

Universal Messaging Administration Guide

Version 10.11

October 2021

This document applies to Software AG Universal Messaging 10.11 and to all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Copyright © 2013-2024 Software AG, Darmstadt, Germany and/or Software AG USA, Inc., Reston, VA, USA, and/or its subsidiaries and/or its affiliates and/or their licensors.

The name Software AG and all Software AG product names are either trademarks or registered trademarks of Software AG and/or Software AG USA Inc. and/or its subsidiaries and/or its affiliates and/or their licensors. Other company and product names mentioned herein may be trademarks of their respective owners.

Detailed information on trademarks and patents owned by Software AG and/or its subsidiaries is located at <https://softwareag.com/licenses/>.

Use of this software is subject to adherence to Software AG's licensing conditions and terms. These terms are part of the product documentation, located at <https://softwareag.com/licenses/> and/or in the root installation directory of the licensed product(s).

This software may include portions of third-party products. For third-party copyright notices, license terms, additional rights or restrictions, please refer to "License Texts, Copyright Notices and Disclaimers of Third Party Products". For certain specific third-party license restrictions, please refer to section E of the Legal Notices available under "License Terms and Conditions for Use of Software AG Products / Copyright and Trademark Notices of Software AG Products". These documents are part of the product documentation, located at <https://softwareag.com/licenses/> and/or in the root installation directory of the licensed product(s).

Document ID: NUM-AG-1011-20240216

Table of Contents

About this Documentation.....	5
Online Information and Support.....	6
Data Protection.....	7
Overview.....	9
2 Universal Messaging Enterprise Manager.....	11
About the Enterprise Manager.....	12
Starting the Enterprise Manager.....	12
Tab-by-Tab Overview.....	13
About the Enterprise View.....	16
Realm Administration.....	17
Zone Administration.....	78
Cluster Administration.....	81
Channel Administration.....	96
Queue Administration.....	112
Data Group Administration (Deprecated).....	121
Container Administration.....	124
Using ACLs for Role-Based Security.....	126
Integration with JNDI.....	131
Administering TCP Interfaces, IP Multicast, and Shared Memory.....	136
Plugins.....	151
Exporting and Importing Realm XML Configurations.....	167
Using the Enterprise Viewer.....	180
3 Using Command Central to Manage Universal Messaging.....	183
About Using Command Central to Manage Universal Messaging.....	184
Managing Universal Messaging Server Instances.....	184
Starting, Stopping, and Restarting Universal Messaging.....	185
Securing Communication Between Command Central and Universal Messaging.....	186
Configuring Universal Messaging.....	189
Securing Access to Command Central.....	212
Administering Universal Messaging.....	214
Viewing Universal Messaging Run-time Monitoring Statuses.....	225
Viewing Universal Messaging KPIs.....	225
Viewing Universal Messaging Logs.....	226
Viewing Universal Messaging Inventory.....	227
Configuration Types That the Universal Messaging Server Supports.....	227
Using the Command Line to Manage Universal Messaging.....	228
Lifecycle Actions for Universal Messaging Server.....	302
Run-time Monitoring States for Universal Messaging Server.....	302
Run-time Monitoring Statuses for Universal Messaging Server.....	303
Deployment of Universal Messaging Assets.....	304

Templates for Provisioning Universal Messaging.....	305
4 Comparison of Enterprise Manager and Command Central Features.....	307
5 Setting up Active/Passive Clustering with Shared Storage.....	315
About Active/Passive Clustering.....	316
Overview of Active/Passive Clustering on Windows.....	320
Overview of Active/Passive Clustering on UNIX.....	322
Configuring a Universal Messaging Active/Passive Cluster on UNIX.....	323
6 Command Line Administration Tools.....	327
Introduction to the Administration Tools.....	328
Starting the Tools using the Tools Runner Application.....	328
Performing Standard Administration Tasks on Realms and Clusters.....	330
Running a Configuration Health Check.....	337
The "Realm Information Collector" Diagnostic Tool.....	347
The ExportEventsFromOfflineMemFile Tool.....	355
The RepublishEventsFromOfflineFile Tool.....	361
The ServerReleaseVersion Tool.....	362
Syntax reference for command line tools.....	364
7 Universal Messaging Administration API.....	439
Introduction.....	440
Administration API Package Documentation.....	443
Namespace Objects.....	443
Realm Server Management.....	450
Security.....	456
Management Information.....	461
8 Configuring the Java Service Wrapper.....	469
9 Thread Pool Monitoring.....	475
10 Using Nginx with Universal Messaging.....	479
About Using Nginx with Universal Messaging.....	480
Configure Nginx to Direct HTTP Requests to Universal Messaging.....	480
Nginx Directives Configuration.....	481
Configure Nginx to Direct HTTPS Requests to Universal Messaging.....	482
Forward Requests Based on URL Matches.....	485
11 Migrating from IPv4 to IPv6.....	487
12 Data Protection and Privacy.....	489

About this Documentation

- Online Information and Support 6
- Data Protection 7

Online Information and Support

Software AG Documentation Website

You can find documentation on the Software AG Documentation website at <https://documentation.softwareag.com>.

Software AG Empower Product Support Website

If you do not yet have an account for Empower, send an email to empower@softwareag.com with your name, company, and company email address and request an account.

Once you have an account, you can open Support Incidents online via the eService section of Empower at <https://empower.softwareag.com/>.

You can find product information on the Software AG Empower Product Support website at <https://empower.softwareag.com>.

To submit feature/enhancement requests, get information about product availability, and download products, go to [Products](#).

To get information about fixes and to read early warnings, technical papers, and knowledge base articles, go to the [Knowledge Center](#).

If you have any questions, you can find a local or toll-free number for your country in our Global Support Contact Directory at https://empower.softwareag.com/public_directory.aspx and give us a call.

Software AG Tech Community

You can find documentation and other technical information on the Software AG Tech Community website at <https://techcommunity.softwareag.com>. You can:

- Access product documentation, if you have Tech Community credentials. If you do not, you will need to register and specify "Documentation" as an area of interest.
- Access articles, code samples, demos, and tutorials.
- Use the online discussion forums, moderated by Software AG professionals, to ask questions, discuss best practices, and learn how other customers are using Software AG technology.
- Link to external websites that discuss open standards and web technology.
- Go to our public GitHub and Docker repositories at <https://github.com/softwareag> and <https://hub.docker.com/u/softwareag> and discover additional Software AG resources.

Data Protection

Software AG products provide functionality with respect to processing of personal data according to the EU General Data Protection Regulation (GDPR). Where applicable, appropriate steps are documented in the respective administration documentation.

Overview

This administration guide covers the following areas:

- [“Universal Messaging Enterprise Manager” on page 11](#): This section describes the Enterprise Manager, which is Universal Messaging's native graphical user interface for management of your Universal Messaging environment. There is also a read-only version of the Enterprise Manager, called the Enterprise Viewer, which allows unprivileged users to view the Universal Messaging environment (see the section [“Using the Enterprise Viewer” on page 180](#) for details).
- [“Using Command Central to Manage Universal Messaging” on page 183](#): This section describes the parts of Command Central that are specific to Universal Messaging. Command Central is a generic tool used by many Software AG products. It provides a web browser and command-line interface to configure and manage Universal Messaging.
- [“Setting up Active/Passive Clustering with Shared Storage” on page 315](#): This section describes how to set up an active/passive cluster, using third party solutions that supply additional hardware and software for cluster management.
- [“Command Line Administration Tools” on page 327](#): This section describes a set of command line tools that allow you to perform many of the common actions available through Universal Messaging.
- [“Universal Messaging Administration API” on page 439](#): This section describes the powerful administration API that allows you to build applications to manage your Universal Messaging environment programmatically.

2 Universal Messaging Enterprise Manager

■ About the Enterprise Manager	12
■ Starting the Enterprise Manager	12
■ Tab-by-Tab Overview	13
■ About the Enterprise View	16
■ Realm Administration	17
■ Zone Administration	78
■ Cluster Administration	81
■ Channel Administration	96
■ Queue Administration	112
■ Data Group Administration (Deprecated)	121
■ Container Administration	124
■ Using ACLs for Role-Based Security	126
■ Integration with JNDI	131
■ Administering TCP Interfaces, IP Multicast, and Shared Memory	136
■ Plugins	151
■ Exporting and Importing Realm XML Configurations	167
■ Using the Enterprise Viewer	180

About the Enterprise Manager

The Enterprise Manager is a powerful, graphical management tool that enables the capture of extremely granular metrics, management, and audit information from multiple Universal Messaging server realms. The Enterprise Manager also enables you to control, configure, and administer all aspects of a Universal Messaging realm or clusters of realms.

The Enterprise Manager is based on the Universal Messaging administration API and any of its functionality can be integrated into bespoke or third-party system management services.

The Enterprise Manager and administration API use in-band management. This ensures that the flexibility of Universal Messaging connections is also made available from a management/monitoring perspective. Universal Messaging realms can be managed remotely over TCP/IP sockets, SSL-enabled sockets, HTTP, and HTTPS as well as through normal and user-authenticated HTTP/S proxies.

The Read-Only Enterprise Viewer

The Enterprise Viewer is a read-only version of the Enterprise Manager. It enables unprivileged users to view the same information as in the Enterprise Manager, but does not allow you to change the Universal Messaging environment in any way. For more information about the Enterprise Viewer, see [“Using the Enterprise Viewer” on page 180](#).

Starting the Enterprise Manager

In order to start administering and monitoring your Universal Messaging realm servers you need to launch the Enterprise Manager. The Enterprise Manager is capable of connecting to multiple Universal Messaging realms at the same time, whether these are part of a cluster / federated namespace or simple standalone realms. A configuration file called `realms.cfg` is created in your home directory which stores the Enterprise Manager's connection info, however the very first time you launch it a bootstrap `RNAME` environment variable can be used to override the default connection information. Subsequent launches will not depend on the environment variable as long as you save your connection information. For more information about saving your configuration, see [“Working with Realm Profiles” on page 33](#).

Launching on Windows platforms can be done by selecting the Enterprise Manager shortcut in the Start Menu.

You can also open a client command prompt and type a command of the following form:

```
<InstallDir>\UniversalMessaging\java\<InstanceName>\bin\nenterprisemgr.exe
```

where `<InstallDir>` is the installation root location and `<InstanceName>` is the name of the Universal Messaging server.

Launching on UNIX platforms can be done by executing the `nenterprisemgr` executable, which you can find under the installation directory at the following location:

```
java/umserver/bin/nenterprisemgr
```

Logging In

When you start the Enterprise Manager, there is a login dialog in which you can enter a user ID and password. The user ID and password are only required for logging in if you have activated basic authentication. If you have not activated basic authentication, the password is ignored, but the user ID is still subject to the usual ACL checks in the Enterprise Manager.

See the section *Basic Authentication* in the Developer Guide for information about setting up basic authentication.

Tab-by-Tab Overview

This section provides a high level overview of Enterprise Manager functionality on a tab by tab basis, for each of the following node types (as displayed in Enterprise Manager's navigation pane).

- [“Enterprise Node” on page 13](#)
- [“Realm Nodes” on page 13](#)
- [“Container \(Folder\) Nodes” on page 15](#)
- [“Channel Nodes” on page 15](#)
- [“Queue Nodes” on page 15](#)

Enterprise Node

Highlighting the **Enterprise** node in the tree provides an **Enterprise Summary** view of all realms to which Enterprise Manager is connected, and includes information such the total number of realms, clusters, channels, queues, events published and received, and more.

Realm Nodes

Highlighting a Realm node in the navigation tree in the left hand panel will bring up a context-sensitive set of tabs in the right hand panel:

- **Status Tab**

Provides a snapshot and historical view of statistics such as the number of events published or consumed, numbers of connections, and memory usage.

- **Monitoring Tab**

A container for multiple panels that enable you to view live information on the selected realm:

- **Logs**

Provides a rolling view of Universal Messaging Logs and Plugin Logs including Access and Error logs.

- **Connections**

Provides a list of all current connections to the realm, along with details such as protocol, user, and host. Allows connections to be "bounced" (forcing them to reconnect).

■ **Threads**

Provides details such as the number of idle and active threads per thread pool, task queue size per thread pool and a total number of executed tasks for the respective thread pool. It also provides details of scheduled operations each task has within the system.

■ **Top**

A "UNIX top"-like view of realm memory usage, JVM garbage collection statistics, channel and connection usage.

■ **Audit**

Displays the contents of the remote audit file and receives real time updates as and when audit events are generated.

■ **Metrics**

Provides metrics on current memory usage, such as on-heap event memory usage.

■ **ACL Tab**

Displays the realm ACL and the list of subjects and their associated permissions for the realm. Permits editing of ACLs.

■ **Comms Tab**

Provides access to management tools for TCP interfaces, IP Multicast and Shared Memory communication methods:

■ **Interfaces**

Management of TCP Interfaces (creation, deletion, starting/stopping) as well as configuration of advanced interface properties.

■ **Multicast**

Management of IP Multicast Configurations (creation/deletion) and advanced configuration tuning.

■ **Shared Memory**

■ **Realms Tab**

Provides a summary of memory, event and interface information for each realm to which Enterprise Manager is connected.

■ **Config Tab**

Manage the settings for many groups of advanced realm configuration parameters.

■ **JNDI Tab**

Enables the creation of references to JMS TopicConnectionFactory and QueueConnectionFactory, as well as references to Topics and Queues.

Container (Folder) Nodes

■ Totals Tab

Provides status information for resources and services contained within the selected container branch of the namespace tree.

■ Monitor Tab

A "Unix top"-like view of the usage of Channels or Queues found within the container node.

Channel Nodes

Highlighting a Channel node in the navigation tree in the left hand panel will bring up a context-sensitive set of tabs in the right hand panel:

■ Status Tab

Provides a snapshot and historical view of statistics such as the number of events published or consumed, rates, and event storage usage.

■ Joins Tab

Permits the user to view, add, delete and edit joins between Channels.

■ ACL Tab

Permits the user to add, remove or modify entries within the Channel ACL.

■ Durables

Enables the viewing and deletion of durables , which provide state information for durable consumers for the channel.

■ Snoop Tab

Permits snooping of events on the Channel

■ Connections

Enables the creation of references to JMS TopicConnectionFactory and QueueConnectionFactory, as well as references to Topics and Queues.

Queue Nodes

Highlighting a Queue node in the navigation tree in the left hand panel will bring up a context-sensitive set of tabs in the right hand panel:

■ Status Tab

Provides a snapshot and historical view of statistics such as the number of events published or consumed, rates, and event storage usage.

■ **Joins Tab**

Permits the user to view, add, delete and edit joins from any Channels to this Queue.

■ **ACL Tab**

Permits the user to add, remove or modify entries within the Queue ACL.

■ **Snoop Tab**

Permits snooping (a non-destructive read) of events on the Queue.

■ **Consumer Info Tab**

Provides information on currently connected queue consumers.

About the Enterprise View

The Enterprise view is the first screen you see when you start the Enterprise Manager. The screen gives an overview of the characteristics as well as current status of the set of Universal Messaging realms to which the Enterprise Manager is currently connected, your Universal Messaging enterprise. This summary view includes any Universal Messaging realms you have added to your connection information whether they are standalone development realms or production clustered realms. Adding a Universal Messaging realm to the Enterprise Manager's connection info will result in the realm's data being included in this view (see [“Connecting to Multiple Realms” on page 75](#) and [“Disconnecting from Realms” on page 76](#)).

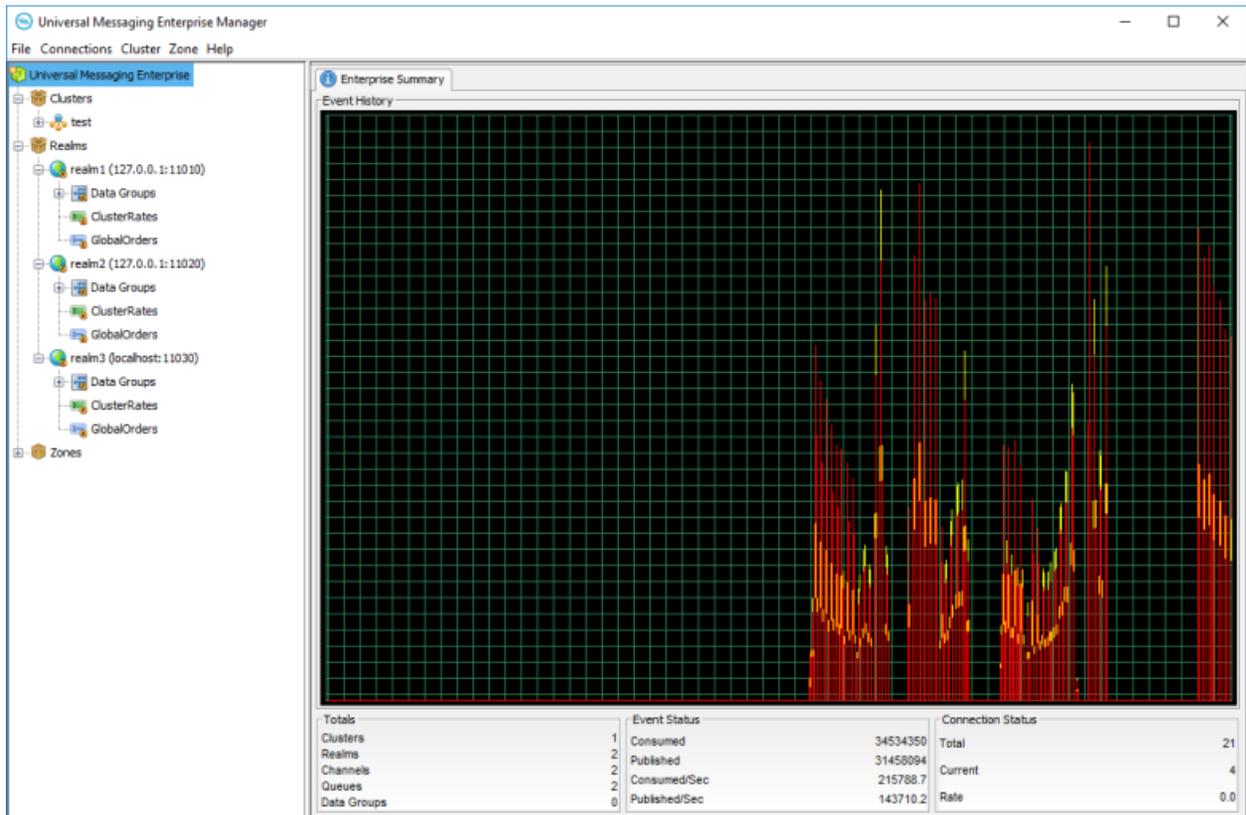
As you navigate through more specific parts of the Universal Messaging enterprise, you can always return to this screen by selecting the root node of the navigation tree named **Universal Messaging Enterprise**.

The view shows a large real time graph illustrating the total number of events published (yellow) and consumed (red) across all Universal Messaging realms. The bottom of the screen displays three panels named **Totals**, **Event Status**, and **Connection Status**.

The **Totals** panel displays the total number of clusters, realms and resources across all Universal Messaging realms.

The **Event Status** panel displays the total number of events consumed and published, as well as the current consume and publish rates (events per second).

The **Connection Status** panel displays the total number, the current number as well as the number of connections (sessions) being made per second across all realms at this point in time, whether application or administrative.



Realm Administration

Creating and Starting a Realm Server

Universal Messaging provides the following tools for performing general administrative tasks on realms, such as creating a realm, checking the status of a realm, and deleting a realm.

- **The Universal Messaging Instance Manager:**

For related information, see the section *Universal Messaging Instance Manager* in the *Installation Guide*.

- **Command Central:** If your installation of Universal Messaging includes the optional Command Central component, you can use the command line tool of Command Central to perform administrative tasks on realms.

For related information, see the section [“Using the Command Line to Manage Universal Messaging”](#) on page 228 in the *Command Central* part of the documentation.

Creating a Realm Server

You can use either the Universal Messaging Instance Manager or Command Central to create the realm server. See the examples in the corresponding documentation pages at the locations mentioned above.

Starting a Realm Server

After you have created the realm server, start the realm server as follows:

On Windows systems:

1. From the Windows Start menu, navigate to the node **Start Servers** that is located under the **Universal Messaging** node.
2. Navigate in the hierarchy to find the node labelled **Start <RealmName>**, and click it. Here, <RealmName> is the name you assigned to the realm server when you created it.

On UNIX systems:

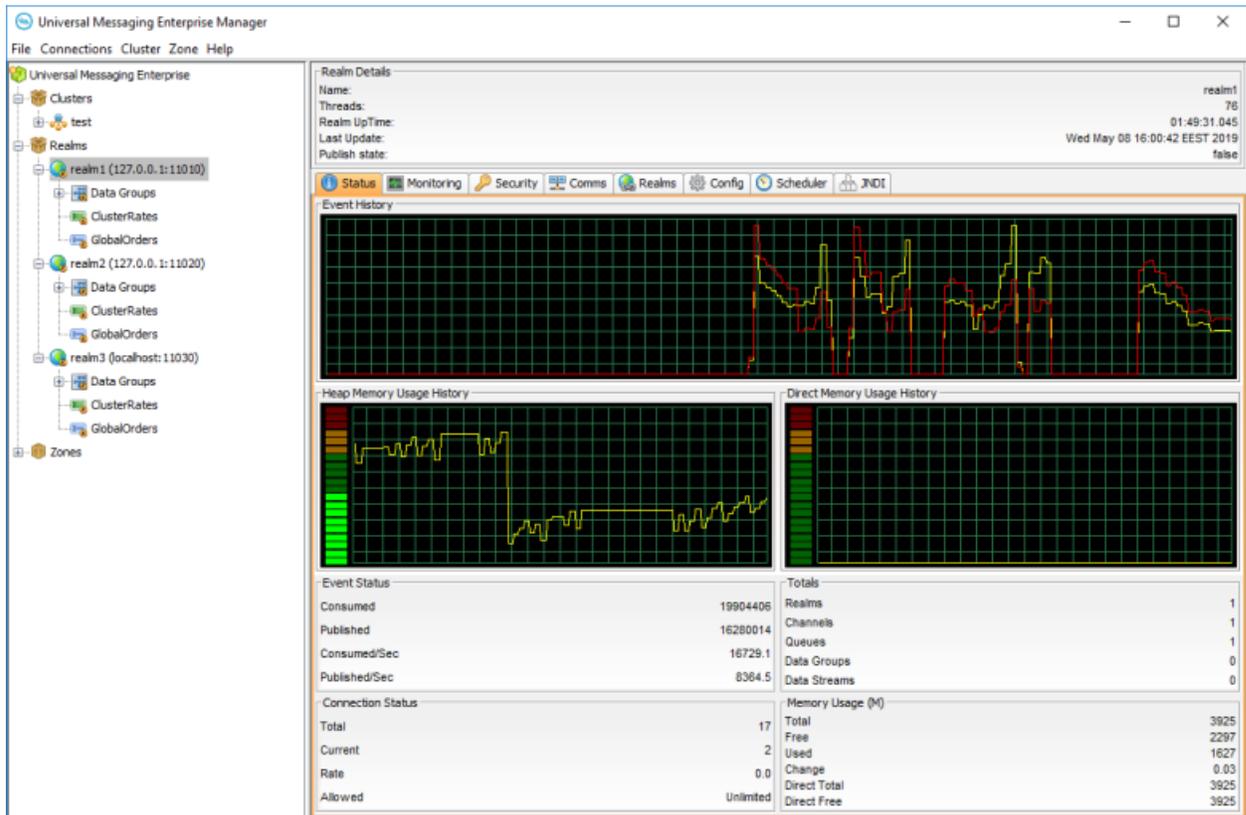
1. Start the script `nserver.sh` that is located in `UniversalMessaging/server/<RealmName>/bin/` under the product installation directory.

Related information on starting and stopping a realm server

For additional information on starting and stopping a realm server, see the sections *Starting the Realm Server* and *Stopping the Realm Server* in the *Installation Guide*.

Viewing a Realm

The Realm view provides information about the current status of the set of Universal Messaging realms that the Enterprise Manager is monitoring. When you select a realm node from the namespace, the status panel is displayed by default for the realm.



The top of the screen displays a panel containing the following information:

- **Name** - The name of the selected realm.
- **Threads** - The number of threads in the realm server's JVM.
- **Realm Up Time** - How long the realm has been running.
- **Last Update** - The time that the last status update was sent by the realm.
- **Publish state** - Whether server publishing is paused.

The Status panel contains real-time graphs illustrating the total number of events published (yellow) and consumed (red) across the Universal Messaging realm, as well as the direct memory usage history and heap memory usage history for the selected realm.

The bottom of the screen displays four panels named **Event Status**, **Totals**, **Connection Status**, and **Memory Usage**. These panels and the information displayed are described below.

Event Status

The Event Status section contains the following parameters:

- **Consumed** - The total number of events consumed by all channels, queues, and services on the realm.
- **Published** - The total number of events published to all channels, queues, and services on the realm.

- **Consumed/Sec** - The number of events consumed per second by all channels, queues, and services on the realm.
- **Published/Sec** - The number of events published per second to all channels, queues, and services on the realm.

Totals

The Totals section contains the following parameters:

- **Realms**- The number of realms mounted within this realm's namespace.
- **Channels**- The number of channels on the realm.
- **Queues**- The number of queues on the realm.
- **Data Groups**- The number of data groups on the realm.
- **Data Streams**- The number of data streams on the realm.

Connection Status

The Connection Status section contains the following parameters:

- **Total** - The total number of connections made to the realm.
- **Current** - The current number of connections to the realm.
- **Rate** - The number of connections being made per second to the realm.
- **Allowed** - The permitted number of concurrent connections.

Memory Usage(M)

The Memory Usage section contains the following parameters:

- **Total** - The total amount of MB allocated to the realm JVM, specified by the -Xmx value for the JVM.
- **Free** - The amount of JVM memory available for the realm.
- **Used** - The amount of JVM memory used by the realm.
- **Change** - The change in used memory for an interval of time in MB.
- **Direct Total** - The total allocatable amount of MB that the JVM can use before an Out Of Memory Exception occurs.
- **Direct Free** - The total amount of free (unused) direct memory in MB.

Monitoring a Realm

About Monitoring a Realm

You can view live information on a Universal Messaging realm server on the **Monitoring** tab for a selected server in the Enterprise Manager.

You can monitor the server log messages in real time, the current connections, thread status, channel and connection usage, audit events, and memory usage.

The Enterprise Manager Logs Panel

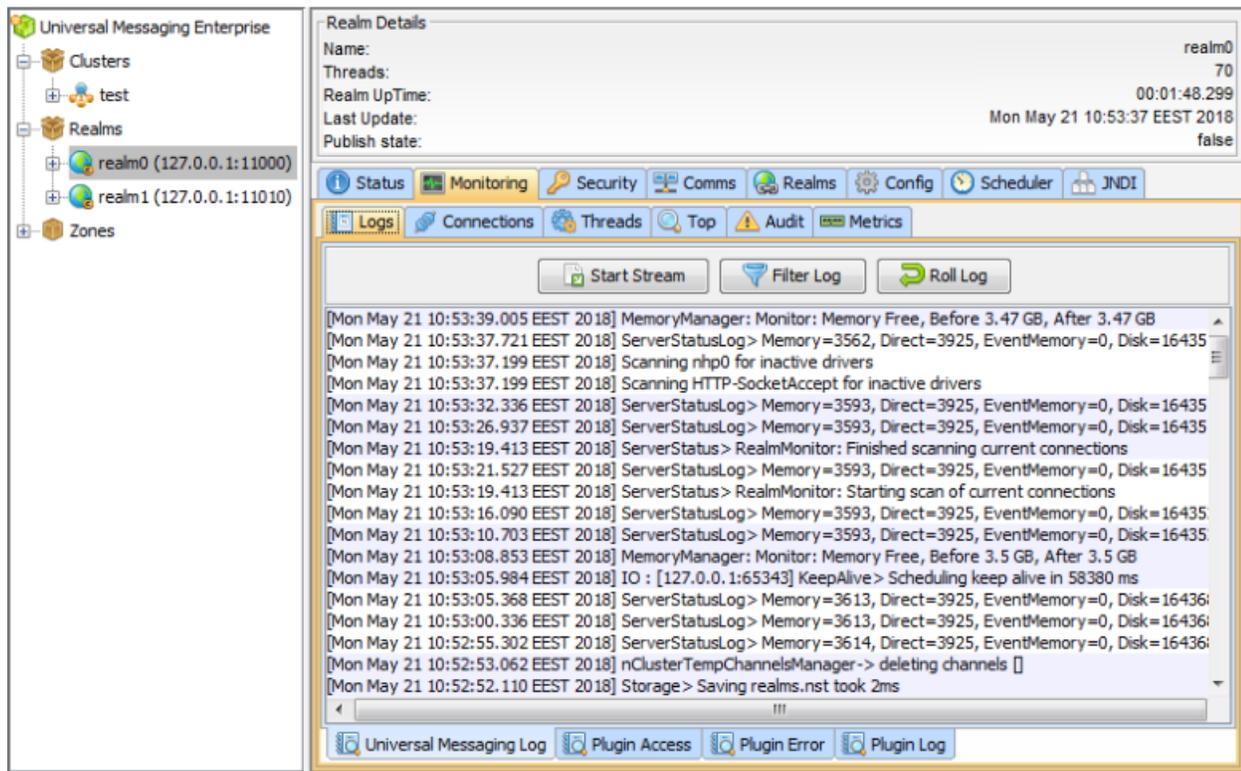
Each Universal Messaging realm server has a log file called `nirvana.log` within the directory `<InstallDir>\UniversalMessaging\server\<InstanceName>\data`, where `<InstallDir>` is the disk root location of your Universal Messaging installation and `<InstanceName>` is the name of the realm server.

The Enterprise Manager provides a panel that displays real time log messages as they are written to the log file. This enables you to remotely view the activity on a realm as it is happening. The Universal Messaging Administration API also provides the ability to consume the log file entries from an `nRealmNode`. See the code example "Monitor the Remote Realm Log and Audit File" for an illustration of usage.

The Universal Messaging log file contains useful information about various activities, such as connection attempts, channels being located and subscribed to, as well as status and warning information.

About the Logs Panel

The Enterprise Manager provides a panel for each realm where you can view the realm's log file. To view the log file, click the realm node from the namespace, select the **Monitoring** tab, and then select the **Logs** tab. This will show the live log messages for the selected realm. The log panel automatically replays the last 20 log entries from the realm server and then each entry thereafter. The image below shows an example of the log panel for a selected realm.



The log panel also enables you to stream the log messages to a local file. Click **Start Stream**, and then enter the name of the file to which you want to stream the log messages. To stop the stream, click **Stop**.

Understanding the log file

Entries in the log file have the following general format:

```
Timestamp LogLevel ThreadName Message
```

Where:

- **Timestamp** gives the date and time that the entry was created, for example:

```
[Fri May 18 09:03:46.610 EEST 2018]
```

The time of day is given in the format `hh:mm:ss.ttt`, representing hours, minutes, seconds, thousandths of a second.

- **LogLevel** determines the depth of information being logged. It is displayed only if the `EmbedTag` logging configuration property is set to true (default is false). See the description later in this section for details of logging levels.
- **ThreadName** is the name of the internal processing thread that generated the log message. This is displayed only if the `DisplayCurrentThread` logging configuration property is set to true (default is true).
- **Message** contains the actual information that is being logged.

See the section “[Realm Configuration](#)” on page 35 for information about configuration properties.

When a server is started, the initial entries in the log file contain useful information about the server's configuration. The following text is an excerpt from a realm server log during startup (the entries for `LogLevel` and `ThreadName` have been suppressed here for clarity) :

```
[Fri May 18 09:03:46.610 EEST 2018] =====
[Fri May 18 09:03:46.610 EEST 2018] Copyright (c) Software AG Limited. All rights
reserved
[Fri May 18 09:03:46.610 EEST 2018] Start date                = Fri May 18 09:03:46 EEST
2018
[Fri May 18 09:03:46.610 EEST 2018] Process ID                = 9040
[Fri May 18 09:03:46.610 EEST 2018]
[Fri May 18 09:03:46.610 EEST 2018] Realm Server Details :
[Fri May 18 09:03:46.610 EEST 2018] Product                    = Universal Messaging
[Fri May 18 09:03:46.610 EEST 2018] Realm Server name          = umserver
[Fri May 18 09:03:46.610 EEST 2018] Release Identifier         = 10.3.0.0.106659
[Fri May 18 09:03:46.610 EEST 2018] Build Date                 = May 17 2018
[Fri May 18 09:03:46.610 EEST 2018] Data Directory             =
C:\SoftwareAG\UniversalMessaging\server\umserver\data
[Fri May 18 09:03:46.610 EEST 2018] Extension Directory       =
C:\SoftwareAG\UniversalMessaging\server\umserver\plugins\ext
[Fri May 18 09:03:46.610 EEST 2018] Low Latency Executor      = false
[Fri May 18 09:03:46.610 EEST 2018] Has License Manager       = true
[Fri May 18 09:03:46.610 EEST 2018] Interfaces Running       :
[Fri May 18 09:03:46.610 EEST 2018]     0) nhp0: nhp://0.0.0.0:9000 Running
[Fri May 18 09:03:46.610 EEST 2018]
[Fri May 18 09:03:46.610 EEST 2018] Realm(s) Reloaded        = 1
[Fri May 18 09:03:46.610 EEST 2018] Channels Reloaded        = 0
[Fri May 18 09:03:46.610 EEST 2018] Queues Reloaded          = 0
[Fri May 18 09:03:46.610 EEST 2018] Data Groups Reloaded     = 0
[Fri May 18 09:03:46.610 EEST 2018] Interfaces Reloaded      = 1
[Fri May 18 09:03:46.610 EEST 2018]
[Fri May 18 09:03:46.610 EEST 2018] Operating System Environment :
[Fri May 18 09:03:46.610 EEST 2018] OS Name                   = Windows 7
[Fri May 18 09:03:46.610 EEST 2018] OS Version                 = 6.1
[Fri May 18 09:03:46.610 EEST 2018] OS Architecture           = amd64
[Fri May 18 09:03:46.610 EEST 2018] Available Processors      = 4
[Fri May 18 09:03:46.610 EEST 2018]
[Fri May 18 09:03:46.610 EEST 2018] Java Environment :
[Fri May 18 09:03:46.610 EEST 2018] Java Vendor                = Oracle Corporation
[Fri May 18 09:03:46.610 EEST 2018] Java Vendor URL            = http://java.oracle.com/
[Fri May 18 09:03:46.610 EEST 2018] Java Version               = 1.8.0_151
[Fri May 18 09:03:46.610 EEST 2018] Java Vendor Name           =
Java HotSpot(TM) 64-Bit Server VM 1.8.0_151-b12
[Fri May 18 09:03:46.610 EEST 2018] Memory Allocation          = 981 MB
[Fri May 18 09:03:46.610 EEST 2018] Memory Warning             = 834 MB
[Fri May 18 09:03:46.610 EEST 2018] Memory Emergency           = 922 MB
[Fri May 18 09:03:46.610 EEST 2018] Nanosecond delay          = Not Supported
[Fri May 18 09:03:46.610 EEST 2018] Time Zone                  = Eastern European Time
[Fri May 18 09:03:46.610 EEST 2018] Security Provider 0        = SUN version 1.8
[Fri May 18 09:03:46.610 EEST 2018] Security Provider 1        = SunRsaSign version 1.8
[Fri May 18 09:03:46.610 EEST 2018] Security Provider 2        = SunEC version 1.8
[Fri May 18 09:03:46.610 EEST 2018] Security Provider 3        = SunJSSE version 1.8
[Fri May 18 09:03:46.610 EEST 2018] Security Provider 4        = SunJCE version 1.8
[Fri May 18 09:03:46.610 EEST 2018] Security Provider 5        = SunJGSS version 1.8
[Fri May 18 09:03:46.610 EEST 2018] Security Provider 6        = SunSASL version 1.8
[Fri May 18 09:03:46.610 EEST 2018] Security Provider 7        = XMLDSig version 1.8
[Fri May 18 09:03:46.610 EEST 2018] Security Provider 8        = SunPCSC version 1.8
```

```
[Fri May 18 09:03:46.610 EEST 2018] Security Provider 9 = SunMSCAPI version 1.8
[Fri May 18 09:03:46.610 EEST 2018] =====
[Fri May 18 09:03:46.610 EEST 2018] Startup: Realm Server Startup sequence completed
```

The above sequence of log entries can be found at the beginning of the Universal Messaging log file, and shows information such as when the realm was started, the build number and build date of the Universal Messaging realm server, as well as environmental information like, OS, Java version, timezone.

Apart from the above-mentioned information, the log file on Unix provides details about the maximum number of file descriptors.

```
[Thu Aug 19 02:30:50.459 EEST 2021] [main] Operating System Environment :
[Thu Aug 19 02:30:50.459 EEST 2021] [main] OS Name = Linux
[Thu Aug 19 02:30:50.459 EEST 2021] [main] OS Version = 3.10.0-1160.6.1.el7.x86_64
[Thu Aug 19 02:30:50.459 EEST 2021] [main] OS Architecture = amd64
[Thu Aug 19 02:30:50.459 EEST 2021] [main] Available Processors = 4
[Thu Aug 19 02:30:50.460 EEST 2021] [main] Physical Memory = 15885 MB
[Thu Aug 19 02:30:50.460 EEST 2021] [main] Total Swap space = 3071 MB
[Thu Aug 19 02:30:50.460 EEST 2021] [main] Max file descriptors = 4096
```

Log Levels

The Universal Messaging log level is a level from 0 to 6 that determines what information is written to the log. Log level 0 is the most verbose level of logging and on a heavily utilized server will produce a lot of log output. Log level 6 is the least verbose level, and will produce low levels of log output. The log level of each log message corresponds to a value from 0 to 6. The following list explains the log file messages levels and how they correspond to the values:

- 0 - TRACE (Log level 0 will output any log entries with a level in the range 0-6; this is the most verbose level)
- 1 - DEBUG (Log level 1 will output any log entries with a level in the range 1-6)
- 2 - INFO (Log level 2 will output any log entries with a level in the range 2-6)
- 3 - WARN (Log level 3 will output any log entries with a level in the range 3-6)
- 4 - ERROR (Log level 4 will output any log entries with a level in the range 4-6)
- 5 - FATAL (Log level 5 will output any log entries with a level in the range 5-6)
- 6 - LOG (Log level 6 will output any log entries with a level of 6; this is the least verbose level)

Log levels can be changed dynamically on the server by using the **Config** panel (see [“Realm Configuration” on page 35](#)). The log file has a maximum size associated with it. When the maximum file size is reached, the log file will automatically roll, and rename the old log file to `_old` and create a new log file. The maximum size for a log file is set to 10000000 bytes (approximately 10MB). This value can be changed within the `Server_Common.conf` file in the `server/<InstanceName>/bin` directory of your installation, where `<InstanceName>` is the name of the Universal Messaging realm. You need to modify the `-DLOGSIZE` property within this file to change the size.

Other Logging Frameworks

By default, Universal Messaging uses a built-in logging framework, but it also supports third-party open-source frameworks including Logback and Log4J2. Note that Log4J2 is supported only in a Docker environment.

To configure Universal Messaging to use one of these frameworks, you can pass a `-DLOG_FRAMEWORK` parameter with the values `LOGBACK` or `LOG4J2`. See the section *Server Parameters* in the Concepts guide for further information.

These frameworks are configured using XML configuration files loaded from the classpath. The Universal Messaging installation provides default versions of these configuration files in the `lib` directory. These files can be modified in order to produce the desired logging output. For more information on configuration see the official documentation of the relevant framework.

When you configure Universal Messaging to use Log4j2 as the logging framework, the **Logs** panel shows only the Universal Messaging server loggers (`com.pcbSys.foundation`, `com.pcbSys.nirvana.base`, `com.pcbSys.nirvana.server`, `com.pcbSys.nirvana.server.handler`, `com.pcbSys.nirvana.server.plugins`, `com.pcbSys.nirvana.server.plugins.protocols`, `com.pcbSys.foundation.security.login`). The **Logs** panel does not show any other loggers defined in the `log4j2.xml` configuration file.

When Universal Messaging is configured to use Logback as the logging framework, the majority of the server startup messages in the server's `nirvana.log` file will be written with status `ERROR`. This happens due to a limitation in Logback that does not provide usage of custom log levels. Therefore, Universal Messaging messages logged with `LOG` level are translated to `ERROR` level when Logback is used.

The Log Manager

Universal Messaging has three different log managers for archiving old log files. When a log file reaches its maximum size, the log manager will attempt to archive it, and a new log file will become active. Options such as the number of log files to keep, and the maximum size of a log file are configurable through the logging section of the **Config** panel (see [“Realm Configuration” on page 35](#)). When a log file is archived and a new log file created, realm specific information such as Universal Messaging version number will be printed to the start of the new log in a similar way to when a realm is started. Each log manager uses a different method to store log files once they are not the active logs for the realm.

- **ROLLING_OLD** : This log manager uses 2 log files. The active log file is stored with the default log name, and the most recently rolled log file is stored with `_old` appended to the log name. e.g. `nirvana.log` and `nirvana.log_old`
- **ROLLING_DATE** : The rolling date manager stores a configurable number of log files (`RolledLogFileDepth`). Rolled log files are stored with the date they were rolled appended to the active log file name. e.g. `nirvana.logWed-Sep-14-02-31-40-117-BST-2011`.
- **ROLLING_NUMBER** : The numbered log manager stores a configurable number of log files (`RolledLogFileDepth`). Rolled log files are stored with a numbered index appended to the file name e.g. `nirvana.log3` is the 3rd oldest log file

Realm Connections

When a Universal Messaging client connects to a realm server, the server maintains information about the connection. For more information, see [“Connection Information” on page 466](#)), which is available through the Universal Messaging Administration API. The API also provides mechanisms for receiving notifications when connections are added and deleted. See the code example [“Connection Watch”](#) for an illustration of using this in the Administration API.

The Universal Messaging Enterprise Manager enables you to view the connections on a realm as well as to view specific information about each connection, such as the last event sent or received, and the rate of events sent and received from each connection.

To view the current realm connections, select a realm node from the namespace, and then click **Monitoring > Connections**. The Enterprise Manager displays a panel containing a table of connections, as shown in the image below. The table lists all the clients connected to the realm server

The screenshot shows the Universal Messaging Enterprise Manager interface. The left sidebar displays a tree view of the namespace, including Clusters, Realms, and Zones. The main panel is titled 'Universal Messaging Enterprise Manager' and has a menu bar with 'File', 'Connections', 'Cluster', 'Zone', and 'Help'. Below the menu bar is a toolbar with icons for Status, Monitoring, Security, Comms, Realms, Config, Scheduler, and JNDI. The 'Connections' tab is selected, showing a 'Connection Summary' table. The table has columns for protocol, user, host, connection, language, and name. Two connections are listed: one for 'vival' on host '127.0.0.1' with connection ID '127.0.0.1:163303' and another for 'vival' on host '127.0.0.1' with connection ID '127.0.0.1:159681'. The table also shows summary statistics: Total 18, Current 2, Rate 0.0, and Allowed Unlimited. At the bottom of the panel are buttons for 'Show Details', 'Show List', 'Bounce', and 'Redirect'.

The connections table contains the following information:

- **protocol** - The protocol used in the connection.
- **user** - The name of the connected user.
- **host** - The host machine from which the user is connecting.
- **connection** - The local connection ID, defined as *hostname:local_port*.

- **language** - The language that the client application is using.
- **name** - The name of the operating system on which the client application is running.
- **build number** - the build number of the client API.

To disconnect a connection and then make the client reconnect again, select a connection in the table and click **Bounce**.

To view more details about a specific connection, double-click the connection in the table or click **Show Details**. The connection details panel is shown in the image below.

The screenshot displays the Universal Messaging Enterprise Manager interface. On the left, a tree view shows the hierarchy of Clusters, Realms, and Zones. The 'realms' folder is expanded, and 'realm1 (127.0.0.1:11010)' is selected. The main panel on the right shows the 'Realms Details' for the selected realm, including Name, Threads, Realm UpTime, Last Update, and Publish state. Below this, there are tabs for Status, Monitoring, Security, Comms, Realms, Config, Scheduler, and JNDI. The 'Connections' tab is active, showing 'Connection Details' and 'Client Environment' information. The 'Tx Event History' and 'Rx Event History' graphs are visible, showing event rates over time. At the bottom, a table displays 'Events Sent' and 'Events Received' statistics, along with 'Status' information like Connect Time, Queue Size, Last Tx, and Last Rx.

Events Sent		Events Received		Status	
Total	958	Total	32	Connect Time	00:07:16.560
Rate	1.8	Rate	0.0	Queue Size	0
Max	11046.4	Max	296009.2	Last Tx	00:00:00.000
Last Evt Type	Publish Event	Last Evt Type	HeartBeat	Last Rx	00:00:08.900
Bytes	314.3 KB	Bytes	484.0		

Connection Details

The Connection Details panel contains information about the user connection, such as user name, host, and protocol.

Client Environment

The Client Environment panel contains information about the client environment for this user. These include API language / Platform, Host OS, and Universal Messaging build number.

The Tx Event History and Rx Event History graphs show the total (yellow) and rates (red) for events received from the server (TX) and sent to the server (RX) for the selected connection.

Events Sent

The Events Sent section contains the following values:

- **Total** - The total number of events sent by the realm server to this connection
- **Rate** - The rate at which events are being sent by the realm server to this connection
- **Max** - The maximum rate at which events have been sent by the realm server to this connection
- **Last Event Type** - The type of the last event sent from the realm server
- **Bytes** - Total bytes sent by the realm server to this connection

Events Received

The Events Received section contains the following values:

- **Total** - The total number of events sent by this connection to the realm server
- **Rate** - The rate at which events are being sent by connection to the realm server
- **Max** - The maximum rate at which events have been sent by this connection to the realm server
- **Last Event Type** - The type of the last event sent from the connection to the realm server
- **Bytes** - Total bytes sent by this connection to the realm server

Status

The Status section contains the following values:

- **Connect Time** - The amount of time this connection has been connected to the realm server
- **Queue Size** - The number of events in the outbound queue of this connection (i.e. events waiting to be sent to the realm server)
- **Last Tx** - The time since the last event was received by this connection from the realm server
- **Last Rx** - The time since the last event was sent to the server from this connection

Click **Show List** to go back to the connections table.

Threads Status

The **Threads** tab on the Monitoring panel provides two statistical views: thread pools and scheduler tasks.

The **Pools** tab shows the number of idle and active threads per thread pool, as well as the task queue size per thread pool and the total number of executed tasks for the respective thread pool.

The **Scheduler** tab provides information about the number of scheduled operations each task has within the system.

The Top Tab

The **Top** tab on the Monitoring panel of a selected realm node provides a view not unlike 'top' for Unix systems or the Task Manager for Windows-based systems. The Top panel gives you a high level view of realm usage, both from a connection perspective and a channel perspective.

You can view real-time graphs of realm memory usage, JVM GC stats, and CPU usage. This section also contains a summary showing the number of mounted realms, the number of resources, and the number of services.

The bottom section of the panel displays a series of tabs showing channel and connection usage throughout the realm.

Channel Usage

The **Top Channel Usage** tab shows channel usage throughout the realm. Each row in the Top Channel Usage table represents a channel. Channel usage can be measured a number of ways. Each measurement corresponds to a column in the table. When you click one of the column headers, all known channels will be sorted according to their value for the selected column. For example, when you click the Connections column, the table will be sorted according to the number of consumers that each channel has. The channel with the most number of consumers will appear at the top of the table.

Channel usage measurements are described below:

- **Connections** - The number of consumers the channel has
- **Published** - The rate of events published per status interval
- **Consumed** - The rate of events consumed per status interval
- **Memory (bytes)** - The number of bytes the channel uses from the JVM memory
- **% Memory** - The percentage of overall JVM memory used by this channel
- **Disk** - The amount of disk space used by this channel, only relevant for persistent / mixed channels

Connection Usage

The **Top Connection Usage** tab represents connection usage. Each row in the table represents a connection. A connection corresponds to the physical aspect of a Universal Messaging Session. Connection usage, like channel usage can be measured in a number of different ways. Each column in the table represents a type of measurement for a realm connection. Clicking on one of the column headers will cause the table of connections to be sorted according to the value of the selected column. For example, one of the columns is 'Events In', i.e. the number of events sent to the server by the connection. By clicking on the column header labeled 'Events In', the table will be sorted according to the number of events each connection has sent to the server. The connection with the most 'Events In' count will appear at the top of the table.

Connection usage measurements are described below:

- **Queued**- The number of event in the connections outbound queue
- **Events In** - The rate of events sent by the connection to the realm server
- **Bytes In** - The rate of bytes sent by the connection to the realm server
- **Events Out** - The rate of events consumed by the connection from the realm server
- **Bytes Out** - The rate of bytes consumed by the connection from the realm server
- **Latency** - The measured time it takes the connection to consume events from the server, i.e. time taken between leaving the realm server and being consumed by the connection.

Monitor Graphs

The monitor panel provides a method of graphing both channel and connection usage. It uses a 3D graph package from [sourceforge](http://sourceforge.net/projects/jfreechart/) (<http://sourceforge.net/projects/jfreechart/>) to display the items in each table as columns in a 3D vertical bar chart. The bar charts can be update live as the values in the tables are updated. Once a column is selected, simply click on the button labeled 'Bar Graph' under either the channel or connections table and a graph panel will appear, as shown in the image below showing a graph of the number of events published for channels within a realm..

Right-clicking anywhere within the graph will show a pop-up menu of options. One of the options is labeled 'Start Live Update', which will ensure the graph consumes updates as and when they occur to the table. Once the live update is started, you can also stop the live update by once again right clicking on the graph and selecting 'Stop Live Update'.

You can also print the graph, and save the graph image as a '.png' file, as well as alter the properties of the graph and its axis.

The Audit Tab

Universal Messaging Realm Servers log administration operations performed on the realm to a file. These events are called audit events and are stored in a local file called NirvanaAudit.mem. These audit events are useful for tracking historical information about the realm and who performed what operation and when. The Universal Messaging Administration API provides the ability to consume the audit file entries from an nRealmNodeM. See the code example "Monitor the Remote Realm Log and Audit File" for an illustration of usage.

The Universal Messaging Enterprise Manager provides an Audit panel that displays the contents of the remote audit file and receives real time updates as and when audit events are generated. The audit events that are written to the audit file are determined by the configuration specified in the Config panel (see "[Realm Configuration](#)" on page 35) of the Universal Messaging Enterprise Manager.

Audit Events

Each audit event corresponds to an operation performed on an object within a realm. The audit event contains the date on which it occurred, the object and the operation that was performed on the object.

The list below shows the objects that audit events correspond to as well as the operations performed on them that are logged to the audit file:

- **Realm** - CREATE, DELETE, ACCESS
- **Interfaces** - CREATE, DELETE, MODIFY, START, STOP
- **Channels** - CREATE, DELETE, MODIFY
- **Queues** - CREATE, DELETE, MODIFY
- **Services** - CREATE, DELETE
- **Joins** - CREATE, DELETE
- **Realm**
- **ACL** - CREATE, DELETE, MODIFY
- **Channel ACL** - CREATE, DELETE, MODIFY
- **Queue ACL** - CREATE, DELETE, MODIFY
- **Service ACL** - CREATE, DELETE, MODIFY

The Audit Panel

To view audit events for a realm, select the realm, and go to **Monitoring > Audit**.

When you first connect to a realm, the Audit panel displays the last 20 audit events from its history. Audit files can become quite large over time on a heavily used realm, so the initial load is limited to just the last 20. After that, all subsequent audit events are shown in the Audit panel.

Each audit event is shown as a row in a table that has the following columns:

- **Date** - The time at which the audit event occurred on the server
- **Originator** - Who performed the operation
- **Type** - What type of object was the action performed on
- **Action** - What action was performed
- **Object** - The name of the object

If the object type is an ACL for either a realm, resource or service, selecting the entry from the table will also display the ACL changes in the bottom section of the audit panel. For modified ACLs, each acl permission that has been granted or removed will be displayed as a green '+', or a red '-' respectively.

Streaming Audit Events

To stream the remote audit events from the realm to a local file, on the Audit panel, click **Start Stream**, and then select a file. This provides you with the option of replaying the entire audit file or just the last 20 audit entries.

The text below is an excerpt from a sample audit file that has been streamed from a server. Each entry that relates to a modified ACL shows the permissions that have been changed, and the permissions that are granted by either a + or -. For permissions that have remained the same, the letter 'N' for not change will be placed after the permission.

```
Fri Jan 21 15:43:40 GMT 2005,CHANACL,/customer/sales:*@*,MODIFY,paul weiss@localhost,
Full(-), Last Eid(N),Purge(-),Subscribe(N),Publish(-),Named Sub(N),Modify Acls(-),
List Acls(-),
Fri Jan 21 15:43:40 GMT 2005,QUEUEACL,/partner/queries:*@*,MODIFY,
paul weiss@localhost,Full(-),Purge(-), Peek(N),Push(-),Pop(-),Modify Acls(-),
List Acls(-),
Fri Jan 21 15:43:40 GMT 2005,QUEUEACL,/partner/queries:paul weiss@localhost,MODIFY,
paul weiss@localhost, Full(N),Purge(N),Peek(N),Push(N),Pop(N),Modify Acls(N),
List Acls(N),
Fri Jan 21 16:13:10 GMT 2005,INTERFACE,nhp0,CREATE,paul weiss@localhost,
Fri Jan 21 16:15:31 GMT 2005,INTERFACE,nhp0,MODIFY,paul weiss@localhost,
```

Archive Audit

Depending on what is logged to the audit file, the file can grow quite large. Because it is an audit and provides historical data, there is no automatic maintenance of the file and it is down to the realm administrators when the file is archived. To archive the audit file and start a new file, on the Audit panel, click **Archive Audit**.

The Metrics Tab

The **Metrics** tab on the Monitoring panel contains the following information:

- **Current Memory Usage** - Current memory used by the server to store events in memory.
- **Maximum Available Memory** - Maximum on-heap memory available.
- **Current Memory Percentage** - Percentage of used on-heap memory at the moment.

Updating Connection Information

The Universal Messaging Enterprise Manager can connect to multiple Universal Messaging realms at the same time and enables you to save connection information in a configuration file named `realms.cfg`. By default, the file is saved to your home directory. The content of the files is updated in the following cases:

- When you select **File > Save** in the Enterprise Manager, the content of the configuration file is replaced with the list of current connections.
- When a connection to a configured realm fails and you opt not to retry connecting to the realm, the failed connection is removed from the configuration file. The Enterprise Manager does not try to connect to that Universal Messaging realm again during startup.
- When you select **File > Edit Details**, in the Edit Realm Connection Info dialog box, you select realms to remove from the configuration file. In the **Realm** field, select a realm and click **Delete**. Click **OK** to save the modified configuration file.

The **Realm** field contains all Universal Messaging realms currently shown in the Enterprise Manager.

Working with Realm Profiles

The Universal Messaging Enterprise Manager enables administrators to group realms and their respective connections into profiles for easy management and accessibility. You can save any number of realms as part of a profile by clicking **File > Save**. The Enterprise Manager creates a default configuration file named `realms.cfg` and saves it to your home directory.

You can also create several configurations (profiles) that contain different sets of realms. To do so, click **File > Save As**, which enables you to choose the name and location of the configuration file.

To load a profile, click **File > Open Profile**. The Universal Messaging Enterprise Manager automatically connects to all realms defined in the loaded profile.

Realm Federation

As well as clustering technology, Universal Messaging supports the concept of a federated namespace which enables realm servers that are in different physical locations to be viewed within one logical namespace.

Note:

Clustering and Realm Federation are mutually exclusive. If a realm is a member of a cluster, you cannot use the realm for federation. Similarly, if a realm is part of a federation, the realm cannot be used for clustering.

If you consider that a Universal Messaging namespace consists of a logical representation of the objects contained within the realm, such as resources and services: a federated namespace is an extension to the namespace that allows remote realms to be visible within the namespace of other realms.

For example, if we had a realm located in the UK (United Kingdom), and 2 other realms located in the US (United States) and DE (Germany), we can view the realms located in DE and US within the namespace of the UK realm. Federation allows us to access the objects within the DE and US realms from within the namespace of the UK realm.

It is possible to add realms to a Universal Messaging namespace using the Universal Messaging Administration API or by using the Enterprise Manger as described below.

Adding Realms

The first step in order to provide federation is to add the realms. Adding a realm to another realm can be achieved in two ways. The first way simply makes a communication connection from one realm to another, so the realms are aware of each other and can communicate. This enables you to create a channel join between these realms.

Note:

For a description of the general principles involved in creating channel joins, see the section *Creating Channel Joins*. The description details the usage based on the Enterprise Manager, but the same general principles apply if you are using the API.

The second option also makes a new communication connection, but if you specify a *mount point*, the realm you add will also be visible within the namespace of the realm you added it to.

Mount Points

Providing a mount point for added realms is similar to the mount point used by file systems when you mount a remote file system into another. It specifies a logical name that can be used to access the resources within the mounted realm. The mount point is therefore the entry point (or reference) within the namespace for the realm's resources and services.

For example, if I have a realm in the UK, and wish to add to it a realm in the US, I could provide a mount point of '/us' when adding the US realm to the UK realm. Using the mount point of '/us', I can then access the channels within the US realm from my session with the UK realm. For example, if I wanted to find a channel from my session with the UK realm, and provided the channel name '/us/customer/sales', I would be able to get a local channel reference to the '/customer/sales' channel within the US realm.

Using the Enterprise Manager to Add Realms

To add a realm to another realm, first of all you need to select the realm node from the namespace that you wish to add the realm to. Then, right-click on the realm node to display the menu options available for a realm node. One of the menu options is labelled 'Add Realm to Namespace', clicking on this menu option will display a dialog that allows you to enter the RNAME of the realm you wish to add and an optional mount point.

The RNAME value in the dialog corresponds to the realm interface that you want the two realms to use for communication. The mount point corresponds to the point within the namespace that the realm will be referenceable.

For example, you can have a realm named 'node1' that has two realms mounted within its namespace, named 'eur' and 'us'. The resources within both the mounted realms are also displayed as part of the namespace of the 'node1' realm.

Sessions connected to the 'node1' realm now have access to three channels. These channels are:

- '/global/orders', which is a local channel
- '/eur/orders,' which is actually a channel on another Universal Messaging realm that has been added to this namespace under the mount point '/eur'
- '/us/orders', which is actually a channel on another Universal Messaging Realm that has been added to this namespace under the mount point '/us'

Example Use of Federation: Remote Joins

Once you have added the realms to one another, it is possible to create remote joins between the channels of the realms. This is very useful when considering the physical distance and

communications available between the different realms. For example, if you wish all events published to the /customer/sales channel in the UK realm to be available on the /customer/sales channel in the US realm, one would create a join from the /customer/sales channel in the UK to the /customer/sales channel on the US realm, so all events published onto the uk channel would be sent to the us channel.

Federation and remote joins provide a huge benefit for your organization. Firstly, any consumers wishing to consume events from the uk channel would not need to do so over a WAN link, but simply subscribe to their local sales channel in the us. This reduces the required bandwidth between the us and uk for your organization, since the data is only sent by the source realm once to the joined channel in the us, as opposed to 1...n times where n is the number of consumers in the us. Remote joins are much more efficient in this respect, and ensure the data is available as close (physically) to the consumers as possible.

Note:

For a description of the general principles involved in creating channel joins, see the section *Creating Channel Joins*. The description details the usage based on the Enterprise Manager, but the same general principles apply if you are using the API.

Realm Configuration

Universal Messaging Realms can be configured based on a number of properties that are accessible both through the Universal Messaging Administration API as well as the Universal Messaging Enterprise Manager. Any changes made to the configuration properties for a Universal Messaging realm are automatically sent to the realm and implemented. This functionality offers major benefits to Administrators, since realms can be configured remotely, without the need to be anywhere near the actual realm itself. More importantly, multiple realms and clustered realms can also be automatically configured remotely.

Note:

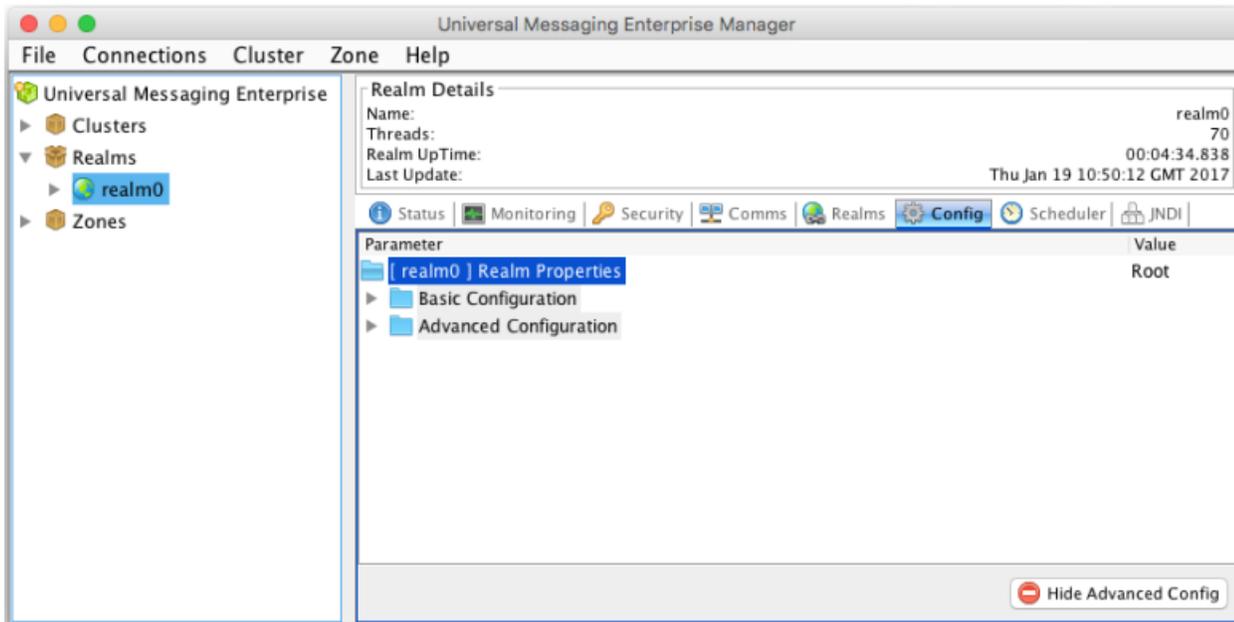
Some Universal Messaging realm properties, such as the AMQP Message Transformation setting, are applied on a per-connection basis, meaning that clients must re-connect to pick up a change in the realm-wide value.

This section describes the different configuration properties that are available using the Universal Messaging Enterprise Manager.

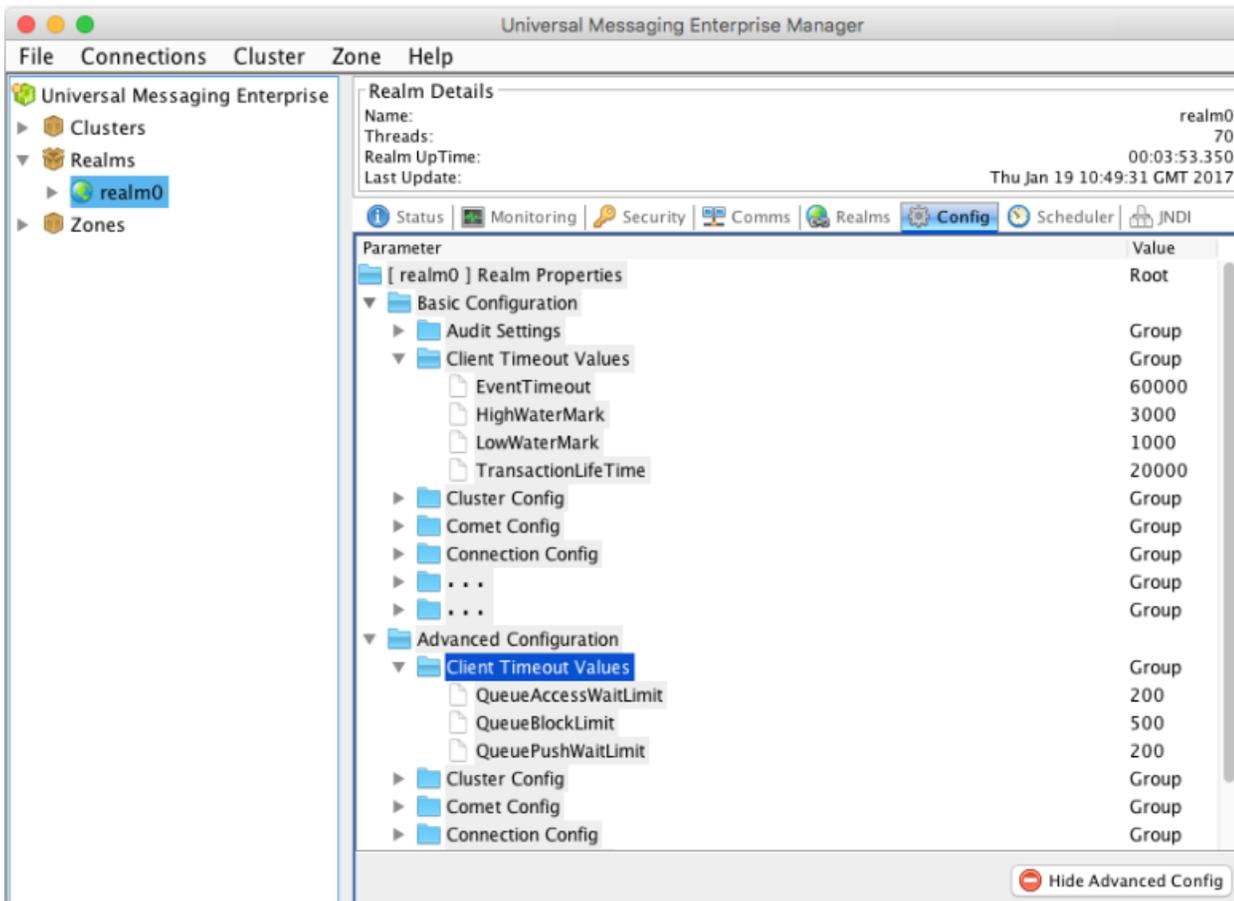
When you select a realm from the namespace, one of the available panels in the Enterprise Manager is labelled 'Config'. Selecting this panel displays various groups of configuration properties, with each group of properties relating to a specific area within the Universal Messaging Realm. Each group of properties contains different values for specific items.

Basic and Advanced Properties

There are currently a large number of configuration properties, and they are divided into two categories, namely Basic and Advanced. The properties in the Basic category are the most commonly used ones. The properties in the Advanced category will probably be less frequently used, and are intended for special cases or expert users.



When the Basic and Advanced categories are expanded, you will see a display of the configuration properties. Properties that have a similar effect are arranged into groups; for example, properties that determine when a client times out are contained in the group "Client Timeout Values":



Note that in the example shown, the group "Client Timeout Values" appears in both the Basic and the Advanced category. However, the properties "EventTimeout", "HighWaterMark" etc. belonging to this group appear only under the Basic category, whereas the properties "QueueAccessWaitLimit" etc. belonging to the same group appear only under the Advanced category. The properties in the Basic category are the ones which you will probably find most useful for your day-to-day work.

Configuration Groups

The configuration groups are:

1. **Audit Settings** - Values relating to what information is stored by the audit process
2. **Client Timeout Values** - Values relating to client / server interaction
3. **Cluster Config** - Values specific to the clustering engine
4. **Comet Config** - Values relating to the configuration of Comet
5. **Connection Config** - Values relating to the client server connection
6. **Data Stream Config** - Values relating to the configuration of Data Streams
7. **DurableConfig** - Values relating to usage of durables
8. **Environment Config** - Read only configuration values that relate to the system environment. These cannot be changed.
9. **Event Storage** - Values specific to how events are stored and retrieved on the server
10. **Fanout Values** - Values specific to the delivery of events to clients
11. **Global Values** - Values specific to the realm process itself
12. **Inter-Realm Comms Config** - Values relating to Inter-Realm communication
13. **JVM Management** - Values relating to the JVM the Realm Server is using
14. **Join Config** - Values specific to channel join management
15. **Logging Config** - Values specific to logging
16. **Metric Config** - Values relating to metric management
17. **Plugin Config** - Values relating to Realm Plugins
18. **Protobuf Config** - Values relating to Protocol Buffers
19. **Protocol AMQP Config** - Values relating to the use of AMQP connections
20. **Protocol MQTT Config** - Values relating to the use of MQTT connections
21. **RecoveryDaemon** - Values relating to clients that are in recovery (i.e. replaying large numbers of events)
22. **Server Protection** - Values specific to server protection

23. **Thread Pool Config** - Values specific to the servers thread pools.

24. **Trace Logging Config** - Values specific to event lifecycle logging (trace logging).

25. **TransactionManager** - Values specific to the transaction engine of the RealmServer

The table below describes the properties that are available within each configuration group. It also shows valid ranges of values for the properties and a description of what each value represents. The "Adv. " column shows "Y" if the property is in the Advanced category, whereas no entry indicates that the property is in the Basic category.

Configuration Group/Property	Valid values	Description	Adv.
Audit Settings			
ChannelACL	True or False	Log to the audit file any unsuccessful channel ACL interactions. Default is true.	
ChannelFailure	True or False	Log to the audit file any unsuccessful realm interactions. Default is true.	
ChannelMaintenance	True or False	Log to the audit file any channel maintenance activity. Default is false.	
ChannelSuccess	True or False	Log to the audit file any successful channel interactions. Default is false.	
DataGroup	True or False	Log to the audit file any changes to Data Group structure	
DataGroupFailure	True or False	Log to the audit file any failed attempts to Data Group structure	
DataStream	True or False	Log to the audit file Data Stream add and removes	
Group	True or False	Log to the audit file any added or removed security groups	
GroupMembers	True or False	Log to the audit file any changes in group membership	
InterfaceManagement	True or False	Log to the audit file any interface management activity. Default is true.	
JoinFailure	True or False	Log to the audit file any unsuccessful join interactions. Default is true.	
JoinMaintenance	True or False	Log to the audit file any join maintenance activity. Default is true.	

Configuration Group/Property	Valid values	Description	Adv.
JoinSuccess	True or False	Log to the audit file any successful join interactions. Default is <code>false</code> .	
QueueACL	True or False	Log to the audit file any unsuccessful queue ACL interactions. Default is <code>true</code> .	
QueueFailure	True or False	Log to the audit file any unsuccessful queue interactions. Default is <code>true</code> .	
QueueMaintenance	True or False	Log to the audit file any queue maintenance activity. Default is <code>false</code> .	
QueueSuccess	True or False	Log to the audit file any successful queue interactions. Default is <code>false</code> .	
RealmACL	True or False	Log to the audit file any unsuccessful realm ACL interactions. Default is <code>true</code> .	
RealmFailure	True or False	Log to the audit file any unsuccessful realm interactions. Default is <code>true</code> .	
RealmMaintenance	True or False	Log to the audit file any realm maintenance activity. Default is <code>true</code> .	
RealmSuccess	True or False	Log to the audit file any successful realm interactions. Default is <code>false</code> .	
SnoopStream	True or False	Log to the audit file Snoop stream add and removes	
Client Timeout Values			
EventTimeout	5000 to No Max	The amount of ms the client will wait for a response from the server. Small values may cause clients to abandon waiting for responses and disconnect prematurely. Large values may cause clients to take an unusually long amount of time waiting for a response before disconnecting. Default is 60000.	
HighWaterMark	2 to 2147483647	The high water mark for the connection internal queue. When this value is reached the internal queue is temporarily suspended and unable to send events to the server. This provides	

Configuration Group/Property	Valid values	Description	Adv.
		flow control between publisher and server. Default is 3000.	
LowWaterMark	1 to 2147483647	The low water mark for the connection internal queue. When this value is reached the outbound internal queue will again be ready to push event to the server. Default is 1000.	
QueueAccessWaitLimit	200 to 2147483647	The maximum number of milliseconds it should take to gain access to an internal connection queue to push events. Once this time has elapsed the client session will inform any listeners registered on the session which monitor these connection queues. Small values may result in an excessive number of notifications. Default is 200.	Y
QueueBlockLimit	500 to 2147483647	The maximum number of milliseconds an internal connection queue will wait before notifying listeners after it has reached the HighWaterMark. Small values may result in excessive notifications. Default is 500.	Y
QueuePushWaitLimit	200 to 2147483647	The maximum number of milliseconds it should take to gain access to an internal connection queue and to push events before notifying listeners. Small values may result in excessive notifications. Default is 200.	Y
TransactionLifeTime	1000 to No Max	The default amount of time a transaction is valid before being removed from the tx store. Default is 20000.	
Cluster Config			
ClientQueueSize	10 to 10000	Size of the client request queue. If this queue is small then the clients will wait longer and performance may drop.	

Configuration Group/Property	Valid values	Description	Adv.
		If too large then client requests are queued but not processed.	
ClientQueueWindow	1 to 1000	<p>The value used when an async consumer of type queue or durables of types shared queue, shared, and serial do not set an explicit value for the window size.</p> <p>Default is 100.</p> <p>Important: A small number will reduce performance.</p>	
ClientStateDelay	0 to 120000	The number of seconds to delay the cluster processing client requests when a cluster state change occurs. A large number will delay client requests longer than required.	
ClusterMode	Active or Replication	<p>Specifies whether to allow non-admin client connections to nodes other than the master node in a cluster.</p> <p>If the value is set to <i>Active</i> (default value), client connections can be made to any node in a cluster. The clients can also make use of the <i>FollowTheMaster</i> feature.</p> <p>If <i>ClusterMode</i> is set to <i>Replication</i>, non-admin client connections can be made to only the master node. Nodes that are not the master node will reject all non-admin client connections. With this setting, attempts by clients to use the <i>FollowTheMaster</i> feature will be ignored.</p> <p>Note: Admin clients can connect to any node in a cluster, irrespective of the <i>ClusterMode</i> configuration.</p>	
DisableHTTPConnections	True or False	Disable HTTP(s) connections between cluster nodes. If <i>true</i> then the server	

Configuration Group/Property	Valid values	Description	Adv.
		will only use nsp(s) connections between realm nodes, and any nhp(s) rnames will be switched to using nsp(s).	
DisconnectWait	1000 to 120000	The time (in milliseconds) to wait for the server to join the cluster while trying to process cluster-wide user requests. If you increase the wait time, have in mind that the server might block the processing of client requests during the wait period.	
EnableMulticast	True or False	Enables cluster requests broadcast to realms to be send through the reliable multicast mechanism within Universal Messaging. This setting only takes effect if a multicast interface is configured for all nodes within the cluster.	
EnableStoreRecoveryRetry	True or False	Enables/Disables the ability for the slave to re-attempt a recovery of a store if it detects changes to the store during recovery. If true the slave will continue to attempt a cluster recovery of a store which may be changing due to TTL or capacity on the store attributes.	Y
EnginePipelineSize	1 to 32	Number of concurrent pipeline threads running within the cluster engine. If set to 1, then all requests are pipelined through one thread, else topics/queues are bound to specific pipelines.	Y
FormationTimeout	60000 to 300000	The time to wait for the state to move from recovery to slave or master. If this value is too small then recovering a large number of events will result in the realms dropping out of the cluster.	
HeartBeatInterval	1000 to 120000	Heart Beat interval in milliseconds. Default is 120000. A small value here will cause excessive messages being generated between realms.	

Configuration Group/Property	Valid values	Description	Adv.
InitialConnectionTimeout	5000 to 240000	The number of milliseconds that the server will wait while trying to establish a connection to a peer. A small value may reduce the chance of a connection in busy networks, while a large number may delay cluster formation.	
IsCommittedDelay	1000 to 30000	When a slave processes an IsCommitted request and it is still recovering the Transaction store, it will block the clients request for this timeout period. If this is set to a large value, clients may experience a substantial delay in response.	Y
MasterRequestTimeout	1000 to 900000	Specifies the amount of time in milliseconds that the master is going to wait for a slave to respond to a single request before disconnecting it. This timeout will prevent a slave from being reconnected if it fails to respond to a master request.	
MasterVoteDelay	1000 to 60000	When a node has requested to be master it will wait this timeout period in milliseconds for the peers to agree. If this number is too high the cluster formation may take some time.	
MasterWaitTimeout	1000 to 600000	When the master is lost from the cluster and the remaining peers detect that the master has the latest state they will wait for this time period for the master to reconnect. If the master fails to reconnect in this time period a new master is elected.	
PublishQueueEnabled	True or False	If enabled the slaves will queue publish requests prior to committing them to the cluster. If enabled and a slave is killed, any outstanding publish events will be lost.	Y
QueueSize	100 to 1000	Number of events outstanding to be processed by the clusters internal queue before sending flow control requests	

Configuration Group/Property	Valid values	Description	Adv.
		back. Increased size increases the memory usage.	
StateChangeScan	10000 to No Max	When a realm loses master or slave state then after this timeout all cluster based connections will be disconnected. If the realm reenters the cluster then the disconnect timeout is aborted. If this value is too low, all clients will be bounced while the cluster is forming.	
SyncPingSize	100 to 10000	Number of events sent before a cluster sync occurs. A small number will affect overall performance, a large number may result in a cluster being too far out of sync.	Y
Comet Config			
BufferSize	1024 to 102400	The buffer size for Comet requests. Large sizes will cause the realm to consume more memory when reading data from Comet clients. Small sizes may introduce delays in the time taken to read requests.	Y
EnableLogging	True or False	Enables logging of all comet queries, will impact server performance.	
Timeout	10000 to No Max	The timeout for a Comet connection. Small sizes may cause Comet-based connections to time out prematurely. Large sizes may increase the time a server holds a disconnected Comet connection open.	
Connection Config			
AllowBufferReuse	True or False	If set to <code>true</code> then buffers will be allocated from the buffer pool and once finished with returned to the pool. If set to <code>false</code> then buffers are allocated on the fly and then left for the system to free them. It is best to leave this set	Y

Configuration Group/Property	Valid values	Description	Adv.
		to true. For object creation limitation it is best to set this to true.	
BufferManagerCount	1 to 256	The number of Buffer Managers that the server will allocate. This is used during startup to size and manage the network buffers. This does not need to be large, but a rule of thumb is 1 per core.	Y
BufferPoolSize	100 to 10000	The underlying Universal Messaging IO utilizes buffers from a pool. By default we pre-load the pool with this number of buffers. As the reads/writes require buffers they are allocated from this pool, then once used are cleared and returned. If the size is too small we end up creating and destroying buffers, and the server may spend time creating them when needed. If the size is too large we have a pool of buffers which are not used taking up memory.	Y
BufferSize	1024 to 1048576	<p>This specifies the default size of the network buffers that Universal Messaging uses for its NIO. If small, then Universal Messaging will require more buffers (up to the maximum specified by BufferPoolSize) to send an event. If too large, then memory may be wasted on large, unused buffers.</p> <p>These buffers are reused automatically by the server, and are used to transfer data from the upper application layer to the network. So, for example, the server might use all BufferPoolSize buffers to stream from 1 application level buffer (depending on the relative sizes of the buffers).</p> <p>An efficient size would be about 40% more than the average client event, or 5K (whichever is largest). If too small, the server will send many small buffers.</p>	

Configuration Group/Property	Valid values	Description	Adv.
CometReadTimeout	1000 to 120000	Specifies the time the server will wait for a client to complete sending the data.	
ConnectionDelay	10 to 60000	When the server has exceeded the connection count, how long to hold on to the connection before disconnecting. If this is too low, the server will be busy with reconnection attempts. Default is 60000.	Y
IdleDriverTimeout	120000 to 2147483647	Specifies the time in milliseconds that a communications driver can be idle before being deemed as inactive. When this happens the server will automatically close and remove the driver. This must be greater than the keep alive timeout else all connections will be closed due to inactivity.	
IdleSessionTimeout	10000 to No Max	If there has been no communication from a client for the configured number of milliseconds, the client is deemed idle and is disconnected. This typically occurs when there are network issues between a client and the server. If the value is too low, the chance of disconnecting a valid session is high.	
KeepAlive	5000 to No Max	The number of milliseconds the server will wait before sending a heartbeat. A small number will cause undue network traffic. Default is 60000. Changes to this property are not applied to existing connections but only to connections established after you modify the value.	
MaxBufferSize	1024 to 2147483647	The maximum buffer size in bytes that the server will accept. Default is 20971520 (20MB). Rather than using larger buffers, it is recommended that you compress if possible to save bandwidth and memory on the server.	

Configuration Group/Property	Valid values	Description	Adv.
		<p>This value exists to stop a user from accidentally or maliciously overloading the server and causing excessive memory consumption.</p> <p>The <code>MaxBufferSize</code> connection configuration option is propagated to client sessions when they are initialized (during the session handshake), therefore changing this option does not have effect for already initialized client sessions.</p>	
MaxNoOfConnections	-1 to 2147483647	The total number of concurrent connections to the server. The default is -1, which indicates no limit on the number of connections. When you set a limit, connections that exceed the limit are rejected. However, a user with <i>both</i> the Override Connection Count realm permission and an admin connection can override the limit and still connect to the server.	
MaxNoOfConnectionsPerUserName	-1 to 2147483647	The number of concurrent connections to the server per user. The default is -1, which indicates no limit on the number of connections. When you set a limit, if connections exceed the specified number, the client gets <code>nSecurityException</code> . However, a user with <i>both</i> the Override Connection Count realm permission and an admin connection can override the limit and still connect to the server.	
MaxWriteCount	5 to 100	When writing many events to a client the write pool thread may continue to send the events before returning to the pool to process other clients requests. So, for example if it is set to 5, then the thread will send 5 events from the clients queue to the client before returning to the pool to process another request. If this number is small it creates additional CPU overhead.	

Configuration Group/Property	Valid values	Description	Adv.
NetworkMonitorThreads	2 to 100	The number of threads to allocate to flushing client data, Please note this will only take effect after a restart. Depending on the number of concurrent clients the latencies during load my be higher then expected.	
PriorityQueueCount	2 to 10	Sets the number of queues to divide priority levels between, up to a maximum of 10 queues.	
PriorityReadSpinLockMaxConnections	0 to 8	Maximum number of clients allowed to allocate high priority spin locks. This property is deprecated and will be removed in a future product release.	
PriorityReadSpinLockTime	1 to 10000	The time interval (in milliseconds), during which the thread spin read handler will continuously try reading events. The setting has effect only when PriorityReadType is set to Thread Spin. Default value is 500 milliseconds. This property is deprecated and will be removed in a future product release.	Y
PriorityReadType	0 to 2	If enabled then high priority sessions will be enabled to run spin locks waiting to read. This property is deprecated and will be removed in a future product release.	
QueueHighWaterMark	100 to 2147483647	The number of events in a client output queue before the server stops sending events. A small number will cause undue work on the server. Default is 3000.	
QueueLowWaterMark	50 to 2147483647	The number of events in the clients queue before the server resumes sending events. Must be less than the high water mark. Default is 1000.	
ReadCount	1 to 20	Number of times the thread will loop around waiting for an event to be delivered before returning. Large	

Configuration Group/Property	Valid values	Description	Adv.
		values may cause read threads to be held for long periods of time, but avoid context switching for delivering events.	
UseDirectBuffering	True or False	If true the server will allocate <code>DirectByteBuffer</code> s to use for network I/O, else the server will use <code>HeapByteBuffer</code> s. The main difference is where the JVM will allocate memory for the buffers the <code>DirectByteBuffer</code> s perform better. For the best performance the <code>DirectByteBuffer</code> s are generally better.	Y
WriteHandlerType	1 to 5	Specifies the type of write handler to use	
whEventThresholdCount	1 to 2000	Number of events to exceed in the <code>whEventThresholdTime</code> to detect a peak. This number should be small enough to trigger peaks.	
whEventThresholdTime	1 to 2000	Number of milliseconds to sample the event rate to detect peaks	
whMaxEventsBeforeFlush	1 to 10000	Total number of events that can be sent before a flush must be done. If this number is too small then too many flushes will result.	
whMaxEventsPerSecond	No Min to No Max	Specifies the total number of events per second that a realm will send to clients before switching modes into peak mode. If this number is small then the server will go into peak mode too soon and latencies will start to increase.	
whMaxTimeBetweenFlush	1 to 1000	Total number of milliseconds to wait before a flush is done. If this number is too large then latencies will increase.	
Data Stream Config			
MonitorTimer	1000 to 120000	Time interval in milliseconds to scan the data group configuration looking for idle / completed streams. Large	Y

Configuration Group/Property	Valid values	Description	Adv.
		values may cause idle and inactive datastreams to remain on datagroups for long periods of time. Small values may cause transient disconnections to trigger datagroup removals for datastreams - requiring them to be added back into the datagroup.	
OffloadMulticastWrite	True or False	If <code>true</code> then all multicast writes will be performed by the parallel fanout engine.	Y
SendInitialMapping	True or False	When any stream registered client connect sends the entire Data Group Name to ID mapping	Y
DurableConfig			
DurableNameFiltering	True or False	If <code>true</code> , the server checks the subscriber ID header of published events. If the header is not empty, it is used to designate that an event can be consumed by a specific durable object, if the subscriber ID matches the name of the durable subscription.	Y
EnableConsumerStateMonitor	True or False	If <code>true</code> , the server checks the state of the store consumers once every minute. When the server finds unhealthy consumers, it logs diagnostic log messages about them in the <code>nirvana.log</code> file. These log entries are prefixed with the 'Consumer Warning:' header and are at the WARNING log level. On a system with thousands of stores, disabling this monitor helps to improve performance. If <code>false</code> , the diagnosing of consumer issues is harder. The default value is <code>true</code> .	
QueuedExtendedException	True or False	If <code>true</code> , then if the selector on a queued durable changes, the selector is added to the exception string.	Y

Configuration Group/Property	Valid values	Description	Adv.
Environment Config			
AvailableProcessors	READ ONLY	Number of CPUs available	
Embedded	READ ONLY	If <code>true</code> , this specifies that the server is running as an embedded server	
InterRealmProtocolVersion	READ ONLY	Universal Messaging Server Inter-Realm Protocol Version	
JavaVendor	READ ONLY	Vendor of Java Virtual Machine	
JavaVersion	READ ONLY	Virtual Machine Version	
NanosecondSupport	READ ONLY	Nanosecond support available through JVM on Native OS	
OSArchitecture	READ ONLY	Operating System Architecture	
OSName	READ ONLY	Operating System Name	
OSVersion	READ ONLY	Operating System Version	
ProcessId	READ ONLY	Process ID	
ServerBuildDate	READ ONLY	Universal Messaging Server Build Date	
ServerBuildNumber	READ ONLY	Universal Messaging Server Build Number	
ServerReleaseDetails	READ ONLY	Universal Messaging Release Details	
ServerVersion	READ ONLY	Universal Messaging Server Build Version	
TimerAdjustment	READ ONLY	The size of the Operating System's time quantum.	
Event Storage			

Configuration Group/Property	Valid values	Description	Adv.
ActiveDelay	100 to No Max	The time in milliseconds that an active channel will delay between scans. The smaller the number, the more active the server. Default is 1000.	Y
AutoDeleteScan	1000 to 500000	Specifies the number of milliseconds between scans on AutoDelete stores to see if they should be deleted. The larger this time frame, the more AutoDelete stores will potentially not be deleted on the server.	
AutoMaintenanceThreshold	0 to 100	<p>Sets the percentage of free space in the persistent disk store before the server should run auto-maintenance on the store. It is by default 50. This means maintenance will be performed when 50% of the number of the events in the file are marked as dead (already consumed and acknowledged) so they can be deleted.</p> <p>Note: The auto-maintenance feature is available for single-file disk stores only. If you are using a multi-file disk store, the auto-maintenance feature is not available for this store, and any realm configuration properties that you set for auto-maintenance will be ignored for this store.</p>	
CacheAge	1000 to No Max	The length of time in milliseconds that cached events will be kept in memory. The larger the value, the more memory will be utilized.	Y
EnableStoreCaching	True or False	<p>If true the server will try to cache events in memory after they have been written/read. Please note the server will need to be rebooted for this to take effect.</p> <p>By default, caching is disabled. To enable caching, set both the</p>	

Configuration Group/Property	Valid values	Description	Adv.
		EnableStoreCaching and EnableCaching configuration properties to true.	
IdleDelay	5000 to No Max	The time in milliseconds that an idle channel will delay between scans. The smaller the number, the more active the server. Default is 10000.	Y
JMSEngineAutoPurgeTime	5000 to 600000	Defines the interval between clean up of events on a JMS Engine Resource. A large interval may result in topics with large numbers of events waiting to be purged.	Y
MaintenanceFileSizeThreshold	1024000	Sets the store file size in bytes that will trigger the auto-maintenance of the persistent disk store. With small store file sizes, the auto-maintenance will be run more often. With large store file sizes, the auto-maintenance may take longer to run. There are no performance issues with a big store file except on startup when the store needs to be reloaded. Note: The auto-maintenance feature is available for single-file disk stores only. If you are using a multi-file disk store, the auto-maintenance feature is not available for this store, and any realm configuration properties that you set for auto-maintenance will be ignored for this store.	
MaintenanceMemoryThreshold	1048576	Maximum size in memory for any topic or queue to reach before maintenance of the in-memory cache is run.	
PageSize	10 to 100000	The page size to use for the event store. This value sets the number of events/page.	
QueueSubscriberFiltering	True or False	If set to true, the server will check the subscriber name/host header of published events and if that header is	

Configuration Group/Property	Valid values	Description	Adv.
		<p>not empty, it will be used to designate that an event can be consumed by a specific subscriber if the subscriber name and/or host matches the subject user and/or host of the subscription. Switching on this option imposes a minor performance penalty as the server then performs additional filtering.</p> <p>Additionally, for clustered subscriptions, the master realm may need to load the event from the store to perform the filtering, which could have additional cost depending on the type of store and caching used.</p> <p>Default is <code>false</code>.</p> <p>Subscriber name/host filtering is activated at the API level by using the <code>setSubscriberName()</code> method of <code>nConsumeEvent</code>.</p>	
StoreReadBufferSize	1024 to 3000000	Size of the buffer to use during reads from the store. Note that the server will need to be restarted for this to take effect.	Y
SyncBatchSize	1 to 1000	Specifies the maximum size before the sync call is made. The lower this value, the more sync calls made and the more overhead incurred.	Y
SyncServerFiles	True or False	If <code>true</code> the server will sync each file operation for its internal files. If <code>true</code> , this adds additional overhead to the server machines and can reduce overall performance.	
SyncTimeLimit	1 to 1000	Specifies the maximum time in milliseconds that will be allowed before the sync is called. The lower this value, the more file sync calls and the more overhead incurred.	Y

Configuration Group/Property	Valid values	Description	Adv.
ThreadPoolSize	1 to 4	The number of threads allocated to perform the management task on the channels. The more channels a server has, the larger this number should be.	
Fanout Values			
ConnectionGrouping	True or False	If true allows the server to group connections with the same selector providing improved performance. This allows the server to optimize the way it processes events being delivered to the clients. This requires a server restart to take effect.	Y
DelayPublishOnCapacity	True or False	Delays the publisher thread when the store capacity is exceeded. If this is not set, an exception is passed back to the client.	
HonourSharedDurableCapacity	True or False	If true, the channel will check any shared durables for capacity before accepting a published event. If any of these durables are over capacity, the server will respond as if the parent channel is over capacity. If false, the event will be published regardless of the number of events on its shared durables.	Y
IteratorWindowSize	1 to 100	Specifies the number of events delivered to each Channel Iterator in a prefetch. This allows the client to perform much faster by prefetching events on fast moving topics requiring less client to server communication. The default is 100.	
JMSQueueMaxMultiplier	1 to 10	The multiplier used on the High Water mark when processing events from a JMS Engine Queue/Topic. If this value is too high the server will consume vast amounts of memory.	Y

Configuration Group/Property	Valid values	Description	Adv.
ParallelThreadPoolSize	2 to 64	Specifies the number of threads to use within the thread pool. If this number is small then there may be adverse overheads. This value requires a restart to take effect.	
PeakPublishDelay	0 to No Max	When clients start to hit high water mark, this specifies how long to delay the publisher to allow the client time to catch up. If this is too small the publisher can overwhelm the server.	Y
PublishDelay	0 to No Max	How long to delay the publisher when the subscriber's queue starts to fill, in milliseconds. If this number is 0 then no delay.	Y
PublishExpiredEvents	True or False	Specifies whether to publish expired events at server startup. Default is true.	
SendEndOfChannelAlways	True or False	Specifies whether to always send an End Of Channel, even if we find no matches within the topic. If set, the subscriber will always be informed that the subscription request has completed the recovery of the topic.	
SendPubEventsImmediately	True or False	Specify whether to send publish events immediately. If true, then the server will send all publish events to clients immediately, if false the server is allowed to collect events before publishing.	
Global Values			
AllowRealmAdminFullAccess	True or False	If true then any user with the full realm access will have access to all channels and queues.	Y
CacheJoinInfoKeys	True or False	If enabled we cache join key information between events passed over joins. This reduces the number of objects created. If this property is set to false then the server will create a new byte[] and string for each joined event.	Y

Configuration Group/Property	Valid values	Description	Adv.
DisableExplicitGC	True or False	If enabled the server will call the Garbage Collector at regular intervals to keep memory usage down. If this is disabled then the garbage collection will be done solely by the JVM.	
EnableCaching	True or False	<p>If set to <code>true</code>, the channel storage properties <code>Cache On Reload</code> and <code>Enable Caching</code> are set to the values specified by the client.</p> <p>If set to <code>false</code>, then the channel storage properties <code>Cache On Reload</code> and <code>Enable Caching</code> are set to <code>false</code>, regardless of the values set by the client for these storage properties.</p> <p>By default, caching is disabled. To enable caching, set both the <code>EnableStoreCaching</code> and <code>EnableCaching</code> configuration properties to <code>true</code>.</p>	
EnableDNSLookups	True or False	If enabled the server will attempt to perform a DNS lookup when a client connects to resolve the IP address to a hostname. In some instances this may slow down the initial client connections.	
EnableWeakReferenceCleanup	True or False	If enabled then the server will hook into the JVM's garbage collection and release cached items when the JVM needs memory. By enabling this, the number of cached events stored will be reduced but memory will be maintained.	Y
ExtendedMessageSelector	True or False	If <code>true</code> , allows the server to use the extended message selector syntax (enabling string to numeric conversions within the message selector). Default is <code>true</code> .	
HTTPCookieSize	14 to 100	The size in bytes to be used by <code>nhp(s)</code> cookies	Y

Configuration Group/Property	Valid values	Description	Adv.
OverrideEveryoneUser	True or False	Override the <code>*@*</code> permission for channels / queues with explicit ACL entry permissions. Default is <code>false</code> .	
PauseServerPublishing	True or False	<p>If <code>true</code>, the Pause Publishing feature is activated. Default is <code>false</code>.</p> <p>This feature causes the server to block all attempts by clients to publish events, and such clients will receive an <code>nPublishPausedException</code>. However, events that already exist in the publishing client queues on the server continue to be consumed by the subscribing clients until the queues are emptied.</p> <p>You can use the Pause Publishing feature when it is necessary to clear the client event queues on the realm server. This could be, for example, before performing maintenance tasks such as increasing buffer storage or performing a backup, or before changing the server configuration.</p>	
SendRealmSummaryStats	True or False	If <code>true</code> sends the realm's status summary updates every second. Default is <code>false</code> .	
StampDictionary	True or False	Place Universal Messaging details into the dictionary. The default is <code>true</code> .	
StampHost	True or False	Stamps the header with the publishing host (<code>true/false</code>). If <code>true</code> adds additional overhead to the server/client.	
StampTime	True or False	Stamps the header with the current time (<code>true/false</code>). If <code>true</code> , adds additional overhead to the server/client.	
StampTimeUseHPT	True or False	If this is set to <code>true</code> , then the server will use an accurate millisecond clock, if available, to stamp the dictionary. This may impact overall performance when delivering events when latency is important.	

Configuration Group/Property	Valid values	Description	Adv.
StampTimeUseHPTScale	0 to 2	This has 3 values, milli, micro or nano accuracy	
StampUser	True or False	Stamps the header with the publishing user (true/false). If true, adds additional overhead to the server/client.	
StatusBroadcast	2000 to No Max	<p>This property has two purposes:</p> <ul style="list-style-type: none"> ■ The number of milliseconds between status events being published to any clients using Admin API or Enterprise Manager. A small value increases the server load. ■ The number of milliseconds between status messages being written to the server log, when periodic status logging has been activated via the EnableStatusLog property. <p>Remember that if you change the value of this property, it will affect the time interval for both status events and status log intervals.</p> <p>The default is 5000, i.e. every 5 seconds.</p>	
Inter-Realm Comms Config			
EstablishmentTime	10000 to 120000	Time for an inter-realm link to be initially established. This value should reflect the latency between nodes.	Y
KeepAliveInterval	1000 to 120000	Time interval where if nothing is sent a Keep Alive event is sent. This can be used to detect if remote members are still up and functioning.	Y
KeepAliveResetTime	10000 to 180000	If nothing has been received for this time the connection is deemed closed. This value must be larger than the KeepAliveInterval.	Y

Configuration Group/Property	Valid values	Description	Adv.
MaximumReconnectTime	1000 to 50000	The maximum number of milliseconds to wait before trying to re-establish a connection. If this value is too large, cluster formation will be delayed. The reconnect will be attempted at a random amount of time between <code>MinimumReconnectTime</code> and <code>MaximumReconnectTime</code> .	Y
MinimumReconnectTime	100 to 10000	The minimum time to wait before trying to re-establish a connection. If this number is too high then it may impact the network during outages. The reconnect will be attempted at a random amount of time between <code>MinimumReconnectTime</code> and <code>MaximumReconnectTime</code> .	Y
Timeout	60000 to 180000	If no events are received within this time limit, the link is assumed dead and will be closed. If this limit is less than the keep alive time then the link will be closed.	Y
WriteDelayTimeout	1000 to 60000	The maximum time to wait on a write if the link has dropped. If a realm disconnects when we are able to write to it, we wait for a set amount of time for the link to come back before abandoning the write and resetting altogether. This insulates the cluster against some transitive network conditions.	Y
JVM Management			
EmergencyThreshold	50 to 99	If the amount of memory used exceeds the <code>EmergencyThreshold</code> value, the connection is paused for a long duration (24 days). If the value of <code>EmergencyThreshold</code> is too large, the server may run out of memory. Default is 94, i.e. 94%.	

