MDS GLOBAL

CMP 8.18

System Administration Guide

Version 1.0

Classification: **Customer Confidential**

Copyright

Confidentiality

Disclaimer

Trademarks

Contact Details

Please visit www.mdsglobal.com for further information on MDS Global products, solutions and services.

Table of Contents

Version Control

Version	Issue Date	Author	Comments
Version 1.0	27 March 2025	MDS	CMP 8.18 Release - Changed the C in CMP to Converged.

Terms Used in this Document

For definitions and explanations of the terms, abbreviations and acronyms used in this document, please see the *CMP Glossary* document.

1.0 Introduction

The System Administration Guide provides a starting point for managing your MDS Global Converged Monetisation Platform (CMP) components and running them optimally.

1. 1 Audience and Assumptions

The information in this guide is aimed at users who are assumed to have at least Basic Red Hat Administration knowledge and an appreciation of networking fundamentals, such as:

- System Administrators
- Consultants
- IT Staff
- Support Specialists.

1. 2 Required Reading and Related Documentation

It is assumed the audience has read and understood the following documentation:

- CMP Overview
- CMP Technical Architecture Overview
- CMP Installation Guide

Other CMP documentation that can assist system administration includes:

- CMP Operational Overview
- CMP Security Guide
- CMP Purge Guide

1. 2. 1 Third Party Documentation Resources

See also:

- Red Hat Linux Documentation
- PostgreSQL Documentation
- Pentaho Documentation
- Spring Framework Guides
- Webswing Documentation
- WSO2 Identity Server Documentation

1. 3 System Administration Tasks

Typical system administration tasks can include the following:

Hardware

For example:

- Install, configure and maintain the hardware required to support CMP.
- Verify that peripherals are working properly.
- Troubleshoot hardware issues. Repair or arrange for repairs.
- Tune hardware to optimise performance.

Every CMP deployment is unique to the customer, and therefore hardware requirements and issues will be specific to that deployment. Contact your MDS Global representative for information.

Software

For example:

- Install, deploy and configure CMP software.
- Maintain software and apply CMP upgrades and patches.
- Troubleshoot software issues.

Data and Database

For example:

- Maintain and administer the CMP database.
- Ensure sensitive data is encrypted.
- Ensure data handling and management meets applicable regulations and standards, for example GDPR[1] obligations.
- Purge old or unwanted data.

Users

For example:

- Administering users and user groups:
  - Managing user accounts, authentication, access, credentials, roles and permissions.
  - Adding, deleting, creating or modifying user information.

Security

For example:

- Implementing and maintaining physical security, for example access control, locked server rooms, staff IDs and anti-theft measures.
- Implementing and maintaining network and software security, for example authentication, firewalls, intrusion detection and antivirus measures.
- Perform server hardening.
- Creating, maintaining and disseminating security policies for equipment and security.

Risk Mitigation

[1]The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy for all individual citizens of the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA.

For example:

- Develop plans for disaster recovery.
- Implement high availability.
- Schedule and perform backups.

Monitoring

For example:

- Monitor
  - CMP system
  - Network communication
  - Users.
- Produce and view reports - daily, weekly and monthly.

Optimisation

For example:

- Optimise processes and lead process improvement.
- Tune CMP system for performance.
- Automate regular tasks, for example backups and purging.

Documentation

Documentation is how system administrators keep records of assets, including hardware and software types, counts, and licences. Document the configuration of the system, security and usage polices, recovery plans, hardware and software inventory. Should there be any issues in the production environment, documentation helps identify the hardware, virtual machine, appliance, software, and so on, that may be involved.

As every CMP implementation is unique, documenting your particular deployment accurately is essential.

2.0 System Overview

The MDS Global Cloud Monetisation Platform (CMP) supports billing and end-to-end customer management for digital service providers.

CMP is built using Java technology and industry standard Open Source components so as not to be intrinsically tied to either specific hardware or a specific operating system.

However, in order to provide the highest quality delivery and support, the system is currently tested and certified only for Red Hat Enterprise Linux 8 running on x86_64. This provides the option to deploy in all the different ways supported by this operating system:

- Directly on physical hardware
- Using server virtualisation with VMWare, Red Hat Virtualisation or Hyper-V
- To virtual machines executing in Google Cloud, Amazon Web Services or Azure.

This section includes:

2. 1 System Components

CMP is delivered as a set of components that are Red Hat Package Manager (RPM) packages.

2. 1. 1 CMP Components

CMP comprises the following independently installable components. An operational CMP system contains at least one instance of each component in the list.

- Database

  Provides the underpinning repository for persisting CMP data supporting a central view of all CMP data.

- Identity Server

  Provides centralised user authentication and authorisation to the user across CMP including Single Sign On.

  This component comprises the following CMP modules:

Module
wso2is-login

- Role Extender

  Translates business roles known to the Identity Server into more granular roles that are actually used for authorisation within CMP.

This component comprises the following CMP modules:

Module
role-extender

- AgentView

  The customer management interface destined for use by agents in a call centre to enrol customers and to maintain their details.

  This component comprises the following CMP modules:

Module
agent-view

- CMP Web Services

  Provide a standard mechanism for online customer data interchange between CMP and other MDS Global and third party systems and applications. CMP has two complimentary sets of web services for customer data: SOAP and RESTful web services.

  This component comprises the following CMP modules:

Module
rest-ws
soap-ws

- Business Configuration

  Allows service providers to manage CMP business configuration either via an interactive GUI and a set of RESTful Web Services.

  This component comprises the following CMP modules:

Module
configuration-centre

- AgentView Interfaces Layer

  Provides the business logic for AgentView.

  This component comprises the following CMP modules:

Module
agent-view-interfaces-layer
agent-view-servlet

- Published Interfaces Layer

  Provides the business logic for CMP SOAP Web Services and Business Configuration.

  This component comprises the following CMP modules:

Module
published-interfaces-layer

- SABRE Server

Executes all asynchronous processing within CMP. This includes both scheduled batch processing and immediate processing required in response to an event. The SABRE server has two parts: a technical framework and a set of independent jobs containing processing functionality that are loaded dynamically.

This component comprises the following CMP modules:

Module
sabre-action-monitor
sabre-batch-error-management
sabre-bill-print
sabre-comms
sabre-credit-reference
sabre-credit-control
sabre-dal
sabre-data-warehouse
sabre-debt-recovery-agency
sabre-device-enrolment
sabre-device-enrolment-adapter
sabre-edit-subscription
sabre-external-configuration
sabre-external-reference-upload
sabre-gdpr-purge
sabre-generic-activity-adapter-daemon
sabre-generic-postingout-daemon
sabre-interface-purge
sabre-invoice-posting
sabre-invoice-production
sabre-ledger-monitor
sabre-managed-number-monitor
sabre-managed-numbers
sabre-mandate-registrations
sabre-mandate-revisions
sabre-mdsledger-adapter
sabre-non-recurring-payments
sabre-provisioning
sabre-rated-charge
sabre-rated-usage
sabre-receipt-print
sabre-recurring-payments
sabre_recurring_prepayments
sabre-sales-order
sabre-server
sabre-sim-profile
sabre-simulator
sabre-statement-production
sabre-usage-archiving
sabre-workflow-monitor
setup-utility

- Administration Console

The operational interface for CMP providing administration of the SABRE server. The console includes documentation of each SABRE job and allows jobs to be controlled, configured, monitored and scheduled.

- Report Server

  Allows standard CMP reports to be executed and scheduled. The Report Server is an instance of a Pentaho server. The necessary Pentaho software is bundled with the CMP installation packages.

For a more detailed overview on each component, see the CMP Technical Architecture Overview.

2. 1. 2 Optional Components

Optional components and modules include:

Bulk Action Console

Bulk Actions provides a framework against which individual bulk action jobs can be developed to support different types of bulk changes. The Bulk Action framework is a combination of a web based user interface (Bulk Action Console) and a batch processing framework which is built on top of the CMP Sabre framework.

This component comprises the following CMP modules:

Module
sabre-bulk-action-console
sabre-bulk-action-framework

Bottomline Adapter

If a customer has chosen to install it, at the end of the billing process, the billing files can be automatically transferred to an optional Bill Formatting system, powered by Bottomline Technologies, that is responsible for the generation of the PDF bill for distribution and enquiry. For more information, see the Bill Print section of the CMP Billing Functionality Guide.

