CiscoWorks LAN Management Solution 4.0 Large-Scale

Deployment Guide

Contents

Overview

Today's network managers are often faced with the task of managing very large and complicated networks. As networks continue to grow in size and complexity, the number of network management tools and products are increasing as well. In such a situation, it is a challenge for administrators to effectively manage networks.

Cisco offers a number of CiscoWorks product bundles for effective network management. Each of these product bundles typically has a documented system recommendation and size limitation (for a single-server installation). However, customers often need additional information about how to manage networks larger than the recommended limit for a single CiscoWorks installation. This paper provides information and recommendations for resolving issues related to managing networks larger than the recommended limit for a single CiscoWorks installation.

It is important to understand that dealing with concerns related to a large network is a complex problem, with a number of factors affecting the end result. Even a simple question such as "What is the size of the server required for CiscoWorks LAN Management Solution (LMS) to manage *x* number of devices?" can be difficult to answer in a meaningful way. The number of devices is, at best, a vague indicator for estimating the required system resources - different devices can have vastly differing numbers and types of managed objects. In addition to the number of devices, the following points must be considered before providing an answer:

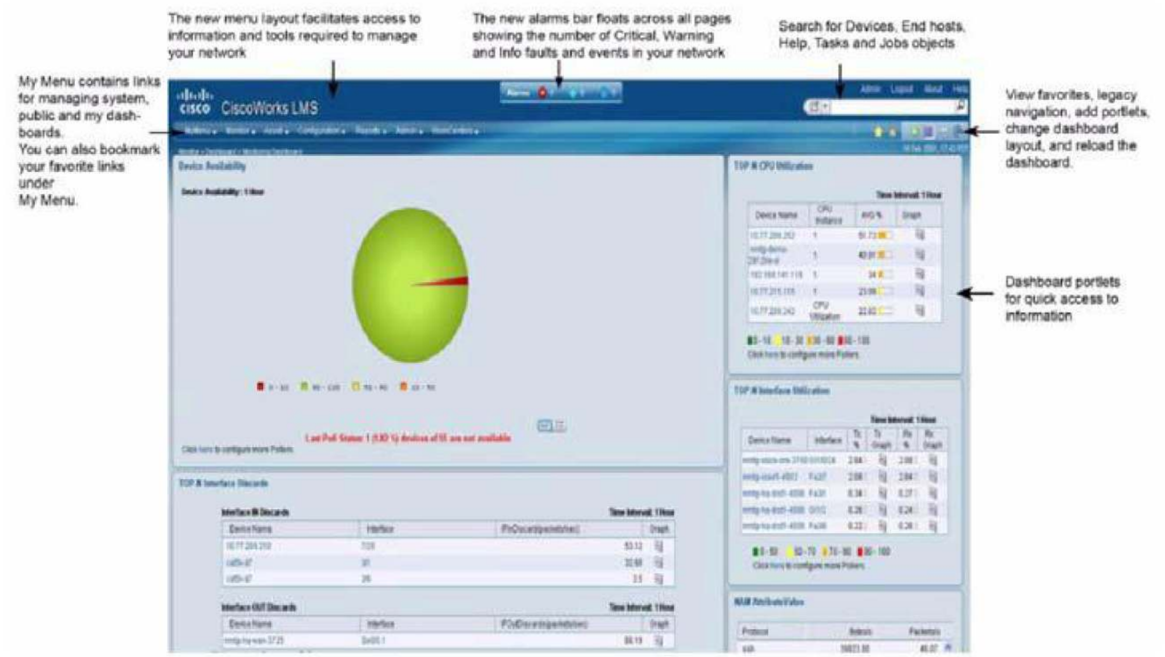
- The components and functions of the products that are most important to the network managers
- The number of users possessing network management tools and the number using the tools simultaneously
- The administrative groupings of the network devices and network management users, in the case of very large networks

These points, along with the information contained in this paper, will help enable users to make informed decisions about deploying CiscoWorks LMS for managing their networks.

CiscoWorks LAN Management Solution 4.0

CiscoWorks LAN Management Solution is an integrated suite of management functions that simplify the configuration, administration, monitoring, and troubleshooting of Cisco® networks. CiscoWorks LMS allows network operators to manage the network through a browser-based interface that can be accessed anytime from anywhere within the network. CiscoWorks LMS 4.0 is a major release that improves the overall user experience, providing new workflows built on functional partitioning that aligns the product with the way network operators do their jobs. Once installed, "out-of-the-box" monitoring and troubleshooting dashboards provide actionable information to quickly isolate and fix network problems before they affect services. Configuring and deploying updates to the network has never been easier with the new Template Center, which incorporates Cisco Validated Designs and links to download the latest configuration templates from Cisco.com, simplifying platform and technology rollout and reducing the chance for errors. Work Centers provide a single area where guided workflows give step-by-step instructions to help operators quickly provision, monitor, and manage new Cisco value-added technologies and solutions, such as EnergyWise, TrustSec/Identity, Auto Smartports, and Smart Install. See Figure 1.

Figure 1. CiscoWorks LMS 4.0 Homepage



The new menu layout facilitates access to information and tools required to manage your network

The new alarms bar floats across all pages showing the number of Critical, Warning and Info faults and events in your network

Search for Devices, End hosts, Help, Tasks and Jobs objects

My Menu contains links for managing system, public and my dash-boards. You can also bookmark your favorite links under My Menu.

View favorites, legacy navigation, add portlets, change dashboard layout, and reload the dashboard.

Dashboard portlets for quick access to information

CiscoWorks LMS is part of the CiscoWorks family of products that provide comprehensive network management solutions to improve IT organizational effectiveness through task automation, simplification, and integration. CiscoWorks LMS is delivered electronically or as physical media (DVD) and supports both Windows and Solaris operating systems.

Related Reading

Refer to the *CiscoWorks LMS 3.2 Deployment Guide* and *Installation and Configuration Guide* for an overview of CiscoWorks LMS 3.2. The CiscoWorks *LMS 3.2 Deployment Guide* focuses on single-server installation, while this white paper is mostly dedicated to multiserver setup where the applications are distributed across multiple servers for better scalability and performance. This white paper also describes the changes in Cisco Secure Access Control Server (ACS) integration as compared to the previous version (LMS 3.2), describes how to do a high availability deployment for LMS, and provides some recommendations for performance improvements in large-scale deployments.

CiscoWorks LMS 4.0 Deployment Guide can be found at the white papers section at http://www.cisco.com/go/lms.

Licensing Options for Large-Scale Deployment

The licenses in CiscoWorks LMS 4.0 are device-based, except for the performance management functionality, where the license is based on the number of configured collectors.

For large-scale deployment, you can select any one of the following SKUs for CiscoWorks LMS 4.0:

- **CWLMS-4.0-5K-K9**

Allows you to manage the following:

  - 5000 devices
  - 5000 collectors (In the Performance section of the Monitoring window)

- **CWLMS-4.0-10K-K9**

Allows you to manage the following:

- 10,000 devices for configuration and image management only
- User tracking: 5000 devices
- Monitoring and troubleshooting: 5000 devices
- 5000 collectors

But the configuration management, user tracking, and monitoring LMS instances have to be on separate servers. The 10,000 license can be applied to these multiple servers.

Licensing and Scalability of CiscoWorks Remote Data Collectors

Table 1 gives the SKUs for CiscoWorks remote data collectors.

Table 1. CiscoWorks Remote Data Collectors SKUs

SKU	License Parameter (Device Count)
L-CWLMS-4.0-COL-S	750
L-CWLMS-4.0-COL-M	1500
L-CWLMS-4.0-COL-L	2500

- Today the maximum SKU that is offered for CiscoWorks remote data collectors is 2500 devices. Adding licenses to increase the number to 10,000 devices is not supported, even though the LMS bundle supports up to 10,000 devices.
- The device count restricts the license options. One CiscoWorks server (from the remote data collection perspective) can support up to 2500 devices. Actually the scalability depends on how many MIB objects are being managed. The maximum number of MIB objects supported is 100,000, with 40,000 on 1-minute and 60,000 on 5-minute polling intervals.

Application Scaling Numbers

This section describes the specific scaling numbers and concerns for each of the CiscoWorks LMS functionalities. This information will help users decide the server size and distribution that would best suit their needs and optimize performance. You need to purchase appropriate CiscoWorks LMS licenses to manage these numbers. For more information on licensing, visit http://preview.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.0/install/guide/lmsig40.pdf.

Functional Scalability Limit on LMS Server

Table 2 lists the scalability limits for the 5000 and 10,000 device licenses (if applicable). Refer to Installing and Migrating to CiscoWorks LAN Management Solution 4.0 for smaller device numbers.

Table 2. Scalability Limits for the 5000 and 10,000 Device Licenses

Functionality	Scalability Limit on LMS Server
Grouping services	• 200 user-defined groups • 100 IP service-level agreement (SLA) groups • 50 fault groups • 100 port and module groups
Inventory, configuration, and image management	• 10,000 devices • 200 port and module configuration (PMC) groups with 90 percent port • groups and 10 percent module groups • Maximum of 500,000 ports with an average of 50 ports per device • Maximum of 100,000 ports in a port and module configuration group • Maximum of 250,000 ports for each LMS job In addition to the above, syslog reports can contain up to 40,000 records.

Functionality	Scalability Limit on LMS Server
Network topology, Layer 2 services, and user tracking	• For LMS 5000 device licenses, the scaling limit is 250,000 end hosts/IP phones • Network topology, Layer 2 services, and user-tracking data collection to discover and track a maximum of 250,000 switch ports • Virtual Route Forwarding (VRF)–lite, an add-on to network topology, Layer 2 services, and user tracking, supports 32 VRFs in all LMS device licenses
Fault management	The functionality supports up to 80,000 ports or interfaces (of which up to 15 percent can be in the managed state)
IP SLA performance management	• You can manage a maximum of 2000 collectors when all the device management functions including the IP SLA performance management functionality are enabled. This collector limit includes: ◦ 1500 collectors (hourly polling frequency) ◦ 500 collectors (minute polling frequency) • You can manage a maximum of 5000 collectors when the other device management functions are disabled and are managing the IP SLA performance management functionality only. This collector limit includes: ◦ 4500 collectors (hourly polling frequency) ◦ 500 collectors (minute polling frequency) • If you want to manage 5000 collectors without disabling any of the device management functions, you can manage: ◦ 2000 collectors in a master server with a 5000 device license ◦ 3000 collectors in a slave server with the LMS monitoring server large edition license (with add-on licenses to manage additional performance collectors) • The IP SLA monitoring collector license limit applies only to historical hourly collectors and not to real-time collectors. However, you are allowed to create real-time collectors even after the license limit is reached. There is no limit to the number of real-time collectors that you could create to manage IP SLA monitoring functionality.

Add-on Licenses to Manage Additional Performance Collectors

You can apply the LMS add-on licenses to manage additional performance collectors in an LMS server. The scalability limits of add-on licenses are as follows:

- For the LMS 750 monitoring server license, the IP SLA collector limit is 1250.
- For the LMS 1500 monitoring server license the IP SLA collector limit is 1500.
- For the LMS 2500 monitoring server license the IP SLA collector limit is 3000.

Concurrent Users Supported

LMS 4.0 can support 20 concurrent users.

General Rule Regarding Number of Servers Needed for CiscoWorks LMS

Note: CiscoWorks LMS 4.0 can manage up to 5000 devices per server, meaning one server with adequate hardware configurations can manage up to 5000 devices with configuration management (refer to Tables 3 and 4 for Windows and Tables 5 and 6 for Solaris below), but an additional server will be needed to run fault management.

Note: For better performance and reliability, it is recommended to distribute the functionality across multiple servers once there are more than 5000 managed devices. For example, many users dedicate a server to the configuration management functionality, with other functionalities such as monitoring running on one or more servers depending on how heavily they are used.