Configuration Group/Property	Valid values	Description	Adv.
EnableJMX	True or False	<p>Enable/disable JMX MBeans within the server. If enabled the server will present JMX MBeans so it can be monitored by any JMX client.</p> <p>Default is <code>false</code>.</p> <p>Note: This property activates or deactivates the JMX MBeans which are available from Universal Messaging v10.7 onwards. <code>EnableJMX</code> and <code>EnableLegacyJMX</code> can have the value <code>true</code> at the same time, meaning that Universal Messaging will activate JMX beans for the old and new versions in the same session.</p>	
EnableLegacyJMX	True or False	<p>Enable/disable JMX MBeans within the server. If enabled the server will present JMX MBeans so it can be monitored by any JMX client. Default is <code>false</code>.</p> <p>Default is <code>false</code>.</p> <p>Note: This property activates or deactivates the JMX MBeans which were available up to and including Universal Messaging v10.5. <code>EnableJMX</code> and <code>EnableLegacyJMX</code> can have the value <code>true</code> at the same time, meaning that Universal Messaging will activate JMX beans for the old and new versions in the same session.</p>	
ExitOnDiskIOError	True or False	If <code>true</code> , the server will exit if it gets an I/O Exception. Setting this to <code>false</code> may result in lost events if the server runs out of disk space. Default is <code>true</code>	Y
ExitOnInterfaceFailure	True or False	If <code>true</code> and for any reason an interface cannot be started when the realm initializes, the realm will shut down.	Y

Configuration Group/Property	Valid values	Description	Adv.
FlatStoreJMXBeanNamespace	True or False	Defines whether JMX topics and queues have flat namespaces. Default is <code>false</code> . If you set the property to <code>true</code> , a JMX queue namespace, for example, will have the format <code>destinationName=/q1/q2/q3</code> .	
IORetryCount	2 to 100	Number of times a file I/O operation will be attempted before aborting	Y
IOSleepTime	100 to 60000	Time between disk I/O operations if an I/O operation fails. If this time is large then the server may become unresponsive for this time.	Y
JMXRMIPort	0 to No Max	The port number to be used for JMX RMI connections. Set the property to a valid, not bound port number. Changes will take effect immediately and no server restart is required. If the port is not available for some reason, the realm server will go through the next 10 consecutive ports and will book the first free port. In order to disable the RMI, set the property to <code>0</code> .	
JMXRMIServerURLString	String	Describes the URL at which you can remotely connect to the Bean Server. Its default value is <code>Not Bound</code> . The field is read-only.	
MemoryMonitoring	60 to 30000	Number of milliseconds between monitoring memory usage on the realm. If this value is too large then the realm will be slow to handle memory usage. Default is <code>2000</code> .	
WarningThreshold	40 to 95	The memory threshold when the server starts to scan for objects to release. If this value is small then the server will release objects too soon, resulting in a lower performing realm. Default is <code>85</code> , i.e. <code>85%</code> .	
Join Config			

Configuration Group/Property	Valid values	Description	Adv.
ActiveThreadPoolSize	1 to No Max	The number of threads to be assigned for the join recovery. Default is 2.	
IdleThreadPoolSize	1 to 2147483647	The number of threads to manage the idle and reconnection to remote servers. This number should be kept small. Default is 1.	
MaxEventsPerSchedule	1 to 2147483647	Number of events that will be sent to the remote server in one run. A low number will increase the time to recover the remote server, a large number will impact other joins which are also in recovery. Default is 50.	Y
MaxQueueSizeToUse	1 to 2147483647	The maximum events that will be queued on behalf of the remote server. A low number increases the time for the remote server to recover, a large number increases the memory used for this server. Default is 100.	Y
RemoteJoinAckBatchSize		Events received through remote joins are acknowledged in batches. This property configures the batch size.	Y
RemoteJoinAckInterval		In addition to the batch acknowledgment, remote join events get acknowledged every n milliseconds. This property configures this interval.	Y
UseQueuedLocalJoinHandler	True or False	Specifies whether to use a queued join event handler. true will enable source channels and destination channels to be process events independently.	Y
Logging Config			
DefaultLogSize	100 to 2147483647	The default size of the log in bytes. Note: This property does not apply for Log4j2.	
DisplayCurrentThread	True or False	If enabled, the log shows the current thread in the log message.	

Configuration Group/Property	Valid values	Description	Adv.
		Default: true	
EnableLog4J	True or False	If enabled, Universal Messaging will intercept log messages and pass to Log4J as well. Restart the server for this configuration to take effect.	
EmbedTag	True or False	Used to control if the message tag is displayed in log messages. Default: false	
EnableStatusLog	True or False	If true, periodic logging of the Universal Messaging server status is activated. The messages will be logged at time intervals given by the StatusBroadcast configuration property described in the <i>Global Values</i> section. The default is true.	
fLoggerLevel	0 to 6	Use only for the fLogger framework or when LogLevelOverride is set to true for Log4j2. The server logging level, between 0 and 6, with 0 indicating very verbose, and 6 indicating very quiet. The more logging requested, the more overhead on the server. Default is 4. When you configure Universal Messaging to use Log4j2 as the logging framework, this property sets the log level only for the Universal Messaging server loggers (com.pcbssystem.foundation, com.pcbssystem.nirvana.base, com.pcbssystem.nirvana.server, com.pcbssystem.nirvana.server.handler, com.pcbssystem.nirvana.server.plugins, com.pcbssystem.nirvana.server.plugins.protocols, com.pcbssystem.foundation.security.login). The property does not set the log level for any other loggers defined in the log4j2.xml configuration file.	

Configuration Group/Property	Valid values	Description	Adv.
		Only the log messages from the internal logger are forwarded to the Universal Messaging administrator connections.	
LogLevelOverride	True or False	Use only for the Log4j2 framework. If set to <code>true</code> , you can configure the <code>fLogLevel</code> property. <code>false</code> restores the configuration from <code>log4j2.xml</code> and makes <code>fLogLevel</code> ineffective in the Enterprise Manager. The default is <code>true</code> .	
LogManager	0 to 2	The Log manager to use. 0 = ROLLING_OLD, 1 = ROLLING_DATE, 2 = ROLLING_NUMBER Default: ROLLING_DATE Note: This property does not apply for Log4j2.	
RolledLogFileDepth	0 to 2147483647	The number of log files to keep on disk when using log rolling. Oldest log files will be deleted when new files are created. Note: This property does not apply for Log4j2.	
Note: For further information about using the log file, see “The Enterprise Manager Logs Panel” on page 21.			
Metric Config			
EnableEventMemoryMonitoring	True or False	If this is set to <code>true</code> , the server will make available memory usage.	

Configuration Group/Property	Valid values	Description	Adv.
EnableMetrics	True or False	If this is set to <code>true</code> , the server will make available system metrics (e.g. memory usage).	
Plugin Config			
EnableAccessLog	True or False	Defines if plugin access log is produced	
EnableErrorLog	True or False	Defines if plugin error log is produced	
EnablePluginLog	True or False	Defines if plugin status log is produced	
MaxNumberOfPluginThreads	10 to 10000	Maximum number of threads to allocate to the plugin manager	Y
PluginTimeout	1000 to 30000	Time in milliseconds that the plugin will read from a client. If too small, the plugin may not load all of the clients requests	Y
Protobuf Config			
CacheEventFilter	True or False	Hold the Protocol Buffer filter cache in memory. Default <code>true</code> .	Y
Protocol AMQP Config			
AnonymousUser	String	The user name to use for anonymous users	
BufferSize	1000 to 60000	The size of the buffer that will be used to read/write on the AMQP connection	
DefaultNodeMode	0 to 1	The type of node if it is not able to detect it. 0=Queue, 1=Topic	
Enable	0 to No Max	If <code>true</code> the server will accept incoming AMQP connections	
EnableWriteThread	True or False	Enables the off loading of the physical write to a thread pool	Y

Configuration Group/Property	Valid values	Description	Adv.
EngineLoopCount	4 to 100	How many times the AMQP state engine will cycle per thread pool allocation	Y
MaxFrameSize	10000 to 2147483647	Maximum size of an AMQP frame	Y
MaxThreadPoolSize	2 to 100	Largest number of threads the pool can have.	
MinThreadPoolSize	1 to 10	Smallest number of threads for the dedicated AMQP thread pool	
QueuePrefix	String	The address prefix for specifying topic nodes as required by some clients	
SASL_Anonymous	True or False	Enable Anonymous SASL	
SASL_CRAM-MD5	True or False	Enable CRAM-MD5 SASL	
SASL_DIGEST-MD5	True or False	Enable DIGEST-MD5 SASL	
SASL_Plain	True or False	Enable Plain SASL	
SubscriberCredit	100 to 2147483647	Sets the subscriber (receiver) credit	
Timeout	10000 to 300000	Sets the network timeout	Y
TopicPrefix	String	The address prefix for specifying topic nodes as required by some clients	
TransformToUse	0 to 3	Selects the type of transformation to use from AMQP style events to native UM events. 0 - No transformation, 1 - Basic Transformation, 2 - Complete Transformation, 3 - User Configurable	
Protocol MQTT Config			

Configuration Group/Property	Valid values	Description	Adv.
AutoCreatedStoreSpindleSize	0 to 100 000	Sets the spindle size for automatically created MQTT stores. The default value is 50000.	
DisconnectClientsOnPublishFailure	True or False	Defines whether the server should disconnect clients to inform them that publishing has failed. The default is true.	
Enable	True or False	If true, the server will accept incoming MQTT connections. The default is true if this feature is enabled in the product licence.	
EnableAutoCreateTopics	True or False	If true, the server will auto-generate Topics for MQTT clients for subscriptions and publishing. The default is true. Note: This property is only applicable for client IDs with no wildcard.	
EnforceAlphaNumericClientID	True or False	If true, the Client ID must consist solely of alphanumeric characters. The default is false. Note: This property is only applicable for MQTT 3.1.1.	Y
IgnoreClientIDLength	True or False	If true, ignore the standard Client ID maximum length check of 23 characters. The default is true. Note: This property is only applicable for MQTT 3.1.1.	Y
MaxOutstanding	100 to 64000	Sets the maximum number of events that the server will send before waiting for the client to acknowledge them (QoS:1 and above). The default is 64000.	
QoS0AsTransient	True or False	If true, the server will not recover publish events with QoS greater than or equal to 0. The default is false.	Y

Configuration Group/Property	Valid values	Description	Adv.
		Note: This property is only applicable for MQTT 3.1.1.	
SessionStateTTL	0 to No Max	The number of milliseconds the state of a Client ID is kept between connections. The default value is set to 3 days. Setting this value to 0 will store the Client ID state until a clean session is received.	Y
SupportZeroLength	True or False	If true, the server will auto-generate the Client ID if it has zero length. The default is true. Note: This property is only applicable for MQTT 3.1.1.	Y
Strict	True or False	To be compliant with MQTT, stores must use the JMS Engine. This flag enforces this check. The default is true.	Y
RecoveryDaemon			
EventsPerBlock	1 to 2147483647	The number of events to send in one block to a recovering connection. Small values may slow down the overall speed of recovery, however large values may saturate the recovery thread and keep it busy from performing recovery tasks for other stores and connections.	Y
ThreadPool	1 to 2147483647	Number of threads to use for client recovery	
Server Protection			
DiskScanEnable	True or False	Enables the disk free space scan, using values defined by <code>DiskUsageFreeThreshold</code> and <code>DiskUsageScanInterval</code> . Default is true.	Y

Configuration Group/Property	Valid values	Description	Adv.
		<p>The scan checks whether there is sufficient free disk space for the Universal Messaging server to continue normal processing. If the disk space available is less than the <code>DiskUsageFreeThreshold</code> value, the server logs an error message. The server will initiate a clean shutdown with an appropriate error message if the disk space available is less than 500 MB.</p> <p>Note: If the server startup parameter <code>DISK_USAGE_SCAN_ENABLE</code> is set to <code>true</code> or <code>false</code>, the setting of <code>DiskScanEnable</code> is ignored. If <code>DISK_USAGE_SCAN_ENABLE</code> is undefined (i.e. set to neither <code>true</code> nor <code>false</code>), the setting of <code>DiskScanEnable</code> is used.</p> <p>See the section <i>Server Parameters</i> in the <i>Concepts</i> guide for information on <code>DISK_USAGE_SCAN_ENABLE</code>.</p>	
DiskUsageFreeThreshold	1 to 50	<p>Specifies the minimum percentage amount of free disk space required for the realm server to continue processing. When the percentage of free disk space drops below this value, the server will shut down. Default is 5.</p> <p>Note: This property is only activated in the following circumstances:</p> <ul style="list-style-type: none"> ■ if <code>DISK_USAGE_SCAN_ENABLE</code> is set to <code>true</code>, or ■ if <code>DISK_USAGE_SCAN_ENABLE</code> is undefined (i.e. set to neither <code>true</code> nor <code>false</code>) and <code>DiskScanEnable</code> is set to <code>true</code>. <p>See the description of <code>DiskScanEnable</code> for further information on <code>DISK_USAGE_SCAN_ENABLE</code>.</p>	Y

Configuration Group/Property	Valid values	Description	Adv.
DiskUsageScanInterval	1000 to 600000	The interval in milliseconds between one disk usage scan and the next disk usage scan. Default is 1000. Note: This property is only activated if the same circumstances apply as for DiskUsageFreeThreshold.	Y
EnableFlowControl	True or False	Enables flow control of producer connections. Default is false. See the section <i>Out-of-Memory Protection</i> in the <i>Concepts guide</i> for further details.	
FlowControlWaitTimeOne	1000 to 120000	The time in milliseconds to hold a producing connection before processing its events. This is the first level of waiting and the shortest wait time. Default is 2000. Only activated if EnableFlowControl is set to true.	Y
FlowControlWaitTimeTwo	1000 to 120000	The time in milliseconds to hold a producing connection before processing its events. This is the second level of waiting. Default is 4000. Only activated if EnableFlowControl is set to true.	Y
FlowControlWaitTimeThree	1000 to 120000	The time in milliseconds to hold a producing connection before processing its events. This is the third level of waiting and the longest wait time. Default is 10000. Only activated if EnableFlowControl is set to true.	Y
Thread Pool Config			
CommonPoolThreadSize	5 to 1000	Maximum number of threads to allocate to the common thread pool.	
ConnectionThreadPoolMaxSize	10 to 2147483647	The maximum number of threads allocated to establish client connections. If this number is too small then connections may be left waiting for a thread to process it.	

Configuration Group/Property	Valid values	Description	Adv.
ConnectionThreadPoolMinSize	4 to 100	The minimum number of threads allocated to establish client connections. If too large then the server will have many idle threads.	
ConnectionThreadWaitTime	10000 to 300000	The time for the thread to wait for the client to finalize the connection. If too low then slow linked clients may not be able to establish a connection.	Y
EnableConnectionThreadPooling	True or False	If true then if NIO is available it will be available for interfaces to use it and then all reads/writes will be done via the Read/Write thread pools. If NIO is not available then a limited used write thread pool is used. This requires a realm restart before it takes effect.	Y
MultiplexReadThreadPoolMaxSize	4 to 2147483647	The maximum number of threads to allocate to the multiplex thread pool to read multiplex sessions. Default is 100.	
MultiplexReadThreadPoolMinSize	4 to 2147483647	The minimum number of threads to allocate to the multiplex thread pool to read multiplex sessions. Default is 4.	
MaxUnauthorisedCount	10 to 10000	The maximum outstanding unauthorized connections per host name (or IP address if host name is unavailable). Default is 1000.	Y
PendingTaskWarningThreshold	100 to 100000	The threshold at which the server starts to warn about the number of pending tasks. When the number of pending tasks is below the threshold, but over 100, the server logs a WARNING message. When the number is above the threshold, the server logs an ERROR message. When the server does not find available threads, it logs a message that the thread pool is exhausted. Default is 1000.	Y
ReadThreadPoolMaxSize	4 to 2147483647	The maximum number of threads that will be allocated to the read pool. If NIO is not available this should be set to the maximum number of clients that	

Configuration Group/Property	Valid values	Description	Adv.
		are expected to connect. If NIO is available then it's best to keep this number under 20.	
ReadThreadPoolMinSize	4 to 2147483647	This is the number of threads that will always be present in the read thread pool. If this is too small then the thread pool will be requesting new threads from the idle queue more often. If too large then the server will have many idle threads.	
SchedulerPoolSize	10 to 100	The number of threads assigned to the scheduler, default is 10.	
SlowTaskWarningTime	1000 to 30000	The time in milliseconds before reporting a slow-running task. The server logs the information at the WARNING log level and generates a thread dump. Default is 5000.	Y
StalledTasksWarningTime	10000 to 60000	The time in milliseconds before reporting a stalled task. The system writes the information at the WARNING log level and generates a thread dump. When you change this configuration, the thread pool monitor interval is updated to monitor at the same time interval as the value you specify for this property. Default is 60000.	Y
ThreadDumpInterval	1000 to 600000	The interval in milliseconds at which a thread dump is generated when the system reports slow or stalled tasks, or when the number of pending tasks exceeds the value of PendingTaskWarningThreshold. The thread dump interval applies across all thread pools in the JVM instance. Default is 60000.	Y
ThreadDumpOnSlowTask	True or False	Whether to generate a thread dump when the system reports a slow task. Default is false.	Y

Configuration Group/Property	Valid values	Description	Adv.
ThreadIdleQueueSize	5 to 50	When threads are released from various pools since they no longer need them they end up in the idle queue. If this idle queue exceeds this number the threads are destroyed. Specify this number to be large enough to accommodate enough idle threads, so that if any thread pool requires to expand then it can be reused. If the number is too large then the server may have many idle threads.	
WriteThreadPoolMaxSize	5 to 2147483647	The maximum number of threads that will be allocated to the write pool. If NIO is not available this should be set to the maximum number of clients that are expected to connect. If NIO is available then it's best to keep this number under 20.	
WriteThreadPoolMinSize	5 to 2147483647	This is the number of threads that will always be present in the write thread pool. If this is too small then the thread pool will be requesting new threads from the idle queue more often. If too large then the server may have many idle threads.	
Trace Logging Config			
TraceStoreLogLevel	OFF, INFO or TRACE	If you set the event tracing log level of a store to INFO, the system logs high-level event operations. If you set the level to TRACE, the system logs a verbose event trace.	
TraceStores		A comma-separated list of stores for which to enable event trace logging. Set '*' to trace all stores or '*!a' to trace all stores except a specific one (a). You can also trace all stores in a specific folder - 'wm/Group/' or just a single store - 'a'	
TraceStoreLogSize	1 to 100	Specifies the size of a single trace log file for a store in MB.	

Configuration Group/Property	Valid values	Description	Adv.
TraceFolderLogSize	1024 to 102400	Specifies the size of the directory that contains the trace log files for the store in MB.	
TransactionManager			
MaxEventsPerTransaction	0 to 2147483647	The maximum number of events per transaction, a 0 indicates no limit.	
MaxTransactionTime	1000 to No Max	Time in milliseconds that a transaction will be kept active. A large number will cause the server to retain these transactions in memory.	
TTLThreshold	1000 to 60000	The minimum time in milliseconds, below which the server will not store the Transaction ID.	Y

Double-clicking on the property you wish to modify in the configuration group will provide you with a dialog window where the new value can be entered. The values of configuration properties will be validated to check whether they are within the correct range of values. If you enter an incorrect value you will be notified.

Connecting to Multiple Realms

An Enterprise Manager can connect to multiple Universal Messaging realms at the same time. These realms can be standalone or clustered, so developers and administrators can now manage and monitor the whole Universal Messaging enterprise infrastructure from a single instance of the Enterprise Manager. After you connect to a set of Universal Messaging realms, you can save the connection information, so that the Enterprise Manager automatically connects to all those realms each time it starts.

A bootstrap RNAME environment variable is needed the first time you run the Enterprise Manager or if your connection info file is empty. If you use the shortcut / link created by the installation process, this will be automatically set to point to the locally installed realm's bootstrap interface, so you do not need to take any additional action. If, however, you open a client command prompt and you want to initially connect to a realm other than the local one, you must change your RNAME environment variable.

For more information about how to set the RNAME variable, see the section *Communication Protocols and RNAMEs* in the Developer Guide.

Note that after your realm connection information is saved, the RNAME environment variable is ignored.

To connect to a realm server in the Enterprise Manager:

1. Select **Connections > Connect To Realm**.
2. In the **RNAME** field of the Connect to a realm dialog box, specify the RNAME that points to the interface of the Universal Messaging realm to which you want to connect. Click **OK**.

If the connection is successful, a new realm node is rendered on the tree with the unique name of that realm. You can manage and monitor the new realm by selecting the newly rendered tree node. The name displayed for the realm uses the syntax: `realmname(host:port)`, for example `realm1(MyHost:11010)`.

When you connect to a realm server that is part of a cluster or zone, the Enterprise Manager automatically connects to and displays the other realms in the cluster or zone.

If you enter an incorrect RNAME, if the realm to which you want to connect is not running, or if the realm is running but the particular interface is not started, the connection will fail.

To make this connection get attempted each time you start the Enterprise Manager, you must save your connection information.

Disconnecting from Realms

When the Enterprise Manager connects to multiple realms, its startup time increases slightly each time you add a Universal Messaging realm to your connection list. If you connect from a different location or network, if the development phase of a Universal Messaging application completes, or if you want to have faster startup times for the Enterprise Manager, you may want to stop connecting to one or more of your Universal Messaging realms.

To disconnect from a realm in the Enterprise Manager:

1. Select **Connections > Disconnect from Realm**.
2. In the Disconnect From Realm dialog box, select the realm from which you want to disconnect and click **OK**.

The disconnected realm node and any other realm nodes that were added by it when the node was created disappear from the namespace tree.

Disconnecting from a realm is not necessarily a permanent operation. If you disconnect from a realm that was listed in your connection information, the disconnect is applicable only for this Enterprise Manager session. Next time you start up, the connection will be attempted again. To make the disconnect permanent, click **File > Save** to save your connection information after you disconnect.

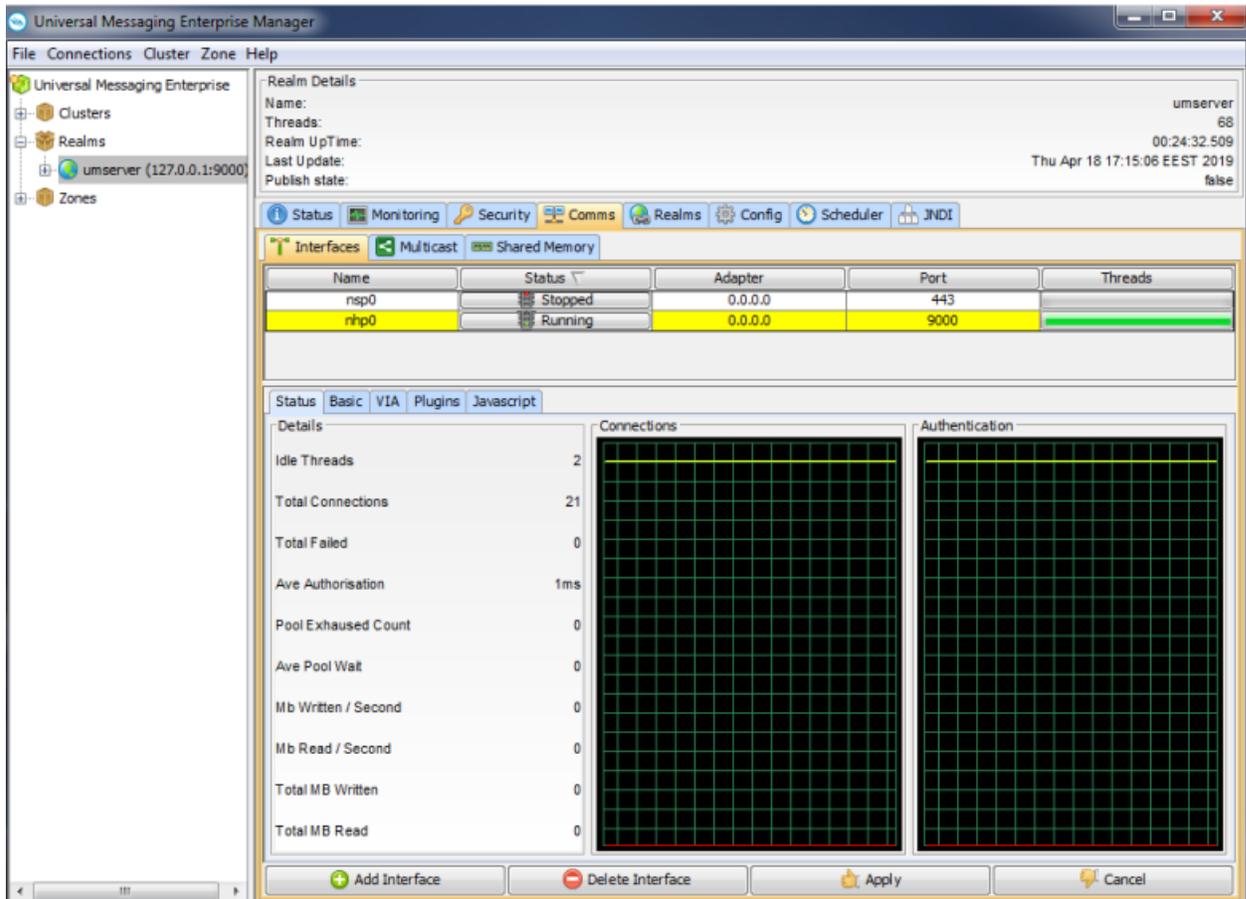
Interface Status

Universal Messaging interfaces (see [“Administering TCP Interfaces, IP Multicast, and Shared Memory” on page 136](#)) enables you to connect to a realm using various protocols and ports on specific physical network interfaces on the host machine. Interfaces are also available through the

Universal Messaging Administration API and can provide useful status information regarding user connections.

The Enterprise Manager provides a summary of this status information for each interface.

To view status information for an interface, select the **Comms** tab for the realm you want to view. Then click the **Interfaces** tab and select the interface from the list of interfaces. The following image shows the Status panel for a selected interface.



Details Panel

The interface status panel has a section that describes the details of the interface status information. The status information contains the following parameters:

- **Idle Threads**- The number of idle threads, calculated as the total threads from the interface accept threads pool - the number of threads from the pool currently accepting connections. Corresponds to available threads
- **Total Connections** - The total number of successful connections made to this interface
- **Total Failed** - The total number of failed connection attempts made to this interface
- **Ave Authorisation** - The average time it takes a connection to authenticate with the realm server

- **Pool Exhausted Count** - The number of times that the interface thread pool has had no threads left to service incoming connection requests. When this count increases, you should increase the number of accept threads (see [“Basic Attributes for an Interface”](#) on page 139) for the interface
- **Ave Pool Wait** - The average time that a client connection has to wait for the accept thread pool to provide an available thread. Like the Pool Exhausted count, this is a good indicator that the number of accept threads for an interface is too low and needs to be increased

The status panel also shows two graphs that depict connection attempts (successful connections are shown in yellow, failed connection attempts are shown in red) and authentication times (average authentication times are shown in yellow, and the last authentication time is shown in red).

Zone Administration

Overview of Zone Administration

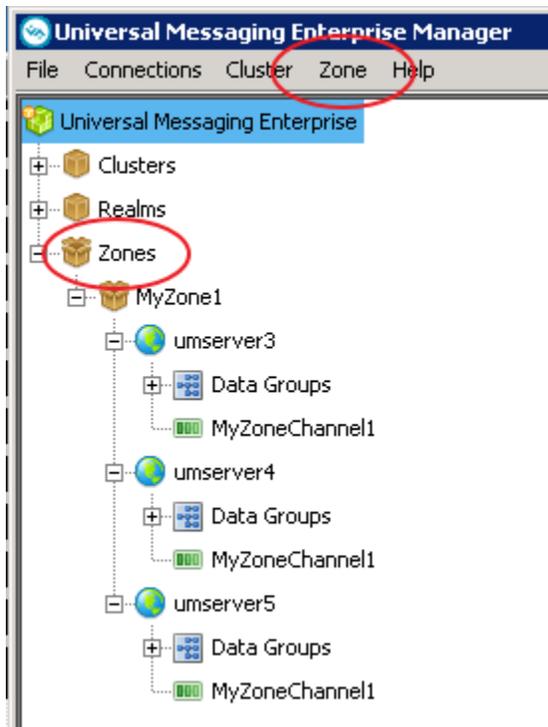
The Enterprise Manager provides menu items for performing the administrative functions on zones. In a zone, messages that are published to a channel on one realm are automatically forwarded to a channel of the same name on other realms in the zone.

Note:

Messages on queues are not forwarded between realms in a zone; the zone functionality applies only to channels.

For general information about using zones, refer to the *Architecture* section of the *Universal Messaging Concepts* guide.

Zone administrative functionality is offered in the Enterprise Manager menu bar and in the navigation tree:



The **Zone** tab in the menu bar allows you to perform operations on zones, such as creating and deleting zones.

The **Zones** node in the navigation tree is the parent node of any zones you create.

The zone administration operations that you can perform are described in the following sections.

Creating a Zone

To create a zone and define it with an initial set of realms or clusters, proceed as follows:

1. Open the dialog for creating a zone.

You can do this in one of the following ways:

- In the Menu bar, select **Zone > Create Zone**, or
- In the navigation tree, select the Zones node, and from the context menu choose **Create Zone**.

2. In the dialog, specify a name that will be assigned to the zone.
3. Add realms or clusters to the zone.

If you select the radio button for realms, you see all of the realms that you can add to the zone. If you select the radio button for clusters, you see all of the clusters that you can add to the zone.

Specify the realms or clusters you want to add to the zone, then click **Add**.

4. Click **OK** to create the zone and close the dialog.

The newly created zone is now displayed under the **Zones** node in the navigation tree.

If you expand the node of the new zone, you will see the realms that belong to the zone.

Note:

1. A zone can contain either realms or clusters, but not a mixture of realms and clusters.
2. A zone cannot be empty; it must contain at least one realm or cluster.

Modifying the set of realms or clusters in a zone

To modify the set of realms or clusters in a zone, proceed as follows:

1. Under the **Zones** node in the navigation tree, select the node representing the required zone. In the context menu, select **Modify Zone Members**.

This displays the realms/clusters that are currently members of the zone, and also the realms/clusters that are currently not members but which are available to become members.

2. As required, add realms/clusters to the zone's existing members, or remove existing members.
3. Click **OK** to save the modified zone and close the dialog.

Deleting a zone

To delete a zone, proceed as follows:

1. Select the **Zones** node in the navigation tree, then in the context menu, select **Delete Zone**.

Alternatively, select **Zone > Delete Zone** from the menu bar.

2. Select the required zone from the displayed list and click **OK** to delete the zone.

Creating a channel in a zone

You can create a channel for a zone, and the channel will be automatically created on all realms/clusters in the zone.

To create a channel in a zone, proceed as follows:

1. Select the node for the zone in the navigation pane. Then, in the context menu of the node, select **Create Channel**.
2. In the **Add Channel** dialog, specify the attributes of the channel that you wish to create.
3. Click **OK** to complete the dialog and create the channel.

The Enterprise Manager now creates the channel on all realms or channels in the zone.

Modifying a channel in a zone

If you wish to modify the attributes of a channel that was created in a zone via **Create Channel**, you must modify the attributes for the channel in each of the zone members (realms, clusters) individually.

Note:

Any changes you make to the channel definition for a realm/cluster in a zone are NOT propagated automatically to the other zone members. If you wish to keep all zone members in sync, you have to update the other zone members individually.

To modify a channel on one realm/cluster in a zone, proceed as follows:

1. Select the node for the channel under the node for the realm/cluster on which the channel is defined.
2. In the context menu of the channel, select **Edit Channel**.
3. In the **Modify Channel** dialog, make your changes and click **OK** to complete the dialog.

Channel interface attributes for use in zones

For the message forwarding mechanism between realms in a zone, Universal Messaging requires each affected realm to use an interface that has the attribute **Allow for InterRealm** activated. See the section [“Basic Attributes for an Interface” on page 139](#) for a description of this attribute.

General notes on using zones

This section summarizes some operational aspects of using zones.

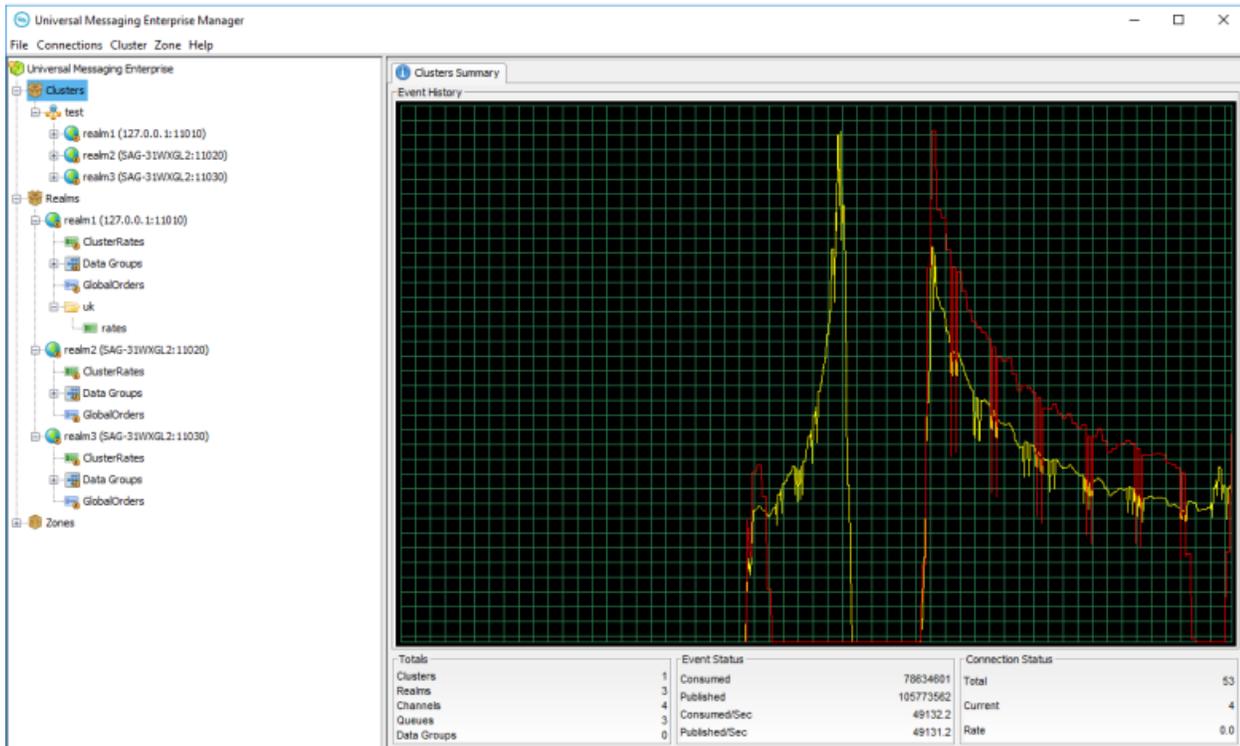
- If a zone member (a realm or cluster) is not active (e.g. the server is down), no Enterprise Manager operations will be allowed on the zone until all zone members are available again.
- Any given realm or cluster cannot be a member of more than one zone at the same time.

Cluster Administration

Viewing the Available Clusters

When you select the **Clusters** node in the Enterprise Manager, the Clusters Summary view displays details about the current status of all Universal Messaging clusters and clustered realms known to the Enterprise Manager.

If you use the Enterprise Manager to connect to a realm that is a member of an existing cluster, the cluster is automatically displayed in the **Clusters** node. When a cluster node is found, the Enterprise Manager also automatically connects to all the cluster member realms. For more information, see [“Connecting to Multiple Realms” on page 75](#).



The top of the screen displays a real-time graph illustrating the total number of events published (yellow) and consumed (red) across all Universal Messaging clusters.

The bottom of the screen displays the Totals, Event Status, and Connection Status panels.

Totals

The Totals panel contains the following information:

- **Clusters**- The number of clusters defined in the Enterprise Manager and its realm nodes
- **Realms**- The number of realms known by the enterprise manager
- **Channels**- The number of channels that exist across all known realms
- **Queues**- The number of queues that exist across all known realms
- **Data Groups**- The number of data groups that exist across all known realms

Event Status

The Event Status contains the following information:

- **Published** - The total number of events published to all channels and queues across all realms in all known clusters
- **Consumed** - The total number of events consumed from all channels and queues across all realms in all known clusters

- **Published/Sec** - The number of events published to all channels and queues per second across all realms in all known clusters
- **Consumed/Sec** - The number of events consumed from all channels and queues per second across all realms in all known clusters

Connection Status

The Connection Status panel contains the following information:

- **Total** - The total number of connections made to all realms in all known clusters
- **Current** - The current number of connections across all realms in all known clusters
- **Rate** - The number of connections being made per second across all realms in all known clusters

Viewing Information for a Cluster

You can view information for an individual cluster by expanding the **Clusters** node in the navigation pane and selecting the node for the required cluster. The view displays information about the cluster members and the current status of the selected cluster.

The screenshot displays the Universal Messaging Enterprise Manager interface. The left navigation pane shows a tree view with 'Clusters' expanded to 'test', which contains three realms: realm1 (127.0.0.1:11010), realm2 (SAG-31WXGL2:11020), and realm3 (SAG-31WXGL2:11030). The main panel shows the 'Cluster Summary' view for the 'test' cluster.

Cluster Members

Name	State	Master	realm1	realm2	realm3
realm1	Slave	realm2	Local	OnLine	OnLine
realm2	Master	realm2	OnLine	Local	OnLine
realm3	Slave	realm2	OnLine	OnLine	Local

Cluster Status

Server	Process Queue	Client Queue	Comms Queue	Broadcast Time	Response Time
realm3	248	0	0	0	0
realm2	451	0	0	0	0
realm1	147	270557	0	0	0

Event History

The graph shows two lines: a yellow line representing 'Published' events and a red line representing 'Consumed' events. The x-axis represents time, and the y-axis represents the number of events. The published events generally exceed the consumed events, indicating a backlog.

Totals

Totals	Event Status	Connection Status
Realms	Consumed	Total
Channels	Published	Current
Queues	Consumed/Sec	Rate
	Published/Sec	

Values from the screenshot:

- Realms: 3
- Channels: 4
- Queues: 3
- Consumed: 81895216
- Published: 120649731
- Consumed/Sec: 0.0
- Published/Sec: 114527.2
- Total: 55
- Current: 3
- Rate: 0.0

The top of the view shows the realms that have been defined for the cluster.

The view includes a real-time graph illustrating the total number of events published (yellow) and consumed (red) across all realms in the cluster.

The bottom of the screen displays the Totals, Event Status, and Connection Status panels.

Totals

The Totals panel describes the following:

- **Realms**- The number of realms in the cluster
- **Channels**- The number of channels across all realms in the cluster
- **Queues**- The number of queues across all realms in the cluster

Event Status

The Event Status panel describes the following:

- **Published** - The total number of events published to all channels and queues across all realms in the cluster
- **Consumed** - The total number of events consumed from all channels and queues in the cluster
- **Published/Sec** - The number of events published to all channels and queues per second across all realms in the cluster
- **Consumed/Sec** - The number of events consumed from all channels and queues per second across all realms in the cluster

Connection Status

The Connection Status panel describes the following:

- **Total** - The total number of connections made to all realms in the cluster
- **Current** - The current number of connections across all realms in the cluster
- **Rate** - The number of connections being made per second across all realms in the cluster

In addition, you can view information about the cluster on the following tabs:

- **Cluster Summary** - Provides an overview of all realms in the cluster. It identifies the current master realm and also shows each realm's perception of the state of all other realms.
- **Connections** - Shows all connections to realms in the cluster.
- **Remote Cluster Connections** - Shows all remote cluster connections for this cluster. Clusters can be remotely connected together, thus providing the ability to create joins between channels in different clusters.
- **Logfile** - Shows a real-time cluster-specific log and provides the option to stream the log output to a file.
- **Sites** - Shows any site configurations for the cluster. For more information about clusters with sites, see [“Creating Clusters with Sites” on page 92](#).

Creating Clusters

Tip:

As the underlying purpose of a cluster is to provide resilience and high availability, we advise against running all the servers in a cluster on a single physical or virtual machine in a production environment.

Before Creating a Cluster

Before you create a cluster, the Enterprise Manager must connect to the realms that will form the cluster. For information about how to connect to realms, see [“Connecting to Multiple Realms” on page 75](#).

If you cannot connect to a realm or you receive a 'Security Alert' message when you click the realm node, you should check if the realm is running, and check the permissions on the realm. If the realms to which you want to connect are running on different machines, you must ensure that all realm machines are given full permissions to connect to the other realms in the cluster. Each realm communicates with the other cluster realms by using its own connection. For more information about realm permissions, see [“About Realm ACL Permissions” on page 126](#).

For example, assume that there are three realms that will form a cluster, and the subject of each connection has the format: `realm-<realmname>@<ip_address>`. Each realm subject must exist in the ACLs of the other realms, so the following realm subjects must be added to the ACL for each realm:

```
realm-realm1@10.140.1.1 realm-realm2@10.140.1.2 realm-realm3@10.140.1.3
```

The permissions given for each realm must be 'Access Realm'. Also, each realm must have a valid entry for the `user@host` that corresponds to the user that will create the cluster using the Enterprise Manager. The permissions for this user must be sufficient in order to create the cluster object. Temporarily, it is often better to give 'Full' privileges to the `*@*` default subject in order to facilitate setting up a realm and clusters.

Creating a Cluster

When you create a cluster, you must either migrate or delete all local stores on any of the realms participating in the cluster.

➤ To create a cluster in the Enterprise Manager

1. Right-click the **Clusters** node and select **Create Cluster**.
2. In the Create New Cluster dialog box, specify a name for the new cluster.

Important:

The Enterprise Manager does not support working with two clusters that have the same name.

3. Add cluster members by selecting realms from the **Available Realms** list. Click **OK**.

Important:

A cluster cannot contain two realm nodes with the same node name, even if their host names and port numbers are different.

One of the selected realms becomes the master realm during the creation of the cluster. The master realm controls synchronizing the state between the other realms and acts as the authoritative source for this information.

4. Select whether to migrate local stores to cluster-wide stores or delete the local stores.

Note:

If the name of a local store is the same as the name of an existing cluster store, the cluster creation will fail due to a name clash.

The Enterprise Manager displays the new cluster and its realms in the **Clusters** node tree. When you select the new cluster node, you can monitor its state on the **Cluster Summary** tab. The tab shows the state of all cluster members and which realm is the current master.

Deleting a Cluster

➤ To delete a cluster in the Enterprise Manager

1. Right-click the **Clusters** node and select **Delete Cluster**.
2. In the **Cluster** field, select the cluster node you want to delete. Click **OK**.
3. Choose whether to delete all existing cluster resources or convert them to local resources:

Migrating cluster stores to local stores will keep any data contained in the stores.

Adding and Removing Cluster Members

Consider the following information before adding or removing cluster members in the Enterprise Manager:

- Before adding a new realm to a cluster, you must connect to the realm. For more information about how to connect to a realm, see [“Connecting to Multiple Realms” on page 75](#).
- If the realm you want to add has local stores with names matching any store on the cluster, the realm will not be added to the cluster. This prevents naming clashes in the cluster.
- You can add and remove cluster members in the same operation.

➤ To modify a cluster in the Enterprise Manager

1. Expand the **Clusters** node.
2. Select the cluster you want to modify and right-click it.

3. Click **Modify Cluster Members**.
4. Do any of the following:
 - From the **Available Realms** list, select realms to add to the cluster. Click **OK**.

Any existing cluster resources are also created on the newly added realms.
 - From the **Cluster Members** list, select realms to remove from the cluster and click **OK**.

Then specify whether to delete all cluster-wide resources on the realms that you removed or whether to convert the cluster resources to local ones.

Converting the cluster resources to local ones keeps any data contained in the cluster resources.

Creating Cluster Channels

Each channel that is created in a cluster consists of a physical object within each Universal Messaging realm in the cluster as well as its logical reference in the namespace of each realm. You can obtain references to the cluster channels by using the Universal Messaging Client and Admin APIs, in the same way as when you have non-clustered channels. You can also monitor and manage cluster channels in the Enterprise Manager.

➤ To create a cluster channel

1. Expand the **Clusters** node.
2. Select a cluster and right-click it.
3. Click **Create Channel**.
4. Specify the channel attributes. For the values to specify, see
5. Click **OK**.

The channel is created on all realms in the cluster and you can see it in the namespace tree of each realm.

Creating Cluster Queues

Each queue that is created in a cluster consists of a physical object within each Universal Messaging realm in the cluster as well as its logical reference in the namespace of each realm. You can obtain references to the cluster queues by using the Universal Messaging Client and Admin APIs, in the same way as when you have non-clustered queues. You can also monitor and manage cluster queues in the Enterprise Manager.

➤ To create a cluster queue

1. Expand the **Clusters** node.
2. Select a cluster and right-click it.
3. Click **Create Queues**.
4. Specify the queue attributes. For the values to specify, see
5. Click **OK**.

The queue is created on all realms in the cluster and you can see it in the namespace tree of each realm.

Setting Up Inter-Realm Communication

Communication between realms can occur in various configurations:

- between realms in the same cluster.
- between realms in a zone.
- between realms in connected clusters.

The communication between realms can be secure (encrypted) or non-secure (non-encrypted). The communication is implemented by defining one or more *interfaces* on each realm. The required setup of the interfaces is the same, regardless of which of the above configurations you use for the communication between realms. For example, the attribute **Allow for InterRealm** must be activated on the interface that you use, otherwise the communication between realms is not possible.

The following description uses some examples from working with a cluster, but the principles apply to all configurations.

Since all realms in a cluster are required to have the same configuration (so that for example if the master realm goes offline, one of the other realms can become the new master), you must ensure that any interface definitions on one realm match the interface definitions on all other realms in the cluster.

For non-encrypted inter-realm communication, you can set up the interfaces to use either NSP (Socket Protocol) or NHP (HTTP Protocol). In general, we recommend you to use NSP rather than NHP for non-encrypted inter-realm communication.

For encrypted inter-realm communication, you can set up the interfaces to use either NSPS (Secure Socket Protocol) or NHPS (Secure HTTP Protocol). In general, we recommend you to use NSPS rather than NHPS for encrypted inter-realm communication.

Information about using the Enterprise Manager to manage a cluster is contained in the section *Cluster Administration*. Information about managing realm interfaces is contained in the section *TCP Interfaces, IP Multicast and Shared Memory*. Managing zones is described in the section *Zone Administration*. Setting up an inter-cluster connection is described in the section *Interconnecting Two Clusters*, and conceptual details are provided in the section *Data Routing using Channel Joins* in the Concepts Guide.

Setting Up Non-Encrypted Inter-Realm Communication

Each realm contains by default one predefined interface, and this interface uses the NSP protocol (i.e. socket protocol without encryption). Also by default, the interface is configured to be usable for inter-realm communication as well as for communication between realm and clients.

If you do not define any additional interfaces on the realm, all communication between the realm and other realms, and between the realm and clients, will use this interface. You can set up a cluster consisting of multiple realms, each of them having just this one default interface defined.

However, in general we recommend you to set up two NSP interfaces on each realm for non-encrypted communication, namely one interface for only inter-realm communication and one interface for only client communication to the realm. The options for setting up this configuration are available in the Enterprise Manager, under the **Comms > Interfaces > Basic** tab of each realm.

On the interface that you will use for inter-realm communication, use the following settings:

- **Allow for InterRealm:** yes
- **Allow Client Connections:** no

Similarly, on the interface that you will use for client communication with the realm, use the following settings:

- **Allow for InterRealm:** no
- **Allow Client Connections:** yes

After you make these changes, restart all of the realms, to ensure that the new interfaces are activated.

When you form the cluster, communication between realms in the cluster will use the NSP interface that you have configured for inter-realm communication.

Setting Up Encrypted Inter-Realm Communication

The assumed starting point in this scenario is that there is no cluster formed yet. All of the realms that will later form the cluster need to be configured.

The steps required are as follows:

1. If you intend to use self-signed certificates, or if you intend to use a custom truststore (which contains the public certificates associated with each Universal Messaging realm's private certificate), the keystore and the truststore must be added to the Universal Messaging JVM process.

In the file `Server_Common.conf` on each realm, provide details of the truststore and keystore, according to the following pattern:

```
wrapper.java.additional.7="-Djavax.net.ssl.trustStore=<TRUSTSTORE>
wrapper.java.additional.8=-Djavax.net.ssl.trustStorePassword=<TRUSTSTORE_PWD>
wrapper.java.additional.9="-Djavax.net.ssl.keyStore=<KEYSTORE>
wrapper.java.additional.10=-Djavax.net.ssl.keyStorePassword=<KEYSTORE_PWD>
```

for example

```
wrapper.java.additional.7="-Djavax.net.ssl.trustStore=
/webmethods/truststores/um_truststore.jks"
wrapper.java.additional.8=-Djavax.net.ssl.trustStorePassword=nirvana
wrapper.java.additional.9="-Djavax.net.ssl.keyStore=
/webmethods/keystores/um_keystore.jks"
wrapper.java.additional.10=-Djavax.net.ssl.keyStorePassword=nirvana
```

See the section *Server Parameters* in the *Concepts* guide for general information about setting up such parameters.

2. On each realm in the cluster, add two secure interfaces:
 - a. Add one interface using the NSPS protocol, to be used only for inter-realm communication.

Note:

The demo certificates generated by the Universal Messaging Certificate Generator tool (see the section [“How to Generate Certificates for Use” on page 146](#)) are only valid for the loopback interface (localhost / 127.0.0.1). Therefore, if you use these demo certificates, ensure that the adapter that you add is bound only on the loopback interface.

For this interface, set the following options (in the Enterprise Manager, they are located under the **Basic** or **Certificates** tabs of the interface definition screen):

- **Allow for InterRealm:** yes
- **Allow Client Connections:** no
- **Enable client certificate validation:** no

The reason for disabling client certificate validation is because Universal Messaging does a certificate exchange between realms already when constructing a cluster, so doing another certificate exchange at the SSL layer would be redundant.

- Specify Certificates and Truststore on the interface as you would normally.
- If you want to use a certain level of SSL / TLS (eg. TLS 1.2)
 1. Pick the right algorithms for that interface.
 2. Enforce the SSL level in the realm (using a JVM argument in `Server_Common.conf`). Example: to enforce TLS1.2 globally on the Universal Messaging server, set:

```
wrapper.java.additional.XX=-DSSLProtocols=TLSv1.2
```

- b. Add one more interface using the NSPS protocol, to be used only by clients for communication with the realm. For this interface, set the following options:

- **Allow for InterRealm:** no
- **Allow Client Connections:** yes
- **Enable client certificate validation:** no

3. Disable the setting for inter-realm communication on the original, non-encrypted, interface.
4. Close and restart the Enterprise Manager.
5. Restart all Universal Messaging realms (to make sure all JVM arguments are activated).
6. Use the Enterprise Manager to form the cluster.

Switching from Non-Encrypted to Encrypted Inter-Realm Communication

The assumed starting point in this scenario is that there is already a cluster in which the inter-realm communication is not encrypted, i.e. the interface protocol is NHP or NSP, and you want to change this to encrypted communication, i.e. using the interface protocol NHPS or NSPS.

Here are the steps to follow to switch from non-encrypted to encrypted inter-realm communication in a Universal Messaging cluster:

1. Close the cluster and stop any running realms.
2. In the file `Server_Common.conf` on each realm, provide details of the truststore and keystore, as described in [“Setting Up Encrypted Inter-Realm Communication” on page 89](#).
3. Restart all realms.
4. On each realm, create two NSPS interfaces, as described in the previous section.
5. Under the **Certificates** tab for each of the NSPS interfaces, add a reference to the custom truststore and the keystores containing the server signed certificates, for example:

```
Key store path : /webmethods/keystores/um_keystore.jks
Trust store path : /webmethods/truststores/um_truststore.jks
```

6. Close Enterprise Manager.
7. Set the environment variables `CAKEystore` and `CAKEystorePWD` for each realm to reference the truststore containing the CA root chain, and the truststore's password. You can set up these variables as follows:
 - a. Open the file `Admin_Tools_Common.conf` that is located in `UniversalMessaging/java/<instanceName>/bin`, where `<instanceName>` is the name of the realm server.
 - b. Locate the lines

```
set.default.CAKEystore=
set.default.CAKEystorePWD=
```
 - c. Set these variables to the required values, for example:

```
set.default.CAKEystore=/webmethods/keystores/um_keystore.jks
set.default.CAKEystorePWD=nirvana
```
 - d. If you choose not to enable client certificate validation, you must comment out the unused SSL keystore properties in the `nenterprisemgr.conf` file using a hash (#).

Note that if these variables have already been assigned a value elsewhere in the session, for example in a startup script, the values defined here in `Admin_Tools_Common.conf` will be ignored.

8. Restart Enterprise Manager.

By restarting the Enterprise Manager after setting values for `CAKEystore` and `CAKEystorepasswd`, the Enterprise Manager will be able to connect over a secured interface.

9. Disable the inter-realm connection option on each realm's non-encrypted interfaces.

10. Form the cluster.

Note on Public/Private Keys Used for Inter-Realm Handshake

When a Universal Messaging realm starts for the first time, it automatically generates a public/private key pair for encryption purposes and stores it in the internal keystore `server.jks` file in the realm's `data/RealmSpecific` directory. The public keys of other nodes are also added to this file whenever the realms are added to form a cluster.

These auto-generated keys are used for server identification only; basically whenever two realms establish a connection, they will exchange a single signed message as part of the handshake routine, in order to confirm they know each other.

After this initial handshake has taken place, all encrypted communication between realms in a cluster uses separate keys and keystores.

Interconnecting Two Clusters

Before you create a connection between two clusters, connect to a realm in each cluster so that both clusters are displayed in the Enterprise Manager

➤ To interconnect two clusters in the Enterprise Manager

1. Expand the **Clusters** node and select one of the clusters you want to connect.
2. Go to the **Remote Cluster Connections** tab and click **Add**.
3. In the **To Cluster** field, select the remote cluster to which you want to connect, and then click **OK**.

After the connection is established, you can create inter-cluster joins, either in the Enterprise Manager or programmatically.

Creating Clusters with Sites

A Universal Messaging cluster with sites can operate with as few as half of the active cluster members, compared with a required quorum of 51% for a cluster without sites. A cluster with sites includes two sites: a primary site and a backup site. The primary site gets allocated an additional vote to achieve the required cluster quorum of 51%. In a cluster with a production site

and a disaster recovery site, you can make either site the primary site, but we recommend that you make the production site the primary site.

For more information about clusters with sites and a discussion on whether to make the production site or the disaster recovery site the primary site, see *Clusters with Sites* in the *Concepts* guide..

Use the following procedure to create sites for an existing cluster in the Enterprise Manager and to select a primary site.

➤ To create sites for a cluster in the Enterprise Manager

1. Go to **Clusters > *cluster_name* > Sites**.
2. On the **Sites** tab, click **New**.
3. Specify a name for the site, and then select a realm to add to the site.

The site is displayed on the **Sites** tab. You can add other cluster realms to the site or remove realms, as required.

4. Repeat the previous two steps to create a second site.
5. In the **IsPrime** column, select the primary site.

Case Study: Migrating Between Single-Node and Multi-Node Active/Active Cluster

This case study examines the following scenarios:

- Migrating from a single node setup to a multi-node active/active cluster.
- Migrating from an active/active cluster to a single-node setup, also known as declustering.

Migrating from a single-node setup to a multi-node active/active setup requires manual steps. A "live" migration from a single node to a cluster is not currently supported. The migration procedure enables you to migrate all local resources to cluster-wide resources. If you choose not to migrate local resources, they are deleted.

The steps outlined below describe behaviors of realms and their local stores (channels and queues) before and after clustering and declustering.

Before you start, see the section [“Creating Clusters” on page 84](#) for general information about creating a cluster.

Preparation

1. Migrating from a single-node setup to a multi-node active/active requires various manual steps. Software AG recommends that you have proper downtime for this cluster setup and not migrate from a running node.

2. Stop all publishers, so that no new events arrive. Also ensure that all channels and queues are completely drained and no pending events exist by waiting until the subscribers consume all pending messages.

This step is needed because Universal Messaging does not support live migration. By stopping publishers and consuming all events we are ensuring no event loss will be experienced. Our current migration allows the migration of all non-cluster wide resources into cluster-wide ones, and vice-versa, but does not take care of the system dynamics, such as transactions and in-flight events from a durable object. Durable subscriber objects will not be re-created after the migration, so client applications need to take care of this.

3. When all channels and queues are completely drained, stop all subscribers.
4. If you are working with a virtual machine (VM), create a snapshot of the existing virtual machine, in case you need to revert to this snapshot at a later stage.
5. Update the Universal Messaging license file with "clustering" capability (if applicable).
6. Ensure that the other Universal Messaging nodes that you will be working with in the clustered environment are at a software level that is identical with your existing node. If possible, update your existing node to the latest released fix level issued by Software AG, and ensure that the same fix level is installed on the other nodes.

Migrating from a Single Node to Multi-Node Active/Active Cluster

You have two scenarios:

- The cluster does not already exist, so you must create a new cluster containing your node and other nodes.
- The cluster exists already, so you will add your single node to the existing cluster.

Scenario 1: Create a new cluster and add your node to it

If the cluster does not already exist, then follow these steps to create the cluster and add the single node to the cluster:

1. Create a new cluster, as described in [“Creating Clusters” on page 84](#).
2. Add your single node and the other required nodes to the cluster.
3. After you have specified all of the nodes to be added to the cluster, choose the option to convert all local stores to cluster stores.

If you choose not to migrate the local stores, they are deleted.

4. Verify successful migration by the following steps:
 - a. Ensure that all nodes joined the cluster, that is, they are in Master or Slave state.
 - b. Ensure that all connection factories are enabled with the new URL for the Universal Messaging realm cluster.

- c. Ensure that JMS and webMethods messaging triggers (durable subscribers) are enabled by selecting the "Cluster Wide" check box on the durable subscription in the Enterprise Manager. If this is not already the case, you will need to delete the non-clustered durable subscribers, then manually synchronize documents using the Software AG Designer.
- d. Update the realm URL in all affected Universal Messaging clients (such as webMethods Integration Server, My webMethods Server) to point to the new Universal Messaging cluster URL. Enable Universal Messaging client connections (webMethods Integration Server, My webMethods Server), and enable publishers and subscribers.
- e. Start the publishers and subscribers.

Scenario 2: Add your node to an existing cluster

If the cluster already exists, then follow these steps to add the single node to the cluster:

1. Add your realm from the list of available realms to the list of existing cluster members.
2. Ensure that all connection factories are extended with the Universal Messaging realm URL of the newly added node.
3. Update the realm URL in all affected Universal Messaging clients (webMethods Integration Server, My webMethods Server) to point to the new Universal Messaging cluster URL.
4. Start publishers and subscribers.

Declustering a Single Node from an Active/Active Cluster

You have two scenarios:

- Deleting the cluster and allowing the individual nodes to continue as non-clustered nodes.
- Removing a single node from a cluster, while allowing the cluster to continue operating with the other cluster nodes.

Scenario 1: Delete the cluster

Follow these steps to delete the cluster and allow the individual nodes to continue as non-clustered nodes:

1. Delete the cluster, as described in ["Deleting a Cluster" on page 86](#).
You can choose whether you want to copy the cluster stores into local stores on the declustered nodes.
2. Ensure that all connection factories are enabled with the Universal Messaging realm URL.
3. Integration Server: Ensure that the "Cluster-Wide" settings for the JMS / webMethods Native Message triggers (DS) are disabled. Documents need to be synchronized from Software AG Designer so all durable objects are re-created. Ensure they have the "Cluster-Wide" option deselected.
4. Update the realm URL in the Universal Messaging clients (webMethods Integration Server, My webMethods Server) to point to the Universal Messaging realm URL.

5. Enable the Universal Messaging client connections.
6. Start the publishers and subscribers.

Scenario 2: Remove a single node from a cluster

Follow these steps to remove a single node from a cluster, while retaining the rest of the cluster:

1. Remove the realm from the list of cluster members, as described in [“Adding and Removing Cluster Members”](#) on page 86.

You can choose whether you want to copy the cluster stores into local stores on the declustered node.

2. Connection factories:
 - For the declustered node: Modify all connection factories so that they refer to only the realm URL of the newly declustered node.
 - For the remaining nodes in the cluster: Modify all connection factories so that the realm URL of the declustered node is removed.
3. Client URLs:
 - For the declustered node: Update the realm URL in the Universal Messaging clients (webMethods Integration Server, My webMethods Server) by providing only the Universal Messaging URL of the newly declustered node.
 - For the remaining nodes in the cluster: Update the realm URL in the Universal Messaging clients (webMethods Integration Server, My webMethods Server) by removing the Universal Messaging URL of the newly declustered node.
4. Start the publishers and subscribers.

Rollback strategy

For a rollback strategy if any severe issues occur during clustering or declustering that cannot be resolved, below are some options:

- Delete the cluster and migrate to local nodes.
- In the worst case, if there are still any potential issues with the local node after deleting the cluster, then roll back to the virtual machine snapshot.

Channel Administration

About Channel Administration

The Enterprise Manager enables you to configure, administer, and monitor Universal Messaging channels.

Channel Status

The Enterprise Manager enables you to monitor a channel's status in terms of publish and consume event totals / rates as well as connection total / rates and persistent store / memory.

Channel Access Control List (ACL)

Universal Messaging offers complete control over security policies. Universal Messaging stores security policies locally or can be driven by any external entitlements service. Universal Messaging's rich set of entitlements ensure that everything from a network connection through to a channel/queue creation can be controlled on a per user and/or host basis. For more information, see the Universal Messaging ACL's FAQ.

Channel Joins

Universal Messaging allows channels to be joined to other channels or queues creating server side routing tables with the possibility to apply filters based on message content on the local or a remote Universal Messaging realm.

Channel Connections

Channel subscribers are reported as channel connections and can be monitored or managed through the Universal Messaging Enterprise Manager.

Channel Durables

Channel subscribers can manage their subscription's event id manually or they can become a named subscriber and let that be managed by the Universal Messaging realm. The Universal Messaging Enterprise Manager allows complete management of channel durables.

Channel Event Snooping

The Universal Messaging Enterprise Manager provides the ability to inspect the contents of messages remotely using the Snoop panel.

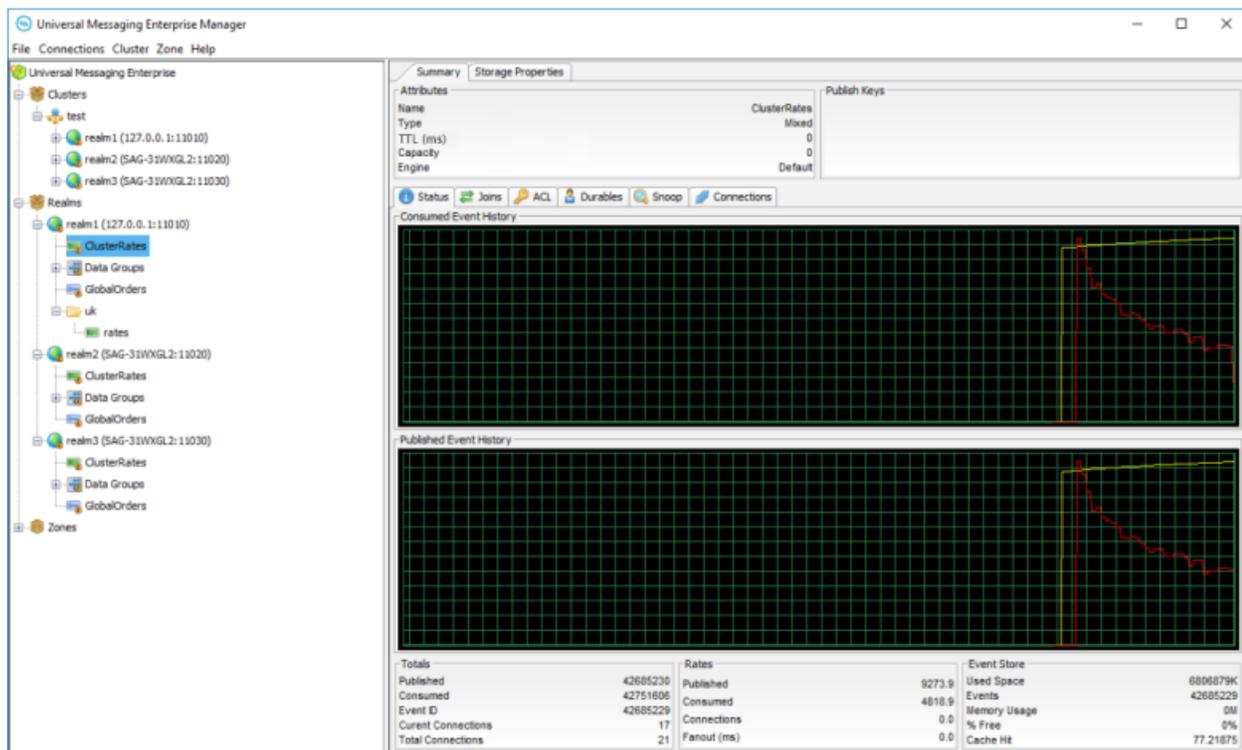
Viewing the Channel Status

When you select a channel object from the namespace, the first panel to be displayed on the right hand side of the Enterprise Manager panel is the Status panel. Configuration information is always displayed at the top section of the Enterprise Manager when a channel is selected. This configuration information shows channel type, TTL (age), capacity as well as any channel key information available. The **Status** tab shows real-time management information for the selected channel.

The top section of the Status panel shows real-time graphs representing the events published and consumed on the channel, both in terms of rates (per status interval) as well as the totals.

The bottom section of the Status panel shows the actual values plotted in the graphs for events published and consumed, as well as information about the actual channel store at the server.

The image below shows the Status panel for an active cluster channel.



The top graph in the panel shows the event history for events consumed from the channel. The red line graphs the rates at which events are being consumed, while the yellow line graphs the total events consumed from the channel.

The bottom graph shows the event history for events published to the channel. The red line graphs the rates at which events are being published, while the yellow line graphs the total events published to the channel. As the status events are consumed, and the channel (nLeafNode) is updated with the new values for events consumed and published, the status panel and its graphs are updated.

The bottom section of the Status panel shows three types of information: Totals, Rates, and Event Store.

Totals

The Totals section shows the following values:

- **Published** - The total number of events published to the channel when the last status events was consumed
- **Consumed** - The total number of events consumed from the channel when the last status event was consumed
- **Event ID** - The event id of the last event published to the channel
- **Current Connections** - The current number of consumers on the channel

- **Total Connections** - Total number of consumers on the channel. The total number includes the current consumers.

Rates

The Rates section shows the following values:

- **Published** - The current rate of events published to the channel, calculated as (total - previous total) / (interval 1000 milliseconds)
- **Consumed** - The current rate of events consumed from the channel, calculated as (total - previous total) / (interval 1000 milliseconds)
- **Connections** - The current rate of subscriptions being made to the channel

Event Store

The Event Store section shows the following values:

- **Used Space** - The amount of space in KB used by the channel on the server (either memory, or disk for persistent / mixed channels)
- **Events** - The current number of events on the channel
- **Memory Usage** - The amount of memory used in MB
- **% Free** - The amount of free space in the channel store calculated as used space minus total space used by all purged or aged events
- **Cache Hit** - The percentage of events consumed from the channel event cache as opposed to from the actual physical store, if the channel is persistent or mixed

Creating Channels

Channels are the logical meeting points for data that is published and subscribed to. If you are using Universal Messaging Provider for JMS, channels are the equivalent of JMS topics.

Each channel consists of a physical channel on the Universal Messaging realm as well as its logical reference in a namespace that may comprise resources that exist across multiple Universal Messaging realm servers. When you create a channel in the Enterprise Manager, a physical object is created on the realm. You can also obtain references to the channel by using the Universal Messaging Client and Admin APIs. You can create a channel in the following ways:

- Create the new channel directly under the realm node.
- Create a container node (folder) that contains the new channel.
- Add the new channel to an already existing container node.

If the realm on which you want to create the channel is part of a cluster, the channel is created as a cluster-wide asset. You cannot create local stores on a clustered realm.

When you connect to a Universal Messaging realm in the Enterprise Manager, all resources and services found in the realm namespace are displayed in a tree structure under the realm node.

➤ **To create a channel in the Enterprise Manager**

1. Expand the **Realms** node.
2. Select a realm, right-click it, and then select **Create Channel**.
3. In the Add channel dialog box, specify a name for the channel.

If you want to create a new container node, you must specify the absolute name of the channel. For example, to create a channel named "rates" in a new container named "eur", type `eur/rates`. For more information about the valid channel names, see [“Valid Channel and Queue Names” on page 100](#).

4. Specify the other channel attributes to configure the behavior of the channel.

For more information about the channel attributes and values to specify, see the summary of Channel Attributes in the *Commonly Used Features* section of the *Universal Messaging Concepts* guide.

5. (Optional) To configure the operational environment of the channel, edit the storage properties associated with the channel.

For more information about the storage properties, see the summary of Storage Properties in the *Commonly Used Features* section of the *Universal Messaging Concepts* guide.

6. (Optional) If you want to publish Protobuf events on the channel, upload a Protobuf descriptor.

For general information about Google protocol buffers, see the section *Google Protocol Buffers* in the *Universal Messaging Concepts* guide.

7. (Optional) To create a channel key, under **Channel Keys**, click **New** and specify the key name and depth.

Channel keys enable a channel to automatically purge old events when new events of the same type are received. For more information about working with channel keys, see the summary of Channel Publish Keys in the *Commonly Used Features* section of the *Universal Messaging Concepts* guide.

8. Click **OK**.

Valid Channel and Queue Names

The channel and queue names can contain any of the following characters:

- All letters and digits

- Slash "/"
- Hyphen "-"
- Underscore "_"
- Hash symbol "#"

Certain character strings are replaced:

- Backslash "\" is replaced by slash "/"
- Two colons "::" are replaced by slash "/"
- Two slashes "//" are replaced by one slash "/"

Valid names have the following length restrictions:

- Channel and queue names have a maximum limit of 235 characters.
- Namespace names have a maximum limit of 255 characters.
- The full path containing the data directory folder path with a channel or queue path appended to it has a maximum limit of 4096 characters.

If your channel or queue name contains slash characters, for example "a/b/c", this is represented in the Enterprise Manager view as a hierarchy, with "a" being the top node, "b" being the child node of "a", and "c" being the child node of "b". This virtual hierarchy is just a visual aid to help you to keep track of your channels and queues, but the store itself is not divided internally into hierarchical parts and can only be referenced by the full name, which in this example is "a/b/c".

Note:

There is a restriction that a channel or queue name cannot be the same as an existing folder name. So if you have named a channel "a/b/c", you cannot name a different channel "a" or "a/b". This would lead to a display conflict in Enterprise Manager, since we would have a folder "a" as the root of the path "a/b/c", as well as a channel "a" at the same position in the display. Similarly, trying to assign the name "a/b" to a new channel would conflict in the display with the folder named "a/b". You can however name a different channel "a/c", since "a" is used here again as a virtual folder. Similarly, you can name another channel "a/b/d", since both "a" and "a/b" are used here as virtual folders.

Editing Channels

Editing channels using the Enterprise Manager enables you to change specific attributes of a channel, such as its name, event time-to-live (TTL), capacity, channel keys, or the realm on which the channel exists.

When you edit a channel, its attributes and any events found on the channel are copied to a temporary channel. The old channel is then deleted, the new channel is created, and the original events are copied from the temporary channel to the new channel. The only exception is when you update the Google protocol buffer (Protobuf) descriptor uploaded on the channel. In this case, the channel is not deleted and then re-created.

Since editing a channel involves deleting the old channel, certain activities and objects associated with the old channel are also terminated and should be recreated. For more information about deleting channels, see [“Deleting Channels and Queues” on page 111](#).

As far as possible, channel events are held in memory for performance reasons. The temporary channel is also held in memory, and requires the same amount of memory as the channel being edited. The realm server must be able to allocate sufficient memory to store the temporary copy, otherwise the channel edit operation will be terminated and an error will be logged. If such a situation occurs, you can resolve it by allocating additional heap size, so that the temporary copy can exist in memory at the same time as the channel being edited.

➤ To edit a channel in the Enterprise Manager

1. Expand the **Realms** node, and then expand the realm on which you want to edit the channel.
2. Select the channel and right-click it.
3. From the drop-down menu, select **Edit channel *channel_name***.
4. Modify the channel attributes as required.

To move the channel to another available realm, in the **Parent Realm** field, select a realm from the list.

For more information about the channel attributes and values to specify, see the summary of Channel Attributes in the Commonly Used Features section of the *Universal Messaging Concepts* guide.

For information about updating the Protobuf descriptor uploaded on the channel, see [“Updating Protobuf Descriptors” on page 102](#).

5. (Optional) Edit the storage properties associated with the channel as required.

For more information about the storage properties, see the summary of Storage Properties in the Commonly Used Features section of the *Universal Messaging Concepts* guide.

6. Click **OK**.

Updating Protobuf Descriptors

The protocol buffer (Protobuf) definition files associated with a store (a channel or a queue) can be updated without requiring the store to be deleted and re-created. After you update the Protobuf descriptor, all filtering will be done with the new Protobuf definitions.

➤ To update protocol buffer definitions in the Enterprise Manager

1. Select the store whose descriptors you want to update and right-click it.

2. From the drop-down menu, select **Update Protocol Buffers**.
3. Select the file or files that contain the descriptors you want to set on the store (multi-select is enabled for loading multiple file descriptor sets). Then click **Open**.

The new Protobuf definitions are applied to the store.

For information about updating protocol buffer definitions programmatically, for example in Java, see the section *Google Protocol Buffers* in the *Developer Guide*.

Exporting Protobuf Descriptors

You can export the protocol buffer (Protobuf) definitions associated with a store (a channel or a queue) to a folder.

➤ To export protocol buffer definitions in the Enterprise Manager

1. Select the store whose Protobuf descriptors you want to export and right-click it.
2. From the drop-down menu, select **Export Protobuf Definitions**.
3. Select the folder where you want the descriptors from the store to be exported. Then click **Open**.

Note:

If a folder named the same way as the store exists and that folder is not empty, the Protobuf descriptors are not exported and an error message is displayed.

The Protobuf definitions are exported from the store.

Copying Channels

Copying channels using the Enterprise Manager enables you to duplicate channels automatically across realms. When you copy a channel, its attributes and any events found on the channel are copied to the new channel.

➤ To copy a channel in the Enterprise Manager

1. Expand the **Realms** node, and then expand the realm from which you want to copy the channel.
2. Select the channel and right-click it.
3. From the drop-down menu, select **Copy channel *channel_name***.
4. In the Copy channel dialog box, in the **Parent Realm** field, select the realm to which you want to copy the channel.

5. (Optional) Modify any channel attributes and storage properties.
6. Click **OK**.

The channel is displayed in the namespace tree of the selected target realm.

Creating Channel Joins

Joining channels using the Enterprise Manager creates a physical link between a source channel and a destination store (a channel or a queue). After you create a join, any events published to the source channel are republished to the destination store. You can create a join between the following sources and destinations:

- A channel on a realm and a store on another realm federated with the source realm.
- A channel on a clustered realm and a store in the same cluster. A non-cluster-wide channel can be joined to a cluster-wide store, but not the other way round.
- A channel in one cluster and a channel in another cluster by using an inter-cluster join. You must first create an inter-cluster connection between the two clusters.
- A source channel and a destination queue. Universal Messaging does not support joins where the source is a queue.

You can join channels programmatically or by using the Enterprise Manager.

➤ To create a channel join in the Enterprise Manager

1. In the namespace tree of a realm, select the channel that you want to use as a source and right-click it.
2. From the drop-down menu, select **Join channel *channel_name***.
3. Specify the following join attributes:
 - a. In the **To Realm** field, select the realm that holds the destination store.
 - b. In the **To Store** field, type the name of the destination store.
 - c. Click **OK**.
4. (Optional) Specify any of the following additional join attributes:
 - In the **Filter** field, specify a filter, so that only specific events published to the source channel, which match certain search criteria, will be routed to the destination store. For example, if you type `CCY='EUR'`, only events with the event property `CCY` equal to `'EUR'` occurring on the source channel will be published to the destination store.

- In the **Hop Count** field, specify the number of join hops through which an event can travel. The default is 10.
- Select the **Allow Purge** option to purge events when the source channel is purged.
- Select the **Archival** option to create an archival join, which is created only between a channel and a destination queue. With an archival join, events on the queue are not checked for duplication, which may result in duplicate events if the queue has multiple sources.

5. Click **OK**.

The Enterprise Manager creates an outgoing join on the source channel and an incoming join on the destination store. You can view the newly created joins and any existing joins on the **Joins** tab of a channel or queue.

Viewing Channel Connections

When a Universal Messaging client connects to a realm server, the server maintains information about the connection, which is available through the Universal Messaging Administration API. The API also provides mechanisms for receiving notifications when connections are added and deleted (See the code example "Connection Watch" that uses the Administration API).

Connection information is also maintained when Universal Messaging clients subscribe to channels.

The Universal Messaging Enterprise Manager enables you to view the connections (channel subscriptions) on a realm as well as more detailed information about each connection, such as the last event sent or received, and the rate of events sent by and received from each connection.

You view connections for a channel on the **Connections** tab for the channel. Connections have the following attributes:

- **Protocol** - The protocol used in the connection.
- **User** - The username of the connected user.
- **Host** - The host machine from which the user has connected.
- **Connection** - The local connection ID, defined as *hostname:local_port*.
- **Sub-Name** - The durable reference, if one is provided. For more information about channel durables, see "[Viewing and Managing Durables for a Channel](#)" on page 111.
- **Filter** - The filter string for the subscription, if one is provided.

To view details for a channel connection, select the connection and click **Show Details**. You can view the following information:

Connection Details

The Connection Details panel shows information about the user connection, such as user name, host, protocol, connection ID, and whether multicast is enabled.

Client Environment

The Client Environment panel shows information about the client environment for this user, such as API language/version, host operating system, and Universal Messaging build number.

The Tx Event History and Rx Event History graphs show the total (yellow) and rates (red) for events received from the server (TX) and sent to the server (RX), respectively, for the selected connection.

Events Sent

The Events Sent panel shows the following information:

- **Total** - The total number of events sent by the realm server to this connection.
- **Rate** - The rate at which events are sent by the realm server to this connection.
- **Max** - The maximum rate at which events have been sent by the realm server to this connection.
- **Last Event Type** - The type of the last event sent from the realm server.
- **Bytes** - Total bytes sent by the realm server to this connection.

Events Received

The Events Received panel shows the following information:

- **Total** - The total number of events sent by this connection to the realm server.
- **Rate** - The rate at which events are sent by connection to the realm server.
- **Max** - The maximum rate at which events have been sent by this connection to the realm server.
- **Last Event Type** - The type of the last event sent from the connection to the realm server.
- **Bytes** - Total bytes sent by this connection to the realm server.

Status

The Events Sent panel shows the following information:

- **Connect Time** - The amount of time this connection has been connected to the realm server.
- **Queue Size** - The number of events in the outbound queue of this connection, that is events waiting to be sent to the realm server.
- **Last Tx** - The time since the last event was received by this connection from the realm server.
- **Last Rx** - The time since the last event was sent to the server from this connection.

Snooping on a Channel

Snooping on a channel in the Enterprise Manager enables you to view the contents of events published on the channel. You can view details about all events on the channel or about a specific set of events, based on their event IDs or additional filtering criteria.

> To start snooping on a channel

1. In the namespace tree of a realm, select the channel on which you want to snoop and click the **Snoop** tab.
2. Do any of the following:
 - To snoop on all events published on the channel, click **Start**.
 - To snoop on a range of events, in the **From** field, specify the ID of the first event in the range, and in the **To** field, specify the ID of the last event in the range. Click **Start**.

Note:

If you do not specify a value in the **From** field, the range of events starts with the first event on the channel and ends with the event specified in the **To** field. If you do not specify a value in the **To** field, the range of events starts with the event specified in the **From** field and ends with the last event on the channel.

- To snoop on events that match specific filtering criteria based on the properties of the event, in the **Filter** field, specify a selector string that will be used for filtering. Click **Start**.

The Enterprise Manager populates the snooped events table with the events published on the channel. You can view details about the events.

You can pause the snoop temporarily or stop the snoop altogether. Stopping the channel snoop clears the snooped events table.

Viewing Details About Snooped Events on a Channel

After you start snooping on a channel in the Enterprise Manager, any events published on the channel are added to the snooped events table on the **Snoop** tab. The table displays information about each event including the event ID, tag, time to live (TTL), and whether the event is persistent.

When you select an event in the table, you can view additional details about the event including a hexadecimal view of the event data and an ASCII representation of the event data, the header and properties of the event.

Purging Events from a Channel

After you start snooping on a channel, you can purge snooped events from the channel. You can purge a single event, a range of events, or all events.

> To purge events from a channel in the Enterprise Manager

1. In the namespace tree of a realm, select the channel from which you want to purge events.
2. Perform any of the following actions:
 - To purge all events, right-click the channel and select **Purge All Events**.
 - To purge a range of events, right-click the channel and select **Purge Events**. In the **Start EID** field specify the ID of the first event in the range, and in the **End EID** field, specify the ID of the last event in the range. In addition, you can specify filtering criteria based on the properties of the event, so that only events that match these criteria are purged.

Note:

If you do not specify a value in the **Start EID** field, the range of events to purge starts with the first event on the channel and ends with the event specified in the **End EID** field. If you do not specify a value in the **End EID** field, the range of events starts with the event specified in the **Start EID** field and ends with the last event on the channel.

- To purge a single event, go to the **Snoop** tab and select the event in the snooped events table. Right-click the event and select **Purge Event**.

Publishing Events on a Channel

Publishing a New Event on a Channel

Use the following procedure to create a new event and publish it on a channel in the Enterprise Manager.

> To publish a new event on a channel in the Enterprise Manager

1. In the namespace tree of a realm, select the channel on which you want to publish an event and right-click it.
2. From the drop-down menu, select **Publish**.
3. In the **Event Data** field of the Publish event to Channel dialog box, specify the content of the event in one of the following ways:
 - Type a string.
 - Click **File** to add a file as event content.

The contents of the file are not displayed, but the file is read in binary format.
4. (Optional) Specify any of the following event details:

Field	Description
Event Tag	The tag of the event.
Event TTL	The time-to-live (TTL) of the event in milliseconds. Defines how long the event remains available on the channel. The default is 0, which means the event remains on the channel indefinitely. <div style="background-color: #f0f0f0; padding: 5px;"> <p>Note: You can publish an event with a specified TTL only on queues and channels of type Mixed. Events on queues and channels of type Persistent or Reliable use the TTL set on store level and ignore any event-level TTL.</p> </div>
Num Of Publishes	The number of times to publish the event. The default is 1.
Is Persistent	Whether the event is persistent.

5. (Optional) Under **Property Input**, add any event properties:
 - a. Specify the event key and value.
 - b. Select the event type.
 - c. Click **Add**.

The property is added to the property display table. To edit an entry in the table, double-click it, make your changes, and then press Enter. To remove a property, select the property, right-click it, and then select **Remove Property**.

6. Click **OK**.

When you start snooping on events on the channel, the Enterprise Manager displays the event in the snooped events table.

Example of Creating a New Event

The following graphic shows the Publish events to Channel dialog box and the values specified for the event with content "Corporate Sale", published on the channel "rates" on the realm "umserver".

Publish event to Channel rates

Publish Location
 Realm:
 Channel:

Event Data

Event Details
 Event Tag:
 Event TTL:
 Num Of Publishes:
 Is Persistent:
 Is Transient:

Property Input
 Key:
 Value:
 Type:

Property Display

Key	Value	Type
discount	0.05	Float
price	56.3	Float
quantity	3.0	Float
SalesPerson_ID	1023	Integer

Purge Original Event:

Republishing Events on a Channel

Use the following procedure to duplicate an already published event or to edit and republish an event on a channel. You can also choose to purge the original event.

Before republishing an event on a channel, you must start snooping on the channel. For more information about snooping on a channel, see [“Snooping on a Channel” on page 107](#).

➤ To republish an event

1. In the namespace tree of a realm, select the channel on which you want to republish the event and click the **Snoop** tab.
2. In the snooped events table, select the event, right-click it, and then select **Edit & Republish Event**.
3. Modify the event properties as required.
4. (Optional) Select the **Purge Original Event** option.

5. Click **OK**.

Viewing and Managing Durables for a Channel

Durables (named objects) are channel objects stored by a realm server, which provide state information for durable consumers. Depending on its type, a durable can have one or more durable consumers connected to it. Each time a consumer connects to a durable, the consumer starts consuming events from the last event ID successfully consumed by the previous consumer connected to the durable. The consumed events include all events sent to the channel after the previous consumer disconnected and before the new consumer connected.

- To view durables for a channel in Enterprise Manager, select the channel and click the **Durables** tab.

The durables table lists all durables present on the channel. Each row of the table shows a separate durable. The columns of the table show the attributes of a durable, such as the name and current event ID, the number of outstanding events, whether the durable is cluster-wide and whether it is persistent, and what its type is.

When a durable is added or removed, or the attributes of a durable are changed, Enterprise Manager updates the table automatically.

Note:

When the attributes of a durable are changed, Enterprise Manager updates the durables table with a delay of several seconds.

- To delete a durable from the durables table, select the durable and click **Delete Durable**.

Deleting Channels and Queues

To delete a store (i.e., a channel or queue), proceed as follows:

1. Select the store in the namespace of the Enterprise Manager,
2. Select **Delete** in the context menu of the store.

Note:

Since *editing* a store involves deleting the existing store before creating the new store, all of the points mentioned below for deleting a store apply also for editing a store.

Upon deletion of a store, all assets dependent on it will be deleted and all content in the store will be deleted. All active subscriptions to the store will be terminated, as well as all shared durables attached to the store, along with the associated messages. Such subscriptions or shared durables need to be recreated by the original creator of those objects after you have finished deleting the channel.

Deleting a store which serves as a dead event store for another store will cause that reference to be removed, therefore the user should re-create the reference.

Any joins from or to this store will need to be recreated as they are now disabled.

Before you delete a store, we suggest that you observe the following procedure:

- Drain the store and its durable subscriptions, otherwise any messages in-flight within the store or related to the store will now be lost and transactions will not be deterministic.
- Prevent all publishing activity on the store while it is being deleted; see the section *Pause Publishing* in the *Concepts* guide for related information.

Queue Administration

Creating Queues

Each queue consists of a physical object on the Universal Messaging realm as well as its logical reference in a namespace that may comprise resources that exist across multiple Universal Messaging realm servers. You can also obtain references to the queue by using the Universal Messaging Client and Admin APIs. You can create a queue in the following ways:

- Create the new queue directly under the realm node.
- Create a container node (folder) that contains the new queue.
- Add the new queue to an already existing container node.

If the realm on which you want to create the queue is part of a cluster, the queue is created as a cluster-wide asset. You cannot create local stores on a clustered realm.

When you connect to a Universal Messaging realm in the Enterprise Manager, all resources and services found in the realm namespace are displayed in a tree structure under the realm node.

➤ To create a queue in the Enterprise Manager

1. Expand the **Realms** node.
2. Select a realm, right-click it, and then select **Create Queue**.
3. In the Add queue dialog box, specify a name for the queue.

If you want to create a new container node, you must specify the absolute name of the queue. For example, to create a queue named "requests" in a new container named "eur", type `eur/requests`.

The set of valid characters that you can use for queue names is the same as the valid character set for channel names. For more information, see [“Valid Channel and Queue Names” on page 100](#).

4. Specify the other queue attributes to configure the behavior of the queue.

For more information about the queue attributes and values to specify, see the summary of Queue Attributes in the *Commonly Used Features* section of the *Universal Messaging Concepts* guide.

5. (Optional) To configure the operational environment of the queue, edit the storage properties associated with the queue.

For more information about the storage properties, see the summary of Storage Properties in the *Commonly Used Features* section of the *Universal Messaging Concepts* guide.

6. (Optional) If you want to publish Protobuf events on the queue, upload a Protobuf descriptor.

For general information about Google protocol buffers, see the section *Google Protocol Buffers* in the *Universal Messaging Concepts* guide.

7. Click **OK**.

Viewing Queues

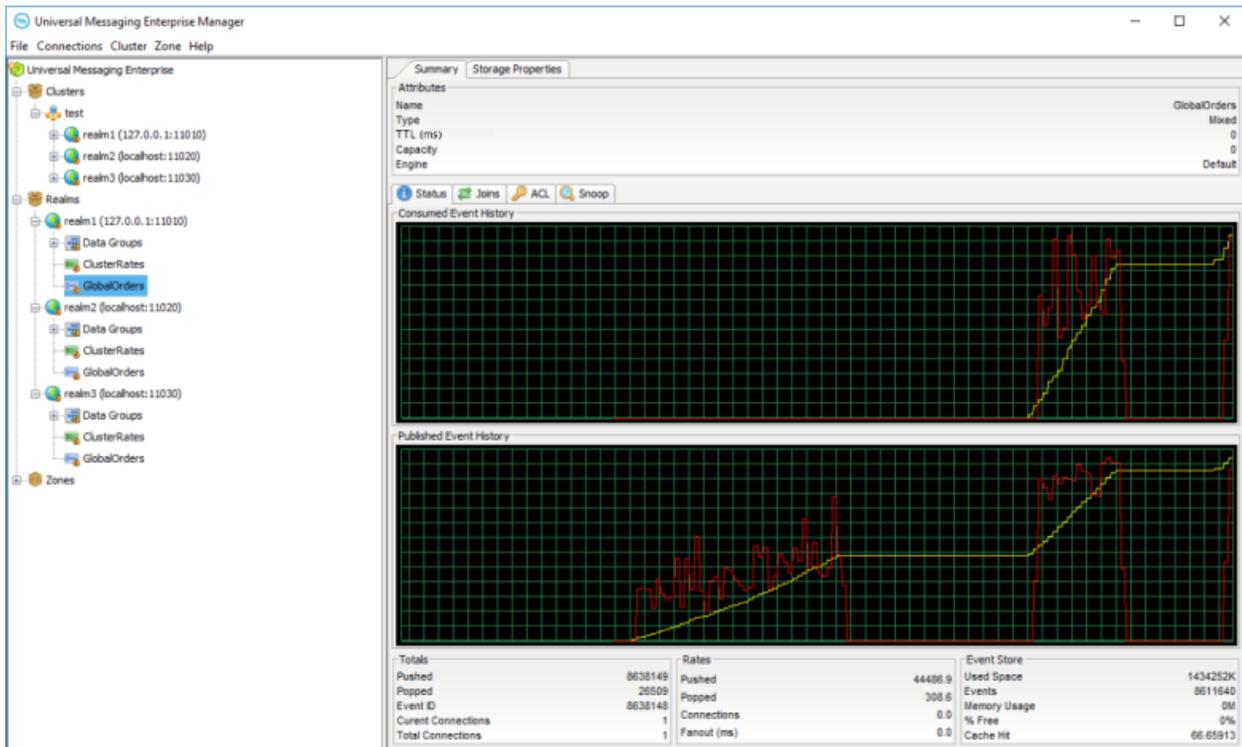
Viewing the Queue Status

When you select a queue object from the namespace, the first panel to be displayed on the right-hand side of the Enterprise Manager panel is the Status panel. Configuration information is always displayed at the top section of the Enterprise Manager when a queue is selected. This configuration information shows the queue type, TTL (age), and capacity. The **Status** tab shows real-time management information for the selected queue.

The top section of the Status panel shows real-time graphs representing the events pushed and popped from the queue, both in terms of rates (status interval) as well as the totals.

The bottom section of the Status panel shows the values plotted in the graphs for events pushed and popped, as well as information about the actual queue store at the server.

The image below shows the Status panel for an active queue.



The top graph in the panel shows the event history for events popped from the queue. The red line graphs the rates at which events are being popped while the yellow line graphs the total events popped from the queue.

The bottom graph shows the event history for events pushed onto the queue. The red line graphs the rates at which events are being pushed, while the yellow line graphs the total events pushed to the queue. As the status events are consumed, and the queue `nLeafNode ()` is updated with the new values for events popped and pushed, the status panel and its graphs are updated.

The bottom section of the Status panel shows three types of information : Totals, Rates, and Event Store.

Totals

The Totals section contains the following values:

- **Pushed** - The total number of events pushed to the queue when the last status event was consumed
- **Popped** - The total number of events popped from the queue when the last status event was consumed
- **Event ID** - The event id of the last event pushed to the queue
- **Current Connections** - The current number of asynchronous consumers on the queue
- **Total Connections** - The total number of asynchronous consumers that have subscribed to the queue

Rates

The Rates section contains the following values:

- **Pushed** - The current rate of events pushed to the queue, calculated as (total - previous total) / (interval 1000 milliseconds)
- **Popped** - The current rate of events popped from the queue, calculated as (total - previous total) / (interval 1000 milliseconds)
- **Connections** - The current rate of asynchronous subscriptions being made to the queue

Event Store

The Event Store section contains the following values:

- **Used Space** - The amount of space in KB used by the queue on the server (either memory, or disk for persistent / mixed queues)
- **Events** - The current number of events stored on the queue, which may include already consumed events. The exact number of delivered and available-for-delivery events on the queue can be seen on the **Consumer Info** tab.
- **Memory Usage** - The amount of memory used in MB
- **% Free** - The amount of free space in the queue store calculated as used space minus total space used by all purged or aged events
- **Cache Hit** - The percentage of events popped from the queue event cache as opposed to from the actual physical store, if the queue is persistent or mixed

Viewing Queue Joins

Universal Messaging enables you to join a source channel to a destination queue, creating server-side routing tables with the possibility to apply filters based on message content on the local or a remote Universal Messaging realm. You can view any joins on the **Joins** tab for a queue. For more information about working with channel joins, see [“Creating Channel Joins” on page 104](#).

Viewing Consumer Information

The **Consumer Info** tab shows the following information.

The Status section gives the following details:

- **Total Pending** - Current count of events waiting to be acknowledged or rolled back.
- **Queue Depth** - The outstanding events for delivery on the queue.
- **Last Read** - The timestamp of the last event that was read (consumed).
- **Last Write** - The timestamp of the last event that was written to the queue (published).

The Connection Details section gives the following details:

- **ID** - The ID of the queue consumer. In most cases, the ID of the consumer contains host and port information, but in addition it can contain the multiplex identifier on the TCP host port and the unique ID of the consumer.
- **Mode** - The client subscription mode (either asynchronous or synchronous).
- **Max Pending** - The window size for this subscription.
- **Acknowledged** - The total number of acknowledged events for this subscription.
- **Rolled Back** - The total number of rolled back events for this subscription.
- **Pending** - The events queued, waiting to be acknowledged or rolled back for this subscription.
- **Last Read** - The last time the session acknowledged, rolled back or read an event for this subscription.

Editing Queues

Editing queues using the Enterprise Manager enables you to change specific attributes of a queue, such as its name, event time-to-live (TTL), capacity, or the realm on which the queue exists.

When you edit a queue, its attributes and any events found on the queue are copied to a temporary queue. The old queue is then deleted, the new queue is created, and the original events are copied from the temporary queue to the new queue.

Since editing a queue involves deleting the old queue, certain activities and objects associated with the old queue are also terminated and should be recreated. For more information about deleting queues, see [“Deleting Channels and Queues” on page 111](#).

As far as possible, queue events are held in memory for performance reasons. The temporary queue is also held in memory, and requires the same amount of memory as the queue being edited. The realm server must be able to allocate sufficient memory to store the temporary copy, otherwise the queue edit operation will be terminated and an error will be logged. If such a situation occurs, you can resolve it by allocating additional heap size, so that the temporary copy can exist in memory at the same time as the queue being edited.

➤ To edit a queue in the Enterprise Manager

1. Expand the **Realms** node, and then expand the realm on which you want to edit the queue.
2. Select the queue and right-click it.
3. From the drop-down menu, select **Edit queue *queue_name***.
4. Modify the queue attributes as required.

To move the queue to another available realm, in the **Parent Realm** field, select a realm from the list.

For more information about the queue attributes and values to specify, see the summary of Queue Attributes in the Commonly Used Features section of the *Universal Messaging Concepts* guide.

For information about updating the Protobuf descriptor uploaded on the queue, see [“Updating Protobuf Descriptors” on page 102](#).

5. (Optional) Edit the storage properties associated with the queue as required.

For more information about the storage properties, see the summary of Storage Properties in the Commonly Used Features section of the *Universal Messaging Concepts* guide.

6. Click **OK**.

Copying Queues

Copying queues using the Enterprise Manager enables you to duplicate queues automatically across realms. When you copy a queue, its attributes and any events found on the queue are copied to the new queue.