The following module is an adapter for Bottom Line:

Module
sabre-bill-pdf-collection-adapter

Analyser Extract

An optional batch job can produce extracts for analysis. The relevant module is:

Module
sabre-analyser-extract

Important

Optional components and adapters are not installed by default. If required, you need to add them to the *additional_modules* section of the inventory file. For more information on the inventory file and installation, see the *About CMP Installation* section of the CMP Installation Guide.

2. 1. 3 Adapters

MDS Global provides the following optional adapters:

- Adapters specifically for the UK market to support BACS direct debit payments and credit reference extracts to Equifax.

  The following table lists the adapters and the relevant CMP modules:

Banking/Credit Reference Service	Adapter Module(s)
ADDACS (Automated Direct Debit Amendment and Cancellation Service)	• sabre-addacs-transformation-adapter
AUDDIS (Automated Direct Debit Instruction Service)	• sabre-auddis-transformation-adapter • sabre-auddis-transformation-inbound-adapter
ARUCS (Automated Return of Unapplied Credit Service)	• sabre-arucs-transformation-adapter
AWACS (Advice of Wrong Account for Automated Credits Service)	• sabre-awacs-transformation-adapter
BACS (Bankers Automated Clearing Services)	• sabre-bacs-transformation-adapter
Equifax	• sabre-equifax-insight2001
Experian	• sabre-experian-transformation-adapter

- Online Charging System (OCS) adapters.

  The following modules are provided specifically for a Real Time Charging environment to support use of Openet and Matrixx as external Online Charging System (OCS) integrated into CMP:

Module
sabre-matrix-usage-transformation-daemon
sabre-openet-provisioning-adapter
sabre-openet-usage-adapter
sabre-openet-recurring-prepayment-adapter

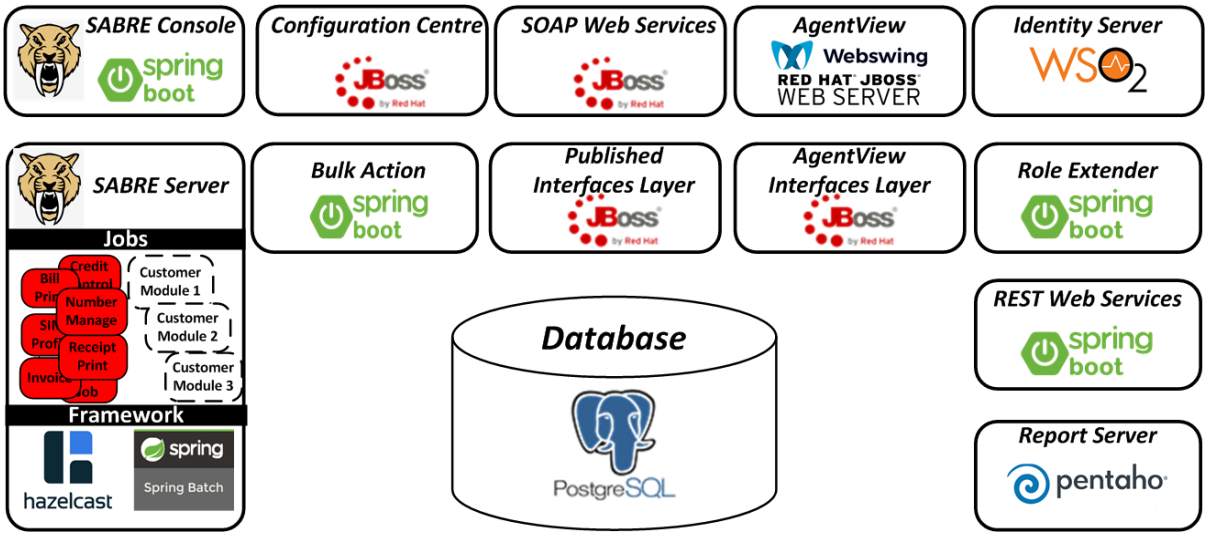
2. 1. 4 Third Party Software Components

See System Software.

The Release Notes list the most up-to-date versions of the CMP modules.

2. 2 System Software

The following diagram shows the required third party software for CMP components.



CMP Components

The following table lists the third party software components and whether the component is bundled as part of CMP:

Third Party Software	Installation Bundled with CMP
Red Hat Enterprise Linux	Install independently before CMP deployment
PostgreSQL	Install independently before CMP deployment
JBoss Enterprise Application Platform	Install independently before CMP deployment
JBoss Web Server	Install independently before CMP deployment
Spring Framework	Bundled with CMP
Spring Boot	Bundled with CMP
Spring Batch	Bundled with CMP
Spring Security	Bundled with CMP
Webswing	Bundled with CMP
Hazelcast	Bundled with CMP
WSO2 IS	Bundled with CMP
Pentaho	Bundled with CMP
Active MQ	Bundled with CMP
pg_partman	Bundled with CMP

The following CMP modules include third party components:

- wso2is
- jboss-postgres-jdbc-driver-eap7
- webswing

The third party components above depend on the following configuration modules:

- jboss-aviewiface-address-lookup-interface-eap
- jboss-aviewiface-common-eap7
- jboss-aviewiface-configuration-eap7
- jboss-ccentre-configuration-eap7
- jboss-pil-configuration-eap7
- jboss-soapws-configuration-eap7
- jboss-aviewiface-stock-check-interface-eap

For more information, such as supported versions, support providers and licensing, see the CMP Technical Architecture overview.

2. 3 System Installation and Upgrade

CMP is delivered as a set of components that are RPM (Red Hat Package Manager) packages and it is installed and deployed by running an Ansible playbook.

The installation repository for CMP is available on the CMP host in the cloud (https://vault.mdsglobal.dev/), accessible via HTTPS with the credentials provided by MDS Global, according to the customer's contract.

2. 3. 1 Upgrading CMP

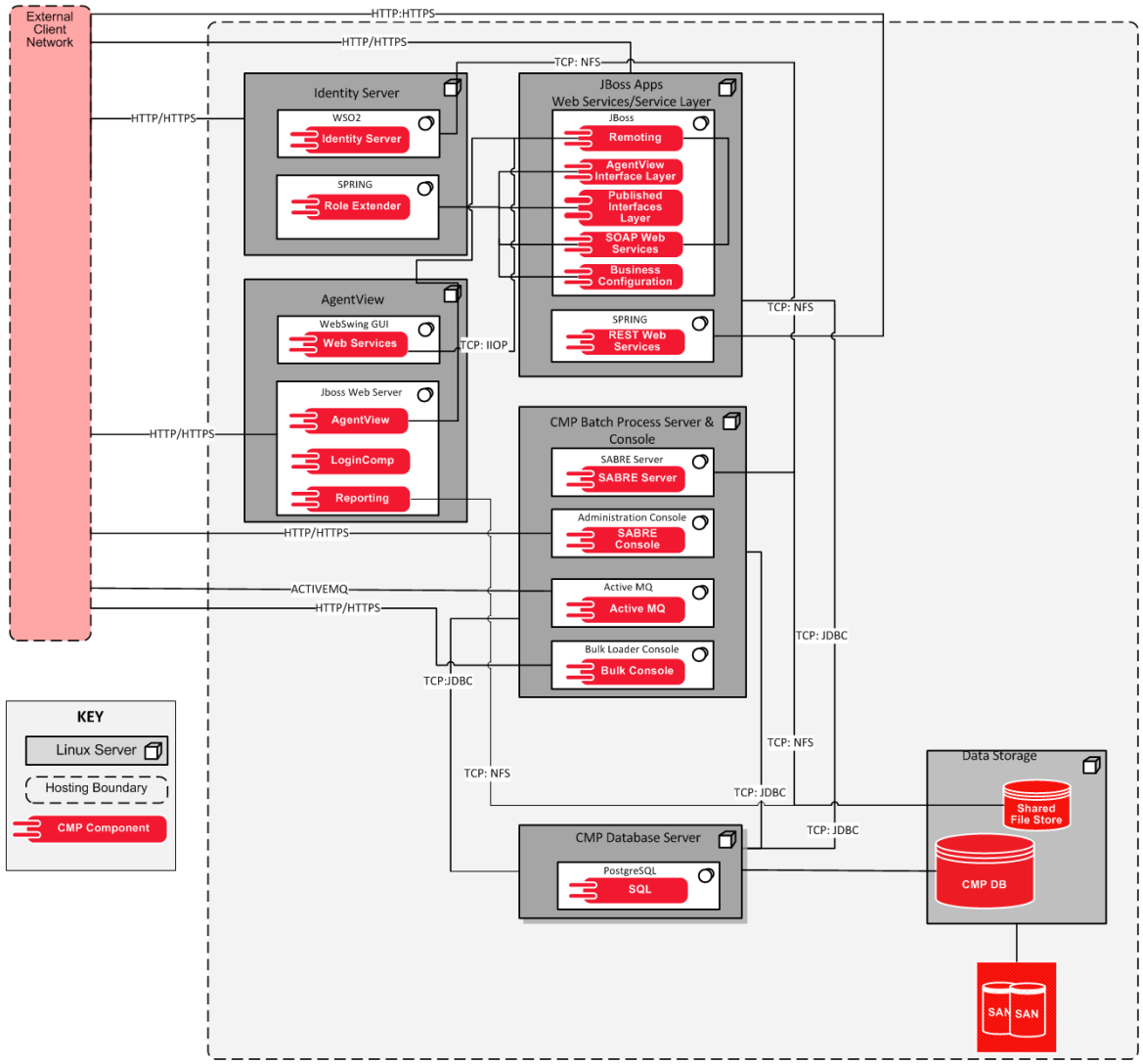
To upgrade an existing CMP installation, use the same ansible-playbook command to deploy a new installation:

```
ansible-playbook --vault-password-file=<vault_password_file> -i
<inventory_file> -b playbooks/deploy.yaml
```

