Cisco Systems Advanced Services

Unified Communications Operations Manager/Service Monitor Multiple Server and Redundant Design Considerations

Version 1.1

Contents

About This Document

Author: Elvis Hernandez

Change Authority: Cisco Systems Advanced Services

History

Version No.	Issue Date	Status	Reason for Change
1.0	2-28-2008	Draft	First release
1.1	3-8-2008	Final	Second release

Review

Reviewer's Details	Version No.	Date
Elvis Hernandez	1.0	02-28-2008
June Zheng	1.0	03-01-2008

Change Forecast: <Low>

This document will be kept under revision control. A printed copy of this document is considered uncontrolled.

Introduction

Document Purpose

This document defines how to design for Unified Communications network management using Unified Communications Operations Manager and Service Monitor for large networks requiring more than a single server.

This design document consists of a number of components. These include:

- Best practices guidance
- Information from associated documentation: User guide, deployment guide

Intended Audience

The intended audience of this document is professional services, delivery agencies, their partners, and the technical staff of the customer.

Scope

The scope of this document is Unified Communications management design for large customers with regional or geographic based needs, or customers that are using Operations Manager/Service Monitor as a managed service provider (MSP) to provide a managed service to other customers. Two example scenarios and considerations are examined.

Assumptions and Caveats

- There will be more than one Operations Manager server, managing more than 1000 devices. Thus, Service Monitor cannot be coresident with Operations Manager and requires its own dedicated server.
- Each Operations Manager server may have up to the maximum amount of IP Phones (30,000) or other maximum limit (for example, 2000 devices) before an additional Operations Manager server is required.
- As a managed service, customer networks managed by a single Operations Manager server cannot have overlapping IP network addresses. Operations Manager does not support multitenant environments.
- The Operations Manager server requirements to support 30,000 phones is a Dual Pentium 4 or Xeon processor equal to or greater than 3 GHz; 4 GB RAM; 4 GB swap file; 60 GB hard drive running on Windows 2003 Server SP1. See Tables 1 and 2 for system capacity and system requirements.
- Operations Manager and Service Monitor disaster recovery/backup is required.

Related Documents

- Operations Manager User Guide

  http://www.cisco.com/en/US/products/ps6535/products_user_guide_list.html
- Operations Manager Deployment Guide

  http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6491/ps6705/ps6535/ps7121/prod_white_paper0900aecd8067e2e6.pdf

- Operations Manager Data Sheet

  http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6491/ps6705/ps6535/ps7121/product_data_sheet0900aecd80578652.html

- Operations Manager Installation Guide

  http://www.cisco.com/en/US/products/ps6535/prod_installation_guides_list.html

System Capacity

Table 1 shows the system capacity for a single Cisco Unified Operations Manager server.

Table 1. System Capacity (per Cisco Unified Operations Manager 2.0 Server)

System Parameter	Capacity
Monitored phones	30,000
Monitored devices	2000
Monitored Cisco Unified Communications Manager clusters	30
Monitored Cisco Unified Communications Manager Express routers	500
Monitored Survivable Remote Site Telephony (SRST) routers	500
Concurrent synthetic tests	250
Concurrent node-to-node (Cisco IOS® Software IP SLA) tests	250
Concurrent client (browser) logons	5

Please view the other Operations Manager limits at http://www.cisco.com/en/US/docs/net_mgmt/cisco_unified_operations_manager/2.0.1/installation/guide/prereq.html#wp1100174.

System Requirements

Table 2 lists the system requirements for a standalone Cisco Unified Operations Manager deployment.

Table 2. System Requirements for Standalone Cisco Unified Operations Manager Deployments

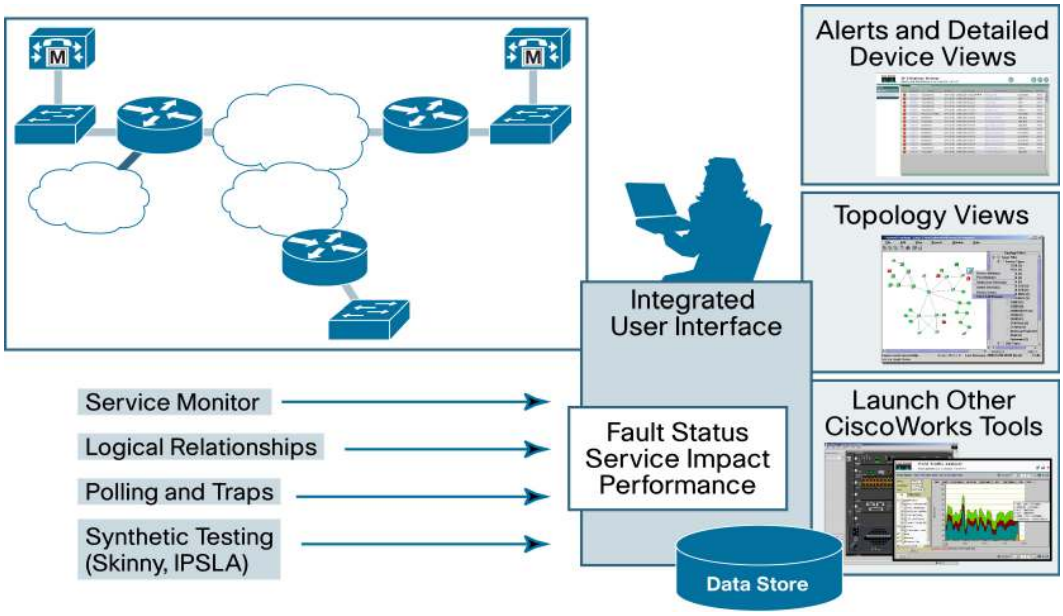
Description	Specification		
Server Requirements			
System parameters	**Up to 1000 phones**	**Up to 10,000 phones**	**Up to 30,000 phones**
Processor	• Intel Pentium or Xeon processor equal to or greater than 2 GHz or • AMD Opteron processor equal to or greater than 2 GHz	• Dual Intel Pentium or Xeon processor equal to or greater than 2 GHz or • Dual AMD Opteron processor equal to or greater than 2 GHz	• Dual Intel Pentium or Xeon processor equal to or greater than 2 GHz or • Dual AMD Opteron processor equal to or greater than 2 GHz
Memory	4 GB RAM	4 GB RAM	4 GB RAM
Swap file	4 GB swap file	4 GB swap file	4 GB swap file
Disk space	36 GB recommended	72 GB recommended	72 GB recommended
Hardware	Server platform	Server platform	Server platform
Software	Windows 2003 Server with Service Pack 1	Windows 2003 Server with Service Pack 1	Windows 2003 Server with Service Pack 1

The requirements in Table 2 outline the minimum hardware configuration needed to operate Cisco Unified Operations Manager 2.0 at different scalability levels. For Cisco Unified Communications systems of more than 30,000 phones, multiple Cisco Unified Operations Manager 2.0 servers must be deployed.

Network Overview

There are several scenarios that require more than a single Operations Manager or Service Monitor server to manage the Unified Communications network, perhaps across several geographical/regional offices or when providing a managed service using Operations Manager and Service Monitor. A single Operations Manager server can manage up to 30,000 IP phones and up to 2000 devices and so on. Operations Manager primary servers will be needed, in addition to backup Operations Manager servers—one for every primary server. Figure 1 shows the deployment architecture for Operations Manager.

Figure 1. Typical Operations Manager/Service Monitor Architecture



For Cisco Unified Communications systems of more than 30,000 phones, multiple Cisco Unified Operations Manager servers can be deployed in several different manners depending upon customer requirements. Regardless of deployment method, Operations Manager servers can all share:

- User authentication
- Device management
- Manager of managers (MOM) providing a common viewpoint for all alerts

