HPE Unified OSS Console Assurance Monitoring OSSM Server Installation and Configuration Guide

Release 2.2
First Edition

Hewlett Packard Enterprise

Notices

Legal notice

Printed in the US

Trademarks

Contents

List of tables

List of figures

Chapter 1 Preface

About this guide

This guide describes how to install and configure the Unified OSS Console server Assurance Monitoring platform.

Audience

This Installation and Configuration guide is for anyone who is responsible for installing/uninstalling or configuring the OSSM Server platform.

The readers are assumed to have minimal knowledge of Linux shell scripts.

Software Versions

The supported software referred to in this document is as follows:

Server:

Software	Version	OS	Database
OSSM Server	2.2.0	Red Hat Linux 6.5 or later	Optional for topology maps or DB adaptor - Oracle 11.2.x - H2 1.4.180 - MySQL 5.1 + - Vertica 7.0.x MS SQL Server 2012 with JDBC Driver 4.0 for DB adaptor

Web browser:

Software	Version	Web Site
Microsoft Internet Explorer (not recommended)	10 or later	http://windows.microsoft.com/en-us/internet-explorer/download-ie
Mozilla Firefox	17 or later	https://www.mozilla.org/en-US/firefox
Google Chrome (recommended)	23 or later	https://www.google.com/chrome

Table 1 Software Version.

Typographical Conventions

Metric Light Font:

- Source code and examples of file contents.
- Commands that you enter on the screen.
- Pathnames
- Keyboard key names

Italic Text:

- Filenames, programs and parameters.
- The names of other documents referenced in this manual.

Bold Text:

- To introduce new terms and to emphasize important words.

Convention	Meaning
#	The Linux root default prompt
Ctrl/x	Indicates that you must hold down the key labeled Ctrl while you press another key or a pointing device button. In examples and procedures, a key combination is enclosed in a box.
[Return]	Indicates that you press the Return key to execute a command line.

Table 2 Convention

Associated Documents

The following documents contain useful reference information:

- HPE Unified OSS Console Assurance Monitoring Version 2.2.0 – User Guide.
- HPE Unified OSS Console Assurance Monitoring Version 2.2.0 – Release Notes.

Support

Please visit our HPE Software Support Online Web site at https://softwaresupport.hp.com/ for contact information, and details about HPE Software products, services, and support.

- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information

Document history

Edition	Date	Description
1.0	Jan 2016	Initial version.

Table 3: Document history

Chapter 1 Code Signing

This Software Product from HPE is digitally signed and accompanied by Gnu Privacy Guard (GnuPG) key.

On Red Hat Enterprise Linux, HP-UX, Windows and Solaris platforms

Below mentioned procedure* allows you to assess the integrity of the delivered Product before installing it, by verifying the signature of the software packages.

Pick the signature (.sig) file shipped along with the product and use following GPG command

```
gpg --verify <product.sig> <product>
```

Example: gpg --verify VPNSVP-X51-3A.zip.sig VPNSVP-X51-3A.zip

Note: Look for the comments shown below in the command output
Good signature from "Hewlett-Packard Company (HP Code signing Service)"

==========

Note: If you are not familiar with signature verification using GPG and intended to verify HP Product signature, follow the steps given below.

1. Check whether gnupg gpg is installed on the system. If no, install gnupg gpg

2. Configure GPG for accepting HPE signature. The steps are the following:
    a. Log as root on your system
    b. Get the hpPublicKey from following location:

        https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning and save it as hpPublicKey.pub

        Note that the hpPublicKey file will be located in the root's home directory.

    c. Follow the instruction found at above URL in the "Verification using GPG" section.

**HPE strongly recommends using signature verification on its products, but there is no obligation. Customers will have the choice of running this verification or not as per their IT Policies.*

Chapter 2 Getting Started

2.1 Introduction to HPE Unified OSS Console Assurance Monitoring Solution

HPE Unified OSS Console for Assurance Monitoring Solution supports business critical service operations and processes. It provides Real time data and metrics allowing reacting to business change as it happens, detecting service failures and protecting vital revenue streams.

The HPE Unified OSS Console for Assurance Monitoring innovative Dashboard Engine is one of the key reasons and stands apart in the industry. Those real-time, highly configurable dashboards provide a crystal clear view of the health, performance and availability of mission critical services, networks, and applications, enabling OSS teams to manage and respond to business change as it happens.

HPE Unified OSS Console Assurance Monitoring dashboard power is supercharged by our software's ability to draw and display aggregated information from a variety of technologies, platforms and vendors, providing with a consolidated and total view of key information from many sources including faults, key performance and quality indicators (KPIs / KQIs), and service level agreements (SLAs). Dashboards are easy to configure, quick to deploy and simple to use thanks to our View Designer drag-and-drop capabilities.

HP Unified OSS Console Software dashboards are 100 percent web-based and instantaneously available from any PC location or browser-enabled device.

The solution is composed of different software components contributing to a flexible and scalable architecture addressing collection and display of large amount of information, delivered to a large number of connected web clients:

- It brings together **ready-to-use solutions** with an **open & flexible** WEB UI foundation
- It is a fully converged Assurance solution across **Advanced NOC & SOC real-time monitoring** and **OSS Analytics** use cases
- It delivers **integrated views** across the different systems which support the business processes
- It provides **one place** to visualize key data and operate traditional and virtualized networks and services
- It is user focused, easy to **personalize, adapt & extent** by design
- It allows modifying and creating new views in a few clicks with the **View Designer**
- It provides a **unified security model,** shared by integrated applications
- It brings high **modularity** for gradual integration & transformation
- It is powered by an **innovative & responsive** WEB UI foundation

Three main components are part of the solution

- **The HPE Unified OSS Console Foundation (UOC Foundation)** provides with a set of GUI core features for
  - Page design and visualization
  - Security & roles
  - Localization, internationalization

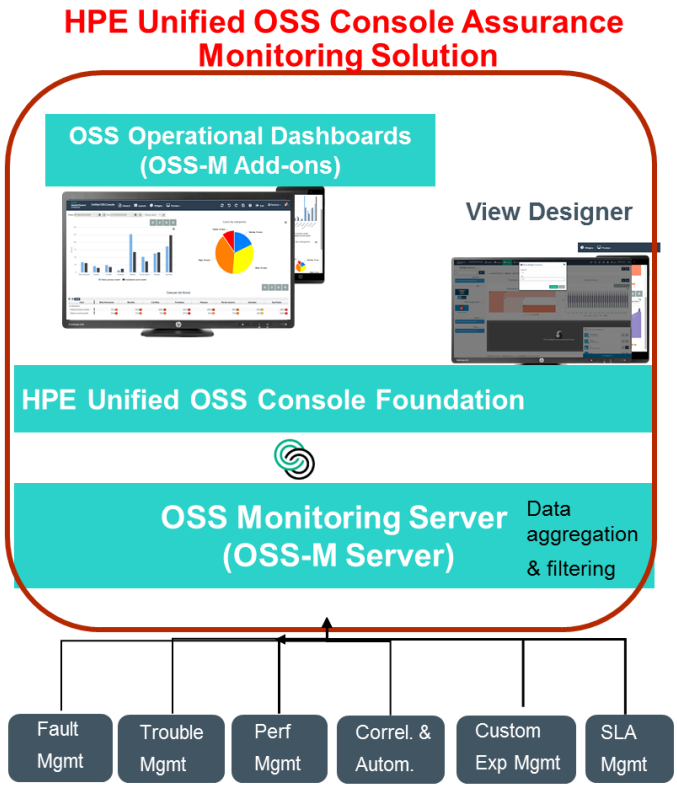
  The architecture of the UI foundation supports large and distributed environments (load balancing).
  The Foundation also provides a **View Designer** allowing administrators and end users to configure their own dashboard pages.

- **The HPE Unified OSS Console OSS Monitoring Server (OSS-M Server)** provides the data collection layer which interfaces with the different OSS Assurance Application (Fault, Performance, Trouble Management, Customer Experience…) to extract, aggregate and compute the data which will be displayed in the dedicated real-time operational views.

- **The HPE Unified OSS Console Monitoring Add-On (OSS-M Add-On)** is a set of preconfigured OSS Assurance Real-Time dashboards which can be the starting point for the deployment of an OSS Assurance solution, and can be further extended by new dashboards views, using the View Designer provided by the solution.

The following picture illustrates how the different components are positioned into the Unified OSS Assurance Monitoring Solution.

Please refer to the different Component User Documentations to install and configure properly the solution.



2.2 Solution Architecture and Security guidelines

2.2.1 Introduction to Hardening

This chapter introduces the concept of a secure HPE Unified OSS Console Solution platform within an entire OSS deployment and discusses the planning and architecture required to implement a secure solution. It is strongly recommended that you read this chapter before proceeding to the following chapters, which describe the actual hardening procedures.

The HPE Unified OSS Console is designed so that it can be part of a secure architecture, and can therefore meet the challenge of dealing with the security threats to which it could potentially be exposed.

The hardening guidelines deal with the configuration required to implement a more secure (hardened) Unified OSS Console platform. The hardening guidelines relate to a distributed deployment of a Unified OSS Console solution as part of an overall OSS Solution.

The hardening information provided is intended primarily for HPE Unified OSS Console architects and administrators, and for the technical operator of each component that is involved in the implementation of a secure Unified OSS Console platform. These people should familiarize themselves with the hardening settings and recommendations prior to beginning the hardening procedures.

To best use the hardening guidelines given here for your particular organization, you should do the following before starting the hardening procedures:

- Evaluate the security risk/security state for your general network, and use the conclusions when deciding how to best integrate the Unified OSS Console solution inside your overall OSS solution into your network.
- Review all the hardening guidelines.

A good understanding of the Unified OSS Console architecture and security capabilities will facilitate designing a solid plan for implementing a secure architecture.

The hardening information provided in this document is not intended as a guide to making a security risk assessment for your computerized systems.

2.2.2 Deploying Unified OSS Console in a secure architecture

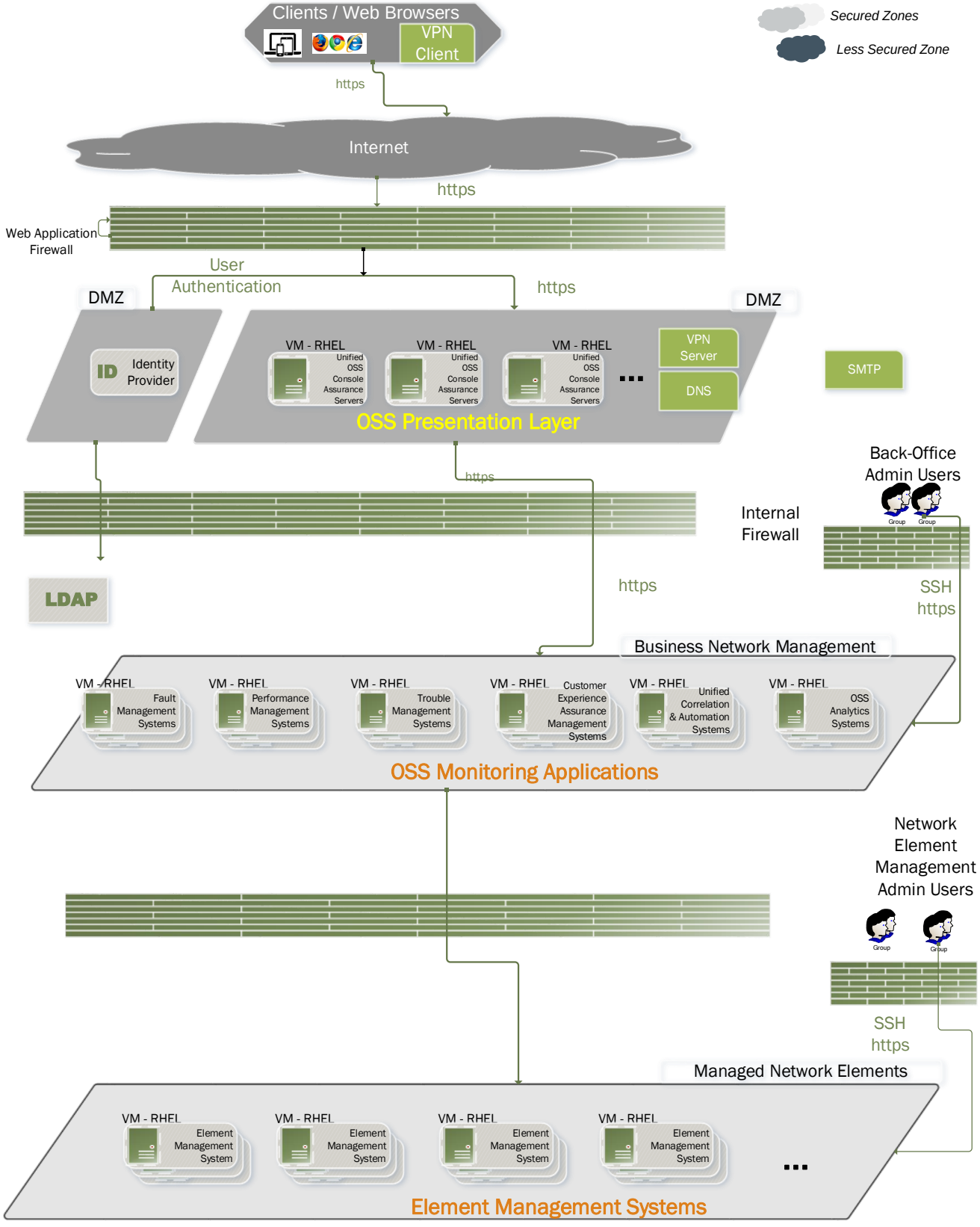
Similar to other software solutions, HPE Unified OSS Console is deployed in a computing and networking environment composed of Virtual or Physical Linux servers, linked together by a computing network which needs to be secured before the HPE Unified OSS Console solution is deployed.

The set of hardware servers with Linux operating system, virtualization middleware, and application servers must be configured with all security mechanisms and deployed inside the customer LAN which should be protected by firewalls, before the HPE Unified OSS Console solution is deployed.

Establishing a complete set of HW, O/S and computer networking security configuration is not within the scope of the HPE Unified OSS Console product user guide for installation. Security of the deployment environment must be ensured by skilled personnel, either from the Customer technical staff or the project delivery responsible, depending on the project deployment statement of work, and following the Customer's security best practices and guidelines.

The following figure illustrates a typical HPE Unified OSS Console deployment and the positioning of the main security aspects to be considered.

Figure 1: HPE Unified OSS Console recommended architecture



The above solution architecture depict a large scale OSS Assurance environment.

In some cases, some customers will implement a simpler architecture, removing internal firewalls between the OSS Assurance Monitoring systems and Element Management systems.

Customer is responsible for restricting the web application firewall (network and firewall is protected from DoS attacks)

- Secure browser

Web browsers must be configured to securely handle Java scripts, applets and cookies…

- SSL communication protocol

Secure Sockets Layer protocol secures the connection between the client and the server. Unified OSS Console URL requires an SSL connection with HTTPS instead of HTTP.

- VPN appliance

Further secure the connection to the web application with a VPN setup between the client desktop or mobile devices and the Unified OSS Console server (in addition to HTTPS configuration).

- DMZ (Demilitarized Zone)

DMZ (Demilitarized Zone) is a network architecture in which an additional network is implemented, enabling to isolate the internal network from the external one.

The following security objectives can be achieved by using DMZ proxy HTTPS communication with Unified OSS Console:

  - No OSS Solution processing resides on the DMZ. All the OSS Monitoring servers (TeMIP Fault Management, Unified Correlation Analyzer…) are sitting in customer intranet protected by an internal firewall from the DMZ.
  - No direct communication between Unified OSS Console clients and servers is permitted.
  - No direct connection from the DMZ to the other OSS Solution components is required.
  - The protocol used to communicate between Client applications and Unified OSS Console Server is HTTPS.
  - A VPN appliance allows to further secure the client communication with the server.
  - The user authentication is done through a secured user authentication using Single Sign On.

When the deployment environment has been set up with the right security level, the HPE Unified OSS Console security features must be configured for deployment into production to benefit from the highest levels of security supported by the HPE Unified OSS Console solution. This includes configuring the HPE Unified OSS to secure the communications between the client and the HPE Unified OSS Console server as well as all other communication paths between the HPE Unified OSS Console server, the domain data servers and the HPE Unified OSS Console assets (files and data bases).

2.2.3 Recommended Security Best practices

To best use the security guidelines given here for your particular organization, you should do the following before starting your deployment

1. Evaluate the security risk/security state of the computing and network environment where you are going to deploy HPE Unified OSS Console, and use the conclusions when deciding how to best integrate the HPE Unified OSS Console into your network.
2. Review all the security HPE Unified OSS Console guidelines: a good understanding of HPE Unified OSS Console security capabilities will facilitate designing a solid plan to deploy a secure HPE Unified OSS Console solution

NOTE: the security information provided in this chapter is not intended as a guide to making a security risk assessment for your computerized systems. Should you require a risk assessment for your computer and networking environment, HP Enterprise security solutions has a comprehensive offer covering Managed Security Services and Security Consulting. Contact your HPE Sales Representative to know more.

The following table comprises a list of security best practices that HPE recommends in the computing and networking environment. This list is provided for information and does replace a security risk assessment guide as mentioned above.

Topic	Best Practice
Accounts	Limit the number of local accounts. Integrate the appliance with your enterprise Identity Provider solution and set them the correct level of rights. Manage the user accounts proactively (forced password renewal, forced password complexity, disabling and deleting obsolete users accounts) Several anonymous users are created like uoc and couchdb. To avoid an attacker to exploit component vulnerabilities, it is recommended to set the minimal privileges to these accounts. A Unix administrator can define limited-privilege roles and associated these roles to users in charge of their administration (http load balancer, Apache CouchDB, uoc, Domain data server(s)…)
Passwords	Change the local HPE Unified OSS Console accounts passwords periodically, according to your password policies. Ensure that passwords are long enough and include at least three of these types of characters: ◦ Numeric character ◦ Lowercase alphabetic character ◦ Uppercase alphabetic character ◦ Special character
System management & auditing	Perform regular O/S patch updates Install & regularly update antivirus engines and software Monitor actively the systems logs, audit files and anti-virus logs to detect any abnormalities Protect key assets such as file systems, databases & storage
Nonessential services	Remove or disable nonessential services in the management environment. Ensure that you continue to minimize services when you configure HPE Unified OSS Console systems and domain specific servers systems (including network ports not in use) to significantly reduce the number of ways your environment could be attacked. Regarding Red Hat Linux Operating system, follow the Red Hat O/S security recommendations (https://access.redhat.com/) such as Security guides, patches, recommended updates, hardening recommendations.
Proactive reviews and updates to security features and patches	Ensure that a process is in place to pro-actively and periodically determine if software, firmware & security updates are available. Install updates for all components in your environment on a regular basis. • Subscribe to the HPE security bulletin as described in the related section later on in this document

	• Subscribe to receiving email notifications of security and enhancement updates advised on the Red Hat Customer Portal https://access.redhat.com/security/ • Consider subscribing to a vulnerability & exposure site (such as the Common Vulnerabilities and Exposures official site)
Network	HPE recommends a strict separation of the management LAN and production LAN, using VLAN or firewall technology (or both) to maintain the separation. Please refer to HPE Unified OSS Console deployment section. Grant management LAN access to authorized personnel only: Infrastructure administrators, Network administrators, and Server administrators. Disable SSH ports Review the TLS (SSL) configuration (ciphers and algorithms) and configure TSL to provide communications security over the network. Do not connect any management systems, inclusive of HPE Unified OSS Console directly to the Internet. If users from your internal organization require to access HPE Unified OSS Console (or other management functionality) to the Internet, use a corporate VPN (virtual private network) that provides firewall protection. If the HPE Unified OSS Console deployment requires that HPE Unified OSS Console functionality is exposed to external parties like Tenants, follow the additional security guidelines for these cases (see relevant section further in the document) If connected on the internet then use this site for a good test (https://www.ssllabs.com/ssltest/), get permission before running the test. Regularly monitor network traffic for suspicious activity
Certificates	Use certificates signed by a trusted certificate authority (CA) to ensure the integrity and authenticity of your HTTPS connections. • between users' browsers and HPE Unified OSS Console server(s) • between HPE Unified OSS Console server(s) and domain specific servers, • between HPE Unified OSS Console server(s) and the GUI Database (Apache CouchDB) • between users' browsers and the Identity Provider (SAML based) Ideally, you should use your company's existing CA and import their trusted certificates. The trusted root CA certificate should be deployed to user's browsers that will contact systems and devices that will need to perform certificate validation.
Accidental actions and other events	Implement systematic backup policy. Employ qualified, skilled, and trained staff Use in-house resources for administration. Secure infrastructure from fire, flood, earthquake, and have disaster recovery plans
Turn on HPE Unified OSS Console security features	Configure all HPE Unified OSS Console security features as described in this document.
Private data	Note that the HPE Unified OSS Console platform alone does not store private data. In the context of an UOC solution, it is the domain specific server(s)

	integrated as part of the end to end solution which may process, store and expose private data through its integration to HPE Unified OSS Console. Make sure that if any domain specific server which is part of the end to end solution processes, exposes and/or store private data is properly configured from a privacy standpoint and that all security capabilities of the Unified OSS Console are configured securely when such data is exposed by through the Unified OSS Console.

2.2.4 Operating System hardening

The HPE Unified OSS Console Assurance Monitoring server resources are running on Virtual or Physical Linux servers which are under the responsibility of the customer or the deployment team, inside a Customer LAN protected by a Firewall.

Information in the subsequent paragraphs regarding HW, O/S and computer networking security are indicative guidelines which should be reviewed, approved and complemented by an IT security expert from the Customer and/or project delivery team. Note that HP Enterprise allows customers subscribe to a security bulletin as outlined in a subsequent section.

Securing the deployments environment addresses several aspects

1. Securing the Operating system: this consists in configuring the Operating system security in order to ensure OS integrity, confidentiality and availability and protect the OS from threats, viruses, worms, and malware or remote hacker intrusions.

   Beyond using the Linux Operating system version recommended in the HPE Unified OSS Console Installation, it is recommended to follow the Red Hat O/S security recommendations (https://access.redhat.com/) such as Security guides, patches, recommended updates, hardening recommendations. Over time, it is highly recommended to pro-actively review & update the O/S security features, possibly through subscribing to receiving email notifications of security and enhancement updates as advised on the Red Hat Customer Portal https://access.redhat.com/security/

2. System management & system auditing
   a. Performing regular O/S patch updates
   b. Installing updated antivirus engines and software
   c. Monitoring actively the systems logs, audit files and anti-virus logs to detect any abnormalities
   d. Protecting key assets such as file system, databases & storage
3. System hardening to eliminate as many security risks as possible. Note that HPE Unified OSS Console solution has been tested and can run with hardened versions of RedHat 5.x or 6.x with SElinux enabled. Please refer to the related section further in this chapter.
4. Securing the network and communications between the systems and with the external world
   a. Scrutinizing all incoming and outgoing network traffic through firewalls
   b. Regularly monitor network traffic for suspicious activity
   c. Configuring TSL to provide communications security over the network
   d. Disabling SSH ports
5. Manage the system users
   a. Deploying secured user authentication with Single Sign on

b. Managing systems users & accounts securely, by creating secure, named accounts with required privileges only, managing the user accounts proactively (forced password renewal, forced password complexity, disabling and deleting obsolete users accounts)

c. Encrypt passwords when transported between systems & stored in a DB

HPE Unified OSS Console solution nodes is delivered with or tested on hardened version of RedHat 5.x or 6.x with SElinux enabled.

The RedHat Enterprise Linux CIS-CAT security benchmark is run after the products are installed, to measure the information security status. The CIS-CAT results can be shared, if required, under NDA.

The Linux OS hardening includes the following components:

- Minimal list of RPM packages installed on the system.
- Minimal list of groups enabled on the system.
- Minimal list of user accounts configured on the system.
- Minimal list of services activated on the system.
- A secure login set-up.
- Password and user account security enforcements.
- Restricted user access and controls.
- Restricted physical access controls.
- System logging.
- Use of grub boot loader.
- Predefined file system and logical volume layout.
- NTP configuration.
- Disabling excess snmpd logs.
- File system access-related settings.
- System inactivity timeout enforcement.
- TCP/IP configuration enforcements.