For more information, see the Upgrading an Existing Installation section of the CMP Installation Guide.

2. 4 System Communication

The following diagram of a simple sample deployment shows how CMP components communicate:



CMP Components Communication

CMP components must be able to communicate with each other, the following table shows which components in the CMP component stack need to communicate and over which (default) port.

Intra Stack Communications		
Source Hosts	**Destination Host**	**Port Numbers**
Identity Server JBoss Server instances - required for • Published Interfaces Layer • AgentView Interfaces Layer • SOAP Web Services • Configuration C enter Role Extender application SABRE Server (Batch sever application instances) Administration Console application instances REST web services application Report Server (Instance of a Pentaho server) Bulk Action UI (optional component)	Database Server	5432
AgentView Interfaces Layer AgentView application instances Published Interfaces Layer Role Extender application Administration Console application instances REST web services application Business Configuration application Bulk Action UI (optional)	Identity Server OAuth2 is used for communication between components and the server.	9443
AgentView Interfaces Layer Published Interfaces Layer	rolext	8081
SABRE Server(Batch sever application instances) Administration Console application instances Bulk Action UI (optional)	SABRE Server Administration Console	27300 27400 22

2. 4. 1 External Access

To provide user access to CMP, communication over the following ports must be allowed from the client networks. Whether to allow the HTTP or HTTPS port depends on the system configuration. For more information, see *Network Communication* in the CMP Installation Guide.

Target Host Groups	HTTP Port	HTTPS Port
JBoss Web Server instances for AgentView application	7080	7443
JBoss Server instances - required for: • Published Interfaces Layer • AgentView Interfaces Layer • SOAP Web Services • Configuration Centre	8080	8443
Identity Server	9763	9443
Administration Console application instances	31212	31212
SABRE Server (Batch sever application instances)	21212	21212
restws	9000	9000

3.0 System Administration

System administration involves the following for each CMP component:

- Deployment

  CMP uses Ansible automated deployment to deploy CMP components.

- Starting

  CMP installs the following services:

Component	Service Name
Database Server	postgresql-16
Identify Server	wso2is
JBoss server instances. Required for: • AgentView Interface Layer • Published Interface Layer • SOAP Web Services Application • Business Configuration	eap7-standalone
JBoss Web Server instances. Required for: • AgentView application • Webswing • Identity Server Customised Login • AgentView Servlet	jws5-tomcat
Role Extender	role-extender
SABRE Server	sabre-server
Administration Console	sabre-console
REST WS	rest-ws

  All CMP 8.18 components are configured to start as `systemd`[1] services. The standard `systemctl` command should be used to start or restart the component services.

- Stopping

  The system is designed to run continuously so resources are available to users 24/7. Occasionally, shutting down or rebooting a system is necessary because of a system configuration change, a scheduled maintenance event, or a power outage.

  When shutting down a system or system component:

[1] Systemd is a system and service manager for Linux operating systems. It provides a number of features such as parallel startup of system services at boot time, on-demand activation of daemons, or dependency-based service control logic. In Red Hat Enterprise Linux 7, systemd replaces Upstart as the default init system.

- Ensure you have the correct privilege to do so, for example by using the `sudo` command to assume `root` user privilege.
- Use a standard monitoring tool to check whether users are using the system or component. Depending on the situation, either request that the users log off or warn the users and use the appropriate tool to log them off.
- Execute the appropriate command to shut down the system or component.

- Monitor Status

  For CMP component services, you can use the `systemctl status` command status to check the status of a service and whether it needs to be stopped or restarted.

- Configuration

  For installation and deployment of components, default values are provided for component properties in the inventory file that describes the configuration of the target hosts. It is also recommended that the Installation Configuration tool is used to prepare the inventory file.

  If you have strong reasons to do so, you can prepare the file manually and/or also alter property values to values other than the default. This must only be done by experienced persons who thoroughly understand the consequences of their actions. If you alter the configuration of components post-installation, the same caveat applies.

- Log files

  Log files are created for each CMP component during installation. The location for the log files is supplied in the summary file which is created at the end of the installation process. For more information, see the Summary File topic in the CMP Installation Guide.

- Troubleshooting

3. 1 Database Administration

The CMP database holds a complete representation of the customer including all personal/business details, proposition, billing, payments and credit control data. The CMP database provides a central view of all CMP data, without the need to maintain/synchronise data across multiple databases.

The CMP database also holds the configuration used by CMP including all propositions, business process rules and reference data.

3. 1. 1 Deployment

CMP does not have a strong dependency on the proprietary features of any particular relational database management system (RDBMS). The product is currently certified and tested using PostgreSQL. For information on how to deploy the CMP database, see the CMP Installation Guide.

3. 1. 2 Starting

To start the database service, use the following command:

```
sudo systemctl start postgresql-16
```

To restart the database service, use the following command:

```
sudo systemctl restart postgresql-16
```

3. 1. 3 Stopping

To stop the database service, use the following command:

```
sudo systemctl stop postgresql-16
```

3. 1. 4 Monitoring Status

To check the status of the PostgreSQL service, use the following command:

```
sudo systemctl status postgresql-16
```

The PostgreSQL database must be monitored and managed in day-to-day operation using standard tools. For more information, see the topic "System Monitoring" on page 38

3. 1. 5 Configuration

For a list of the properties that must be configured during installation and configuration, see the Database Properties section of the *CMP Installation Guide*.

3. 1. 6 Database Purging

Data purging helps to keep obsolete and unwanted data to a minimum - subject to regulatory constraints - and can improve the application's performance. CMP provides a suite of purge batch jobs that run in SABRE server.

For more information on the purge routines and how to run them, see:

- CMP Purge Guide
- CMP Operational Overview
- The online help for the Administration Console.

3. 1. 7 Other Database Administration Considerations

Other considerations when managing the CMP database include:

- Database Inventory
- Managing Databases
- Scheduling Database Maintenance
- Moving Databases
- Changing Databases
- Database Access
- Adding/Deleting Users to Database
- Setting User Permissions for Database
- Adding/Deleting Groups for Database
- Re-indexing Database
- Data Entry/Modification/Deletion
- Database Backup and Restore
- Database Reporting.

3. 2 JBoss Server Instance Administration

The following CMP Components run in an instance of a JBoss Enterprise Application Platform server:

- AgentView Interfaces Layer
- Published Interfaces Layer
- SOAP Web Services
- Business Configuration.

3. 2. 1 Deployment

JBoss Enterprise Application Platform is not bundled with CMP and should be installed independently prior to installation and deployment of CMP. See the CMP Technical Architecture Overview for more details.

For information on how to deploy the dependant CMP components, see the CMP Installation Guide.

