

Hitachi Content Platform for Cloud Scale

v1.2.0

System Management Guide

This document describes the System Management application, part of the Hitachi Content Platform for cloud scale (HCP for cloud scale) software, that you use to configure HCP for cloud scale for your users, enable and disable system features, and monitor the system and its connections.

© 2019 Hitachi, Ltd. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including copying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Vantara Corporation (collectively "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara Corporation at https://support.hitachivantara.com/en_us/contact-us.html.

Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara Corporation.

By using this software, you agree that you are responsible for:

1. Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals; and
2. Verifying that your data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

Hitachi and Lumada are trademarks or registered trademarks of Hitachi, Ltd., in the United States and other countries.

AIX, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, GDPS, HyperSwap, IBM, Lotus, MVS, OS/390, PowerHA, PowerPC, RS/6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z14, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, the Microsoft Corporate Logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

All other trademarks, service marks, and company names in this document or website are properties of their respective owners.

Copyright and license information for third-party and open source software used in Hitachi Vantara products can be found at <https://www.hitachivantara.com/en-us/company/legal.html>.

Contents

Preface	11
About this document.....	11
Intended audience.....	11
Product version.....	11
Release notes.....	11
Related documents.....	11
Accessing product documentation.....	12
Getting help.....	12
Comments.....	12
Chapter 1: Services	13
Service list.....	14
Service units.....	30
Viewing services.....	31
Viewing all services.....	31
Viewing individual service status.....	31
Related CLI command(s).....	32
Related REST API method(s).....	32
Managing services.....	32
Moving and scaling services.....	33
Configuring the service relocation operations manually.....	33
Configuring the service operations automatically.....	34
Related CLI command(s).....	34
Related REST API method(s).....	35
Configuring service settings.....	35
Configuring service settings.....	35
Related CLI command(s).....	35
Related REST API method(s).....	35
Repairing services.....	35
Chapter 2: Jobs	36
Managing jobs.....	36
Configuring where jobs run.....	36
Related CLI command(s).....	38
Related REST API method(s).....	38

Configuring job settings.....	38
Scheduling jobs.....	39
Chapter 3: Monitoring.....	41
Monitoring instances.....	41
Viewing all instances.....	41
Viewing the services running on an instance.....	42
Related CLI command(s).....	43
Related REST API method(s).....	43
Monitoring services.....	43
Viewing all services.....	44
Viewing individual service status.....	44
Related CLI command(s).....	45
Related REST API method(s).....	45
Monitoring jobs.....	45
Monitoring all jobs.....	45
Related CLI command(s).....	46
Related REST API method(s).....	46
Monitoring job types.....	46
Related CLI command(s).....	47
Related REST API methods GET jobs types.....	47
Monitoring individual jobs.....	47
Related CLI command(s).....	48
Related REST API method(s).....	48
Monitoring processes.....	49
Monitoring service operations.....	49
Related CLI command(s).....	49
Related REST API method(s).....	49
Monitoring system processes.....	49
Related CLI command(s).....	50
Related REST API method(s).....	50
System events.....	50
Related CLI command(s).....	50
Related REST API method(s).....	51
Alerts.....	51
Viewing alerts.....	53
Related CLI command(s).....	53
Related REST API method(s).....	54
Creating email notification rules.....	54
Creating email notification rules.....	55
Related CLI command(s).....	55
Related REST API method(s).....	55

Creating syslog notification rules.....	56
Creating syslog notification rules.....	57
Related CLI command(s).....	57
Related REST API method(s).....	57
Logs and diagnostic information.....	57

Chapter 4: Security..... 62

Granting access to users.....	62
Setting the session timeout limit.....	62
Related CLI command(s).....	62
Related REST API method(s).....	63
Identity providers.....	63
Adding identity providers.....	63
Related CLI command(s).....	63
Related REST API method(s).....	63
Identity provider configuration settings.....	63
User information caching.....	66
Related CLI command(s).....	66
Related REST API method(s).....	66
Viewing identity providers.....	67
Related CLI command(s).....	67
Related REST API method(s).....	67
Deleting identity providers.....	67
Related CLI command(s).....	67
Related REST API method(s).....	67
Groups.....	68
Adding groups.....	68
Related CLI command(s).....	68
Related REST API method(s).....	68
Viewing groups.....	68
Related CLI command(s).....	69
Related REST API method(s).....	69
Assigning roles to groups.....	69
Related CLI command(s).....	69
Related REST API method(s).....	69
Deleting groups.....	70
Related CLI command(s).....	70
Related REST API method(s).....	70
Roles.....	70
Creating roles.....	70
Related CLI command(s).....	71
Related REST API method(s).....	71

Viewing roles.....	71
Related CLI command(s).....	72
Related REST API method(s).....	72
Editing roles.....	72
Related CLI command(s).....	73
Related REST API method(s).....	73
Deleting roles.....	73
Related CLI command(s).....	74
Related REST API method(s).....	74
Permissions.....	74
Changing the admin account password.....	77
Related CLI command(s).....	77
Related REST API method(s).....	77
Certificates.....	77
Viewing installed certificates.....	78
Related CLI command(s).....	78
Related REST API method(s).....	78
Adding data source certificates.....	79
Uploading data source certificates manually.....	79
Related CLI command(s).....	79
Related REST API method(s).....	79
Changing the system certificate.....	79
System certificate considerations.....	80
Installing a certificate you created.....	80
Installing a new self-signed certificate.....	81
Creating a CSR and installing the returned certificate.....	82
Chapter 5: System management.....	85
Setting the system hostname.....	85
Related CLI command(s).....	85
Related REST API method(s).....	85
System scaling.....	86
Networking.....	86
Handling network changes.....	92
Safely changing an instance IP address.....	92
After a network change.....	93
Volumes.....	93
Viewing volumes.....	94
Viewing job volumes.....	95
Viewing service volumes.....	95
Instances.....	95
About master and worker instances.....	95

Single-instance systems versus multi-instance systems.....	96
Requirements for running system instances.....	97
Hardware requirements.....	97
Operating system and Docker minimum requirements.....	98
Operating system and Docker qualified versions.....	98
Docker considerations.....	98
SELinux considerations.....	99
Supported browsers.....	99
Time source requirements.....	99
Adding new instances.....	99
Before adding a new instance.....	100
Install Docker on each server or virtual machine	100
Configure Docker on each server or virtual machine.....	100
(Optional) Configure Docker volume drivers.....	101
Configure maximum map count setting.....	101
(Optional) Enable or disable SELinux on each server or virtual machine.....	102
Configure the firewall rules on each server or virtual machine.....	102
Install and configure NTP.....	102
Run Docker on each server or virtual machine.....	102
Unpack the installation package.....	103
Set up networking.....	104
Run the setup script on each server or virtual machine.....	104
Start the application on each server or virtual machine.....	106
Configure services and jobs on the new instances.....	107
Viewing instances.....	107
Viewing all instances.....	107
Viewing the services running on an instance.....	108
Related CLI command(s).....	109
Related REST API method(s).....	109
Removing instances.....	110
(Optional) Shut down the instance you want to remove.....	110
Remove the shut down instance from the system.....	111
Replacing a failed instance.....	111
Plugins.....	112
Viewing installed plugins.....	112
Related CLI command(s).....	112
Related REST API methods GET plugins.....	112
Upgrading plugin bundles.....	113
Related CLI command(s).....	113
Related REST API method(s).....	113
Setting the active plugin bundle version.....	113

Related CLI command(s).....	114
Related REST API method(s).....	114
Deleting plugin bundles.....	114
Related CLI command(s).....	114
Related REST API method(s).....	114
Packages.....	114
Exporting packages.....	115
Related CLI command(s).....	115
Related REST API method(s).....	115
Importing packages.....	115
Related CLI command(s).....	116
Related REST API method(s).....	117
Setting a login welcome message.....	117
Related CLI command(s).....	117
Related REST API method(s).....	117
Updating the system.....	117
To update system:.....	119
Related CLI command(s).....	119
Related REST API method(s).....	119
Viewing update history.....	120
Related CLI command(s).....	120
Related REST API method(s).....	120
Uninstalling the system.....	120
Chapter 6: Best practices.....	122
Best practices for distributing services.....	122
Best practices for maintaining system availability.....	122
Chapter 7: Reference.....	123
Troubleshooting.....	123
CLI reference.....	123
Accessing the CLI tools on a system instance.....	123
Accessing the CLI tools from your computer.....	124
Syntax.....	124
Viewing available commands.....	125
Viewing request models.....	126
Editing configuration preferences.....	126
System error responses.....	127
REST API Reference.....	129
Input and output formats.....	129
Access and authentication.....	129
Viewing and using REST API methods.....	131

Error responses..... 132

Preface

About this document

This document describes the System Management application, part of the Hitachi Content Platform for cloud scale (HCP for cloud scale) software, that you use to configure HCP for cloud scale for your users, enable and disable system features, and monitor the system and its connections.

Intended audience

This document is intended for people who are managing HCP for cloud scale systems. It assumes you have some experience writing scripts that issue API calls.

Product version

This document applies to v1.2.0 of Hitachi Content Platform for cloud scale.

Release notes

Read the release notes before installing and using this product. They may contain requirements or restrictions that are not fully described in this document or updates or corrections to this document. Release notes are available on Hitachi Vantara Support Connect: <https://knowledge.hitachivantara.com/Documents>.

Related documents

The following documents contain additional information about HCP for cloud scale:

- *Installing Hitachi Content Platform for Cloud Scale* (MK-HCPCS002-03): This document provides the information you need to install the HCP for cloud scale software.
- *Hitachi Content Platform for Cloud Scale Object Storage Management Application Help* (MK-HCPCS000-02): This help system explains how to use the HCP for cloud scale Object Storage Management application to configure and operate a common object storage interface for clients to interact with.

- *Hitachi Content Platform for Cloud Scale Management API Reference* (MK-HCPCS007-01): This document is for customers, and describes the management application programming interface (API) endpoints available for customer use.
- *Hitachi Content Platform for Cloud Scale Third-party Copyrights and Licenses* (MK-HCPCS003-01): This document contains copyright and license information for third-party software distributed with or embedded in the HCP for cloud scale operating system, core software, and applications.
- *Hitachi Content Platform for Cloud Scale Release Notes* (RN-HCPCS004-03): This document is for customers, and describes new features, product documentation, and resolved and known issues, and provides other useful information about this release of the product.

Accessing product documentation

Product user documentation is available on Hitachi Vantara Support Connect: <https://knowledge.hitachivantara.com/Documents>. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

[Hitachi Vantara Support Connect](#) is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to Hitachi Vantara Support Connect for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

[Hitachi Vantara Community](#) is a global online community for Hitachi Vantara customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Comments

Please send us your comments on this document to doc.comments@hitachivantara.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara Corporation.

Thank you!

Chapter 1: Services

This is a description of the services of Hitachi Content Platform for cloud scale, as well as how to view, configure, move, and repair services.

Services perform functions essential to the health or functionality of the system. For example, the Metrics service stores and manages system events, while the Watchdog service ensures that other services remain running. Internally, services run in Docker containers on the instances in the system.

Service categories

Services are grouped into these categories depending on what actions they perform:

- **Services** — Enable product functionality. You can scale, move, and reconfigure these services.
- **System services** — Maintain the health and availability of the system. You cannot scale, move, or reconfigure these services.

Some system services run only on master instances.

Applications

Some services are classified as applications. These are the services with which users interact. Services that are not applications typically interact only with other services.



Note: In this document, the terms System Management application and Admin App refer to the same service.

Service instances

Services run on instances in the system. Most services can run simultaneously on multiple instances. That is, you can have multiple instances of a service running on multiple instances in the system. Some services run on only one instance.

Each service has a recommended and required number of instances on which it should run.

You can configure where Hitachi Content Platform for cloud scale services run, but not system services.

Floating services

If a service supports *floating*, you have flexibility in configuring where new instances of that service are started when service instances fail.

Non-floating (or *persistent*) services run on the specific instances that you specify. If one of those service instances fails, the system does not automatically bring up a new instance of that service on another system instance.

With a service that supports floating, you specify a pool of eligible system instances and the number of service instances that should be running at any time. If a service instance fails, the system brings up another one on one of the system instances in the pool that doesn't already have an instance of that service running.

Networking

Each service binds to a number of ports and to one type of network, either internal or external. Networking for each service is configured during system installation and cannot be changed once a system is running.

Storage for services

Services can use volumes for storing data.

Service list

The table below describes the services that HCP for cloud scale runs. Each service runs within its own Docker container. For each service, the table lists:

- Configuration settings: The settings you can configure for the service.
- RAM needed per instance: The amount of RAM that, by default, the service needs on each instance on which it's deployed. For all services except for System services, this value is also the default Docker value of Container Memory for the service.
- Number of instances:
 - Shows the required number of instances on which a service must run to function properly.
 - Shows the recommended number of instances on which a service should run. These are recommended minimums; if your system includes more instances, you should take advantage of them by running services on them.
- Whether the service is persistent (it must run on a specific instance) or supports floating (it can run on any instance).
- Whether the service is scalable or not.



Note: For system services, you cannot set the **Container Memory** size larger than the **Max Heap Size** setting. For other services, you should not set the **Container Memory** size larger than the **Max Heap Size** setting.

Service name and description	Configuration settings (changes cause the service to redeploy)	Properties
Product services: These services perform system functions. You can move and reconfigure these services.		

Service name and description	Configuration settings (changes cause the service to redeploy)	Properties	
<p>Cassandra</p> <p>Decentralized database that can be scaled across large numbers of hardware nodes.</p>	<p>Container Options: Default</p> <ul style="list-style-type: none"> ▪ Container Memory: The hard memory limit for the service's Docker container, in MB. The default is 2.4 GB. ▪ CPU: The relative CPU usage weight for the service's Docker container. Generally, a higher value means that the container received more CPU resources than other processes (including other service Docker containers) running on the instance. Enter a decimal number. The default is 0.1. 	RAM needed per instance:	2.4 GB
	<p>Service Options</p> <ul style="list-style-type: none"> ▪ Max heap: Maximum amount of memory to allocate to the Java heap for each instance of the service. Enter an integer number of bytes. You can optionally specify the suffixes k (kilobytes), m (megabytes), or g (gigabytes). The default is 1800m. ▪ Heap new size: Heap size for the Java virtual machine. Valid values are integers representing a number of bytes. You can optionally specify the suffixes k (kilobytes), m (megabytes), or g (gigabytes). The default is 512 MB. 	Number of instances:	Required: 3 Recommended: All
	<p>Advanced Options:</p> <p>Compaction Frequency: How often database compaction operations are run. The options are Weekly (default) and Daily.</p> <p>Caution: Changing this setting can negatively affect the service. Use with caution.</p>	Persistent or floating?	Persistent
		Supports volume configuration?	No
		Single or multiple types?	Single
		Scalable?	Yes

Service name and description	Configuration settings (changes cause the service to redeploy)	Properties	
Chronos Job scheduling.	Container Options: Default <ul style="list-style-type: none"> ▪ Container Memory: The hard memory limit for the service's Docker container, in MB. The default is 712 MB. ▪ CPU: The relative CPU usage weight for the service's Docker container. Generally, a higher value means that the container received more CPU resources than other processes (including other service Docker containers) running on the instance. Enter a decimal number. The default is 0.1. 	RAM needed per instance:	712 MB
	Service Options <ul style="list-style-type: none"> ▪ Heap settings: Maximum amount of memory to allocate to the Java heap for each instance of the service. Enter an integer number of bytes. You can optionally specify the suffixes k (kilobytes), m (megabytes), or g (gigabytes). The default is 512 MB. 	Number of instances:	<ul style="list-style-type: none"> ▪ 1 required ▪ 1 recommended
		Persistent or floating?	Floating
		Supports volume configuration?	Yes
		Single or multiple types?	Single
		Scalable?	No
Elasticsearch Data indexing and search platform.	Container Options: Default <ul style="list-style-type: none"> ▪ Container Memory: The hard memory limit for the service's Docker container, in MB. The default is 2 GB. ▪ CPU: The relative CPU usage weight for the service's Docker container. Generally, a higher value means that the container received more CPU resources than other processes (including other service Docker containers) running on the instance. Enter a decimal number. The default is 0.1. 	RAM needed per instance:	2 GB

Service name and description	Configuration settings (changes cause the service to redeploy)	Properties	
	<p>Service Options</p> <ul style="list-style-type: none"> ▪ Heap settings: Maximum amount of memory to allocate to the Java heap for each instance of the service. Enter an integer number of bytes. You can optionally specify the suffixes k (kilobytes), m (megabytes), or g (gigabytes). The default is 1024 MB. ▪ Days to keep logs: The number of days to keep service logs, including access and metrics indexes. The default is 30 days. ▪ Index Protection Level: The number of additional replicas (copies) to keep of each index file (shard). Replicas are kept on separate instances. You can set this value for every shard. The default is 1 replica (which means that two copies are kept). The maximum is the number of instances less one. 	Number of instances:	Required: 3 Recommended: All
		Persistent or floating?	Persistent
		Supports volume configuration?	Yes
		Single or multiple types?	Single
		Scalable?	Yes
<p>Kafka</p> <p>Stream processing platform for handling real-time data streams.</p>	<p>Container Options: Default</p> <ul style="list-style-type: none"> ▪ Container Memory: The hard memory limit for the service's Docker container, in MB. The default is 2 GB. ▪ CPU: The relative CPU usage weight for the service's Docker container. Generally, a higher value means that the container received more CPU resources than other processes (including other service Docker containers) running on the instance. Enter a decimal number. The default is 0.1. 	RAM needed per instance:	2 GB
	<p>Service Options</p> <ul style="list-style-type: none"> ▪ Heap settings: Maximum amount of memory to allocate to the Java heap for each instance of the service. Enter an integer number of bytes. You can optionally specify the suffixes k (kilobytes), m (megabytes), or g (gigabytes). The default is -Xmx1800m-Xms512m. 	Number of instances:	Required: 3 Recommended: All
		Persistent or floating?	Persistent
		Supports volume configuration?	Yes

Service name and description	Configuration settings (changes cause the service to redeploy)	Properties	
		Single or multiple types?	Single
		Scalable?	Yes
Logstash Logging.	Container Options: Default <ul style="list-style-type: none"> ▪ Container Memory: The hard memory limit for the service's Docker container, in MB. The default is 700 MB. ▪ CPU: The relative CPU usage weight for the service's Docker container. Generally, a higher value means that the container received more CPU resources than other processes (including other service Docker containers) running on the instance. Enter a decimal number. The default is 0.1. 	RAM needed per instance:	700 MB
	Service Options <ul style="list-style-type: none"> ▪ Max heap: Maximum amount of memory to allocate to the Java heap for each instance of the service. Enter an integer number of bytes. You can optionally specify the suffixes k (kilobytes), m (megabytes), or g (gigabytes). The default is 512 MB. 	Number of instances:	Required: 1 Recommended: 1
		Persistent or floating?	Floating
		Supports volume configuration?	No
		Single or multiple types?	Single
		Scalable?	No