Configuration

For large deployments, it may be necessary to distribute network management applications across multiple servers for enhancing performance or to accommodate a larger number of network devices. If a single server for CiscoWorks applications cannot handle the load when multiple applications are required, one solution is to distribute the following functionalities across several servers:

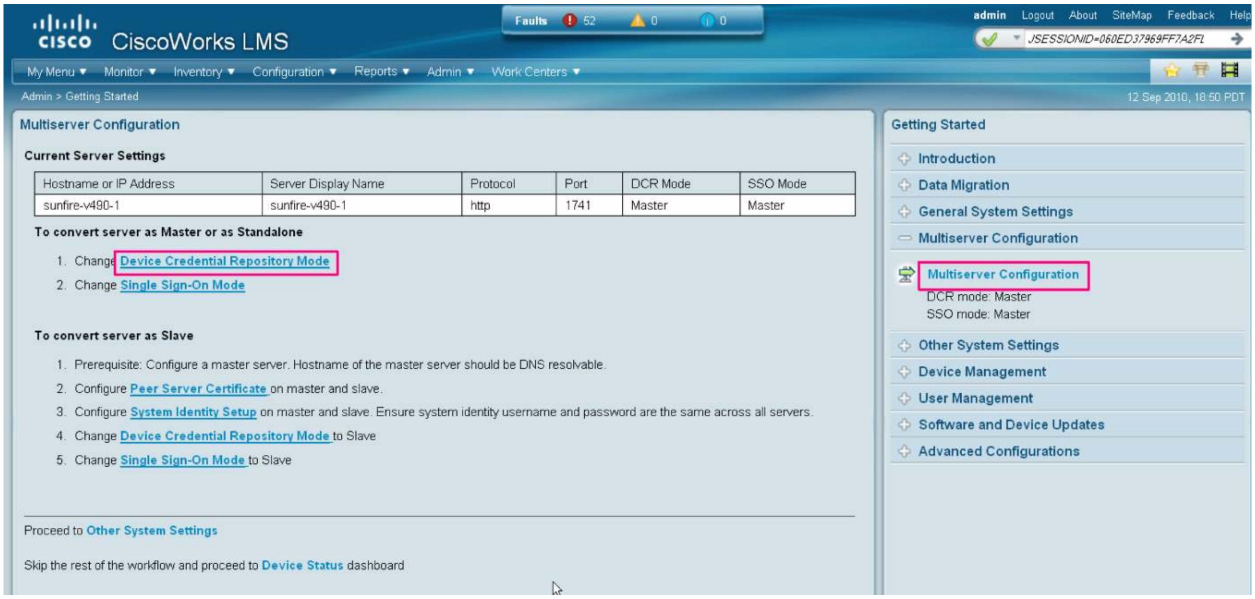
- Inventory, configuration, and image management

- Network topology, Layer 2 services, and user tracking
- Fault management
- IP SLA performance management

Steps for Setup

To set up the servers, select **Admin → Getting Started → Multiserver Configuration**. See Figure 2.

Figure 2. CiscoWorks LMS Multiserver Configuration Window


CiscoWorks LMS
Faults 52 0 0
admin Logout About SiteMap Feedback Help
JSESSIONID=060ED37969FF7A2FL
My Menu ▾ Monitor ▾ Inventory ▾ Configuration ▾ Reports ▾ Admin ▾ Work Centers ▾

Admin > Getting Started

12 Sep 2010, 18:50 PDT

Multiserver Configuration

Current Server Settings

Hostname or IP Address	Server Display Name	Protocol	Port	DCR Mode	SSO Mode
sunfire-v490-1	sunfire-v490-1	http	1741	Master	Master

To convert server as Master or as Standalone

1. Change Device Credential Repository Mode
2. Change Single Sign-On Mode

To convert server as Slave

1. Prerequisite: Configure a master server. Hostname of the master server should be DNS resolvable.
2. Configure Peer Server Certificate on master and slave.
3. Configure System Identity Setup on master and slave. Ensure system identity username and password are the same across all servers.
4. Change Device Credential Repository Mode to Slave
5. Change Single Sign-On Mode to Slave

Proceed to Other System Settings

Skip the rest of the workflow and proceed to Device Status dashboard

Getting Started

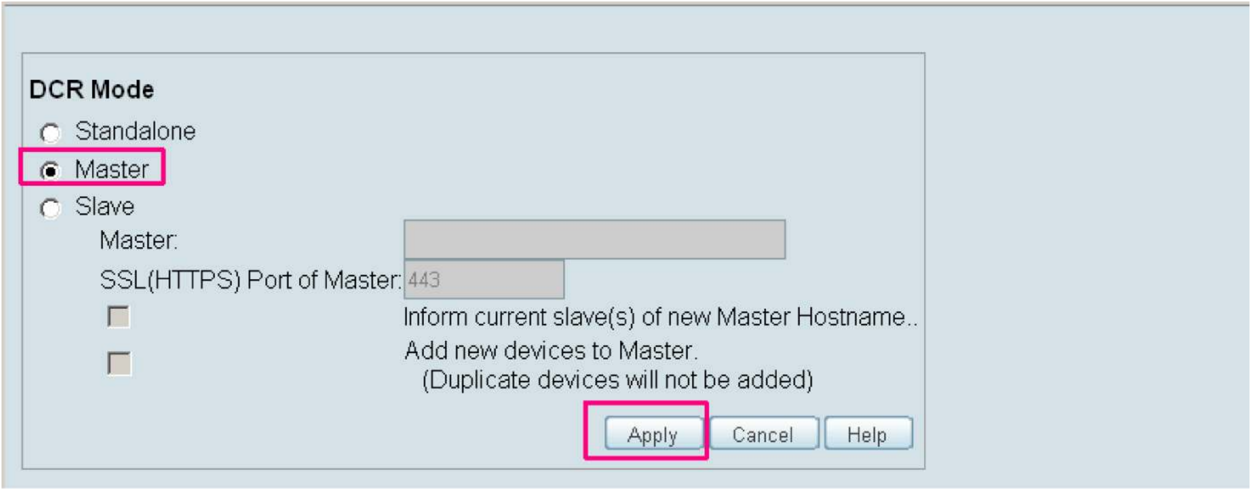
- Introduction
- Data Migration
- General System Settings
- Multiserver Configuration
  - Multiserver Configuration
    DCR mode: Master
    SSO mode: Master
- Other System Settings
- Device Management
- User Management
- Software and Device Updates
- Advanced Configurations

- **Set the Device Credential Repository (DCR) Mode**

  Chose the DCR mode. Standalone is the mode for single-server deployment.

  Choose either the master or the slave option, depending upon whether the current server that you are configuring is designated to be the master or a slave. If a server is designated as the master DCR server, all the discovered devices are added in the DCR of the master. If a server is designated as slave, then the devices that are discovered by the slave are added to the master DCR. See Figure 3.

Figure 3. Set the DCR Mode



DCR Mode

○ Standalone

● Master

○ Slave

Master:

SSL(HTTPS) Port of Master: 443

□ Inform current slave(s) of new Master Hostname..

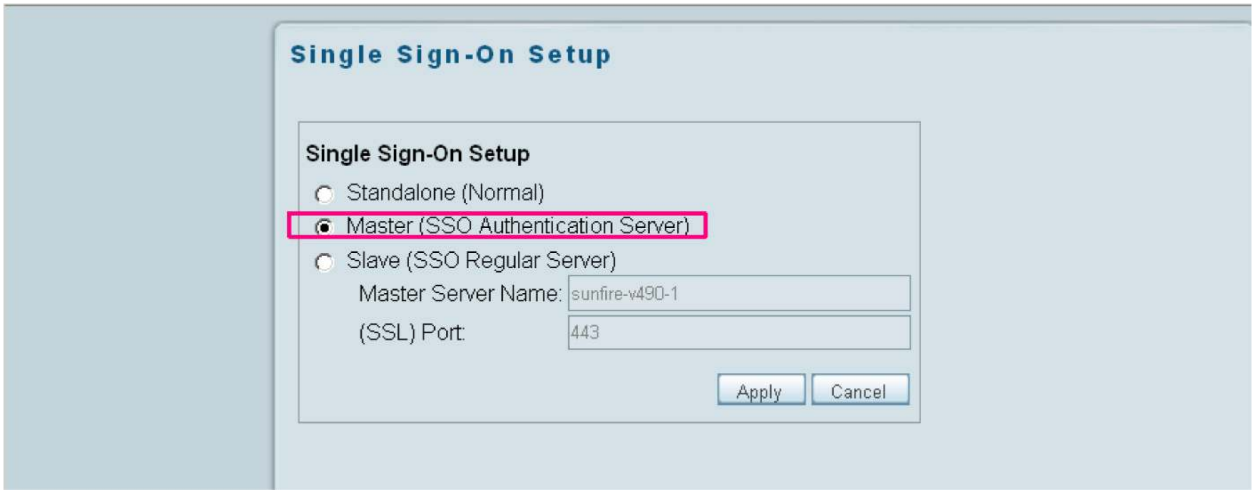
□ Add new devices to Master.
(Duplicate devices will not be added)

- **Set the Single Sign-on Mode**

With single sign-on mode, the user can sign on only once at the master server and need not also sign on to the servers that are designated as the slaves of the master. Single sign-on is also needed to configure the remote portlets of the slave servers into the dashboard of the master LMS server.

Again, whether you choose master or slave depends on whether you want to designate this server as the master or the slave. See Figure 4.

Figure 4. Set the Sign-on Mode



Single Sign-On Setup

Single Sign-On Setup

○ Standalone (Normal)

● Master (SSO Authentication Server)

○ Slave (SSO Regular Server)

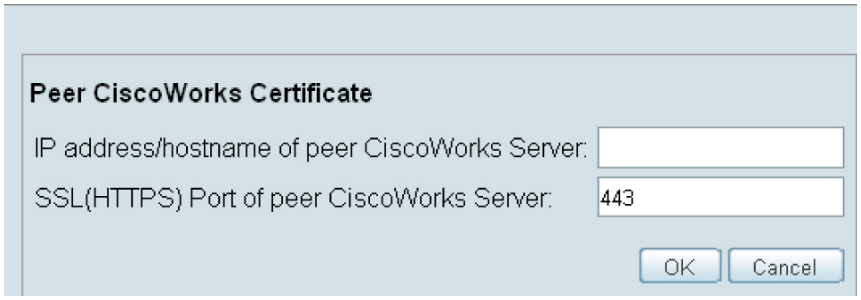
Master Server Name: sunfire-v490-1

(SSL) Port: 443

- **Exchange Peer Certificates**

  Enter the IP address of the peer CiscoWorks server. See.Figure 5.

Figure 5. Set the Peer Certificates



Peer CiscoWorks Certificate

IP address/hostname of peer CiscoWorks Server:

SSL(HTTPS) Port of peer CiscoWorks Server: 443

- **System Identity Setup**

  A default system identity user, admin, is created during installation. During the installation, the user should provide the password for the system identity user. This password can be different from that of the usual administrator user.

Note: It is recommended that the password be different for the usual administrator user and the system identity user, admin. Alternatively, you can create another user called sysadmin with full administrator access and use that ID for communication. In the multiserver setup, the same username/password combination (system identity user, password, and peer server user) should be configured across all servers.

Please refer to the “Multiserver Configuration” section of the *LMS 4.0 Deployment Guide* for more information.

Deployment Scenarios

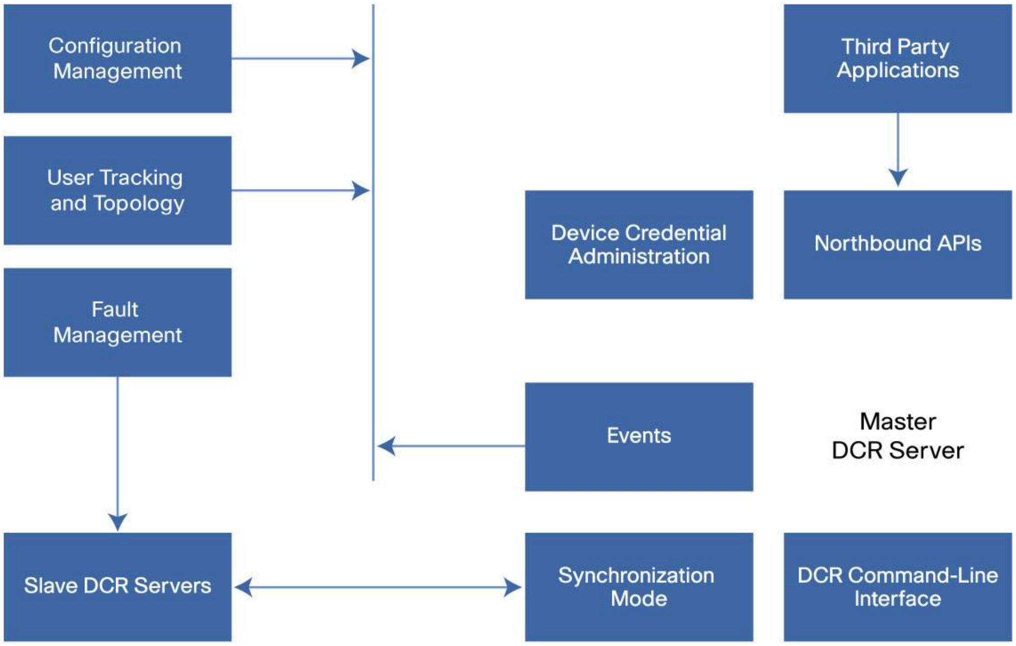
When working with large-scale deployments, it is important to determine the required server size and to decide whether to deploy the network management tools across multiple network management servers. Beyond the point where a single server is adequate, there may be a need to use multiple servers for a single management domain (a single managed network) by distributing applications across multiple servers for better performance and scaling.

Larger networks have to be split into multiple management domains and multiple groups managed by individual management servers or groups of servers. When a network is split into multiple domains, the division can be made in many ways: by administrative groups, by geography, or any other parameter that fits the network's administrative needs.

Device Credentials Repository

Figure 6 ullistrates the DCR architecture.

Figure 6. DCR Architecture



The DCR allows the user to manage the device list and associated credentials and other user-defined device attributes in a management domain. In a multiserver setup, where each server could host one or more CiscoWorks LMS management feature (such as configuration, monitoring, and so on) instances, the DCR could serve as the single repository where the user could manage the device lists and related attributes for use by all the applications in the domain.