3. 2. 2 Starting

To start the JBoss Server service, use the following command:

```
sudo systemctl start eap7-standalone
```

To restart the JBoss Server service, use the following command:

```
sudo systemctl restart eap7-standalone
```

3. 2. 3 Stopping

To stop the JBoss Server service use the following command:

```
sudo systemctl stop eap7-standalone
```

3. 2. 4 Monitoring Status

To check the status of the JBoss Server service, use the following command:

```
sudo systemctl status eap7-standalone
```

Check the log file for any errors – sometimes the process is still running but not functioning.

3. 2. 5 Configuration

For a list of the properties that must be configured during installation and configuration, see the JBoss Server Properties section of the *CMP Installation Guide*.

3. 2. 6 Logs

The Summary File generated at the end of the installation process provides the location of log files for the JBoss Server service, for example:

```
JBoss

======

Logs:

Host: server2.example.demo.com

Path: /var/log/eap7/server.log
```

3. 3 JBoss Web Server Instance Administration

The following CMP Components and required third party software run in an instance of a JBoss Web Server:

- AgentView
- WSO2 customised login
- WebSwing.

3. 3. 1 Deployment

JBoss Web Server is not bundled with CMP and should be installed independently prior to installation and deployment of CMP. See the CMP Technical Architecture Overview for more details.

For information on how to deploy the dependant CMP components, see the CMP Installation Guide.

3. 3. 2 Starting

To start the JBoss Web Server service, use the following command:

```
sudo systemctl start jws5-tomcat
```

To restart the JBoss Web Server service, use the following command:

```
sudo systemctl restart jws5-tomcat
```

3. 3. 3 Stopping

To stop the JBoss Web Server service use the following command:

```
sudo systemctl stop jws5-tomcat
```

3. 3. 4 Monitoring Status

To check the status of the JBoss Web Server service, use the following command:

```
sudo systemctl status jws5-tomcat
```

Check the log file for any errors - sometimes the process is still running but not functioning.

3. 3. 5 Configuration

For a list of the properties that must be configured during installation and configuration, see the JBoss Web Server Properties section of the *CMP Installation Guide*.

3. 3. 6 Logs

The Summary File generated at the end of the installation process provides the location of log files for the JBoss Web Server service.

3. 4 Identity Server Administration

WSO2 Identity Server is an identity and access management server that facilitates security, while connecting and managing multiple identities across different applications. It provides centralised user authentication and authorisation to the user across CMP including Single Sign On.

3. 4. 1 Deployment

The Identity Server is an instance of WSO2 and OAuth2 is used for communication between the CMP components and the Identity Server.

For information on how to deploy the Identity Server, see the CMP Installation Guide.

3. 4. 2 Starting

To start the Identity Server service, use the following command:

```
sudo systemctl start wso2is
```

To restart the Identity Server service, use the following command:

```
sudo systemctl restart wso2is
```

3. 4. 3 Stopping

To stop the Identity Server service, use the following command:

```
sudo systemctl stop wso2is
```

3. 4. 4 Monitoring Status

To check the status of the Identity Server service, use the following command:

```
sudo systemctl status wso2is
```

Check the log file for any errors – sometimes the process is still running but not functioning.

3. 4. 5 Configuration

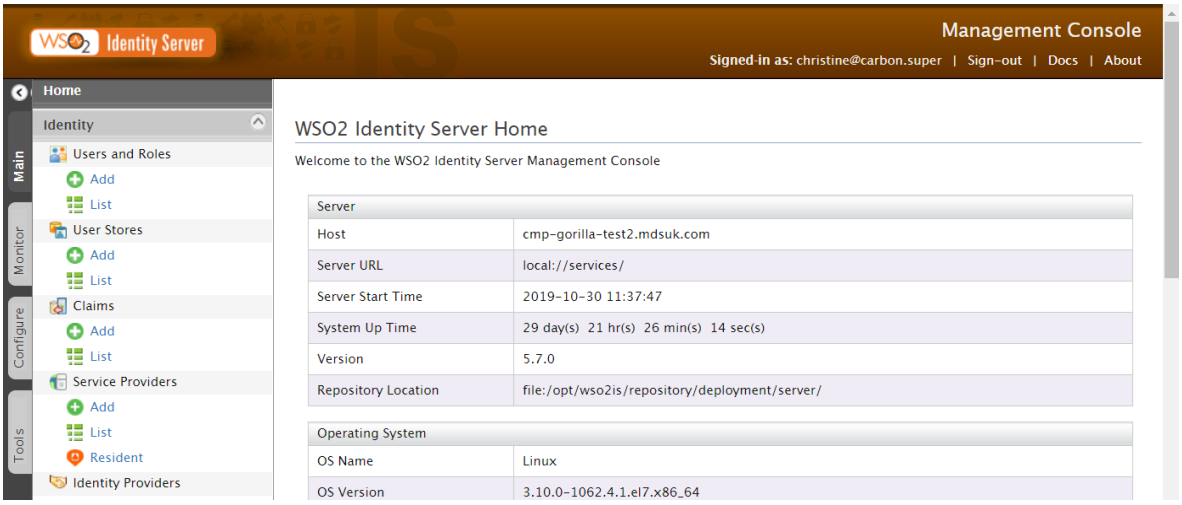
For a list of the properties that must be configured during installation and configuration, see the WSO2 Identity Server Properties section of the *CMP Installation Guide*.

3. 4. 6 Logs

The Summary File generated at the end of the installation process provides the location of log files for the Identity Server, for example the section pertaining to the Identity Server can look as follows:

```
WSO2 IS
=========
URL: https://server.example.demo.com:9443
Logs:
Host: server.example.demo.com
Path: /var/log/wso2carbon/wso2carbon.log
```

3. 4. 7 The Identity Server Management Console

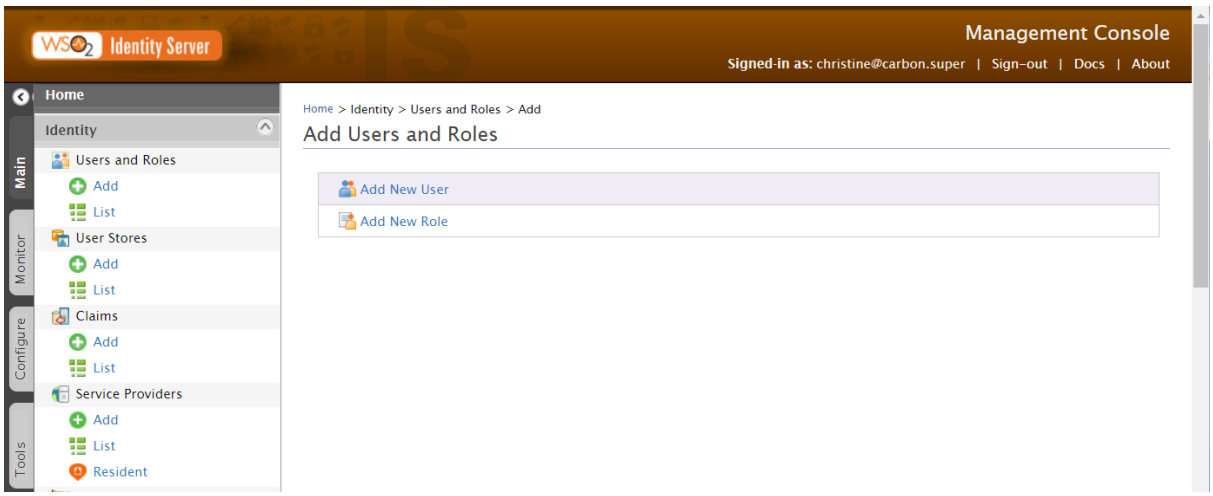


The Home screen of the Identity Server Management Console

The Identity Server is managed in the Management Console, which has four main areas accessed by tabs on the left:

Main

The **Main** menu in the Management Console includes the main list of features that the WSO2 Identity Server provides. The main menu is divided into different sections. Use the **Identity** section for security-related tasks, such as managing users, roles and permissions.