The HPE Unified OSS Console software must run with non-root Linux OS privileges and are administered by non-root users.

The operating system must be regularly updated with security patches: level to be agreed on with customer.

Regular checks of OS and application audit logs must be performed to detect non-authorized access.

High Availability / Load balancing deployment model

To further minimize security risks and business disruption, the Unified OSS Console platform can be deployed redundantly so that high availability of solution components is guaranteed.

2.2.5 HP Enterprise Security Bulletin

HP Enterprise has a well-defined process when a security defect is found that culminates with the publication of a security bulletin. The security bulletin provides you with a high level description of the problem and explains how to mitigate the security defect.

Procedure for Subscribing to Security Bulletins

1. Open a browser to go to the HPE Updates page

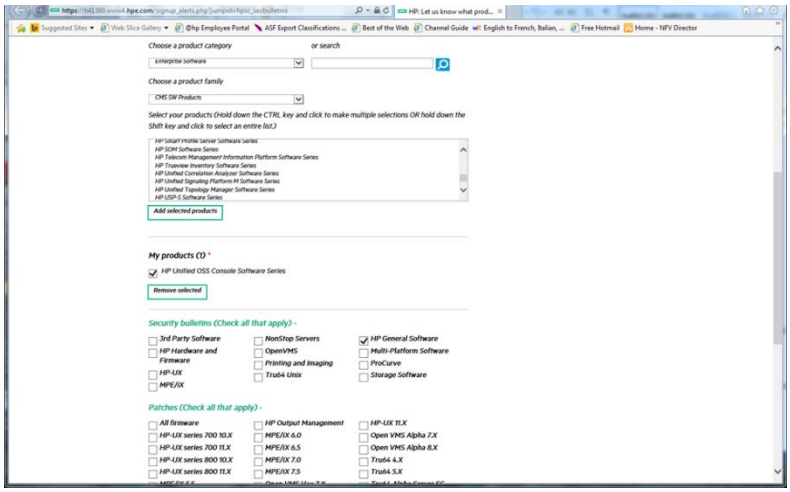
https://h41360.www4.hpe.com/signup_alerts.php?jumpid=hpsc_secbulletins

2. Do one of the following:
   - Sign in if you are a registered customer.
   - Enter your email address to sign-up now.

3. Select the following fields
   Product Category: Enterprise Software
   Product Family: CMS SW Products
   Select your product(s) – For HPE Unified OSS Console, select " HP Unified OSS Console Software Series"

4. Select subscription
   - select the relevant security bulleting you want to subscribe to (HP General Software and Multi-Platform Software)
   - select OS "patches" if relevant to your solution

5. Click "Subscribe"



Chapter 2
Installation

2.1 Prerequisites

2.1.1 Hardware

The table below lists the minimum hardware requirements for a OSSM server installation. Appropriate sizing is of course subject to real volume of data or throughput and is therefore subject to specific adaptations.

	Minimal	Optimum
CPU	Dual-Core 2 1.6GB Processor	8 Cores
Memory Size	8GB	64GB
Hard Disk Size	10GB	10GB (only configuration data is stored on disk)
Network	100MB Ethernet	100MB Ethernet

Table 4. Hardware requirements for an OSSM Server.

TIP: For large volume of data loading, it is recommended to tune these values to optimize the performance of the system.

2.1.2 OS and Java

The OSSM Server V2.2.0 software is officially supported only on Red Hat Enterprise Linux 5.x or 6.x X86-64 Systems

You can check the installed OS version of your server with the following commands:

```
$ lsb_release -id
```

or

```
$ cat /etc/issue
```

A java JDK 1.7 is necessary for running OSSM processes.

You can check which JDK version is present on your system with the following commands:

```
$ rpm -qa | grep jdk
```

or

```
$ javac -version
```

2.1.3 Environment

The environment variable JAVA_HOME must be set correctly, with the path to the JDK.

```
$JAVA_HOME/bin/java -version
```

A “uoc” user must be created on the system (this step is optional, but recommended, especially to avoided warnings during an installation without root privileges).

```
# useradd -m uoc
```

Don’t forget to change its password.

```
# passwd uoc
```

2.2 Installation Locations

The OSSM server can be installed anywhere on disk. The installation is split in 2 separate folders: $OSSM_HOME and $OSSM_DATA. These two locations can be freely chosen during the installation process.

The OSSM_HOME directory contains the binary files like java libraries (jars), executable or sample data files. These “product” files are read-only (with very limited exceptions). These files can typically be replaced by newer versions during a software upgrade. Likewise, the uninstallation procedure can potentially remove all these files, and therefore all changes done on them can be lost during a software upgrade.

On the other hand, the $OSSM_DATA directory contains configurations files or user data files. These files can be preserved during a software upgrade. They can usually be edited by users (either directly or through a graphical designer which generates the file). It is also a good idea to backup them regularly. For the OSS console, the $OSSM_DATA location contains typically the views definitions, filters, user profiles, etc…

The $OSSM_HOME and $OSSM_DATA directories must be different.

The default values are respectively: /opt/OSSM and /var/opt/OSSM. Using these default values generally requires **root privileges**.

2.2.1 OSSM Server component list

```
RMI Registry
ActiveMQ 5.9.0
 LICENSE_MAN
 ARRIVAL
 CONF MAN
 CSV ADAPTER
NOM TEMIP ADAPTER
 QC_PROVIDER
 TRANSFORMER
 RECEIVER
 H2SERVER
Tomcat 7.0.64
```

2.3 Installation Steps

The OSS Console comes in a standard tar file.

```
uoc-server-ossm-2.2.0-linux.tar
```

Unpack the archive in a temporary directory of your choice:

```
$ tar -xvf uoc-server-ossm-2.2.0-linux.tar


OSSMSERVER-V2.2-01A.noarch.rpm
install-ossm-server.sh
licenses/LICENSE-ojdbc.txt
licenses/LICENSE-Vertica.txt
```

Then the installation procedure differs slightly, depending on which user is performing it, and the desired target installation locations.

Generally, Linux packages require root credentials to be installed on the system. The package is registered in the central package database, and the software is made available to anyone. This is also the default approach for installing OSSM.

However, regular users can also install the OSSM server if they want too (for testing or simply if do not have root access). In this case, the rpm packages won't be visible in the central package database. Users will have to remember where the kit is installed. This can however be automated by adding the OSSM environment setup in their profile (see below).

Several OSSM installations can cohabit on the same system. However, running different instances at the same time is not possible.

2.3.1 Standard Installation (with root credentials)

If you have root access on your server, it's easier to stick to default locations and settings.

In this case, all installed files will be owned by the "uoc" user created previously (see the pre-requisites section).

To install the UOC as root, execute the following command:

```
# ./install-ossm-server.sh

Installing the HP OSS Console server package using OSSM_HOME=/opt/OSSM and
OSSM_DATA=/var/opt/OSSM:
-------------------------------------------------------------------------------

The OSSM product delivers the Oracle JDBC driver.
To be able to use it, you must accept the Oracle license terms.
Please read the license terms from the file ./licenses/LICENSE-ojdbc.txt
Please read carefully the content of the specific file.
Answer "Y" to the question if you accept the license terms.
Answer "N" to quit the installation wizard.
    Do you accept the license terms? [Y]

Y
The installation will continue!
Preparing...                ########################################### [100%]
   1:OSSMSERVER              ########################################### [100%]
        creating /var/opt/OSSM
        creating /var/opt/OSSM/conf
```

```
        creating /var/opt/OSSM/data
        creating /var/opt/OSSM/data/snapshot
        creating /var/opt/OSSM/data/cmstore/
        creating /var/opt/OSSM/data/cmstore/custfile
        creating /var/opt/OSSM/data/cmstore/dimension
        creating /var/opt/OSSM/data/cmstore/filter
        creating /var/opt/OSSM/data/cmstore/group
        creating /var/opt/OSSM/data/cmstore/locks
        creating /var/opt/OSSM/data/cmstore/pivot
        creating /var/opt/OSSM/data/cmstore/role
        creating /var/opt/OSSM/data/cmstore/snap
        creating /var/opt/OSSM/data/cmstore/user
        creating /var/opt/OSSM/data/cmstore/viewtype
        creating /var/opt/OSSM/data/cmstore/transformer
        creating /var/opt/OSSM/data/cmstore/nocmap
        creating /var/opt/OSSM/logs
        creating /var/opt/OSSM/tmp
        creating /var/opt/OSSM/topology_maps
        creating /var/opt/OSSM/topology_maps/images
        creating /var/opt/OSSM/adapters
        creating /var/opt/OSSM/adapters/nom_temip
        creating /var/opt/OSSM/adapters/nom_temip/resources
        creating /var/opt/OSSM/adapters/nom_temip/resources/META-INF
        creating /var/opt/OSSM/adapters/nom_temip/resources/META-INF/spring
        copying demo data files
        copying temip data files
        copying custom data files
        copying csv, db adapters configuration files
        copying topology maps images
OSSM server package installed successfully.
Source the file /opt/OSSM/.environment.sh to set environment variables related
to your new installation.
Edit the file /var/opt/OSSM/conf/application.conf for TeMIP configuration details
.
Bye.
```

You must accept the Oracle ODBC and Vertica licenses terms before proceeding with the installation.

Don’t try to install the rpm package by yourself, as the installation script does quite a lot of configuration under the hood, in particular for managing the split between the OSSM_HOME and OSSM_DATA parts.

It is also recommended to use the “uoc” user to start or stop the Console server, or to edit the configuration files. For this, source the $OSSM_HOME/.environment.sh from the uoc user profile setup script. This will set in particular the OSSM_HOME and OSSM_DATA environment variables to the correct values and update the PATH to locate the uoc command.

```
# echo ''. /opt/OSSM/.environment.sh'' >> /home/uoc/.bash_profile
# su - uoc
$ which ossm
/opt/OSSM/bin/ossm
```

TIP: On RHEL 5.x, you may see a warning message during the installation like: “error: can't create transaction lock on /tmp/OSSM_HOME/rpm/__db.000”.

You may safely disregard this message.

2.3.2 Regular User Installation

It is sometimes convenient to install the OSSM server as a regular user. In such a case, use the "-t" option as follows:

```
$ ./install-ossm-server.sh -t -r /tmp/OSSM_HOME -d /tmp/OSSM_DATA


Using local rpm db in /tmp/OSSM_HOME/rpm
Installing the HP OSS Console server package using OSSM_HOME=/tmp/OSSM_HOME and
OSSM_DATA=/tmp/OSSM_DATA:
-------------------------------------------------------------
The OSSM Server product delivers the Oracle and Vertica JDBC drivers.
To be able to use them, you must accept the Oracle and Vertica licenses terms.
Please read the Oracle licenses terms from the file ./licenses/LICENSE-ojdbc.txt.
Please read the Vertica licenses terms from the file ./licenses/LICENSE-
Vertica.txt.
Answer "Y" to the question if you accept the license terms.
Answer "N" to quit the installation wizard.
    Do you accept the license terms? [Y]
Y
The installation will continue!
Preparing...                ########################################### [100%]
   1:OSSMSERVER              ########################################### [100%]
        creating /tmp/OSSM_DATA
        creating /tmp/OSSM_DATA/conf
        creating /tmp/OSSM_DATA/data
        creating /tmp/OSSM_DATA/data/snapshot
        creating /tmp/OSSM_DATA/data/cmstore/
        creating /tmp/OSSM_DATA/data/cmstore/custfile
        creating /tmp/OSSM_DATA/data/cmstore/dimension
        creating /tmp/OSSM_DATA/data/cmstore/filter
        creating /tmp/OSSM_DATA/data/cmstore/group
        creating /tmp/OSSM_DATA/data/cmstore/locks
        creating /tmp/OSSM_DATA/data/cmstore/pivot
        creating /tmp/OSSM_DATA/data/cmstore/role
        creating /tmp/OSSM_DATA/data/cmstore/snap
        creating /tmp/OSSM_DATA/data/cmstore/user
        creating /tmp/OSSM_DATA/data/cmstore/viewtype
        creating /tmp/OSSM_DATA/data/cmstore/transformer
        creating /tmp/OSSM_DATA/data/cmstore/nocmap
        creating /tmp/OSSM_DATA/logs
        creating /tmp/OSSM_DATA/tmp
        creating /tmp/OSSM_DATA/topology_maps
        creating /tmp/OSSM_DATA/topology_maps/images
        creating /tmp/OSSM_DATA/adapters
        creating /tmp/OSSM_DATA/adapters/nom_temip
        creating /tmp/OSSM_DATA/adapters/nom_temip/resources
        creating /tmp/OSSM_DATA/adapters/nom_temip/resources/META-INF
        creating /tmp/OSSM_DATA/adapters/nom_temip/resources/META-INF/spring
        copying demo data files
        copying temip data files
        copying custom data files
        copying csv, db adapters configuration files
        copying topology maps images
OSSM server package installed successfully.
Source the file /tmp/OSSM_HOME/.environment.sh to set environment variables
related to your new installation.
Edit the file /tmp/OSSM_DATA/conf/application.conf for TeMIP configuration
details.
Bye.
```

The “-t” option is generally used in conjunction with the “-r” (for “root” or home directory) and “-d” (for “data” directory) options, as regular users probably do not have permissions to create folders in the default /opt or /var/opt locations.

Like in the previous case, it is recommended to source the $OSSM_HOME/.environment.sh script in your user profile.

```
$ echo ‘‘/tmp/OSSM_HOME/.environment.sh’’ >> ~/.bash_profile
```

This will update the path with the OSSM commands and set the required environment variables for administrating the OSSM server.

2.3.3 Alternate Installations

Several installation combinations are possible. The installation script has a –h option (for help) that describes the other various options available:

```
$ ./install-ossm-server.sh -h

Usage:

    install-ossm-server.sh [-h] [-t] [-u] [-r root directory]  [-d data directory]
[--dbpath rpm db path]


 -r DIRECTORY : use an alternate OSSM OSSM_HOME root Directory (default is
/opt/OSSM)


 -d DIRECTORY : use an alternate OSSM OSSM_DATA data directory (default is
/var/opt/OSSM)


 -u : installed files will be owned by the user executing this script instead of
the uoc user. When used with the --dbpath option, this lets install OSSM server
without root credentials. This -u option generally requires also the -r and -d
ones, as the default user may not have permissions to create the default /opt/OSSM
or /var/opt/OSSM directories.


 --dbpath DIRECTORY : use an alternate rpm database (default is /var/lib/rpm).
This is useful to install OSSM server without root credentials. You have to
remember the value provided here to be able to track the installed packages or
remove them later on. A typical value can be ~/lib/rpm. The rpm database can also
be located in . If so, consider the -t option which sets the rpm database to /rpm
automatically.


 -t : means -u and --dbpath /rpm at the same time. This overrides the -u or --
dbpath options if provided.


 -h displays this usage message


EXAMPLES:


      install-ossm-server.sh
```

```
      This uses the default values and must be executed by root. All files
installed in /opt/OSSM and /var/opt/OSSM will be owned by uoc.


      install-ossm-server.sh -t -r /tmp/OSSM_HOME -d /tmp/OSSM_DATA

      This installs OSSM with location OSSM_HOME=/tmp/OSSM_HOME and
OSSM_DATA=/tmp/OSSM_DATA. The rpm db is /tmp/OSSM_HOME/rpm and all installed
files are owned by the current user.
```

2.4 Installation Verification

After installation, you can check what release is currently installed with the “ossm inventory” command.

```
$ ossm inventory


HP OSSM packages currently installed:


package                          summary
-------------------------------------------------------------------


OSSMSERVER-V2.2-01A              HPE OSS Assurance Monitoring Server Version V2.2
Level 01 Rev A
```

You can check the directories layout for $OSSM_HOME:

```
/opt/OSSM
|-- 3pps
|   |-- activemq -> /opt/OSSM/3pps/apache-activemq-5.9.0
|   |-- apache-activemq-5.9.0
|   |-- apache-tomcat-7.0.64
|   |-- apache-tomcat-7.0.64-custom
|   |   |-- bin
|   |   |-- conf
|   |   `-- lib
|   |-- kits
|   `-- tomcat -> /opt/OSSM/3pps/apache-tomcat-7.0.64
|-- adapters
|   |-- csv
|   |   |-- bin
|   |   |-- conf
|   |   `-- lib
|   |-- db
|   |   |-- bin
|   |   |-- conf
|   |   `-- lib
|   |       `-- 3rd
|   |-- qc
|   |   |-- bin
|   |   |-- conf
|   |   `-- lib
|   `-- nom_temip
|       |-- bin
|       |-- lib
|       `-- resources
|-- bin
|-- conf
|-- data
|   `-- cmstore
```

```
|       |-- dimension
|       |-- group
|       |-- role
|       |-- user
|       `-- viewtype
|-- examples
|   |-- custom
|   |   |-- data
|   |   |   `-- cmstore
|   |   |       |-- custfile
|   |   |       |-- dimension
|   |   |       |-- group
|   |   |       |-- pivot
|   |   |       |-- role
|   |   |       |-- user
|   |   |       `-- viewtype
|   |   `-- data-samples
|   |       |-- alarm
|   |       `-- h2
|   |-- demo
|   |   |-- data
|   |   |   `-- cmstore
|   |   |       |-- custfile
|   |   |       |-- dimension
|   |   |       |-- filter
|   |   |       |-- group
|   |   |       |-- nocmap
|   |   |       |   |-- CEA
|   |   |       |   |   |-- XML
|   |   |       |   |   `-- bg_image
|   |   |       |   |-- France
|   |   |       |   |   |-- XML
|   |   |       |   |   `-- bg_image
|   |   |       |   `-- India
|   |   |       |       |-- XML
|   |   |       |       `-- bg_image
|   |   |       |-- pivot
|   |   |       |-- role
|   |   |       |-- transformer
|   |   |       |-- user
|   |   |       `-- viewtype
|   |   `-- data-samples
|   |       |-- SiteMonitoring
|   |       |-- TTMonitoring
|   |       |-- cea
|   |       |-- gsm_topo_map
|   |       |   `-- sample-transformer
|   |       |       |-- lib
|   |       |       `-- src
|   |       |           `-- com
|   |       |               `-- hp
|   |       |                   `-- uoc
|   |       |-- sample_views
|   |       `-- service_noc
|   |           |-- config
|   |           |   |-- CEA
|   |           |   |-- France
|   |           |   `-- India
|   |           |-- data
|   |           |   |-- CEA
|   |           |   |-- France
|   |           |   `-- India
|   |           `-- sample-transformer
```

```
|   |               |-- ServiceNocTransformer
|   |               |   |-- lib
|   |               |   `-- src
|   |               |       `-- com
|   |               |           `-- hp
|   |               |               `-- uoc
|   |               `-- lib
|   |   |-- data
```

You can also check the directories layout for $OSSM_DATA:

```
/var/opt/OSSM
|-- adapters
|   `-- nom_temip
|       `-- resources
|           `-- META-INF
|               `-- spring
|-- conf
|-- data
|   |-- cmstore
|   |   |-- custfile
|   |   |-- dimension
|   |   |-- filter
|   |   |-- group
|   |   |-- locks
|   |   |-- nocmap
|   |   |   |-- CEA
|   |   |   |   |-- XML
|   |   |   |   `-- bg_image
|   |   |   |-- France
|   |   |   |   |-- XML
|   |   |   |   `-- bg_image
|   |   |   `-- India
|   |   |       |-- XML
|   |   |       `-- bg_image
|   |   |-- pivot
|   |   |-- role
|   |   |-- snap
|   |   |-- transformer
|   |   |-- user
|   |   `-- viewtype
|   `-- snapshot
|-- logs
|-- tmp
`-- topology_maps
    `-- images
```

Chapter 3 Configuration

3.1 NOM TeMIP Adapter

3.1.1 Pre-requisites

To be able to monitor TeMIP through the OSS console, we assume that:

1. A TeMIP V6 server is installed and configured. If not, please refer to the "TeMIP Installation Guide for Linux" document.

2. TeMIP Web Services is installed and configured on this server (as the OSS console connects to TeMIP through web services). If not, please refer to the "TeMIP Web Services Installation and Administration Guide" document.

3. HP OSS Open mediation (NOM) is installed and configured on a server. If not, please refer to the "Open Mediation Installation and Configuration Guide" document.

4. HP OSS TeMIP Channel Adapter (TeMIP CA) is installed and configured on a server. If not, please refer to the "TeMIP CA Installation and Configuration Guide" document.

3.1.2 TeMIP Web Services Configuration

NOM TeMIP adapter supports both "security" and "no security" mode of TeMIP application.

By default the NOM TeMIP adapter is configured to support the "no security" mode.

3.1.2.1 Switch from "security" mode to a "no security" mode on TeMIP server

To change the TWS mode to "no security", perform the following **on the TeMIP server:**

```
# cd /var/opt/temip/TWS/tomcat/webapps/TeMIP_WS/WEB-INF/conf
# cp axis2.xml.nosecu axis2.xml
# manage ''restart mcc 0 app temip_web_services''
```

3.1.2.2 How to configuration NOM to support "security password clear" mode of TeMIP application

1. On TeMIP server the TWS axis2.xml file should be changed.

```
cd /var/opt/temip/TWS/tomcat/webapps/TeMIP_WS/WEB-INF/conf
cp axis2.xml.user_password_clear axis2.xml

manage restart mcc 0 appli temip_web_services
```

2. To allow the report of alarms to NOM, the axis2.xml file of NOM should be updated

```
cd /var/opt/openmediation-72/containers/instance-0/ips/temip-ca-22/etc/conf

Edit the axis2.xml file and add the ''UsernameToken'' string for items tag.
<action>
<items>UsernameToken</items>
```

```
        <passwordCallbackClass>com.hp.temip.temip_ws.common.pwcallback.PWCallba
ck</passwordCallbackClass>
<passwordType>PasswordText</passwordType>
```

3. Then, some other files should be updated in NOM to take into account directives.

```
cd /var/opt/openmediation-72/containers/instance-0/ips/temip-ca-22/etc


Edit the following files:
actions.to-temip.ao.request.xslt
actions.to-temip.tt.request.xslt
and add in each of them the following red lines:

<!-- Generic request -->
<!-- *************** -->

< xsl:template name="generic_request">

<xsl:param name="request_type" />

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
 xmlns:tt="http://tt_server.types.ws.temip.ov.hp.com">
<soapenv:Header>
<wsse:Security  xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-secext-1.0.xsd" soapenv:mustUnderstand="1">

<wsse:UsernameToken    xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="UsernameToken-43">

<wsse:Username>temip</wsse:Username>
<wsse:Password    Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
username-token-profile-1.0#PasswordText">TeMIP</wsse:Password>
</wsse:UsernameToken>
</wsse:Security>
<tt:InCallParams>
<xsl:if test="command/entry[key='SOAP_Handle']">
<tt:Handle><xsl:value-of
select="command/entry[key='SOAP_Handle']/value"/></tt:Handle>

</xsl:if>
<xsl:if test="command/entry[key='SOAP_Cancel']">

<tt:Cancel>
<xsl:value-of
select="command/entry[key='SOAP_Cancel']/value"/>
</tt:Cancel>
```

4. To finish, please restart NOM container

```
# nom_admin --shutdown-container
# nom_admin --start-container
```

5. Then restart or start the OSSM server.

```
$ ossm stop
$ ossm start
```

3.1.3 NOM Configuration

On the server where NOM and the TeMIP channel adapter have been installed check for connectivity details, the following configuration files (or equivalent depending on your NOM containers):

```
$cd /var/opt/openmediation-72/containers/instance-0/ips/temip-ca-22/etc/conf/
$ vi TeMIP_configuration.dynamic.xml
<Authentication>
   <UserName>temip</UserName>
   <Password>TeMIP</Password>
 </Authentication>
  <Axis>
   <RepositoryPath>conf/repository</RepositoryPath>
   <XmlPath>conf/axis2.xml</XmlPath>
  </Axis>
  <DirectorConfiguration>
   <MachineName>localhost</MachineName>
   <!--
    Put here TeMIP director name.
  If you leave this field as is, dynamic flows operations will not work
 -->
 <TeMIPDirectorEntity>.temip.vm1_temip</TeMIPDirectorEntity>
   <TWSServerPort>7180</TWSServerPort>
  </DirectorConfiguration>
```

MachineName is the system name where the TWS server is running.