➤ To copy a queue in the Enterprise Manager

1. Expand the **Realms** node, and then expand the realm from which you want to copy the queue.
2. Select the queue and right-click it.
3. From the drop-down menu, select **Copy queue *queue_name***.
4. In the Copy queue dialog box, in the **Parent Realm** field, select the realm to which you want to copy the queue.
5. (Optional) Modify any queue attributes and storage properties.
6. Click **OK**.

The queue is displayed in the namespace tree of the selected target realm.

Snooping on a Queue

Snooping on a queue in the Enterprise Manager enables you to view the contents of events published on the queue. You can view details about all events on the queue or about a specific set of events, based on their event IDs or additional filtering criteria.

➤ To start snooping on a queue

1. In the namespace tree of a realm, select the queue on which you want to snoop and click the **Snoop** tab.

2. Do any of the following:

- To snoop on all events published on the queue, click **Start**.
- To snoop on a range of events, in the **From** field, specify the ID of the first event in the range, and in the **To** field, specify the ID of the last event in the range. Click **Start**.

Note:

If you do not specify a value in the **From** field, the range of events starts with the first event on the queue and ends with the event specified in the **To** field. If you do not specify a value in the **To** field, the range of events starts with the event specified in the **From** field and ends with the last event on the queue.

- To snoop on events that match specific filtering criteria based on the properties of the event, in the **Filter** field, specify a selector string that will be used for filtering. Click **Start**.

The Enterprise Manager populates the snooped events table with the events published on the queue. You can view details about the events.

You can pause the snoop temporarily or stop the snoop altogether. Stopping the queue snoop clears the snooped events table.

Viewing Details About Snooped Events on a Queue

After you start snooping on a queue in the Enterprise Manager, any events published on the queue are added to the snooped events table on the **Snoop** tab. The table displays information about each event including the event ID, tag, time to live (TTL), and whether the event is persistent.

When you select an event in the table, you can view additional details about the event including a hexadecimal view of the event data and an ASCII representation of the event data, the header and properties of the event.

Purging Events from a Queue

After you start snooping on a queue, you can purge snooped events from the queue. You can purge a single event, a range of events, or all events.

➤ To purge events from a queue in the Enterprise Manager

1. In the namespace tree of a realm, select the queue from which you want to purge events.
2. Perform any of the following actions:
 - To purge all events, right-click the queue and select **Purge All Events**.

- To purge a range of events, right-click the queue and select **Purge Events**. In the **Start EID** field specify the ID of the first event in the range, and in the **End EID** field, specify the ID of the last event in the range. In addition, you can specify filtering criteria based on the properties of the event, so that only events that match these criteria are purged.

Note:

If you do not specify a value in the **Start EID** field, the range of events to purge starts with the first event on the queue and ends with the event specified in the **End EID** field. If you do not specify a value in the **End EID** field, the range of events starts with the event specified in the **Start EID** field and ends with the last event on the queue.

- To purge a single event, go to the **Snoop** tab and select the event in the snooped events table. Right-click the event and select **Purge Event**.

Publishing Events on a Queue

Publishing a New Event on a Queue

Use the following procedure to create a new event and publish it on a queue in the Enterprise Manager.

➤ To publish a new event on a queue in the Enterprise Manager

1. In the namespace tree of a realm, select the queue on which you want to publish an event and right-click it.
2. From the drop-down menu, select **Publish**.
3. In the **Event Data** field of the Publish event to Queue dialog box, specify the content of the event in one of the following ways:
 - Type a string.
 - Click **File** to add a file as event content.

The contents of the file are not displayed, but the file is read in binary format.

4. (Optional) Specify any of the following event details:

Field	Description
Event Tag	The tag of the event.
Event TTL	The time-to-live (TTL) of the event in milliseconds. Defines how long the event remains available on the queue. The default is 0, which means the event remains on the queue indefinitely.

Note:

Field	Description
	You can publish an event with a specified TTL only on queues and channels of type Mixed. Events on queues and channels of type Persistent or Reliable use the TTL set on store level and ignore any event-level TTL.
Num Of Publishes	The number of times to publish the event. The default is 1.
Is Persistent	Whether the event is persistent.

5. (Optional) Under **Property Input**, add any event properties:

- a. Specify the event key and value.
- b. Select the event type.
- c. Click **Add**.

The property is added to the property display table. To edit an entry in the table, double-click it, make your changes, and then press Enter. To remove a property, select the property, right-click it, and then select **Remove Property**.

6. Click **OK**.

When you start snooping on events on the queue, the Enterprise Manager displays the event in the snooped events table.

Republishing Events on a Queue

Use the following procedure to duplicate an already published event or to edit and republish an event on a queue in the Enterprise Manager. You can also choose to purge the original event.

Before republishing an event on a queue, you must start snooping on the queue. For more information about snooping on a queue, see [“Snooping on a Queue” on page 117](#).

➤ To republish an event

1. In the namespace tree of a realm, select the queue on which you want to republish the event and click the **Snoop** tab.
2. In the snooped events table, select the event, right-click it, and then select **Edit & Republish Event**.
3. Modify the event properties as required.
4. (Optional) Select the **Purge Original Event** option.

5. Click **OK**.

Data Group Administration (Deprecated)

About Data Groups

Important:

The data group functionality is deprecated.

Universal Messaging data groups provide a lightweight grouping structure that enables developers to manage user subscriptions remotely and transparently. Data groups provide an alternative to channels (JMS topics).

Each data group is a resource that exists on a Universal Messaging realm server or in a cluster of realm servers. When you create a data group, the Enterprise Manager creates a physical object on the realm. After you create a data group, you can obtain references to the data group by using the Universal Messaging Client and Admin APIs. You can also manage and monitor the data group in the Enterprise Manager.

When you connect to a Universal Messaging realm in the Enterprise Manager, all resources and services found in the realm namespace are displayed in a tree structure under the realm node.

Creating Data Groups

Important:

The data group functionality is deprecated.

You can create a data group directly under the **Data Groups** node in the namespace tree of a realm or add a nested data group to an existing data group.

> To create a data group in the Enterprise Manager

1. In the namespace tree of a realm, do one of the following:
 - To create a data group under the **Data Groups** node, right-click the **Data Groups** node and select **Create Data Group**.
 - To create a nested data group, expand the **Data Groups** node, right-click an existing data group, and select **Add A Data Group to *data_group_name***.
2. Specify a name for the new data group.
3. (Optional) Specify values for any of the following fields:

Field	Description
Multicast	Whether multicast is supported on the data group.
Priority	The default message priority for events on the data group.
Merge	Whether to merge events when multiple events arrive for this data group.
Drop	Whether to drop events that are made obsolete by newer events.
Interval (ms)	The interval in milliseconds at which events are sent.

4. Click **OK**.

Publishers with the Publish to DataGroups ACL permission can now publish messages to the new data group programmatically.

Viewing the Data Group Status

When you select the **Data Groups** node in the namespace tree of a realm in the Enterprise Manager, on the **Status** tab, you can view information about the published and consumed events on all data groups, as well as the number of data groups and data streams currently connected.

The Event History graph shows the rates at which events are published (red) and consumed (yellow) across all data groups in the current realm. The graph is updated each time a status event is received from the realm in which data groups are actively used.

In addition, you can view information on the Event Status and Totals panels.

Event Status

The Event Status panel contains the following information:

- **Total Consumed** - The total number of events consumed by all data groups on the realm, including the default data group.
- **Total Published** - The total number of events published to all data groups on the realm, including the default data group.
- **Consumed/Sec** - The rate at which events are consumed across all data groups on the realm, including the default data group.
- **Published/Sec** - The rate at which events are published across all data groups on the realm, including the default data group.

Totals

The Totals panel contains the following information:

- **Current Groups** - The number of data groups on the realm, excluding the default data group.

- **Current Streams** - The number of currently connected data streams.
- **Total Streams** - The total number of streams that have been added to all data groups since the last start of the realm.

Adding Existing Data Groups to Data Groups

➤ To add an existing data group to another data group in the Enterprise Manager

1. In the namespace tree of a realm, expand the **Data Groups** node.
2. Select the data group to which you want to add an existing data group and right-click it.
3. Select **Add A Data Group to *data_group_name***.
4. In the Add Data Group dialog box, type the name of the existing data group and click **OK**.

Any events published to the parent data group will be delivered to any data streams that are members of the newly-added data group.

Removing Data Groups from data Groups

➤ To remove an existing data group from another data group in the Enterprise Manager

1. In the namespace tree of a realm, expand the **Data Groups** node and locate the parent data group.
2. Right-click the data group you want to remove and select **Remove *data_group_name* from *data_group_name***.
3. Click **OK**.

If the removed data group has no other parent data groups, it appears under the top-level **Data Groups** node. If the removed data group has other parent data groups, it remains in them.

Deleting Data Groups

To delete a data group in the Enterprise Manager, perform any of the following actions in the namespace tree of a realm:

- Right-click the **Data Groups** node, select **Delete A Data Group**, and then type the name of the data group you want to delete.
- Expand the **Data Groups** node and locate the data group you want to delete. Right-click the data group and select **Delete *data_group_name***.

Container Administration

Viewing the Container Status

When you select a container (folder) in the namespace tree of a realm and go to the **Totals** tab, you can view status information about the resources in the container.

The Event History graph shows the rates at which events are published (red) and consumed (yellow) across all channels and queues in the container. The Storage Usage History graph shows the total amount of storage space used by each channel and queue in the container. Both graphs are updated each time a status event is received from the realm in which the container exists.

You can view additional details in the Event Status, Totals, Connection Status, and Storage Usage panels.

Event Status

The Event Status panel contains the following information:

- **Consumed** - The total number of events consumed by all channels and queues in the container.
- **Published** - The total number of events published to all channels and queues in the container.
- **Consumed/Sec** - The number of events per second consumed by all channels and queues in the container.
- **Published/Sec** - The number of events per second published to all channels and queues in the container.

Totals

The Totals panel contains the following information:

- **Realms**- The number of realms mounted in the container.
- **Channels**- The number of channels that exist in the container.
- **Queues**- The number of queues that exist in the container.

Connection Status

The Connection Status panel contains the following information:

- **Total** - The total number of connections made to channels and queues in the container.
- **Current** - The current number of connections made to channels and queues in the container.
- **Rate** - The number of connections being made per second to channels and queues in the container.

Storage Usage (K)

The Storage Usage panel contains the following information:

- **Total** - The total amount of memory and disk space in KB used by all events, both consumed and unconsumed, on all channels and queues in the container.
- **Free** - The amount of disk space in KB occupied by consumed and purged events on all channels and queues in the container, which can be reclaimed by auto-maintenance.
- **Used** - The amount of memory and disk space used by unconsumed events on all channels and queues in the container.
- **Used/Sec** - The rate per second at which the total amount of used storage space changes.

Monitoring Container Usage

When you select a container (folder) in the namespace tree of a realm and go to the **Monitor** tab, you can find usage information, such as heap memory usage history, CPU and disk space usage, and JVM GC stats, based on the channels and queues in the container. In addition, you can view the number of mounted realms, channels, and queues in the container.

For each channel and queue, you can also find the following details in the usage details table:

- **Name** - The name of the channel or queue.
- **Connections** - The number of consumers the channel or queue has.
- **Published** - The rate of events published per status interval.
- **Consumed** - The rate of events consumed per status interval.
- **Memory (bytes)** - The number of bytes the channel or queue uses from the JVM memory.
- **% Memory** - The percentage of overall JVM memory used by the channel or queue.
- **Disk (KB)** - The amount of disk space in KB used by the channel or queue when the channel or queue is of persistent or mixed type.

Creating Monitor Graphs

On the **Monitor** tab, you can also create a graph of channel and queue usage. The graph uses a 3D graph package from SourceForge (<http://sourceforge.net/projects/jfreechart/>) to display the items in the usage details table as columns in a 3D vertical bar chart. You can create a graph for each usage metric and update the graph in real time.

- To create a graph, select a column in the usage details table and click the **Bar Graph** button.
- To update a graph in real time, right-click anywhere in the graph and select **Start Live Update**.
- To stop live updates, right-click in the graph and select **Stop Live Updates**.

Using ACLs for Role-Based Security

About Realm ACL Permissions

To perform operations within a realm, clients connecting to the realm must have the correct ACL (Access Control List) permissions. A realm ACL contains a list of subjects, which can be username and host pairs, or security groups, and what operations each subject can perform within the realm.

You can manage ACL permissions for a realm in the Enterprise Manager or by using the Universal Messaging Administration API. You can add, remove, and modify ACL entries, and view ACL permissions on the **Security > ACL** tab for a realm in the Enterprise Manager. A green check icon indicates the permissions given to each subject.

A subject in the ACL list can have the following permissions to perform operations on the realm:

- **Manage ACL** - Can get and manage the list of ACL entries.

Note:

This permission is a combination of two permissions at the Administration API level. The boolean `setModify()` API function allows or denies permission to change an ACL value, and the boolean `setList()` API function allows or denies permission to access the current list of ACLs. If both of these functions return the value `true`, Manage ACL is allowed, otherwise Manage ACL is not allowed. If the green check icon is displayed in the **Manage ACL** field, the corresponding two API functions for this field are set to `true`. You cannot modify the value of this permission in the Enterprise Manager.

- **Full** - Has complete access to the secured object.
- **Access** - Can connect to this realm.
- **Configure** - Can set run-time parameters on the realm.
- **Channels** - Can add and delete channels on the realm.
- **Realm** - Can add and remove realms from the realm.
- **Admin API** - Can use the nAdminAPI package.
- **Manage DataGroups** - Can add and remove data groups from the realm.
- **Pub DataGroups** - Can publish to data groups, including the default one, on the realm.
- **Own DataGroups** - Can add, delete, and publish to data groups even when they were not created by the user.

The green check icon shows that a subject is permitted to perform the operation. The minimum requirement for a client to use a realm is the Access permission. Without this permission for the default `*@*` subject, any Universal Messaging client whose subject does not appear in the ACL list cannot establish a session to the realm server.

About Channel ACL Permissions

After a client has established a session to a Universal Messaging realm and is successfully authenticated, and the subject has the correct user entitlements, in order to perform operations on a channel, the subject must have the appropriate ACL permissions for the channel. Each channel has an associated ACL that contains a list of subjects and a set of permissions the subject is given for operations on the channel.

You can add, remove, and modify ACL entries, and view ACL permissions on the **ACL** tab for a channel in the Enterprise Manager. A green check icon indicates the permissions given to each subject.

A subject in the ACL list can have the following permissions to perform operations on the channel:

- **Manage ACL** - Can get and manage the list of ACL entries.

Note:

This permission is a combination of two permissions at the Administration API level. The boolean `setModify()` API function allows or denies permission to change an ACL value, and the boolean `setList()` API function allows or denies permission to access the current list of ACLs. If both of these functions return the value `true`, Manage ACL is allowed, otherwise Manage ACL is not allowed. If the green check icon is displayed in the **Manage ACL** field, the corresponding two API functions for this field are set to `true`. If you remove the green check icon, this sets the corresponding two API functions for this field to `false`.

- **Full** - Has complete access to the secured object.
- **Purge** - Can delete events on the channel.
- **Subscribe** - Can subscribe to events on the channel.
- **Publish** - Can publish events to the channel.
- **Named** - Can connect using a durable subscriber.

The green check icon shows that a subject is permitted to perform the operation. For example, if the subject `*@*` has only Subscribe permissions for a channel, this means that any client that has successfully established a session and has obtained a reference to this channel within its application code can only subscribe to the channel and read events.

About Queue ACL Permissions

After a client has established a session to a Universal Messaging realm and is successfully authenticated, and the subject has the correct user entitlements, in order to perform operations on a queue, the subject must have the appropriate ACL permissions for the queue. Each queue has an associated ACL that contains a list of subjects and a set of permissions the subject is given for operations on the queue.

You can add, remove, and modify ACL entries, and view ACL permissions on the **ACL** tab for a queue in the Enterprise Manager. A green check icon indicates the permissions given to each subject.

A subject in the ACL list can have the following permissions to perform operations on the queue:

- **Manage ACL** - Can get and manage the list of ACL entries.

Note:

This permission is a combination of two permissions at the Administration API level. The boolean `setModify()` API function allows or denies permission to change an ACL value, and the boolean `setList()` API function allows or denies permission to access the current list of ACLs. If both of these functions return the value `true`, Manage ACL is allowed, otherwise Manage ACL is not allowed. If the green check icon is displayed in the **Manage ACL** field, the corresponding two API functions for this field are set to `true`. If you remove the green check icon, this sets the corresponding two API functions for this field to `false`.

- **Full** - Has complete access to the secured object.
- **Purge** - Can delete events on the queue.
- **Peek** - Can snoop on the queue (non-destructive read).
- **Push** - Can publish events to the queue.
- **Pop** - Can consume events on the queue (destructive read).

The green check icon shows that a subject is permitted to perform the operation. For example, if the subject `*@*` has only Peek permissions for a queue, this means that any client that has successfully established a session and has obtained a reference to this queue within its application code can only snoop on the queue and read events.

Adding and Removing ACL Subjects

You add and remove subjects and security groups to the Access Control List (ACL) of a Universal Messaging realm on the **Security > ACL** tab in the Enterprise Manager. You perform the same operations for a store (a channel or queue) on the **ACL** tab of the store.

➤ To add or remove an ACL subject for a realm or store in the Enterprise Manager

1. Select the realm or store and go to the **ACL** tab.
2. Perform one of the following actions:
 - To add a subject to the ACL table, click **Add**, specify the subject, and click **OK**.
 - To add an existing security group to the ACL table, click **Add Group**, select a group, and click **OK**.
 - To remove an entry from the ACL table, select the entry in the table and click **Delete**.

Modifying ACL Permissions

Consider the following information when you make changes to ACL permission for a subject in the Enterprise Manager:

- Any ACL changes made by other Enterprise Manager users, or by any programs using the Universal Messaging Admin API to modify ACLs, are received by all other Enterprise Managers. The reason for this is that ACL changes are automatically sent to all Universal Messaging Admin API clients, including the Enterprise Manager.
- Any changes made to a realm or store ACL where the realm or store is part of a cluster are replicated to all other cluster realms or stores.

➤ To modify the ACL permissions for a subject in the Enterprise Manager

1. Select the realm or store where you want to modify the ACL permissions and go to the **ACL** tab.
2. To add or remove a permission for a subject, click in the respective cell in the ACL table.
3. Click **Apply**.

Creating Security Groups

Security groups can contain a list of subjects (username and host pairs) as well as other security groups. After you create a security group, you can add it to the ACL list of a realm or store. In this way, you can assign ACL permissions to a set of users through a single entry in the ACL list.

Membership of security groups can be altered dynamically, and the changes are reflected in the permissions for all ACLs where the security group is an entry in the ACL list.

As with all ACLs in Universal Messaging, permissions are cumulative. This means that, for example, if a user is in a group that has publish permissions on a channel, but not subscribe permissions, the user cannot subscribe on the channel. Then, if an ACL entry is added on the channel for this specific username/host pair with subscribe permissions but no publish permissions, the user will be able to both subscribe and publish on the channel.

➤ To create a security group in the Enterprise Manager

1. Select the realm for which you want to create a security group and go to the **Security > Groups** tab.
2. Click **Add Group** and specify a name for the new group.
3. Do any of the following to add members to the group:
 - To add a subject, click **Add Member** and specify the subject.

- To add an existing group, click **Add Group To Group** and select a group from the list.

About Interface VIA Lists

Each interface defined on a Universal Messaging realm server can have an associated ACL list, known as a VIA list. The VIA list enables you to define users who can connect to the Universal Messaging realm using a specific protocol *via* a specific interface.

For example, if a realm has an HTTP (nhp) interface running on port 10000 and a sockets (nsp) interface running on port 15000, and you want all external clients to connect using the nhp interface, and all internal clients to connect using the nsp interface, you can create separate lists of subjects (username and host pairs) associated with the nhp and nsp interfaces.

This ensures that any user who tries to connect using the nsp interface, who is not part of the nsp interface VIA list, but exists in the nhp VIA list, will be rejected and will not be able to establish a connection via nsp. The same applies for the nhp interface. This enables you to tie specific users to specific interfaces.

The default behavior for all interfaces is that when no VIA lists exist on any defined interfaces, all users can connect on any interface. When a user subject exists on an interface, that subject cannot use any other interface other than the one in which they are listed.

VIA lists offer an extra level of security that enables server administrators to define a strict approach to who can connect to the realm via specific protocols. This is particularly useful if, for example, you run many services on a single Universal Messaging realm and want to ensure that specific clients or groups of clients use completely separate interfaces.

Managing Interface VIA Lists

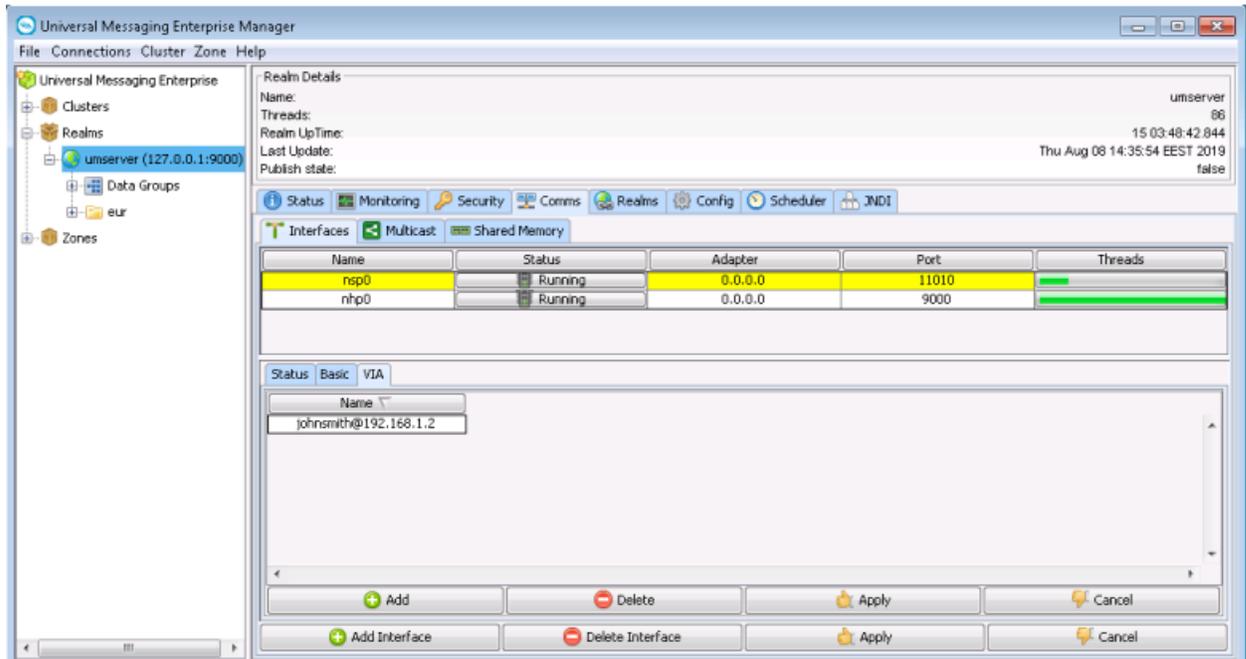
➤ **To view and manage the VIA list for an interface in the Enterprise Manager**

1. Select the realm on which the interface is running and go to the **Comms > Interfaces** tab.
2. Select the interface in the table of interfaces and click the **VIA** tab.
3. Perform any of the following actions:
 - To add a subject to the VIA list, click **Add** and specify the subject as a username and host pair.
 - To delete a subject from the VIA list, select the subject in the list and click **Delete**.
4. Click **Apply** for the changes to take effect.

VIA List Example

The following image shows the result of adding the user "johnsmith@192.168.1.2" to the VIA list of the interface "nsp0" that uses the sockets protocol on port "11010".

As with all Universal Messaging ACLs, wildcards are fully supported so that, for example, `*@192.168.1.2` or `johnsmith@*` are both valid VIA rules.



Integration with JNDI

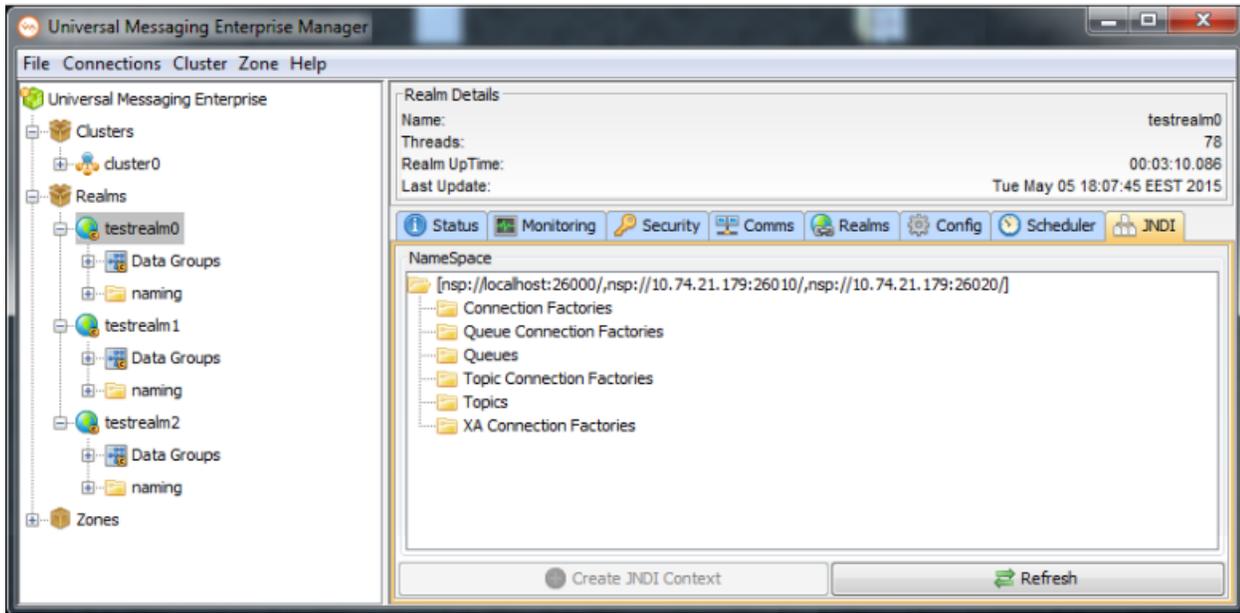
About Integration with JNDI

Universal Messaging supports integration with JNDI through its own provider for JNDI. The Universal Messaging provider for JNDI enables clients using *Universal Messaging Provider for JMS* to locate references to JMS administered objects.

As with all Java APIs that interface with host systems, JNDI is independent of the system's underlying implementation. The Universal Messaging provider for JNDI stores object references in the Universal Messaging channel `/naming/defaultContext`. The channel represents the initial context for JNDI and locates references to the objects using a channel iterator. Note that if a realm is part of a cluster, the channel is created on all cluster realm servers. This ensures that any object references bound into the context are available on each realm server in the cluster.

You manage the provider for JNDI on the **JNDI** tab for a realm in the Enterprise Manager. On the **JNDI** tab, you can create the provider and initial context for JNDI, TopicConnectionFactory and QueueConnectionFactory references for JMS, as well as references to topics and queues.

The following image shows the JNDI namespace tree on the JNDI panel for a clustered realm after the initial context was created.



The Initial JNDI Context and the JNDI Namespace

When you select the **JNDI** tab for a realm in the Enterprise Manager, if the initial JNDI context does not exist, you are prompted to create it. The Enterprise Manager creates the channel `/naming/defaultContext` in the namespace tree of the realm and, if the realm is part of a cluster, on all other cluster realms. When the channel is initially created, full permissions are assigned to the first client who creates it and to all other users and clients who want to use the channel.

Important:

If you delete the `/naming/defaultContext` channel, the JNDI context is destroyed and all existing JNDI references are lost.

After you create the JNDI context, you can view the JNDI namespace tree. The root of the tree is the JNDI provider URL. In the case of a cluster, the root shows a comma-separated list of RNAME values for each server in the cluster.

If you are using a *horizontal scalability* connection factory, the URL syntax enables you to specify multiple connection URLs, where each connection URL can specify either a standalone realm or a cluster.

The JNDI namespace tree also contains the following folders:

- Connection Factories
- Queue Connection Factories
- Queues
- Topic Connection Factories
- Topics
- XA Connection Factories

To update the contents of the JNDI namespace tree with any changes done outside the current Enterprise Manager instance, click **Refresh**.

Creating Connection Factories

You can create the following types of connection factories in the JNDI namespace of a realm in the Enterprise Manager:

- Connection factory - connects to both topics and queues
- Topic connection factory - connects to topics
- Queue connection factory - connects to queues
- XA connection factory

➤ To create any type of connection factory in the Enterprise Manager

1. Select a realm and go to the **JNDI** tab.
2. Right-click the relevant connection factory node, and then select the context menu to create a new connection factory.
3. In the Add JNDI Connection Factory dialog box, specify values for the following fields:

Field	Description
Name	Required. The name of the new connection factory, for example <code>connectionFactory1</code> .
Connection URL (RNAME)	<p>Required. The Universal Messaging realm URL for binding the connection factory, for example <code>nsp://localhost:9000</code>. You can specify a cluster of realms by typing a comma-separated list of connection URLs, for example <code>nsp://localhost:9000,nsp://localhost:9010</code>.</p> <p>To use a <i>horizontal scalability</i> connection factory for round-robin message delivery, you can specify several connection URLs, where each connection URL can point to a standalone realm or a cluster. For information about the URL syntax, see “The URL Syntax of a Horizontal Scalability Connection Factory” on page 134.</p> <div style="background-color: #f0f0f0; padding: 5px;"> <p>Note: Round-robin delivery is not supported for XA connection factories.</p> </div>
Durable Type	<p>Supported only for the connection factory and topic connection factory types. The durable type for durable consumers. Values are:</p> <ul style="list-style-type: none"> ■ Named - Only one active consumer can exist at a time.

Field	Description
	<ul style="list-style-type: none">■ Shared - Multiple durable consumers can connect to the same durable subscription and can consume messages in a round-robin manner.■ Serial - Multiple durable consumers can connect to the same durable subscription and can consume messages in a serial manner.

4. Click **OK**.

The URL Syntax of a Horizontal Scalability Connection Factory

Horizontal scalability connection factories enable clients to publish messages to a set of servers or consume messages from a set of servers in a round-robin manner. The following rules apply to the round-robin URL syntax:

- Each connection URL must be enclosed in round brackets.
- Each set of brackets must contain at least one valid connection URL.
- There is no limit to the number of sets of brackets in the URL.
- Each set of brackets indicates a unique connection, and the realm names in each set of brackets are supplied unchanged to the underlying implementation.

Consider the following examples:

- (UM1)(UM2)(UM3)(UM4) - Indicates four standalone realms, UM1, UM2, UM3, and UM4, so four connections will be constructed here.
- (UM1,UM2)(UM3,UM4) - Indicates two clusters, one consisting of UM1 and UM2, and the other consisting of UM3 and UM4, so only two connections will be constructed here.
- (UM1)(UM2,UM3)(UM4) - Indicates one cluster consisting of UM2 and UM3, and two standalone realms: UM1 and UM4. A total of three connections will be constructed here.

Note:

Round-robin delivery is not supported for XA connection factories.

For more information about *horizontal scalability* connection factories, see the section "Overview of the Provider for JMS" in the Developer Guide.

Creating References to Topics and Queues

When JMS clients use the Universal Messaging initial context for JNDI, they also reference the topics and queues from the same initial context. In order for the clients to access these objects, you must create references to each topic and queue. Creating such references also creates the underlying channel or queue if it does not already exist, or you can create a reference that corresponds to a

channel or queue that already exists. Note that channels or queues created in this way have the same default permissions as channels or queues created manually.

To create a reference to a channel or queue on the **JNDI** tab of a realm, right-click the **Queues** or **Topics** node, then select **New Queue** or **New Topic** and specify a name for the queue or topic.

For example, if you create a topic named `rates`, and no corresponding channel existed previously, the Enterprise Manager creates the `rate` topic under the **Topics** node in the JNDI namespace as well as a new channel named `rates` that corresponds to it.

Viewing and Editing JNDI Settings of a Connection Factory

➤ To view and edit JNDI setting for any type of connection factory

1. Go to the **JNDI** tab of a realm and expand the connection factory node.
2. Double-click the connection factory you want to edit.

The Edit JNDI Connection Factory dialog box displays the required JNDI settings including the connection factory name, connection URL, and durable type for topic and generic connection factories. You can also view any optional parameters defined for the connection factory.

3. Edit the connection factory settings as necessary:
 - For the required JNDI connection factory parameters, edit the value of the parameter.
 - For optional parameters, edit the key, value, or data type in the optional parameter table.
 - To add a new optional parameter, under **Property Input**, specify a key, value, and type for the parameter, then click **Add**. The new parameter is added to the optional parameter table.
 - To remove an optional parameter, select the parameter in the optional parameter table, right-click it, and select **Remove Property**.
4. Click **OK**.

The Enterprise Manager publishes an event that contains the new JNDI settings to the `/naming/defaultContext` channel and purges the old event that contained the previous settings.

Using Channel Snoop to View JNDI Settings

JNDI settings are stored as events on the `/naming/defaultContext` channel. You can use the channel snoop functionality to view the individual events on the channel.

To snoop on the `/naming/defaultContext` channel in the Enterprise Manager, select the channel, go to the **Snoop** tab, and click **Start**. The Snoop panel displays the events representing any JNDI entries that have been created. When you select an event, you can see the event content and the corresponding JNDI context information given to the JMS applications that require it.

Note:

You cannot use the snoop functionality to edit and republish JNDI settings on the `/naming/defaultContext` channel. You can edit JNDI settings only on the **JNDI** tab of a realm. If an old event on the channel is purged while you are viewing the Snoop panel, you must stop the snoop and then start it again to see the changes reflected on the panel.

For more information about channel snooping, see [“Snooping on a Channel” on page 107](#).

Administering TCP Interfaces, IP Multicast, and Shared Memory

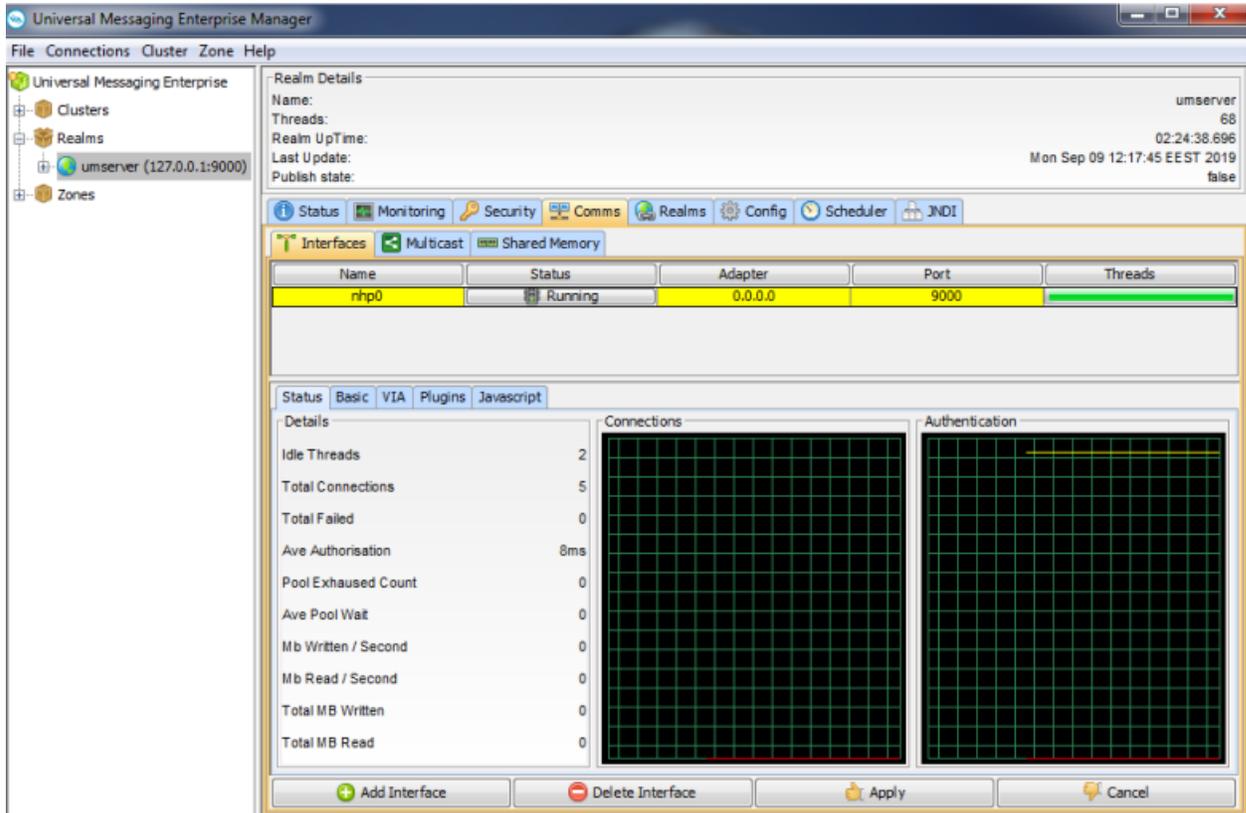
About Working with Interfaces

Interfaces within a Universal Messaging realm server define a protocol, a network interface, and a port number. When a Universal Messaging client connects to a realm using an RNAME, the client actually connects to an interface that has been created on the Universal Messaging realm.

If a machine that is running a Universal Messaging realm has multiple physical network interfaces, with different IP addresses, you can bind specific protocols to specific ports. This way you can segment incoming network traffic to specific clients. For example, if a realm is running on a machine that has an external Internet-facing network interface, as well as an internal interface, you can create a Universal Messaging interface that uses `nhp` or `nhps` on port 80 or 443, respectively, using the external facing interface. However, if you do not want to segment network traffic for specific protocols, you can choose to bind to all known network interfaces to the specified protocol and port.

The default Universal Messaging interface is `nhp`. The default `nhp` interface enables clients to connect to it using not only the `nhp` protocol, but also the `nsp` protocol. If you do not specify a port for the default interface when you install or create a Universal Messaging server instance, the default port is 9000.

You create, configure, and manage interfaces on the **Comms > Interfaces** tab for a realm in the Enterprise Manager, as shown in the following image.



Creating Interfaces

The default Universal Messaging interface is nhp. The nhp interface enables clients to connect to it using not only the nhp protocol, but also the nsp protocol. If you do not specify a port for the default interface when you install or create a Universal Messaging server instance, the default port is 9000. The default interface binds to 0.0.0.0, or to all known interfaces.

If you plan to add an SSL-enabled interface, either nsp or nhps, you must perform additional steps. For more information, see [“Creating an SSL-Enabled Interface” on page 144](#).

➤ To add a new interface in the Enterprise Manager

1. Expand the **Realms** node and select the realm on which you want to create the interface.
2. Go to the **Comms > Interfaces** tab and click **Add Interface**.
3. Specify values for the following interface attributes:

Attribute	Value
Interface Protocol	The protocol of the interface. Values are: <ul style="list-style-type: none"> ■ NSP (Socket Protocol)

Attribute	Value
	<ul style="list-style-type: none"> ■ NHP (HTTP Protocol) ■ NSPS (Secure Socket Protocol) ■ NHPS (Secure HTTP Protocol) ■ RDMA Protocol. Requires network adapters that support remote direct memory access (RDMA).
Interface Port	The port on which the interface binds.
Interface Adapter	The physical network to which to bind, expressed either as an IP address or a hostname. The default is 0.0.0.0, or all known interfaces. You can use the hostname if you want the interface to be independent of the underlying IP address. For details about using the 0.0.0.0 IP address, see “Usage of 0.0.0.0 When Defining Interfaces” on page 138.
Auto Start	Whether the interface starts automatically after it is created, and after the server is restarted.

4. Click **OK**.

The Enterprise Manager adds the new interface to the interfaces table. The interfaces table shows the following attributes for an interface:

- **Name** - Defined as protocol + *n*, where *n* is a unique sequence number for the interfaces for that protocol.
- **Status** - Shows whether the interface is in status 'Running', 'Stopped', or 'Error'. The error status indicates that the interface did not start due to an error.
- **Adapter** - The interface adapter.
- **Port** - The interface port.
- **Threads** - An indicator for the number of threads that the interface has free to accept connections. A full green bar denotes all threads are free.

5. Define basic attributes for the interface.

Various default attributes for the interface are displayed in the **Comms > Interfaces > Basic** panel. You may wish to modify these default values to suit your requirements. The attributes are described in the section [“Basic Attributes for an Interface” on page 139.](#)

Usage of 0.0.0.0 When Defining Interfaces

When a client connects to a server, the server will deliver all interfaces that are marked as "advertised" (this is, set using the check box **Advertise Interface** on the **Comms > Interfaces > Basic** tab). If you have interfaces bound to 0.0.0.0 (that is all known interfaces), then this will

include both 127.0.0.1 (localhost) and any IP address that the server node has. This means that the client will receive at least two interfaces that it will use to reconnect to the realm.

If the client connection is restarted, the client will attempt to iterate through this list of interfaces until it is successful on reconnection. However, the order of iterating through this list is not deterministic.

On a successful connection, the Universal Messaging realm server will construct a client principal name in the format <userName>@<IP-Address> used to check permissions on realm resources, such as channels or queues, where <IP-Address> is the IP address of the machine where the client is running. The IP address of the client in turn depends on the network interface the client used to connect to the server. In the example with a server adapter bound on all network interfaces (0.0.0.0), a local client (on the same machine as the server) may connect over the loopback interface to the server (localhost) so the connection will come from 127.0.0.1, but that same client may also connect over the real network interface, in which case the IP address will be the address of this network interface. Thus one and the same client may end up with different principal names when reconnecting to the realm server. This may lead to permission issues if a resource's default ACL has been established using one principal name, and is subsequently accessed with a different principal name after a reconnection.

To avoid this, you should either create the interface for an external IP address (not "localhost") or ensure that required ACLs are configured.

Basic Attributes for an Interface

Each interface on a Universal Messaging realm has a number of configurable attributes that determine the interface behavior. The following sections describe the attributes that you can configure on the **Basic** tab for an nsp, nsps, nhp, or nhps interface.

Accept Threads

Each Universal Messaging realm interface contains a server socket. The **Accept Threads** attribute corresponds to the number of threads that are able to perform the `accept()` for a client connection. The `accept()` operation on a Universal Messaging interface performs the handshake and authentication for the client connection. For more heavily utilised interfaces, the accept threads will need to be increased. For example, on an nhp (http) or nhps (https) interface, each client request corresponds to a socket `accept()` on the interface, and so the more requests being made, the busier the interface will be, so the accept threads needs to be much higher than that of say an nsp (socket) interface. Socket interfaces maintain a permanent socket connection, and so the `accept()` is only performed once when the connection is first authenticated.

Advertise Interface

All interfaces that are advertised by a realm server are available to users (with the correct permissions) of the Universal Messaging Admin API. This property specifies whether the interface is indeed advertised to such users.

Alias

Each interface on a Universal Messaging realm server can have an associated alias in the form of *host:port*. This alias can be specified here.

For information on interface plugins, see [“Plugins” on page 151](#).

For information on adding VIA rules for an interface, see [“About Interface VIA Lists” on page 130](#).

Allow Client Connections

If this attribute is activated, clients are allowed to connect to the realm over this interface.

If this attribute is deactivated, clients are not allowed to connect to the realm over this interface. Note that Administration API connections, such as the Enterprise Manager, count as client connections, so at least one of the available interfaces should allow such Administration API connections. If a realm has been defined with only one interface and you deactivate the **Allow Client Connections** attribute on the interface, this setting will be ignored. This is because essential administration tools like the Enterprise Manager would not otherwise be able to access the realm.

Allow for InterRealm

If this attribute is activated, the interface can be used for any of the following kinds of internal communication (i.e. Universal Messaging's own message passing) between realms:

- Inter-realm communication: between realms in the same cluster.
- Inter-zone communication: between realms in a zone.
- Inter-cluster communication: between realms in connected clusters.

Important:

If you do not activate this attribute for the interface, the interface cannot be used for any of the above scenarios.

If you activate **Allow for InterRealm** and deactivate **Allow Client Connections** for the same interface, the interface can **only** be used for internal communication between realms, so no communication with an external client is possible using such an interface. There are situations in which this configuration can be useful. For more information, see the section [“Setting Up Inter-Realm Communication” on page 88](#).

Autostart Interface

The **Autostart** attribute specifies whether the interface is started automatically when the Universal Messaging realm server is started. When this option is not selected, the interface must be started manually in order for it to be used by connecting clients. Please note that if **Autostart** is not set it must be started either manually or using the Universal Messaging Administration API whenever after the realm is started.

If **Autostart** is selected then the interface will be started once the **Apply** button is pressed.

Auth Time

The **Auth Time** attribute corresponds to the amount of time a client connection using this interface can take to perform the correct handshake with the realm server. For example, the default is 10000 milliseconds, but for some clients connecting on slow modems, and who are using the nhps (https) protocol, this default **Auth Time** may need to be increased. If any client connection fails to perform the handshake in the correct timeframe, the connection is closed by the realm server.

Backlog

The **Backlog** attribute specifies the maximum size of the incoming IP socket request queue. The operating system that the realm server is running on may specify a maximum value for this property. When the maximum queue size is reached the operating system will refuse incoming connections until the request queue reduces in size and more requests can be serviced. For more information on this value, please see the system administration documentation for your Operating System.

Enable HTTP 1.1

Enable the usage of HTTP 1.1 protocol on this interface.

Enable NIO

Specify whether NIO should be used for this interface.

Receive Buffersize

This specifies the size of the receive buffer on the socket.

Select Threads

The **Select Threads** option specifies the number of threads allocated to monitor socket reads/writes on the interface if NIO is enabled. When a socket needs to be read, these threads will fire and pass on the request to the read thread pool. If the socket is blocked during a write, then when the socket is available to be written to, these threads will fire and the request will be passed on to the write thread pool. The number of select threads should not typically exceed the number of cores available.

Send Buffersize

This specifies the size of the send buffer on the socket.

Starting and Stopping Interfaces

To start or stop an interface for a realm in the Enterprise Manager, go to the **Comms > Interfaces** tab for the realm and in the interfaces table, double-click in the interface row or, alternatively, click in the **Status** column. In the dialog box that opens, click the **Start** or **Stop** button.

Modifying Interface Attributes

Each interface within a Universal Messaging realm has a number of common configuration attributes that you can modify using the Enterprise Manager.

➤ To modify the attributes for an interface

1. On the **Comms > Interfaces** tab for a realm, select the interface that you want to modify.
2. Click the **Basic** tab for the interface and modify the interface attributes as required.

For a description of each attribute, see [“Basic Attributes for an Interface” on page 139](#).

3. Click **Apply** for the changes to take effect.

The interface is restarted. Any clients connected to the interface automatically reconnect to it after the restart.

JavaScript Configuration Properties

Universal Messaging HTTP and HTTPS (nhp and nhps) interfaces have configuration properties specific to their communication with web clients using JavaScript. You configure these properties on the **JavaScript** tab for an nhp or nhps interface.

JavaScript Interface Properties

Property Name	Description
Enable JavaScript	Recommended Setting: Enabled Allows JavaScript clients to connect on this interface.
Enable WebSockets	Recommended Setting: Enabled Toggles the ability for clients to communicate with the server using the HTML WebSocket Protocol on this interface.
CORS Allow Credentials	Recommended Setting: Enabled Toggles the server sending an "Access-Control-Allow-Credentials: true" header in response to XHR-with-CORS requests from the client. This is required if the application, or website hosting the application, or intermediate infrastructure such as reverse proxy servers or load balancers, uses cookies. Leave this enabled unless recommended otherwise by support. Disabling this will in most environments prevent all CORS-based drivers from working correctly.

Property Name	Description
CORS Allowed Origins	<p>Recommended Setting: *</p> <p>A comma-separated list of the host names (and IP addresses, if they appear in URLs) of the server/s that host your JavaScript application's HTML. Use an * (asterisk) as a wildcard value if you do not want to limit the hosts that can serve applications to clients. This server will accept and respond with the required Access-Control-Allow-Origin header when requests originate from a hostname in this list. This header allows CORS enabled transport mechanism to bypass cross site security restrictions in modern browsers.</p> <p>It is important that this is set appropriately, or approximately half of the communication drivers available to JavaScript clients will fail.</p>
Enable GZIP for LongPoll	<p>Recommended Setting: Enabled</p> <p>This will allow the server to gzip responses sent to LongPoll clients. This can reduce network utilization on servers with many LongPoll clients. It increases CPU resource utilization.</p>
GZIP Minimum Threshold	<p>Recommended Setting: 1000</p> <p>The minimum message size is bytes required for the server to begin compressing data sent to LongPoll clients.</p>
Long Poll Active Delay	<p>Recommended Setting: 100</p> <p>The time between clients sending long poll requests to the server in milliseconds. Reducing this may reduce latency up to a certain threshold but will increase both client and server memory, CPU and network usage.</p>
Long Poll Idle Delay	<p>Recommended Setting: 25000</p> <p>The time between clients sending long poll when the client is in idle mode. A client is put in idle mode when no communication takes place between client and server for a period of time. Reducing this may be necessary if a client is timing out owing to local TCP/IP settings, proxy settings, or other infrastructure settings, but will result in higher memory, CPU and network usage on both the client and the server. It is however vital that this value is lower than the timeouts used in any intermediate proxy server, reverse proxy server, load balancer or firewall. Since many such infrastructure components have default timeouts of as little as 30 seconds, a value of less than 30000 would be prudent. If long polling client sessions continually disconnect and reconnect, then lower this value.</p>
Custom Header Config	<p>Header Key/Value pairs which are sent in the HTTP packets to the client.</p>

About SSL Interfaces

Universal Messaging supports SSL encryption by providing the nsps and nhps SSL-enabled protocols. These protocols enable clients to connect to a Universal Messaging realm server running a specific protocol on a port using all or specific physical network interfaces.

Defining an SSL-enabled interface ensures that clients can connect to a realm server only after presenting the correct SSL credentials and authenticating with the server.

SSL authentication occurs within the Universal Messaging handshake, which uses the JVM's JSSE provider. This ensures that any unauthorized connections are SSL-authenticated before any Universal Messaging specific operations can be performed.

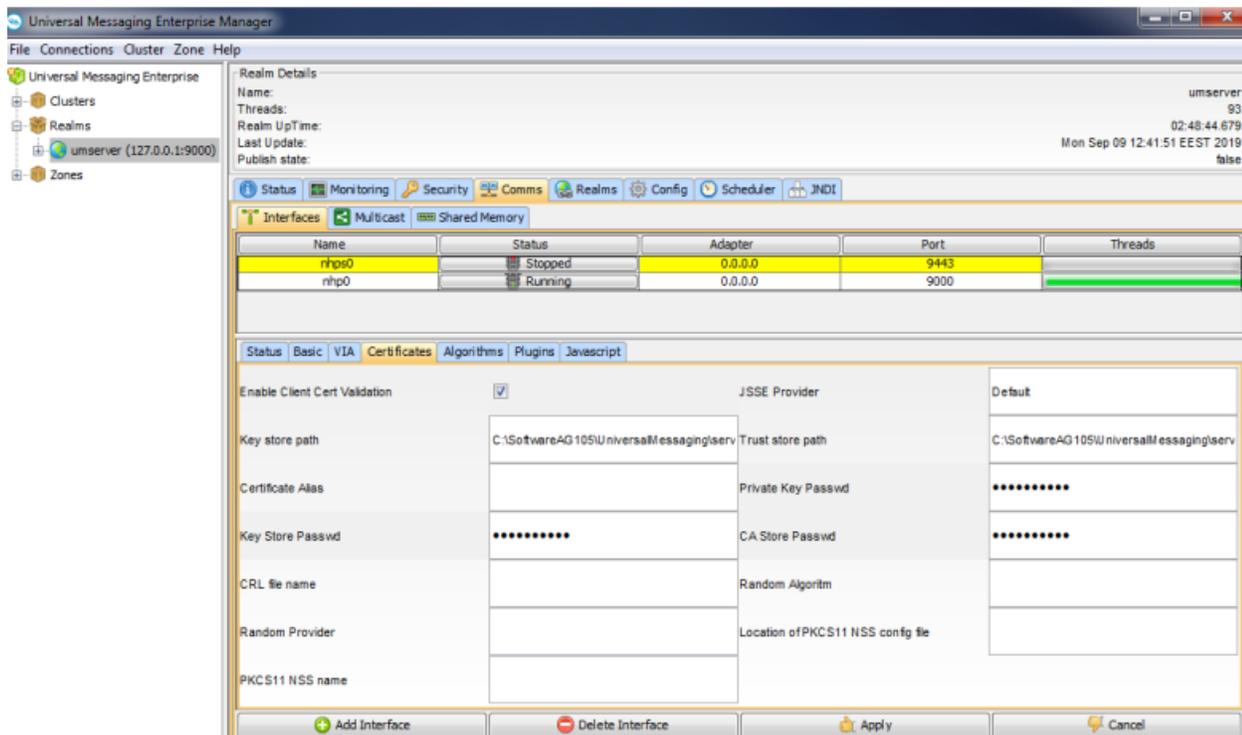
You create an SSL-enabled interface in the same way as you create a non-SSL interface, but you must configure several SSL-related attributes in addition to the basic attributes.

For information about how to create an SSL interface using the Universal Messaging Enterprise Manager, see [“Creating an SSL-Enabled Interface” on page 144](#).

Creating an SSL-Enabled Interface

To add an SSL-enabled interface using the Enterprise Manager, first create an nsps or nhps interface as described in [“Creating Interfaces” on page 137](#).

The following image shows an nhps (HTTPS) interface listening on port 9443.



Click the **Certificates** tab. The values for the **Key store path** and **Trust store path** fields are specified by default. Universal Messaging provides a utility called Certificate Generator that can generate sample .jks files containing certificates bound to localhost, for the server, the client, and the truststore used by JSSE. The example uses the sample jks files to show how to create an SSL interface. For detailed information about generating certificates, see [“How to Generate Certificates for Use” on page 146](#).

The **Key store path** field must contain something similar to:

```
c:\SoftwareAG_directory\UniversalMessaging\server\umserver\bin\server.jks
```

which is the path to the sample Java keystore for the server, bound to localhost.

The **Trust store path** field must contain something similar to the following:

```
c:\SoftwareAG_directory\UniversalMessaging\server\umserver\bin\nirvanacacerts.jks
```

Then specify the value `password` for **Key Store Passwd** and **CA Store Passwd**. This is the password for both the server keystore and the CA (truststore) keystore.

Next, go to the **Basic** tab and select the **Autostart Interface** option to start the interface automatically when the Universal Messaging realm server starts.

Note:

If you intend to use an SSL interface for inter-realm communication, you should ensure that the **Allow for InterRealm** option is selected and the **Allow Client Connections** option is cleared. Alternatively, if you intend to use an SSL interface for communication between clients and the realm, you should ensure that the **Allow for InterRealm** option is cleared and the **Allow Client Connections** option is selected. For information about inter-realm communication, see [“Setting Up Inter-Realm Communication” on page 88](#).

Click **Apply** to save your changes and start the interface. If the network interface fails to start, inspect the Universal Messaging log file.

There is no limit to the number of network interfaces that can be added to a realm and each can have its own configuration, such as SSL chains, applied. This enables you to isolate customers from each other while still using only one Universal Messaging realm server.

The sample Java keystores work only when you use the loopback interface of your realm server host. If you want to provide SSL capabilities for remote connections, you must have your own keystores and valid certificate chains.

Connecting to an NHPS Interface

To connect to an nhps interface on a Universal Messaging server in the Enterprise Manager, you configure the following truststore and client keystore properties in the `Software AG_directory\UniversalMessaging\java\instance_name\bin\Admin_Tools_Common.conf` file of the server:

- `set.default.CAKEYSTORE=<path_to_truststore>` - Required.
- `set.default.CAKEYSTOREPASSWD=<truststore_password>` - Required.

- `set.default.CKEYSTORE=<path_to_client_keystore>` - Required only when client authentication is enabled.
- `set.default.CKEYSTOREPASSWORD=<keystore_password>` - Required only when client authentication is enabled.

The certificates must be in .jks (java keystore) or PKCS12 format.

If you choose not to specify a client keystore certificate and a keystore password, you must comment out these properties using a hash (#) in the `nenterprisemgr.conf` and `Admin_Tools_Common.conf` files.

Important:

If you have these properties configured both in the *Software AG_directory* \UniversalMessaging\java*instance_name*\bin\nenterprisemgr.conf file and Admin_Tools_Common.conf file, the values in nenterprisemgr.conf override the values in Admin_Tools_Common.conf. Software AG recommends that you configure the properties in the Admin_Tools_Common.conf file.

In addition, optionally, you can configure an nhps url to which clients connect by default. You specify the url as a value of the `-DRNAME` property in the `nenterprisemgr.conf` file of the server, for example:

```
wrapper.java.additional.3=-DRNAME=nhps://umserver:8000
```

Enabling Client Authentication

You use the **Enable Client Cert Validation** check box on the **Interfaces > Certificates** tab to enable or disable client authentication for an nhps or an nsps interface on a Universal Messaging server. If you enable client authentication, you must specify the client keystore certificate and keystore password as properties in the `nenterprisemgr.conf` or the `Admin_Tools_Common.conf` file of the server instance.

How to Generate Certificates for Use

Generating Demo / Development Certificates

To generate a demo SSL certificate, you can use the Java keytool utility or the Universal Messaging Certificate Generator utility.

Note:

The Certificate Generator utility is deprecated in Universal Messaging v10.2 and will be removed in a future version of the product.

The third-party Java keytool utility can be used to create and handle certificates. Keytool stores all keys and certificates in a keystore.

The Universal Messaging Certificate Generator utility can be used to generate a self signed server certificate, a self signed client certificate, and a trust store for the above two.

You can run the Certificate Generator from the Start Menu on Windows by selecting the server/<realm name>/Create Demo SSL Certificates.

Alternatively, you can open a server command prompt and run the utility as required for your platform:

- Windows systems:

```
CertificateGenerator.exe
```

- UNIX-based systems:

```
./CertificateGenerator
```

- OS X:

```
./CertificateGenerator.command
```

This will generate three files:

- client.jks : Self signed certificate you could use if you have client certificate authentication enabled.
- server.jks : Self signed certificate with a CN=localhost . Please note: You can only connect to interfaces using this by specifying a localhost RNAME due to the HTTPS protocol restrictions.
- nirvanacacerts.jks: Keystore that contains the public certificate part of the 2 key pairs above. This should be used as a trust store by servers and clients.

It is also possible to customize some elements of these certificates stores such as the password, the host bound to the server CN attribute and they key size. This can be done by passing the following optional command line arguments to the Certificate Generator:

- Windows systems:

```
CertificateGenerator.exe <password> <host> <key size>
```

- UNIX-based systems:

```
./CertificateGenerator <password> <host> <key size>
```

- OS X:

```
./CertificateGenerator.command <password> <host> <key size>
```

Generating Production Certificates

To obtain a real SSL certificate, you must first generate a CSR (Certificate Signing Request). A CSR is a body of text that contains information specific to your company and domain name. This is a public key for your server.

The Java keytool utility can be used to create and handle certificates. Keytool stores all keys and certificates in a keystore. For a detailed description of keytool please see its documentation.

Step 1: Create a keystore

Use the keytool to create a keystore with a private/public keypair.

```
keytool -genkey -keyalg "RSA" -keystore keystore -storepass password -validity 360
```

You will be prompted for information about your organization. Please note that when it asks for "User first and last name", please specify the hostname that Universal Messaging will be running on (e.g. www.yoursite.com).

Step 2: Create a certificate request

Use the keytool to create a certificate request.

```
keytool -certreq -keyalg "RSA" -file your.host.com.csr -keystore keystore
```

This will generate a file containing a certificate request in text format. The request itself will look something like this :

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBtTCCAR4CAQAwTELMAkGA1UEBhMCVVMxDzANBgNVBAgTBmxxvbmRvbjEPMA0GA1UEBxMGbG9u
ZG9uMRQwEgYDVQQKEWtteS1jaGFubmVsczEMMAoGA1UECxMDYm16MSAwHgYDVQQDEXdub2RlMjQ5
Lm15LWNoYW5uZWxzLmNvbTCBnzANBeddiegkqhkiG9w0BAQEFAAOBjQAwYkCgYEAycg0MJ7PXkQM9sLj
1vWa8+7Ce0FDU4tpcMXLL647dwok3uUGXuaz72DmFtb80ninjawingsjxrMBDK9fXG9hqfDvxWGU0DEgbn+Bg
03XqmUbyI6eMzGdf0vTyBFSeQIinigomontoyaU9Ahq1T7C6zLryJ9n6XZTW79E5UcbSGjoNAPB0gVOCPKBs7/CR
hZECaWEEAAaAAMA0GCSqGSIb3DQEBAUAA4GBAB7TkFzQr+KvsZCV/pP5IT0c9tM58vMXkds2J77Y
Op3AueMVixRo14ruLq1obbTudhc385pPgHLz07QHEKI9gJnM5pR9yLL72zpVKPQ9X0ImShv005Tw
0os69BjZew8LTV60v4w3md47IeGE9typGGxBWscVbXzB4sgVlv0JtE7b
-----END NEW CERTIFICATE REQUEST-----
```

Step 3: Submit your certificate request to a certificate supplier

Certificate vendors will typically ask you to paste the certificate request into a weborder form. This will be used as a public key to generate your private key. Please include the (BEGIN and END) tags when you paste the certificate request.

Please note that a cert of PKCS #7 format is required so that it can be imported back into keytool. (step 4)

The certificate vendor will then provide you with a certificate which that will look something like this:

Please paste this certificate into a file called your.host.com.cer [Note. please include the (BEGIN and END) tags]

```
-----BEGIN PKCS #7 SIGNED DATA-----
MIIFpAYJKoZIhvcNAQcCoIIFLTCBZECAQExADALBgkqhkiG9w0BBWgGggV5MIIC
2DCCAkGgAwIBAgICErYwDQYJKoZIhvcNAQEEBQAwwYkCgYEAycg0MJ7PXkQM9sLj
dGUgQ2VydGlmawNhdGlvbWJEXMBUGA1UECxM0VEVTVCBURVNUIFRFRU1QxHDAaBgNV
BAMTE1RoYXd0ZSBUZUN0IENBIFJvb3QwHhcNMDQwOTA2MTYwOTIwWhcNMDQwOTI3
MTYwOTIwWjB1MQswCQYDVQQGEWJVVzEPMA0GA1UECBMGbG9uZG9uMQ8wDQYDVQQH
EwZsb25kb24xZDASBgNVBAoTC215LWNoYW5uZWxzMQwwCgYDVQQLEWNoXDAe
BgNVBAMTF25vZGUyNDkubXktY2hhbm5lbHMUy29tMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDjYdQwns9eRAz2wuPW9Zrz7sJ7QUNTi2lwxeUvrjt3CiTe5QZe
5rPvYOYw1vw6PGswEMr19cb2Gp80/FYbJtQMSBuf4GA7deqZRvIjp4zMZ1/S9PIE
VJ5AhT0CGrVPsLr0WvIn2fpdlnbv0TLRxtIa0g0CkE6BU4I8oGzv8JGfKQIDAQAB
o2QwYjAMBgNVHRMBAf8EAjAAMDGA1UdHwQsMCowKKAmoCSGImh0dHA6Ly93d3cu
```


1. Expand the **Realms** node and select the realm to which you want to add a multicast configuration.
2. Go to the **Comms > Multicast** tab and click **Add Multicast Config**.
3. Specify values for the following multicast attributes:

Attribute	Description
Multicast Address	The multicast IP address.
Adapter Address	The address of the network adapter that you configured for multicast.

4. Click **OK**.

You can view the new multicast configuration in the multicast configurations table.

5. Click the **Basic** tab of the multicast configuration and do any of the following:
 - To use the configuration for data groups, select **Use for DataGroups**.
 - To use the configuration for inter-realm communication in a cluster, select **Use for Clusters**.
6. Click **Apply**.

Considerations When Using Multicast

Depending on the purpose of your multicast configuration, consider the following information:

- To use your multicast configuration for data groups, when you create a data group in the Enterprise Manager, you must select the **Multicast** option. For more information about how to create a data group, see [“Creating Data Groups” on page 121](#). If you create your data groups programmatically, when you call `nSession.createDataGroup`, you must pass an additional boolean that marks the data group as multicast-enabled.
- To use your multicast configuration for inter-realm communication in a cluster, you must set the **Use for Clusters** option on each cluster realm that has multicast configured. The multicast address can be the same for all realms, or you can choose a different multicast address for each realm. With this feature enabled, each realm will know the multicast address for each of the other realms in the cluster and will listen on these addresses for inter-realm cluster communication.

Advanced Multicast Settings

The default settings for the multicast configurations you create are aimed at providing the lowest possible latency. With this in mind, the configuration is such that the multicast client will ack every one second, and the server will maintain a list of un-acked events (default 9000). If the publish rate exceeds 9000 per second, the delivery rates might be quite irregular. This is due to the fact that the client will only acknowledge every one second, and so the server will automatically

back off the delivery until it receives an acknowledgement from the client and can therefore clear its unacknowledged queue. If this happens, you can change both the Unacked Window Size to be greater than 9000 and the Keep Alive Interval (ack interval) to be less than one second.

Adding a Shared Memory Configuration

➤ To add a shared memory (SHM) configuration in the Enterprise Manager

1. Expand the **Realms** node and select the realm to which you want to add a shared memory configuration.
2. Go to the **Comms > Shared Memory** tab and click **Add SHM Config**.
3. Specify values for the following shared memory attributes:

Attribute	Description
Path	The directory in which the files required for SHM communication are created. When choosing a path, ensure that the local user id of the server can access this directory, for example, <code>/dev/shm</code> requires root / super user access, otherwise SHM communication will not work. The default value is <code>/dev/shm</code> .
Buffer Size	The size of the allocated memory in bytes that a connection will use. Creates a file of the same size, which is used for mapping. The default value is <code>1024000</code> .
Timeout	The idle timeout for a connection in milliseconds. If no activity is detected on the connection, the connection is closed. The default value is <code>20000</code> .

4. Click **OK**.

You can view and edit the new SHM configuration in the shared memory configurations table. To edit an attribute, double-click in the row and type a new value, then click **Apply**.

Plugins

The Universal Messaging realm server supports the concept of plugins within the context of the NHP or NHPS protocol. The plugins are initiated when the underlying Universal Messaging driver receives an HTTP/S packet that is not part of the standard Universal Messaging protocol. At this point, it passes the request over to the plugin manager to see if there is any registered plugin interested in the packet's URL. If there is such a plugin, the request is forwarded to this plugin for processing. Universal Messaging supports several plugins.

Note:

The following server plugins are deprecated in Universal Messaging v10.2 and will be removed in a future version of the product: *Graphics, XML, Proxy passthrough, Servlet*.

Configuring a Plugin

You can configure a plugin using both the Administration API and the Enterprise Manager.

Before adding a plugin, you must create the nhp or nhps interface that will use the plugin on the realm where you want to run the plugin. For more information, see [“Creating Interfaces” on page 137](#).

After you create the interface, proceed as follows to add a plugin using the Enterprise Manager:

1. In the navigation frame, select the realm where you want to add the plugin.
2. In the **Realm Details** frame, navigate to the list of defined interfaces for the realm, using **Comms > Interfaces**.
3. Select the interface from the table of configured interfaces.
4. Select the tab **Plugins** from the interface configuration panel.
5. Click **Add Plugin**. This displays the plugin configuration dialog, which enables you to choose which plugin you want to add.

The URL Path

When you configure a plugin, you are required to add a URL path. The URL path is what the realm server uses to determine if the request is destined for a plugin. If the server name and path within the URL supplied in the plugin configuration dialog match the server name and path within the request to a configured plugin, the request is passed to the correct configured plugin for processing.

For example, if a request with a URL of `http://realmServer/pluginpath/index.html` is made to the server, the file path will be extracted, i.e. `pluginpath/index.html`, and the configured plugins will be scanned for a match. If there is a file plugin configured with a URL path `pluginpath`, then this plugin will get a request for `index.html`.

Similarly, if a request with a URL of `http://realmServer/pluginpath/pictures/pic1.jpg` is received, then the same file plugin will get a request for `pictures/pic1.jpg`.

When adding the Health Monitor plugin, the URL path should always include a trailing slash, for example `http://localhost:9000/test/`.

File Plugin

The file plugin enables the Universal Messaging realm server to serve static web pages. This can be used for example to have the realm server serve applets and supported files without the need for a dedicated web server. For example, if you are running a file plugin on your realm server host called `webhost`, on an nhp interface running on port 80, you could type in a URL within a web

browser `http://webhost:80/index.html` which will return the index page defined within the file plugin's base path directory.

This enables the realm server to act as a web server and can even be used to serve applets to client browsers that may directly communicate with the realm server and publish and consume events from channels.

Important:

The root file directory that the file plugin points to using the `BasePath` parameter can be any disk location. All files under that location are potentially visible to any HTTP client that can connect to the Universal Messaging realm server. We would recommend that you do not point the file plugin to a directory that contains any sensitive data, without also configuring suitable access controls. These could be at the network level (restricting network access to the server), in the file plugin configuration (it supports HTTP basic authentication with a username/password file) or by using file permissions at the Operating System level (so that sensitive data cannot be read by the realm server process). Or of course a combination of these.

Configuration

Once you have created the file plugin on the interface you require it on, you can then select it from the **Plugins** panel for the selected interface and enter values as you wish for the configuration parameters.

The file plugin requires configuration information defining its behavior as well as the location of the files it is required to serve to the clients. Below is a table that shows each configuration parameter and describes what it is used for.

Parameter Name	Description	Default Value
BufferSize	Size of the internal buffer to use to send the data.	1024
BasePath	Path used to locate the files.	The <code>UniversalMessaging/doc</code> directory under the product installation directory.
DefaultName	If no file name is specified which file should be returned.	<code>index.html</code>
FileNotFoundPage	Name of the file to send when file cannot be located	None.
UserFile	Name of the file containing the usernames and passwords.	None.
Security Realm	Name of the authentication realm	None.
MimeType	Name of the file to load the mime type information from. The format of this file is : <code><mime-type> <fileExtension></code>	Built in types used.

Parameter Name	Description	Default Value
CachedObjects	Number of objects to store in the cache	100
CacheObjectSize	Size in bytes that can be stored in the cache	20K
SeparateAccessandErrorLogs	Choose true to have separate log files for the access and error logs.	FALSE

For example, on the **Comms > Interfaces** tab, you can have an nhp interface running on port 9000. This interface has a file plugin configured with the default settings and its URL path is /. The default BasePath setting is the `UniversalMessaging/doc` directory in the file hierarchy for your local product installation, which is where the default product installation places the Universal Messaging API docs. Once the plugin is created, you can click the **Apply** button, which will restart the interface and enable the new file plugin.

From a browser, it is now possible to enter the URL `http://localhost:9000/` which will then render the default `index.html` page from the `UniversalMessaging/doc` directory for the API docs.

XML Plugin

You can use the XML plugin to query the realm server, its queues and channels. It returns the data in XML format. This plugin also supports style sheets, so the XML can be transformed into HTML or any format required. For example, a client can publish XML data onto a Universal Messaging realm's channel, then using a standard web browser, get the server to transform the XML into HTML via a stylesheet, thereby enabling the web browser to view events on the realm.

This functionality enables realm data to be viewed from a channel without any requirement for a Java client. All that is required is for the client to have a browser.

Important:

Never include XSL code from untrusted sources into the plugin's XSL code, as this can lead to a security risk for the client browser (or other client application) accessing the plugin. The Universal Messaging realm server itself is not at risk, since it does not execute the plugin's XSL code.

Configuration

Once you have created the XML plugin on the interface you require it on, you can then select it from the **Plugins** panel for the selected interface and enter values as you wish for the configuration parameters.

The XML plugin requires configuration information relating to its behavior as well as the entry point in the namespace for the channels you wish to make available to serve to the clients. Below is a table that shows each configuration parameter and describes what it is used for.

Parameter Name	Description	Default Value
ChannelRoot	Name of the channel or folder to render. /	
Security Realm	Name of the authentication realm	None.
StyleSheet	Name of the style sheet file to use to process the resulting XML.	None. If you specify a filename without a path, the default path is <code>UniversalMessaging/server/<InstanceName>/bin</code> under the product installation root location.
UserFile	Name of the file containing the usernames and passwords	None.

Note:

As a starting point for creating your own stylesheet, you can use the stylesheet `xml2html.xsl` that is supplied in the `UniversalMessaging/doc/style` directory in the file hierarchy for your local product installation.

For example, on the **Comms > Interfaces** tab, you can have an nhp interface running on port 9005. This interface has an XML plugin configured to use the `xml2html.xsl` stylesheet and its URL path as `/xml`. The default ChannelRoot setting is `/`, which is the root of the namespace, i.e. all channels. Once the plugin is created, you can click the **Apply** button, which will restart the interface and enable the new XML plugin.

From a browser, you can now enter the URL `http://localhost:9005/xml/` which will render the realm information page using the stylesheet.

The XML plugin will determine whether the events on the channel contain byte data or dictionaries and return the relevant elements within the XML document. The stylesheet applied to the XML document then examines each element to find out how to render it within the browser. Each event on the channel or queue is shown in the table with event ID, its size in bytes and links to either the byte data or the dictionary. These links are generated by the stylesheet. Clicking on the data or dictionary links will again return an XML document from the XML plugin that will be rendered to show either the base64 encoded event data or the event dictionary.

Proxy Passthrough Plugin

The Proxy Passthrough Plugin can be used to forward http(s) requests from specific URLs to another host. For example, if you want to forward requests from one realm to another realm, or to another web server, you can use the proxy passthrough plugin.

This functionality enables realms to act as a proxy to forward URL requests to any host that accepts http(s) connections.

Configuration

Once you have created the proxy passthrough plugin on the interface you require it on, you can then select it from the plugins panel for the selected interface and enter values as you wish for the configuration parameters.

The proxy passthrough plugin requires configuration information relating to the host and port that requests will be forwarded to. Below is a table that shows each configuration parameter and describes what it is used for.

Parameter Name	Description	Default Value
HostName	Host name of the process that requests for the URL will be forwarded to	
Port	Port on which the requests will be sent to the host	80

For example, on the **Comms > Interfaces** tab, you can have an nhp interface running on port 9000. This interface has a proxy passthrough plugin configured to redirect requests from this interface using the URL path of `/proxy` and will forward these requests to any File Plugins and XML Plugins located on the `productionmaster` realm's nhp interface running on port 9005.

From a browser, it is now possible to enter the URL `http://localhost:9000/proxy/` which will redirect this request to the interface on the `productionmaster` realm interface running on port 9005. This will display the details of the `productionmaster` realm as if you had specified the URL `http://productionmaster:9005/` in your browser.

REST Plugin

The REST plugin allows access to the Universal Messaging REST API, and can be enabled on any HTTP or HTTPS (NHP or NHPS) interface. The Universal Messaging REST API is designed for publishing, purging, and representing events published on channels and queues in a JSON initial representation.

The Universal Messaging REST API supports three different HTTP commands. GET is used for representations of events, POST for publishing, and PUT for purging. JSON supports byte arrays and dictionary events for publishing, which map to native Universal Messaging event types. Two MIME types are available: text and application.

Configuration

After you create a REST plugin for an interface, you can select the plugin on the plugins panel for that interface and enter values for the configuration parameters.

Parameter Name	Description	Default Value
AddUserAsCookie	Add the username to the session's cookies.	Blank

Parameter Name	Description	Default Value
AuthParameters	A list of key=value strings, which are passed to the Authenticator's init() function.	Blank
Authenticator	Classname of Authenticator to use. If blank, no authentication is used.	Blank
EnableStatus	Enables Realm status details. Default is disabled, for security reasons.	False
GroupNames	A comma separated list of groups. The user must be a member of at least one in order to be granted access.	Blank
IncludeTypeInfo	Includes type information for event dictionaries.	False
NamespaceRoot	Name of the namespace folder to be used as root.	Blank
ReloadUserFileDynamically	If set to true and authentication is enabled, fAuthenticator.reload() is called on each request.	True
RoleNames	A comma-separated list of names. The user must have at least one to gain access.	Blank
Security Realm	Name of the authentication realm.	Blank
SessionTimeout	Time in seconds to time-out inactive http sessions.	300

The REST plugin supports WADL documentation which is accessible through the HTTP OPTIONS command. Once you have completed setting up your REST plugin, you can verify it works by opening a browser to the NHP interface in the mount URL path, and appending the query string `?method=options`. For example, for an NHP interface running on port 9000 on localhost, and having the plugin mounted on `/rest`, open a browser to `http://localhost:9000/rest/API?method=options`.

Following this will display an HTML version of the full Universal Messaging REST API documentation which is generated by applying an XSL processor to the WADL XML document. The XML document itself can be obtained by accessing the plugin URL without the `?method=options` query string. For example, the curl command line tool can be used as follows:

```
curl -XOPTIONS http://localhost:9000/rest/API
```

What follows is a summary of the three HTTP commands for JSON, and what functionality each provides, as well as detailed examples of requests and responses for each command.

GET

Provides JSON representations of channels/queues or events in a channel or queue as specified by the ChannelOrQueue parameter. The parameter is represented by the URI Path following the REST Plugin mount.

If the value supplied corresponds to a Universal Messaging namespace container, the representation returned is a list of channels and queues present in the container. If the value supplied corresponds

to a channel or queue then the representation returned is a list of events. Finally if the value supplied does not correspond to either a container or a channel / queue a 404 response will be returned with no body.

Available response representations:

- [“application/json” on page 158](#)

POST

Allows publishing of an event to a channel or queue specified by the ChannelOrQueue parameter, which is represented by the URI Path following the REST plugin mount. For example `http://localhost:9000/rest/API/json/testchannel` expects a JSON byte or dictionary event to be published to channel **testchannel**.

Acceptable request representations:

- [“application/json” on page 161](#)

Available response representations:

- [“application/json” on page 163](#)

PUT

Allows purging of 1 or more events already published on a channel or queue specified by the ChannelOrQueue parameter, which is represented by the URI Path following the REST Plugin mount. For example `http://localhost:9000/rest/API/json/testchannel` expects a request to purge events to be published to channel **testchannel**. Purging can be specified by EID and selector.

Acceptable request representations:

- [“application/json” on page 163](#)

Available response representations:

- [“application/json” on page 163](#)

JSON Representation

A JSON representation of channels/queues or events in a channel or queue as specified by the ChannelOrQueue parameter.

If the parameter points to an existing container, the response code is 200 and the response looks like this:

```
{
  "Channels":
  [ {
    "EventsConsumed": "0",
    "EventsPublished": "0",
    "LastEventID": "-1",
    "Name": "testqueue",
    "NumberEvents": "0",
```

```

    "fqdn": "http://localhost:8080/rest/API/json/testqueue"
  }, {
    "EventsConsumed": "0",
    "EventsPublished": "0",
    "LastEventID": "212",
    "Name": "testchannel",
    "NumberEvents": "0",
    "fqdn": "http://localhost:8080/rest/API/json/testchannel"
  } ],
  "Comment": "Constructed by my-channels Nirvana REST-Plugin :
    Wed Mar 02 11:38:30 EET 2011",
  "Name":
  "Nirvana-RealmServer-ChannelList",
  "NumberOfChannels": "2",
}

```

If the REST plugin is configured to include realm status, some additional information about the realm is presented:

```

{
  "Channels":
  [ {
    "EventsConsumed": "0",
    "EventsPublished": "0",
    "LastEventID": "-1",
    "Name": "testqueue",
    "NumberEvents": "0",
    "fqdn": "http://localhost:8080/rest/API/json/testqueue"
  }, {
    "EventsConsumed": "0",
    "EventsPublished": "0",
    "LastEventID": "212",
    "Name": "testchannel",
    "NumberEvents": "0",
    "fqdn": "http://localhost:8080/rest/API/json/testchannel"
  } ],
  "Comment": "Constructed by my-channels Nirvana REST-Plugin :
    Wed Mar 02 11:38:30 EET 2011",
  "Name": "Nirvana-RealmServer-ChannelList",
  "NumberOfChannels": "2",
  "Realm": {
    "FreeMemory": "503291048",
    "RealmName": "nirvana6",
    "Threads": "104",
    "TotalConnections": "1",
    "TotalConsumed": "0",
    "TotalMemory": "530186240",
    "TotalPublished": "0"
  }
}

```

If the parameter points to an existing channel or queue, the response code is 200 and the response looks like this:

```

{
  "ChannelName": "http://localhost:8080/rest/API/json/testsrc",
  "Comment": "Constructed by my-channels Nirvana REST-Plugin : Wed
  Mar 02 12:19:22 EET 2011",
  "Events":

```

```
[ {
  "ByteLink": "http://localhost:8080/rest/API/json/testsrc?Data=Byte&EID=213",
  "DataSize": "9",
  "EID": "213",
  "Tag": "Test Tag",
  "hasByte": "true"
}, {
  "DictionaryLink":
    "http://localhost:8080/rest/API/json/testsrc?Data=Dictionary&EID=214",
  "EID": "214",
  "hasDictionary": "true"
} ],
"FirstEvent":
"http://localhost:8080/rest/API/json/testsrc?Data=Dictionary&EID=first",
"LastEID": "214",
"LastEvent": "http://localhost:8080/rest/API/json/testsrc?Data=Dictionary&EID=last",
"Name": "Nirvana-RealmServer-EventList",
"NextLink": "http://localhost:8080/rest/API/json/testsrc?EID=215",
"StartEID": "213"
}
```

You can follow the provided links to view individual events. If you choose to look at an individual byte event, the response code is 200 and the response looks like this:

```
{
  "ChannelName": "http://localhost:8080/rest/API/json/testsrc",
  "Comment": "Constructed by my-channels Nirvana REST-Plugin :
    Wed Mar 02 12:21:46 EET 2011",
  "Data": "VGVzdCBCb2R5",
  "EID": "213",
  "Name": "Nirvana-RealmServer-RawData",
  "Tag": "Test Tag"
}
```

If you choose to look at an individual dictionary event, the response code is 200 and the response looks like this:

```
{
  "dictionary":
  {
    "testboolean": [true],
    "testcharacter": ["a"],
    "testdictionary": [
      {
        "testboolean": [true],
        "testcharacter": ["a"],
        "testdouble": [1],
        "testfloat": [1],
        "testinteger": [1],
        "testlong": [1],
        "teststring": ["teststringvalue"]
      }
    ],
    "testdouble": [1],
    "testfloat": [1],
    "testinteger": [1],
    "testlong": [1],
    "teststring": ["teststringvalue"],
    "teststringarray": [
      "one",

```

```

        "two",
        "three"
    ]
  },
  "isPersistent": true
}

```

If the rest plugin is configured to include type information in representations, dictionary event representations will include them. In this case, responses looks like this:

```

{
  "dictionary":
  {
    "testboolean": [ true, 3 ],
    "testcharacter": [ "a", 6 ],
    "testdictionary":
    [ {
      "testboolean": [ true, 3 ],
      "testcharacter": [ "a", 6 ],
      "testdouble": [ 1, 2 ],
      "testfloat": [ 1, 5 ],
      "testinteger": [ 1, 4 ],
      "testlong": [ 1, 1 ],
      "teststring": [ "teststringvalue", 0 ]
    }, 9 ],
    "testdouble": [ 1, 2 ],
    "testfloat": [ 1, 5 ],
    "testinteger": [ 1, 4 ],
    "testlong": [ 1, 1 ],
    "teststring": [ "teststringvalue", 0 ],
    "teststringarray":
    [ [
      "one",
      "two",
      "three"
    ], 100, 0 ]
  },
  "isPersistent": true
}

```

Finally, if the parameter points to a non-existing container, or channel or queue, the response code is 404 without a response body.

JSON PUBLISH REQUEST

JSON Byte events can be represented as follows:

```

{
  "data": "VGZzdCBCb2R5",
  "isPersistent": true,
  "tag": "VGZzdCBUYWc="
}

```

Important:

data and tag should always be submitted in base64 encoded form.

JSON DOM events can be represented as follows:

```
{
  "data": "VGVzdCBCb2R5",
  "isDOM": true,
  "isPersistent": true,
  "tag": "VGVzdCBUYWc="
}
```

Important:

data and tag should always be submitted in base64 encoded form.

JSON dictionary events can be represented as follows:

```
{
  "dictionary":
  {
    "testboolean": [true],
    "testcharacter": ["a"],
    "testdictionary":
    [{
      "testboolean": [true],
      "testcharacter": ["a"],
      "testdouble": [1],
      "testfloat": [1],
      "testinteger": [1],
      "testlong": [1],
      "teststring": ["teststringvalue"]
    }],
    "testdouble": [1],
    "testfloat": [1],
    "testinteger": [1],
    "testlong": [1],
    "teststring": ["teststringvalue"],
    "teststringarray":
    [[
      "one",
      "two",
      "three"
    ]]
  },
  "isPersistent": true
}
```

Optionally, dictionary events can include type information (see [“Types” on page 164](#)). This allows the Universal Messaging REST API to preserve these types when publishing the event. The types are defined as byte constants to keep typed dictionary events compact in size.

Dictionary events (with type information) can be represented as follows:

```
{
  "dictionary":
  {
    "testboolean": [ true, 3 ],
    "testcharacter": [ "a", 6 ],
    "testdictionary":
    [ {
      "testboolean": [ true, 3 ],
      "testcharacter": [ "a", 6 ],
      "testdouble": [ 1, 2 ],
      "testfloat": [ 1, 5 ],
```

```

        "testinteger": [ 1, 4 ],
        "testlong": [ 1, 1 ],
        "teststring": [ "teststringValue", 0 ]
    }, 9 ],
    "testdouble": [ 1, 2 ],
    "testfloat": [ 1, 5 ],
    "testinteger": [ 1, 4 ],
    "testlong": [ 1, 1 ],
    "teststring": [ "teststringValue", 0 ],
    "teststringarray":
    [ [
        "one",
        "two",
        "three"
    ], 100, 0 ]
    },
    "isPersistent": true
}

```

Important:

byte[] types should always be submitted in base64 encoded form.

JSON PUBLISH RESPONSE : A JSON representation to indicate the status of attempting to publish an event to the channel or queue specified by the ChannelOrQueue parameter.

If the publish call is successful, the response code is 201 and the response looks like this:

```

{
  "Response": "OK"
}

```

If the publish call fails for any reason, the response code is 400 and the response looks like this:

```

{
  "errorcode": "ErrorCode",
  "errormessage": "Error Message",
  "response": "failInput"
}

```

JSON PURGE REQUEST : A JSON representation of a Purge Request that indicates the event(s) to purge.

A JSON purge request looks as follows:

```

{
  "endEID": 20,
  "purgeJoins": false,
  "selector": "",
  "startEID": 10
}

```

JSON PURGE RESPONSE : A JSON representation to indicate the status of attempting to purge an event to the channel or queue specified by the ChannelOrQueue parameter

If the purge call is successful, the response code is 200 and the response looks like this:

```

{
  "Response": "OK"
}

```

```
}
```

If the purge call fails for any reason, the response code is 400 and the response looks like this:

```
{  
  "errorcode": "ErrorCode",  
  "errormessage": "Error Message",  
  "response": "failInput"  
}
```

Types

Type	ID
String	0
Long	1
Double	2
Boolean	3
Integer	4
Float	5
Character	6
Byte	7
Short	8
Dictionary	9
Array	100

Servlet Plugin

The servlet plugin enables the Universal Messaging realm server to serve Java servlets.

Configuration

Once you have created the servlet plugin on an interface, you can then select it from the **Plugins** panel for the interface and configure the plugin parameters.

The servlet plugin requires configuration information relating to its behavior, as well as the location of the servlets it is required to serve to the clients. Below is a table that shows each configuration parameter and describes what each is used for.

To ensure security, the `EnforceConfigFile` option can be set to true; this allows only those classes specified in the configuration file to be loaded. Alternatively, the `EnforceStrictClassLoader` option

can be set; this prevents classes being loaded from different class loaders to that of the servlet, and thereby also prevents arbitrary classes from being loaded.

Parameter Name	Description	Default Value
AddUserAsPlugin	Add the username to the session cookies.	false
AuthParameters	List of key=value string which is passed to authenticators init function.	
AddUserAsPlugin	Classname of authenticator to use, leave blank (default) for default	
EnableClassReload	Automatically reload servlet class if it changes	true
EnforceConfigFile	If true, only servlets within the ServletConfigFile will be executed.	true
EnforceStrictClassLoader	If true, only servlets loaded by the initial class loader will be executed. Any classes loaded by parent loader will be ignored.	true
GroupNames	A comma separated list of groups to which a user must be a member of to be granted access.	
MimeType	Name of the file to load the mime type information from. The format of the file is same as the apache mime types.	
Properties	File containing the servlet properties. The file should be a java properties file that contains one property per line prefixed with the full class name. For example for a servlet class com.example.Servlet defining a property called RNAME you should have a line as follows: com.example.Servlet.RNAME=nsp://localhost:9000	
ReloadUserFileDynamically	If true, the user file will get reloaded on each auth request.	true
RoleNames	A comma separated list of groups to which a user must have one to be granted access.	
Security Realm	Name of the authentication realm.	
Servlet Config File	File which contains all the valid servlets which will run. The file should be a text file containing one full servlet class name per line, indicating only these should be allowed to run. For example having a single line com.example.Servlet would mean that only that	

Parameter Name	Description	Default Value
	servlet will be allowed to run irrespective of how many exist in the server classpath.	
Servlet Path	Directory in which to locate servlet classes	
SessionTimeout	Time in seconds before timeout of servlet session not in use.	

Health Monitor Plugin

The Health Monitor plugin adds an HTTP REST endpoint to the URL of the session to which the realm server is connected. This allows clients to query the current state of the realm server. The endpoint defines the "liveness" of the server. The plugin returns the result of the health checks that run on the server at periodic intervals.

Adding the plugin to the realm server

The plugin can be added to a realm server using either of the following methods:

- Using the **Add Plugin** feature in the **Comms > Interfaces > Plugins** dialog of the Enterprise Manager. In this case, you define the name of the new URL endpoint in the **URL Path** field of the **Add Plugin** dialog.

See the section [“Plugins” on page 151](#) for details.

- Using the command line tool `AddHealthMonitorPlugin`. In this case, you define the name of the new URL endpoint using the `-mountpath` argument of the tool.

For details of running this command line tool, see the section [“Syntax: Miscellaneous Tools” on page 429](#).

Server monitoring tasks

The realm server runs four different tasks at regular intervals on the server to monitor the health status of the server:

- **Memory monitor Task (MemoryHealthMonitor):**

This task monitors the memory status of the server and will produce an alert/error as soon as any memory related issues are found. The task checks the heap and direct memory usage, and if the usage exceeds a threshold value of 95%, then it is considered as an error and the error will be reported and logged.

The server is not considered to be unhealthy when the first such error occurs; instead a server is considered unhealthy only if the memory monitor task returns an error 3 times consecutively.

- **Stalled-Tasks Monitor Task (StalledTasksMonitor):**

If any thread pool has more than 5 stalled tasks, this is considered an error, but the status is only reported as unhealthy if the error occurs 5 times consecutively.

- **Cluster state monitor Task (ClusterStateMonitor):**

If a server is configured to be part of a cluster, and the last time that the server successfully joined the cluster is more than 600000 milliseconds (10 minutes) ago, then the server is considered to be unhealthy.

- **Server round trip Task (ServerRoundTripMonitor):**

The server round trip checks the processing time in a cluster. `nClusterRoundTripEvent` events are synchronous events that measure the processing time in a cluster. The realm server sends these events into the cluster and records the time it takes to complete the processing in cluster. If the event takes more than 30 seconds to complete processing and get acknowledged, then that is considered to be an error. Not getting an acknowledgement back for this event is also considered to be an error. If 5 consecutive such errors, the server is considered to be unhealthy.

Server responses

If the server is fully operational, and is an active member of the cluster (if a cluster is configured), the query returns a response "OK" of the following form:

```
{"ServerStatus":"OK","ServerStatusDetails":{}}
```

Even if the return code is "OK", the response can contain additional information (in JSON format). This information can be in the form of useful statistics, or as an indication that the server is approaching certain limits.

If the server is not fully operational, the query returns a status "ERROR" with an appropriate description of the problem, for example:

```
{"ServerStatus":"ERROR","ServerStatusDetails":
  {"MemoryHealthMonitor":
    "Max threshold of used Heap memory is exceeded, Heap memory used - 338 MB"
  }
}
```

Exporting and Importing Realm XML Configurations

You can export a realm configuration into an XML representation, and then import the XML representation into another realm, using the Enterprise Manager. The XML export and import functionality enables you to automatically configure multiple realms based on a standard structure, for example when you want to clone realms and their internal structure.

You can export specific elements of a realm or the entire realm structure. The exported XML can contain any or all of the following elements:

- Clusters
- Realm access control lists (ACLs)
- Channels

- Channel ACLs
- Queues
- Queue ACLs
- Configuration parameters
- JNDI assets
- Durables
- Interfaces
- Plugins
- Scheduling information

After you exported the realm configuration, you can import the XML into another realm. Importing the XML automatically creates and configures the objects selected for import from the XML file. The export and import marshal the realm objects from their Administration API representation into XML and back again.

Exporting a Realm Configuration into an XML File

Use the following procedure to export a realm or specific elements of a realm into an XML file.

➤ To export a realm configuration into an XML file

1. In the Enterprise Manager, go to **Realms** and select the realm that you want to export.
2. Right-click the realm node and select **Export Realm to XML**.
3. In the **Export to** field, specify the path to the file to which you want to export the realm configuration.
4. Select the realm elements to export:
 - Select **Export all** to export the entire realm structure.
 - Select one or more options under **Realm Export**, **Channels**, **Cluster Export**, **Interfaces**, **Queues**, and **Data Groups** to export specific elements of the realm structure.
5. Click **OK**.

Importing a Realm Configuration from an XML File

Before importing an XML representation of a realm configuration to another realm, you must export the realm configuration as described in [“Exporting a Realm Configuration into an XML File” on page 168](#).

Use the following procedure to import a realm or specific elements of a realm from an XML file into another realm.

➤ **To import a realm configuration from an XML file**

1. In the Enterprise Manager, go to **Realms** and select the realm into which you want to import the XML configuration.
2. Right-click the realm node and select **Import Realm from XML**.
3. In the **Import from** field, specify the path to the file from which you want to import the realm configuration.
4. Select the realm elements to import:
 - Select **Import all** to import the entire realm structure.
 - Select one or more options under **Realm Export, Channels, Cluster Export, Interfaces, Queues**, and **Data Groups** to import specific elements of the realm structure.
5. Click **OK**.

Version Compatibility Issues

Store types

In Universal Messaging v10.5, the store types Simple, Paged, Transient and Offheap were removed.

For details of how v10.5 deals with these store types, refer to the section *Removed Features in v10.5* in the v10.5 Release Notes.

Sample XML File for Import

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<NirvanaRealm name="realm0" exportDate="2021-01-12+02:00"
  comment="Realm configuration from realm0"
  version="BuildIdentifier" buildInfo="BuildIdentifier">
  <RealmConfiguration>
    <ConfigGroup name="Audit Settings">
      <ConfigItem name="ChannelACL" value="true"/>
      <ConfigItem name="ChannelFailure" value="true"/>
      <ConfigItem name="ChannelMaintenance" value="false"/>
      <ConfigItem name="ChannelSuccess" value="false"/>
      <ConfigItem name="DataGroup" value="false"/>
      <ConfigItem name="DataGroupFailure" value="false"/>
      <ConfigItem name="DataStream" value="false"/>
      <ConfigItem name="Group" value="true"/>
      <ConfigItem name="GroupMembers" value="true"/>
      <ConfigItem name="InterfaceManagement" value="true"/>
      <ConfigItem name="JoinFailure" value="true"/>
    </ConfigGroup>
  </RealmConfiguration>
</NirvanaRealm>
```

```

<ConfigItem name="JoinMaintenance" value="true"/>
<ConfigItem name="JoinSuccess" value="false"/>
<ConfigItem name="QueueACL" value="true"/>
<ConfigItem name="QueueFailure" value="true"/>
<ConfigItem name="QueueMaintenance" value="false"/>
<ConfigItem name="QueueSuccess" value="false"/>
<ConfigItem name="RealmACL" value="true"/>
<ConfigItem name="RealmFailure" value="true"/>
<ConfigItem name="RealmMaintenance" value="true"/>
<ConfigItem name="RealmSuccess" value="false"/>
<ConfigItem name="SnoopStream" value="false"/>
</ConfigGroup>
<ConfigGroup name="Client Timeout Values">
  <ConfigItem name="EventTimeout" value="60000"/>
  <ConfigItem name="HighWaterMark" value="3000"/>
  <ConfigItem name="LowWaterMark" value="1000"/>
  <ConfigItem name="QueueAccessWaitLimit" value="200"/>
  <ConfigItem name="QueueBlockLimit" value="500"/>
  <ConfigItem name="QueuePushWaitLimit" value="200"/>
  <ConfigItem name="TransactionLifeTime" value="20000"/>
</ConfigGroup>
<ConfigGroup name="Cluster Config">
  <ConfigItem name="ClientQueueSize" value="1000"/>
  <ConfigItem name="ClientQueueWindow" value="100"/>
  <ConfigItem name="ClientStateDelay" value="5000"/>
  <ConfigItem name="ClusterMode" value="0"/>
  <ConfigItem name="DisableHTTPConnections" value="true"/>
  <ConfigItem name="DisconnectWait" value="30000"/>
  <ConfigItem name="EnableMulticast" value="true"/>
  <ConfigItem name="EnableStoreRecoveryRetry" value="true"/>
  <ConfigItem name="EnginePipelineSize" value="2"/>
  <ConfigItem name="FormationTimeout" value="120000"/>
  <ConfigItem name="HeartBeatInterval" value="120000"/>
  <ConfigItem name="InitialConnectionTimeout" value="30000"/>
  <ConfigItem name="IsCommittedDelay" value="5000"/>
  <ConfigItem name="MasterRequestTimeout" value="60000"/>
  <ConfigItem name="MasterVoteDelay" value="10000"/>
  <ConfigItem name="MasterWaitTimeout" value="10000"/>
  <ConfigItem name="PublishQueueEnabled" value="true"/>
  <ConfigItem name="QueueSize" value="1000"/>
  <ConfigItem name="StateChangeScan" value="60000"/>
  <ConfigItem name="SyncPingSize" value="1000"/>
</ConfigGroup>
<ConfigGroup name="Comet Config">
  <ConfigItem name="BufferSize" value="5120"/>
  <ConfigItem name="EnableLogging" value="false"/>
  <ConfigItem name="Timeout" value="60000"/>
</ConfigGroup>
<ConfigGroup name="Connection Config">
  <ConfigItem name="AllowBufferReuse" value="true"/>
  <ConfigItem name="BufferManagerCount" value="16"/>
  <ConfigItem name="BufferPoolSize" value="100"/>
  <ConfigItem name="BufferSize" value="102400"/>
  <ConfigItem name="CometReadTimeout" value="20000"/>
  <ConfigItem name="ConnectionDelay" value="60000"/>
  <ConfigItem name="IdleDriverTimeout" value="300000"/>
  <ConfigItem name="IdleSessionTimeout" value="300000"/>
  <ConfigItem name="KeepAlive" value="60000"/>
  <ConfigItem name="MaxBufferSize" value="20971520"/>
  <ConfigItem name="MaxNoOfConnections" value="-1"/>

