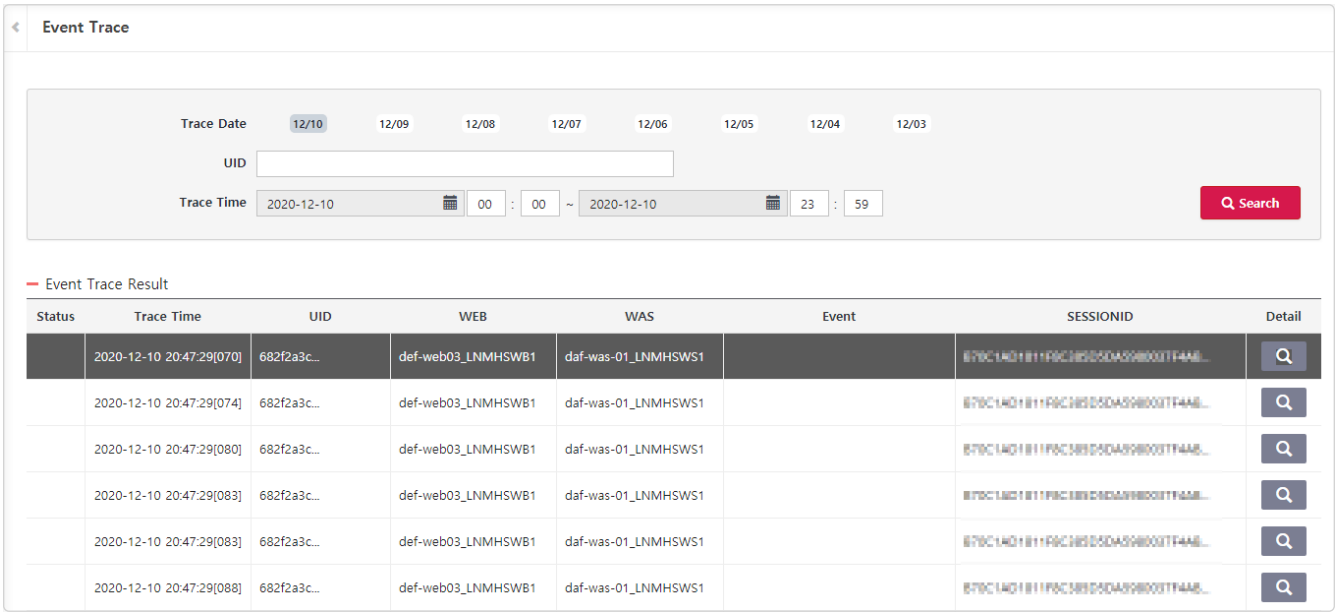


Figure 85. Event Trace Screen

Trace information is stored for only one week. The date when the event occurred is displayed in the Trace Date of the search conditions. The Status item in the search results indicates the importance of the occurred event.

Table 174. Event Trace Search Result Items

Item	Description	Notes
Trace Time	Processing completion time of the Request when the event occurred	Web Server completion time
UID	User ID that called the Request. If one User uses different browsers, UID is processed differently.	
WEB	Web Server that processed the Request	
WAS	WAS that processed the Request	
Event	Occurred Event	
SESSION ID	Session ID of the Request	
Detail	Button to check detailed information	

Click the **Detail Query button** in Detail of the search results to check detailed information. Each item is as follows.

Table 175. Detailed Information Items of Event Trace Information

Item	Description	Notes
Trace Time	Processing completion time of the Request when the event occurred	Web Server completion time
UID	User ID that called the Request. If one User uses different browsers, UID is processed differently.	
WEB	Web Server that processed the Request	
WAS	WAS that processed the Request	
Event	Occurred Event	
JVMRoute	JVMRoute value of the WAS that processed the Request	
SESSION ID	SESSION ID of the Request	
Session Server	Session Server that processed the Request	Displayed as Primary/Secondary Session Server of the connected WAS
URL	URL of the Request	

The events that are traced are as follows. (Event Codes can be checked by viewing Log files. The screen shows the codes as sentences.)

Table 176. Event Codes and Descriptions that are Traced

Event Code	Description	Notes
sywz	Session ID and JVMRoute information are different. (May occur when Failover occurs due to WAS failure.)	Session ID does not match with JVMRoute.
wxso	No Session information in WAS but Session information exists in Session Server. (May occur when Failover occurs due to WAS failure.)	Session does not exist in Application Server.
wosx	Session information exists in WAS but no Session information in Session Server. (May occur when two Session Servers are restarted.)	Session does not exist in Session Server.
wxsx	No Session information in WAS and no Session information in Session Server. (May occur when both Session Servers are stopped)	Session does not exist in any Server.
woxx	Session information exists in WAS but connection to Primary & Secondary session server is broken. (May occur when both Session Servers are stopped)	Session Server does not respond.

Event Code	Description	Notes
wxxx	No Session information in WAS and connection to Primary & Secondary session server is broken. (May occur when the Session in WAS times out and both Session Servers are stopped)	Session Server does not respond.

When sywz event and wxso event occur simultaneously in one Request, both events are displayed in one search result.

7.7.3. Trace Setting

The following is a screen for configuring Event/Time Trace settings.

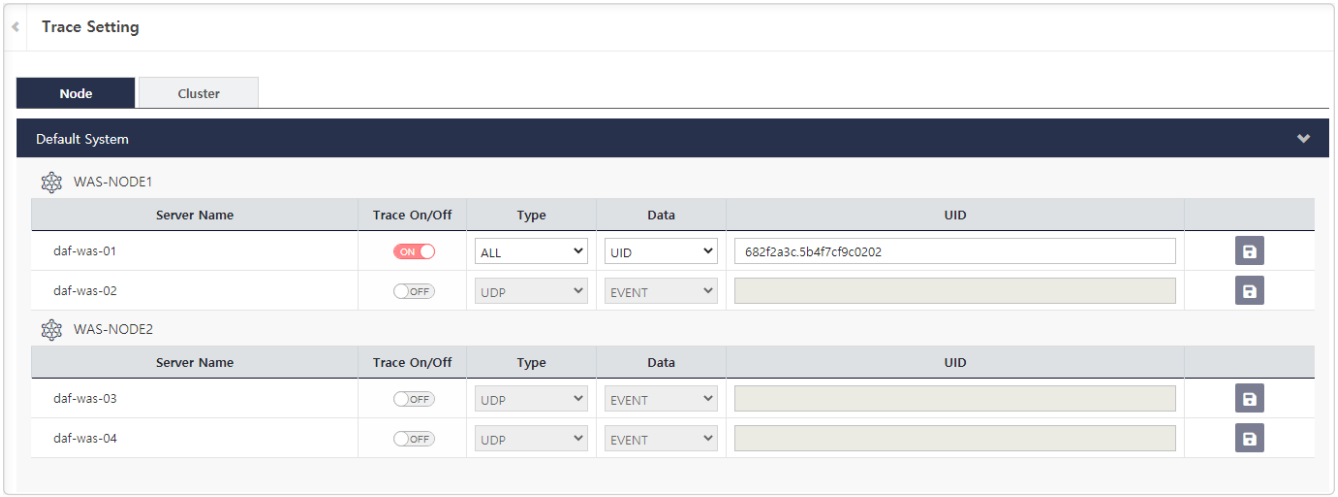


Figure 86. Trace Setting Screen

The Trace configuration items are as follows.

Table 177. Trace Setting Items

Item	Description	Notes
Trace On/Off	Whether to Trace	Applied without restart
Type	UDP: When Trace generation conditions are met, send Trace information to Manager via UDP LOG: When Trace generation conditions are met, save Trace information as Log ALL: When Trace generation conditions are met, use both UDP and LOG functions	
Data	EVENT: Record Trace when Event occurs UID: Record only Requests with the corresponding UID as Trace	
UID	Record only Requests with the entered UID as Trace	

Chapter 8. Topology

You can see the configuration status of each system at a glance, and it provides installation and configuration functions, as well as resource monitoring and start/stop control.

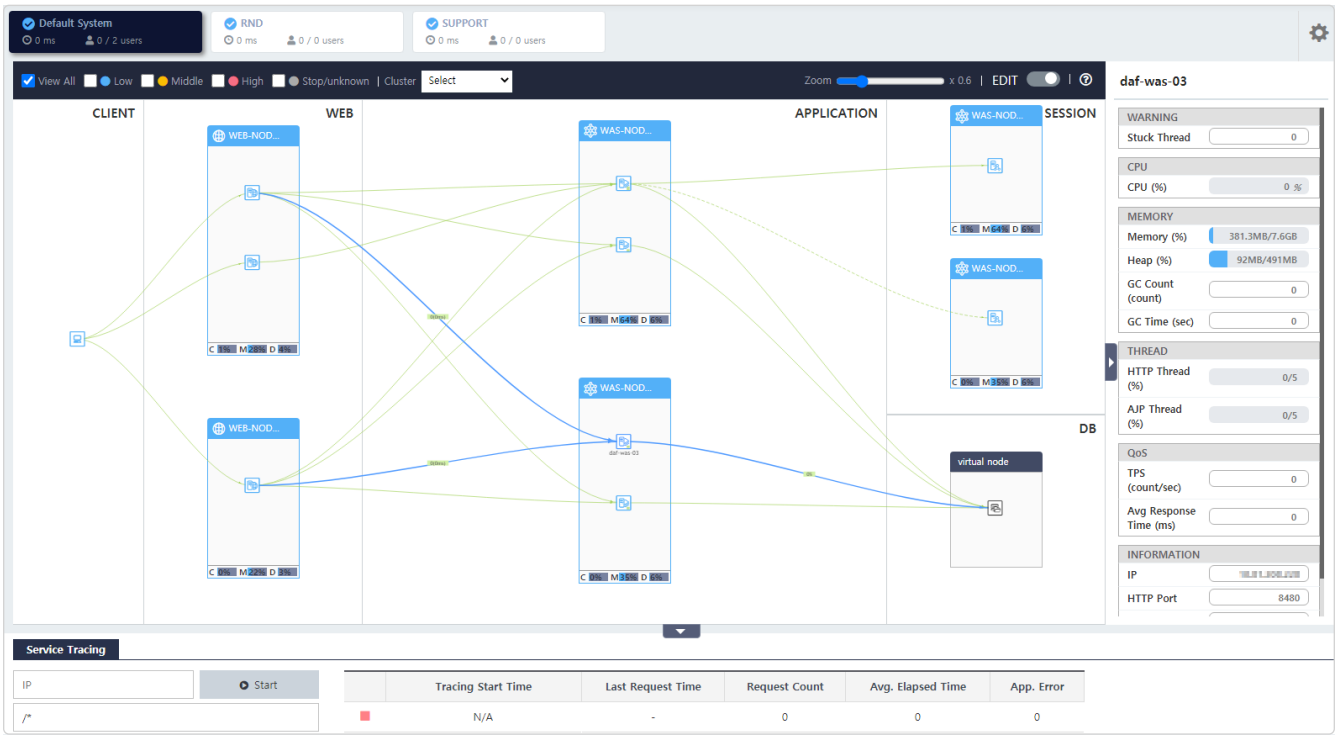


Figure 87. Topology Screen

8.1. Screen Configuration

It is divided into System area, Topology area, Resource monitoring area, and Service tracing area.

- System Area

  Provides a list of registered Systems in card format.

  The icon to the left of the system name in the card represents the system status, which is displayed in 3 levels based on the Resources constituting the system and diagnostic results.

  - **Blue circle icon** : When all servers constituting the system have Low resource usage and diagnostic processes are not performed
  - **Orange circle icon** : When all servers constituting the system have Middle or lower resource usage, or diagnostic process results are in Abnormal status
  - **Red circle icon** : When some servers constituting the system have High resource usage, or diagnostic process results are in Fault status

  The **clock icon** below the system name represents the average response time of WASs within the system, and the **user icon** represents the current number of users (in the last 5 minutes) / total users today.

  > The criteria for Low, Middle, and High resource usage can be changed in DIAGNOSTICS > Policy > Common Rule Setting > Dashboard items.

- Topology Area

Shows the configuration status of nodes and server instances by system in topology chart format. You can install and run Web Server, WAS, and Session Server installed on each Node, perform clustering, and check server status information. Additionally, you can configure integration between Web Server-WAS, WAS-Session Server, and WAS-Datasource.

- Resource Monitoring Area

  Provides detailed resource monitoring information such as CPU and Memory of Nodes and Servers.

- Service Tracing Area

  You can trace services based on specific Client IP and requested Service Pattern to check the number of requests, average response time, and number of service response errors.

Through the **Settings button** on the right side of the system list, you can change the following items:

Chart

- Refresh Interval : Data retrieval cycle for the topology area
- Refresh Topology Chart : Metadata consistency verification and restoration for drawing charts in the topology area

System List

- Selection of Systems to display in the System list and order change

Elements

- Show Endpoint : Setting for displaying the Endpoint area
- Show Edge Info : Setting for displaying detailed information on Edges
- Show Server Name : Setting for displaying server names

Transparency

- Node : Setting transparency for Nodes in the topology area
- Edge : Setting transparency for Edges in the topology area

8.2. Topology Area Details

In topology, information is displayed differently according to the view mode.

- View All : Shows all information.
- Low : Shows only instances with Low resource usage on servers.
- Middle : Shows only instances with Middle resource usage on servers.
- High : Shows only instances with High resource usage on servers.
- Stop/unknown : Shows only stopped instances.

Also, instances are activated and displayed by Cluster unit.

For WAS with diagnostic functionality configured, the diagnostic results of server status (Abnormal or Fault) are checked first before checking resource usage. If the status is determined to be in that state, it is displayed as High status.

8.2.1. Control [Edit: OFF]

Provides detailed monitoring information and control functions from Client to Database from an E2E (End to End) perspective.

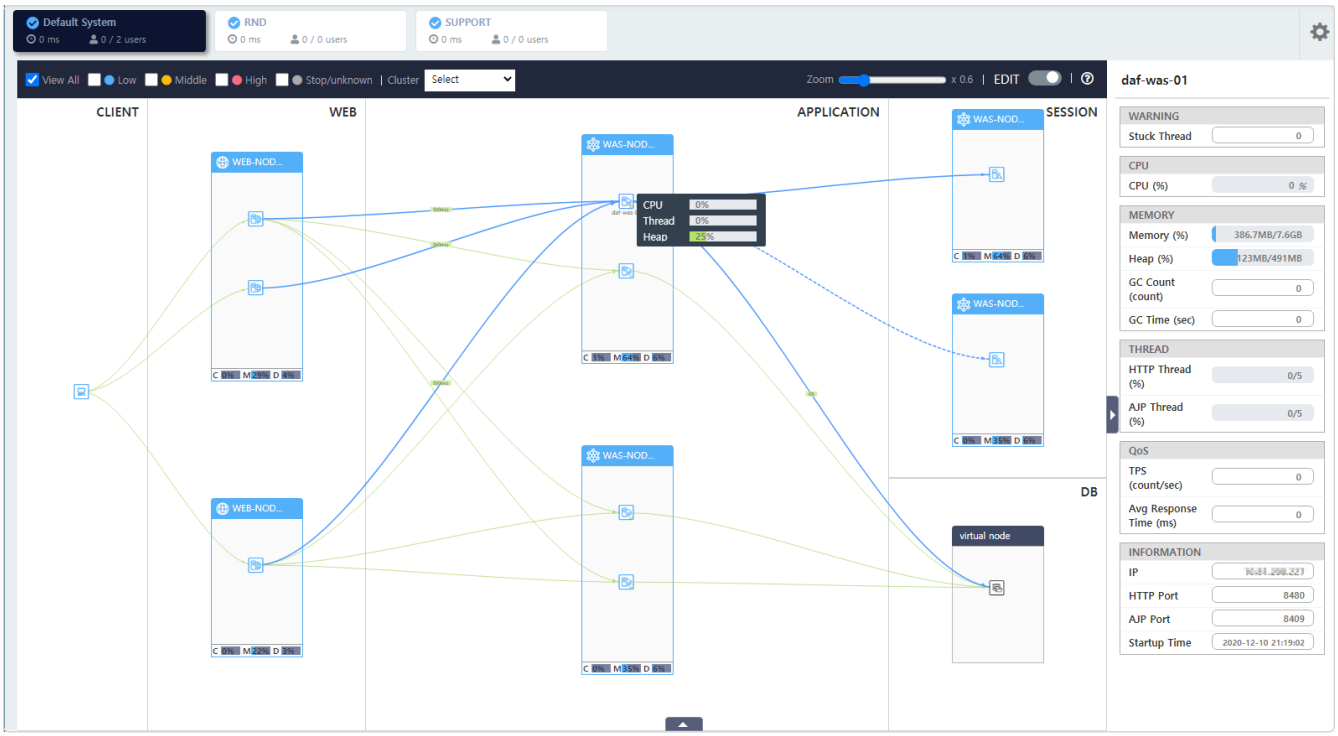


Figure 88. Topology Control [Edit: OFF]

CLIENT Area

Client refers to users, and you can check the browser screen rendering time when users make requests to the Web Server and the content of script errors.