Some of the key benefits of DCR are:

- Secure storage in one place
- Single-point management of devices and attributes
- Automatic replication among servers (for continuous operation even in the case of interserver link failures)
- Changes to the store allowed only in the master server

In a single-server scenario, the DCR will be operating in a standalone mode (the default mode after installation). In a multi-server scenario, the user should designate one of the servers as the master and configure the other servers in a slave mode. The copy of the DCR data in the slave servers is always in sync with the master DCR.

Note: The only data replicated between the master and slave servers is the DCR. Replication of other application data such as configuration, syslog, and so on are not supported yet.

The master DCR server contains the master repository of device list and credential data. There is only one master repository for each management domain, and it contains the most up-to-date device list and credentials. DCR slaves are slave instances of the DCR on other servers and provide transparent access to applications installed on those servers. Any change to the repository data occurs first in the master with the changes being propagated to all the slaves. There can be more than one slave in a management domain, but any slave can become a master at any time.

In a standalone mode, the DCR maintains an independent repository of device list and credential data. It does not participate in a management domain, and its data is not shared with any other DCR. It does not communicate with or contain registration information about any other master, slave, or standalone DCR.

Devices newly added in the DCR can be managed by the LMS management feature in the following ways:

- **Automanage mode:** In this mode, applications listen for the Add Device event and automatically start managing the device if it is relevant to the application. All the applications in the CiscoWorks LMS bundle are by default in automanage mode.
- **Manual-manage mode:** In this mode, the application keeps track of all newly added devices and shows the list to the user. The user chooses few or all devices from the list for the application to manage.

If the two servers are set up as master/slave, they will share the same copy of DCR. All changes to DCR must be done on the master first then replicate to the slave. In case of failure:

- If the slave fails permanently, the master will continue to work.
- If the master fails permanently, the slave will continue to work, but it cannot add or discover new devices. The slave needs to be changed back to standalone mode or promoted to be a master when joined by other slaves to be fully functional.
- If either the master or slave fails transiently, the servers automatically recover once they get back online.

Managing 5000 Devices on the Same Server

License requirement: **CWLMS-4.0-5K-K9**

For a single server as a network management platform with all functionalities on one server, you could manage up to 5000 devices, and that is the highest tested and certified number in the single-server configuration. See Tables 3, 4, 5, and 6 for detailed requirements.

Recommended Hardware Requirements (Windows)

Table 3. Recommended Windows System Requirements

Windows	Recommended System Requirements
CPU	2 CPUs 8 core or 4 CPUs with quad core (For supported CPU types refer to Table 4)
RAM	16 GB
Disk space	120 GB or more free space for CiscoWorks LMS applications and data
Virtual memory (swap space)	32 GB

Windows	Recommended System Requirements
Software for Windows	Windows 2003 Standard Edition (with Service Pack 2) Windows 2003 Enterprise Edition (with Service Pack 2) Windows 2003 Standard Edition R2 (with Service Pack 2) Windows 2003 Enterprise Edition R2 (with Service Pack 2) Windows 2008 Server Standard Edition Release 1 with Service Pack 1 and Service Pack 2 Windows 2008 Enterprise Editions Release 1 with S Service Pack 1 and Service Pack 2 **Note:** Both 32-bit and 64-bit operating systems are supported on the above versions.

Table 4. Processors Supported

Vendor	Supported Processor
Intel	Intel Xenon Processor Intel Core Duo processor T2600 – T2300 Intel-VT processors (VMware Optimized hardware) Intel Xeon processor 5400 series Intel Xeon processor 5300 series Intel Xeon processor 7300 series Intel Xeon processor 5500 series Intel Xeon processor 5600 series
AMD	AMD Opteron Processor AMD Athlon 64 FX Processor AMD Athlon 64 X2 AMD -V

LMS 4.0 Virtualization Systems Support

- VMware ESX server 3.0.x
- VMware ESX Server 3.5.x
- VMware ESX 4.x
- VMware ESXi 4.x
- Hyper V Virtualization

Unified Computing System support

LMS 4.0 is supported on the Unified Computing System (UCS) B-series blade servers (B200-M1 or M2 and B250-M1 or M2) and C-series rack-mount servers (C200-M1 or M2, C210-M1or M2, and C250-M1 or M2). The server requirements on UCS blade servers and rack-mount servers remain the same as the server requirements on Windows systems.

The supported processor in UCS B-series blade servers is Intel Xeon 5500 or 5600 Series processors. For more information see http://www.cisco.com/en/US/prod/collateral/ps10265/ps10280/data_sheet_c78-524797_ps10279_Products_Data_Sheet.html.

The supported processor in UCS C-series rack-mount servers is Intel Xeon 5500 or 5600 Series processors with their choices mentioned explicitly. For more information see http://www.cisco.com/en/US/products/ps10493/products_data_sheets_list.html.

Recommended Hardware Requirements (Solaris)

Table 5. Recommended Solaris System Requirements

Solaris	Recommended System Requirements
CPU	2 CPUs with 8 core or 4 CPUs with quad core
RAM	16 GB
Disk space	72 GB or more free space for CiscoWorks LMS applications and data
Swap space	32 GB
Software	LMS 4.0 supports the following Solaris 10 releases: ● Solaris 10, 10/09 release ● Solaris 10, 05/09 release ● Solaris 10, 10/08 release ● Solaris 10, 05/08 release ● Solaris 10, 08/07 release ● Solaris 10, 11/06 release Solaris Zones (Supported from Solaris 10) is a virtualization technology from Sun Microsystems (http://www.sun.com). It allows you to create isolated and secure environments called zones for running applications. LMS 4.0 is installed on the global zone of the Solaris 10 operating system by default. LMS 4.0 supports installing LMS in the whole-root nonglobal zone. If the whole-root nonglobal zone is configured in the server, installing LMS 4.0 in the global zone is not supported. Sparse root zone is not supported. There is no specific hardware or software requirement for zone support. LMS works in the same way in nonglobal zones as it works in global zone. LMS 4.0 also supports logical domains (LDoms) and the ZFS file system.

Table 6. Supported CPUs for Solaris

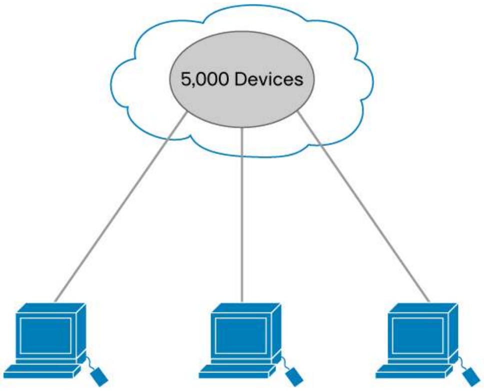
Supported Processor
● UltraSPARC IV processor ● UltraSPARC IV+ processor ● UltraSPARC T1 processor ● UltraSPARC T2 processor ● UltraSPARC T2+ processor ● SPARC64 VI processor ● SPARC64 VII processor

Applications on Separate Servers Managing a Single Domain

License requirement: **CWLMS-4.0-5K-K9**

Figure 7 shows four management servers being used to manage a network of 5000 devices, with each management feature from CiscoWorks LMS distributed across a separate server. The distribution has been done based on the tested scaling limit for each management feature.

Figure 7. Distributed Deployment Scenario: Single Management Domain



The hardware and software configuration recommendation for each server, namely, CiscoWorks for configuration management, fault management, topology and user tracking, and IP SLA performance management, is similar; please refer to Tables 3 and 4 for Windows and Tables 5 and 6 for Solaris.

Concept: Device Management Functions

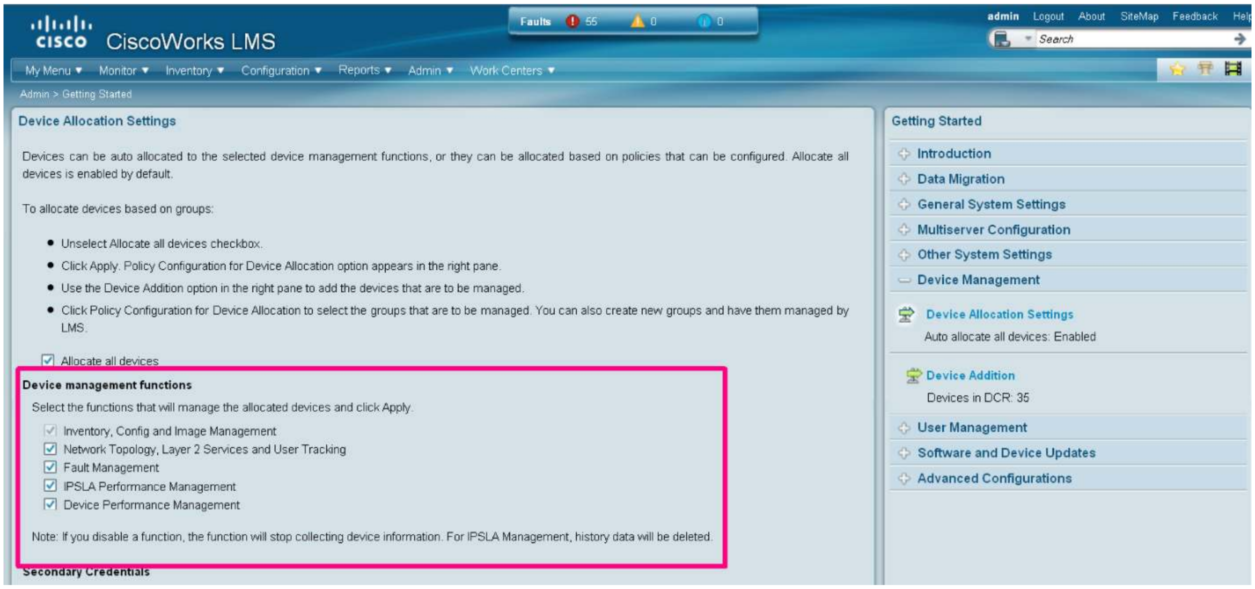
In LMS, the functionalities are divided into five broad categories:

- Inventory, configuration, and image management
- Network topology, Layer 2 services, and user tracking
- Fault management
- IP SLA performance management
- Device performance management

Any of these functionalities can be turned on/off on any given server, except for the inventory, configuration, and image management functionality, which is always on.

To turn any of these functionalities on/off, select **Admin → Getting Started → Device Management → Device Allocation Settings**. See Figure 8.

Figure 8. The CiscoWorks LMS Device Allocation Settings Window



Device Allocation Settings

Devices can be auto allocated to the selected device management functions, or they can be allocated based on policies that can be configured. Allocate all devices is enabled by default.

To allocate devices based on groups:

- Unselect Allocate all devices checkbox.
- Click Apply. Policy Configuration for Device Allocation option appears in the right pane.
- Use the Device Addition option in the right pane to add the devices that are to be managed.
- Click Policy Configuration for Device Allocation to select the groups that are to be managed. You can also create new groups and have them managed by LMS.

☑ Allocate all devices

Device management functions

Select the functions that will manage the allocated devices and click Apply.

☑ Inventory, Config and Image Management
☑ Network Topology, Layer 2 Services and User Tracking
☑ Fault Management
☑ IPSLA Performance Management
☑ Device Performance Management

Note: If you disable a function, the function will stop collecting device information. For IPSLA Management, history data will be deleted.

Auto allocate all devices: Enabled

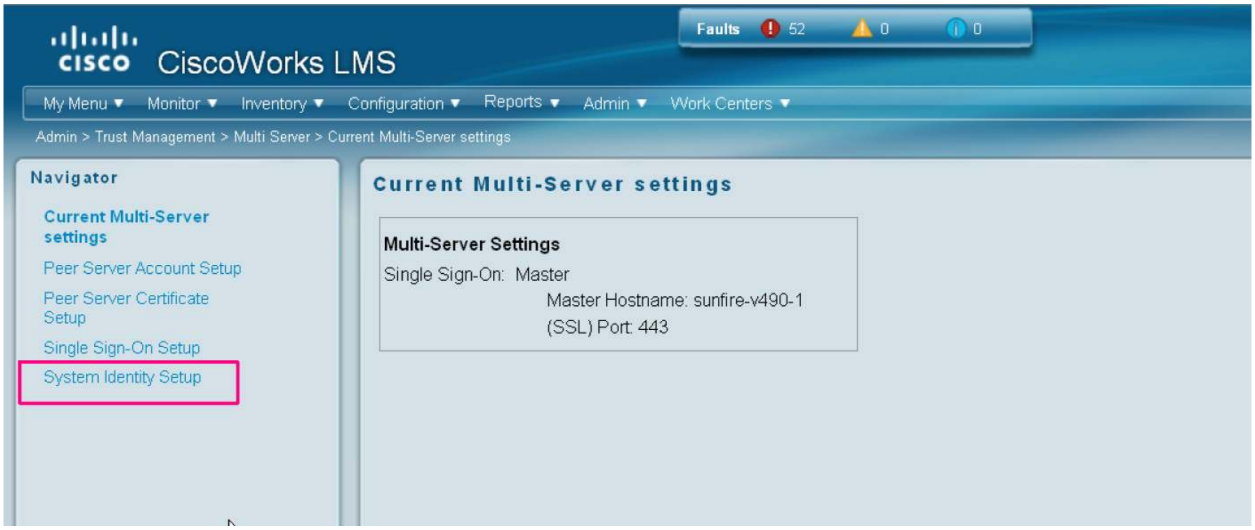
Devices in DCR: 35

In this deployment scenario, you will use and deploy the master-slave concept of DCR. You could install Server 1 with the inventory, configuration, and image management functionality and disable the other functionalities, where DCR could be configured as the master. Server 2 will have network topology, Layer-2 services, and user tracking turned on and the other functionalities turned off. Server 3 will have only fault management turned on, and Server 4 will have only IP SLA performance management turned on. In Servers 2, 3, and 4, DCR mode will be configured as slave to Server 1.