```

```

<ConfigItem name="MaxNoOfConnectionsPerUserName" value="-1"/>
<ConfigItem name="MaxWriteCount" value="30"/>
<ConfigItem name="NetworkMonitorThreads" value="4"/>
<ConfigItem name="PriorityQueueCount" value="10"/>
<ConfigItem name="PriorityReadSpinLockMaxConnections" value="2"/>
<ConfigItem name="PriorityReadSpinLockTime" value="500"/>
<ConfigItem name="PriorityReadType" value="1"/>
<ConfigItem name="QueueHighWaterMark" value="3000"/>
<ConfigItem name="QueueLowWaterMark" value="1000"/>
<ConfigItem name="ReadCount" value="10"/>
<ConfigItem name="UseDirectBuffering" value="true"/>
<ConfigItem name="WriteHandlerType" value="3"/>
<ConfigItem name="whEventThresholdCount" value="350"/>
<ConfigItem name="whEventThresholdTime" value="500"/>
<ConfigItem name="whMaxEventsBeforeFlush" value="100"/>
<ConfigItem name="whMaxEventsPerSecond" value="100000"/>
<ConfigItem name="whMaxTimeBetweenFlush" value="2"/>
</ConfigGroup>
<ConfigGroup name="Data Stream Config">
  <ConfigItem name="MonitorTimer" value="10000"/>
  <ConfigItem name="OffloadMulticastWrite" value="false"/>
  <ConfigItem name="SendInitialMapping" value="true"/>
</ConfigGroup>
<ConfigGroup name="DurableConfig">
  <ConfigItem name="DurableNameFiltering" value="false"/>
  <ConfigItem name="QueuedExtendedException" value="false"/>
</ConfigGroup>
<ConfigGroup name="Environment Config">
  <ConfigItem name="AvailableProcessors" value="4"/>
  <ConfigItem name="Embedded" value="false"/>
  <ConfigItem name="InterRealmProtocolVersion" value="1"/>
  <ConfigItem name="JavaVendor" value="Oracle Corporation"/>
  <ConfigItem name="JavaVersion" value="1.8.0_271"/>
  <ConfigItem name="NanosecondSupport" value="false"/>
  <ConfigItem name="OSArchitecture" value="amd64"/>
  <ConfigItem name="OSName" value="Windows 10"/>
  <ConfigItem name="OSVersion" value="10.0"/>
  <ConfigItem name="ProcessId" value="14256"/>
  <ConfigItem name="ServerBuildDate" value="..."/>
  <ConfigItem name="ServerBuildNumber" value="BuildNumberHere"/>
  <ConfigItem name="ServerReleaseDetails" value="BuildIdentifier"/>
  <ConfigItem name="ServerVersion" value="RealmServerVersion"/>
</ConfigGroup>
<ConfigGroup name="Event Storage">
  <ConfigItem name="ActiveDelay" value="1000"/>
  <ConfigItem name="AutoDeleteScan" value="5000"/>
  <ConfigItem name="AutoMaintenanceThreshold" value="50"/>
  <ConfigItem name="CacheAge" value="60000"/>
  <ConfigItem name="EnableStoreCaching" value="false"/>
  <ConfigItem name="IdleDelay" value="10000"/>
  <ConfigItem name="JMSEngineAutoPurgeTime" value="5000"/>
  <ConfigItem name="MaintenanceFileSizeThreshold" value="104857600"/>
  <ConfigItem name="MaintenanceMemoryThreshold" value="104857600"/>
  <ConfigItem name="PageSize" value="5000"/>
  <ConfigItem name="QueueSubscriberFiltering" value="false"/>
  <ConfigItem name="StoreReadBufferSize" value="32768"/>
  <ConfigItem name="SyncBatchSize" value="50"/>
  <ConfigItem name="SyncServerFiles" value="false"/>
  <ConfigItem name="SyncTimeLimit" value="20"/>
  <ConfigItem name="ThreadPoolSize" value="4"/>

```

```

</ConfigGroup>
<ConfigGroup name="Fanout Values">
  <ConfigItem name="ConnectionGrouping" value="true"/>
  <ConfigItem name="DelayPublishOnCapacity" value="true"/>
  <ConfigItem name="HonourSharedDurableCapacity" value="true"/>
  <ConfigItem name="IteratorWindowSize" value="100"/>
  <ConfigItem name="JMSQueueMaxMultiplier" value="10"/>
  <ConfigItem name="ParallelThreadPoolSize" value="2"/>
  <ConfigItem name="PeakPublishDelay" value="1"/>
  <ConfigItem name="PublishDelay" value="1"/>
  <ConfigItem name="PublishExpiredEvents" value="true"/>
  <ConfigItem name="SendEndOfChannelAlways" value="false"/>
  <ConfigItem name="SendPubEventsImmediately" value="true"/>
</ConfigGroup>
<ConfigGroup name="Global Values">
  <ConfigItem name="AllowRealmAdminFullAccess" value="true"/>
  <ConfigItem name="CacheJoinInfoKeys" value="true"/>
  <ConfigItem name="DisableExplicitGC" value="true"/>
  <ConfigItem name="EnableCaching" value="false"/>
  <ConfigItem name="EnableDNSLookups" value="true"/>
  <ConfigItem name="EnableWeakReferenceCleanup" value="true"/>
  <ConfigItem name="ExtendedMessageSelector" value="true"/>
  <ConfigItem name="HTTPCookieSize" value="14"/>
  <ConfigItem name="NHPScanTime" value="5000"/>
  <ConfigItem name="NHPTimeout" value="120000"/>
  <ConfigItem name="OverrideEveryoneUser" value="false"/>
  <ConfigItem name="PauseServerPublishing" value="false"/>
  <ConfigItem name="SendRealmSummaryStats" value="false"/>
  <ConfigItem name="StampDictionary" value="true"/>
  <ConfigItem name="StampHost" value="true"/>
  <ConfigItem name="StampTime" value="true"/>
  <ConfigItem name="StampTimeUseHPT" value="false"/>
  <ConfigItem name="StampTimeUseHPTScale" value="0"/>
  <ConfigItem name="StampUser" value="true"/>
  <ConfigItem name="StatusBroadcast" value="5000"/>
</ConfigGroup>
<ConfigGroup name="Inter-Realm Comms Config">
  <ConfigItem name="EstablishmentTime" value="30000"/>
  <ConfigItem name="KeepAliveInterval" value="10000"/>
  <ConfigItem name="KeepAliveResetTime" value="35000"/>
  <ConfigItem name="MaximumReconnectTime" value="20000"/>
  <ConfigItem name="MinimumReconnectTime" value="1000"/>
  <ConfigItem name="Timeout" value="120000"/>
  <ConfigItem name="WriteDelayTimeout" value="30000"/>
</ConfigGroup>
<ConfigGroup name="JVM Management">
  <ConfigItem name="EmergencyThreshold" value="94"/>
  <ConfigItem name="EnableJMX" value="false"/>
  <ConfigItem name="ExitOnDiskIOError" value="true"/>
  <ConfigItem name="ExitOnInterfaceFailure" value="false"/>
  <ConfigItem name="IORetryCount" value="10"/>
  <ConfigItem name="IOSleepTime" value="500"/>
  <ConfigItem name="JMXRMIServerURLString"
    value="service:jmx:rmi:///jndi/rmi://localhost:9999/server"/>
  <ConfigItem name="MemoryMonitoring" value="2000"/>
  <ConfigItem name="WarningThreshold" value="85"/>
</ConfigGroup>
<ConfigGroup name="Join Config">
  <ConfigItem name="ActiveThreadPoolSize" value="2"/>
  <ConfigItem name="IdleThreadPoolSize" value="1"/>

```

```

<ConfigItem name="MaxEventsPerSchedule" value="1000"/>
<ConfigItem name="MaxQueueSizeToUse" value="100"/>
<ConfigItem name="RemoteJoinAckBatchSize" value="100"/>
<ConfigItem name="RemoteJoinAckInterval" value="1000"/>
<ConfigItem name="UseQueuedLocalJoinHandler" value="false"/>
</ConfigGroup>
<ConfigGroup name="Logging Config">
  <ConfigItem name="DefaultLogSize" value="10000000"/>
  <ConfigItem name="DisplayCurrentThread" value="true"/>
  <ConfigItem name="EmbedTag" value="false"/>
  <ConfigItem name="EnableLog4J" value="false"/>
  <ConfigItem name="EnableStatusLog" value="true"/>
  <ConfigItem name="LogManager" value="1"/>
  <ConfigItem name="RolledLogFileDepth" value="10"/>
  <ConfigItem name="fLoggerLevel" value="0"/>
</ConfigGroup>
<ConfigGroup name="Metric Config">
  <ConfigItem name="EnableEventMemoryMonitoring" value="true"/>
  <ConfigItem name="EnableMetrics" value="true"/>
</ConfigGroup>
<ConfigGroup name="Plugin Config">
  <ConfigItem name="EnableAccessLog" value="true"/>
  <ConfigItem name="EnableErrorLog" value="true"/>
  <ConfigItem name="EnablePluginLog" value="true"/>
  <ConfigItem name="MaxNumberOfPluginThreads" value="200"/>
  <ConfigItem name="PluginTimeout" value="30000"/>
</ConfigGroup>
<ConfigGroup name="Protobuf Config">
  <ConfigItem name="CacheEventFilter" value="true"/>
</ConfigGroup>
<ConfigGroup name="Protocol AMQP Config">
  <ConfigItem name="AnonymousUser" value="anonymous_amqp"/>
  <ConfigItem name="BufferSize" value="10240"/>
  <ConfigItem name="DefaultNodeMode" value="0"/>
  <ConfigItem name="Enable" value="true"/>
  <ConfigItem name="EnableWriteThread" value="false"/>
  <ConfigItem name="EngineLoopCount" value="50"/>
  <ConfigItem name="MaxFrameSize" value="10000000"/>
  <ConfigItem name="MaxThreadPoolSize" value="10"/>
  <ConfigItem name="MinThreadPoolSize" value="1"/>
  <ConfigItem name="QueuePrefix" value="queue://"/>
  <ConfigItem name="SASL_Anonymous" value="true"/>
  <ConfigItem name="SASL_CRAM-MD5" value="false"/>
  <ConfigItem name="SASL_DIGEST-MD5" value="false"/>
  <ConfigItem name="SASL_Plain" value="false"/>
  <ConfigItem name="SubscriberCredit" value="1000"/>
  <ConfigItem name="Timeout" value="60000"/>
  <ConfigItem name="TopicPrefix" value="topic://"/>
  <ConfigItem name="TransformToUse" value="2"/>
</ConfigGroup>
<ConfigGroup name="Protocol MQTT Config">
  <ConfigItem name="DisconnectClientsOnPublishFailure" value="true"/>
  <ConfigItem name="Enable" value="true"/>
  <ConfigItem name="EnableAutoCreateTopics" value="true"/>
  <ConfigItem name="EnforceAlphaNumericClientID" value="false"/>
  <ConfigItem name="IgnoreClientIDLength" value="true"/>
  <ConfigItem name="MaxOutstanding" value="64000"/>
  <ConfigItem name="QoS0AsTransient" value="false"/>
  <ConfigItem name="SessionStateTTL" value="259200000"/>
  <ConfigItem name="Strict" value="true"/>

```

```

    <ConfigItem name="SupportZeroLength" value="true"/>
  </ConfigGroup>
  <ConfigGroup name="RecoveryDaemon">
    <ConfigItem name="EventsPerBlock" value="500"/>
    <ConfigItem name="ThreadPool" value="4"/>
  </ConfigGroup>
  <ConfigGroup name="Server Protection">
    <ConfigItem name="EnableFlowControl" value="false"/>
    <ConfigItem name="FlowControlWaitTimeOne" value="16000"/>
    <ConfigItem name="FlowControlWaitTimeThree" value="10000"/>
    <ConfigItem name="FlowControlWaitTimeTwo" value="13332"/>
  </ConfigGroup>
  <ConfigGroup name="Thread Pool Config">
    <ConfigItem name="CommonPoolThreadSize" value="5"/>
    <ConfigItem name="ConnectionThreadPoolMaxSize" value="10"/>
    <ConfigItem name="ConnectionThreadPoolMinSize" value="4"/>
    <ConfigItem name="ConnectionThreadWaitTime" value="120000"/>
    <ConfigItem name="EnableConnectionThreadPooling" value="true"/>
    <ConfigItem name="MaxUnauthorisedCount" value="1000"/>
    <ConfigItem name="PendingTaskWarningThreshold" value="1000"/>
    <ConfigItem name="ReadThreadPoolMaxSize" value="100"/>
    <ConfigItem name="ReadThreadPoolMinSize" value="4"/>
    <ConfigItem name="SchedulerPoolSize" value="10"/>
    <ConfigItem name="SlowTaskWarningTime" value="5000"/>
    <ConfigItem name="StalledTasksWarningTime" value="60000"/>
    <ConfigItem name="ThreadDumpInterval" value="60000"/>
    <ConfigItem name="ThreadDumpOnSlowTask" value="false"/>
    <ConfigItem name="ThreadIdleQueueSize" value="10"/>
    <ConfigItem name="WriteThreadPoolMaxSize" value="1000"/>
    <ConfigItem name="WriteThreadPoolMinSize" value="5"/>
  </ConfigGroup>
  <ConfigGroup name="Trace Logging Config">
    <ConfigItem name="TraceFolderLogSize" value="1024"/>
    <ConfigItem name="TraceStoreLogLevel" value="2"/>
    <ConfigItem name="TraceStoreLogSize" value="10"/>
    <ConfigItem name="TraceStores" value=""/>
  </ConfigGroup>
  <ConfigGroup name="TransactionManager">
    <ConfigItem name="MaxEventsPerTransaction" value="0"/>
    <ConfigItem name="MaxTransactionTime" value="300000"/>
    <ConfigItem name="TTLThreshold" value="1000"/>
  </ConfigGroup>
</RealmConfiguration>
<RealmPermissionSet>
  <RealmACLEntry listACLEntries="false" modifyACLEntries="false" fullControl="true"

    connectToRealm="false" changeRealmConfig="false" addremoveChannels="false"

    addremoveJoins="false" addremoveRealms="false"
overrideConnectionCount="false"
    useAdminAPI="false" manageDatagroups="false" publishDatagroups="false"
    ownDatagroups="false" host="0:0:0:0:0:0:0:1" name="..."/>
  <RealmACLEntry listACLEntries="false" modifyACLEntries="false" fullControl="true"
    connectToRealm="false" changeRealmConfig="false" addremoveChannels="false"
    addremoveJoins="false" addremoveRealms="false"
overrideConnectionCount="false"
    useAdminAPI="false" manageDatagroups="false" publishDatagroups="false"
    ownDatagroups="false" host="127.0.0.1" name="..."/>
  <RealmGroupACLEntry listACLEntries="true" modifyACLEntries="true" fullControl="true"
    connectToRealm="true" changeRealmConfig="true" addremoveChannels="true"

```

```

        addremoveJoins="true" addremoveRealms="true" overrideConnectionCount="true"
        useAdminAPI="true" manageDatagroups="true" publishDatagroups="true"
        ownDatagroups="true" groupname="Everyone"/>
</RealmPermissionSet>
<ClusterSet>
  <ClusterEntry name="cluster_1">
    <ClusterMember name="realm0" rname="nsp://localhost:11000" canBeMaster="true"/>
    <ClusterMember name="realm1" rname="nsp://localhost:11010" canBeMaster="true"/>
    <ClusterMember name="realm2" rname="nsp://localhost:11020" canBeMaster="true"/>
  </ClusterEntry>
</ClusterSet>
<RealmSet>
  <RealmEntry name="realm1" rname="nhp://...:11010"/>
  <RealmEntry name="realm2" rname="nhp://...:11020"/>
</RealmSet>
<ChannelSet>
  <ChannelEntry>
    <ChannelAttributesEntry name="/customer/sales/JMSTopic" TTL="0"
      capacity="0" EID="0" jmsEngine="true"
      mergeEngine="false" type="MIXED_TYPE"/>
    <StorePropertiesEntry HonorCapacityWhenFull="true" SyncOnEachWrite="false"
      SyncMaxBatchSize="0" SyncBatchTime="0"
PerformAutomaticMaintenance="true"
      EnableCaching="true" CacheOnReload="true" EnableReadBuffering="true"

      ReadBufferSize="10240" Priority="4" EnableMulticast="false"
      MultiFileEventsPerSpindle="50000" StampDictionary="0"/>
  <ChannelPermissionSet>
    <ChannelACLEntry listACLEntries="false" modifyACLEntries="false"
      fullControl="false" getLastEID="true" purgeEvents="false"
      subscribe="true" publish="true" useNamedSubscription="false"
      host="*" name="user"/>
    <ChannelACLEntry listACLEntries="true" modifyACLEntries="true"
      fullControl="true" getLastEID="true" purgeEvents="true"
      subscribe="true" publish="true" useNamedSubscription="true"
      host="..." name="user"/>
    <ChannelGroupACLEntry listACLEntries="false" modifyACLEntries="false"
      fullControl="false" getLastEID="true" purgeEvents="false"
      subscribe="true" publish="false" useNamedSubscription="true"
      groupname="Everyone"/>
  </ChannelPermissionSet>
</ChannelEntry>
  <ChannelEntry>
    <ChannelAttributesEntry name="/naming/defaultContext" TTL="0"
      capacity="0" EID="2" jmsEngine="false"
      mergeEngine="false" type="MIXED_TYPE"/>
    <StorePropertiesEntry HonorCapacityWhenFull="true" SyncOnEachWrite="false"
      SyncMaxBatchSize="0" SyncBatchTime="0"
PerformAutomaticMaintenance="true"
      EnableCaching="true" CacheOnReload="true" EnableReadBuffering="true"

      ReadBufferSize="10240" Priority="4" EnableMulticast="false"
      MultiFileEventsPerSpindle="50000" StampDictionary="0"/>
  <ChannelPermissionSet>
    <ChannelACLEntry listACLEntries="true" modifyACLEntries="true"
      fullControl="true" getLastEID="true" purgeEvents="true"
      subscribe="true" publish="true" useNamedSubscription="true"
      host="..." name="..."/>
    <ChannelGroupACLEntry listACLEntries="true" modifyACLEntries="true"
      fullControl="true" getLastEID="true" purgeEvents="true"

```

```

        subscribe="true" publish="true" useNamedSubscription="true"
        groupname="Everyone"/>
</ChannelPermissionSet>
<ChannelKeySet>
  <ChannelKeyEntry keyName="alias" keyDepth="1"/>
</ChannelKeySet>
<EventsSet>
  <Event id="0">
    <EventAttribSet>
      <EventAttrib name="nrvpublish.time" type="Long" value="1610454161489"/>
      <EventAttrib name="nrvpublish.host" type="String" value="..."/>
      <EventAttrib name="nrvpublish.name" type="String" value="..."/>
      <EventAttrib name="JMSDeliveryMode" type="String" value="PERSISTENT"/>
      <EventAttrib name="JMSPriority" type="Byte" value="4"/>
    </EventAttribSet>
    <EventPropSet>
      <EventProp name="JMS_my-channels_EnableMultiplexedConnections"
type="Boolean" value="true"/>
      <EventProp name="JMS_my-channels_RandomRNames" type="Boolean"
value="false"/>
      <EventProp name="JMS_my-channels_RetryCommit" type="Boolean" value="false"/>
      <EventProp name="JMS_my-channels_ConxExceptionOnRetryFailure" type="Boolean"
value="false"/>
      <EventProp name="JMS_my-channels_MaxReconnectAttempts" type="Integer"
value="-1"/>
      <EventProp name="JMS_my-channels_EnableSharedDurable" type="Boolean"
value="true"/>
      <EventProp name="JMS_my-channels_EnableSerialDurable" type="Boolean"
value="false"/>
      <EventProp name="JMS_my-channels_EnableSingleSharedDurableAck"
type="Boolean" value="false"/>
      <EventProp name="JMS_my-channels_EnableSingleQueueAck" type="Boolean"
value="false"/>
      <EventProp name="JMS_my-channels_SyncWritesToDisc" type="Boolean"
value="false"/>
      <EventProp name="JMS_my-channels_SyncSendPersistent" type="Boolean"
value="true"/>
      <EventProp name="JMS_my-channels_InitialConnectionRetryCount" type="Integer"
value="2"/>
      <EventProp name="JMS_my-channels_SyncBatchSize" type="Integer" value="50"/>
      <EventProp name="JMS_my-channels_SyncTime" type="Integer" value="20"/>
      <EventProp name="JMS_my-channels_GlobalStoreCapacity" type="Integer"
value="0"/>
      <EventProp name="JMS_my-channels_AutoAckCount" type="Integer" value="50"/>
      <EventProp name="JMS_my-channels_WindowSize" type="Integer" value="100"/>
      <EventProp name="JMS_my-channels_useInfiniteWindowSize" type="Boolean"
value="false"/>
      <EventProp name="JMS_my-channels_UnAckedSize" type="Integer" value="100"/>
      <EventProp name="JMS_my-channels_RedliveredSize" type="Integer"
value="100"/>
      <EventProp name="JMS_my-channels_ThreadPoolSize" type="Integer" value="30"/>
      <EventProp name="JMS_my-channels_AutoReconnectAfterACL" type="Boolean"
value="false"/>
      <EventProp name="JMS_my-channels_ImmediateReconnect" type="Boolean"
value="true"/>
      <EventProp name="JMS_my-channels_ReconnectInterval" type="Long"
value="2000"/>
      <EventProp name="JMS_my-channels_UseJMSEngine" type="Boolean" value="true"/>
      <EventProp name="JMS_my-channels_DisconnectAfterClusterFailure"
type="Boolean" value="true"/>
    </EventPropSet>
  </Event>
</EventsSet>

```

```

        <EventProp name="JMS_my-channels_ConnectionTimeout" type="Long"
value="10000"/>
        <EventProp name="JMS_my-channels_PermittedKeepAlivesMissed" type="Integer"
value="2"/>
        <EventProp name="JMS_my-channels_SyncNamedTopicAcks" type="Boolean"
value="true"/>
        <EventProp name="JMS_my-channels_AdapterBuffer" type="Integer"
value="1310720"/>
        <EventProp name="JMS_my-channels_WriteHandler" type="Integer" value="3"/>
        <EventProp name="JMS_my-channels_SyncQueueAcks" type="Boolean"
value="true"/>
        <EventProp name="JMS_my-channels_SyncTopicAcks" type="Boolean"
value="true"/>
        <EventProp name="JMS_my-channels_AutoCreateResource" type="Boolean"
value="true"/>
        <EventProp name="JMS_my-channels_FollowMaster" type="Boolean"
value="false"/>
        <EventProp name="alias.type" type="Integer" value="1"/>
        <EventProp name="alias" type="String" value="ExampleConnectionFactory"/>
        <EventProp name="alias.reference.classname" type="String"
value="javax.jms.ConnectionFactory"/>
        <EventProp name="alias.reference.factoryclass" type="String"
value="com.pcbsys.nirvana.nJMS.ConnectionFactoryFactory"/>
        <EventProp name="alias.reference.url" type="String" value="{...}"/>
        <EventProp name="alias.stringRefAddr.type" type="String"
value="ConnectionFactory"/>
        <EventProp name="alias.stringRefAddr.addr" type="String"
value="nsp://localhost:11000,nsp://localhost:11010,nsp://localhost:11020"/>
    </EventPropSet>
    <EventData>...</EventData>
</Event>
<Event id="1">
    <EventAttribSet>
        <EventAttrib name="nrpub.time" type="Long" value="1610454171673"/>
        <EventAttrib name="nrpub.host" type="String" value="..."/>
        <EventAttrib name="nrpub.name" type="String" value="..."/>
        <EventAttrib name="JMSDeliveryMode" type="String" value="PERSISTENT"/>
        <EventAttrib name="JMSPriority" type="Byte" value="4"/>
    </EventAttribSet>
    <EventPropSet>
        <EventProp name="alias.type" type="Integer" value="1"/>
        <EventProp name="alias" type="String" value="/customer/sales/JMSTopic"/>
        <EventProp name="alias.reference.classname" type="String"
value="javax.jms.Topic"/>
        <EventProp name="alias.reference.factoryclass" type="String"
value="com.pcbsys.nirvana.nJMS.TopicFactory"/>
        <EventProp name="alias.reference.url" type="String" value=""/>
        <EventProp name="alias.stringRefAddr.type" type="String" value="Topic"/>
        <EventProp name="alias.stringRefAddr.addr" type="String"
value="/customer/sales/JMSTopic"/>
    </EventPropSet>
    <EventData>...</EventData>
</Event>
<Event id="2">
    <EventAttribSet>
        <EventAttrib name="nrpub.time" type="Long" value="1610454193768"/>
        <EventAttrib name="nrpub.host" type="String" value="..."/>
        <EventAttrib name="nrpub.name" type="String" value="..."/>
        <EventAttrib name="JMSDeliveryMode" type="String" value="PERSISTENT"/>

```

```

    <EventAttrib name="JMSPriority" type="Byte" value="4"/>
  </EventAttribSet>
  <EventPropSet>
    <EventProp name="alias.type" type="Integer" value="1"/>
    <EventProp name="alias" type="String" value="/customer/sales/JMSQueue"/>
    <EventProp name="alias.reference.classname" type="String"
value="javax.jms.Queue"/>
    <EventProp name="alias.reference.factoryclass" type="String"
      value="com.pcbsys.nirvana.nJMS.QueueFactory"/>
    <EventProp name="alias.reference.url" type="String" value=""/>
    <EventProp name="alias.stringRefAddr.type" type="String" value="Queue"/>
    <EventProp name="alias.stringRefAddr.addr" type="String"
value="/customer/sales/JMSQueue"/>
  </EventPropSet>
  <EventData>...</EventData>
</Event>
</EventsSet>
</ChannelEntry>
<ChannelEntry>
  <ChannelAttributesEntry name="/partner/sales" TTL="0" capacity="0"
    EID="0" jmsEngine="false" mergeEngine="false"
    type="MIXED_TYPE"/>
  <StorePropertiesEntry HonorCapacityWhenFull="true" SyncOnEachWrite="false"
    SyncMaxBatchSize="0" SyncBatchTime="0"
PerformAutomaticMaintenance="true"
    EnableCaching="true" CacheOnReload="true" EnableReadBuffering="true"

    ReadBufferSize="10240" Priority="4" EnableMulticast="false"
    MultiFileEventsPerSpindle="50000" StampDictionary="0"/>
  <ChannelPermissionSet>
    <ChannelACLEntry listACLEntries="false" modifyACLEntries="false"
      fullControl="false" getLastEID="true" purgeEvents="false"
      subscribe="true" publish="true" useNamedSubscription="false"
      host="*" name="user"/>
    <ChannelACLEntry listACLEntries="true" modifyACLEntries="true"
      fullControl="true" getLastEID="true" purgeEvents="true"
      subscribe="true" publish="true" useNamedSubscription="true"
      host="..." name="user"/>
    <ChannelGroupACLEntry listACLEntries="false" modifyACLEntries="false"
      fullControl="false" getLastEID="true" purgeEvents="false"
      subscribe="true" publish="false" useNamedSubscription="true"
      groupname="Everyone"/>
  </ChannelPermissionSet>
  <DurableSet>
    <durableEntry name="serial_durable" EID="-1" outstandingEvents="0"
      clusterWide="true" shared="false" serial="true"/>
    <durableEntry name="shared_durable" EID="-1" outstandingEvents="0"
      clusterWide="true" shared="true" serial="false"/>
  </DurableSet>
</ChannelEntry>
</ChannelSet>
<QueueSet>
  <QueueEntry>
    <ChannelAttributesEntry name="/customer/sales/JMSQueue" TTL="0"
      capacity="0" EID="0" jmsEngine="false"
      mergeEngine="false" type="MIXED_TYPE"/>
    <StorePropertiesEntry HonorCapacityWhenFull="true"
      SyncOnEachWrite="false" SyncMaxBatchSize="0" SyncBatchTime="0"
PerformAutomaticMaintenance="true" EnableCaching="true"
      CacheOnReload="true" EnableReadBuffering="true" ReadBufferSize="10240"

```

```

        Priority="4" EnableMulticast="false" MultiFileEventsPerSpindle="50000"
        StampDictionary="0"/>
    <QueuePermissionSet>
        <QueueACLEntry listACLEntries="false" modifyACLEntries="false"
            fullControl="false" purge="false" peek="true" push="true"
            pop="true" host="*" name="user"/>
        <QueueACLEntry listACLEntries="true" modifyACLEntries="true"
            fullControl="true" purge="true" peek="true" push="true"
            pop="true" host=".." name="user"/>
        <QueueGroupACLEntry listACLEntries="false" modifyACLEntries="false"
            fullControl="false" purge="false" peek="true" push="false"
            pop="false" groupname="Everyone"/>
    </QueuePermissionSet>
</QueueEntry>
<QueueEntry>
    <ChannelAttributesEntry name="/partner/queries" TTL="0"
        capacity="0" EID="0"
        jmsEngine="false" mergeEngine="false" type="MIXED_TYPE"/>
    <StorePropertiesEntry HonorCapacityWhenFull="true"
        SyncOnEachWrite="false" SyncMaxBatchSize="0" SyncBatchTime="0"
        PerformAutomaticMaintenance="true" EnableCaching="true"
        CacheOnReload="true" EnableReadBuffering="true" ReadBufferSize="10240"

        Priority="4" EnableMulticast="false" MultiFileEventsPerSpindle="50000"
        StampDictionary="0"/>
    <QueuePermissionSet>
        <QueueACLEntry listACLEntries="false" modifyACLEntries="false"
            fullControl="false" purge="false" peek="true" push="true"
            pop="true" host="*" name="user"/>
        <QueueACLEntry listACLEntries="true" modifyACLEntries="true"
            fullControl="true" purge="true" peek="true" push="true"
            pop="true" host=".." name="user"/>
        <QueueGroupACLEntry listACLEntries="false" modifyACLEntries="false"
            fullControl="false" purge="false" peek="true" push="false"
            pop="false" groupname="Everyone"/>
    </QueuePermissionSet>
</QueueEntry>
</QueueSet>
<DataGroupSet/>
<RealmInterfaces>
    <RealmNHPInterface>
        <RealmInterface name="nhp0" port="11000" adapter="0.0.0.0"
            autostart="true" advertise="true" authtime="10000" backlog="100"
            acceptThreads="10" selectThreads="2" sendbuffersize="1310720"
            receivebuffersize="1310720" allowforinterrealm="true"
            allowclientconnections="true" EnableNIO="true"/>
        <RealmInterfacePlugin mountPoint="/" name="File Plugin">
            <NirvanaFilePlugin>
                <PluginConfigEntry name="AddUserAsCookie" value=""
                    description="Add the username to the sessions cookies"/>
                <PluginConfigEntry name="AuthParameters" value=""
                    description="List of key=value string which is passed to the
authenticators init function"/>
                <PluginConfigEntry name="Authenticator" value=""
                    description="Name of authenticator to use, leave to use default, else
classname to use"/>
                <PluginConfigEntry name="BasePath" value="C:\.."
                    description="Path used to locate the files"/>
            </NirvanaFilePlugin>
        </RealmInterfacePlugin>
    </RealmNHPInterface>

```

```
<PluginConfigEntry name="BufferSize" value=""
  description="Size of the internal buffer to use to send the data"/>
<PluginConfigEntry name="Cache-Control" value=""
  description="Specifies the cache control for the plugin"/>
<PluginConfigEntry name="CacheObjectSize" value=""
  description="Size in bytes that can be stored in the cache"/>
<PluginConfigEntry name="CachedObjects" value=""
  description="Number of objects to store in the cache"/>
<PluginConfigEntry name="DefaultName" value="index.html"
  description="If no file name is specified which file should be
returned"/>
<PluginConfigEntry name="EnableURLRewrite" value=""
  description="If the plugin will scan the source and rewrite the urls"/>
<PluginConfigEntry name="FileNotFoundPage" value=""
  description="name of the file to send when file can not be located"/>
<PluginConfigEntry name="GroupNames" value=""
  description="A comma separated list of groups one of which the user
must be a member of at least one to be granted access"/>
<PluginConfigEntry name="MimeType" value=""
  description="Name of the file to load the mime type information from"/>
<PluginConfigEntry name="ReloadUserFileDynamically" value=""
  description="Choose true to have the user file get reloaded on each auth
request"/>
<PluginConfigEntry name="RoleNames" value=""
  description="A comma separated list of roles which the user must have
at least one of to be granted access"/>
<PluginConfigEntry name="Security Realm" value=""
  description="Name of the authentication realm"/>
<PluginConfigEntry name="SeparateAccessandErrorLogs" value=""
  description="Choose true to have separate log files"/>
</NirvanaFilePlugin>
</RealmInterfacePlugin>
<JavascriptConfigEntry CORSAllowedOrigins="*" EnableJavaScript="true"
  EnableWebSockets="true" CORSAllowCredentials="true"
  EnableGZipLP="true" MinimumBytesBeforeGZIP="1000"
  AjaxLPIdleDelay="60000" AjaxLPActiveDelay="100"/>
</RealmNHPInterface>
</RealmInterfaces>
<RealmSecurityGroupSet/>
</NirvanaRealm>
```

Using the Enterprise Viewer

The Enterprise Viewer is a read-only version of the Enterprise Manager. Its purpose is to allow clients to view the Universal Messaging environment without the need for special administration rights.

Basically, it offers the same views as the Enterprise Manager, but you cannot use it to modify your Universal Messaging environment in any way. This means, for example, that you cannot create or delete channels and queues, and you cannot publish any events.

Starting the Enterprise Viewer

Windows platforms

Windows users can start the Enterprise Viewer by selecting the appropriate component from the Universal Messaging group in the Windows Start menu.

You can also type a command of the following form on the command line:

```
<InstallDir>\UniversalMessaging\java\<InstanceName>\bin\nterpriseview.exe
```

where *<InstallDir>* is the installation root location and *<InstanceName>* is the name of the Universal Messaging server.

UNIX-based platforms

You can launch the Enterprise Viewer on UNIX-based platforms by starting the `nenterpriseview` executable, which you can find at the following location:

```
<InstallDir>/UniversalMessaging/java/umserver/bin/nenterpriseview
```


3 Using Command Central to Manage Universal Messaging

■ About Using Command Central to Manage Universal Messaging	184
■ Managing Universal Messaging Server Instances	184
■ Starting, Stopping, and Restarting Universal Messaging	185
■ Securing Communication Between Command Central and Universal Messaging	186
■ Configuring Universal Messaging	189
■ Securing Access to Command Central	212
■ Administering Universal Messaging	214
■ Viewing Universal Messaging Run-time Monitoring Statuses	225
■ Viewing Universal Messaging KPIs	225
■ Viewing Universal Messaging Logs	226
■ Viewing Universal Messaging Inventory	227
■ Configuration Types That the Universal Messaging Server Supports	227
■ Using the Command Line to Manage Universal Messaging	228
■ Lifecycle Actions for Universal Messaging Server	302
■ Run-time Monitoring States for Universal Messaging Server	302
■ Run-time Monitoring Statuses for Universal Messaging Server	303
■ Deployment of Universal Messaging Assets	304
■ Templates for Provisioning Universal Messaging	305

About Using Command Central to Manage Universal Messaging

The topics in *Using Command Central to Manage Universal Messaging* provide information about how to manage Universal Messaging server instances, and how to configure and administer Universal Messaging from the Command Central web-user interface and command-line interface.

For general information about working with Command Central, see *Software AG Command Central Help*.

Managing Universal Messaging Server Instances

You can create and delete Universal Messaging server instances using the Command Central web-user interface.

Creating a Universal Messaging Server Instance

> To create a server instance in Command Central

1. In the **Environments** pane, select the environment in which you want to create the new server instance.
2. Click the **Installations** tab and select an installation in which to create the instance.
3. Click the **Instances** tab of the installation.
4. Click  and select **Universal Messaging Server**.
5. Specify the following instance properties:

Property	Description
Instance name	Required. Name of the new Universal Messaging server instance. The name is case-insensitive and can include upper and lower case alphabetic characters, digits (0-9), underscores (_), and non-leading hyphens (-).
NHP interface binding	Specific host or IP address to bind. If you do not specify a value, the instance binds to all available interfaces.
NHP interface port	Port number for the Universal Messaging server instance.
Data directory	Absolute path to the data directory of the Universal Messaging server instance. If you do not specify a value, the default " <i>Software AG_directory/UniversalMessaging/server/instance_name</i> " directory is used.

Property	Description
License file	The registered Universal Messaging license file. Select one of the registered license files from the list.
Configuration profile	Initial configuration settings for the Universal Messaging server instance. Values are: <ul style="list-style-type: none"> ■ webMethods suite use cases ■ Standalone use cases ■ Custom

6. Click **Next**, and then click **Finish**.

Deleting a Universal Messaging Server Instance

> To delete a server instance in Command Central

1. In the **Environments** pane, select the environment in which you want to delete the server instance.
2. Click the **Installations** tab and select an installation.
3. Click the **Instances** tab if the installation.
4. Select the Universal Messaging server instance to delete, and then click .
5. Click **OK** to confirm the deletion, and then click **Finish**.

The Windows service associated with the instance is automatically deleted when you delete the instance.

Starting, Stopping, and Restarting Universal Messaging

You can start, stop, and restart a Universal Messaging server instance on the **Instances** tab in Command Central or from the dashboard of the server instance.

Command Central does not support other lifecycle actions for a Universal Messaging server instance.

Securing Communication Between Command Central and Universal Messaging

How does Command Central Connect to Universal Messaging?

Command Central uses one of the Universal Messaging ports (interfaces) for configuration and administration. Command Central checks the interfaces of a Universal Messaging server instance in the following order and chooses the first available interface to connect to the server:

1. Interfaces that use the HTTP protocol (nhp).
2. Interfaces that use the socket protocol (nsp).
3. Interfaces that use the HTTPS protocol (nhps).
4. Interfaces that use the SSL protocol (nsps).
5. Interfaces that use the shared memory protocol (shm).

If Command Central disconnects from the Universal Messaging server, Command Central uses the same order to connect to a new Universal Messaging port.

About Securing Communication Between Command Central and Universal Messaging

Important:

To guarantee secure communication between Command Central and Universal Messaging, you must have only an nhps or nsps port (interface) configured on the Universal Messaging server. For information about how to create a port and how to configure an nhps or nsps port specifically, see [“Working with Universal Messaging Configuration Types” on page 190](#), [“NHPS Ports” on page 203](#), and [“NSPS Ports” on page 206](#), respectively.

When the Universal Messaging server instance is configured with a single nhps or nsps interface, Command Central uses this interface to connect automatically to the Universal Messaging server. By default, Command Central uses the same truststore file and, in case of client-side authentication, the same keystore file that are configured in the nhps or nsps interface.

If you want to specify truststore and keystore files that are different from the ones configured in the nhps or nsps interface, you can use either the standard Java Secure Socket Extension (JSSE) system properties or the Universal Messaging client system properties for secure communication. For information about how to configure the properties, see [“Configuring the JSSE System Properties” on page 187](#) and [“Configuring the Universal Messaging Client Properties” on page 188](#).

Considerations When Using System Properties to Specify Truststore and Keystore Files

Consider the following information before you use system properties to specify custom truststore and keystore files for secure communication between Command Central and a Universal Messaging server instance:

- If you want to connect to a Universal Messaging server instance that is part of a cluster or a zone, or that you plan to add to a cluster or a zone, ensure that the custom truststore contains the certificates of all server instances that are part of the cluster or zone.
- Configuring the standard JSSE system properties might impact all product instances that use secure sockets layer (SSL) in the same Platform Manager installation.

Configuring the JSSE System Properties

Use the following procedure to configure the JSSE system properties for a custom truststore and keystore to secure communication between Command Central and Universal Messaging.

Important:

Setting the JSSE system properties might impact all run-time components that use SSL in the same Platform Manager installation.

➤ To configure the JSSE system properties

1. In the Command Central web user interface, go to the Platform Manager instance that is in the same installation as the Universal Messaging server.
2. Click **Configuration > Java System Properties > Edit**.
3. Add the following properties:
 - `com.softwareag.um.plugin.use.ssl.system.properties=true`
 - `javax.net.ssl.keyStore=<path to the custom keystore>` - Required only if client authentication is enabled on the nsps or nhps interface.
 - `javax.net.ssl.keyStorePassword=<password of the custom keystore>` - Required only if client authentication is enabled on the nsps or nhps interface.
 - `javax.net.ssl.trustStore=<path to the custom truststore>`
 - `javax.net.ssl.trustStorePassword=<password of the custom truststore>`
4. Click **Apply**.
5. Restart Platform Manager.

Configuring the Universal Messaging Client Properties

Use the following procedure to configure the Universal Messaging client system properties for a custom truststore and keystore to secure communication between Command Central and Universal Messaging.

➤ To configure the Universal Messaging client system properties

1. In the Command Central web user interface, go to the Platform Manager instance that is in the same installation as the Universal Messaging server.
2. Click **Configuration > Java System Properties > Edit**.
3. Add the following properties:
 - `com.softwareag.um.plugin.use.ssl.system.properties=true`
 - `com.softwareag.um.client.ssl.keystore_path=<path to the custom keystore>` - Required only if client authentication is enabled on the nsps or nhps interface.
 - `com.softwareag.um.client.ssl.keystore_password=<password of the custom keystore>` - Required only if client authentication is enabled on the nsps or nhps interface.
 - `com.softwareag.um.client.ssl.certificate_alias=<the alias of the certificate in the keystore that Command Central should use>` - Required only if client authentication is enabled on the nsps or nhps interface and the keystore contains more than one certificate.
 - `com.softwareag.um.client.ssl.truststore_path=<path to the custom truststore>`
 - `com.softwareag.um.client.ssl.truststore_password=<password of the custom truststore>`
4. Click **Apply**.
5. Restart Platform Manager.

Switching Off the System Properties Mode

To stop using custom truststore and keystore files for secure communication between Command Central and a Universal Messaging server instance, you must set `com.softwareag.um.plugin.use.ssl.system.properties` to `false`.

➤ To stop using custom truststore and keystore files

1. In the Command Central web user interface, go to the Platform Manager instance that is in the same installation as the Universal Messaging server instance.

2. Click **Configuration > Java System Properties > Edit**.
3. Set `com.softwareag.um.plugin.use.ssl.system.properties` to `false`.
4. Click **Apply**.
5. Restart Platform Manager.

Configuring Universal Messaging

About Configuring Universal Messaging

This topic provides general information about how to work with the configuration types that Universal Messaging supports. You can also find reference information about the fields and values to specify when you create an instance of each configuration type.

You can create instances of the following configuration types for a Universal Messaging server instance in the Command Central web-user interface:

- Channels
- Clustering
- General Properties
- Groups
- Internal Users
- JNDI Connection Factories
- JNDI Destinations
- JVM Options
- Java System Properties
- License Keys
- Memory
- Ports
- Queues
- Realm ACL
- Zones

For detailed reference information about the configuration properties and their values, see the topics under *Concepts*.

Working with Universal Messaging Configuration Types

You create, edit, and delete instances of configuration types for a Universal Messaging server on the `Universal-Messaging-instanceName` > Configuration page in Command Central.

The Universal Messaging server instance must be running during configuration.

➤ To create, edit, or delete an instance of a Universal Messaging configuration type

1. In Command Central, go to **Environments > All > Instances > Universal-Messaging-*instanceName***.
2. Click the **Configuration** tab.
3. Select the configuration type from the drop-down list.

Universal Messaging displays the available or default values for the selected Universal Messaging configuration type.

4. Perform any of the following actions:

- To create an instance of a configuration type, click . Specify the required values for the fields and click **Save**. Optionally, you can test the configuration before saving it.
- To edit an instance of a configuration type, click the instance and then click **Edit**. Make the necessary changes and click **Save**. Optionally, you can test the configuration before saving it.
- To delete an instance of a configuration type, click .

Channels

The following tables show the properties you can configure when you create a channel in Command Central.

Channel Properties

Property	Description
Name	Required. Name of the channel. Note: After a channel is created, you cannot edit the channel name.
Type	Type of the channel. The Universal Messaging channel types are: <ul style="list-style-type: none"> ■ Reliable

Property	Description
	<ul style="list-style-type: none"> ■ Persistent ■ Mixed (default)
TTL (ms)	Specifies how long (in milliseconds) each event is retained on the channel after being published. For example, if you specify a TTL of 10000, the events on the channel will be automatically removed by the server after 10000 milliseconds. Specify 0 for events to remain on the channel indefinitely.
Capacity	Event capacity of the channel. Specifies the maximum number of events that can be on a channel, once published. Specify 0 to store unlimited events. The maximum channel capacity is 2147483646.
Dead event store	Channel or queue to be used to store events that are purged before being consumed.
Engine	Type of engine to be used for the channel. By default, Universal Messaging retains all events on the channel for a specified TTL, modify the retention behavior by selecting JMS engine or Merge engine.
Cluster-wide	Selected automatically if the Universal Messaging server instance is part of a cluster.
Protobuf descriptor	Absolute path to the Protocol Buffer (protobuf) descriptor file that is stored on the machine where Software AG Platform Manager is installed.

Storage Properties

Property	Description
Auto-maintenance	Select to retain events till they reach their TTL. Cancel the selection to purge events from the channel storage file.
Honor capacity	Select to prevent publishing of data when the channel is full. Cancel the selection to purge the oldest published event.
Enable caching	Select for the events to be stored in the cache memory and reused. Cancel the selection to read and stored in the file store.
Cache on reload	Select to enable caching during reload.
Enable read buffering	Select to enable read buffering for the store on the Universal Messaging server.
Enable multicast	Select to enable multicast client to receive events over multitask connections.

Property	Description
Read buffer size	Read buffer size in bytes.
Sync each write	Select to sync each write to the file system.
Sync batch size	Configurable only when Sync each write is selected. Number of events that is to be synced with the file system at once.
Sync batch time	Configurable only when Sync each write is selected. Time in milliseconds (ms) between syncs with the file system.
Priority	Priority range. 0 (lowest) to 9 (highest).
Events per spindle	Maximum number of events allowed per file.
Stamp dictionary	Select to stamp events on the channel by the server.

Channel Keys

Column	Description
Key name	Name of the channel publish key.
Depth	Depth of the channel publish key. Depth is the maximum number of events that can exist on a channel for a specific key name.

Channel ACL

Column	Description
Subject	User name in the format <code>user@host</code> or the name of an existing group.
Manage ACL	Select to allow the user or group to manage ACLs.
Full	Select to grant full privileges to the user or group.
Purge	Select to allow the user or group to delete events.
Subscribe	Select to allow the user or group to subscribe to events.
Publish	Select to allow the user or group to publish events.
Named (durable)	Select to allow the user or group to connect to this channel using durable subscriptions.

Joins

You can add and delete joins, but you cannot edit channel join properties.

Column	Description
Type	Type of join. Outgoing: channel is source. Incoming: channel is destination.
Destination name	Destination channel or queue.
Target instance name	Name of the target instance. Required only if the channel or queue is in a remote Universal Messaging server instance.
Target instance URL	URL of the target Universal Messaging server instance that has the destination channel or queue for the join.
Filter	Type the filtering criteria, a string or a regular expression. Events will be routed to the destination channel based on the filtering criteria.
Hop count	Type the maximum number of subsequent joins.
Event ID	Last retrieved event ID.
Allow purge	Select to allow purging of events on the channel.
Archival	Select to enable archival join. Archival join is a join between a channel and a queue where events will not be checked for duplication.

Clustering

Before You Create a Universal Messaging Cluster

Before you create or update a Universal Messaging cluster, perform the following tasks:

- Ensure that the server instances that you want to add to the cluster are running.
- Verify that the permissions on the server machines allow connections to the other servers in the cluster.
- Ensure that the `/naming/defaultContext` channel exists only on one or none of the nodes that will form the cluster. The Universal Messaging server instance used as a JNDI provider uses the `/naming/defaultContext` channel to store JMS references and JNDI objects. If the `/naming/defaultContext` channel exists on multiple nodes, you cannot create the cluster.
- Ensure that the keystore and truststore of each server instance in the cluster contain the certificates required for communicating with the rest of the server instances. This is required when the server instances that you want to add to the cluster have only `nsps` or `nhps` interfaces. Perform the following steps for a server instance:
 1. Create a keystore and a truststore.
 2. Import the certificate of the server instance into the keystore.

3. Import the certificates of all servers that you want to add to the cluster into the truststore.
4. Add the paths to the keystore and truststore, and the keystore and truststore passwords, to the corresponding JSSE system properties in the `Server_Common.conf` file of the server instance. The file is located in the *Software AG_directory* `\UniversalMessaging\server\instanceName\bin` directory.

Cluster Configuration Properties

The following tables show the properties you configure when you create a Universal Messaging cluster in Command Central.

Property	Description
Cluster Name	A unique name for the cluster.
Server URL	The server URL (for example, <code>nsp://127.0.0.1:9002</code>) of each server node. When you save the cluster details, the Server Name field is populated with the name of the server corresponding to the specified server URL.
Cluster Site	The name of the site (Optional) to which the server node belongs.
Prime Site	The name of the primary site (Optional), if you have configured sites in the cluster.

Supported Cluster Configuration Tasks

You can perform the following cluster configuration tasks:

- Create a cluster of two or more server instances. The cluster create operation converts the local stores to cluster-wide stores for the selected master node. For the other nodes, the stores must be empty for the cluster create operation to be successful.
- Add one or more server instances to an existing cluster.
- Remove one or more server instances from an existing cluster.
- Upgrade a cluster.
- Create sites and assign server instances to the sites.
- Assign a site as the prime site of a cluster.
- Remove one or more server instances from a cluster site.
- Remove sites from a cluster.
- Delete a cluster. The cluster delete operation does not delete any stores on the nodes.
- Migrate a cluster.

Cluster Migration

You can now automatically migrate Universal Messaging clusters using Command Central composite templates. Use Command Central composite templates to migrate all the Universal Messaging server instances that are part of the cluster, and add the following property to resolve the cluster node connections successfully after migration:

- Add the following property to the `um-cluster` section of the composite template YAML file present in the following directory: `<InstallDir>/profiles/CCE/data/templates/composite :`

```
<ClusterSettings>
  ...
  <ExtendedProperties>
    <Property name="migrationType">SAME_HOST or CROSS_HOST</Property>
  </ExtendedProperties>
</ClusterSettings>
```

Note:

A Universal Messaging server instance mapping file called `remote_realms_bootstrap.conf` containing information about the new Universal Messaging hosts is automatically generated in each of the Universal Messaging server instances. The mapping file is used to identify the new hosts, and to form the new cluster.

General Properties

You can configure a Universal Messaging server instance by editing the server configuration parameters. The Universal Messaging configuration parameters are organized into groups. The parameters in each group are organized in two categories: Basic and Advanced. The properties in the Basic category are commonly used. The properties in the Advanced category are less frequently used and are intended for special cases or expert users.

You can view and configure properties only when the Universal Messaging server instance is running.

The following table lists the property groups and which properties you can configure in each group.

Property Group	Description
Audit Settings	Parameters to configure what gets logged in the audit file.
Client Timeout Values	Parameters to configure client-server communication timeout settings.
Cluster Config	Parameters to configure clustering.
Comet Config	Parameters to configure Comet communication protocol connection.
Connection Config	Parameters to configure client-server connection.

Property Group	Description
Data Stream Config	Parameters to configure data streams.
Environment Config	System environment configuration parameters. You cannot modify the environment configuration parameters, the parameters are read-only.
Event Storage	Parameters to configure how events are stored, and retrieved from the server.
Fanout Values	Parameters to configure delivery of events to the clients.
Global Values	Parameters to configure various global Universal Messaging server instance properties, for example, <code>AllowRealmAdminFullAccess</code> .
Inter-Realm Comms Config	Parameters to configure communication across Universal Messaging server instances.
JVM Management	Parameters to configure the JVM used by the Universal Messaging server.
Join Config	Parameters to modify join properties.
Logging Config	Parameters to modify logging configuration.
Metric Config	Parameters to enable or disable system metrics such as memory usage.
MQTT Config	Parameters to configure MQTT.
Plugin Config	Parameters for Universal Messaging server plugin configuration.
Protobuf Config	Parameters to configure Google protocol buffers.
Protocol AMQP Config	Parameters to configure AMQP connections.
Protocol MQTT Config	Parameters to configure MQTT connections.
RecoveryDaemon	Parameters to configure clients that are in recovery and replaying large number of events.
Server Protection	Parameters to configure server protection such as flow control of producer connections.
Thread Pool Config	Parameters for server thread pools.
TransactionManager	Parameters for Universal Messaging transaction engine.

For more information about the server configuration properties and their values, see [“Realm Configuration” on page 35](#).

Groups

You can add, edit, or delete a security group using the Command Central web user interface.

When you create a group, you must specify a name for the group and add subjects. The subjects can be an existing group or an individual user in the format *user@host*.

Internal Users

You can add new users, list existing users, change the password of a user, and delete a user from the user repository of a Universal Messaging server instance.

Information to authenticate the users of a Universal Messaging server instance is stored in the user repository `users.txt` file. The default location of the `users.txt` file is *Software AG_directory* \common\conf. The `users.txt` file is generated only after you create a new internal user.

The path to the `users.txt` file is added to the `jaas.conf` file present in the *Software AG_directory* \UniversalMessaging\server*instanceName*\bin directory. If you specify a relative path in the `jaas.conf` file, the `users.txt` file is created in a directory relative to the bin directory of the Universal Messaging server instance. You can specify a custom file name instead of the default `users.txt` and a custom path in the `jaas.conf` file.

You can also use the Command Central command-line interface or the `internaluserrepo.bat` and `internaluserrepo.sh` scripts in *Software AG_directory* \common\bin to configure users.

JNDI Connection Factories

You can perform create, get, update, and delete operations on the following connection factory types:

- Connection Factory
- Topic Connection Factory
- Queue Connection Factory
- XA Connection Factory

The following table describes the fields and values to specify when you create or update a connection factory.

Field	Description
Name	Required. Unique name of the new connection factory, for example, <code>connectionfactory1</code> . You cannot edit the name after you create the connection factory.
Type	Type of the connection factory. You cannot edit this field.

Field	Description
Connection URL	<p>Required. Universal Messaging server URL for binding the connection factory, for example, <code>nsp://localhost:9000</code>. To specify a cluster of server instances, use a comma-separated list of connection URLs, for example, <code>nsp://localhost:9000,nsp://localhost:9010</code>. You can use a <i>horizontal scalability</i> connection factory to specify several connection URLs, where each connection URL can point to a standalone realm or a cluster.</p> <p><i>Horizontal scalability</i> connection factories enable clients to publish messages to a set of servers or consume messages from a set of servers in a round-robin manner:</p> <ul style="list-style-type: none"> ■ For round-robin publishing, one message or transaction gets published to the first realm node or cluster, the next message to the next realm node or cluster, and so on. ■ For round-robin consuming, there is no guarantee about the order in which the events are delivered. <p>For a <i>horizontal scalability</i> connection factory, you specify several connection URLs, using the <i>horizontal scalability URL syntax</i>.</p> <p>For information about the syntax, see the section <i>URL Syntax for Horizontal Scalability</i> in the <i>Concepts</i> guide.</p> <p>Consider the following example:</p> <p><code>(UM1,UM2)(UM3,UM4)</code> - Indicates 2 clusters, one consisting of UM1 and UM2 and the other consisting of UM3 and UM4, so only two connections are constructed here.</p> <div style="background-color: #f0f0f0; padding: 5px;"> <p>Note: Round-robin delivery is not supported for XA Connection Factory.</p> </div>
Durable type	Select the durable type for Connection Factory and Topic Connection Factory. The default type is Named .

JNDI Destinations

You can perform create, get, and delete operations on topic and queue JNDI destination types.

Consider the following information when you create a JNDI destination:

- Creating a connection factory and destination with the same name is not allowed for a Universal Messaging server instance.
- Updating a JNDI destination is not supported.

- Deleting a JNDI destination does not delete the channel or queue that exists on the Universal Messaging server instance.

The following table describes the fields and values to specify when you create a JNDI destination.

Field	Description
Lookup name	Required. Unique name of the JNDI destination. Once created, you cannot edit the JNDI destination name. The name can include upper and lower case alphabetic characters, digits (0-9), a double colon (::), slash (/), and periods (.), for example, <code>destination1</code> . Use a double colon (::) to specify a nested name space, for example, <code>destination1::destination2</code> .
Destination type	Type of destination. You cannot edit this field.
Store name	Required. Unique name of the JMS channel or queue. Once created, you cannot edit the store name. The store name can include upper and lower case alphabetic characters, digits (0-9), a double colon (::), and slash (/).
Auto-create JMS channel	Select to enable auto-creation of the JMS channel.
Auto-create JMS queue	Select to enable auto-creation of the JMS queue.

JVM Options

You can add, view, edit, and delete JVM options in the Command Central web-user interface. Restart the Universal Messaging instance for the changes to take effect.

The JVM options are stored in the `Server_Common.conf` file located in the `Software AG_directory \UniversalMessaging\server\instanceName\bin` directory. If you add a custom JVM option, it is added to the `Custom_Server_Common.conf` file. These options are given to the Java Service Wrapper when it launches the JVM.

For more information about the Java Service Wrapper, see *Software AG Infrastructure Administrator's Guide*.

To export the JVM options in XML format, click **Export**. To add a custom JVM option, click **Edit**.

Note:

You can edit, but you cannot delete the default JVM options that are already present.

Java System Properties

You can add, view, edit, and delete Java system properties in the Command Central web-user interface. Restart the Universal Messaging instance for the changes to take effect.

You can perform the following actions:

- To add a custom property or update the value of an existing property, click **Edit**.
- To export the Java system properties in XML format, click **Export**.
- To restore the default value of a property, pass an empty value for the property.

Note:

You cannot delete the default Java system properties that are already present.

The following table shows the Java system properties you can edit.

Property	Description
LICENCE_FILE	Name of the license file.
LICENCE_DIR	Absolute path to the location of the license file.
DATADIR	Absolute path to the location of the data directory.

Note:
Modifying the DATADIR property does not copy the existing data directory to the new location.

License Keys

You can view license details, update the license key, and retrieve the location of the license file for a Universal Messaging server.

Note:

You cannot change the location of a Universal Messaging license file.

Memory

You can view and update the initial memory size and maximum memory size of a Universal Messaging server instance.

Ports

In the Command Central web user interface, you can view, create, enable, disable, and edit all types of Universal Messaging server ports (interfaces).

On the Configuration > Ports page, you can view all the ports configured for a Universal Messaging server instance and the basic port attributes described in the following table.

Field	Description
Enabled	Whether the port is enabled or disabled.

Field	Description
Alias	An alias used to recognize the port. Each port on a Universal Messaging server instance has an associated alias.
Address	<ul style="list-style-type: none"> ■ The number of an NSP, NHP, NHPS, or NSPS port. The port number is unique. ■ The path of an SHM port.
Protocol	<p>The type of the port. The port uses one of the following protocols:</p> <ul style="list-style-type: none"> ■ NSP (Socket protocol) ■ NHP (HTTP protocol) ■ NHPS (HTTPS protocol) ■ NSPS (SSL protocol) ■ SHM (shared memory protocol)

NSP Ports

The following table shows the fields and values to specify when you configure an NSP port (interface) in Command Central.

Field	Description
Enabled	Whether to enable or disable the port.
Adapter alias	An alias for the port. Each Universal Messaging server instance can have an associated alias in the form of <i>host:port</i> . The alias is used to inform other servers how to contact the server, if the server is behind a NAT or a Proxy Server. This alias is not the same as the Universal Messaging assigned interface alias.
Number	Required. A unique port number for the server.
Backlog	The size of the Internet Protocol (IP) socket queue.
Bind address	<p>The IP address to which to bind this port, if your machine has multiple IP addresses and you want the port to use this specific address.</p> <p>You cannot change this attribute after you create the port.</p>
Autostart interface	Whether to automatically start this port when you start the Universal Messaging server instance.
Advertise interface	Allow the Universal Messaging server instance to send information about this port to the client.

Field	Description
Allow for inter-realm	Allow port communication between two or more Universal Messaging server instances. For example, enable communication between clusters or joins.
Allow client connections	Allow clients to connect to this port.
Enable NIO	Enable NIO (Network Input/Output) on this port.
Enable policy server	Enable the port to respond to policy requests. You can run a policy file server on a socket interface that automatically handles these requests. Then you must set up a client access policy in the <code>clientaccesspolicy.xml</code> file in the <code>/install/server/name/plugins/htdocs</code> directory of the server.
Auth time	The time in milliseconds (ms) that the Universal Messaging server instance waits for the client to complete the authentication process. The default value is 10000.
Accept threads	The number of threads that process the accepted sockets.
Select threads	The number of threads allocated for selection.
Send buffer size	The size of the socket send buffer.
Receive buffer size	The size of the socket receive buffer.

NHP Ports

The following table shows the fields and values to specify when you configure an NHP port (interface) in Command Central.

Field	Description
Enabled	Whether to enable or disable the port.
Adapter alias	An alias for the port. Each interface on a Universal Messaging server instance can have an associated alias in the format <code>host:port</code> . The alias is used to tell other servers how to contact the server, if the server is behind a NAT or a Proxy Server. This alias is not the same as the Universal Messaging assigned interface alias.
Number	Required. A unique port number for the server.
Backlog	The size of the Internet Protocol (IP) socket queue.
Bind address	The IP address to which to bind this port, if your machine has multiple IP addresses and you want the port to use this specific address.

Field	Description
	You cannot change this attribute after you create the port.
Autostart interface	Whether to automatically start the port when you start the Universal Messaging server instance.
Advertise interface	Allow the Universal Messaging server instance to send information about this port to the client.
Allow for inter-realm	Allow port communication between two or more Universal Messaging server instances. For example, allow communication between clusters or joins.
Allow client connections	Allow clients to connect to the port.
Enable NIO	Enable NIO (Network Input/Output) on the port.
Enable HTTP 1.1	Enable the usage of HTTP 1.1 protocol on the port.
Auth time	The time in milliseconds (ms) that the Universal Messaging server instance waits for the client to complete the authentication process. Default is 10000 milliseconds.
Accept threads	The number of threads that process the accepted sockets.
Select threads	The number of threads allocated for selection.
Send buffer size	The size of the socket send buffer.
Receive buffer size	The size of the socket receive buffer.

NHPS Ports

The following tables show the fields and values to specify when you configure an NHPS port (interface) in Command Central.

Connection Basics

Field	Description
Enabled	Whether to enable or disable the port.
Adapter alias	An alias for the port. Each Universal Messaging server instance can have an associated alias in the form of <i>host:port</i> . The alias is used to tell other servers how to contact this server, if this server is behind a NAT or a Proxy Server. This alias is not the same as the Universal Messaging assigned interface alias.
Number	Required. A unique port number.
Backlog	The size of the Internet Protocol (IP) socket queue.

Field	Description
Bind address	The IP address to which to bind this port, if your machine has multiple IP addresses and you want the port to use this specific address. You cannot change this attribute after you create the port.
Autostart interface	Whether to automatically start this port when you start the Universal Messaging server instance.
Advertise interface	Allow the Universal Messaging server instance to send information about this port to the client.
Allow for inter-realm	Allow port communication between two or more Universal Messaging server instances. For example, allow communication between clusters, or joins.
Allow client connections	Allow clients to connect to the port.
Enable NIO	Enable NIO (Network Input/Output) on the port.
Enable HTTP 1.1	Enable the usage of HTTP 1.1 protocol on the port.
Auth time	The time in milliseconds (ms) that the Universal Messaging server instance waits for the client to complete the authentication process. The default value is 10000.
Accept threads	The number of threads processing the accepted sockets.
Select threads	The number of threads allocated for selection.
Send buffer size	The size of the socket send buffer.
Receive buffer size	The size of the socket receive buffer.

JavaScript Interface Properties

Set these properties to configure communication with web clients using JavaScript.

Field	Description
Enable JavaScript	Enable JavaScript client connections using this port.
Enable WebSockets	Toggle the ability for clients to communicate with the server using the HTML WebSocket Protocol on this interface.
Enable GZIP for long poll	Enable GZIP compression on HTTP long poll connections.
CORS allow credentials	Allow Cross-Origin Resource Sharing (CORS) credentials.

Field	Description
CORS allowed origins	<p>A comma-separated list of the host names (and IP addresses if they appear in URLs) of the servers that host your JavaScript application's HTML files.</p> <p>Important: If this property is not set correctly, many communication drivers available to JavaScript clients may fail.</p>
Long poll active delay	The time between clients sending long poll requests to the server in milliseconds. Reducing this may reduce latency but will increase both client and server memory, CPU, and network usage.
GZIP minimum threshold	The minimum message size in bytes required for the server to begin compressing data sent to long poll clients.
Long poll idle delay	The time between clients sending long poll when the client is in idle mode.

Custom Headers

Custom headers are paired with Header Key/Value pairs that are sent in the HTTP packets to the client.

Security Configuration

Field	Description
Client authentication	<p>Whether or not Universal Messaging requires client certificates for all requests. Select:</p> <ul style="list-style-type: none"> ■ None if Universal Messaging does not require client certificates for all requests. ■ REQUIRE_CERTIFICATE if you want Universal Messaging to require client certificates for all requests.
Keystore type	File type of the keystore file. Universal Messaging supports the JKS and PKCS12 file types. The default file type is PKCS12.
Keystore server location	Location of the keystore file.
Keystore password	Password required to access the SSL certificate in the keystore file.
Keystore key password	Password required to access a specific private key in the keystore file.
Truststore type	File type of the truststore file. Universal Messaging supports the JKS and PKCS12 file types. The default file type is PKCS12.

Field	Description
Truststore server location	Location of the truststore file.
Truststore password	Password required to access the SSL certificate in the truststore file.

NSPS Ports

The following tables show the fields and values to specify when you configure an NSPS port (interface) in Command Central.

Connection Basics

Field	Description
Enabled	Whether to enable or disable the port.
Adapter alias	An alias for the port. Each Universal Messaging server instance can have an associated alias in the form of <i>host:port</i> . The alias is used to tell other servers how to contact the server if the server is behind a NAT or a Proxy Server. This alias is not the same as the Universal Messaging assigned interface alias.
Number	Required. A unique port number.
Backlog	The size of the Internet Protocol (IP) socket queue.
Bind address	The IP address to which to bind this port, if your machine has multiple IP addresses and you want the port to use this specific address. You cannot change this attribute after you create the port.
Autostart interface	Whether to automatically start the port when you start the Universal Messaging server instance.
Advertise interface	Allow the Universal Messaging server instance to send information about this port to the client.
Allow for inter-realm	Allow port communication between two or more Universal Messaging server instances. For example, allow communication between clusters or joins.
Allow client connections	Allow clients to connect to the port.
Enable NIO	Enable NIO (Network Input/Output) on the port.
Enable policy server	Enable the port to respond to policy requests. You can run a policy file server on a socket interface that will automatically handle these requests. Then you must set up a client access policy

Field	Description
	in the clientaccesspolicy.xml file in the /install/server/name/plugins/htdocs directory of the server.
Auth time	The time in milliseconds (ms) that the Universal Messaging server instance waits for the client to complete the authentication process. The default value is 10000.
Accept threads	The number of threads that process the accepted sockets.
Select threads	The number of threads allocated for selection.
Send buffer size	The size of the socket send buffer.
Receive buffer size	The size of the socket receive buffer.

Security Configuration

Field	Description
Client authentication	Whether or not Universal Messaging requires client certificates for all requests. Select: <ul style="list-style-type: none"> ■ None if Universal Messaging does not require client certificates for all requests. ■ REQUIRE_CERTIFICATE if you want Universal Messaging to require client certificates for all requests.
Keystore type	File type of the keystore file. Universal Messaging supports the JKS and PKCS12 file types. The default file type is PKCS12.
Keystore server location	Location of the keystore file.
Keystore password	Password required to access the SSL certificate in the keystore file.
Keystore key password	Password required to access a specific private key in the keystore file.
Truststore type	File type of the truststore file. Universal Messaging supports the JKS and PKCS12 file types. The default file type is PKCS12.
Truststore server location	Location of the truststore file.
Truststore password	Password required to access the SSL certificate in the truststore file.

SHM Ports

The following table shows the fields and values to specify when you configure an SHM port (interface) in Command Central.

Field	Description
Enabled	Whether to enable or disable the port.
Path	The directory in which the files required for SHM (shared memory) communication are created. The default value is /dev/shm. Note: When you choose a path, ensure that the local ID of the server can access this directory.
Buffer size	The size in bytes of the allocated memory that a connection uses. The default value is 1024000. A file of the same size is also created for mapping.
Timeout	The idle time in milliseconds before a connection is closed. The default value is 20000.

Queues

The following tables show the properties you can configure when you create a queue in Command Central.

Queue Properties

Property	Description
Name	Required. Name of the queue to be created. You cannot edit the queue name.
Type	Type of the queue. The Universal Messaging queue types are: <ul style="list-style-type: none"> ■ Reliable ■ Persistent ■ Mixed (default)
TTL (ms)	Specifies how long (in milliseconds) each event is retained in the queue after being published. For example, if you specify a TTL of 10000, the events on the queue will be automatically removed by the server after 10000 milliseconds. Specify 0 for events to remain on the queue indefinitely.
Capacity	Event capacity of the queue. Specifies the maximum number of events that can be on a queue once published. Specify 0 to store unlimited events. The maximum queue capacity is 2147483646.

Property	Description
Dead event store	Channel or queue to be used to store events that are purged before being consumed.
Cluster-wide	Selected automatically if the Universal Messaging server instance is part of a cluster.
Protobuf descriptor	Absolute path to the Protocol Buffer descriptor file that is stored on the machine where Software AG Platform Manager is installed.

Storage Properties

Property	Description
Auto-maintenance	Select to retain events till they reach their TTL. Cancel the selection to purge events from the queue storage file.
Honor capacity	Select to prevent publishing of data when the queue is full. Cancel the selection to purge the oldest published event.
Enable caching	Select for the events to be stored in the cache memory and reused. Cancel the selection to read and stored in the file store.
Cache on reload	Select to enable caching during reload.
Enable read buffering	Select to enable read buffering for the store on the Universal Messaging server.
Enable multicast	Select to enable multicast client to receive events over multithread connections.
Read buffer size	Read buffer size in bytes.
Sync each write	Select to sync each write to the file system.
Sync batch size	Configurable only when Sync each write is selected. Number of events that is to be synced with the file system at once.
Sync batch time	Configurable only when Sync each write is selected. Time in milliseconds (ms) between syncs with the file system.
Priority	Priority range. 0 (lowest) to 9 (highest).
Events per spindle	Maximum number of events allowed per file.
Stamp dictionary	Select to stamp events on the channel by the server.

Queue ACL

Column	Description
Name	User name in the format <code>user@host</code> or the name of an existing group.
Manage ACL	Select to allow the user or group to manage ACLs.
Full	Select to grant full privileges to the user or group.
Purge	Select to allow the user or group to purge events.
Peek	Select to allow the user or group to peek events.
Push	Select to allow the user or group to push events.
Pop	Select to allow the user or group to pop events.

Joins

You can view the following join properties:

Column	Description
Type	Type of join.
Destination name	Destination channel.
Target instance name	Name of the target instance. Required only if the target channel is in a remote Universal Messaging server instance.
Target instance URL	URL of the target Universal Messaging server instance that has the destination channel for the join.
Remote node	Destination channel.
Hop count	Maximum number of subsequent joins.
Event ID	Last retrieved event ID.
Allow purge	Allow purging of events in the queue.
Archival	Archival join is a join between a channel and a queue where events will not be checked for duplication.

Realm ACL

The following table describes the fields and values to specify when you configure permissions for a Universal Messaging server instance.

Field	Description
Subject	User name in the format <i>user@host</i> or name of an existing group in the format <i>groupname</i> .
Manage ACL	Allow ACL management.
Full	Grant full privileges to the user or group.
Access	Allow access to the realm.
Configure	Allow realm configuration.
Channels	Allow channel configuration and administration.
Realm	Allow realm configuration and management.
Admin API	Allow use of Universal Messaging Admin API.
Manage data groups	Allow management of data groups.
Own data groups	Allow ownership of data groups.
Publish to data groups	Allow publishing to global data groups.

Zones

Zones are a logical grouping of one or more Universal Messaging server instances (realms) that maintain active connections to each other. Each Universal Messaging server instance can be a member of zero or one zone, but a server instance cannot be a member of more than one zone. For more information about zones, see the Zones section in the Universal Messaging Concepts guide.

You can create, edit, or delete a zone using the Command Central web user interface. You can create either a **Zone with Realms** consisting of one or more realms, or a **Zone with Clusters** consisting of one or more Universal Messaging clusters. You can export the zone configuration using the **Export** option.

Important:

If the server instances that you want to add to the zone have only `nsps` or `nhps` interfaces, ensure that the keystore and truststore of each server instance contain the certificates required for communicating with the rest of the server instances. To do so for a server instance:

1. Create a keystore and a truststore.
2. Import the certificate of the server instance into the key store.
3. Import the certificates of all servers that you want to add to the zone into the truststore.
4. Add the paths to the keystore and truststore, as well as the keystore and truststore passwords, to the corresponding JSSE system properties in the `Server_Common.conf` file of the server instance. The file is located in the *Software AG_directory* `\UniversalMessaging\server\instanceName\bin` directory.

The table following table describes the fields and values to specify when you create a zone with realms or a zone with clusters.

Field	Description
Zone name	Required. Name of the zone used to uniquely identify this zone.
Servers (for Zone with Realms) or Clustered servers (for Zone with Clusters)	<p>Required. Server URL and name if you are creating a Zone with Realms, or one or all of the cluster nodes if you are creating a Zone with Clusters.</p> <ul style="list-style-type: none"> ■ Server URL: Universal Messaging server URL. ■ Server name: Name of the Universal Messaging server. ■ Cluster configuration: Automatically populated with the cluster name.
	<p>Note: You can provide any cluster node and all the running nodes of the cluster are added to the zone.</p>

Securing Access to Command Central

Changing the Authentication Mode

1. Click the Instances tab to view all the available Universal Messaging server instances.
2. Click an Universal Messaging instance name to access the Dashboard.

The Dashboard contains information about the specific Universal Messaging server instance such as status, alerts, and KPIs.

3. In the Details section of the Dashboard, click  in the **Authentication** field to change the authentication mode.

The **Authentication Mode** dialog box appears.

4. Select one of the following authentication modes:
 - **System default:** Use default authentication method.
 - **None:** No authentication method is used.
 - **Trusted:** Password-less authentication for predefined administrative user account.
 - **Delegated:** SAML-based authentication and authorization for the currently logged in user.
 - **Fixed user:** Authenticate the specified administrative user credentials. Provide a user name and password for the user.

Note:

To use basic authentication, you must change the authentication mode for a run-time component to **Fixed User**. Command Central uses basic authentication with a fixed user to communicate with Platform Manager. With **Fixed User** authentication, the authentication credentials for the Platform Manager will be fixed.

Verifying the Outbound Authentication Settings

Use the following steps to verify that Command Central is configured with the correct outbound authentication settings.

> To verify that Command Central is configured with the correct user credentials

1. In Command Central, on the Overview tab for the product component, click . Check that the product status is **Online** and the JVM KPIs are updated.
2. On the Logs tab, check the product log for authentication errors.

Using Unix Shell Scripts to Change Connection Credentials for Managed Products

You can use the following sample UNIX shell script to configure basic authentication credentials for product components managed by Command Central.

```

NODE_ALIAS=local
USERNAME=Administrator
PASSWORD=secret
RCID=integrationServer-default
# RCID=MwsProgramFiles-default
# RCID=Universal-Messaging-nirvana
# RCID=OSGI-CTP
# RCID=OSGI-InfraDC

sagcc get configuration data $NODE_ALIAS $RCID COMMON-LOCAL-USERS-Administrator

-o administrator.xml
sed "s,/>, <<Password>${PASSWORD}</Password></User>,g" administrator.xml >
  administrator_new.xml
sagcc update configuration data $NODE_ALIAS $RCID COMMON-LOCAL-USERS
-Administrator -o administrator_new.xml

# verify connection
sagcc get monitoring runtimestatus $NODE_ALIAS $RCID -e ONLINE

```

Enabling Basic Authentication for Universal Messaging Users

Perform the following steps to enable basic authentication for Universal Messaging server instance users. For more information about authentication, see the Authentication Overview section in the Universal Messaging Concepts guide.

Important:

JAAS Authentication with Software AG Security infrastructure component is required for completing basic authentication configuration, for more information see the Server JAAS Authentication with Software AG Security infrastructure component section in the Universal Messaging Concepts guide.

1. Use the **Internal Users** configuration type in Command Central if you want to add new internal users.
2. Use the **Realm ACL** configuration type to add internal users in the format `username@host` and configure the Access Control Lists (ACLs) of the server. For more information about how to manage ACLs, see [“Realm ACL” on page 210](#).
3. Change the default Authentication Mode from **None** to **Fixed User** and provide a new user name and password. For more information about how to change the authentication mode, see [“Changing the Authentication Mode” on page 212](#).

Administering Universal Messaging

You can administer and monitor channels, durable subscribers, and queues on the Universal-Messaging-*instanceName* > Administration page in Command Central.

In addition, you can publish events and snoop on events on a channel or queue.

Administering Channels

You can view the following details about a channel on the Universal-Messaging-*instanceName* > Administration > Channels page in Command Central:

Attribute	Description
Name	The name of the channel.
Event ID	The event ID of the last event that was consumed from the channel. The event ID is -1 when the channel is empty.
Events	The number of events on the channel that are yet to be consumed.
Current connections	The number of current connections to the channel.
% Free	The percentage of free storage available on the channel.

Select a channel to view detailed information about the status of the channel and the durable subscribers (named objects) subscribed to the channel. You can also delete a durable subscriber subscribed to the channel.

Administering Durable Subscribers

You can search, monitor, and delete durable subscribers on the Universal-Messaging-*instanceName* > Administration > Durable Subscribers page in Command Central. You can also browse events on a specific durable subscriber and purge events for shared durable subscribers.

The table displays the following durable subscriber attributes.

Attribute	Description
Name	The name of the durable subscriber.
Channel	The name of the channel to which the durable subscriber belongs.
Durable type	The type of durable subscriber (Shared, Serial, or Durable).
Last event ID	The event ID of the last successfully consumed event.
Outstanding events	The number of events outstanding for a particular durable subscriber.
	<p>Note: The outstanding event count displayed for a non-shared durable is only an estimate.</p>
Last read time	The last date and time when the durable subscriber read, committed, or rolled back an event.

Select a durable subscriber to perform the following operations:

- View durable details.
- Browse events.
- Bulk purge.

The Durable details page contains the following information about a durable subscriber:

Details

Attribute	Description
Name	The name of the durable subscriber.
Channel	The name of the channel to which the durable subscriber belongs.
Durable type	The type of durable subscriber (Shared, Serial, or Durable).

Attribute	Description
Cluster-wide	Whether the durable subscriber is on a channel that is part of a Universal Messaging cluster.
Persistent	Whether the durable subscriber is persistent. Persistent durable subscribers retrieve the last event ID consumed before the Universal Messaging server instance was restarted.
Selector	Events are filtered based on the defined selector.

Status

Attribute	Description
Last event ID	The event ID of the last successfully consumed event.
Total events	The number of outstanding events for the durable subscriber.
Pending events	The number of outstanding events waiting for a commit or a rollback.
Last read time	The last date and time when the durable subscriber read, committed, or rolled back an event.
Last write time	The last time the durable was written to. Typically, this is the last time an event was added to the durable subscriber.

Connections

Attribute	Description
ID	The connection ID.
Mode	The client subscription mode (subscription based or getNext).
Max pending	The window size specified by the client.
Acknowledged	The total acknowledged events.
Rolled back	The total rolled-back events.
Pending	The event queues waiting to be acknowledged or rolled back.
Last read time	The last time the session acknowledged, rolled back, or read an event from the durable subscriber.

The Browse events page displays the event list and lets you to browse events for a durable subscriber. Events are displayed in the order of old to new. A maximum of 1000 events are displayed in the table with a maximum combined size of 10 MB. For example, if two events of size 10 MB and 100 MB are present for the durable subscriber, only the event of size 10 MB is displayed, and no other events are displayed. Click **Browse events** to refresh the events displayed in the table.

Attribute	Description
Event ID	A unique ID to identify the event.
TTL (ms)	Specifies how long (in milliseconds) each event is retained. Note: You can publish an event with a specified TTL only on queues and channels of type Mixed. Events on queues and channels of type Persistent or Reliable use the TTL set on store level and ignore any event-level TTL.
Tag	The tag information of the event if an event tag exists.
Event data	The content of the event. For Protobuf events, the content is a JSON string.
Event size (bytes)	The size of the event in bytes. The event size is the total size of the event that is the sum of the event data and event properties.
Event properties	The event properties represented as key-value pairs.
Persistent	Whether the event is persistent or not.

When you select an event ID in the table, you can view additional details about the event including the type of event (persistent, transient, or Protobuf event), a hexadecimal view of the event data, an ASCII representation of the event data, the header and properties of the event. If the event is a Protobuf event and its tag matches the name of a Protobuf file descriptor that has already been uploaded on the channel, the ASCII representation of the event is the decoded Protobuf content in JSON format.

Use the **Bulk purge** option to purge events in bulk for a durable subscriber. You can purge events by providing an event range and event filter, or purge all the events.

Administering Queues

You can view the following details about a queue on the `Universal-Messaging-instanceName > Administration > Queues` page in Command Central:

Attribute	Description
Name	The name of the queue.
Event ID	The event ID of the last event that was popped from the queue. The event ID is -1 if the queue is empty.
Events	The number of events in the queue that are yet to be consumed.
Current connections	The number of current connections to the queue.
% Free	The percentage of free storage available on the queue.

Select a queue to view detailed information about the status of the queue.

Snooping on Channels

When you select a channel on the Universal-Messaging-*instanceName* > Administration > Channels page in Command Central, you can perform the following operations:

- Start snooping on events on the channel.
- Stop snooping on events on the channel.
- View details about a snooped event.
- Purge one or more events from the channel.

Considerations When Snooping on Channels

Consider the following information when you want to snoop on events on a channel:

- Snooping on events on a channel is performed per user. Only the user who started snooping can stop it. However, Command Central allows more than one person to log in as Administrator at the same time, which might result in simultaneous attempts to perform various snooping operations on the same channel.
- When snooping is inactive for five minutes, for example, because the user logged off or navigated away from the channel details page, the snoop stops automatically.
- If the Universal Messaging server becomes unavailable after the snoop on the channel started, Command Central stops snooping on all channels on that Universal Messaging server for all Command Central users. If you try to start snooping while the Universal Messaging server is still unavailable, Command Central returns an error.

Starting the Channel Snoop

➤ To start snooping on events on a channel

1. In Command Central, go to **Environments > Instances > All > Universal-Messaging-*instanceName* > Administration > Channels**.
2. Select the channel on which you want to start snooping on events, and then click the **Snoop** tab.
3. Do one of the following:
 - To snoop on all events published on the channel, click **Start**.
 - To snoop on a range of events, in the **From Event ID** field specify the ID of the first event in the range, and in the **To Event ID** field, specify the ID of the last event in the range. Click **Start**. You can also specify additional filtering criteria based on the properties of the event.

Note:

If you do not specify a value in the **From Event ID** field, the range of events starts with the first event on the channel and ends with the event specified in the **To Event ID** field. If you do not specify a value in the **To Event ID** field, the range of events starts with the event specified in the **From Event ID** field and ends with the last event on the channel.

Command Central populates the snooped events table with the events published on the channel.

Stopping the Channel Snoop

➤ To stop snooping on events on a channel

1. In Command Central, go to **Environments > Instances > All > Universal-Messaging-*instanceName* > Administration > Channels**.
2. Select the channel on which you want to stop snooping.
3. Click the **Snoop** tab, and then click **Stop**.

Viewing Channel Event Details

After you start snooping on a channel in the Command Central web user interface, the snooped events table on the channel details page displays information about each event including the event ID, tag, time to live (TTL), and data, as well as whether the event is persistent.

When you select an event in the table, you can view additional details about the event including the type of event (persistent, transient, or Protobuf event), a hexadecimal view of the event data, an ASCII representation of the event data, the header and properties of the event, and the Protobuf descriptor for Protobuf events.

If the event is a Protobuf event and its Protobuf descriptor matches the name of a Protobuf file descriptor that has already been uploaded on the channel, the ASCII representation of the event is the decoded Protobuf content in JSON format.

Purging Snooped Events from a Channel

After you start snooping on a channel, you can purge snooped events from the channel. You can purge a single event, a range of events, or all events.

For information about how to start snooping, see [“Starting the Channel Snoop” on page 218](#).

➤ To purge events

1. In Command Central, go to **Environments > Instances > All > Universal-Messaging-*instanceName* > Administration > Channels**.
2. Select the channel on which you want to purge snooped events, and then click the **Snoop** tab.

3. (Optional) To purge a single event directly from the snooped events table, click .
4. Click **Purge Events** and on the Purge Events page, do one of the following:
 - To purge all events, click **Purge**.
 - To purge a range of events, in the **From Event ID** field specify the ID of the first event in the range, and in the **To Event ID** field, specify the ID of the last event in the range. Then click **Purge**.

Note:

If you do not specify a value in the **From Event ID** field, the range of events to purge starts with the first event on the channel and ends with the event specified in the **To Event ID** field. If you do not specify a value in the **To Event ID** field, the range of events to purge starts with the event specified in the **From Event ID** field and ends with the last event on the channel.

Snooping on Queues

When you select a queue on the Universal-Messaging-*instanceName* > Administration > Queues page in Command Central, you can perform the following operations:

- Start snooping on events on the queue.
- Stop snooping on events on the queue.
- View details about a snooped event.
- Purge all events from the queue.

Considerations When Snooping on Queues

Consider the following information when you want to snoop on events on a queue:

- Snooping on events on a queue is performed per user. Only the user who started snooping can stop it. However, Command Central allows more than one person to log in as Administrator at the same time, which might result in simultaneous attempts to perform various snooping operations on the same queue.
- When snooping is inactive for five minutes, for example, because the user logged off or navigated away from the queue details page, the snoop stops automatically.
- If the Universal Messaging server becomes unavailable after the snoop on the queue started, Command Central stops snooping on all queues on that Universal Messaging server for all Command Central users. If you try to start snooping while the Universal Messaging server is still unavailable, Command Central returns an error.

Starting the Queue Snoop

> To start snooping on events on a queue

1. In Command Central, go to **Environments > Instances > All > Universal-Messaging-*instanceName* > Administration > Queues**.
2. Select the queue on which you want to start snooping on events, and then click the **Snoop** tab.
3. Do one of the following:
 - To snoop on all events published on the queue, click **Start**.
 - To snoop on a range of events, in the **From Event ID** field specify the ID of the first event in the range, and in the **To Event ID** field, specify the ID of the last event in the range. Click **Start**. You can also specify additional filtering criteria based on the properties of the event.

Note:

If you do not specify a value in the **From Event ID** field, the range of events starts with the first event on the queue and ends with the event specified in the **To Event ID** field. If you do not specify a value in the **To Event ID** field, the range of events starts with the event specified in the **From Event ID** field and ends with the last event on the queue.

Command Central populates the snooped events table with the events published on the queue.

Stopping the Queue Snoop

> To stop snooping on events on a queue

1. In Command Central, go to **Environments > Instances > All > Universal-Messaging-*instanceName* > Administration > Queues**.
2. Select the queue on which you want to stop snooping.
3. Click the **Snoop** tab, and then click **Stop**.

Viewing Queue Event Details

After you start snooping on a queue in the Command Central web user interface, the snooped events table on the queue details page displays information about each event including the event ID, tag, time to live (TTL), and data, as well as whether the event is persistent.

When you select an event in the table, you can view additional details about the event including the type of event (persistent or Protobuf event), a hexadecimal view of the event data, an ASCII representation of the event data, the header and properties of the event, and the Protobuf descriptor for Protobuf events.

If the event is a Protobuf event and its Protobuf descriptor matches the name of a Protobuf file descriptor that has already been uploaded on the queue, the ASCII representation of the event is the decoded Protobuf content in JSON format.

Purging Snooped Events from a Queue

After you start snooping on a queue, you can purge all snooped events from the queue.

For information about how to start snooping, see [“Starting the Queue Snoop” on page 220](#).

> To purge events

1. In Command Central, go to **Environments > Instances > All > Universal-Messaging-*instanceName* > Administration > Queues**.
2. Select the queue on which you want to purge snooped events, and then click the **Snoop** tab.
3. (Optional) To purge a single event directly from the snooped events table, click .
4. Click **Purge Events** and on the Purge Events page, do one of the following:
 - To purge all events, click **Purge**.
 - To purge a range of events, in the **From Event ID** field specify the ID of the first event in the range, and in the **To Event ID** field, specify the ID of the last event in the range. Then click **Purge**.

Note:

If you do not specify a value in the **From Event ID** field, the range of events to purge starts with the first event on the queue and ends with the event specified in the **To Event ID** field. If you do not specify a value in the **To Event ID** field, the range of events to purge starts with the event specified in the **From Event ID** field and ends with the last event on the queue.

Publishing Events

Publishing Events on a Channel or Queue

Use the following procedure to create a new event and publish it on a Universal Messaging channel or queue, using the Command Central web user interface.

> To publish an event on a channel or queue

1. In Command Central, go to **Environments > Instances > All > Universal-Messaging-*instanceName* > Administration**.

2. Do one of the following:
 - To publish an event on a channel, from the drop-down menu, select **Channels** and then select the channel on which you want to publish the event.
 - To publish an event on a queue, from the drop-down menu, select **Queues** and then select the queue on which you want to publish the event.
3. Click the **Publish** tab and specify values for the following fields as required:

Property	Value
Event data	Required. The content of the event.
Tag	Optional. The tag of the event.
TTL (ms)	Optional. The time-to-live (TTL) of the event in milliseconds. Defines how long the event remains available on the channel or queue. If you specify a TTL of 0, the event remains on the channel or queue indefinitely. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p>Note: You can publish an event with a specified TTL only on queues and channels of type Mixed. Events on queues and channels of type Persistent or Reliable use the TTL set on store level and ignore any event-level TTL.</p> </div>
Persistent	Optional. Whether the event is persistent.
Transient	Optional. Supported only for channels. Whether the event is transient.
Properties	Optional. Click  to add event properties. For each property, specify the name, type, and value.
Number of publishes	Optional. The number of times to publish the event. If you do not select the option, it defaults to 1.
Publish as a Protobuf event	Optional. Whether to send the event as a Protobuf event. For more information about how to publish Protobuf events, see “Publishing Protobuf Events” on page 224 .
Protobuf descriptor	Required only for Protobuf events. The Protobuf file descriptor that defines the message schema used for converting the event data to a Protobuf event.

4. Click **Publish**.

When you start snooping on events on the channel or queue, Command Central displays the event in the snooped events table.

For information about how to snoop on channels and queues, see [“Snooping on Channels” on page 218](#) and [“Snooping on Queues” on page 220](#).

Publishing Protobuf Events

Perform the following actions to publish a Protobuf event, using the Command Central web user interface:

1. Before publishing the Protobuf event, upload on the channel or queue the Protobuf file descriptor that defines the Protobuf schema, as part of a file descriptor set. For information about uploading a Protobuf file descriptor set on a channel or queue, see [“Channels” on page 190](#) or [“Queues” on page 208](#).
2. When you create the event on the **Publish** tab for a channel or queue, do the following:
 - a. In the **Event data** field, specify a JSON string that represents the Protobuf event.
 - b. Select the **Publish as a Protobuf event** option.
 - c. In the **Protobuf descriptor** field, specify the name of the Protobuf file descriptor that defines the message schema.

Important:

If you do not specify a Protobuf descriptor or if the specified Protobuf descriptor value does not correspond to any Protobuf file descriptor on the channel or queue, the system returns an error that no Protobuf descriptor was found on the channel or queue and does not create a Protobuf event.

For information about how to publish events, see [“Publishing Events on a Channel or Queue” on page 222](#).

For more information about working with Protobuf events, see the "Google Protocol Buffers" section in the *Universal Messaging Concepts* guide.

Republishing Events on a Channel or Queue

Before republishing a snooped event, you must start snooping on the channel or queue. For information about how to start snooping, see [“Snooping on Channels” on page 218](#) and [“Snooping on Queues” on page 220](#).

➤ To republish an event

1. In Command Central, go to **Environments > Instances > All > Universal-Messaging-*instanceName* > Administration**.
2. Do one of the following:
 - To republish an event on a channel, from the drop-down menu, select **Channels** and then select the channel on which you want to republish the event.

- To republish an event on a queue, from the drop-down menu, select **Queues** and then select the queue on which you want to republish the event.
3. Click the **Snoop** tab and then click the snooped event that you want to republish.
 4. Click **Republish** and modify the event fields as required.
 5. Optionally, select **Purge Original Event**.
 6. Click **Publish**.

Viewing Universal Messaging Run-time Monitoring Statuses

The Command Central instances page displays the run-time status of a Universal Messaging server instance in the status column. The Universal Messaging can have one of the following run-time status:

- Online  : Server instance is online.
- Failed  : Server instance failed. For example, the Universal Messaging server instance stopped unexpectedly due an error or system failure.
- Stopped  : Server instance is not running.
- Stopping  : Server instance is stopping.
- Unresponsive  : Server instance is running, but it is unresponsive. When none of the server interfaces are connected to the server.
- Unknown  : Server instance status cannot be determined.

When you have set up a Universal Messaging cluster, the run-time status indicates if a server instance is:

- Online Master  : Server instance is online and it is the master node in the cluster.
- Online Slave  : Server instance is online and it is the slave node in the cluster.
- Error  : Server instance is part of a cluster that does not satisfy the requisite quorum.

Viewing Universal Messaging KPIs

You can view the following key performance indicators (KPIs) to monitor the performance of the Universal Messaging servers:

KPI	Description
JVM Memory	<p>Indicates the utilization of JVM memory.</p> <p>The marginal, critical, and maximum values for this KPI depend on the maximum memory size of the JVM.</p> <ul style="list-style-type: none">■ Marginal is 80% of the maximum JVM memory.■ Critical is 95% of the maximum JVM memory.■ Maximum is 100% of the maximum JVM memory.
Fanout Backlog	<p>Indicates the total number of events currently waiting to be processed by the fanout engine. If the fanout backlog is more than the critical value, there is a possibility that the subscribers receive the published events after some delay.</p> <p>The KPI uses the following marginal, critical, and maximum values:</p> <ul style="list-style-type: none">■ Marginal is 80% of the maximum value.■ Critical is 95% of the maximum value.■ Maximum is 100% of the peak value (high-water mark) of fanout backlog. Default is 100.
Queued Tasks	<p>Indicates the total number of tasks in the read, write, and common read/write pools. If the number of read and write tasks queued is more than the critical value, it indicates that the Universal Messaging server is unable to match the speed of the publishers and subscribers.</p> <p>The KPI uses the following marginal, critical, and maximum values:</p> <ul style="list-style-type: none">■ Marginal is 80% of the maximum value.■ Critical is 95% of the maximum value.■ Maximum is 100% of the peak value (high-water mark) of read and write tasks queued. Default is 100.

Viewing Universal Messaging Logs

You can view, search, and download all Universal Messaging logs on the **Logs** tab for a server instance in the Command Central web-user interface. You can view the alias and size of a log, and when it was last updated. You can also click a log to view and search its contents.

Viewing Universal Messaging Inventory

When you view installations in an environment, Command Central displays the Universal Messaging server instances listed in the *Software AG_directory \UniversalMessaging\server* directory of an installation. Command Central lists all the folders (except the templates) in the server directory.

Configuration Types That the Universal Messaging Server Supports

The Universal Messaging realm server run-time component supports creating instances of the configuration types listed in the following table.