WEB Area

The WEB area provides information about installed Web Nodes and Web servers and allows server control.

- Configuration Information

  Web Node is the area where Web servers are installed, and you can check the server installation status by node.

- Monitoring Information

  Web Node provides basic CPU, Memory, Disk status information by default.

  When you hover over a Web Server, it provides CPU, Memory, Thread status information in a popup form.

  When you select a Web Node and a Server, you can get real-time detailed monitoring information for each in the Resource Monitoring Area on the right side of the Topology Area.

  - Node : CPU, Memory, Disc, Network and basic information
  - Server : CPU, Memory, Thread, QoS and basic information

- Control Functions

Server provides three main control functions.

1. Server Control : Start, Stop, Service Control

Service Control provides uninterrupted deployment functionality. This is a method in which the source corrected for an error service is immediately deployed to the WAS and then the Web Server (timely server) that calls this WAS is configured to forward the error service to the timely server, thereby ensuring normal service provision.

To use this function, the LSC module must be enabled in the Web Server (httpd-lsc.conf file, change LscEnable to On, and restart the server).

After defining the control time, control conditions (Header, Cookie, URL) and the server to forward (http://IP:Port) to save, it connects incoming requests in real-time to the corresponding server according to the defined content, thereby providing service without server restart.

2. Move to : Configuration
3. Cluster : Compare, Sync, Snapshot, Graceful Restart

APPLICATION Area

APPLICATION Area provides information about installed WAS Nodes and WAS servers and allows server control.

- Configuration Information

  WAS Node is the area where WAS servers are installed, and you can check the server installation status by node.

- Monitoring Information

  WAS Node provides basic CPU, Memory, Disk status information by default.

  When you hover over a WAS Server, it provides CPU, Thread, Heap status information in a popup form.

  When you select a WAS Node and a Server, you can get real-time detailed monitoring information for each in the Resource Monitoring Area on the right side of the Topology Area.

  - Node : CPU, Memory, Disc, Network and basic information
  - Server : Warning, CPU, Memory, Thread, QoS and basic information

- Control Functions

  Server provides four main control functions.

  1. Server Control : Start, Stop, Forced Stop
  2. Dump : Thread Dump, Active Service Dump, Heap Dump
  3. Move to : Configuration, Monitoring
  4. Cluster : Compare, Sync, Snapshot, Graceful Restart

SESSION Area

SESSION Area provides information about installed Session Nodes and Session servers and allows server control.

- Configuration Information

  Session Node is the area where Session servers are installed, and you can check the server installation status by node.

- Monitoring Information

  Session Node provides basic CPU, Memory, Disk status information by default.

  When you hover over a Session Server, it provides CPU, Session Count, Heap status information in a popup form.

  When you select a Session Node and a Server, you can get real-time detailed monitoring information for each in the Resource Monitoring Area on the right side of the Topology Area.

  - Node : CPU, Memory, Disc, Network and basic information
  - Server : CPU, Memory, Session Count and basic information

- Control Functions

  Server provides two main control functions.

  1. Server Control : Start, Stop
  2. Move to : Configuration

DB Area

DB Area provides information about the Database connected to WAS. The Database must be registered in the RESOURCE menu. Nodes are represented as virtual nodes to be consistent with other areas. Monitoring and control functions for each DB are not provided.

Edge Information

The connection line means the connection between instances, or between an instance and a Database, and represents the average response time of the server and the number of connected connections.

- Client-WEB : Connection count (Average browser rendering completion time (ms)/Average Web Server response time (ms))
- WEB-APPLICATION : Active Connection count (Average WAS response time (ms))
- APPLICATION-DB : Active Datasource usage rate (%)

End to End monitoring functionality is set to off by default.

Therefore, to view the average browser rendering response time between Client-WEB or the average response time of the server, you must set it in the following order.

1. manager.conf file, set diagnostics.e2e.enable=true
2. In the httpd.conf file of the Web Server, uncomment httpd-eum.conf

```
<IfDefine MOD_EUM>
  #LENA E2E Monitoring Extension settings
  Include ${INSTALL_PATH}/conf/extra/httpd-eum.conf <--
Uncomment this line
</IfDefine>
```

3. Web Server's eum/eum.properties file, modify agent_enable value to true

However, this function is not supported on window OS.

8.2.2. Control [Edit: ON]

When you select the **Edit button** in the upper right corner of the Topology Area, it switches to the editing mode. Here, you can provide node and instance installation functions within the system.

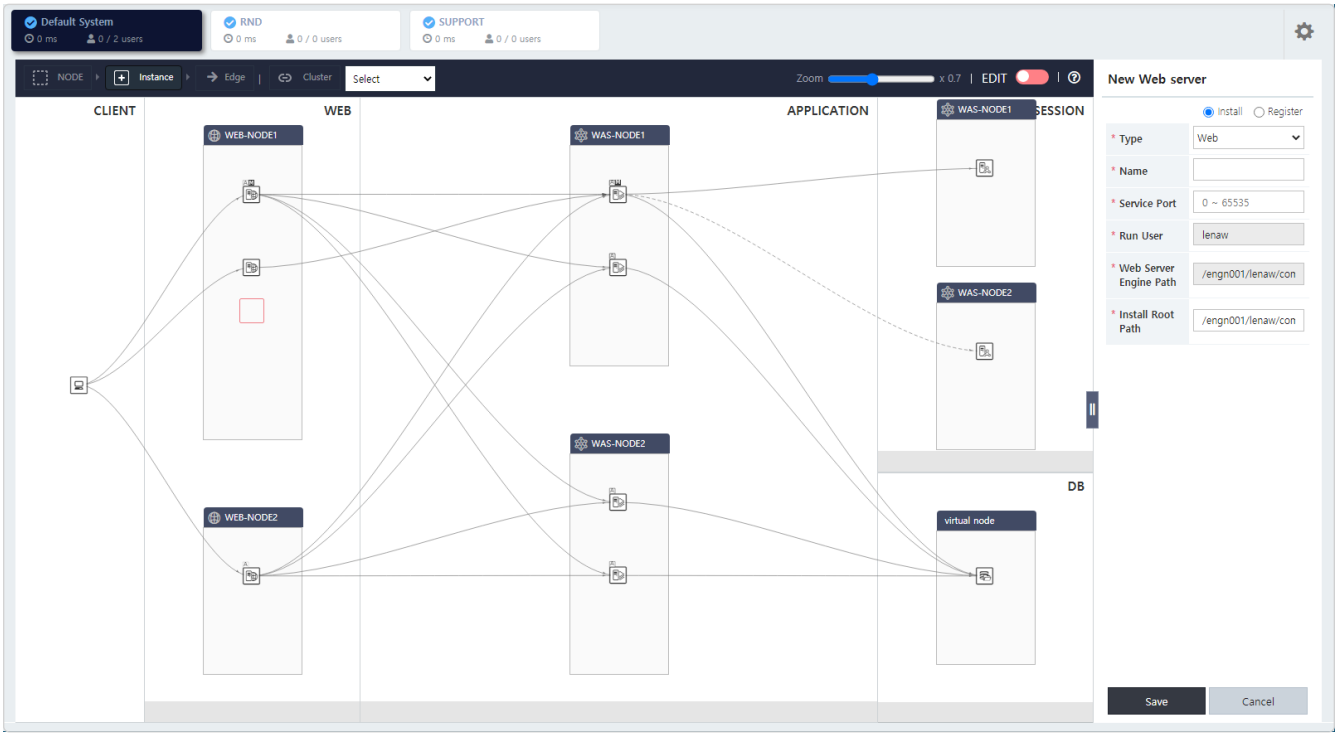


Figure 89. Topology Control [Edit: ON]

Node

The installation/modification/deletion operation of the Node is the same as Node, so only the usage method is described here.

- Installation

1. Select the **Node button** and click on the area you want to install above.
2. Enter the corresponding information in the detailed information area on the right side of the screen.
3. Select the **Save button** .

- Modification
  1. Select the node you want to change.
  2. Change the corresponding information in the detailed information area on the right side of the screen.
  3. Select the **Save button** .
- Deletion
  1. Select the node you want to delete.
  2. Right-click and select Hide, Unregister, Uninstall from the menu.

When deleting a Node, there must be no servers installed in the Node.

Instance

The installation/modification/deletion operation of the Server is the same as server, so only the usage method is described here.

- Installation
  1. Select the **Instance button** and click on the Node above the area you want to install.
  2. Enter the corresponding information in the detailed information area on the right side of the screen.
  3. Select the **Save button** .

The list of Nodes with no servers installed in each area is provided in the gray background below the area, as a square button. If you want to install a server in an empty node, double-click the node button.

- Modification
  1. Select the server you want to change.
  2. Change the corresponding information in the detailed information area on the right side of the screen.
  3. Select the **Save button** .
- Deletion
  1. Select the server you want to delete.
  2. Right-click and select Unregister, Delete from the menu.

Edge

Edge means the connection between servers, and you can connect servers within the WEB-APPLICATION, APPLICATION-SESSION, APPLICATION-DB areas.

- Connection
  1. Select the **Edge button** and drag from the starting server you want to connect to the destination server.

2. Enter the corresponding information in the detailed information area on the right side of the screen.
3. Select the **Save button** .

When connecting between APPLICATION-SESSION, the solid line means the Primary Server, and the dotted line means the Secondary Server.

- Change Connection Information
  1. Select the edge you want to change.
  2. Change the corresponding information in the detailed information area on the right side of the screen.
  3. Select the **Save button** .
- Disconnection
  1. Select the edge you want to delete.
  2. Select the Delete button in the menu of the right-click button.

Cluster

You can set up Server Cluster functionality provided by the CLUSTER menu.

- Creation
  1. Select the **Cluster button** .
  2. Enter the corresponding information in the detailed information area on the right side of the screen.
  3. Select the **Save button** .
- Change
  1. Select the server cluster you want to change in the select box next to the **Cluster button** .
  2. Change the corresponding information in the detailed information area on the right side of the screen.
  3. Select the **Save button** .
- Deletion
  1. Select the server cluster you want to change in the select box next to the **Cluster button** .
  2. Select the **Delete button** in the detailed information area on the right side of the screen.

Chapter 9. Admin

9.1. IAM

Manager provides user management and menu permission management functionality for each user.

9.1.1. Users

User List

The ADMIN > Users menu provides functionality to create, modify, and delete Manager users.

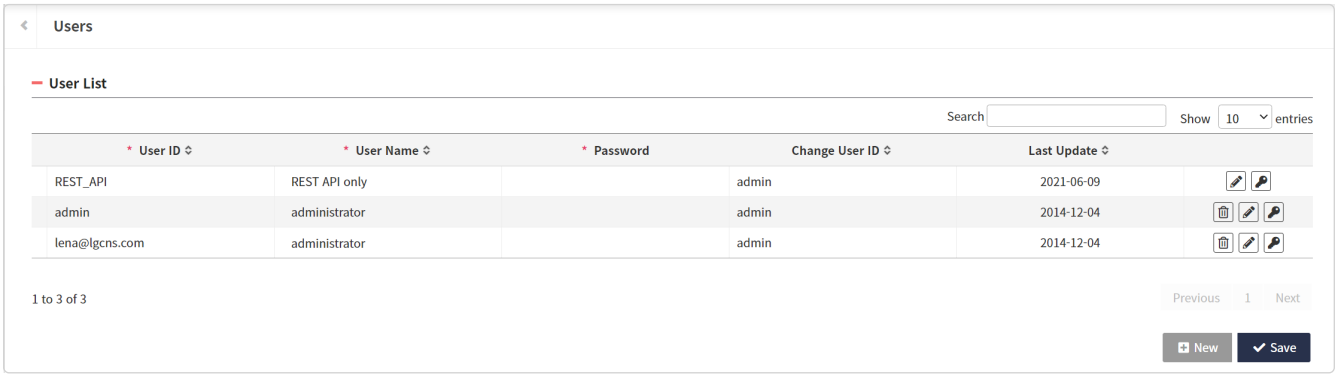


Figure 90. Users Screen

The properties of user management are as follows.

Table 178. User Management Properties

Item (* indicates required)	Description	Remarks
User ID(*)	User identifier	
User Name(*)	User name	
Password(*)	User password	Password must be at least 8 characters combining special characters, numbers, and letters
Change User ID	User who modified and created the user data	
Last Password Update	Date when user password was modified	
+ Icon	Click **New button**, **Edit button** to indicate that selected permission information is being changed	
- Icon	Click **Delete button** to indicate that selected permission information has been deleted	

By default, two users with administrator privileges and one API account are provided. It is recommended to add users beyond the provided users for use.

User Registration

1. Click **New button** to prepare for new user registration.
2. Enter User ID, User Name, and User Password.
   - User passwords are encrypted and stored.
   - Passwords should be 8-20 characters combining uppercase/lowercase letters, numbers, and special characters (!@#$%^*+=-).
3. Click **Save button** to save user information.

- Password encryption uses hash algorithm (SHA-512).

User Modification

1. Click **Edit button** to change the user name and user password.
   - User passwords are encrypted and stored.
2. Click **Save button** to save user information.

- If login to Manager fails 7 times or more, the corresponding ID becomes locked and cannot be used.
- To unlock the locked status, the password for that ID must be modified in the user management screen.
- If there is no user logged into Manager to modify the password, you can run $LENA_HOME/bin/reset-manager-pw.sh to modify the password.

User Deletion

1. Select the user to delete.
2. Click **Delete button** to change the user to deletable status.
3. Click **Save button** to save user information.

Users cannot be deleted when only one user remains.

User Role Inquiry

Manager users must belong to at least one group to acquire menu usage roles. When a user is selected, the Roles for [User ID] table displays the roles assigned to the user.

User Role Addition

1. Click on the user to add a role to, and view the roles currently assigned to the user.
2. Click **Add Role** to open the role list popup.
3. Select the desired role to add.
4. Click **Save button** to save the roles mapped to the user.

User Role Deletion

1. Click on the user to add a role to, and view the roles currently assigned to the user.
2. Click **Delete button** to change the role to deletable status.

3. Click **Save button** to delete the role from the user.

9.1.2. Roles

Manager must create roles for menu-specific permission management. You can create, modify, and delete roles through the ADMIN > Roles menu.

Role List

[admin roles] | manual/admin_roles.png

Figure 91. Roles Screen

The properties of permission management are as follows.

Table 179. Permission Management Properties

Item (* indicates required)	Description	Remarks
Role ID(*)	Role identifier	
Role Name(*)	Role name	
Description	Description of the registered role	
Permissions	Permissions allowed for the role	
Change User ID	User who modified and created the role data	
Last Update	Date when role data was modified and created	
+ Icon	Click **New button**, **Edit button** to indicate that selected role information is being changed	
- Icon	Click **Delete button** to indicate that selected role information has been deleted	

Role Creation

1. Click **New button** to prepare for new permission registration.
2. Enter Role ID, Role Name, and Role Description.
3. Click **Save button** to save role information.

Role Modification

1. Select the role to modify.
2. Click **Edit button** to change the role name and role description.
3. Click **Save button** to save role information.

Role Deletion

1. Select the role to delete.
2. Click **Delete button** to change the role to deletable status.
3. Click **Save button** to save role information.

Role-Menu Mapping

You can configure accessible menus for each role created in LENA Manager. Select one role among the roles created through role selection to configure menu permissions. Select the menu to configure access control from the menu list showing all menus registered in LENA Manager and configure menu permissions.

Menu Permission Inquiry

When you select the desired role from the role list, the menu access permissions for the selected role are displayed below.

When adding Node, Server, Server Cluster, Resource in the sub-screens of "SERVER", "CLUSTER", "RESOURCE" menus, the added items are automatically displayed in the menu list of the "Menu Permission Management" screen.

Therefore, to add new menus, register and create each item in the "SERVER", "CLUSTER", "RESOURCE" sub-screens.

When changing permissions for a server, the same permissions must be reflected in the menus below.

- The corresponding server under "SERVER"
- The corresponding server under "CLUSTER"

If this is not followed and you configure permissions for some server menus under Server Cluster as follows (example, not recommended):

- Server under "SERVER": Has permission
- Server under "CLUSTER": No permission

In this case, the menu and Server Cluster, Server permissions are expressed as follows:

- Number of servers constituting Server Cluster: Number of servers with permissions based on "CLUSTER" sub-server permissions
- Sub-menus of Server Cluster: Only servers with permissions based on "CLUSTER" sub-server menu permissions are visible
- Server list in Server Cluster's Overview, Application Server, Web Server tabs: Since it must show the configuration information of Server Cluster, all server lists are retrieved regardless of "CLUSTER" sub-permissions
- Server detail links in Server Cluster's Overview, Application Server, Web Server tabs: Since it's access to individual servers, access to servers without permissions under the "SERVER" menu is blocked

Menu Permission Mapping

1. Select the menu to configure permissions.
   - When selecting permissions, permissions for menus are also displayed.
2. Select the menu to configure permissions from the menu list.
   - When selecting a menu, menu permissions are displayed in the menu permission list.
3. If permission changes are needed, select Y or N.