The following setup is recommended for the scenario shown in Figure 4:

- Import the peer server certificate from Servers 2, 3, and 4 to Server 1.
- Set up a system identity user on Server 1, and configure the same user as for the peer server account on Servers 2, 3, and 4. Select **Admin → Trust Management → Multi Server → System Identity Setup**. See Figures 9 and 10.

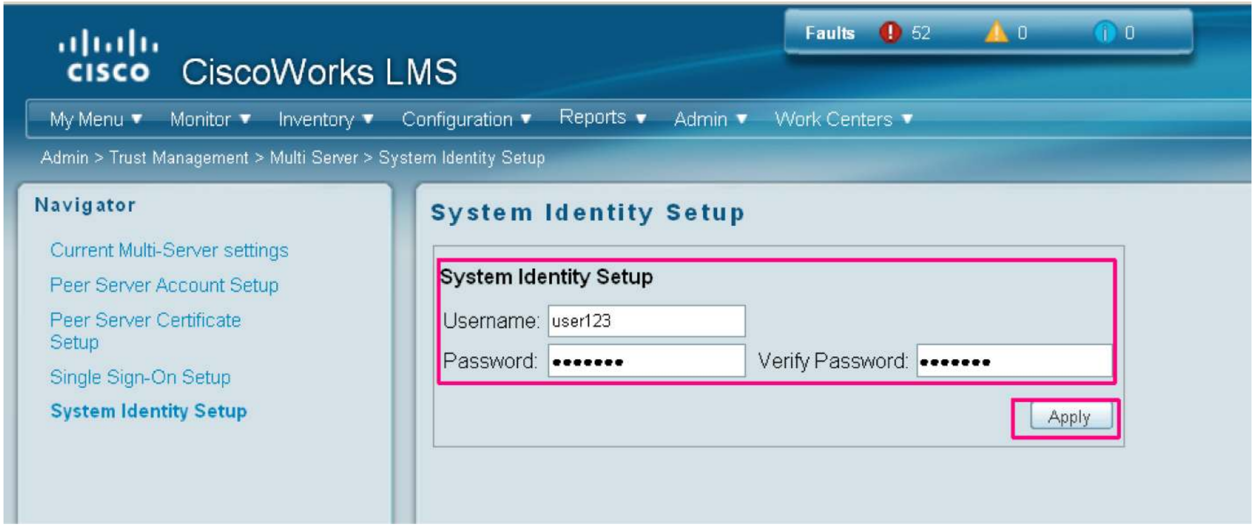
Figure 9. Configuring the Multiserver Settings


CiscoWorks LMS
Faults 52 0 0
My Menu ▼ Monitor ▼ Inventory ▼ Configuration ▼ Reports ▼ Admin ▼ Work Centers ▼
Admin > Trust Management > Multi Server > Current Multi-Server settings
Navigator
Current Multi-Server settings
Peer Server Account Setup
Peer Server Certificate Setup
Single Sign-On Setup
System Identity Setup

Current Multi-Server settings

Multi-Server Settings
Single Sign-On: Master
Master Hostname: sunfire-v490-1
(SSL) Port: 443

Figure 10. Configuring the System Identity Setup


CiscoWorks LMS
Faults 52 0 0
My Menu ▼ Monitor ▼ Inventory ▼ Configuration ▼ Reports ▼ Admin ▼ Work Centers ▼
Admin > Trust Management > Multi Server > System Identity Setup
Navigator
Current Multi-Server settings
Peer Server Account Setup
Peer Server Certificate Setup
Single Sign-On Setup
System Identity Setup
Apply

System Identity Setup

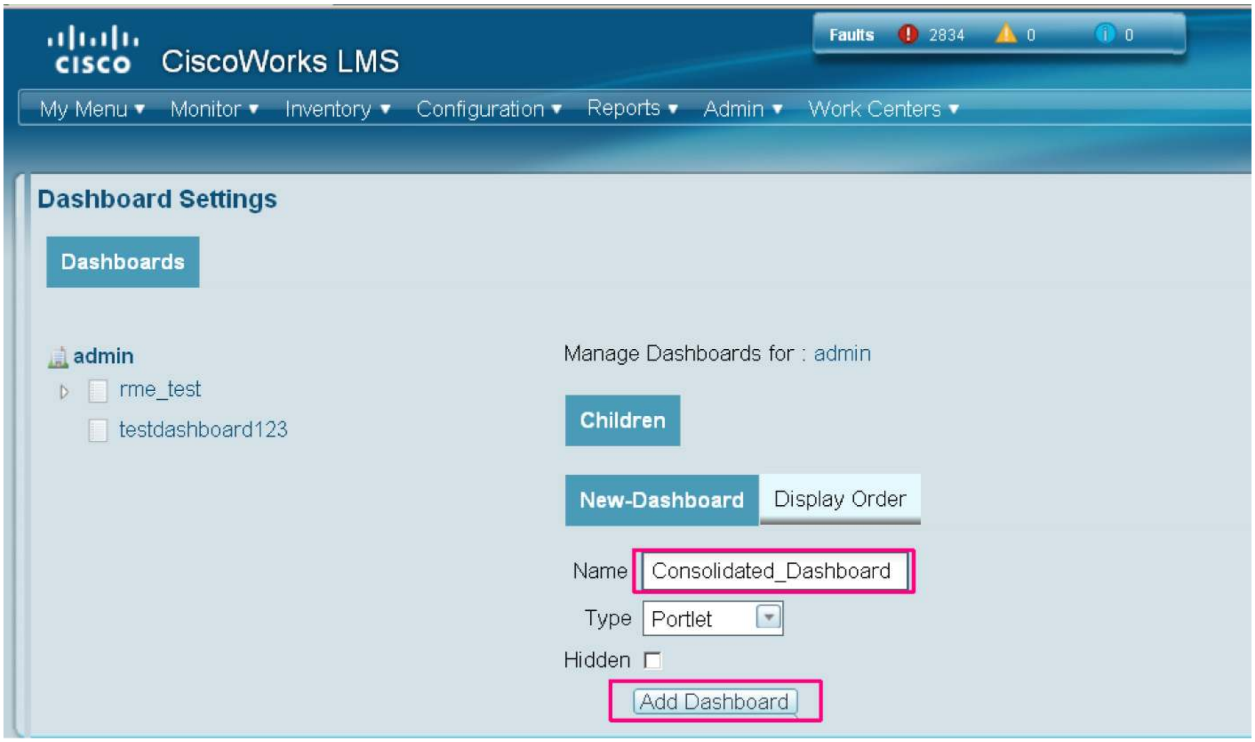
System Identity Setup
Username: user123
Password: ••••••• Verify Password: •••••••

- Configure Server 1 DCR as master, and then configure Servers 2, 3, and 4 DCR as slaves of Server 1.

- Enable the default credential sets in DCR, and select the default credential sets while configuring device discovery.
- Run a complete discovery of the network, which in turn populates the master DCR server.
- Direct syslog messages to the CiscoWorks configuration management server and SNMP traps to the CiscoWorks fault management server, which could also forward Simple Network Management Protocol (SNMP) traps to other trap listeners.

Configure one of the servers for the CiscoWorks homepage to register applications installed on remote servers, and configure the remote portlets to be included in master server. Select **My Menu → Manage Dashboards**. See Figure 11.

Figure 11. Configuring the Dashboard Settings



Dashboard Settings

Manage Dashboards for : admin

Name Consolidated_Dashboard

Type Portlet

Hidden ☐

Select **My Menu → My Dashboards**.

Click the newly created dashboard (Consolidated_Dashboard).

Now add the remote portlets (from other servers).

To do this, see Figures 12, 13, and 14.

Figure 12. Select the '+' icon

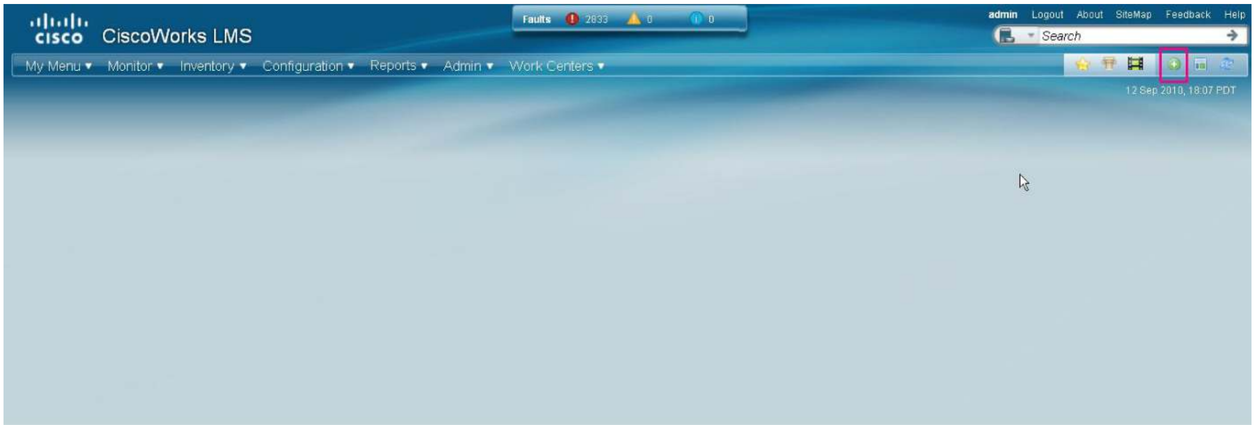

CiscoWorks LMS
Faults 2833 0 0
admin Logout About SiteMap Feedback Help
Search
My Menu ▾ Monitor ▾ Inventory ▾ Configuration ▾ Reports ▾ Admin ▾ Work Centers ▾
12 Sep 2010, 18:07 PDT

Figure 13. Set the Multiserver Settings

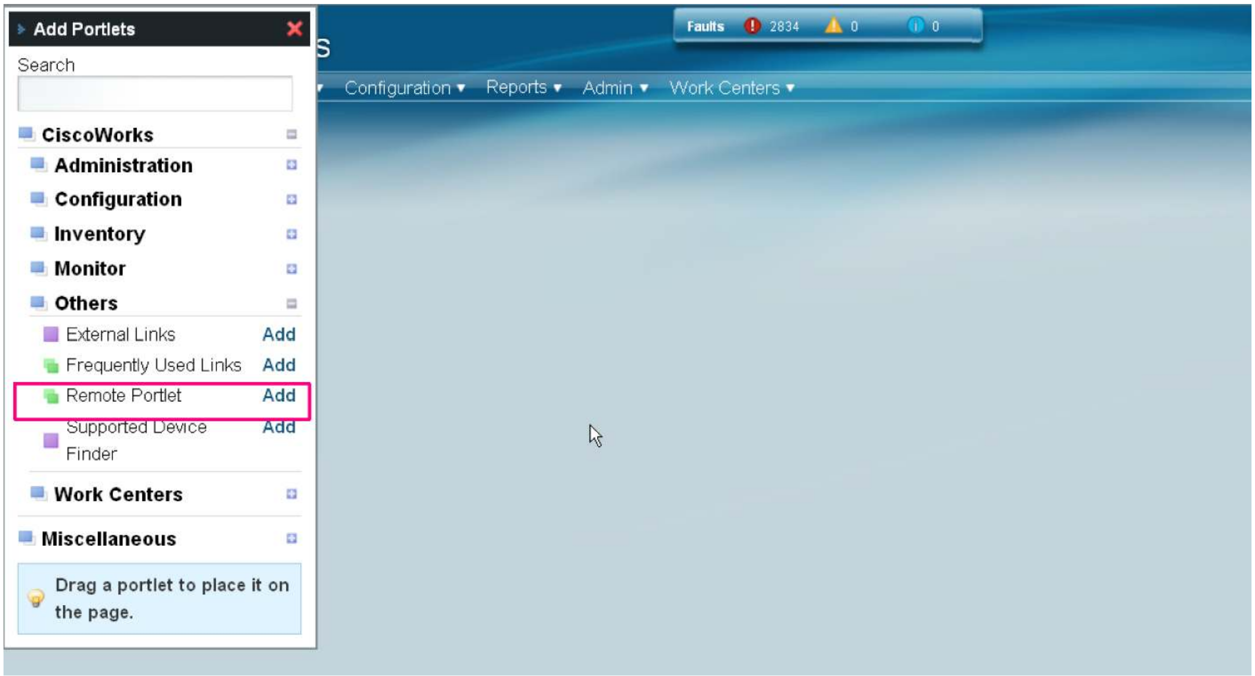
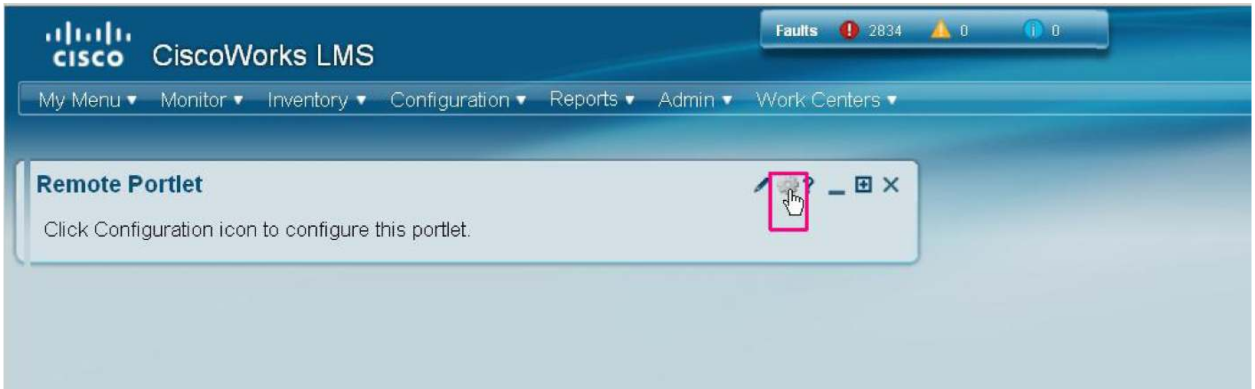