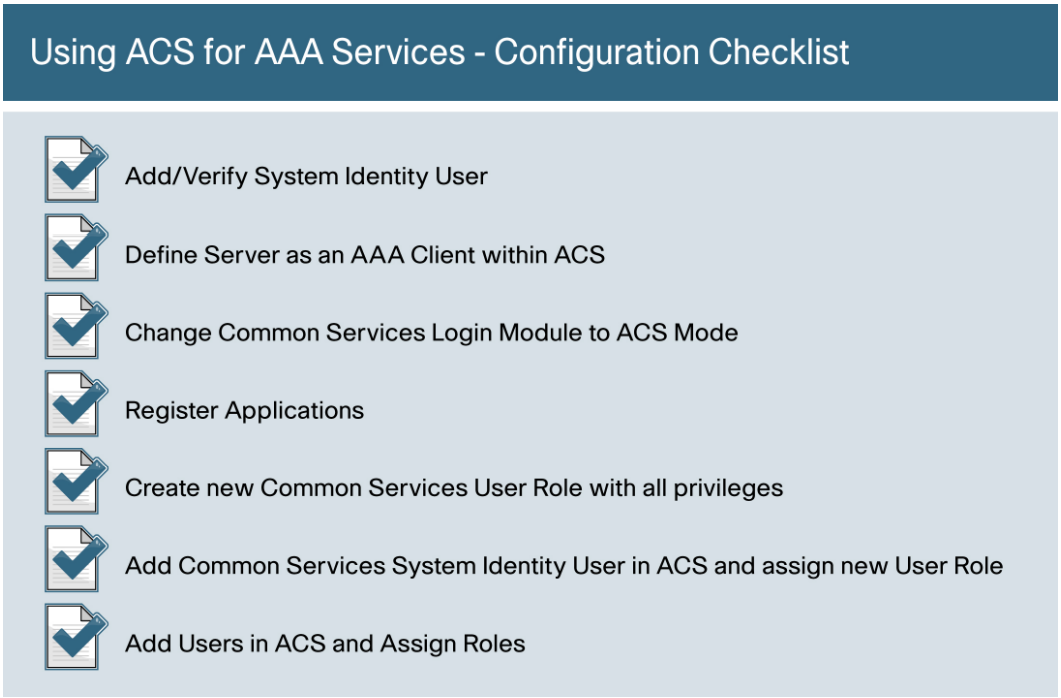
These servers can share device and credential information between them using the Device Credentials Repository (DCR), and administrators can perform centralized device and credential management. By integrating Cisco Unified Operations Manager with Cisco Secure Access Control Server (ACS), administrators can centrally control user access. Also, each of these Operations Manager servers will roll up the status of the network being monitored to a higher-level entity (typically a manager of managers) through Simple Network Management Protocol (SNMP) traps and syslog notifications.

Centralized User Authentication, Trap Viewing, and Device Management

Centralized User Authentication

The Cisco ACS product, when used in conjunction with Operations Manager and Service Monitor, can provide a means for central user authentication across all servers, regardless of the number of servers. When the active and standby servers are configured to operate in ACS mode, all the user and role setup is done with ACS, so, the user information is not local to the active server. Any changes to user information happen centrally and automatically propagate to the active and standby servers. Figure 2 provides a checklist for using ACS for authentication, authorization, and accounting (AAA).

Figure 2. Configuration Checklist for Using ACS



Integrating with the ACS Server

In ACS, network device groups are collections of AAA clients and AAA servers. You can assign AAA clients and AAA servers to the network device groups. For the Network Device Groups table to be displayed in the ACS server, the Network Device Groups option must be selected.

To select the Network Device Groups table, do the following:

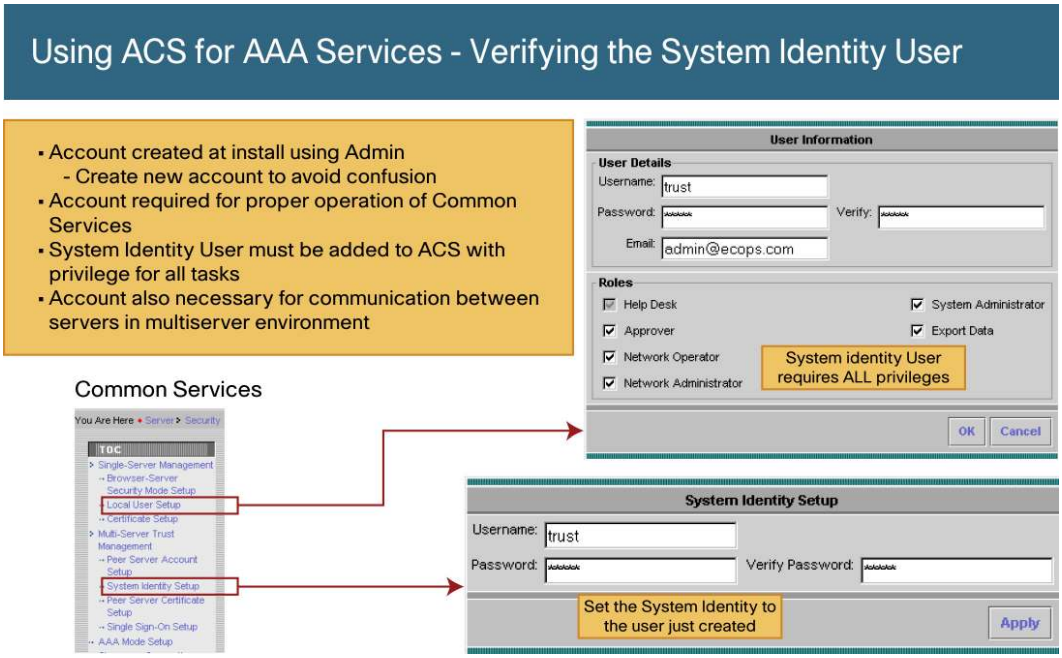
Step 1. From the ACS navigation menu, select **Network Configuration**.

Step 2. Click **Advanced Options**.

Step 3. Select the **Network Device Groups** check box.

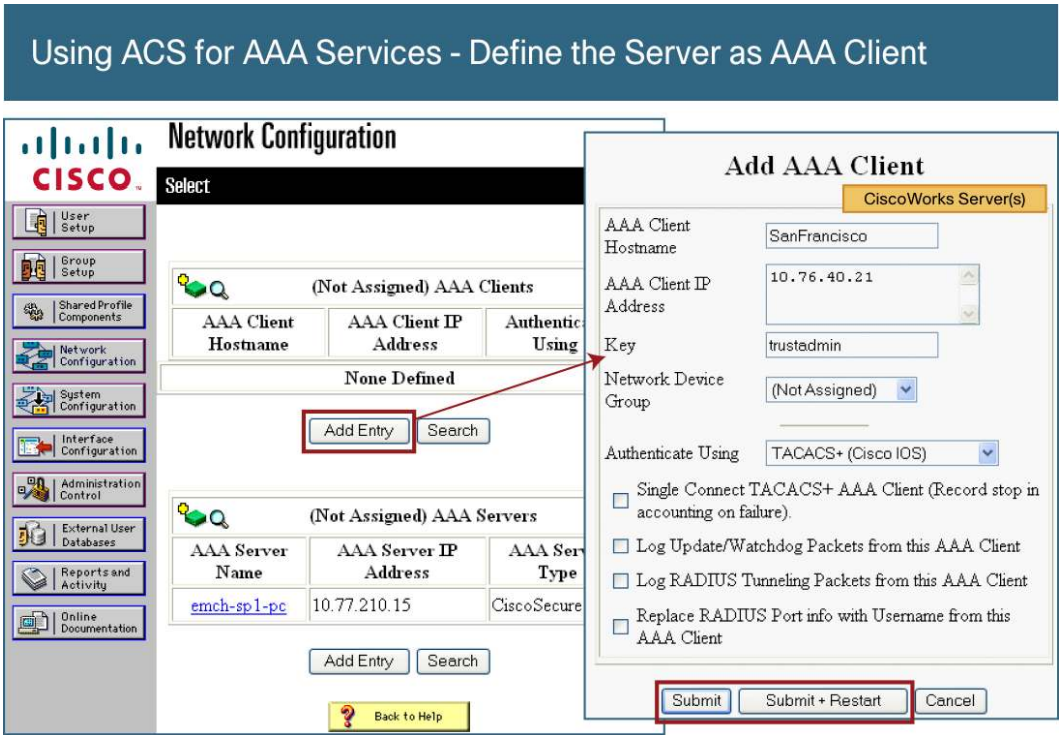
Step 4. Click **Submit+Restart**.

Figure 3. System Identity Setup



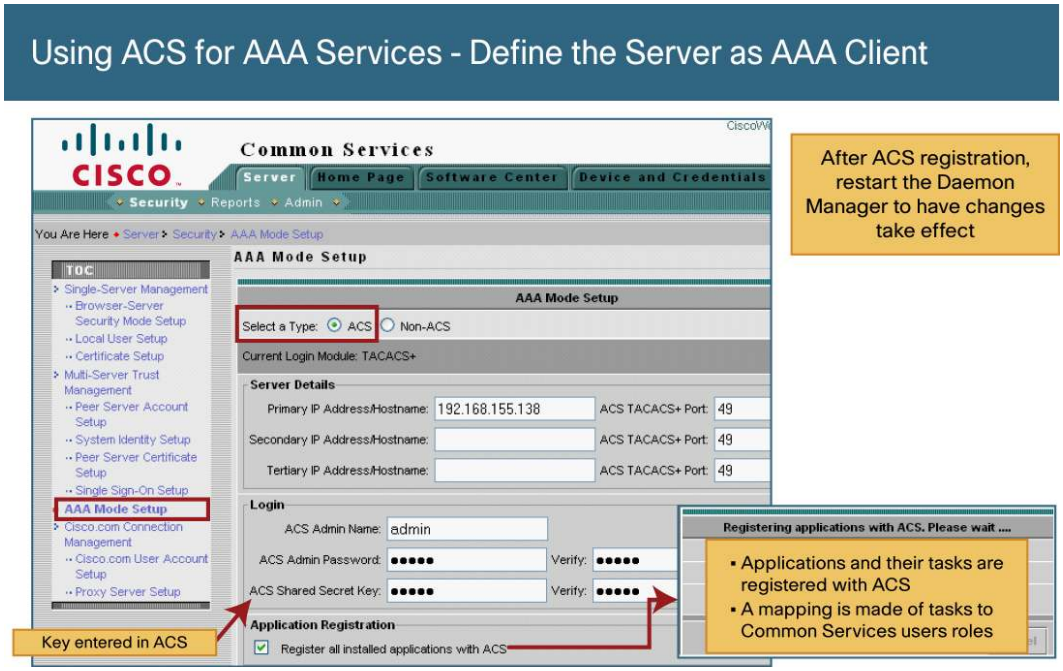
Add the system identity user in Operations Manager from CiscoWorks Common Services (Figure 3).