TeMIPDirectorEntity should be the name of the TeMIP instance where to create collection services (“manage show temip *” displays the instance names).

```
$ cd /var/opt/openmediation-72/containers/instance-0/ips/temip-ca-22/etc/
$ vi actions-to-temip-jms-connector.xml
<endpoint id="tws"
uri="http:localhost:7180/TeMIP_WS/services/TEMIP?throwExceptionOnFailure=false&
bridgeEndpoint=true"/>
```

Replace localhost with the real TeMIP server name.

After changing these files, you need to restart NOM:

Assuming that the NOM container is default 0:

```
# nom_admin --shutdown-container
# nom_admin --start-container
```

TIP: For making these changes permanent, even in case of TeMIP CA un-deployement, please refer to the HPE OSS Open Mediation User Guide.

Note that on RHEL 6.x systems, NOM can conflict with webmin (for port 10000). You can:

1- Either stop webmin before starting NOM.

```
# /etc/webmin/stop
```

2- Or reconfigure OpenMediation network ports.

Please refer to the HPE OSS Open Mediation guide to know how to change port.

3.1.4 NOM TeMIP adapter configuration

If OSSM and the NOM TEMIP CA are installed on different servers you have to update some particular OSSM files. So, please edit and update the following files:

```
$ vi $OSSM_DATA/adapters/nom_temip/resources/camel-context.xml
<bean id="nomjms" class="org.apache.activemq.camel.component.ActiveMQComponent">
       <property name="brokerURL" value="tcp://localhost:10000"/>
</bean>
```

Replace above “localhost” by your NOM server name.

```
$ vi $OSSM_DATA/conf/application.conf
nom_temip_adapter {
    ca_name = "uoc-ca"
    nom_flow_name = "dynamic_flow_uoc"
     monitored_ocs = ["test_oc"]
     tt_server = "TT_SERVER .SM"
     scope = "NOT_CLOSED"
}
```

Replace “test_oc” by the list of Operation Context names you want to monitor with the OSS console. For example: [“demo_oc1”,”demo_oc2”,”demo_oc3”]

Make sure that all monitored OCs have the TeMIP “Emit Aggregate Event” attribute set to true, as this is the default for NOM.

The “tt_server” is the name of the Service Manager, if user wants to integrate the Service Manager with the OSSM, after the Service Manager is already integrated NOM, set the name of the Service Manager to this attribute.

The “scope” defines the shown alarms scope. The scope can be "NOT_CLOSED" or "NOT_TERMINATED". The default scope is "NOT_TERMINATED", means to display all the alarms that have not the state equals to "terminated" (which are acknowledged, outstanding). Another scope "NOT_CLOSED" means to display all the alarms that have not the problem status equals to Closed.

In some circumstances/configurations the request timeout timer of NOM may expired too early. This timer duration could be extended by modifying the camel-context.xml file (cf below):

```
$ edit $OSSM_DATA/adapters/nom_temip/resources/camel-context.xml
```

```
 Replace
<endpoint id="actionsToNom"
 uri="nomjms:topic:com.hp.openmediation.actions"/>
By
<endpoint id="actionsToNom"
 uri="nomjms:topic:com.hp.openmediation.actions?requestTimeout=30000"/>
```

Where 30000 means 30 seconds. The default value is 20000.

Then restart or start the OSSM server.

```
$ ossm stop
$ ossm start
```

3.1.5TeMIP data sample

TeMIP demo views are provided by default as examples in the OSSM server. To be able to use them out of the box, a set of sample data is also provided. TeMIP FCL scripts to generate alarms can be found in the $OSSM_HOME/examples/temip/data-samples directory.

- create_entities.cmd: this script can be used to create TeMIP entities.

```
$manage do create_entities.cmd
```

- send_alarms.cmd: this script can be used to send a burst of alarms.

```
$ manage do send_alarms.cmd
```

- Endurance/Loop_send_alarms.sh: this script can be used to simulate endless endurance.

```
$ Endurance/Loop_send_alarms.sh
```

- delete_entities.cmd: this script can be used to clean-up TeMIP Entities.

```
$ manage do delete_entities.cmd
```

TIP: The scripts must be executed on the TeMIP director. Alarms are created in OCs called demo_oc1, demo_oc2, demo_oc3, demo_oc4 and demo_oc5.

3.2 Firewall / Ports

It may happen that some TCP port numbers are already in use by other processes on the system. Here is how to change the ports used by tomcat and the rmi registry if necessary.

3.2.1Tomcat

The infamous default value is: 8080. A conflict may occur if another tomcat server is running on the same host.

To change this default value, edit the file:

$OSSM_HOME/3pps/tomcat/conf/server.xml, and change the following line:

```
<connector port=''8080'' protocol=''HTTP/1.1''
```

Replace 8080 by the desired value, like for example: 9090.

Note: if a new version of the OSSM Server is installed, you may have to perform this change again manually.

If this port number is modified, the default URL for the OSS console home page is changed accordingly. For example:

```
http://localhost:9090/uoc/auth/login.html
```

3.2.2 RMI registry

The default value is 1099. A port conflict may occur for example if NNM is installed on the same host as the OSSM server.

As the rmi registry is used for inter process communication, several files need to be updated.

In $OSSM_DATA/conf, change the following files (to choose port number 2000 instead):

arrival.xml:

```
<server />
```

To:

```
<server rmi_port="2000" />
```

arrival_client.xml:

```
<server />
```

To:

```
<server rmi_port="2000" />
```

And

```
<client />
```

To:

```
<client rmi_port="2000" />
```

cm.xml:

```
<rmi_port>1099</rmi_port>
```

To:

```
<rmi_port>2000</rmi_port>
```

lcheck.xml:

```
<rmi_port>1099</rmi_port>
```

To:

```
<rmi_port>2000</rmi_port>
```

Finally, if you have modified the default RMI registry port, use the “-r” option when starting the OSSM server:

```
ossm -r 2000 start
```

3.2.2 Firewall settings

Netfilter is a host-based firewall for Linux operating systems. It is included as part of the Linux distribution and it is activated by default on RHEL6. This firewall is controlled by the program called iptables. Netfilter filtering takes place at the kernel level, before a program can even process the data from the network packet.

Therefore, when iptables is up and filtering packets, its settings should be modified in order to let OSSM work properly.

Let's suppose we have the default iptables configuration file.

```
# cat /etc/sysconfig/iptables


# Generated by iptables-save v1.4.7 on Wed Jan 29 15:46:33 2014
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [17238040:2593637303]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT

# Completed on Wed Jan 29 15:46:33 2014
```

On top of this, or on top of your current iptables settings, you will need to add filters to open ports used by OSSM server.

By default, 3 chains are used: INPUT, OUTPUT, FORWARD. Please refer to the Red Hat Linux guide for a better understanding of what a chain is and what the packet matching rules are, that apply within a chain.

Here we are going to create a new custom chain, used by INPUT, dedicated to control OSSM port, for example for the default instance.

Let's call it OSSM. To do so, you will need to:

Add 2 lines to define the OSSM chain

Add 1 line to open ports used by the OSSM default instance

Please make sure to specify the same port numbers as the ones defined in the $OSSM_HOME/3pps/tomcat/conf/server.xml file.

Please see below for an updated version of the configuration file (added lines are in **blue**):

```
# cat /etc/sysconfig/iptables


# Generated by iptables-save v1.4.7 on Wed Jan 29 15:46:33 2014
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [17238040:2593637303]
:OSSM - [0:0]
-A INPUT -j OSSM
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
-A OSSM -p tcp -m tcp --dport 8080 -m comment --comment "OSS Console GUI" -j
ACCEPT COMMIT

# Completed on Wed Jan 29 15:46:33 2014
```

Then, you need to validate your settings using the iptables command or the iptables service.

```
# service iptables restart


iptables: Flushing firewall rules:                                         [
OK  ]
iptables: Setting chains to policy ACCEPT: filter                          [
OK  ]
iptables: Unloading modules:                                               [
OK  ]
iptables: Applying firewall rules:                                         [
OK  ]
```

And then you need to check that your settings are up and running:

```
# iptables -list OSSM


Chain OSSM (1 references)
target       prot opt    source               destination
ACCEPT  tcp    --     anywhere          anywhere  tcp dpt:webcache /* OSS Console
GUI */
```

Of course, you may also disable the Linux kernel firewall, to prevent any additional system administration tasks.

3.3 OSSM License

License check module is an independent part can be integrated to OSSM. After installing OSSM, it will be deployed with the default configuration.

lcheck.xml

```
# vi $OSSM_DATA/conf/lcheck.xml


<?xml version="1.0" encoding="UTF-8"?>
<lcheck>
        <rmi_hostname>localhost</rmi_hostname>
        <rmi_port>1099</rmi_port>
</lcheck>
```

rmi_hostname : it is the RMI host name. The default value is “localhost”. It means it will use the same host as OSSM. If user changes it to other server means the license service will be deployed in another specific server.

Usually we should use the default configuration.

rmi_port : RMI port . Just like the RMI_REGISTRY . Usually we should use the default value.

License Files

```
# ls -l $OSSM_DATA/licenses
... data
... OSST_Unified_Console_LicKey.txt
... OSST_Unified_Console_PD_File_Master.bin
```

data folder: Some log information is recorded in this folder.

OSST_Unified_Console_LicKey.txt: All license keys should be in this file. For example:

HP Unif OSS Console 5Conc Viewers

9CDG B9MA H9PQ GHXY VWA5 HW25 29JL KMPL B89H MZVU DXAU 2CSM GHTG L762 RMW6 E4BE KJVT D5KM GFVW TSNJ QD3J 5RW8 BNTM 9GW6 Q9S5 HXLZ VW69 95VL LYTK X7EQ FL73 PN3G 4WVD YDUS NWS2 XD9S 5YNP FST7 NKCY H4SP 4MJ9 AAEH EZWH 2E4X ENUU BGN5 S8CH K7DX E8TJ BGLF 29JK 69MC "MP_UOC_20140919 JK232FAE HP Unif OSS Console 5Conc Viewers E-LTU"

HP Unified OSS Console 5Conc Oper

ACTG A9MA H9PA 8HXZ U2A4 HW2F 29JL KMPL B89H MZVU DXAU 2CSM GHTG L762 7MG6 W3BE KJVT D5KM GFVW TSNJ QD3J 5RW8 BNTM 9GW6 Q9S5 HXLZ VW69 95VL LYTK X7EQ FL73 PN3G 4WVD YDUS NWS2 XD9S 5YNP FST7 NKCY H4SP 4MJ9 AAEH EZWH 2E4X ENUU BGN5 S8CH K7DX E8TJ BGLN 29JK 69MC "MP_UOC_20140919 JK234FAE HP Unified OSS Console 5Conc Oper E-LTU"

HP Unified OSS Console 1 Conc Edit

QCDA D9MA H9PA 8HU2 U2A4 HW2N Y9JL KMPL B89H MZVU DXAU 2CSM GHTG L762 PM82 V3BE KJVT D5KM EFVW TSNJ QD3J 5RW8 BNTM 9GW6 Q9S5 HXLZ VW69 95VL LYTK X7EQ FL73 PN3G 4WVD YDUS NWS2 XD9S 5YNP FST7 NKCY H4SP 4MJ9 AAEH EZWH 2E4X ENUU BGN5 S8CH K7DX E8TJ BGLV 29JK 69MC "MP_UOC_20140919 JK236FAE HP Unified OSS Console 1 Conc Edit E-LTU"

HP Unif OSS Console Data Coll Serv

9CLE C9MA H9PA GHU2 U2A4 HW2V Y9JL KMPL B89H MZVU DXAU 2CSM GHTG L762 JMG6 G4RE KJVT D5KM EFVW TSNJ YD3J 5RW8 BNTM 9GW6 Q9S5 HXLZ VW69 95VL LYTK X7EQ FL73 PN3G 4WVD YDUS NWS2 XD9S 5YNP FST7 NKCY H4SP 4MJ9 AAEH EZWH 2E4X ENUU BGN5 S8CH K7DX E8TJ BGLZ 29JK 69MC "MP_UOC_20140919 JK237FAE HP Unif OSS Console Data Coll Serv E-LTU"

HP Unif OSS Cons DataCol DR/Dev

AC3A B9MA H9PA GHX2 U2A4 HW2V Y9JL KMPL B89H MZVU DXAU 2CSM GHTG L762 RMG6 F4RE KJVT D5KM EFVW TSNJ YD3J 5RW8 BNTM 9GW6 Q9S5 HXLZ VW69 95VL LYTK X7EQ FL73 PN3G 4WVD YDUS NWS2 XD9S 5YNP FST7 NKCY H4SP 4MJ9 AAEH EZWH 2E4X ENUU BGN5 S8CH K7DX M8TJ BGLZ 29JK 69MC "MP_UOC_20140919 JK237FBE HP Unif OSS Cons DataCol DR/Dev E-LTU"

OSST_Unified_Console_PD_File_Master.bin: This is the core file for license check,it should not be modified.

After OSSM is started, user will see the license check process : "LICENSE_MAN" through "ossm show" command.

```
# ossm show
      PROCESS_NAME          PID          USER         CPU_TIME
-------------------------------------------------------------------------------
---------------------------------------
      RMI Registry          5314         uoc          00:00:02
      ActiveMQ 5.7.0        5341         uoc          00:00:14
      LICENSE_MAN           5365         uoc          00:00:05
      ARRIVAL               5379         uoc          00:00:05
      CONF_MAN              5394         uoc          00:00:13
      CSV_ADAPTER           5410         uoc          00:00:04
      DB_ADAPTER            5423         uoc          00:00:08
      NOM_TEMIP_ADAPTER     5439         uoc          00:00:23
      QC_PROVIDER           5454         uoc          00:00:05
      Tomcat 7.0.64         5483         uoc          00:00:51
```

"ossm lcheck" command is used to show the online user limitation value and list.

The command of lcheck can display the online user info.

cd $OSSM_HOME/bin

```
# ossm lcheck
-------------------------------------------------------
```

```
Capacity : 5


-------------------------------------------------------
Online List :


User Id    User Name   IP Address         Host Name
------------------------------------------------------------
  temip     temip         16.31.78.173  llorca1.emea.hpqcorp.net
  temip     temip         16.28.34.31      16.28.34.31
  temip     temip         16.31.78.173  llorca1.emea.hpqcorp.net
  admin     admin         16.17.178.6      16.17.178.6
```

Capacity value is 5 means the maximum online user number is five.

Online list has four properties, those are User Id, User Name, IP Address and Host Name. Sometimes, the hostname, which can't be obtained, is replaced by the IP Address.

Notice:

License check module can't check user offline if user quit OSSM system that have not logout by OSSM logout function. So it wills only listen the event of tomcat session timeout to handle user offline. And usually the timeout value is about 30 minutes. During this period, the online total value is inconsistent the really online user.

3.4 ActiveMQ 5.9 Web Control Password

If the user wants to login to the activeMQ web control page, the default user/password is admin/admin, if anyone wants to change it, please check the file jetty-realm.properties in the $OSSM_HOME/3pps/apache-activemq-5.9.0/conf.

Chapter 4 OSSM server

4.1 OSSM commands

The OSSM server side platform is managed by a central “ossm” command located in $OSSM_HOME/bin, and available in your PATH if you have followed the installation instructions.

You can display the command usage with the –h option:

```
# ossm -h


Usage:
    ossm [options] action

options:
  -s time :    change delay (in sec) between each started process (default is 2
sec)
  -r port :    change the port number used by the rmiregistry process at startup
           (default is 1099)
  -v:          set verbose mode
  -d:          set debug mode
  -h:          displays this usage message

actions:
  start:       start the OSS console server processes
  stop :       stop the OSS console server processes
  show :    show the OSS console server processes
  inventory:   list the currently installed OSSM packages
  diagnose:    search for potential errors in log files
  archive:  package log files into a folder named by current date
```

4.2 Start Server

You can start the OSSM server with the start command.

```
# ossm start


Starting OSSM processes (with OSSM_HOME=/opt/UOC and OSSM_DATA=/var/opt/UOC):
      rmiregistry

        activemq

        license mgt

        arrival

        cm

        csv adapter

        db adapter

        nom_temip adapter

        qc provider

        tomcat

        receiver
        db transformer
```

4.3 List Processes

To see what process are running, use the show command:

```
# ossm show


PROCESS_NAME            PID          USER            CPU_TIME
RMI Registry            5576         root            00:00:00
ActiveMQ 5.9.0          5624         root            00:00:05
LICENSE_MAN             5638         root            00:00:02
ARRIVAL                 5651         root            00:00:01
CONF_MAN                5670         root            00:00:06
CSV_ADAPTER             5701         root            00:00:05
DB_ADAPTER              5718         root            00:00:03
NOM_TEMIP_ADAPTER       5749         root            00:00:06
QC_PROVIDER             5768         root            00:00:02
RECEIVER                5852         root            00:00:06
Tomcat 7.0.64           5800         root            00:00:09
```

4.4 Access to the console

OSSM is a web-based application. When Tomcat and all other processes have been started successfully, user can use a web browser (IE, Firefox…) to access OSS Console GUI.

The default URL is similar to the following:

http://<OSSM server Ip>:<port>

Default port is 3000.

To log in, and have a look to all the demo sample views the username/password are admin/admin.

4.5 Stop server

To stop the OSSM server, use the stop command:

```
# ossm stop
Stopping OSSM processes:
        5800 - tomcat
        5701 - CSV_ADAPTER
        5718 - DB_ADAPTER
        5749 - NOM_TEMIP_ADAPTER
        5768 - QC_PROVIDER
        5670 - CONF_MAN
        5651 - ARRIVAL
        5638 - LICENSE_MAN
        5852 - RECEIVER
        5624 - activemq
        5576 - rmiregistry
```

Chapter 5 Advanced Configuration

5.1 TeMIP Custom AO Support

5.1.1 Standard TeMIP attributes management

Currently, some standard attributes of TeMIP alarms are not received in the OSSM due to some naming mismatch in the chain from TeMIP to OSSM. Some names seen in mcc_dap_browser are not consistent with what is returned by TWS.

Example of such standard attributes that are not consistent:

"Creation Timestamp" encoded by TWS "Creation_Time" in the event.

It is encoded "Creation_Timestamp" in summarize directive.

"Problem Occurrences" is encoded by TWS "Problem_Occurrence".

To cope with this issue, some modifications should be done both on TeMIP side and NOM side as described below.

Please follow the steps below to handle correctly the following attributes, inconsistently encoded:

- **Acknowledgement time stamp**
- **last modification timestamp**
- **Previous state**
- **Alarm Origin**
- **Original Event time**
- **Acknowledgement User ID**
- **Operator Note**
- **Clearance report flag**
- **escalated alarm**
- **sa total**
- **problem occurrence**
- **creation timestamp**
- **specific problem**
- **problem Information**

Step 1: TeMIP server side

The following attributes are not present in the AggregateEvent partition and also in Object Creation event.
So, they must be added to TeMIP object model.

1. Update the two following msl files

a- /usr/opt/temip/mmtoolkit/msl/temip_ah_fm_ao_events.ms

Add the following line in aggregate event part:

```
ARGUMENT  Acknowledgement Time Stamp = 39 : BinAbsTim
DISPLAY = TRUE,
SYMBOL = AO_ARG_ACK_TIME
END ARGUMENT;

ARGUMENT  Last Modification Timestamp = 9901 : BinAbsTim
DISPLAY = TRUE,
SYMBOL = AO_LASTMOD_TIME
```

```
END ARGUMENT ;

ARGUMENT   Previous State = 68 : AlarmObjectStateType
DISPLAY = TRUE,
SYMBOL = AO_PREVIOUS_STATE
END ARGUMENT ;

ARGUMENT   Clearance Report Flag =32: Boolean
DISPLAY = TRUE,
SYMBOL = AO_COND_CLEAR
END ARGUMENT ;
```

b- /usr/opt/temip/mmtoolkit/msl/temip_ah_fm_ao_events_common_args.ms

Add the following lines:

```
ARGUMENT  Acknowledgement Time Stamp = 39 : BinAbsTim
DISPLAY = TRUE,
SYMBOL = AO_ARG_ACK_TIME
END ARGUMENT ;

ARGUMENT  Last Modification Timestamp = 9901 : BinAbsTim
DISPLAY = TRUE,
SYMBOL = AO_LASTMOD__TIME
END ARGUMENT ;

ARGUMENT   Previous State = 68 : AlarmObjectStateType
DISPLAY = TRUE,
SYMBOL = AO_PREVIOUS_STATE
END ARGUMENT ;

ARGUMENT   Clearance Report Flag =32: Boolean
DISPLAY = TRUE,
SYMBOL = AO_COND_CLEAR
END ARGUMENT ;
```

Please execute the following commands:

 # mcc_msl -I/usr/opt/temip/mmtoolkit/msl -m/usr/opt/temip/mmtoolkit/msl/temip_ah_fm_srvc_if.ms

```
mcc_msl - Info: File write locked "/var/opt/temip/tmp/mcc_msl_mcc_fdictionary.dat.lock"

mcc_msl - Info: Loading existing binary MIR database file "/var/opt/temip/conf/en_US.iso88591/mcc_fdictionary.dat"

mcc_msl - Info: stat "/var/opt/temip/conf/en_US.iso88591/mcc_fdictionary.dat" mode: 0644 user: temip group: users size: 227736132 mtime: Fri Dec 6 04:25:44 2013 atime: Fri Apr 25 14:54:36 2014 sum: 22142

mcc_msl - Info: Checking the Built-In Data Types file version "/usr/opt/temip/mmtoolkit/msl/builtin_types.dat"


mcc_msl - Info: Merging MSL file "/usr/opt/temip/mmtoolkit/msl/temip_ah_fm_srvc_if.ms"

mcc_msl - Info: Merging Object Acknowledgement Time Stamp = 39

mcc_msl - Info: Ending Compilation of MSL file (31 lines)
```

```
mcc_msl - Info: File write locked "/var/opt/temip/tmp/mcc_fdictionary.dat.lock" before output file dump

mcc_msl - Info: /var/opt/temip/conf/en_US.iso88591/mcc_fdictionary.dat file saved into /var/opt/temip/conf/en_US.iso88591/mcc_fdictionary.dat.bak

mcc_msl - Info: stat "/var/opt/temip/conf/en_US.iso88591/mcc_fdictionary.dat.bak" mode: 0644 user: temip group: users size: 227736132 mtime: Fri Dec 6 04:25:44 2013 atime: Fri Apr 25 14:54:36 2014 sum: 22142


mcc_msl - Info: Generating Binary Output to "/var/opt/temip/conf/en_US.iso88591/mcc_fdictionary.dat"

mcc_msl - Info: stat "/var/opt/temip/conf/en_US.iso88591/mcc_fdictionary.dat" mode: 0644 user: temip group: users size: 227736396 mtime: Fri Apr 25 20:10:51 2014 atime: Fri Apr 25 20:10:51 2014 sum: 59909


# mcc_ptb


# temip_stop


# temip_start
```