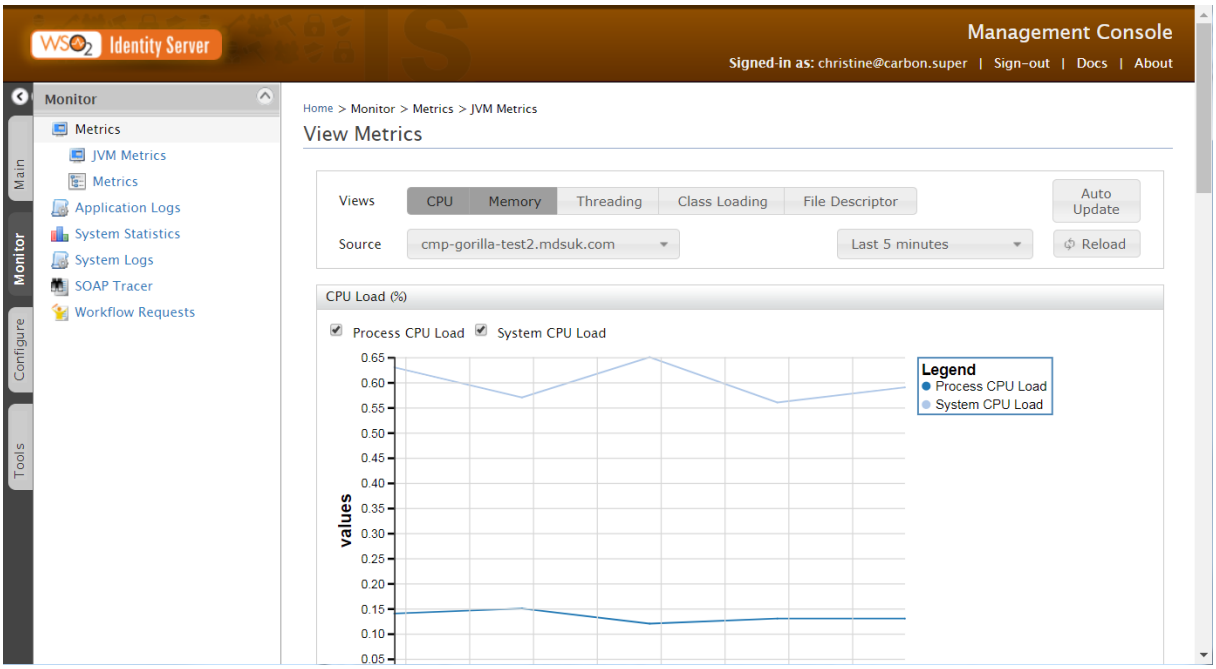


Identity Server Management Console - Main Menu > Identity

For more information of users and roles, see the CMP Security Guide.

Monitor

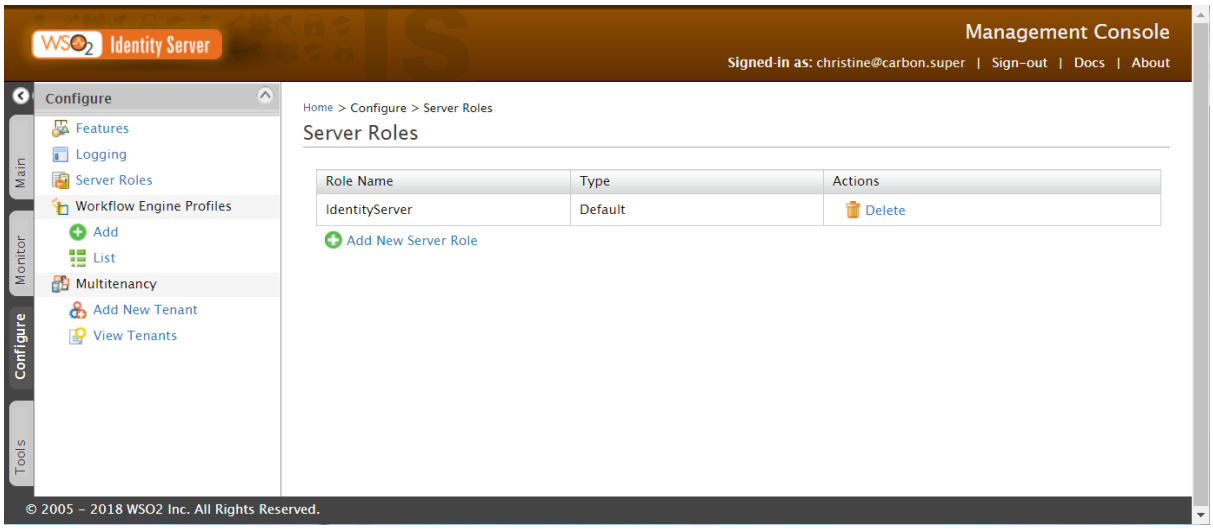
The Monitor menu includes features related to monitoring the Identity Server, focused on providing logs and statistics.



Monitor Menu in the Identity Server Management Console

Configure

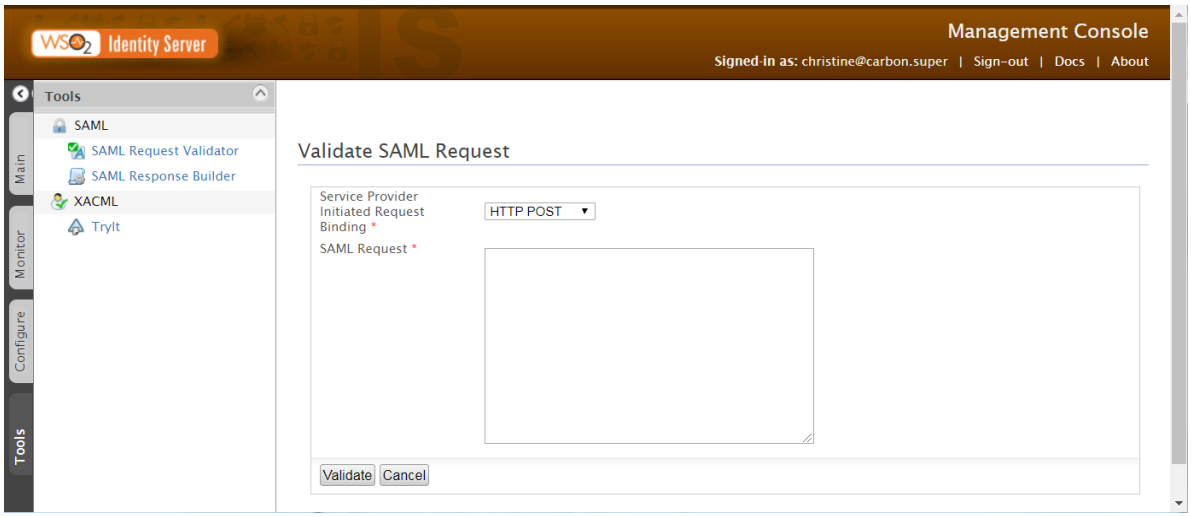
Use the **Configure** menu to access features that allow you to customise Identity Server for the specific needs of your CMP deployment.



Configure Menu in the Identity Server Management Console

Tools

The **Tools** menu provides utilities for developers. Developers can use the tools to validate configurations and build sample response.



Tools Menu in the Identity Server Management Console

For more information, consult the WSO2 Identity Server Documentation.

3. 5 Role Extender Administration

The Role Extender translates business roles known to the Role Extender into more granular roles that are actually used for authorisation within CMP. The Role Extender takes a role to which access has been granted in the Identity Server and returns the full list of lower level roles that this maps to.

3. 5. 1 Deployment

The Role Extender executes in Spring Boot. For information on how to deploy the Role Extender, see the CMP Installation Guide.

3. 5. 2 Starting

To start the Role Extender service, use the following command:

```
sudo systemctl start role-extender
```

To restart the Role Extender service, use the following command:

```
sudo systemctl restart role-extender
```

3. 5. 3 Stopping

To stop the Role Extender service, use the following command:

```
sudo systemctl stop role-extender
```

3. 5. 4 Monitoring Status

To check the status of the Role Extender service, use the following command:

```
sudo systemctl status role-extender
```

Check the log file for any errors – sometimes the process is still running but not functioning.

3. 5. 5 Configuration

For a list of the properties that must be configured during installation and configuration, see the Role Extender Properties section of the *CMP Installation Guide*.

3. 5. 6 Logs

The Role Extender used the same log file as the Identity Server.

3. 6 SABRE Server Administration

The SABRE Server is a batch server that executes all asynchronous processing within CMP. This includes both scheduled batch processing and immediate processing required in response to an event.

> For information on monitoring and managing the day-to-day operation of SABRE batch jobs, processes, probes and daemons, see the Operational Overview.