Figure 4. Add an AAA Client



Define the Operations Manager server as an AAA client in ACS (Figure 4).

Figure 5. Change AAA mode setup to ACS



Change Operations Manager to ACS mode (Figure 5).

Note: To revert back from this change may require a restore of Operations Manager. Make sure to perform an Operations Manager backup prior to this task if you may need to revert back to non-ACS mode.

Figure 6. Create a new User Role

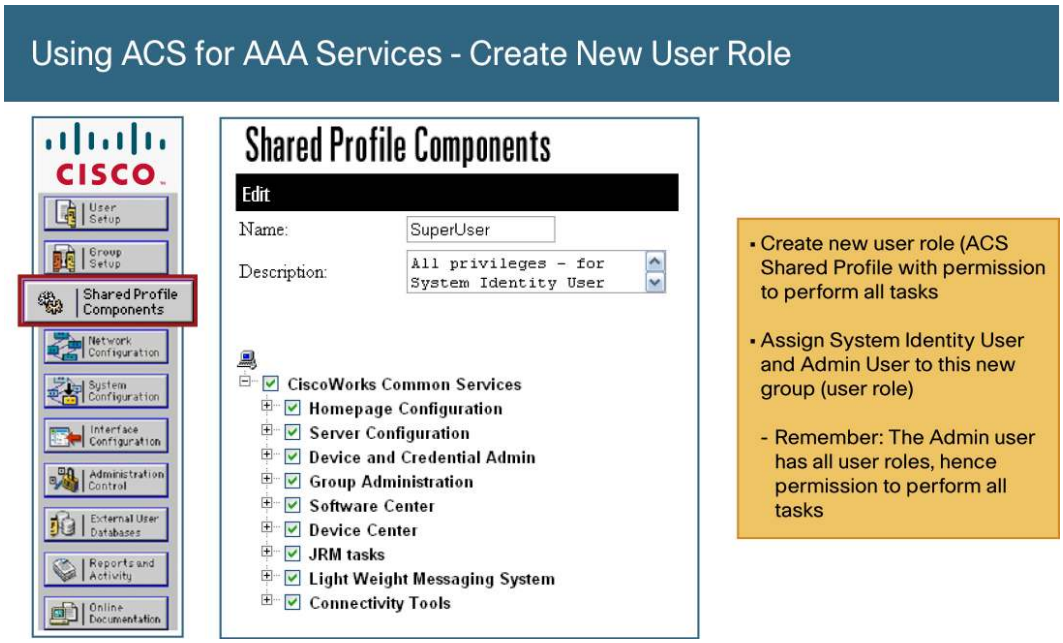
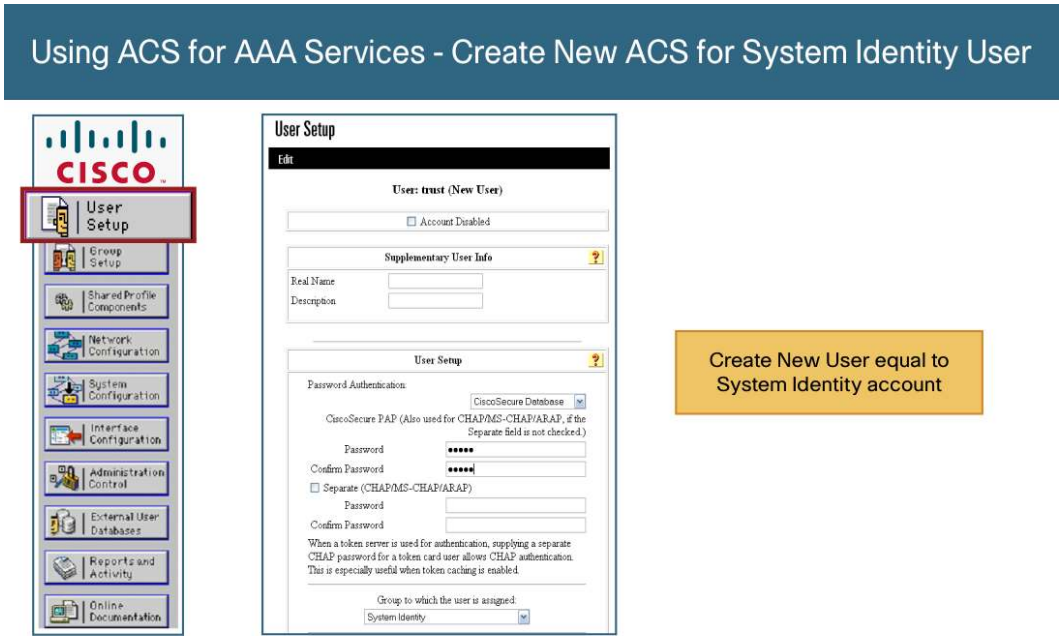
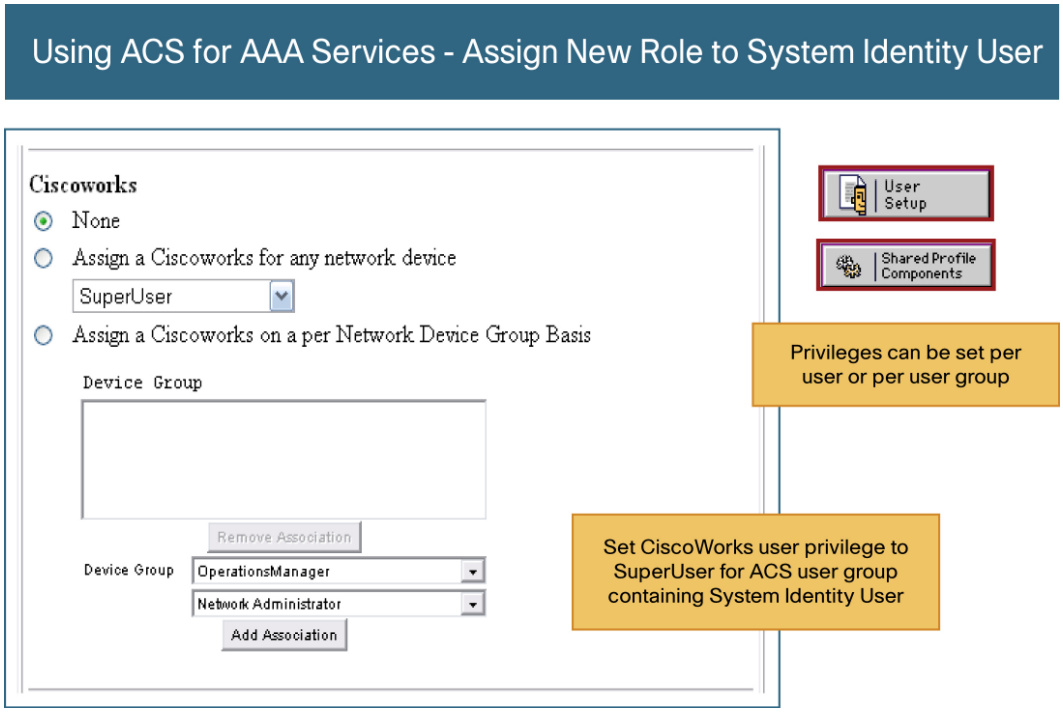


Figure 7. User Setup



Create a new user (Figure 7).

Figure 8. Assign User Privileges



Centralized Trap Viewing

Both Operations Manager and Service Monitor can be configured to forward traps to a manager of managers. This provides a method for a central view of all alarms across all of the Operations Manager and Service Monitor servers.