Step 2: NOM server side

1. Update the TeMIP_configuration.dynamic.xml file

Those attributes must be added to the /var/opt/openmediation-72/containers/instance-0/ips/temip-ca-22/etc/conf/TeMIP_configuration.dynamic.xml file as follow (red lines):

```
<CustomAttributes>
<CustomAttribute>
        <!-- Works only for TeMIP 6.1 and above -->
        <Attribute>Creation_Timestamp</Attribute>
        <Datatype>BinAbsTime</Datatype>
      </CustomAttribute>
       <CustomAttribute>
         <!-- Works only for TeMIP 6.1 and above -->
         <Attribute>Creation_Time</Attribute>
          <Datatype>BinAbsTime</Datatype>
          </CustomAttribute>
       <CustomAttribute>
         <Attribute>Children</Attribute>
         <Datatype>XmlString</Datatype>
     </CustomAttribute>
     <CustomAttribute>
         <Attribute>Parents</Attribute>
         <Datatype>XmlString</Datatype>
```

```
      </CustomAttribute>
      <CustomAttribute>
            <Attribute>Pb</Attribute>
            <Datatype>XmlString</Datatype>
      </CustomAttribute>
      <CustomAttribute>
             <Attribute>User_Text</Attribute>
             <Datatype>XmlString</Datatype>
      </CustomAttribute>
       <CustomAttribute>
              <Attribute>User_Identifier</Attribute>
              <Datatype>XmlString</Datatype>
       </CustomAttribute>
<CustomAttribute>
              <Attribute>Problem_Status</Attribute>
             <Datatype>XmlString</Datatype>
      </CustomAttribute>
      <CustomAttribute>
              <Attribute>Original_Severity</Attribute>
              <Datatype>XmlString</Datatype>
       </CustomAttribute>
      <CustomAttribute>
               <Attribute>Acknowledgement_User_Identifier</Attribute>
               <Datatype>XmlString</Datatype>
        </CustomAttribute>
   <CustomAttribute>
    <Attribute>Acknowledgement_Time_Stamp</Attribute>
            <Datatype>BinAbsTime</Datatype>
            </CustomAttribute>
   <CustomAttribute>
              <Attribute>Handled_User_Identifier</Attribute>
              <Datatype>XmlString</Datatype>
         </CustomAttribute>
         <CustomAttribute>
              <Attribute>Handle_Time_Stamp</Attribute>
              <Datatype>BinAbsTime</Datatype>
         </CustomAttribute>
       <CustomAttribute>
              <Attribute>Termination_User_Identifier</Attribute>
              <Datatype>XmlString</Datatype>
        </CustomAttribute>
        <CustomAttribute>
```

```
            <Attribute>Termination_Time_Stamp</Attribute>
            <Datatype>BinAbsTime</Datatype>
        </CustomAttribute>
        <CustomAttribute>
            <Attribute>Clearance_Time_Stamp</Attribute>
            <Datatype>BinAbsTime</Datatype>
        </CustomAttribute>
      <CustomAttribute>
            <Attribute>Handled_By</Attribute>
<Datatype>EntitySet</Datatype>
     </CustomAttribute>
     <CustomAttribute>
           <Attribute>Correl_Notif_Info</Attribute>
           <Datatype>XmlString</Datatype>
      </CustomAttribute>
      <CustomAttribute>
            <Attribute>Alarm_Comment</Attribute>
            <Datatype>CommentTypeSet</Datatype>
      </CustomAttribute>
      <CustomAttribute>
              <Attribute>Last_Modification_Timestamp</Attribute>
              <Datatype>BinAbsTime</Datatype>
         </CustomAttribute>
        <CustomAttribute>
              <Attribute>Original_Event_Time</Attribute>
              <Datatype>BinAbsTime</Datatype>
         </CustomAttribute>
        <CustomAttribute>
              <Attribute>Problem_Occurrences</Attribute>
               <Datatype>XmlString</Datatype>
        </CustomAttribute>
        <CustomAttribute>
               <Attribute>Problem_Occurrence</Attribute>
               <Datatype>XmlString</Datatype>
        </CustomAttribute>
        <CustomAttribute>
               <Attribute>Alarm_Origin</Attribute>
               <Datatype>XmlString</Datatype>
          </CustomAttribute>
          <CustomAttribute>
               <Attribute>Previous_State</Attribute>
               <Datatype>XmlString</Datatype>
```

```
                </CustomAttribute>
                <CustomAttribute>
                        <Attribute>Alarm_Object_Operator_Note</Attribute>
                        <Datatype>XmlString</Datatype>
        </CustomAttribute>
                <CustomAttribute>
                        <Attribute>Clearance_Report_Flag</Attribute>
                        <Datatype>XmlBoolean</Datatype>
                  </CustomAttribute>
                <CustomAttribute>
                         <Attribute>Escalated_Alarm</Attribute>
                         <Datatype>XmlBoolean</Datatype>
                 </CustomAttribute>
                <CustomAttribute>
                          <Attribute>Sa_Total</Attribute>
                          <Datatype>XmlString</Datatype>
                  </CustomAttribute>
  </CustomAttributes>
```

2. Handle the ProblemInformation attribute inside the attribute Value Change event.
   Since NOM V7.2 (TeMIP CA V2.2) any change on ProblemInformation is not handled. To handle it correctly we need to customize TeMIP CA to add 'problemInformation' attribute change entry to AVC.
   TeMIP CA allows to customize message translation with Groovy postprocessor. In this particular case we need to enrich AVC that contains 'handeledBy' attribute change entre with new entry named 'problemInformation' and the same new/old values as old entry.
   Here are below the step that you must follow:

a- Create this processor code file

 # cat AvcProblemInformationPostprocessor.groovy

```
package com.hp.openmediation.ca.temip.utaf.transform;
import com.hp.openmediation.alarms._2011._08.AlarmAttributeValueChangeInterface;
import com.hp.openmediation.alarms._2011._08.AlarmBaseInterface;
import com.hp.openmediation.alarms. 2011. 08.Alarms;
import com.hp.openmediation.alarms. 2011. 08.AttributeChange;
import com.hp.openmediation.cautils.alarms.AttributeChangesUtil;
import org.apache.commons.collections.CollectionUtils;

public class AvcProblemInformationPostprocessor implements TransformPostprocessor {

    @Override
    public void process(Alarms alarms) {
        if (alarms == null) {
            return;
        }
        if (CollectionUtils.isEmpty(alarms.getBaseAlarms())) {
            return;
        }
        for (AlarmBaseInterface alarm : alarms.getBaseAlarms()) {
            if (alarm instanceof AlarmAttributeValueChangeInterface) {
                enrichProblemInformation((AlarmAttributeValueChangeInterface) alarm);
            }
        }
    }

    private void enrichProblemInformation(AlarmAttributeValueChangeInterface alarm) {
        if (alarm == null) {
            return;
        }
        if (alarm.getAttributeChanges() == null) {
            return;
        }
        AttributeChange handledByAttributeChange =
```

```
                AttributeChangesUtil.getAttributeChange(alarm, "handledBy");
        if (handledByAttributeChange == null) {
            return;
        }
        /*
         * Create 'problemInformation' attribute change entry with new and old
         * values as in 'handledBy' entry.
         */
        AttributeChange problemInfoAttributeChange = new AttributeChange();
        problemInfoAttributeChange.setName("problemInformation");
        problemInfoAttributeChange.setNewValue(handledByAttributeChange.getNewValue());
        problemInfoAttributeChange.setOldValue(handledByAttributeChange.getOldValue());
        /* Add 'problemInformation' attribute change entry to the alarm. */
        alarm.getAttributeChanges().getAttributeChange()
                .add(problemInfoAttributeChange);
    }
}
```

b- Copy it into /var/opt/openmediation-72/containers/instance-0/ips/temip-ca-22/etc

```
cp AvcProblemInformationPostprocessor.groovy /var/opt/openmediation-72/containers/instance-0/ips/temip-ca-22/etc
```

c- Update /var/opt/openmediation-72/containers/instance-0/ips/temip-ca-22/etc/uca-mediation-vp-utaf.xml

add below configuration in red:

```
       <lang:groovy id="transformPostprocessor" scope="prototype" script-source="file:/var/opt/openmediation-72/containers/instance-0/ips/temip-ca-22/etc/AvcProblemInformationPostprocessor.groovy"/>

<utaf:provider service="ca:utaf bc dynamic flows" endpoint="endpoint" targetService="ca:alarms_from_temip_jms_provider" targetEndpoint="endpoint" configurationFile="ips/temip-ca-22/etc/conf/TeMIP_configuration.dynamic.xml" rootDirectory="ips/temip-ca-22/etc" staticConfiguration="false" transformPostprocessorBeanName="transformPostprocessor" />
```

3. Restart container (as root user)

```
# /opt/openmediation-72/bin/nom_admin -shutdown-container

# /opt/openmediation-72/bin/nom_admin -start-container
```

Step 3: OSSM server side

Some fields corresponding to these attributes must be added to the $OSSM_DATA/data/cmstore/dimension/temip_alarm.xml temip_alarm.xml dimension (red lines)

```
<Field name="acknowledgement_timestamp" type="date"/>
   <Field name="acknowledgement_user_identifier" type="string"/>
   <Field name="additional_text" type="string"/>
    <Field name="alarm_origin" type="enum:alarm_origin"/>
   <Field name="alarm_type" type="string"/>
   <Field name="children" type="string" multiple="true"/>
   <Field name="clearance_report_flag" type="boolean"/>
   <Field name="creation_timestamp" type="date"/>
   <Field name="domain" type="string"/>
   <Field name="escalated_alarm" type="boolean"/>
   <Field name="event_time" type="date"/>
   <Field name="identifier" type="number" isKey="true"/>
   <Field name="last_modification_timestamp" type="date"/>
    <Field name="managed_object" type="string"/>
    <Field name="operation_context" type="string" isKey="true"/>
```

```
    <Field name="operator_note" type="string"/>
    <Field name="original_event_time" type="date"/>
    <Field name="original_severity" type="enum:perceived_severity"/>
    <Field name="parents" type="string" multiple="true"/>
    <Field name="perceived_severity" type="enum:perceived_severity"/>
    <Field name="previous_state" type="enum:state"/>
    <Field name="probable_cause" type="string"/>
    <Field name="problem_occurrences" type="number"/>
        <Field name="problem_information" type="string" multiple="true"/>
    <Field name="problem_status" type="enum:problem_status"/>
    <Field name="sa_total" type="number"/>
    <Field name="specific_problems" type="string" multiple="true"/>
    <Field name="state" type="enum:state"/>
    <Field name="target_entities" type="string" multiple="true"/>
    <Field name="user_text" type="string"/>
    <Field name="uniqueid" type="string" isKey="true"/>
    <Field name="map_association_id" type="string"/>
```

Restart OSSM

```
# $OSSM_HOME/bin/ossm stop
# $OSSM_HOME/bin/ossm start
```

5.1.2 Customer specific attributes management

To be able to receive specific Customer Attributes of alarms on the OSS Console the following steps should be executed.

1. Update Custom AO field in the Channel Adapter part
   - Look in the TeMIP dictionary the TeMIP presentation name of the Custom attribute you want to forward to UOC console.
     Example: "SITE_CODE" and "UCA Custom Field1".

   - Update the channel adapter configuration file accordingly (TeMIP_configuration.dynamic.xml)

```
# cd /var/opt/openmediation-72/containers/instance-0/ips/temip-ca-22/etc/conf

---- edit TeMIP_configuration.dynamic.xml file and add the following:

<CustomAttribute>
      <Attribute>SITE_CODE</Attribute>
    <Datatype>XmlString</Datatype>
</CustomAttribute>

<CustomAttribute>
        <Attribute>UCA Custom Field1</Attribute>
        <Datatype>XmlString</Datatype>
            </CustomAttribute>
```

2. Update the temip_alarm raw dimension file in OSSM server part with the CustomAO

```
# cd $OSSM_DATA/data/cmstore/dimension/
--- edit temip_alarm.xml file and add the following
<Field>
<name>sitecode</name>
    <type>string</type>
 </Field>
<Field>
   <name>ucacustomfield1</name>
    <type>string</type>
 </Field>
```

TIP: Attribute Naming convention

Be careful: the naming convention in NOM and OSSM are different for Custom AO attribute names.

Example1:

SITE_CODE in TeMIP Side becomes

sitecode in OSSM server part (no uppercase, no underscore)

Example2:

UCA Custom Field1 in TeMIP Side becomes

Ucacustomfield1 in OSSM server part (no uppercase, no blank)

TIP: Attribute Type convention

Custom attribute value that will be received by OSS Console will be a string in any case but the type specified in TeMIP CA configuration controls encoding and decoding of data.

For TeMIP attributes of types FullEntityName, EntitySet and BinAbsTim it's best to use corresponding types in TeMIP CA configuration:

- EntitySpec
- EntitySet,
- BinAbsTime

If XmlString is specified instead then attribute will be returned in quite unreadable format.

supported type list:

- XmlDecimal
- XmlString
- XmlBoolean
- EntitySpec
- EntitySet

BinAbsTime

3. Restart the Container

```
--- at NOM adapter server side
--- assuming that the NOM container is by default 0:
#nom_admin --shutdown-container
#nom_admin --start-container
```

4. Restart OSSM server

```
--- at OSSM server side
# $OSSM_HOME/bin/ossm stop
# $OSSM_HOME/bin/ossm start
```

5. Open the TeMIP Real time Alarm view through OSS Console URL.

   Select settings icon, and then choose the custom attribute that should be displayed in the temip_alarm window.

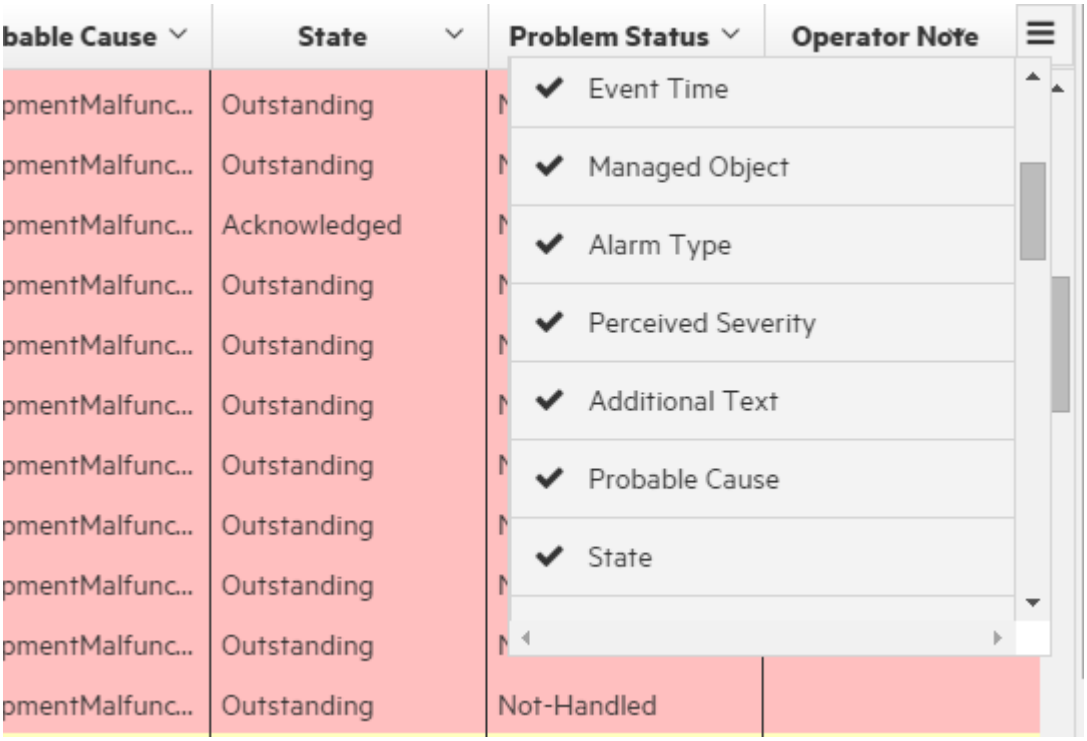


Figure 1. OSS console real-time alarm table view columns configuration

5.2 CSV adapter

Each time you create, update a new view that will be fed by the content of at least one csv file, you need to update the csv adapter configuration file.

This file is used to associate a csv data source file to a given dimension.

All the sample views delivered by OSSM kit and accessible through demo/demo account are configured with the csv adapter.

1. **Update csv_adapter.xml configuration file**

   Once your dimension has been defined, you can update the csv adapter configuration file as below:

```
# cd $OSSM_DATA/conf

--- edit and update csv_adapter.xml file
```

```
<?xml version="1.0" encoding="UTF-8"?>

<csv_adapters>

 <instance      dimension="my_dimension"      datafiles="/tmp/my_data-file.csv"
mode="full" delimiter=";" >

 <field name="([\s\S]*)" datepattern="yyyy/MM/dd HH:mm" />

 </instance>

</csv_adapters>
```

Where:

dimension: is the name of the raw dimension defined with the dimension manager and located into $OSSM_DATA/data/cmstore/dimension directory.

datafiles: is the name and location of the csv data source file from which data will be collected,

mode: represents the way data will be collected. "full" mode meaning that each time the csv data file will be updated, all the data will be reloaded. "delta" mode meaning that only updated lines will be reread. Today csv adapter only supports the full mode.

delimiter: is the separator used in the csv file. Default value is the comma ",".

name (field)/datepattern: is used to specify, in case csv file provide date fields, the format of these fields. "name" attribute is a regular expression allowing to specify the name or a set of name field(s) that match(es) the given datepattern.

Example1:

```
<field name="([\s\S]*)" datepattern="yyyy/MM/dd HH:mm" />
```

All the fields which contain date in the csv file, have the same date format which is "yyyy/MM/dd HH:mm"

Example2:

```
<field name="([\s\S]*)" datepattern="yyyy/MM/dd HH:mm" />
<field name="([\s\S]*)" datepattern="yyyy/MM/dd HH:mm:ss" />
```

Some fields containing date in the csv file, have "yyyy/MM/dd HH:mm" some other have "yyyy/MM/dd HH:mm:ss" date formats.

Example3:

```
<field name="(^aaa)" datepattern="yyyy/MM/dd HH:mm" />
<field name="(^bbb)" datepattern="yyyy/MM/dd HH:mm:ss" />
```

Field names in the csv file that start with "aaa" string have the "yyyy/MM/dd HH:mm" date format.

Field names in the csv file that start with "bbb" string have "yyyy/MM/dd HH:mm:ss" date format.

1. **Restart the csv adapter**

After each update of the csv configuration file, you need to restart the adapter.

```
# $OSSM_HOME/adapters/csv/bin/stop.sh
# $OSSM_HOME/adapters/csv/bin/start.sh
```

Add the encoding info to support 2 bytes characters(if needed):

If there is any 2 bytes characters in the csv file (like Chinese, Korean, Japanese language characters), we need to add encoding in the instance. For example:

```
# vi $OSSM_DATA/conf/csv_adapter.xml

# <!--sample views-->

        <instance                                          dimension="demo_alarm"
datafiles="${OSSM_HOME}/examples/demo/data-samples/alarm/Export.csv"
mode="full" encoding="GB18030" >
```

```
            <field name="([\s\S]*)" datepattern="yyyy/MM/dd HH:mm" />
        </instance>
```

Then we need to **restart** the adapter as step 2.

5.4 DB adapter

Each time you create or update a new view that will be fed by the content of at JDBC database, you need to update the db adapter configuration file.

This file is used to associate a DB instance to a given dimension.

The sample view "Service Site monitoring H2" delivered by OSSM kit and accessible by user through custom/custom account in the "Service Management" category is configured with the db adapter.

1. Update db_adapter.xml configuration file

Once your dimension has been defined, you can update the db adapter configuration file as below:

```
   # cd $OSSM_DATA/conf

   --- edit and update db_adapter.xml file


<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

   <db_adapter>

       <!-- Example connection with Oracle -->
        <connection          id="connection1"          driver="oracle.jdbc.OracleDriver"
       url="jdbc:oracle:thin:@16.17.98.197:1521:TOPOv1"   username="UOC"   password="UOC"
       reconn="true" maxconn="10" maxidle="6"  maxwait="30" />
        <instance dimension="test" table="UOC_TEST" mode="full" connection="connection1"
       period="1 second" lazy="true" />

       <!-- Example connection with h2 -->
         <connection               id="connection2"               driver="org.h2.Driver"
       url="jdbc:h2:tcp://localhost/${OSSM_HOME}/examples/custom/data-
       samples/h2/SiteMonMemDB" username="" password="" />
        <instance       table="SITEMON_DATA"       dimension="sitemonH2"       mode="full"
       connection="connection2" />

       <!-- Example connection with mysql -->


       <connection             id="connection3"             driver="com.mysql.jdbc.Driver"
url="jdbc:mysql://16.156.194.168:3306/nfvdemo" username="root" password="root" />

       <instance        table="T_UOCTEST"        dimension="mysql_test"        mode="full"
connection="connection4" period="15 second" />



       <!-- Example connection with vertica -->



        <connection         id="fault_rpt_conn"         driver="com.vertica.jdbc.Driver"
url="jdbc:vertica://16.173.234.159:5433/ossdb"     reconn="false"     username="fault_rpt"
password="!qazxsw2" />

  <instance         dimension="fault_rpt"         table="alarmobject"         mode="full"
connection="fault_rpt_conn" />
```

```
</db_adapter>
```

Where:

connection Id: is a name for the connection.

driver: is the jdbc driver used.

url: represent the parameters of the connection to access the DB instance.

username/password: used to connect to the DB instance.

reconn: used to define if database connection broken, will the db adapter try to reconnect to database next time.

maxconn: the max database connection could be used, it's optional, default value is 50.

maxidle: the maximum number of connections that can remain idle, it's optional, default value is 30.

maxwait: the max waiting second when a request try to get a database connection, it's optional, default value is 30.

And

instance dimension: is the name of the raw dimension defined with the dimension manager and located into $OSSM_DATA/data/cmstore/dimension directory.

table: is the name of the table where data will be collected.

connection: is the name of the connection defined previously that will be used to access the table.

mode: represents the way data will be collected. "full" mode meaning that each time the DB data table will be updated, all the data will be reloaded. "delta" mode meaning that only updated records will be reread.

period: represents the timer interval between next time JDBC adapter refresh the database.

lazy: represents whether the instance provides subscribe service or not. "true" means that the instance does not provide subscribe services, "false" means it does. The default value is "false" if the "lazy" attribute is not set.