4. Click **Save button** to save menu permission information.

9.2. License

Manager provides functionality to view and renew currently applied licenses for each node.

9.2.1. License List

When you open the License screen, you can view the list of currently applied licenses by node.

You can verify the license status by checking the Status item.

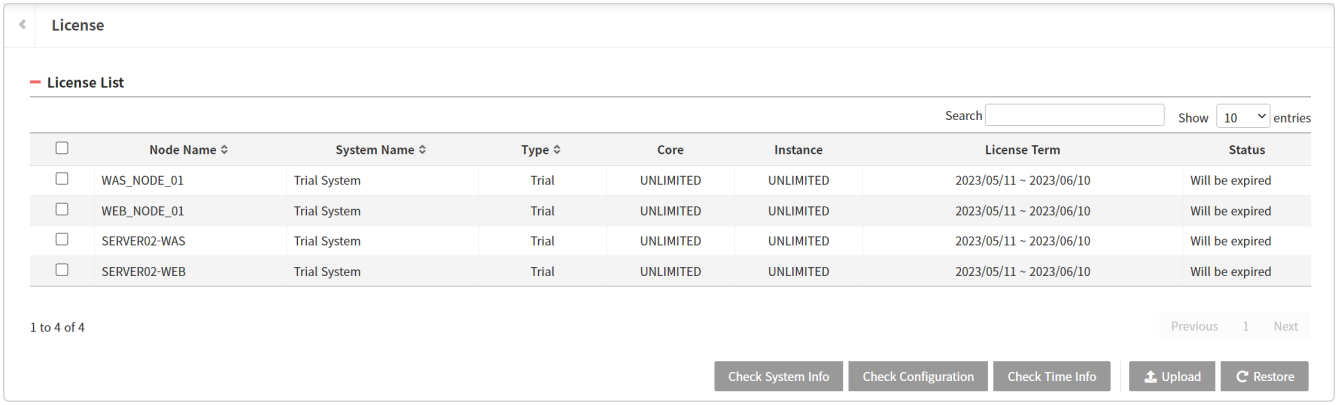


Figure 92. License List Screen

9.2.2. License Details

When you click on a license in the license list, you can verify the detailed information of the license.

The detailed information items are as follows.

Table 180. License Detail Information Items

Item	Description	Remarks
Node Name	Node name	
Type	License classification	Trial, Standard
Customer Name	Purchasing customer company name	
System Name	Installed system name	
Issue No	License issue number	
Issue Date	License issue date	
License Term	License allowed period	
Lena Home	Lena Home path	
IP Address	Node's IP address	
Hardware ID	ID that recognizes H/W	MAC Address or Host name

Item	Description	Remarks
Contract CPU Core Limit	Maximum core count under contract	
CPU Core Limit	Actually measured core count	
Contract Instance Limit	Maximum instance count under contract	
Instance Limit	Actually measured instance count	
Contract Type	Contract type	Subscription, Perpetual
Node Type	Node type	WEB, WAS, MDS
LENA Version	LENA version	
Status	License validity status	

Notification messages are provided 15 days before the license expiration date. You can verify notification messages from the **bell icon** in the upper right corner of Manager.

9.2.3. License Upload / Recovery

Upload

Select the node to apply a new license from the node list and use the **Upload button** at the bottom of the list. When you click this button, a license upload popup window opens where you can find and upload the issued license file, and the license will be applied to the selected nodes.

Recovery

Select the node to recover the license from the node list and use the **Restore button** at the bottom of the list. When you click this button, the license is recovered from the backup file.

9.2.4. License-related System Status Check

In the license list view screen, select a Node and click **Check System Info button**, you can verify the system status required for license issuance.

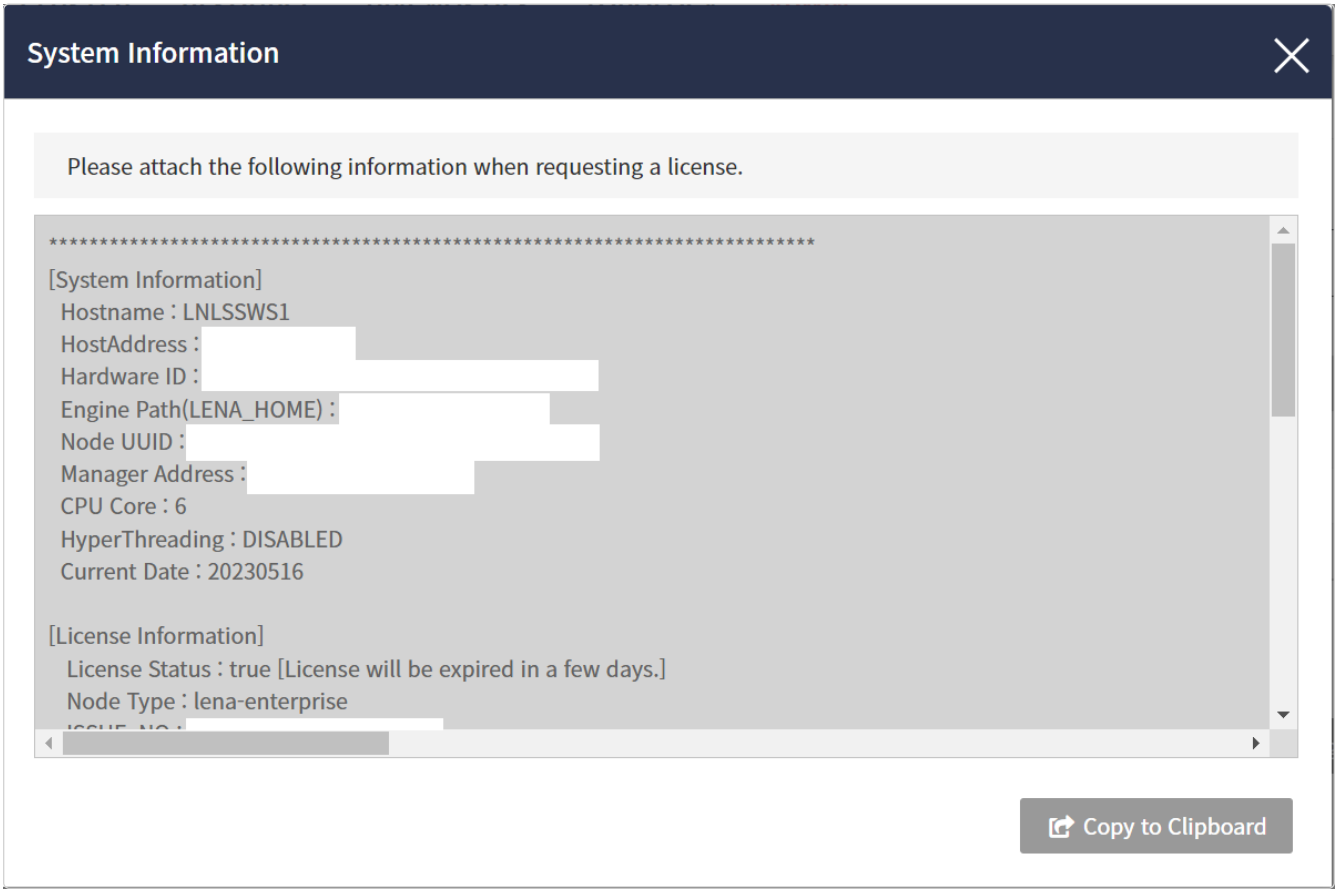


Figure 93. System Information

Shell Scripts are also provided in CLI environment to check license status for each node. The shell file is ${LENA_HOME}/bin/check-license.sh. An example of the result of running this script is as follows.

check-license.sh Execution Example

```
[bin]$ ./check-license.sh
*************************************************************************
[System Information]
  Hostname : solweb2
  HostAddress : 127.0.0.1
  Hardware ID : 52:54:00:E9:AC:A1 ( 52:54:00:E9:AC:A1 )
  Engine Path(LENA_HOME) : /engn001/lena/dev
  Node UUID : e46da220-db50-3854-84a0-7b61e1b6e7cd
  Manager Address : 127.0.0.1:7700
  CPU Core : 4
  HyperThreading : DISABLED
  Current Date : 20180705

[License Information]
  License Status : true [License is valid.]
  Node Type : lena-enterprise
  ISSUE_NO : 201807041532438300001
  TYPE : Standard
  CUSTOMER_NAME : LG
  SYSTEM_NAME : CNS
  SYSTEM_TYPE : PROD
  HARDWARE_ID : 52:54:00:E9:AC:A1
  LENA_HOME : /engn001/lena/dev
  CONTRACT_CPU_CORE_LIMIT : 8
  CPU_CORE_LIMIT : 8
  CONTRACT_INSTANCE_LIMIT : 8
  INSTANCE_LIMIT : 8
  MANAGER_ADDRESS : UNLIMITED
  WEB_CONTRACT_CPUCOREDAY_LIMIT :
  WEB_CPUCOREDAY_LIMIT : N
  WAS_CONTRACT_CPUCOREDAY_LIMIT :
  WAS_CPUCOREDAY_LIMIT : N
  RE_ISSUEANCE :
  USE_POSTPAID :
  START_DATE : 20180501
  END_DATE : 20190531
  LICENSE_KEY :
H2VaDEE9fjFlvHBRsQeGXasYT5l4tBc6ebayNIdtVZ5/lj4/EM0mYf38karMTKgcLLmPMMFa8BOEFt
5zRfBc/IiOxlmDgy
j0+iq30ABfJoyAhY3nWBVJhBy7h0U3hzJWr1hyCuZMFAHquL4dinwWAqmJeL+jntJKFufD38vdF2Yw
KEoRNH9dGQnqXZHO
U8wQZmN4UHk5YB5/O6YIUfFNGU3wyzjfKCfF9Golu9zQAsSZ358ptjC/TBUy+ccvLa75H32XPxiNSS
xytn0hGFbcVc61kv
zi7YMNUgnuEyDEQ/dhFKxJ17ijUQBZj5xbFQ9qUTzL1QKGLl+cbYVsr6kvZg==
*************************************************************************
```

The output items are the same as described in the previous section, and since they output basic information required for license issuance, they are utilized when requesting license issuance.

Among the output items, "HyperThreading" checks whether HyperThreading is used, and when HyperThreading is used, the core count is calculated as 2 times the physical core count.

9.2.5. Host-based License Check Configuration

License checks the target H/W according to the contract using Mac Address or Host name. Since the default configuration is based on Mac Address, to execute license check based on Host name, for Linux/Unix OS, open the start-agent.sh, check-license.sh files located in ${LENA_HOME}/bin and each Application Server's setenv.sh file and modify them as follows.

start-agent.sh File Configuration (Add to variable $JAVA_OPTS)

```
JAVA_OPTS="$\{JAVA_OPTS} -Dlicense.check-type=hostname"
```

check-license.sh File Configuration (Uncomment the following item)

```
_JAVA_OPTS="$\{_JAVA_OPTS} -Dlicense.check-type=hostname"
```

Each Application Server's setenv.sh File Configuration (Uncomment the following item)

```
CATALINA_OPTS=" $\{CATALINA_OPTS} -Dlicense.check-type=hostname"
```

9.2.6. Time Information Inquiry

In the license list, select the node for which you want to check time information, then click **Check Time Info button**, you can verify the time and timezone information for the selected nodes.

9.3. License(Scaling)

Manager provides functionality to view and renew currently applied Manager License.

9.3.1. Manager License

You can verify the status, usage, and usage period of Manager License. You can upload License files through **Upload Manager License button**. The uploaded License is transmitted to VMs during Scale-out and performs authentication when starting servers.

9.3.2. License List

You can view the list of currently applied licenses by node. You can verify the license status by checking the Status item.

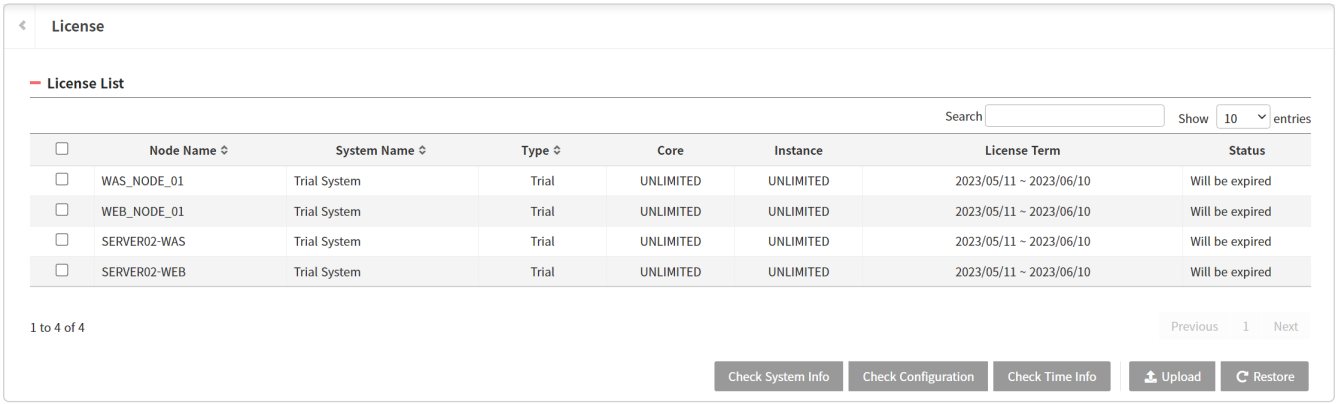


Figure 94. License List Screen

9.3.3. License Details

When you click on a license in the license list, you can verify the detailed information of the license.

The detailed information items are as follows.

Table 181. License Detail Information Items

Item	Description	Remarks
Node Name	Node name	
Type	License classification	Trial, Enterprise, Standard, Developer
Customer Name	Purchasing customer company name	
System Name	Installed system name	
Issue No	License issue number	
Issue Date	License issue date	
License Term	License allowed period	
Engine Path	LENA Engine installation path	
IP Address	Node's IP address	
Hardware ID	ID that recognizes H/W	MAC Address or Host name
Contract CPU Core Limit	Maximum core count under contract	
CPU Core Limit	Actually measured core count	
Contract Instance Limit	Maximum instance count under contract	
Instance Limit	Actually measured instance count	
Status	License validity status	

9.3.4. License Upload / Recovery

Upload

Select the node to apply a new license from the node list and use the **Upload button** at the bottom of the list. When you click this button, a license upload popup window opens where you can find and upload the issued license file, and the license will be applied to the selected nodes.

Recovery

Select the node to recover the license from the node list and use the **Restore button** at the bottom of the list. When you click this button, the license is recovered from the backup file.

9.3.5. License-related System Status Check

In the license list view screen, select a Node and click **Check System Info button**, you can verify the system status required for license issuance.