Figure 9. Operations Manager and Service Monitor servers forward traps to a MOM

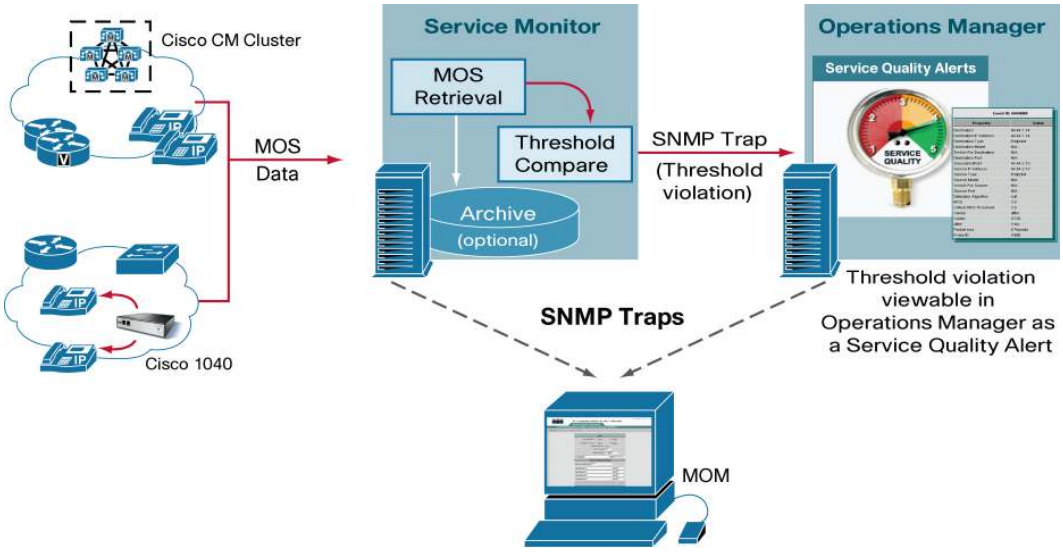
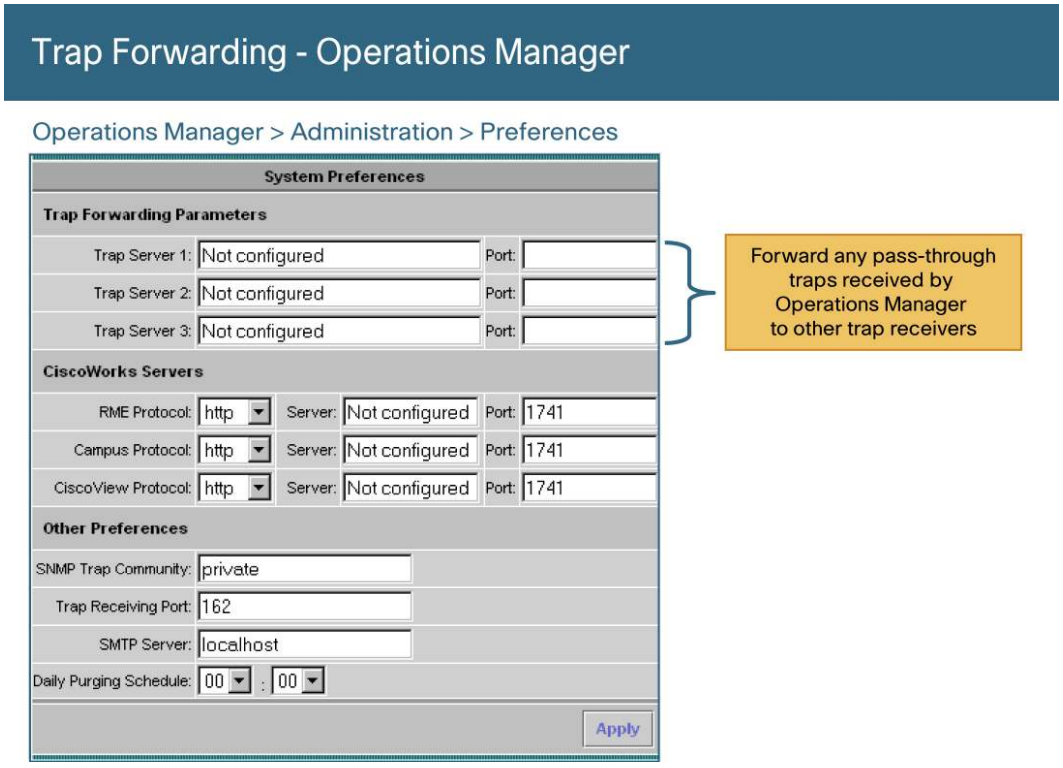
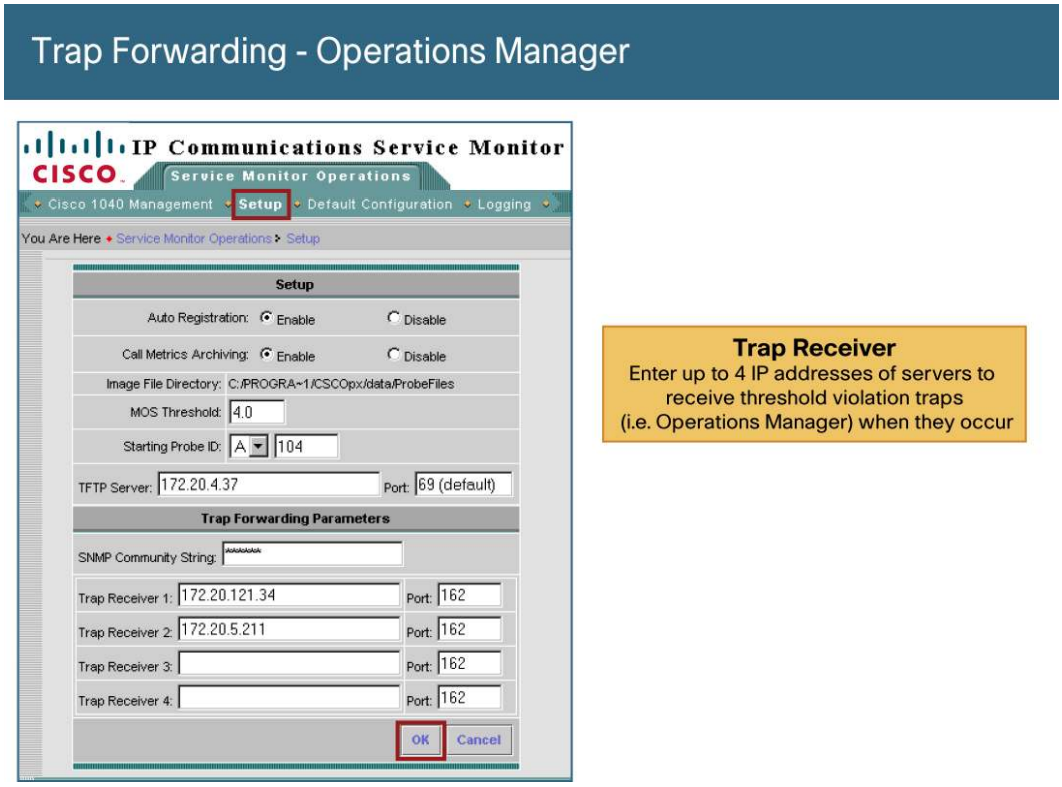


Figure 10. Trap Forwarding



The Operations Manager configuration in Figure 10 will send all traps to the MOM. If instead only a select type of alarm is required to be forwarded, then use Operations Manager SNMP trap notifications instead of trap forwarding. See the user guide for details.

Figure 11. Service Monitor will send SNMP traps to the configured receiver or receivers



Centralized Device Management

Two or more Operations Manager servers can be synchronized to provide centralized device management. One Operations Manager server is designated as the master and the others as a slave. If this configuration is used, then henceforth all devices must be added and deleted from the master. The slaves are then instructed to pull down a set of devices from the master. In this fashion, one can synchronize the backup to the primary Operations Manager server. Another scenario is a situation in which the backup Operations Manager server has a master list of all customers and is used to feed the other slave Operations Manager servers each with their own subset of that master list.

Synchronize the Operations Manager Device Credentials Repository

Operations Manager uses CiscoWorks Common Services 3.0 as its application framework. The Device Credentials Repository (DCR), a function of CiscoWorks Common Services 3.0, is a common repository of devices, their attributes, and their credentials required to manage devices in a management domain. The DCR lets you share device information among various network management applications.

For example, device credentials can be shared between:

- Multiple instances of Operations Manager
- Instances of Operations Manager and any CiscoWorks applications running on Common Services version 3.0 or later

To share the device credentials, the DCR server can run in master mode, slave mode, or standalone mode. You can change mode through the user interface or the DCR command-line interface.

Note: The document has examples of other CiscoWorks products, such as LAN Management Solution (LMS), Routed WAN (RWAN) Management Solution, and VPN/Security Management Solution (VMS) bundles. The setup of the DCR is similar to those applications.

Note: To revert back from this change may require a restore of Operations Manager. Make sure to perform an Operations Manager backup prior to this task if you may need to revert out of master/slave mode.

In the active server:

1. Select **Common Services > Server > Security**. The Security Settings page appears.
2. Click **Peer Server Account Setup** in the TOC. The Peer Server Account Setup page appears displaying the list of current users configured.
3. To add users, click **Add** in the main window. A pop-up appears where you can add the details of the user. In this screen, enter **"admin"** as the user name and the password of the standby server.
4. Go to **Common Services > Server > Multi Server Trust Management > Peer Server certificate**. Import the "Standby" server certificate.
5. Go to **Common Services > Device and Credentials > Admin > Mode Settings**. Change the mode to "Master."

In the standby server:

1. Go to **Common Services > Server > Multi Server Trust Management > Peer Server certificate**. Import the "Active" server certificate.
2. Go to **Common Services > Device and Credentials > Admin > Mode Settings**. Change the mode to "Slave," and provide the master address. Make sure the master address provided here is identical to the host name field in the Master's certificate.