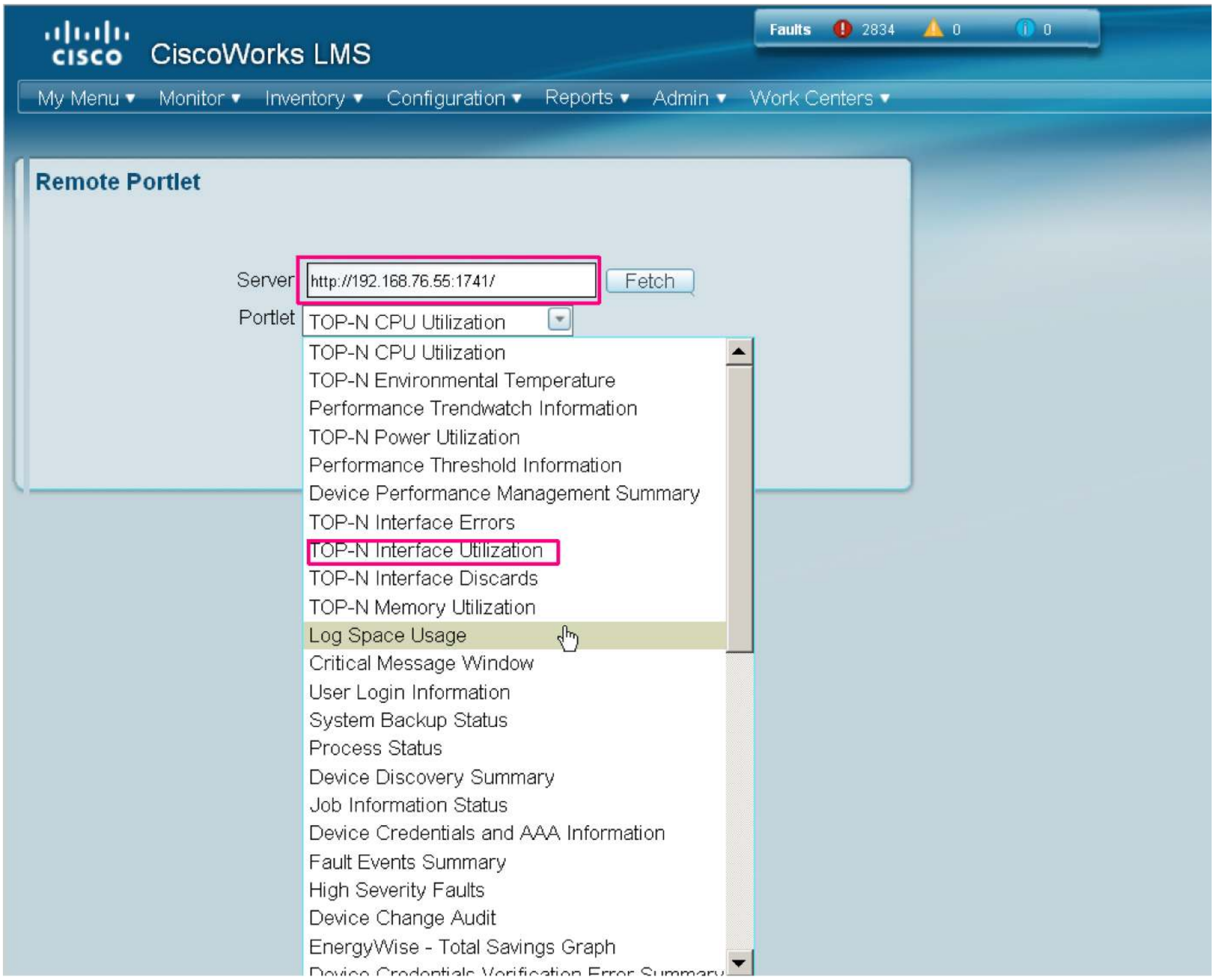
Figure 14. Configure the System Identity Setup


CiscoWorks LMS
Faults 2834 0 0
My Menu ▾ Monitor ▾ Inventory ▾ Configuration ▾ Reports ▾ Admin ▾ Work Centers ▾

Remote Portlet

Click Configuration icon to configure this portlet.

Figure 15. Choose the Server and Portlet to Include in the Dashboard



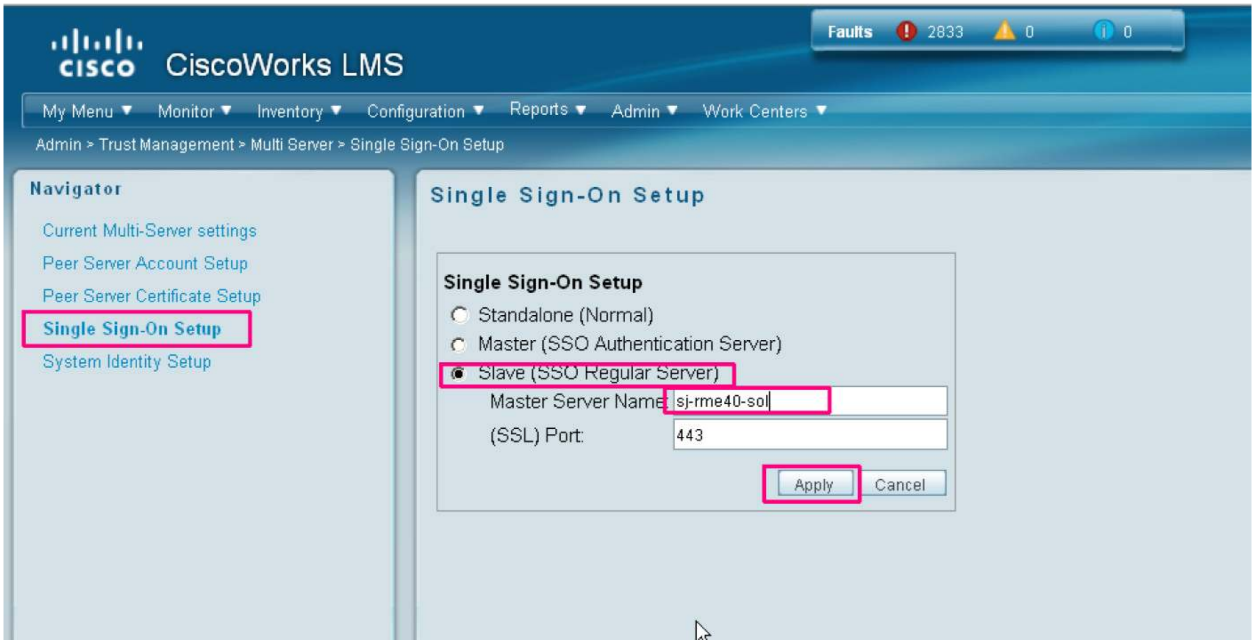
Server: http://192.168.76.55:1741/

Portlet: TOP-N CPU Utilization

In Figure 15, **chose the server and the** portlet that you want to include in this dashboard. Repeat the process to add as many remote portlets as you desire to consolidate the portlets from the remote severs.

Configure stateful switchover (SSO) across all the servers to help ensure better navigation between applications installed on different servers. Assign 1 server as the master and the others as slaves and configure the SSOs. On the slave servers, select **Admin → Trust Management → Multi Server → Single Sign-on Setup**. See Figure 16.

Figure 16. Assigning the SSOs



Single Sign-On Setup

○ Standalone (Normal)
○ Master (SSO Authentication Server)
● Slave (SSO Regular Server)

Master Server Name: sj-rme40-sol
(SSL) Port: 443

Multiple Instances of CiscoWorks LMS Bundle (Multiple Management Domains)

License requirement: Three **CWLMS-4.0-5K-K9** (The number of licenses required equals the number of servers, and in this scenario, three **CiscoWorks LMS licenses are required.)**

When the network contains more than 13,000 devices, it must be divided into multiple management domains, and multiple servers (or groups of servers) must be deployed. In specific instances, it may be preferable to do so for administrative reasons, even if the numbers do not warrant a division.

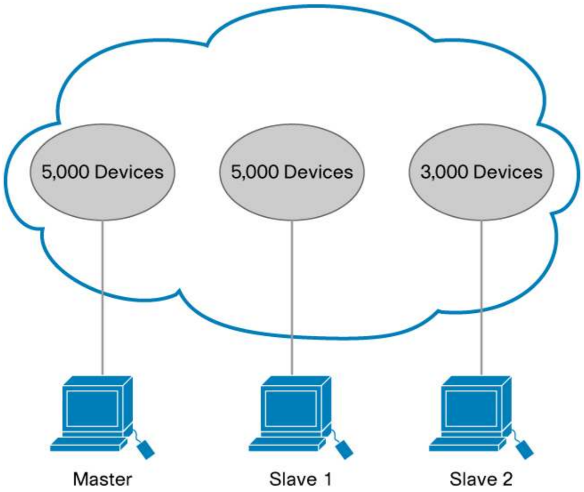
The network could be segmented based on:

- SYS location
- IP address ranges
- LAN and WAN boundaries

Look for administrative logic - separate management teams or regions, or administrative groupings. Make sure there is a clear demarcation of which management workstation is managing which device and vice versa and remember to account for future growth.

Consider the scenario shown in Figure 17, where a network of 13,000 devices is broken into three groups of up to 3500 devices with a separate CiscoWorks LMS server for each segment of the network.

Figure 17. Distributed Deployment Scenario--Multiple Management Domains



Configure each instance of CiscoWorks to discover the part of the network that it intends to manage. You can achieve this by limiting the discovery by IP range. In this scenario, there is no communication between servers and, thus, no sharing of information. See Tables 3 and 4 for Windows and Tables 5 and 6 for Solaris for the recommended system requirements.

In the preceding setup, anyone requiring centralized access to the servers can get it by creating a CiscoWorks private dashboard view. Install CiscoWorks LMS on a server (master) and then register all applications from all the other servers (slaves) in the newly configured dashboard as described in the previous pages.

Centralized CiscoWorks Configuration Management Server

License requirement: **One CWLMS-3.0-10K-K9**

In this scenario, a centralized CiscoWorks configuration management server is used because of better scalability compared to other functionalities in CiscoWorks LMS. Assume that the customer has 10,000 devices and each server manages a set of devices. There is a centralized server that helps manage the entire set of devices and can be used as a backup server.

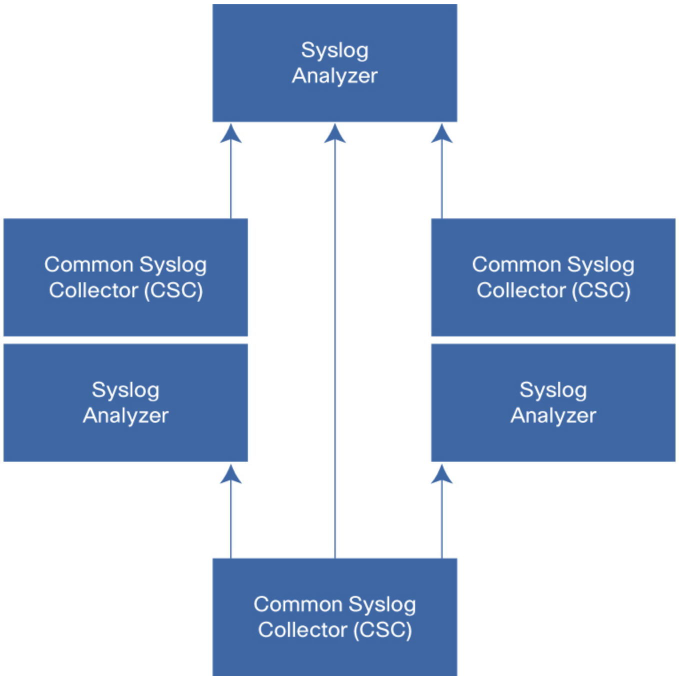
Before discussing details of the centralized server, it is important to understand the new concept of a distributed syslog collector and analyzer introduced in CiscoWorks RME.