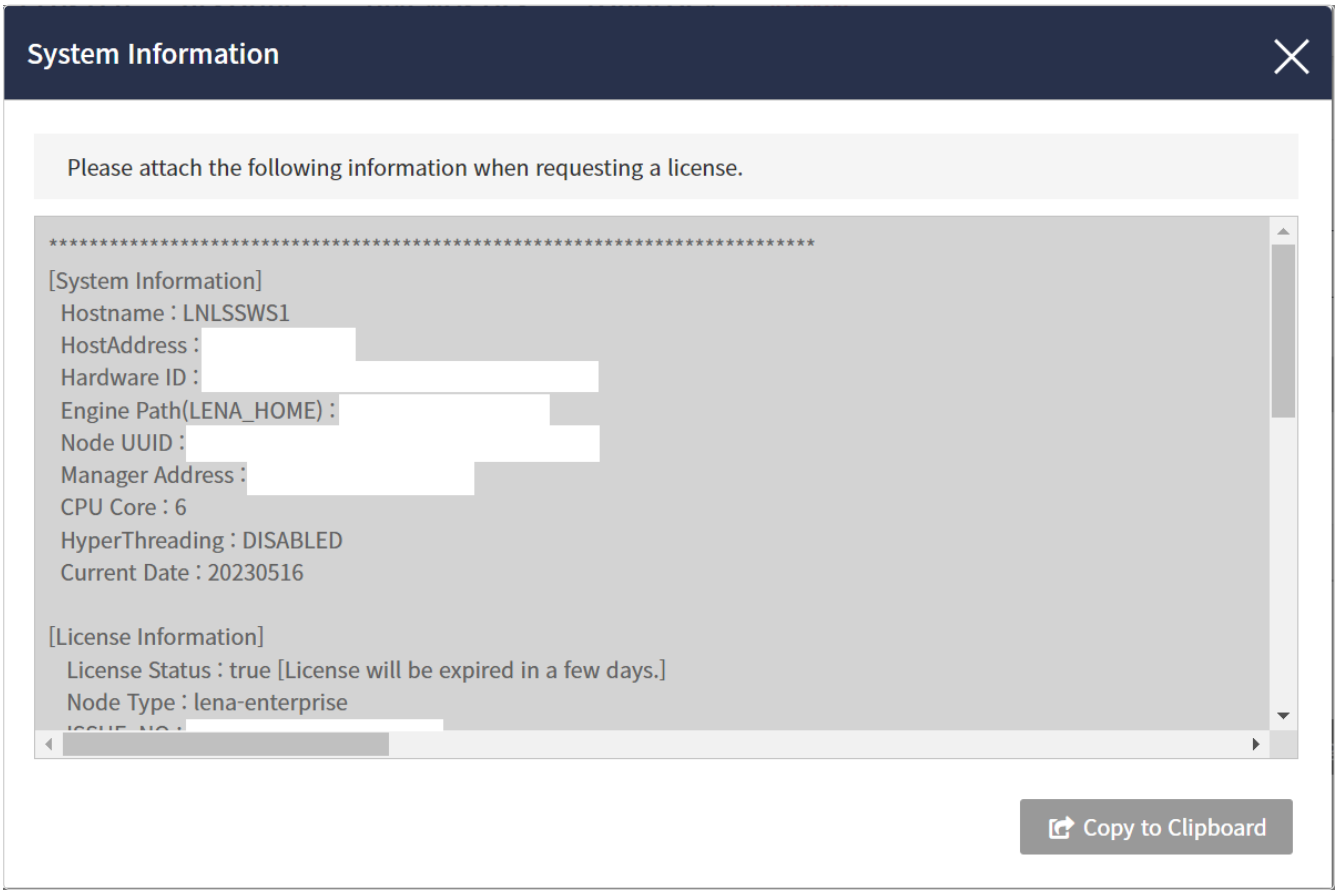


Figure 95. System Information

Shell Scripts are also provided in CLI environment to check license status for each node. The shell file is ${LENA_HOME}/bin/check-license.sh (check-license.bat for Windows version). An example of the result of running this script is as follows.

check-license.sh Execution Example

```
[bin]$ ./check-license.sh
**************************************************************************
[System Information]
  Hostname : solweb2
  HostAddress : 127.0.0.1
  Hardware ID : 52:54:00:E9:AC:A1 ( 52:54:00:E9:AC:A1 )
  Engine Path(LENA_HOME) : /engn001/lena/1.3
  Node UUID : e46da220-db50-3854-84a0-7b61e1b6e7cd
  CPU Core : 4
  HyperThreading : DISABLED
  Current Date : 20180705

[License Information]
  License Status : true [License is valid.]
  ISSUE_NO : 201807041532438300001
  TYPE : Enterprise
  CUSTOMER_NAME : LG
  SYSTEM_NAME : CNS
  SYSTEM_TYPE : PROD
  HARDWARE_ID : 52:54:00:E9:AC:A1
  LENA_HOME : /engn001/lena/1.3
  CONTRACT_CPU_CORE_LIMIT : 8
  CPU_CORE_LIMIT : 8
  CONTRACT_INSTANCE_LIMIT : 8
  INSTANCE_LIMIT : 8
  START_DATE : 20180501
  END_DATE : 20190531
  LICENSE_KEY :
H2VaDEE9fjFlvHBRsQeGXasYT5l4tBc6ebayNIdtVZ5/lj4/EM0mYf38karMTKgcLLmPMMFa8BOEFt
5zRfBc/IiOxlmDgy
j0+iq30ABfJoyAhY3nWBVJhBy7h0U3hzJWr1hyCuZMFAHquL4dinwWAqmJeL+jntJKFufD38vdF2Yw
KEoRNH9dGQnqXZHO
U8wQZmN4UHk5YB5/O6YIUfFNGU3wyzjfKCfF9Golu9zQAsSZ358ptjC/TBUy+ccvLa75H32XPxiNSS
xytn0hGFbcVc61kv
zi7YMNUgnuEyDEQ/dhFKxJ17ijUQBZj5xbFQ9qUTzL1QKGLl+cbYVsr6kvZg==
**************************************************************************
```

The output items are the same as described in the previous section, and since they output basic information required for license issuance, they are utilized when requesting license issuance.

Among the output items, "HyperThreading" checks whether HyperThreading is used, and when HyperThreading is used, the core count is calculated as 2 times the physical core count.

9.3.6. Host-based License Check Configuration

License checks the target H/W according to the contract using Mac Address or Host name. Since the default configuration is based on Mac Address, to execute license check based on Host name, for Linux/Unix OS, open the start-agent.sh, check-license.sh files located in ${LENA_HOME}/bin and each Application Server's setenv.sh file and modify them as follows.

start-agent.sh File Configuration (Add to variable $JAVA_OPT)

```
JAVA_OPTS="$\{JAVA_OPTS} -Dlicense.check-type=hostname"
```

check-license.sh File Configuration (Uncomment the following item)

```
_JAVA_OPTS="$\{_JAVA_OPTS} -Dlicense.check-type=hostname"
```

Each Application Server's setenv.sh File Configuration (Uncomment the following item)

```
CATALINA_OPTS=" $\{CATALINA_OPTS} -Dlicense.check-type=hostname"
```

9.3.7. Time Information Inquiry

In the license list, select the node for which you want to check time information, then click **Check Time Info button**, you can verify the time and timezone information for the selected nodes.

9.4. License(Container)

Through Manager, you can view licenses applied to containers and see the current status/list of servers in service.

9.4.1. Container License

Shows the status, usage, and usage period of Container License. Click **Check System Info button** to verify system information such as Manager UUID.

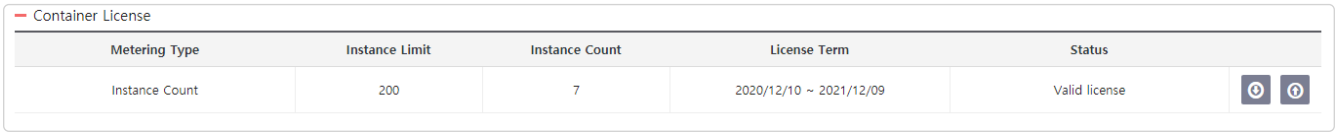


Figure 96. Container License

9.4.2. Server Instance Count

Shows the number of started containers in a graph based on Month/Day. When based on Month, it shows the cumulative value of server count by day in a graph, When based on Day, it shows the cumulative value of server count by hour in a graph.

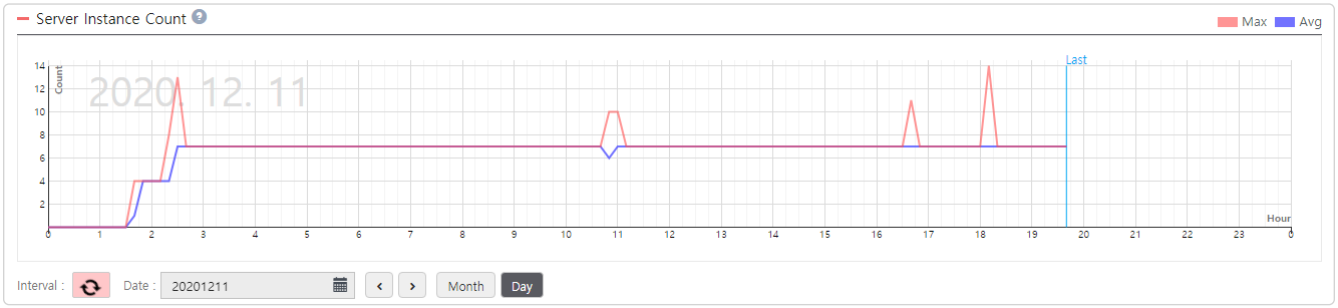


Figure 97. Server Instance Count

9.4.3. Server List

Shows the list of containers currently in service.

Server List

Search Show 10 entries

Status	Start Time	Elapsed Time	Name	Address	Service Port
✓	2020-12-11 18:14:48	1H 16m	lena-session-1	10.42.157.151	5180
✓	2020-12-11 18:14:48	1H 16m	lena-session-0	10.42.157.163	5180
✓	2020-12-11 18:15:07	1H 16m	lena-was-5758c76996-cbhq7	10.42.157.190	8180
✓	2020-12-11 18:15:07	1H 16m	lena-was-5758c76996-plxsv	10.42.157.164	8180
✓	2020-12-11 18:15:28	1H 16m	lena-web-585f64fc4-gbx99	10.42.157.167	7180
✓	2020-12-11 18:15:28	1H 16m	lena-web-585f64fc4-lb9w9	10.42.157.160	7180
✓	2020-12-11 18:15:27	1H 16m	lena-web-585f64fc4-dmphf	10.42.157.168	7180

1 to 7 of 7 Previous 1 Next

Figure 98. Server List

9.5. Security (Service Control)

This is a functionality to restrict user requests to Application Server based on IP or URL.

9.5.1. Rule Setting (Rule Configuration)

When you want to control requests from specific IPs or URLs, configure new rules through the screen. Provides search functionality for convenience in new rule configuration and rule deletion. Server attributes applied to all applications can be processed as error pages.

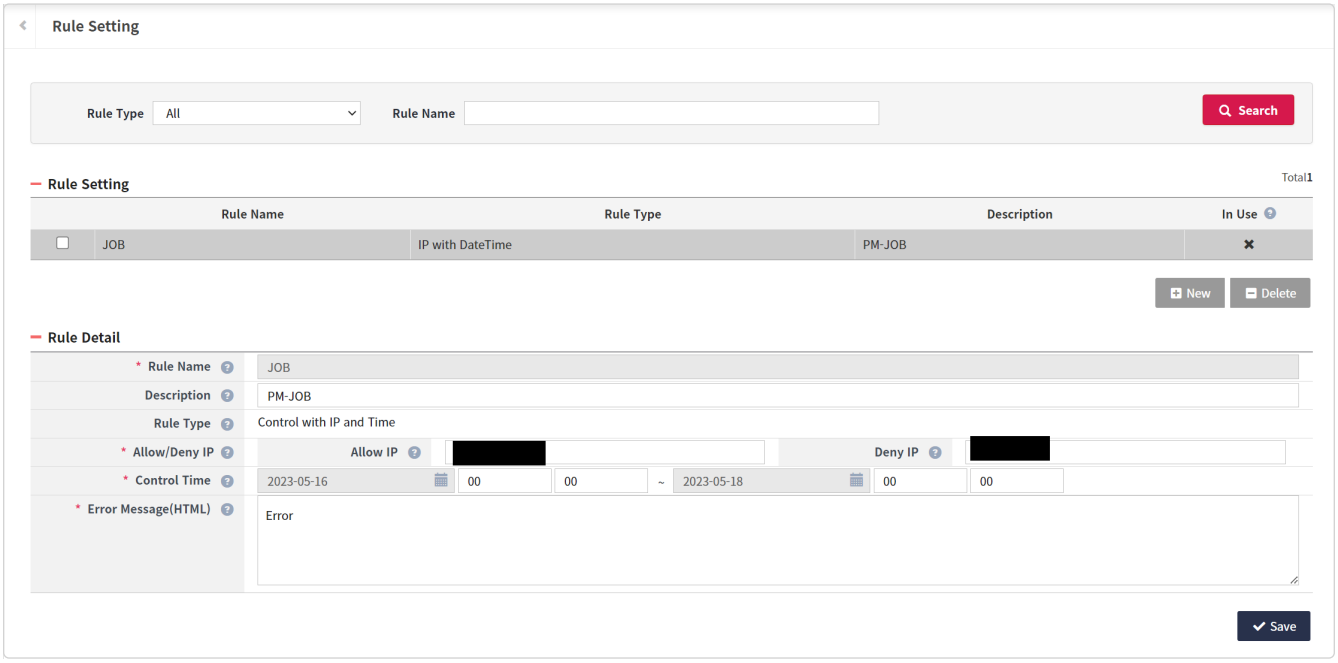


Figure 99. Rule Setting Screen

The Use column in the Rule list indicates whether the corresponding rule is applied to the Application Server.

The configurable properties when adding rules are as follows.

Table 182. Configurable Properties When Adding Rules

Item (* indicates required)	Description	Remarks
Rule Name(*)	Name of the rule to add	
Description	Description of the rule to add	
Rule Type	Unit to control	IP, URL
Allow IP(*)	IP addresses to allow requests from	Can be entered in regex format
Deny IP(*)	IP addresses to deny requests from	Can be entered in regex format
Control Time(*)	Time unit to apply the rule	
Error Message(HTML)(*)	Error page to display for requests filtered by control	

If you apply a rule with control type "IP with DateTime" to an Application Server that is relayed through a Proxy Server, you may not be able to apply the rule because User IP cannot be obtained due to the Proxy Server's security characteristics.

Applied rules among created rules cannot be deleted.

9.5.2. Rule Applying (Rule Application)

Select one of the added rules to apply to the Application Server. Provides search functionality for rule

type, application unit, and rule name for convenience in application.

Select one from the rule list and use **shuffle buttons** in rule application to select the target to apply, then click **On/Off button** to apply and save. To exclude from the application target, also use **shuffle buttons** to exclude.

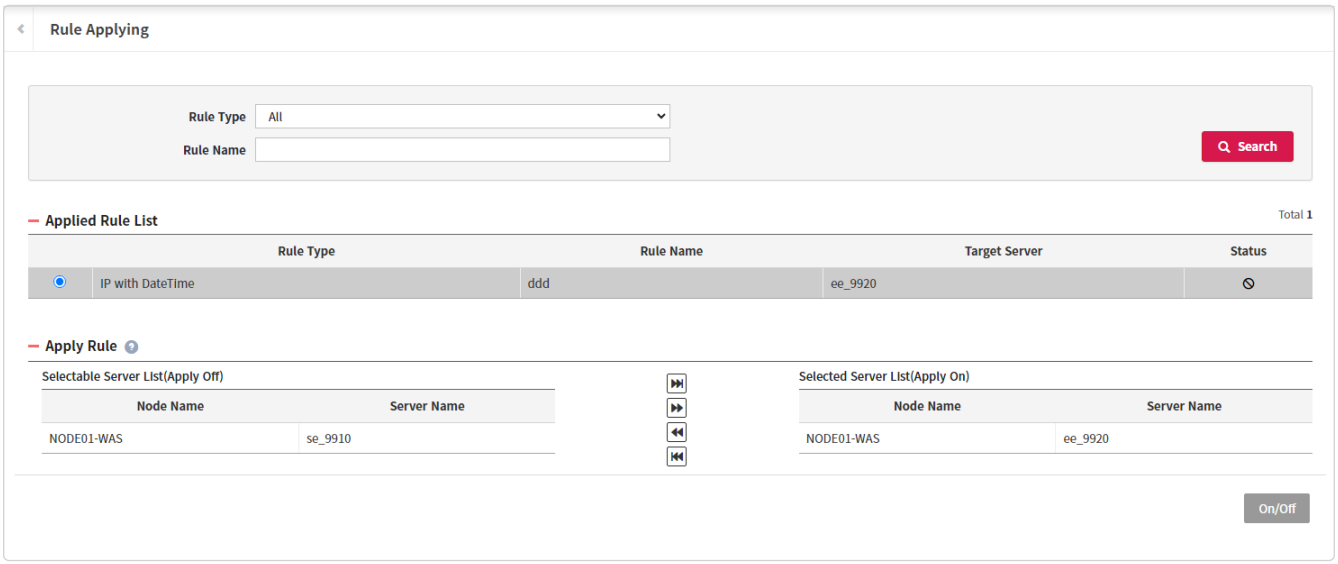


Figure 100. Rule Applying Screen

The properties used in the rule status and application screen are similar to the rule configuration screen, and the following properties are additional properties.

Table 183. Additional Properties

Item	Description	Remarks
Node Name	Node name under the registered system	
Server Name	Server name under the registered node	

When new targets are added to the selected rule, they are added to server.xml or context.xml according to the application unit, and when excluding from the applied targets, the rule configuration added to the above configuration files is deleted.

9.5.3. Service Control Log (Rule Application Result Inquiry)

The processing results for items with applied rules are output as a list. Provides search functionality for rule type, application unit, rule name, and log time for convenience in processing result verification.