As soon as you do this, the standby server is in slave mode and gets all the device information from the active server.

Unified Communications Operations Manager

For Cisco Unified Communications systems of more than 30,000 phones, multiple Cisco Unified Operations Manager servers can be deployed. These servers can share device and credential information between them, and administrators can perform centralized device and credential management. By integrating Cisco Unified Operations Manager with Cisco Secure Access Control Server, administrators can centrally control user access. Each of these Operations Manager servers will roll up the status of the network being monitored to a higher-level entity (typically a manager of managers) through SNMP traps and syslog notifications. Most customers will hit port/interface limits before they hit the 2000 device/30,000 phone limit. You can view the other Operations Manager soft limits at http://www.cisco.com/en/US/docs/net_mgmt/cisco_unified_operations_manager/2.0.1/installation/guide/prereq.html#wp1100174.

Scenario 1: Decentralized Network Operations Centers Deployed Geographically, Each with Its Own Operations Manager and Service Monitor Servers

Operations Manager Design Overview

- In each of the regions, there will be a pair of Operations Manager servers—primary and backup.
- Devices and phones will be about equally distributed across the regions—for example, a single Communications Manager cluster per region—managing 30,000 phones per Operations Manager instance.
- All voice infrastructure elements and servers will be monitored by these Operations Manager servers on a regional basis.
- Node-to-node tests and path analysis will be regionalized, because Operations Manager servers are managing only a subset of devices.
- Operations Manager reports will be regionalized and limited to those phones and alerts for that region. Service Statistics Manager (SSM) can be used to centralize reporting.
- A single Service Monitor server, at a minimum, will also be required in each region. A second backup Service Monitor server could be deployed per region, or a Service Monitor server from another region could be used as the failover backup. The Cisco 1040 sensors can be configured with a primary and a backup Service Monitor server. Note that in this case the Operations Manager server in that other region will be receiving the Quality of Voice (QoV) traps for the other region. However, one can temporarily configure the backup Service Monitor server to also send QoV traps to the other region's Operations Manager server in addition to the Operations Manager to which it is associated. This way alerts are still received by the proper regional server.
- A maximum of 5 to 10 Cisco 1040 sensors per region can be deployed (depends on the Service Monitor failover architecture).
- Service Monitor sends events to the local Operations Manager server and possibly to the MOM as well. Operations Manager displays events in the GUI, e-mails notifications, and sends SNMP traps to MOM. See Figures 12 and 13.

Figure 12. Operations Manager/Service Monitor Global Design

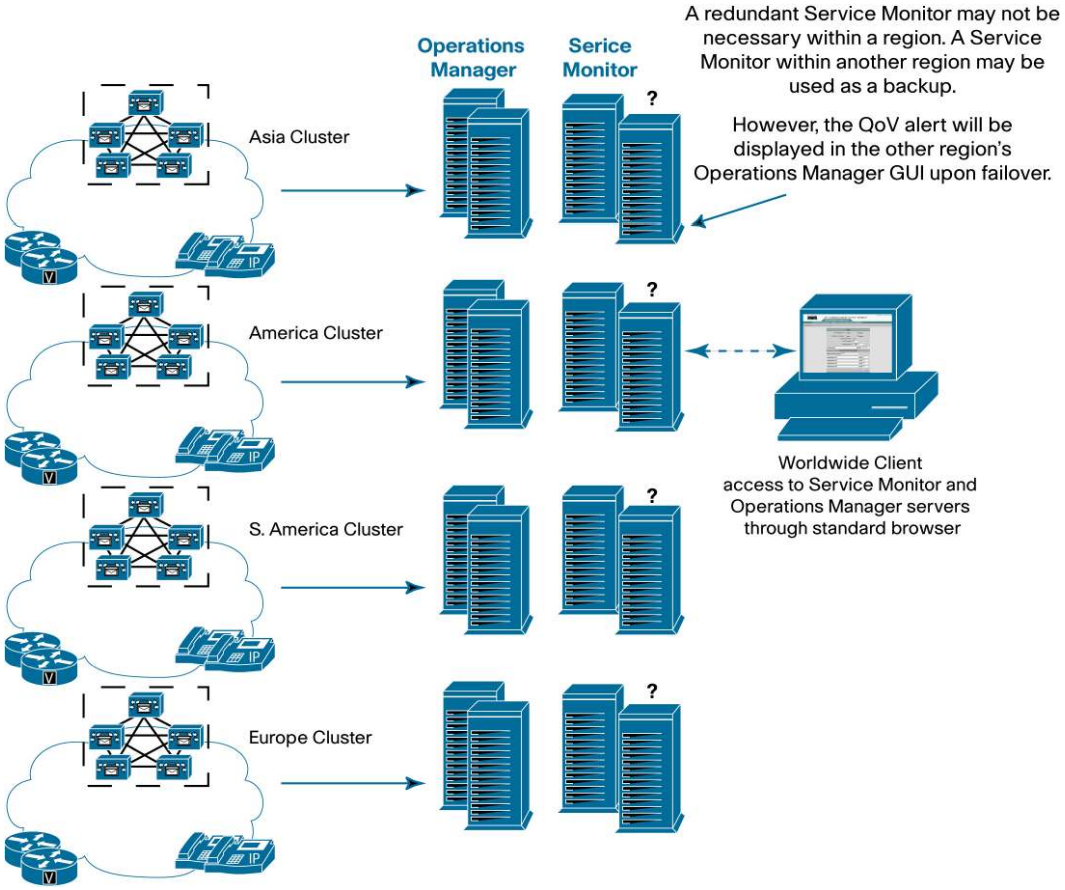
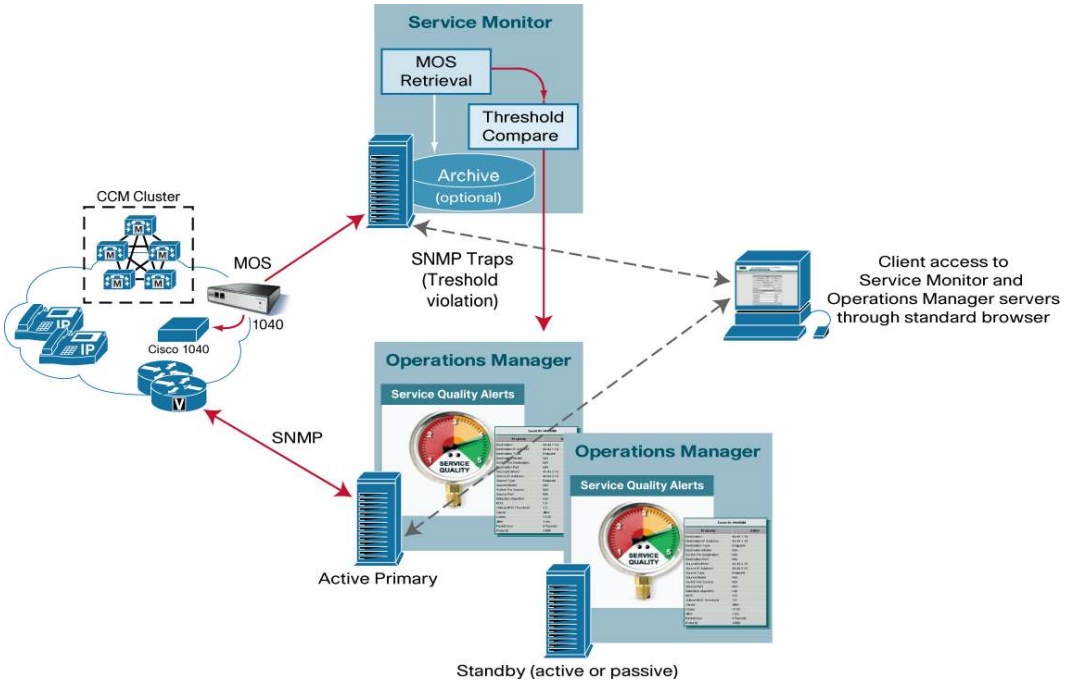