Configuration Type	Use to...
COMMON-LOCAL-USERS	Configure and manage users of a Universal Messaging server instance. COMMON-LOCAL-USERS- <i>userId</i> supports configuring the user ID and password of each user. By default, the users have administrator privileges for the Universal Messaging server instance.
COMMON-LICENSE	Configure the Universal Messaging-specific SagLic license file.
COMMON-LICLOC	View the location of a Universal Messaging server instance's license file. You cannot change the location of the license file.
COMMON-JAVASYSPROPS	Extended Java system properties.
COMMON-JVM-OPTIONS	Extended JVM options.
UM-JNDI-CF	Configure the following JNDI connection factories: <ul style="list-style-type: none"> ■ Connection Factory ■ Topic Connection Factory ■ Queue Connection Factory ■ XA Connection Factory
UM-JNDI-DEST	Configure the following JNDI destinations: <ul style="list-style-type: none"> ■ Topics ■ Queues
COMMON-CLUSTER	Configure an active/active Universal Messaging cluster.

Configuration Type	Use to...
COMMON-MEMORY	Configure the initial memory size and maximum memory size of a Universal Messaging server instance.
COMMON-PORTS	Configure the Universal Messaging server interfaces. <div style="background-color: #f0f0f0; padding: 5px;">Note:<ul style="list-style-type: none">■ You cannot change the protocol, bind address, port number, or alias of a port of an existing server interface.■ If you change the SSL certificates of a secured interface, you must restart the interface.</div>
UM-ZONE	Create and manage Universal Messaging zones.
UM-CHANNELS	Create and manage Universal Messaging channels.
UM-QUEUES	Create and manage Universal Messaging queues.
UM-REALM-ACL	Manage Universal Messaging Access Control List (ACL).
UM-GROUPS	Manage Universal Messaging security groups.
COMMON-SYSPROPS	DEPRECATED. Use COMMON-JAVASYSPROPS.

Using the Command Line to Manage Universal Messaging

The information about the Command Central commands that Universal Messaging supports is organized into topics based on functionality. You can find reference information about how to perform the following tasks from the command line:

- Manage Universal Messaging server instances.
- Configure Universal Messaging.
- Administer Universal Messaging.
- Deploy Universal Messaging assets.

For general information about using the commands, see *Software AG Command Central Help*.

Universal Messaging Instance Management

Create Instances

Creates an instance of a Universal Messaging realm server, Enterprise Manager, or Template Applications.

Syntax

```
sagcc create instances nodeAlias
NUMRealmServer|NUMEnterpriseManager|NUMTemplateApplications instance.name=name
[instance.ip=ipAddress] [instance.port=portNumber] [instance.dataDir=directoryPath]
[license.file=filePath] [instance.config.profile={wM|TC|CUSTOM}]
[instance.config.file=filePath] [install.service={true|false}]
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which you want to create a server instance.

NUMRealmServer|NUMEnterpriseManager|NUMTemplateApplications

Required. The product ID of the Universal Messaging realm server, Enterprise Manager, or Template Applications instance, respectively.

instance.name=*name*

Required. The name of the new instance. The name of a Universal Messaging server instance can contain case-insensitive upper-case and lower-case alphabetic characters, digits (0-9), underscores, and non-leading hyphens.

Important:

You cannot rename a Universal Messaging instance.

[instance.ip=*ipAddress*]

Optional. The IP address of the Universal Messaging server interface. If you do not specify a value, the default value is 0.0.0.0.

[instance.port=*portNumber*]

Optional. The port number of the Universal Messaging server. If you do not specify a value, the default value is 9000.

[instance.dataDir=*directoryPath*]

Optional. The absolute path to the Universal Messaging server data directory. If you do not specify a path, the default directory location is used: *Software AG_directory* \UniversalMessaging\server*instanceName*

[license.file=*filePath*]

Optional. The absolute path to the Universal Messaging license file. If you do not specify a path, the default license is used, which is located in the *Software AG_directory* \UniversalMessaging\server*instanceName* directory.

[instance.config.profile={wM|TC|CUSTOM}]

Optional. Initial configuration settings for the Universal Messaging server instance. Values are:

- wM - for webMethods suite use cases.
- TC - for standalone use cases.
- CUSTOM - for a custom configuration.

[instance.config.file=*filePath*]

Required if the value of `instance.config.profile` is `CUSTOM`. The absolute path to the custom configuration XML file.

[install.service={true | false}]

Optional. Whether a Windows service is registered for the server instance. The default is `false`.

Usage Notes

- If you register a Windows service for a new Universal Messaging server instance, the service is automatically deleted when you delete the server instance.
- Use the Universal Messaging Instance Manager tool to delete Enterprise Manager and Template Applications instances. You cannot use the Command Central command-line interface because such instances are not listed in the product inventory.

Examples

- To check if Universal Messaging supports instance management operations for the installation with alias name "sag01":

```
sagcc list instances sag01 supportedproducts
```

- To create a new instance for an installed Universal Messaging server, with instance name "umserver" and default port number "9000", in the installation with alias name "sag01":

```
sagcc create instances sag01 NUMRealmServer instance.name=umserver
```

- To create a new instance for an installed Universal Messaging server, with instance name "umserver" and port number "9001", and with a custom data directory path and license file, in the installation with alias name "sag01":

```
sagcc create instances sag01 NUMRealmServer instance.name=umserver  
instance.port=9001 instance.dataDir=C:\UM\data  
license.file=C:\Licenses\licenseUM.xml
```

- To create a new instance for an installed Universal Messaging realm server, with instance name "umserver" and port number "9001", in the installation with alias name "sag01", and use "wM" initial configuration settings:

```
sagcc create instances sag01 NUMRealmServer instance.name=umserver  
instance.port=9001 instance.config.profile=wM
```

- To create a new instance for an installed Universal Messaging server, with instance name "umserver" and port number "9001", in the installation with alias name "sag01", and use custom configuration settings:

```
sagcc create instances sag01 NUMRealmServer instance.name=umserver  
instance.port=9001 instance.config.profile=CUSTOM  
instance.config.file=C:\configurations\UMconfig.xml
```

- To register a Windows service when creating the Universal Messaging server instance named "umserver" in the installation with alias name "sag01":

```
sagcc create instances sag01 NUMRealmServer instance.name=umserver  
install.service=true
```

- To read the following properties of the Universal Messaging server instance named “umserver” in the installation with alias name “sag01”:
 - Port number
 - License path
 - Interface IP address
 - Server data directory path
 - Service status

```
sagcc list instances sag01 Universal-Messaging-umserver
```

- To create an Enterprise Manager instance named “em1” in the installation with alias name “sag01”:

```
sagcc create instances sag01 NUMEnterpriseManager instance.name=em1
```

- To create a Template Applications instance named “ta1” in the installation with alias name “sag01”:

```
sagcc create instances sag01 NUMTemplateApplications instance.name=ta1
```

Update Instances

Updates a Universal Messaging server instance. You can change only whether a Windows service is registered for the server instance.

Syntax

```
sagcc update instances nodeAlias Universal-Messaging-instanceName  
install.service={true|false}
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance you want to update.

install.service={true|false}

Required. Whether a Windows service is registered for the instance. The default is `false`.

Examples

To update the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01":

```
sagcc delete instances sag01 Universal-Messaging-umserver install.service=false
```

Delete Instances

Deletes a Universal Messaging server instance.

Note:

Use the Universal Messaging Instance Manager tool to delete Enterprise Manager and Template Applications instances. You cannot use the Command Central command-line interface because such instances are not listed in the product inventory.

Syntax

```
sagcc delete instances nodeAlias Universal-Messaging-instanceName
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-instanceName

Required. The ID of the Universal Messaging server instance you want to delete.

Examples

To delete the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01":

```
sagcc delete instances sag01 Universal-Messaging-umserver
```

Migrate Instances

Ensure that the target Universal Messaging server has the migration utility installed. For information about the migration utility, see *Upgrading Software AG Products*.

Important:

You must run the commands in the context and order documented in *Upgrading Software AG Products*. Otherwise, you may experience unpredictable results, possibly including corruption of your installation and data.

- View the command line help for the migration utility using the `sagcc list administration product node_alias NUMRealmServer migration help` command.
- Migrate all Universal Messaging server instances present in a source installation using the `sagcc exec administration product node_alias NUMRealmServer migration migrate srcDir=SAG_Installation_directory` command.

Note:

Use this command when migrating from Universal Messaging server version 9.8 and later.

- Start migration by providing the source Universal Messaging instance name using the `sagcc exec administration product node_alias NUMRealmServer migration migrate srcDir=SAG_Installation_directory instanceName=instance_name[, instance_name, instance_name...] command`.

Note:

Use this command when migrating from Universal Messaging server version 9.8 and later.

- Start migration by passing arguments and using the `migrate.dat` file using the `sagcc exec administration product node_alias NUMRealmServer migration migrate srcDir=SAG_Installation_directory importFile=migrate.dat` command.

Note:

Use this command when migrating from Universal Messaging server 9.0 through 9.7. The argument `silent` is set to `true` and `continueOnError` is set to `false` by default.

- Start migration using the zip file from the old product installation using the `sagcc exec administration product node_alias NUMRealmServer migration migrate srcFile=old_installation.zip importFile=migrate.dat` command.
- Start migration using the zip file from the old product installation and specifying the source Universal Messaging instance name using the `sagcc exec administration product node_alias NUMRealmServer migration migrate srcFile=old_installation.zip instanceName=instance_name[, instance_name, instance_name...] command`.
- View APIs under the migration namespace using the `sagcc list administration product node_alias NUMRealmServer migration` command.
- View if Universal Messaging supports migration as a custom API using the `sagcc list administration product node_alias NUMRealmServer` command.

Examples

- To view the command line help:

```
sagcc list administration product sag01 NUMRealmServer migration help
```

where `sag01` is the alias name of the installation where `NUMRealmServer` server instance is running. `migration` is the namespace for the custom Command Central API. `help` is the command to view the migration tool's command line help.

- To migrate all Universal Messaging server instances present in a source installation:

```
sagcc exec administration product sag01 NUMRealmServer migration migrate srcDir=C:\SoftwareAG
```

where `sag01` is the alias name of the installation where `NUMRealmServer` server instance is running. `migration` is the namespace for the custom Command Central API. `migrate` is the command to access the migration tool. `srcDir` is the source Software AG installation directory.

- To start migrating an older server instance to a new `NUMRealmServer` server instance by providing the source instance name:

```
sagcc exec administration product sag01 NUMRealmServer
migration migrate srcDir=C:\SoftwareAG
instanceName=umserver1,umserver2
```

where `sag01` is the alias name of the installation where `NUMRealmServer` server instance is running. `migration` is the namespace for the custom Command Central API. `migrate` is the command to access the migration tool. `srcDir` is the source Software AG installation directory. `instanceName` contains the comma-separated names of the Universal Messaging instances that will be migrated.

- To start migrating an older server instance to a new `NUMRealmServer` server instance using the `migrate.dat` file:

```
sagcc exec administration product sag01 NUMRealmServer
migration migrate srcDir=C:\SoftwareAG
silent=true importFile=migrate.dat
```

where `sag01` is the alias name of the installation where `NUMRealmServer` server instance is running. `migration` is the namespace for the custom Command Central API. `migrate` is the command to access the migration tool. `srcDir` is the source Software AG installation directory. `importFile` specifies the data file containing the migration settings.

- To start migration using the zip file from the old product installation:

```
sagcc exec administration product sag01 NUMRealmServer
migration migrate srcFile=99Src.zip importFile=migrate.dat
```

where `sag01` is the alias name of the installation where `NUMRealmServer` server instance is running. `migration` is the namespace for the custom Command Central API. `migrate` is the command to access the migration tool. `srcFile` argument is used to provide the name of the zip file from the source Universal Messaging instance. `importFile` specifies the archive file path containing migration settings.

- To view APIs under the migration namespace for the `NUMRealmServer` server instance:

```
sagcc list administration product sag01 NUMRealmServer migration
```

where `sag01` is the alias name of the installation where `NUMRealmServer` server instance is running.

- To view if Universal Messaging supports migration as a custom API:

```
sagcc list administration product sag01 NUMRealmServer
```

where `sag01` is the alias name of the installation where `NUMRealmServer` server instance is running.

User Configuration

Create Users

Creates new users in the user repository of a Universal Messaging server instance.

Syntax

```
sagcc create configuration data nodeAlias Universal-Messaging-instanceName
COMMON-LOCAL-USERS [--input|-i] file.xml
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance on which you want to create a user.

COMMON-LOCAL-USERS

Required. The ID of the configuration type of which you want to create an instance.

{--input|-i} *file.xml*

Required. The absolute path to the XML file that contains the user ID and password.

Usage Notes

Information to authenticate the users of a Universal Messaging server instance is stored in the user repository (users.txt file) of the Universal Messaging server instance. The users.txt file is generated only after you create an internal user. While creating the user repository, if you specify a relative path in the jaas.conf file, the users.txt file is created in a directory relative to the bin directory of the Universal Messaging server instance.

The path to the users.txt file is added to the jaas.conf file in the *Software AG_directory* /UniversalMessaging/server/*instanceName*/bin directory. If you specify a relative path in the jaas.conf file, the users.txt is created in a directory relative to the bin directory of the Universal Messaging server instance.

Examples

To create a user with ID "user2" on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", using the "user2.xml" file that contains the user ID and password:

```
sagcc create configuration data sag01 Universal-Messaging-umserver
COMMON-LOCAL-USERS --input c:\input\xmls\user2.xml
```

The user2.xml file has the following format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<User id="user2">
<Password>test</Password>
</User>
```

List Users

Lists all users in the user repository of a Universal Messaging server instance or retrieves information about a specific user.

Syntax

- To list all users of a Universal Messaging server instance and the path to the user repository :

```
sagcc get configuration instances nodeAlias Universal-Messaging-instanceName
```

- To retrieve information about a user:

```
sagcc get configuration instances nodeAlias Universal-Messaging-instanceName  
COMMON-LOCAL-USERS-userName
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to retrieve user information.

COMMON-LOCAL-USERS-*userName*

Optional. The ID of the user for whom you want to retrieve information.

Examples

- To list the path of the user repository and the users of the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01":

```
sagcc get configuration instances sag01 Universal-Messaging-umserver
```

- To retrieve information about the user with ID "user1" on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01":

```
sagcc get configuration instances sag01 Universal-Messaging-umserver  
COMMON-LOCAL-USERS-user1
```

Update Users

Updates the password of an existing user.

Syntax

```
sagcc update configuration data nodeAlias Universal-Messaging-instanceName  
COMMON-LOCAL-USERS-userName [--input|-i] file.xml
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance on which you want to update the user password.

COMMON-LOCAL-USERS-*userName*

Required. The ID of the user whose password you want to update.

{--input|-i} *file.xml*

Required. The absolute path to the XML file that contains the user ID and the new password.

Examples

To update the password of the user with ID "user2" in the "user2.xml" file on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01":

```
sagcc update configuration data sag01 Universal-Messaging-umserver
COMMON-LOCAL-USERS-user2 --input c:\inputxmls\user2.xml
```

The user2.xml file has the following format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<User id="user2">
<Password>test</Password>
</User>
```

Delete Users

Deletes a user from the user repository of a Universal Messaging server instance.

Syntax

```
sagcc delete configuration data nodeAlias Universal-Messaging-instanceName
COMMON-LOCAL-USERS-userName
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance on which you want to delete a user.

COMMON-LOCAL-USERS-*userName*

Required. The ID of the user you want to delete.

Examples

To delete the user with ID "user2" from the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01":

```
sagcc delete configuration data sag01 Universal-Messaging-umserver  
COMMON-LOCAL-USERS-user2
```

License Configuration

Add License Keys

Adds a Universal Messaging license key file with the specified alias to the Command Central license key manager.

Syntax

```
sagcc add license-tools keys licenseKeyAlias  
{--input|-i} filename
```

Arguments and Options

licenseKeyAlias

Required. The alias of the license key file to add. Specify an alias that is unique across all license keys in the license key manager.

{--input|-i} *filename*

Required. The absolute path to the license file.

Examples

To add the Universal Messaging license key file "new_license.xml" with alias "um_lic" to the Command Central license key manager:

```
sagcc add license-tools keys um_lic -i C:\umllicense\new_license.xml
```

Get License Details

Retrieves license details and the license location for a Universal Messaging server instance.

Syntax

- To retrieve the license details for a Universal Messaging server instance:

```
sagcc get configuration data nodeAlias  
Universal-Messaging-instanceName COMMON-LICENSE-Universal-Messaging
```

- To retrieve the license location for a Universal Messaging server instance:

```
sagcc get configuration data nodeAlias
Universal-Messaging-instanceName COMMON-LICLOC-Universal-Messaging
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to retrieve license information.

COMMON-LICENSE-Universal-Messaging

Required for retrieving license details. The ID of the configuration type.

COMMON-LICLOC-Universal-Messaging

Required for retrieving the license location. The ID of the configuration type.

Examples

- To view the license details for a server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc get configuration data sag01 Universal-Messaging-umserver
COMMON-LICENSE-Universal-Messaging
```

- To view the license file location for a server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc get configuration data sag01 Universal-Messaging-umserver
COMMON-LICLOC-Universal-Messaging
```

Update License Keys

Updates a license key file assigned to the specified license key alias.

Syntax

```
sagcc update configuration license nodeAlias
Universal-Messaging-instanceName COMMON-LICENSE-Universal-Messaging
licenseKeyAlias
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to update the license key.

COMMON-LICENSE-Universal-Messaging

Required. The ID of the configuration type.

licenseKeyAlias

Required. The alias of the license key file that you want to update.

Examples

To update the license key file assigned to the license key alias "um_lic" of the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01" :

```
sagcc update configuration license sag01 Universal-Messaging-umserver  
COMMON-LICENSE-Universal-Messaging um_lic
```

Port Configuration

Create Ports

Creates a port for a Universal Messaging server instance.

Syntax

```
sagcc create configuration data nodeAlias Universal-Messaging-instanceName COMMON-PORTS  
{--input|-i} filename.xml --password password
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance on which you want to create a port.

COMMON-PORTS

Required. The ID of the configuration type of which you want to create an instance.

--input|-i *filename.xml*

Required. The XML file that contains the port configuration data.

--password *password*

Required. Your Command Central password.

Examples

To create a port for the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01", using the port configuration file "port_data.xml":

```
sagcc create configuration data sag01 Universal-Messaging-umserver
COMMON-PORTS --input port_data.xml --password secret
```

Because the `{--server | -s}` and `{--username | -u}` options are not specified, the command uses the default server and user name. For more information about these options, see *Software AG Command Central Help*. The command specifies "secret" for the user's password.

The XML port configuration file must have the following format:

```
<PortSettings>
  <Port alias="nhp1">
    <Enabled>true</Enabled>
    <Type>STANDARD</Type>
    <Number>9001</Number>
    <Protocol>NHP</Protocol>
    <Backlog>100</Backlog>
    <ExtendedProperties>
      <Property name="autostart">true</Property>
      <Property name="allowforinterrealm">true</Property>
      <Property name="authtime">1000</Property>
      <Property name="EnableNIO">true</Property>
      <Property name="acceptThreads">2</Property>
      <Property name="receivebuffersize">1310721</Property>
      <Property name="SelectThreads">4</Property>
      <Property name="advertise">true</Property>
      <Property name="allowclientconnections">true</Property>
      <Property name="Backlog">100</Property>
      <Property name="Alias"/>
      <Property name="keyAlias"/>
      <Property name="sendbuffersize">1310721</Property>
      <Property name="EnableHTTP11">true</Property>
      <Property name="EnableJavaScript">true</Property>
      <Property name="CORSAAllowCredentials">true</Property>
      <Property name="CORSAAllowedOrigins">*</Property>
      <Property name="AjaxLPActiveDelay">100</Property>
      <Property name="EnableWebSockets">true</Property>
      <Property name="EnableGZipLP">true</Property>
      <Property name="MinimumBytesBeforeGZIP">1000</Property>
      <Property name="AjaxLPIdleDelay">60000</Property>
      <Property name="header1Name">foo</Property>
      <Property name="header1Value">bar</Property>
      <Property name="header1UserAgent">mozilla</Property>
    </ExtendedProperties>
  </Port>
</PortSettings>
```

Update Ports

Updates the configuration of a port for a Universal Messaging server instance.

Syntax

```
sagcc update configuration data nodeAlias Universal-Messaging-instanceName  
COMMON-PORTS-portAlias  
{--input|-i} filename.xml --password password
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance on which you want to update a port.

COMMON-PORTS-*portAlias*

Required. The ID of the port instance that you want to update.

--input|-i *filename.xml*

Required. The XML file that contains the port configuration data.

--password *password*

Required. Your Command Central password.

Examples

To update the port with alias "nhp1" for the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01", using the port configuration file "port_data.xml":

```
sagcc update configuration data sag01 Universal-Messaging-umserver COMMON-PORTS-nhp1  
--input port_data.xml --password secret
```

Because the {--server | -s} and {--username | -u} options are not specified, the command uses the default server and user name. For more information about these options, see *Software AG Command Central Help*. The command specifies "secret" for the user's password.

The XML port configuration file must have the following format:

```
<PortSettings>  
  <Port alias="nhp1">  
    <Enabled>true</Enabled>  
    <Type>STANDARD</Type>  
    <Number>9001</Number>  
    <Protocol>NHP</Protocol>  
    <Backlog>100</Backlog>  
    <ExtendedProperties>  
      <Property name="autostart">true</Property>  
      <Property name="allowforinterrealm">true</Property>  
      <Property name="authtime">1000</Property>  
      <Property name="EnableNIO">true</Property>  
      <Property name="acceptThreads">2</Property>  
      <Property name="receivebuffersize">1310721</Property>
```

```

    <Property name="SelectThreads">4</Property>
    <Property name="advertise">true</Property>
    <Property name="allowclientconnections">true</Property>
    <Property name="Backlog">100</Property>
    <Property name="Alias"/>
    <Property name="keyAlias"/>
    <Property name="sendbuffersize">1310721</Property>
    <Property name="EnableHTTP11">true</Property>
    <Property name="EnableJavaScript">true</Property>
    <Property name="CORSAAllowCredentials">true</Property>
    <Property name="CORSAAllowedOrigins">*</Property>
    <Property name="AjaxLPActiveDelay">100</Property>
    <Property name="EnableWebSockets">true</Property>
    <Property name="EnableGZipLP">true</Property>
    <Property name="MinimumBytesBeforeGZIP">1000</Property>
    <Property name="AjaxLPIdleDelay">60000</Property>
    <Property name="header1Name">foo</Property>
    <Property name="header1Value">bar</Property>
    <Property name="header1UserAgent">mozilla</Property>
  </ExtendedProperties>
</Port>
</PortSettings>

```

Delete Ports

Deletes a port for a Universal Messaging server instance.

Syntax

```
sagcc delete configuration data nodeAlias Universal-Messaging-instanceName
COMMON-PORTS-portAlias --password password
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance on which you want to delete a port.

COMMON-PORTS-*portAlias*

Required. The ID of the port instance that you want to delete.

--password *password*

Required. Your Command Central password.

Examples

To delete the port with alias "nhp1 for the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc delete configuration data sag01 Universal-Messaging-umserver COMMON-PORTS-nhp1
```

```
--password secret
```

Because the `{--server | -s}` and `{--username | -u}` options are not specified, the command uses the default server and user name. For more information about these options, see *Software AG Command Central Help*. The command specifies "secret" for the user's password.

Security Group Configuration

Get Security Group Configuration Data

Retrieves configuration data about a specific security group for a Universal Messaging server instance.

Syntax

```
sagcc get configuration data nodeAlias  
Universal-Messaging-instanceName UM-GROUPS-groupName
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to retrieve security group information.

UM-GROUPS-*groupName*

Required. The ID of the security group for which you want to retrieve information.

Examples

To retrieve information about the security group "Everyone" on the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc get configuration data sag01 Universal-Messaging-umserver  
UM-GROUPS-Everyone
```

Realm ACL Configuration

Get Realm ACL Configuration Data

Retrieves configuration data about realm ACLs for a Universal Messaging server instance.

Syntax

```
sagcc get configuration data nodeAlias
```

```
Universal-Messaging-instanceName UM-REALM-ACL
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to retrieve realm ACL information.

UM-REALM-ACL

Required. The ID of the configuration type for which you want to retrieve information.

Examples

To retrieve the realm ACL configuration information for the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc get configuration data sag01 Universal-Messaging-umserver
UM-REALM-ACL
```

General Properties Configuration

Get Configuration Properties

Retrieves the configuration properties for a specific configuration property group.

For information about the configuration properties that the Universal Messaging server supports, see [“General Properties” on page 195](#).

Syntax

```
sagcc get configuration data nodeAlias Universal-Messaging-instanceName
COMMON-SYSPROPS-propertyGroupName
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to retrieve configuration property information.

COMMON-SYSPROPS-*propertyGroupName*

Required. The ID of the configuration type and the name of the property group for which you want to retrieve information.

Usage Notes

When the name of the property group contains two or more words, you must join each word by an underscore (_) when you specify *propertyGroupName*. For example, for the Data Stream Config property group, you will type `COMMON-SYSPROPS-Data_Stream_Config`.

Examples

To retrieve the configuration properties for the Cluster Config property group of the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias "sag01":

```
sagcc get configuration data sag01 Universal-Messaging-umserver  
COMMON-SYSPROPS-Cluster_Config
```

Update Configuration Properties

Updates the configuration properties for a specific configuration property group.

For information about the configuration properties that the Universal Messaging server supports, see [“General Properties” on page 195](#).

Syntax

```
sagcc update configuration data nodeAlias Universal-Messaging-instanceName  
COMMON-SYSPROPS-propertyGroupName [--input|-i] file.properties
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to update the configuration properties.

COMMON-SYSPROPS-*propertyGroupName*

Required. The ID of the configuration type and the name of the property group for which you want to update the configuration properties.

{--input|-i} *file.properties*

Required. The absolute path to the properties file that contains the modified configuration properties.

Usage Notes

- When the name of the property group contains two or more words, you must join each word by an underscore (_) when you specify *propertyGroupName*. For example, for the Data Stream Config property group, you will type `COMMON-SYSPROPS-Data_Stream_Config`.

- Configuration parameter names are case-sensitive. For parameter values of the enumeration type, specify values ranging from 0 to n to map to the corresponding enumeration values in the Command Central user interface.
- The `sagcc update configuration data` command exits and displays an error when it first meets an incorrectly defined parameter. For example, the command will exit and display an error if the `MonitorTimer` property has a string value.

Examples

To modify configuration properties in the Data Stream Config property group for the server instance with ID "Universal-Messaging-umserevr" installed in the installation with alias "sag01", using the properties file "datastreamconfig.properties":

```
sagcc update configuration data sag01 Universal-Messaging-umserver
COMMON-SYSPROPS-Data_Stream_Config --input c:\datastreamconfig.properties
```

The properties file contains parameter-value pairs in the following format:

```
MonitorTimer=10000
OffloadMulticastWrite=false

SendInitialMapping=true
```

JNDI Connection Factories Configuration

Create Connection Factories

Creates a JNDI connection factory for a Universal Messaging server instance. You can create the following types of connection factory:

- Connection factory
- Topic connection factory
- Queue connection factory
- XA connection factory

Syntax

```
sagcc create configuration data nodeAlias Universal-Messaging-instanceName
UM-JNDI-CF [--input|-i] file.xml
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-instanceName

Required. The ID of the Universal Messaging server instance for which you want to create a JNDI connection factory.

UM-JNDI-CF

Required. The ID of the configuration type of which you want to create an instance.

--input **-i** *file.xml*

Required. The absolute path to the XML file that contains configuration information about the connection factory.

Usage Notes

- The input XML file must contain configuration parameters in the following format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<connectionFactory>
  <name>connection_factory_name</name>
  <type>connection_factory_type</type>
  <url>connection_factory_binding_url</url>
  <durableType>type_of_durable</durableType>
</connectionFactory>
```

The name, type, and url parameters are required. The durableType parameter is optional.

- Creating a JNDI connection factory and JNDI destination with the same name is not allowed for a Universal Messaging server instance.

Examples

To create a connection factory for the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", using the "connection_factory.xml" file:

```
sagcc create configuration data sag01 Universal-Messaging-umserver
UM-JNDI-CF -i C:\jndi\connecton_factory.xml
```

The XML file contains the following parameters:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<connectionFactory>
  <name>connectionFactory1</name>
  <type>ConnectionFactory</type>
  <url>nhp://124.597.890:9100</url>
  <durableType>Shared</durableType>
</connectionFactory>
```

Get Connection Factory Data

Retrieves information about a specific JNDI connection factory for a Universal Messaging server instance.

Syntax

```
sagcc get configuration data nodeAlias Universal-Messaging-instanceName
UM-JNDI-CF-connectionFactoryName
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to retrieve connection factory information.

UM-JNDI-CF-*connectionFactoryName*

Required. The ID of the connection factory for which you want to retrieve information.

Examples

To retrieve information about the connection factory with name "connectionFactory1" for the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc get configuration data sag01 Universal-Messaging-umserver
UM-JNDI-CF-connectionFactory1
```

Update Connection Factories

Updates a JNDI connection factory for a Universal Messaging server instance. You can update the *name*, *url*, and *durableType* parameters for a connection factory. You cannot update the type of the connection factory.

Syntax

```
sagcc update configuration data nodeAlias Universal-Messaging-instanceName
UM-JNDI-CF-connectionFactoryName [--input|-i] file.xml
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to update a JNDI connection factory.

UM-JNDI-CF-*connectionFactoryName*

Required. The ID of the connection factory that you want to update.

--input|-i *file.xml*

Required. The absolute path to the XML file that contains configuration information about the connection factory.

Usage Notes

- The input XML file must contain configuration parameters in the following format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<connectionFactory>
  <name>connection_factory_name</name>
  <type>connection_factory_type</type>
  <url>connection_factory_binding_url</url>
  <durableType>type_of_durable</durableType>
</connectionFactory>
```

The `name`, `type`, and `url` parameters are required. The `durableType` parameter is optional.

- Creating a JNDI connection factory and JNDI destination with the same name is not allowed for a Universal Messaging server instance.

Examples

To update the connection factory with name "connectionFactory1" for the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", using the "connection_factory.xml" file:

```
sagcc update configuration data sag01 Universal-Messaging-umserver
UM-JNDI-CF-connectionFactory1 -i C:\jndi\connecton_factory.xml
```

The XML file contains the following parameters:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<connectionFactory>
  <name>connectionFactory2</name>
  <type>ConnectionFactory</type>
  <url>nhp://124.597.890:9100</url>
  <durableType>Serial</durableType>
</connectionFactory>
```

Delete Connection Factories

Deletes a JNDI connection factory for a Universal Messaging server instance.

Syntax

```
sagcc delete configuration data nodeAlias Universal-Messaging-instanceName
UM-JNDI-CF-connectionFactoryName
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-instanceName

Required. The ID of the Universal Messaging server instance for which you want to delete a connection factory.

UM-JNDI-CF-connectionFactoryName

Required. The ID of the connection factory you want to delete.

Examples

To delete the connection factory with name "connectionFactory1" for the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc delete configuration data sag01 Universal-Messaging-umserver
UM-JNDI-CF-connectionFactory1
```

JNDI Destinations Configuration

Create Destinations

Creates a JNDI destination for a Universal Messaging server instance. You can create topic and queue destinations.

Important:

Updating a JNDI destination, using the command-line interface, is not supported.

Syntax

```
sagcc create configuration data nodeAlias Universal-Messaging-instanceName
UM-JNDI-DEST [--input|-i] file.xml
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to create a JNDI destination.

UM-JNDI-DEST

Required. The ID of the configuration type of which you want to create an instance.

--input|-i *file.xml*

Required. The absolute path to the XML file that contains configuration information about the destination.

Usage Notes

- The input XML file must have the following format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<destination>
  <name>destination_name</name>
  <type>destination_type</type>
  <storeName>jms_channel_or_queue_name</storeName>
  <autoCreateDest>true|false</autoCreateDest>
</destination>
```

The `name` parameter can include upper-case and lower-case alphabetic characters, digits (0-9), a double colon (::), slash (/), and periods (.), for example, `destination1`. Use a double colon (::) to specify a nested namespace, for example, `destination1::destination2`. A combination of special characters is not allowed, for example, `destination1::destination2/destination3`.

The `storeName` parameter can include upper-case and lower-case alphabetic characters, digits (0-9), a double colon (::), slash (/), and underscores (_), but cannot include periods (.).

- Creating a JNDI connection factory and JNDI destination with the same name is not allowed for a Universal Messaging server instance.

Examples

To create a destination for the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", using the "destination.xml" file:

```
sagcc create configuration data sag01 Universal-Messaging-umserver
UM-JNDI-DEST -i C:\jndi\destination.xml
```

The XML file contains the following parameters:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<destination>
  <name>destination1</name>
  <type>Topic</type>
  <storeName>topic1</storeName>
  <autoCreateDest>true</autoCreateDest>
</destination>
```

Get Destination Data

Retrieves information about a specific JNDI destination for a Universal Messaging server instance.

Syntax

```
sagcc get configuration data nodeAlias Universal-Messaging-instanceName
UM-JNDI-DEST-destinationName
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to retrieve destination information.

UM-JNDI-DEST-*destinationName*

Required. The ID of the destination for which you want to retrieve information.

Examples

To retrieve information about the destination with name "destination1" for the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc get configuration data sag01 Universal-Messaging-umserver
UM-JNDI-DEST-destination1
```

Delete Destinations

Deletes a JNDI destination for a Universal Messaging server instance.

Note:

Deleting a JNDI destination does not delete the channel or queue that exists on the Universal Messaging server instance.

Syntax

```
sagcc delete configuration data nodeAlias Universal-Messaging-instanceName
UM-JNDI-DEST-destinationName
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to delete a JNDI destination.

UM-JNDI-DEST-*destinationName*

Required. The ID of the destination you want to delete.

Examples

To delete the destination with name "destination1" for the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc delete configuration data sag01 Universal-Messaging-umserver
UM-JNDI-DEST-destination1
```

Channel Configuration

Create Channels

Creates a channel on a Universal Messaging server instance.

Syntax

```
sagcc create configuration data nodeAlias Universal-Messaging-instanceName  
UM-CHANNELS [--input|-i] file.xml
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance on which you want to create a channel.

UM-CHANNELS

Required. The ID of the configuration type of which you want to create an instance.

--input|-i *file.xml*

Required. The absolute path to the XML file that contains the configuration properties of the channel.

Examples

To create a channel on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", using the "channel_create.xml" file:

```
sagcc create configuration data sag01 Universal-Messaging-umserver  
UM-CHANNELS -i C:\Channels\channel_create.xml
```

The XML file contains the channel attributes and has the following format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>  
<Channel>  
  <name>channel1</name>  
  <type>Persistent</type>  
  <ttl>0</ttl>  
  <capacity>0</capacity>  
  .....  
</Channel>
```

Get Channel Data

Retrieves configuration information about a specific channel on a Universal Messaging server instance.

Syntax

```
sagcc get configuration data nodeAlias Universal-Messaging-instanceName
UM-CHANNELS-channelName
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to retrieve channel information.

UM-CHANNELS-*channelName*

Required. The ID of the channel for which you want to retrieve information.

For channels inside a folder, you must use two hyphens, "--", to separate the name of the folder and the channel. For example, if you have a channel named "test/myChannel", the argument will have the value UM-CHANNELS-test--myChannel.

Examples

To retrieve information about the channel with name "channel2" on the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc get configuration data sag01 Universal-Messaging-umserver UM-CHANNELS-channel2
```

Update Channels

Updates a channel on a Universal Messaging server instance.

Syntax

```
sagcc update configuration data nodeAlias Universal-Messaging-instanceName
UM-CHANNELS-channelName [--input|-i] file.xml
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance on which you want to update a channel.

UM-CHANNELS-*channelName*

Required. The ID of the channel you want to update.

For channels inside a folder, you must use two hyphens, "--", to separate the name of the folder and the channel. For example, if you have a channel named "test/myChannel", the argument will have the value `UM-CHANNELS-test--myChannel`.

--input|-i file.xml

Required. The absolute path to the XML file that contains the configuration properties of the channel.

Examples

To update the channel "channel2" on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", using the "channel_update.xml" file:

```
sagcc update configuration data sag01 Universal-Messaging-umserver
UM-CHANNELS-channel2 -i C:\Channels\channel_update.xml
```

The XML file contains the channel attributes and has the following format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Channel>
  <name>channel2</name>
  <type>Persistent</type>
  <ttl>50000</ttl>
  <capacity>50000</capacity>
  <deadEventStore/>
  <engine>JMS Engine</engine>
  .....
</Channel>
```

Queue Configuration

Create Queues

Creates a queue on a Universal Messaging server instance.

Syntax

```
sagcc create configuration data nodeAlias Universal-Messaging-instanceName
UM-QUEUES [--input|-i] file.xml
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-instanceName

Required. The ID of the Universal Messaging server instance on which you want to create a queue.

UM-QUEUES

Required. The ID of the configuration type of which you want to create an instance.

--input | -i *file.xml*

Required. The absolute path to the XML file that contains the configuration properties of the queue.

Examples

To create a queue on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", using the "queue_create.xml" file:

```
sagcc create configuration data sag01 Universal-Messaging-umserver
UM-QUEUES -i C:\Queues\queue_create.xml
```

The XML file contains the queue attributes and has the following format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Queue>
  <name>queue1</name>
  <type>Persistent</type>
  <ttl>78</ttl>
  <capacity>99</capacity>
  <parent>umserver</parent>
  .....
</Queue>
```

Get Queue Data

Retrieves configuration information about a specific queue on a Universal Messaging server instance.

Syntax

```
sagcc get configuration data nodeAlias Universal-Messaging-instanceName
UM-QUEUES-queueName
```

Arguments and Options***nodeAlias***

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to retrieve queue information.

UM-QUEUES-*queueName*

Required. The ID of the queue for which you want to retrieve information.

Examples

To retrieve information about the queue with name "queue1" on the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc get configuration data sag01 Universal-Messaging-umserver UM-QUEUES-queue1
```

Update Queues

Updates a queue on a Universal Messaging server instance.

Syntax

```
sagcc update configuration data nodeAlias Universal-Messaging-instanceName  
UM-QUEUES-queueName [--input|-i] file.xml
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance on which you want to update a queue.

UM-QUEUES-*queueName*

Required. The ID of the queue you want to update.

--input|-i *file.xml*

Required. The absolute path to the XML file that contains the configuration properties of the queue.

Examples

To update the queue "queue1" on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", using the "queue_update.xml" file:

```
sagcc update configuration data sag01 Universal-Messaging-umserver  
UM-QUEUES-queue1 -i C:\Queues\queue_update.xml
```

The XML file contains the queue attributes and has the following format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>  
<Queue>  
  <name>queue1</name>  
  <type>Persistent</type>  
  <ttl>50000</ttl>  
  <capacity>50000</capacity>  
  <parent>umserver</parent>  
  <deadEventStore/>  
  .....  
</Queue>
```

Zone Configuration

Create Zones

Creates a zone of Universal Messaging servers.

Syntax

```
sagcc create configuration data nodeAlias Universal-Messaging-instanceName
UM-ZONE [--input|-i] file.xml
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to create a zone.

UM-ZONE

Required. The ID of the configuration type of which you want to create an instance.

--input|-i *file.xml*

Required. The path to the XML file that contains the zone configuration information. Specify the absolute path to the XML file if the file is not in the same directory from which you run the command.

Examples

To create a zone for the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", using the "zone_create.xml" file:

```
sagcc create configuration data sag01 Universal-Messaging-umserver UM-ZONE
-i=C:\zones\zone_create.xml
```

The zone_create.xml file has the following format for a zone with realms:

```
<?xml version="1.0" encoding="UTF-8"?>
<Zone>
  <name>RealmZone</name>
  <type>Realm</type>
  <realms>
    <server name="um_realm1">
      <url>nsp://localhost:9701</url>
    </server>
    <server name="um_realm2">
      <url>nsp://localhost:9702</url>
    </server>
  </realms>
```

```
<clusters/>
</Zone>
```

The `zone_create.xml` file has the following format for a zone with clusters:

```
<?xml version="1.0" encoding="UTF-8"?>
<Zone>
  <name>ClusterZone</name>
  <type>Cluster</type>
  <realms />
  <clusters>
    <server name="um_cluster1">
      <url>nsp://localhost:9704</url>
      <clusterName />
      <status />
    </server>
    <server name="um_cluster2">
      <url>nsp://localhost:9705</url>
      <clusterName />
      <status />
    </server>
  </clusters>
</Zone>
```

Get Zone Data

Retrieves configuration information about a zone for a specific server instance.

Syntax

```
sagcc get configuration data nodeAlias Universal-Messaging-instanceName UM-ZONE
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-instanceName

Required. The ID of the Universal Messaging server instance for which you want to retrieve information.

UM-ZONE

Required. The ID of the configuration type for which you want to retrieve information.

Examples

To retrieve zone information for the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01":

```
sagcc get configuration data sag01 Universal-Messaging-umserver UM-ZONE
```

Update Zones

Updates a zone of Universal Messaging servers.

Syntax

```
sagcc update configuration data nodeAlias Universal-Messaging-instanceName
UM-ZONE [--input|-i] file.xml
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to update a zone.

UM-ZONE

Required. The ID of the configuration type of which you want to update an instance.

--input|-i *file.xml*

Required. The path to the XML file that contains the zone configuration information. Specify the absolute path to the XML file if the file is not in the same directory from which you run the command.

Examples

To update a zone for the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", using the "zone_update.xml" file:

```
sagcc update configuration data sag01 Universal-Messaging-umserver UM-ZONE
-i=C:\zones\zone_update.xml
```

The zone_update.xml file has the following format for a zone with realms:

```
<?xml version="1.0" encoding="UTF-8"?>
<Zone>
  <name>RealmZone</name>
  <type>Realm</type>
  <realms>
    <server name="um_realm1">
      <url>nsp://localhost:9701</url>
    </server>
    <server name="um_realm2">
      <url>nsp://localhost:9702</url>
    </server>
  </realms>
  <clusters/>
</Zone>
```

The zone_update.xml file has the following format for a zone with clusters:

```
<?xml version="1.0" encoding="UTF-8"?>
<Zone>
```

```
<name>ClusterZone</name>
<type>Cluster</type>
<realms />
<clusters>
  <server name="um_cluster1">
    <url>nsp://localhost:9704</url>
    <clusterName />
    <status />
  </server>
  <server name="um_cluster2">
    <url>nsp://localhost:9705</url>
    <clusterName />
    <status />
  </server>
</clusters>
</Zone>
```

Delete Zones

Deletes the zone to which the specified Universal Messaging server instance belongs.

Syntax

```
sagcc delete configuration data nodeAlias Universal-Messaging-instanceName UM-ZONE
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to delete a zone.

UM-ZONE

Required. The ID of the configuration type of which you want to delete an instance.

Usage Notes

You can remove specific server instances from a zone by removing the server instances from the zone configuration XML file, and then using the update zone command. For information about the update zone command, see [“Update Zones” on page 260](#).

Examples

To delete a zone for the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01":

```
sagcc delete configuration data sag01 Universal-Messaging-umserver UM-ZONE
```

Java System Properties Configuration

Get Java System Properties

Retrieves the Java system properties for a Universal Messaging server instance.

Syntax

```
sagcc get configuration data nodeAlias Universal-Messaging-instanceName
COMMON-JAVASYSPROPS
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to retrieve the Java system properties.

COMMON-JAVASYSPROPS

Required. The ID of the configuration type for which you want to retrieve information.

Examples

To retrieve the Java system properties for the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc get configuration data sag01 Universal-Messaging-umserver COMMON-JAVASYSPROPS
```

Update Java System Properties

Updates the Java system properties for a Universal Messaging server instance.

Important:

After you run the command, you must restart the Universal Messaging server for the changes to take effect.

Syntax

```
sagcc update configuration data nodeAlias Universal-Messaging-instanceName
COMMON-JAVASYSPROPS [--input|-i] file.xml
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-instanceName

Required. The ID of the Universal Messaging server instance for which you want to update the Java system properties.

COMMON-JAVASYSPROPS

Required. The ID of the configuration type of which you want to update an instance.

--input | -i file.xml

Required. The absolute path to the XML file that contains the updated system properties.

Examples

To update the Java system properties for the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01", using the file "jvmoptions.xml":

```
sagcc update configuration data sag01 Universal-Messaging-umserver  
COMMON-JAVASYSPROPS -i C:\jvmoptions.xml
```

JVM Options Configuration

Get JVM Options

Retrieves the JVM options for a Universal Messaging server instance.

Syntax

```
sagcc get configuration data nodeAlias Universal-Messaging-instanceName  
COMMON-JVM-OPTIONS
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-instanceName

Required. The ID of the Universal Messaging server instance for which you want to retrieve the JVM options.

COMMON-JVM-OPTIONS

Required. The ID of the configuration type for which you want to retrieve information.

Examples

To retrieve the JVM options for the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc get configuration data sag01 Universal-Messaging-umserver
COMMON-JVM-OPTIONS
```

Update JVM Options

Updates the JVM options for a Universal Messaging server instance.

Important:

After you run the command, you must restart the Universal Messaging server for the changes to take effect.

Syntax

```
sagcc update configuration data nodeAlias Universal-Messaging-instanceName
COMMON-JVM-OPTIONS [--input|-i] file.xml
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to update the JVM options.

COMMON-JVM-OPTIONS

Required. The ID of the configuration type of which you want to update an instance.

--input|-i *file.xml*

Required. The absolute path to the XML file that contains the updated JVM options.

Examples

To update the JVM options for the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01", using the file "javasysprop.xml":

```
sagcc update configuration data sag01 Universal-Messaging-umserver
COMMON-JVM-OPTIONS -i C:\javasysprop.xml
```

The XML file has the following format:

```
<?xml version="1.0"?>
-<jvmOptions>
<option>-XX:+TraceClassLoading</option>
</jvmOptions>
```

Cluster Configuration

Before You Create or Update a Cluster

- Make sure the server instances that you want to add to the cluster are running.
- Verify that the permissions on the server machines allow connections to the other servers in the cluster.
- Make sure the /naming/defaultContext channel exists only on one or none of the nodes that will form the cluster. The Universal Messaging server instance used as a JNDI provider uses the /naming/defaultContext channel to store JMS references and JNDI objects. If the channel exists on multiple nodes, you cannot create the cluster.
- If you have a custom composite template for Command Central 9.9 or earlier, you must remove the Universal Messaging server instance.name suffix from the COMMON-CLUSTER configuration type in the template when you apply the composite template in Command Central 9.10 or later.

In the following example, you have a composite template created in Command Central 9.9 and earlier, and then the same template in Command Central 9.10 and later.

In Command Central 9.9 and earlier:

```
um-cluster:
  description: Cluster configuration for two UM instances
  products:
    NUMRealmServer:
      ${node.host}:
        instance.port: ${um.instance.port}
        instance.ip:   ${um.host}
        runtimeComponentId: Universal-Messaging-${instance.name}
        configuration:
          Universal-Messaging-${instance.name}:
            COMMON-CLUSTER:
              COMMON-CLUSTER-${instance.name}: &umClusterConfig
              Name: ${um.cluster}
              Servers:                               # two UM instances cluster
                Server:
                  -
                    "@name": ${um.host}
                    URL: "nsp://${um.host}:${um.instance.port}"
                  -
                    "@name": ${um.host2}
                    URL: "nsp://${um.host2}:${um.instance.port2}"
```

In Command Central 9.10 and later:

```
um-cluster:
  description: Cluster configuration for two UM instances
  products:
    NUMRealmServer:
      ${node.host}:
        instance.port: ${um.instance.port}
        instance.ip:   ${um.host}
        runtimeComponentId: Universal-Messaging-${instance.name}
        configuration:
          Universal-Messaging-${instance.name}:
            COMMON-CLUSTER:
              COMMON-CLUSTER: &umClusterConfig
              Name: ${um.cluster}
              Servers:                               # two UM instances cluster
```

```

Server:
-
  "@name": ${um.host}
  URL: "nsp://${um.host}:${um.instance.port}"
-
  "@name": ${um.host2}
  URL: "nsp://${um.host2}:${um.instance.port2}"

```

Create Clusters

Creates an active/active cluster of Universal Messaging servers.

Syntax

```

sagcc create configuration data nodeAlias Universal-Messaging-instanceName
COMMON-CLUSTER [--input|-i] filename.xml

```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance running in the specified installation.

COMMON-CLUSTER

Required. The ID of the configuration type of which you want to create an instance.

--input|-i *filename.xml*

Required. The XML file that contains the cluster configuration data.

Usage Notes

- The XML input file must contain the following cluster configuration properties:
 - Cluster name (required). A cluster name that is unique to the installation.
 - Server instances (required). The name, URL, and port of each server node in the cluster.
 - Sites (optional). The name of the site to which each server node belongs. *siteName* is a server-level property.
 - Primary site (optional). The name of the primary site, if you have configured sites in the cluster. *primeSite* is a cluster-level property that holds the name of the site that is flagged as *isPrime*.
- A Universal Messaging server instance can be part of only one cluster.
- If you remove all the server instances from a site, the site will be deleted. Server instance deletion is not allowed if the deletion operation leaves fewer than two server instances in the cluster.

Examples

The example creates a cluster with the following configuration properties specified in the `umSalesClusterConfig.xml` file:

- Cluster name: `umSales`
- Cluster sites: `site1` and `site2`
- Primary site: `site1`
- Server instances in `site1`: `um9000`, `um9001`
- Server instances in `site2`: `um9002`, `um9003`

To create the cluster "umSales" on the server instance with ID "Universal-Messaging-um9001", installed in the installation with alias name "sag01", using the file "umSalesClusterConfig.xml":

```
sagcc create configuration data sag01 Universal-Messaging-um9001  
COMMON-CLUSTER --input C:\inputxmls\umSalesClusterConfig.xml
```

The `umSalesClusterConfig.xml` file has the following format:

```
<?xml version="1.0" encoding="UTF-8"?>  
<ClusterSettings>  
  <Name>umSales</Name>  
  <Servers>  
    <Server name="um9000">  
      <URL>nsp://127.0.0.1:9000</URL>  
      <ExtendedProperties>  
        <Property name="siteName">site1</Property>  
      </ExtendedProperties>  
    </Server>  
    <Server name="um9001">  
      <URL>nsp://127.0.0.1:9001</URL>  
      <ExtendedProperties>  
        <Property name="siteName">site1</Property>  
      </ExtendedProperties>  
    </Server>  
    <Server name="um9002">  
      <URL>nsp://127.0.0.1:9002</URL>  
      <ExtendedProperties>  
        <Property name="siteName">site2</Property>  
      </ExtendedProperties>  
    </Server>  
    <Server name="um9003">  
      <URL>nsp://127.0.0.1:9003</URL>  
      <ExtendedProperties>  
        <Property name="siteName">site2</Property>  
      </ExtendedProperties>  
    </Server>  
  </Servers>  
  <ExtendedProperties>  
    <Property name="primeSite">site1</Property>  
  </ExtendedProperties>  
</ClusterSettings>
```

View Cluster Details

Retrieves details about a Universal Messaging cluster. You can retrieve the following information:

- The name of the cluster.
- The name, URL, and port of each Universal Messaging server instance in the cluster.
- Site information, if sites are configured.

Syntax

```
sagcc get configuration data nodeAlias Universal-Messaging-instanceName COMMON-CLUSTER
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance that is part of the cluster and runs in the specified installation.

COMMON-CLUSTER

Required. The ID of the configuration type for which you want to retrieve instance information.

Examples

To retrieve information about the cluster in which the server instance with ID "Universal-Messaging-um9001", installed in the installation with alias "sag01", participates:

```
sagcc get configuration data sag01 Universal-Messaging-um9001 COMMON-CLUSTER
```

Update Clusters

Updates an existing Universal Messaging cluster.

You can make the following changes in the input configuration XML file for the cluster:

- To add one or more server instances to the cluster, include the name, URL, and port of the server instances.
- To remove one or more server instances from the cluster, remove the configurations of the server instances.
- To create sites and assign server instances to sites, set the `siteName` extended property of the server instances.
- To make a site the prime site of the cluster, specify the name of the prime site as a value of the `primeSite` cluster-level property.

- To remove one or more server instances from a cluster site, remove the `siteName` extended property of the server instances.
- To remove sites from the cluster, remove the site definitions of all the server instances in the cluster.

Syntax

```
sagcc update configuration data nodeAlias Universal-Messaging-instanceName  
COMMON-CLUSTER [--input|-i] filename.xml
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance that runs in the specified installation and is part of the cluster you want to update.

COMMON-CLUSTER

Required. The ID of the configuration type of which you want to update an instance.

--input|-i *filename.xml*

Required. The XML file that contains the cluster configuration data.

Usage Notes

- The XML input file must contain the following cluster configuration properties:
 - Cluster name (required). A cluster name that is unique to the installation.
 - Server instances (required). The name, URL, and port of each server node in the cluster.
 - Sites (optional). The name of the site to which each server node belongs. `siteName` is a server-level property.
 - Primary site (optional). The name of the primary site, if you have configured sites in the cluster. `primeSite` is a cluster-level property that holds the name of the site that is flagged as `isPrime`.
- When you update a cluster, you edit only the parameters that specify the change. Other parameters in the cluster configuration file must not be changed.
- A Universal Messaging server instance can be part of only one cluster.
- If you remove all the server instances from a site, the site will be deleted. Server instance deletion is not allowed if the deletion operation leaves fewer than two server instances in the cluster.

Examples

To update the cluster "umSales" for the server instance with ID "Universal-Messaging-um9001", installed in the installation with alias name "sag01", using the file "umSalesClusterConfig.xml":

```
sagcc update configuration data sag01 Universal-Messaging-um9001
COMMON-CLUSTER --input C:\inputxmls\umSalesClusterConfig.xml
```

The umSalesClusterConfig.xml file has the following format:

```
<?xml version="1.0" encoding="UTF-8"?>
<ClusterSettings>
  <Name>umSales</Name>
  <Servers>
    <Server name="um9000">
      <URL>nsp://127.0.0.1:9000</URL>
      <ExtendedProperties>
        <Property name="siteName">site1</Property>
      </ExtendedProperties>
    </Server>
    <Server name="um9001">
      <URL>nsp://127.0.0.1:9001</URL>
      <ExtendedProperties>
        <Property name="siteName">site1</Property>
      </ExtendedProperties>
    </Server>
    <Server name="um9002">
      <URL>nsp://127.0.0.1:9002</URL>
      <ExtendedProperties>
        <Property name="siteName">site2</Property>
      </ExtendedProperties>
    </Server>
    <Server name="um9003">
      <URL>nsp://127.0.0.1:9003</URL>
      <ExtendedProperties>
        <Property name="siteName">site2</Property>
      </ExtendedProperties>
    </Server>
  </Servers>
  <ExtendedProperties>
    <Property name="primeSite">site1</Property>
  </ExtendedProperties>
</ClusterSettings>
```

Delete Clusters

Deletes a Universal Messaging cluster.

Syntax

```
sagcc delete configuration data nodeAlias Universal-Messaging-instanceName
COMMON-CLUSTER
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-instanceName

Required. The ID of the Universal Messaging server instance that runs in the specified installation and is part of the cluster you want to delete.

COMMON-CLUSTER

Required. The ID of the configuration type of which you want to delete an instance.

Examples

To delete the cluster that contains the server instance with ID "Universal-Messaging-um9001" installed in the installation with alias name "sag01":

```
sagcc delete configuration data sag01 Universal-Messaging-um9001 COMMON-CLUSTER
```

Migrate Clusters

You can migrate a Universal Messaging cluster automatically even if the nodes are installed on multiple hosts.

To automatically migrate a Universal Messaging cluster:

1. Add the following extended property to the source Universal Messaging cluster configuration XML file:

```
<ExtendedProperties>  
  <Property name="crossHostMigration">true</Property>  
</ExtendedProperties>
```

2. Run the `sagcc update configuration data` command.

A remote realms bootstrap configuration file is created in the *Universal Messaging_directory/bin* directory.

Channel and Queue Monitoring

List Administration Namespaces

Retrieves a list of the administration namespaces for a Universal Messaging server instance.

Syntax

```
sagcc get administration component nodeAlias Universal-Messaging-instanceName
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to retrieve the administration namespaces.

Examples

To retrieve the administration namespaces for the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc get administration component sag01 Universal-Messaging-umserver
```

List Monitoring Options

Retrieves information about the options available for monitoring channels and queues on a Universal Messaging server instance.

Syntax

- To list the options for monitoring channels:

```
sagcc get administration component nodeAlias Universal-Messaging-instanceName channels
```

- To list the options for monitoring queues:

```
sagcc get administration component nodeAlias Universal-Messaging-instanceName queues
```

Arguments and Options***nodeAlias***

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to retrieve the monitoring options.

Examples

- To retrieve the options for monitoring channels on the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc get administration component sag01 Universal-Messaging-umserver channels
```

- To retrieve the options for monitoring queues on the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc get administration component sag01 Universal-Messaging-umserver queues
```

List Channels or Queues

Lists all the channels or queues on a Universal Messaging server instance.

Syntax

- To list the channels on a server instance:

```
sagcc get administration component nodeAlias Universal-Messaging-instanceName channels list
```

- To list the queues on a server instance:

```
sagcc get administration component nodeAlias Universal-Messaging-instanceName queues list
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-instanceName

Required. The ID of the Universal Messaging server instance for which you want to list the channels or queues.

Examples

- To list the channels on the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc get administration component sag01 Universal-Messaging-umserver channels list
```

- To list the queues on the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc get administration component sag01 Universal-Messaging-umserver queues list
```

Get Channel or Queue Status

Retrieves the status of a specific channel or queue in TSV format for a Universal Messaging server instance.

Syntax

- To retrieve the status of a channel:

```
sagcc get administration component nodeAlias Universal-Messaging-instanceName channels status name=channelName
```

- To retrieve the status of a queue:

```
sagcc get administration component nodeAlias Universal-Messaging-instanceName queues status name=queueName
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-instanceName

Required. The ID of the Universal Messaging server instance for which you want to retrieve the channel or queue status.

name={channelName | queueName}

Required. The name of the channel or queue for which you want to retrieve status information.

Examples

- To view the status of channel "channel3" on the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc get administration component sag01 Universal-Messaging-umserver channels
status name=channel3
```

- To view the status of queue "queue1" on the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc get administration component sag01 Universal-Messaging-umserver queues
status name=queue1
```

Durable Subscribers Monitoring

View Administration Namespaces

Retrieves a list of the administration namespaces for a Universal Messaging server instance.

Syntax

```
sagcc get administration component nodeAlias Universal-Messaging-instanceName
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-instanceName

Required. The ID of the Universal Messaging server instance for which you want to retrieve the administration namespaces.

Examples

To retrieve the administration namespaces for the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc get administration component sag01 Universal-Messaging-umserver
```

View Monitoring Options

Retrieves information about the options available for monitoring durable subscribers on a Universal Messaging server instance.

Syntax

```
sagcc get administration component nodeAlias Universal-Messaging-instanceName  
durableSubscribers
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-instanceName

Required. The ID of the Universal Messaging server instance for which you want to retrieve the monitoring options.

Examples

To retrieve the options for monitoring durable subscribers on the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc get administration component sag01 Universal-Messaging-umserver durableSubscribers
```

List Durable Subscribers

Lists the durable subscribers on a Universal Messaging server instance in XML, TSV, or CSV format.

Syntax

```
sagcc get administration component nodeAlias Universal-Messaging-instanceName  
durableSubscribers list [--format|-f] {tsv|xml|csv}
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to list the durable subscribers.

{--format|-f} {tsv|xml|csv}

Required. The format in which to retrieve the list of durable subscribers. Values are:

- tsv
- xml
- csv

Examples

To list the durable subscribers in XML format on the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc get administration component sag01 Universal-Messaging-umserver durablesubscribers
list -f xml
```

List Durable Subscriber Attributes

Retrieves the attributes of a specific durable subscriber or a set of attributes for all durable subscribers on a Universal Messaging server instance.

Syntax

- To retrieve the attributes of a specific durable subscriber:

```
sagcc get administration component nodeAlias Universal-Messaging-instanceName
durablesubscribers details channel=channelName name=durableSubscriberName
{--format|-f} {xml|tsv|csv}
```

- To retrieve a set of attributes for all durable subscribers:

```
sagcc get administration component nodeAlias Universal-Messaging-instanceName
durablesubscribers list {--format|-f} {tsv|csv} properties=commaSeparatedList
```

Arguments and Options***nodeAlias***

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to retrieve a set of durable-subscriber attributes.

{--format|-f} {xml|tsv|csv}

Required. The format in which to retrieve the attributes of the durable subscribers. Values are:

- xml - Can be used only for retrieving the attributes of a specific durable subscriber.

- tsv
- csv

[properties=*commaSeparatedList*]

Required for retrieving a set of attributes. A comma-separated list of the attributes you want to retrieve.

Examples

- To list in XML format the attributes of durable subscriber "dsubscriber1" on channel "channel2", on the server instance with ID "Universal-Messaging-umserver", installed in the installation with alias name "sag01":

```
sagcc get administration component sag01 Universal-Messaging-umserver
durablesubscribers details channel=channel2 name=dsubscriber1 -f xml
```

- To list in TSV format the attributes "name", "channel", "lastEventID", and "outstandingEvents" of the durable subscribers on the server instance with ID "Universal-Messaging-umserver", installed in the installation with alias name "sag01":

```
sagcc get administration component sag01 Universal-Messaging-umserver
durablesubscribers list -f tsv properties=name,channel,lastEventID,outstandingEvents
```

List Events

Retrieves a list of events for a durable subscriber.

Syntax

```
sagcc get administration component nodeAlias Universal-Messaging-instanceName
durablesubscribers getDurableEvents durableName=durableSubscriberName
chanName=channelName
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to retrieve a list of events.

durableName=*durableSubscriberName*

Required. The name of the durable subscriber for which you want to retrieve a list of events.

chanName=*channelName*

Required. The name of the channel to which the durable subscriber is subscribed.

Examples

To retrieve the list of events for durable subscriber "dsubscriber1" on channel "channel2", on the server instance with ID "Universal-Messaging-umserver", installed in the installation with alias name "sag01":

```
sagcc get administration component sag01 Universal-Messaging-umserver
durablesubscribers getDurableEvents durableName=dsubscriber1 chanName=channel2
```

Purge Events

Purges a set of events or all events for a durable subscriber.

Syntax

- To purge a range of events:

```
sagcc exec administration component nodeAlias Universal-Messaging-instanceName
durablesubscribers purgeStartEndID startEID=startEventID endEID=endEventID
durableName=durableSubscriberName chanName=channelName
```

- To purge all events:

```
sagcc exec administration component nodeAlias Universal-Messaging-instanceName
durablesubscribers purgeAll durableName=durableSubscriberName chanName=channelName
```

- To purge specific events using filtering criteria:

```
sagcc exec administration component nodeAlias Universal-Messaging-instanceName
durablesubscribers purgeFilter durableName=durableSubscriberName chanName=channelName
filter=filterExpression
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-instanceName

Required. The ID of the Universal Messaging server instance for which you want to purge events.

durableName=durableSubscriberName

Required. The name of the durable subscriber for which you want to purge events.

chanName=channelName

Required. The name of the channel to which the durable subscriber is subscribed.

[startEID=startEventID]

Required for purging a range of events. The ID of the first event in the range.

[endEID=endEventID]

Required for purging a range of events. The ID of the last event in the range.

[filter=*filterExpression*]

Required when using a filter to purge events. The criteria used to purge events.

Examples

- To purge the events with IDs from "10" to "20" for durable subscriber "dsubscriber1" on channel "channel2", on the server instance with ID "Universal-Messaging-umserver", installed in the installation with alias name "sag01":

```
sagcc exec administration component sag01 Universal-Messaging-umserver
durableSubscribers purgeStartEndID startEID=10 endEID=20 durableName=dsubscriber1
chanName=channel2
```

- To purge all events for durable subscriber "dsubscriber1" on channel "channel2", on the server instance with ID "Universal-Messaging-umserver", installed in the installation with alias name "sag01":

```
sagcc exec administration component sag01 Universal-Messaging-umserver
durableSubscribers purgeAll durableName=dsubscriber1 chanName=channel2
```

- To purge the events with a size between "10.0" and "12.0" for durable subscriber "dsubscriber1" on channel "channel2", on the server instance with ID "Universal-Messaging-umserver", installed in the installation with alias name "sag01":

```
sagcc exec administration component sag01 Universal-Messaging-umserver
durableSubscribers purgeFilter durableName=dsubscriber1 chanName=channel2
filter=size BETWEEN 10.0 AND 12.0
```

Delete a Durable Subscriber

Deletes a durable subscriber on a specific channel.

Syntax

```
sagcc exec administration component nodeAlias Universal-Messaging-instanceName
durableSubscribers delete channel=channelName name=durableSubscriberName
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance on which you want to delete a durable subscriber.

channel=*channelName*

Required. The name of the channel on which you want to delete a durable subscriber.

name=*durableSubscriberName*

Required. The name of the durable subscriber you want to delete.

Examples

To delete durable subscriber "dsubscriber1" on channel "channel3", on the server instance with ID "Universal-Messaging-umserver", installed in the installation with alias name "sag01":

```
sagcc exec administration component sag01 Universal-Messaging-umserver
durablesubscribers delete channel=channel3 name=dsubscriber1
```

Channel Snoop

Start Snooping on a Channel

Starts snooping on events on a channel for a specific user.

Syntax

- To start snooping on events on a channel for a specific user:

```
sagcc exec administration component nodeAlias Universal-Messaging-instanceName
channels startSnoop name=channelName user=userName
```

- To start snooping on events on a channel for a specific user with filtering criteria:

```
sagcc exec administration component nodeAlias Universal-Messaging-instanceName
channels startSnoop name=channelName user=userName [fromid=firstEventId]
[toeid=lastEventId] [filter=filterString]
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance on which you want to start snooping.

name=*channelName*

Required. The name of the channel on which you want to snoop.

user=*userName*

Required. The username of the user for whom you want to start snooping.

[*fromid=firstEventId*]

Optional. The ID of the first event in the event range on which you want to start snooping.

[*toeid=lastEventId*]

Optional. The ID of the last event in the event range on which you want to start snooping.

[*filter=filterString*]

Optional. Additional filtering criteria based on the properties of the event.

Usage Notes

When you want to start snooping on a range of events:

- If you do not specify `fromeid`, the range of events starts with the first event on the channel and ends with the event specified for `toeid`.
- If you do not specify `toeid`, the range of events starts with the event specified for `fromeid` and ends with the last event on the channel.

Examples

- To start snooping on events on channel "channel2", created on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", for user "Administrator":

```
sagcc exec administration component sag01 Universal-Messaging-umserver
channels startSnoop name=channel2 user=Administrator
```

- To start snooping on the events with IDs from "2" to "10" on channel "channel2", created on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", for user "Administrator":

```
sagcc exec administration component sag01 Universal-Messaging-umserver
channels startSnoop name=channel2 user=Administrator fromid=2 toid=10
```

List Snooped Events on a Channel

Lists the snooped events on a channel for a specific user in TSV, XML, or JSON format.

Syntax

- To list the snooped events on a channel for a specific user in TSV format:

```
sagcc exec administration component nodeAlias Universal-Messaging-instanceName
channels snoop name=channelName user=userName
```

- To list the snooped events on a channel for a specific user in XML or JSON format:

```
sagcc exec administration component nodeAlias Universal-Messaging-instanceName
channels snoop name=channelName user=userName [--format|-f] {xml|json}
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to list snooped events.

name=channelName

Required. The name of the channel for which you want to list snooped events.

user=userName

Required. The username of the user for whom you want to list snooped events.

 [--format | -f] {xml | json}

Optional. Whether to list the snooped events in XML or JSON format.

Usage Notes

If the Universal Messaging server becomes unavailable after the snoop on the channel started, Command Central stops snooping all channels on that Universal Messaging server for all Command Central users. If you run the command that lists snooped events while the Universal Messaging server is unavailable, the system returns "snoopStarted=false" and an empty list of events.

Examples

- To list the snooped events in TSV format on channel "channel2", created on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", for user "Administrator":

```
sagcc exec administration component sag01 Universal-Messaging-umserver
channels snoop name=channel2 user=Administrator
```

- To list the snooped events in JSON format on channel "channel2", created on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", for user "Administrator":

```
sagcc exec administration component sag01 Universal-Messaging-umserver
channels snoop name=channel2 user=Administrator --format json
```

View Details of a Snooped Event on a Channel

Retrieves the details of a snooped event on a channel for a specific user in TSV, XML, or JSON format.

Syntax

- To retrieve the details of a snooped event on a channel for a specific user in TSV format:

```
sagcc exec administration component nodeAlias Universal-Messaging-instanceName
channels snoop name=channelName user=userName id=eventId
```

- To retrieve the details of a snooped event on a channel for a specific user in XML or JSON format:

```
sagcc exec administration component nodeAlias Universal-Messaging-instanceName
channels snoop name=channelName user=userName id=eventId [--format|-f] {xml|json}
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-instanceName

Required. The ID of the Universal Messaging server instance for which you want to retrieve a snooped event.

name=channelName

Required. The name of the channel on which the snooped event is published.

user=userName

Required. The username of the user for whom you want to retrieve the snooped event.

id=eventId

Required. The ID of the event that you want to view.

[[--format|-f] {xml|json}]

Optional. Whether to view the snooped event in XML or JSON format.

Usage Notes

The TSV format is tabular and does not display the header and properties of an event. To see the header and properties of an event, use the XML or JSON format.

Examples

- To view details of a snooped event with ID "2" in TSV format on channel "channel2", created on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", for user "Administrator":

```
sagcc exec administration component sag01 Universal-Messaging-umserver
channels event name=channel2 user=Administrator id=2
```

- To view details of a snooped event with ID "2" in XML format on channel "channel2", created on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", for user "Administrator":

```
sagcc exec administration component sag01 Universal-Messaging-umserver
channels event name=channel2 user=Administrator id=2 --format xml
```

Purge Snooped Events from a Channel

Purges a snooped event or a range of snooped events from a channel for a specific user.

Syntax

- To purge a snooped event from a channel and the snooped events list for a specific user:

```
sagcc exec administration component nodeAlias Universal-Messaging-instanceName
channels purgeEvent name=channelName user=userName id=eventId
```

- To purge a range of snooped events from a channel and the snooped events list for a specific user:

```
sagcc exec administration component nodeAlias Universal-Messaging-instanceName
channels purgeEvents name=channelName user=userName
[fromeid=firstEventId] [toeid=lastEventId]
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance on which you want to purge snooped events.

name=*channelName*

Required. The name of the channel from which you want to purge events.

user=*userName*

Required. The username of the user for whom you want to purge events.

id=*eventId*

Required with the `sagcc exec administration component purgeEvent` command. The ID of the event to purge.

[fromeid=*firstEventId*]

Optional. The ID of the first event in the event range that you want to purge.

[toeid=*lastEventId*]

Optional. The ID of the last event in the event range that you want to purge.

Usage Notes

When you want to purge a range of snooped events:

- If you do not specify `fromeid`, all events from the first one on the channel to the one with ID smaller than or equal to `toeid` are purged.
- If you do not specify `toeid`, all events from the one with ID greater than or equal to `fromeid` to the last one on the channel are purged.
- If you do not specify both `fromeid` and `toeid`, all events on the channel are purged.

Examples

- To purge a snooped event with ID "2" from channel "channel2", created on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", for user "Administrator":

```
sagcc exec administration component sag01 Universal-Messaging-umserver
channels purgeEvent name=channel2 user=Administrator id=2
```

- To purge the snooped events with IDs from "2" to "6" from channel "channel2", created on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", for user "Administrator":

```
sagcc exec administration component sag01 Universal-Messaging-umserver
channels purgeEvents name=channel2 user=Administrator fromid=2 toid=6
```

Stop Snooping on a Channel

Stops snooping on events on a channel for a specific user.

Syntax

```
sagcc exec administration component nodeAlias Universal-Messaging-instanceName
channels stopSnoop name=channelName user=userName
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-instanceName

Required. The ID of the Universal Messaging server instance on which you want to stop snooping.

name=channelName

Required. The name of the channel on which you want to stop snooping.

user=userName

Required. The username of the user for whom you want to stop snooping.

Examples

To stop snooping on events on channel "channel2", created on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", for user "Administrator":

```
sagcc exec administration component sag01 Universal-Messaging-umserver
channels stopSnoop name=channel2 user=Administrator
```

Queue Snoop

Start Snooping on a Queue

Starts snooping on events on a queue for a specific user.

Syntax

- To start snooping on events on a queue for a specific user:

```
sagcc exec administration component nodeAlias Universal-Messaging-instanceName
queues startSnoop name=queueName user=userName
```

- To start snooping on events on a queue for a specific user with filtering criteria:

```
sagcc exec administration component nodeAlias Universal-Messaging-instanceName
queues startSnoop name=queueName user=userName [fromeid=firstEventId]
[toeid=lastEventId] [filter=filterString]
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance on which you want to start snooping.

name=*queueName*

Required. The name of the queue on which you want to snoop.

user=*userName*

Required. The username of the user for whom you want to start snooping.

[*fromeid=firstEventId*]

Optional. The ID of the first event in the event range on which you want to start snooping.

[*toeid=lastEventId*]

Optional. The ID of the last event in the event range on which you want to start snooping.

[*filter=filterString*]

Optional. Additional filtering criteria based on the properties of the event.

Usage Notes

When you want to start snooping on a range of events:

- If you do not specify *fromeid*, the range of events starts with the first event on the queue and ends with the event specified for *toeid*.
- If you do not specify *toeid*, the range of events starts with the event specified for *fromeid* and ends with the last event on the queue.

Examples

- To start snooping on events on queue "queue1", created on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", for user "Administrator":

```
sagcc exec administration component sag01 Universal-Messaging-umserver
queues startSnoop name=queue1 user=Administrator
```

- To start snooping on the events with IDs from "2" to "10" on queue "queue1", created on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", for user "Administrator":

```
sagcc exec administration component sag01 Universal-Messaging-umserver
queues startSnoop name=queue1 user=Administrator fromid=2 toid=10
```

List Snooped Events on a Queue

Lists the snooped events on a queue for a specific user in TSV, XML, or JSON format.

Syntax

- To list the snooped events on a queue for a specific user in TSV format:

```
sagcc exec administration component nodeAlias Universal-Messaging-instanceName
queues snoop name=queueName user=userName
```

- To list the snooped events on a queue for a specific user in XML or JSON format:

```
sagcc exec administration component nodeAlias Universal-Messaging-instanceName
queues snoop name=queueName user=userName [--format|-f] {xml|json}
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-instanceName

Required. The ID of the Universal Messaging server instance for which you want to list snooped events.

name=queueName

Required. The name of the queue for which you want to list snooped events.

user=userName

Required. The username of the user for whom you want to list snooped events.

[--format|-f] {xml|json}

Optional. Whether to list the snooped events in XML or JSON format.

Usage Notes

If the Universal Messaging server becomes unavailable after the snoop on the queue started, Command Central stops snooping on all queues on that Universal Messaging server for all Command Central users. If you run the command that lists snooped events while the Universal Messaging server is unavailable, the system returns "snoopStarted=false" and an empty list of events.

Examples

- To list the snooped events in TSV format on queue "queue1", created on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", for user "Administrator":

```
sagcc exec administration component sag01 Universal-Messaging-umserver
queues snoop name=queue1 user=Administrator
```

- To list the snooped events in JSON format on queue "queue1", created on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", for user "Administrator":

```
sagcc exec administration component sag01 Universal-Messaging-umserver
queues snoop name=queue1 user=Administrator --format json
```

View Details of a Snooped Event on a Queue

Retrieves the details of a snooped event on a queue for a specific user in TSV, XML, or JSON format.

Syntax

- To retrieve the details of a snooped event on a queue for a specific user in TSV format:

```
sagcc exec administration component nodeAlias Universal-Messaging-instanceName
queues event name=queueName user=userName id=eventId
```

- To retrieve the details of a snooped event on a queue for a specific user in XML or JSON format:

```
sagcc exec administration component nodeAlias Universal-Messaging-instanceName
queues event name=queueName user=userName id=eventId [--format|-f] {xml|json}
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-instanceName

Required. The ID of the Universal Messaging server instance for which you want to retrieve a snooped event.

name=queueName

Required. The name of the queue on which the snooped event is published.

user=*userName*

Required. The username of the user for whom you want to retrieve the snooped event.

id=*eventId*

Required. The ID of the event that you want to view.

[[--format|-f] {xml|json}]

Optional. Whether to view the snooped event in XML or JSON format.

Usage Notes

The TSV format is tabular and does not display the header and properties of an event. To see the header and properties of an event, use the XML or JSON format.

Examples

- To view details of a snooped event with ID "2" in TSV format on queue "queue1", created on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", for user "Administrator":

```
sagcc exec administration component sag01 Universal-Messaging-umserver
queues event name=queue1 user=Administrator id=2
```

- To view details of a snooped event with ID "2" in XML format on queue "queue1", created on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", for user "Administrator":

```
sagcc exec administration component sag01 Universal-Messaging-umserver
queues event name=queue1 user=Administrator id=2 --format xml
```

Purge Snooped Events from a Queue

Purges all snooped events from a queue and the snooped events list for a specific user.

Syntax

```
sagcc exec administration component nodeAlias Universal-Messaging-instanceName
queues purgeEvents name=queueName user=userName
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance on which you want to purge snooped events.

name=*queueName*

Required. The name of the queue from which you want to purge events.

user=*userName*

Required. The username of the user for whom you want to purge events.

Usage Notes

You cannot purge a single event or a range of events from a queue.

Examples

To purge all snooped events from queue "queue1", created on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", for user "Administrator":

```
sagcc exec administration component sag01 Universal-Messaging-umserver
queues purgeEvents name=queue1 user=Administrator
```

Stop Snooping on a Queue

Stops snooping on events on a queue for a specific user.

Syntax

```
sagcc exec administration component nodeAlias Universal-Messaging-instanceName
queues stopSnoop name=queueName user=userName
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance on which you want to stop snooping.

name=*queueName*

Required. The name of the queue on which you want to stop snooping.

user=*userName*

Required. The username of the user for whom you want to stop snooping.

Examples

To stop snooping for events on queue "queue1", created on the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01", for user "Administrator":

```
sagcc exec administration component sag01 Universal-Messaging-umserver
queues stopSnoop name=queue1 user=Administrator
```

Event Publishing

Publish Events

Publishes an event on a channel or queue.

Syntax

- To publish an event on a channel:

```
cc exec administration component nodeAlias Universal-Messaging-instanceName
channels publish name=channelName data=eventContent [tag=eventTag] [ttl=ttlValue]
[persistent={true|false}] [transient={true|false}] [properties=propertiesString]
[pubcount=publishCount] [sendasprotobuf={true|false}]
[protobufdescriptor=protobufDescriptor]
```

- To publish an event on a queue:

```
cc exec administration component nodeAlias Universal-Messaging-instanceName
queues publish name=queueName data=eventContent [tag=eventTag] [ttl=ttlValue]
[persistent={true|false}] [properties=propertiesString]
[pubcount=publishCount] [sendasprotobuf={true|false}]
[protobufdescriptor=protobufDescriptor]
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance on which you want to publish an event.

name=*channelName*

Required for publishing an event on a channel. The name of the channel on which you want to publish an event.

name=*queueName*

Required for publishing an event on a queue. The name of the queue on which you want to publish an event.

data=*eventContent*

Required. The content of the event.

[tag=*eventTag*]

Optional. The tag of the event.

[ttl=*ttlValue*]

Optional. The time-to-live (TTL) of the event in milliseconds. Defines how long the event remains available on the channel or queue. If you specify a TTL of 0, the event remains on the channel or queue indefinitely.

[persistent={true | false}]

Optional. Whether the event is persistent. Values are:

- true
- false (default)

[transient={true | false}]

Optional. Supported only for channels. Whether the event is transient. Values are:

- true
- false (default)

[properties=propertiesString]

Optional. A string that contains event properties in the following JSON format:

```
[ { name: "property1_name", type: "property1_type", value: property1_value }, { name:
"property2_name", type: "property2_type", value: property2_value }, ... ]
```

where

- propertyX_name is the name of the property.
- propertyX_type is the type of the property and can have one of the following values: int, byte, long, short, float, double, boolean, char, string, int[], byte[], long[], short[], float[], double[], boolean[], char[], and string[].
- propertyX_value is the value of the property.

[pubcount=publishCount]

Optional. The number of times to republish an event. If you omit pubcount, the option defaults to 1.

[sendasprotobuf={true | false}]

Optional. Whether to convert the event content in the data option to a Protobuf event that matches a Protobuf schema specified in the protobufdescriptor option and already uploaded on the channel or queue. Values are:

- true
- false (default)

For more information about working with Protobuf events, see the "Google Protocol Buffers" section in the *Universal Messaging Concepts* guide.

[protobufdescriptor=protobufDescriptor]

Required for Protobuf events. The Protobuf file descriptor that defines the messaging schema to be used for converting the event content in the data option to a Protobuf event.

For more information about working with Protobuf events, see the "Google Protocol Buffers" section in the *Universal Messaging Concepts* guide.

Usage Notes

- When you use the properties option, consider the following information:

- Include the `-f json` option to specify the format of the properties string.
- Enclose char and string property values, and values with spaces in double quotes (`"`). If the value contains double quotes, replace them with a backslash and double quotes (`\"`).
- For array values, specify a valid JSON array of the corresponding type.
- When you want to publish a Protobuf event, consider the following information:
 - Before publishing a Protobuf event, you must upload on the channel or queue the Protobuf file descriptor that defines the Protobuf schema, as part of a file descriptor set. For information about uploading a Protobuf file descriptor set on a channel or queue, see [“Channels” on page 190](#) or [“Queues” on page 208](#).
 - The value of the `data` option is a JSON string that represents the Protobuf event.
 - The value of the `protobufdescriptor` option is the name of the Protobuf file descriptor that defines the message schema.

Examples

- To publish an event with event data "CustomerOrders" and event tag "COrders" on channel "channel2" that is created on the server instance with ID "Universal-Messaging-umserver", installed in the installation with alias name "sag01":

```
cc exec administration component sag01 Universal-Messaging-umserver channels
publish name=channel2 data=CustomerOrders tag=COrders
```

- To publish a persistent event with event data "CustomerOrders", event tag "COrders", and TTL "10000" three times on queue "queue1" that is created on the server instance with ID "Universal-Messaging-umserver", installed in the installation with alias name "sag01":

```
cc exec administration component sag01 Universal-Messaging-umserver queues
publish name=queue1 data=CustomerOrders tag=COrders ttl=10000
persistent=true pubcount=3
```

- To publish an event with event data "CustomerOrders", event tag "COrders", and custom properties in JSON format on queue "queue1" that is created on the server instance with ID "Universal-Messaging-umserver", installed in the installation with alias name "sag01":

```
cc exec administration component sag01 Universal-Messaging-umserver queues
publish name=queue1 data=CustomerOrders tag=COrders
properties="[ { name: \"orderNumber\", type: \"string\", value: \"F18LP\" },
{ name: \"items\", type: \"int\", value: 3 },
{ name: \"itemIds\", type: \"int[]\", value: [ 509, 19, 100 ] } ]" -f json
```

- To publish a Protobuf event on channel "channel2" that is created on the server instance with ID "Universal-Messaging-umserver", installed in the installation with alias name "sag01":

```
cc exec administration component sag01 Universal-Messaging-umserver channels
publish name=channel2
data="{ header: { id: 1, time: 1541163198345 },
contents: { intData: 124, doubleData: 3.141593, stringData: \"Software AG\" } }"
protobufdescriptor=Event sendasprotobuf=true
```

The example assumes that a Protobuf file descriptor set containing the following descriptors has already been uploaded on "channel2". The Protobuf event in the example is created from the "Event" message type in the file descriptor set. The event data is a valid JSON string that represents a message of type "Event" and has the same fields as the "Event" message type.

```
file {
  name: "EventWrapper"
  package: "um"
  dependency: "HeaderWrapper"
  dependency: "ContentsWrapper"
  message_type {
    name: "Event"
    field {
      name: "header"
      number: 1
      label: LABEL_REQUIRED
      type: TYPE_MESSAGE
      type_name: "Header"
    }
    field {
      name: "contents"
      number: 2
      label: LABEL_REQUIRED
      type: TYPE_MESSAGE
      type_name: "Contents"
    }
  }
}
file {
  name: "HeaderWrapper"
  package: "um"
  message_type {
    name: "Header"
    field {
      name: "id"
      number: 1
      label: LABEL_REQUIRED
      type: TYPE_INT32
    }
    field {
      name: "time"
      number: 2
      label: LABEL_REQUIRED
      type: TYPE_SINT64
    }
  }
}
file {
  name: "ContentsWrapper"
  package: "um"
  message_type {
    name: "Contents"
    field {
      name: "intData"
      number: 1
      label: LABEL_REQUIRED
      type: TYPE_SINT32
    }
    field {
```

```

    name: "doubleData"
    number: 4
    label: LABEL_REQUIRED
    type: TYPE_DOUBLE
  }
  field {
    name: "stringData"
    number: 5
    label: LABEL_REQUIRED
    type: TYPE_STRING
  }
}
}

```

Republish Events

Republishes a snooped event on a channel or queue.

Syntax

- To republish a snooped event on a channel:

```

cc exec administration component nodeAlias Universal-Messaging-instanceName
channels publish name=channelName data=eventContent id=originalEventId
user=userName republish=true [tag=eventTag] [ttl=ttlValue]
[persistent={true|false}] [transient={true|false}] [properties=propertiesString]
[pubcount=publishCount] [sendasprotobuf={true|false}]
[protobufdescriptor=protobufDescriptor] [purgeoriginal={true|false}]

```

- To republish a snooped event on a queue:

```

cc exec administration component nodeAlias Universal-Messaging-instanceName
queues publish name=queueName data=eventContent republish=true [tag=eventTag]
[ttl=ttlValue] [persistent={true|false}]
[properties=propertiesString] [pubcount=publishCount]
[sendasprotobuf={true|false}] [protobufdescriptor=protobufDescriptor]

```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance on which you want to republish a snooped event.

name=*channelName*

Required for republishing an event on a channel. The name of the channel on which you want to republish a snooped event.

name=*queueName*

Required for republishing an event on a queue. The name of the queue on which you want to republish a snooped event.

data=eventContent

Required. The content of the event.

id=originalEventId

Required when republishing an event on a channel. The ID of the original event.

user=userName

Required when republishing an event on a channel. The username of the user who started snooping on the event on the channel.

republish={true | false}

Required. Whether to republish the snooped event. Values are:

- true
- false (default)

[purgeoriginal={true | false}]

Optional. Whether to purge the original event from the channel. Values are:

- true
- false (default)

[tag=eventTag]

Optional. The tag of the event.

[ttl=ttlValue]

Optional. The time-to-live (TTL) of the event in milliseconds. Defines how long the event remains available on the channel or queue. If you specify a TTL of 0, the event remains on the channel or queue indefinitely.

[persistent={true | false}]

Optional. Whether the event is persistent. Values are:

- true
- false (default)

[transient={true | false}]

Optional. Supported only for channels. Whether the event is transient. Values are:

- true
- false (default)

[properties=propertiesString]

Optional. A string that contains event properties in the following JSON format:

```
[ { name: "property1_name", type: "property1_type", value: property1_value }, { name: "property2_name", type: "property2_type", value: property2_value }, ... ]
```

where

- propertyX_name is the name of the property.

- `propertyX_type` is the type of the property and can have one of the following values: `int`, `byte`, `long`, `short`, `float`, `double`, `boolean`, `char`, `string`, `int[]`, `byte[]`, `long[]`, `short[]`, `float[]`, `double[]`, `boolean[]`, `char[]`, and `string[]`.
- `propertyX_value` is the value of the property.

[`pubcount=publishCount`]

Optional. The number of times to republish an event. If you omit `pubcount`, the option defaults to 1.

[`sendasprotobuf={true|false}`]

Optional. Whether to convert the event content in the `data` option to a Protobuf event that matches a Protobuf schema specified in the `protobufdescriptor` option and already uploaded on the channel or queue. Values are:

- `true`
- `false` (default)

For more information about working with Protobuf events, see the "Google Protocol Buffers" section in the *Universal Messaging Concepts* guide.

[`protobufdescriptor=protobufDescriptor`]

Required for Protobuf events. The Protobuf file descriptor that defines the messaging schema to be used for converting the event content in the `data` option to a Protobuf event.

For more information about working with Protobuf events, see the "Google Protocol Buffers" section in the *Universal Messaging Concepts* guide.

Usage Notes

- When you use the `properties` option, consider the following information:
 - Include the `-f json` option to specify the format of the `properties` string.
 - Enclose `char` and `string` property values, and values with spaces in double quotes (`"`). If the value contains double quotes, replace them with a backslash and double quotes (`\`).
 - For array values, specify a valid JSON array of the corresponding type.
- Before republishing a snooped event on a channel or queue, you must start snooping on the channel or queue and obtain the event ID.

Examples

To republish an event with ID "3", modified event data "CancelledCustomerOrders", and modified event tag "CCOrders", snooped by user "Administrator", on channel "channel2" that is created on the server instance with ID "Universal-Messaging-umserver", installed in the installation with alias name "sag01":

```
cc exec administration component sag01 Universal-Messaging-umserver channels
publish name=channel2 data=CnancelledCustomerOrders tag=CCOrders
republish=true id=3 user=Administrator
```

Server Inventory Commands

Get Server Inventory

Retrieves information about a Universal Messaging server instance. The following list shows the information you can view and the value the command returns for each property:

- Display name - `Universal-Messaging-instanceName`
- Run-time component ID - `Universal-Messaging-instanceName`
- Product ID - `NUMRealmServer`
- Run-time component category - `PROCESS`

Syntax

```
sagcc get inventory components nodeAlias Universal-Messaging-instanceName
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-instanceName

Required. The ID of the Universal Messaging server instance for which you want to retrieve information.

Examples

To retrieve information about the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc get inventory components sag01 Universal-Messaging-umserver
```

List Server Inventory

Lists information about a Universal Messaging server instance. The following list shows the information you can view and the value the command returns for each property:

- Display name - `Universal-Messaging-instanceName`
- Run-time component ID - `Universal-Messaging-instanceName`
- Product ID - `NUMRealmServer`
- Run-time component category - `PROCESS`

Syntax

```
sagcc list inventory components nodeAlias Universal-Messaging-instanceName
```

Arguments and Options

nodeAlias

Required. The alias name of the installation in which the Universal Messaging server instance is installed.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to retrieve information.

Examples

To retrieve information about the server instance with ID "Universal-Messaging-umserver" installed in the installation with alias name "sag01":

```
sagcc list inventory components sag01 Universal-Messaging-umserver
```

Asset Deployment

List Assets

Lists the assets that are installed on the specified installation for the specified Universal Messaging server instance.

Important:

The asset inventory commands are a preview feature that is subject to change in the future. This preview has limited functions and is not intended for use in a production environment. If you want to provide feedback for this preview feature, go to the Command Central area on the Software AG TechCommunity website.

Syntax

```
sagcc list inventory assets nodeAlias Universal-Messaging-instanceName
```

Arguments and Options

nodeAlias

Required. The alias name of the installation for which you want to retrieve asset information.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to retrieve asset information.

Examples

To list the assets for the server instance with ID "Universal-Messaging-umserver" that is installed in the installation with alias name "sag01":

```
sagcc list inventory assets sag01 Universal-Messaging-umserver
```

Install Assets

Installs Universal Messaging assets from an asset repository into a target node.

Important:

- Universal Messaging does not support the `sagcc exec provisioning assets uninstall` command for uninstalling assets.
- The asset inventory commands are a preview feature that is subject to change in the future. This preview has limited functions and is not intended for use in a production environment. If you want to provide feedback for this preview feature, go to the Command Central area on the Software AG TechCommunity website.

Syntax

```
sagcc exec provisioning assets install nodeAlias repoName  
Universal-Messaging-instanceName [assets=AssetId1,AssetId2,...]
```

Arguments and Options

nodeAlias

Required. The alias name of the target node on which you want to install assets.

repoName

Required. The name of the asset repository from which you want to install assets.

Universal-Messaging-*instanceName*

Required. The ID of the Universal Messaging server instance for which you want to install assets.

[*assets=AssetId1,AssetId2,...*]

Optional. A comma-separated list of the IDs of the assets you want to install. You can omit this argument if you install assets from a repository that contains only assets for a single Universal Messaging server instance. If the asset repository has assets for several run-time components, you must include the argument and list only the assets for the Universal Messaging server instance specified in the command.

Usage Notes

Command Central supports installing only composite assets created with the Asset Build Environment and stored in an asset repository registered in Command Central.

Examples

The asset repository with name "repo1" contains assets only for the server instance with ID "Universal-Messaging-umserver". To install the assets from "repo1" for the "Universal-Messaging-umserver" server instance on the target installation with alias name "sag01":

```
sagcc exec provisioning assets install sag01 repo1 Universal-Messaging-umserver
```

Lifecycle Actions for Universal Messaging Server

The following table lists the actions that Universal Messaging supports with the `sagcc exec lifecycle` command and the operation taken against a Universal Messaging server when an action is executed.

Important:

When a Universal Messaging server instance is running as a service, you cannot perform administrative tasks such as check the status, or start and stop the server instance.

Action	Description
start	Starts the Universal Messaging server instance. When successful, the Universal Messaging server instance run-time status is set to ONLINE.
stop	Stops the Universal Messaging server instance. The Universal Messaging server run-time status is STOPPED.
restart	Stops, then restarts the Universal Messaging server instance. The Universal Messaging server run-time status is set to ONLINE.

Run-time Monitoring States for Universal Messaging Server

The `sagcc get monitoring runtimestate` and `sagcc get monitoring state` commands provide information about the following key performance indicators (KPIs) for a Universal Messaging server instance.

KPI	Description
JVM memory usage	<p>Indicates the utilization of JVM memory.</p> <p>The KPI uses the following marginal, critical, and maximum values:</p> <ul style="list-style-type: none"> ■ Marginal is 80% of the maximum JVM memory. ■ Critical is 95% of the maximum JVM memory. ■ Maximum is 100% of the maximum JVM memory.
Fanout backlog	Indicates the total number of events currently waiting to be processed by the fanout engine. If the fanout backlog is more than the critical

KPI	Description
	<p>value, there is a possibility that the subscribers receive the published events after some delay.</p> <p>The KPI uses the following marginal, critical, and maximum values:</p> <ul style="list-style-type: none"> ■ Marginal is 80% of the maximum value. ■ Critical is 95% of the maximum value. ■ Maximum is 100% of the peak value (high-water mark) of fanout backlog. Default is 100.
Tasks queued for read and write	<p>Indicates the total number of tasks in the read, write, and common read/write pools. If the number of read and write tasks queued is more than the critical value, it indicates that the Universal Messaging server instance is unable to match the speed of the publishers and subscribers.</p> <p>The KPI uses the following marginal, critical, and maximum values:</p> <ul style="list-style-type: none"> ■ Marginal is 80% of the maximum value. ■ Critical is 95% of the maximum value. ■ Maximum is 100% of the peak value (high-water mark) of read and write tasks queued. Default is 100.

Run-time Monitoring Statuses for Universal Messaging Server

The following table lists the run-time statuses that a Universal Messaging server instance can return in response to the `sagcc get monitoring state` command, and the meaning of each status.

Important:

When a Universal Messaging server instance is running as a service, you cannot perform administrative tasks such as check the status, or start and stop the server instance.

Note:

The Universal Messaging server instance does not return the STOPPING and STARTING statuses.

Run-time Status	Meaning
ONLINE	Universal Messaging server instance is running.
FAILED	Universal Messaging server instance is not running due to some failure. LOCK file exists.

Run-time Status	Meaning
STOPPED	Universal Messaging server instance is not running because it was shut down normally. LOCK file does not exist.
UNRESPONSIVE	Universal Messaging server instance does not respond to a ping operation. LOCK file exists and the Universal Messaging server instance is running.
UNKNOWN	The status of Universal Messaging server instance cannot be determined.
ONLINE_MASTER	Server instance is online and it is the master node in the cluster.
ONLINE_SLAVE	Server instance is online and it is the slave node in the cluster.
ERROR	Server instance is part of a cluster that does not satisfy the requisite quorum.

Deployment of Universal Messaging Assets

On-Premise Deployment of Assets

You can deploy Universal Messaging assets on-premise, using the Command Central command-line interface. On-premise deployment is based on a push model. For information about the asset deployment commands, see [“Asset Deployment” on page 300](#).

Asset Deployment in the Cloud

For cloud-based deployment, the cloud and container deployments require a pull-model approach for asset deployment.

The pull model is based on Landscape Asset Registry (LAR) and its change listeners. Universal Messaging needs to integrate with the LAR-based update mechanism for deployment of its assets.

Configuration types supported for cloud deployment

The following table lists the configuration types supported for cloud deployment.

Configuration type	Description
JNDI connection factory	On JNDI look-up for the connection factory, the connection factory URL is set to the value used while building the JNDI context (<code>java.naming.provider.url</code>)

Configuration type	Description
JNDI destinations	<p>For native messaging, Integration Server creates the channel or queue as soon as the publishable document type is created. This would include the protocol buffer definitions.</p> <p>Only JMS destination deployment is supported for cloud-based deployment as native ones are created by Integration Server. All the JNDI destinations are exported with the parameter <code>autoCreateDest</code> set to true, so that all the channels or queues are created automatically. The newly created channel or queues will have default Universal Messaging configurations. For more information about JNDI destinations, see “JNDI Destinations Configuration” on page 251.</p> <p>The durables will be created automatically after the Integration Server triggers are started for the first time.</p>
Realm ACLs and groups	Basic authentication is enabled by default, and the default ACL setting has full privileges.
Common users	Universal Messaging users are migrated, and the users are created (stored in <code>users.txt</code> file) with custom passwords.