Service name and description	Configuration settings (changes cause the service to redeploy)	Properties	
MAPI Gateway Serves MAPI endpoints.	Container Options: Default <ul style="list-style-type: none"> ▪ Container Memory: The hard memory limit for the service's Docker container, in MB. The default is 768 MB. ▪ CPU: The relative CPU usage weight for the service's Docker container. Generally, a higher value means that the container received more CPU resources than other processes (including other service Docker containers) running on the instance. Enter a decimal number. The default is 0.1. 	RAM needed per instance:	768 MB
	Service Options <ul style="list-style-type: none"> ▪ Max Heap Size: Maximum amount of memory to allocate to the Java heap for each instance of the service. Enter an integer number of bytes. You can optionally specify the suffixes k (kilobytes), m (megabytes), or g (gigabytes). The default is 64 MB. 	Number of instances:	Required: 1 Recommended: All
		Persistent or floating?	Floating
		Supports volume configuration?	No
		Single or multiple types?	Single
		Scalable?	Yes
Metadata Cache Cache for system metadata.	Container Options: Default <ul style="list-style-type: none"> ▪ Container Memory: The hard memory limit for the service's Docker container, in MB. The default is 768 MB. ▪ CPU: The relative CPU usage weight for the service's Docker container. Generally, a higher value means that the container received more CPU resources than other processes (including other service Docker containers) running on the instance. Enter a decimal number. The default is 0.1. 	RAM needed per instance:	768 MB

Service name and description	Configuration settings (changes cause the service to redeploy)	Properties	
	<p>Service Options</p> <ul style="list-style-type: none"> ▪ Max Heap Size: Maximum amount of memory to allocate to the Java heap for each instance of the service. Enter an integer number of bytes. You can optionally specify the suffixes k (kilobytes), m (megabytes), or g (gigabytes). The default is 512 MB. 	Number of instances:	Required: 1 Recommended: 1
		Persistent or floating?	Persistent
		Supports volume configuration?	No
		Single or multiple types?	Single
		Scalable?	No
<p>Metadata Coordination</p> <p>Coordinates metadata gateway service instances, and coordinates scaling and balancing.</p>	<p>Container Options: Default</p> <ul style="list-style-type: none"> ▪ Container Memory: The hard memory limit for the service's Docker container, in MB. The default is 768 MB. ▪ CPU: The relative CPU usage weight for the service's Docker container. Generally, a higher value means that the container received more CPU resources than other processes (including other service Docker containers) running on the instance. Enter a decimal number. The default is 0.1. 	RAM needed per instance:	768 MB
	<p>Service Options</p> <ul style="list-style-type: none"> ▪ Max Heap Size: Maximum amount of memory to allocate to the Java heap for each instance of the service. Enter an integer number of bytes. You can optionally specify the suffixes k (kilobytes), m (megabytes), or g (gigabytes). The default is 64 MB. 	Number of instances:	Required: 1 Recommended: 1
		Persistent or floating?	Floating
		Supports volume configuration?	No
		Single or multiple types?	Single

Service name and description	Configuration settings (changes cause the service to redeploy)	Properties	
		Scalable?	No
<p>Metadata Gateway</p> <p>Stores and protects metadata and serves it to other services.</p>	<p>Container Options: Default</p> <ul style="list-style-type: none"> ▪ Container Memory: The hard memory limit for the service's Docker container, in MB. The default is 4096 MB. ▪ CPU: The relative CPU usage weight for the service's Docker container. Generally, a higher value means that the container received more CPU resources than other processes (including other service Docker containers) running on the instance. Enter a decimal number. The default is 0.1. <p>Service Options</p> <ul style="list-style-type: none"> ▪ Max Heap Size: Maximum amount of memory to allocate to the Java heap for each instance of the service. Enter an integer number of bytes. You can optionally specify the suffixes k (kilobytes), m (megabytes), or g (gigabytes). The default is 2048 MB. 	RAM needed per instance:	768 MB
		Number of instances:	Required: 3 Recommended: All
		Persistent or floating?	Persistent
		Supports volume configuration?	No
		Single or multiple types?	Single
		Scalable?	Yes
<p>Metadata Policy Engine</p> <p>Executes asynchronous metadata updates.</p>	<p>Container Options: Default</p> <ul style="list-style-type: none"> ▪ Container Memory: The hard memory limit for the service's Docker container, in MB. The default is 2048 MB. ▪ CPU: The relative CPU usage weight for the service's Docker container. Generally, a higher value means that the container received more CPU resources than other processes (including other service Docker containers) running on the instance. Enter a decimal number. The default is 0.1. 	RAM needed per instance:	768 MB

Service name and description	Configuration settings (changes cause the service to redeploy)	Properties	
	<p>Service Options</p> <ul style="list-style-type: none"> ▪ Max Heap Size: Maximum amount of memory to allocate to the Java heap for each instance of the service. Enter an integer number of bytes. You can optionally specify the suffixes k (kilobytes), m (megabytes), or g (gigabytes). The default is 1024 MB. 	Number of instances:	Required: 1 Recommended: 1
		Persistent or floating?	Floating
		Supports volume configuration?	No
		Single or multiple types?	Single
		Scalable?	No
Metrics	<p>Container Options: Default</p> <ul style="list-style-type: none"> ▪ Container Memory: The hard memory limit for the service's Docker container, in MB. The default is 768 MB. ▪ CPU: The relative CPU usage weight for the service's Docker container. Generally, a higher value means that the container received more CPU resources than other processes (including other service Docker containers) running on the instance. Enter a decimal number. The default is 0.1. 	RAM needed per instance:	768 MB
	<p>Service Options</p> <ul style="list-style-type: none"> ▪ Prometheus Scrape Interval: The time interval between runs of the metrics collection task. Enter an integer number of seconds. You can optionally specify the suffix s (seconds). The default is 10 seconds. ▪ Prometheus Database Path: Storage location for prometheus local time-series db. Enter a path. The default is tsdb/. ▪ Prometheus Database Retention: The number of days to retain files. Enter an integer number of days. You can optionally specify the suffix d (days). The default is 15 days. 	Number of instances:	Required: 1 Recommended: All
		Persistent or floating?	Persistent
		Supports volume configuration?	No
		Single or multiple types?	Single

Service name and description	Configuration settings (changes cause the service to redeploy)	Properties	
		Scalable?	Yes
S3 Gateway Serves S3 API endpoints and communicates with storage components.	Container Options: Default <ul style="list-style-type: none"> ▪ Container Memory: The hard memory limit for the service's Docker container, in MB. The default is 768 MB. ▪ CPU: The relative CPU usage weight for the service's Docker container. Generally, a higher value means that the container received more CPU resources than other processes (including other service Docker containers) running on the instance. Enter a decimal number. The default is 0.1. 	RAM needed per instance:	768 MB
	Service Options <ul style="list-style-type: none"> ▪ Max Heap Size: Maximum amount of memory to allocate to the Java heap for each instance of the service. Enter an integer number of bytes. You can optionally specify the suffixes k (kilobytes), m (megabytes), or g (gigabytes). The default is 512 MB. 	Number of instances:	Required: 1 Recommended: All
	HTTP Options: <ul style="list-style-type: none"> ▪ Enable HTTP: Select to enable HTTP connections. ▪ Max Http Request Headers: The maximum number of HTTP request headers to allow. Enter an integer. The default is 100 request headers. 	Persistent or floating?	Floating
		Supports volume configuration?	No
		Single or multiple types?	Single
		Scalable?	Yes

Service name and description	Configuration settings (changes cause the service to redeploy)	Properties	
<p>Tracing Agent</p> <p>Provides end-to-end distributed tracing for S3 API calls and MAPI calls.</p>	<p>Container Options: Default</p> <ul style="list-style-type: none"> ▪ Container Memory: The hard memory limit for the service's Docker container, in MB. The default is 768 MB. ▪ CPU: The relative CPU usage weight for the service's Docker container. Generally, a higher value means that the container received more CPU resources than other processes (including other service Docker containers) running on the instance. Enter a decimal number. The default is 0.1. 	RAM needed per instance:	768 MB
	<p>Service Options</p> <ul style="list-style-type: none"> ▪ Collector TChannel Hostname: Enter a host name. The default is localhost. ▪ Collector TChannel Port: Enter a port number. The default is 14267. 	Number of instances:	Required: All
		Persistent or floating?	Floating
		Supports volume configuration?	No
		Single or multiple types?	Single
		Scalable?	Yes
<p>Tracing Collector</p> <p>Provides end-to-end distributed tracing for S3 API calls and MAPI calls.</p>	<p>Container Options: Default</p> <ul style="list-style-type: none"> ▪ Container Memory: The hard memory limit for the service's Docker container, in MB. The default is 768 MB. ▪ CPU: The relative CPU usage weight for the service's Docker container. Generally, a higher value means that the container received more CPU resources than other processes (including other service Docker containers) running on the instance. Enter a decimal number. The default is 0.1. 	RAM needed per instance:	768 MB
	<p>Service Options</p> <ul style="list-style-type: none"> ▪ ElasticSearch Hostname: Enter a host name. The default is localhost. 	Number of instances:	Required: 1 Recommended: All

Service name and description	Configuration settings (changes cause the service to redeploy)	Properties	
	<ul style="list-style-type: none"> ▪ ElasticSearch Port: Enter a port number. The default is 9200. ▪ Sampling Rate: The sampling rate for all clients implementing remote sampling. Enter a number between 0 and 1 inclusive. The default is 1. ▪ Max open Index age: How long to keep tracing indexes open in the database, in days. Enter a value from 1 to 365 days inclusive. The default is 30 days. ▪ Max Index age: How long to keep tracing indexes in the database, in days. Enter a value from 1 to 365 days inclusive. The default is 60 days. 	Persistent or floating?	Floating
		Supports volume configuration?	No
		Single or multiple types?	Single
		Scalable?	Yes
<p>Tracing Query</p> <p>Provides end-to-end distributed tracing for S3 API calls and MAPI calls.</p>	<p>Container Options: Default</p> <ul style="list-style-type: none"> ▪ Container Memory: The hard memory limit for the service's Docker container, in MB. The default is 768 MB. ▪ CPU: The relative CPU usage weight for the service's Docker container. Generally, a higher value means that the container received more CPU resources than other processes (including other service Docker containers) running on the instance. Enter a decimal number. The default is 0.1. 	RAM needed per instance:	768 MB
	<p>Service Options</p> <ul style="list-style-type: none"> ▪ ElasticSearch Hostname: Enter a host name. The default is localhost. ▪ ElasticSearch Port: Enter a port number. The default is 9200. 	Number of instances:	Required: 1 Recommended: All
		Persistent or floating?	Floating
		Supports volume configuration?	No
		Single or multiple types?	Single
		Scalable?	Yes

Service name and description	Configuration settings (changes cause the service to redeploy)	Properties	
System services: These services manage system resources and ensure that the system remains available and accessible. These services cannot be moved or reconfigured.			
System Management application The system management application.	Service Options <ul style="list-style-type: none"> ▪ Max heap size: Maximum amount of memory to allocate to the Java heap for each instance of the service. Enter an integer number of bytes. You can optionally specify the suffixes k (kilobytes), m (megabytes), or g (gigabytes). The default is 512 MB. 	RAM needed per instance:	N/A
		Number of instances:	N/A
		Persistent or floating?	Persistent
		Supports volume configuration?	Yes
		Single or multiple types?	Single
		Scalable?	No
Cluster Coordination Manages hardware resource allocation.	N/A	RAM needed per instance:	N/A
		Number of instances:	N/A
		Persistent or floating?	Persistent
		Supports volume configuration?	No
		Single or multiple types?	Single

Service name and description	Configuration settings (changes cause the service to redeploy)	Properties	
		Scalable?	No
Cluster Worker Receives and performs work from other services.	N/A	RAM needed per instance:	N/A
		Number of instances:	N/A
		Persistent or floating?	Persistent
		Supports volume configuration?	Yes
		Single or multiple types?	Single
		Scalable?	No
Network Proxy Network request load balancer.	Security Protocol: Select which TLS versions to use: <ul style="list-style-type: none"> ▪ TLS 1.0 ▪ TLS 1.1 ▪ TLS 1.2 ▪ TLS 1.3 	RAM needed per instance:	N/A
	SSL Ciphers: If you want to provide your own cipher suite, enter it here.	Number of instances:	N/A
	Custom Global Configuration: Select Enable Advanced Global Configuration to enable adding your own parameters to the HAProxy "global" section.	Persistent or floating?	Persistent
	Custom Defaults Configuration: Select Enable Defaults Configuration to enable adding your own parameters to the HAProxy "global" section.	Supports volume configuration?	Yes

Service name and description	Configuration settings (changes cause the service to redeploy)	Properties	
		Single or multiple types?	Single
		Scalable?	No
<p>Sentinel</p> <p>Runs internal system processes and monitors the health of the other services.</p>	<p>Service Options</p> <ul style="list-style-type: none"> ▪ Max heap size: Maximum amount of memory to allocate to the Java heap for each instance of the service. Enter an integer number of bytes. You can optionally specify the suffixes k (kilobytes), m (megabytes), or g (gigabytes). The default is 256 MB. 	RAM needed per instance:	N/A
		Number of instances:	N/A
		Persistent or floating?	persistent
		Supports volume configuration?	Yes
		Single or multiple types?	Single
		Scalable?	No
<p>Service Deployment</p> <p>Handles deployment of high-level services (that is, the services that you can configure).</p>	N/A	RAM needed per instance:	N/A
		Number of instances:	N/A
		Persistent or floating?	Persistent
		Supports volume configuration?	Yes

Service name and description	Configuration settings (changes cause the service to redeploy)	Properties	
		Single or multiple types?	Single
		Scalable?	No
<p>Synchronization</p> <p>Coordinates service configuration settings and other information across instances.</p>	<p>Service Options</p> <ul style="list-style-type: none"> ▪ Max heap size: Maximum amount of memory to allocate to the Java heap for each instance of the service. Enter an integer number of bytes. You can optionally specify the suffixes k (kilobytes), m (megabytes), or g (gigabytes). The default is 1024 MB. 	RAM needed per instance:	N/A
		Number of instances:	N/A
		Persistent or floating?	Persistent
		Supports volume configuration?	Yes
		Single or multiple types?	Single
		Scalable?	No
<p>Watchdog</p> <p>Monitors the other System services and restarts them if necessary. Also responsible for initial system startup.</p>	<p>Service Options</p> <ul style="list-style-type: none"> ▪ Max heap size: Maximum amount of memory to allocate to the Java heap for each instance of the service. Enter an integer number of bytes. You can optionally specify the suffixes k (kilobytes), m (megabytes), or g (gigabytes). The default is 1024 MB. ▪ Heap new size: Heap size for the Java virtual machine. Valid values are integers representing a number of bytes. You can optionally specify the suffixes k (kilobytes), m (megabytes), or g (gigabytes). The default is 512 MB. 	RAM needed per instance:	N/A
		Number of instances:	N/A
		Persistent or floating?	Persistent
		Supports volume configuration?	Yes

Service name and description	Configuration settings (changes cause the service to redeploy)	Properties	
		Single or multiple types?	Single
		Scalable?	No

Service units

Your system license limits grants you a number of service units. These limit how and where you can run services and jobs:

- For services, each service costs a certain number of service units per instance to run. For example, a service with a cost of one service unit that's running on three instances counts for three service units against your licensed limit.
- For jobs, service unit cost is assessed based on where job types are allowed to run, not on the number of individual jobs that you run.

Each job type has its own service unit cost. If an instance is configured to run multiple job types, only the job type with the highest service unit cost counts.

For example, suppose that your system has four instances and supports two job types: X, which costs 50 service units, and Y, which costs 25. Job type X is configured to run on three instances. Job type Y is configured to run on those same three instances, plus an additional instance (for a total of four instances). In this case, your total service unit cost for jobs is equal to:

$$50 + 50 + 50 + 25 = 175$$

Recommended service unit limits

The system makes recommendations on the maximum number of service units that you should run on each instance. An instance that runs more than the recommended number of service units in use is likely to experience decreased performance.

The recommended service unit limits are based on whether an instance meets the recommended hardware requirements:

- If an instance meets the recommended hardware requirements, you can run up to 180 service units on that instance.
- If an instance does not meet the recommended hardware requirements, you can run up to 100 service units on that instance.

Viewing services

You can use Admin App, CLI, and REST API to view the status of all services for the system.

Viewing all services

Admin App instructions

Procedure

1. To view the status of all services, in the Admin App, click on **Services**.

For each service, the page shows:

- The service name
- The service state:
 - **Healthy:** The service is running normally.
 - **Unconfigured:** The service has yet to be configured and deployed.
 - **Deploying:** The system is currently starting or restarting the service. This can happen when:
 - You move the service to run on a completely different set of instances.
 - You repair a service.

For information on viewing the status service operations, see [Monitoring service operations \(on page 49\)](#).

- **Balancing:** The service is running normally, but performing some background maintenance operations.
- **Under-protected:** In a multi-instance system, one or more of the instances on which a service is configured to run are offline.
- **Failed:** The service is not running or the system cannot communicate with the service.
- **CPU Usage:** The current percentage CPU usage for the service across all instances on which it's running.
- **Memory:** The current RAM usage for the service across all instances on which it's running.
- **Disk Used:** The current total amount of disk space that the service is using across all instances on which it's running.

Viewing individual service status

Procedure

1. To view the detailed status for an individual service, click on the service on the **Services** page.

In addition to the information above, the page shows:

- **Instances** — A list of all instances on which the service is running.
- **Volumes** — To view a list of volumes used by the service, click on the row for an instance in the **Instances** section.
- **Network: [Internal | External]** — Which network type this service uses to receive communications.

This section also displays a list of the ports that the service uses.

- **Configuration settings** — The settings you can configure for the service.
- **Service Units** — The total number of service units currently being spent to run this service. This value is equal to the service's service unit cost times the number of instances on which the service is running. For more information, see [Service units](#).
- **Service unit cost** — The number of service units required to run the service on one instance.
- **Service Instance Types** — For services that have multiple types, the types that are currently running.
- **Instance Pool** — For floating services, the instances that this service is eligible to run on.
- **Events** — A list of all system events for the service.

Related CLI command(s)

getService

listServices

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

GET /services

GET /services/{id}

You can get help on specific REST API methods for the Admin App at [REST API - Admin](#).

Managing services

This section describes how you can reconfigure, restart, and otherwise manage the services running on your system.