NOTE: Provided drivers

Some drivers are delivered by the OSSM packages. These drivers are:

- Oracle driver
- H2 driver
- MySQL driver
- VERTICA driver

After having modified the db_adapter.xml file, restart the db_adapter as follow:

```
# $OSSM_HOME/adapters/db/bin/stop.sh
# $OSSM_HOME/adapters/db/bin/start.sh
```

To check the db adapter restart, edit the DB_ADAPTER.log file

```
# cd $OSSM_DATA/logs
# tail -f DB_ADAPTER.log
```

Configuration File Name	Configuration Item	Description	Default Value
receiverglobal.conf	receiver.dimensions	Define the dimensions to be subscribe data from adaptors	["temip_alarm",”demo_alarm”]
	receiver.startServer	If to start H2 DB service within Receiver.' true' to start 'false' not	true

	receiver.ServerParam	The parameters to startup H2 server. Don't change the default value.	-tcpAllowOthers
	receiver.maxDBWorkerPerConsumer	This parameter is not active, keep the default value	1
	receiver.remoteDataHandler.active	Must keep the default value	false
	receiver.remoteDataHandler.path	This paramter is not actived, keep the default value	"akka.tcp://RemoteDataHandler@localhost:2553/user/dataHandler"
	receiver.localDataHandler	The actor address of the local data handler. If the service is not started on the localhost, i.e.. 192.168.0.1, then ONLY update the 'localhost' to the IP address or the host name. MUST keep the left part unchanged! The host value must be same as akka .remote.netty.tcp.hostname in recciverservice.conf	"akka.tcp://ReceiverService@localhost:2553/user/dataHandler"
reciverservice.conf	akka.loggers	Log configuration. Don't change it.	["akka.event.slf4j.Slf4jLogger"]
	akka.logger-startup-timeout	Log configuration. Don't change it.	"25s"
	akka.actor .provider	System configuration. Don't change it.	"akka.remote.RemoteActorRefProvider"
	akka .remote.netty.tcp.hostname	The host value must be same as receiver.localDataHandler in receiverglobal.conf	"localhost"
	akka .remote.netty.tcp.port	The port used by receiver service. If modify the default value, MUST keep the same port value in the receiver.localDataHandler in receiverglobal.conf	2553
receiverconsole.conf	akka.loggers	Log configuration. Don't change it.	["akka.event.slf4j.Slf4jLogger"]
	akka.logger-startup-timeout	Log configuration. Don't change it.	"25s"
	akka.actor .provider	System configuration. Don't change it.	"akka.remote.RemoteActorRefProvider"
	akka .remote.netty.tcp.hostname	The host to run the receiver console. Suggest not updating.	"localhost"
	akka .remote.netty.tcp.port	The port used by receiver console service. If modify the default value, MUST keep different with the port value in the receiver.localDataHandler in receiverglobal.conf	2552
h2_conf.xml	<type>	the db pool type will be used, by now, it could be :h2,dbcp or just remain nothing. h2 : the db pool implement by H2, it could support multi h2 instance. Dbcp: the db pool implement by DBCP, it could support multi h2 instance. nothing: it mean no value was input , just like <type></type>, in this mode, the db pool implement by H2, but it could not support mulit h2 instancel.	<type></type>
	<url>	JDBC url to the h2 database. Don't change it.(this item effect just when <type> is blank)	jdbc:h2:tcp://localhost/mem:uocCenterPool;DB_CLOSE_DELAY=-1;MULTI_THREADED=1;LOCK_MODE=3;LOG=0;UNDO_LOG=0
	<usr>	User name to access the DB. Don't change it.(this item effect just when <type> is blank)	sa
	<pwd>	Password to access the DB. Don't change it.	
	<maxConnNumber>	The max db connection pool size. Need tune this value to get the best performance. (this item effect just when <type> is blank)	300
	<h2>	when type is h2, the QC module will use setting in this tag	
	<dbcp>	when type is dbcp, the QC module will use setting in this tag	

<pool>	it mean a new db pool tag,use in <h2>,<dbcp> tag	
<name>	a db pool name, it is mandatory,use in <h2>,<dbcp> tag	
<driver>	db driver name, don't change it,use in <h2>,<dbcp> tag	org.h2.Driver
<maxtotal>	it is same as <maxConnNumber>, it just use in <h2>,<dbcp> tag.	150
<maxwaitmillis>	it mean the max waiting milli second when a request try to get a database connection,use in <h2>,<dbcp> tag	60000
<initialsize>	The initial number of connections that are created when the pool is started,use in <dbcp> tag	0
<maxidle>	the maximum number of connections that can remain idle in the pool, without extra ones being released, or negative for no limit.	120
<minidle>	The minimum number of connections that can remain idle in the pool, without extra ones being created, or zero to create none.	30
<remove abandoned>	Flag to remove abandoned connections if they exceed the removeAbandonedTimout. If set to true a connection is considered abandoned and eligible for removal if it has not been used for longer than the removeAbandonedTimeout. Creating a Statement, PreparedStatement or CallableStatement or using one of these to execute a query (using one of the execute methods) resets the lastUsed property of the parent connection. Setting this to true can recover db connections from poorly written applications which fail to close a connection.	false
<removeabandonedtimeout>	Timeout in seconds before an abandoned connection can be removed	300
<timebetweenevictionrunsmillis>	The number of milliseconds to sleep between runs of the idle object evictor thread. When non-positive, no idle object evictor thread will be run	600000

5.5 Receiver

Receiver module collects data from adaptors and builds the UOC center data pool in H2 data base. The H2 data base is started with Receiver.

How to start Receiver

Start with OSSM by ‘ossm start’ command

Start individually by ‘receiver_start’ command

How to stop Receiver

Stop with OSSM by ‘ossm stop’ command

Stop individually by ‘receiver_console -shutdown’ command

Note: H2 database will stopped with Receiver and all the cached data will be rebuild when receiver started.

How to configure Receiver

There are 4 files used by Receiver module under $OSSM_DATA/conf

H2_conf.xml

receiverglobal.conf

receiverservice.conf

receiverconsole.conf

Most parameters shall keep the default values.

To collect data automatically into the H2 database, it required to update the list defined in the receiverglobal.conf or to use receiver_console command to collect data manually.

NOTE: Don't add too many dimension in the collection list, if some of them are unavailable it will block the whole data collection.

Flow table show the details of the configuration items.

Configuration File Name	Configuration Item	Description	Default Value
receiverglobal.conf	receiver.dimensions	Define the dimensions to be subscribe data from adaptors	["temip_alarm","demo_alarm"]
	receiver.startServer	If to start H2 DB service within Receiver.' true' to start 'false' not	true
	receiver.ServerParam	The parameters to startup H2 server. Don't change the default value.	-tcpAllowOthers
	receiver.maxDBWorkerPerConsumer	This parameter is not active, keep the default value	1
	receiver.remoteDataHandler.active	Must keep the default value	false
	receiver.remoteDataHandler.path	This paramter is not actived, keep the default value	"akka.tcp://RemoteDataHandler@localhost:2553/user/dataHandler"
	receiver.localDataHandler	The actor address of the local data handler. If the service is not started on the localhost, i.e.. 192.168.0.1, then ONLY update the 'localhost' to the IP address or the host name. MUST keep the left part unchanged! The host value must be same as akka .remote.netty.tcp.hostname in recciverservice.conf	"akka.tcp://ReceiverService@localhost:2553/user/dataHandler"
recciverservice.conf	akka.loggers	Log configuration. Don't change it.	["akka.event.slf4j.Slf4jLogger"]
	akka.logger-startup-timeout	Log configuration. Don't change it.	"25s"
	akka.actor .provider	System configuration. Don't change it.	"akka.remote.RemoteActorRefProvider"
	akka .remote.netty.tcp.hostname	The host value must be same as receiver.localDataHandler in receiverglobal.conf	"localhost"
	akka .remote.netty.tcp.port	The port used by receiver service. If modify the default value, MUST keep the same port value in the receiver.localDataHandler in receiverglobal.conf	2553
receiverconsole.conf	akka.loggers	Log configuration. Don't change it.	["akka.event.slf4j.Slf4jLogger"]
	akka.logger-startup-timeout	Log configuration. Don't change it.	"25s"
	akka.actor .provider	System configuration. Don't change it.	"akka.remote.RemoteActorRefProvider"
	akka .remote.netty.tcp.hostname	The host to run the receiver console. Suggest not updating.	"localhost"
	akka .remote.netty.tcp.port	The port used by receiver console service. If modify the default value, MUST keep different with the port value in the receiver.localDataHandler in receiverglobal.conf	2552

h2_conf.xml	<type>	the db pool type will be used, by now, it could be :h2,dbcp or just remain nothing. h2 : the db pool implement by H2, it could support multi h2 instance. Dbcp: the db pool implement by DBCP, it could support multi h2 instance. nothing: it mean no value was input , just like <type></type>, in this mode, the db pool implement by H2, but it could not support mulit h2 instancel.	<type></type>
	<url>	JDBC url to the h2 database. Don't change it.(this item effect just when <type> is blank)	jdbc:h2:tcp://localhost/mem:uocCenterPool;DB_CLOSE_DELAY=-1;MULTI_THREADED=1;LOCK_MODE=3;LOG=0;UNDO_LOG=0
	<usr>	User name to access the DB. Don't change it.(this item effect just when <type> is blank)	sa
	<pwd>	Password to access the DB. Don't change it.	
	<maxConnNumber>	The max db connection pool size. Need tune this value to get the best performance. (this item effect just when <type> is blank)	300
	<h2>	when type is h2, the QC module will use setting in this tag	
	<dbcp>	when type is dbcp, the QC module will use setting in this tag	
	<pool>	it mean a new db pool tag,use in <h2>,<dbcp> tag	
	<name>	a db pool name, it is mandatory,use in <h2>,<dbcp> tag	
	<driver>	db driver name, don't change it,use in <h2>,<dbcp> tag	org.h2.Driver
	<maxtotal>	it is same as <maxConnNumber>, it just use in <h2>,<dbcp> tag.	150
	<maxwaitmillis>	it mean the max waiting milli second when a request try to get a database connection,use in <h2>,<dbcp> tag	60000
	<initialsize>	The initial number of connections that are created when the pool is started,use in <dbcp> tag	0
	<maxidle>	the maximum number of connections that can remain idle in the pool, without extra ones being released, or negative for no limit.	120
	<minidle>	The minimum number of connections that can remain idle in the pool, without extra ones being created, or zero to create none.	30
	<removeabandoned>	Flag to remove abandoned connections if they exceed the removeAbandonedTimout. If set to true a connection is considered abandoned and eligible for removal if it has not been used for longer than the removeAbandonedTimeout. Creating a Statement, PreparedStatement or CallableStatement or using one of these to execute a query (using one of the execute methods) resets the lastUsed property of the parent connection. Setting this to true can recover db connections from poorly written applications which fail to close a connection.	false
	<removeabandonedtimeout>	Timeout in seconds before an abandoned connection can be removed	300
	<timebetweenevictionrunsmillis>	The number of milliseconds to sleep between runs of the idle object evictor thread. When non-positive, no idle object evictor thread will be run	600000

How to collect data from adaptor

In OSSM data are organized by 'Dimension'. If the dimensions are defined in the receiverglobal.conf, receiver module will subscribe data from adaptors automatically. To subscribe new dimension online use:

```
receiver_console  -r <DimensionName>
```

NOTE: Only RAW dimension is collect from adaptors.

NOTE: When adaptor restart, the existing subscribe collection is broken, need restart the Receiver or use receiver_console to reestablish the connection.

NOTE: If a subscribed RAW dimension is updated, i.e. add new customized fields, must restart the Receiver.

5.6 Receiver H2 port

5.6.1 Default port

The default port is "9092".

By default Receiver module start H2 server on the default port which is 9092.It is can be configured in $OSSM_DATA/conf/receiverglobal.conf

Below is the default configuration context:

$OSSM_DATA/conf/receiverglobal.conf

```
receiver {
    dimensions=["temip_alarm","topo_map_sample_alarm"]
    dimensionsWithPivot=["temip_alarm","topo_map_sample_alarm"]
    startServer=true
    ServerParam=-tcpAllowOthers
    maxDBWorkerPerConsumer=1
    ...
}
```

The property "ServerPort" is not present. That means the default port is 9092.

By default QC_Provider module is connected to H2 server on the default port which is 9092.

It can be configured in $OSSM_DATA/conf/h2_conf.xml

Below is the default configuration:

$OSSM_DATA/conf/h2_conf.xml

```
<?xml version="1.0" encoding="UTF-8"?>
    <db>
        <type></type>
                <url>jdbc:h2:tcp://localhost/mem:uocCenterPool;DB_CLOSE_DELAY=-
1;MULTI_THREADED=1;LOCK_MODE=3;LOG=0;UNDO_LOG=0</url>
```

```
        <usr>sa</usr>
        <pwd></pwd>
```

tcp://localhost/mem:uocCenterPool means the default port is 9092.

Topology map also needs to connect to H2 database, the default port is 9092. It can be configured in $OSSM_DATA/conf/context.xml

$OSSM_DATA/conf/context.xml

```
<Context>
    <!-- Default set of monitored resources -->
    <WatchedResource>WEB-INF/web.xml</WatchedResource>
    <!-- Uncomment this to disable session persistence across Tomcat restarts -
->
    <!--<Manager pathname="" />-->
    <!-- Uncomment this to enable Comet connection tacking (provides events on
session expiration as well as webapp lifecycle) -->
    <!--<Valve
className="org.apache.catalina.valves.CometConnectionManagerValve" />-->
    <!-- Don't edit this part -->
    <Resource name="jdbc/dimension_datasource" auth="Container"
    type="javax.sql.DataSource"                driverClassName="org.h2.Driver"
url="jdbc:h2:tcp://localhost:9092/mem:uocCenterPool;DB_CLOSE_DELAY=-
1;MULTI_THREADED=1;LOCK_MODE=3;LOG=0;UNDO_LOG=0"    username="sa"    password=""
maxActive="20" maxWait="-1"/>
    <!-- End don't edit -->
        <!--
        <Resource name="jdbc/OSSM_DATAsource" auth="Container"
              type="javax.sql.DataSource"
driverClassName="oracle.jdbc.OracleDriver"
              url="jdbc:oracle:thin:@127.0.0.1:1521:TOPOv1"
              username="UOC" password="UOC" maxActive="20" maxWait="-1"/>
        -->
    <Resource name="jdbc/OSSM_DATAsource" auth="Container"
     type="javax.sql.DataSource"                driverClassName="org.h2.Driver"
url="jdbc:h2:tcp://localhost:9092/mem:uocCenterPool;DB_CLOSE_DELAY=-
1;MULTI_THREADED=1;LOCK_MODE=3;LOG=0;UNDO_LOG=0"    username="sa"    password=""
maxActive="20" maxWait="-1"/>
</Context>
```

5.6.2 Change the default port

If user want to change the default port, user need to update the hereunder two configuration files:

$OSSM_DATA/ receiverglobal.conf

$OSSM_DATA/conf/h2_conf.xml

$OSSM_DATA/conf/context.xml

And ensure new port is exact same in two files. For example, we want to change the port to 9093.

$OSSM_DATA/ receiverglobal.conf:

```
receiver {
```

```
    dimensions=["temip_alarm","topo_map_sample_alarm"]
    dimensionsWithPivot=["temip_alarm","topo_map_sample_alarm"]
    startServer=true
     ServerParam=-tcpAllowOthers
     ServerPort=9093
    maxDBWorkerPerConsumer=1
    ...
}
```

$OSSM_DATA/conf/h2_conf.xml:

```
<?xml version="1.0" encoding="UTF-8"?>
     <db>
         <type></type>

<url>jdbc:h2:tcp://localhost:9093/mem:uocCenterPool;DB_CLOSE_DELAY=-
1;MULTI_THREADED=1;LOCK_MODE=3;LOG=0;UNDO_LOG=0</url>
         <usr>sa</usr>
         <pwd></pwd>
```

$OSSM_DATA/conf/context.xml

```
<Context>
    <!-- Default set of monitored resources -->
    <WatchedResource>WEB-INF/web.xml</WatchedResource>
    <!-- Uncomment this to disable session persistence across Tomcat restarts -
->
    <!--<Manager pathname="" />-->
    <!-- Uncomment this to enable Comet connection tacking (provides events on
session expiration as well as webapp lifecycle) -->
    <!--<Valve
className="org.apache.catalina.valves.CometConnectionManagerValve" />-->
    <!-- Don't edit this part -->
    <Resource name="jdbc/dimension_datasource" auth="Container"
    type="javax.sql.DataSource"                driverClassName="org.h2.Driver"
url="jdbc:h2:tcp://localhost:9093/mem:uocCenterPool;DB_CLOSE_DELAY=-
1;MULTI_THREADED=1;LOCK_MODE=3;LOG=0;UNDO_LOG=0"    username="sa"    password=""
maxActive="20" maxWait="-1"/>
    <!-- End don't edit -->
        <!--
        <Resource name="jdbc/OSSM_DATAsource" auth="Container"
              type="javax.sql.DataSource"
driverClassName="oracle.jdbc.OracleDriver"
              url="jdbc:oracle:thin:@127.0.0.1:1521:TOPOv1"
              username="UOC" password="UOC" maxActive="20" maxWait="-1"/>
        -->
```

```
    <Resource name="jdbc/OSSM_DATAsource" auth="Container"
     type="javax.sql.DataSource"                    driverClassName="org.h2.Driver"
url="jdbc:h2:tcp://localhost:9093/mem:uocCenterPool;DB_CLOSE_DELAY=-
1;MULTI_THREADED=1;LOCK_MODE=3;LOG=0;UNDO_LOG=0"    username="sa"    password=""
maxActive="20" maxWait="-1"/>


</Context>
```

5.7 DB Transformer

DB Transformer is an advanced module for UOC administrators. The module executes customized scripts on the H2 database to **implement extra features**, like:

1. Build index on RAW dimension data tables to optimize the performance.
2. Register UDF function
3. Create transformer views

All the script files are stored under $OSSM_HOME/scripts/dbtransformer/init. The files are executed in sequence.

Note: If an error occurs during a script file, the remaining commands in this file are skipped and the transformer will execute the next files.

How to create index

In H2 database each dimension maps to a table with the same name. To create index on the table will help to improve the performance. For example to build an index on dimension 'temip_alarm', create a file containing the following:

```
create index i1 on temip_alarm(event_time, IDENTIFIER,operation_context);
```

How to build UDF

UDF (User Defined Function) is supported by H2 data. Users can develop their own UDF in JAVA. Here is an example to split a data column into two columns by specific delimiters.

```
public static ResultSet spliter(Connection conn, String sql, String sp)    throws
SQLException {
                    SimpleResultSet rs = new SimpleResultSet();
                    rs.addColumn("KEY", Types.VARCHAR, 128, 0);
             rs.addColumn("X", Types.VARCHAR, 128, 0);
             rs.addColumn("Y", Types.VARCHAR, 128, 0);
          ResultSet r=conn.createStatement().executeQuery(sql);
          while(r!=null && r.next()){
              String s=r.getString(1);
              String [] ss=s.split(sp);
              if(ss.length>=2){
                 rs.addRow(s,ss[0],ss[1]);
              }else{
                 rs.addRow(s,s,null);
              }
```

```
        }
        r.close();
        return rs;

}
```

Then build a jar file and put it under $OSSM_HOME/lib. To make it take effective you must restart the H2 Database. (Receiver Module). To register the new function build a new file under $OSSM_HOME/scripts/dbtransformer/init, with a content like

```
create alias SPLITER for "com.hp.uoc.h2.udf.UserDefineFunctions.spliter";
```

NOTE: For more details of H2 UDF please refer to H2 official website http://www.h2database.com/

How to start DB Transformer

DB Transformer will started with 'ossm start' or 'receiver_start'. When it executes all script files it will exit automatically.

Use case: Use DB Transformer to implement N to N real relationship aggregation

To build a dashboard as follow:

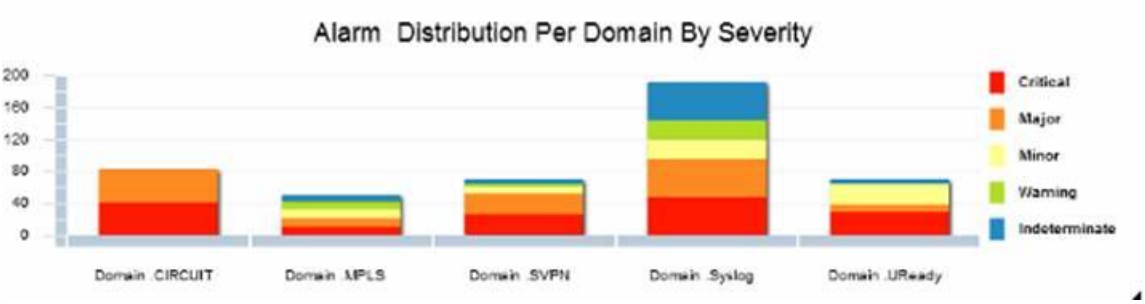


Figure 2 Dashboard

Source Data:

Fact Table: temip_alarm (columns: OPERATION_CONTEXT, ORIGINAL_SEVERITY…)

IDENTIFIER	LAST_MODIFICATION_TIMESTAMP	MANAGED_OBJECT	OPERATION_CONTEXT
26500	1412603427075	OSI_SYSTEM perf_osi1 TESTOBJ t5	perf_op1
26499	1412603427074	OSI_SYSTEM perf_osi1 TESTOBJ t5	perf_op1
26498	1412603427074	OSI_SYSTEM perf_osi1 TESTOBJ t5	perf_op1
26497	1412603427074	OSI_SYSTEM perf_osi1 TESTOBJ t5	perf_op1
26496	1412603427074	OSI_SYSTEM perf_osi1 TESTOBJ t5	perf_op1
26495	1412603427073	OSI_SYSTEM perf_osi1 TESTOBJ t5	perf_op1
26494	1412603427073	OSI_SYSTEM perf_osi1 TESTOBJ t5	perf_op1
26493	1412603427073	OSI_SYSTEM perf_osi1 TESTOBJ t5	perf_op1
26492	1412603427073	OSI_SYSTEM perf_osi1 TESTOBJ t5	perf_op1
26491	1412603427073	OSI_SYSTEM perf_osi1 TESTOBJ t5	perf_op1
26490	1412603427072	OSI_SYSTEM perf_osi1 TESTOBJ t5	perf_op1
26489	1412603427072	OSI_SYSTEM perf_osi1 TESTOBJ t5	perf_op1
26488	1412603427072	OSI_SYSTEM perf_osi1 TESTOBJ t5	perf_op1
26487	1412603427072	OSI_SYSTEM perf_osi1 TESTOBJ t5	perf_op1
26486	1412603427072	OSI_SYSTEM perf_osi1 TESTOBJ t5	perf_op1
26485	1412603427071	OSI_SYSTEM perf_osi1 TESTOBJ t5	perf_op1
26484	1412603427071	OSI_SYSTEM perf_osi1 TESTOBJ t5	perf_op1

NOTE: Receiver create a table for RAW OSSM dimensions the table name is same as the OSSM dimension and the columns' name are same as the attributes' name. If receiver subscribes the raw data from adaptor successfully, the data will be store in the table.

Dimension Table: oc_domain (columns: OC, Domains) OC and Domain are in N to N relationship.

OC	DOMAINS
perf_op5	domain2
perf_op5	domain3
perf_op16	domain2
perf_op16	domain3
perf_op16	domain4
perf_op9	domain3
perf_op9	domain4
perf_op9	domain5
perf_op1	domain4
perf_op1	domain5
perf_op1	domain6
perf_op6	domain5
perf_op6	domain6
perf_op6	domain7
perf_op38	domain6
perf_op38	domain7
perf_op38	domain8
perf_op17	domain7
perf_op17	domain8
perf_op17	domain9
perf_op13	domain8

NOTE: To build this table could define a OSSM dimension and build a csv files, Then use csv adaptor and receiver to collect it. The other way if the data is immutable it can be created and loaded by DB Transformer.

Step1: define a new RAW dimension in OSSM named domain_alarm as

Domain as String

SEVERITY as String

AlarmNumber as number

Step 2: Develop a new UDF function as

```
public static ResultSet CounterEx(Connection conn, String dim, String fact, String dimcol, String dimgroup,String factcol, String factgroup )    throws SQLException
{
 SimpleResultSet rs = new SimpleResultSet();
 rs.addColumn(dimgroup, Types.VARCHAR, 128, 0);
 rs.addColumn(factgroup, Types.VARCHAR, 128, 0);
 rs.addColumn("Count", Types.INTEGER,10 , 0);
 String sql="select  distinct " +dimgroup+ " from "+ dim;

 ResultSet r=  conn.createStatement().executeQuery(sql);
 while(r!=null && r.next()){
      String g=r.getString(1);
      String sql2="select a."+factgroup+", count(1) from " + fact + " a , " + dim + " b    where a."+factcol+"=b."+dimcol+" and b."+dimgroup+"='"+g+"' group by a."+factgroup;
      ResultSet rt=  conn.createStatement().executeQuery(sql2);
      if(rt!=null){
        while( rt.next()){
            String gf=rt.getString(1);
            int i=rt.getInt(2);
            rs.addRow(g,gf,i);
       }
       rt.close();
      }
    }
     r.close();
     return rs;
}
```

Build a jar file and put it into $OSSM_HOME/lib.

Step 3. Create a script file domain_alarm.sql under $OSSM_HOME/scripts/dbtransformer/init as:

```
Drop table if exists domain_alarm;  -- receiver will create a table for each RAW OSSM dimension.
create alias countEx for "com.hp.uoc.h2.udf.UserDefineFunctions.CounterEx";  -- register the UDF
create or replace view domain_alarm as (select * from countEx('OC_DOMAIN','TEMIP_ALARM','OC','DOMAINS','OPERATION_CONTEXT','ORIGINAL_SEVERITY'));    --create the view replace the dropped table
```

DOMAINS	ORIGINAL_SEVERITY	Count
domain30	Major	3600
domain30	Indeterminate	3600
domain30	Warning	3600
domain30	Minor	3600
domain30	Critical	3600
domain31	Major	3598
domain31	Indeterminate	3594
domain31	Warning	3600
domain31	Minor	3596
domain31	Critical	3610
domain10	Major	3600

Step 4. Restart UOC or restart Receiver module using follow commands:

```
$ receiver_console -shutdown
$ receiver_start
```

Step 5. Build a dashboard on the dimension domain_alarm.