Distributed Syslog Collection

The syslog application has the following features (see Figure 18):

- **Common Syslog Collector (CSC):** Helps in receiving, validating, filtering, and forwarding syslogs.
- **Syslog Analyzer:** Responsible for receiving syslogs from the collector, invoking automated actions and storing them in the database, and generating reports.
- **Collectors and analyzers:** Help in balancing the syslog processing load by making syslog servers subscribe to syslog collectors.
- **Easy time zone support:** Supports any time zone by allowing you to edit the configuration file.
- **Drop/keep filtering:** Allows you to keep or drop syslogs. The enhanced filtering capabilities allow you to consider interfaces as well.
- **Import/export:** Helps in import and export of automated actions and message filters in syslogs.

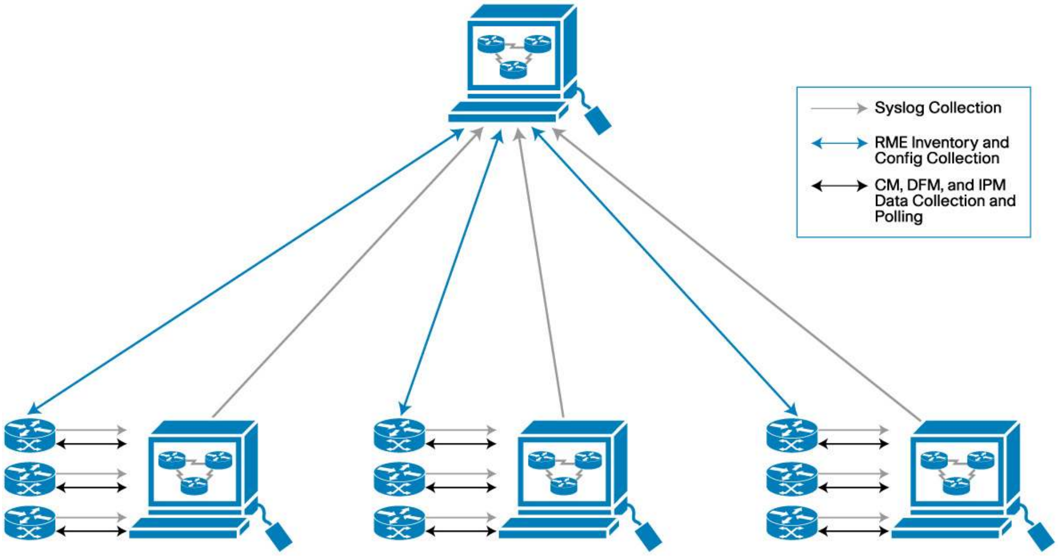
Figure 18. Distributed Syslog Collection


Syslog Analyzer
Common Syslog Collector (CSC)
Syslog Analyzer
Common Syslog Collector (CSC)
Syslog Analyzer
Common Syslog Collector (CSC)

This central CiscoWorks configuration management design provides a single reporting server for inventory, configurations, and syslogs. In this scenario, there will be multiple CiscoWorks LMS servers that will manage parts of the network, and there will be one CiscoWorks configuration management server that will manage the enterprise with customized policies. The policies will allow scalability up to the maximum permitted number of devices in the network.

A central CiscoWorks configuration management server could be populated with all the network devices by importing the device list from a central network management system (NMS), such as HP OpenView Network Node Manager, or by exporting/importing the device list from each local CiscoWorks LMS server. The inventory and configuration archive collection will be configured with multiple jobs, each containing a set of devices. Each device will be configured to send the syslog to the respective local CiscoWorks server where the device is managed. The syslog analyzer on the central CiscoWorks server will subscribe to the syslog collector of each of these CiscoWorks servers with central log filters. See Figure 19.

Figure 19. Centralized CiscoWorks Server


Syslog Collection
RME Inventory and Config Collection
CM, DFM, and IPM Data Collection and Polling

High Availability Configuration

Overview

CiscoWorks LMS does not support high availability (HA) by design, but high availability could be achieved by using the Veritas solution. HA functionality can also be achieved in the VMware environment by using the VMware HA feature. For detailed description of HA for Veritas as well as VMware, please refer to Chapters 4 and 5 in *Installing and Migrating to CiscoWorks LAN Management Solution 4.0.*

High Availability Configuration Using Veritas

The main steps for HA setup for Veritas are as follows:

- Install Veritas Storage Foundation HA 5.0 on Windows.
- Create Disk Groups and Volumes on the primary and secondary servers.
  - A disk group is a collection of disks that is ported as a single unit. Veritas Storage Foundation uses disk groups to organize disks for management purposes.
  - Volumes are logical entities that consist of portions of one or more physical disks and are accessed by a drive letter or mount point. Volumes can be configured for performance and high availability.
- Install LMS on the primary and secondary servers. Make sure that:
  - Admin password, database password, and HTTP ports are the same on both the primary and secondary servers
  - Name of the LMS volume is the same on both the servers
  - Causer settings are the same on both the servers
- Set up Veritas Volume Replication.

Veritas Volume Replicator is a fully integrated component of Veritas Volume Manager that replicates **data to remote locations over any standard IP network to provide continuous data availability.**

  - Set up RDS, RVG, and RLINK

    Replication Data Set (RDS) is an important step to get replication started. Data is replicated from a primary node (where the application is running) to one or more secondary nodes.

An RDS consists of a Replication Volume Group (RVG) on the primary node and the corresponding RVG on the secondary nodes.

A Replication Link (RLINK) is associated with an RVG and it establishes the link between the primary and a secondary RVG. The RLINKs associated with the primary RVG control the replication settings.

  - Set Causer permissions on the cscopx volume.

- Set the Veritas Cluster.

High Availability Using VMware

VMware High Availability is a simple and cost-effective solution that helps ensure high levels of availability during a planned or unplanned downtime.

VMware HA uses multiple ESX or ESXi hosts configured as a cluster to provide rapid recovery from outages and high availability for applications running in virtual machines. You must create a cluster, populate it with hosts, and configure VMware HA settings before failover protection can be established. After you finish the initial setup of the host, download and install the vSphere Client. The vSphere Client is a Windows program that you can use to configure the host and to operate its virtual machines. It allows you to connect to an ESX or ESXi host and to a vCenter Server system. Connect to the host and add your virtual machine by importing a virtual appliance.

VMware HA protects application availability in two ways:

- It protects against a server failure by automatically restarting the virtual machines on other hosts within the cluster.
- It protects against application failure by continuously monitoring a virtual machine and resetting it in the event that a failure is detected.

Steps to Set HA Using VMware HA

1. Install ESX or ESXi 4.0 in two or more servers.
2. Install vCenter Server 4.0 in any server with a proper license.
3. Install vSphere Client in the client server and connect to vCenter Server.
4. Create a cluster and add ESX or ESXi hosts to it.
5. Configure the shared storage that is accessible to all the hosts in the cluster.
6. Create a virtual machine and select a data store as a shared storage disk.
7. Configure VMware HA settings for the cluster created.
8. Make sure that sufficient resources are available in the cluster.
9. Make sure that there are no errors or alert messages (select **Cluster → Summary page**) in the vSphere Client.
10. Install LMS 4.0 in the virtual machine created in the shared storage.

CiscoWorks 4.0 Authentication and Authorization

Overview

It is easy to confuse the mechanisms of *authentication* with *authorization*.

Authentication is the mechanism whereby systems may securely identify their users. The authentication mechanism provides answers to the following questions:

- Who is the user?
- Is the user really who he/she represents himself/herself to be?

Authorization, by contrast, is the mechanism by which a system determines what level of access a particular authenticated user should have to secured resources or functionality. Authorization systems provide answers to the following questions:

- Is user X authorized to access resource R?
- Is user X authorized to perform operation P?
- Is user X authorized to perform operation P on resource R?

Authorization and authentication are somewhat tightly coupled mechanisms - authorization systems depend on authentication to help ensure that users are whom they claim to be and thus prevent unauthorized users from gaining access to secured resources.

Authentication in LMS 4.0

CiscoWorks 4.0 supports the following authentication modes:

- **Local mode:** Users are defined and managed in LMS
- **Remote mode:** Allows the LMS application to authenticate users with external authentication servers for central control. The following external authentication methods are available:
  - Local UNIX system
  - IBM SecureWay Directory
  - Microsoft Active Directory
  - Netscape Directory
  - RADIUS
  - Kerberos
  - TACACS+

To set up the authentication mode, go to:

Admin → System → Authentication Mode Setup

Notes:

- In the remote mode, the administrator will still have to add the user (same user ID as in ACS) to LMS.
- The user's local password in LMS will be used to authenticate in case the remote ACS is down.

Authorization in LMS 4.0

In the earlier releases of LMS (LMS 3.2 and prior), it was required that the ACS 4.x server be configured to determine on which devices the user could perform the tasks. That is, the authorization was performed in the ACS server. **In 4.0, authorization is done locally within the LMS server.**

Benefits of doing the authorization locally in LMS:

- No need for additional setups in ACS.
- Access control happens on the same group of devices that are known to LMS, instead of groups defined in ACS.
- Multiple roles can be assigned to the user.

To manage user roles:

Admin → Getting Started → Manage Roles (Add)

To create users in LMS:

Admin → Getting Started → Manage Users (Add)

For further information on how to define roles, add users, and assign roles to users, please refer to the LMS 4.0 User's Guide.

Recommendations and Tips for Performance Improvements

The UI performance of the application client can be improved by using device groups when executing application tasks, especially when a single server is managing a large number of devices.

When you configure systems to manage a large number of devices, consider the following:

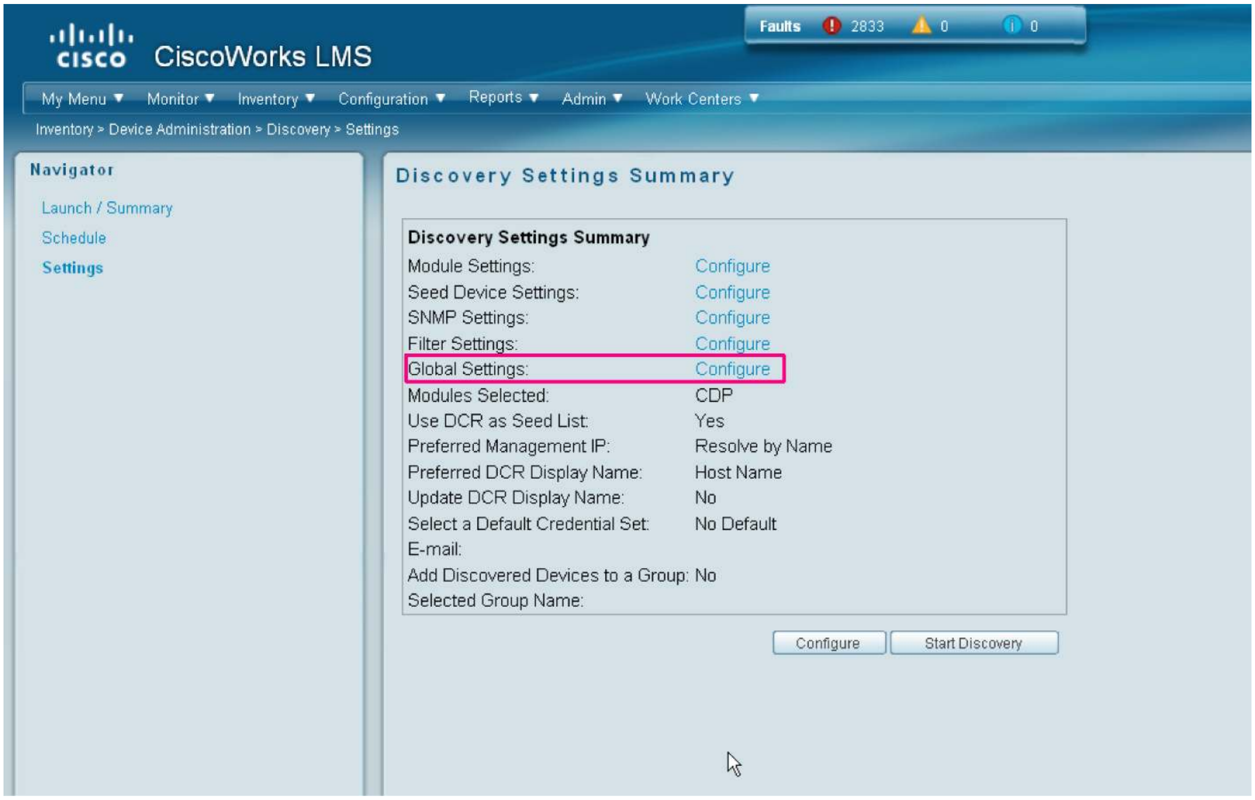
Device Discovery

It is recommended that you set up the discovery schedule to a less frequent one and choose the time most appropriate to you. (This process is required to find the new devices added to your network.) Select the discovery parameters most suitable to your environment so that it could speed up the discovery process, and discover and populate correct values.