Figure 13. Operations Manager/Service Monitor Global Design—Regional View

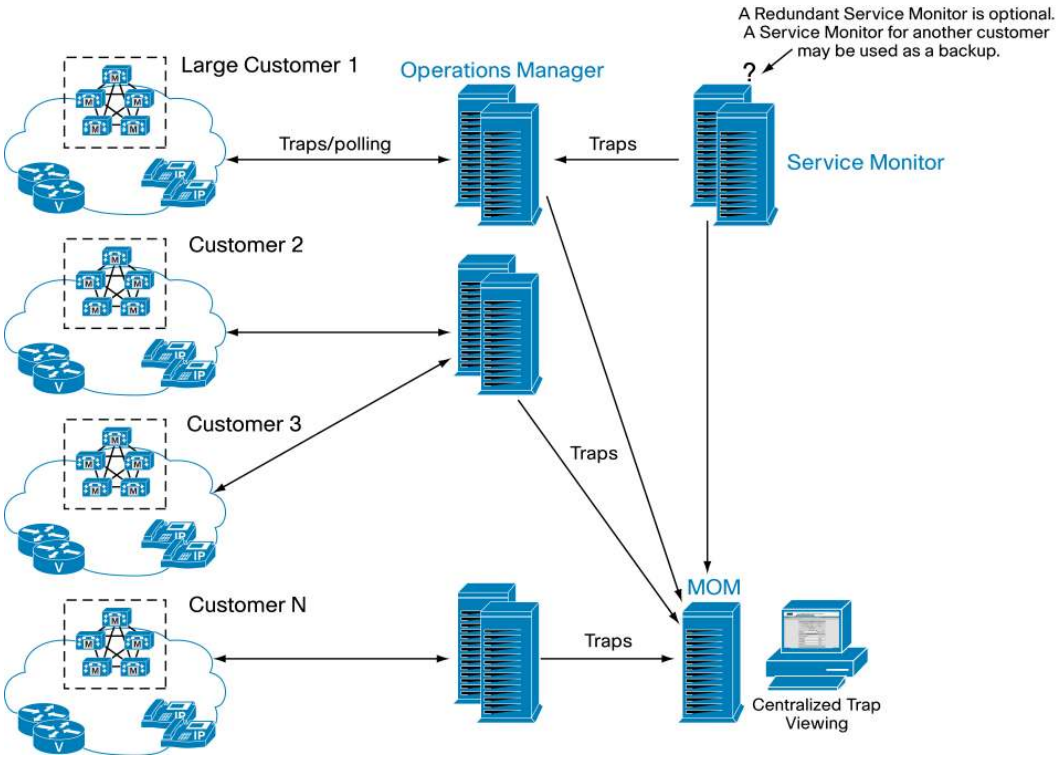


Scenario 2: Centralized Network Operations Center—Managed Service Provider

Operations Manager Design Overview

- Typically, for larger customers a single Operations Manager server is dedicated per customer. Smaller customers can coreside on a single server unless overlapping IP addresses exist.
- All voice infrastructure elements and servers for a customer will be monitored by a single Operations Manager server.
- User-defined device groups should be used to organize those smaller customers into groups for viewing and customized polling within a single Operations Manager server.
- Each Operations Manager server will require a cold standby backup, which can be shared among several customers or dedicated to a single large customer.
- Node-to-node tests and path analysis will be end to end across the WAN because the Operations Manager server is managing all of the voice devices. See Figure 14.

Figure 14. Operations Manager Centralized Design



Operations Manager Redundancy

Regardless of architecture deployed, Operations Manager supports a cold standby server. There is no communication between the various Operations Manager servers specifically in support standby. Each Operations Manager server is an independent instance.

The first step is to have two identical servers available for configuration. One server acts as an active and the second as a standby server. Please refer to the Operations Manager installation guide for the hardware specification of these servers at http://www.cisco.com/en/US/products/ps6535/products_installation_guide_chapter09186a008063d8b5.html#wp1093273.

It is recommended that these servers connect to the network through redundant paths. This helps ensure that a failure in one part of the network that affects the active server does not also affect connectivity of the standby server.

Redundant deployment can be considered in four parts:

- Setting up the active Operations Manager server
- Setting up the standby Operations Manager server by creating a baseline
- Replicate the active Operations Manager configuration to the standby Operations Manager configuration on an ongoing basis
- Things to do in case of failure of the active server

Setting Up the Active Operations Manager server

This is the same as setting up a standalone Operations Manager server. Typical tasks include:

- Setting up users and associating roles
- Providing a device list by manually adding devices to the Device Credentials Repository or discovering the network using a seed device
- Setting up the polling intervals based on your monitoring requirements (default is 4 minutes)
  - Creating phone status tests
  - Creating synthetic tests
  - Creating node-to-node tests
  - Setting up SRST polling by creating SRST tests
  - Enabling performance polling
  - Setting up notification profiles for northbound notifications
  - Configuring Service Monitor to forward traps to Operations Manager
  - Configuring Cisco 1040 probes to register to Service Monitor
- Configuring system preferences such as forwarding trap servers, trap community strings, Simple Mail Transfer Protocol (SMTP) servers for northbound notifications

For explanations about each task, see the user guide at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cuom/cuom20/index.htm.

Setting up the Standby Server

Once the active server is set up, the standby server needs to be set up in such a way that it has exactly the same configuration as the active server. This can be achieved using the Backup and Restore feature in Operations Manager.

Backup:

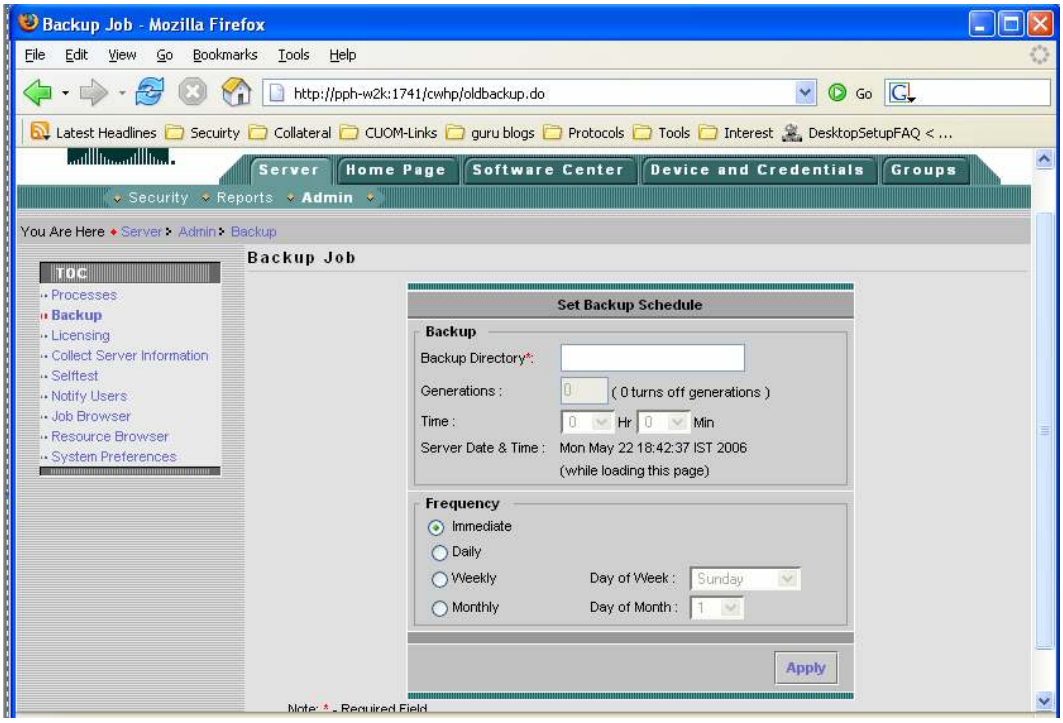
Go to the active Operations Manager server.

```
<INSTALL_DIR>\bin\perl <INSTALL_DIR>\bin\backup.pl <BackUp Dir> <Log
file> <Num_Generations>
```

This tool creates a backup of all the data on the active Operations Manager server and copies it into the backup directory mentioned. The number of generations refers to the maximum backups that can be stored under the backup directory. For example, if the number of generations is 2, then two consecutive invocations of this script would create <Backup dir>\0, and <Backup_dir>\1 until it starts wrapping.

Instead of the command line, you could also use the Common Services user interface shown in Figure 15.

Figure 15. Backing Up Server Data



From the user interface, it is possible to schedule a periodic backup of the active server. Periodic backups allow you to move to the latest backups if required.

It is recommended that this backed up data directory be kept on a separate system so that it is not affected by disk crashes or any issues associated with the active server.

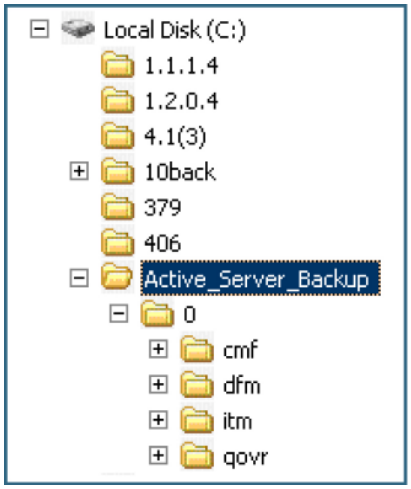
Once the data backup is completed, this information needs to be imported to the standby server using the Restore Facility in Operations Manager.

Restore:

Go to the standby server. Transfer the backup directory from the active server to the standby server. The complete directory and its contents should be transferred.

For example, if you have C:\Active_Server_Backup while running the Backup script, then you will see the directory structure shown in Figure 16.

Figure 16. C:\ folder



Copy the entire contents under C:\Active_Server_Backup to the Standby server with the exact same structure.

1. Run "**perl <INSTALL_DIR>\objects\vhm\utilities\dbclean.pl**"(this will clean the database).
2. Run **"net stop crmdmgtd"** to stop the Daemon Manager.
3. Run **"perl <INSTALL_DIR>\CSCOpx\bin\restoreBackup.pl -d <backupDir>"** (the backup directory is C:\Active_Server_Backup in the example mentioned above). Copy qovrx.log from the backup directory, that is, C:\Active_Server_Backup, to <INSTALL_DIR>\CSCOpx\databases\qovr.
4. Run **"net start crmdmgtd"** to start the Daemon Manager.