3. 6. 1 Deployment

The SABRE Server is based on Spring Batch and uses Hazelcast for in-memory storage and communication to distribute processing. Multiple instances of the SABRE Server, or nodes, can be installed to form a cluster, distributing processing load to provide horizontal scalability.

For information on how to deploy the SABRE Server, see the CMP Installation Guide.

3. 6. 2 Starting

To start the SABRE Server service, use the following command:

```
sudo systemctl start sabre-server
```

To restart the SABRE Server service, use the following command:

```
sudo systemctl restart sabre-server
```

3. 6. 3 Stopping

To stop the SABRE Server service, use the following command:

```
sudo systemctl stop sabre-server
```

3. 6. 4 Sequence

The sequence for stopping and starting sabre-console and sabre-service services is as follows:

Non High Availability Environment

Stopping

Step 1: `sudo systemctl stop sabre-console`

Step 2: `sudo systemctl stop sabre-server`

Starting

Step 1: `sudo systemctl start sabre-server`

Step 2: `sudo systemctl start sabre-console`

High Availability Environment

Stopping

Step 1: `sudo systemctl stop sabre-console` (on both active and passive servers)

Step 2: `sudo systemctl stop sabre-server` (on both active and passive servers)

Starting

Step 1: `sudo systemctl start sabre-server` (on both active and passive servers)

Step 2: `sudo systemctl start sabre-console` (on both active and passive servers)

3. 6. 5 Monitoring Status

To check the status of the SABRE Server service, use the following command:

```
sudo systemctl status sabre-server
```

Check the log file for any errors – sometimes the process is still running but not functioning.

3. 6. 6 Configuration

For a list of the properties that must be configured during installation and configuration, see the SABRE Server Properties section of the *CMP Installation Guide*.

3. 6. 7 Logs

The Summary File generated at the end of the installation process provides the location of log files for the SABRE Server, for example the section pertaining to SABRE Server can look as follows:

```
Sabre Server

==============

URL: https://server2.example.demo.com:21212/

Logs:

Host: server2.example.demo.com

Path: /var/log/sabre-server/
```

3. 7 Administration Console Administration

The operational interface for CMP providing administration of the SABRE server. The console includes documentation of each SABRE job and allows jobs to be controlled, configured, monitored and scheduled.

> For information on monitoring and managing the day-to-day operation of SABRE batch jobs, processes, probes and daemons, see the Operational Overview.

3. 7. 1 Deployment

The SABRE Administration Console runs in Spring Boot.

For information on how to deploy the Administration Console, see the CMP Installation Guide.

3. 7. 2 Starting

To start the Administration Console service, use the following command:

```
sudo systemctl start sabre-console
```

To restart the Administration Console service, use the following command:

```
sudo systemctl restart sabre-console
```

3. 7. 3 Stopping

To stop the Administration Console service, use the following command:

```
sudo systemctl stop sabre-console
```

3. 7. 4 Sequence

The sequence for stopping and starting sabre-console and sabre-service services is as follows:

Non High Availability Environment

Stopping

Step 1: `sudo systemctl stop sabre-console`

Step 2: `sudo systemctl stop sabre-server`

Starting

Step 1: `sudo systemctl start sabre-server`

Step 2: `sudo systemctl start sabre-console`

High Availability Environment

Stopping

Step 1: `sudo systemctl stop sabre-console` (on both active and passive servers)

Step 2: `sudo systemctl stop sabre-server` (on both active and passive servers)

Starting

Step 1: `sudo systemctl start sabre-server` (on both active and passive servers)

Step 2: `sudo systemctl start sabre-console` (on both active and passive servers)

3. 7. 5 Monitoring Status

To check the status of the Administration Console service, use the following command:

```
sudo systemctl status sabre-console
```

Check the log file for any errors – sometimes the process is still running but not functioning.

3. 7. 6 Configuration

For a list of the properties that must be configured during installation and configuration, see the Administration Console Properties section of the *CMP Installation Guide*.

3.7.6.1 Configuring Administration Console Modules

Administration Console modules are JAR packages that contain the code for all the processes, jobs and daemons that make up the console functionality. For a list of the modules, see "SABRE Server" on page 5 in the *System Components* section. In the **Modules** screen of the Administration Console, you can configure system-wide parameters, application parameters and parameters for all modules installed on the system.

For more information, see Modules in the CMP Operational Overview.

3. 7. 7 Logs

The Summary File generated at the end of the installation process provides the location of log files for the Administration Console, for example the section pertaining to the Administration Console can look as follows:

```
Sabre Console
==============
URL: https://server.example.demo.com:31212/
Logs:
Host: server.example.demo.com
Path: /var/log/sabre-console/
```

3.7.7.1 Logging in the Administration Console

In the Logging screen of the Administration Console, you can:

- View the loggers that monitor the console operations.
- Add new loggers.
- Change the logging level for a logger.

For more information, see Logging in the CMP Operational Overview.

3. 8 AgentView Administration

AgentView is the primary user interface for CMP used by call centre staff to enrol customers onto the system and to maintain their details.

3. 8. 1 Deployment

AgentView is a web client served by Webswing running in a JBoss Web Server. The AgentView application contains only presentation and validation logic. All required business logic resides in the AgentView Interfaces Layer. One instance of the AgentView web server connects to a single specified instance of the AgentView Interfaces Layer.

For information on how to deploy AgentView, see the CMP Installation Guide.

3. 8. 2 Starting

WebSwing is a web application and is deployed to a JBoss Web Server. To start WebSwing, use the following command:

```
sudo systemctl start jws5-tomcat
```

To restart WebSwing, use the following command:

```
sudo systemctl restart jws5-tomcat
```

3. 8. 3 Stopping

The AgentView application is stopped when WebSwing is restarted.

To stop WebSwing, use the following command:

```
sudo systemctl stop jws5-tomcat
```

3. 8. 4 Monitoring Status

To check the status of AgentView, use the following command to check the status of the JBoss Web Server instance on which WebSwing is installed:

```
sudo systemctl status jws5-tomcat
```

Check the log file for any errors – sometimes the process is still running but not functioning.

3. 8. 5 Configuration

During installation and deployment, you need to configure the name of the host(s) on which AgentView will be installed.

3. 8. 6 Logs

The Summary File generated at the end of the installation process provides the location of log files for the AgentView, for example the section pertaining to the AgentView can look as follows:

```
Agent View

==========
```

```
URL: https://server.example.demo.com:8443/agent-view
Logs:
Host: server.example.demo.com
Path: /var/log/webswing/
```

3. 9 AgentView Interfaces Layer Administration

The AgentView Interfaces Layer contains the business logic used by the AgentView user interface to access the CMP database.

3. 9. 1 Deployment

The interfaces layer is accessed via RMI/JRMP and then connects to the CMP database via JDBC.

The AgentView Interfaces Layer is installed as a set of Enterprise Java Beans (EJBs) to a JBoss Enterprise Application Platform (EAP). The business logic is shared with the Published Interfaces Layer such that AgentView and the CMP SOAP Web Services expose functions in a consistent manner.

For information on how to deploy the AgentView Interfaces Layer, see the CMP Installation Guide.

3. 9. 2 Starting

The AgentView Interfaces Layer is deployed to a JBoss Server instance and thus starts when the server instance service starts. To start the service, use the following command:

```
sudo systemctl start eap7-standalone
```

To restart the JBoss service, use the following command:

```
sudo systemctl restart eap7-standalone
```

3. 9. 3 Stopping

The AgentView Interfaces Layer is deployed to a JBoss Server instance and thus stops when the server instance service is killed. To stop the service, use the following command:

```
sudo systemctl stop eap7-standalone
```

3. 9. 4 Monitoring Status

To check the status of the JBoss service, use the following command:

```
sudo systemctl status eap7-standalone
```

Check the log file for any errors – sometimes the process is still running but not functioning.

3. 9. 5 Configuration

During installation and deployment, you need to configure the name of the host(s) on which the Published Interfaces Layer will be installed.

3. 9. 6 Logs

The Summary File generated at the end of the installation process provides the location of log files for JBoss service, for example:

```
JBoss

======

Logs:

Host: server2.example.demo.com

Path: /var/log/eap7/server.log
```

3. 10 Published Interfaces Layer Administration

The Published Interfaces Layer contains the business logic used by the CMP SOAP Web Services.