- Choose Use Loopback Address if loopback addresses are configured on the devices and you want those addresses to be the management IP address in CiscoWorks LMS.

Select **Inventory → Discovery → Settings**. See Figures 20 and 21.

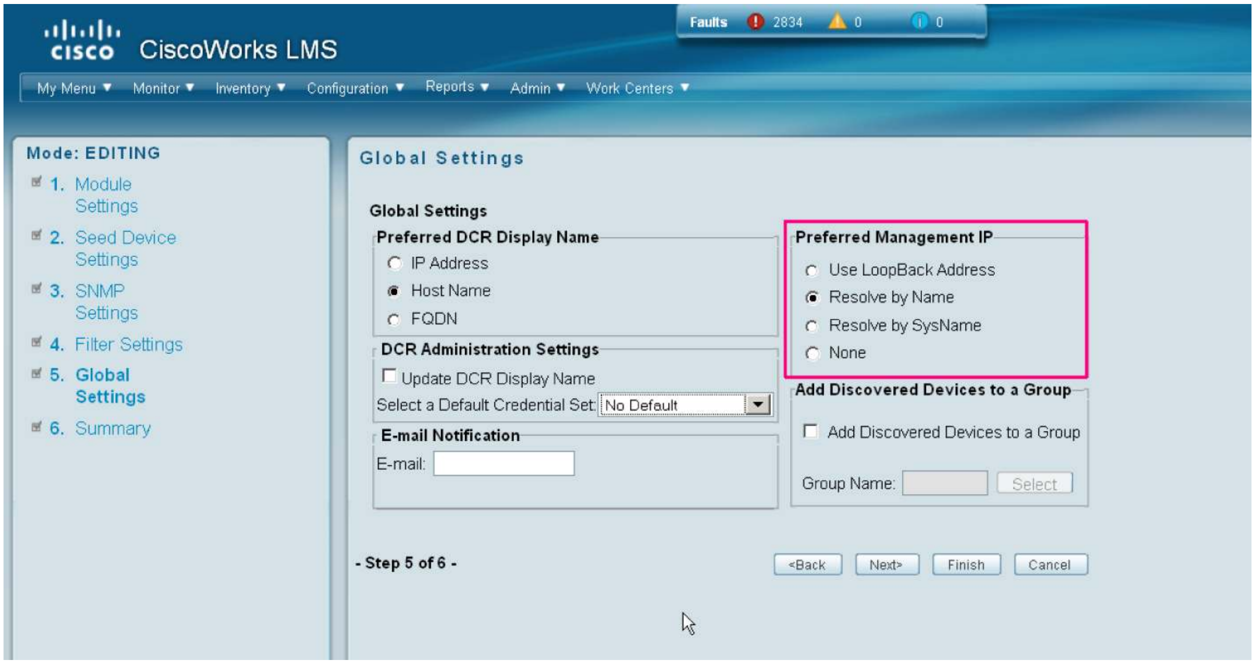
Figure 20. Configuring the Global Settings


CiscoWorks LMS
Faults 2833 0 0
My Menu ▼ Monitor ▼ Inventory ▼ Configuration ▼ Reports ▼ Admin ▼ Work Centers ▼
Inventory > Device Administration > Discovery > Settings
Navigator
Launch / Summary
Schedule
Settings
Discovery Settings Summary
Configure
Start Discovery

Discovery Settings Summary

Module Settings:	Configure
Seed Device Settings:	Configure
SNMP Settings:	Configure
Filter Settings:	Configure
Global Settings:	Configure
Modules Selected:	CDP
Use DCR as Seed List:	Yes
Preferred Management IP:	Resolve by Name
Preferred DCR Display Name:	Host Name
Update DCR Display Name:	No
Select a Default Credential Set:	No Default
E-mail:	
Add Discovered Devices to a Group:	No
Selected Group Name:	

Figure 21. Selecting the Preferred Management IP


Faults 2834 0 0
CiscoWorks LMS
My Menu ▼ Monitor ▼ Inventory ▼ Configuration ▼ Reports ▼ Admin ▼ Work Centers ▼
<Back
Next>
Finish
Cancel

Mode: EDITING

1. Module Settings
2. Seed Device Settings
3. SNMP Settings
4. Filter Settings
5. Global Settings
6. Summary

Global Settings

Global Settings

Preferred DCR Display Name
○ IP Address
● Host Name
○ FQDN

DCR Administration Settings
□ Update DCR Display Name
Select a Default Credential Set: No Default

E-mail Notification
E-mail:

Preferred Management IP
○ Use LoopBack Address
● Resolve by Name
○ Resolve by SysName
○ None

Add Discovered Devices to a Group
□ Add Discovered Devices to a Group
Group Name: Select

- Step 5 of 6 -

- Choose Use Loopback Address if loopback addresses are configured on the devices and you want those addresses to be the management IP address in CiscoWorks LMS.
- Choose Use Reverse DNS Lookup only if DNS is configured in your environment for network devices. Otherwise, deselect that option to speed up the discovery process.
- Choose Resolve by Sysname or Resolve by Name depending on the DNS configuration. If you have configured the management IP address of the device using any of the above settings, select the corresponding checkbox. Please refer to a document that discusses device discovery at https://supportforums.cisco.com/docs/DOC-9005.

Data Collection Settings

The data collection is configured to run every four hours starting at midnight. Run discovery manually once to determine an appropriate polling cycle. Four hours is enough for smaller networks, but larger networks can take long for the initial poll. The subsequent polls will be shorter in duration, but you should still give it a 20 percent buffer. For example, if it took four hours to poll the whole network the first time, you could set the frequency to five hours to make sure that there is no overlapping between the two consecutive data collection processes.

Select **Admin → Collection Settings → Data Collection**. See Figures 22, 23, and 24.

Figure 22. The Data Collection Settings

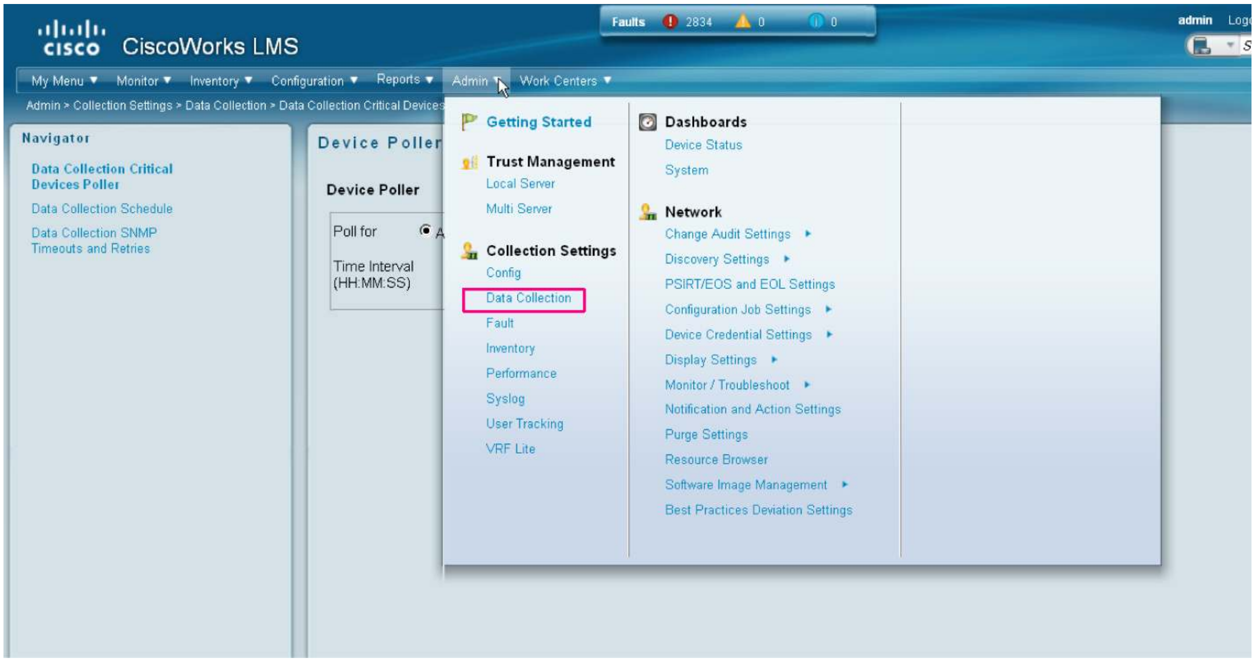
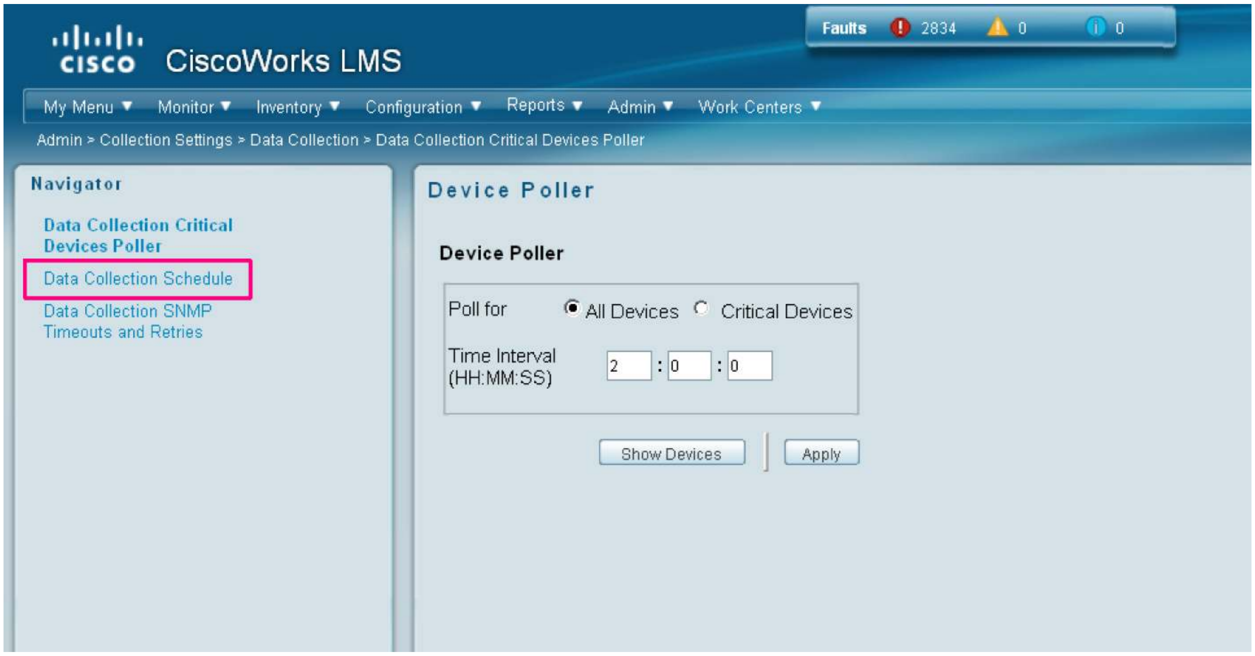


Figure 23. Setting the Device Poller

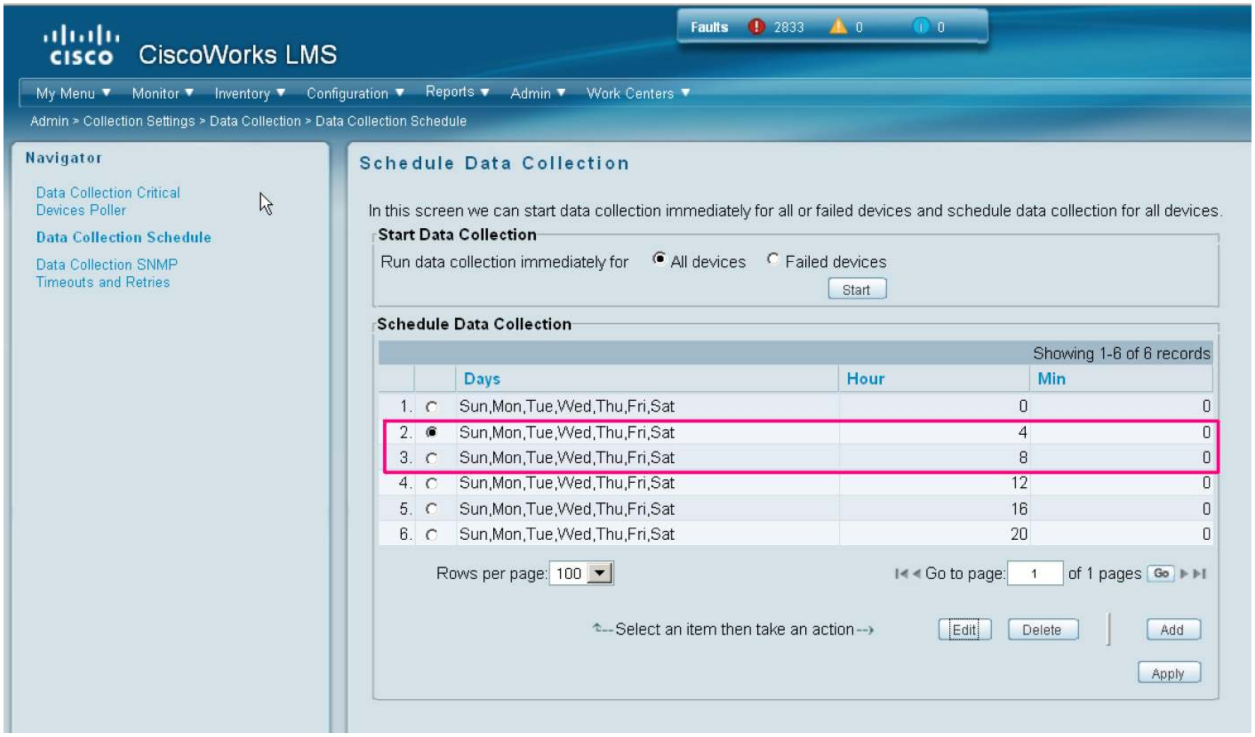

CiscoWorks LMS
Faults 2834 0 0
My Menu ▼ Monitor ▼ Inventory ▼ Configuration ▼ Reports ▼ Admin ▼ Work Centers ▼
Admin > Collection Settings > Data Collection > Data Collection Critical Devices Poller
Navigator
Data Collection Critical Devices Poller
Data Collection Schedule
Data Collection SNMP Timeouts and Retries
Device Poller
Show Devices
Apply