5.8 Topology Map

5.8.1 Overview

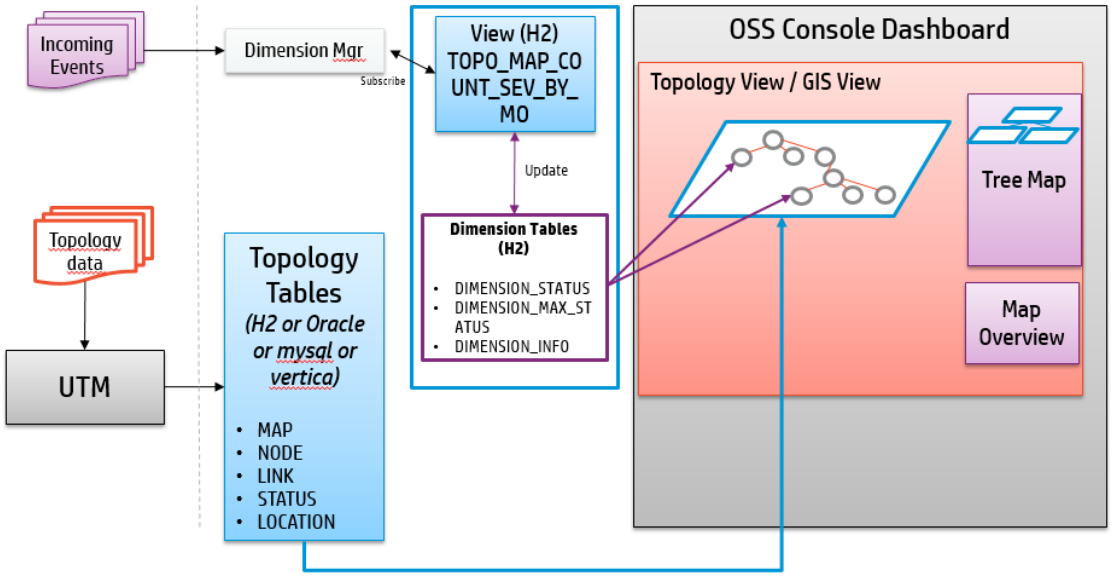


Figure 3 Topology Map Overview

Topology Maps uses topology maps tables to load the map and its hierarchy and uses dimension tables to decorate the topology maps based on dimension values computed by the dimension server.

The topology map table needs to be populated by an external tool like UTM for example.

The topology maps are decorated using computed dimensions.

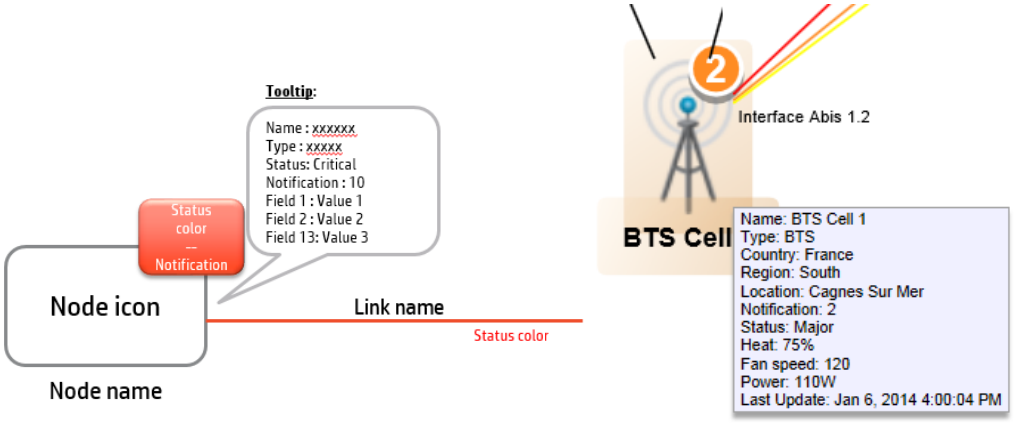


Figure 4.Topology Map node/link visual decoration

5.8.2 Topology Map database

5.8.2.1 Create a database user

Before the installation, you must create a new user (UOC) for the Topology map feature in the Unified OSS Console depending on your database. UOC supports following databases: MySQL, Oracle, H2, Vertica.

Oracle Database:

Please create the user performing the following steps:

1. Log in to the oracle database server as **sysdba**
2. To create a user use the following command:

```
SQL> create user UOC identified by UOC default tablespace users temporary tablespace temp;
```

3. To grant proper privileges:

```
SQL> grant create session,create procedure,create sequence,create table,create trigger,create view to UOC;

SQL> grant unlimited tablespace to UOC;
```

MySQL database:

Please create the user performing the following steps:

1. Log in to the MySQL database as root

```
shell> mysql --user=root mysql
```

2. To create a user use the following command:

```
mysql> CREATE USER 'UOC'@'%' IDENTIFIED BY 'UOC';
```

3. To grant proper privileges:

```
mysql> GRANT ALL PRIVILEGES ON *.* TO 'UOC'@'%' IDENTIFIED BY 'UOC' WITH GRANT OPTION;
```

H2 database:

No need to do anything**, it use** the H2 DB that created by Receiver and the tables created by DB Transformer.

5.8.2.2 Create Topology map tables

You need to create database schema for UOC manually before performing any other configuration. You will be required to execute the scripts mentioned in the following steps.

The database scripts are deployed during OSSM server kit installation into the following location:

$OSSM_HOME/scripts

Following is a list **of the concerned** scripts:

- **uoc_tpm_tables-oracle.sql** for oracle schema creation
- **uoc_tpm_tables-mysql.sql** for mysql schema creation
- **uoc_tpm_tables-h2.sql** for H2 schema creation (Demo only)

To create the schema, you will be required to log into the database with the user created (UOC) and run the SQL script to create the required topology map tables according to the database vendor.

The script will create the following empty tables:

UOC_TPM_LINK
UOC_TPM_LOCATION
UOC_TPM_MAP
UOC_TPM_NODE
UOC_TPM_STATUS

At start of the OSSM server, the following tables will be automatically created into H2 memory database.

UOC_TPM_DIMENSION_INFO
UOC_TPM_DIMENSION_STATUS
UOC_TPM_DIMENSION_MAX_STATUS

5.8.2.3 Topology map table description

5.8.2.3.1 UOC_TPM_MAP

This table describes all map item available in the map hierarchy and their parent relationships. This table will be used to populate the Topology map tree.

Column	Type	Optional (Y/N)	Description	Example
(*) MAP_ID	String(100)	N	Identifier of the map	M15
MAP_NAME	String(100)	N	Name of the map	Paris
PARENT_MAP_ID (**)	String(100)	N	Map identifier of the parent map (if the map is not a top map else null)	Null
DOMAIN_NAME	String(100)	Y	Name of the domain of the map (MPLS...)	Network
SOURCE_ID	String(100)	Y	Decoration key. Not use for MAP today.	Null

(*) Primary key, must be **unique**

(**) It must exist in UOC_TPM_MAP

5.8.2.3.2 UOC_TPM_NODE

This table describes all node item available in a map to build the topology map and the decoration keys to retrieve values computed by dimensions.

Column	Type	Optional (Y/N)	Description	Example
(*) NODE_ID	String(100)	N	Identifier of the node	N8
NODE_NAME	String(100)	N	Name of the node	BTS 345
NODE_TYPE	String(100)	Y	type of the node (router, switch...). 'Default' if not set. This will select the icons from the graphic library. **$OSSM_DATA/topology_maps/images/<type>.png**	BTS
MAP_ID (**)	String(100)	N	Map identifier where the node is child of	M15
CHILD_MAP_ID (**)	String(100)	Y	Map id of the map to navigate to (child map)	M16
LOCATION_ID(***)	String(100)	Y	Location Identifier of the node	LOC5
SOURCE_ID	String(100)	Y	Decoration key associated to this node to dynamically retrieve the information (status, notification, info…) computed by dimensions.	TeMIP:Node_B_123
IP_ADDRESS	String(100)	N	The IP address for the node	

(*) Primary key, must be unique

(**) It must exist in **UOC_TPM**_MAP

(***) It must exist in UOC_TPM_LOCATION

5.8.2.3.3 UOC_TOM_LINK

This table describes all links between nodes available in a map to build the topology map graph and the decoration keys to retrieve values computed by dimensions.

Column	Type	Optional (Y/N)	Description	Example
(*) LINK_ID	String(100)	N	Identifier of the link	L8
LINK_NAME	String(100)	N	Name of the node	Interface A 123
LINK_TYPE	String(100)	Y	Type of the link (ex: optical, interface, fiber…)	Interface A
FROM_NODE_ID (***)	String(100)	N	Identifier of the node FROM	N5
TO_NODE_ID (***)	String(100)	N	Identifier of the node TO	N6
MAP_ID (**)	String(100)	N	Map identifier where the link is child of	M15
CHILD_MAP_ID (**)	String(100)	Y	Map id of the map to navigate to (child map)	M16
SOURCE_ID	String(100)	Y	Decoration key associated to this link to dynamically retrieve the information (status, notification, info…) computed by dimensions.	Null

FROM_PORT	String(100)	N	Port of the node FROM
TO_PORT	String(100)	N	Port of the node TO

(*) Primary key, must be unique

(**) It must exist in UOC_TPM_MAP

(***) It must exist in UOC_TPM_NODE

5.8.2.3.4 UOC_TMP_LOCALTION

This table describes all the location available for nodes.

Column	Type	Optional (Y/N)	Description	Example
(*) LOCATION_ID	String(100)	N	Identifier of the location	LOC5
LOCATION	String(100)	Y	Name of the node	Paris
COUNTRY	String(100)	Y	Country of the location (France, China,...)	France
REGION	String(100)	Y	Region of the location (ex: North, South...)	North
LATITUDE	Double	Y	Identifier of the node TO	48,856614
LONGITUDE	Double	Y	Map identifier where the link is child of	2,352222

(*) Primary key, must be unique

5.8.2.3.5 UOC_TPM_STATUS

This table describes the list of available node and link status. It provides the name and their associated color for the topology map display.

Column	Type	Optional (Y/N)	Description	Example
(*) ID	Number	N	Identifier of the status	6
NAME	String(100)	N	Name of the status (ex: Critical, Major…)	Critical
COLOR	String(20)	N	RGB color associated to the status	255 0 0

(*) Primary key, must be unique

After running the creation script, status table definition contains by default:

ID	NAME	COLOR
0	OK	128 128 128
2	Indeterminate	38 140 196
3	Warning	109 217 69
4	Minor	255 255 0
5	Major	255 140 35
6	Critical	255 0 0
1	Clear	102 255 255

5.8.2.3.6 UOC_TPM_DIMENSION_STATUS

This table is created in H2 database and provides all the dynamic dimensions computation used to decorate the topology maps.

Column	Type	Optional (Y/N)	Description	Example
(*) SOURCE_ID	String(100)	N	Decoration key of the device. Default is MO in alarm.	TeMIP:domain A
(*) STATUS (**)	Number	N	Status identifier of the source to display on the map. Color of the status will be used to color the bubble indicator.	6
SOURCE	String(100)	Y	Source of the data (TeMIP, NNM, SQM...)	TeMIP
NOTIFICATION	String(100)	Y	Notification (alarm count, etc…) of the source to display on the map with a bubble indicator	N5
DIM_NAME	String(100)	Y	Private and internal information to track the dimension that computed this source	
UPDATE_TIMESTAMP	Date	N	Map id of the map to navigate to (child map)	06/01/14 16:00:04,453000000

(*) SOURCE_ID and STATUS are the primary key and must be unique.

(**) It must exist in UOC_TPM_STATUS

5.8.2.3.7 UOC_TPM_DEMENSION_MAX_STATUS

This table is created in H2 database and provides all the dynamic dimensions computation with the highest alarm severity used to decorate the topology maps.

Column	Type	Optional (Y/N)	Description	Example
(*) SOURCE_ID	Number	Y	Decoration key of the device. Default is MO in alarm.	TeMIP:domain A
(*) STATUS	String(100)	Y	Status identifier of the source to display on the map. Color of the status will be used to color the bubble indicator.	6

(*) Primary key, must be unique

5.8.2.3.8 UOC_TPM_DIMENSION_INFO

This table is created in H2 database and provides all the dynamic dimension computation used to decorate the topology maps.

Column	Type	Optional (Y/N)	Description	Example
(*) SOURCE_ID	String(100)	N	Decoration key of the device. Default is MO in alarm.	TeMIP:domain A
FIELD_1	String(100)	Y	Custom Field Name 1 associated to the source to display on the map	Fan

VALUE_1	String(100)	Y	Value associated to the field 1	85%
FIELD_2	String(100)	Y	Custom Field Name 2 associated to the source to display on the map	Heat
VALUE_2	String(100)	Y	Value associated to the field 2	38
FIELD_3	String(100)	Y	Custom Field Name 3 associated to the source to display on the map	Null
VALUE_3	String(100)	Y	Value associated to the field 3	null
UPDATE_TIMESTAMP	Date	N	Map id of the map to navigate to (child map)	06/01/14 16:00:04,453000000

(*) Primary key, must be unique

5.8.3 Topology map dataload

The topology map component used a database as an interface to store and load map data (oracle or mysql).

TIP: *H2 is dedicated to demonstration purpose and should not be used in production environment*

It is recommended to use UTM to populate the topology maps tables and leverage all the advanced features of the product to minimize updates.

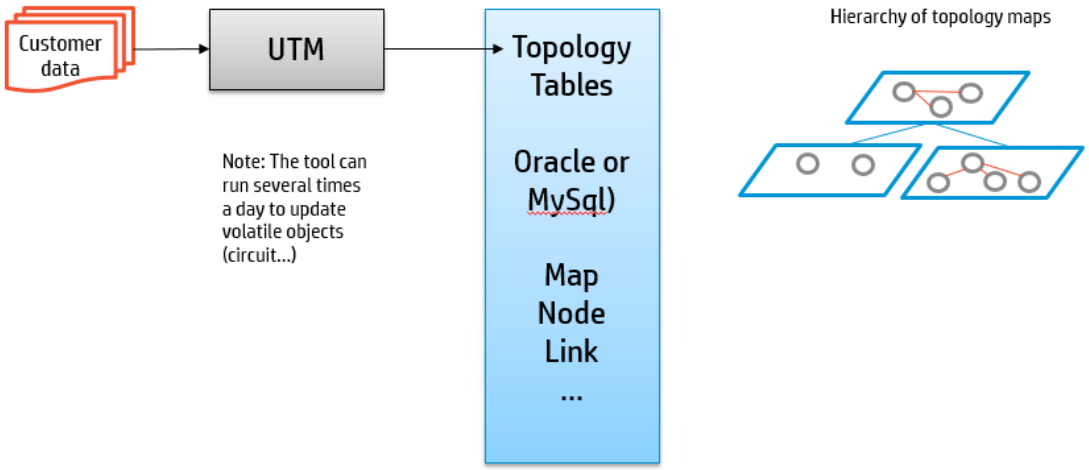


Figure 5Topology Map node/link visual decoration

5.8.4 Tomcat configuration

After database tables creation step, you have to correctly define your database setting to the Tomcat context descriptor file to define required parameter to access to the database tables.

Please edit the file located in **$OSSM_HOME\3pps\Tomcat\conf\context.xml**

And define the correct parameters to setup the login and password of the database user. Here is an example with user UOC / password UOC:

```
<Context>
    <!-- Don't edit this part : Topology map dimension tables are always on H2 -->
```

```
        <Resource name="jdbc/dimension_datasource" auth="Container"
type="javax.sql.DataSource" driverClassName="org.h2.Driver"

url="jdbc:h2:tcp://localhost:9092/mem:uocCenterPool"username="sa"       password=""
maxActive="20" maxWait="-1"/>
    <!-- End don't edit -->

        <!-- Topology Map tables on Oracle -->
        <Resource name="jdbc/OSSM_DATAsource" auth="Container"
              type="javax.sql.DataSource"
driverClassName="oracle.jdbc.OracleDriver"
              url="jdbc:oracle:thin:@127.0.0.1:1521:TOPOv1"
              username="UOC" password="UOC" maxActive="20" maxWait="-1"/>


        <!-- Topology Map tables on mysql
        <Resource            name="jdbc/OSSM_DATAsource"            auth="Container"
type="javax.sql.DataSource"
               maxActive="50" maxIdle="30" maxWait="10000"
               username="UOC" password="UOC"
               driverClassName="com.mysql.jdbc.Driver"
               url="jdbc:mysql://localhost:3306/TOPOv1"/>
        -->

        <!-- Topology Map tables on H2 / Demo only
        <Resource name="jdbc/OSSM_DATAsource" auth="Container"
              type="javax.sql.DataSource" driverClassName="org.h2.Driver"
              url="jdbc:h2:tcp://localhost:9092/mem:uocCenterPool"
              username="sa" password="" maxActive="20" maxWait="-1"/>
        -->
</Context>
```

5.8.5 Topology map Graphic library

All icons and background images are stored in an external directory **$OSSM_DATA/topology_maps**

Graphic type	Location
Topology Map Icons	**$OSSM_DATA/topology_maps/images**
Topology Maps Background	**$OSSM_DATA/topology_maps/backgrounds**

TIP: *All images are in format .PNG with images size : 64x64 pixels.*

Node Icon follows a naming convention to get external icon ***<NodeType>.png.***

If the image is not found, a default image named ***_default_.png*** *is used.*

5.8.6 Topology map GSM sample

The embedded sample describes a global GSM network 3G. Its hierarchy looks like:

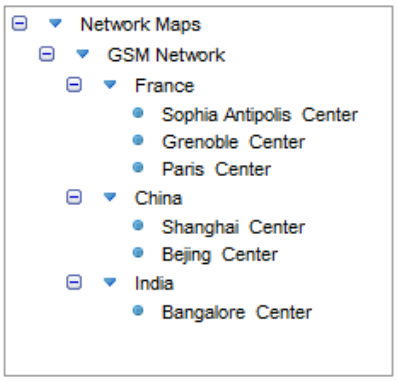


Figure 6 Topology Map View - Network Maps Hierarchy

The topology maps will display as a sample the following maps. The end user can use the map tree to navigate or double-click to nodes to explore the area.

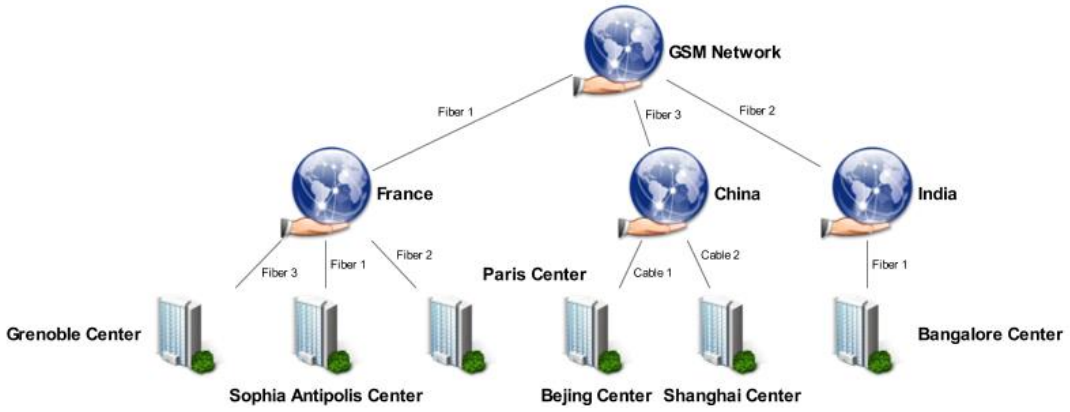


Figure 7 GSM Network

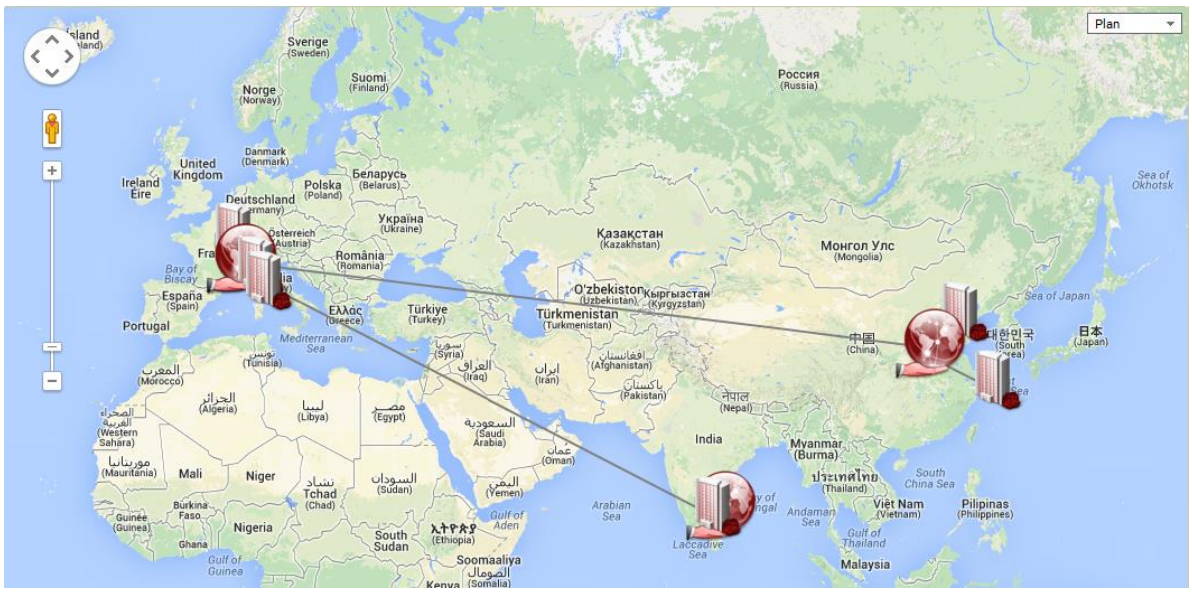


Figure 8 GSM Network (Geographical view)