3. 10. 1Deployment

The interfaces layer is accessed via RMI/JRM and then connects to the CMP database via JDBC.

The Published Interfaces Layer is installed as a set of Enterprise Java Beans (EJBs) to a JBoss Enterprise Application Platform (EAP). The business logic is shared with the AgentView Interfaces Layer such that CMP SOAP Web Services and AgentView expose functions in a consistent manner.

For information on how to deploy the Published Interfaces Layer, see the CMP Installation Guide.

3. 10. 2Starting

The Published Interfaces Layer is deployed to a JBoss Server instance and thus starts when the server instance service starts. To start the service, use the following command:

```
sudo systemctl start eap7-standalone
```

To restart the JBoss service, use the following command:

```
sudo systemctl restart eap7-standalone
```

3. 10. 3Stopping

The Published Interfaces Layer is deployed to a JBoss Server instance and thus stops when the server instance service is killed. To stop the service, use the following command:

```
sudo systemctl stop eap7-standalone
```

3. 10. 4Monitoring Status

To check the status of the JBoss service, use the following command:

```
sudo systemctl status eap7-standalone
```

Check the log file for any errors – sometimes the process is still running but not functioning.

3. 10. 5Configuration

For more information on deploying and configuring the Published Interfaces Layer, see the CMP Installation Guide.

3. 10. 6Logs

The Summary File generated at the end of the installation process provides the location of log files for JBoss service, for example:

```
JBoss

======

Logs:

Host: server2.example.demo.com

Path: /var/log/eap7/server.log
```

3. 11 Business Configuration Administration

Business Configuration provides for viewing and modification of business and user applicable system configuration. It allows CMP business configuration to be created and

maintained either via a web-based graphical interface or via a set of RESTful web services exposing the same capabilities.

3. 11. 1Deployment

Business Configuration runs in an instance of JBoss Enterprise Application Platform (EAP) and the web-based graphical interface, web services, functional business logic and connection to the database via JDBC.

For information on how to deploy the Identity Server, see the CMP Installation Guide.

3. 11. 2Starting

Business Configuration is deployed to a JBoss Server instance and thus starts when the server instance service starts. To start the service, use the following command:

```
sudo systemctl start eap7-standalone
```

To restart the JBoss service, use the following command:

```
sudo systemctl restart eap7-standalone
```

3. 11. 3Stopping

Business Configuration is deployed to a JBoss Server instance and thus stops when the server instance service is killed. To stop the service, use the following command:

```
sudo systemctl stop eap7-standalone
```

3. 11. 4Monitoring Status

To check the status of the JBoss service, use the following command:

```
sudo systemctl status eap7-standalone
```

Check the logfile for any errors – sometimes the process is still running but not functioning.

3. 11. 5Configuration

During installation and deployment, you need to configure the name of the host(s) on which Business Configuration will be installed.

3. 11. 6Logs

The Summary File generated at the end of the installation process provides the location of log files for Business Configuration, for example:

```
Configuration Centre
====================
```

```
URL: https://server2.example.demo.com:8443/config
Logs:
Host: server.example2.demo.com
Path: /var/opt/rh/eap7/log/wildfly/standalone/server.log
```

3. 12 RESTful Web Services Administration

Provide a standard mechanism for online customer data interchange between CMP and other MDS Global and third party systems and applications. CMP has two complimentary sets of web services for customer data: SOAP and RESTful web services.

3. 12. 1Deployment

RESTful web services run in Spring Boot with in-built validation, business logic and connection to the CMP database via JDBC

For information on how to deploy the RESTful Web Services, see the CMP Installation Guide.

3. 12. 2Starting

To start the RESTful Web Services service, use the following command:

```
sudo systemctl start rest-ws
```

To restart the RESTful Web Services service, use the following command:

```
sudo systemctl restart rest-ws
```

3. 12. 3Stopping

To stop the RESTful Web Services service, use the following command:

```
sudo systemctl stop rest-ws
```

3. 12. 4Monitoring Status

To check the status of the RESTful Web Services service, use the following command:

```
sudo systemctl status rest-ws
```

Check the logfile for any errors – sometimes the process is still running but not functioning.

3. 12. 5Configuration

For a list of the properties that must be configured during installation and configuration, see the REST Web Services Properties section of the *CMP Installation Guide*.

3. 12. 6Logs

The Summary File generated at the end of the installation process provides the location of log files for the RESTful Web Services, for example the section pertaining to the RESTful Web Services can look as follows:

```
REST WS

==============

URL: https://server.example.demo.com:9000/

Logs:

Host: server.example.demo.com

Path: /var/log/rest-ws/boot.log
```

3. 13 SOAP Web Services Administration

CMP web services allow systems and applications to create, view and manage data in the CMP database, reflecting core customer care activities that can be performed manually through the AgentView client. CMP SOAP web services are exposed using SOAP over HTTP to exchange XML data.

3. 13. 1Deployment

These services run in an instance of JBoss Enterprise Application Platform (EAP) and call the Published Interfaces Layer using RMI/JRMP for validation, business logic and communication with the CMP database.

For information on how to deploy the Identity Server, see the CMP Installation Guide.

3. 13. 2Starting

The CMP SOAP Web Services application deployed to a JBoss Server instance and thus starts when the server instance service starts. To start the service, use the following command:

```
sudo systemctl start eap7-standalone
```

To restart the JBoss service, use the following command:

```
sudo systemctl restart eap7-standalone
```

3. 13. 3Stopping

The CMP SOAP Web Services application is deployed to a JBoss Server instance and thus stops when the server instance service is killed. To stop the service, use the following command:

```
sudo systemctl stop eap7-standalone
```

3. 13. 4Monitoring Status

To check the status of the JBoss service, use the following command:

```
sudo systemctl status eap7-standalone
```

Check the log file for any errors - sometimes the process is still running but not functioning.

3. 13. 5Configuration

During installation and deployment, you need to configure the name of the host(s) on the CMP SOAP Web Services will be installed.

3. 13. 6Logs

The Summary File generated at the end of the installation process provides the location of log files for SAP web services, for example:

```
SOAP WS

====================

URL: https://server2.example.demo.com:8443/ws

Path: /var/log/eap7/server.log
```

4.0 System Monitoring

Monitoring system resources and performance can:

- Collect data to form a baseline for comparisons to measure performance.
- Determine the most valuable and efficient use of resources.
- Identify whether CMP is running as expected - allowing early detection and prevention of issues.
- Detect issues that affect CSAs productively.

4. 1 Monitoring CMP Components

This section lists the CMP components that require monitoring, and what to monitor. Because CMP deployments will differ to meet the unique needs of each customer, this list is not intended to be exhaustive.

Infrastructure, Virtual Machines and Operation System (RHEL)

Items to monitor can include:

- CPU utilisation
- Memory utilisation
- Storage space
- Storage throughput and input/output
- Network utilisation

Third Party System Software

Items to monitor can include:

- Java Virtual Machine (JVM) /memory usage
- Request rate
- Garbage collection

Database (PostgreSQL)

Items to monitor can include:

- Buffercache usage
- Vacuum monitor
- Tablespace/disk size
- Number of concurrent sessions
- Commits rollbacks
- Checkpoints
- Deadlocks
- Long-running SQL
- Log monitoring
- Replication status/lag

CMP Software

Items to monitor can include:

- Process availability - are all processes running?
- Number of AgentView users.
- Monitoring provided by SABRE Administration Console for batch jobs.

  For more information, see the CMP Operational Overview.
- Status of Report Server reports.

4. 2 System Monitoring Tools

System monitoring tools focus on processes, memory, storage and net connections. Many general third party system monitoring tools are available, for example Nimsoft, Nagios and Solar Winds, as well as more specific tools such as PEM for PostgreSQL. The choice of monitoring tools is up to the customer.

The following links compare system monitors:

- https://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems
- https://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.htm

5.0 System Security

5. 1 System Access and Authorisation

The CMP components that provide identity, access and authorisation are the Identity Server and Role Extender.

The Identity Server is an instance of WSO2 and provides centralised user authentication, including Single Sign On, and role management across the different components of CMP. Users can be created and assigned roles in the Management Console of Identity Server.

You can also create users and assign them access to CMP applications and functionality in the Administration Console. See the Administration Console **Users** screen and the online help for more information. More granular maintenance takes place directly in the Identity Server Management Console.