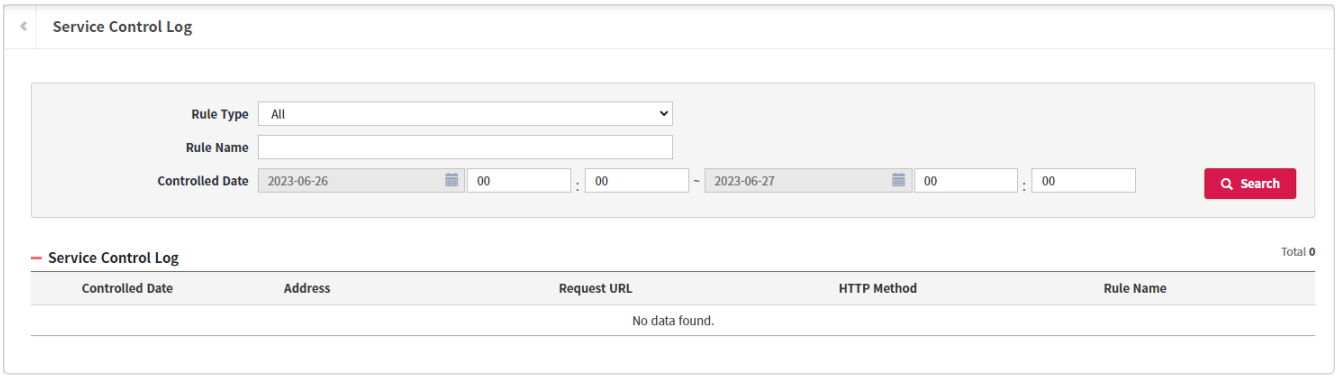


Figure 101. Service Control Log Screen

The properties used in the processing list are as follows.

Table 184. Log Information Items

Item	Description	Remarks
Controlled Date	Processing time of the request with applied rule configuration	
Address	Processed remote address	
Request URL	URL of the processed request	
HTTP Method	HTTP Method of the processed request	
Rule Name	Name of the rule applied to process the request	

For rule history, you must configure the access filter log aggregation listener usage in the Manager's /conf/manager.conf configuration file to true. Logs are recorded in the access_filter.log."date".txt file in each server's logs folder, and Manager periodically aggregates logs from each server and stores them in the database. (At this time, aggregated logs are backed up in access_filter_log."date".txt.gathered file) Aggregated logs in the database can be verified in the processing list screen.

The configuration example for the configuration file item in manager.conf is as follows.

```
#Whether to use access filter log aggregation listener and
operation cycle (seconds) default is false, 60
accessfilter.listener=false
accessfilter.interval=60
```

9.6. Notification configuration

You can configure notifications to be displayed in Manager and SNS information to be linked with notifications.

9.6.1. Manager Notification

When you open the Manager Notification menu, you can verify currently active notifications, and levels are classified as Critical, Warning, and Info.

If you uncheck the notification checkbox and save, even if a notification occurs, it will not be displayed on the bell icon.

Notifications that are not displayed on the icon can be verified by clicking the Notification Detail button in the upper right corner of the popup that appears when you click the bell icon.

9.6.2. SNS Notification

You can manage SNS information to be linked with notifications generated in Manager.

It operates based on WebHook and can be linked with SNS at the system level.

Table 185. Detailed Information Items for SNS to be Linked

Item	Description
Name	Name specified by the user
System	Name of the system to be linked
DuplicateTime(s)	If the same notification occurs consecutively within DuplicateTime(s), it is not linked to SNS.
Request	Method to send the request
Encoding	Encoding of the request
Header	You can input the request header, and if using multiple headers, separate them with line breaks.
Body	You can input the request body, and the replaceable parameters are as follows: ${alarmLevel} - Level of the generated alarm, ${message} - Message content
Webhook URL	URL to send the request to
SSL	Whether SSL authentication is required

Table 186. Types of Notifications to be Linked with SNS

Item	Description
AUDIT	When a notification occurs from items specified in the server's Audit configuration
DIAGNOSTICS	When a notification occurs that violates the DIAGNOSTICS Rule configured on the server
LICENSE	When a LICENSE-related notification occurs
INFO	When a notification related to server information occurs

After entering the configuration items, you can verify whether the request works normally through the Test button.

If the test is successful, save it through Save, then configure the item's on/off toggle to on to enable the linkage.

9.7. Patch

Provides patches for functional improvements and bug fixes of installed LENA.

Patches are provided in compressed file format and operate as independently running Java processes.

Patch functionality can be executed through CLI and Management UI, and in case of service issues during patching, you can restore to the original state through the Restore functionality.

The patch sequence is as follows.

1. Patch file upload

2. Manager patch application
3. Node patch application
4. Server (Application Server, Session Server) patch application
5. Patch commit

The recovery sequence is as follows.

1. Server patch recovery
2. Node patch recovery
3. Manager patch recovery
4. Recovery commit

Refer to the Appendix for CLI patching methods.

9.7.1. Overview

Provides patch file upload functionality and displays patch reflection status information for Manager and each Node's Node Agent.

Patch File Upload

The Patch Info area displays detailed information of the highest version among patch files uploaded to the manager.

Table 187. Patch Info Items

Item	Description	Remarks
Patch File Ver.	Version information of the patch file	
Release Date	Release date of the patch file	
Patch Note	Click **Detail (Note) button** to view detailed patch note content.	Patch note popup display

The process of uploading patch files is as follows.

1. Click **Upload button**.
2. Verify if it's in patchable status, and if normal, display a popup for patch file upload

Patchable Status Conditions

1. All nodes registered in Manager must be in start status.
2. Patch must be in commit status.
3. Manager, node, and server must all be the same version.
4. No unregistered servers exist in manager.
    a. If unregistered servers exist, register them in manager
    b. If servers exist in the node engine's servers folder, delete that folder

3. When you select the patch file to upload, upload is automatically executed.

Uploadable files are zip and tar.gz, and if you try to upload other files, error messages will be displayed.

Manager Patch

The Manager Info area displays the Manager's patch status and you can execute Manager patching and recovery.

The description of each item displayed on the screen is as follows.

Table 188. Manager Info Items

Item	Description	Remarks
Patch Status	Manager's patch application status • **Sun icon** : Manager has applied the latest patch (up to date) status • **Cloud icon** : Manager has not applied the latest patch (patch available) status	
Current Ver.	Manager's current version	
Patch Ver.	Patch version	
History	Button to view patch history	When handwork is required, **Detail (Note) button** is displayed in red.

When you click the **Detail (Note) button** displayed in the History item of the Manager Info screen, you can verify patch execution history through a popup window.

The description of each item displayed on the screen is as follows.

Table 189. History Items

Item	Description	Remarks
Action	Displays patch/restore history	
Patch Version	Version of the patch file that performed patch/restore	
Previous Version	Server version before applying patch/restore	
Timestamp	Time when patch/restore was applied	
Log/Handwork	**Detail (Note) button** provides execution result logs when selected. **Handwork (Wrench) button** provides Handwork (additional manual work required) content when selected. When handwork is required, this button is displayed in red.	

Patch

Click the **Patch button** at the bottom of Manager Info to apply the latest patch.

The content described in Handwork is manual work required after patch execution, so you must execute and reflect the described content. After handwork, uncheck the checkbox at the bottom of the popup window, then the **Handwork button** in the Manager Patch Info screen changes to white.

When Manager patch is applied, you cannot perform functions such as Node installation/registration, Server installation/registration/cloning until you press the **Commit button** after applying patches to Node and Server.

After patching, you must clear the browser cache to use the patched version of Manager.

Restore

Click the **Restore button** at the bottom of Manager Info to recover to the version before patching.

Recovery is performed when all nodes registered in Manager have patch status as Patch Available.

Commit

After applying all patches to Manager, Node, and Server, press the **Commit button** to confirm. After confirmation, you cannot revert to the previous version.

Node Patch

The Node Patch Status area shows the total count of servers with the latest patch applied and servers without patches applied, comprehensively for nodes registered in the manager.

The description of each item displayed on the screen is as follows

Table 190. Node Patch Status Items

Item	Description	Remarks
Status	Node's patch application status • **Sun icon** : All servers have applied the latest patch (up to date) status • **Cloud icon** : Node Agent has not applied the latest patch (patch available) status • **Half circle icon** : Node Agent has applied the latest patch, but the latest patch has not been applied to servers installed on the Node status • **Exclamation icon** : Node agent is incompatible with lena-manager status.	
Node name	Node name	
Address	Node's IP	

Item	Description	Remarks
Node Ver.	Node's current version	
Node Hotfix.	Node's Hotfix version	
History	Button to view patch history	When handwork is required, **Detail (Note) button** is displayed in red.
WAS	Web Application Server's patch status information • Up To Date : Count of servers with latest patch applied • Patch Available : Count of servers without latest patch applied	
Session Server	Session Server's patch status information • Up To Date : Count of servers with latest patch applied • Patch Available : Count of servers without latest patch applied	

Click **Node Patch button** to select a Node in the provided popup window, then proceed with patching or recovery for that Node.

Nodes installed in Windows OS environment perform patching through CLI, not Manager.

Server Cluster Patch Status

Displays patch status for each Server Cluster.

The description of each item displayed on the screen is as follows.

Table 191. Server Cluster Patch Status Items

Item	Description	Remarks
Status	Cluster's patch application status • **Sun icon** : All servers have applied the latest patch (up to date) status • **Cloud icon** : Some servers have not applied the latest patch (patch available) status	
Cluster Group	Cluster group name	

Item	Description	Remarks
Cluster Name	Cluster name	
LENA Patch	Application Server's patch status information • Up To Date : Count of servers with latest patch applied • Patch Available : Count of servers without latest patch applied	

9.7.2. WAS

For Application Servers included in Node/Cluster, provides functionality to proceed with patching using the latest patch file uploaded to the manager, and in case of problems, restore to the status immediately before patch application.

List

Search for servers to apply patches by group conditions (node unit, cluster unit).

Table 192. Application Server Patch Status Items

Item	Description	Remarks
Patch Status	Application Server's patch application status • **Sun icon** : Latest patch applied (up to date) status • **Cloud icon** : Can apply latest patch (patch available) status	
Node	Node name where Application Server is installed	
Name	Application Server name	
Type	Application server type • Standard : Application Server Standard Edition • Enterprise : Application Server Enterprise Edition	
Address	IP of the Node where Application Server is installed	
HTTP Port	Application Server's HTTP Connector port	
AJP Port	Application Server's AJP Connector port	

Item	Description	Remarks
Start/Stop	Application Server's start and stop execution	
Current Version	Application Server's currently installed version information	
Hotfix	Hotfix version information	
Patch Version	Version information to apply patch. When latest patch is applied, it displays 'N/A'.	Latest patch version uploaded to manager
History	View patch/restore history information applied to the server	

If Node Agent process kill or other reasons cause abnormal operation, server information for that node will not be displayed.

Patch

1. Verify the server's stop status before applying patch (**Start button** activated status), and if not in stop status, click **Stop button** to stop the server.
2. Check the checkbox of the server to apply patch to. (Multiple checks possible)
3. Click **Patch button** to proceed with patching. A log popup will appear, and if there are items requiring manual work after patch completion, **Handwork (Wrench) button** is displayed in red in the Handwork column.
4. When you close the log popup, the server's patch status changes to **Sun icon**, and current ver., patch ver. display the currently applied patch version and N/A respectively.
5. Validation
   a. Cannot apply patch when server is in start status
   b. Cannot apply patch again to servers that already have the latest patch applied

When applying patches to servers, if it's the first time applying patches to that Node, internally the Node's patch is performed first, then server patching proceeds.

Restore

1. Verify the server's stop status before applying recovery (**Start button** activated status), and if not in stop status, click **Stop button** to stop the server.
2. Check the checkbox of the server to apply recovery to. (Multiple checks possible)
3. Click **Restore button** to proceed with recovery. A log popup will appear.
4. When you close the log popup, the server's patch status changes to **Cloud icon**, and current ver., patch ver. display the previous version and patch file version respectively.
5. Validation
   a. Cannot apply recovery when server is in start status
   b. Cannot recover again after recovery (Manager recovery supports only 1 step)

After proceeding with server recovery, if no servers with patches applied exist on the Node, internally the Node's recovery is also performed together.

History Inquiry

Click **Detail (Note) button** to view the most recent 5 patch/restore histories.

Table 193. History Items

Item	Description	Remarks
Action	Displays patch/restore history	
Patch Version	Version of the patch file that performed patch/restore	
Previous Version	Server version before applying patch/restore	
Timestamp	Time when patch/restore was applied	
Log/Handwork	**Detail (Note) button** provides execution result logs when selected. **Handwork (Wrench) button** provides Handwork (additional manual work required) content when selected. When handwork is required, this button is displayed in red.	

9.7.3. Session Server

For Session Servers, provides functionality to proceed with patching using the latest patch file uploaded to the manager, and in case of problems, restore to the status immediately before patch application.

List

Search for servers to apply patches by group conditions (node unit).

Table 194. Session Server Patch Status Items

Item	Description	Remarks
Patch Status	Session Server's patch application status • **Sun icon** : Latest patch applied (up to date) status • **Cloud icon** : Can apply latest patch (patch available) status	
Node	Node name where Session Server is installed	

Item	Description	Remarks
Name	Session Server name	
Type	Session server type	
Address	Session Server's address	
Port	Session Server's port	
Start/Stop	Session Server's start and stop execution	
Current Version	Session Server's currently installed version information	
Hotfix	Hotfix version information	
Patch Version	Version information to apply patch. When latest patch is applied, it displays 'N/A'.	Latest patch version uploaded to manager
History	View patch/restore history information applied to the server	

If Node Agent process kill or other reasons cause abnormal operation, server information for that node will not be displayed.

Patch

1. Verify the server's stop status before applying patch (**Start button** activated status), and if not in stop status, click **Stop button** to stop the server.
2. Check the checkbox of the server to apply patch to. (Multiple checks possible)
3. Click **Patch button** to proceed with patching. A log popup will appear, and if there are items requiring manual work after patch completion, **Handwork (Wrench) button** is displayed in red in the Handwork column.
4. When you close the log popup, the server's patch status changes to **Sun icon**, and current ver., patch ver. display the currently applied patch version and N/A respectively.
5. Validation
   a. Cannot apply patch when server is in start status
   b. Cannot apply patch again to servers that already have the latest patch applied

When applying patches to servers, if it's the first time applying patches to that Node, internally the Node's patch is performed first, then server patching proceeds.

Restore

1. Verify the server's stop status before applying recovery (**Start button** activated status), and if not

in stop status, click **Stop button** to stop the server.

2. Check the checkbox of the server to apply recovery to. (Multiple checks possible)
3. Click **Restore button** to proceed with recovery. A log popup will appear.
4. When you close the log popup, the server's patch status changes to **Cloud icon**, and current ver., patch ver. display the previous version and patch file version respectively.
5. Validation
   a. Cannot apply recovery when server is in start status
   b. Cannot recover again after recovery (Manager recovery supports only 1 step)

After proceeding with server recovery, if no servers with patches applied exist on the Node, internally the Node's recovery is also performed together.

History Inquiry

Click **Detail (Note) button** to view the most recent 5 patch/restore histories.

Table 195. History Items

Item	Description	Remarks
Action	Displays patch/restore history	
Patch Version	Version of the patch file that performed patch/restore	
Previous Version	Server version before applying patch/restore	
Timestamp	Time when patch/restore was applied	
Log/Handwork	**Detail (Note) button** provides execution result logs when selected. **Handwork (Wrench) button** provides Handwork (additional manual work required) content when selected. When handwork is required, this button is displayed in red.	

9.8. Preferences

9.8.1. Action Trace

Through Manager, logs are kept of the execution history of add/modify/delete operations performed by each user. Action Trace provides functionality to view/track these execution histories.

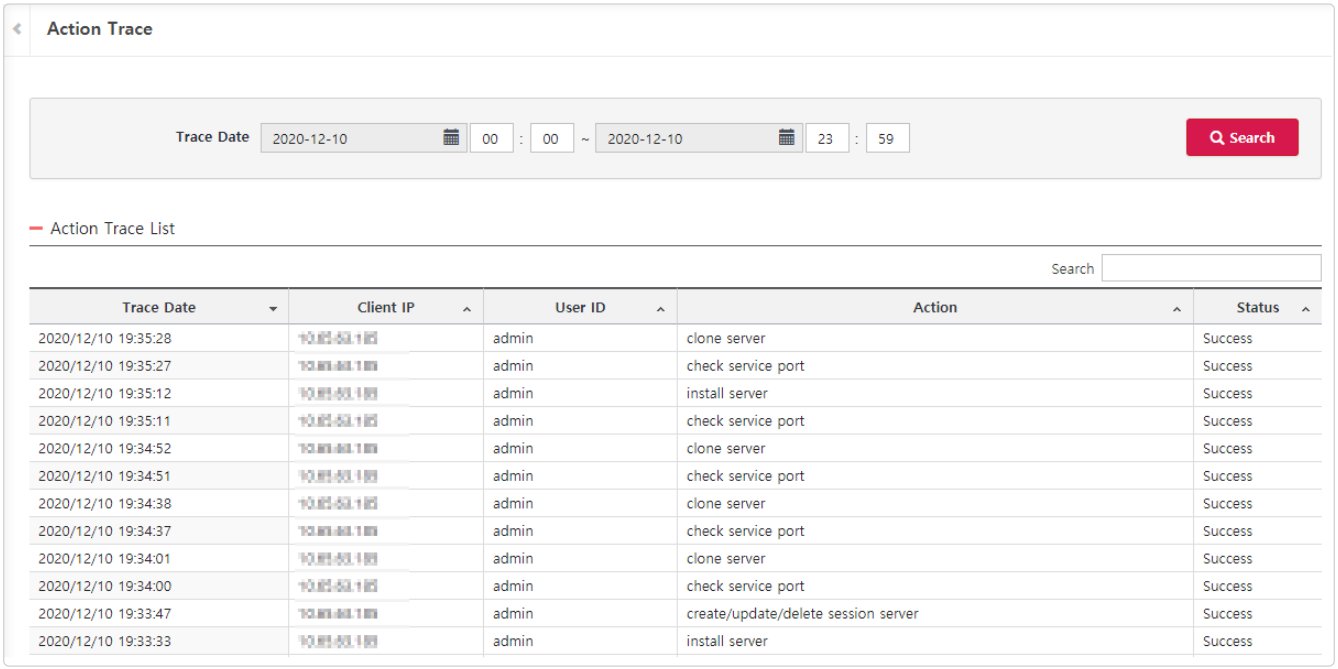


Figure 102. Action Trace Screen

History Inquiry

After entering search conditions and clicking, you can view the history. When you select one from the list, you can also verify detailed information.