Moving and scaling services

You can change a service to run on:

- Additional instances (for example, if you need improved service performance and availability)
- Fewer instances (for example, if you want to free up resources on an instance for running other services)
- A different set of instances (for example, if you are retiring the piece of hardware on which an instance is installed)

Moving and scaling floating services

For floating services, instead of specifying the specific instances on which the service runs, you can specify a pool of eligible instances, any of which can run the service.

Moving and scaling services with multiple types

When moving or scaling a service that has multiple types, you can simultaneously configure separate rebalancing operations for each type.

Considerations

- You cannot remove a service from an instance if doing so would cause or risk causing data loss.
- Service relocation operations may take a long time to complete and may impact system performance while they are running.
- Instance requirements vary from service to service. Each service defines the minimum and maximum number of instances on which it can run.



Tip: Use the **Available Instances** option to have a floating service be eligible to run on any instance in the system, including any new instances added in the future.

Configuring the service relocation operations manually

To manually reconfigure a service relocation operation, in the Admin App:

Procedure

1. Select **Services**.
2. Locate a service that you want to scale or move and click **Configure**.
3. On the **Scale** tab, if the service has more than one type, select the instance type that you want to scale.
4. If the service is a floating service, you are presented with options for configuring an instance pool:
 - a. In the **Service Instances** field, specify the number of instances on which the service should be running at any time.

b. Configure the instance pool:

- To have the service run on any instance in the system, select the **All Available Instances** option.

With this option, the service can be restarted on any instance, including instances that were added to the system after the service was configured.

- To have the service run on a specific set of instances, deselect the **All Available Instances** option. Then:
 - To remove an instance from the pool, select it from the **Instance Pool** list on the left and click **Remove Instances**.
 - To add an instance to the pool, select it from the **Available Instances** list on the right and click **Add Instances**.

5. If the service is a non-floating service, you are presented with options for selecting the specific instances that the service should run on. Do one or both of these, then click **Next**:

- To remove the service from the instances it's currently on, select one or more instances from the list on the left and click **Remove Instances**.
- To add the service to other instances, select one or more instances from the **Available Instances** list on the right and click **Add Instances**.

6. Click **Update Service**.

Configuring the service operations automatically

The system can check whether your services are currently deployed on the recommended minimum number of instances. If they aren't, the system can configure service scale operations for you.

To have the system do this for you, in the Admin App:

Procedure

1. Click on the **Services** panel.
2. Click on the **Manage Services** button.
3. Click on the **Auto Scale** option. Then click on the **Next** button.

The system examines your service layout to ensure that each service is running on the minimum recommended number of instances. If one or more services are not running on enough instances, the system automatically creates scale operations for them.

For example, if you have the service running on only one instance, the system configures an operation to scale the service to run on three instances.
4. Click on the **Update Service** button.

Related CLI command(s)

updateServiceConfig

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

POST /services/configure

You can get help on specific REST API methods for the Admin App at [REST API - Admin](#).

Configuring service settings

You can configure settings for some of the services that the system runs.



Note: If you make an unwanted change to a service configuration, wait for the operation to finish before creating a new operation to correct the service configuration.

Configuring service settings

Procedure

1. Click on the **Services** panel.
2. Click on the service you want to configure.
3. On the **Configuration** tab, configure the service.
4. Click on the **Update** button.

Related CLI command(s)

updateServiceConfig

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

POST /services/configure

You can get help on specific REST API methods for the Admin App at [REST API - Admin](#).

Repairing services

If a service becomes slow, unresponsive, or shows a status of **Failed**, you can run a service operation to repair it. Repairing a service stops and restarts the service on each instance on which it's running.



Important: Depending on which service you're repairing, parts of the system will be unavailable until the repair operation finishes.

To repair a service:

Procedure

1. Click on the **Services** panel.
2. Select the service you want to repair.
3. Click on the **Repair** button.

Chapter 2: Jobs

Jobs are operations that services run to perform work, usually transient in nature. Like services, jobs are run in Docker containers on system instances. However when the job completes its work, its container exits.

Jobs are run by services. You cannot start or stop them yourself on demand, but you can schedule the times when they are allowed to run and specify which instances in the system that they are allowed to run on.



Note: Some functions described here are not used with HCP for cloud scale. They are not visible in the System Management application, or have no effect when used.

Job types

Jobs are grouped into *job types*. All jobs in a type share the same default configuration settings. Newly created jobs inherit their settings from their job type. However, each job in a type can be configured with settings different from the job type default settings.

Storage for jobs

You can configure storage usage for jobs by associating volumes with job types.

Networking

You can configure network ports for job types and individual jobs.

Managing jobs

This section describes how you can reconfigure, move, schedule, and otherwise manage the jobs that can run on your system.



Note: Some functions described here are not used with HCP for cloud scale. They are not visible in the System Management application, or have no effect when used.

Configuring where jobs run

The Hitachi Content Platform for cloud scale system lets you limit the system instances that jobs are allowed to run on. You can specify lists of allowed instances for all jobs, for jobs of a specific type, or for each individual job.

For example, if your system includes instances numbered 101 through 104, you could specify that:

- Only instances 101, 102, and 103 can run jobs.
- Only instances 101 and 102 can run Example-type jobs.
- Only instance 101 can run the Example-type job named Example1.



Note: Some functions described here are not used with HCP for cloud scale. They are not visible in the System Management application, or have no effect when used.

Procedure

1. Click on **Jobs**.
2. Select the job you want and click on **Configure**.
3. Specify which instances can run jobs on the **Scale** tab:
 - a. From the **Available Instances** list, select the instances where you want jobs to run. Then click on the **Add Instances** button.
 - b. Optionally, enable the **Add newly selected instances to existing jobs** option.
With this option enabled, any new instances that you selected in the previous step will automatically be added as selected instances to all existing jobs. When disabled, existing jobs of this type keep their current lists of selected instances.
 - c. From the **Selected Instances** list, select any instances where you don't want jobs to run. Then click on the **Remove Instances** button.



Note:

- If you remove instances where jobs are already running, any existing jobs remain running on those instances, but new jobs will not run on the removed instances.
- You cannot remove all selected instances from the **All Jobs** menu. If you don't want jobs to run anywhere, you need to remove the selected instances for each job type

- d. Click on the **Update** button.
4. Specify which instances can run jobs of a particular type:
 - a. Select a job type and click on **Configure**.
 - b. On the **Scale** tab, from the **Eligible Instances** list, select the instances where you want this type of job to run. Then click on the **Add Instances** button.
 - c. Optionally, enable the **Add newly selected instances to existing jobs** option.
With this option enabled, any new instances that you selected in the previous step will automatically be added as selected instances to all existing jobs of this type. When disabled, existing jobs of this type keep their current lists of selected instances.
 - d. From the **Selected Instances** list, select any instances where you don't want this type of job to run. Then click on the **Remove Instances** button.



Note: If you remove instances where any jobs of this type are already running, the existing jobs remain running on those instances, but new jobs of this type will not run on the removed instances.

- e. Click on the **Update** button.
 - f. Repeat this step for any other job types you want to configure.
5. Specify which instances can run a particular job
- a. On the **Scale** tab, select the instances you want from the **Available Instances** list and click on the **Add Instances** button. Here, the **Available Instances** list displays all instances where jobs of this type are allowed to run.
 - b. Click on the **Update** button.
 - c. Repeat this step for any other jobs you want to configure.

Related CLI command(s)

editJob

editJobSettings

editJobType

Related REST API method(s)

PUT /jobs/{uuid}

PUT /jobs/settings

PUT /jobs/types/{name}

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Configuring job settings

Configurable settings

You can configure these Docker container settings for all job types and individual jobs:

- **Container Memory** — The hard memory limit for a job's Docker container, in megabytes (MB).
- **CPU** — The relative CPU usage weight for a job's Docker container. Generally, a higher value means that the container receives more CPU resources than other processes (including other service Docker containers) running on the instance.

Valid values are decimal numbers.

Other configurable settings are determined by the jobs and job types themselves.



Note: Some functions described here are not used with HCP for cloud scale. They are not visible in the System Management application, or have no effect when used.

Job setting inheritance

When you configure settings for a job type, those settings are inherited by newly created jobs, not by the jobs that exist at the time you make the configuration change.

Procedure

1. Click on **Jobs**.
2. Select a job type
3. On the **Configuration** tab, configure the settings you want.
4. Click on the **Update** button.

Scheduling jobs

You can configure a schedule for both job types and individual jobs.



Note: Some functions described here are not used with HCP for cloud scale. They are not visible in the System Management application, or have no effect when used.

Job type schedules

When you configure a schedule for a job type, the schedule is inherited by newly created jobs, not by the jobs that exist at the time you make the configuration change.

Individual job schedules

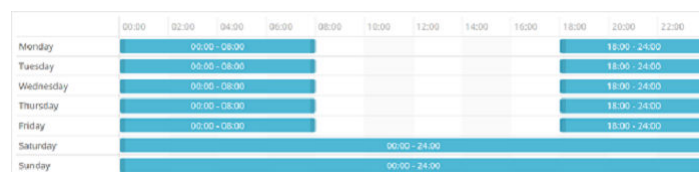
If a job has a schedule, the job enters the state Running state automatically when a scheduled time period begins, regardless of the job's current state. A job can also be started by a service outside of the job's scheduled time periods.

When the end of a scheduled time period arrives:

- If the job is still running, the job stops and enters the state Idle.
- If the job is not running (for example, it's in the state Completed or Failed), the job remains in its current state.

Procedure

1. Click on **Jobs**.
2. Select a job type or individual job.
3. On the **Schedule** tab, use the calendar tool to specify when the job or job type should run.



In this tool, click on a day to add a block of time. Click and drag the block to cover the hours you want the job or jobs to run.

To remove a block, right-click on it.

4. Click on the **Update** button.

Chapter 3: Monitoring

Your system provides a number of mechanisms that allow you to monitor the health and performance of the system and all of its instances and services.

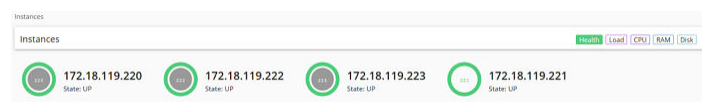
Monitoring instances

You can use the Admin App, CLI, and REST API to view a list of all instances in the system.


Viewing all instances

To view all instances, in the Admin App, click on Dashboard > Instances.

The page shows all instances in the system. Each instance is identified by its IP address.



This table describes the information shown for each instance.

Property	Description
State	<ul style="list-style-type: none">Up: The instance is reachable by other instances in the system.Down: The instance cannot be reached by other instances in the system.
Services	The number of services running on the instance.
Service Units	<p>The total number of service units for all services and job types running on the instance, out of the recommended service unit limit for the instance.</p> <p>An instance with a higher number of service units is likely to be more heavily utilized by the system than an instance with a lower number of service units.</p> <p>The Instances page displays a blue bar for instances running less than the recommended service unit limit.</p> <p>The Instances page displays a red bar for instances running more than the recommended service unit limit.</p> 

Property	Description
Load Average	The load averages for the instance for the past one, five, and ten minutes.
CPU	The sum of the percentage utilization for each CPU core in the instance.
Memory Allocated	This section shows both: <ul style="list-style-type: none"> ▪ The amount of RAM on the instance that's allocated to all services running on that instance. ▪ The percentage of this allocated RAM to the total RAM for the instance.
Memory Total	The total amount of RAM for the instance.
Disk Used	The current amount of disk space that your system is using in the partition on which it is installed.
Disk Free	The amount of free disk space in the partition in which your system is installed.

Viewing the services running on an instance

To view the services running on an individual instance, in the Admin App:

Procedure

1. Click on **Dashboard > Instances**.
2. Click on the instance you want.

The page lists all services running on the instance.

For each service, the page shows:

- The service name
- The service state:
 - **Healthy:** The service is running normally.
 - **Unconfigured:** The service has yet to be configured and deployed.
 - **Deploying:** The system is currently starting or restarting the service. This can happen when:
 - You move the service to run on a completely different set of instances.
 - You repair a service.

For information on viewing the status service operations, see [Monitoring service operations \(on page 49\)](#).

- **Balancing:** The service is running normally, but performing some background maintenance operations.
- **Under-protected:** In a multi-instance system, one or more of the instances on which a service is configured to run are offline.
- **Failed:** The service is not running or the system cannot communicate with the service.
- **CPU Usage:** The current percentage CPU usage for the service across all instances on which it's running.
- **Memory:** The current RAM usage for the service across all instances on which it's running.
- **Disk Used:** The current total amount of disk space that the service is using across all instances on which it's running.

Related CLI command(s)

getInstance

listInstances

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

GET /instances

GET /instances/{uuid}

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Monitoring services

You can use Admin App, CLI, and REST API to view the status of all services for the system.

Viewing all services

To view the status of all services, in the Admin App, click on Services.

For each service, the page shows:

- The service name
- The service state:
 - Healthy: The service is running normally.
 - Unconfigured: The service has yet to be configured and deployed.
 - Deploying: The system is currently starting or restarting the service. This can happen when:
 - You move the service to run on a completely different set of instances.
 - You repair a service.

For information on viewing the status service operations, see [Monitoring service operations. \(on page 49\)](#)

- Balancing: The service is running normally, but performing some background maintenance operations.
- Under-protected: In a multi-instance system, one or more of the instances on which a service is configured to run are offline.
- Failed: The service is not running or the system cannot communicate with the service.
- CPU Usage: The current percentage CPU usage for the service across all instances on which it's running.
- Memory: The current RAM usage for the service across all instances on which it's running.
- Disk Used: The current total amount of disk space that the service is using across all instances on which it's running.

Viewing individual service status

To view the detailed status for an individual service, click on the service on the **Services** page.

In addition to the information above, the page shows:

- **Instances** — A list of all instances on which the service is running.
- **Volumes** — To view a list of volumes used by the service, click on the row for an instance in the **Instances** section. For more information, see Viewing volumes.
- **Network: [Internal | External]** — Which network type this service uses to receive communications.

This section also displays a list of the ports that the service uses. For more information, see Networking.

- **Configuration settings** — The settings you can configure for the service.

- **Service Units** — The total number of service units currently being spent to run this service. This value is equal to the service's service unit cost times the number of instances on which the service is running. For more information, see [Service units](#).
- **Service unit cost** — The number of service units required to run the service on one instance. For more information, see [Services](#).
- **Service Instance Types** — For services that have multiple types, the types that are currently running.
- **Instance Pool** — For floating services, the instances that this service is eligible to run on. For more information, see [Floating services](#).
- **Events** — A list of all system events for the service.

Related CLI command(s)

getService

listServices

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

GET /services

GET /services/{id}

You can get help on specific REST API methods for the Admin App at [REST API - Admin](#).

Monitoring jobs

You can use Admin App, CLI, and REST API to monitor jobs. You can monitor information for all jobs, for all jobs of a type, or for each job individually.



Note: Some functions described here are not used with HCP for cloud scale. They are not visible in the System Management application, or have no effect when used.

Monitoring all jobs

You can use Admin App, CLI, and REST API to view the status of all jobs for the system.



Note: Some functions described here are not used with HCP for cloud scale. They are not visible in the System Management application, or have no effect when used.

To view the status of all jobs, in the Admin App, click on **Jobs**.

On this page, the **All Jobs** section shows cumulative information for all jobs in the system.

- **Service Units** — The total number of service units currently being spent for running jobs.

This value is determined by where your system's job types are allowed to run.

Each job type has its own service unit cost. If an instance is configured to run multiple job types, only the job type with the highest service unit cost counts.

For example, suppose that your system has 4 instances and supports two job types: X, which costs 50 service units, and Y, which costs 25. Job type X is configured to run on 3 instances. Job type Y is configured to run on those same 3 instances, plus an additional instance (4 total). In this case, your total service unit cost for jobs is equal to 175:

$$50 + 50 + 50 + 25 = 175$$

- **Total CPU** — The total CPU percentage utilization for all jobs across all instances in the system.
- **Total Memory** — The total RAM consumed by all jobs across all instances in the system.
- **Total Disk** — The total disk space consumed by all jobs across all instances in the system.

The **Job Types** section shows a box for each job type that the system supports.

Related CLI command(s)

listJobs

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

GET /jobs

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Monitoring job types

You can use Admin App, CLI, and REST API to view the status of all jobs of a particular type.



Note: Some functions described here are not used with HCP for cloud scale. They are not visible in the System Management application, or have no effect when used.

To view the detailed status for all jobs of a type, in the Admin App, click on **Jobs**. Then click on the box for the job type you want.

The **Job Type** page shows cumulative information for all jobs of the selected type.

- **Total CPU** — The total CPU percentage utilization for all jobs of this type across all instances in the system.
- **Total Memory** — The total RAM consumed by all jobs of this type across all instances in the system.
- **Total Disk** — The total disk space consumed by all jobs of this type across all instances in the system.

The **Jobs** section lists each individual job of this type.

The **Instances** section shows a list of all system instances where jobs of this type are currently running.

The **Pool** section shows the instances that jobs of this type are allowed to run on.

The **Events** section shows a list of all events related to this job type.

Related CLI command(s)

getJobTypes

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API methods GET jobs types

GET /jobs/types

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Monitoring individual jobs

You can use Admin App, CLI, and REST API to view the status of individual jobs.



Note: Some functions described here are not used with HCP for cloud scale. They are not visible in the System Management application, or have no effect when used.

To view the detailed status for all jobs of a type, in the Admin App:

Procedure

1. Click on **Jobs**.
2. Click on the box for the job type you want.
3. Click on the box for the job you want.

The **Jobs** page shows this information about the job:

- **Error Count:** A tally of the number of errors encountered by the system when running the job or relocating it to other instances.
- **Status:**
 - **Idle:** The job has not run yet or, for jobs that have a schedule, the job is not scheduled to be running at the current time.
 - **Pending:** The job has been submitted for execution but is not yet running.
 - **Running:** The job is being executed.
 - **Completed:** The job finished execution without error.
 - **Failed:** The job finished execution with errors.
 - **Canceled:** The job has been canceled and is no longer running.
- If the task is configured to run according to a schedule, the **Status** panel shows this icon:



- **Service Units:** The per-instance cost for this job's type. Individual jobs do not cost any service units to run.
- **Total CPU:** The total CPU percentage utilization for this job across all instances in the system.
- **Total Memory:** The total RAM consumed by this job across all instances in the system.
- **Total Disk:** The total disk space consumed by this job across all instances in the system.

The **Instances** section shows a list of all system instances where the job is currently running.

To view information about the volumes that the job uses, click on the row for an instance in the **Instances** section.

The **Pool** section shows the instances that job is allowed to run on.

The **Events** section shows a list of all events related to this job.

Related CLI command(s)

```
getJobStatus
```

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

```
GET /jobs/status/{uuid}
```

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Monitoring processes

The **Processes** page lets you view information about what the system is doing. This includes any service operations you started and any internal maintenance processes the system needs to run.