Templates for Provisioning Universal Messaging

You can provision and configure Universal Messaging servers using Command Central templates. You can start with the sample micro templates available in the [sagdevops-templates.git](#) project, which you can adapt for your own use case:

- [sag-um-cluster](#) - provision Universal Messaging clusters. You can use the template as a sample to provision a cluster with two nodes, a cluster with three nodes, as well as a four-node cluster with two sites.
- [sag-um-config](#) - configure Universal Messaging queues.

Note:

Universal Messaging no longer supports transient, simple, offheap, and paged queues. If you created a custom template, based on the `sag-um-config` template, which contains any of these queue types as a value for the `um.q.type` parameter, you must update the parameter value and re-import the template in Command Central.

- [sag-um-server](#) - provision a Universal Messaging server.

You can also export an installed Universal Messaging instance to a micro template and use it to create a Universal Messaging layer in a stack. If you are familiar with template development in Command Central, you can also create a custom micro template from scratch.

For details about creating and using the Command Central templates, see *Software AG Command Central Help* and the readmes of the Universal Messaging sample templates in [sagdevops-templates.git](#).

4 Comparison of Enterprise Manager and Command Central Features

Area	Enterprise Manager Feature	Supported in Command Central
Audit	View audit log entries: Order by user, type etc. Stream or archive audit file	No
Channel/Queue	Create a join from a channel ... set name source channel remote realm/cluster for inter-cluster joins filter hop count purge forward archival	Yes
Channel/Queue	View and/or delete <i>named objects</i> View outstanding events, configuration, etc. view messages purge messages view status e.g. last eventID	Yes
Channel/Queue	Create channel ... name, type, TTL, capacity, dead event store	Yes

Area	Enterprise Manager Feature	Supported in Command Central
	JMS engine and merge engine protobuf descriptor channel key (with name and depth) full storage properties	
Channel/Queue	Update protocol buffer definition	Yes
Channel/Queue	View/modify incoming/outgoing joins	Yes
Channel/Queue	View and modify ACLs	Yes
Channel/Queue	Edit channel/queue Full storage properties dialogue	Partial Properties can be changed but any messages on the channel/queue will not be retained
Channel/Queue	Publish to any channel/queue Full message properties dialogue	No
Channel/Queue	Create a copy of any channel/queue with option to edit specific fields/settings	No
Channel/Queue	View store-level connection lists and stats	Yes <i>Find under:</i> Consumer Info tab, along with other durable details
Channel/Queue	Bounce and redirect connections	Partial <i>Find under:</i> durables stats page, along with other durable details
Channel/Queue	Bulk apply ACL changes to folders of channels or queues	No
Channel/Queue	Purge events from EID to EID filter	Yes

Area	Enterprise Manager Feature	Supported in Command Central
	purge all	
Channel/Queue	Perform maintenance	No
Channel/Queue	Snoop events on store Edit and republish events with full message edit dialogue	No
Channel/Queue	Snoop (edit and republish) message content of events encoded as protocol buffers	No
Cluster	Create/delete clusters Set name of cluster at creation time	Yes
Cluster	Modify Cluster membership	Yes
Cluster	See Clusterwide stats: cluster matrix (state of each node as seen by other nodes) event rates connections etc.	Partial cluster members and their state can be viewed
Cluster	Optionally choose to migrate stores at cluster migration and warn of conflicts	No
Comms	Allow creating, deleting, starting, stopping of interfaces	Yes
Comms	View and edit all configuration options available on interfaces, including JavaScript configuration	Yes
Comms	View live per-interface level stats (connections, idle threads, etc.)	No
Comms	Set up via lists on interfaces	No
Comms	Configure, add, delete and view multicast configuration and state Multicast configuration: view configuration and state	No

Area	Enterprise Manager Feature	Supported in Command Central
	configure, add. delete	
Comms	Shared memory View configuration Configure, add and delete	Yes
Comms	Bounce and redirect connections	No
Connection	View details per connection	No
DataGroups	Add datagroup and their properties: name multicast priority conflation:merge/drop/interval	No
DataGroups	Delete datagroup	No
DataGroups	Publish to any datagroup (including default datagroup) Full message properties dialogue	No
DataGroups	Add/remove datagroups from other datagroups	No
Inter-cluster connections	Add, modify, view inter-cluster connections	No
Inter-cluster, joins	Add joins between stores in different clusters or on remote realms (unclustered)	No
Realm	Enterprise Manager tab <i>Config</i> View and change realm configuration options	Yes
Realm	Connect to realms Auto-discover other realms in cluster	Yes
Realm	Display IP/host and port of realms/clusters	Yes
Realm	View logs: UM log	Yes, with some additional options

Area	Enterprise Manager Feature	Supported in Command Central
	stream log to file filter log force roll log	
Realm	Apply namespace filter to see only partial list of resources on realm	Yes ... but separate for channels and queues
Realm	View all channels/queues/datagroups	Partial <i>Exception:</i> DataGroups
Realm	View graphs of ... event history/rate heap memory usage direct memory usage	Partial <i>Limited to:</i> Fanout backlog JVM memory Queued tasks of a server No graphs
Realm	Event status consumed published consumed/published rates connection rates numbers current total numbers of channels datagroups data streams Memory usage total free used change	Partial <i>Find under:</i> channels memory config

Area	Enterprise Manager Feature	Supported in Command Central
	direct total direct free	
Realm	Bulk apply ACLs to all channels or queues.	Partial ... available using templates
Realms	View all known connected realms and their state	Partial Stats are only shown in the channels
Realm	View ... current connections rate of connections total connections And for each connection see ... protocol user host connection description, including ephemeral port, language and name	No
Realm	Enterprise Manager tab <i>JNDI</i> View and modify JNDI on the realm	Yes
Realm	Add/Remove realms from each other Mount realms in namespace	No
Realm	Import/Export full/partial realmXML	No ... but most configurations can be exported
Realm	Request ... maintenance thread dump release of cached memory	No

Area	Enterprise Manager Feature	Supported in Command Central
	roll of server log	
Realm	Enterprise Manager tab <i>Monitoring</i> > <i>Top View ...</i> CPU usage garbage collection heap usage per channel stats on disk and memory usage	Partial
Security	Set resource specific ACLs on realm, channel and queue. Add/remove ACLs including security groups.	Yes
Security	Define user security groups with name and member IP Add/remove members to groups, including other groups	Yes
Sites	Add/remove, modify sites Modify prime site membership	Yes
Threads	View all threadpool:	No
Zones	Zones: Add Modify Configure	Yes

5 Setting up Active/Passive Clustering with Shared Storage

- About Active/Passive Clustering 316
- Overview of Active/Passive Clustering on Windows 320
- Overview of Active/Passive Clustering on UNIX 322
- Configuring a Universal Messaging Active/Passive Cluster on UNIX 323

About Active/Passive Clustering

Active/passive clustering is a solution that uses clustering software and special purpose hardware to minimize system downtime. Active/passive clusters are groups of computing resources that are implemented to provide high availability of software and hardware computing services. Active/passive clusters operate by having redundant groups of resources (such as CPU, disk storage, network connections, and software applications) that provide service when the primary system resources fail.

In a high availability active/passive clustered environment, one of the nodes in the cluster will be active and the other nodes will be inactive. When the active node fails, the cluster fails over to one of the inactive nodes automatically. As a part of this failover process, clustering software will start the resources on the redundant node in a predefined order (or resource dependency) to ensure that the entire node comes back up correctly.

Universal Messaging can run in an active/passive cluster environment, under Windows or UNIX. This approach does not provide load balancing or scalability.

Active/Passive Clustering Requirements

You need the following to configure a Software AG Universal Messaging active/passive cluster:

- Cluster control software to manage the clusters on Windows or UNIX.
- Shared Storage for sharing data files.
- IP address for running the Universal Messaging cluster service.
- Universal Messaging installed on the cluster nodes in the same directory path (for example, C:\SoftwareAG_UM). In the installations, the data directory path for the shared storage must be the same.

Important: Universal Messaging installation must be identical on all cluster nodes. All instances of Universal Messaging must point to the same Universal Messaging storage files on the shared storage.

Universal Messaging Capabilities for Active/Passive Clustering

The following capabilities of Universal Messaging enable the vendor-specific cluster control software to monitor and manage Universal Messaging in an active/passive cluster.

- Functionality to start, stop, and monitor the servers.
- Ability to store the server's state information and data on a shared disk.
- Ability to survive a crash and restart itself in a known state.
- Ability to meet license requirements and host name dependencies.

Virtual IP Address of an Active/Passive Cluster

A virtual IP address is like any other IP address except it does not have a specific host or node to resolve to. It resolves at run time to a server wherever the IP is physically bound and reachable on the network.

For client applications to access the services in an active/passive cluster in a transparent way, the virtual IP address of the cluster must be supplied to the client applications. This virtual IP address is usually referred to as the "logical host." This logical host identity is a network address (or host name) and is not tied to a single cluster server.

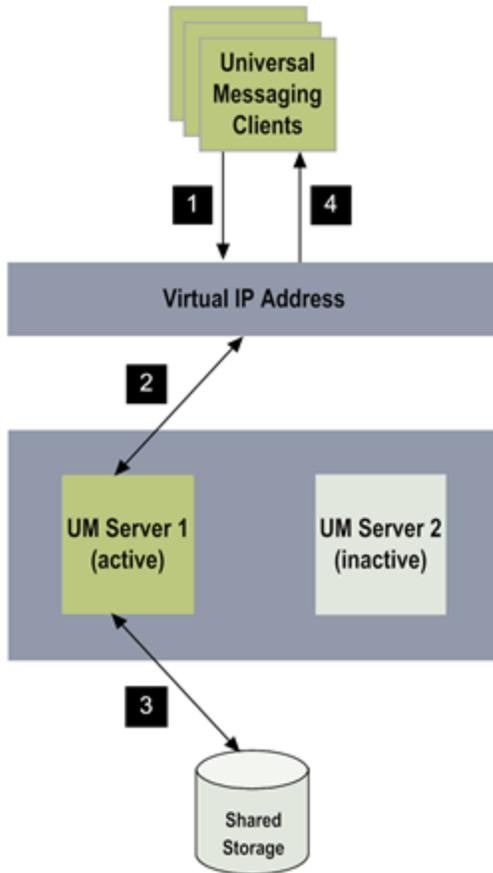
When there is a failover, the cluster control software will resolve the virtual IP address to the physical IP address of the current active server in the cluster. The client application is not affected in any way other than experiencing a brief outage of the services.

Failover Mechanism in an Active/Passive Cluster

Universal Messaging runs as a service in a cluster. Within an active/passive cluster, there only be a single instance of Universal Messaging server running at any given time. The other Universal Messaging servers are inactive.

In a clustered environment, when a client makes a request to a server, the server handles the request much the same as in an unclustered environment, except that the server writes the client information to a shared disk instead of a private data store.

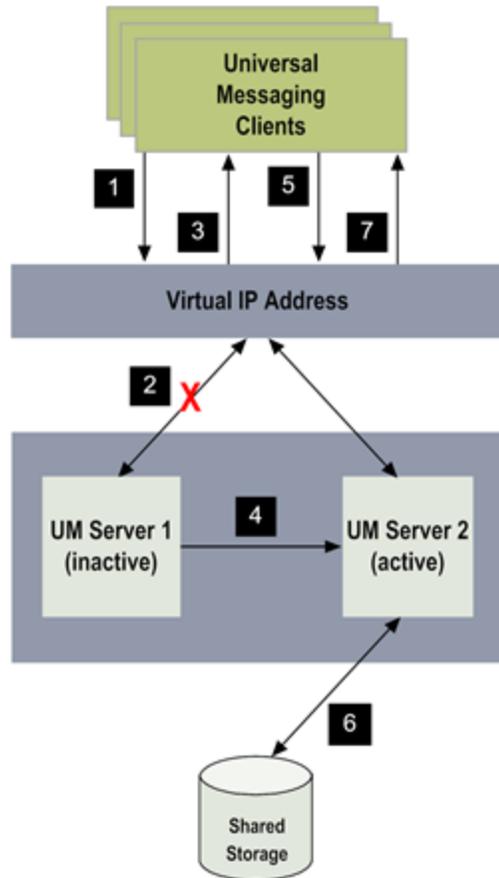
The following diagram illustrates the flow of documents through a typical clustered environment.



Steps	Description
-------	-------------

- | | |
|---|---|
| 1 | Universal Messaging clients use the virtual IP address of the cluster to connect to the active/passive Universal Messaging cluster. |
| 2 | Cluster control software forwards the client request to the active server in the cluster. |
| 3 | The active server reads data from or writes data to the shared storage. |
| 4 | Universal Messaging returns the results to the client application. |

The following diagram illustrates the failover in a clustered environment. If a server fails, subsequent requests for the session are redirected to a spare server in the cluster that is currently active and running.



Steps	Description
1	Universal Messaging clients use the virtual IP address of the cluster to connect to the active/passive Universal Messaging cluster.
2	The active server experiences failure and shuts down.
3	The cluster software returns the error code to the client.
4	Cluster control software marks the spare server as active.
5	Cluster control software forwards the client request to the active server in the cluster.
6	The active server reads data from or writes data to the shared storage.
7	Universal Messaging returns the results to the client application.

Cluster Verification

A cluster installation consultant will typically perform the cluster installation for you; however, verify the following to make sure that the cluster is installed properly:

- The shared drive can be accessed from the cluster nodes.
- The virtual IP address of the cluster is accessible on the public network.
- Only one Universal Messaging server instance in the cluster can access the shared drive at any given time.

Roles and Responsibilities for Configuring an Active/Passive Cluster

Configuring Universal Messaging in a high-availability cluster requires the efforts of the following people:

- System administrator
- Cluster vendor's installation consultant
- Universal Messaging administrator

Role	Responsibilities
System administrator	Perform system and network administration tasks.
Cluster vendor's installation consultant	Install cluster hardware and software (for example, Windows Server, Veritas, HP ServiceGuard, IBM HACMP, or Oracle Solaris Cluster) installation.
Universal Messaging administrator	Install Universal Messaging and high availability (HA) scripts.

Overview of Active/Passive Clustering on Windows

This section describes how to configure Universal Messaging with shared storage on Windows Server 2008 R2, Windows Server 2012 R2, and Windows Server 2016.

How Does Universal Messaging Run in a Windows Cluster?

In a Windows cluster environment, Universal Messaging runs as a service or as an application defined within a Windows cluster group. You use the Failover Cluster Manager to configure and monitor the Universal Messaging servers and all the associated resources. For more information about the settings in Failover Cluster Manager, see the Microsoft Windows Failover Cluster Manager manuals.

Active/Passive Cluster Configuration on Windows Server

Perform the following steps to configure Universal Messaging for high availability.

1. Mount and configure the shared drive, and add the shared drive to the cluster. For more information about adding and configuring a shared drive, see the Microsoft Server documentation for your Microsoft Server version.
2. Install Universal Messaging on the cluster nodes.

Use the same directory name on all cluster nodes. Ensure that the data directory paths for the shared storage and the log file are the same in all the installations (for example, C:\SoftwareAG_UM).

The data directory path in the `Server_Common.conf` configuration files must correctly refer to the same shared storage path. For example, the data directory path in all the nodes is specified as `wrapper.java.additional.4="-DDATADIR=H:\UMSharedStorage\Data"`.

The log file path in the `Server_Common.conf` configuration files must correctly refer to the same shared log directory path. For example, the log file path in all the nodes is specified as `wrapper.java.additional.22="-DLOGFILE=H:\UMSharedStorage\Data\nirvana.log"`.

If you are using the Software AG default internal user repository, ensure the user database file is located in the shared location. By default, the location is *Universal Messaging_directory*/common/conf/users.txt. The user database file is defined in the `jaas.conf` configuration file:

```
{com.softwareag.security.jaas.login.internal.InternalLoginModule sufficient
template_section=INTERNAL internalRepository="../../../../common/conf/users.txt";}
```

Note:

If you want to make changes that are automatically migrated in a future upgrade/migration, set the corresponding properties in the `Custom_Server_Common.conf` file as described in the section [“JVM Options” on page 199](#).

3. Create the Universal Messaging cluster in Windows Server. See the Microsoft Server documentation for instructions to create a failover cluster.
4. Create the Universal Messaging cluster group. Define all the resources and dependencies required to run Universal Messaging.
5. Configure Universal Messaging as a clustered service.

You can run Universal Messaging as a service or an application.

6. Customize the Universal Messaging startup behavior. For instructions to configure the startup behavior, see the relevant Microsoft Server documentation.

You can configure the number of possible attempts for starting the Universal Messaging server before failover.

7. Verify failover in the cluster using Windows Server tools.

You or a system administrator can verify failover when there is a hardware failure.

8. Ensure that the installation and configuration enables the Universal Messaging server to failover correctly from one cluster node to the other.

Overview of Active/Passive Clustering on UNIX

This section describes how to configure Universal Messaging with shared storage on UNIX.

Cluster Monitoring Scripts

The cluster control software determines the health of the servers by periodically probing the servers using the monitor scripts. When the cluster control software determines that one of the servers in the cluster has failed, it will shut down that server and start the server on the spare node.

You must incorporate the UNIX shell scripts for starting, stopping, and monitoring the servers in the cluster control software's infrastructure. You might have to customize code to enable the cluster control software to invoke these UNIX shell scripts.

Summary of Active/Passive Cluster Configuration on UNIX

This section is written primarily to a Universal Messaging administrator to gain a better understanding of the configuration process.

➤ To configure Universal Messaging in an active/passive cluster

1. Ask the cluster vendor's installation consultant to perform these tasks:
 - a. Install the HA cluster environment.
 - b. Configure the HA cluster environment including the shared disk storage.
2. Ask the system administrator to perform these tasks:
 - a. Administer the HA cluster environment so it is ready for software installation.
 - b. Configure the external network connection to the HA cluster and create the virtual host (virtual IP address) for the HA cluster.
3. Ask the cluster vendor's installation consultant and the system administrator to test the basic HA installation to ensure it functions properly.
4. Install and configure Universal Messaging on the cluster nodes with the help of the cluster vendor's installation consultant.

For information about how to install the cluster nodes and configure the cluster, see [“Configuring a Universal Messaging Active/Passive Cluster on UNIX” on page 323](#).

5. Verify that Universal Messaging runs on the cluster node. For instructions, see [“Verify the Universal Messaging Server Installation” on page 324](#).
6. Make sure the cluster is installed properly and configured. For information, see [“Verify Failover in the Cluster” on page 325](#).
7. Configure and test the scripts according to the cluster vendor’s specification for starting, stopping, and monitoring the Universal Messaging servers. For instructions, see [“Configure the Start, Stop, and Status Scripts” on page 324](#).
8. Verify failover in the cluster. For instructions, see [“Verify Failover in the Cluster” on page 325](#).

Configuring a Universal Messaging Active/Passive Cluster on UNIX

Install Universal Messaging on Cluster Nodes

When you install Universal Messaging on cluster nodes, you must:

- Follow the instructions in the *Using Software AG Installer* guide.
- Work with the cluster vendor’s installation consultant to prepare the cluster node to respond to the virtual IP address and have access to the storage files on the shared storage.

➤ To install Universal Messaging on cluster nodes

1. Install Universal Messaging on the first cluster node and configure to use the shared storage and log file.

Use the same directory name on all cluster nodes. Ensure that the data directory paths for the shared storage and the log file are the same in all the installations (for example, `opt/SoftwareAG_UM`).

The data directory path in the `Server_Common.conf` configuration files must correctly refer to the same shared storage path. For example, the data directory path in all the nodes is specified as `wrapper.java.additional.4="-DDATADIR=opt/UMSharedStorage/data"`.

The log file path in the `Server_Common.conf` configuration files must correctly refer to the same shared log directory path. For example, the log file path in all the nodes is specified as `wrapper.java.additional.22="-DLOGFILE=opt/UMSharedStorage/data/nirvana.log"`.

If you are using the Software AG default internal user repository, ensure the user database file is located in the shared location. By default, the location is *Universal Messaging_directory*/`common/conf/users.txt`. The user database file is defined in the `jaas.conf` configuration file:

```
{com.softwareag.security.jaas.login.internal.InternalLoginModule sufficient
template_section=INTERNAL internalRepository="../../../../common/conf/users.txt";}
```

Note:

If you want to make changes that are automatically migrated in a future upgrade/migration, set the corresponding properties in the `Custom_Server_Common.conf` file as described in the section [“JVM Options” on page 199](#).

2. Unmount the shared storage from cluster node 1 and mount it on cluster node 2.
3. Make the first cluster node inactive.
4. Install Universal Messaging on the second cluster node and configure it to use the shared storage and log file, following the configuration instructions for the first cluster.
5. Make the second cluster node active so that it will respond to the virtual IP address and have access to the storage files on the shared storage.

Verify the Universal Messaging Server Installation

Use the Universal Messaging Enterprise Manager to verify that the Universal Messaging server is properly installed and working.

➤ To verify that the servers are installed properly

1. Start the Enterprise Manager.
2. Connect to the servers that are part of the cluster.
3. Verify the status of the servers in the cluster.

Configure the Start, Stop, and Status Scripts

Incorporate the scripts of each cluster node into the cluster control software with the help of the cluster vendor’s installation consultant.

➤ To configure the start, stop, and status scripts of a server

1. Provide the location of the start and stop scripts to the cluster vendor consultant.

The scripts to start and stop a Universal Messaging server are located here:

- `Universal Messaging_directory /server/server_name/bin/nserver` to start the server.
- `Universal Messaging_directory /server/server_name/bin/nstopserver` to stop the server.

2. Implement a status script using the Universal Messaging API and provide the script to the cluster vendor consultant. For example, to return the server time stamp, you can use:
`Universal Messaging_directory /java/server_name/bin/ngetservertime.`

Important:

When you have basic authentication enabled on the server, you must configure the `UM_PASSWORD` or `PASS_PASSWORD_IN_CONSOLE` property before running the `ngetservertime` command. For more information about `UM_PASSWORD` and `PASS_PASSWORD_IN_CONSOLE`, see the section *Running the Java Sample Applications when Basic Authentication is Enabled* in the *Developer Guide*.

- a. Modify `env.sh` and change last command from “`$SHELL`” to “`$SHELL $*`”.
- b. Run this command to monitor the server status:

```
./env.sh -c "ngetservertime" | grep "Server Time"
```

Verify Failover in the Cluster

Test the entire cluster with an application to make sure that the cluster functions properly. With the help of the system administrator and the cluster vendor’s installation consultant, you can verify the cluster configuration and installation by causing a failover.

➤ To verify failover in a cluster

1. In the Enterprise Manager, provide the virtual IP address of the cluster to connect to the server and view the status.
2. Shut down the server on cluster node 1.
3. Start the server on cluster node 2 or let the cluster software start the server on cluster node 2.
4. Verify the status of the servers.

6 Command Line Administration Tools

■ Introduction to the Administration Tools	328
■ Starting the Tools using the Tools Runner Application	328
■ Performing Standard Administration Tasks on Realms and Clusters	330
■ Running a Configuration Health Check	337
■ The "Realm Information Collector" Diagnostic Tool	347
■ The ExportEventsFromOfflineMemFile Tool	355
■ The RepublishEventsFromOfflineFile Tool	361
■ The ServerReleaseVersion Tool	362
■ Syntax reference for command line tools	364

Introduction to the Administration Tools

Universal Messaging provides a set of command line tools that allow you to perform many of the common actions available through Universal Messaging. Examples of how to use the tools are also provided.

The tools can in general be grouped into the following categories:

Category	Description
General administration tasks	<p>This is a set of tools for performing many of the common administration actions available through Universal Messaging.</p> <p>For example, the <code>CreateChannel</code> tool allows you to create a channel on a specified realm, with a number of optional arguments - including TTL, ACLs, and many more - available through the parameters passed to the tool.</p>
Configuration health checker	<p>This tool allows you to check your configuration setup for either a single realm or for a cluster. The tool notifies you of any errors or inconsistencies in your setup.</p> <p>You can run the health check on a running system (realm or cluster). You can also run the health check offline on the basis of XML files containing the configuration of a realm or cluster (one XML configuration file per realm).</p>
Realm information collector	<p>This is a command-line diagnostic tool that gathers files and data from one or more Universal Messaging realm servers. The servers can be live or offline. The tool makes it easier for you to collect information that Software AG support may require to diagnose issues with Universal Messaging, but the information collected may also be useful for internal support within your organization.</p>

These tools are described in the following sections.

Starting the Tools using the Tools Runner Application

To run a tool, you start the *Tools Runner* application and pass the name of the required tool as a parameter to this application, as well as any additional parameters required by the tool.

The Tools Runner application is located in `<InstallDir>/UniversalMessaging/tools/runner`.

To start the Tools Runner application, use the appropriate command for Windows or Linux:

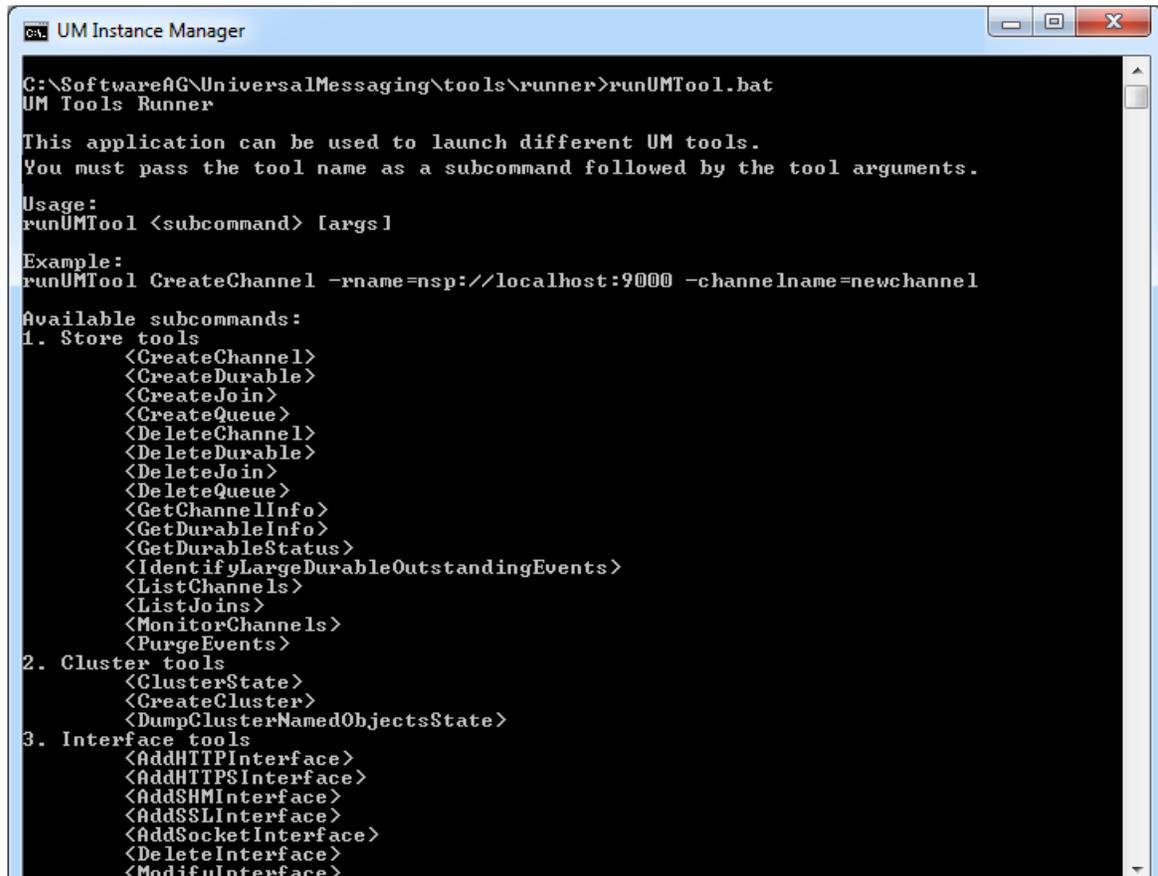
Windows:

```
runUMTool.bat
```

Linux:

```
runUMTool.sh
```

If you run Tools Runner with no arguments, this displays a list of installed tools, as well as instructions for using the Tools Runner, as shown in the following image.



```

C:\SoftwareAG\UniversalMessaging\tools\runner>runUMTool.bat
UM Tools Runner

This application can be used to launch different UM tools.
You must pass the tool name as a subcommand followed by the tool arguments.

Usage:
runUMTool <subcommand> [args]

Example:
runUMTool CreateChannel -rname=nsp://localhost:9000 -channelname=newchannel

Available subcommands:
1. Store tools
   <CreateChannel>
   <CreateDurable>
   <CreateJoin>
   <CreateQueue>
   <DeleteChannel>
   <DeleteDurable>
   <DeleteJoin>
   <DeleteQueue>
   <GetChannelInfo>
   <GetDurableInfo>
   <GetDurableStatus>
   <IdentifyLargeDurableOutstandingEvents>
   <ListChannels>
   <ListJoins>
   <MonitorChannels>
   <PurgeEvents>
2. Cluster tools
   <ClusterState>
   <CreateCluster>
   <DumpClusterNamedObjectsState>
3. Interface tools
   <AddHTTPInterface>
   <AddHTTPSInterface>
   <AddSHMInterface>
   <AddSSLInterface>
   <AddSocketInterface>
   <DeleteInterface>
   <ModifyInterface>

```

Running a Tool

To run a specific tool, you pass the name of the tool as the first argument to the Tools Runner application. Doing so without any additional arguments will print the usage for the specific tool. For example, running

```
runUMTool.bat CreateChannel
```

will print the usage for the `CreateChannel` tool. The usage contains a description of the tool, and a list of the required and optional arguments that you can supply. Arguments which have a specific set of legal values will have these values displayed here. Also included in the usage are command line examples of running the tool.

To run a tool with additional arguments, each of the required arguments must be specified in the command. For example, the `CreateChannel` tool requires both a realm name and channel name to be specified:

```
runUMTool.bat CreateChannel -rname=nsp://localhost:9000 -channelname=channel
```

Additional optional arguments can be appended to the command in the same way; adding a channel type to the `CreateChannel` tool command would then be:

```
runUMTool.bat CreateChannel -rname=nsp://localhost:9000 -channelname=channel
-type=R
```

Using the Debug Logging option

You can use the optional `enableDebug` argument on the command line to create a log file that shows the progress of the tool while it is running. It will log most of the exceptions that can occur during the tool execution. For example:

```
runUMTool.bat DumpACL -rname=nhp://localhost:11000 -enableDebug
```

The log file is called `toolsLog.log` and is located in the same directory as the Tools Runner application.

Performing Standard Administration Tasks on Realms and Clusters

Using the Tools Runner application, you can launch command line tools for performing standard administration tasks on realms and clusters.

Tools are available to perform tasks such as:

- Creating, deleting and monitoring channels and queues
- Creating and deleting clusters
- Adding, modifying and deleting interfaces (HTTP, HTTPS, SSL, Sockets)
- Adding and deleting ACL entries for channels, queues and realms

For example, the `CreateChannel` tool allows you to create a channel on a specified realm, with a number of optional arguments - including TTL, ACLs, and many more - available through the parameters passed to the tool.

To see the complete set of administration tools available, start the `Tools Runner` application without any parameters, as described in the section [“Starting the Tools using the Tools Runner Application” on page 328](#).

The following table lists the available tools. The tools are organized into categories, according to the general purpose for which the tools are used.

Tool name / Category	Description
Category: Store tools	For the command line syntax of the tools in this category, see the section “Syntax: Store Tools” on page 364 .

Tool name / Category	Description
CreateChannel	Creates a channel with the specified name on the specified server. A single permission can be set during channel creation using optional arguments. For adding a set of permissions use the client API.
CreateDurable	Creates a Durable with the specified name and type on the specified channel.
CreateJoin	Joins two channels.
CreateQueue	Creates a queue with the specified name on the specified server. A single permission can be set during queue creation using optional arguments. For adding a set of permissions use the client API.
DeleteChannel	Deletes a channel with the specified name on the specified session.
DeleteDurable	Deletes a Durable with the specified name on the specified channel.
DeleteJoin	Deletes a join between two channels.
DeleteQueue	Deletes a queue with the specified name on the specified session.
GetChannelInfo	Gets the attributes and storage properties of a specified channel in a specified realm.
GetDurablesInfo	Displays the durables details saved in a .nsb file.
GetDurableInfo	Gets the attributes of a specific Durable in a specific channel.
GetDurableStatus	Gets the current state of durables on a realm, sorted by a given field.
IdentifyLargeDurableOutstandingEvents	Identifies channels containing Durables with a large number of outstanding events.
ListChannels	Lists details of the channels on the specified server.
ListJoins	Lists joins on a given realm.
MonitorChannels	Monitors the channels and queues in a realm and prints totals.
PurgeEvents	Purges events from a channel with the specified name on the specified session.

Tool name / Category	Description
Category: Cluster tools	For the command line syntax of the tools in this category, see the section “Syntax: Cluster Tools” on page 377.
ClusterState	Checks the cluster state by a given RNAME, which is part of a cluster.
CreateCluster	Creates a cluster with the specified name, consisting of the specified realms.
DeleteCluster	Deletes the cluster that has the specified cluster name and that contains a server with the given RNAME.
DumpClusterNamedObjectsState	Dumps the state of named objects (durables) on channels present on the specified cluster servers.
Category: Interface tools	For the command line syntax of the tools in this category, see the section “Syntax: Interface Tools” on page 379.
AddHTTPInterface	Adds an HTTP interface on the specified adapter and port, on the specified realm.
AddHTTPSInterface	Adds an HTTPS interface on the specified adapter and port, on the specified realm.
AddSHMInterface	Adds a shared memory interface with the specified path, buffer size and timeout, on the specified realm.
AddSSLInterface	Adds an SSL interface on the specified adapter and port, on the specified realm.
AddSocketInterface	Adds a socket interface on the specified adapter and port, on the specified realm.
DeleteInterface	Deletes the specified interface from the specified realm.
ListInterfaces	Lists details of the interfaces on the specified realm.
ModifyInterface	Modifies the specified interface on the specified realm.
Category: Data group tools	For the command line syntax of the tools in this category, see the section “Syntax: Data Group Tools” on page 388.
AddDataGroup	Adds a child data group to a parent data group. Both of these data groups must exist.
CreateDataGroup	Creates a data group with the specified name on the specified server. Additionally, conflation attributes and other options of the data group can be set.

Tool name / Category	Description
DeleteDataGroup	Removes the data group with the specified name from the server.
ListenDataGroup	Listens for data group events on a realm.
PublishDataGroup	Publishes messages to a data group.
Category: Publish tools	For the command line syntax of the tools in this category, see the section "Syntax: Publish Tools" on page 391.
PublishChannel	Publishes events to a channel.
PublishCompressed	Publishes events to a store, using compression.
PublishQueue	Publishes events to a queue.
PublishTX	Publishes events, as a part of a transaction, to a channel or queue.
Category: Subscribe tools	For the command line syntax of the tools in this category, see the section "Syntax: Subscribe Tools" on page 394.
PeekQueue	Peeks all events on a queue and prints statistics for the bandwidth rates.
SubscribeChannel	Reads all the messages from a channel.
SubscribeChannelAsync	Listens for messages on a channel.
SubscribeChannelAsyncDurable	Listens for messages on a channel. Running the tool with the same "-name" argument will continue reading from the last unconsumed event.
SubscribeChannelDurable	Listens for messages on a channel. Running the tool with the same "-name" argument will continue reading from the last unconsumed event.
SubscribeCompressed	Listens for compressed messages on a channel.
SubscribeQueue	Reads all the messages from a queue.
SubscribeQueueAsync	Listens for messages on a queue.
Category: Security tools	For the command line syntax of the tools in this category, see the section "Syntax: Security Tools" on page 399.
AddChannelACLEntry	Adds an ACL entry on the specified channel for the specified user and host, on the specified session.

Tool name / Category	Description
AddContainerACLEntry	Adds an ACL entry on the specified container for the specified user and host.
AddQueueACLEntry	Adds an ACL entry on the specified queue for the specified user and host, on the specified session.
AddRealmACLEntry	Adds an ACL entry on the specified realm for the specified user and host.
AddSecurityGroup	Adds a security group to the specified realm with the specified name.
AddUserToSecurityGroup	Adds a specified user and host subject to a given security group on a specified realm.
DeleteChannelACLEntry	Deletes the ACL entry from the specified channel with the specified user and host.
DeleteContainerACLEntry	Removes an ACL entry from the specified container with the specified user and host.
DeleteQueueACLEntry	Deletes an ACL entry from the specified queue with the specified user and host.
DeleteRealmACLEntry	Removes an ACL entry from the specified realm with the specified user and host.
DeleteSecurityGroup	Removes a security group from the specified realm with the specified name.
DumpACL	Dumps all the ACL data for a realm.
ModifyChannelACLEntry	Updates an ACL entry on the specified channel for the specified user and host, on the specified session.
ModifyContainerACLEntry	AddContainerACLEntry adds an ACL entry on the specified container for the specified user and host.
ModifyQueueACLEntry	Updates an ACL entry on the specified queue for the specified user and host, on the specified session.
ModifyRealmACLEntry	Modifies an ACL entry on the specified realm for the specified user and host.
RemoveUserFromSecurityGroup	Removes a specified user from a given security group on the specified realm.
Category: Zone tools	For the command line syntax of the tools in this category, see the section “Syntax: Zone Tools” on page 412.

Tool name / Category	Description
AddMemberToZone	Adds a realm to a specified realm's zone.
CreateZone	Creates a zone with the specified name containing the specified realms.
DeleteZone	Deletes a zone with the specified name on the specified session.
RemoveMemberFromZone	Removes a realm from its current zone.
Category: JMS tools	For the command line syntax of the tools in this category, see the section “Syntax: JMS Tools” on page 414.
CreateConnectionFactory	Creates a JMS connection factory with the specified server.
CreateJMSQueue	Creates a JMS queue with the specified name on the specified session.
CreateJMSTopic	Creates a JMS topic with the specified name on the specified session.
JMSPublish	Publishes one or more messages to a JMS queue or topic.
JMSSubscribe	Reads messages arriving to a JMS destination.
ModifyConnectionFactory	Modifies settings of a JMS connection factory on the specified server.
ViewConnectionFactory	Views settings of a JMS connection factory on the specified server.
Category: Recovery tools	For the command line syntax of the tools in this category, see the section “Syntax: Recovery Tools” on page 423.
AddInterfaceOffline	Adds a new interface to an offline realm.
DeleteInterfaceOffline	Removes an interface from an offline realm using configuration data.
DumpInterfacesOffline	Dumps the list of interfaces for a specified offline realm.
ExportEventsFromOfflineMemFile	Dumps events from the specified offline .mem file to an XML or JSON file. Events can be filtered in several ways when dumping. For more details, see the section “The ExportEventsFromOfflineMemFile Tool” on page 355 .
ModifyInterfaceOffline	Modifies an interface of an offline realm.

Tool name / Category	Description
ModifyPrimeFlagOffline	Modifies the prime flag of a site while the realm is offline.
RepublishEventsFromOfflineFile	Imports events from an XML, JSON or .mem file, optionally using a filter and protocol buffered descriptor file set, and republishes it to the specified store. For more details, see the section “The RepublishEventsFromOfflineFile Tool” on page 361.
Category: Durable tools	For the command line syntax of the tools in this category, see the section “Syntax: Durable Tools” on page 428.
ViewDurableEvent	Gets all events for all durables or all events for a specific durable.
Category: Miscellaneous	For the command line syntax of the tools in this category, see the section “Syntax: Miscellaneous Tools” on page 429.
EditRealmConfiguration	Edits realm configuration parameters.
ExportRealmXML	Exports a selected realm to an XML file.
HealthChecker	Runs the Health Checker tool for analysing configuration items and highlighting robustness improvements. For more details, see the section “Running a Configuration Health Check” on page 337.
ImportRealmXML	Imports a realm from an XML file.
Category: Site tools	For the command line syntax of the tools in this category, see the section “Syntax: Site Tools” on page 435.
CreateSite	Creates a site with the specified name, consisting of the specified nodes.
DeleteSite	Deletes a site with the specified name from all the nodes associated with it.
SetPrimeSite	Toggles the specified site's prime status.
ShowSites	Displays the configuration of the sites.
Category: Diagnostic tools	For the command line syntax of the tools in this category, see the section “Syntax: Diagnostic Tools” on page 437.

Tool name / Category	Description
RealmInformationCollector	<p>Collects diagnostic information from a realm server installation and stores it in a zip archive.</p> <p>For more details, see the section “The "Realm Information Collector" Diagnostic Tool” on page 347.</p>

Running a Configuration Health Check

Overview

The HealthChecker is a tool for checking the correctness of a realm or cluster configuration.

The tool is primarily intended for use by Software AG support staff for analyzing possible problems in customer configurations, but you might also find it useful for checking your configuration.

The tool can be used in the following ways:

- To check the configuration of a live realm (which can be a single entity or a node of a cluster) or a cluster. If the realm is a node of the cluster, the checks will also be automatically executed against all the other cluster members.
- To do an offline check of the configuration of a realm or cluster, based on configuration information that has been exported to XML files. Each such XML file contains the configuration data of a realm, regarding channels, queues, durables, datagroups, etc. The tool will only run the checks against all the cluster members if their XML paths are given explicitly in the call of the tool.

Typical configuration aspects that can be checked in a clustered realm are:

- **Datagroups:**

Datagroups belonging to a cluster must be present on all nodes of the cluster and their attributes must be the same.

- **Durables:**

Durables belonging to clusterwide channels should also be clusterwide. They must be present on all nodes of the cluster and their attributes must be the same.

- **Joins:**

Joins between clusterwide channels must be present on all nodes of the cluster and their attributes have to be the same.

- **Stores:**

Stores belonging to a cluster must be present on all nodes of the cluster and their attributes and properties must be the same.

Typical configuration aspects that can be checked in a non-clustered realm are:

- **Durables:**

Durables belonging to a non-clustered realm must be non-clusterwide and must be attached to a non-clusterwide channel.

- **Stores:**

Some store configurations may impact the performance of the system and they need to be highlighted.

Checks against a live realm

The checks that can be run against a live realm are the following:

Name of Check	Description	Default check?
DataGroupMismatchCheck	Check if datagroups are coherent across all nodes of the cluster.	
DurableMismatchCheck	Check if durables are coherent across all nodes of the cluster.	Y
DurableSubscriberLargeStoreCheck	Check the number of remaining events to be consumed in a shared durable. If the number is greater than the threshold a warning will be displayed. The default value for the threshold is 1000. This check takes an additional parameter <code>-threshold</code> that allows you to specify a custom value for the threshold.	Y
DurableWarningCheck	Check durable which has no JMSEngine and no active consumer.	Y
EnvironmentStateCheck	Check and display the status of a running environment. The HealthChecker first checks if the server configuration property <code>Enable Flow Control</code> in the configuration group <code>Server Protection</code> (see the note after this table) is set to true. If it is set to true then the HealthChecker will check what percentage of memory is taken by events from the whole heap memory. If the percentage exceeds a certain value, an appropriate log message will be displayed (see details below). The general idea is that the Server Protection mechanism gradually slows the consumption of	Y

Name of Check	Description	Default check?
	<p>events from clients when certain thresholds are reached.</p> <p>The degree of slowing down is marked by these three server configuration properties: <code>FlowControlWaitTimeOne</code>, <code>FlowControlWaitTimeTwo</code> and <code>FlowControlWaitTimeThree</code>. These represent a period of time, measured in milliseconds, by which client publishing requests will be delayed when the corresponding threshold has been reached.</p> <p>Threshold 70%-80%: A log message is displayed that client publishing requests will be delayed by <code>FlowControlWaitTimeOne</code> milliseconds.</p> <p>Threshold 80%-90%: A log message is displayed that client publishing requests will be delayed by <code>FlowControlWaitTimeTwo</code> milliseconds.</p> <p>Threshold 90%-94%: A log message is displayed that client publishing requests will be delayed by <code>FlowControlWaitTimeThree</code> milliseconds.</p> <p>Threshold higher than 94%: A log message is displayed that client publishing requests will be delayed by a long duration (24 days).</p> <p>See the section <i>Out-of-Memory Protection</i> in the <i>Concepts</i> guide for further details.</p>	
FixLevelCheck	Check if all nodes of a cluster are on the same fix level. It is strongly recommended they are.	Y
JNDIStatusCheck	Check JNDI status and mismatches for stores.	Y
JoinLastEIDMismatchCheck	Check for joins that are ahead of the channel's last EID. You can use this check both on standalone and cluster UM servers.	Y
JoinMismatchCheck	Check if joins are coherent across all nodes of the cluster.	Y
JoinSyncWarningCheck	Check if join is out of sync on the cluster.	Y
RealmACLCheck	Check the realm ACL access control list.	
RealmConfigurationChecks	Check the realm configuration with default configuration list.	Y

Name of Check	Description	Default check?
ResourcesSafetyLimitsCheck	Check that channel/queue resources have either TTL or Capacity configured to a non-zero value. If both of these values are zero, this means that the channel/queue is not configured with any safety limits.	
ServerProtectionConsistencyCheck	Check if the server configuration properties in the configuration group <code>Server Protection</code> group (see the note after this table) are coherent across the nodes of a cluster against a running environment.	
StoreACLCheck	Check store ACL warnings.	
StoreMemoryCheck	Check the memory usage of stores.	Y
StoreMismatchCheck	Check if stores are coherent across all nodes of the cluster.	Y
StoreWarningsCheck	Check store warnings on the specified realm.	Y

A "Y" in the column "Default check?" indicates that the check is included in the `-mode=default` setting (see the topic *The -mode parameter* below).

Important:

When the tool checks for outstanding durable events or event ID mismatches in a **live** environment, there is a chance of getting warning messages, even though the cluster is working correctly. This is because the check is not atomic for the live cluster, so a small synchronization discrepancy can be expected.

Note:

For further information about the server configuration parameters and the configuration group `Server Protection` mentioned in the table above, see the section [“Realm Configuration” on page 35](#).

Checks against a realm's stored XML configuration

The checks that can be run against a stored XML configuration are the following:

Name of Check	Description	Default check?
DataGroupMismatchCheck	Check if datagroups are coherent across all the nodes of the cluster.	
DurableMismatchCheck	Check if durables are coherent across all nodes of the cluster.	Y

Name of Check	Description	Default check?
FixLevelCheck	Check if all nodes of a cluster are on the same fix level. It is strongly recommended they are.	Y
JNDIStatusCheck	Check JNDI status and mismatches for stores on all the nodes of the cluster.	Y
JoinMismatchCheck	Check if joins are coherent across all nodes of the cluster.	Y
RealmACLCheck	Check realm ACL warnings.	
RealmConfigurationCheck	Check realm configuration property warnings.	Y
ResourcesSafetyLimitsCheck	Check that channel/queue resources have either TTL or Capacity (maximum number of events) configured to a non-zero value. If both of these values are zero, this means that the channel/queue is not configured with any safety limits.	
ServerProtectionConsistencyCheck	Check if the server configuration properties in the configuration group <code>Server Protection</code> are coherent across the nodes of a cluster against the exported configurations from the nodes.	
StoreACLCheck	Check store ACL security checks.	
StoreMismatchCheck	Check if stores are coherent across all nodes of the cluster.	Y
StoreWarningsCheck	Check store warnings on the specified realm.	Y

Command Usage

Displaying help text

To display a help text showing a summary of the command usage, call the HealthChecker without parameters:

```
runUMTool HealthChecker
```

Command Syntax

The HealthChecker requires either the `-rname` parameter, which offers checks against a live realm, or the `-xml` parameter, which offers checks against a realm's stored XML configuration. Note that you cannot use these two parameters in the same invocation of the HealthChecker.

The syntax is as follows:

```
runUMTool HealthChecker {-rname=<rname> | -xml=/path/to/xml1,...}
  [-check=<checktype>[,<checktype> ...] ]
  [-mode=<modetype>]
  [-include=<checktype>[,<checktype> ...] ]
  [-exclude=<checktype>[,<checktype> ...] ]
  [-<additionalParameter1>=<value>] [-<additionalParameter2>=<value>] ...
```

Running a health check of a running realm

```
runUMTool HealthChecker -rname=nsp://localhost:11000
```

This will run the HealthChecker tool against the given running realm.

Running a health check of a stored realm configuration

```
runUMTool HealthChecker -xml=/path/to/xml1.xml, /path/to/xml2.xml
```

This will run the HealthChecker tool against the realm configurations stored in the given XML files.

The **-check** parameter

This parameter allows you to explicitly specify the check or checks that you want to be executed. No other checks will be included. This parameter can only be used together with the `-rname` or `-xml` parameter; the other additional parameters have no meaning in the context of `-check` so they can't be used.

Example - Execute only the Store Warnings Check check against the running realm:

```
runUMTool HealthChecker -rname=nsp://localhost:11000
  -check=StoreWarningsCheck
```

Example - Execute only the Store Warnings Check and Fix Level Check checks against the running realm:

```
runUMTool HealthChecker -rname=nsp://localhost:11000
  -check=StoreWarningsCheck, FixLevelCheck
```

The **-mode** parameter

This parameter allows you to select a predefined set of checks without having to name the checks explicitly. The `-mode` and `-check` parameters are mutually exclusive.

The mode parameter can take one of the following values:

- **default** - this value selects the recommended minimal subset of checks. This is the default option.
- **all** - this mode selects all checks.

You can use the `-include` and `-exclude` parameters to modify the set of checks selected by the `-mode` parameter.

If neither `-mode` nor `-check` is specified, the default set of checks will be executed.

The **-include** and **-exclude** parameters

You can use the `-include` and `-exclude` parameters to further refine the set of checks that have been selected by the `-mode` parameter. You can use `-include` and `-exclude` in the same call of the health checker, as long as they do not specify the same check.

- **include** - Run all checks from the set defined by the `-mode` parameter, and additionally include the check or checks specified by this parameter. The parameter may contain a single check or a comma-separated list of checks.
- **exclude** - Run all checks from the set defined by the `-mode` parameter, except the specified check or checks. The parameter may contain a single check or a comma-separated list of checks.

The `-<additionalParameter>` parameters

Some of the health checks allow you to specify one or more additional parameters when calling the HealthChecker. The name and purpose of each additional parameter is specific to the individual health check being run.

For example, the `DurableSubscriberLargeStoreCheck` check allows you to specify the additional parameter `-threshold=<value>`, which defines a threshold for the number of remaining events to be consumed in a shared durable.

The following general rules apply:

- Each additional parameter has a default value, so if you do not specify the additional parameters explicitly, the default values will be taken.
- If multiple additional parameters and multiple checks are specified, each individual check uses only its own additional parameters.
- The additional parameters can be given in any order.
- Checks that do not require additional parameters will ignore the additional parameters.

Syntax Examples

Example - Execute all available checks for a live realm check:

```
runUMTool HealthChecker -rname=nsp://localhost:11000 -mode=all
```

Example - Execute all the available checks for a live realm check, except the ones mentioned.

```
runUMTool HealthChecker -rname=nsp://localhost:11000
    -mode=all -exclude=JNDIStatusCheck, FixLevelCheck, JoinMismatchCheck
```

Example - Execute the default set of checks for a live realm check, adding the `StoreWarningsCheck` which is not part of the default set.

```
runUMTool HealthChecker -rname=nsp://localhost:11000
    -mode=default -include= StoreWarningsCheck
```

Example - Execute the default set of checks for a live realm check, but excluding the `JNDIStatusCheck`, `FixLevelCheck` and adding the `StoreWarningsCheck`.

```
runUMTool HealthChecker -rname=nsp://localhost:11000
    -mode=default -include= StoreWarningsCheck
```

```
-exclude=JNDIStatusCheck, FixLevelCheck
```

Note:

The previous examples are based on live checks using the `-rname` parameter. The same logic applies if you use the `-xml` parameter instead.

Full Example

The following example compares the XML configuration files of two realms in a cluster. The realms are named `realm0` and `realm1`, and their configuration files are named `clustered_realm0.xml` and `clustered_realm1.xml`.

XML configuration file `clustered_realm0.xml` for `realm0`:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<NirvanaRealm name="realm0" exportDate="2016-11-08Z"
  comment="Realm configuration from realm0" version="BuildIdentifier"
  buildInfo="BuildIdentifier">
  <ClusterSet>
    <ClusterEntry name="cluster1">
      <ClusterMember name="realm1" rname="nsp://localhost:11010/"
        canBeMaster="true"/>
      <ClusterMember name="realm0" rname="nsp://localhost:11000/"
        canBeMaster="true"/>
    </ClusterEntry>
  </ClusterSet>
  <ChannelSet>
    <ChannelEntry>
      <ChannelAttributesEntry name="channel1" TTL="0" capacity="5" EID="0"
        clusterWide="true" jmsEngine="false" mergeEngine="false"
        type="PERSISTENT_TYPE"/>
      <StorePropertiesEntry HonorCapacityWhenFull="false"
        SyncOnEachWrite="false" SyncMaxBatchSize="0" SyncBatchTime="0"
        PerformAutomaticMaintenance="false" EnableCaching="true"
        CacheOnReload="true" EnableReadBuffering="true"
        ReadBufferSize="10240" Priority="4" EnableMulticast="false"
        StampDictionary="0" MultiFileEventsPerSpindle="50000"/>
      <ChannelJoinSet>
        <ChannelJoinEntry filter="" hopcount="50" to="channel2"
          from="channel1" allowPurge="false" archival="false"/>
      </ChannelJoinSet>
    </ChannelEntry>
    <ChannelEntry>
      <ChannelAttributesEntry name="channel2" TTL="0" capacity="0" EID="0"
        clusterWide="true" jmsEngine="false" mergeEngine="false"
        type="RELIABLE_TYPE"/>
      <StorePropertiesEntry HonorCapacityWhenFull="false"
        SyncOnEachWrite="false"
        SyncMaxBatchSize="0" SyncBatchTime="0"
        PerformAutomaticMaintenance="false"
        EnableCaching="true" CacheOnReload="true"
        EnableReadBuffering="true"
        ReadBufferSize="10240" Priority="4" EnableMulticast="false"
        StampDictionary="0" MultiFileEventsPerSpindle="50000"/>
      <DurableSet>
        <durableEntry name="durable1" EID="-1" outstandingEvents="0">
```

```

        clusterWide="true" persistent="true"
        priorityEnabled="false" shared="true"/>
    </DurableSet>
</ChannelEntry>
</ChannelSet>
<QueueSet>
    <QueueEntry>
        <ChannelAttributesEntry name="queue1" TTL="0" capacity="0" EID="0"
            clusterWide="true" jmsEngine="false" mergeEngine="false"
            type="RELIABLE_TYPE"/>
        <StorePropertiesEntry HonorCapacityWhenFull="false"
            SyncOnEachWrite="false" SyncMaxBatchSize="0" SyncBatchTime="0"
            PerformAutomaticMaintenance="true" EnableCaching="true"
            CacheOnReload="true" EnableReadBuffering="true"
            ReadBufferSize="10240" Priority="4" EnableMulticast="false"
            StampDictionary="0" MultiFileEventsPerSpindle="50000"/>
    </QueueEntry>
</QueueSet>
</NirvanaRealm>

```

XML configuration file clustered_realm1.xml for realm1:

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<NirvanaRealm name="realm1" exportDate="2016-11-16Z"
    comment="Realm configuration from realm1"
    version="BuildIdentifier" buildInfo="BuildIdentifier">
    <ClusterSet>
        <ClusterEntry name="cluster1">
            <ClusterMember name="realm1" rname="nsp://localhost:11010/"
                canBeMaster="true"/>
            <ClusterMember name="realm0" rname="nsp://localhost:11000/"
                canBeMaster="true"/>
        </ClusterEntry>
    </ClusterSet>
    <ChannelSet>
        <ChannelEntry>
            <ChannelAttributesEntry name="channel1" TTL="0" capacity="5" EID="0"
                clusterWide="true" jmsEngine="false" mergeEngine="false"
                type="RELIABLE_TYPE"/>
            <StorePropertiesEntry HonorCapacityWhenFull="false"
                SyncOnEachWrite="false" SyncMaxBatchSize="0" SyncBatchTime="0"
                PerformAutomaticMaintenance="false" EnableCaching="true"
                CacheOnReload="true" EnableReadBuffering="true"
                ReadBufferSize="10240" Priority="4" EnableMulticast="false"
                StampDictionary="0" MultiFileEventsPerSpindle="50000"/>
            <ChannelJoinSet>
                <ChannelJoinEntry filter="" hopcount="10" to="channel2"
                    from="channel1" allowPurge="false" archival="false"/>
            </ChannelJoinSet>
        </ChannelEntry>
        <ChannelEntry>
            <ChannelAttributesEntry name="channel2" TTL="0" capacity="0" EID="0"
                clusterWide="true" jmsEngine="false" mergeEngine="false"
                type="RELIABLE_TYPE"/>
            <StorePropertiesEntry HonorCapacityWhenFull="false"
                SyncOnEachWrite="false" SyncMaxBatchSize="0" SyncBatchTime="0"
                PerformAutomaticMaintenance="false" EnableCaching="true"
                CacheOnReload="true" EnableReadBuffering="true"
                ReadBufferSize="10240" Priority="4" EnableMulticast="false"

```

```

        StampDictionary="0" MultiFileEventsPerSpindle="50000"/>
    </ChannelEntry>
</ChannelSet>
<DataGroupSet>
    <DataGroupEntry>
        <DataGroupAttributesEntry name="dg1" id="3422373812" priority="1"
            multicasterenabled="false"/>
    </DataGroupEntry>
</DataGroupSet>
</NirvanaRealm>

```

From a first analysis we can say that these two realms belong to the same cluster (cluster1) and that they both contain various stores, joins and data groups. But let's see what happens when we run the HealthChecker tool specifying both XML files and running all the checks. Note that we need to exclude the ServerProtectionConsistencyCheck since the specified XML files do not contain the RealmConfiguration section.

Here is the call of the tool (using Windows syntax) and the result:

```

runUMTool.bat HealthChecker -xml=clustered_realm0.xml,clustered_realm1.xml
                    -exclude=ServerProtectionConsistencyCheck
HealthChecker Tool - Version: 1.0

XML JOIN MISMATCHES CHECK
ERROR: Join from (channel1) to (channel2) HopCount mismatch [realm1] does not
       equal [realm0]

XML JNDI PROPERTIES CHECK
WARN: Realm realm0: No JNDI entry for store channel1
WARN: Realm realm0: No JNDI entry for store channel2
WARN: Realm realm0: No JNDI entry for store queue1
WARN: Realm realm1: No JNDI entry for store channel1
WARN: Realm realm1: No JNDI entry for store channel2

XML DURABLE STATUS CHECK
ERROR: Could not find durable (durable1) on realm [realm1] but it is present
       on [realm0]

XML STORE MISMATCHES CHECK
WARN: Store (channel1) Type mismatch [realm1] does not equal [realm0]
ERROR: Could not find store (queue1) on realm [realm1] but it is present
       on realm [realm0]

XML DATAGROUP MISMATCHES CHECK
ERROR: Could not find Data Group (dg1) on realm [realm0] but it is present
       on realm [realm1]

```

These errors and warnings tell us:

- Joins: a join between two clusterwide channels has to be the same on all the nodes - in our case there is a mismatch in the HopCount;

- JNDIs: these simple warnings are saying: "Are you sure that you don't need any JNDI for these stores?";
- Durables: if a durable is clusterwide, then it has to be present on all the other nodes (and it has to be the same);
- Stores: if a store is clusterwide, then it has to be the same on all the other nodes.
- Datagroups: the same rule applies for datagroups, which are always clusterwide and have to be present on all the other nodes.

The "Realm Information Collector" Diagnostic Tool

Overview

`RealmInformationCollector` is a command-line diagnostic tool that gathers files and live data from one or more Universal Messaging realm servers. The tool makes it easier for you to collect information that Software AG support may require to diagnose issues with Universal Messaging, but the information collected may also be useful for internal support within your organization.

The tool can be executed in live and offline mode:

- **Live mode:** In live mode, the specified Universal Messaging realm server(s) must be running. The tool will collect files that contain operational data for each running realm server, but will also attempt to connect to and gather information directly from each running server process.
- **Offline mode:** In offline mode, the specified Universal Messaging realm server(s) must be offline.

In this mode, the tool will only collect files that contain operational data for each realm server.

The mode of operation (either offline or live) is a mandatory argument and must be specified when running the tool. You must ensure that the specified Universal Messaging realm servers are stopped when `-mode=offline`, or running when `-mode=live`.

Depending on the mode, the tool will collect different files. For example, in live mode, it will not collect the content of realm server's "data" directory, because this might cause failures on the server.

The tool collects information by executing a list of *collectors*. Each collector is responsible for gathering a specific subset of the realm's information.

Collectors for a live realm server

The collectors that can be run against a live realm server are shown in the following table. Path names of files and directories given in the table are the installation defaults.

Name of Collector	Description	Default collector?
clientinfo	Collects client connection information from a running realm server.	
consumerinfo	Collects consumer connection information from a running realm server.	
env	Collects environment information from a running realm server. Y This includes all JVM system properties and the list of Universal Messaging interfaces.	
healthchecker	Acquires health information from a running realm server using the HealthChecker tool. See the section “Running a Configuration Health Check” on page 337 for details.	Y
heapdump	Acquires a heap dump from a running realm server. Note: This collector is not available on all platforms. See the section <i>Operational Issues</i> below for related information.	
heapdumps	Collects the heap dump directory of a realm server. The location of this directory is <InstallDir>/UniversalMessaging/server/<realmname>/heap_dumps. See the section <i>The Dump file for Out-of-Memory Errors (OOM)</i> in the <i>Installation Guide</i> for related information about heap dumps.	
installlogs	Collects the product's installation log files. These files are located in <InstallDir>/install/logs.	Y
instancemgr	Collects the realm server's manager log. This file is located in <InstallDir>/UniversalMessaging/tools/InstanceManager/instanceLog.txt.	Y
jaas	Collects the JAAS configuration of a realm server. This file is located in <InstallDir>/UniversalMessaging/server/<realmname>/bin/jaas.conf.	Y
license	Collects the license file of a realm server. This file is located in <InstallDir>/UniversalMessaging/server/<realmname>/licence.xml.	
logs	Collects logs of a realm server.	Y

Name of Collector	Description	Default collector?
	<p>The location of the file is <code><InstallDir>/UniversalMessaging/server/<realmname>/data/nirvana.log</code> If there are any rolled log files in addition to the current log file, for example <code>nirvana.log_<timestamp1></code> and <code>nirvana.log_<timestamp2></code>, these are collected also.</p> <p>Additionally, it collects logs created by the trace logger, if present. The location of the trace logging directory is <code><InstallDir>/UniversalMessaging/server/<realmname>/data/traceLogging</code> by default. If this directory is changed via the <code>com.softwareag.um.server.log.TraceLoggerPath</code> system property, this will also be taken into account when the Realm Information Collector is executed and the log files will be collected.</p>	
migrationlogs	Collects Software AG migration logs.	
osinfo	<p>Collects operating system and hardware information. The collector will gather hardware, processor, memory, file system, and network information from the operating system. The data will be stored in the file generated/osinfo.txt in the generated archive.</p> <p>The <code>osinfo</code> tool runs on Windows, Apple macOS, Red Hat Enterprise Linux, and Solaris operating systems.</p>	Y
plugins	<p>Collects the <code>plugins</code> directory of a realm server.</p> <p>This directory is located at <code><InstallDir>/UniversalMessaging/server/<realmname>/plugins</code>.</p>	Y
psinfo	<p>Collects information about processes in the operating system. The collector records the top 20 processes in terms of CPU consumption and stores the data in the generated/osinfo.txt file in the generated archive.</p> <p>The <code>psinfo</code> collector runs together with the <code>osinfo</code> collector, which is selected by default. If you try to run <code>psinfo</code> without <code>osinfo</code>, the system returns an error.</p> <p>The <code>psinfo</code> tool runs on Windows, Apple macOS, Red Hat Enterprise Linux, and Solaris operating systems.</p>	Y
realmconfig	<p>Collects the realm configuration properties of a realm server. The properties are listed in the section “Realm Configuration” on page 35. The collector delivers the configuration properties as a serialized XML file.</p>	Y
secfile	Collects the security file of a realm server.	Y

Name of Collector	Description	Default collector?
	This file is located at <InstallDir>/UniversalMessaging/server/<realmname>/bin/secfile.conf.	
spmlogs	Collects SoftwareAG spm logs.	
tanukiconf	Collects the Tanuki service wrapper configuration of a realm server. This includes the files nserverdaemon.conf, Server_Common.conf and Custom_Server_Common.conf, located at <InstallDir>/UniversalMessaging/server/<realmname>/bin.	Y
tanukilogs	Collects Tanuki service wrapper logs of a realm server. This file is located at <InstallDir>/UniversalMessaging/server/<realmname>/bin/UMRealmService.log If there are any rolled log files in addition to the current log file, for example UMRealmService.log.1 and UMRealmService.log.2, these are collected also.	Y
threaddump	Generates three thread dumps of a realm server. The dumps are taken at 15-second intervals. Having three dumps instead of one can make it easier to analyze time-related thread issues.	Y

A "Y" in the column "Default collector?" indicates that the collector is included by default when you run the RealmInformationCollector tool.

Collectors for an offline realm server

The collectors that can be run against an offline realm server are the following (collectors that can be used also against a live realm server are indicated). Path names of files and directories given in the table are the installation defaults.

Name of Collector	Description	Default collector?
data	Collects the data directory of a realm server. The location of this directory is <InstallDir>/UniversalMessaging/server/<realmname>/data.	
heapdumps	(Same as the live collector)	
installlogs	(Same as the live collector)	Y
instancemgr	(Same as the live collector)	Y
jaas	(Same as the live collector)	Y

Name of Collector	Description	Default collector?
license	(Same as the live collector)	
logs	(Same as the live collector)	Y
migrationlogs	(Same as the live collector)	
osinfo	(Same as the live collector)	Y
plugins	(Same as the live collector)	Y
psinfo	(Same as the live collector)	Y
secfile	(Same as the live collector)	Y
spmlogs	(Same as the live collector)	
tanukiconf	(Same as the live collector)	Y
tanukilogs	(Same as the live collector)	Y
version	Collects the realm server version from a non-running UM server instance. The version will be stored in the file <code>UniversalMessaging/lib/nServer.jar_version.txt</code> in the generated archive.	

Command Usage

The syntax is as follows:

```
runUMTool RealmInformationCollector
  -mode=live|offline [-username=<username> -password=<password>]
  -instance=*|<instanceName>[,<instanceName> ...]
  [-include=<collectorName>[,<collectorName> ...] ]
  [-exclude=<collectorName>[,<collectorName> ...] ]
  [-outputfile=<dir_or_file>]
  [-logsduration=<duration>]
```

Displaying help text

To display a help text showing a summary of the command usage, call the `RealmInformationCollector` tool without parameters:

```
runUMTool RealmInformationCollector
```

The `-mode` parameter

This parameter allows you to select the execution mode of the tool. The mode parameter is mandatory and can take one of the following values:

- **live** - the `RealmInformationCollector` tool will collect operational data files for each running realm server and also attempt to connect and gather information directly from each running realm server
- **offline** - the tool will collect operational data files only

In live mode, all specified realm servers (see the `-instance` parameter) must be running, whereas in offline mode, all specified realm servers must be stopped.

Also in live mode, the following collectors will connect to each specified running realm server to gather information, and will store the information in the following files under `UniversalMessaging/server/<InstanceName>/generated` in the generated archive:

Collector name	Generated file
env	envinfo.txt
realmconfig	RealmConfig.xml
healthchecker	healthchecker.txt
threaddump	Three thread dump files, generated at 15-second intervals, named <code>threaddump_<timestamp>.txt</code>

The `-username` and `-password` parameters

When establishing the connection to a live realm server, the `RealmInformationCollector` tool will authenticate using the current operating system user. It is therefore recommended to run the `RealmInformationCollector` tool using the same user as the one used to run the realm server.

You can specify a different user using the `-username` and `-password` arguments.

The `-instance` parameter

This parameter allows you to select the set of realm servers to collect information from. The parameter is mandatory and must contain either a single realm server name or a comma-separated list of realm server names. The specified realm servers must be available in the installation where the `RealmInformationCollector` tool is run from. You can specify `-instance=*` to select all installed realm servers.

The `-include` and `-exclude` parameters

You can use the `-include` and `-exclude` parameters to further refine the set of collectors that have been selected by the `-mode` parameter. You can use `-include` and `-exclude` in the same call of the `RealmInformationCollector` tool as long as they do not specify the same collector name.

- **include** - Run all default collectors available with the specified `-mode` parameter, and additionally include the collector or collectors specified by this parameter. The parameter may contain a single collector name or a comma-separated list of collector names.
- **exclude** - Run all default collectors available with the specified `-mode` parameter, except the specified collector or collectors. The parameter may contain a single collector name or a comma-separated list of collector names.

The **-outputfile** parameter

Specifies the path where the generated zip archive will be stored.

If the path specifies a directory without a filename, the directory must already exist. The archive file will be generated in the specified directory using the following naming convention:

```
<InstallDir>_<mode>_<timestamp>.zip
```

For example, if the product installation directory is C:\SoftwareAG and the RealmInformationCollector tool is executed with `-mode=live`, the generated archive will be named for example `SoftwareAG_live_20171120100757940.zip`

If the path specifies a directory with a filename, the directory must already exist but the file must not already exist, and the tool will use the filename you specify.

If the parameter is not specified, the tool will generate an archive with a name corresponding to the naming convention mentioned above, and store the archive under the directory `<InstallDir>/UniversalMessaging/tools/runner`.

The **-logsduration** parameter

Specifies the age of the oldest log that is to be returned, relative to the current time. The age can be specified in days or hours or both.

For example, if the logs are required for the past 2 days and 4 hours, the option can be specified as:

```
-logsduration=2d4h
```

Syntax Examples

Example: Execute default collectors in offline mode against the umserver instance:

```
runUMTool RealmInformationCollector -mode=offline -instance=umserver
```

Example: Execute default collectors and also optional collectors data and heapdumps in offline mode against the umserver instance:

```
runUMTool RealmInformationCollector
  -mode=offline -instance=umserver -include=data,heapdumps
```

Example: Execute default collectors and the optional collectors data and heapdumps, excluding the jaas collector, in offline mode against all realm server instances:

```
runUMTool RealmInformationCollector
  -mode=offline -instance=* -include=data,heapdumps -exclude=jaas
```

Example: Execute default collectors in live mode against the umserver instance:

```
runUMTool RealmInformationCollector -mode=live -instance=umserver
```

Example: Execute the default collectors and optional collectors heapdump and heapdumps in live mode against the umserver instance:

```
runUMTool RealmInformationCollector
```

```
-mode=live -instance=umserver -include=heapdump,heapdumps
```

Example: Execute the default collectors and optional collectors `heapdump` and `heapdumps`, excluding the `jaas` collector, in live mode against the `umserver` and `umserver2` instances:

```
runUMTool RealmInformationCollector  
-mode=live -instance=umserver,umserver2 -include=heapdump,heapdumps -exclude=jaas
```

Example: Execute the default collectors and optional collectors `heapdump` and `heapdumps` in live mode against the `umserver` instance and specify a custom location of the generated zip archive:

```
runUMTool RealmInformationCollector  
-mode=live -instance=umserver -include=heapdump,heapdumps  
-outputfile=C:/SoftwareAG_umserver_live.zip
```

Example: Execute default and `logs` collectors in live mode against all realm servers and collect logs for a specific duration:

```
runUMTool RealmInformationCollector  
-mode=live -instance=* -include=logs -logsDuration=2d4h
```

Example: Execute default and `clientinfo` and `consumerinfo` collectors in live mode against the `umserver` server instance:

```
runUMTool RealmInformationCollector  
-mode=live -instance=umserver -include=clientinfo,consumerinfo
```

Operational Issues

- On Windows, if the product installation directory path is too long, acquiring a live heap dump may fail with the error "CreateProcess error=267, The directory name is invalid". You can work around this error by configuring the `-outputFile` parameter to use a shorter directory/file path, for example `C:/SoftwareAG_live.zip`.
- The `RealmInformationCollector` tool does not support connecting via SSL-secured network interfaces to the realm server. If all realm server network interfaces are secured using SSL, live collectors which need to connect to the server (`env`, `realmconfig`, `healthchecker`, `threaddump`) will fail to connect to the server. You can work around this by configuring a temporary non-SSL secured network interface.
- Live heap dump generation using the `heapdump` collector is only available with the JVM that is delivered with the Universal Messaging distribution kit on Windows and Solaris machines. This feature is currently not available for use with other JVMs.
- The `RealmInformationCollector` tool might fail to acquire a live heap dump if the tool run with a different operating system user than the one used for running the realm server. It is recommended to run the tool with the same operating system user that was used to run the realm server.

The ExportEventsFromOfflineMemFile Tool

Overview

The `ExportEventsFromOfflineMemFile` tool is a command-line recovery tool that dumps events from mem files of Universal Messaging realm server stores to XML or JSON format. Event filtering can be applied while dumping with the tool. Events can also be dumped to both XML and JSON format in a single run of the tool, resulting in two output files that have a common structure.

The output file will contain a first element describing the export details and then a list of events. The `ExportDetails` element contains the tool version number and the protocol buffer file descriptor set in base64-encoded format, if the protocol buffer file descriptor set was specified by the user when starting the export tool.

Event structure in the output file

In XML and JSON output files, the `Event` element contains the following information:

```
id: event EID (nPublished.getKey());
size: event size (nPublished.getSize());
chanID: event ChannelAttributesId (nPublished.getChannelAttributesId());
ttl: event TTL (nPublished.getTTL());
tag: event tag (nPublished.getTag());
eventData: event data;
persistent: event isPersistent property (nPublished.isPersistent());
transient: event isTransientProperty(nPublished.isTransient());
headerProps: event header attributes;
dictionaryProps: event dictionary properties;
```

For now, the XML output file event `eventData` value is base64-encoded.

In the JSON output file, the event element contains an additional property `eventDataFormat` which can contain the value "Base64" or "GoogleProtobufJson".

In the JSON output file event element `eventData`, the value can be base64-encoded or can be a JSON node containing protocol buffer data.

XML output file example

```
<?xml version="1.0" encoding="utf-8"?>
<EventsDetails>
  <ExportDetails>
    <ToolVersion>1.0</ToolVersion>
    <ProtocolBufferFileDescriptorSet>
      <Base64EncodedFileDescriptorSet>
        <Base64EncodedFileDescriptorSet>
          <Base64EncodedFileDescriptorSet>
            <Base64EncodedFileDescriptorSet>
              <Base64EncodedFileDescriptorSet>
                <Base64EncodedFileDescriptorSet>
                  <Base64EncodedFileDescriptorSet>
                    <Base64EncodedFileDescriptorSet>
                      <Base64EncodedFileDescriptorSet>
                        <Base64EncodedFileDescriptorSet>
                          <Base64EncodedFileDescriptorSet>
                        </Base64EncodedFileDescriptorSet>
                      </Base64EncodedFileDescriptorSet>
                    </Base64EncodedFileDescriptorSet>
                  </Base64EncodedFileDescriptorSet>
                </Base64EncodedFileDescriptorSet>
              </Base64EncodedFileDescriptorSet>
            </Base64EncodedFileDescriptorSet>
          </Base64EncodedFileDescriptorSet>
        </Base64EncodedFileDescriptorSet>
      </ProtocolBufferFileDescriptorSet>
    </ExportDetails>
  <Events>
    <Event>
      <id>0</id>
      <size>306</size>
      <chanID>63565653663178134</chanID>
      <ttl>0</ttl>
      <tag>tag0</tag>
```

```
<eventData>dGVzdGRhdGFib2R5MCBkYXRh</eventData>
<persistent>true</persistent>
<transient>>false</transient>
<dictionaryProps>
  <item>
    <name>string_key</name>
    <value>value0</value>
    <type>String</type>
  </item>
  <item>
    <name>boolean_key</name>
    <value>true</value>
    <type>Boolean</type>
  </item>
  <item>
    <name>int_key</name>
    <value>0</value>
    <type>Integer</type>
  </item>
  <item>
    <name>long_key</name>
    <value>0</value>
    <type>Long</type>
  </item>
  <item>
    <name>short_key</name>
    <value>0</value>
    <type>Short</type>
  </item>
  <item>
    <name>byte_key</name>
    <value>0</value>
    <type>Byte</type>
  </item>
  <item>
    <name>char_key</name>
    <value>0</value>
    <type>Character</type>
  </item>
  <item>
    <name>byte_arr_key</name>
    <value>dGVzdDA=</value>
    <type>byte[]</type>
  </item>
  <item>
    <name>float_key</name>
    <value>0.0</value>
    <type>Float</type>
  </item>
  <item>
    <name>double_key</name>
    <value>0.0</value>
    <type>Double</type>
  </item>
</dictionaryProps>
<headerProps>
  <item>
    <name>nrvpub.time</name>
    <value>1588946429779</value>
    <type>Long</type>
  </item>
</headerProps>
</eventData>
```

```

        </item>
        <item>
            <name>nrvpub.host</name>
            <value>127.0.0.1</value>
            <type>String</type>
        </item>
        <item>
            <name>nrvpub.name</name>
            <value>ekob</value>
            <type>String</type>
        </item>
        <item>
            <name>JMSPriority</name>
            <value>4</value>
            <type>Byte</type>
        </item>
    </headerProps>
</Event>
</Events>
</EventsDetails>

```

JSON output file example

```

[
  {
    "toolVersion": "1.0",
    "descriptor":
    "GVzZdGRhdGFib2R5MkYXRh",
  },
  {
    "eventData": {
      "encodedData": "dGVzZdGRhdGFib2R5MkYXRh"
    },
    "eventDataFormat": "Base64",
    "id": 0,
    "size": 306,
    "chanID": 63565653663178136,
    "ttl": 0,
    "tag": "tag0",
    "isPersistent": true,
    "isTransient": false,
    "type": 0,
    "dictionaryProps": [
      {
        "name": "string_key",
        "value": "value0",
        "type": "String"
      },
      {
        "name": "boolean_key",
        "value": "true",
        "type": "Boolean"
      }
    ]
  }
]

```

```
    "name": "int_key",
    "value": "0",
    "type": "Integer"
  },
  {
    "name": "long_key",
    "value": "0",
    "type": "Long"
  },
  {
    "name": "short_key",
    "value": "0",
    "type": "Short"
  },
  {
    "name": "byte_key",
    "value": "0",
    "type": "Byte"
  },
  {
    "name": "char_key",
    "value": "0",
    "type": "Character"
  },
  {
    "name": "byte_arr_key",
    "value": "dGVzdDA=",
    "type": "byte[]"
  },
  {
    "name": "float_key",
    "value": "0.0",
    "type": "Float"
  },
  {
    "name": "double_key",
    "value": "0.0",
    "type": "Double"
  }
],
"headerProps": [
  {
    "name": "nrtpub.time",
    "value": "1588946429779",
    "type": "Long"
  },
  {
    "name": "nrtpub.host",
    "value": "127.0.0.1",
    "type": "String"
  },
  {
    "name": "nrtpub.name",
    "value": "ekob",
    "type": "String"
  },
  {
    "name": "JMSDeliveryMode",
    "value": "PERSISTENT",
    "type": "String"
  }
]
```

```

    },
    {
      "name": "JMSPriority",
      "value": "4",
      "type": "Byte"
    }
  ]
}
]

```

Difference between XML and JSON export formats

The JSON output file event element can have `eventData` as a JSON node and `"eventDataFormat": "GoogleProtobufJson"` if events are dumped from the mem file of a protobuf channel and the export tool had the input parameter `protobufdescriptor` specified.

Here is an example of a JSON event dumped from a protobuf channel with `protobufdescription` specified :

```

{
  "eventData": {
    "student": [
      {
        "name": "StudentName0",
        "id": 1,
        "email": "StudentName0@softwareag.com",
        "phone": [
          {
            "number": "19150",
            "type": "HOME"
          }
        ]
      }
    ]
  },
  "teacher": {
    "name": "TeacherName0",
    "id": 2,
    "email": "TeacherName0@softwareag.com",
    "phone": [
      {
        "number": "77430",
        "type": "HOME"
      }
    ]
  }
},
  "eventDataFormat": "GoogleProtobufJson",
  "id": 0,
  "size": 215,
  "chanID": 39103550381024424,
  "ttl": 0,
  "tag": "tag0",
  "isPersistent": true,
  "isTransient": false,
  "type": 0,
  "headerProps": [
    {
      "name": "nrvpub.time",

```

```

    "value": "1588946429899",
    "type": "Long"
  },
  {
    "name": "nrtpub.host",
    "value": "127.0.0.1",
    "type": "String"
  },
  {
    "name": "nrtpub.name",
    "value": "ekob",
    "type": "String"
  },
  {
    "name": "JMSType",
    "value": "School",
    "type": "String"
  },
  {
    "name": "JMSDeliveryMode",
    "value": "PERSISTENT",
    "type": "String"
  },
  {
    "name": "JMSPriority",
    "value": "4",
    "type": "Byte"
  },
  {
    "name": "JMSMsgType",
    "value": "6",
    "type": "Integer"
  }
]
}

```

Input parameters

-protobufdescriptor

The `-protobufdescriptor` input parameter is an optional parameter specifying the path to the protocol buffer file descriptor set for filtering events based on event data.

The protocol buffer file descriptor set can be received as:

```

protoc.exe <proto_file_name>.proto
--descriptor_set_out=<protocol_buffer_file_descriptor_set_name>.fds

```

If the input parameter `protobufdescriptor` is specified and the mem file's store is a protobuf channel with the same protobuf descriptor, then event filtering can be done based on the event protocol buffer data. The protocol buffer descriptor will be exported to the output file as a base64-encoded string.

If the input parameter `protobufdescriptor` was not specified and the mem file's store is a protobuf channel, then event filtering cannot be done based on the event protocol buffer data.

If the input parameter `protobufdescriptor` is specified but the mem file's store is a protobuf channel with a different protobuf descriptor, then dumping will not be performed.

If the input parameter `protobufdescriptor` is specified but the mem file's store is not a protobuf channel, then the event will be considered as `nPublished` events anyway. The protocol buffer descriptor will be exported to the output file as a base64-encoded string.

batchsize

The default value of the batch size is 100. It can be optionally specified when running the tool. It defines the number of events which will be read/loaded to the memory/ from the mem file, filtered and then written to the output file at once.

The RepublishEventsFromOfflineFile Tool

The `RepublishEventsFromOfflineFile` tool is a command-line recovery tool that imports events into a Universal Messaging realm server store (channel or queue) from any of the following sources:

- An XML file or JSON file.
- A copy of the store's persistent memory file (or multiple memory files for a multi-file store).

Event filtering can be applied while importing with the tool. Republishing is done as transaction event publishing.

Input files

Importing can be done from an XML or JSON file produced by the `ExportEventsFromOfflineMemFile` tool.

Importing can be done from offline memory files of the store taken from the parent realm's `data` directory. The offline memory files have the filetype `*.mem`. When importing multi-file stores, you specify the folder that contains the `*.mem` files. When importing a mixed/persistent store, you specify a single `.mem` file.

When you invoke the tool, you can specify either a mem file (or mem folder name), or an XML file, or a JSON file, but not a combination of these options.

The -protobufdescriptor input parameter

Import from the mem file of a protobuf store

If the import is performed from a protobuf store's mem file and the `protobufdescriptor` parameter specified is the same as for the "source" channel, then filtering can be done based on the protocol buffer event data. If the "republish" channel has the same protocol buffer file descriptor set as the "source" store, events will be republished as protobuf events.

If the import is performed from a protobuf store's mem file and the `protobufdescriptor` parameter specified is the same as for the "source" channel, but the "republish" channel has another protocol buffer file descriptor or is not a protobuf channel, then event republishing will not be done.

If the import is performed from a protobuf store's mem file but the `protobufdescriptor` parameter is not specified, then filtering cannot be done based on protobuf data. Events will be republished as non-protobuf events to a non-protobuf store and as protobuf events to a store with the protocol buffer file descriptor set.

Import from mem file of non-protobuf store

If the import is performed from a non-protobuf store's mem file and the `protobufdescriptor` parameter is not specified, events will be republished as non-protobuf events to any channel.

If the import is performed from a non-protobuf store's mem file and the `protobufdescriptor` parameter is specified and coincides with the descriptor of the "republish" channel, events will be republished as non-protobuf events.

But if the import is performed from a non-protobuf store's mem file and the `protobufdescriptor` parameter is specified and does not coincide with the descriptor of the "republish" channel, events will not be republished.

Import from XML and JSON files

If the source file belongs (was exported from) to a protobuf channel's mem file and was exported with its protobuf descriptor, the import will be done with the protobuf descriptor specified in the file. So it is possible to specify only a selector to filter events based on protobuf data. Events will be republished as protobuf events to a store with the protobuf descriptor and as non-protobuf events to other channels.

If the source file belongs to a protobuf channel and was exported without a protobuf descriptor and no `protobufdescriptor` was specified or another is specified as input parameter, the import will be done without possible filtering based on the protobuf event data. Events will be republished as protobuf events to a store with the protobuf descriptor and as non-protobuf events to other channels. If the correct `protobufdescriptor` parameter is specified as an input parameter, then filtering will be possible based on protobuf eventdata.

The -batchsize input parameter

This parameter can be optionally specified when running the tool. It defines the number of events which will be read/loaded to the memory/ from mem/XML/JSON file, filtered and then published to the "destination" store as a single batch.

The default batch size is 100.

The ServerReleaseVersion Tool

The `ServerReleaseVersion` tool retrieves the release versions for a list of Universal Messaging servers or for servers that are part of a Horizontal Scalability (HS) RNAME. The tool returns the release version of each server to which a client can establish a session at the moment. The release version is in a *major.minor* format, for example 10.7. If a session to any of the servers cannot be established, the tool lists the server as unknown and displays the reason for the unsuccessful connection to the server .

When you specify an HS RNAME as input, the `ServerReleaseVersion` tool generates a valid HS RNAME that contains the `hsReleaseVersion` attribute. If the servers that are part of the HS RNAME are different versions, the `hsReleaseVersion` attribute contains the highest release version supported by all servers.

For a list of servers, the tool returns information about each server.

In addition, the tool returns the release version of the client.

Syntax

■ On Windows:

```
runUMTool.bat ServerReleaseVersion -rname=rname [username=username]
[password=password]
```

■ On Unix:

```
runUMTool.sh ServerReleaseVersion -rname=rname [username=username]
[password=password]
```

Arguments and Options

-rname=rname

Required. String. The URLs of the servers for which you want to retrieve the release version. The URL of each server is in the form `protocol://hostname:port`. The `-rname` parameter must have the following values:

- An HS RNAME in the form of `(protocol://hostname:port,protocol://hostname:port,...)` for a cluster or `(protocol://hostname:port)` for a standalone server.
- A list of server URLs separated by a comma or a semicolon without any white spaces in the form of
`protocol://hostname:port,protocol://hostname:port,protocol://hostname:port,...` or
`protocol://hostname:port;protocol://hostname:port;protocol://hostname:port;...`

username=username

Optional. Typically set by an administrator to establish server resource access levels.

password=password

Optional. Typically set by an administrator to establish server resource access levels.

Examples

- To retrieve the release versions for a list of servers with URLs "nsp://localhost:9000", "nsp://localhost:9001", and "nsp://localhost:9002" on Windows:

```
runUMTool.bat ServerReleaseVersion
-rname=nsp://localhost:9000,nsp://localhost:9001,nsp://localhost:9002
```

The command prints the following output:

```
We have initialised ServerReleaseVersion with:
```

```
{rname=nsp://localhost:9000,nsp://localhost:9001,nsp://localhost:9002}
Server URLs and version of each one:
nsp://localhost:9000 -> 10.11
nsp://localhost:9001 -> 10.11
nsp://localhost:9002 -> 10.11
Client version -> 10.11
Tool execution has finished successfully.
```

- To retrieve the release versions for two clusters of two servers each, where the servers are different versions and the server with URL `nsp://localhost:9001` is a lower version than the rest, as part of an HS RNAME on Windows:

```
runUMTool.bat ServerReleaseVersion
-rname=(nsp://localhost:9000,nsp://localhost:9001)(nsp://localhost:9002,nsp://localhost:9003)
```

The command prints the following output:

```
We have initialised ServerReleaseVersion with:
{rname=(nsp://localhost:9000,nsp://localhost:9001)(nsp://localhost:9002,nsp://localhost:9003)}
Server URLs and version of each one:
nsp://localhost:9000 -> 10.11
nsp://localhost:9001 -> 10.7
nsp://localhost:9002 -> 10.11
nsp://localhost:9003 -> 10.11
Client version -> 10.11
Correct HS url to be used is:
(nsp://localhost:9000,nsp://localhost:9001)(nsp://localhost:9002,nsp://localhost:9003)
?hsReleaseVersion=10.7
Tool execution has finished successfully.
```

Syntax reference for command line tools

Syntax: Store Tools

CreateChannel

```
Tool name:
  CreateChannel
Description:
  Creates a channel with the specified name on the specified server.
  A single permission can be set during channel creation using
  optional arguments.
  For adding a set of permissions use the client API.
Usage:
  runUMTool CreateChannel -rname=<rname> -channelname=<channelname>
  [optional_args]
Examples:
  CreateChannel -rname=nsp://localhost:8080 -channelname=channel0
  -maxevents=10
Required arguments:
  rname :
```

URL of the realm to which the channel will be connected.
channelname :
Name of the channel to be created.

Optional Parameters:

maxevents :
Capacity of the new store (default 0).
ttl :
Time to Live for the new store (default 0).
type :
Type of the new store (default S).
R - Reliable (stored in memory), with persistent EIDs
P - Persistent (stored on disk)
S - Simple (stored in memory)
T - Transient (no server-based storage)
M - Mixed (allows both memory and persistent events)
O - Off-Heap
G - Paged (uses a memory-mapped file for storage)
publishkeys :
Set of publish keys for the new store (default null).
Multiple pairs - each pair is separated by a ';'!
Pairs - each name and depth is separated by a ','
e.g. name,depth;name2,depth2
isclusterwide :
Whether the new store is cluster-wide.
Will only work if the realm is part of a cluster.
usejmsengine :
Whether to use the JMS style fanout engine.
usemergeengine :
Whether to use the merge style fanout engine.
isautodelete :
Whether the store is auto-deleted upon disconnection of its creator.
isdurable :
Whether the store is durable (restores after a server restart).
isautomaintenance :
Whether the store will have automatic maintenance as events are
being removed.
honourcapacity :
Whether the store capacity setting will prevent publishing of any more
data once full.
enablecaching :
Whether the server will cache events in memory or will always refer back
to the file-backed store.
cacheonreload :
Whether the server will cache events in memory for fast replay upon restart.
enablereadbuffering :
Whether reads will be buffered to optimise the I/O access to the
file-based store.
readbuffersize :
The size in bytes of the buffer to use when read buffering (default 10240).
enablemulticast :
Whether multicast is supported on the new store.
synceachwrite :
Whether each write to the store will also call sync on the file system
to ensure all data is written to disk.
syncbatchsize :
Maximum size of batch written to disk on sync.
syncbatchtime :
Time for writing data to disk on sync.
priority :

```

The default message priority for events on the new store.
stampdictionary :
  StampDictionary setting value for the new store.
subject :
  The subject in format user@host for which the permission
  will be set. For a group permission, this value will be set
  as a group name. If this parameter is missing, the other parameters
  related to the permission entry are considered invalid.
group :
  Whether a group permission entry must be created. Such permissions
  can be applied during channel creation only for already existing
  security groups.
manage :
  Whether the subject or group has permissions to manage ACLs
  (default is set to false).
publish :
  Whether the subject or group has permissions to publish
  events to this channel (default is set to false).
subscribe :
  Whether the subject or group has permissions to subscribe to the
  channel (default is set to false).
purge :
  Whether the subject or group has permissions to purge events
  from the channel (default is set to false).
fullprivileges :
  Whether the subject or group has full permissions for this channel
  (default is set to false).
getlasteid :
  Whether the subject or group has permissions to get the last event ID
  (default is set to false).
named :
  Whether the subject or group has permissions to use named
  subscription on the channel (default is set to false).
multifileeventsperspindle :
  Number of events that will be stored per individual file for a store
  (default is 50000).
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.

```

CreateDurable

```

Tool name:
  CreateDurable
Description:
  Creates a Durable (also known as Named Object) with the specified name and type
  on the specified channel.

Usage:
  runUMTool CreateDurable -rname=<rname> -channelname=<channelname>
  -durablename=<durablename> -durabletype=<durabletype> [optional_args]

Examples:
  CreateDurable -rname=nsp://localhost:8080 -channelname=channel0
  -durablename=durable0 -durabletype=N

Required arguments:

```

```

rname :
    URL of the realm to list the details of all the channels within.

channelname :
    Name of the channel on which the Durable will be created.
durablename :
    Name of the Durable to be created.
durabletype :
    Type of the new Durable.
    N - Named
    S - Shared
    SE - Serial

```

Optional Parameters:

```

isclusterwide :
    Whether the durable should be created in the entire cluster.
username :
    Your Universal Messaging server username
password :
    Your Universal Messaging server password

```

CreateJoin

```

Tool name:
    CreateJoin
Description:
    Joins two channels.

Usage:
    runUMTool CreateJoin -rname=<rname> -channelhost=<channelhost>
    -channeldest=<channeldest> [optional_args]

Examples:
    CreateJoin -rname=nsp://localhost:8080 -rnamedest=nsp://localhost:8090
    -channelhost=source -channeldest=destination

Required arguments:
    rname :
        URL of the realm from which the source channel will be retrieved.
    channelhost :
        Name of the source channel.
    channeldest :
        Name of the destination channel.

Optional Parameters:
    rnamedest :
        URL of the realm from which the destination channel
        will be retrieved (default is set to be -rname).

    routed :
        Set routed parameter (default is set to be false).
    hopcount :
        Set maximum number of hops (default is set to be 10).
    selector :
        Set selector string (default is set to be null).
    allowpurge :
        Set allowPurge parameter when connecting to a channel
        (default is set to be true).

```

```
createtwoway :  
  Set createtwoway parameter to create a two way  
  channel join (default is set to be false)  
username :  
  Your Universal Messaging server username.  
password :  
  Your Universal Messaging server password.
```

CreateQueue

```
Tool name:  
  CreateQueue  
Description:  
  Creates a queue with the specified name on the specified server.  
  A single permission can be set during queue creation using  
  optional arguments. For adding a set of permissions use the client API.  
Usage:  
  runUMTool CreateQueue -rname=<rname> -queuename=<queuename> [optional_args]  
Examples:  
  CreateQueue -rname=nsp://localhost:8080 -queuename=queue0 -maxevents=10  
Required arguments:  
  rname :  
    URL of the realm to which the queue will be connected.  
  
  queuename :  
    Name of the queue to be created.  
Optional Parameters:  
  
  maxevents :  
    Capacity of the new store (default 0).  
  
  ttl :  
    Time to Live for the new store (default 0).  
  
  type :  
    Type of the new store (default S).  
    R - Reliable (stored in memory), with persistent EIDs  
    P - Persistent (stored on disk)  
    S - Simple (stored in memory)  
    T - Transient (no server-based storage)  
    M - Mixed (allows both memory and persistent events)  
    O - Off-Heap  
    G - Paged (uses a memory-mapped file for storage)  
  
  isclusterwide :  
    Whether the new store is cluster-wide.  
    Will only work if the realm is part of a cluster.  
  
  usejmsengine :  
    Whether to use the JMS style fanout engine.  
  usemergeengine :  
    Whether to use the merge style fanout engine.  
  isautodelete :  
    Whether the store is auto-deleted upon disconnection of its creator.  
  isdurable :
```

Whether the store is durable (restores after a server restart).

isautomaintenance :
Whether the store will have automatic maintenance as events are being removed.

honourcapacity : Whether the store capacity setting will prevent publishing of any more data once full.

enablecaching :
Whether the server will cache events in memory or will always refer back to the file-backed store.

cacheonreload :
Whether the server will cache events in memory for fast replay upon restart.

enablereadbuffering :
Whether reads will be buffered to optimise the I/O access to the file-based store.

readbuffersize :
The size in bytes of the buffer to use when read buffering (default 10240).

enablemulticast :
Whether multicast is supported on the new store.

synceachwrite :
Whether each write to the store will also call sync on the file system to ensure all data is written to disk.

syncbatchsize :
Maximum size of batch written to disk on sync.

syncbatchtime :
Time for writing data to disk on sync.

priority :
The default message priority for events on the new store.

stampdictionary :
StampDictionary setting value for the new store.

subject :
The subject in format user@host for which the permission will be set. For a group permission this value will be set as a group name. If this parameter is missing the other parameters related to the permission entry are considered invalid.

group :
Whether a group permission entry must be created. Such permissions can be applied during channel creation only for already existing security groups.

manage :
Whether the subject or group has permissions to manage ACLs (default is set to false).

fullprivileges : Whether the subject or group has full permissions for this channel (default is set to false).

purge :
Whether the subject or group has permissions to purge events from the channel (default is set to false).

pop :
Whether the subject or group has permissions to pop events from the queue (default is set to false).

peek :
Whether the subject or group has permissions to peek events from this queue (default is set to false).

push :
Whether the subject or group has permissions to push events in the queue (default is set to false).

username :
Your Universal Messaging server username.

```
password :  
  Your Universal Messaging server password.
```

DeleteChannel

```
Tool name:  
  DeleteChannel  
Description:  
  Deletes a channel with the specified name on the specified realm.  
Usage:  
  runUMTool DeleteChannel -rname=<rname> -channelname=<channelname>  
    [optional_args]  
Examples:  
  DeleteChannel -rname=nsp://localhost:8080 -channelname=channel0  
Required arguments:  
  rname :  
    URL of the realm to which the channel will be connected.  
  
  channelname :  
    Name of the channel to be deleted.  
Optional Parameters:  
  username :  
    Your Universal Messaging server username.  
  password :  
    Your Universal Messaging server password.
```

DeleteDurable

```
Tool name:  
  DeleteDurable  
Description:  
  Deletes a Durable with the specified name on the specified channel.  
Usage:  
  runUMTool DeleteDurable -rname=<rname> -channelname=<channelname>  
    -durablename=<durablename> [optional_args]  
Examples:  
  DeleteDurable -rname=nsp://localhost:8080 -channelname=channel0  
    -durablename=durable0  
Required arguments:  
  
  rname :  
    URL of the realm to list the details of all the channels within.  
  channelname :  
    Name of the channel from which the Durable will be deleted.  
  durablename :  
    Name of the Durable to be deleted.  
Optional Parameters:  
  username :  
    Your Universal Messaging server username.  
  password :
```

Your Universal Messaging server password.