The items displayed on the inquiry screen are as follows.

Table 196. History Detail Information Items

Item	Description	Remarks
Trace Date	Time when the Action was performed	
Status	Action execution result	Success : Success, Failure : Fail
Client IP	IP address of the user who performed the Action	
User ID	User ID who performed the Action	
Action	Name of the performed activity (Action)	
Method	Method name used for the Action	
Request	LENA Manager HTTP Request URL	
Input	Http Request Input parameters	

Among the above items, "Input" stores Request parameters as-is, so Server ID, Node ID, Server Cluster ID are displayed as data management Key values (serial numbers, "serverID=31" as shown in the capture screen). To view detailed information of the corresponding Server/Node/Cluster, utilize the "Search ID" functionality located at the bottom of the "Action Trace Detail" information. The input/output items of this functionality are as follows.

Table 197. Search ID Functionality Input/Output Items

Item	Description	Remarks
ID	• Left Combo : Choose between serverId / nodeId / serverClusterId • Right : Enter the ID value from Input	Input item
Data	Retrieved Server/Node/Cluster information	Output item

9.8.2. Documentation

You can download LENA introduction materials and manuals.

9.8.3. Manager Environment

Provides information for Manager environment configuration.

Manager Environment

Provides information stored in env-manager.sh/bat among Manager environment configuration information.

- Manager Allow IPs : Configures IP items that can access the Manager.
- Java Home Path : Configures the java home path used by the Manager.

Manager Configuration

Provides information stored in manager.conf among Manager environment configuration information.

Provides 2 items by default.

- use JMX for Server Status : Whether to retrieve server status information through JMX (default : false)

Table 198. When using JMX for Server Status: true, WAS Status display

Status	Status name	Description
	Started	Both WAS and Application are normally started
	Started(Warning)	WAS normally started, Application partially (or entirely) not started
	Stopped	WAS stopped
	Error	WAS Status verification impossible

- use Server Delete Protection : Whether to disable server deletion functionality in Manager (default : false)

Click the **configuration button** on the right side of the screen to verify and change detailed information.

OpenID Connect Configuration

Configures login functionality through OpenID Provider that follows OpenID Connect standards. When enabled, you can verify the OpenID Connect Toggle button on the login screen.

Item	Description	Remarks
Enable	Whether to enable OpenID Connect login functionality	
Enable Auto User Creation	Whether to create a user when authentication succeeds from the authentication provider but the user doesn't exist in LENA	
Provider	Authentication provider	
Grant Type	Method for client to request tokens	authorization_code, password
Client ID	Unique identifier for the OpenID Connect client application	
Client Secret	Secret key used for authentication between client application and authentication server.	
Key for Login	Key name of UserInfo that maps to LENA Manager User ID.	
Authorization URL	URL used when redirecting users to the authentication provider for authentication	
Redirect URL	URL used when redirecting from authentication provider to Manager after login	
Token URL	URL used when requesting tokens from the authentication provider	
Userinfo URL	URL used when requesting user information from the authentication provider	
End Session URL	URL used when requesting session termination from the authentication provider	

Metadata Refresh

Performs metadata consistency verification and restoration functionality used to draw system-specific configuration information as topology charts in the Topology menu.

Reset manager address of all registered nodes

Provides functionality to collectively change the changed Manager Address to all nodes registered in the Manager.

Start Hook Script

This script is executed before Manager starts when the Manager Container starts.

Stop Hook Script

This script is executed after Manager stops when the Manager Container stops.

9.8.4. Manager HA

You can manage configuration for Manager redundancy and view the current status of redundancy.

Manager redundancy is a function where Primary and Secondary LENA Managers that have started synchronize databases and important files, so that when the Primary Manager is down, the Secondary Manager temporarily takes over the Primary's services.

The services that the Secondary Manager takes over are the following two:

- Server Cluster - Scaling service
- Service Cluster - Server Template and License download

For Manager redundancy, you must modify the following part of the environment configuration file 'env-manager.sh' according to each Manager's role and start it.

LENA Manager Environment Variable File (env-manager.sh) Configuration

```
CATALINA_OPTS=" ${CATALINA_OPTS} -Dspring.profiles.active=ha-none"
```

The spring.profiles property configured in the above file can have the following 3 configurations, and if incorrectly written, the Manager will not start normally.

- ha-none : Default value, standalone Manager that does not perform redundancy
- ha-primary : Performs Primary Manager role during redundancy
- ha-secondary : Performs Secondary Manager role during redundancy

Local Manager

Provides current Manager information. Regardless of the Manager's role, the Manager that provides the current management screen is called Local Manager, and the remote Manager is called Remote Manager.

Table 199. Local Manager Information Items

Item	Description	Remarks
Status	Server status, always Active status.	
Start Time	Local Manager start time	
HA Mode	Whether Primary or Secondary	

Item	Description	Remarks
HA Pairing Configuration	• Indicates whether the connection information of the Remote Manager configured in the Local Manager matches the actual Remote Manager information. Items compared are address, Http/Udp service port, and DB service port. • When pairing configuration information is normal, **Green ○ icon** is displayed, when abnormal, **Red X icon** is displayed, and when connection to Remote is impossible, **Red ! icon** is displayed.	

Remote Manager

Provides information about the remote Manager.

Table 200. Remote Manager Information Items

Item	Description	Remarks
Status	Server status, displays as Active when normally connected, and InActive when not connected.	
Start Time	Remote Manager start time	
HA Mode	Whether Primary or Secondary	
HA Pairing Configuration	• Indicates whether the connection information of the Remote Manager configured in the Remote Manager matches the actual Local Manager information. Items compared are address, Http/Udp service port, and DB service port. • When pairing configuration information is normal, **Green ○ icon** is displayed, when abnormal, **Red X icon** is displayed, and when connection to Remote is impossible, **Red ! icon** is displayed.	
Address	Remote Manager's address, used when configuring connection information.	
Http Port	Remote Manager's Http service Port, used when configuring connection information.	

Click **Connection Test button** to test whether actual connection is possible using the Remote Manager's Address and Http Port.

Primary Manager and Secondary Manager can configure information for mutual synchronization through Pairing. Click **Sync Settings button** to perform Pairing that synchronizes configuration information with the Remote Manager.

Latest Sync Status

You can view the latest history of Database and File synchronization between redundant Managers.

Table 201. Latest Sync Status Information Items

Item	Description	Remarks
Type	Database or File	
Status	**Green ○ icon** when normal, **Red X icon** when error occurs, **Red ! icon** when connection to Remote is impossible.	
Time	Synchronization attempt time	
Result	Whether synchronization was successful	
Message	Result message generated during synchronization	
List button	Click **List button** to view previous synchronization history. Up to 10 histories are displayed, only histories after Manager start are displayed, and synchronization information from Remote Manager is only displayed when normally connected.	

Chapter 10. Appendix

10.1. LENA System Requirements

The minimum requirements for installing and using LENA are as follows.

Category	JVM	CPU	Memory	Disk	Support OS	Remarks
Basic Installation Package	JDK 1.8 or higher	2 Core or higher	4 GB or higher	10GB or higher (excluding root)	Linux (CentOS 7 or higher) or Windows 7 or higher	Installation files provided for each component

10.2. Manager Supported Browsers

Browsers that can use Manager functions include Chrome/Edge (version 70 or higher) and Firefox (version 62 or higher). For IE, some functions may not work properly, so it is recommended to use other browsers. The recommended minimum browser size is 1680*900.

10.3. Supported Specification Versions

Specification	Version	Remarks
Java Development Kit (JDK)	1.8~	
Java Servlet	3.1	
Java Server Pages (JSP)	2.3	
Expression Language (EL)	2.2	
JavaServer Pages Standard Tag Library (JSTL)	1.2	
Enterprise JavaBeans (EJB)	3.2	
Java Message Service (JMS)	1.1	
Java Transaction API (JTA)	1.2	
Java API for RESTful Services (JAX-RS)	2.0	
Java API for XML Web Services (JAX-WS)	2.2	

10.4. Manager DB File Backup

HSQL DB files for internal data management of Manager generate backup files periodically (daily). The generation location is ${LENA_HOME}/repository/backup/database.

By default, backup information older than 30 days is deleted. If you want to change the retention period, open the manager.conf file in the ${LENA_HOME}/repository/conf folder and enter

dbbackup.size=retention_period, then restart Manager to change the retention period.

10.5. Manager Internal History Deletion

The history that Manager leaves internally is scheduled to be deleted periodically. The information being deleted is Action Trace history and Server History history.

By default, Action Trace history is retained for up to 30 days, and Server History history is retained for up to 90 days. If you want to change this retention period, open the manager.conf file in the ${LENA_HOME}/repository/conf folder and enter actiontrace.size=retention_period, serverhistory.size=retention_period, then restart Manager to change the retention period.

10.6. Manager Admin Password Reset

If you lose the Manager admin user password or exceed the password error count, you must reset the password through the console.

1. Connect to the equipment where Manager is installed via console (telnet or ssh).
2. Execute the $LENA_HOME/bin/reset_manager_pw.sh file.
3. Enter admin as the user to reset the password.
4. Enter the password to reset. Note that the password must be 8 characters or more, a combination of alphabet/numbers/special characters. The password is not displayed on the console for security reasons.

```
[bin]$ ./reset-manager-pw.sh

 ******************************
* LENA Server Install ! *
 ******************************

+-------------------------------------------------------------------------------
--
| 1. USER_ID is the user id to reset
| ex : admin
| 2. NEW_PASSWORD is the password to change
| - password rule #1 : more than 8 length
| - password rule #2 : inclusion of one or more alphabet characters
| - password rule #3 : inclusion of one or more numerical digits
| - password rule #4 : inclusion of one or more special characters
+-------------------------------------------------------------------------------
--

Input USER_ID for installation. (q:quit)
administrator

Input NEW_PASSWORD for installation. (q:quit)

The password has been changed successfully.

Execution is completed.!!
```

10.7. LENA Installation Recommended OS Parameters (CentOS Standard)

When installing LENA, it is recommended to set the max user processes value to 8192 or higher.

parameter	Recommended Value	Default Value
max user processes	8192	1024
open files	8192	1024

For CentOS, you can check the max user processes setting by running the 'ulimit –a' command as follows.

```
$ ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
scheduling priority             (-e) 0
file size               (blocks, -f) 8192
pending signals                 (-i) 14891
max locked memory       (kbytes, -l) 64
max memory size         (kbytes, -m) unlimited
open files                      (-n) 1024
pipe size            (512 bytes, -p) 8
POSIX message queues     (bytes, -q) 819200
real-time priority              (-r) 0
stack size              (kbytes, -s) 10240
cpu time               (seconds, -t) unlimited
*max user processes              (-u) 1024*
virtual memory         (kbytes, -v) unlimited
file locks                      (-x) unlimited
```

For CentOS, you can set the number of processes and open files using the commands 'ulimit –u' and 'ulimit –n'. To permanently reflect the above changes, add the ulimit execution command to each user's profile (.profile, .bash_profile), or you can force the setting (CentOS standard).

```
*$ cat $HOME/.bash_profile

*.. (omitted)*

*ulimit -u 8192

*ulimit -n 8192
```

Another configuration method is to open the /etc/security/limits.conf (CentOS standard) file and set the maximum number of processes (nproc) and maximum number of open files (nofile).

```
*$ cat /etc/security/limits.conf

*.. (omitted)*

** soft nproc 8192

** hard nproc 8192

** soft nofile 8192

** hard nofile 8192
```

10.8. LENA Periodically Increasing Files

Item	Path	Deletion Cycle	Monthly Expected Increase	Remarks
Manager Regular Maintenance Logging	LENA_HOME/repository/monitoringDB/maintenance	6 months	10MB	Expected increase based on 6 servers Auto deletion
Manager Monitoring, Diagnostic Reports	LENA_HOME/repository/monitoringDB/{yyyyMMdd}	7 days	N/A	Auto deletion
Manager Diagnostic Statistics	LENA_HOME/repository/monitoringDB/statistics	Permanent	1MB or less	
Manager DB Backup Files	LENA_HOME/repository/backup/database	30 days	100MB or less	Auto deletion
Manager Logs	LENA_HOME/logs/lena-manager	30 days	100MB or less	Auto deletion
Agent Logs	LENA_HOME/logs/lena-agent	30 days	N/A	Auto deletion
Installer Logs	LENA_HOME/logs/lena-installer	Permanent	1MB or less	
Patch Applied Files	LENA_HOME/etc/patch	Permanent	N/A	Only generated during patching Can be deleted after patch completion
Patch Backup Files	LENA_HOME/etc/backup/lena-patcher	Permanent	N/A	Generated during patching Can be deleted after patch completion
Patch Logs	LENA_HOME/logs/lena-patcher	Permanent	N/A	Generated during patching Can be deleted after patch completion

Item	Path	Deletion Cycle	Monthly Expected Increase	Remarks
Server Instance Logs	Server instance installation path LENA_HOME/servers/server_id/logs	Permanent	Judged based on load	Path changeable
Server Instance History	Server instance installation path LENA_HOME/servers/server_id/history	Permanent	N/A	Only configuration file updates are generated when server settings are modified through Manager
Server Instance Snapshots	Server instance installation path LENA_HOME/servers/server_id/snapshot	Permanent	N/A	Only generated when creating Cluster Snapshot through Manager
WAS Dump Files	LENA_HOME/repository/monitoringDB/dump	Permanent	N/A	Only generated when performing WAS dump through Manager

10.9. Patch CLI (Command Line Interface)

Patch is a function provided for functional improvements and bug fixes of installed LENA. It is provided in compressed file format and operates as an independently running Java process.

The method of execution through Management UI is provided in patch. Here, we explain how to patch and restore through CLI.

10.9.1. Patch File Upload and Extraction

Upload the received patch file to the server where LENA is installed individually using FTP, etc.

Extract the uploaded file to the location below and change the directory name to the version name. If uploaded through Manager, it is automatically extracted to the corresponding path.

```
Node/Server patch file path: /engn001/lena/1.3/etc/patch/{patch_version}
Manager patch file case: /engn001/lena/1.3/repository/patch/{patch_version}
```

10.9.2. Patch

Node Patch

Execute patch.sh to patch the Node.

```
<patch_file_extraction_path>/bin/patch.sh lena-node
```

During Node patching, the Node will restart.

```
[bin]$ ./patch.sh lena-node

*****************************
* LENA Server Patch ! *
*****************************

2018-05-28 14:06:43:915 [INFO] Patch started to lena-node
2018-05-28 14:06:47:075 [INFO] Stopping node-agent
...
2018-05-28 14:06:52:595 [INFO] Starting node-agent
2018-05-28 14:06:52:748 [INFO] Patch completed to lena-node

 ======================== Execution Result ========================
MESSAGE : Patch succeeded
RESULT : Success
PATCH_HISTORY_ID : patch-20180528140643905
PATCH_TARGET : lena-node
PATCH_VERSION : 1.3.1.1
 ==================================================================
patch is completed.!!
```

Manager Patch

Execute patch.sh to patch the Manager.

manager patch

```
<patch_file_extraction_path>/bin/patch.sh lena-manager
```

During Manager patching, the Manager will restart.

```
[bin]$ ./patch.sh lena-manager

*****************************
* LENA Server Patch ! *
*****************************

2018-05-28 14:05:32:752 [INFO] Patch started to manager
2018-05-28 14:05:36:032 [INFO] Stopping manager
...
2018-05-28 14:05:46:062 [INFO] Starting manager
2018-05-28 14:05:47:066 [INFO] Patch completed to manager

 ======================== Execution Result ========================
MESSAGE : Patch succeeded
RESULT : Success
PATCH_HISTORY_ID : patch-20180528140532668
PATCH_TARGET : lena-manager
PATCH_VERSION : 1.3.1.1
 ==================================================================

patch is completed.!!
```

Server Patch

Execute patch.sh to patch individual servers.