Monitoring service operations

You can use the Admin App, CLI, and REST API to monitor all service operations. These operations include:

- The initial deployments of services when the system was installed.
- Service relocation operations that you initiate.

For each service operation, the system shows:

- The name of the service involved
- The status of the operation
- The number of steps completed out of the total number of steps for the operation

Admin App instructions

Procedure

1. Click on the **Processes** panel.

Result

The **Service Operations** tab shows information about in-progress and completed service operations.

Related CLI command(s)

`listSystemTasks`

`getSystemTask`

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

GET /tasks/system

GET /tasks/system/{uuid}

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Monitoring system processes

You can use Admin App, REST API, and CLI to view the progress of internal system processes. These include package installation tasks and regularly scheduled system maintenance activities such as log rotation.

For each process, your system shows:

- The process name
- The process state
- The times at which each step in the process run occurred



Note: System processes have a type of SCHEDULED or ONE-TIME.

Admin App instructions

Procedure

1. In the Admin App, click on **Processes**.
2. To view the currently running processes, click on the **System** tab.
3. To view the scheduled processes, click on the **Scheduled** tab.

Related CLI command(s)

listSystemTasks

getSystemTask

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

GET /tasks/system

GET /tasks/system/{uuid}

You can get help on specific REST API methods for the Admin App at REST API - Admin.

System events

Your system maintains a log of system events that you can view through the Admin App, CLI, and REST API.

Admin App instructions

Procedure

1. To view all system events, in the Admin App, click on **Events**.

Related CLI command(s)

queryEvents

To view events through the CLI, your requests need to specify which events you want to retrieve.

For example, this JSON request body searches the event log for all events that have a severity level of `warning`:

```
{
  "severities": [
    "warning"
  ]
}
```

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

POST /events

To view events through the REST API, your requests need to specify which events you want to retrieve.

For example, this JSON request body searches the event log for all events that have a severity level of `warning`:

```
{
  "severities": [
    "warning"
  ]
}
```

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Alerts

Your system displays alert messages to notify you of situations that require your attention. You can view these alerts through the Admin App, CLI, and REST API.

Each alert corresponds to a system event.

List of alerts


Severity	Alert Description	Action
Severe	Instance <ip-address> disk usage severe threshold	The specified instance has less than 10% free disk space. Add additional storage to the instance. Important: If an instance runs out of disk space, the system may become unresponsive.
Severe	Master Instance <ip-address> is down	Do one of these: <ul style="list-style-type: none"> Restart the instance hardware or virtual machine. Restart the <code>run</code> script on the instance. This script is located in the <code>bin</code> directory in the <code>install</code> directory.
Severe	Service is down	Check the health of your instances. If one is down, do one of these: <ul style="list-style-type: none"> Restart the instance hardware or virtual machine. Restart the <code>run</code> script on the instance. This script is located in the <code>bin</code> directory in the <code>install</code> directory. Otherwise, if your instances are healthy and the problem persists, contact support.
Severe	Worker Instance <ip-address> is down	Do one of these: <ul style="list-style-type: none"> Restart the instance hardware or virtual machine. Restart the <code>run</code> script on the instance. This script is located in the <code>bin</code> directory in the <code>install</code> directory.
Warning	Instance <ip-address> disk usage warning threshold	The specified instance has less than 25% free disk space. Add additional storage to the instance. Important: If an instance runs out of disk space, the system may become unresponsive.
Warning	Package installation failed	Your system failed to install a package that you uploaded.
Warning	Service below recommendation	The service is currently running on fewer than the recommended number of instances. Configure this service to run on additional instances.
Warning	Service under-protected	A service has lost redundancy; that is, one or more instances on which that service is running are unresponsive.

Severity	Alert Description	Action
		<p>Check the health of your instances. If one is down, do one of these:</p> <ul style="list-style-type: none"> Restart the instance hardware or virtual machine. Restart the <code>run</code> script on the instance. This script is located in the <code>bin</code> directory in the install directory. <p>Otherwise, if your instances are healthy and the problem persists, contact support.</p>
Warning	SSL server certificate chain expires soon	A certificate in the SSL server certificate chain for this system expires soon. If the certificate chain expires, users will be unable to access the system.
Warning	SSL server certificate chain expired	The SSL server certificate chain for this system contains an expired certificate. Users cannot access the system until the certificate chain is replaced.
Info	Package installation in progress	Your system is currently installing a package that you uploaded. Depending on the contents of the package, this may take a while.
Warning	The certificate for the storage component (storage_id) is about to expire in n days	Renew the storage component certificate.
Info	The storage component (storage_id) is unavailable	Verify that the storage component id is correct and valid and that the storage component is active.

Viewing alerts

Admin App instructions

Procedure

- To view alerts, click on the user icon () in the top righthand corner of each Admin App page, then click on Notifications.

Related CLI command(s)

`listAlerts`

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

GET /alerts

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Creating email notification rules

For the system to send email notifications, you need to create a rule that specifies who to email, what email server to use, what events to send emails about, and what information to include in email messages.

SMTP settings

- **Enable** — Turns on email notifications.
- **Host** — The hostname or IP address of the email server.
- **Port** — The port on which the email server listens for email messages.
- **Security** — The security protocol used by the email server (**SSL** or **STARTTLS**) or **None** if the email server doesn't use a security protocol.
- **Authenticated** — Enable this if the email server requires authentication, then specify:
 - In the **Username** field, the username for an email account that's authorized to establish the connection between the system and the email server.
 - In the **Password** field, the password for the email account.

Message settings

You use the email notification message settings to configure a template for formatting all email notifications sent by the system.

- **From** — The email address from which you want email notifications to be sent.
- **Subject** — The email subject.
- **Body** — The email message body.

Message variables

This table lists the variables you can use to construct the email notification template. When it sends an email notification, the system replaces the variables with event-specific information.

Variable	Description
\$severity	Event severity: INFO, WARNING, or SEVERITY
\$subject	A short description of the event
\$message	Event message text

Variable	Description
\$userName	Name of the user responsible for the event
\$objectId	Unique identifier for component affected by the event
\$subsystem	Category for the component affected by the event
\$objectSourceId	Unique identifier of the internal system component or process that was the source of the event. Value is [unknown] for most events.

Recipient settings

- **Email addresses** — A comma-separated list of email addresses to send notification emails to.
- **Severity Filter** — The event severities about which to send email notifications. Can be one or more of these: INFO, WARNING, SEVERITY.

Creating email notification rules

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Notifications**.
3. Click on the **Create** button.
4. In the **Type** field, select **Email**.
5. Enter a name for the notification rule.
6. Configure the SMTP settings and message settings for the notification rule.
7. Specify a comma-separated list of emails to send notifications to.
8. Specify a comma-separated list of emails to send notifications to.
9. Click on the **Create** button

Related CLI command(s)

createNotificationRule

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

POST /notifications

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Creating syslog notification rules

When you create a syslog notification rule, the system sends log messages to your syslog server for each applicable system event.

Syslog settings

- **Enable:** Turns on syslog notifications
- **Host:** The hostname or IP address of the syslog server
- **Port:** The port on which the syslog server listens for log messages
- **Facility:** Category for the messages sent by this notification rule

Message settings

You use the syslog notification message settings to configure a template for formatting all syslog notifications sent by this notification rule.

- **Message** The message to send. You can use these variables as part of the message:

Variable	Description
\$severity	Event severity: INFO, WARNING, or SEVERITY
\$subject	A short description of the event
\$message	Event message text
\$time	Time at which the event occurred
\$userName	Name of the user responsible for the event
\$subsystem	Category for the component affected by the event
\$objectId	Unique identifier for component affected by the event
\$objectType	The type of the component affected by the event.
\$objectSourceId	Unique identifier of the internal system component or process that was the source of the event. Value is [unknown] for most events.
\$objectSourceType	Type of the internal system component or process that was the source of the event. Value is [unknown] for most events.

- **Sender Identity:** Identity of the sender for the event. Sent with every syslog message.

Severity filter

The event severities about which to send email notifications. Can be one or more of these: INFO, WARNING, or SEVERITY.

Creating syslog notification rules

Admin App instructions

Procedure

1. Click on the **Configuration** panel
2. Click on **Notifications**.
3. Click on the **Create** button.
4. In the **Type** field, select **Syslog**.
5. Enter a name for the notification rule.
6. Configure the settings for the notification rule.
7. Specify a severity filter for the notification rule.
8. Click on the **Create** button

Related CLI command(s)

createNotificationRule

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

POST /notifications

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Logs and diagnostic information

Each service maintains its own set of logs. By default, the logs are maintained in the *install_path/log* directory on each instance in the system. During installation, you can configure each service to store its logs in a different, non-default location.

Log management

You can manage any of the log files yourself if you want to. That is, you can delete or archive them as necessary.



Note: Deleting log files may make it more difficult for support personnel to resolve issues you may encounter.

System logs are managed automatically in one or more of these ways:

- All log files are periodically added to a compressed file and moved to `install_path/retired/`. This occurs at least once a day, but can also occur at other times. For example:
 - Whenever you run the `log_download` script.
 - Hourly, if the system instance's disk space is more than 60% full.
 - At the optimum time for a specific service.
- When a log file grows larger than an optimum size, the system stops writing to that file, renames it, and begins writing to a new file. For example, if the file `exampleService.log.0` grows to 10MB, it is renamed to `exampleService.log.1` and the system creates a new file named `exampleService.log.0` to write to.
- When an optimum number of log files for a specific service is reached, the system can overwrite the oldest file. For example, if a service is limited to 20 log files, when the file `exampleService.log.19` is filled, the system overwrites the file named `exampleService.log.0`.

Retrieving logs and diagnostic information

The tool `log_download` lets you easily retrieve logs and diagnostic information from all instances in the system. This tool is located at this path on each instance:

```
install_path/bin/log_download
```

For information about running the tool, use this command:

```
install_path/bin/log_download -h
```



Note:

- When using the tool `log_download`, if you specify the option `--output`, do not specify an output path that contains colons, spaces, or symbolic links. If you omit the option `--output`, you cannot run the script from within a directory path that contains colons, spaces, or symbolic links.
- When you run the script `log_download`, all log files are automatically compressed and moved to the directory `install_path/retired/`.
- If an instance is down, you need to specify the option `--offline` to collect the logs from that instance. If your whole system is down, you need to run the `log_download` script with the `--offline` option on each instance.

Default log locations

By default, each service stores its logs in its own directory at this path:

```
install_path/log
```

This table shows the default log directory names for each service. Depending on how your system was configured when first deployed, your system's logs may not be stored in these directories.

Default log directory name	Related service	Contains information about
com.hds.ensemble.plugins.service.adminApp	Admin-App	The System Management application.
com.hds.ensemble.plugins.service.cassandra	Database	<ul style="list-style-type: none"> ▪ System configuration data. ▪ Document fields and values.
com.hds.ensemble.plugins.service.chronos	Scheduling	Workflow task scheduling.
com.hds.ensemble.plugins.service.elasticsearch	Metrics	<p>The storage and indexing of:</p> <ul style="list-style-type: none"> ▪ System events ▪ Performance and failure metrics for workflow tasks
com.hds.ensemble.plugins.service.haproxy	Network-Proxy	Network requests between instances.
com.hds.ensemble.plugins.service.kafka	Message Queue	Transmission of data between instances.
com.hds.ensemble.plugins.service.logstash	Logging	The transport of system events and workflow task metrics to the Metrics service.
com.hds.ensemble.plugins.service.marathon	Service-Deployment	The deployment of high-level services across system instances. High-level services are the ones that you can move and configure, not the services grouped under System Services.

Default log directory name	Related service	Contains information about
com.hds.ensemble.plugins.service.mesosAgent	Cluster-Worker	Work ordered by the Cluster-Coordination service.
com.hds.ensemble.plugins.service.mesosMaster	Cluster-Coordination	Hardware resource allocation.
com.hds.ensemble.plugins.service.remoteAction	Watchdog	Internal system processes.
com.hds.ensemble.plugins.service.sentinel	Sentinel	Internal system processes.
com.hds.ensemble.plugins.service.solr	Index	Index collections and search indexes.
com.hds.ensemble.plugins.service.watchdog	Watchdog	General diagnostic information.
com.hds.ensemble.plugins.service.zookeeper	Synchronization	Coordination of actions and database operations across instances.
com.hitachi.aspen.foundry.service.mapi.gateway	MAPI-Gateway	Management of API requests.
com.hitachi.aspen.foundry.service.metadata.cache	Metadata-Cache API requests	Transmission of system metadata between instances.
com.hitachi.aspen.foundry.service.metadata.coordination	Metadata-Coordination	Transmission of system metadata between instances.
com.hitachi.aspen.foundry.service.metadata.gateway	Metadata-Gateway	Transmission of system metadata between instances.
com.hitachi.aspen.foundry.service.metadata.async.policy.engine	Metadata-Policy-Engine	Update operations.
com.hitachi.aspen.foundry.service.clientaccess.data	S3-Gateway	Transmission of S3 requests to endpoints.

Default log directory name	Related service	Contains information about
com.hitachi.aspen.foundry.service.jaeger.agent	Tracing-Agent	Usage of tracing operations.
com.hitachi.aspen.foundry.service.jaeger.collector	Tracing-Collector	Usage of tracing collections.
com.hitachi.aspen.foundry.service.jaeger.query	Tracing-Query	Usage of tracing queries.

Chapter 4: Security

This section contains information on configuring system security features, including user authentication.

Granting access to users

These are the general steps you need to take to grant users access to the system:

1. Add one or more identity providers to the system.
For information, see [Adding identity providers \(on page 63\)](#).
2. Add one or more groups from your identity providers to the system.
For information, see [Adding groups \(on page 68\)](#).
3. Create a role that contains the system permissions you want to associate with a group of users.
For information, see [Creating roles \(on page 70\)](#).
4. Associate roles with groups.
For information, see [Assigning roles to groups \(on page 69\)](#).

Setting the session timeout limit

You can use the Admin App, REST API, or CLI to set the system session timeout limit. This limit affects user sessions in all applications that your system runs and also affects the length of time that REST API authorization tokens are valid.

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Security**.
3. On the **Settings** tab, type a number of minutes in the **Session Timeout** field.
4. Click on the **Update** button.

Related CLI command(s)

`editSecuritySettings`

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

PUT /security/settings

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Identity providers

The system supports these identity provider types for user authentication:

- Active Directory (AD)
- OpenLDAP
- 389 Directory Server
- LDAP Compatible — Other LDAP-compatible identity providers not listed above.

To use one of these systems to authenticate users with your system, you need to first add your identity provider to the system.

Adding identity providers

For information on the types of identity providers you can add, see [Identity provider configuration settings \(on page 63\)](#).

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Security**.
3. On the **Identity Providers** tab, click on the **Create** button.
4. Select an identity provider type and configure it. For information, see [Identity provider configuration settings \(on page 63\)](#).
5. Click on the **Create** button.

Related CLI command(s)

createIdentityProvider

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

POST /security/identityProviders

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Identity provider configuration settings

These sections describe the configuration settings for each type of identity provider that your system supports.

All types

Security Realm Name — The name by which to identify this identity provider in the system. This name appears as an option in the Security Realm drop-down on Admin App login pages.



Tip: To ensure that your users can easily log into the system, pick security realm names that your users will recognize and understand.

Active Directory

- **Identity Provider Hostname** — Hostname or IP address for the identity provider.
- **Transport Security** — The protocol to use for securing communications between the system and the identity provider. Options are:
 - **None**
 - **TLS Security (Transport Layer Security)**
 - **SSL (Secure Sockets Layer)**
- **Identity Provider Host Port** — Network port used to communicate with the identity provider. The default value depends on the **Transport Security** setting:
 - For **None** or **TLS Security (Transport Layer Security)**, 389
 - For **SSL (Secure Sockets Layer)**, 636
- **User Name** — A user account on the identity provider. Your system uses this user account to read information from the identity provider.
- **Password** — The user account password.
- **Domain** — The AD domain in which the user account is defined.



Note: Use the short name for the AD domain. For example, use `MYACTIVEDIRECTORY` instead of `MYACTIVEDIRECTORY.local`.

- **Search Base DN** — The distinguished name (DN) of the identity provider location where you want your system to begin its searches for users and groups.
For example, if you specify a value of **OU=Users,DC=corp,DC=example,DC=com**, the system searches for users and groups in the organization unit called **Users** in the **corp.example.com** domain.
- **Default Domain Name** — The default domain for users logging into the Admin App and Search App. For example, if you specify a default domain name of **east.example.com**, the user **jdoh@east.example.com** needs to specify only **jdoh** when logging into either app.

LDAP Compatible

- **Identity Provider Hostname** — Hostname or IP address for the identity provider.
- **Transport Security** — The protocol to use for securing communications between the system and the identity provider. Options are:
 - **None**
 - **TLS Security (Transport Layer Security)**
 - **SSL (Secure Sockets Layer)**
- **Identity Provider Host Port** — Network port used to communicate with the identity provider. The default value depends on the **Transport Security** setting:
 - For **None** or **TLS Security (Transport Layer Security)**, 389
 - For **SSL (Secure Sockets Layer)**, 636
- **User Name** — A user account on the identity provider. Your system uses this account to read information from the identity provider.
- **Password** — The user account password.
- **User DN Template** — A template on the LDAP server. When a user logs into their system, the provided username is inserted into this template to determine the user's LDAP distinguished name (DN).
- **Unique ID** — The unique identifier for the specified LDAP server.
- **Member Name Attribute** — The name of the attribute that each group on the identity provider uses to list its members.
- **Search Base DN** — The distinguished name (DN) of the identity provider location where you want your system to begin searching for users and groups.
 For example, if you specify a value of **OU=Users,DC=corp,DC=example,DC=com**, your system searches for users and groups in the organization unit called **Users** in the **corp.example.com** domain.
- **Group Object Class** — The objectClass value for groups on the LDAP server.

OpenLDAP and 389 Directory Server

- **Identity Provider Hostname** — Hostname or IP address for the identity provider.
- **Transport Security** — The protocol to use for securing communications between the system and the identity provider. Options are:
 - **None**
 - **TLS Security (Transport Layer Security)**
 - **SSL (Secure Sockets Layer)**
- **Identity Provider Host Port** — Network port used to communicate with the identity provider. The default value depends on the **Transport Security** setting:
 - For **None** or **TLS Security (Transport Layer Security)**, 389
 - For **SSL (Secure Sockets Layer)**, 636

- **User Name** — A user account on the identity provider. Your system uses this account to read information from the identity provider.
- **Password** — The user account password.
- **User DN Template** — A template on the LDAP server. When a user logs into their system, the provided username is inserted into this template to determine the user's LDAP distinguished name (DN).
- **Unique ID** — The unique identifier for the specified LDAP server.
- **Member Name Attribute** — The name of the attribute that each group on the identity provider uses to list its members.
- **Search Base DN** — The distinguished name (DN) of the identity provider location where you want your system to begin searching for users and groups.