DeleteJoin

Tool name:
DeleteJoin

Description:
Deletes a join between two channels.

Usage:
runUMTool DeleteJoin -rname=<rname> -channelhost=<channelhost>
-channeldest=<channeldest> [optional_args]

Examples:
DeleteJoin -rname=nsp://localhost:8080 -rnamedest=nsp://localhost:8090
-channelhost=source -channeldest=destination

Required arguments:

- rname :
URL of the realm from which the source channel will be retrieved.
- channelhost :
Name of the source channel.
- channeldest :
Name of the destination channel.

Optional Parameters:

- rnamedest :
URL of the realm from which the destination channel will be retrieved (default is set to be -rname).
- username :
Your Universal Messaging server username.
- password :
Your Universal Messaging server password.

DeleteQueue

Tool name:
DeleteQueue

Description:
Deletes a queue with the specified name on the specified realm.

Usage:
runUMTool DeleteQueue -rname=<rname> -queuename=<queuename> [optional_args]

Examples:
DeleteQueue -rname=nsp://localhost:8080 -queuename=queue0

Required arguments:

- rname :
URL of the realm to which the queue is connected.
- queuename :
Name of the queue to be deleted.

Optional Parameters:

- username :
Your Universal Messaging server username.
- password :
Your Universal Messaging server password.

ExportProtobufDefinitions

```
Tool Name:
  ExportProtobufDefinitions
Description:
  Exports the protobuf definitions from a store with the specified name on the specified
  server.
Usage:
  runUMTool ExportProtobufDefinitions -rname=<rname> -storename=<storename>
  -dirname=<dirname> [optional_args]
Examples:
  ExportProtobufDefinitions -rname=nsp://localhost:9000 -storename=store0
  -dirname=../build/change-management/test/protobuf/
Required arguments:

  rname :
    URL of the session to which the store will be connected.

  storename :
    Name of the store from which to export the protobuf definitions.

  dirname :
    Directory in which to save the exported definition files.
    If the directory that you entered does not exist, the tool creates the directory.
    If the directory exists and contains a non-empty folder with the same name as the
    store,
    the tool displays an error message.
Optional Parameters:

  username :
    Your Universal Messaging server username.
  password :
    Your Universal Messaging server password.
```

GetChannelInfo

```
Tool name:
  GetChannelInfo
Description:
  Gets the attributes and storage properties of a specified channel
  in a specified realm.
Usage:
  runUMTool GetChannelInfo -rname=<rname> -cname=<cname> [optional_args]
Examples:
  GetChannelInfo -rname=nsp://localhost:8080 -cname=channel0 -format=plaintext
Required arguments:
  rname :
    URL of the realm to which the channel will be connected.
  cname :
    Name of the channel to return info for.
Optional Parameters:
  format :
    Format to print output in (plaintext/xml/json).
  username :
```

Your Universal Messaging server username.

password :
Your Universal Messaging server password.

GetDurableInfo

Tool name:
GetDurableInfo

Description:
Gets the attributes of a specific Durable in a specific channel.

Usage:
runUMTool GetDurableInfo -rname=<rname> -channelname=<channelname>
-durablename=<durablename> [optional_args]

Examples:
GetDurableInfo -rname=nsp://localhost:8080 -channelname=channel0
-durablename=durable0 -format=plaintext

Required arguments:

- rname :
URL of the realm to list the details of all the channels within.
- channelname :
Name of the channel from where to get the Durable.
- durablename :
Name of the Durable to return info for.

Optional Parameters:

- format :
Format to print output in (plaintext/xml/json).
- username :
Your Universal Messaging server username.
- password :
Your Universal Messaging server password.

GetDurablesInfo

Tool name:
GetDurablesInfo

Description:
Displays the durables details saved in a .nsb file.

Usage:
runUMTool GetDurablesInfo -nsbfileloc=<nsbfileloc> [optional_args]

Examples:
GetDurablesInfo -nsbfileloc=C:\filepath

Required arguments:

- nsbfileloc :
Absolute path for the nsb files location. This can be a folder which consists of multiple nsb files or a single nsb file.

Optional Parameters:

- textfileexport :
Path to a text file in which the .nsb content will be saved. Must be an absolute path to a text file or the name of a

```
text file which will be created in the working directory.
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.
```

GetDurableStatus

```
Tool name:
  GetDurableStatus
Description:
  Gets the current state of durables on a realm, sorted by a given field.
Usage:
  runUMTool GetDurableStatus -rname=<rname> [optional_args]
Examples:
  GetDurableStatus -rname=nsp://localhost:8080 -sort=storesize -v=true
Required arguments:
  rname :
    URL of the realm to find durables for.
Optional Parameters:
  sort :
    Field to sort objects by. May be depth, depthtx, storesize,
    lasteid, lastread or lastwrite (default lastread).
  v :
    Whether the final output includes all fields or only
    the one specified. May be true or false (default false).
  username :
    Your Universal Messaging server username.
  password :
    Your Universal Messaging server password.
```

IdentifyLargeDurableOutstandingEvents

```
Tool name:
  IdentifyLargeDurableOutstandingEvents
Description:
  Identifies channels containing Durable with a large number
  of outstanding events.
Usage:
  runUMTool IdentifyLargeDurableOutstandingEvents -rname=<rname>
  -threshold=<threshold> [optional_args]
Examples:
  IdentifyLargeDurableOutstandingEvents -rname=nsp://localhost:8080
  -threshold=100
Required arguments:
  rname :
    URL of the realm to list the details of all the channels within.
  threshold :
    Long value representing the tolerated number of outstanding events.
```

Optional Parameters:

```
username :  
    Your Universal Messaging server username.  
  
password : Your Universal Messaging server password.
```

ListChannels

Tool name:

```
ListChannels
```

Description:

```
Lists details of the channels on the specified server.
```

Usage:

```
runUMTool ListChannels -rname=<rname> [optional_args]
```

Examples:

```
ListChannels -rname=nsp://localhost:8080
```

Required arguments:

```
rname :  
    URL of the realm to list the details of all the channels within.
```

Optional Parameters:

```
format :  
    Format to print output in (plaintext/xml/json).  
username :  
    Your Universal Messaging server username.  
password :  
    Your Universal Messaging server password.
```

ListJoins

Tool name:

```
ListJoins
```

Description:

```
Lists joins on a given realm.
```

Usage:

```
runUMTool ListJoins -rname=<rname> [optional_args]
```

Examples:

```
ListJoins -rname=nsp://localhost:8080 -v=true
```

Required arguments:

```
rname :  
    URL of the realm to which we will connect.
```

Optional Parameters:

```
v :  
    Output additional information for each join.  
username :  
    Your Universal Messaging server username.  
password :  
    Your Universal Messaging server password.
```

MonitorChannels

```
Tool name:
  MonitorChannels
Description:
  Monitors the channels and queues in a realm and prints totals.

Usage:
  runUMTool MonitorChannels -rname=<rname> [optional_args]

Examples:
  MonitorChannels -rname=nsp://localhost:8080 -channelname=channel0
  -format=plaintext
  MonitorChannels -rname=nsp://localhost:8080 -channelname=queue1
  -format=plaintext

Required arguments:
  rname :
    URL of the realm to monitor channels and queues for.

Optional Parameters:
  channelname :
    Name of a specific channel or queue to monitor
  format :
    Format to print output in (plaintext/xml/json)
  username :
    Your Universal Messaging server username.
  password : Your Universal Messaging server password.
```

PurgeEvents

```
Tool name:
  PurgeEvents
Description:
  Purges events from a channel with the specified name on the
  specified realm.

Usage:
  runUMTool PurgeEvents -rname=<rname> -channelname=<channelname>
  [optional_args]

Examples:
  PurgeEvents -rname=nsp://localhost:8080 -channelname=channel0

Required arguments:
  rname :
    URL of the realm to which the channel will be connected.
  channelname :
    Name of the channel to be created.

Optional Parameters:
  starteid :
    Starting event ID of range to purge.
  endeid :
    Ending event ID of range to purge.
  selector :
    Selector query to filter which events to purge.
  purgejoins :
```

```

Whether to purge events from joined channels.
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.

```

Syntax: Cluster Tools

ClusterState

```

Tool name:
  ClusterState
Description:
  Checks the cluster state by a given RNAME, which is part of a cluster.

Usage:
  runUMTool ClusterState -rname=<rname> [optional_args]

Examples:
  ClusterState -rname=nsp://localhost:8080

Required arguments:
  rname :
    Name of a realm, which is part of a cluster.

Optional Parameters:
  username :
    Your Universal Messaging server username.
  password :
    Your Universal Messaging server password.

```

CreateCluster

```

Tool name:
  CreateCluster
Description:
  Creates a cluster with the specified name, consisting of the specified realms.

Usage:
  runUMTool CreateCluster -clustername=<clustername> -convertlocal=<convertlocal>
  -rnames=<rnames> [optional_args]

Examples:
  CreateCluster -clustername=cluster0 -convertlocal=true
  -rnames=nsp://localhost:8080,nsp://localhost:9090

Required arguments:
  clustername :
    Name of the cluster to be created.
  convertlocal :
    Whether the local stores of the master should be converted
    to cluster-wide stores.
  rnames :
    Server URLs to be included in the cluster. Can be more than one,
    separated by a comma.
    The proper format is [nsp/nhp/nsps/nhps]://[hostname]:[port] or

```

```
shm://[path/to/file].
```

Optional Parameters:

```
username :  
    Your Universal Messaging server username.  
password :  
    Your Universal Messaging server password.
```

DeleteCluster

Tool name:

```
DeleteCluster
```

Description:

```
Deletes the cluster with the specified name.  
The RNAME of a server in the cluster must also be given.
```

Usage:

```
runUMTool DeleteCluster -clustername=<clustername>  
    -rname=<rname> -deletestores=<deletestores> [optional_args]
```

Examples:

```
DeleteCluster -clustername=cluster0 -rname=nsp://localhost:8080 -deletestores=true
```

Required arguments:

```
clustername :  
    Name of the cluster to be deleted.
```

rname :

```
The URL of a server which belongs to the cluster to be deleted.  
The proper format is [nsp/nhp/nsps/nhps]://[hostname]:[port] or
```

```
shm://[path/to/file].
```

deletestores :

```
True/false flag indicating whether or not cluster-wide stores should be deleted  
when the cluster is destroyed.
```

Optional Parameters:

```
username :  
    Your Universal Messaging server username.
```

```
password :  
    Your Universal Messaging server password.
```

DumpClusterNamedObjectsState

Tool name:

```
DumpClusterNamedObjectsState
```

Description:

```
Dumps the state of named objects (also called durable subscriptions)  
on channels present on the specified cluster servers.
```

Usage:

```
runUMTool DumpClusterNamedObjectsState -rnames=<rnames>  
    -verbosemode=<verbosemode> [optional_args]
```

Examples:

```
DumpClusterNamedObjectsState -rnames=nsp://localhost:8080,nsp://localhost:9090  
    -verbosemode=true
```

```

Required arguments:
  rnames :
    Comma-separated list of rNames of clustered nodes.
  verbosemode :
    Set true to see all node states; set false to see only those
    with mismatched node states.

Optional Parameters:
  username :
    Your Universal Messaging server username.
  password :
    Your Universal Messaging server password.

```

Syntax: Interface Tools

AddHTTPInterface

```

Tool name:
  AddHTTPInterface
Description:
  Adds a HTTP interface on the specified adapter and port,
  on the specified realm.

Usage:
  runUMTool AddHTTPInterface -rname=<rname> -adapter=<adapter> -port=<port>
  [optional_args]

Examples:
  AddHTTPInterface -rname=nsp://localhost:8080 -adapter=0.0.0.0 -port=9090
  -usewebsockets=true

Required arguments:
  rname :
    URL of the realm to which the realm node, on which the interface
    will be created, is connected.
  adapter :
    Adapter (network card) to which interface will bind.
  port :
    Port on which the interface will listen.

Optional Parameters:
  usehttp1.1 :
    Whether to use HTTP1.1.
  usewebsockets :
    Whether WebSockets are used.
  ajaxactivedelay :
    Time to wait (for additional events) before delivering to
    Long Poll style subscribers.
  ajaxidledelay :
    Time to wait before returning from a Long Poll call if no events
    have been received.
  isnativecomet :
    Whether JavaScript is enabled on the interface.
  allowedorigins :
    Set the Allowed Origins for CORS as a comma-separated list of origins
    (use '*' to allow all), e.g. origin1,origin2,origin3
  crossorigincredentials :

```

```

Whether to allow credentials header to be sent with CORS requests.
enablegzip :
  Whether or not GZIP compression is enabled for javascript Long Poll
  connections.
minimumbytes :
  Set the minimum number of bytes in a packet before GZIP
  is enabled (default 1000).
autostart :
  Whether this interface will automatically be started when
  the realm server starts.
advertise :
  Set the current advertise status for this interface.
allowinterrealm :
  Whether this interface is allowed to be used in
  inter realm/cluster communication.
allowclientconnections :
  Whether this interface can accept client connections or not.
allownio :
  Whether NIO is enabled on the interface.
authtimeout :
  Set the number of milliseconds that the remote client
  has to authenticate with the server.
backlog :
  Set the number of connections to queue before the Operating System
  will send rejects to the remote client.
threads :
  Set the thread pool size handling the client connections.
selectthreads :
  Set the number of select threads used by NIO.
adaptersalias :
  Set the interface's alias.
receivebuffersize :
  Set the socket buffer size in bytes used by this
  interface when receiving data.
sendbuffersize :
  Set the socket buffer size in bytes used by this
  interface when sending data.
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.

```

AddHTTPSInterface

```

Tool name:
  AddHTTPSInterface
Description:
  Adds a HTTPS interface on the specified adapter and port,
  on the specified server.

Usage:
  runUMTool AddHTTPSInterface -rname=<rname> -adapter=<adapter> -port=<port>
  [optional_args]

Examples:
  AddHTTPSInterface -rname=nsp://localhost:8080 -adapter=0.0.0.0 -port=9090
  -alias=myAlias

Required arguments:

```

```

rname :
    URL of the realm to which the realm node, on which the interface
    will be created, is connected.
adapter :
    Adapter (network card) to which interface will bind.
port :
    Port on which the interface will listen.

```

Optional Parameters:

```

alias :
    Set the certificate name/alias that this interface will use to
    select its certificate from a keystore with multiple entries.
keystore :
    Set the keystore file that this interface uses to load the certificate.
kspassword :
    Set the keystore password that this interface will use to
    access the keystore file specified.
truststore :
    Set the truststore file against which this interface will
    validate the client certificate.
tspassword :
    Sets the truststore password that the server uses to access the
    trust store.
privatepassword :
    Private key password; used so that the key can be loaded
    from the key store.
ciphers :
    Names of the ciphers enabled for use by this interface, as a
    comma-separated list of ciphers, e.g. cipher1,cipher2,cipher3.
rndalg :
    Set the SecureRandom algorithm to use for this interface.
rndprov :
    Set the SecureRandom provider to use for this interface.
clientcertrequired :
    Whether this interface requires SSL client authentication.
crl :
    Set the certificate revocation list file name that the interface
    should use to check incoming SSL connections.
crlclassname :
    Name of the class used to validate a client connection.
provider :
    Name of the JSSE provider to use for the interface.
usehttp1.1 :
    Whether to use HTTP1.1.
usewebsockets :
    Whether WebSockets are used.
ajaxactivedelay :
    Time to wait (for additional events) before delivering
    to Long Poll style subscribers.
ajaxidleldelay :
    Time to wait before returning from a Long Poll call if
    no events have been received.
isnativecomet :
    Whether JavaScript is enabled on the interface.
allowedorigins :
    Set the Allowed Origins for CORS as a comma-separated list of origins
    (use '*' to allow all), e.g. origin1,origin2,origin3.
crossorigincredentials :
    Whether to allow credentials header to be sent with CORS requests.

```

```
enablegzip :
  Whether or not GZIP compression is enabled for javascript
  Long Poll connections.
minimumbytes :
  Set the minimum number of bytes in a packet before GZIP
  is enabled (default 1000).
autostart :
  Whether this interface will automatically be started when
  the realm server starts.
advertise :
  Set the current advertise status for this interface.
allowinterrealm :
  Whether this interface is allowed to be used in
  inter realm/cluster communication.
allowclientconnections :
  Whether this interface can accept client connections.
allownio :
  Whether NIO is enabled on the interface.
authtimeout :
  Set the number of milliseconds that the remote client
  has to authenticate with the server.
backlog :
  Set the number of connections to queue before the Operating System
  will send rejects to the remote client.
threads :
  Set the thread pool size handling the client connections.
selectthreads :
  Set the number of select threads used by NIO.
adapartialias :
  Set the interface's alias.
receivebuffersize :
  Set the socket buffer size in bytes used by this
  interface when receiving data.
sendbuffersize :
  Set the socket buffer size in bytes used by this interface
  when sending data.
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.
```

AddSHMInterface

```
Tool name:
  AddSHMInterface
Description:
  Adds a shared memory interface with the specified path, buffer size and
  timeout, on the specified server.

Usage:
  runUMTool AddSHMInterface -rname=<rname> -path=<path> [optional_args]

Examples:
  AddSHMInterface -rname=nsp://localhost:11000 -path=/dev/shm -buffer=1024
  -timeout=2000 -autostart=true

Required arguments:
  rname :
  URL of the realm to which the realm node, on which the interface
```

```

    will be created, is connected.
  path :
    The path where the shared memory files will be stored.

Optional Parameters:
  buffer :
    The size of the shared memory buffer which will be used. If not
    provided a default value of 1024000 will be used.
  timeout :
    The timeout value that will be used for read / write. If not
    provided a default value of 20000 will be used.
  autostart :
    Whether this interface will be automatically started when
    the Realm Server starts. Default is set to true.
  interrealmallow :
    Sets whether this interface is allowed to be used
    in inter realm / cluster communication. Default is set to false.
  username :
    Your Universal Messaging server username.
  password :
    Your Universal Messaging server password.

```

AddSSLInterface

```

Tool name:
  AddSSLInterface
Description:
  Adds a SSL interface on the specified adapter and port,
  on the specified server.

Usage:
  runUMTool AddSSLInterface -rname=<rname> -adapter=<adapter> -port=<port>
  [optional_args]

Examples:
  AddSSLInterface -rname=nsp://localhost:8080 -adapter=0.0.0.0 -port=9090
  -alias=myAlias

Required arguments:
  rname :
    URL of the realm to which the realm node, on which the interface
    will be created, is connected.
  adapter :
    Adapter (network card) to which interface will bind.
  port :
    Port on which the interface will listen.

Optional Parameters:
  alias :
    Set the certificate name/alias that this interface will use to
    select its certificate from a keystore with multiple entries.
  keystore :
    Set the keystore file that this interface uses to load the
    certificate.
  kspassword :
    Set the keystore password that this interface will use to
    access the keystore file specified.
  truststore :
    Set the truststore file against which this interface will

```

```
validate the client certificate.
tspassword :
  Sets the truststore password that the server uses to access
  the trust store.
privatepassword :
  Private key password; used so that the key can be loaded
  from the key store.
ciphers :
  Names of the ciphers enabled for use by this interface,
  as a comma-separated list of ciphers, e.g. cipher1,cipher2,cipher3.
rndalg :
  Set the SecureRandom algorithm to use for this interface.
rndprov :
  Set the SecureRandom provider to use for this interface.
clientcertrequired :
  Whether this interface requires SSL client authentication.
crl :
  Set the certificate revocation list file name that the interface
  should use to check incoming SSL connections.
crlclassname :
  Name of the class used to validate a client connection.
provider :
  Name of the JSE provider to use for the interface.
autostart :
  Whether this interface will automatically be started when the
  realm server starts.
advertise :
  Set the current advertise status for this interface.
allowinterrealm :
  Whether this interface is allowed to be used in
  inter realm/cluster communication.
allowclientconnections :
  Whether this interface can accept client connections.
allownio :
  Whether NIO is enabled on the interface.
authtimeout :
  Set the number of milliseconds that the remote client has to
  authenticate with the server.
backlog :
  Set the number of connections to queue before the Operating System
  will send rejects to the remote client.
threads :
  Set the thread pool size handling the client connections.
selectthreads :
  Set the number of select threads used by NIO.
adapartialias :
  Set the interface's alias.
receivebuffersize :
  Set the socket buffer size in bytes used by this
  interface when receiving data.
sendbuffersize :
  Set the socket buffer size in bytes used by this interface
  when sending data.
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.
```

AddSocketInterface

```

Tool name:
  AddSocketInterface
Description:
  Adds a socket interface on the specified adapter and port,
  on the specified server.

Usage:
  runUMTool AddSocketInterface -rname=<rname> -adapter=<adapter> -port=<port>
  [optional_args]

Examples:
  AddSocketInterface -rname=nsp://localhost:8080 -adapter=0.0.0.0 -port=9090
  -autostart=true

Required arguments:
  rname :
    URL of the realm to which the realm node, on which the interface
    will be created, is connected.
  adapter :
    Adapter (network card) to which interface will bind.
  port :
    Port on which the interface will listen.

Optional Parameters:
  autostart :
    Whether this interface will automatically be started when the
    realm server starts.
  advertise :
    Set the current advertise status for this interface.
  allowinterrealm :
    Whether this interface is allowed to be used in
    inter realm/cluster communication.
  allowclientconnections :
    Whether this interface can accept client connections.
  allownio :
    Whether NIO is enabled on the interface.
  authtimeout :
    Set the number of milliseconds that the remote client has
    to authenticate with the server.
  backlog :
    Set the number of connections to queue before the Operating System
    will send rejects to the remote client.
  threads :
    Set the thread pool size handling the client connections.
  selectthreads :
    Set the number of select threads used by NIO.
  adapteralias :
    Set the interface's alias.
  receivebuffersize :
    Set the socket buffer size in bytes used by this
    interface when receiving data.
  sendbuffersize :
    Set the socket buffer size in bytes used by this interface
    when sending data.
  username :
    Your Universal Messaging server username.
  password :

```

Your Universal Messaging server password.

DeleteInterface

Tool name:
DeleteInterface

Description:
Deletes the specified interface from the specified server.

Usage:
runUMTool DeleteInterface -rname=<rname> -interface=<interface>
[optional_args]

Examples:
DeleteInterface -rname=nsp://localhost:8080 -interface=interface0

Required arguments:

- rname :
URL of the realm to which the realm node, from which the interface will be deleted, is connected.
- interface :
Name of the interface to be deleted.

Optional Parameters:

- username :
Your Universal Messaging server username.
- password :
Your Universal Messaging server password.

ListInterfaces

Tool name:
ListInterfaces

Description:
Lists details of the interfaces on the specified server.

Usage:
runUMTool ListInterfaces -rname=<rname> [optional_args]

Examples:
ListInterfaces -rname=nsp://localhost:9000

Required arguments:

- rname:
URL of the realm for which the details of all the interfaces will be listed.

Optional Parameters:

- format:
Format to print output in (plaintext/xml/json).

ModifyInterface

Tool name:
ModifyInterface

Description:
Modifies the specified interface on the specified server .

Usage:

```
runUMTool ModifyInterface -rname=<rname> -interface=<interface>
  -command=<command> [optional_args]
```

Examples:

```
ModifyInterface -rname=nsp://localhost:9000 -interface=interface0
  -command=modify -usewebsockets=true
```

Required arguments:

```
rname :
  URL of the realm to which the realm node, on which the interface
  will be modified, is connected.
interface :
  Name of the interface to be modified.
command :
  Whether the interface is to be stopped (STOP), started (START),
  or have its fields modified (MODIFY).
```

Optional Parameters:

```
usehttp1.1 :
  Whether to use HTTP1.1.
usewebsockets :
  Whether WebSockets are used.
ajaxactivedelay :
  Time to wait (for additional events) before delivering
  to Long Poll style subscribers.
ajaxidledelay :
  Time to wait before returning from a Long Poll call if no
  events have been received.
isnativecomet :
  Whether JavaScript is enabled on the interface.
allowedorigins :
  Set the Allowed Origins for CORS as a comma-separated list of origins
  (use '*' to allow all), e.g. origin1,origin2,origin3.
crossorigincredentials :
  Whether to allow credentials header to be sent with CORS requests.
enablegzip :
  Whether or not GZIP compression is enabled for javascript
  Long Poll connections.
minimumbytes :
  Set the minimum number of bytes in a packet before GZIP is
  enabled (default 1000).
alias :
  Set the certificate name/alias that this interface will use to
  select its certificate from a keystore with multiple entries.
keystore :
  Set the keystore file that this interface uses to load the certificate.
kspassword :
  Set the keystore password that this interface will use to
  access the keystore file specified.
truststore :
  Set the truststore file against which this interface will
  validate the client certificate.
tspassword :
  Sets the truststore password that the server uses to access
  the trust store.
privatepassword :
  Private key password; used so that the key can be loaded
  from the key store.
ciphers :
```

```
Names of the ciphers enabled for use by this interface,
as a comma-separated list of ciphers, e.g. cipher1,cipher2,cipher3.
rndalg :
  Set the SecureRandom algorithm to use for this interface.
rndprov :
  Set the SecureRandom provider to use for this interface.
clientcertrequired :
  Whether this interface requires SSL client authentication.
crl :
  Set the certificate revocation list file name that the interface
  should use to check incoming SSL connections.
crlclassname :
  Name of the class used to validate a client connection.
provider :
  Name of the JSSE provider to use for the interface.
autostart :
  Whether this interface will automatically be started when the
  realm server starts.
advertise :
  Set the current advertise status for this interface.
allowinterrealm :
  Whether this interface is allowed to be used in
  inter realm/cluster communication.
allowclientconnections :
  Whether this interface can accept client connections.
allownio :
  Whether NIO is enabled on the interface.
authtimeout :
  Set the number of milliseconds that the remote client has
  to authenticate with the server.
backlog :
  Set the number of connections to queue before the Operating System
  will send rejects to the remote client.
threads :
  Set the thread pool size handling the client connections.
selectthreads :
  Set the number of select threads used by NIO.
adaptersalias :
  Set the interface's alias.
receivebuffersize :
  Set the socket buffer size in bytes used by this
  interface when receiving data.
sendbuffersize :
  Set the socket buffer size in bytes used by this interface
  when sending data.
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.
```

Syntax: Data Group Tools

Important:

The data group and data stream functionality is deprecated.

AddDataGroup

```

Tool name:
  AddDataGroup
Description:
  Adds a child data group to a parent data group.
  Both of these data groups must exist.

Usage:
  runUMTool AddDataGroup -rname=<rname> -datagroupname=<datagroupname>
    -parentname=<parentname> [optional_args]

Examples:
  AddDataGroup -rname=nsp://localhost:9000 -datagroupname=mydatagroup01
    -parentname=mydatagroup02

Required arguments:
  rname :
    Connection URL to the realm where the data groups exist.
  datagroupname :
    Name of the child data group.
  parentname :
    Name of the parent data group.

Optional Parameters:
  username :
    Your Universal Messaging server username.
  password :
    Your Universal Messaging server password.

```

CreateDataGroup

```

Tool name:
  CreateDataGroup
Description:
  Creates a data group with the specified name on the specified server.
  Additionally, conflation attributes and other options of the data group
  can be set.

Usage:
  runUMTool CreateDataGroup -rname=<rname> -datagroupname=<datagroupname>
    [optional_args]

Examples:
  CreateDataGroup -rname=nsp://localhost:9000 -datagroupname=mydatagroup01
    -confinterval=2000 -enablemulticast=true

Required arguments:
  rname :
    Connection URL to the realm where the data group will be created.
  datagroupname :
    Name of the data group to be created.

Optional Parameters:
  enablemulticast :
    Whether multicast is supported on the new data group.
  priority :
    The default message priority for events on the new data group.

```

```
dropexpired :
  Don't send events that are made obsolete by newer ones.
confinterval :
  Interval at which all the events are sent.
confaction :
  Action to take when multiple events arrive for this data group.
  0 = drop old events
  1 = merge events
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.
```

DeleteDataGroup

```
Tool name:
  DeleteDataGroup
Description:
  Removes the data group with the specified name from the server.

Usage:
  runUMTool DeleteDataGroup -rname=<rname> -datagroupname=<datagroupname>
  [optional_args]

Examples:
  DeleteDataGroup -rname=nsp://localhost:9000 -datagroupname=mydatagroup01

Required arguments:
  rname :
    Connection URL to the realm from which the data group will be deleted.
  datagroupname :
    Name of the data group to be deleted.

Optional Parameters:
  username :
    Your Universal Messaging server username.
  password :
    Your Universal Messaging server password.
```

ListenDataGroup

```
Tool name:
  ListenDataGroup
Description:
  Listens for data group events on a Universal Messaging realm.

Usage:
  runUMTool ListenDataGroup -rname=<rname> [optional_args]

Examples:
  ListenDataGroup -rname=nsp://localhost:9000

Required arguments:
  rname :
    Connection URL to the realm from which messages will be received.

Optional Parameters:
  username :
```

```
Your Universal Messaging server username.
password :
Your Universal Messaging server password.
```

PublishDataGroup

```
Tool name:
  PublishDataGroup
Description:
  Publishes messages to a data group.

Usage:
  runUMTool PublishDataGroup -rname=<rname> -datagroupname=<datagroupname>
  [optional_args]

Examples:
  PublishDataGroup -rname=nsp://localhost:9000 -datagroupname=mydatagroup01
  -size=20

Required arguments:
  rname :
    Connection URL to the realm to which the messages will be published.
  datagroupname :
    Name of the data group to publish to.

Optional Parameters:
  message :
    Message to send. Put the message in quotes if it contains spaces.
    You can't use -size along with -message.
  size :
    Size of the message to send. Message will be generated.
    You can't use -message along with -size.
  count :
    How many times to send the event. Default 1.
  username :
    Your Universal Messaging server username.
  password :
    Your Universal Messaging server password.
```

Syntax: Publish Tools

PublishChannel

```
Tool name:
  PublishChannel
Description:
  Publishes events to a Universal Messaging channel.

Usage:
  runUMTool PublishChannel -rname=<rname> -channelname=<channelname>
  [optional_args]

Examples:
  PublishChannel -rname=nsp://localhost:9000 -channelname=mychannel
  -message="hello world"
```

Required arguments:

rtype :
Connection URL to the realm where the channel exists.
channelname :
Name of the channel on the Universal Messaging Realm.

Optional Parameters:

message :
Message to send. Put the message in quotes if it contains spaces.
You can't use -size along with -message.
count :
How many times to send the event. Default 1.
size :
Size in bytes of the message to send. Message will be generated.
You can't use -message along with -size.
properties :
Properties, if any, of the event. Expected syntax is
"propertyName1:value1;propertyName2:value2",
e.g. "shirt:green;price:80;sleeve:long".
username :
Your Universal Messaging server username.
password :
Your Universal Messaging server password.

PublishCompressed

Tool name:

PublishCompressed

Description:

Publishes events to a store, using compression.

Usage:

```
runUMTool PublishCompressed -rtype=<rtype> -storename=<storename>  
[optional_args]
```

Examples:

```
PublishCompressed -rtype=nsp://localhost:9000 -storename=mychannel  
-message="hello world"
```

Required arguments:

rtype :
Connection URL to the realm where the store exists.
storename :
Name of the store or queue on the Universal Messaging Realm.

Optional Parameters:

message :
Message to send. Put the message in quotes if it contains spaces.
You can't use -size along with -message.
count :
How many times to send the event. Default 1.
size :
Size in bytes of the message to send. Message will be generated.
You can't use -message along with -size.
username :
Your Universal Messaging server username.
password :
Your Universal Messaging server password.

PublishQueue

```

Tool name:
  PublishQueue
Description:
  Publishes events to a queue.

Usage:
  runUMTool PublishQueue -rname=<rname> -queuename=<queuename> [optional_args]

Examples:
  PublishQueue -rname=nsp://localhost:9000 -queuename=myqueue
    -message="hello world"

Required arguments:
  rname :
    Connection URL to the realm where the channel exists.
  queuename :
    Name of the queue on the Universal Messaging Realm.

Optional Parameters:
  message :
    Message to send. Put the message in quotes if it contains spaces.
    You can't use -size along with -message.
  count :
    How many times to send the event. Default 1.
  size :
    Size in bytes of the message to send. Message will be generated.
    You can't use -message along with -size.
  username :
    Your Universal Messaging server username.
  password :
    Your Universal Messaging server password.

```

PublishTX

```

Tool name:
  PublishTX
Description:
  Publishes events, as a part of a transaction, to a Universal Messaging
  channel or queue.

Usage:
  runUMTool PublishTX -rname=<rname> -storename=<storename> [optional_args]

Examples:
  PublishTX -rname=nsp://localhost:9000 -storename=myStore
    -message="hello world" -count=20 -txsize=5
  PublishTX -rname=nsp://localhost:9000 -storename=myStore -size=2048

Required arguments:
  rname :
    Connection URL to the realm where the channel exists.
  storename :
    Name of the channel or queue on the Universal Messaging Realm.

Optional Parameters:
  message :

```

```
Message to send. Put the message in quotes if it contains spaces.
You can't use -size along with -message.
count :
  How many times to send the event. Default 1.
size :
  Size in bytes of the message to send. Message will be generated.
  You can't use -message along with -size.
txsize :
  How many events to batch in a single transaction. Default 1.
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.
```

Syntax: Subscribe Tools

PeekQueue

```
Tool name:
  PeekQueue
Description:
  Peeks all events on a Universal Messaging queue and prints statistics for
  the bandwidth rates.
Usage:
  runUMTool PeekQueue -rname=<rname> -queuename=<queuename> [optional_args]
Examples:
  PeekQueue -rname=nsp://localhost:9000 -queuename=myqueue
Required arguments:
  rname :
    Connection URL to the realm where the channel exists.
  queuename :
    Name of a queue on the Universal Messaging Realm.
Optional Parameters:
  selector :
    Optional filter for the messages.
  statevents :
    How many events to peek before printing event statistics.
    Default 1000.
  username :
    Your Universal Messaging server username.
  password :
    Your Universal Messaging server password.
```

SubscribeChannel

```
Tool name:
  SubscribeChannel
Description:
  Reads all the messages from a Universal Messaging channel.
Usage:
```

```
runUMTool SubscribeChannel -rname=<rname> -channelname=<channelname>
[optional_args]
```

Examples:

```
SubscribeChannel -rname=nsp://localhost:9000 -channelname=channel
```

Required arguments:

```
rname :
    Connection URL to the realm where the channel exists.
channelname :
    Name of a channel on the Universal Messaging Realm.
```

Optional Parameters:

```
selector :
    Optional filter for the messages.
starteid :
    Starting EID of the messages to consume.
statevents :
    How many events to peek before printing event statistics.
    Default 1000.
username :
    Your Universal Messaging server username.
password :
    Your Universal Messaging server password.
```

SubscribeChannelAsync

Tool name:

```
SubscribeChannelAsync
```

Description:

```
Listens for messages on a Universal Messaging channel.
```

Usage:

```
runUMTool SubscribeChannelAsync -rname=<rname> -channelname=<channelname>
[optional_args]
```

Examples:

```
SubscribeChannelAsync -rname=nsp://localhost:9000 -channelname=channel
```

Required arguments:

```
rname :
    Connection URL to the realm where the channel exists.
channelname :
    Name of a channel on the Universal Messaging Realm.
```

Optional Parameters:

```
selector :
    Optional filter for the messages.
starteid :
    Start event ID of the messages to consume.
statevents :
    How many events to peek before printing event statistics.
    Default 1000.
username :
    Your Universal Messaging server username.
password :
    Your Universal Messaging server password.
```

SubscribeChannelAsyncDurable

```
Tool name:
  SubscribeChannelAsyncDurable
Description:
  Listens for messages on a Universal Messaging channel.
  Running the tool with the same "-name" argument will continue reading
  from the last unconsumed event.

Usage:
  runUMTool SubscribeChannelAsyncDurable -rname=<rname>
    -channelname=<channelname> [optional_args]

Examples:
  SubscribeChannelAsyncDurable -rname=nsp://localhost:9000 -channelname=channel

Required arguments:
  rname :
    Connection URL to the realm where the channel exists.
  channelname :
    Name of a channel on the Universal Messaging Realm.

Optional Parameters:
  selector :
    Optional filter for the messages.
  name :
    Unique name of the durable subscriber. The name will be created
    if it doesn't exist. Default is "STGE".
  starteid :
    Start EID of the messages to consume.
  clusterwide :
    Whether the durable name should be registered in the entire
    cluster. Default is false.
  autoack :
    Whether each event will be automatically acknowledged by the API.
    Default is true.
  statevents :
    How many events to peek before printing event statistics.
    Default 1000.
  username :
    Your Universal Messaging server username.
  password :
    Your Universal Messaging server password.
```

SubscribeChannelDurable

```
Tool name:
  SubscribeChannelDurable
Description:
  Listens for messages on a Universal Messaging channel.
  Running the tool with the same "-name" argument will continue reading
  from the last unconsumed event.

Usage:
  runUMTool SubscribeChannelDurable -rname=<rname> -channelname=<channelname>
    [optional_args]

Examples:
```

```
SubscribeChannelDurable -rname=nsp://localhost:9000 -channelname=channel
```

Required arguments:

rname :
Connection URL to the realm where the channel exists.
channelname :
Name of a channel on the Universal Messaging Realm.

Optional Parameters:

selector :
Optional filter for the messages.
name :
Unique name of the durable subscriber. The name will be created if it doesn't exist. Default is "STGE".
starteid :
Start event ID of the messages to consume.
clusterwide :
Whether the durable name should be registered in the entire cluster. Default is false.
autoack :
Whether each event will be automatically acknowledged by the API. Default is true.
statevents :
How many events to peek before printing event statistics. Default 1000.
timeout :
Maximum wait time (milliseconds) when attempting to synchronously retrieve message from the server. Default is 1000ms.
username :
Your Universal Messaging server username.
password :
Your Universal Messaging server password.

SubscribeCompressed

Tool name:

SubscribeCompressed

Description:

Listens for compressed messages on a Universal Messaging channel.

Usage:

```
runUMTool SubscribeCompressed -rname=<rname> -storename=<storename>
[optional_args]
```

Examples:

```
SubscribeCompressed -rname=nsp://localhost:9000 -storename=channel
```

Required arguments:

rname :
Connection URL to the realm where the channel exists.
storename :
Name of a channel or queue on the Universal Messaging Realm.

Optional Parameters:

selector :
Optional filter for the messages.
starteid :
If the chosen store is a channel, only messages with ID greater than this will be consumed.

```
statevents :
  How many events to peek before printing event statistics.
  Default 1000.
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.
```

SubscribeQueue

```
Tool name:
  SubscribeQueue
Description:
  Reads all the messages from a Universal Messaging queue.

Usage:
  runUMTool SubscribeQueue -rname=<rname> -queuename=<queuename> [optional_args]

Examples:
  SubscribeQueue -rname=nsp://localhost:9000 -queuename=myqueue

Required arguments:
  rname :
    Connection URL to the realm where the channel exists.
  queuename :
    Name of a queue on the Universal Messaging Realm.

Optional Parameters:
  selector :
    Optional filter for the messages.
  transacted :
    Set to true to use transacted subscriber. Default is false.
  statevents :
    How many events to peek before printing event statistics.
    Default 1000.
  username :
    Your Universal Messaging server username.
  password :
    Your Universal Messaging server password.
```

SubscribeQueueAsync

```
Tool name:
  SubscribeQueueAsync
Description:
  Listens for messages on a Universal Messaging queue.

Usage:
  runUMTool SubscribeQueueAsync -rname=<rname> -queuename=<queuename>
  [optional_args]

Examples:
  SubscribeQueueAsync -rname=nsp://localhost:9000 -queuename=myqueue

Required arguments:
  rname :
    Connection URL to the realm where the channel exists.
  queuename :
```

Name of a queue on the Universal Messaging Realm.

Optional Parameters:

selector :
Optional filter for the messages.

transacted :
Set to true to use transacted subscriber. Default is false.

statevents :
How many events to peek before printing event statistics.
Default 1000.

username :
Your Universal Messaging server username.

password :
Your Universal Messaging server password.

Syntax: Security Tools

AddChannelACLEntry

Tool name:

AddChannelACLEntry

Description:

Adds an ACL entry on the specified channel for the specified user and host, on the specified realm.

Usage:

```
runUMTool AddChannelACLEntry -channelname=<channelname> -rname=<rname>
  -type=<type> [optional_args]
```

Examples:

```
AddChannelACLEntry -rname=nsp://localhost:8080 -channelname=channel0
  -type=group -groupname=security_group0 -fullprivileges=true
AddChannelACLEntry -rname=nsp://localhost:8080 -channelname=channel0
  -type=subject -user=username -host=127.0.0.1 -fullprivileges=true
```

Required arguments:

channelname :
Name of the channel to which the ACL entry is being applied.

rname :
URL of the server on which the channel exists.

type :
Type of ACL entry, either 'group' or 'subject'. If group is chosen, 'groupname' must be set. Otherwise 'user' and 'host' must be set.

Optional Parameters:

groupname :
Name of the group for which ACL is being updated.

user :
User for which ACL is being updated.

host :
Host for which ACL is being updated.

canlistacl :
Specify that the 'list' ACL permission should be added.

canmodifyacl :
Specify that the 'modify' ACL permission should be added.

fullprivileges :
Specify that the 'full permissions' ACL permission should be added.

```

cangetlasteid :
  Specify that the 'get last EID' ACL permission should be added.
canread :
  Specify that the 'read' ACL permission should be added.
canwrite :
  Specify that the 'write' ACL permission should be added.
canpurge :
  Specify that the 'purge' ACL permission should be added.
cannamed :
  Specify that the 'named' ACL permission should be added.
canpop :
  Specify that the 'pop' ACL permission should be added.
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.

```

AddContainerACLEntry

```

Tool name:
  AddContainerACLEntry
Description:
  Adds an ACL entry on the specified container for the specified user and host.

Usage:
  runUMTool AddContainerACLEntry -containername=<containername> -rname=<rname>
  -type=<type> [optional_args]

Examples:
  AddContainerACLEntry -rname=nsp://localhost:8080 -containername=container0
  -type=group -groupname=security_group0 -fullprivileges=true

  AddContainerACLEntry -rname=nsp://localhost:8080 -containername=container0
  -type=subject -user=username -host=127.0.0.1 -fullprivileges=true

Required arguments:
  containername :
    Name of the container to which the ACL entry is being applied.
  rname :
    URL of the server from which to start searching for the container.
  type :
    Type of ACL entry, either 'group' or 'subject'. If group is chosen,
    'groupname' must be set. Otherwise 'user' and 'host' must be set.

Optional Parameters:
  groupname :
    Name of the group for which ACL is being updated.
  user :
    User for which ACL is being updated.
  host :
    Host for which ACL is being updated.
  canlistacl :
    Specify that the 'list' ACL permission should be added.
  canmodifyacl :
    Specify that the 'modify' ACL permission should be added.
  fullprivileges :
    Specify that the 'full permissions' ACL permission should be added.
  cangetlasteid :
    Specify that the 'get last EID' ACL permission should be added.

```

```

canread :
    Specify that the 'read' ACL permission should be added.
canwrite :
    Specify that the 'write' ACL permission should be added.
canpurge :
    Specify that the 'purge' ACL permission should be added.
cannamed :
    Specify that the 'named' ACL permission should be added.
canpop :
    Specify that the 'pop' ACL permission should be added.
username :
    Your Universal Messaging server username.
password :
    Your Universal Messaging server password.

```

AddQueueACLEntry

```

Tool name:
    AddQueueACLEntry
Description:
    Adds an ACL entry on the specified queue for the specified user and host,
    on the specified realm.
Usage:
    runUMTool AddQueueACLEntry -queueName=<queueName> -rname=<rname> -type=<type>
    [optional_args]
Examples:
    AddQueueACLEntry -rname=nsp://localhost:8080 -queueName=queue0 -type=group
    -groupName=security_group0 -fullprivileges=true
    AddQueueACLEntry -rname=nsp://localhost:8080 -queueName=queue0 -type=subject
    -user=username -host=127.0.0.1 -fullprivileges=true
Required arguments:
    queueName :
        Name of the queue to which the ACL entry is being applied.
    rname :
        URL of the server on which the queue exists.
    type :
        Type of ACL entry, either 'group' or 'subject'. If group is chosen,
        'groupName' must be set. Otherwise 'user' and 'host' must be set.
Optional Parameters:
    groupName :
        Name of the group for which ACL is being updated.
    user :
        User for which ACL is being updated.
    host :
        Host for which ACL is being updated.
    canlistacl :
        Specify that the 'list' ACL permission should be added.
    canmodifyacl :
        Specify that the 'modify' ACL permission should be added.
    fullprivileges :
        Specify that the 'full permissions' ACL permission should
        be added.
    canread :
        Specify that the 'read' ACL permission should be added.
    canwrite :

```

```
Specify that the 'write' ACL permission should be added.
canpurge :
Specify that the 'purge' ACL permission should be added.
canpop :
Specify that the 'pop' ACL permission should be added.
username :
Your Universal Messaging server username.
password :
Your Universal Messaging server password.
```

AddRealmACLEntry

```
Tool name:
AddRealmACLEntry
Description:
Adds an ACL entry on the specified realm for the specified user and host.

Usage:
runUMTool AddRealmACLEntry -rname=<rname> -type=<type> [optional_args]

Examples:
AddRealmACLEntry -rname=nsp://localhost:8080 -type=group
  -groupname=security_group0 -fullprivileges=true
AddRealmACLEntry -rname=nsp://localhost:8080 -type=subject -user=username
  -host=127.0.0.1 -fullprivileges=true

Required arguments:

rname :
URL of the realm to which the ACL entry is being applied.
type :
Type of ACL entry, either 'group' or 'subject'. If group is chosen,
'groupname' must be set. Otherwise 'user' and 'host' must be set.

Optional Parameters:
groupname :
Name of the group for which ACL is being updated.
user :
User for which ACL is being updated.
host :
Host for which ACL is being updated.
canlistacl :
Specify that the 'list' ACL permission should be added.
canmodifyacl :
Specify that the 'modify' ACL permission should be added.
fullprivileges :
Specify that the 'full permissions' ACL permission should be added.
canuseadminapi :
Specify that the 'use admin api' ACL permission should be added.
canmanagerealm :
Specify that the 'manage realms' ACL permission should be added.
canmanagejoins :
Specify that the 'manage joins' ACL permission should be added.
canmanagechannels :
Specify that the 'manage channels' ACL permission should be added.
canaccess :
Specify that the 'access' ACL permission should be added.
canoverrideconnectioncount :
Specify that the 'override connection count' ACL permission should be added.
```

```

canconfigure :
  Specify that the 'configuration' ACL permission should be added.
canmanagedatagroups :
  Specify that the 'manage data groups' ACL permission should be added.
canpublishglobaldatagroups :
  Specify that the 'publish global data groups' ACL permission should
  be added.
cantakeownershipdatagroups :
  Specify that the 'take ownership of data groups' ACL permission should
  be added.
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.

```

AddSecurityGroup

```

Tool name:
  AddSecurityGroup
Description:
  Adds a security group to the specified realm with the specified name.

Usage:
  runUMTool AddSecurityGroup -rname=<rname> -groupname=<groupname> [optional_args]

Examples:

  AddSecurityGroup -rname=nsp://localhost:8080 -groupname=security_group0

Required arguments:
  rname :
    URL of the realm to which the security group is being added.
  groupname :
    Name of the security group to be added.

Optional Parameters:
  username :
    Your Universal Messaging server username.
  password :
    Your Universal Messaging server password.

```

AddUserToSecurityGroup

```

Tool name:
  AddUserToSecurityGroup
Description:
  Adds a specified user and host subject to a given security group on a
  specified realm.

Usage:
  runUMTool AddUserToSecurityGroup -rname=<rname> -groupname=<groupname>
  -user=<user> -host=<host> [optional_args]

Examples:

  AddUserToSecurityGroup -rname=nsp://localhost:8080 -groupname=security_group0
  -user=username -host=127.0.0.1

```

Required arguments:

 rname :
 URL of the realm on which is the security group.
 groupname :
 Name of the security group to which the user is being added.
 user :
 User of the subject being added to security group.
 host :
 Host of the subject being added to security group.

Optional Parameters:

 username :
 Your Universal Messaging server username.
 password :
 Your Universal Messaging server password.

DeleteChannelACLEntry

Tool name:

DeleteChannelACLEntry

Description:

Deletes the ACL entry from the specified channel with the specified user and host.

Usage:

```
runUMTool DeleteChannelACLEntry -channelname=<channelname> -rname=<rname>  
    -type=<type> [optional_args]
```

Examples:

```
DeleteChannelACLEntry -rname=nsp://localhost:8080 -channelname=channel0  
    -type=group -groupname=security_group0  
DeleteChannelACLEntry -rname=nsp://localhost:8080 -channelname=channel0  
    -type=subject -user=username -host=127.0.0.1
```

Required arguments:

 channelname :
 Name of the channel from which the ACL entry is being removed.
 rname :
 URL of the server on which the channel exists.
 type :
 Type of ACL entry, either 'group' or 'subject'. If group is chosen,
 'groupname' must be set. Otherwise 'user' and 'host' must be set.

Optional Parameters:

 groupname :
 Name of the group for which the ACL entry is being removed.
 user :
 User for which the ACL entry is being removed.
 host :
 Host for which the ACL entry is being removed.
 username :
 Your Universal Messaging server username.
 password :
 Your Universal Messaging server password.

DeleteContainerACLEntry

```

Tool name:
  DeleteContainerACLEntry
Description:
  Removes an ACL entry from the specified container with the specified user
  and host.

Usage:
  runUMTool DeleteContainerACLEntry -containername=<containername> -rname=<rname>
  -type=<type> [optional_args]

Examples:
  DeleteContainerACLEntry -rname=nsp://localhost:8080 -containername=container0
  -type=group -groupname=security_group0
  DeleteContainerACLEntry -rname=nsp://localhost:8080 -containername=container0
  -type=subject -user=username -host=127.0.0.1

Required arguments:
  containername :
    Name of the container from which the ACL entry is being removed.
  rname :
    URL of the server from which to start searching for the container.
  type :
    Type of ACL entry, either 'group' or 'subject'. If group is chosen,
    'groupname' must be set. Otherwise 'user' and 'host' must be set.

Optional Parameters:
  groupname :
    Name of the group for which the ACL entry is being removed.
  user :
    User for which the ACL entry is being removed.
  host :
    Host for which the ACL entry is being removed.
  username :
    Your Universal Messaging server username.
  password :
    Your Universal Messaging server password.

```

DeleteQueueACLEntry

```

Tool name:
  DeleteQueueACLEntry
Description:
  Deletes the ACL entry from the specified queue with the specified user and host.

Usage:
  runUMTool DeleteQueueACLEntry -queuename=<queuename> -rname=<rname>
  -type=<type> [optional_args]

Examples:
  DeleteQueueACLEntry -rname=nsp://localhost:8080 -queuename=queue0
  -type=group -groupname=security_group0
  DeleteQueueACLEntry -rname=nsp://localhost:8080 -queuename=queue0
  -type=subject -user=username -host=127.0.0.1

Required arguments:
  queuename :

```

```
Name of the queue from which the ACL entry is being removed.
rname :
  URL of the server on which the queue exists.
type :
  Type of ACL entry, either 'group' or 'subject'. If group is chosen,
  'groupname' must be set. Otherwise 'user' and 'host' must be set.
```

Optional Parameters:

```
groupname :
  Name of the group for which the ACL entry is being removed.
user :
  User for which the ACL entry is being removed.
host :
  Host for which the ACL entry is being removed.
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.
```

DeleteRealmACLEntry

```
Tool name:
  DeleteRealmACLEntry
Description:
  Removes an ACL entry from the specified realm with the specified user and host.
```

Usage:

```
runUMTool DeleteRealmACLEntry -rname=<rname> -type=<type> [optional_args]
```

Examples:

```
DeleteRealmACLEntry -rname=nsp://localhost:8080 -type=group
  -groupname=security_group0
DeleteRealmACLEntry -rname=nsp://localhost:8080 -type=subject -user=username
  -host=127.0.0.1
```

Required arguments:

```
rname :
  URL of the realm from which the ACL entry is being removed.
type :
  Type of ACL entry, either 'group' or 'subject'. If group is chosen,
  'groupname' must be set. Otherwise 'user' and 'host' must be set.
```

Optional Parameters:

```
groupname :
  Name of the group for which the ACL entry is being removed.
user :
  User for which the ACL entry is being removed.
host :
  Host for which the ACL entry is being removed.
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.
```

DeleteSecurityGroup

```
Tool name:
  DeleteSecurityGroup
```

Description:
Removes a security group from the specified realm with the specified name.

Usage:
runUMTool DeleteSecurityGroup -rname=<rname> -groupname=<groupname>
[optional_args]

Examples:
DeleteSecurityGroup -rname=nsp://localhost:8080 -groupname=security_group

Required arguments:
rname :
URL of the realm from which the security group is being removed.
groupname :
Name of the security group to be removed.

Optional Parameters:
username :
Your Universal Messaging server username.
password :
Your Universal Messaging server password.

DumpACL

Tool name:
DumpACL

Description:
Dumps all the ACL data for a realm.

Usage:
runUMTool DumpACL -rname=<rname> [optional_args]

Examples:
DumpACL -rname=nsp://localhost:8080
DumpACL -rname=nsp://localhost:8080 -format=XML
DumpACL -rname=nsp://localhost:8080 -format=JSON

Required arguments:
rname :
URL of the realm for which to dump the ACL data.

Optional Parameters:
format :
Which format to output ACL data. Defaults to plaintext, other options are: plaintext, xml, json.
username :
Your Universal Messaging server username.
password :
Your Universal Messaging server password.

ModifyChannelACLEntry

Tool name:
ModifyChannelACLEntry

Description:
Updates an ACL entry on the specified channel for the specified user and host, on the specified realm.

Usage:

```
runUMTool ModifyChannelACLEntry -channelname=<channelname> -rname=<rname>
  -type=<type> [optional_args]
```

Examples:

```
ModifyChannelACLEntry -rname=nsp://localhost:8080 -channelname=channel0
  -type=group -groupname=security_group0 -fullprivileges=true
ModifyChannelACLEntry -rname=nsp://localhost:8080 -channelname=channel0
  -type=subject -user=username -host=127.0.0.1 -fullprivileges=true
```

Required arguments:

```
channelname :
  Name of the channel on which the ACL entry is being updated.
rname :
  URL of the server on which the channel exists.
type :
  Type of ACL entry, either 'group' or 'subject'. If group is chosen,
  'groupname' must be set. Otherwise 'user' and 'host' must be set.
```

Optional Parameters:

```
groupname :
  Name of the group for which ACL is being updated.
user :
  User for which ACL is being updated.
host :
  Host for which ACL is being updated.
canlistacl :
  Specify that the 'list' ACL permission should be added.
canmodifyacl :
  Specify that the 'modify' ACL permission should be added.
fullprivileges :
  Specify that the 'full permissions' ACL permission should be added.
cangetlasteid :
  Specify that the 'get last EID' ACL permission should be added.
canread :
  Specify that the 'read' ACL permission should be added.
canwrite :
  Specify that the 'write' ACL permission should be added.
canpurge :
  Specify that the 'purge' ACL permission should be added.
cannamed :
  Specify that the 'named' ACL permission should be added.
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.
```

ModifyContainerACLEntry

Tool name:

```
ModifyContainerACLEntry
```

Description:

```
AddContainerACLEntry adds an ACL entry on the specified container for the
specified user and host.
```

Usage:

```
runUMTool ModifyContainerACLEntry -containername=<containername> -rname=<rname>
  -type=<type> [optional_args]
```

Examples:

```
ModifyContainerACLEntry -rname=nsp://localhost:8080 -containername=container0
  -type=group -groupname=security_group0 -fullprivileges=true
ModifyContainerACLEntry -rname=nsp://localhost:8080 -containername=container0
  -type=subject -user=username -host=127.0.0.1 -fullprivileges=true
```

Required arguments:

```
containername :
  Name of the container to which the ACL entry is being applied.
rname :
  URL of the server from which to start searching for the container.
type :
  Type of ACL entry, either 'group' or 'subject'. If group is chosen,
  'groupname' must be set. Otherwise 'user' and 'host' must be set.
```

Optional Parameters:

```
groupname :
  Name of the group for which ACL is being updated.
user :
  User for which ACL is being updated.
host :
  Host for which ACL is being updated.
canlistacl :
  Specify that the 'list' ACL permission should be added.
canmodifyacl :
  Specify that the 'modify' ACL permission should be added.
fullprivileges :
  Specify that the 'full permissions' ACL permission should be added.
cangetlasteid :
  Specify that the 'get last EID' ACL permission should be added.
canread :
  Specify that the 'read' ACL permission should be added.
canwrite :
  Specify that the 'write' ACL permission should be added.
canpurge :
  Specify that the 'purge' ACL permission should be added.
cannamed :
  Specify that the 'named' ACL permission should be added.
canpop :
  Specify that the 'pop' ACL permission should be added.
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.
```

ModifyQueueACLEntry**Tool name:**

```
ModifyQueueACLEntry
```

Description:

```
Updates an ACL entry on the specified queue for the specified user and host,
on the specified realm.
```

Usage:

```
runUMTool ModifyQueueACLEntry -queueaname=<queueaname> -rname=<rname> -type=<type>
  [optional_args]
```

Examples:

```
ModifyQueueACLEntry -rname=nsp://localhost:8080 -queueaname=queue0 -type=group
```

```
-groupname=security_group0 -fullprivileges=true
ModifyQueueACLEntry -rname=nsp://localhost:8080 -queuename=queue0 -type=subject
-user=username -host=127.0.0.1 -fullprivileges=true
```

Required arguments:

```
queuename :
  Name of the queue on which the ACL entry is being updated.
rname :
  URL of the server on which the queue exists.
type :
  Type of ACL entry, either 'group' or 'subject'. If group is chosen,
  'groupname' must be set. Otherwise 'user' and 'host' must be set.
```

Optional Parameters:

```
groupname :
  Name of the group for which ACL is being updated.
user :
  User for which ACL is being updated.
host :
  Host for which ACL is being updated.
canlistacl :
  Specify that the 'list' ACL permission should be added.
canmodifyacl :
  Specify that the 'modify' ACL permission should be added.
fullprivileges :
  Specify that the 'full permissions' ACL permission should be added.
canread :
  Specify that the 'read' ACL permission should be added.
canwrite :
  Specify that the 'write' ACL permission should be added.
canpurge :
  Specify that the 'purge' ACL permission should be added.
canpop :
  Specify that the 'pop' ACL permission should be added.
username :
  Your Universal Messaging server username.
password : Your Universal Messaging server password.
```

ModifyRealmACLEntry

Tool name:

```
ModifyRealmACLEntry
```

Description:

```
Modifies an ACL entry on the specified realm for the specified user and host.
```

Usage:

```
runUMTool ModifyRealmACLEntry -rname=<rname> -type=<type> [optional_args]
```

Examples:

```
ModifyRealmACLEntry -rname=nsp://localhost:8080 -type=group
  -groupname=security_group0 -fullprivileges=true
ModifyRealmACLEntry -rname=nsp://localhost:8080 -type=subject -user=username
  -host=127.0.0.1 -fullprivileges=true
```

Required arguments:

```
rname :
  URL of the realm on which ACL is being updated.
type :
  Type of ACL entry, either 'group' or 'subject'. If group is chosen,
```

'groupname' must be set. Otherwise 'user' and 'host' must be set.

Optional Parameters:

```

groupname :
    Name of the group for which ACL is being updated.
user :
    User for which ACL is being updated.
host :
    Host for which ACL is being updated.
canlistacl :
    Specify that the 'list' ACL permission should be added.
canmodifyacl :
    Specify that the 'modify' ACL permission should be added.

fullprivileges :
    Specify that the 'full permissions' ACL permission should be added.
canuseadminapi :
    Specify that the 'use admin api' ACL permission should be added.
canmanagerealms :
    Specify that the 'manage realms' ACL permission should be added.
canmanagejoins :
    Specify that the 'manage joins' ACL permission should be added.
canmanagechannels :
    Specify that the 'manage channels' ACL permission should be added.
canaccess :
    Specify that the 'access' ACL permission should be added.
canoverrideconnectioncount :
    Specify that the 'override connection count' ACL permission should be added.
canconfigure :
    Specify that the 'configuration' ACL permission should be added.
canmanagedatagroups :
    Specify that the 'manage data groups' ACL permission should be added.
canpublishglobaldatagroups :
    Specify that the 'publish global data groups' ACL permission should be added.
cantakeownershipdatagroups :
    Specify that the 'take ownership of data groups' ACL permission should be added.

username :
    Your Universal Messaging server username.
password :
    Your Universal Messaging server password.

```

RemoveUserFromSecurityGroup

```

Tool name:
    RemoveUserFromSecurityGroup
Description:
    Removes a specified user from a given security group on the specified realm.

Usage:
    runUMTool RemoveUserFromSecurityGroup -rname=<rname> -groupname=<groupname>
    -user=<user> -host=<host> [optional_args]

Examples:
    RemoveUserFromSecurityGroup -rname=nsp://localhost:8080
    -groupname=security_group0 -user=username -host=127.0.0.1

Required arguments:
    rname :

```

```
URL of the realm on which the security group resides.  
groupname :  
  Name of the security group user is being removed from.  
user :  
  User being removed from security group.  
host :  
  Host of subject being removed from security group.
```

Optional Parameters:

```
username :  
  Your Universal Messaging server username.  
password :  
  Your Universal Messaging server password.
```

Syntax: Zone Tools

AddMemberToZone

```
Tool name:  
  AddMemberToZone  
Description:  
  Adds a realm to a specified realm's zone.  
  
Usage:  
  runUMTool AddMemberToZone -rname=<rname> -zonememberrname=<zonememberrname>  
  [optional_args]  
  
Examples:  
  AddMemberToZone -rname=nsp://localhost:8080 -zonememberrname=nsp://localhost:9090  
  
Required arguments:  
  rname :  
    URL of the realm you want to add to the zone.  
  zonememberrname :  
    URL of a realm in the zone you want to expand.  
  
Optional Parameters:  
  username :  
    Your Universal Messaging server username.  
  password :  
    Your Universal Messaging server password.
```

CreateZone

```
Tool name:  
  CreateZone  
Description:  
  Creates a zone with the specified name containing the specified realms.  
  
Usage:  
  runUMTool CreateZone -rnames=<rnames> -zonename=<zonename> [optional_args]  
  
Examples:  
  CreateZone -rnames=nsp://localhost:8080,nsp://localhost:9090 -zonename=zone0  
  
Required arguments:
```

```

rnames :
  Comma separated list of URLs of the realms which the zone will contain.
zonename :
  Name of the zone to be created.

Optional Parameters:
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.

```

DeleteZone

```

Tool name:
  DeleteZone
Description:
  Deletes a zone with the specified name on the specified realm.

Usage:
  runUMTool DeleteZone -rname=<rname> [optional_args]

Examples:
  DeleteZone -rname=nsp://localhost:8080
  DeleteZone -rname=nsp://localhost:8080 -removejoins=true

Required arguments:
  rname :
    URL of a realm which belongs to the zone to be deleted.

Optional Parameters:
  removejoins :
    Whether to remove intra-zone connections when the zone
    is deleted. Defaults to false.
  username :
    Your Universal Messaging server username.
  password :
    Your Universal Messaging server password.

```

RemoveMemberFromZone

```

Tool name:
  RemoveMemberFromZone
Description:
  Removes a realm from its current zone.

Usage:
  runUMTool RemoveMemberFromZone -rname=<rname> [optional_args]

Examples:
  RemoveMemberFromZone -rname=nsp://localhost:8080
  RemoveMemberFromZone -rname=nsp://localhost:8080 -removejoins=true

Required arguments:
  rname :
    URL of the realm you want to remove from the zone.

Optional Parameters:
  removejoins :

```

```

Whether or not to remove realm links with the former zone member.
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.

```

Syntax: JMS Tools

Note:

The JMS Client for Universal Messaging supports JMS 1.1. The client does not support JMS 2.0.

CreateConnectionFactory

```

Tool name:
  CreateConnectionFactory
Description:
  Creates a JMS connection factory with the specified server.

Usage:
  runUMTool CreateConnectionFactory -rname=<rname> -factoryname=<factoryname>
  [optional_args]

Examples:
  CreateConnectionFactory -rname=nsp://localhost:9000 -factoryname=factory0
  Connects to a Universal Messaging server at nsp://localhost:9000 and creates
  a connection factory named 'factory0' that uses the nsp://localhost:9000 connection
  URL.
  CreateConnectionFactory -rname=nsp://localhost:9000 -connectionurl=nsp://SomeFQDN:9000
  -factoryname=factory0
  Connects to a Universal Messaging server at nsp://localhost:9000 and creates a
  connection
  factory named 'factory0' that uses the nsp://SomeFQDN:9000 connection URL.

Required arguments:
  rname :
    The URL of the Universal Messaging server on which to create the connection factory.
    The -rname is used as a connection factory URL unless the -connectionurl parameter
    is specified.
  factoryname :
    Name of the connection factory to create.

Optional parameters:

  connectionurl :
    The URL that the connection factory uses to connect to the JMS provider.
    If -connectionurl is not specified, the connection factory uses the URL specified
    in the -rname argument.
  factorytype :
    Connection factory type to be created. The default is ConnectionFactory,
    if no parameter is passed.
    Values are:
    -factorytype=default (Creates a ConnectionFactory)
    -factorytype=queue (Creates a QueueConnectionFactory)
    -factorytype=topic (Creates a TopicConnectionFactory)
    -factorytype=xa (Creates an XAConnectionFactory)

  contextfactory :
    The name of the ContextFactory class to use

```

```

(default: com.pcbsys.nirvana.nSpace.NirvanaContextFactory).
When using an AMQP connection this should be changed to:
org.apache.qpid.jms.jndi.JmsInitialContextFactory
to use the QPID Proton JMS Client libraries;
Hint: AMQP connections work only over nsp and nsp interfaces, they do not
work over nhp or nhps.
autocreateresource :
Creates resources on the server when performing a lookup
on a queue or channel.
synctopicacks :
Specifies for a specific connection whether the topic acknowledgements
are sent synchronously.
syncqueueacks :
Specifies for a specific connection whether the queue acknowledgements
are sent synchronously.
writehandler :
Specifies for a specific connection the write handler type to use.
Ignored unless between 1-4.
adapterbuffer :
Specifies for a specific connection the adapter send / receive buffer size.
If the value is 0 or less it is ignored .
syncnamedtopicacks :
Specifies for a specific connection whether the durable topic
acknowledgements will be sent synchronously.
permittedkeepalivesmissed :
Set the number of keep server keep alives the client is allowed to miss
before detecting a network issue and terminating the connection.
connectiontimeout :
Set the timeout used for connection / reconnection to realms.
If the connection fails to establish within this time-frame it will fail.
disconnectafterclusterfailure :
If connected to a cluster of realms, and cluster quorum is lost,
this flag determines whether the client will be disconnected.
usejmsengine :
JMS engine ensures no events are available for topic replay
unless durable subscriptions are being used. Non JMS engine fanout enables
events to be stored even after events are delivered. Default is true.
reconnectinterval :
If a client is disconnected, and Immediate Reconnect is set to true,
this value represents the interval between reconnect attempts.
immediatereconnect :
If a client is disconnected, this flag will indicate whether the client
will immediately reconnect and attempt to reconnect as fast as possible,
rather than rely on a back off period.
autoreconnectafteracl :
If a client is disconnected because of a security change, this flag
will indicate whether the automatic session reconnection logic will kick in.
threadpoolsize :
Gets the maximum number of threads used by the client for delivery of
all messages to listeners.
redeliveredsize :
Specifies the maximum number of messages that the client will keep
reference to if they are marked as redelivered.
unackedsize :
The client will keep a list of messages that have not been
acknowledged. This value sets the maximum size of this list.
useinfinitewindowsize :
When set to true, the consumer can consume as many events as required
before committing.
windowsize :

```

When asynchronously consuming messages from the server, they will be delivered in batches (windows). This property sets the size of that window.
autoackcount :

With AUTO acknowledgement mode, in order to improve performance, the acknowledgement of messages can be batched so that not every message consumed results in communication with the server. This value determines how many events can be consumed before an acknowledgement is sent to the server.

globalstorecapacity :

Each topic or queue store can have a maximum number of messages that can exist before no more messages are allowed to be published.

synctime :

When file sync is set, you can buffer the sync calls into batches in order to prevent the underlying system from being overloaded during busy periods. This value specifies the maximum time in milliseconds between sync calls. The smaller the value, the more frequent the sync will be called on the physical file system.

syncbatchsize :

When file sync is set, you can buffer the sync calls into batches in order to prevent the underlying system from being overloaded during busy periods. This value specifies the number of messages in each batch. The smaller the value, the more frequent the sync will be called on the physical file system.

initialconnectionretrycount :

When a connection is first established, the default number of connection attempts is 2. This allows this value to be overridden.

syncsendpersistent :

For each persistent message written to the server, ensure the send is a synchronous call.

syncwritetodisc :

For each persistent message written to the server, perform a file system sync to ensure the OS has written the data.

enabledurablepriority :

If enabled, durable subscriptions of the same name can exist on the same topic, but only the first in will consume the events for that subscription.

enablesinglequeueack :

If enabled, message acknowledgements on a queue consumer will only acknowledge that specific message rather than all messages consumed prior to that message, on that queue.

enablesingleshareddurableack :

If enabled, message acknowledgements on a shared durable consumer will only acknowledge that specific message rather than all messages consumed prior to that message, on that shared durable.

enablesheardedurable :

If enabled, durable subscriptions of the same name can exist on the same topic, and events will be distributed in a round robin fashion to each subscriber using that name (i.e. once and once only per durable name).

maxreconnectattempts :

When `getConnectionOnFailure()` is enabled, this value is used to prevent the disconnection exceptions being thrown via the `ExceptionListener` on the JMS Connection. The default value is -1, which represents infinite retries.

conexceptiononretryfailure :

When enabled, any disconnections from the JMS Connection will not result in an Exception being generated through the `ExceptionListener`. An exception will only be thrown to the `ExceptionListener` when the `getMaxReconAttempts()` value is reached.

retrycommit :

```

Determines whether the commit call to a transacted session will
retry if any exceptions are detected, rather than simply throw an exception.
randomrnames :
  Allows the list of RNAME urls to be randomised to provide simple load
  balancing across a list of servers.
enablemultiplexedconnections :
  Support the use of a shared physical connection by multiple sessions
  when the same topic or queue is used by multiple receivers.
durabletype :
  Type of the new Durable:
  N - Named
  S - Shared
  Serial - Serial
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.

```

CreateJMSQueue

```

Tool name:
  CreateJMSQueue
Description:
  Creates a JMS queue with the specified name on the specified realm.

Usage:
  runUMTool CreateJMSQueue -rname=<rname> -queuename=<queuename> [optional_args]

Examples:
  CreateJMSQueue -rname=nsp://localhost:8080 -queuename=queue0

Required arguments:
  rname :
    URL of the realm to which the queue will be connected.
    When connecting to the nodes in a UM cluster, the rname parameter should specify
    a comma-separated list of the rnames of the clustered nodes, for example:
    -rname=nsp://localhost:9000,nsp://localhost:9001,nsp://localhost:9002
  queuename :
    Name of the queue to be created.

Optional Parameters:
  maxevents :
    Capacity of the new store (default 0).
  synceachwrite :
    Whether each write to the store will also call sync on the
    file system to ensure all data is written to disk.
  username :
    Your Universal Messaging server username.
  password :
    Your Universal Messaging server password.
For a full list of the available optional parameters, see the usage of the tool when
you run
runUMTool.

```

CreateJMSTopic

```

Tool name:
  CreateJMSTopic

```

Description:

Creates a JMS topic with the specified name on the specified realm.

Usage:

```
runUMTool CreateJMSTopic -rname=<rname> -channelname=<channelname> [optional_args]
```

Examples:

```
CreateJMSTopic -rname=nsp://localhost:8080 -channelname=channel0
```

Required arguments:

rname :

URL of the realm to which the channel will be connected.

When connecting to the nodes in a UM cluster, the rname parameter should specify a comma-separated list of the rnames of the clustered nodes, for example:

```
-rname=nsp://localhost:9000,nsp://localhost:9001,nsp://localhost:9002
```

channelname :

Name of the channel to be created.

Optional Parameters:

maxevents :

Capacity of the new store (default 0).

synceachwrite :

Whether each write to the store will also call sync on the file system to ensure all data is written to disk.

username :

Your Universal Messaging server username.

password :

Your Universal Messaging server password.

For a full list of the available optional parameters, see the usage of the tool when you run

runUMTool.

JMSPublish

Tool name:

JMSPublish

Description:

Publishes one or more messages to a JMS queue or topic.

Usage:

```
runUMTool JMSPublish -rname=<rname> -connectionfactory=<connectionfactory>
  -destination=<destination> [optional_args]
```

Examples:

```
JMSPublish -rname=nsp://localhost:9000 -connectionfactory=factory
  -destination=topic -message=hello
```

Required arguments:

rname :

Connection URL to the realm where the data group will be created.

connectionfactory :

Name of the connection factory in the Universal Messaging Realm's JNDI namespace. Must exist.

destination :

Name of the JMS destination (queue or topic). Must exist.

Optional Parameters:

size :

```

    Size of the message to send. Message will be generated. You can't use
    -message along with -size.
message :
    Message to send. Put the message in quotes if it contains spaces.
    You can't use -size along with -message.
count :
    How many times to send the message. Default is 1.
transacted :
    If the session is transacted. Default is false.
username :
    Your Universal Messaging server username.
password :
    Your Universal Messaging server password.

```

JMSSubscribe

```

Tool name:
    JMSSubscribe
Description:
    Reads messages arriving to a JMS destination.

Usage:
    runUMTool JMSSubscribe -rname=<rname> -connectionfactory=<connectionfactory>
    -destination=<destination> [optional_args]

Examples:
    JMSSubscribe -rname=nsp://localhost:9000 -connectionfactory=factory
    -destination=topic

Required arguments:
    rname :
        Connection URL to the realm where the data group will be created.
    connectionfactory :
        Name of the connection factory in the Universal Messaging Realm's
        JNDI namespace. Must exist.
    destination :
        Name of the JMS destination (queue or topic). Must exist.

Optional Parameters:
    transacted :
        If the session is transacted. Default is false.
    selector :
        Optional JMS message selector.
    username :
        Your Universal Messaging server username.
    password :
        Your Universal Messaging server password.

```

ModifyConnectionFactory

```

Tool name:
    ModifyConnectionFactory
Description:
    Modifies settings of a JMS connection factory on the specified server.

Usage:
    runUMTool ModifyConnectionFactory -rname=<rname> -factoryname=<factoryname>
    [optional_args]

```

Examples:

```
ModifyConnectionFactory -rname=nsp://localhost:8080 -factoryname=factory0
```

Required arguments:

```
rname :
  URL of the realm to which the ConnectionFactory is attached.
factoryname :
  Name of the connection factory to locate.
```

Optional Parameters:

```
contextfactory :
  The name of the ContextFactory class to use
  (default: com.pcbssys.nirvana.nSpace.NirvanaContextFactory)
  When using an AMQP connection this should be changed to:
  org.apache.qpid.jms.jndi.JmsInitialContextFactory
  to use the QPID Proton JMS Client libraries;
```

Hint: AMQP connections work only over nsp and nsps interfaces, they won't work over nhp or nhps.

```
autocreateresource :
  If set will create resources on the server when performing a lookup
  on a queue or channel.
```

```
synctopicacks :
  Specifies for a specific connection whether the topic
  acknowledgements will be sent synchronously.
```

```
syncqueueacks :
  Specifies for a specific connection whether the queue
  acknowledgements will be sent synchronously.
```

```
writehandler :
  Specifies for a specific connection the write handler type to use.
  Ignored unless between 1-4.
```

```
adapterbuffer :
  Specifies for a specific connection the adapter send / receive
  buffer size. If the value is 0 or less it is ignored.
```

```
syncnamedtopicacks :
  Specifies for a specific connection whether the durable
  topic acknowledgements will be sent synchronously.
```

```
permittedkeepalivesmissed :
  Set the number of keep server keep alives the client is allowed
  to miss before detecting a network issue and terminating the connection.
```

```
connectiontimeout :
  Set the timeout used for connection / reconnection to realms.
  If the connection fails to establish within this time-frame it will
  fail.
```

```
disconnectafterclusterfailure :
  If connected to a cluster of realms, and cluster quorum is lost,
  this flag determines whether the client will be disconnected.
```

```
usejmsengine :
  JMS engine ensures no events are available for topic replay
  unless durable subscriptions are being used. Non JMS engine fanout enables
  events to be stored even after events are delivered. Default is true.
```

```
reconnectinterval :
  If a client is disconnected, and Immediate Reconnect is set to true,
  this value represents the interval between reconnect attempts.
```

```
immediatereconnect :
  If a client is disconnected, this flag will indicate whether the client
  will immediately reconnect and attempt to reconnect as fast as possible,
  rather than rely on a back off period.
```

```
autoreconnectafteracl :
  If a client is disconnected because of a security change, this flag
```

will indicate whether the automatic session reconnection logic will kick in.

threadpoolsize :
Gets the maximum number of threads used by the client for delivery of all messages to listeners.

redeliveredsized :
Specifies the maximum number of messages that the client will keep reference to if they are marked as redelivered.

unackedsized :
The client will keep a list of messages that have not been acknowledged. This value sets the maximum size of this list.

useinfinitewindow sized :
When set to true, the consumer can consume as many events as required before committing.

window sized :
When asynchronously consuming messages from the server, they will be delivered in batches (windows). This property sets the size of that window.

autoackcount :
With AUTO acknowledgement mode, in order to improve performance, the acknowledgement of messages can be batched so that not every message consumed results in communication with the server. This value determines how many events can be consumed before an acknowledgement is sent to the server.

globalstorecapacity :
Each topic or queue store can have a maximum number of messages that can exist before no more messages are allowed to be published.

synctime :
When file sync is set, you can buffer the sync calls into batches in order to prevent the underlying system from being overloaded during busy periods. This value specifies the maximum time in milliseconds between sync calls. The smaller the value, the more frequent the sync will be called on the physical file system.

syncbatchsize :
When file sync is set, you can buffer the sync calls into batches in order to prevent the underlying system from being overloaded during busy periods. This value specifies the number of messages in each batch. The smaller the value, the more frequent the sync will be called on the physical file system.

initialconnectionretrycount :
When a connection is first established, the default number of connection attempts is 2. This allows this value to be overridden.

syncsendpersistent :
For each persistent message written to the server, ensure the send is a synchronous call.

syncwritetodisc :
For each persistent message written to the server, perform a file system sync to ensure the OS has written the data.

enabledurablepriority :
If enabled, durable subscriptions of the same name can exist on the same topic, but only the first in will consume the events for that subscription.

enablesinglequeueack :
If enabled, message acknowledgements on a queue consumer will only acknowledge that specific message rather than all messages consumed prior to that message, on that queue.

enablesingleshareddurableack :
If enabled, message acknowledgements on a shared durable consumer will only acknowledge that specific message rather than all messages consumed prior to that message, on that shared durable.

```

enableshearedurable :
  If enabled, durable subscriptions of the same name can
  exist on the same topic, and events will be distributed in a round robin
  fashion to each subscriber using that name (ie once and once only per
  durable name).
maxreconnectattempts :
  When getConxExceptionOnFailure() is enabled, this value is used to
  prevent the disconnection exceptions being thrown via the
  ExceptionListener on the JMS Connection. The default value is -1, which
  represents infinite retries.
conxexceptiononretryfailure :
  When enabled, any disconnections from the JMS Connection will not
  result in an Exception being generated through the ExceptionListener.
  An exception will only be thrown to the ExceptionListener when the
  getMaxReconAttempts() value is reached.
retrycommit :
  Determines whether the commit call to a transacted session will
  retry if any exceptions are detected, rather than simply throw an exception.
randomrnames :
  Allows the list of RNAME urls to be randomised to provide simple
  load balancing across a list of servers.
enablemultiplexedconnections :
  Support the use of a shared physical connection by multiple sessions
  when the same topic or queue is used by multiple receivers.
durabletype :
  Type of the new Durable:
  N - Named
  S - Shared
  Serial - Serial
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.

```

ViewConnectionFactory

```

Tool name:
  ViewConnectionFactory
Description:
  Views settings of a JMS connection factory on the specified server.

Usage:
  runUMTool ViewConnectionFactory -rname=<rname> -factoryname=<factoryname>
  [optional_args]

Examples:
  ViewConnectionFactory -rname=nsp://localhost:8080 -factoryname=factory0

Required arguments:
  rname :
    URL of the realm to which the ConnectionFactory is attached.
  factoryname :
    Name of the connection factory to locate.

Optional Parameters:
  contextfactory :
    The name of the ContextFactory class to use
    (default: com.pcbSYS.nirvana.nSpace.NirvanaContextFactory).
    When using an AMQP connection this should be changed to:
    org.apache.qpid.jms.jndi.JmsInitialContextFactory

```

to use the QPID Proton JMS Client libraries;

Hint: AMQP connections work only over nsp and nsps interfaces, they do not work over nhp or nhps.

```
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.
```

Syntax: Recovery Tools

AddInterfaceOffline

```
Tool name:
  AddInterfaceOffline
Description:
  Adds a new interface to an offline realm.

Usage:
  runUMTool AddInterfaceOffline -dirname=<dirname> -protocol=<protocol>
    -adapter=<adapter> -port=<port> [optional_args]

Examples:
  AddInterfaceOffline -dirname=~/.realmDirectories/realm0/data/ -protocol=socket
    -adapter=0.0.0.0 -port=11000

Required arguments:
  dirname :
    Data directory of the realm to add interface to.
  protocol :
    Protocol for the interface to use.
  adapter :
    Adapter the interface wants setting to.
  port :
    Port that the interface will listen on.

Optional Parameters:
  interface :
    Name of the interface to be created.
  autostart :
    Whether or not the interface should be autostarted when the realm
    starts.
  canadvertise :
    Whether or not the interface will be advertised.
  authtimeout :
    Number of milliseconds for authorisation timeout.
  interrealm :
    Whether or not this interface should be used for inter-realm
    communication.
  clientconnections :
    Whether or not this interface should be used for client
    connections.
  username :
    Your Universal Messaging server username.
  password :
    Your Universal Messaging server password.
```

DeleteInterfaceOffline

```
Tool name:
  DeleteInterfaceOffline
Description:
  Removes an interface from an offline realm using config data.

Usage:
  runUMTool DeleteInterfaceOffline -dirname=<dirname> -interface=<interface>
  [optional_args]

Examples:
  DeleteInterfaceOffline -dirname=~/.realmDirectories/realm0/data/ -interface=nhp0

Required arguments:
  dirname :
    Data directory of the realm to dump interfaces for.
  interface :
    Name of the interface to be removed.

Optional Parameters:
  username :
    Your Universal Messaging server username.
  password :
    Your Universal Messaging server password.
```

DumpInterfacesOffline

```
Tool name:
  DumpInterfacesOffline
Description:
  Dumps the list of interfaces for a specified offline realm.

Usage:
  runUMTool DumpInterfacesOffline -dirname=<dirname> [optional_args]

Examples:
  DumpInterfacesOffline -dirname=~/.realmDirectories/realm0/data/

Required arguments:
  dirname :
    Data directory of the realm to dump interfaces for.

Optional Parameters:
  username :
    Your Universal Messaging server username.
  password :
    Your Universal Messaging server password.
```

ExportEventsFromOfflineMemFile

```
Tool name:
  ExportEventsFromOfflineMemFile
Description:
  Dumps events to XML or JSON optionally using filter and protobuf description file.
Usage:
```

```
runUMTool ExportEventsFromOfflineMemFile -memfileloc=<memfileloc> [optional_args]
```

Examples:

```
ExportEventsFromOfflineMemFile
  -memfileloc=C:\source_folder\protobuf_channel94fab9fe6d3a92
  -dumpdata=true
  -jsonfilename=C:\destination_folder\file_name.json
  -xmlfilename=C:\destination_folder\file_name.xml
  -protobufdescriptor="C:\folder\School.fds"
ExportEventsFromOfflineMemFile
  -memfileloc=C:\source_folder\protobuf_channel94fab9fe6d3a92
  -dumpdata=true
  -jsonfilename=C:\destination_folder\file_name.json
  -xmlfilename=C:\destination_folder\file_name.xml
  -protobufdescriptor="C:\folder\School.fds"
  -selector="teacher.name = 'Person2' or teacher.name = 'Person4'"
  -starteid=10 -endeid=30
ExportEventsFromOfflineMemFile
  -memfileloc=C:\source_folder\mixed_channel_name231859db942796.mem
  -jsonfilename=C:\destination_folder\file_name.json
  -selector="EVENTDATA.AS-STRING(0, 8) = 'data2702'"
  -batchsize=1000
```

Required arguments:

memfileloc :
 Required parameter specifying the absolute path for the location of the memory file. The path can also be the location of a folder that contains multiple mem files.
 A folder with mem files can be specified only for multi-file storage.
 A single memory file can be specified only for mixed/persistent store.

xmlfilename/jsonfilename : Required parameter specifying the file path to export events to. xmlfilename exports to an XML-formatted file, whereas jsonfilename exports to a JSON-formatted file.
 You must specify at least one of these arguments (xmlfilename or jsonfilename), and you can also specify both.

Optional Parameters:

selector :
 Optional parameter specifying the selector to filter the events.

dumpdata :
 Optional parameter, when set to true the tool will dump event data (base64 encoded). Default value is true.
 The exported JSON file will contain event data as JSON node for protobuf events if protocol buffer file descriptor set is specified.

starteid :
 Optional parameter specifying the startEID of event from mem file to start filtering/dumping from (default = 0).

endeid :
 Optional parameter specifying the endEID of event from mem file to filter/dump to (if not specified, filtering/dumping will be done till the last storage event id).

protobufdescriptor:
 Optional parameter specifying the path to the protocol buffer file descriptor for filtering based on event data. The specified protocol buffer file descriptor will be applied if the mem file belongs to the protobuf channel with the same descriptor.

batchsize :
 Optional parameter specifying the events batch size to read from mem file and dump to output file, default value is 100.

ModifyInterfaceOffline

```
Tool name:
  ModifyInterfaceOffline
Description:
  Modifies and interface of an offline realm.

Usage:
  runUMTool ModifyInterfaceOffline -dirname=<dirname> -interface=<interface>
  [optional_args]

Examples:
  ModifyInterfaceOffline -dirname=~/.realmDirectories/realm0/data/
  -interface=nhp0 -port=11000

Required arguments:
  dirname :
    Data directory of the realm to dump interfaces for.
  interface :
    Name of the interface to be modified.

Optional Parameters:
  adapter :
    Adapter the interface wants setting to.
  port :
    Port that the interface will be set to.
  autostart :
    Whether or not the interface should be autostarted when the
    realm starts.
  canadvertise :
    Whether or not the interface will be advertised.
  authtimeout :
    Number of milliseconds for authorisation timeout.
  interrealm :
    Whether or not this interface should be used for inter-realm
    communication.
  clientconnections :
    Whether or not this interface should be used for client
    connections.
  username :
    Your Universal Messaging server username.
  password :
    Your Universal Messaging server password.
```

ModifyPrimeFlagOffline

```
Tool name:
  ModifyPrimeFlagOffline
Description:
  Modifies the prime flag of a site while a realm is offline.

Usage:
  runUMTool ModifyPrimeFlagOffline -datadirectory=<datadirectory> [optional_args]

Examples:
  ModifyPrimeFlagOffline -datadirectory=~/.realmDirectories/realm0/data/
  (This will show current state of prime flag per cluster sites)
```

```
ModifyPrimeFlagOffline -datadirectory=~/.realmDirectories/realm0/data/
                        -Site1=true -Site2=false
(This will set prime flag to true on site1 and to false on site 2 in
 directory ~/.realmDirectories/realm0/data/ )
```

Required arguments:

```
datadirectory :
    Data directory of the realm to be modified.
```

Optional Parameters:

```
force :
    Skip confirmation step before modifying cluster sites.
NOTE - if you want to edit the prime flag for sites inside a cluster you need to
specify it like an optional parameter :
    -<site_name>=<new_value>.
You need to specify the value of the flag for all sites inside the cluster.
For example, if you want to set the prime flag to true on Site1 and you have
another site called Site2, the optional parameter will look like :
    -Site1=true -Site2=false
```

```
username :
    Your Universal Messaging server username.
password :
    Your Universal Messaging server password.
```

RepublishEventsFromOfflineFile

Tool Name:

```
RepublishEventsFromOfflineFile
```

Description:

Imports events from an XML, JSON or .mem file, optionally using filter and protocol buffer file descriptor, and republishes events to specified store.

Usage:

```
runUMTool RepublishEventsFromOfflineFile -realm=<realm> -channelname=<channelname>
[optional_args]
```

Examples:

```
RepublishEventsFromOfflineFile
    -jsonfilename=C:\source_folder\filename.json
    -protobufdescriptor="C:\protobuf_folder\School.fds"
    -selector="teacher.name = 'Person2' or teacher.name = 'Person4'"
    -realm="nhp://0.0.0.0:11000" -channelname="destination_channel_name"
RepublishEventsFromOfflineFile
    -memfileloc=C:\source_folder\proto_channelb31238f42a49b
    -selector="EVENTDATA.AS-STRING(0, 8) = 'data2702'" -realm="nhp://0.0.0.0:11000"
    -channelname="destination_queue_name" -starteid=0 -endeid=90
RepublishEventsFromOfflineFile
    -xmlfilename=C:\source_folder\filename.xml
    -selector="EVENTDATA.TAG = '3' or EVENTDATA.TAG = '33'"
    -realm="nhp://0.0.0.0:11000" -channelname="destination_channel_name"
    -endeid=50 -batchsize=1000
```

Required arguments:

```
realm :
    Required parameter specifying realm server name/address for republishing events.
```

```
channelname :
```

Required parameter specifying destination store name for republishing events.

Optional Parameters:

memfileloc :

Optional parameter specifying absolute path for the memory file location.

The path can also be the location of a folder that contains multiple mem files.

A folder with mem files can be specified only for multi-file storage, and a single memory file can be specified only for mixed/persistent store.

One source file should be specified: memfileloc, xmlfilename or jsonfilename.

xmlfilename :

Optional parameter specifying an XML file path to import events from.

One source file should be specified: memfileloc, xmlfilename or jsonfilename.

jsonfilename :

Optional parameter specifying a JSON file path to import events from.

One source file should be specified: memfileloc, xmlfilename or jsonfilename.

protobufdescriptor:

Optional parameter specifying the path to a protocol buffer file descriptor set for filtering events based on event data.

selector :

Optional parameter specifying the selector to filter the events.

started :

Optional parameter specifying the startEID of event from source file to start filtering/importing from (default = 0).

endeid :

Optional parameter specifying the endEID of event from source file to filter/import to.

If not specified, filtering/importing will be done till last storage event id).

batchsize :

Optional parameter specifying the event batch size used for import and republishing events

to the store (default = 100).

Syntax: Durable Tools

ViewDurableEvent

Tool name:

ViewDurableEvent

Description:

Gets all events for all durables or all events for a specific durable.

The tool has two required parameters (rname , channelname) and two optional parameters (durablename , maxevents , startid). By default, if no optional parameters are added it will list the events on all durables. Default number of events is 1000 per durable.

Usage:

```
runUMTool ViewDurableEvent -rname=<rname> -channelname=<channelname>
[optional_args]
```

Examples:

```
ViewDurableEventWith required parameters: -rname=nhp://localhost:11000
-channelname=testchan With optional parameters:
-rname=nhp://localhost:11000 -channelname=testchan
```

```
-durablename=testdurable -maxevents=100 -startid=50 -displayanydata=true
```

Required arguments:

```
  rname :
    Name of the realm.
  channelname :
    Channel which durable is subscribed to.
```

Optional Parameters:

```
  durablename :
    The name of the durable to browse events.(Optional Parameter).
  maxevents :
    The number of maximum events to display.(Optional Parameter).
  startid :
    The EID of the starting event to display events from.
    (Optional Parameter)
  displayanydata :
    If the data displayed should be of any kind. By default
    only UTF-8 encoded data is shown. (Optional Parameter)
  username :
    Your Universal Messaging server username.
  password :
    Your Universal Messaging server password.
```

Syntax: Miscellaneous Tools

AddHealthMonitorPlugin

Note:

For more details of the purpose of this plugin, see the section [“Health Monitor Plugin” on page 166](#) in the documentation of the Enterprise Manager.

Tool name:

```
AddHealthMonitorPlugin
```

Description:

```
Adds the health monitor plugin to an interface on a realm server.
The URL endpoint for this plugin must always include a trailing slash, for example
http://localhost:9000/test/
There are two modes available: Offline and Online.
- Online mode adds the plugin on a running server,
- Offline mode can be used to add the plugin on an offline server.
```

Usage:

```
runUMTool AddHealthMonitorPlugin -rname=<rname> -protocol=<protocol>
      -adapter=<adapter> -port=<port> -mountpath=<mountpath> [optional_args]
```

Example:

```
AddHealthMonitorPlugin -rname=nsp://0.0.0.0:9000 -protocol=http
      -adapter=0.0.0.0 -port=11000 -mountpath=monitor
```

Required arguments:

```
  protocol :
    Protocol for the interface to use/add.
  adapter :
    Adapter that the interface will be set to.
```

```
port :  
    Port that the plugin will be added on.  
  
mountpath :  
    Path that the plugin will be mounted to.
```

Optional Parameters:

```
rname :  
    URL of the session to which the realm server, on which the plugin will be created,  
    is connected. This is applicable only for online mode;  
    for offline mode, the 'dirname' parameter needs to be set.  
  
dirname :  
    Data directory of the realm server where the plugin will be added.  
autostart:  
    Boolean value to set the interface to "autostart".  
    Applicable only if the interface is not present already.  
  
username :  
    Your Universal Messaging server username.  
password :  
    Your Universal Messaging server password.
```

EditRealmConfiguration

```
Tool name:  
    EditRealmConfiguration  
Description:  
    Edits realm configuration parameters.
```

```
Usage:  
    runUMTool EditRealmConfiguration -rname=<rname> [optional_args]
```

```
Examples:  
    EditRealmConfiguration -rname=nsp://localhost:9000 -listgroupconfiguration=all  
    (This will show all realm configuration parameters and their current value)
```

```
    EditRealmConfiguration -rname=nsp://localhost:9000  
    -listgroupconfiguration=Thread_Pool_Config  
    (This will show Thread Pool Config parameters and their current values)
```

```
    EditRealmConfiguration -rname=nsp://localhost:9000  
    -Audit_Settings.ChannelACL=false -Join_Config.MaxQueueSizeToUse=50  
    (This will set channelACL to false and MaxQueueSizeToUse to 50)
```

```
Required arguments:  
    rname :  
        Connection URL to the realm you want to edit configuration.
```

Optional Parameters:

```
NOTE - If you want to edit a realm configuration parameter you should  
specify it like an optional parameter :  
-<group_name>.<parameter>=<new_value>  
where space is escaped in <group_name> by using an underscore("_").  
For example, if you want to change the parameter ChannelACL in the
```

```
group Audit Settings to "true" the optional parameter will look like:
-Audit_Settings.ChannelACL=true
```

```
listgroupconfiguration :
  The configuration group for which you want to see values of parameters.
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.
```

ExportRealmXML

```
Tool name:
  ExportRealmXML
Description:
  Exports selected realm to an XML file.

Usage:
  runUMTool ExportRealmXML -rname=<rname> -filename=<filename> [optional_args]

Examples:
  ExportRealmXML -rname=nsp://localhost:9000 -filename=test.xml -exportall=true
  (This will export all the information)

  ExportRealmXML -rname=nsp://localhost:9000 -filename=test.xml -realms=true
  -realmconfiguration=true -channels=true -queues=true
  (This will export information about realm set, realm configuration, channels
  and queues)

Required arguments:
  rname :
    Connection URL to the realm you want to export.
  filename :
    File name where the information will be exported.

Optional Parameters:
  exportall :
    Export all information for the chosen realm.
  clusters :
    Include Cluster information in the export file.
  datagroups :
    Include DataGroups information in the export file.
  realmall :
    Export all information for realm including RealmSet,
    RealmConfiguration, RealmSchedulerSet and RealmACLS(RealmPermissionSet)
  realms :
    Include RealmSet information in the export file.
  realmconfiguration :
    Include RealmConfiguration information in the export file.
  realmschedule :
    Include RealmSchedulerSet information in the export file.
  realmacLS :
    Include RealmACLS (RealmPermissionSet) information in the export file.
  channelsall :
    Export all information for channels in the chosen realm
    including ChannelEntry, ChannelACLS (ChannelPermissionSet), ChannelJoins,
    DurableSet and JNDI Configuration.
  channels :
```

```

    Include ChannelEntry information in the export file.
channelacls :
    Include ChannelACLs (ChannelPermissionSet) information in
    the export file.
channeljoins :
    Include ChannelJoins information in the export file.
durables :
    Include DurableSet information in the export file.
jndiconfig :
    Include JNDI Configuration information in the export file.
interfacesall :
    Export all information for interfaces in the chosen realm
    including Interfaces, InterfaceVIA (ACLs) and Interface Plugins.
interfaces :
    Include Interfaces information in the export file.
interfacevia :
    Include InterfaceVIA (ACLs) information in the export file.
plugins :
    Include Interface Plugins information in the export file.
queuesall :
    Export all information for interfaces in the chosen realm
    including QueueEntry and QueueACLs (QueuePermissionSet).
queues :
    Include QueueEntry information in the export file.
queueacls :
    Include QueueACLs (QueuePermissionSet) information in the export file.
username :
    Your Universal Messaging server username.
password :
    Your Universal Messaging server password.