   If the server is integrated with ACS, you may get a question asking whether you want to register your application with ACS. If you have successfully configured your primary server with ACS (which is recommended because managing centralized users and roles is far easier in a redundancy setup), all your application roles and tasks are already there in ACS. In this case, select **NO** and proceed.

   If, in a rare scenario, your configuration in ACS has been wiped out, select **YES**. This will register your application in ACS.
5. Run **"net start crmdmgtd"** to restart the Daemon Manager.
6. Wait until **"pdshow"** lists all the processes running. This will imply that the Daemon Manager has completely started.
7. Rediscover all the devices. **Go to Devices > View/Rediscover/Delete**.

Essentially this creates a baseline for the standby server. The standby server would have the complete device list and all the configurations that are identical to the active server.

This means that the standby server will poll the network in exactly the same way as the active server. To reduce the impact of polling on network bandwidth, there are two options: reduce/suspend polling on the standby server or use a passive standby server. Devices can be updated automatically (from active to standby), and backups can occur easier when the standby server is not passive. Thus, if many changes are occurring on the Operations Manager server, a

passive standby server may require more time to bring up to speed and get online in case of an Operations Manager active primary failover. A passive standby Operations Manager server is easier to set up and does not require much upkeep, assuming the active primary Operations Manager server is not changing often.

Setting Up a Passive Standby Server

In some deployments, instead of having the backup server actively polling the network, administrators prefer to have a backup server configured but not have the server online.

- Configure the primary active server.
- Set up periodic backups on the primary server.
- Install the backup on the standby server. Shut down the standby server by using **"net stop crmdmgtd"** at the command line. This will stop all activity on the standby server.
- In the event of a failure of the primary server, restore from the latest backup (or whichever you desire).
- Bring up the standby server by executing **"net start crmdmgtd"**.
- Wait until all the processes come up.
- Redo any changes to the configuration since the last backup on the standby server. This may include devices, tests, users, and so on.

Now, your standby server is ready to be used.

Setting Up an Active Standby Server

This means that the standby server will be active on the network, but will poll the network less frequently, suspend notifications, and stop all tests compared to the active server. To reduce the impact of polling on network bandwidth:

1. Increase the polling interval to a very large value (1 hour) to reduce the impact on network bandwidth. You can do this by going to **Administration > Polling Parameters**, selecting each group, and editing the polling interval values.
2. Go to **Notifications > Notification Criteria**. Select all notification criteria and select Suspend.
3. Go to **Diagnostics > Synthetic Tests**. For each test select the **Stop** button. This will stop the synthetic tests.
4. Go to **Diagnostics > Phone Status Tests**. You will see a list of configured tests. For each test, click **Edit** and make the schedule to run between "00:00" to "00:00". This essentially stops the test.
5. Suspend monitoring of SRST routers used in SRST tests: Go to **Administration > SRST Poll Settings > SRST Operations**. You will see a list of SRST tests configured. Note down all the target routers. Go to **Devices > Device Management**. You will see the overview of all managed devices. Click **Monitored Devices**. Click the SRST router IP address in this report; Detailed Device View is launched. In this UI, suspend the device. This will automatically stop the SRST tests.

Continuous Data Sync Up

Once the active and standby servers are in operation, any changes thereon to the active server need to be propagated to the standby server. Different kinds of data that can change and recommendation for replication are listed below.

Device List

Changes to the device list can be propagated by using a central DCR. There are two possibilities:

- Central LMS server as the source of device list for both primary and backup servers. In this case, the LMS server acts as a master repository of devices, which pushes any additions or deletions to the device list to the two slaves—the active and the standby servers.
- Active server as the source of the device list for the standby server. In this case, the active server acts as the master device repository. It pushes any changes to the device list to the standby server.

In either of the cases, the main idea is setting up the master/slave configuration in DCR. The steps are explained below, taking the example of active as the master DCR and slave as the standby DCR.

In the active server:

1. Select **Common Services > Server > Security**. The Security Settings page appears.
2. Click **Peer Server Account Setup** in the TOC. The Peer Server Account Setup page appears, displaying the list of current users configured.
3. To add users, click **Add** in the main window. A pop-up menu appears in which you can add the details of the user. In this screen, enter **"admin"** as the username and the password of the standby server.
4. Go to **Common Services > Server > Multi Server Trust Management > Peer Server certificate**. Import the "Standby" server certificate.
5. Go to **Common Services > Device and Credentials > Admin > Mode Settings**. Change the mode to "Master"

In the standby server:

1. Change the DCR Group ID in the standby server. Go to <INSTALL_DIR>\CSCOpx\lib\classpath\com\cisco\nm\dcr and change the DCR_Group_ID to any number in dcr.ini (the DCR_Group_ID of the master and slave servers should not be same) and restart the Daemon Manager.
2. Go to **Common Services > Server > Multi Server Trust Management > Peer Server certificate**. Import the "Active" server certificate.
3. Go to **Common Services > Device and Credentials > Admin > Mode Settings**. Change the mode to "Slave," provide the Master address, and restart the Daemon Manager. Make sure the Master address provided here is identical to the host name field in the Master's certificate.

As soon as you do this, the standby server is in slave mode and gets all the device information from the active server.

User Information

Active and standby Operations Manager servers can be configured to operate in ACS mode. In this mode, all the user and role setup is done on the ACS server, so, the user information is not local to the active server. Any changes to user information happen centrally and then automatically propagate to the active and standby servers.

Otherwise, user information must be added to each local server.

Other Configurations

Any other changes to the configuration of the active server need to be also done on the standby server. This includes any new diagnostic tests since the baseline was created and any changes to notification profiles.

If the amount of changes is more, then it is advisable to back up and restore the data so that manually changing the configuration is totally avoided.

Things to Do When the Active Server Goes Down

Failure of the primary server can be detected externally by polling the sysApplMIB on the primary Operations Manager server. The status of all the processes that are necessary for normal functioning of Operations Manager can be obtained from this MIB. Table 3 lists the processes that need to be running for a fully functional Operations Manager server.

Table 3. Processes for Operations Manager

Tomcat	Apache
TomcatMonitor	QOVRMultiProcLogger
QOVRDbEngine	QOVRDbMonitor
QOVR	LicenseServer
IVR	IPIUDbEngine
IPIUDbMonitor	INVDbEngine
INVDbMonitor	FHDbEngine
FHDbMonitor	ESS
EssMonitor	InventoryCollector
TISServer	IPIUDataServer
ITMDiagServer	VHMIntegrator
EPMDbEngine	EPMDbMonitor
EPMServer	AdapterServer
FHServer	IPSLAServer
PIFServer	SRSTServer
QoVMServer	STServer
SIRServer	DfmBroker
DfmServer	VHMServer
CmfDbEngine	CmfDbMonitor
DCRServer	CMFOGSServer
ITMOGSServer	GPF
NOTSServer	PTMServer
TopoServer	VsmServer
Jrm	

If any of the processes are “down,” it means that Operations Manager is in an indeterminate state, and under such circumstances, you should activate your standby server.

In case the active server goes down, the standby (not passive) can be made operational by doing the following:

- Using the polling parameters UI on the standby server, switch over to the default polling interval of 4 minutes.

- Activate synthetic tests. You can “Start” the tests that are stopped.
- Shift back to the original schedule for phone status tests.
- “Resume” the notification criteria.
- Verify that you are able to monitor the status of the network and the validity and execution of diagnostic tests and the notification profiles.
- Create a backup of the configuration of the newly activated server.
- Decommission the previously active server.
- You may need to configure into Service Monitor the new Operations Manager server IP address to send traps to the backup server (depends on how Service Monitor failover is implemented).

Unified Communications Service Monitor

This document is meant as a supplement to the Service Monitor deployment guide located at http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6491/ps6705/ps6536/ps7124/prod_white_paper0900aecd80724961.pdf.

The failover capability of Service Monitor is only for 1040 sensors. There is no failover capability for Cisco Voice Transmission Quality (CVTQ) capability. However, Communications Manager can be added to multiple Service Monitor servers. Up to three Service Monitor servers can be configured as billing application servers in Cisco Unified Communications Manager 5.x or above to receive Cisco Voice Transmission Quality data. When one Service Monitor server is down, the other Service Monitor server will still be able to obtain the Cisco Voice Transmission Quality data from Cisco Unified Communications Manager.

A Cisco 1040 Sensor supports up to 50 active calls (100 Real-Time Transport Protocol [RTP] streams). At an 8-to-1 ratio (a typical public switched telephone network [PSTN] line-to-user ratio), a Cisco 1040 can monitor approximately up to 400 phones. The 8:1 ratio is typically used when provisioning phone lines. This ratio would be different for a call center environment and may vary for your customer. Nonetheless, if there are more than 100 RTP streams, some of the RTP streams might not be collected consistently. In this case, since the Cisco 1040 might have missed certain RTP streams, when the mean opinion score (MOS) is calculated, the MOS is diluted.