For example, if you specify a value of **OU=Users,DC=corp,DC=example,DC=com**, your system searches for users and groups in the organization unit called **Users** in the **corp.example.com** domain.

User information caching

The system caches the following information from each of your identity providers:

- The names of users who access the system
- The groups that each user belongs to

As long as this information is in the system's cache, your users can perform any activities for which they have permissions, without the system needing to reconnect to the identity provider.

LDAP user information remains in the cache for four hours.

Clearing the cache

Any changes that you make on the identity provider are not reflected in the system until the information is removed from the cache. For example, if you add a user to an LDAP identity provider, that user will be unable to access the system for up to four hours, or until the cache is cleared. If you delete a user from an LDAP identity provider, that user will be able to access the system for up to four hours, or until the cache is cleared.

To ensure that a change is reflected immediately, use the `clearCache` command or API.

Related CLI command(s)

`clearCache`

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

POST `/security/clearCache`

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Viewing identity providers

You can use the Admin App, REST API, and CLI to view the identity providers that have been added to your system.

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Security**.
3. Click on the **Identity Providers** tab.

Related CLI command(s)

```
getIdentityProvider
```

```
listIdentityProviders
```

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

```
GET /security/identityProviders/{uuid}
```

```
GET /security/identityProviders
```


You can get help on specific REST API methods for the Admin App at REST API - Admin.

Deleting identity providers

When you delete an identity provider from your system, all users from that provider lose access to the system.

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Security**.
3. On the **Identity Providers** tab, click on the delete icon () for the server you want to remove.

Related CLI command(s)

```
deleteIdentityProvider
```

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

```
DELETE /security/identityProviders/{uuid}
```

You can get help on specific REST API methods for the Admin App at [REST API - Admin](#).

Groups

To allow user access to your system, you need to add groups to your system. These groups are defined on your organization's identity providers. Once you've added a group to your system, you can specify what roles its members have.

For information on:

- Adding identity providers to your system, see [Adding identity providers \(on page 63\)](#).
- Roles, see [Roles \(on page 70\)](#).

Adding groups

You use the REST API, Admin App, or CLI to add groups from your identity providers to your system.

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Security**.
3. On the **Groups** tab, click on the **Create** button.
4. Select an identity provider and type a string on which to query the identity provider for groups.
5. Click on the **Discover Groups** button.
6. Click on the **Continue** button.
7. Select one or more roles to associate with the group.
8. Click on the **Create** button.

Related CLI command(s)

`createGroup`

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

`POST /security/groups`

You can get help on specific REST API methods for the Admin App at [REST API - Admin](#).

Viewing groups

You use the REST API, CLI, or Admin App to view all the groups that have been created for your system.

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Security**.
3. Click on the **Groups** tab.

Related CLI command(s)

getGroup

listGroups

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

GET /security/groups/{uuid}

GET /security/groups

For information on specific REST API methods, in the Admin App, click on the help icon (🗨). Then:

- To view the administrative REST API methods, click on **Admin API**.
- To view the API methods used for performing searches, click on **Search API**.

For general information about the administrative REST API, see [REST API reference](#).

Assigning roles to groups

You use the REST API, Admin App, and CLI to assign roles to the groups that you've added your system.

Admin App instructions**Procedure**

1. Click on the **Configuration** panel.
2. Click on **Security**.
3. On the **Groups** tab, click on the group you want to edit.
4. On the **Roles** tab, select one or more roles to enable for the group.
5. Click on the **Update** button.

Related CLI command(s)

editGroup

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

PUT /security/groups/{uuid}


You can get help on specific REST API methods for the Admin App at REST API - Admin.

Deleting groups

When you delete a group, all users in the group lose access to your system.

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Security**.
3. Click on the **Groups** tab.
4. Click on the delete icon () for the group you want to remove.

Related CLI command(s)

```
deleteGroup
```

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

```
DELETE /security/groups/{uuid}
```

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Roles

Roles determine what actions a group of users can perform. You create your own roles, each of which can grant permission to perform any combination of actions.

For information on associating a role with a group of users, see [Assigning roles to groups \(on page 69\)](#).

Creating roles

You can use the REST API, Admin App, and CLI to create roles and select which permissions the roles contain.

About permissions

Each permission in a role grants a user the ability to perform an action in some area of the system. For example, the **admin:services:read** permission grants the ability to view services through the Admin App.

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Security**.
3. On the **Roles** tab, click on the **Create** button.

4. Specify a name and, optionally, a description for the role.
5. Use the **Individual** and **Wildcard** tabs to edit the permissions for the role.
On the **Individual** tab, you can enable individual permissions or categories of permissions:

- Click on a category of permissions and select one or more individual permissions within the category.

For example, with the permissions selected in this image, a user can read, create, and update certificates, but cannot delete them.

Permissions Group - Certificates		BACK
<input checked="" type="checkbox"/>	Name ↑	Description
<input checked="" type="checkbox"/>	workflowcertificates:create	Create certificate
<input type="checkbox"/>	workflowcertificates:delete	Delete certificates
<input checked="" type="checkbox"/>	workflowcertificates:read	Read certificate(s)
<input checked="" type="checkbox"/>	workflowcertificates:update	Generate certificate

- On the **Wildcard** tab, you can enable permissions for multiple categories at the same time. To do this:
 - a. Click on the **Add Permission** button.
 - b. Use the drop-down menus to select a category of permissions.
 - c. Leave the last drop-down menu set to the wildcard character (*).
6. Click on the **Create** button.
 7. Click on the **Update** button.

Related CLI command(s)

createRole

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

POST /security/roles

Viewing roles

You can use the REST API, CLI, and Admin App to view all the roles that have been created for your system.

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Security**.
3. Click on the **Roles** tab.

Related CLI command(s)

getRole

listRoles

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

GET /security/roles/{uuid}

GET /security/roles

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Editing roles

You can use the REST API, Admin App, and CLI to change the permissions that a role contains.

About permissions

Each permission in a role grants a user the ability to perform an action in some area of the system. For example, the **admin:services:read** permission grants the ability to view services through the Admin App.

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Security**.
3. Click on the **Roles** tab.
4. Click on the role you want to edit.
5. Use the **Individual** and **Wildcard** tabs to edit the permissions for the role.

On the **Individual** tab, you can enable individual permissions or categories of permissions:

- Click on a category of permissions and select one or more individual permissions within the category.

For example, with the permissions selected in this image, a user can read, create, and update certificates, but cannot delete them.

Permissions Group - Certificates		BACK
<input checked="" type="checkbox"/>	Name ↑	Description
<input checked="" type="checkbox"/>	workflowcertificates:create	Create certificate
<input type="checkbox"/>	workflowcertificates:delete	Delete certificates
<input checked="" type="checkbox"/>	workflowcertificates:read	Read certificate(s)
<input checked="" type="checkbox"/>	workflowcertificates:update	Generate certificate

- On the **Wildcard** tab, you can enable permissions for multiple categories at the same time. To do this:
 - Click on the **Add Permission** button.
 - Use the drop-down menus to select a category of permissions.
 - Leave the last drop-down menu set to the wildcard character (*).
- Click on the **Create** button.
- Click on the **Update** button.

Related CLI command(s)

editRole

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

PUT /security/roles/{uuid}


You can get help on specific REST API methods for the Admin App at REST API - Admin.

Deleting roles

When you delete a role, all groups associated with that role lose the permissions that the role granted.

Admin App instructions

Procedure

- Click on the **Configuration** panel.
- Click on **Security**.
- Click on the **Roles** tab.
- Click on the delete icon () for the role you want to remove.

Related CLI command(s)

deleteRole

For information on running CLI commands, see [CLI reference \(on page 123\)](#).**Related REST API method(s)**

DELETE /security/roles/{uuid}

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Permissions

The following tables list the permissions available for system roles. The words *Yes* and *No* indicate whether or not the permission is assigned for a default role.

Bucket Sync-to and Sync-from		
Permission name	Description	Default admin role permission?
bucket_sync:read	View bucket sync rules for buckets the user owns or has access to	Yes
bucket_sync:to:write	Create bucket sync-to rules for buckets the user owns or has access to	Yes
bucket_sync:from:write	Create bucket sync-from rules for buckets the user owns or has access to	Yes

MAPI Alerts		
Permission name	Description	Default admin role permission?
mapi:alert:list	List all active alerts	Yes

MAPI Job Configurations		
Permission name	Description	Default admin role permission?
mapi:job_configuration:list	List all job configurations	Yes
mapi:job_configuration:run	Run a job configuration immediately	Yes
mapi:job_configuration:update	Modify a job configuration	Yes

MAPI S3 Settings		
Permission name	Description	Default admin role permission?
mapi:s3_settings:get	Read S3 settings	Yes
mapi:s3_settings:set	Modify S3 settings	Yes

MAPI Storage Component		
Permission name	Description	Default admin role permission?
mapi:storage_component:activate	Activate a storage component	Yes
mapi:storage_component:create	Create a storage component	Yes
mapi:storage_component:list	List storage component(s)	Yes
mapi:storage_component:test	Test a storage component	Yes
mapi:storage_component:update	Modify a storage component	Yes
mapi:storage_component:update_state	Modify state of a storage component	Yes

MAPI Stored Objects		
Permission name	Description	Default admin role permission?
map:client_object:lookup	List stored objects	Yes

MAPI System		
Permission name	Description	Default admin role permission?
map:system:info	List system information	Yes

MAPI User		
Permission name	Description	Default admin role permission?
map:user:list	List system information	Yes
map:user:list_bucket	List user buckets	Yes
map:user:revoke_credentials	Revoke S3 credentials	Yes
map:user:revoke_tokens	Revoke OAuth tokens	Yes

S3 User		
Permission name	Description	Default admin role permission?
s3:user:generate_credentials	Generate S3 credentials	Yes

Serial Number		
Permission name	Description	Default admin role permission?
mapi:serial_number:get	Read serial number	Yes
mapi:serial_number:set	Modify serial number	Yes

Changing the admin account password

Your system includes a single local user account called admin, which is available when you first install the system. You can use the REST API, Admin App, or CLI to change the password for this account.

Admin App instructions

Procedure

1. When logged into the Admin App with the admin user account, click on the user icon (👤) in the top righthand corner of the screen.
2. Click on **Change Password**.
3. Confirm your current password and specify a new password.
4. Click on the **Change Password** button.

Related CLI command(s)

updateCurrentUserPassword

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

POST /setup/password

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Certificates

Your system uses SSL to provide security for the Admin App. To enable SSL security, you need a valid SSL server certificate or chain of certificates.

Your system comes with its own self-signed SSL server certificate, which is generated and installed automatically when the system is installed. This certificate is not automatically trusted by web browsers.

You can choose to trust this self-signed certificate or to replace it with one from a certificate authority (CA) or one that you create yourself. You can also have the system generate and install a new self-signed SSL server certificate. You would do this, for example, if the current certificate is close to expiring and you are waiting to retrieve a new one from your CA.

Viewing installed certificates

You can use the REST API, CLI, and Admin App to view information about:

- The system certificate. That is, the certificate used to secure communications for your system's applications, CLIs, and REST APIs.
- Data source certificates. These are the certificates retrieved from the systems that your system has connected to using a data connection.

For each certificate, you can view:

- The distinguished name of the certificate
- The date and time when the certificate goes (or went) into effect
- The date and time when the certificate expires (or expired)

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Certificates**.
The **System** tab displays the currently active system certificate.
3. To view the data source certificates, click on the **Client** tab.

Related CLI command(s)

listCertificates

getCertificate

getSystemCertificate

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

GET /certificates

GET /certificates/system

GET /certificates/{subjectDn}

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Adding data source certificates

For your system to retrieve documents from a data source that uses SSL-protected communication, it must accept the certificate from the data source. Your system prompts you to accept a data source certificate when it tests the connection to the data source. You can also upload data source certificates manually.

Uploading data source certificates manually

Procedure

1. Retrieve the SSL certificate from your data source.
2. In the Admin App, click on **Configuration**.
3. Click on **Certificates**.
4. On the **Client** tab, click on **Upload Client Certificate**.
5. Click and drag the certificate file into the **Upload License** box.

Related CLI command(s)

```
testDataSource  
createCertificate
```

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

```
POST /datasources/test  
POST /certificates
```

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Changing the system certificate

By default, your system includes a self-signed certificate when the system is first installed.

You cannot delete the currently installed certificate. However, you can replace it by:

- Installing a new PKCS12 certificate (for instructions, see [Installing a certificate you created \(on page 80\)](#))
- Generating and installing a new self-signed certificate (for instructions, see [Installing a new self-signed certificate \(on page 81\)](#))
- Generating a certificate signing request (CSR) and installing the certificate you receive in response to this request (for instructions, see [Creating a CSR and installing the returned certificate \(on page 82\)](#))

System certificate considerations

Keep the following in mind when configuring SSL certificates for your system, especially if you are configuring the system to use one or more certificates that you create yourself:

- Do not allow any of the SSL certificates to expire.
- Adhere to the established best practices for setting up SSL certificates. For example, if you are using wildcards to identify hostnames in an SSL certificate, a wildcard should appear only at the beginning of the hostname, not in the middle.

For information on SSL best practices, see <http://tools.ietf.org/html/rfc5280> and <http://tools.ietf.org/html/rfc6125>.

- Ensure that the DNS name for the system matches the name defined in the certificate.
- When configuring a certificate chain, ensure that all intermediate issuers have the appropriate signing authority permissions so that the entire chain is signed.

Installing a certificate you created

You can create an SSL server certificate by using a third-party tool such as OpenSSL. When creating the certificate, you specify two passwords — one for the PKCS12 object containing the certificate and one for the private key for the certificate. To use the certificate with your system, these passwords must be the same.

When you create your own SSL server certificate, you can choose to have that certificate signed by a certificate authority (CA). In this case, the CA you use may provide you with one or more intermediate certificates. These certificates are used in conjunction with the SSL server certificate you created to establish a certificate chain, an ordered list of certificates in which each certificate is trusted by the next.

To preserve the chain of trust among the certificates, you need to upload the certificates in the correct order. That is, each certificate you upload must be immediately followed by the certificate that signs it. For information on the correct order for the certificate chain, see your CA.



Important: Read and understand the topic [System certificate considerations \(on page 80\)](#) before creating your own SSL certificates and especially if you are using an in-house CA.

Admin App instructions

To install your certificates:

Procedure

1. Click on the **Configuration** panel.
2. Click on **Certificates**.
3. Click on the **Update System Certificate** button.
4. On the **PKCS12** panel, click and drag your certificate into the **Upload Certificate Chain** box.
5. In the **PKCS12 Password** field, type the password for your certificate.
6. Click and drag the certificate into the **Upload Certificate Chain** box.

7. Click on the **Continue** button.
8. Click on the **Accept** button.

Related CLI command(s)

uploadPKCS12Certificate

applyCertificateChanges

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

POST /certificates/system/pkcs12

POST /certificates/system

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Installing a new self-signed certificate

Your system can generate and install a new self-signed SSL server certificate. The new certificate is good for five years.



Note: If the system is using a self-signed certificate, when you change the hostname name of the system, you need to generate a new SSL certificate.

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Certificates**.
3. Click on **Update System Certificate**.
4. Click on the **Self-Signed** panel.
5. Click on the **Continue** button.
Your system generates a new self-signed server certificate.
6. Click on the **Accept** button.
Your system installs the new certificate.
7. To continue using the Admin App, log out and then log back in.

Related CLI command(s)

generateSelfSignedCertificate

applyCertificateChanges

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

POST /certificates/system/selfsigned

POST /certificates/system

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Creating a CSR and installing the returned certificate

SSL server certificates are available from several trusted sources. To obtain a certificate created by a certificate authority (CA), you need to create a certificate signing request (CSR) and give it to the CA. The CA then generates the requested certificate and makes it available to you.

Creating a certificate signing request

You can create a CSR using the Admin App or a third-party tool. When you use the Admin App, the system securely stores the private key needed for installing the returned certificate, so you don't need to save it yourself.

To know exactly what information is required, check with the CA you plan to use.

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Certificates**.
3. Click on the **System** tab.
4. Click on **Update System Certificate**.
5. Click on the **CSR** panel.
6. Choose **Generate a new certificate signing request** and click on the **Continue** button.
7. Fill in the fields as needed:
 - In the **Common Name (CN)** field, type the DNS name of the system preceded by an asterisk (*) and a period (.) (for example, *.system.example.com).
The **Common Name (CN)** field is required.
 - In the **Organizational Unit (OU)** field, type the name of the organizational unit that uses the system (for example, the name of a division or a name under which your company does business).
 - In the **Organization (O)** field, type the full legal name of your organization.
 - In the **Location (L)** field, type the name of the city in which your organization's headquarters are located.
 - In the **State/Province (ST)** field, type the full name of the state or province in which your organization's headquarters are located.
 - In the **Country (C)** field, type the two-letter ISO 3166-1 abbreviation for the country in which your organization's headquarters are located (for example, US for the United States).
8. Click on the **Generate CSR** button.
The page displays the generated certificate request.

9. Copy and paste the request text into a file and send that file to your CA.
10. Continue to [Installing the certificates returned for a system-generated CSR \(on page 83\)](#).

Related CLI command(s)

generateCSR

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

PUT /certificates/system/csr

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Installing the certificates returned for a system-generated CSR

In response to a CSR, your CA provides you with an SSL server certificate and any required **intermediate certificates**. These certificates are used in conjunction with the SSL server certificate to establish a **certificate chain**, an ordered list of certificates in which each certificate is trusted by the next. You need to upload and install these certificates on your system.

To preserve the chain of trust among the certificates, you need to upload the certificates in the correct order. That is, each certificate you upload must be immediately followed by the certificate that signs it. For information on the correct order for the certificate chain, see your CA.

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Certificates**.
3. Click on the **System** tab.
4. Click on **Update System Certificate**.
5. Click on the **CSR** panel.
6. Select the **I already generated a CSR and obtained a signed certificate** option and click on the **Continue** button.
7. Click and drag the certificate into the **Upload certificate obtained from Certificate Authority** box.
8. Click on the **Accept** button.

Related CLI command(s)

uploadCSR

applyCertificateChanges

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API methods

POST /certificates/system/csr

POST /certificates/system

You can get help on specific REST API methods for the Admin App at [REST API - Admin](#).

Chapter 5: System management

As an administrator, you play a role in ensuring the continued accessibility and performance of the system. You can use the Admin App, command line, or REST API to manage the system.