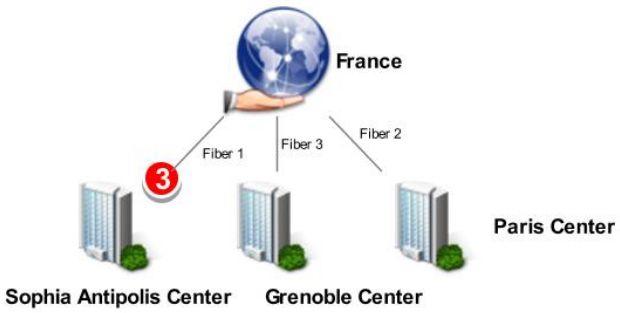


Figure 9 GSM Network/France

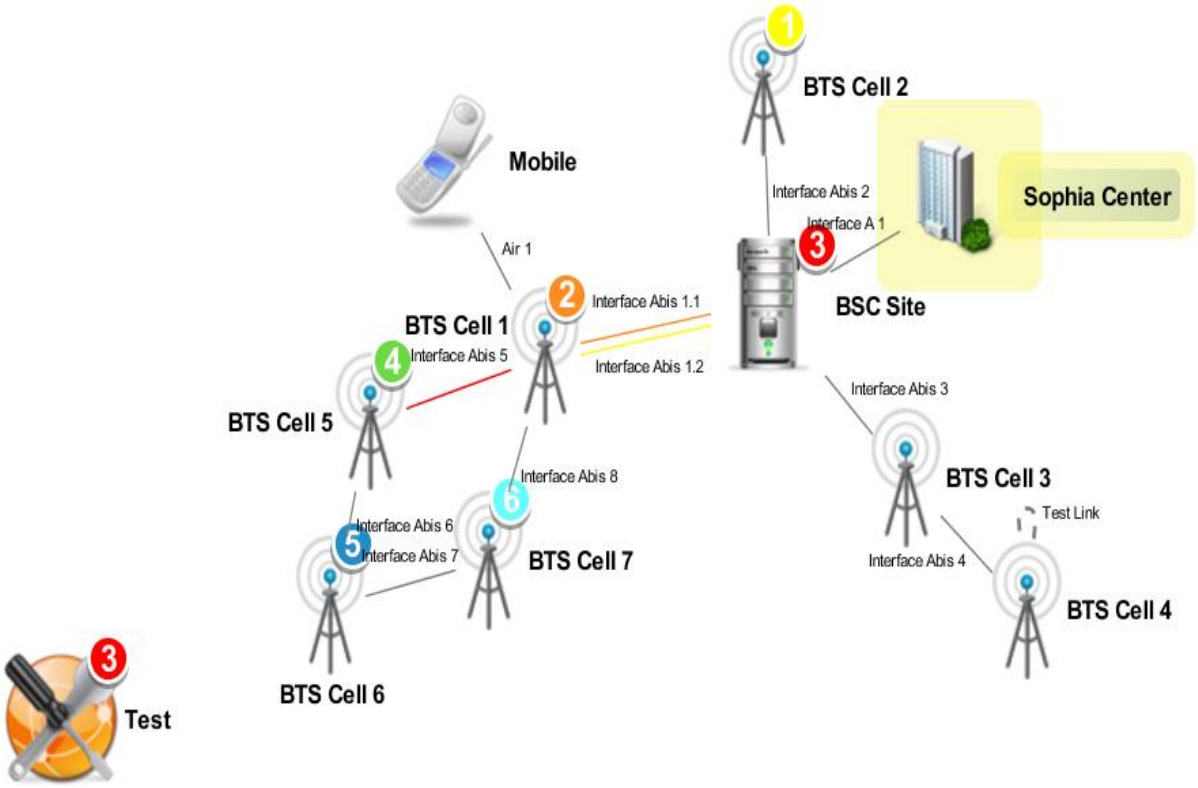


Figure 10 GSM Network/France/Sophia-Antipolis

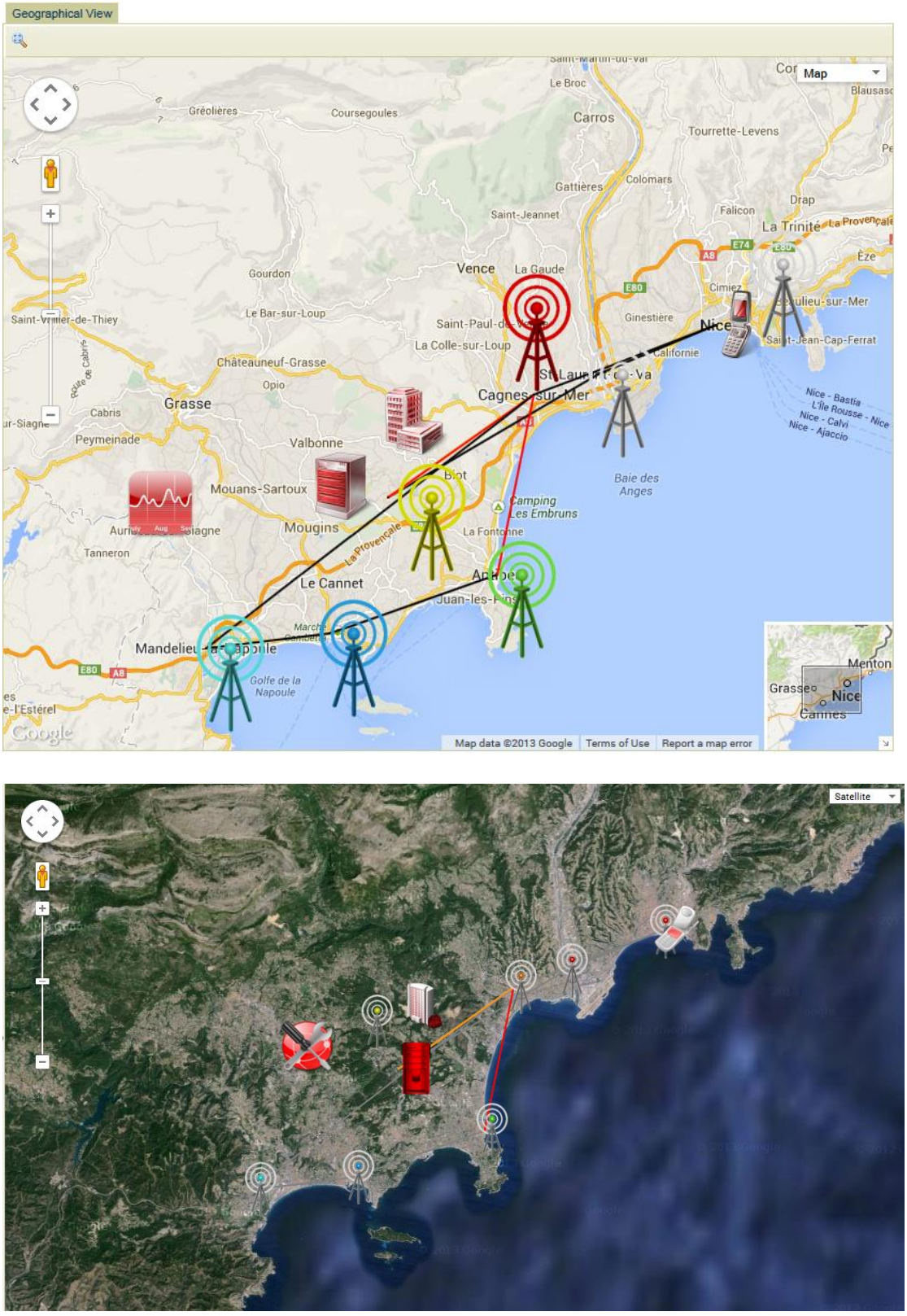


Figure 11 GSM Network/France/Sophia-Antipolis (Geographical view)

Figure 12 GSM Network/France/Grenoble

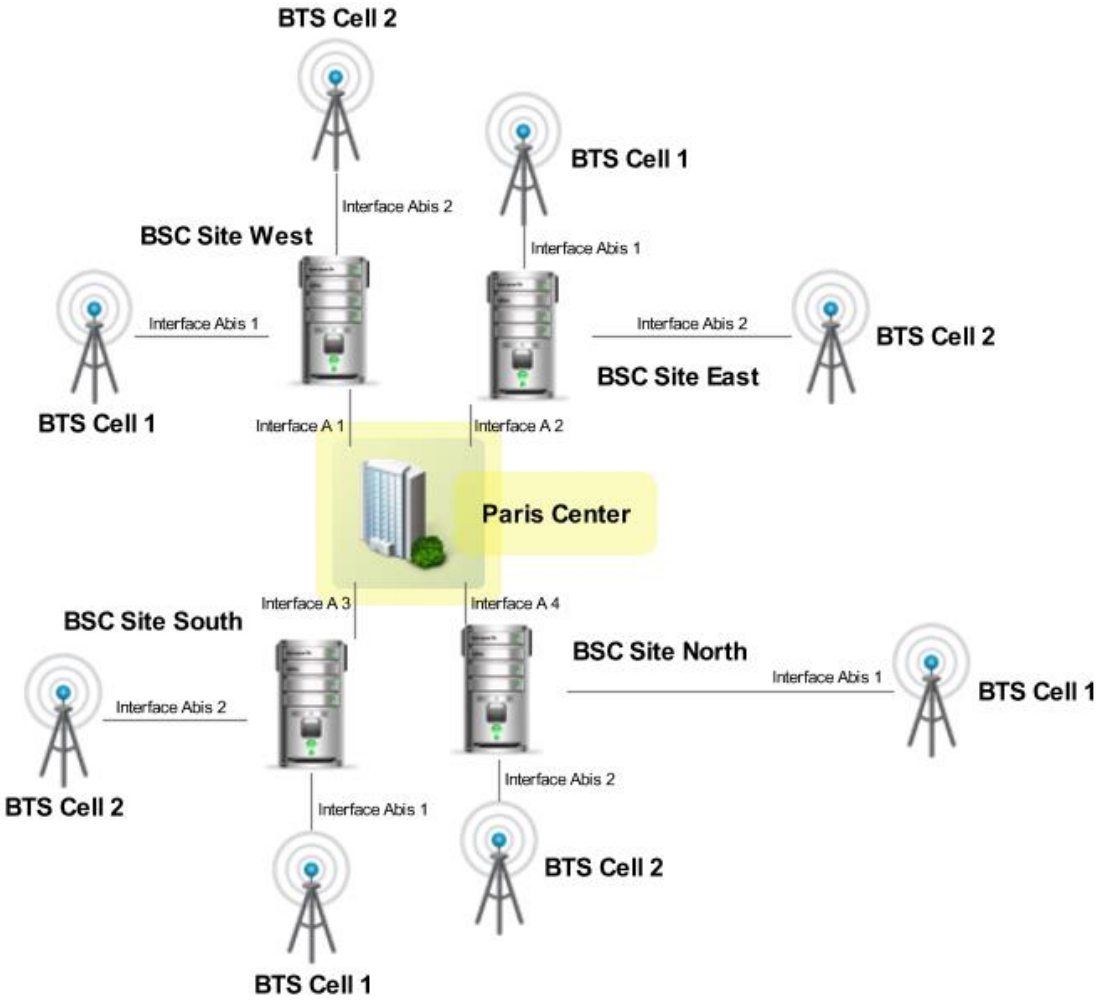


Figure 13 GSM Network / France / Paris

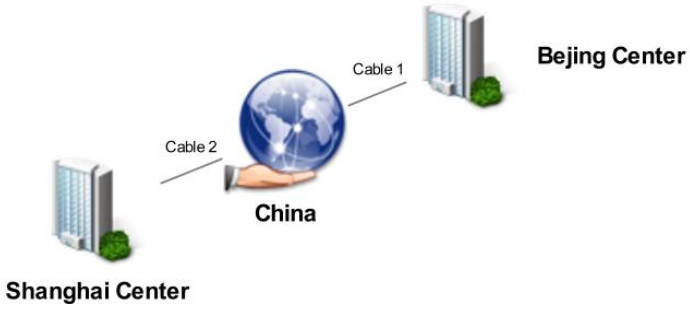


Figure 14 GSM Network / China

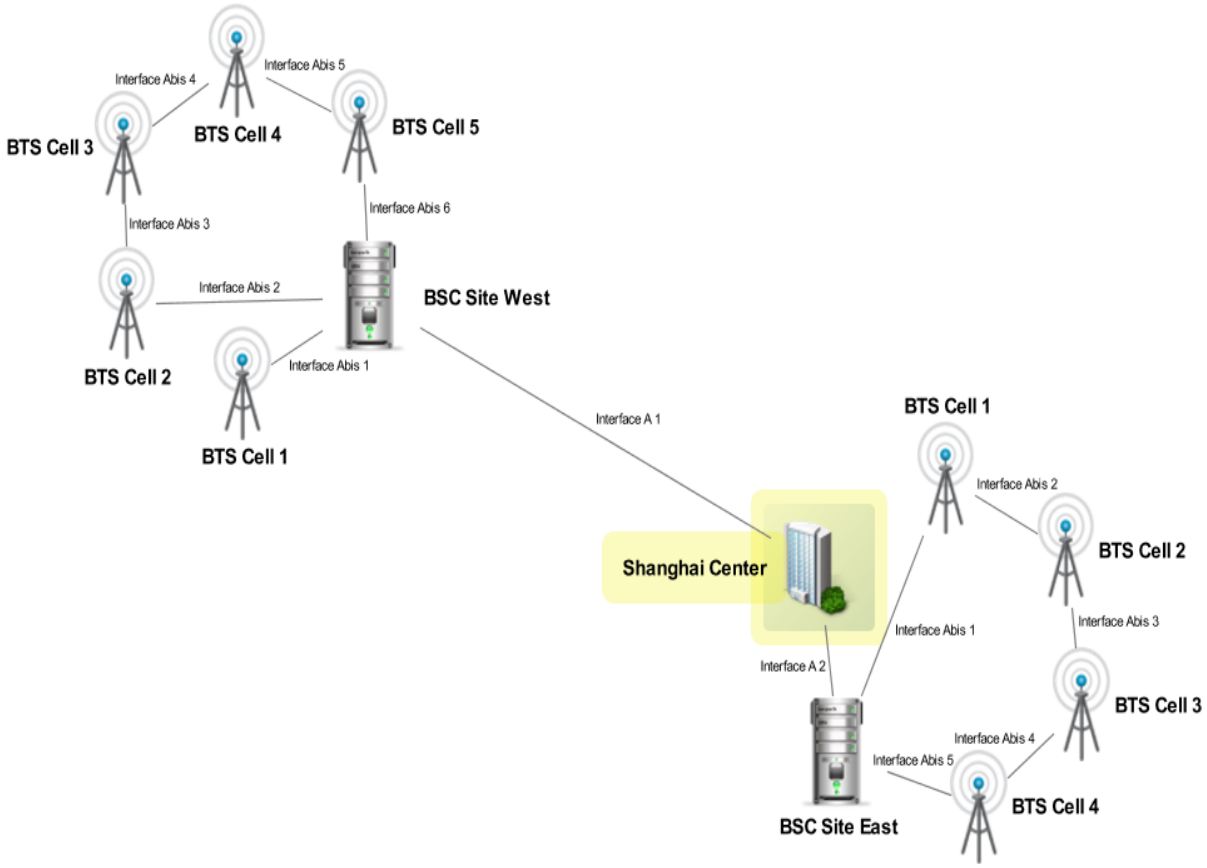


Figure 15 GSM Network / China / Shanghai

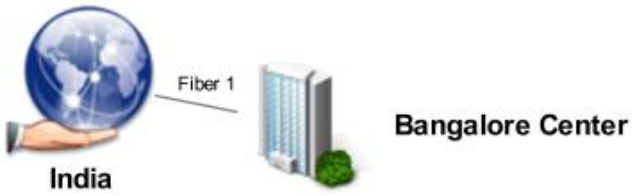


Figure 16 GSM Network / India

5.8.7 Customized Icon

User can use their customized icon images for node. The type of the image should be PNG, and the name of the image should be lower case letters. Then put the icon images into $OSSM_HOME/topology_maps/images.

5.9 HTTPS

5.9.1 Importing Self-signed Certificate

Below is step of HTTPS configuration in UOC.

1. Generate key store

The domain name with red italic characters should be replaced by the domain name of the server where the UOC is running.

The blue italic character should be decided by the operator and maintained for the certificate lifecycle

```
keytool -genkey -alias uocssl -keyalg RSA -keysize 1024 -keypass uocssl -validity
365 -dname "CN=HITTBSS5, OU=hp, O=ldap, L=shanghai,      ST=shanghai,   C=CN"   -
keystore /tmp/uocssl.keystore -storepass uocssl
```

For more about keytool command, you could refer following
URL:http://docs.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html

2. Export certificate

The orange italic part is decided by last step that the alias you made, in this example is “uocssl”.

The blue italic part should be decided by the operator

```
keytool    -export    -alias    uocssl    -keystore    /tmp/uocssl.keystore    -file
      /tmp/uocssl.crt -storepass uocssl
```

3. Edit $OSSM_HOME/3pps/tomcat/conf/server.xml of CAS server tomcat enable HTTPS

```
      <!-- clientAuth=false means only need server certificate, it is one way SSL

           clientAuth=want means client certificate exits, validate it, but not
mandatory clientAuth=true means client certificate is required, it is 2 way SSL -->
<Connector  port="8443"  protocol="HTTP/1.1"  SSLEnabled="true"  maxThreads="150"
scheme="https"          secure="true"          keystoreFile="/tmp/uocssl.keystore"
keystorePass="uocssl" clientAuth="false" sslProtocol="TLS" URIEncoding="UTF-8"/>
```

4. Import certificate to the keystore of JRE of the web server

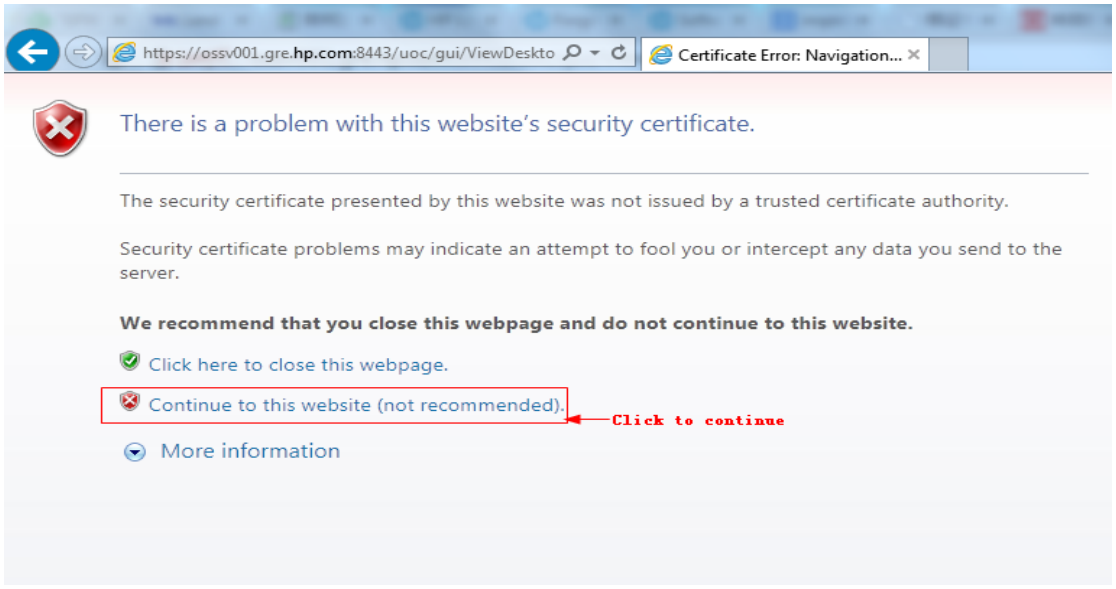
This step is for the JAVA applications that need to visit UOC by URL, for other kinds of applications, need to find their own ways.

keytool -import -keystore $JAVA_HOME/jre/lib/security/cacerts -file /tmp/uocssl.crt -alias uocssl Enter keystore password: changeit (changeit is the default password of JRE).

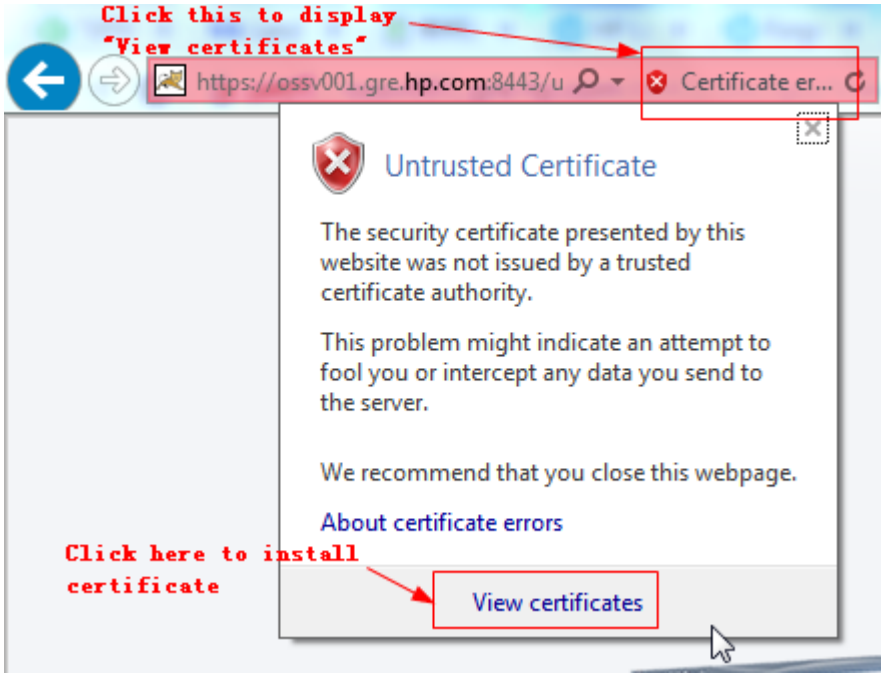
5. End user trust the certificate. (If customer is using a certificate published by a trusted 3-rd party CA, we may do not need this)

a) End user should use domain name to visit the UOC URL.

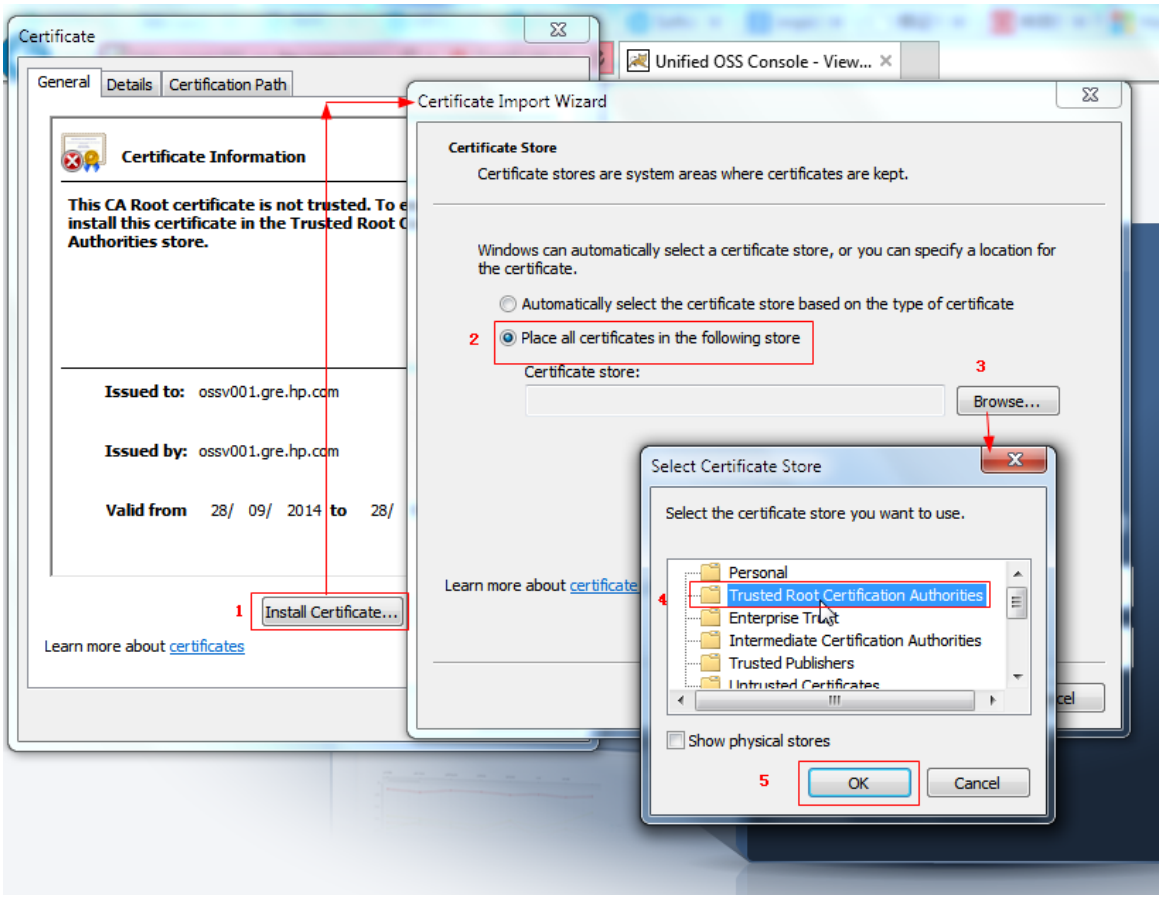
b) When first time to visit the UOC URL, you could see a certificate error notification in the browser, and click the “Continue to this web site” to display next page



c) Click the Certificate Error link to view certificate.



d) Import certificate to trusted root certificate database



For other browsers import certificate, please refer to the following URL:

http://docs.oracle.com/cd/E19146-01/821-1828/gfyvq/index.html

5.9.2 Importing Third Party Certificate

Please follow Tomcat official guide to install a third certificate:
http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html#Installing_a_Certificate_from_a_Certificate_Authority

NOTE: **Configuring and maintaining the TLS security configuration is customer responsibility.**

5.10 SSO Configuration

To be able to support SSO with SAML2.0, we assume that:

1. Before Install ADFS, please make sure Active Directory installed, and SSL configured enabled for IIS, make sure https://localhost can be available by browser. The Active Directory installation please refer to office site.

2. ADFS2.0 (Active Directory Federation Server) has been installed. If not, please refer to the installation guide from the official site:

http://www.microsoft.com/en-us/download/details.aspx?id=10909

3. ADFS2.0 has been well configured. If not, please refer to the official site and run ADFS 2.0 Federation Server Configuration Wizard in the ADFS 2.0 Management Console.