It must be executed on the server where the node is installed, and executed separately for each LENA server installation type. Node patching must precede server patching.

WAS standard type patch

```
<patch_file_extraction_path>/bin/patch.sh lena-se
```

WAS enterprise type patch

```
<patch_file_extraction_path>/bin/patch.sh lena-ee
```

Session Server patch

```
<patch_file_extraction_path>/bin/patch.sh lena-session
```

Table 202. patch.sh input arguments and input items

Item	Description	Remarks
PATCH_TARGET	Patch target (input as argument of patch.sh)	lena-node lena-manager lena-se lena-ee lena-session
SERVER_ID	Server ID corresponding to the patch target	lena-node, lena-manager patching not required

```
[bin]$ ./patch.sh lena-ee

******************************
* LENA Server Patch ! *
******************************

2018-05-28 14:17:18:840 [INFO] Patch started to lena-se

Input SERVER_ID for execution. (q:quit)
wasEE_9100
...
2018-05-28 14:17:26:820 [INFO] Saving patch history
2018-05-28 14:17:26:842 [INFO] Patch completed to lena-se

 ======================== Execution Result ========================
MESSAGE : Patch succeeded
RESULT : Success
PATCH_HISTORY_ID : patch-20180528141639064
PATCH_TARGET : lena-ee
PATCH_VERSION : 1.3.1.1
 ==================================================================
patch is completed.!!
```

10.9.3. History

Execute history.sh to check patch history. Basic history excludes restored history and shows it, while full history shows all history.

Basic history

```
<patch_file_extraction_path>/bin/history.sh
```

Full history

```
<patch_file_extraction_path>/bin/history.sh all
```

```
[bin]$ ./history.sh

*****************************
* LENA Server Patch ! *
*****************************

LENA Patch History
1 lena-node / patch-20180528140643905
- action : PATCH
- id : patch-20180528140643905
- target : lena-node
- serverId : lena-node
- oldVersion : 1.3.1.0
- patchVersion : 1.3.1.1
- backupRoot:
/engn001/lena/1.2/etc/backup/lena-patcher/backup-20180528140643903
- timestamp : 20180528140643905
- restored : false
- handwork-status : NO_WORK

2 lena-manager / patch-20180528140532668
- action : PATCH
- id : patch-20180528140532668
- target : lena-manager
- serverId : lena-manager
- oldVersion : 1.3.1.0
- patchVersion : 1.3.1.1
- backupRoot:
/engn001/lena/1.2/etc/backup/lena-patcher/backup-20180528140532666
- timestamp : 20180528140532668
- restored : false
- handwork-status : NEED_WORK
- start of handwork-detail
...
- end of handwork-detail

3 lena-ee / patch-20180528141639064
- action : PATCH
- id : patch-20180528141639064
- target : lena-ee
- serverId : wasEE_9100
- oldVersion : 1.3.1.0
- patchVersion : 1.3.1.1
```

```
- backupRoot:
/engn001/lena/1.2/etc/backup/lena-patcher/backup-20180528141639062
- timestamp : 20180528141639064
- restored : false
- handwork-status : NO_WORK

history is completed.!!
```

10.9.4. Restore

Execute restore.sh to restore the applied patch. (When patch application problems occur)

When Restore is executed, files changed at the patch point are restored to their pre-change state.

```
<patch_file_extraction_path>/bin/restore.sh <PATCH_HISTORY_ID>

(PATCH_HISTORY_ID is the id value retrieved from ./ history.sh)
```

```
[bin]$ ./restore.sh patch-20180423130610713

******************************
* LENA Server Patch ! *
******************************

2018-05-28 14:40:05:404 [INFO] Restore started to lena-ee
...
2018-05-28 14:40:05:532 [INFO] Restore completed to lena-ee

 ======================== Execution Result ========================
MESSAGE : Restore succeeded
RESULT : Success
 =================================================================
restore is completed.!!
```

10.9.5. Version Check

Execute version.sh to check the patch status of currently installed servers.

```
<patch_file_extraction_path>/bin/version.sh
```

```
[bin]$ ./version.sh

*****************************
* LENA Server Patch ! *
*****************************

LENA Patch Information
1. Base Information
- Version : 1.3.1.1 (Up to date)
- LENA_HOME : /engn001/lena/1.3.1

2. lena-manager
2.1 - id : lena-manager / version : 1.3.1.1 (Up to date)

3. lena-se
3.1 - id : wasSE_9100 / version : 1.3.1.1 (Up to date)
3.2 - id : wasSE_9200 / version : 1.3.1.1 (Up to date)

4. lena-ee
4.1 - id : wasEE_9300 / version : 1.3.1.0 (Patch available to 1.3.1.1)
4.2 - id : wasEE_9400 / version : 1.3.1.0 (Patch available to 1.3.1.1)

5. lena-session
5.1 - id : session_5000 / version : 1.3.1.0 (Patch available to 1.3.1.1)
5.2 - id : session_5500 / version : 1.3.1.0 (Patch available to 1.3.1.1)

version is completed.!!
```

10.10. DBCP Additional Functions

Control Application Server through Database connection testing or generate logs for operations performed in DBCP.

Set through environment variables or JVM Options, with JVM Option settings taking priority.
(If the same option is set in both environment variables and JVM Options, the JVM Option value is followed)

When using Application Server registered as a Windows service, only JVM Options can be set

10.10.1. Application Server Control

When starting the Application Server, if it cannot connect to the Database, or if pool creation, validation query failure, etc. are detected, the server is terminated.

Table 203. DBCP Additional Functions, Application Server Control

Environment Variable	JVM Option	Description	Default
SHUTDOWN_IF_DBCONN_FAIL	lena.shutdownIfDbConnFail	When true, server terminates in Database connection / Pool creation failure / validation query failure situations	false

10.10.2. DBCP Logging

Logging for Datasource creation, Connection creation, Validation query execution, Borrow Connection, Return Connection / Detailed Stack Trace logging

Environment Variable	JVM Option	Description	Default
DBCPLOG_ON	lena.dbcplogOn	When true, logs during Datasource creation, Connection creation	false
DBCPLOG_ON_DETAIL	lena.dbcplogOnDetail	When true, logs Validation query execution, Borrow Connection, Return Connection (does not work if DBCPLOG_ON is false)	false
DBCPLOG_ON_STACKTRACE	lena.dbcplogOnStacktrace	When true, adds Stack Trace information to logs.	false
DBCPLOG_MAX_TRACE	lena.dbcplogMaxTrace	Maximum number of Stack Traces to output in logs	5
DBCPLOG_EXC_DBCP_PACKAGE	lena.dbcplogExcDbcpPackage	Whether to exclude dbcp-related package information from Stack Trace logging	true

10.11. Manager Language Setting Change

You can change the language setting of LENA Manager.

Table 204. LENA Manager Configurable Languages

Language	Default
English(US)	O
Korean(KR)	

10.11.1. Language Setting Change Method

To turn on the language setting change function, first enter the following menu.

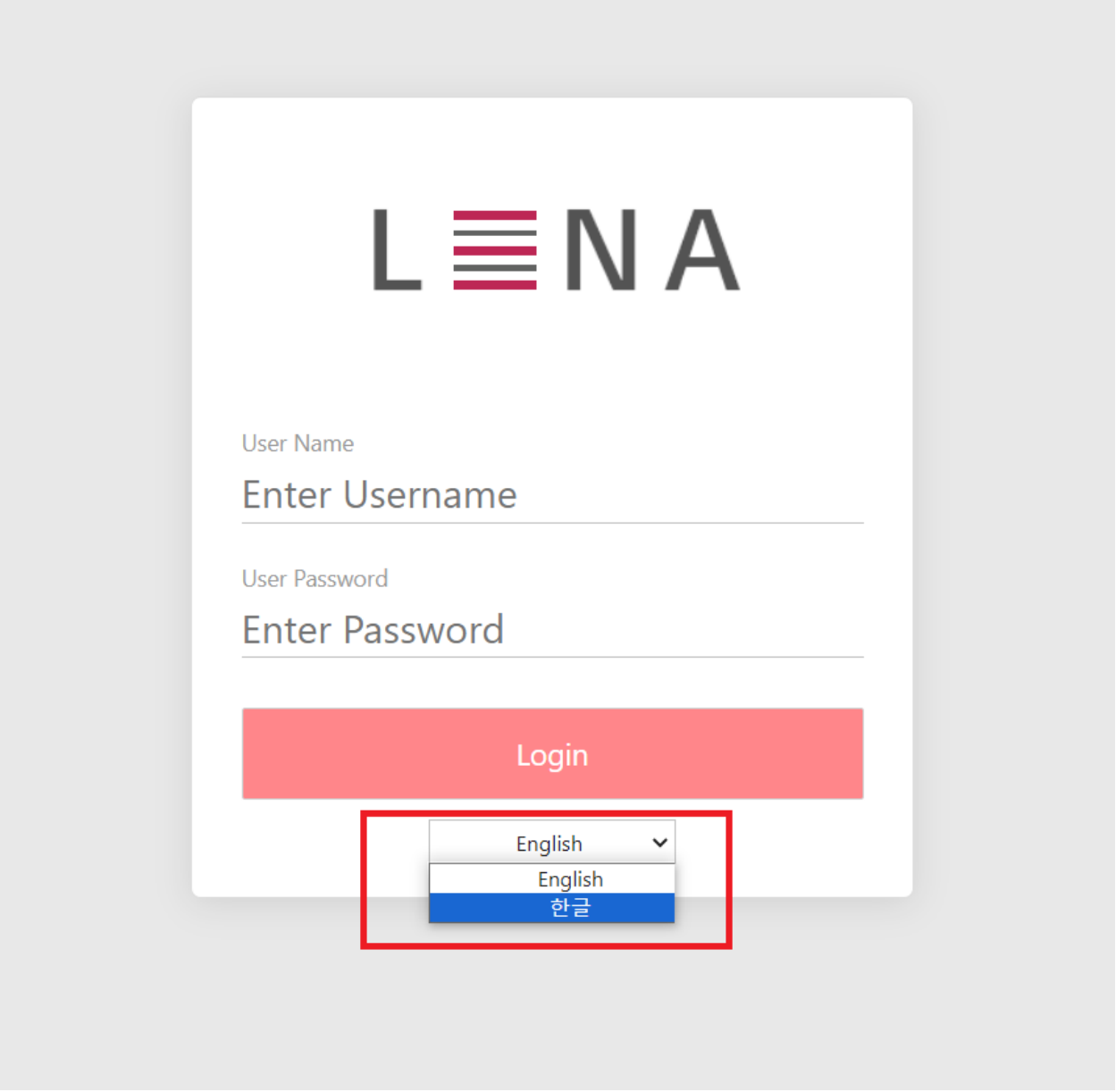
ADMIN > Preference > Manager Environment

(Based on default English setting)

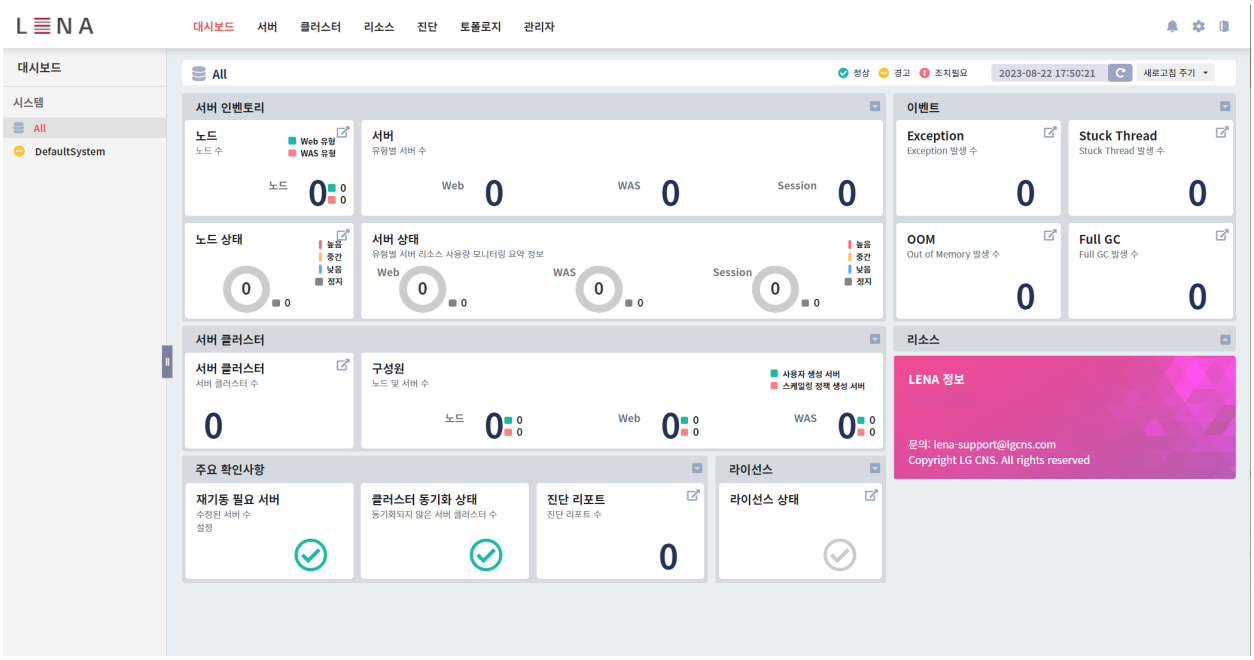
Click the gear button of Manager Configuration to open detailed settings and modify as follows.

```
...
 9  # i18n On/off
10  lena.i18n.enable=true # false -> true
...
```

Now you can change the language setting on the Login Page. If you are logged in, log out and go to the Login page.



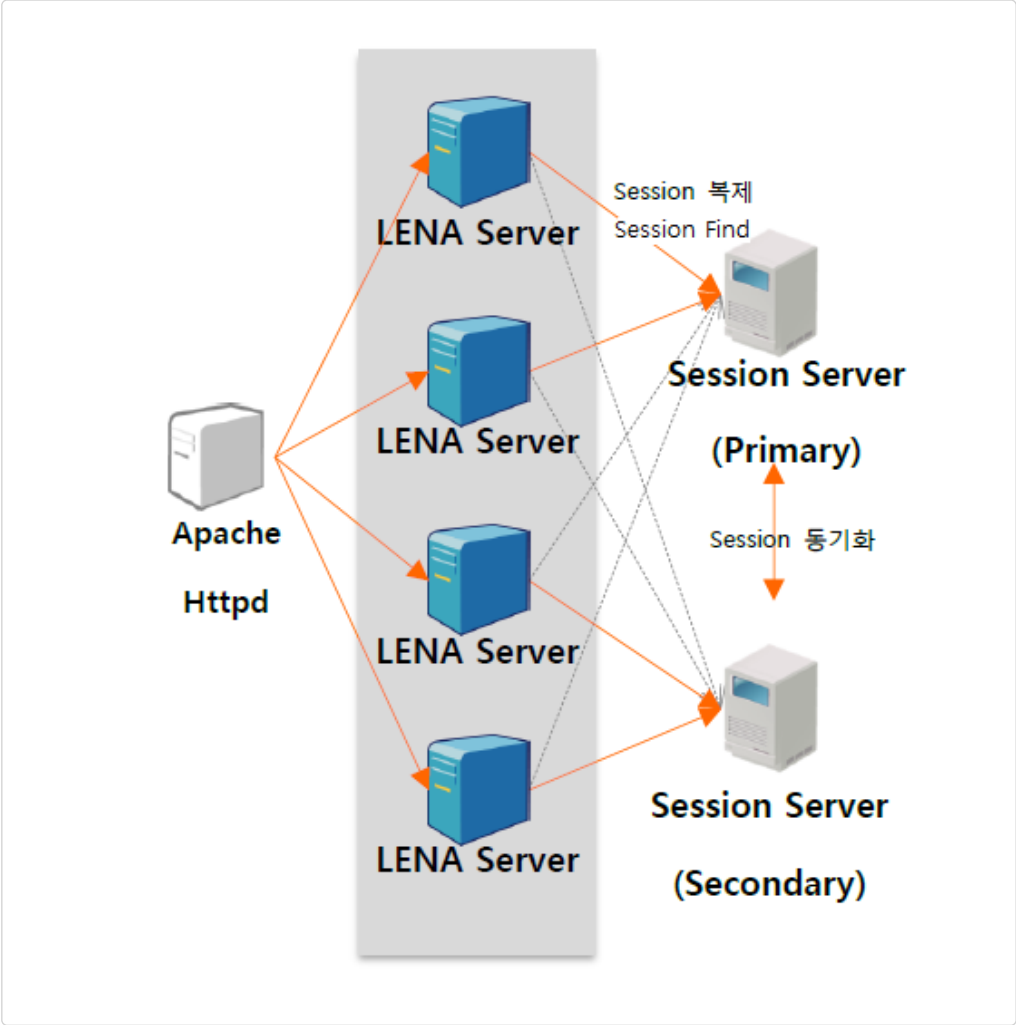
After selecting the language to use and logging in, you can use LENA Manager in the changed language.