Your responsibilities for administering the system include:

- Managing and monitoring system performance and resource usage by configuring how instances are deployed in your infrastructure.
- Expanding functionality by writing and installing plugins.
- Setting up email notifications.
- Upgrading the system.

Setting the system hostname

After installing your system, you need to configure it with the hostname that you've assigned to it in your corporate DNS environment.

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Security**.
3. On the **Settings** tab, specify the hostname in the **Cluster Hostname** field.
4. Click on the **Update** button.

Related CLI command(s)

`editSecuritySettings`

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

`PUT /security/settings`

You can get help on specific REST API methods for the Admin App at REST API - Admin.

System scaling

You manage how the system scales by adding or removing instances to the system and also by specifying which services run on those instances.

Instances

An instance is a server or virtual machine on which the software is running. A system can have either a single instance or multiple instances. Multi-instance systems have a minimum of four instances.

A system with multiple instances maintains higher availability in case of instance failures. Additionally, a system with more instances can run tasks concurrently and can typically process tasks faster than a system with fewer or only one instance.

A multi-instance system has two types of instances: master instances, which run an essential set of services, and non-master instances, which are called workers.

Services

Each instance runs a configurable set of services, each of which performs a specific function. For example, the Metadata Gateway service stores metadata persistently.

In a single-instance system, that instance runs all services. In a multi-instance system, services can be distributed across all instances.

Networking

This topic describes the network usage by, and requirements for, both system instances and services.



Note:

- You can configure the network settings for each service when you install the system. You cannot change these settings after the system is up and running.
- If your networking environment changes such that the system can no longer function with its current networking configuration, you need to reinstall the system.

Site hostname

The HCP for cloud scale site hostname is configured during installation. This hostname is very important because it is required for access to:

- The HCP for cloud scale user interface
- The S3 API

Instance IP address requirements

All instance IP addresses must be static. This includes both internal and external network IP addresses, if applicable to your system.



Important: If the IP address of any instance changes, you must reinstall the system.

Network types

Each of the HCP for cloud scale services can bind to one type of network, either **internal** or **external**, for receiving incoming traffic. If your network infrastructure supports having two networks, you may want to isolate the traffic for most system services to a secured internal network that has limited access. You would then leave the following services on your external network for user access:

- Admin-App
- Metadata-Cache
- Metadata-Coordination
- Metadata-Gateway
- Metadata-Policy-Engine
- Metrics
- S3-Gateway
- Tracing-Agent
- Tracing-Collector
- Tracing-Query
- MAPI-Gateway

You can use either a single network type for all services or a mix of both types. If you want to use both types, every instance in your system must be addressable by two IP addresses; one on your internal network, and one on your external network. If you use only one network type, each instance needs only one IP address.

Allowing access to external resources

Regardless of whether you're using a single network type or a mix of types, you need to configure your network environment to ensure that all instances have outgoing access to the external resources you want to use, such as:

- The storage components where your object data is stored
- Identity providers for user authentication
- Email servers that you want to use for sending email notifications

Ports

Each service binds to a number of ports for receiving incoming traffic.

Before installing HCP for cloud scale, you can configure the services to use different ports, or use the default values shown in the tables below.

External ports

The following table contains information about the service ports that users use to interact with the system.

On every instance in the system, each of these ports:

- Must be accessible from any network that requires administrative or data access to the system
- Must be accessible from every other instance in the system



Note: Debugging ports are accessible only when `debug` is set to `true` in `install_path/hcpcs/config/cluster.config`

Default Port Value	Used by Service	Purpose
80 (S3 HTTP port, if enabled)	S3 Gateway	Object persistence and access
443 (S3 HTTPS port)	S3 Gateway	Object persistence and access
8000	Admin App	System Management application GUI
9099	MAPI Gateway	Object Storage Management application GUI

Internal ports

This table lists the ports used for intrasystem communication by the services. On every instance in the system, each of these ports:

- Must be accessible from every other instance in the system
- Should not be accessible from outside the system

You can find more information about how these ports are used in the documentation for the third-party software underlying each service

Default Port Value	Used By	Purpose
2181	Synchronization	Primary port used to communicate with the service
2888	Synchronization	Server-server communication
3888	Synchronization	Leader elections
5000	Synchronization	Debugging
5001	Admin App	Debugging
5004	Watchdog	Debugging

Default Port Value	Used By	Purpose
5007	Sentinel	Debugging
5050	Cluster Coordination	Primary port used to communicate with the master service
5051	Cluster Worker	Primary port used to communicate with the worker service
5555	Watchdog	Primary port used for JMX inter-service communication
5778	Tracing Agent	Agent HTTP port
6831	Tracing Agent	UDP port
7000	Cassandra	TCP port for database commands and data
7199	Cassandra	Used for database JMX connections
7203	Kafka	Used for message queue JMX connections
8005	Admin App	Tomcat shutdown port
8007	Sentinel	Tomcat shutdown port
8022	Watchdog	SSH
8080	Service Deployment	Primary port used to communicate with the service
8081	Chronos	Primary port used to communicate with the scheduling service
8889	Sentinel	Primary port used to communicate with the service
9042	Cassandra	Primary port used to communicate with the database service
9091	Network Proxy	Primary port used to communicate with the HA proxy service
9092	Kafka	Primary port used to communicate with the message queue service
9190	OAuth	OAuth port
9191	Metrics	Primary port used to communicate with the service
9200	Elasticsearch	Used to communicate with Elasticsearch cluster

Default Port Value	Used By	Purpose
9201	Elasticsearch	Used to communicate with Elasticsearch nodes
9301	Elasticsearch	Elasticsearch intercluster communication
9600	Logstash	Primary port used to communicate with the logging service
9601	Logstash	Port used to listen for syslog connections
9750	S3 Gateway	Support
9751	Metadata Gateway	Support
9752	MAPI Gateway	Support
9753	Metadata Cache	Support
9758	Metadata Policy Engine	Support
9760	Metadata Coordination	Support
9990	S3 Gateway	Remote monitoring
9991	Metadata Gateway	Monitoring
9992	MAPI Gateway	Monitoring
9993	Metadata Cache	Monitoring
9998	Metadata Policy Engine	Monitoring
10000	Metadata Coordination	Monitoring
12000	S3 Gateway	Debugging
12001	Metadata Gateway	Debugging
12002	MAPI Gateway	Debugging
12003	Metadata Cache	Debugging
12004	Metrics	Debugging
12005	Tracing Collector	Debugging
12006	Tracing Query	Debugging
12007	Tracing Agent	Debugging
12008	Metadata Policy Engine	Debugging
12010	Metadata Coordination	Debugging

Default Port Value	Used By	Purpose
12500	Metadata Gateway	Raft RPC Communication
12501	Metadata Gateway	Metadata RPC Communication
12510	Metadata Coordination	RPC communication
12520	Metadata Policy Engine	RPC communication
13300	Metadata Cache	Cache TCP discovery
13370	S3 Gateway	Cache TCP communication
13371	Metadata Gateway	Cache TCP communication
13372	MAPI Gateway	Cache TCP communication
13373	Metadata Cache	Cache TCP communication
13378	Metadata Policy Engine	Cache TCP communication
13380	Metadata Coordination	Cache TCP communication
13453	Metadata Cache	Cache TCP communication
13500	S3 Gateway	Cache client connector
13501	Metadata Gateway	Cache client connector
13502	MAPI Gateway	Cache client connector
13503	Metadata Cache	Cache client connector
13508	Metadata Policy Engine	Cache client connector
13510	Metadata Coordination	Cache client connector
14267	Tracing Collector	Collecting thrift spans from tracing agents
14268	Tracing Collector	HTTP port
15050	Cluster Coordination	Local port to which the service directly binds
16686	Tracing Query	HTTP port (APIs and user interface)
18000	Admin App	Local port to which the service directly binds
18080	Service Deployment	Local port to which the service directly binds
18889	Sentinel	Local port to which the service directly binds
31000 to 34000	Service Deployment	Port range used by both Service Deployment and Docker for running containers

Default Port Value	Used By	Purpose
47000	Cache	TCP cache communication
47008	Metadata Policy Engine	TCP cache communication
47500	Cache	TCP cache discovery
48000	Cache	TCP connector
48500	Cache	Client connector
48508	Metadata Policy Engine	Client connector

Handling network changes

Once your system is deployed, its network infrastructure and configuration should not change. Specifically:

- All instance IP addresses should not change.
- All services should continue to use the same ports.
- All services and instances should continue to use the same network types.

If any of the above change, you will need to reinstall the system.

Safely changing an instance IP address

If you need to change the IP addresses for one or more instances in the system, use this procedure to manually change the IP addresses without risk of data loss.

For each instance whose IP address you need to change:

Procedure

1. Move all services off of the instance. Distribute those services among all the other instances.
2. On the instance from step 1, stop the `run` script using whatever tool or process you used to run it. For example, with `systemd`, run:


```
systemctl stop <service-name>
```
3. Remove the instance from the system.
4. Delete the installation directory from the instance.
5. Add the instance back to the system.

After a network change

If a network infrastructure or configuration change occurs that prevents your system from functioning with its current network settings, you need to reinstall all instances in the system.

Procedure

1. If the Admin App is accessible, back up your system components by exporting a package.
2. On each instance in the system:
 - a. Navigate to the installation directory.
 - b. Stop the run script using whatever tool or process you used to run it. For example, with systemd, run:


```
systemctl stop <service-name>
```
 - c. Run `bin/stop`
 - d. Run the setup script, including the list of master instances:

```
sudo bin/setup -i <ip-address-for-this-instance> -m
<comma-separated-list-of-master-instance-IP-addresses>
```

- e. Run the run script using whatever methods you usually use to run scripts.
3. Log into Admin App and use the wizard to setup the system.
4. After the system has been setup, upload your package.

Volumes

Volumes are properties of services that specify where and how a service stores its data.

You can use volumes to configure services to store their data in external storage systems, outside of the system instances. This allows data to be more easily backed up or migrated.

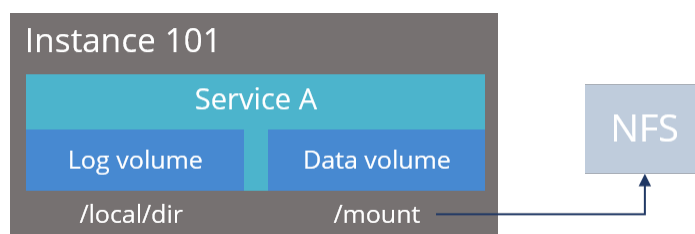
Volumes can also allow services to store different types of data in different locations. For example, a service may use two separate volumes, one for storing its logs and the other for storing all other data.



Note: Some functions described here are not used with HCP for cloud scale. They are not visible in the System Management application, or have no effect when used.

Example

In this example, service A runs on instance 101. The service's Log volume stores data in a directory on the system instance and the service's Data volume stores data in an NFS mount.



Creating and managing volumes

Volumes are separated into these groups, depending on how they are created and managed:

- **System-managed volumes** are created and managed by the system. When you deploy the system, you can specify the volume driver and options that the system should use when creating these volumes.

Once the system is deployed, you cannot change the configuration settings for these volumes.

- **User-managed volumes** can be added to services and job types after the system has been deployed. These are volumes that you manage; you need to create them on your system instances before you can configure a service or job to use them.



Note: As of release 1.3.0, none of the built-in services support adding user-managed volumes.

Volume drivers

When configuring a volume, you specify the volume driver that it should use. The volume driver determines how and where data is stored.

Because services run in Docker containers on instances in the system, volume drivers are provided by Docker and other third-party developers, not by the system itself. For information about volume drivers you can use, see the applicable Docker or third-party developer's documentation.

By default, all services do not use volume drivers but instead use the **bind-mount** setting. With this setting, data for each service is stored within the system installation directory on each instance where the service runs.

For more information on volume drivers, see the Docker documentation.

Viewing volumes

The System Management application shows this information about the Docker volumes used by jobs and services:

- **Name** — The unique identifier for the volume.
- **Type** — Either of these:
 - **System** — The volume is managed automatically for you by the system.
 - **User** — You need to manage the volume yourself.
- **Capacity** — Total storage space available in the volume.

- **Used** — Space used by the job or service.
- **Pool** — The volume category, as defined by the service or job that uses the volume.



Note: Some functions described here are not used with HCP for cloud scale. They are not visible in the System Management application, or have no effect when used.

For each volume, you can also view this information about the volume driver that controls how the volume stores data:

- **Volume driver** — The name of the volume driver.
- **Option/Value** — The command-line options used to create the volume, and their corresponding values. The available options and valid values for those options are determined by the volume driver.

Viewing job volumes

To view the volumes being used by a job:

Procedure

1. In the Admin App, click on the **Jobs** panel.
2. On the **Job Type** page, click on the job you want.
3. Click on the **Volumes** tab.

Viewing service volumes

To view the volumes being used by a service:

Procedure

1. In the Admin App, click on the **Services** panel.
2. Click on the service you want.
3. Click on the **Volumes** tab.

Instances

A system is made up of one or more instances of the software. This section includes information on adding and removing instances to the system.

About master and worker instances

Master instances are special instances that run an essential set of services, including:

- Admin-App service
- Cluster-Coordination service

- Synchronization service
- Service-Deployment service

Non-master instances are called **workers**. Workers can run any services except for those listed above.

Single-instance systems have one master instance while multi-instance systems have either one or three master instances.



Important: You cannot add master instances to a system after it's installed. You can, however, add any number of worker instances.

Single-instance systems versus multi-instance systems

A system can have a single instance or can have multiple instances (four or more).



Note: Every instance must meet the minimum RAM, CPU, and disk space requirements.

Single instance

A single-instance system is useful for testing and demonstration purposes. It requires only a single server or virtual machine and can perform all product functionality.

However, a single-instance system has these drawbacks:

- It has a single point of failure. If the instance hardware fails, you lose access to the system.
- With no additional instances, you cannot choose where to run services. All services run on the single instance.

Multiple instances

A multi-instance system is suitable for use in a production environment because it offers these advantages over a single-instance system:

- You can control how services are distributed across the multiple instances, providing improved service redundancy, scale out, and availability.
- A multi-instance system can survive instance outages. For example, with a four-instance system running the default distribution of services, the system can lose one instance and still remain available.
- Performance is improved as work can be performed in parallel across instances.
- You can add additional instances to the system at any time.



Note: You cannot change a single-instance system into a production-ready multi-instance system by adding new instances. This is because you cannot add master instances. Master instances are special instances that run a particular set of HCP for cloud scale services. Single-instance systems have one master instance. Multi-instance systems have at least three.

By adding additional instances to a single-instance system, your system still has only one master instance, meaning there is still a single point of failure for the essential services that only a master instance can run.

Three-instance system considerations

Three-instance systems should have only a single master instance. If you deploy a three-instance system where all three instances are masters, the system may not have enough resources to do much beyond running the master services.

Requirements for running system instances

This section lists the hardware and operating system requirements for running system instances.

Hardware requirements

To install HCP for cloud scale on on-premises hardware for production use, you must provision at least four instances (nodes) with sufficient CPU, RAM, disk space, and networking capabilities. This table shows the minimum and recommended hardware requirements for each instance in an HCP for cloud scale system.

Resource	Minimum	Recommended
RAM	32 GB	128 GB
CPU	8-core	24-core
Available disk space	500 GB 10k SAS RAID	2000 GB 15k SAS RAID
Network interface controller (NIC)	(1) 10 Gb Ethernet	(2) 10 Gb Ethernet
IP addresses	(1) static	(2) static
Firewall Port Access	Port 443 for S3 API Port 8000 for Admin App GUI Port 9084 for MAPI and Storage Management App GUI	Same
Internal IP Ports	See Networking (on page 86)	Same
Network Time	IP address of time service (NTP)	Same



Important: Each instance uses all available RAM and CPU resources on the server or virtual machine on which it's installed.

Operating system and Docker minimum requirements

Each server or virtual machine you provide must meet these requirements:

- 64-bit Linux distribution
- Docker version 1.13.1 or later installed
- IP and DNS addresses configured

Additionally, you should install all relevant patches on the operating system and perform appropriate security hardening tasks.



Important: Install the current Docker version suggested by your operating system, unless that version is earlier than 1.13.1. The system cannot run with Docker versions prior to 1.13.1.

Operating system and Docker qualified versions

This table shows the operating systems, Docker and SELinux configurations with which the HCP for cloud scale system has been qualified.

Operating system	Docker version	Docker storage configuration	SELinux setting
Fedora 27	Docker 18.03.0-ce	direct-lvm	Enforcing
Red Hat Enterprise Linux 7.4	Docker 18.03.0-ce	direct-lvm	Enforcing
Ubuntu 16.04-LTS	Docker 17.03.0-ce	aufs	N/A
CentOS 7.4	Docker 18.03.1-ce	overlay2	Enforcing

Docker considerations

- The Docker installation directory on each instance must have at least 20 GB available for storing the Docker images.
- Make sure that the Docker storage driver is configured correctly on each instance before installing the product.

After installing the product, changing the Docker storage driver requires a reinstallation of the product.

To view the current Docker storage driver on an instance, run:

```
docker info
```

- If you want to enable SELinux on the system instances, you need to use a Docker storage driver that supports it. The storage drivers that SELinux supports differ depending on the Linux distribution you're using. For more information, see the Docker documentation.
- If you are using the Docker `devicemapper` storage driver:
 - Make sure that there's at least 40 GB of Docker metadata storage space available on each instance. The product requires 20 GB to install successfully and an additional 20 GB to successfully update to a later version.

To view Docker metadata storage usage on an instance, run:

```
docker info
```

 - On a production system, do not run `devicemapper` in `loop-lvm` mode. This can cause slow performance or, on certain Linux distributions, the product may not have enough space to run.

SELinux considerations

- You should decide whether you want to run SELinux on system instances and enable or disable it before installing additional software on the instance.
- Enabling or disabling SELinux on an instance requires you to reboot the instance.
- To view whether SELinux is enabled on an instance, run: `sestatus`
- If you want to enable SELinux on the system instances, you need to use a Docker storage driver that supports it.
- The storage drivers that SELinux supports differ depending on the Linux distribution you're using. For more information, see the Docker documentation.

Supported browsers

The HCP for cloud scale web applications support these web browsers:

- Google Chrome latest
- Mozilla Firefox latest

Time source requirements

If you are installing a multi-instance system, each instance should run NTP (network time protocol) and use the same external time source. For information, see support.ntp.org.

Adding new instances

You may want to add additional instances to the system if:

- You want to improve system performance.
- You are running out of disk space on one or more instances.

! **Important:** You cannot add new master instances, only new worker instances.

However, these situations may also be improved by adding additional CPU, RAM, or disks to the instances you already have.

Before adding a new instance

- Obtain the product installation file. When adding an instance, you unpack and deploy this file on a bare-metal server or a pre-existing Linux virtual machine.