4. DNS name of your Windows Server is available at the UOC.

5. UOC has been configured to use HTTPS (required by ADFS). If not, please refer to chapter 5.9 HTTPS.

6. UOC has been correctly installed and configure. If not, please refer to installation Guide, and make sure that "authentication_*.jar" has been correctly deployed under:
   $OSSM_HOME/3pps/tomcat/webapps/uoc/WEB-INF/lib/

To initialize IDP metadata:

1. Download ADFS2.0 metadata from:
   https://*servername*/FederationMetadata/2007-06/FederationMetadata.xml
   where servername is the ADFS2.0 installed host name.

2. Store the downloaded file under:
   $OSSM_HOME/3pps/apache-tomcat-7.0.64/webapps/uoc/WEB-INF/classes/metadata/

3. Add the configuration file named "metadatas.xml" under $OSSM_DATA/conf/

The content is like in the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<Metadatas>
<IDP>
<name>adfs2.0</name>
<metadataFile>/metadata/FederationMetadata.xml</metadataFile>
<url>https://servername/FederationMetadata/2007-06/FederationMetadata.xml</url>
</IDP>
</Metadatas>
```

Attribute	Description
Name	Idp product name
metadataFile	The idp metadata file stored in OSSM under $OSSM_HOME/3pps/apache-tomcat-7.0.64/webapps/uoc/WEB-INF/classes/metadata/, it's strongly recommend to put the files here. If you want to change the file name, please don't forget to modify the idp.xml under $OSSM_DATA/conf/
url	The url is the download link from IDP product, it's optional setting.

To initialize SP metadata:

1. Make sure that Ossm starts successfully, download the SP metadata file from:
   https://*servername*/uoc/saml/metadata
   where servername is the OSSM installed hostname.

2. Store the download file to ADFS2.0 , In ADFS 2.0 Management Console select "Add Relying Party Trust"

3. Select "Import data about the relying party from a file" and select the metadata.xml file download earlier. Select Next

4. The wizard may complain that some content of metadata is not supported. You can safely ignore this warning

5. Continue with the wizard. On the "Ready to Add Trust" make sure that tab endpoints contains multiple endpoint values. If not, verify that your metadata was generated with HTTPS protocol URLs

6. Leave "Open the Edit Claim Rules dialog" checkbox checked and finish the wizard

7. Select "Add Rule", choose "Send LDAP Attributes as Claims" and press Next

8. Add NameID as "Claim rule name", choose "Active Directory" as Attribute store, choose "SAM-Account-Name" as LDAP Attribute and "Name ID" as "Outgoing claim type", finish the wizard and confirm the claim rules window

9. Open the provider by double-clicking it, select tab Advanced and change "Secure hash algorithm" to SHA-1

10. Modify the configuration file named “metadatas.xml” under:
    $OSSM_DATA/conf/ to add SP config.

The content is like the part highlighted in red of the example below:

```
<?xml version="1.0" encoding="UTF-8"?>
<Metadatas>
<IDP>
<name>adfs2.0</name>
<metadataFile>/metadata/FederationMetadata.xml</metadataFile>
<url>https://servername/FederationMetadata/2007-06/FederationMetadata.xml</url>
</IDP>

<SP>
<name>uoc2.2</name>
<metadataFile>/metadata/uoc_saml_metadata.xml</metadataFile>
<url>https://192.168.152.131:8443/uoc/saml/metadata</url>
</SP>
</Metadatas>
```

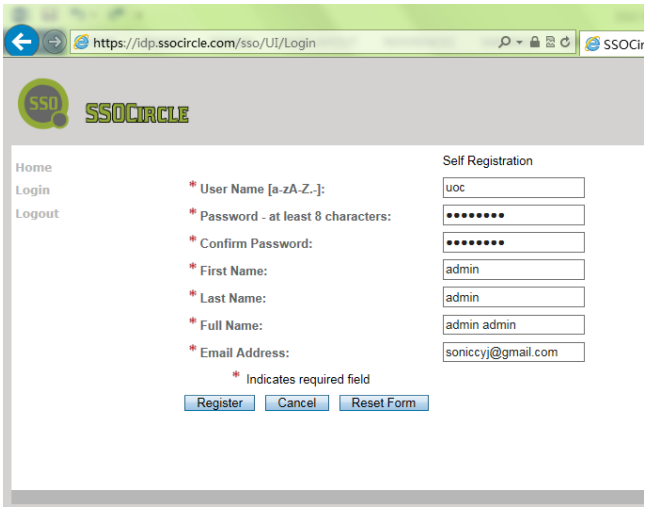
Attribute	Description
Name	SP app name
metadataFile	The sp metadata file stored in OSSM under $OSSM_HOME/3pps/apache-tomcat-7.0.64/webapps/uoc/WEB-INF/classes/metadata/, it’s strongly recommend that put the files here. If you want to change the file name, please don’t forget to modify the idp.xml under $OSSM_DATA/conf/
url	The url is the download link from SP app, it’s optional setting.

11. If you want to change the EntityID of metadata you downloaded before, please edit file $OSSM_HOME/3pps/apache-tomcat-7.0.64/webapps/uoc/WEB-INF/classes/webapp-context.xml, change the red line below and restart OSSM.
    `<bean id="metadataGeneratorFilter"`

```
 class="org.springframework.security.saml.metadata.MetadataGeneratorFil
ter">
        <constructor-arg>
            <bean
class="org.springframework.security.saml.metadata.MetadataGenerator">
                <property name="entityId" value="uoc_sp_local" />
                <property name="requestSigned" value="true" />
            </bean>
        </constructor-arg>
</bean>
```

To test with ssocircle in public network:

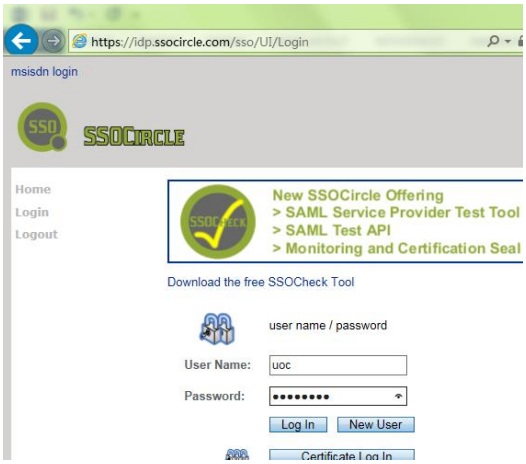
1. Open http://www.ssocircle.com/en/ and follow the introduction to register a new account.



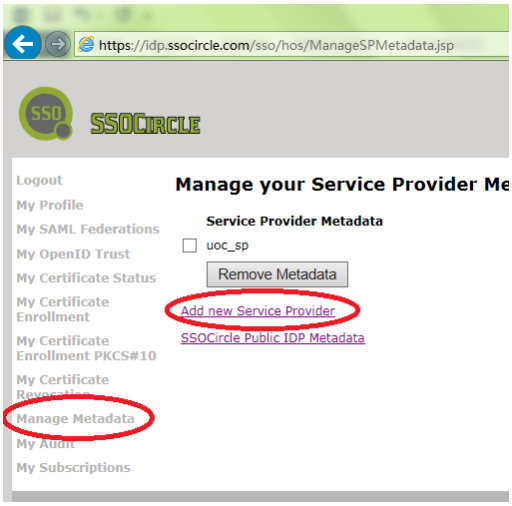
For example, register username uoc, password test@123

2. Download metadata from the UOC link, for example the server is 16.17.100.35: http://16.17.100.35:8080/uoc/saml/metadata

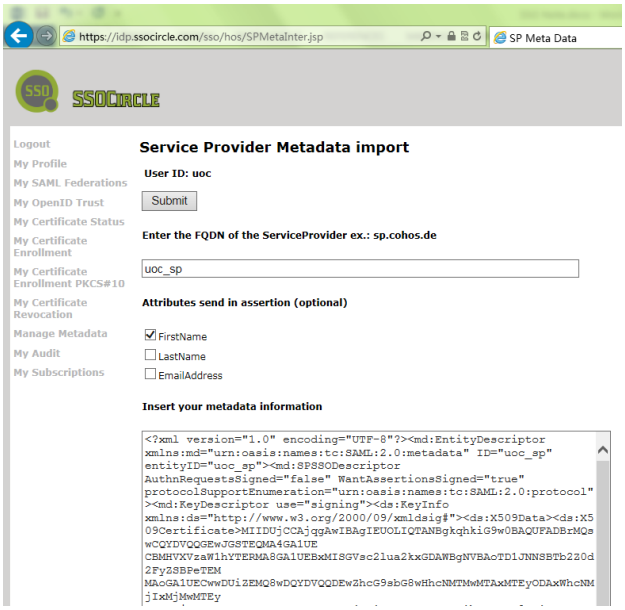
3. Login ssocircle with example account uoc/test@123.



4. Upload metadata on web site.



Click “Manage Metadata” in the left menu, then click “Add new Service Provider”.

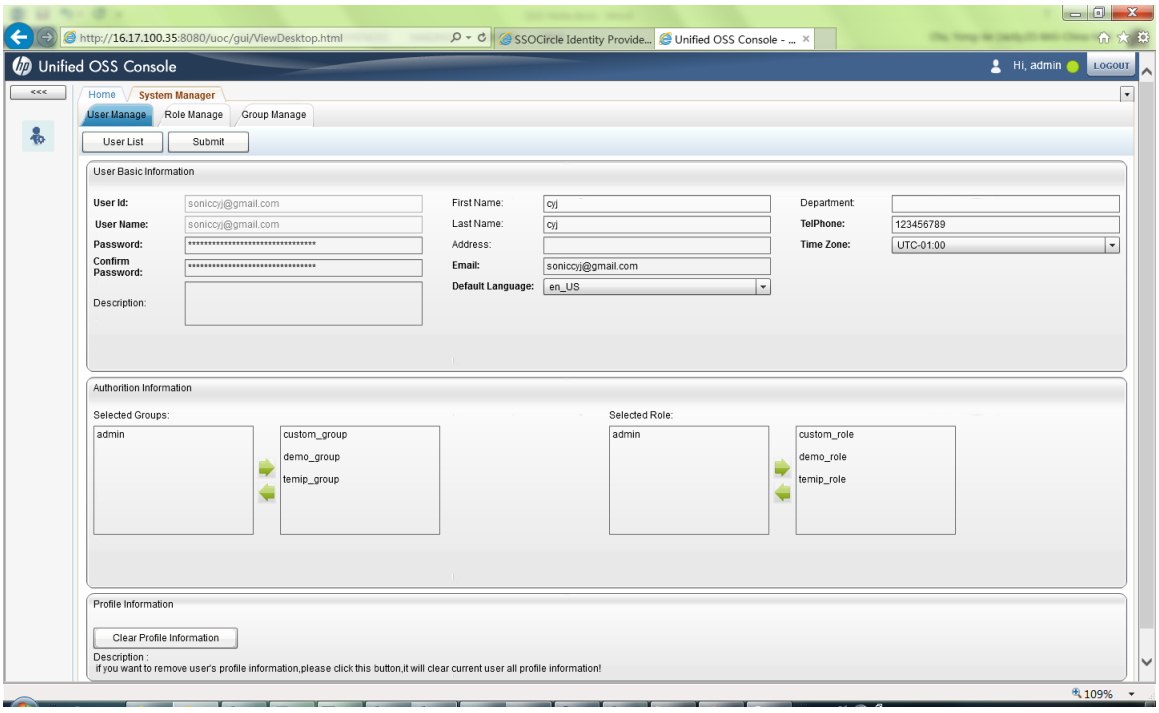


Input the value of entity ID and the metadata information in the “uoc_saml_metadata.xml” downloaded from UOC, check “FirstName”, then click “Submit” button.

After that, check the successful page, and access the metadata by clicking the “Manage Metadata” menu.

5. Logout from ssocircle

6. Create a new user by using the email address that registered in ssocircle.
For example user id and name is soniccyj@gmail.com.



7. Validate the SSO.
   - Open the login page in UOC: http://16.17.100.35:8080/uoc/saml/login, then it will automatically jump to the SSO login page.
   - Login as the account: uoc/test@123.
   - Web page will automatically jump to UOC and login successful.

5.11 LDAP Configuration

To be able to integrate with Active Directory, we assume that:

1. Active Directory has been installed and configured. If not, please refer to Active Directory installation Guide from the official site. We recommend to install version 2000 or 2003.

2. If the installed Active Directory needs security communication, please refer to configuration guide to install CA from official site.

3. UOC has been correctly installed. If no, please refer to installation Guide, and make sure that "authentication_*.jar" is deployed under $OSSM_HOME/3pps/tomcat/webapps/uoc/WEB-INF/lib/

Add the configuration file named "authentication.xml" under $OSSM_DATA/conf/

The content is like blow example:

```
<?xml version="1.0" encoding="UTF-8"?>
<Auth>
<AD>
<domain>uoc.com</domain>
<url>ldap://192.168.152.130:389/</url>
<enable>no</enable>
<ignoreUOCPassValidation>yes</ignoreUOCPassValidation>
</AD>
```

```
</Auth>
```

Attribute	Description
Domain	Active Directory Domain Name
url	Active Directory ldap protocol connection URL name, AD default port is “389”
enableAuthentication	Enable or disable ad authentication in UOC, “yes” or “no”
ignoreUOCPasswordValidation	If enableAuthentication=yes, this settings will work and this setting is to enable or disable password validation in UOC,set “yes” or “no”
enableSSL	It’s optional , if need SSL communication , set value as “Yes”
keystore	It’s optional, if enableSSL = “Yes”, need set value as keystore file path like:/tmp/ad.keystore
keyPassword	It’s optional, if enableSSL = “Yes”, Set value as keystore password

5.12 Password Encryption

The OSSM server supports both MD5 (default) and PBKDF2 encryption method. Before Ossm startup, please make sure the preferred method is correctly defined in ${OSSM_DATA}/conf/cm_context.xml.

```
<bean id="dataSource" class="com.hp.uoc.cm.um.util.CmDataSource"
destroy-method="close">
<property name="driverClassName" value="org.h2.Driver" />
                                                <property                 name="url"
value="jdbc:h2:tcp://localhost:9192/${OSSM_DATA}/db/uoc_umm_md5;ifexists=true"
/>
<property name="username" value="sa" />
<property name="password" value="" />
</bean>
```

driverClassName: commonly don’t need change

url: if you use “md5” encryption method, it don’t need change, but if you use “pbkdf2” encryption method, you only need change the database name as:

‘**jdbc:**h2:tcp://localhost:9192/${OSSM_DATA}/db/uoc_umm_pbkdf2;ifexists=true’

Username:H2 database user name, commonly is “sa”

Password: H2 Database user’s password, default is empty, but if you have change the user’s password, here need change corresponding.

Chapter 6 Uninstallation

This chapter describes how to uninstall the server subset of UOC product.

6.1 Uninstallation

When uninstalling UOC, the OSSM server must be firstly stopped.

```
$ $OSSM_HOME/bin/ossm stop
```

⚠ CAUTION: If the installation has been done with root user, to stop OSSM server, user has to login to OSSM server as uoc user because only uoc user is allowed to operate on UOC program.
If the installation has been done with a non-root user, the OSSM server will have to be stopped by this non-root user

Check that no processes remains:

```
$OSSM_HOME/bin/ossm show
```

If some processes are still running, you can stop them with the standard Unix “kill” command.

You can check the currently installed version of UOC with the following command:

```
$OSSM_HOME/bin/ossm inventory
```

Then use the following script to uninstall the OSSM server:

```
$OSSM_HOME/scripts/uninstall-ossm-server.sh


Currently installed OSSM server packages:
               [0]     OSSMSERVER-x2.2-03A.noarch
Select the one to un-install ('Enter' to Cancel): 0
removing package OSSMSERVER-X2.2-03A.noarch ...
OSSM server package OSSMSERVER-X2.2-03A.noarch removed successfully
```

6.2 Uninstalling verification

If the installation had been done with root user, the default RPM db path is usually used. The un-installation verification can be done without specifying the RPM db Path option.

```
$ rpm –qa | grep UOC
```

If the installation had been done instead with non-root user, a specific RPM db path was used.

```
$ rpm –qa --dbpath $UOC_RPMDBPATH | grep UOC
```

If the removal was successful, the $OSSM_HOME folders should be empty.

Chapter 7 Troubleshooting

7.1 Frequent issues / error messages

1	can't access UOC through web by IP:8080/UOC/auth/login.html	Make sure all processes are running, especially the tomcat server one (server the web pages we want to display in the browser). Use the “ossm show” command to check the status of the processes on the server side. Check also for exceptions in the log files. Check for firewall configuration, and that the server system is effectively accessible for HTTP requests.
2	After updating the period for snapshot in Dashboard, there isn't any change in the Dashboard view.	Restart the OSSM server in order to load the latest updates.
3	Error in temip_adapter.log Exception in thread "main" javax.jms.JMSException: Could not connect to broker URL: tcp://16.173.245.94:61616. Reason: java.net.Conn ectException: Connection refused	Please check the firewall settings for this server, to make sure the TWS port isn’t blocked.
4	Failed to start Apache ActiveMQ	If after starting OSSM ActivMQ is not started. Check the log: $OSSM_HOME/3pps/apache-activemq-5.9.0/data/activemq.log If you get the following error: 2015-08-03 18:51:09,257 | ERROR | Failed to start Apache ActiveMQ ([localhost, ID:ossv035.gre.hp.com-48834-1438620669088-0:1], java.io.IOException: Transport Connector could not be registered in JMX: Failed to bind to server socket: amqp://0.0.0.0:5672?maximumConnections=1000&wireFormat.maxFrameSize=104857600 due to: java.net.BindException: Address already in use) | org.apache.activemq.broker.BrokerService | main This means that maybe the following service qpidd is already using the same port. To check which process uses the port please execute the following command: netstat -plnt | grep 5672 tcp 0 0 0.0.0.0:5672 0.0.0.0:* LISTEN 2404/qpidd tcp 0 0 :::5672 :::* LISTEN 2404/qpidd It is qpidd service [root@ossv035 data]# ps -ef | grep 2404 root 587 554 0 18:57 pts/5 00:00:00 grep 2404 qpidd 2404 1 0 Jul23 ? 00:01:16 /usr/sbin/qpidd --data-dir /var/lib/qpidd –daemon you should stop the service # /sbin/service qpidd stop Stopping Qpid AMQP daemon: [OK] Then restart UOC

Chapter 8 Logging configuration

8.1 Configuring OSSM Logs

OSSM uses Logback to output log statements to a variety of output targets. The logging behavior is controlled by editing an external configuration file ($OSSM_DATA/conf/logback.xml), without modifying the application.

Logback has three main components (loggers, appenders and layout) which work together to log messages according to levels, and to control at runtime how these messages are formatted and where they should be logged.

To enable, disable or change the level of tracing in the log, the administrator needs to modify the **logback** configuration file located under:

$OSSM_HOME/conf/logback.xml

It is recommended to follow recommendations in logback documentation to manage correctly the log level and the log layout. Refer to http://logback.qos.ch/manual/index.html

The sample configuration looks as below:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration scan="true" scanPeriod="10 seconds" debug="true">
  <appender name="STDOUT" class="ch.qos.logback.core.ConsoleAppender">
        <encoder>
          <pattern>%d{HH:mm:ss.SSS}      [%thread]      %-5level      %logger{36}
- %msg%n</pattern>
        </encoder>
  </appender>
```

```
<appender                                                    name="CONF_MAN"
class="ch.qos.logback.core.rolling.RollingFileAppender">
        <File>${OSSM_DATA}/logs/CONF_MAN.log</File>
        <rollingPolicy
class="ch.qos.logback.core.rolling.TimeBasedRollingPolicy">
                 <fileNamePattern>${OSSM_DATA}/logs/UOC-%d{yyyy-MM-
dd}-%i.log.gz</fileNamePattern>
               <timeBasedFileNamingAndTriggeringPolicy
class="ch.qos.logback.core.rolling.SizeAndTimeBasedFNATP">
           <!-- or whenever the file size reaches10MB -->
           <maxFileSize>10MB</maxFileSize>
        </timeBasedFileNamingAndTriggeringPolicy>
        <!-- keep 30 days' worth of history -->
        <maxHistory>30</maxHistory>
        <append>true</append>
        </rollingPolicy>
    <layout class="ch.qos.logback.classic.PatternLayout">
      <Pattern>%d %p %t %c - %m%n</Pattern>
    </layout>
  </appender>

    <logger name="com.hp" level="INFO">
      <appender-ref ref="CONF_MAN"/>
    </logger>

    <root level="DEBUG">
        <appender-ref ref="STDOUT"/>
    </root>

</configuration>
```

In the sample configuration above, we only declared one logger named “com.hp”, and whose level is “INFO”. For later use, it can be defined as several different loggers, with each one a different name, so that we can distribute for each module with different log level.

8.2 Log Files

Every OSSM component logs information in a dedicated log file. All log files are under **${OSSM_DATA}/logs**

Log Name	**Description**
NOM_TEMIP_ADAPTER.log	NOM TeMIP Adapter logs
CSV_ADAPTER.log	CSV Adpater logs
DB_ADAPTER.log	Database Adapter logs
CONF_MAN.log	Configuration Management logs
DB_TRANSFORMER.log	DB Transformer logs
ARRIVAL.log	Arrival logs
PRESENTER.log	Presenter logs
QC_PROVIDER.log	QC Provider logs
RECEIVER.log	Receiver logs

LICENSE_MAN.log	License logs

Default level for all these loggers is: **INFO**

8.3 Log Levels

The administrator can change the name of the log file if needed and the level of traces. It can be one of the following levels:

- TRACE
- DEBUG
- **INFO (Default)**
- WARN
- ERROR

Warning: a level of TRACE or DEBUG will produce megabytes of logging and slow startup of Tomcat. These levels must be reserved for time-bounded troubleshooting sessions, for example on request by the Support team.

Example of log level INFO for component Receiver

…

```
<logger name="com.hp.uoc.centerpool" level="INFO">
  <appender-ref ref="RECEIVER" />
</logger>
```

8.4 dLog Appender

An output destination for logging is called an appender and can be changed in the XML configuration file. Default appenders are console (output) or files (stored on disk)

Refer to the pattern appender http://logback.qos.ch/manual/appenders.html to get the detailed string definition to use.

Example of appender customization:

Logs will be stored in a rolling files whose maximum size is 10MB, and up to 5 previous files are stored. Current tracing will be in file RECEIVER.log

…

```
<appender name="RECEIVER" class="ch.qos.logback.core.rolling.RollingFileAppender">
<File>${OSSM_DATA}/logs/RECEIVER.log</File>
  <rollingPolicy class="ch.qos.logback.core.rolling.TimeBasedRollingPolicy">
    <fileNamePattern>${OSSM_DATA}/logs/RECEIVER-%d{yyyy-MM-dd}-%i.log.gz</fileNamePattern>
      <timeBasedFileNamingAndTriggeringPolicy
class="ch.qos.logback.core.rolling.SizeAndTimeBasedFNATP">
      <!-- or whenever the file size reaches10MB -->
      <maxFileSize>10MB</maxFileSize>
    </timeBasedFileNamingAndTriggeringPolicy>
    <!-- keep 30 days' worth of history -->
    <maxHistory>30</maxHistory>
    <append>true</append>
```

```
        </rollingPolicy>
      <layout class="ch.qos.logback.classic.PatternLayout">
        <Pattern>%d %p %t %c - %m%n</Pattern>
      </layout>
    </appender>
```

8.5 Log Layout

Administrator can customize the output destination but also the output format. This is achieved by associating a layout with an appender. The layout is responsible for formatting the logging request according to the user's wishes, whereas an appender takes care of sending the formatted output to its destination.

Refer to the pattern layout http://logback.qos.ch/manual/layouts.html to get the detailed string definition to use.

Example of customized layout

```
<appender name="RECEIVER" class="ch.qos.logback.core.rolling.RollingFileAppender">
    …
   <layout class="ch.qos.logback.classic.PatternLayout">
     <Pattern>%d %p %t %c - %m%n</Pattern>
    </layout>
  </appender>
```