A single Service Monitor server supports up to 10 Cisco 1040s (or about 4000 phones). One does not need to monitor every phone call. A sampling of phone calls is sufficient. A 5 percent to 10 percent sampling should suffice for a single cluster and 30,000 phones, but it depends upon customer requirements. Thus, five to the maximum 10 Cisco 1040 Sensors per region would register to a single Service Monitor regional server and provide sufficient QoV sampling (6 percent and 12 percent respectively) for that one region.

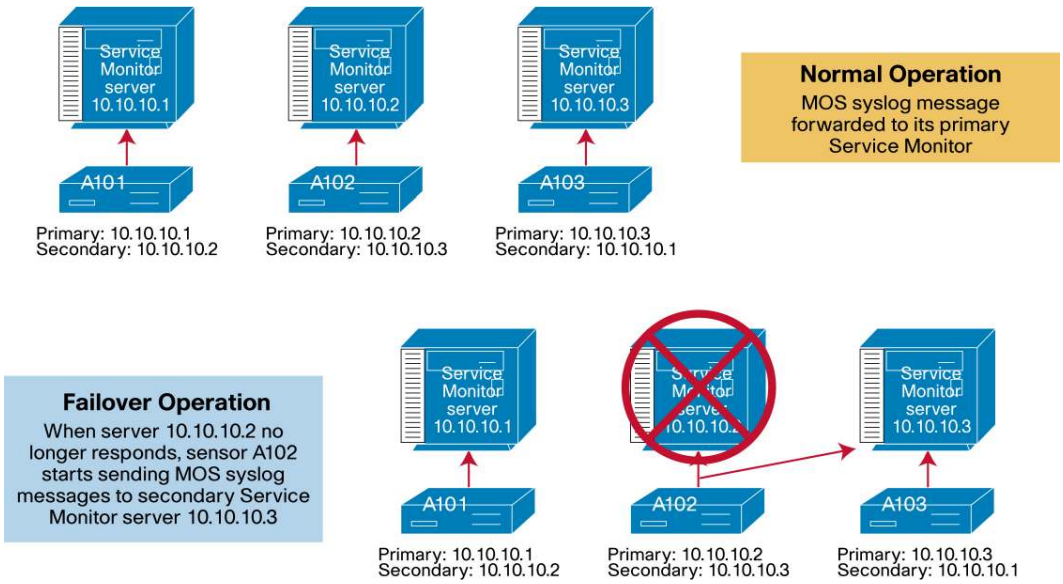
A single Operations Manager server supports up to 10 Service Monitor servers.

Span as close to the phone switch port as possible for the Cisco 1040 to calculate an accurate MOS that closely emulates the end user experience. Span the voice VLAN, or span individual switch ports. For the case of gateways, span the switch port that the gateway is connected into. The sensors can monitor any device that originates and/or terminates RTP streams, including gateways and Cisco Unity® devices. Switch port spanning is the method through which one controls the amount of RTP traffic flowing into the 1040 sensors.

From the Operations Manager server, go to **Administration > Service Quality Settings** and add all of the Service Monitor servers that will integrate with this Operations Manager server.

Scenario 1: Decentralized Network Operations Centers Deployed Geographically, Each with Its Own Operations Manager and Service Monitor Servers

Figure 17. 1040 Sensor Failover to a Secondary Service Monitor Server in Another Region



A Service Monitor server will be required in each region at a minimum. See Figure 17.

You have three choices regarding a backup Service Monitor server:

- The Service Monitor server could be deployed as a hot backup, with no active sensors, awaiting any other active Service Monitor server to fail. This backup Service Monitor server could support up to 10 sensors (two Service Monitor servers per region).
- It could be deployed as an active backup. If say, this active backup was supporting five active sensors, then it can serve as a backup to five other sensors from some other Service Monitor (two Service Monitor servers per region).
- An active Service Monitor server for another region could be used as the failover backup (one Service Monitor server per region).

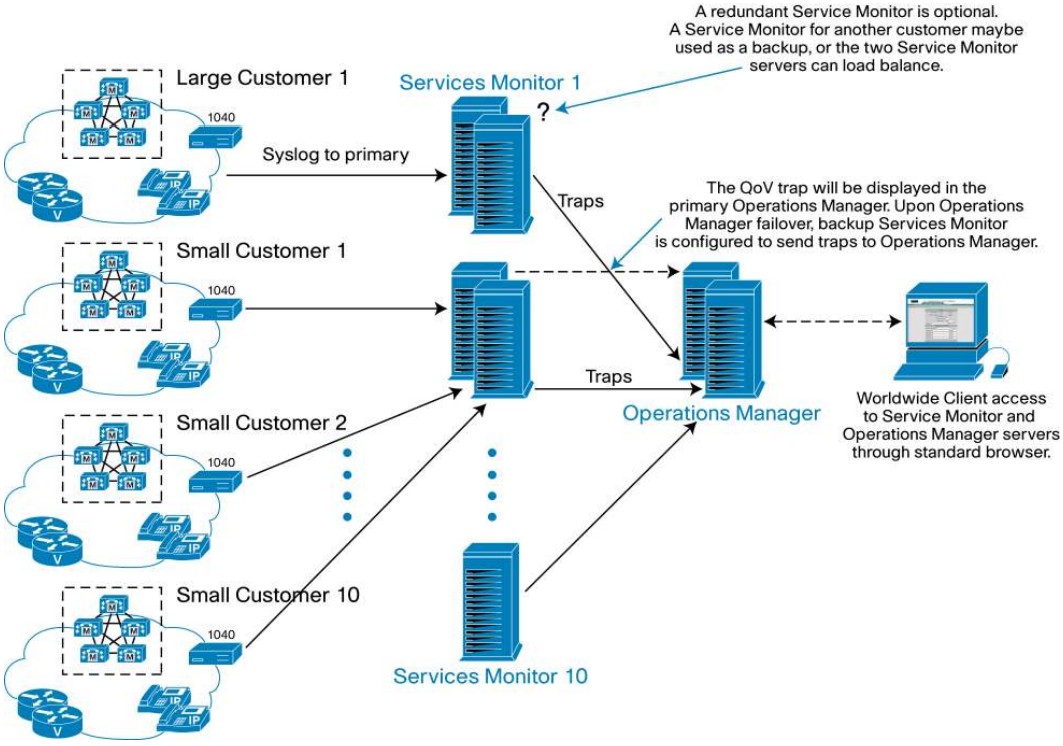
However, in this case:

- The Service Monitor QoV events reported during a failover will be reported on that other region's Operations Manager GUI. (Service Monitor reports QoV events to Operations Manager, but one could temporarily configure the backup Service Monitor to also send traps to the other regions Operations Manager server—use Service Monitor > Configuration > Trap Receivers).
- The Service Monitor server can then support only a maximum of five Cisco 1040 sensors per region (assuming the sensor are maxed at 100 RTP streams each). This way when a failover occurs, the five 1040s from its own region, plus the new five 1040s from the failed Service Monitor, would total the maximum 10 Cisco 1040 sensors per Service Monitor server.

Scenario 2: Centralized Network Operations Center—Managed Service Provider

With a centralized network operations center (NOC), Service Monitor servers can monitor a single customer or monitor several customers. Traps can be sent centralized to one Operations Manager server (or a select number of Operations Manager servers). If there exists an Operations Manager server with fewer than 1000 phones, then Service Monitor can be coresident on that Operations Manager server. A single Operations Manager server can communicate with up to 10 Service Monitor servers. Each Service Monitor server may represent one or more customers, and they may all be sending traps to one Operations Manager server in addition to a MOM. Certainly Service Monitor traps for any one customer should be sent to the same Operations Manager server. It may not be ideal to send Service Monitor traps from one customer to two different Operations Manager servers. See Figure 18.

Figure 18. Services Manager Centralized Design



You have three choices regarding a backup Service Monitor server:

- The backup Service Monitor server could be deployed as a hot backup, with no active sensors, awaiting any other active Service Monitor server to fail. This backup Service Monitor server could support up to 10 sensors (two Service Monitor servers per customer or customer group).
- It could be deployed as an active backup. If say, this active backup was supporting five active sensors, then it can serve as a backup to five other sensors from some other Service Monitor server (two Service Monitor servers per customer or customer group).
- An active Service Monitor server for another set of customers could be used as the failover backup (one Service Monitor server per customer or customer group).

However, in this case:

- The Service Monitor QoV events reported during a failover would be reported on another Operations Manager server serving another customer or customers. One can reconfigure the Service Monitor trap receivers to temporarily also send traps to the proper Operations Manager server.
- All Service Monitor servers can then support only a maximum of five Cisco 1040 sensors per customer (assuming the sensors are maxed at 100 RTP streams each). This way when a failover occurs, the five 1040s from the Service Monitor, plus the new five 1040s from the failed Service Monitor, would total the maximum 10 Cisco 1040 sensors per Service Monitor server.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C07-469725-00 05/08