- Record the IP address(es) of at least one of the master instances in the system.

If your system uses internal and external networks, you need to record both the internal and external IP addresses for the master instances.

You can view instance IP addresses on the **Instances** page in the Admin App.

- Ensure that the new instances you are adding meet the minimum hardware, OS, and networking requirements. For information, see [Requirements for running system instances \(on page 97\)](#).

- Record the Docker volume drivers currently used by services and jobs across all existing instances. You need to install all of these volume drivers on the new instance that you're adding.

To find the volume drivers currently in use by your system, run this command on each system instance:

```
docker volume ls
```

Take note of each value for the **DRIVER** field.

Install Docker on each server or virtual machine

On each server or virtual machine that is to be an HCP for cloud scale instance:

Procedure

1. In a terminal window, check whether Docker 1.13.1 or later is installed:
`docker -version`
2. If Docker is not installed or if you have a version prior to 1.13.1, install the current Docker version suggested by your operating system.

The installation method you use depends on your operating system. See the [Docker website](#) for instructions.

Configure Docker on each server or virtual machine

Before installing the product, configure Docker with settings suitable for your environment. For guidance on configuring and running Docker, see the applicable Docker documentation.

Procedure

1. Ensure that the Docker installation directory on each instance has at least 20 GB available for storing the product Docker images.
2. Ensure that the Docker storage driver is configured correctly on each instance.
After installation, changing the Docker storage driver requires reinstallation of the product.
To view the current Docker storage driver on an instance, run: `docker info`.
3. If you want to enable SELinux on the system instances, use a Docker storage driver that supports it.
The storage drivers that SELinux supports differ depending on the Linux distribution you're using. For more information, see the Docker documentation.
4. If you are using the Docker `devicemapper` storage driver, ensure that there's at least 40 GB of Docker metadata storage space available on each instance.
The product requires 20 GB to install successfully and an additional 20 GB to successfully update to a later version.
To view Docker metadata storage usage on an instance, run: `docker info`

Next steps

On a production system, do not run `devicemapper` in `loop-lvm` mode. This can cause slow performance or, on certain Linux distributions, the product may not have enough space to run.

(Optional) Configure Docker volume drivers

If any services or jobs on your system are using Docker volume drivers (that is, not the `bind-mount` setting) for storing data, you need to install those volume drivers on the new instance that you are adding. If you don't, jobs and services may fail to run on the new instance.

Volume drivers are provided by Docker and other third-party developers, not by the system itself. For information on volume drivers, their capabilities, and their valid configuration settings, see the applicable Docker or third-party developer's documentation.

Configure maximum map count setting

You need to configure a value in the file `sysctl.conf`.

Procedure

1. On each server or virtual machine that is to be a system instance, open the file `/etc/sysctl.conf`.
2. Append this line: `vm.max_map_count = 262144`
If the line already exists, ensure that the value is greater than or equal to 262144.
3. Save and close the file.

(Optional) Enable or disable SELinux on each server or virtual machine

You should decide whether you want to run SELinux on system instances before installation.

Procedure

1. Enable or disable SELinux on each instance.
2. Restart the instance.

Configure the firewall rules on each server or virtual machine

Before you begin

Determine the port values currently used by your system. To do this, on any instance, view the file `install_path/config/network.config`.

On each server or virtual machine that is to be a system instance:

Procedure

1. Edit the firewall rules to allow communication over all network ports that you want your system to use. You do this using a firewall management tool such as `firewalld`.
2. Restart the server or virtual machine.

Install and configure NTP

Install NTP (Network Time Protocol) on the new server or virtual machine and configure it to use the same time source as the other system instances. For information, see <http://support.ntp.org>.

Run Docker on each server or virtual machine

On each server or virtual machine that is to be a system instance, you need to start Docker and keep it running. You can use whatever tools you typically use for keeping services running in your environment.

For example, to run Docker using `systemd`:

Procedure

1. Verify that Docker is running:
`systemctl status docker`
2. If Docker is not running, start the `docker` service:
`sudo systemctl start docker`
3. (Optional) Configure the Docker service to start automatically when you restart the server or virtual machine:
`sudo systemctl enable docker`

Unpack the installation package

On each server or virtual machine that is to be a system instance:

Procedure

1. Download the product installation package and MD5 checksum file and store them in a directory on the server or virtual machine.
2. Verify the integrity of the installation package:

```
md5sum -c product-version_number.tgz.md5
```

 If the package integrity is verified, the command displays OK.
3. In the largest disk partition on the server or virtual machine, create a product installation directory.

```
mkdir install_path/product
```
4. Move the installation package from the directory where you stored it to the product installation directory.

```
mv product-version_number.tgz install_path/product/product-version_number.tgz
```
5. Navigate to the installation directory.

```
cd install_path/product
```
6. Unpack the installation package:

```
tar -zxvf hcpcs-version_number.tgz
```

 A number of directories are created within the installation directory.



Note:

If you encounter problems unpacking the installation file (for example, the error message "tar: This does not look like a tar archive"), the file may have been packed more than once during download. Use the following commands to fully extract the file:

```
$ gunzip product-version_number.tgz
$ mv product-version_number.tar product-version_number.tgz
$ tar -zxvf product-version_number.tgz
```

7. Run the installation script `install`, located within a directory matching the version number of system software used by the product software.

```
sudo ./cluster/sys_ver_num/bin/install
```

 This version number is different from the product version number. It is the only subdirectory in the directory `cluster`.
 For example:

```
sudo ./cluster/1.4.0.260/bin/install
```



Note:

- Don't change directories after running the installation script. The following tasks are performed in your current directory.
- The installation script can be run only once on each instance. You cannot rerun this script to try to repair or upgrade a system instance.

Set up networking

On each server or virtual machine that is to be a system instance, edit the `<installation-directory>/config/network.config` file to be identical to the copies of the same file on the existing system instances.

Run the setup script on each server or virtual machine

Before you begin



Note:

- When installing a multi-instance system, make sure you specify the same list of master instance IP addresses on every instance that you are installing.
- When entering IP address lists, do not separate IP addresses with spaces. For example, the following is correct:

```
sudo install_path/hcpcs/bin/setup -i 192.0.2.4
-m 192.0.2.0,192.0.2.1,192.0.2.3
```

On each server or virtual machine that is to be a system instance:

Procedure

1. Run the script `setup` with the applicable options:

Option	
-i	The external network IP address for the instance on which you're running the script
-I	The internal network IP address for the instance on which you're running the script
-m	Comma-separated list of external network IP addresses of each master instance
-M	Comma-separated list of internal network IP addresses of each master instance

Use this table to determine which options you need to use:

Number of instances in the system	Network type usage	Options to use
Multiple	Single network type for all services	Either: -i and -m or -I and -M

Number of instances in the system	Network type usage	Options to use
Multiple	Internal for some services, external for others	All of these: -i, -I, -m, -M
Single	Single network type for all services	Either -i or -I
Single	Internal for some services, external for others	Both -i and -I

Result



Note: If the terminal displays Docker errors when you run the `setup` script, ensure that Docker is running.

For information, see Run Docker on each server or virtual machine.

Example

This example sets up a single-instance system that uses only one network type for all services:

```
sudo install_path/hcpcs/bin/setup -i 192.0.2.4
```

To set up a multi-instance system that uses both internal and external networks, enter the command in this format:

```
sudo install_path/hcpcs/bin/setup -i external_instance_ip
-I internal_instance_ip -m external_master_ips_list
-M internal_master_ips_list
```

For example:

```
sudo install_path/hcpcs/bin/setup -i 192.0.2.4 -I 10.236.1.0
-m 192.0.2.0,192.0.2.1,192.0.2.3 -M 10.236.1.1,10.236.1.2,10.236.1.3
```

This table shows sample commands to create a four-instance system. Each command is entered on a different server or virtual machine that is to be a system instance. The resulting system contains three master instances and one worker instance, and uses both internal and external networks.

Instance internal IP	Instance external IP	Master or worker	Command
192.0.2.1	10.236.1.1	Master	<pre>sudo install_path/hcpcs/bin/setup -I 192.0.2.1 -i 10.236.1.1 -M 192.0.2.1,192.0.2.2,192.0.2.3 -m 10.236.1.1,10.236.1.2,10.236.1.3</pre>

Instance internal IP	Instance external IP	Master or worker	Command
192.0.2.2	10.236.1.2	Master	<code>sudo install_path/hcpcs/bin/setup -I 192.0.2.2 -i 10.236.1.2 -M 192.0.2.1,192.0.2.2,192.0.2.3 -m 10.236.1.1,10.236.1.2,10.236.1.3</code>
192.0.2.3	10.236.1.3	Master	<code>sudo install_path/hcpcs/bin/setup -I 192.0.2.3 -i 10.236.1.3 -M 192.0.2.1,192.0.2.2,192.0.2.3 -m 10.236.1.1,10.236.1.2,10.236.1.3</code>
192.0.2.4	10.236.1.4	Worker	<code>sudo install_path/hcpcs/bin/setup -I 192.0.2.4 -i 10.236.1.4 -M 192.0.2.1,192.0.2.2,192.0.2.3 -m 10.236.1.1,10.236.1.2,10.236.1.3</code>

Start the application on each server or virtual machine

On each server or virtual machine that is to be a system instance:

Procedure

1. Start the application script `run` using whatever methods you usually use to run scripts.



Important: Ensure that the method you use can keep the `run` script running and can automatically restart it in case of a server reboot or other availability event.

Result

Once the service starts, the server or virtual machine automatically joins the system as a new instance.

Example

Here are some examples of how you can start the script:

- You can run the script in the foreground:

```
sudo install_path/product/bin/run
```

When you run the `run` script this way, the script does not automatically complete, but instead remains running in the foreground.

- You can run the script as a service using `systemd`:

- Copy the product `.service` file to the appropriate location for your OS. For example:

```
cp install_path/product/bin/product.service /etc/systemd/system
```

- Enable and start the `product.service` service:

```
sudo systemctl enable product.service
sudo systemctl start product.service
```

Configure services and jobs on the new instances

The system does not automatically begin running services on the instances you've added. You need to manually configure services to run on those new instances.

Also, depending on how your jobs are configured, jobs may not run on the new instances that you've added. You need to manually configure jobs to run on them.

Viewing instances

You can use the Admin App, CLI, and REST API to view a list of all instances in the system.

Viewing all instances


To view all instances, in the Admin App, click on Dashboard > Instances.

The page shows all instances in the system. Each instance is identified by its IP address.



This table describes the information shown for each instance.

Property	Description
State	<ul style="list-style-type: none"> Up: The instance is reachable by other instances in the system. Down: The instance cannot be reached by other instances in the system.

Property	Description
Services	The number of services running on the instance.
Service Units	<p>The total number of service units for all services and job types running on the instance, out of the recommended service unit limit for the instance.</p> <p>An instance with a higher number of service units is likely to be more heavily utilized by the system than an instance with a lower number of service units.</p> <p>The Instances page displays a blue bar for instances running less than the recommended service unit limit.</p> <p>The Instances page displays a red bar for instances running more than the recommended service unit limit.</p>  <p style="text-align: right; font-size: small;">138 of 100 recommended Service Units</p>
Load Average	The load averages for the instance for the past one, five, and ten minutes.
CPU	The sum of the percentage utilization for each CPU core in the instance.
Memory Allocated	<p>This section shows both:</p> <ul style="list-style-type: none"> ▪ The amount of RAM on the instance that's allocated to all services running on that instance. ▪ The percentage of this allocated RAM to the total RAM for the instance.
Memory Total	The total amount of RAM for the instance.
Disk Used	The current amount of disk space that your system is using in the partition on which it is installed.
Disk Free	The amount of free disk space in the partition in which your system is installed.

Viewing the services running on an instance

To view the services running on an individual instance, in the Admin App:

Procedure

1. Click on **Dashboard > Instances**.
2. Click on the instance you want.

The page lists all services running on the instance.

For each service, the page shows:

- The service name
- The service state:
 - **Healthy:** The service is running normally.
 - **Unconfigured:** The service has yet to be configured and deployed.
 - **Deploying:** The system is currently starting or restarting the service. This can happen when:
 - You move the service to run on a completely different set of instances.
 - You repair a service.

For information on viewing the status service operations, see [Monitoring service operations \(on page 49\)](#).
 - **Balancing:** The service is running normally, but performing some background maintenance operations.
 - **Under-protected:** In a multi-instance system, one or more of the instances on which a service is configured to run are offline.
 - **Failed:** The service is not running or the system cannot communicate with the service.
- **CPU Usage:** The current percentage CPU usage for the service across all instances on which it's running.
- **Memory:** The current RAM usage for the service across all instances on which it's running.
- **Disk Used:** The current total amount of disk space that the service is using across all instances on which it's running.

Related CLI command(s)

getInstance

listInstances

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

GET /instances

GET /instances/{uuid}

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Removing instances

You would typically remove an instance from your system in these situations:

- You are retiring the hardware on which the instance runs
- The instance is in the Down state and cannot be recovered
- You want to run a system with fewer instances

(Optional) Shut down the instance you want to remove

If the instance has already shut down as a result of a failure, the instance is in the Down state. Your system automatically attempts to move all services from that instance to other instances in the system. After all services have been moved, the instance is eligible for removal. Continue to the next step ([Remove the shut down instance from the system \(on page 111\)](#)).

If the instance that you want to remove is in the Up state, you need to shut it down yourself before you can remove it from the system.

Procedure

1. Move all the services that the instance is currently running to the other instances in the system.



Important: Shutting down an instance without first moving its services can cause data loss.

2. If the system has jobs configured to run on only the failed instance, configure those jobs to run on other instances.
3. Stop the `run` script from running. You do this using whatever method you're currently using to run the script.
4. Run this command to stop all system Docker containers on the instance:


```
sudo <installation-directory>/bin/stop
```
5. Delete the system Docker containers:
 - a. List all Docker containers:


```
sudo docker ps
```
 - b. Note the container IDs for all containers that use a `com.hds.ensemble` or `com.hitachi.aspen` image.
 - c. Delete each of those containers:


```
sudo docker rm <container-id>
```
6. Delete the system Docker images:
 - a. List all Docker images:


```
sudo docker images
```
 - b. Note the image IDs for all images that use a `com.hds.ensemble` or `com.hitachi.aspen` repository.
 - c. Delete each of those images:


```
sudo docker rmi <image-id>
```

7. Delete the system installation directory:

```
rm -rf /<installation-directory>
```

Remove the shut down instance from the system

Admin App instructions

Procedure

1. Click on the **Instances** panel.
2. Click on the instance you want to remove.
3. Click on **Remove Instance**.

Related CLI command(s)

deleteInstance

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

DELETE /instances/{uuid}

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Replacing a failed instance

If an instance suffers an unrecoverable failure, you need to replace that instance with a new one.

Procedure

1. In the Admin App, view the **Instances** page to determine whether the failed instance was a master instance.
2. Select a new server or virtual machine to add as a new instance to the system. For information on instance requirements, see Requirements for running system instances.
3. Remove the failed instance from the system. For information, see Removing instances.



WARNING: If the failed instance was a master, after removing it, you have only two master instances remaining. If any other instance fails while you are in this state, the system becomes completely unavailable until you add a third master back to the system by completing this procedure.

4. Add the replacement instance to the system. For information, see Adding new instances.



Important: If the instance you are replacing was a master instance, when you run setup on the replacement instance, the list of masters that you specify for the **-m** option needs to include:

- The IP addresses of the two remaining healthy master instances.
- The IP address of the new instance that you're adding.

For example, in a system with master instance IPs ranging from 192.0.2.1 to 192.0.2.3 and you are replacing instance 192.0.2.3 with 192.0.2.5, run setup with these options:

```
sudo bin/setup -i 192.0.2.5 -m
192.0.2.1,192.0.2.2,192.0.2.5
```

This does not apply when you're replacing a worker instance. In that case, specify the IP addresses of the 3 existing masters.

Plugins

Plugins are modular pieces of code that allow your system to perform specific activities.

Plugins are organized in groups called **plugin bundles**. When adding or removing plugins from your system, you work with plugin bundles, not individual plugins.

Viewing installed plugins

Use the Admin App, REST API, and CLI to view all plugin bundles and individual plugins that have been installed. You can view all individual plugins at the same time or filter the list based on plugin type.

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Plugins**.
The **Plugin Bundles** tab shows all installed plugin bundles.
3. To view all individual plugins, click on the **All Plugins** tab.

Related CLI command(s)

listPlugins

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API methods GET plugins

GET /plugins

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Upgrading plugin bundles

To upgrade plugins, you upload a new version of the bundle that contains those plugins.

You can select which version of the plugin bundle is the active one (that is, the one that connectors or stages will use). If you select the new version, all connectors and stages immediately begin using the new versions of the plugins in the bundle.

You can change the active plugin bundle version at any time.

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Plugins**.
3. Click on the **Upload Bundle** button.
4. In the **Upload Plugins** window, drag and drop the new version of the plugin bundle.
5. In the list of plugin bundles, click on the row for the plugin bundle version that you want.
If the bundle you uploaded isn't listed, click on the **Reload Plugins** button.
6. Click on the **Set Active** button.

Related CLI command(s)

uploadPlugin

setPluginBundleActive

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

POST /plugins/upload

POST /plugins/bundles/{name}/{bundleVersion}/active

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Setting the active plugin bundle version

If you've uploaded multiple versions of a plugin bundle, only one version can be active at a time. The active plugin bundle version is the one that the system uses.

When you change the active version of a plugin bundle, any workflow tasks that contain connectors and stages that use the bundle immediately begin using the new active version.

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Plugins**.

3. Click on the row for the plugin bundle version that you want.
4. Click on the **Set Active** button.

Related CLI command(s)

setPluginBundleActive

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

POST /plugins/bundles/{name}/{bundleVersion}/active

You can get help on specific REST API methods for the Admin App at REST API - Admin.


Deleting plugin bundles

To delete plugins from your system, you delete plugin bundles from the system. You cannot delete individual plugins.

You cannot delete a plugin bundle, or any of its versions, if any of that bundle's plugins are currently in use by the system.

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Plugins**.
3. Click on the delete icon () for the plugin bundle you want to remove.

Related CLI command(s)

deletePluginBundle

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

DELETE /plugins/bundles/{name}/{bundleVersion}

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Packages

You can back up all of your system configuration by exporting packages. You can back up these package files and use them to restore your configurations in case of a system failure.

Exporting packages

You can export the configurations for system components as package files. You can back up these package files and use them to restore your configurations in case of a system failure.

After exporting a package, you can store it in one of your data sources. When you want to import the package, your system can retrieve it directly from the data source.