```

HealthChecker

```

Tool name:
    HealthChecker
Description:
    Tool for analysing configuration items and highlighting robustness improvements.

Usage:
    runUMTool HealthChecker -rname=<rname> [optional_args]
    or..
    runUMTool HealthChecker -xml=<xml> [optional_args]

Live Mode :
Examples:
HealthChecker -rname=nsp://localhost:9000
HealthChecker -rname=nsp://localhost:9000 -mode=all
HealthChecker -rname=nsp://localhost:9000
                -check=StoreWarningsCheck,RealmConfigurationCheck
HealthChecker -rname=nsp://localhost:9000 -mode=all
                -exclude=StoreWarningsCheck,RealmConfigurationCheck
                -include=RealmACLCheck,ResourcesSafetyLimitsCheck

XML Check Mode :
Examples:
HealthChecker -xml=/path/to/xml1,/path/to/xml2
HealthChecker -xml=/path/to/xml1,/path/to/xml2 -mode=all
HealthChecker -xml=/path/to/xml1,/path/to/xml2
                -check=StoreWarningsCheck,RealmConfigurationCheck
HealthChecker -xml=/path/to/xml1,/path/to/xml2 -mode=all
                -exclude=FixLevelCheck,DurableMismatchCheck

```

```

        -include=ResourcesSafetyLimitsCheck,RealmACLCheck
Required arguments:
  rname: URL of the realm, or cluster member, against which to run the health check.
  or..
  xml: XML files containing realm configuration.
Optional arguments:
  mode: Defines the initial set of 'HealthChecker' checks that you
        can manipulate (with 'exclude' or 'include' options) if you choose to.
        There are two modes :
        default:
            This option gives access to the recommended minimal subset of checks.
            This is the default option if mode is not specified.
        all:
            This option gives access to additional checks.
            Executed without 'exclude' or 'check' it will execute all HealthChecker
checks.
  check: Run only the specified check or checks.
        It should not be used together with 'mode','include' or 'exclude arguments.

  exclude: Run all checks from the specified set (see 'mode') except the specified
check or checks.
        The parameter may contain a single check or a comma-separated list of
checks.
  include: Run all checks available with the given mode and
        additionally include the check(s) specified via this parameter.
        The parameter may contain a single check to include or a comma-separated
list of checks
  *: All additional parameters are passed down to the checks.
        If any given check has the capability to process any of the additional
arguments then it will, and the given check will ignore any
additional parameters that it cannot process.

additionalArg<n>:
  Some of the health checks allow you to specify one or more additional
parameters when calling the HealthChecker. The name and purpose of each
additional parameter is specific to the individual health check being run.
For example, the DurableSubscriberLargeStoreCheck check allows you
to specify the additional parameter -threshold=<value>, which defines
a threshold for the number of remaining events to be consumed in a
shared durable.
  All additional parameters are passed to all the HealthChecker checks;
if any given check has the capability to process any of the additional
arguments then it will, and the given check will ignore any
additional parameters that it cannot process.
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.

```

ImportRealmXML

```

Tool name:
  ImportRealmXML
Description:
  Imports selected realm from an XML file

Usage:
  runUMTool ImportRealmXML -rname=<rname> -filename=<filename> [optional_args]

```

Examples:

```
ImportRealmXML -rname=nsp://localhost:9000 -filename=test.xml -importall=true  
(This will import all the information present in selected file)
```

```
ImportRealmXML -rname=nsp://localhost:9000 -filename=test.xml -realms=true  
-realmconfiguration=true -channels=true -queues=true  
(This will import information about realm set, realm configuration, channels and  
queues if present in selected file)
```

Required arguments:

```
rname :  
    Connection URL to the realm you want to import configuration.  
filename :  
    File name from which the information will be imported.
```

Optional Parameters:

```
importall :  
    Import all information for the chosen realm.  
clusters :  
    Import Cluster information if present in file.  
datagroups :  
    Import Data Groups information if present in file.  
realmall :  
    Import all information for realm including RealmSet,  
    RealmConfiguration, RealmSchedulerSet and RealmACLS(RealmPermissionSet)  
    if present in file.  
realms :  
    Import RealmSet information if present in file.  
realmconfiguration :  
    Import RealmConfiguration information if present in file.  
realmschedule :  
    Import RealmSchedulerSet information if present in file.  
realmacls :  
    Import RealmACLS(RealmPermissionSet) information if present in file.  
channelsall :  
    Import all information for channels including ChannelEntry,  
    ChannelACLS (ChannelPermissionSet), ChannelJoins, DurableSet and  
    JNDI Configuration if present in file.  
channels :  
    Import ChannelEntry information if present in file.  
channelacls :  
    Import ChannelACLS information if present in file.  
channeljoins :  
    Import ChannelJoins information if present in file.  
durables :  
    Import DurableSet information if present in file.  
jndiconfig :  
    Import JNDI Configuration information if present in file.  
interfacesall :  
    Import all information for interfaces including Interfaces,  
    InterfaceVIA (ACLS) and Interface Plugins if present in file.  
interfaces :  
    Import Interfaces information if present in file.  
interfacevia :  
    Import InterfaceVIA (ACLS) information if present in file.  
plugins :  
    Import Interface Plugins information if present in file.  
queuesall :  
    Import all information for interfaces including QueueEntry and
```

```

QueueACLs (QueuePermissionSet) if present in file.
queues :
  Import QueueEntry information if present in file.
queueacIs :
  Import QueueACLs (QueuePermissionSet) information if present in
  file.
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.

```

Syntax: Site Tools

CreateSite

```

Tool name:
  CreateSite
Description:
  Creates a site with the specified name, consisting of the specified nodes.

Usage:
  runUMTool CreateSite -sitename=<sitename> -rnames=<rnames> [optional_args]

Examples:
  CreateSite -sitename=site0 -rnames=nsp://localhost:11000,nsp://localhost:11010

Required arguments:
  sitename :
    Name of the site to be created.
  rnames :
    Server URLs to be considered for the site. Can be more than one URL,
    separated by a comma.
    The proper format is [nsp/nhp/nsps/nhps]://[hostname]:[port] or
    shm://[path/to/file].

Optional Parameters:
  username :
    Your Universal Messaging server username.
  password :
    Your Universal Messaging server password.

```

DeleteSite

```

Tool name:
  DeleteSite
Description:
  Deletes a site with the specified name from all the nodes associated with it.

Usage:
  runUMTool DeleteSite -sitename=<sitename> -rname=<rname> [optional_args]

Examples:
  DeleteSite -sitename=site0 -rname=nsp://localhost:11000

Required arguments:
  sitename :

```

```
Name of the site to be deleted.
rname :
  Server URL to be considered for the site. Can be more than one URL,
  separated by a comma.
  The proper format is [nsp/nhp/nsps/nhps]://[hostname]:[port] or
  shm://[path/to/file].
```

Optional Parameters:

```
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.
```

SetPrimeSite

```
Tool name:
  SetPrimeSite
Description:
  Toggles the specified site's prime status.

Usage:
  runUMTool SetPrimeSite -sitename=<sitename> -rname=<rname>
  -setprime=<setprime> [optional_args]

Examples:
  SetPrimeSite -sitename=site0 -rname=nhp://localhost:11000 -setprime=true

Required arguments:
sitename :
  Name of the site to be configured.
rname :
  Server URL to be considered for the site.
setprime :
  True/False flag to set/unset a site being the prime site.

Optional Parameters:
username :
  Your Universal Messaging server username.
password :
  Your Universal Messaging server password.
```

ShowSites

```
Tool name:
  ShowSites
Description:
  Displays the configuration of the sites.

Usage:
  runUMTool ShowSites -rname=<rname> [optional_args]

Examples:
  ShowSites -rname=nhp://localhost:11000

Required arguments:
rname :
  Server URL to be considered for the site.
```

Optional Parameters:

```
username :
    Your Universal Messaging server username.
password :
    Your Universal Messaging server password.
```

Syntax: Diagnostic Tools

RealmInformationCollector

Tool name:

```
RealmInformationCollector
```

Description:

```
Collects diagnostic information from a Universal Messaging realm server
installation and stores it in a zip archive.
```

Usage:

```
runUMTool RealmInformationCollector -mode=<mode> -instance=<instance>
    [optional_args]
```

Examples:

```
RealmInformationCollector -mode=offline -instance=umserver
RealmInformationCollector -mode=offline -instance=umserver
    -include=data,heapdumps
RealmInformationCollector -mode=offline -instance=*
RealmInformationCollector -mode=live -instance=umserver,umserver2
    -include=heapdump
RealmInformationCollector -mode=live -instance=umserver,umserver2
    -exclude=jaas,plugins
RealmInformationCollector -mode=live -instance=umserver,umserver2
    -outputfile=/path/to/outputfile.zip
```

Required arguments:

```
mode : Operating mode, either 'offline' or 'live'.
```

The chosen mode determines what information is collected.

If 'offline' is specified, the tool will ensure that all instances to collect information from are not running.

If 'live' is specified, the tool will ensure that all instances are running.

In live mode, certain Universal Messaging directories/files are not collected, because reading them may cause failures on the server.

For example, if the content of the data directory is needed, it can be collected only in offline mode.

The following collectors will be executed by default in live mode:

```
tanukilogs    - Collects Tanuki wrapper logs of an UM server instance.
secfile       - Collects the security file of an UM server instance.
installlogs   - Collects SoftwareAG installer logs.
tanukiconf    - Collects Tanuki wrapper configuration of an UM server
                instance.
env           - Collects environment information from a running UM server.
license       - Collects the license file of an UM server instance.
realmconfig   - Exports realm configuration from a running UM server instance.

instancemgr   - Collects Universal Messaging instance manager logs.
healthchecker - Acquires health information from a running UM server instance
                using UM HealthChecker tool
```

```

jaas          - Collects JAAS configuration of an UM server instance.
threaddump   - Generates 3 thread dumps of a running UM server instance.
plugins      - Collects plugins directory of an UM server instance.

```

Collectors not enabled per default in live mode (need to be explicitly included):

```

heapdump     - Acquires heap dump from a running UM server instance.
               Note: This collector is not available on all platforms.
heapdumps    - Collects heap dumps directory of an UM server instance.

```

The following collectors will be executed by default in offline mode:

```

tanukilogs   - Collects Tanuki wrapper logs of an UM server instance.
secfile      - Collects the security file of an UM server instance.
installlogs  - Collects SoftwareAG installer logs.
tanukiconf   - Collects Tanuki wrapper configuration of an UM server instance.

```

```

license      - Collects the license file of an UM server instance.
instancemgr  - Collects Universal Messaging instance manager logs.
jaas         - Collects JAAS configuration of an UM server instance.
logs         - Collects logs of an UM server instance.
plugins      - Collects plugins directory of an UM server instance.

```

Collectors not enabled per default in offline mode (need to be explicitly included):

```

data         - Collects data directory of an UM server instance.
heapdumps    - Collects heap dumps directory of an UM server instance.

```

instance :

Specifies a comma-separated list of realm server instance names to collect information from. Specify '*' to include all available instances.

Optional Parameters:

outputfile :

The directory or file to write generated archive to.
If a directory is specified, it must exist.
If a file is specified and it is already present, the tool will fail.
If this argument is omitted, the tool will generate the archive in the current working directory.

exclude :

Specifies a comma-separated list of collector names to exclude.
See 'mode' for list of available collectors.

include :

Specifies a comma-separated list of collector names to include.
See 'mode' for list of available collectors.

username :

Your Universal Messaging server username.

password :

Your Universal Messaging server password.

7 Universal Messaging Administration API

■ Introduction	440
■ Administration API Package Documentation	443
■ Namespace Objects	443
■ Realm Server Management	450
■ Security	456
■ Management Information	461

Universal Messaging provides a feature rich Administration API capable of capturing all metrics, management and audit information from Universal Messaging realms. The API allows you to control and administer all aspects of any Universal Messaging realm or clusters of realms.

Universal Messaging's Enterprise Manager GUI has been written entirely using the Universal Messaging Administration API as a means of demonstrating how useful the API can be for the management of your messaging infrastructure.

Some example code showing how to use the Universal Messaging management API can be found in the examples section.

The Administration API is available in the following languages:

- Java
- C#.NET
- C++

Note:

The Administration APIs for C# and C++ are deprecated and will be removed from the product distribution in the next official release.

Introduction

Getting Started

The Universal Messaging Admin API (see the Package Documentation) allows management, configuration, audit and monitoring of all aspects of a Universal Messaging realm server.

The starting point for the Admin API is connecting to a realm. In order to connect to a realm using the Admin API, you need to ensure you are familiar with the concept of an RNAME. Once you have the RNAME that corresponds to your realm, you can then connect to the realm.

The way you connect to a realm is by constructing an `nRealmNode` object. The `nRealmNode` object is the main object you need to access all of the objects you wish to configure, monitor and manage:

```
String[] RNAME={"nsp://127.0.0.1:9000"};
nSessionAttributes nsa=new nSessionAttributes(RNAME);
nRealmNode realm = new nRealmNode(nsa);
```

Universal Messaging namespace

Access to resources on a Universal Messaging realms, or indeed objects in a multi Universal Messaging realm server namespace, is based on a simple tree structure, where the `nRealmNode` is the root of the tree. All nodes within the tree are subclasses of a base class `nNode`. From the root, it is possible to obtain references to all child nodes. Child nodes may be other realm nodes, containers (folders containing other realms, channels etc), channels and queues.

For example, to obtain an enumeration of all child nodes within a realm node, simply call the following:

Java:

```
Enumeration children = realm.getNodes();
```

C#:

```
System.Collections.IEnumerator children = realm.getNodes();
```

C++:

```
fSortedList nodes = pNode->getNodes();
```

From this enumeration you can then perform operations on the child nodes. For example, if you have a realm with 1 channel and 1 queue, and wanted to find the number of events currently on each, the following code would do that:

Example: Finding out how many events are on a channel / queue

Java:

```
while (children.hasMoreElements()) {
    nNode child = (nNode)children.nextElement();
    if (child instanceof nLeafNode) {
        nLeafNode leaf = (nLeafNode)child;
        System.out.println("Leaf node contains "+leaf.getCurrentNumberOfEvents());
    }
}
```

C#:

```
while (children.MoveNext()){
    nNode child = (nNode)children.Current;
    if (child is nLeafNode) {
        nLeafNode leaf = (nLeafNode)child;
        Console.WriteLine("Leaf node contains "+leaf.getCurrentNumberOfEvents());
    }
}
```

C++:

```
void searchNodes(fSortedList nodes)
    for (fSortedList::iterator iterator = nodes.begin(); iterator != nodes.end();
        iterator++)
    {
        nNode *pNode = iterator->second;
        int type = pNode->getType ();
        if (type == fBase::LEAFNODE)
        {
            printf("Leaf node contains %ll events",pNode->getCurrentNumberOfEvents());
        }
    }
}
```

The namespace structure is dynamic and is managed asynchronously for you, so as and when objects are created, deleted modified, stopped or started, the namespace will manage those state changes and keep the structure up to date automatically.

Management / Configuration / Security

As well as the namespace nodes, there are also other objects that can be obtained from the nodes but which are not part of the namespace tree structure.

For example, from an `nRealmNode` it is possible to obtain the following objects:

- **nClusterNode** - The cluster node that this realm may be part of, allowing the administration of Universal Messaging realm clusters
- **nACL** - The realm acl object (see [“About Realm ACL Permissions” on page 126](#)), allowing control of the ACL permissions (see [“Access Control Lists” on page 456](#))
- **nInterfaceManager** - The realm interface manager, allows me to add, remove, stop, start interfaces on a realm (see [“Interfaces” on page 450](#))
- **nConfigGroup** - an enumeration of these corresponds to all configuration (see [“Config” on page 452](#)) and tuning parameters for a given realm.

From an `nLeafNode` which could be a channel or a queue, the following objects are available:

- **nACL** - The leaf node acl object, allows me to control acl permissions (see [“About Channel ACL Permissions” on page 127](#)) for resources
- **nJoinInfo** - All join information associated with a channel or queue

Monitoring

As well access to the channel resources as described above, there are also many monitoring tools available to developers that provide information asynchronously as and when events occur on a realm. This can be extremely useful in ongoing real time management of one or more Universal Messaging Realm servers.

For example, for a realm node you can provide listeners for the following :

- **Connections** - get notified as new connections (see [“Connection Information” on page 466](#)) to the realm occur, showing connection information
- **Creation / Deletions / Stop / Start** - get notified when new objects are created, deleted, modified, stopped or started (see [“nRealmNode” on page 461](#)) (for example new channels being created, acls being changed etc)
- **State Changes** - get notified when changes occur to any of the objects in the namespace (see [“nLeafNode” on page 465](#)), such as events being published / consumed. All updates are asynchronously received from the realm server and the API manages those changes for you.
- **Audit / Logging** - when security or state changes occur, get notified of audit events, as well as remotely receiving log file information from the server.

The following sections in this guide will work through in more detail, each of what has been discussed above.

Administration API Package Documentation

The Administration API is provided in the package `com.pcbsys.nirvana.nAdminAPI`

The API documentation is available in the *Universal Messaging Reference Guide* section of the documentation.

Namespace Objects

nRealmNode

Universal Messaging's namespace contains objects that can be administered, monitored and configured. The `nRealmNode` object in the `nAdminAPI`, corresponds to a Universal Messaging Realm server process. The `nRealmNode` is used to make an admin connection to a realm.

In order to connect to a realm you need to ensure you are familiar with the concept of an `RNAME`. Once you have the `RNAME` that corresponds to your realm, you can then construct the `nRealmNode` and connect to the corresponding realm. This is achieved by the following calls:

Java:

```
String[] RNAME={"nsp://127.0.0.1:9000"};
nSessionAttributes nsa=new nSessionAttributes(RNAME);
nRealmNode realm = new nRealmNode(nsa);
```

C++:

```
std::string rName = "nsp://127.0.0.1:9000";
nSessionAttributes* nsa=new nSessionAttributes(rName);
nRealmNode* realm = new nRealmNode(nsa);
```

By constructing an `nRealmNode`, and connecting to a realm, the realm node will automatically begin receiving status information from the realm periodically, as well as when things occur.

nRealmNode

The `nRealmNode` is the root of a Universal Messaging Realm's namespace, which is a tree like structure that contains child nodes. The tree nodes are all subclasses of a base class `nNode`. Each node corresponds to one of the following node subclasses:

- **nRealmNode** - other realm nodes that have been added to this realm's namespace
- **nContainer** - folders, if there was a channel called `/eur/uk/rates`, there would be a child `nContainer` node called, 'eur' which would have a child called 'uk' etc.
- **nLeafNode** - these correspond to channels and queues
- **nDurableNode** - represents the status of a durable object.

The `nRealmNode` itself is a subclass of the `nContainer` class. To obtain an enumeration of all child nodes within a realm node, simply call the following:

Java:

```
Enumeration children = realm.getNodes();
```

C#:

```
System.Collections.IEnumerator children = realm.getNodes();
```

C++:

```
fSortedList nodes = pNode->getNodes();
```

Once you have this enumeration of nodes, you can then perform the various operations on those nodes available through the `nAdminAPI`.

If you know the name of the child node you wish to obtain a reference to, you can use the following method:

Java:

```
nNode found = realm.findNode("/eur/uk/rates");
```

C++:

```
nNode* found = realm->findNode("/eur/uk/rates");
```

Which should return you an `nLeafNode` that corresponds to the channel called `'/eur/uk/rates'`.

As well as obtaining references to existing nodes, it is also possible to create and delete channels and queues using the `nRealmNode`. For example, to create a channel called `'/eur/fr/rates'`, we would write the following code:

```
nChannelAttributes cattrib = new nChannelAttributes();
cattrib.setMaxEvents(0);
cattrib.setTTL(0);
cattrib.setType(nChannelAttributes.SIMPLE_TYPE);
cattrib.setName("/eur/fr/rates");
nLeafNode channel = realm.createChannel(cattrib);
```

C++:

```
nChannelAttributes* cattrib = new nChannelAttributes();
cattrib->setMaxEvents(0);
cattrib->setTTL(0);
cattrib->setType(nChannelAttributes.SIMPLE_TYPE);
cattrib->setName("/eur/fr/rates");
nLeafNode* channel = realm->createChannel(cattrib);
```

To remove channel or a queue, you can simply call the following method on your realm node (using the channel created above):

```
realm.delLeafNode(channel);
```

C++:

```
realm->delLeafNode(channel);
```

For more information on Universal Messaging Administration, please see the API documentation, and the [“Enterprise Manager Guide” on page 11](#).

nLeafNode (Channels and Queues)

Before you use the administration objects associated with the namespace of a realm, you should understand:

- The concept of the Universal Messaging Namespace, as discussed in the nRealmNode guide (see [“nRealmNode” on page 443](#)).
- The publish/subscribe and message queue functions of Universal Messaging.
- The concept of the nRealmNode and how to create it.

nLeafNode

The nLeafNode is either a channel or a queue, and is, as its name suggests, an end point of a branch of the namespace tree. The parent of an nLeafNode is always an instance of nContainer. Since nRealmNode is a subclass of nContainer, sometimes the parent of an nLeafNode is also an instance of an nRealmNode. For example, consider the following 2 channels within the namespace:

```
/eur/uk/rates
/rates
```

The nLeafNode that corresponds to the channel '/eur/uk/rates' will have a parent which is an instance of nContainer, and is called 'uk', whereas the nLeafNode that corresponds to the channel '/rates' has a parent which is also an instance of nContainer, however it is also an instance of an nRealmNode (i.e. the namespace root), since it does not contain any folder information in its name.

When channels and queues are created, they are added to the tree structure of the nRealmNode as nLeafNodes. Universal Messaging adds the nLeafNode automatically, but will send notifications to indicate that the namespace structure has changed so that the application handles the changes. For more details about managing the structure, see the "Management Information" section in this guide.

To determine if an nLeafNode is a channel or a queue, you can use one of the methods in the following code snippets to search the namespace and print out whether each leaf node it finds is a channel or a queue.

Example : Find channels and queues in the namespace

Java:

```
public void searchNodes(nContainer container)
    Enumeration children = container.getNodes();
    while (children.hasMoreElements()) {
        nNode child = (nNode)children.nextElement();
        if (child instanceof nContainer) {
            searchNodes((nContainer)child);
        } else if (child instanceof nLeafNode) {
            nLeafNode leaf = (nLeafNode)child;
            if (leaf.isChannel) {
```

```
        System.out.println("Leaf Node "+leaf.getName()+" is a channel");
    } else if (leaf.isQueue()) {
        System.out.println("Leaf Node "+leaf.getName()+" is a queue");
    }
}
}
```

C#:

```
public void searchNodes(nContainer container)
System.Collections.IEnumerator children = realm.getNodes();
while (children.MoveNext()){
    nNode child = (nNode)children.Current;
    if (child is nContainer) {
        searchNodes((nContainer)child);
    } else if (child is nLeafNode) {
        nLeafNode leaf = (nLeafNode)child;
        if (leaf.isChannel) {
            Console.WriteLine("Leaf Node "+leaf.getName()+" is a channel");
        } else if (leaf.isQueue()) {
            Console.WriteLine("Leaf Node "+leaf.getName()+" is a queue");
        }
    }
}
}
```

C++:

```
void searchNodes(fSortedList nodes)
    for (fSortedList::iterator iterator = nodes.begin(); iterator != nodes.end();
        iterator++)
    {
        nNode *pNode = iterator->second;
        int type = pNode->getType ();
        if (type == fBase::LEAFNODE)
        {
            if(iterator->second->isChannel()){
                printf("Leaf Node %s is a Channel");
            } else if(iterator->second->isQueue()){
                printf("Leaf Node %s is a Queue");
            }
        }
        else if (type == fBase::CONTAINER)
        {
            searchNodes(((nContainer*)pNode)->getNodes());
        }
    }
}
```

In the above code example, by the `searchNodes(realm)` method searches the namespace from the realm node, and this `isChannel()` and `isQueue()` methods are used to determine whether each leaf node is a queue or a channel.

Associated with each leaf node, is the `nChannelAttributes` for the queue or channel, this is obtained by using the `getAttributes()` method, so it is possible to determine the characteristics of each leaf node.

Each leaf node also has an associated `nACL` object that can be modified to change security permissions for users. This is discussed in more detail in the security section of this guide.

For more information on Universal Messaging Administration, please see the API documentation, and the Enterprise Manager Guide.

nDurableNode

Before you use the administration objects associated with the namespace of a realm, you should understand:

- The concept of the Universal Messaging Namespace, as discussed in the nRealmNode guide (see “nRealmNode” on page 443).
- The publish/subscribe and message queue functions of Universal Messaging.
- The concept of the nRealmNode and how to create it.
- The concept of the nTopicNode and how to access it from the namespace of a realm.

nDurableNode

nDurableNode represents the status of a durable object in a Universal Messaging namespace.

When a durable node is created, it is added to the tree structure of the nRealmNode as an nDurableNode. Universal Messaging adds the nDurableNode automatically, and will send notifications to indicate that the namespace structure has changed so that the application handles the changes. For more details about managing the structure, see the "Management Information" section in this guide.

To access the durable nodes associated with a channel/topic, you can use one of the methods in the following code snippets to search the namespace for:

- the name of a specific durable node
- the list of the durable nodes associated with the topic
- the iterator of the durable nodes associated with a channel/topic

Example: Find a durable node associated with the topic node based on the name of that durable node.

Java:

```
nDurableNode durableNode = topicNode.getDurable(durable_name);
```

Example: List the durable nodes associated with the topic node.

Java:

```
List<nDurableNode> durableNodeList = topicNode.getDurableList()
```

Example: Get the iterator of durable nodes associated with the topic node and then use it to iterate through the durable nodes.

Java:

```
Iterator<nDurableNode> iterator = topicNode.getDurables()
```

The `nDurableNode` class determines the durable characteristics using APIs, such as `isSerial()`, `isShared()`, and `isClusterWide()`. Status information of the durable object, such as `lastReadTime`, `lastWriteTime`, `depth`, is updated periodically by the server. To configure the time interval, use the `StatusBroadcast` realm configuration property. The default is 5 seconds.

Before fetching the `nDurableNode` from `topicNode`, set the application to wait for durables to get updated in the namespace using `nRealmNode# waitForDurableInformation()`. To determine whether the `nDurableNode` status is updated by the server for the first time, use `nDurableNode# isStatusInitialised()`. `true` indicates that the durable node receives the first update from the server.

For more information on administering `nDurableNode` APIs, see the API documentation.

Realm Federation

A Universal Messaging Realm is an instance of the server and a container for resources. Each Universal Messaging Realm defines a namespace of its own but it is possible to merge the namespaces of multiple Realms into one large one. This is known as *realm federation*.

Note:

Clustering and Realm Federation are mutually exclusive. If a realm is a member of a cluster, you cannot use the realm for federation. Similarly, if a realm is part of a federation, the realm cannot be used for clustering.

While adding a Universal Messaging Realm into the namespace of another, there is one compulsory options and two optional. The compulsory option is the `RNAME` of that Realm. The optional parameter is the mount point that the Realm should be added in the existing Realm.

If you are specifying the name of the Realm you are adding it should be specified exactly as it appears in the Enterprise Manager. It appears adjacent to the globe icon specifying the realm to which this realm is being added.

A Universal Messaging Realm can also be added to another Realm's namespace using the Enterprise Manager (see [“Realm Federation” on page 448](#)).

A Realm is added into the namespace of another programmatically as follows.

Java, C#:

```
//Create an instance of the Universal Messaging Realm object to be added
String rname = "nsp://remoteHost:9002";
nRealm nr = new nRealm( realmName, rname);
//Set the mountpoint in the local realm's Namespace
nr.setMountPoint( mountPnt );
//Add the remote realm to the local one.
//assuming mySession has already been connected to your local realm
mySession.addRealm( nr );
```

C++

```
//Create an instance of the Universal Messaging Realm object to be added
string rname = "nsp://remoteHost:9002";
nRealm* nr = new nRealm( realmName, rname);
```

```
//Set the mountpoint in the local realm's Namespace
nr->setMountPoint( mountPnt );
//Add the remote realm to the local one.
//assuming mySession has already been connected to your local realm
mySession->addRealm( nr );
```

Example Usage of a Federated Universal Messaging Namespace

You can then provide filters for channel joins across the multiple realms you have added to the namespace. This allows you to ensure that events are routed to the correct channel based on the content of the event.

Note:

For a description of the general principles involved in creating channel joins, see the section *Creating Channel Joins*. The description details the usage based on the Enterprise Manager, but the same general principles apply if you are using the API.

For example, if channel1 on Realm1 is joined to channels channel2, channel3, channel4, channel5 on realms Realm2, Realm3, Realm4, Realm5, and each event is published using an nEventProperties dictionary that contains a key called 'DESTINATION'.

If each channel join from channel1 is created with a filter, for example for the join from channel1 to channel2 on Realm2 the filter would be:

```
DESTINATION='realm2'
```

This guarantees only those events that are published to channel1 and that contain 'realm2' in the 'DESTINATION' key will be published to channel2 on Realm2.

For further example code demonstrating adding Universal Messaging Realms to a names space please see the addRealm example.

Channel Join

Joining a channel to another allows you to set up content routing such that events on the source channel will be passed on to the destination channel also. Joins also support the use of filters thus enabling dynamic content routing.

Channels can be joined using the Universal Messaging Enterprise Manager GUI or programmatically.

In joining two Universal Messaging channels there is one compulsory option and two optional ones. The compulsory option is the destination channel. The optional parameters are the maximum join hops and a JMS message selector to be applied to the join.

Note:

For a description of the general principles involved in creating channel joins, see the section *Creating Channel Joins* in the *Administration Guide*. The description details the usage based on the Enterprise Manager, but the same general principles apply if you are using the API.

Channel joins can be created using the nmakechanjoin join sample application which is provided in the <InstallDir>/UniversalMessaging/server/<InstanceName>/bin directory of the Universal

Messaging installation. For further information on using this example please see the [nmakechanjoin](#) example page.

Universal Messaging joins are created as follows:

Java, C#:

```
//Obtain a reference to the source channel
nChannel mySrcChannel = mySession.findChannel( nca );
//Obtain a reference to the destination channel
nChannel myDstChannel = mySession.findChannel( dest );
//create the join
mySrcChannel.joinChannel( myDstChannel, true, jhc, SELECTOR );
```

C++:

```
//Obtain a reference to the source channel
nChannel* mySrcChannel = mySession->findChannel( nca );
//Obtain a reference to the destination channel
nChannel* myDstChannel = mySession->findChannel( dest );
//create the join
mySrcChannel->joinChannel( myDstChannel, true, jhc, SELECTOR );
```

Realm Server Management

Interfaces

Universal Messaging Realm servers provide the ability for connections to be made using any available physical network interface on the server machine. For example, if a machine has 4 physical network interfaces, Universal Messaging provides the ability to bind specific network interface addresses to specific ports and different protocols. This provides the ability to run segment the communication between client and server. There is no limit to the number of separate interfaces that can be run on a Universal Messaging realm server.

For example, a Realm Server that is visible to Internet users may have 4 Network cards, each one having its own physical IP address and hostname. Two of the network interfaces may be externally visible, while the other 2 may be only visible on internal sub-nets.

The 2 external interfaces may be specified as using `nhp`, and `nhps` on ports 80 and 443 respectively, since for firewall purposes, these ports are the most commonly accessible ports to external clients connecting to the realm. The remaining internal interfaces, visible to internal client connections do not have the same restrictions, and so could be defined as using `nsp` and `nsps` protocols on other ports, say 9000 and 9002 respectively.

What this guarantees is separation of internal and external connections based on network interface and protocol.

nInterfaceManager

When you have connected to a realm, and have a reference to an `nRealmNode` object (see [“nRealmNode” on page 443](#)), you can access an object called `nInterfaceManager`, which provides

the ability to add, modify, delete, stop and start interfaces on the Universal Messaging realm. To get access to this object, you can call the following method from a realm node:

Java, C#:

```
nInterfaceManager iMgr = realm.getInterfaceManager();
```

C++:

```
nInterfaceManager* iMgr = realm->getInterfaceManager();
```

Using the `nInterfaceManager` object you can then obtain a list of known interfaces for that realm:

Java:

```
Vector ifaces = iMgr.getInterfaces();
```

C#:

```
List ifaces = iMgr.getInterfaces();
```

C++:

```
int numInterfaces; nInterfaceStatus** pTemp = iMgr->getInterfaces(numInterfaces);
```

All interfaces extend a base class called `nInterface`. There are 4 types of interface object that correspond to the different types of protocols that an interface can use. These are:

- `nSocketInterface` - standard socket interface, Universal Messaging protocol is `nsp`
- `nHTTPInterface` - http interface, Universal Messaging protocol is `nhp`
- `nSSLInterface` - ssl socket interface, Universal Messaging protocol is `nspS`
- `nHTTPSInterface` - https interface, Universal Messaging protocol is `npps`

Each of these interface objects contain standard configuration information and allows the same operations to be performed on them. For example, if there is an interface called 'nsp1', and you wanted to change the 'autostart' property to true (i.e. make the interface start automatically when the realm is started) this can be achieved with the following code:

Java, C#:

```
nInterface iface = iMgr.findInterface("nsp0");
iface.setAutostart(true);
iMgr.modInterface(iface);
```

C++:

```
nInterface* iface = iMgr->findInterface("nsp0");
iface->setAutostart(true);
iMgr->modInterface(iface);
```

Which will modify the interface configuration at the server, stop and restart the interface. When performing a `modInterface` operation, if you are modifying the interface that your `nRealmNode` is connected to, you will be disconnected and reconnected when the interface restarts. This is important to remember when using the stop method of an interface too, since if you stop the

interface you are connected to, you cannot start it again, since your connection needs to be active, and the stop operation will close your connection. If you wish to restart an interface you should therefore do it from a connection which has been made via another interface.

Example: creating an NHPS interface

You can create an NHPS interface using code such as the following:

```
nRealmNode rnode = ...;
nHTTPSInterface nhps = new nHTTPSInterface("0.0.0.0", 9443,
autoStart);
nhps.setKeyStore(keystore);
nhps.setKeyStorePassword(kpass);
nhps.setPrivateKeyPassword(kpass);
nhps.setTrustStore(tstore);
nhps.setTrustStorePassword(tpass);
rnode.getInterfaceManager().addInterface(nhps);
```

Config

Universal Messaging Realm servers contain a large number of configurable parameters. These parameters can be modified using the `nAdminAPI`.

The Universal Messaging Realm config can also be managed via the Realm enterprise manager (see [“Realm Configuration” on page 35](#)). This also provides a useful guide to the configuration groups and their specific config entities.

nConfigGroup

When connected to a realm, and using a reference to an `nRealmNode` object (see [“nRealmNode” on page 443](#)), you can access configuration objects that correspond to a group of configuration entries. To get access to the config groups, call the following method from a realm node:

Java, C#

```
Enumeration children = realm.getNodes();
```

C++

```
fSortedList nodes = pNode->getNodes();
```

The enumeration will contain a number of `nConfigGroup` objects. Each `nConfigGroup` contains a number of `nConfigEntry` objects, each one corresponds to a specific configurable parameter in the realm server.

For example, to change the log level of the realm server, we need to obtain the config group called 'Logging Config' and set the 'fLoggerLevel' property:

Java, C#:

```
nConfigGroup grp = realm.getConfigGroup("Logging Config");
nConfigEntry entry = grp.find("fLoggerLevel");
entry.setValue("0");
```

C++

```
nConfigGroup* grp = realm->getConfigGroup("Logging Config");
nConfigEntry* entry = grp->find("fLoggerLevel");
entry->setValue("0");
```

For a definitive list of available configuration groups and their specific properties please see [“Realm Configuration” on page 35](#) in the enterprise manager guide.

For more information on Universal Messaging Administration, please see the API documentation, and the Enterprise Manager Guide.

Clustering

Universal Messaging provides the ability to group Realm servers together to form a cluster. A cluster is a logical group of realm servers that share common resources. The resources and any operations performed on them are replicated across all cluster members. Clients connecting to 'Realm A' in cluster 1, are able to access the same logical objects as clients connecting to Realms B or C in cluster1.

The state of these objects is fully replicated by each realm in the cluster. For example, if you create a queue (queue1) within cluster 1, it is physically created in realms A, B and C. If there are 3 consumers on queue1, say one on each of realms A, B and C respectively, each realm in the cluster will be aware as each message is consumed and removed from the different physical queue1 objects in the 3 realms.

If one of the realms within cluster1 stops, due to a hardware or network problems, then clients can automatically reconnect to any of the other realms and start from the same point in time on any of the other realms in the cluster.

This ensures a number of things:

- **Transparency** - Any client can connect to any Universal Messaging realm server within a cluster and see the same cluster objects with the same state. Clients disconnected from one realm will automatically be reconnected to another cluster realm.
- **24 x 7 Availability** - If one server stops, the other realms within the cluster will take over the work, providing an always on service

nClusterNode

Using the nAdmin API, if you wish to create a cluster that contains 3 realms, and you know the RNAME values for all 3, then the following call will create the cluster.

Java, C#, C++:

```
String[] RNAME= {"nsp://127.0.0.1:9000",
"nsp://127.0.0.1:10000","nsp://127.0.0.1:11000"};
nRealmNode realms[] = new nRealmNode[RNAME.length];
nClusterMemberConfiguration[] config = new nClusterMemberConfiguration[RNAME.length];
for (int x = 0; x < RNAME.length; x++) {
    // you don't have to create the realm nodes
    // here, since the member configuration will create
```

```
// them for you from the RNAME values
realms[x] = new nRealmNode(new nSessionAttributes(RNAME[x]));
config[x]=new nClusterMemberConfiguration(realms[x], true);
}
nClusterNode cluster = nClusterNode.create("cluster1", config);
```

Once the cluster node is created, each realm node within the cluster will know of the other realms within the cluster, and be aware of the cluster they are part of. For example, calling the following method:

Java, C#, C++:

```
nClusterNode cluster = realms[0].getCluster();
```

will return the cluster node just created with the realm with nsp://127.0.0.1:9000 for an RNAME.

Cluster nodes contain information about the member realms (nRealmNode objects) as well as the current state of the cluster members. This information can be found by calling the `getClusterConnectionStatus()` method on the cluster node, which returns a vector of nClusterStatus objects, each of which corresponds to a realm.

nRealmNode

Once a realm becomes part of a cluster, channels and queues can be created that are part of the cluster, as well as standard local resources within the realms. For example, if you were to use the following calls:

Java, C#, C++:

```
nChannelAttributes cattrib = new nChannelAttributes();
cattrib.setMaxEvents(0);
cattrib.setTTL(0);
cattrib.setType(nChannelAttributes.PERSISTENT_TYPE);
cattrib.setClusterWide(true);
cattrib.setName("clusterchannel");
nLeafNode=.createChannel(cattrib);
realms[0].createChannel(cattrib);
```

This would create a channel that is visible to all realms within a cluster. Any administrative changes made to this channel such as ACL modifications will also be propagated to all cluster members in order for the channel to be kept in sync across all realms.

Inter-Cluster Connections

Inter-cluster connections can be created programmatically through the Administration API. To do this, connect to a realmNode in each cluster and then do the following:

Java, C#, C++:

```
cluster1realm1.getCluster().registerRemoteCluster(cluster2realms1.getCluster());
```

Similarly, the inter-cluster connection can be removed programmatically:

Java, C#, C++:

```
cluster1realm1.getCluster().deregisterRemoteCluster(cluster2realm1.getCluster());
```

For more information on Universal Messaging Administration, please see the API documentation, and the Enterprise Manager Guide.

Multicast

A common way to add a multicast configuration is via the Enterprise Manager (see [“Adding a Multicast Configuration” on page 149](#)) but you can also do this programmatically.

Creating the nMulticastConfiguration

In order to create an nMulticastConfiguration object you need to specify two parameters:

- multicastAddress - Multicast IP address to use
- adapter - Network adapter address of your multicast configuration

Java, C#:

```
String multicastAddress = "227.0.0.98";
String adapter = "10.150.12.1";
nMulticastConfiguration mConf = new nMulticastConfiguration(multicastAddress,
adapter);
```

C++:

```
std::string multicastAddress = "227.0.0.98";
std::string adapter = "10.150.12.1";
nMulticastConfiguration* mConf = new nMulticastConfiguration(multicastAddress,
adapter);
```

Enabling multicast for cluster communication

In order to use multicast for intra-cluster communication you need to set a flag on the nMulticastConfiguration:

Java, C#:

```
mConf.setUseForCluster(true);
```

C++:

```
mConf->setUseForCluster(true);
```

Enabling multicast on DataGroups

When you create a DataGroup you have the option to enable multicast delivery. However you also need to enable multicast for DataGroups on the multicast configuration:

Java, C#:

```
mConf.setUseForDataGroups(true);
```

C++:

```
mConf->setUseForDataGroups(true);
```

Then (after the configuration has been applied) when you create a `DataGroup` you need to set the `enableMulticast` flag to true:

Java, C#:

```
boolean enableMulticast = true;
String name = "newGroup";
mySession.createDataGroup(name,enableMulticast);
```

C++:

```
bool enableMulticast = true;
std::string name = "newGroup";
mySession->createDataGroup(name,enableMulticast);
```

Applying the multicast configuration

In order to register the new configuration on the server you will need to connect to a Universal Messaging Realm and establish an `nRealmNode` (see [“nRealmNode” on page 443](#)). You can then get a reference to the `nMulticastManager`:

Java, C#:

```
nMulticastManager mMgr = realm.getMulticastManager();
```

C++:

```
nMulticastManager* mMgr = realm->getMulticastManager();
```

You can now use the `nMulticastManager` to send the new configuration to the server:

Java, C#:

```
mMgr.addMulticastConfiguration(mConf);
```

C++:

```
mMgr->addMulticastConfiguration(mConf);
```

Security

Access Control Lists

The Universal Messaging Administration API allows Access Control Lists (ACLs) to be set using the `nACL` object defines a set of `nACLEntry` objects that consist of a user subject and a value that corresponds to the operations permitted for that subject. With an `nACL` object, it is possible to added, delete and modify acl entries for specific subjects.

The nACL Object

There are subclasses of the base nACLEntry object. These are :

- nRealmACLEntry - defines permissions for a specific subject on the Universal Messaging Realm server itself
- nChannelACLEntry - defines permissions for a subject on a channel or queue

ACL Lists can contain any combination and number of user@host entries, along with Security Groups (see [“Nirvana Admin API - Nirvana Security Groups” on page 457](#)).

Nirvana Admin API - Nirvana Security Groups

The Administration API allows groups of users to be defined. These groups can then be used in ACL lists in-place of individual ACL entries for each user.

Security Groups can contain any number of users (user@host pairs), and may also include other Security Groups.

A new security group can be registered as follows:

Java, C#, C++:

```
nSecurityGroup grp = new nSecurityGroup("mySecurityGroup");
grp.add(add(new nSubject("user@host"));
realmNode.getSecurityGroupManager.registerSecurityGroup(grp);
```

The SecurityGroupManager can be used to edit memberships of multiple groups at the same time, for example:

Java, C#, C++:

```
nSecurityGroupManager mgr = realmNode.getSecurityGroupManager();
mgr.registerGroupMembers(group, members);
//Members can be a single subject(user@host), a group, or a collection
//containing many subjects, groups or a combination of these.
```

Once a security group has been registered, it can be added into ACL lists as you would normally add a user@host entry. Subsequent changes to the membership of the group will be reflected in which users have permissions for the corresponding resources.

Java, C#, C++:

```
nSecurityGroup grp = securityGroupManager.getGroup("myGroupName");
nChannelACLEntry aclEntry = new nChannelACLEntry(grp);
aclEntry.setFullPrivileges(true);
leafNode.addACLEntry(aclEntry);
```

Groups can also be deregistered from the realm. This will remove the group and will remove the group reference from all ACL lists where the group currently appears. As with the other examples, this can be done via the nSecurityGroupManager:

Java, C#, C++:

```
mgr.deregisterSecurityGroup(grp);
```

As with all ACLs in Universal Messaging, privileges are cumulative. This means that, for example, if a user is in a group which has publish permissions on a channel, but not subscribe permissions, the user will not be able to subscribe on the channel. Then, if an ACL entry is added on the channel for his specific username/host pair, with subscribe but no publish permissions, the user will then be able to both subscribe (from the non-group ACL permission), and publish (from the group ACL permission).

Deeply nested Security Groups hierarchies are generally discouraged, since this type of configuration can negatively impact the speed of checking ACLs, and may result in worse performance than a shallow hierarchy.

Realm Access Control List (nACL)

When you have connected to a realm, and have a reference to an `nRealmNode` object (see [“nRealmNode” on page 443](#)), you can access the realm's `acl` object. This object contains a list of `nRealmACLEntry` objects that represent a subject and a set permissions for various operations on a realm.

You can also, add, delete and modify `acl` entry objects. To obtain the realm `acl` object, simply call the following method from a realm node:

Java, C#:

```
nACL acl = realm.getACLs();
```

C++:

```
nACL* acl = realm->getACLs();
```

nRealmACLEntry

Once you have the `acl` object, you can then add, remove or modify `acl` entries:

To find a specific `acl` entry from the realm `acl`, you can search the `acl` using the subject. For example, if I wished to change the default permissions for the `*@*` subject (i.e. the default permission for a realm), I could use the following code:

```
nRealmACLEntry entry = acl.find("Everyone");
entry.setFullPrivileges(false);
acl.replace(entry);
realm.setACLs(acl);
```

C++:

```
nRealmACLEntry* entry = acl->find("Everyone");
entry->setFullPrivileges(false);
acl->replace(entry);
realm->setACLs(acl);
```

which would set the full privileges flag to false for the default subject.

For more information on Universal Messaging Administration, please see the API documentation, and the Enterprise Manager Guide.

Channel Access Control List (nACL)

When connected to a Universal Messaging realm server, with a reference to an `nRealmNode` object (see “[nRealmNode](#)” on page 443) it is possible to get a reference to an `nLeafNode` (see “[nLeafNode \(Channels and Queues\)](#)” on page 445) that corresponds to a channel. This can then be used to get access the node's nACL. This object contains a list of `nChannelACLEntry` objects that represent a subject and a set permissions for various operations on a channel. There is a separate `nChannelACLEntry` object for each subject that has been permissioned on the `nLeafNode`.

You can also, add, delete and modify ACL entry objects.

In order to obtain a reference to the correct channel ACL object for a channel called `"/products/prices"`, simply call the following method from a realm node:

Java, C#, C++:

```
nLeafNode chan = realm.findNode("/products/prices");
nACL acl = chan.getACLs();
```

C++:

```
nLeafNode* chan = realm->findNode("/products/prices");
nACL* acl = chan->getACLs();
```

nChannelACLEntry

Once you have the ACL object, you can then add, remove or modify acl entries:

To find a specific ACL entry from the channel ACL, the ACL object can be searched using the subject.

For example, to change the default permissions for the `*@*` subject (i.e. the default permission for the channel), the following code can be used:

Java, C#:

```
nChannelACLEntry entry = acl.find("Everyone");
entry.setFullPrivileges(false);
acl.replace(entry);
chan.setACLs(acl);
```

C++:

```
nChannelACLEntry* entry = acl->find("Everyone");
entry->setFullPrivileges(false);
acl->replace(entry);
chan->setACLs(acl);
```

which would set the full privileges flag to false for the default subject.

Click [here](#) to see example of how to modify channel ACLs programmatically or to see example of modifying ACLs using the enterprise manager.

For more information on Universal Messaging Administration, please see the API documentation, and the Enterprise Manager Guide.

Queue Access Control List

When you have connected to a realm, and have a reference to an `nRealmNode` object (see [“nRealmNode” on page 443](#)), and an `nLeafNode` (see [“nLeafNode \(Channels and Queues\)” on page 445](#)) that corresponds to a queue, you can access the node's ACL object. This object contains a list of `nChannelACLEntry` objects that represent a subject and a set permissions for various operations on a queue.

You can also, add, delete and modify acl entry objects. To obtain the queue ACL object, simply call the following method from a realm node:

Java, C#:

```
nLeafNode queue = realm.findNode("/eur/uk/orders");
nACL acl = queue.getACLs();
```

C++:

```
nLeafNode* queue = realm->findNode("/eur/uk/orders");
nACL* acl = queue->getACLs();
```

Once you have the acl object, you can then add, remove or modify acl entries:

nChannelACLEntry

To find a specific ACL entry from the queue ACL, you can search the ACL using the subject. For example, if I wished to change the default permissions for the `*@*` subject (i.e. the default permission for the queue), I could use the following code:

Java, C#:

```
nChannelACLEntry entry = acl.find("Everyone");
entry.setFullPrivileges(false);
acl.replace(entry);
queue.setACLs(acl);
```

C++:

```
nChannelACLEntry* entry = acl.find("Everyone");
entry->setFullPrivileges(false);
acl->replace(entry);
queue->setACLs(acl);
```

which would set the full privileges flag to false for the default subject.

Click [here](#) to see example of how to add queue ACLs programmatically or to see example of modifying ACLs using the enterprise manager.

For more information on Universal Messaging Administration, please see the API documentation, and the Enterprise Manager Guide.

Management Information

nRealmNode

The Universal Messaging admin API provides real time asynchronous management information on all objects within a realm server. By creating an nRealmNode (see [“nRealmNode” on page 443](#)), and connecting to a realm, information is automatically delivered to the nRealmNode object from the realm. This information is delivered periodically in summary form, and also as and when the state changes for one or all of the objects managed within a realm.

Before reading this section it may be useful to look at the management information available via the Universal Messaging enterprise manager. A full description of all Realm management screens is available in the enterprise manager guide. All functionality seen in the enterprise manager can be easily added to bespoke admin and monitoring processes as it is written entirely using the Universal Messaging Admin API.

This section discusses the following different types of information that can be obtained through the nAdmin API for the nRealmNode object:

Status Information

The nRealmNode extends nContainer, that extends nNode which is a subclass of Observable, so when the status information is received for a realm node, (by default this is every 5 seconds although it is configurable (see [“Realm Configuration” on page 35](#)) by setting the StatusBroadcast property under the Global Values config group) the nRealmNode will trigger the update callback on any known Observers. For example, if you write a class that implements the Observer interface, it can be added as an observer as follows:

Java, C#, C++:

```
realm.addObserver(this);
```

Assuming 'this' is the instance of the class implementing Observer, then the implementation of the update(Observable obs, Object obj) will be notified that the realm node has changed.

When regular status events are sent, the Observable object referenced in the update method will be the realm node that you added your observer to, and the Object will be null.

State Change Events

When events occur on a realm node that you have added an observer to, the Observable/Observer mechanism will notify you of the details of that event. For example, the following implementation of the update method of the Observer interface demonstrates how to detect that a new channel or queue has been created or deleted :

Java, C#:

```
public void update(Observable obs, Object obj){
    if (obs instanceof nContainer) {
        if (obj instanceof nLeafNode) {
            nLeafNode leaf = (nLeafNode)obj;
            nContainer cont = (nContainer)obs;
            if (cont.findNode(leaf) == null) {
                // node has been deleted
                System.out.println("Node "+leaf.getName()+" removed");
            } else {
                // node has been added
                System.out.println("Node "+leaf.getName()+" added");
            }
        }
    }
}
```

C++:

```
void ObservableMapping::update(Observable *pObs, void *pObj)
{
    if (obs->getType() == fBase::CONTAINER) {
        if (obj->getType() == fBase::LEAFNODE) {
            nLeafNode leaf = (nLeafNode*)obj;
            nContainer cont = (nContainer*)obs;
            if (cont->findNode(leaf)) {
                // node has been deleted
                printf("Node %s removed", leaf->getName());
                System.out.println("Node "+leaf.getName()+" removed");
            } else {
                // node has been added
                printf("Node %s added", leaf->getName());
            }
        }
    }
}
```

Any changes to the realm ACL will also use the same notification mechanism. For example, if an ACL entry was changed for a realm, the update method would be fired calling with the realm node object and the nACLEntry that had been modified.

Logging and Audit

An nRealmNode allows you to asynchronously receive realm log file entries as well as audit file entries as they occur.

Firstly, for receiving asynchronous log file entries, there is an interface called nLogListener which your class must implement. This interface defines a callback method called report(String) that will deliver each new log entry as a string. Once implemented, the following call will add your log listener to the realm node:

Java, C#, C++:

```
realm.addLogListener(this);
```

Assuming 'this' is the instance of the class implementing the nLogListener interface.

The following is an example of the report(String) method implementation:

Java, C#:

```
public void report(String msg) {
    System.out.println("LOG "+msg);
}
```

C++:

```
printf("Log : %s\n", msg);
```

Secondly, realm servers provide an audit file that tracks object creations and deletions, acl changes, connection attempts and failures. This information can be very useful for tracking who has created ACL entries for example and when they were done.

This information, as with log file entries can be asynchronously received by implementing an interface called `nAuditListener`. This interface defines a callback method called `audit(nAuditEvent)` that delivers contains the details of the audit entry. Once implemented, the following call will add your log listener to the realm node:

Java, C#, C++:

```
realm.addAuditListener(this);
```

Assuming 'this' is the instance of the class implementing the `nAuditListener`.

For more information on Universal Messaging Administration, please see the API documentation, and the Enterprise Manager Guide.

nClusterNode

Universal Messaging's admin API provides real time asynchronous information on all objects within a realm server. By creating an `nRealmNode` (see [“nRealmNode” on page 443](#)), and connecting to a realm, information is automatically delivered to the realm node from the realm. This information is delivered periodically in summary form, and also as and when the state changes for one or all of the objects managed within a realm.

Before reading this section it may be useful to look at the management information available via the Universal Messaging enterprise manager. A full description of all Realm management screens is available in the enterprise manager guide. All functionality seen in the enterprise manager can be easily added to bespoke admin and monitoring processes as it is written entirely using the Universal Messaging Admin API.

This section discusses the following different types of information that can be obtained through the `nAdmin` API for the `nClusterNode` object. The `nClusterNode` corresponds to a cluster that 2 or more realms are members of. Each `nRealmNode` will have access to its cluster node object once it has been added to a new or existing cluster:

Status Information

Firstly, in order to detect that a cluster node has been created, one has to observe the realm to which you are connected. When the realm is added to a cluster, the Observer/Observable mechanism will notify you of the cluster creation.

As well as implementing the Observer interface to detect new clusters, there is an interface that can be used to be notified of specific cluster events when clusters already exist. This interface is the `nClusterEventListener`. The interface defines various methods that enable your program to receive callbacks for specific cluster events. When the status changes for a cluster node, this will trigger an callback on any known listeners of the `nClusterNode`. For example, when you have constructed your `nRealmNode`, if your class implements the `nClusterEventListener` interface, then we can do the following:

Java, C#:

```
realm.addObserver(this);
nClusterNode cluster = realm.getCluster();
if (cluster != null) {
    cluster.addListener(this);
}
```

C++:

```
pRealm->addObserver(this);
nClusterNode *pCluster = pRealm->getCluster();
pCluster->addListener(this);
```

If the realm is not part of a cluster, then the `getCluster()` method will return null. However, by adding an observer to the realm, if a cluster is created that contains the realm you are connected to, the `update()` method of the Observer implementation will notify you that a cluster has been created. For example, the following code demonstrates how to detect if a cluster has been created with the realm you are connected to as a member:

Java, C#:

```
public void update(Observable o, Object arg) {
    if (arg instanceof nClusterNode) {
        System.out.println("New cluster formed, name = "+ (nClusterNode)arg.getName());
        ((nClusterNode)arg).addListener(this);
    }
}
```

C++:

```
nNode *pNode = iterator->second;
int type = pNode->getType ();
if (type == fBase::LEAFNODE)
{
    ((nLeafNode*)pNode)->addListener(new nChannelWatch((nLeafNode*)pNode, this));
}
```

For more information on how to monitor cluster nodes programmatically please see the appropriate code example.

For more information on how to monitor cluster nodes using the enterprise manager please see the enterprise manager guide.

For more information on Universal Messaging Administration, please see the API documentation and the Enterprise Manager Guide.

nLeafNode

Universal Messaging's admin API provides real time asynchronous information on all objects within a realm server. By creating an nRealmNode (see [“nRealmNode” on page 443](#)), and connecting to a realm, information is automatically delivered to the realm node from the realm. This information is delivered periodically in summary form, and also as and when the state changes for one or all of the objects managed within a realm.

Before reading this section it may be useful to look at the management information available via the Universal Messaging enterprise manager. A full description of all Realm management screens is available in the enterprise manager guide. All functionality seen in the enterprise manager can be easily added to bespoke admin and monitoring processes as it is written entirely using the Universal Messaging Admin API.

This section will discuss the basic information that can be obtained through the nAdmin API for the nLeafNode object:

Status Events

The nLeafNode extends nNode which is a subclass of Observable, so when the status information is received for a leaf node, (this occurs only when things change on the channel or queue, i.e. acl, connections, events published / consumed etc) the nLeafNode will trigger the update callback on any known Observers. For example, if you write a class that implements the Observer interface, then we can do the following:

Java, C#:

```
Enumeration children = realm.getNodes();
while (children.hasMoreElements());
    nNode child = (nNode)children.nextElement();
    if (child instanceof nLeafNode) {
        child.addObserver(this);
    }
}
```

C++:

```
pNode->addObserver(this);
pNode->addConnectionListener(new nRealmWatch(this));
fSortedList nodes = registerNodes(pNode->getNodes());
for (fSortedList::iterator iterator = nodes.begin(); iterator != nodes.end();
iterator++)
{
    if (type == fBase::LEAFNODE)
    {
        ((nLeafNode*)pNode)->addListener(new nChannelWatch((nLeafNode*)pNode,
this));
    }
}
```

Assuming 'this' is the instance of the class implementing Observer, then the implementation of the update(Observable obs, Object obj) will be notified that the leaf node has changed.

When events occur on a leaf node that you have added an observer to, the Observable/Observer mechanism will notify you of the details of that event. For example, the following implementation of the update method of the Observer interface demonstrates how to detect that a channel or queue acl has been added or deleted:

Java, C#:

```
public void update(Observable obs, Object obj){
    if (obs instanceof nLeafNode) {
        if (obj instanceof nACLEntry) {
            nLeafNode leaf = (nLeafNode)obs;
            nACLEntry entry = (nACLEntry)obj;
            if (leaf.isChannel()) {
                // acl modified / added / deleted
                System.out.println("Channel "+leaf.getName()+" acl event for
"+entry.getSubject());
            } else {
                // acl modified / added / deleted
                System.out.println("Queue "+leaf.getName()+" acl event for
"+entry.getSubject());
            }
        }
    }
}
```

C++:

```
void ObservableMapping::update(Observable *pObs, void *pObj)
{
    if (obs->getType() == fBase::LEAFNODE) {
        if (obj->getType() == fBase::ACLENTY) {
            nLeafNode leaf = (nLeafNode*)obs;
            nACLEntry entry = (nACLEntry*)obj;
            if (leaf->isChannel()) {
                // acl modified / added / deleted
                printf("Channel %s acl event for %s",leaf->getName(),+entry->getSubject());
            } else {
                // acl modified / added / deleted
                printf("Queue %s acl event for %s",leaf->getName(),+entry->getSubject());
            }
        }
    }
}
```

For more information on Universal Messaging Administration, please see the API documentation, and the Enterprise Manager Guide.

Connection Information

Universal Messaging's admin API provides real time asynchronous information on all objects within a realm server. By creating an `nRealmNode` (see [“nRealmNode” on page 443](#)), and connecting to a realm, information is automatically delivered to the realm node from the realm. This information is delivered periodically in summary form, and also as and when the state changes for one or all of the objects managed within a realm.

Before reading this section it may be useful to look at the management information available via the Universal Messaging enterprise manager. A full description of all Realm management screens is available in the enterprise manager guide. All functionality seen in the enterprise manager can be easily added to bespoke admin and monitoring processes as it is written entirely using the Universal Messaging Admin API.

This section will discuss the connection information that is available through the nAdmin API for the nRealmNode and the nLeafNode objects:

nRealmNode Connections

The nRealmNode provides the ability to be notified of connections to the realm, and when connections are closed. When a client attempts a connection, a callback will be made that gives the details of the connection, such as the user name, hostname, protocol and connection id. When a user connection is closed, again, you will receive notification. This information can be useful for monitoring activity on a realm.

In order to receive this kind of information, you need to implement the nConnectionListener class. This class defines 2 methods, newConnection and delConnection. To receive notifications, you can use the following method:

Java, C#, C++:

```
realm.addConnectionListener(this);
```

Assuming 'this' is the instance of the class implementing nConnectionListener, then the implementation of the newConnection and delConnection methods will be notified when connections are made or closed with the realm.

nLeafNode Connections

Universal Messaging provides the ability to issue notifications of connections to leaf nodes. Connections to leaf nodes correspond to subscriptions on a channel, so when a user subscribes to a channel or removes the subscription, you can be notified. Notification is via a callback that contains the details of the connection, such as the user name, hostname, protocol, connection id, durable name and subscription filter.

In order to receive this kind of information, you need to implement the nConnectionListener class. This class defines 2 methods, newConnection and delConnection. To receive notifications, you can use the following method:

Java, C#:

```
leafaddListener(this);
```

C++:

```
leaf->addListener(this);
```

Assuming 'this' is the instance of the class implementing nConnectionListener, then the implementation of the newConnection and delConnection methods will be notified when channel subscriptions are made or removed.

8 Configuring the Java Service Wrapper

The Java Service Wrapper is an application developed by Tanuki Software, Ltd. It is a utility program that allows an application such as a JVM to run as a Windows service or UNIX daemon.

Several components of Universal Messaging run in a Java Service Wrapper. You can configure your Universal Messaging environment by adding or modifying the Java Service Wrapper properties for each of these components.

In addition, the Java Service Wrapper offers features for monitoring the JVM, logging console output, and generating thread dumps. The following sections describe how Universal Messaging components use the features of the Java Service Wrapper.

For an overview of the Java Service Wrapper, see the cross-product document, *Software AG Infrastructure Administrator's Guide*.

Product Components that Use the Java Service Wrapper

Each of the following Universal Messaging components runs in its own dedicated Java Service Wrapper:

- The Universal Messaging realm server, located under `<InstallDir>/UniversalMessaging/server/<InstanceName>/bin`, where `<InstanceName>` is the name of the realm server instance. If there are multiple realm servers, each instance runs in its own Java Service Wrapper.
- The Enterprise Manager and the Enterprise Viewer, located under `<InstallDir>/UniversalMessaging/java/<InstanceName>/bin`
- All of the Java sample applications, located under `<InstallDir>/UniversalMessaging/java/<InstanceName>/bin`.
- The certificate generator, server configurator, and interface configurator server applications under `<InstallDir>/UniversalMessaging/server/<InstanceName>/bin`.

The Java Service Wrapper Configuration Files

When you start a Java Service Wrapper, properties in configuration files determine the configuration of the Java Service Wrapper and the behavior of the logging and monitoring features. There is typically one configuration file per wrapper that determines a default set of properties, and a

second configuration file per wrapper that determines your customized set of properties. A typical arrangement can be as follows:

File name	Description
wrapper.conf	Contains initial property settings. <i>Do not modify the contents of this file unless asked to do so by Software AG.</i>
custom_wrapper.conf	Contains properties that modify the installed settings in wrapper.conf. If you need to modify the property settings for the Java Service Wrapper, then modify this file. The settings in this file override settings in the wrapper.conf file.

Note:

The filenames wrapper.conf and custom_wrapper.conf shown here are just examples, and can be different for any given wrapper. See the following table for details.

Component	Configuration files
Command Central	<InstallDir>/profiles/CCE/configuration/wrapper.conf, custom_wrapper.conf
Software AG Platform Manager	<InstallDir>/profiles/SPM/configuration/wrapper.conf, custom_wrapper.conf
Realm Server <InstanceName>	<p><InstallDir>/UniversalMessaging/server/<InstanceName>/bin/serverdaemon.conf : this is the default Tanuki configuration for the Universal Messaging realm server.</p> <p><InstallDir>/UniversalMessaging/server/<InstanceName>/bin/Server_Common.conf : this file contains common Tanuki configuration settings for the Universal Messaging realm server. Historically the server could be started in different modes and this file would contain common configuration options.</p> <p><InstallDir>/UniversalMessaging/server/<InstanceName>/bin/Custom_Server_Common.conf : this file should be used to customize the default Tanuki configuration.</p>
Java sample applications for <InstanceName>	<p>There is a generic <InstallDir>/UniversalMessaging/java/<InstanceName>/bin/Samples_Common.conf file that provides the common settings for all sample applications.</p> <p>Additionally, each sample application has its own *.conf file in <InstallDir>/UniversalMessaging/java/<InstanceName>/bin/</p>

Component	Configuration files
Administration Tools (Enterprise Manager / Enterprise Viewer)	<p>There is a <code><InstallDir>/UniversalMessaging/java/<InstanceName>/bin/Admin_Tools_Common.conf</code> file that provides common settings for the Enterprise Manager and the Enterprise Viewer tools.</p> <p>Additionally, <code><InstallDir>/UniversalMessaging/java/<InstanceName>/bin/enterprisemgr.conf</code> provides settings for the Enterprise Manager</p> <p><code><InstallDir>/UniversalMessaging/java/<InstanceName>/bin/enterpriseview.conf</code> provides settings for the Enterprise Viewer</p>
Server applications	<p>There is a generic <code><InstallDir>/UniversalMessaging/server/<InstanceName>/bin/Server_Tools_Common.conf</code> file that provides common settings for all server applications.</p> <p>Additionally each application has its own configuration file:</p> <p><code><InstallDir>/UniversalMessaging/server/<InstanceName>/bin/CertificateGenerator.conf</code> provides settings for the certificate generator application.</p> <p><code><InstallDir>/UniversalMessaging/server/<InstanceName>/bin/ServerConfiguration.conf</code> provides settings for the server configurator application.</p> <p><code><InstallDir>/UniversalMessaging/server/<InstanceName>/bin/inconfig.conf</code> provides settings for the interface configurator application.</p>

The JVM property settings that Universal Messaging installs are suitable for most environments. However, you can modify the properties if the installed settings do not suit your needs. For procedures and additional information, see the cross-product document, *Software AG Infrastructure Administrator's Guide*.

The Wrapper Log

The Java Service Wrapper records console output in a log file. The log contains the output sent to the console by the wrapper itself and by the Universal Messaging component running in the wrapper. The wrapper log is especially useful when you run the component as a Windows service because console output is normally not available to you in this mode.

Component	Log file
Command Central	<code><InstallDir>/profiles/CCE/logs/wrapper.log</code>
Software AG Platform Manager	<code><InstallDir>/profiles/SPM/logs/wrapper.log</code>
Realm Server <code><InstanceName></code>	<code><InstallDir>/UniversalMessaging/server/<InstanceName>/bin/UMRealmService.log</code>

Logging Properties

The `wrapper.console` and `wrapper.log` properties in the wrapper configuration files determine the content, format, and behavior of the wrapper log.

The default logging settings are suitable for most environments. However, you can modify the following properties if the installed settings do not suit your needs. For procedures and additional information, see the cross-product document, *Software AG Infrastructure Administrator's Guide*.

Property	Value
<code>wrapper.console.loglevel</code>	Level of messages to display in the console.
<code>wrapper.console.format</code>	Format of messages in the console.
<code>wrapper.logfile</code>	File in which to log messages.
<code>wrapper.logfile.loglevel</code>	Level of messages to write in the log file.
<code>wrapper.logfile.format</code>	Format of messages in the log file.
<code>wrapper.logfile.maxsize</code>	Maximum size to which the log can grow.
<code>wrapper.logfile.maxfiles</code>	Number of old logs to maintain.
<code>wrapper.syslog.loglevel</code>	Level of messages to write to the Event Log on Windows systems or the syslog on UNIX.

Fault Monitoring

The Java Service Wrapper can monitor the JVM for the certain conditions and then restart the JVM or perform other actions when it detects these conditions.

The following table gives some examples. To learn more about these features, see the cross-product document, *Software AG Infrastructure Administrator's Guide*.

Feature	Enabled?	User configurable?
JVM timeout	Yes	No. Do not modify the <code>wrapper.ping</code> properties unless asked to do so by Software AG.
Deadlock detection	No	Yes. For more details see, <i>Deadlock-Detecting Properties</i> .
Console filtering	No	Yes. For more details see, <i>Console Filtering Properties</i> .

JVM Timeout Properties

The `wrapper.ping.interval` properties in the wrapper configuration files determine whether the wrapper monitors the JVM for timeout and what action it takes when a timeout occurs. The following table gives some examples.

Property	Value
<code>wrapper.ping.interval</code>	How often, in seconds, the Java Service Wrapper pings JVM to ensure that it is active. The default is 5 seconds.
<code>wrapper.ping.timeout</code>	Length of time, in seconds that the Wrapper waits for a response to a ping. Set this property to 60. If the Wrapper does not receive a response in the specified time, it initiates the action specified in <code>wrapper.ping.timeout.action</code> .
<code>wrapper.ping.timeout.action</code>	Action to take if the Wrapper does not receive a response to a ping in the allotted time. Set this property to <code>DEBUG,DUMP,RESTART</code> .

Deadlock-Detection Properties

The `wrapper.check.deadlock` properties in the wrapper configuration files determine whether the wrapper monitors the JVM for deadlocks and what action it takes when a deadlock occurs. The following table gives some examples.

Property	Value
<code>wrapper.check.deadlock</code>	Flag (TRUE or FALSE) that enables or disables deadlock detection. The default is FALSE.
<code>wrapper.check.deadlock.interval</code>	How often, in seconds, the Java Service Wrapper evaluates the JVM for a deadlock condition. The default is 60 seconds.
<code>wrapper.check.deadlock.action</code>	Action that occurs if the Java Service Wrapper detects a deadlock condition.
<code>wrapper.check.deadlock.output</code>	Information to log when the Wrapper detects a deadlock condition. Set this property to <code>DEBUG,DUMP,RESTART</code> .

Console Filtering Properties

The `wrapper.filter` properties in the wrapper configuration files determine whether the wrapper monitors the console for specified messages and what action it takes when a specified message occurs. To use console filtering, you can configure the following properties. However, Software AG recommends that you do not modify these properties unless asked to do so. The following table gives some examples.

Property	Value
<code>wrapper.filter.trigger.n</code>	String of text that you want to detect in the console output.

Property	Value
<code>wrapper.filter.action.n</code>	Action that occurs when the Java Service Wrapper detects the string of text.
<code>wrapper.filter.allow_wildcards.n</code>	Flag (TRUE or FALSE) that specifies whether the Java Service Wrapper processes wildcard characters that appear in <code>wrapper.filter.trigger.n</code> .
<code>wrapper.filter.message.n</code>	Message that displays when Java Service Wrapper detects the string of text.

Generating a Thread Dump

The Java Service Wrapper provides a utility for generating a thread dump of the JVM when running as a Windows service. A thread dump can help you locate thread contention issues that can cause thread blocks or deadlocks.

Go to the `bin` directory of the Wrapper and execute the command `service -dump`. The Java Service Wrapper writes the thread dump to the wrapper log file.

9 Thread Pool Monitoring

In addition to the thread dump generation provided by the Java Service Wrapper, you can configure the Universal Messaging realm servers to monitor the thread pool for slow-running threads and generate thread dumps when certain events occur. The thread dumps and messages generated from the user-defined monitoring of the thread pool are logged into *Software AG_directory \UniversalMessaging\server\InstanceName\data\nirvana.log*.

The thread pool monitoring generates thread dumps for stalled or slow-moving tasks, and reports reduced thread availability. Stalled tasks are tasks that run longer than the specified time. Slow-moving tasks are tasks that run slower than the timeout for the task execution. You can also set a threshold for pending tasks to monitor thread availability. You can then use the thread dump entries in the log to troubleshoot the task execution.

To ensure that the logs are not too big, you can configure the interval at which the server generates a thread dump.

Thread-Pool Monitoring Configuration Properties

You configure the thread-pool monitoring properties for a realm in the **Thread Pool Config** group on the Config tab in the Enterprise Manager.

For information about working with Universal Messaging configuration properties in the Enterprise Manager, see .

StalledTasksWarningTime

The time in milliseconds before reporting a stalled task. The system writes the information at the WARNING log level and generates a thread dump. When you change this configuration, the thread pool monitor interval is updated to monitor at the same time interval as the value you specify for this property. Valid values range from 10000 to 60000. Default is 60000.

SlowTaskWarningTime

The time in milliseconds before reporting a slow-running task. The server logs the information at the WARNING log level and generates a thread dump. Valid values range from 1000 to 30000. Default is 5000.

PendingTaskWarningThreshold

The threshold at which the server starts to warn about the number of pending tasks. When the number of pending tasks is below the threshold, but over 100, the server logs a WARNING message. When the number is above the threshold, the server logs an ERROR message. When

the server does not find available threads, it logs a message that the thread pool is exhausted. Valid values range from 100 to 100000. Default is 1000.

ThreadDumpOnSlowTask

Whether to generate a thread dump when the server reports a slow task. Valid values are true - generate a thread dump, or false - do not generate a thread dump. Default is false.

ThreadDumpInterval

The interval in milliseconds at which a thread dump is generated when the system reports slow or stalled tasks, or when the number of pending tasks exceeds the value of PendingTaskWarningThreshold. The thread dump interval applies across all thread pools in the JVM instance. Valid values range from 1000 to 600000. Default is 60000.

Examples

In the following example, the slow-moving task warning timeout is set to 1000ms and the server is configured to generate a thread dump for a slow task. The task completed in 1060ms and the server reports that the task execution time exceeds 1000ms and generates a thread dump. The following entries will show in the log:

```
[Wed Feb 17 07:39:32.790 IST 2021] [ThreadPoolTest-Slow:9] ThreadPool:
<ThreadPool-SlowTasksTest> Slow moving task detected. ThreadPool-SlowTasksTest:9 has
been active
for over 1060(ms) running task class
com.pcbsys.foundation.threads.fThreadPoolTaskReportTest$TestTask, Idle Threads 7,
Allocated
Threads 10, Queued Tasks 0, Task Executed 10
[Wed Feb 17 07:39:32.790 IST 2021] [ThreadPoolTest-Slow:0] ThreadPool:
<ThreadPool-SlowTasksTest>
Slow moving task detected. ThreadPool-SlowTasksTest:0 has been active for over 1060(ms)
running
task class com.pcbsys.foundation.threads.fThreadPoolTaskReportTest$TestTask, Idle
Threads 7,
Allocated Threads 10, Queued Tasks 0, Task Executed 10
```

```
[Wed Feb 17 07:39:41.000 IST 2021] [ThreadPoolTest-Slow:7] ThreadPool:
<ThreadPool-SlowTasksTest> Slow moving task detected. ThreadPool-SlowTasksTest:7 has
been active
for over 1020(ms) running task class
com.pcbsys.foundation.threads.fThreadPoolTaskReportTest$TestTask, Idle Threads 7,
Allocated
Threads 10, Queued Tasks 0, Task Executed 10
[Wed Feb 17 07:39:41.000 IST 2021] [ThreadPoolTest-Slow:7] Producing thread dump.
Reason : Slow
moving task detected on thread pool: ThreadPool-SlowTasksTest
```

In the following example, the threshold for pending tasks is set to 200. Because the number of pending tasks in the thread pool is 209, the server logs an error message and generates a thread dump. The following entries will show in the log:

```
[Wed Feb 17 07:39:39.949 IST 2021] [Time-limited test] ThreadPool:
<ThreadPoolTest-Pending> Pending tasks are above the threshold 200 pending tasks 209,
Idle Threads
0, Allocated Threads 1, Queued Tasks 209, Task Executed 210
[Wed Feb 17 07:39:39.949 IST 2021] [Time-limited test] Producing thread dump. Reason
: Pending
```

```
tasks are above the threshold: 200 pending tasks: 209
```

Troubleshooting Task Execution

To correct or improve the task execution, you can take the following actions:

- In the thread pool configuration, check whether you have allocated enough threads. If the logs report a large number of queued tasks, allocate more threads to the pool.
- Check for overall system slowdown, such as disk speed, network speed, CPU speed and allocation, and JVM garbage collection.
- Check for product behavior that might cause a slow performance.

10 Using Nginx with Universal Messaging

■ About Using Nginx with Universal Messaging	480
■ Configure Nginx to Direct HTTP Requests to Universal Messaging	480
■ Nginx Directives Configuration	481
■ Configure Nginx to Direct HTTPS Requests to Universal Messaging	482
■ Forward Requests Based on URL Matches	485

About Using Nginx with Universal Messaging

Nginx is open-source software for web serving, reverse proxying, caching, and load balancing. You can use Nginx as a reverse proxy server for Universal Messaging. To do so, you must configure Nginx to redirect HTTP and HTTPS traffic to Universal Messaging.

Important:

Note that Universal Messaging does not support load balancing using Nginx but only proxying.

Consider the following requirements before configuring Nginx for use with Universal Messaging:

- You must be familiar with the Nginx structure, configuration, and terminology, including the `nginx.conf` configuration file and the directives, blocks, and contexts included in it.
- You must have Nginx installed. For information about installing and configuring Nginx, see <https://nginx.org/en/docs/>.
- You must configure an `nhp` or `nhps` interface on the Universal Messaging server for redirecting HTTP or HTTPS traffic, respectively. For information about how to configure `nhp` and `nhps` interfaces, see “Creating Interfaces” on page 137 and “Creating an SSL-Enabled Interface” on page 144.

Configure Nginx to Direct HTTP Requests to Universal Messaging

Nginx provides an `http` block that includes directives for handling web traffic. The `http` block in turn includes a `server` block where you specify virtual server configurations.

To configure Nginx to serve `http` requests to Universal Messaging, add the following code to the `nginx.conf` file or to a separate `conf` file that you include in the main Nginx configuration module. If Nginx is running, you must reload it for the changes to take effect.

```
user          nginx;
worker_processes  auto;
pid           /var/run/nginx.pid;
#Set the number of open file descriptors configuration according to the resource limits
  of the machine.
worker_rlimit_nofile  25000;
events {
    #Set this configuration according to the resource limits of the machine.
    worker_connections  20000;
}
http {
    #Log settings. You can customize them as required.
    log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
        '$status $body_bytes_sent "$http_referer" '
        '"$http_user_agent" "$http_x_forwarded_for"';

    #The server closes idle connections after this timeout.
    keepalive_timeout  300s;

    #The number of requests that the client can make over a single connection.
    keepalive_requests 1000000;
```

```

    #Required setting because the UM client sends "User-Agent: Mozilla/4.0 (compatible;
    MSIE 6.0;
    #Windows NT 5.0)." The Nginx default value is 'msie6', which causes Nginx to
close
    #UM client connections.
    keepalive_disable    none;

    server {
        listen            80;
        server_name      proxy_server;
        location / {
            #Important: Nginx must continuously send data to the Universal
Messaging
            #client rather than buffering it.
            proxy_buffering    off;

            #Important: Configure proxy http protocol version 1.1 to enable the
connection
            #keepalive and specify an empty string for the connection header.
            proxy_http_version    1.1;
            proxy_set_header    Connection "";
            proxy_pass          http://umhost:port;
        }
    }
}

```

In the provided configuration, the Nginx server listens on port 80 and redirects client requests to the Universal Messaging server URL specified in the `proxy_pass` directive that is part of the server > location block.

For example, if you specify `http://umserver1host:9000` for `proxy_pass`, when a client is trying to connect to `http://nginxhost:80`, which is the address of the Nginx server, all requests to this server will be redirected to the Universal Messaging server configured at `http://umserver1host:9000`.

Ngix Directives Configuration

The following table describes the Nginx directives you must configure for redirecting both HTTP and HTTPS traffic to Universal Messaging and their required values.

Directives	Required Value	Description
<code>proxy_buffering</code>	<code>off</code>	Disable this directive for serving Universal Messaging requests because Universal Messaging does not send a content length to initial HTTP connections. This option optimizes stateless HTTP environments, but Universal Messaging uses a streaming protocol. Default is on.
<code>proxy_pass</code>	<code>http https://umhost:port</code>	The URL of the proxied Universal Messaging server. Configure Universal Messaging with either an nhp or an nhps protocol. This directive takes either an HTTP or an HTTPS protocol respectively to redirect the requests, for example, <code>http://umhost1:9000</code> or <code>https://umhost1:9100</code> .

Directives	Required Value	Description
keepalive	100	Number of keepalive idle connections that the Universal Messaging server can have. Part of the upstream directive. Keepalive settings are important when handling many client connections. This directive has no default value.
keepalive_requests	100000	Number of requests that can be served through a single keepalive connection to Universal Messaging. Software AG recommends that you set a high value. Default is 1000.
keepalive_timeout	300s	Timeout in seconds for idle connections that remain open for the specified amount of time. Default is 75s.
proxy_http_version	1.1	Set the http version to 1.1. Default is 1.0.
proxy_set_header	Connection ""	Connection headers. Set an empty value. Default is close, which closes the connections of the Universal Messaging server.

Configure Nginx to Direct HTTPS Requests to Universal Messaging

Use SSL Passthrough

With SSL passthrough, traffic passes through a proxy server to a backend server without being decrypting on the proxy server. Proxy SSL passthrough is the simplest way to configure SSL in a proxy server but is suitable only for smaller deployments.

To use SSL passthrough with Nginx, add the following code to the nginx.conf file. If Nginx is running, you must reload it for the changes to take effect.

```
server {
    listen 443 ssl;
    server_name proxy_server;

    #Setting Nginx to serve HTTPS traffic requires private keys and certificates.
    ssl_certificate      /etc/nginx/certificates/servercerts/server.pem;
    ssl_certificate_key  /etc/nginx/certificates/servercerts/server.key;
    ssl_trusted_certificate /etc/nginx/certificates/servercerts/truststore.crt;

    location / {
        #Important: Nginx must continuously send data to the Universal Messaging
        client rather than
        #buffering it.
        proxy_buffering off;
        #SSL settings for validating Nginx by the Universal Messaging server
        proxy_ssl_certificate
/etc/nginx/certificates/servercerts/server.pem;
        proxy_ssl_certificate_key
/etc/nginx/certificates/servercerts/server.key;
```

```

        proxy_ssl_trusted_certificate
/etc/nginx/certificates/servercerts/truststore.crt;

        #Important: Configure proxy http protocol version 1.1 to enable the
connection keepalive
        #and specify an empty string for the connection header.
        proxy_http_version 1.1;
        proxy_set_header Connection "";
        proxy_pass https://umhost:port;
    }
}

```

Use SSL Termination

SSL termination or offloading decrypts all HTTPS traffic on the proxy server. SSL offloading allows data to be inspected as the data passes between the proxy server and the backend server. It also reduces CPU demand on an application server by decrypting data in advance. However, SSL offloading is vulnerable to attacks because the data travels unencrypted between the proxy server and the application server.

Nginx decrypts the request before sending it to the backend server and encrypts the response before sending it to the client. This action takes extra CPU cycles to encrypt and decrypt messages.

Add the following code to the `nginx.conf` file with the `nhps` interface that you configured for your Universal Messaging server and reload Nginx:

```

server {
    listen 443 ssl;
    server_name proxy_server;
    #SSL certificates and keys
    ssl_certificate      /etc/nginx/certificates/servercerts/server.pem;
    ssl_certificate_key  /etc/nginx/certificates/servercerts/server.key;
    ssl_trusted_certificate /etc/nginx/certificates/servercerts/truststore.crt;

    location / {
        #Important: Nginx must continuously send data to the UM client rather
than buffering it.
        proxy_buffering off;

        #Important: Configure proxy http protocol version 1.1 to enable the
connection keepalive
        #and specify an empty string for the Connection header.
        proxy_http_version 1.1;
        proxy_set_header Connection "";
        proxy_pass http://umhost:port;
    }
}

```

SSL Directives

The following table describes the Nginx SSL directives to configure and their required values for redirecting HTTPS traffic to Universal Messaging.

Directives	Required Value	Description
<code>ssl_certificate</code>	<code><certificate_file_path></code>	Server certificate file in pem format.
<code>ssl_certificate_key</code>	<code><certificate_key_file_path></code>	Server private key in pem format.
<code>ssl_trusted_certificate</code>	<code><truststore_file_path></code>	File with trusted CA certificates in pem format used to verify clients.
<code>proxy_ssl_certificate</code>	<code><certificate_file_path></code>	Specifies a file with the certificate in pem format used for authentication to a proxied HTTPS server.
<code>proxy_ssl_certificate_key</code>	<code><certificate_file_path></code>	Specifies a file with the secret key in pem format used for authentication to a proxied HTTPS server. You can specify the value <code>engine:name:id</code> instead of the file (1.7.9), which loads a secret key with the specified ID from the OpenSSL engine name.
<code>proxy_ssl_trusted_certificate</code>	<code><truststore_file_path></code>	Specifies a file with trusted CA certificates in pem format used to verify the certificate of the proxied HTTPS server.

Client Code

Update the keystore and truststore certificates of the client in the session attributes in the `createSession()` method of the following program:

```
public void createSessionAndCreateChannel(String arg) throws Exception {
    nSessionAttributes attr = new nSessionAttributes("nhps://localhost:443");
    attr.setName("client");
    attr.setTruststore("C:\\certs\\truststore.jks", "nirvana");
    attr.setKeystore("C:\\certs\\myclient.jks", "nirvana");
    attr.setSSLProtocol("TLS");
    nSession session = nSessionFactory.create(attr);
    session.init();
    nChannel chan = session.createChannel(new nChannelAttributes("MyChannel"));
    session.close();
}
```

The program creates a session to the Universal Messaging sever that is specified in the `proxy_pass` location directive of the `nginx.conf` file.

When you run the program specify the Nginx HTTPS URL in the format `nhps://nginxhost:port`, for example, `nhps://localhost:443`. You can also create a channel on the Universal Messaging server with the proxied Nginx server.

Forward Requests Based on URL Matches

The Nginx `location` directive in the `nginx.conf` file enables you to route requests to a location in the file system.

While Nginx matches or searches a `location` block against the requested URL, the `location` directive tells Nginx where to search for a specific path by including all files and directories.

The `location` directive has the following syntax:

```
location [modifier] [URL-match] {
    ...
}
```

For more information about how to use regular expressions (regex) to forward requests to specific locations, see <https://www.nginx.com/blog/regular-expression-tester-nginx/>.

The following example shows how to redirect requests to specific Universal Messaging servers by using regex:

```
server {
    listen 80;
    server_name proxy_server;

    location / {
        #Important: Nginx must continuously send data to Universal Messaging
        clients
            #rather than buffering it.
            proxy_buffering off;

        #Important: Configure proxy http 1.1 protocol version to enable the
        connection
            #keepalive and rewrite the Connection header.
            proxy_http_version 1.1;
            proxy_set_header Connection "";
            proxy_pass http://umhost:port;
    }
    location /umserver1/ {
        #Important: Nginx must continuously send data to Universal Messaging
        clients
            #rather than buffering it.
            proxy_buffering off;

        #Important: Configure proxy http 1.1 protocol version to enable the
        connection
            #keepalive and rewrite the Connection header.
            proxy_http_version 1.1;
            proxy_set_header Connection "";
            proxy_pass http://umserver1host:port;
    }
    location = /umserver2 {
        #Important: Nginx must continuously send data to Universal Messaging
        clients
            #rather than buffering it.
            proxy_buffering off;
    }
}
```

```

#Important: Configure proxy http 1.1 protocol version to enable the
connection
#keepalive and rewrite the Connection header.
proxy_http_version 1.1;
proxy_set_header Connection "";
proxy_pass http://umserver2host:port;
}
}

```

In the example, traffic is redirected as follows:

- location /umserver1/ - requests that start with umserver1 are redirected to `http://umserver1host:port`.
- location = /umserver2 - requests that match the umserver2 block are redirected to `http://umserver2host:port`.
- Requests that do not match location /umserver1/ or location = /umserver2 are served by the default location directive.

Client Code Example

```

public void createSessionAndCreateChannel(String arg) throws Exception {
    // The request initiated with nhp://localhost:80/ without any endpoint is redirected
    to
    // http://umhost:port; in the code sample above.

    nSessionAttributes defaultAttr = new nSessionAttributes("nhp://localhost:80/");
    defaultAttr.setName("defaultAttr-client");
    nSession defaultServerSession= nSessionFactory.create(defaultAttr);
    defaultServerSession.init();
    nChannel chan = session.createChannel(new
nChannelAttributes("defaultServerChannel"));
    defaultServerSession.close();
    // The request initiated with nhp://localhost:80/umserver1 without any endpoint
    is
    // redirected to http://umserver1host:port; in the code sample above.

    nSessionAttributes attr1 = new nSessionAttributes("nhp://localhost:80/umserver1");
    attr1.setName("umserver1-client");
    nSession session1 = nSessionFactory.create(attr1);
    session1.init();
    nChannel chan1 = session.createChannel(new nChannelAttributes("umserver1Channel"));
    session1.close();

    // The request initiated with nhp://localhost:80/umserver2 without any endpoint
    is
    // redirected to http://umserver2host:port; in the code sample above.

    nSessionAttributes attr2 = new nSessionAttributes("nhp://localhost:80/umserver2");
    attr2.setName("umserver2-client");
    nSession session2 = nSessionFactory.create(attr2);
    session2.init();
    nChannel chan2 = session.createChannel(new nChannelAttributes("umserver2Channel"));
    session2.close();
}

```

11 Migrating from IPv4 to IPv6

Overview

If you currently use an IPv4 infrastructure for network communications, there is a general recommendation within the IT industry to move to an IPv6 infrastructure. One of the main reasons is that the number of available new IPv4 addresses has reduced to practically zero, whereas new IPv6 addresses are expected to be plentiful for a long time to come.

Universal Messaging can support an environment that uses only IPv4, or an environment that uses only IPv6, or an environment that supports a combination of IPv4 and IPv6. Universal Messaging is written in Java, which by design works seamlessly with IPv4 and IPv6 in parallel (the mechanism is called *dual stack*). If the underlying operating system and network infrastructure support dual stack, then the Universal Messaging server socket can communicate with both IPv4 and IPv6 clients at the transport layer without any changes in the source code or settings.

The server sockets that are expected to serve both IPv4 and IPv6 clients should be bound to "0.0.0.0" or ":::0", and not to any specific IPv4 or IPv6 address.

The following setups are supported:

- If your environment uses only IPv4 addressing, Universal Messaging will continue to support your environment. There is no technical requirement to move to IPv6.
- If you intend to migrate your entire environment to IPv6 addressing, Universal Messaging will in most cases continue to work after the migration without manual reconfiguration, but there are some points to watch out for. See the section *Migrating to IPv6* below for details.
- If you intend to use IPv4 addressing for some clients, and IPv6 addressing for other clients, this is also supported in Universal Messaging.

Migrating to IPv6

If you plan to migrate all of your clients from IPv4 to IPv6 addressing, Universal Messaging will in most cases work with the new IPv6 clients without needing any manual configuration changes. However, you need to check for any hard-coded IPv4 addresses in the locations mentioned below and update them accordingly before you activate the IPv6 environment:

- **The hosts file**

Check the entries in the hosts file. If required, map the host name to the required IPv6 address. On Linux, the hosts file is `/etc/hosts`, and on Windows it is typically `C:\Windows\System32\drivers\etc\hosts`.

■ The **Server_Common.conf** file

Check if `Server_Common.conf` uses a specific IPv4 address for the default adapter. If so, do the following:

- Change the default adapter to "0.0.0.0" or "::0" or hostname as per the requirement.
- Take a backup of `adapters.nst`, then delete `adapters.nst`.

The file `adapters.nst` is a binary file that contains the interface details of the realm server. It is present in `<InstallDir>/UniversalMessaging/server/<InstanceName>/data/RealmSpecific`.

- Restart the server. This will create a new `adapters.nst` file.

Also, before migrating to IPv6, check if your Universal Messaging server setup uses any other interface that was created using a specific IPv4 address. If you do not intend to support the IPv4 address any more after migration, you need to delete the interface. If, however, the IPv4 address will still be valid after migration, the interface does not need to be deleted, as Universal Messaging supports IPv4 and IPv6 at the same time.

To ensure that all of the IPv4 interface addresses that you wish to convert in a Universal Messaging realm have indeed been converted to IPv6 addresses, we suggest that you proceed as follows:

1. Export the current realm configuration to an XML file.
2. In the XML file, if there are any hard-coded IPv4 addresses that you wish to migrate, change them to either the host name or the corresponding IPv6 address.
3. If you made any changes in the XML file, import the XML file in order to update the realm to the new configuration. If you made no changes in the XML file, you can of course omit this step.

The instructions for exporting and importing a realm are given in the section “[Exporting and Importing Realm XML Configurations](#)” on page 167.

12 Data Protection and Privacy

Introduction

Legislation in various parts of the world – such as the General Data Protection Regulation (GDPR) of the European Union (EU) - specifies that personal data cannot be collected and processed without a person's consent or other legitimate basis, and that organizations are responsible for protecting personal data that is entrusted to them. The concept of “personal data” typically covers details that can be used to identify a person, such as the person's name, email address or IP address.

Note:

In the different countries of the EU, the GDPR may be known under another, language-specific name. For example, it known as the Datenschutz-Grundverordnung (DSGVO) in Germany and as Règlement Général sur la Protection des Données (RGPD) in France.

Universal Messaging includes personal data such as user names, and client IP addresses / host names in the logs. Universal Messaging includes personal data in logs for purposes of auditing, monitoring activity with the server, and diagnosing and correcting problems.

Universal Messaging is a middleware platform on which customers build their own applications. Most of the data handled by Universal Messaging is arbitrary customer-defined data whose meaning is defined by the customer who developed the application. Some of that customer-defined data may qualify as “personal data”, so if you are developing applications on the Universal Messaging platform, you should be careful to ensure compliance with laws related to that data.

If Software AG support personnel request you to send diagnostic data such as operational logs for the purposes of diagnosing product issues, and if this diagnostic data contains personal data, you should be aware that Software AG has GDPR processes in place to ensure that data is held securely and deleted when no longer needed.

Summary of Log Files used by Universal Messaging

Universal Messaging uses the log files described in the following table. The log files can contain personal data associated with a current activity, such as a user ID and client IP address. The length of time that a Universal Messaging server stores log data depends on the log.

Log	
standard server log file	<p>The log file is named <code>nirvana.log</code> and resides in the <code>server/<RealmServerName>/data</code> directory. The data remains there for as long as the log file is retained.</p> <p>When using the default Universal Messaging logger, the log file policy is defined by the <code>DefaultLogSize</code> realm server property which defines the maximum size of the log file, and the <code>RolledLogFileDepth</code> realm server property, which defines the number of log files to keep if log rolling is activated.</p> <p>The personal data can be removed by either manually removing lines from the file, or deleting a log file altogether.</p>
audit log file	<p>The audit log file is named <code>NirvanaAudit.mem</code> and resides in the <code>server/<RealmServerName>/data/RealmSpecific</code> directory. The data remains in the audit log file for as long as the file exists.</p> <p>There is no mechanism to partially remove data from this log file. The only way to remove the personal data is by deleting the <code>NirvanaAudit.mem</code> file.</p>

Ad-hoc creation of data collections

In addition to standard operational data that is collected by Universal Messaging, some data can be collected on an ad-hoc basis by the Universal Messaging administrator. Such ad-hoc data is typically written to a location on your file system.

Examples are:

Realm Information Collector

The files collected by the Realm Information Collector tool can include files that may contain personal data related to messages that are being handled by the server.

Exported Realm Configuration File

When you export a realm's configuration to an XML file for a later re-import, the XML file can contain personal data, such as user IDs and client IPs related to ACL permissions for accessing realm components.

Heap Dump

A heap dump (which Software AG may request you to generate for the purpose of diagnosing problems) may contain personal data related to messages that are being handled by the server, or the server's log files.

Protecting and erasing data from log files

As there are many situations in which user names, IP addresses or events containing personal data may be logged, including by customer-provided plug-ins and third-party libraries, it is not

practical to enumerate all of the log messages that may contain such data, or the set of categories they may be logged under.

Log files are formatted for reading by human system administrators (not machines), so rectification of data contained within them does not make sense, and erasure of data for individual persons is not practical. The retention of complete information in log files also serves an important and legitimate purpose, in providing a security audit trail, and the ability to diagnose and fix accidental or unlawful events compromising the availability, integrity or confidentiality of the application and personal data it contains.

For these reasons, the recommended approach to protecting personal data in log files is to regularly rotate the logs (also termed log rolling) in cases where log rotation is activated, and archive the old log files to a secured location protected by encryption.