CMP employs a multi-level role-based security model in which each user who has rights to access a CMP component is assigned zero or more roles that define which functional area or resource they can access once they are successfully authenticated.

The authorisation implementation in many parts of CMP uses very granular level roles for maximum flexibility and future proofing. It would be too cumbersome to have to grant access to all of these granular roles directly to users. A number of granular roles are therefore mapped to higher level business roles and access is granted to these business roles.

The Role Extender, executing in Spring Boot, takes a role to which access has been granted in the Identity Server and returns the full list of lower level roles that this maps to. CMP components use roles to which that access has been directly granted and the corresponding extended lists of roles returned by the Role Extender to determine whether to allow an action to be performed.

The mapping of business roles to granular roles is factory configuration that is not designed to be modified when CMP is installed.

For more information, see the CMP Security Guide, which covers:

- CMP role-based security
- Security groups and roles
- How to create users and assign roles in Identity Server

5. 2 Secure Communication and Encryption

By default, all CMP components communicate over HTTPS protocol. The required SSL certificates must be obtained prior to installation.

For more information, see SSL Certificates in the *CMP Installation Guide*.

5. 2. 1 SABRE Server Encryption

CMP is capable of encryption of all outgoing files and decryption of all incoming files using PGP[1] encryption following the OpenPGP standard (RFC 4880) for encrypting and decrypting data.

For more information, see SABRE Server Encryption in the *CMP Installation Guide*.

[1]Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is an asymmetric algorithm meaning it requires a key pair (public and private) to support encryption and decryption. Payloads are encrypted using the public key and can only be decrypted using the matching private key along with a passphrase

6.0 System Availability and Recovery

This section includes:

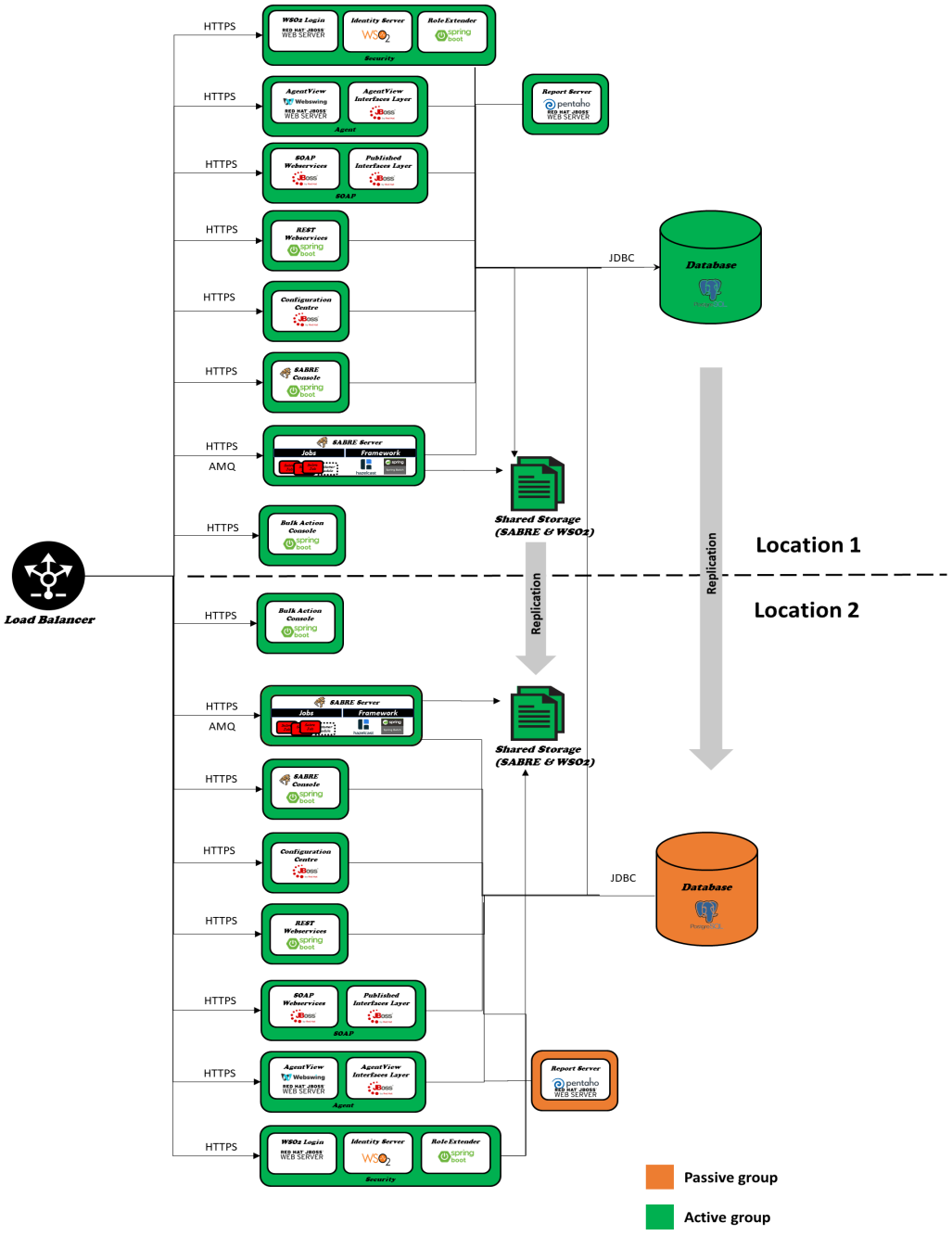
6. 1 High Availability

High availability (HA) is the ability of a system or system component to be continuously operational for a desirably long length of time. HA is an option as part of a CMP deployment. For more information in HA deployment, see the *CMP Installation Guide*.

For HA, the elements of the solution directly handling persisted data operate in an Active/Passive Configuration while the other parts of CMP operate in an Active/Active configuration. Configuring replication and the load balancing is not part of the CMP deployment and needs to be configured using relevant third party software and hardware as a separate step to the installation itself.

The diagram below shows the simplest of CMP high availability deployment over two different locations.

For more information, see High Availability in the *CMP Technical Architecture Overview*.



Simple CMP Deployment for High Availability

6. 2 Disaster Recovery

CMP HA options can be extended to disaster recovery by, for example, one half of the CMP stack in a different data centre, or availability zone for cloud deployments. Single or dual site HA is the only configuration option available with CMP 8. Please contact your MDS Global representative for more information.

7.0 System Optimisation

System optimisation can include tuning the CMP system for performance and automating tasks and processes, such as backups and purging.

7. 1 Metrics for System Performance and Sizing

Metric	Comments
Number of subscribers	Basic dimension on which to base call data
Average call/text/data records per month / subscriber	Basic dimension of call data
Bill cycles / month	Basic dimension of invoicing process
Average Size of bill PDF	Average size of PDF file
CSA Concurrent Users	Number of users concurrently connected to CMP AgentView
CSA Total Users	Total number of users of CMP AgentView
Invoice Data Online Retention	Number of months/years to hold invoice data online in the database
Invoice Data Offline Retention	Number of months/years to hold invoice data offline using backup or other media
Call Data Online Retention	Number of months/years to hold detailed call data online in the database
Call Data Offline Retention	Number of months/years to hold detailed call data offline using backup or other media
Bill PDF Online Retention	Number of months/years to hold bill PDF files for
Average number of SOAP API Requests	Average number of requests by SOAP web services
Peak number of SOAP API Requests	Highest number of requests by SOAP web services
Average number of REST API Requests	Average number of requests by RESTful web services
Peak number of REST API Requests	Highest number of requests by RESTful web services
Retention of application log data	Number of days/months/years to retain application logs
Retention of audit data	Number of days/months/years to retain audit logs
Number of Billing Accounts	The number of billing accounts
Maximum number of subscribers in hierarchy	The highest number of subscribers in a CMP hierarchy, for example at account, corporate or group level
Average number of subscribers in hierarchy	The highest number of subscribers in a CMP hierarchy, for example at account, corporate or group level
Number of workflow events per Subscriber	How many workflow events are associated with a subscriber

7. 2 Automating Tasks and Process

The SABRE Administration Console allows you to automate batch processes, which include housekeeping tasks such as purging, by creating schedules.

For more information, see the System Management section of the *CMP Operational Overview*.