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Packages**.
3. Click on **Export**.
4. Under **Customize Package Description**, give your package a name and an optional description.
5. Under **Configuration**, select any configuration items to export.
6. Under **Plugins**, select any plugin bundles to export.
7. Under **Components**, select any available components to export.

If you select one component but not the components it depends on, the Admin App prompts you to add those missing components to the package.

8. Under **Validate**, make sure your package is valid and click on the **Download Package** button.
9. Once your package downloads, click on the **Download Package** button to download it again, or click on the **Finish** button to exit.

Related CLI command(s)

buildPackage

downloadPackage

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

POST /package/build

POST /package/download

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Importing packages

To import a package, you can upload it from your computer or have your system retrieve it from one of your data sources. After you import the package, your system runs a system task to synchronize the package components across all instances in your system.

The system can have only one imported package at a time.



Note:

- Importing a component that already exists on your system may cause conflicts and should be avoided.
- You need to manually resolve conflicts with Components, while conflicts with Configuration are handled automatically by the system.

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Packages**.
3. Click on **Import**.
4. Do one of these:
 - If the package you want to import is stored on your computer, click and drag the package file into the **Upload Package** panel.
 - If the package you want to import is stored in one of your data sources, click on the **Click to Upload** panel. Then, browse for the package file.
5. Under **Package Description**, review the description and click on the **Continue** button.
6. Under **Configuration**, select any configuration items to import.
7. Under **Plugins**, select any plugin bundles to import.
8. Under **Components**, select any available components to import.
9. Under **Validate**, make sure your package is valid and click on the **Install Package** button.

Your system starts a system task to install the package components on all instances in the system.

You can monitor the task from the current page or from the **Processes** page.

10. Once the task has completed and all package components have been installed, clicking on the **Complete Install** button will delete the package from the system.

Related CLI command(s)

uploadPackage

loadPackage — (Loads a package from a data connection)

installPackage

getPackageStatus

deletePackage

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

POST /package — (Uploads a package)

POST /package/load — (Loads a package from a data connection)

POST /package/install

GET /package — (Gets the status of the imported package)

DELETE /package

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Setting a login welcome message

You can use the Admin App, REST API, and CLI to set a welcome message for the Admin App. The message appears on the app's login page.

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Security**.
3. On the **Settings** tab, type a message in the **Single Sign-on Welcome Message** field.
4. Click on the **Update** button.

Related CLI command(s)

editSecuritySettings

For information on running CLI commands, see [CLI reference \(on page 123\)](#).


Related REST API method(s)

PUT /security/settings

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Updating the system

You can update system software by uploading new update packages.

 **Important:** Hitachi Vantara does not provide updates or security fixes for the host operating systems running on system instances.

Before updating

In order for a system to be updated:

- All instances and services must be healthy.
- Each service must be running on its recommended number of instances.
- Each instance must have enough disk space for the update.
- All required network ports must be available on each instance.
- There can be no in-progress package uploads or installations.

During an update

- All running jobs are paused.
- System availability considerations:
 - Instances shut down and restart one at a time during the upgrade. Other instances remain online and able to service requests.
 - The Admin App remains available but is in a read-only state. You can monitor the progress of the update, but you cannot make any other changes to the system.



Note: Systems with two instances are more susceptible to availability outages during an update than systems with three or more instances.

Checking update status

As an update runs, you can view its progress on the **Configuration > Update** page. Also on this page, you can view all system events related to system updates.

Results of an update

After an update, the system runs a new version of the software. Additionally:

- If any of the built-in plugins were updated, your system automatically uses the latest versions of those plugins.
- If an existing service is replaced with a new service, the system automatically runs that new, replacement service.
- If any new services were added, you may need to manually configure those services to run on the system instances.

Update errors

If errors occur during an update, the **Update** page displays information about each error and also displays a **Retry** button for starting the update over again. Some errors may not be resolved by restarting the update.

If you encounter errors during an update, contact your authorized service provider.

New services and components added during an update

A system update may add new services or plugins. You need to manually configure your system to start using these new components; your system does not start using them automatically.

To update system:

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Update**.
3. Click on the **Install** tab.
4. Click and drag the file into the **Upload** panel.
The update file is uploaded and the system checks to make sure the file is valid. This may take several minutes.
5. On the **Update** page, click on the **View** button in the **Update Status** panel.
The **Verify & Apply Update** page displays information about the contents of the update.
6. To start the update, click on the **Apply Update** button.

Result

The system begins checking to make sure the system is ready to be updated. If it isn't, the update stops. In this case, you need to correct the problems before the update can continue.

Related CLI command(s)

getUpdateStatus

installUpdate

deleteUpdate

loadUpdate

uploadUpdate

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

GET /update

POST /update/install

DELETE /update/package

POST /update/package

POST /update/package/load — (Retrieves update package from a data connection)

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Viewing update history

You can view a list of all updates that have previously been applied to your system. For each update, you can view the corresponding version number and the date on which it was installed.

Admin App instructions

Procedure

1. Click on the **Configuration** panel.
2. Click on **Update**.

Result

The **History** tab lists previously installed versions and when each was installed.

Related CLI command(s)

`getUpdateHistory`

For information on running CLI commands, see [CLI reference \(on page 123\)](#).

Related REST API method(s)

GET /update/history

You can get help on specific REST API methods for the Admin App at REST API - Admin.

Uninstalling the system

To completely uninstall your system, do the following on all instances:

Procedure

1. Stop the `run` script from running. You do this using whatever method you're currently using to run the script.
2. Run this command to stop all system Docker containers on the instance:


```
sudo <installation-directory>/bin/stop
```
3. Delete the system Docker containers:
 - a. List all Docker containers:


```
sudo docker ps
```
 - b. Note the container IDs for all containers that use a `com.hds.ensemble` or `com.hitachi.aspen` image.
 - c. Delete each of those containers:


```
sudo docker rm <container-id>
```
4. Delete the system Docker images:

- a. List all Docker images:
`sudo docker images`
 - b. Note the image IDs for all images that use a `com.hds.ensemble` or `com.hitachi.aspen` repository.
 - c. Delete each of those images:
`sudo docker rmi <image-id>`
- 5. Delete the system installation directory:**
`rm -rf /<installation-directory>`

Chapter 6: Best practices

This section contains topics that describe some best practices for administering your system.

Best practices for distributing services

Each service has an associated service unit cost. These costs indicate how computationally expensive one service is to run compared to another. You can use these costs as a guide for how to distribute services across the instances in your system.

Recommendations

- Avoid running multiple services with high service unit costs together on the same instance.
- On master instances, avoid running any services besides those classified as System services.
- To utilize your instances evenly, try to deploy a comparable number of service units on each instance.

Best practices for maintaining system availability

Run master instances on separate physical hardware

For a multi-instance system, master instances should run on separate physical hardware. If your instances run on virtual machines, run the master instances on separate physical hosts.

Run services on more than one instance

In a multi-instance system, you can choose which and how many instances that each service can run on. For redundancy, you should run each service on more than one instance.

Chapter 7: Reference

This section contains information about troubleshooting, information on using the command-line interface, and information on using the REST API.

Troubleshooting

System event issues

For information on viewing system events, see [System events \(on page 50\)](#).

Issue	Description/Resolution
The event log contains instances of event id 6007 with this message: <pre>Service <service-name> health check against HTTP / health <port> cannot succeed because it is on a different network than service Cluster-Worker. Health check ignored to prevent service interruption.</pre>	Your system uses both internal and external networks, but the service specified by the event is on a different network type from the Cluster-Worker service. Because of this, the system cannot perform an additional health check on the specified service. You can ignore this event. The additional health check is not required and does not affect the other health checks used to display the service status on the Monitoring > Services page in the Admin App.

CLI reference

The system includes an administrative CLI for system management. This interface allows you to perform all tasks relating to system setup and configuration. Any administrative activity that you can perform in the Admin App or REST API can be performed through the CLI.

Your system may also include additional, product-specific CLI tools.

Accessing the CLI tools on a system instance

You can access the CLI tools from any instance. To do this:

Procedure

1. Log in or SSH into a system instance.
2. Navigate to the CLI tool directory:
`cd <installation-directory>/cli/`
3. Navigate to the directory for the CLI tool you want. For example:
`cd admin`

Accessing the CLI tools from your computer

You can install your system's CLI tools on your Linux computer. To do this, you must have version 1.8 of the Java Runtime Environment (JRE) installed.

Your system's CLI tools are distributed in .tgz files along with the software installation package.

To install a CLI tool:

Procedure

1. Store the .tgz file in a directory on your computer.
2. Unpack the file:
`tar zxvf filename`

Syntax

The CLI tools have this syntax:

```
<tool-name> [options] [command] [command-specific-options]
```

Options

```
-c, --command <command|category>
```

Specifies the command you want to run. When used with the `--help` option, displays information about the specified command.

You can also use this option to specify a category of commands when using the `--help` option. Doing this displays information about all commands within the specified category.

```
-d, --model-definition <name>
```

Returns information about the specified request model. See [Viewing request models \(on page 126\)](#).

```
--debug
```

Includes verbose debug output for troubleshooting purposes.

```
-h, --help <all>
```

Displays help information. If you specify the `all` argument, displays information on all commands. If you specify the `--help` option, displays information about commands in the specified category.

`-k, --check-ssl-cert <true|false>`

Whether to enable SSL security checking. When false, insecure connections are allowed.

`-m, --model-schema <ModelName>`

Returns the JSON-formatted schema for the specified request model. See [Viewing request models \(on page 126\)](#).

`-p, --password <password>`

Password for the specified user account.

`--port`

The port for the system application that supports the CLI tool.

`-r, --realm <realm>`

Security realm where your user account is defined. For information, see [Adding identity providers \(on page 63\)](#).

`-s, --server <server>`

The hostname or IP address of a system instance.

`-u, --username <username>`

Username for an account that has permission to access system.

`-V, --version`

Displays the CLI version.

Viewing available commands

- To view all available commands, run:
`<cli-tool-name> --help all`
- To view all command categories, run:
`<cli-tool-name> --help`
- To view all commands within a category, run:
`<cli-tool-name> --help -c <category>`

For example:

```
admincli --help -c instances
```

- To view all information about a single command, run:

```
<cli-tool-name> --help -c <command>
```

For example:

```
admincli --help -c listInstances
```

Viewing request models

Some commands require that you include a JSON-formatted request body along with the command. The command's request model determines how you need to format the request body.

The help command for an individual command indicates what request model it requires.

For example, this help command output indicates that a command to update a service requires a ServiceUpdateModel request:

```
# ./admincli -c updateServiceConfig -h
usage: updateServiceConfig
Name:
  updateServiceConfig
Description:
  Configure service instances
Added:
  1.0
Usage:
  admincli -c updateServiceConfig <options>
Options:
  --service-update-model <ServiceUpdateModel>
File containing JSON text representing a ServiceUpdateModel for the
command
updateServiceConfig. Use the -m and -d options to retrieve information on
request and
response models.
```

Viewing request model information

To view detailed information about the contents of a request model, run:

```
<cli-tool-name> -d <ModelName>
```

For example:

```
admincli -d ServiceUpdateModel
```

Viewing request model formatting

To view the JSON format for the request model, run:

```
<cli-tool-name> -m <ModelName>
```

Editing configuration preferences

You can use the CLI tool's `.conf` file to specify settings to use every time you run a CLI command.

The CLI configuration file has this format:

```
{
  "defaultSettings": {
    "checkSSLCert": "[false|true]", (optional)
```

```

"server": "<hostname>", (optional)
"realm": "[local|<security-realm-name>]", (optional)
"username": "<your-username>", (optional)
"password": "<your-password>" (optional)
}
}

```

For example, with the following configuration, all commands:

- Are run against the `system.example.com` system
- Check the SSL certificate for the system before connecting
- Uses the `exampleUsersEast` security realm to authenticate the specified username and password

```

{
  "defaultSettings": {
    "checkSSLCert": "true",
    "server": "system.example.com",
    "realm": "exampleUsersEast"
  }
}

```

File location

You can configure CLI preference by editing the existing `.conf` files in the CLI installation directory.

The options you specify explicitly in a CLI command override the options specified in the `.conf` file.

System error responses

If a CLI request reaches the system and the system returns an error, the CLI response contains:

- An HTTP status code
- Conditionally, a product-specific error code
- A JSON-formatted error response body

HTTP status codes

This table describes the typical reasons why these HTTP status codes are returned.

Status code	Description
400 (Bad Request)	The request body contains one or more of these: <ul style="list-style-type: none"> An invalid entry An invalid value for an entry Invalidly formatted JSON If the request includes a UUID, the UUID may be invalidly formatted.
401 (Unauthorized)	The provided credentials are invalid.
403 (Forbidden)	You do not have permission to perform the request.
404 (File not found)	The resource you are trying to retrieve or edit cannot be found.
409 (Conflict)	The resource you are trying to create already exists.
500 (Server Error)	The system experienced an error.
599 (Network Connection Timeout Error)	The CLI request timed out while attempting to connect to the system or one of its instances.

Product-specific error codes

Some CLI requests return product-specific error codes in addition to an HTTP status code. These error codes are listed in the `errorCodes` field in the JSON response body. This table describes these error codes.

Error code	Description
4000	SSL certificate not trusted.

JSON response body

Error response bodies have this format:

```
{
  "statusCode": <HTTP-status-code>,
  "errorCode": <product-specific-error-code>,
  "errorMessage": <message>,
  "errorProperties": [
    {
      "name": <error-property>,
      "message": <error-property-message>
    }
  ]
}
```


REST API Reference

Your system provides a RESTful API that you can use for writing applications that manage the system. Anything you can do in the System Management application can also be performed using the REST API.

Information is available about the APIs in two places:

- For information about System Management application APIs, see the topics in this document.
- For information about Object Storage Management and S3 APIs, see the Help for the Object Storage Management application.

Input and output formats

The REST API accepts and returns JSON.

Access and authentication

To use the REST API, you need a user account that has permission to perform the actions you want.

Requesting an access token

Once you have a user account, you need to request an authentication token from the system. To do this, you send an HTTP POST request to the `/auth/oauth` endpoint.

When you generate a new access token, a refresh token also gets generated automatically.

Here's an example using the cURL command-line tool:

```
curl -ik -X POST https://mysystem.example.com:8000/auth/oauth/ \
-d grant_type=password \
-d username=user1 \
-d password=password1 \
-d scope=* \
-d client_secret=my-client \
-d client_id=my-client \
-d realm=marketingUsers
```

In response to this request, you receive a JSON response body containing an `access_token` field. The value for this field is your token. For example:

```
{"access_token" : "eyJr287bjle..."}
```

**Note:**

- To get a list of security realms for the system, send an HTTP GET request to the /setup endpoint. For example, to do this with cURL:

```
curl -k -X GET --header 'Accept: application/json'
'https://mysystem.example.com:<admin-app-port>/api/admin/setup'
```

For information on configuring security realms, see [Adding identity providers \(on page 63\)](#).

- To get an access token for the local admin user account, you can omit the realm option for the request, or specify a realm value of **Local**.

Submitting your access token

You need to specify your access token as part of all REST API requests that you make. You do this by submitting an Authorization header along with your request. Here's an example that uses cURL:

```
curl -X GET --header "Accept:application/json" https://
mysystem.example.com:<admin-app-port>
/api/admin/instances --header "Authorization: Bearer eyJr287bjle..."
```

Changing a password

You can use the REST API to change your system's password using the following cURL command.

```
$1=<server-name>
```

```
$2=<current-password>
```

```
$3=<new-password>
```


```
TOKEN=$(curl -ik -X POST https://$1.mysystem.com:8000/auth/oauth/ -d
grant_type=password
-d username=admin -d password=$2 -d scope=* -d client_secret=hci-client -
d client_id=hci-client
-d realm=local 2>&1 | grep access_token | awk -F: '{print $2}' | awk -F
\" '{print $2}')
```

```
curl -v -X POST --header 'Content-Type: application/json' --header
"Authorization: Bearer $TOKEN"
https://$1.mysystem.com:8000/api/admin/setup/password -d '{"password":
"""$3"""}'
```

Viewing and using REST API methods

Your system provides web-based documentation pages where you can view all supported REST API methods, including the request bodies, request URLs, response bodies, and return codes for each. You can also use these pages to run each REST API method.

Viewing the API documentation

To view the REST API documentation, in the System Management application, click on the user icon (). Then click on REST API - Admin.

To view the HCP for cloud scale API documentation, click REST API in the Object Storage Management application.

Making requests

You can use the REST API documentation pages to experiment with the REST API.



Note: Any requests you submit on the REST API page take effect on the system.

To use the REST API page to run a method:

Procedure

1. Click on the row for the method you want.
2. If the method you want requires that you specify a UUID:
 - a. Click on the row for the GET method for the resource type that you want.
 - b. Click on the **Try it Out!** button.
 - c. In the JSON response body, copy the value for the **uuid** field for the resource that you want.



Note: If you specify UUIDs when creating resources, the UUIDs are ignored.

3. If the method you want requires that you specify a request body:
 - a. In the **Parameters** section, under **Model Schema**, click inside the JSON text box.
The JSON text is added to the **Value** field.
 - b. Edit the JSON in the **Value** field.



Note: Some methods may require other information in addition to or instead of UUIDs or JSON-formatted text. Some require particular string values or require that you browse for and select a file to upload.

4. Click on the **Try it out!** button.

Error responses

When an API request fails, the API returns:

- An HTTP status code
- Conditionally, a system-specific error code
- A JSON-formatted error response body

HTTP status codes

This table describes the typical reasons why these HTTP status codes are returned. For information on the status codes for a particular method, view the system REST API web interface.

Status code	Description
400 (Bad Request)	The request body contains one or more of these: <ul style="list-style-type: none"> ▪ An invalid entry ▪ An invalid value for an entry ▪ Invalidly formatted JSON If the request includes a UUID, the UUID may be invalidly formatted.
403 (Forbidden)	You do not have permission to perform the request.
404 (File not found)	The resource you are trying to retrieve or edit cannot be found.
409 (Conflict)	The resource you are trying to create already exists.
500 (Server Error)	The system experienced an error.

System-specific error codes

Some API requests return system-specific error codes in addition to an HTTP status code. These error codes are listed in the `errorCodes` field in the JSON response body. This table describes these error codes.

Error code	Description
4000	SSL certificate not trusted.

JSON response body

REST API error responses have this format:

```
{
  "statusCode": <HTTP-status-code>,

```

```
"errorCode": <system-specific-error-code>,  
"errorMessage": <message>,  
"errorProperties": [  
  {  
    "name": <error-property>,  
    "message": <error-property-message>  
  }  
]  
}
```

Hitachi Vantara



Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA
HitachiVantara.com | community.HitachiVantara.com

Contact Information
USA: 1-800-446-0744
Global: 1-858-547-4526
HitachiVantara.com/contact