10.12. Session Server Details

Application Server's Session Clustering installs a separate Session Server to share Sessions for Clustering. Session Server has Standalone mode that operates on a separate VM and Embedded mode that embeds the Session Server module in the Application Server.

10.12.1. Session Server Standalone Mode



Installation

For installation method, refer to the Install section.

Start/Stop and Startup Status Check

For start/stop and start status check, refer to Start/Stop.

Environment Configuration

The location where Session Server is installed is called ${ZODIAC_HOME}. Session Server is located in the /servers folder under LENA home.

Environment configuration information is managed in ${ZODIAC_HOME}/session.conf. Environment configuration configurable items are as follows.

Item	Description
server_id	server ID
server_name	server Name
primary_port	TCP listening port for this Session Server
session_max_count	Maximum HTTP session count

Item	Description
server_recv_queue_size	Queue size for processing requests from Secondary Server or Application Server (latest information changes / new registrations, Logout processing)
server_req_queue_size	Queue size for holding Session information requests from other Servers (Session information requests, latest information checks, etc.)
resp_queue_size	Queue size for holding responses to Session information requests from other Servers
send_queue_size	Queue size for holding Session information to send to other Servers
keep_alive_time	Interval for sending dummy messages to maintain TCP connection between Application Server and Session Server, must be smaller than so_timeout. It's good to match each Application Server's settings.
so_timeout	Read timeout in connection with Application Server
thread_request_handler	Number of Threads that process data in request Queue.
thread_data_handler	Number of Threads that process data in receive Queue.
debug_clustering	Whether to leave Debug Logs
enable_auto_was_sync	When set to true, sends Sync request to WAS that reconnected due to failure, etc. to sync WAS's Session data.
enable_auto_peer_sync	Whether to send Sync request to Secondary Session Server that reconnected (due to failure, etc.) to sync Slave Session Server's Session data
server_expire_sec	Time for server to expire HTTP session information (Session Timeout) When 0, uses the session timeout time set in the Application
server_expire_check_sec	Session Timeout check cycle. (unit: seconds)
secondary_host	Secondary session server address
secondary_port	Secondary session server port
enable_ready_after_sync	Whether to send Clustering service available status (Ready) to connected WAS after performing Session data synchronization with Secondary Server (true sends ready status after synchronization)
wait_server_ready_timeout	If ready status (Session Clustering service available status) is not achieved within this time, automatically creates ready status.
server_ready_time	Startup wait time for connection with Secondary Server (this value * 100 ms).
max_logoutset	Maximum number of logged out HTTP sessions
enable_auto_logout_sync	When true, during session entry information sync, logout information is also synced. (needed when not sticky but round-robin)

Logs

Logs are written to ${LENA_HOME}/logs/session-server/lena-[Session Server Name]_[YYYYMMDD].log. To check logs, you can also execute ${ZODIAC_HOME}/log.sh file.

```
[session_5002]$ ./log.sh

May 09, 2018 02:55:50 PM [ZODIAC] TCP listen 5002
May 09, 2018 02:55:54 PM [ZODIAC] ACCEPT NODE(Tomcat) /127.0.0.1:33138
May 09, 2018 02:55:55 PM [ZODIAC] SERVER_READY, no peer, time=5000
May 09, 2018 02:59:57 PM [ZODIAC] Zodiac Stop
May 09, 2018 03:00:00 PM [ZODIAC] Zodiac Session Server 1.3.0 20160420
May 09, 2018 03:00:01 PM [ZODIAC] TCP listen 5002
May 09, 2018 03:00:01 PM [ZODIAC] ACCEPT NODE(Tomcat) /127.0.0.1:33359
May 09, 2018 03:00:03 PM [ZODIAC] ACCEPT SERVER /127.0.0.1:46818
May 09, 2018 03:00:04 PM [ZODIAC] SYNC[session_5002] recv bulk
sessions : #0 recv bulk logout sessions : #0 recv bulk dupInfo : #0 2ms
May 09, 2018 03:00:04 PM [ZODIAC] SERVER_READY sync is done
May 09, 2018 03:00:05 PM [ZODIAC] TCP Primary name=session_5002
/127.0.0.1:5002
May 09, 2018 03:00:05 PM [ZODIAC] SYNC start 127.0.0.1:5002
May 09, 2018 03:00:05 PM [ZODIAC] SYNC Send bulk sessions send to
127.0.0.1:5002 #0 and logout session send : 0 and dupInfo send : 0
```

Console

Zodiac Session Server can query Session Server information and perform Application Server Sync commands through JMX. Execute the console.sh file in ${ZODIAC_HOME} to use Zodiac Session Server's JMX functionality.

```
[session_5002]$ ./console.sh

 =====zodiac session server JMX Console=====

 ------------------------------------------------------------

- Usage: ./console.sh <COMMAND> -
- <COMMAND> is one of the following: -
- 1. was_list -
- 2. status -
- 3. was_serverq -
- 4. was_sync -
-    It needs WAS ID -
-    example: ./console.sh was_sync <was id> -
- 5. search -
-    It needs SESSION ID. -
-    example: ./console.sh search <session id> -

 ------------------------------------------------------------
```

The following is a description of console.sh commands.

- Application Server List

  Shows the list of Application Servers currently connected to Session Server.

  Execute shell command console.sh was_list.

  ```
  [session_5002]$ ./console.sh was_list

   =====zodiac session server JMX Console=====

  RUN OPERATION: getServerInfo

  RESULT:server=\{addr:/127.0.0.1:54001,name:wasEE7_29100,
  info:\{server_name=wasEE7_29100,pid=24915,hostname=solwas4,jvmName=bde0fbb29
  e8100285,context=/jpetstoreJTA;ROOT;/lena;/EPS;/HelloWorldWeb,type=INSTANCE}
  }server=
  \{addr:/127.0.0.1:33912,name:wasEE3_29100,
  info:\{server_name=wasEE3_29100,pid=10607,hostname=solmanager,jvmName=2b2451
  dd049f00285,context=/jpetstoreJDBC;ROOT;/jpetstore3,type=INSTANCE}}
  ```

- Session Server Status

  Shows the current status values of Session Server.

  Execute shell command console.sh status.

```
[session_5002]$ ./console.sh status

 =====zodiac session server JMX Console=====

RUN OPERATION:

getStatusString\{request_getfresh_logout:0,session_count:0,req_lost:0,reques
t_
getfresh_not_new:0,request_getfresh_nodata:0,request_getnew_secondary:0,sess
ion_expired:0,request_getnew_logout:0,session_timeout:1800,request_getnew_no
data:0,session_max_count:2000000
,logout_from_nodes:0,pid:32705,session_recv_lost:0,logout_from_secondary:0,r
equest_getfresh_secondary:0,request_getfresh:0,request_getnew:0,logout_count
:0,data_from_nodes:0,resp_lost:0,request_getfresh_data:0,data_from_secondary
:0}
```

- Session Server ServerQ Status

  Shows the ServerQ status of Zodiac Session Server. ServerQ is a module that manages Application Server connections connected to Session Server. The data shown here is Queue information that holds Session information (data) sent from Application Server and Request information (Request).

  Execute shell command console.sh was_serverq.

```
[session_5002]$ ./console.sh was_serverq

=====zodiac session server JMX Console=====

PRINT ATTRIBUTEdataQ.size: 0requestQ.size: 0dataQ.overCnt:
0requestQ.overCnt: 0
```

- Session Id Search

  Shows the Application Server List that has the Session matching the entered Session ID.

  Execute shell command console.sh search [Session ID].

```
[session_5002]$ ./console.sh search
B38E30BDE5223BAA0221B9479AF3DDAF.6ef7931859a200285
 =====zodiac session server JMX Console=====

RUN OPERATION: search

RESULT:\{'AE4_29100'=\{lastAccessTime='2018-05-24
15:55:48.503',context='ROOT',attributeNames=[sessiontest.counter,
ARGO_DUPLICATION_STATUS],lastUpdateTime='2018-05-24
15:55:48.501',addr='/127.0.0.1:44568',id=B38E30BDE5223BAA0221B9479AF3DDAF.6e
f7931859a200285,createTime='2018-05-24
15:55:43.241'}}
```

- Application Server Session Sync

  Execute when syncing Application Server's Session information to Session Server.

  Execute shell command console.sh was_sync [Application Server jvmName (value output as jvmName in was_list)].

```
[session_5002]$ ./console.sh was_list

 =====zodiac session server JMX Console=====

RUN OPERATION: getServerInfo

RESULT:server=\{addr:/127.0.0.1:54001,name:wasEE7_29100,
info:\{server_name=wasEE7_29100,pid=24915,hostname=solwas4,jvmName=bde0fbb29
e8100285,context=/jpetstoreJTA;ROOT;/lena;/EPS;/HelloWorldWeb,type=INSTANCE}
}server=
\{addr:/127.0.0.1:33912,name:wasEE3_29100,
info:\{server_name=wasEE3_29100,pid=10607,hostname=solmanager,jvmName=2b2451
dd049f00285,context=/jpetstoreJDBC;ROOT;/jpetstore3,type=INSTANCE}}}
```

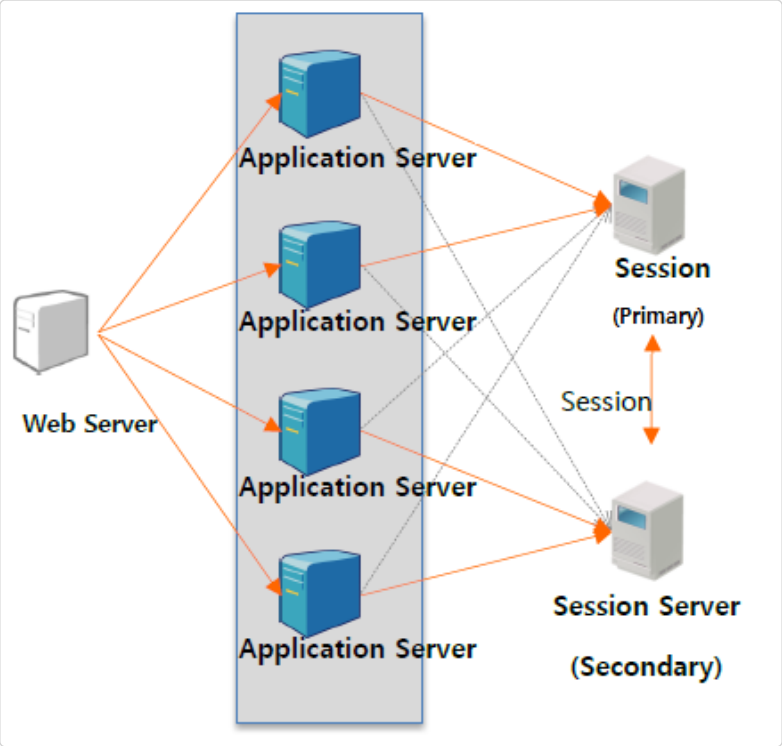
```
[session_5002]$ ./console.sh was_sync bde0fbb29e8100285

 =====zodiac session server JMX Console=====

RUN OPERATION: serverSyncsync complete
```

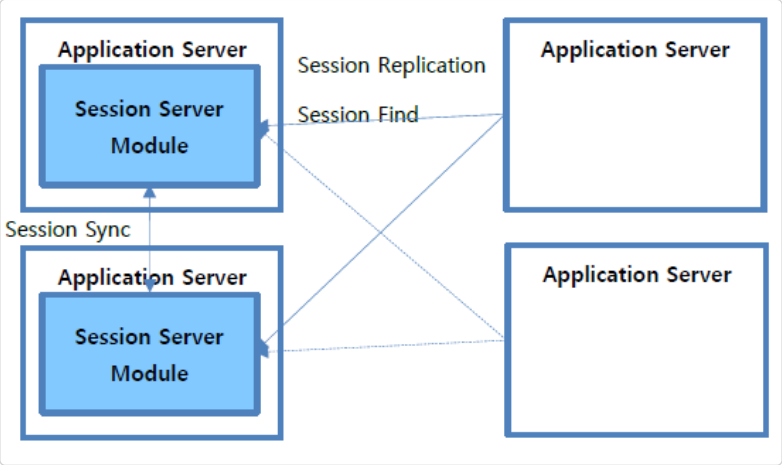
Session Server Failover

Session Server is configured as Primary/Secondary and synchronizes Session information in real time. Since Application Server maintains connection with Primary/Secondary Session Server, when Primary Session Server failure occurs, failover to Secondary Session Server occurs from the point of failure detection.



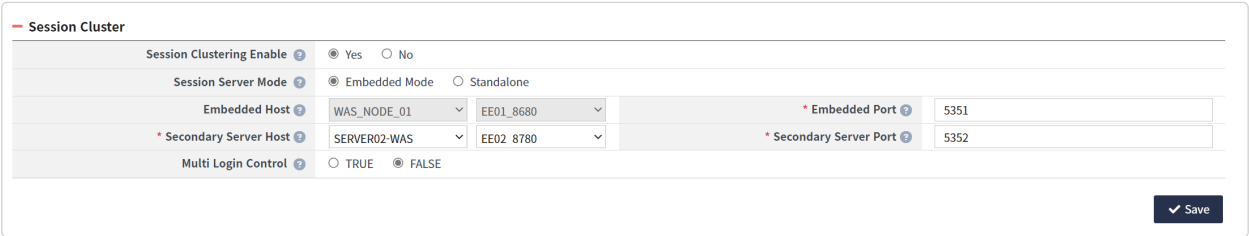
10.12.2. Session Server Embedded Mode

Session Server Embedded mode is a method of embedding Session Server Module within Application Server.



Environment Configuration

To configure Session Server in Embedded mode, set it in Manager's Application Server configuration screen or modify ${LENA_HOME}/servers/[ApplicationServerName]/conf/session.conf.



The description of items displayed on the screen is as follows.

Item	Description	Remarks
Session Server Mode	Select Embedded or Standalone Session Server's Client mode	
Embedded Host	Node name and server name of Session Cluster's Primary server	
Embedded Port	Service port of Session Cluster's Primary server	
Secondary Server Host	Node name and server name of Session Cluster's Secondary server	
Secondary Server Port	Service port of Session Cluster's Secondary server	
Multi Login Control	Whether to check multiple logins	false
Logout Page when Multi Login check (Multi Login)	Logout result page displayed to the user who logged in first when multiple logins occur	
Logout Message when Multi Login check (Multi Login)	Logout result message when multiple logins occur, provided to ajax Client in JSON format	
Expected Page When Multi Login Check (Multi Login)		

Manager has limited configurable values. Basically, follow the default settings.

Below are the environment configuration values that can be changed through session.conf file.

Item	Description	Default Value
enable_clustering	Whether to do Session clustering. If False, Session Server doesn't find sessions.	TRUE
debug_clustering	Whether to debug	FALSE
primary_host	Primary Session Server address In Embedded mode, it's the Embedded Host value	127.0.0.1
primary_port	Primary Session Server port In Embedded mode, it's the Embedded Port value	5005
secondary_host	Secondary Session Server address, only used when connection between Application Server and Primary Session Server is broken. In Embedded mode, it's the Slave Server Host value	127.0.0.1

Item	Description	Default Value
secondary_port	Secondary Session Server port, only used when connection between Application Server and Primary Session Server is broken In Embedded mode, it's the Slave Server Port value	5006
recv_queue_size	Queue size for processing Session information processing requests received from other Servers (latest information changes / new registrations, Logout processing)	512
req_queue_size	Queue size for holding Session information requests received from other Servers (Session information requests, latest information checks, etc.)	512
resp_queue_size	Queue size for holding responses to Session information requests received from other Servers	512
send_queue_size	Queue size for holding Session information to send to other Servers	512
keep_alive_time	Interval for sending dummy messages to maintain TCP connection between Application Server and Session Server, must be smaller than so_timeout.	3000
so_timeout	Read timeout in connection with Session Server	8000
tcp_open_try_interval	Interval for reconnection attempts when connection with Session Server is broken	5000
find_timeout	Time to wait for server response when Application Server searches for sessions during transactions. If there's no server response within this time, Application Server considers that the server doesn't have the session	500
wait_server_ready_cnt	When communication connection with Server is established but Server status is not ready, wait for maximum configured seconds. If -1, wait indefinitely.	-1
server_embedded	Whether to embed session server module. If true, embeds session server module.	false
max_logoutset	Size of set that stores logged out HTTP sessions	20000
check.duplication.login	Whether to check duplicate logins	false

Note 1) Other Servers: Connected Session Server or Clustered Application Server