Device Poller

Poll for ● All Devices ○ Critical Devices

Time Interval (HH:MM:SS) 2 : 0 : 0

Figure 24. Scheduling Data Collection


cisco CiscoWorks LMS
Faults 2833 0 0
My Menu ▼ Monitor ▼ Inventory ▼ Configuration ▼ Reports ▼ Admin ▼ Work Centers ▼
Admin > Collection Settings > Data Collection > Data Collection Schedule
Navigator
Data Collection Critical Devices Poller
Data Collection Schedule
Data Collection SNMP Timeouts and Retries

Schedule Data Collection

In this screen we can start data collection immediately for all or failed devices and schedule data collection for all devices.

Start Data Collection

Run data collection immediately for ● All devices ○ Failed devices

Start

Schedule Data Collection

Showing 1-6 of 6 records

		Days	Hour	Min
1.	○	Sun,Mon,Tue,Wed,Thu,Fri,Sat	0	0
2.	●	Sun,Mon,Tue,Wed,Thu,Fri,Sat	4	0
3.	○	Sun,Mon,Tue,Wed,Thu,Fri,Sat	8	0
4.	○	Sun,Mon,Tue,Wed,Thu,Fri,Sat	12	0
5.	○	Sun,Mon,Tue,Wed,Thu,Fri,Sat	16	0
6.	○	Sun,Mon,Tue,Wed,Thu,Fri,Sat	20	0

Rows per page: 100 | Go to page: 1 of 1 pages Go

←--Select an item then take an action--> Edit Delete Add

Apply

Here make sure that the schedules are apart for more than 5 hours for larger networks.

User-Tracking Discovery

Configure the time so that two consecutive schedules do not overlap:

Admin → Collection Settings → User Tracking → Acquisition Schedule

Filter subnets for which you do not want to perform end-host discovery or subnets where no end hosts are present. Configure subnets that you want excluded from doing a ping sweep before the discovery process.

Admin → Collection Settings → User Tracking → Subnet Acquisition Configuration

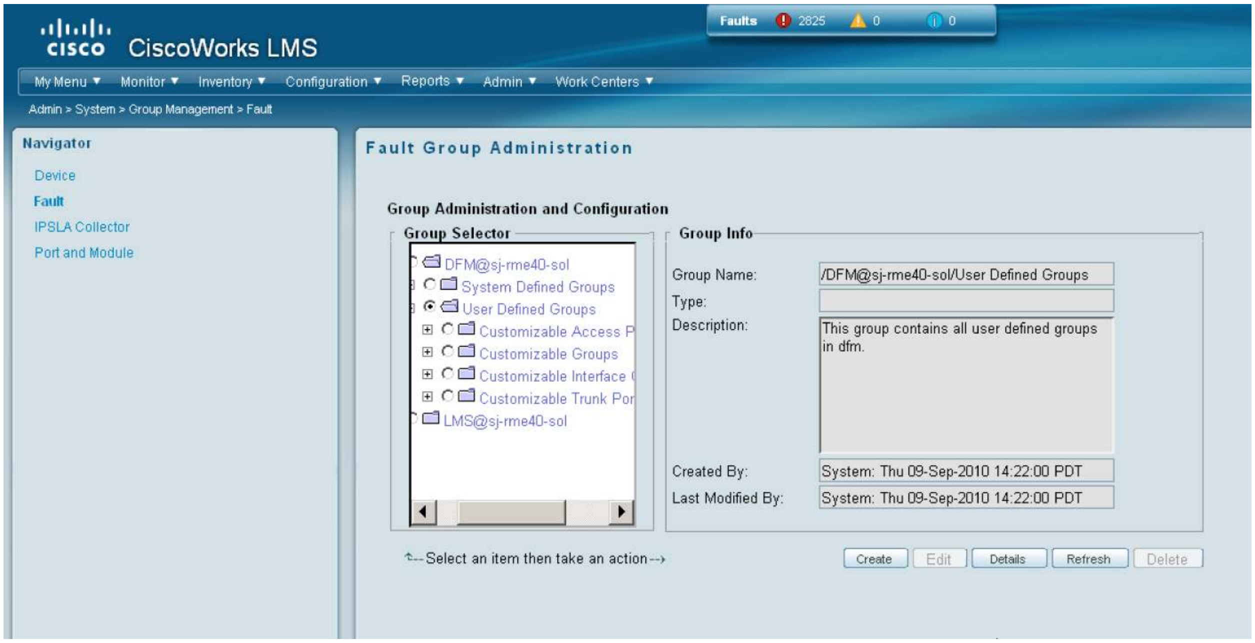
Fault Management Polling Parameters and Threshold

Default CiscoWorks fault management polling and threshold parameters are configured for CiscoWorks fault management system-defined groups; however, you need to look at these configurations based on critical and noncritical devices in your network.

To accomplish this:

- Start by adding devices to the customizable groups under **Admin → System → Group Management → Fault**. See Figure 25.

Figure 25. The CiscoWorks LMS Fault Group Administration Window



Group Name: /DFM@sj-rme40-sol/User Defined Groups

Type:

Description: This group contains all user defined groups in dfm.

Created By: System: Thu 09-Sep-2010 14:22:00 PDT

Last Modified By: System: Thu 09-Sep-2010 14:22:00 PDT

Follow the workflow to create a customized group.

- Set the priority of the customizable group. By default, customizable groups have a lower priority than system-defined groups. Change the priority based on group members (critical or noncritical).
- Change the polling parameters for the customizable device groups to larger or smaller values. You could even disable polling based on devices in that group.

Select **Monitor → Fault Settings → Setup → Polling Parameters**. See Figures 26 and 27.

Figure 26. The CiscoWorks LMS Polling Parameters Window

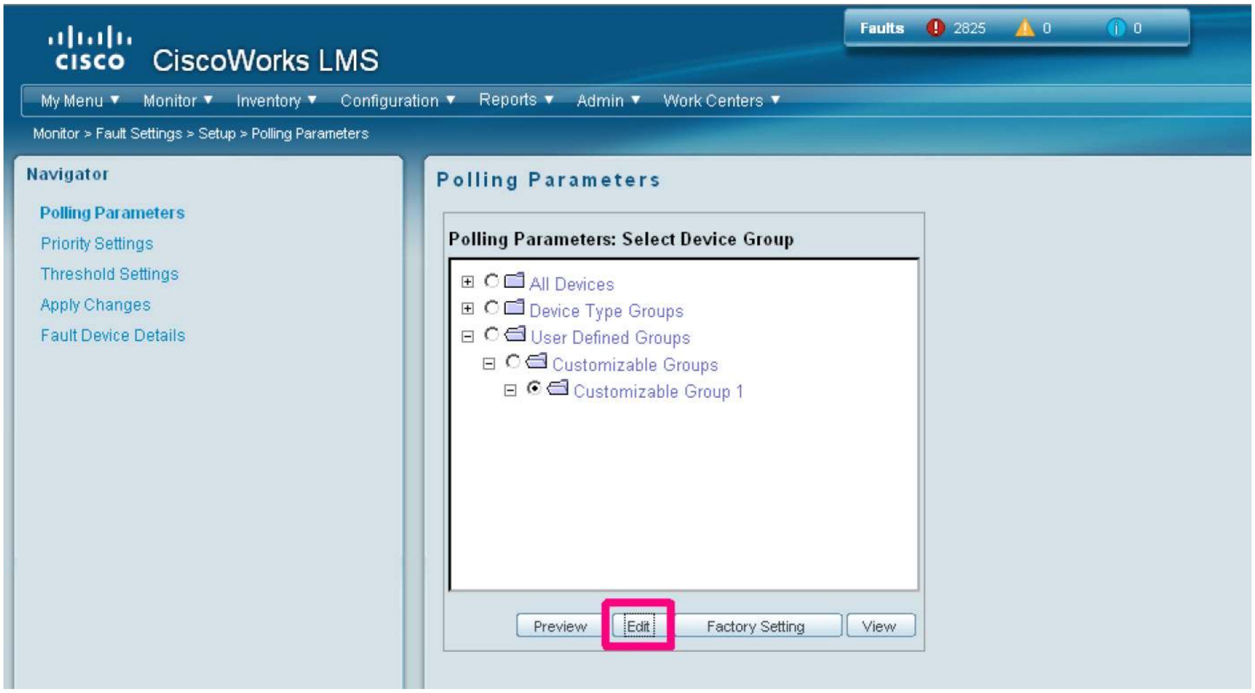
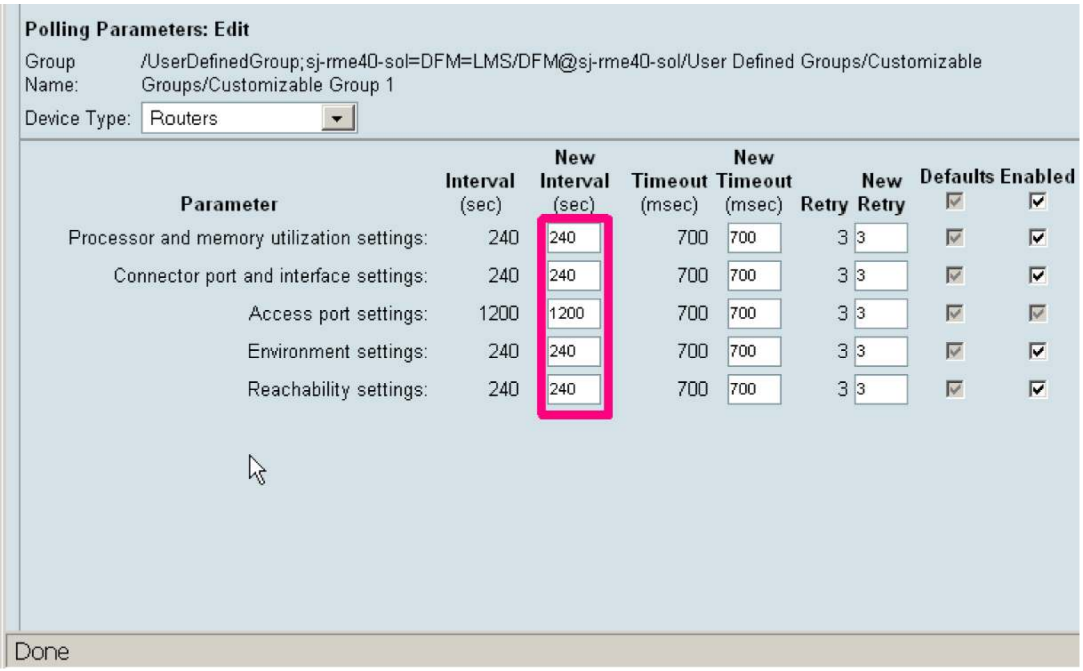


Figure 27. Changing the Polling Parameters



Polling Parameters: Edit

Group Name: /UserDefinedGroup;sj-rme40-sol=DFM=LMS/DFM@sj-rme40-sol/User Defined Groups/Customizable Groups/Customizable Group 1

Device Type: Routers

Parameter	Interval (sec)	New Interval (sec)	Timeout (msec)	New Timeout (msec)	Retry	New Retry	Defaults ☑	Enabled ☑
Processor and memory utilization settings:	240	240	700	700	3	3	☑	☑
Connector port and interface settings:	240	240	700	700	3	3	☑	☑
Access port settings:	1200	1200	700	700	3	3	☑	☑
Environment settings:	240	240	700	700	3	3	☑	☑
Reachability settings:	240	240	700	700	3	3	☑	☑

CiscoWorks Inventory, Configuration, and Image Management

During CiscoWorks installation, system jobs are created for inventory collection and polling, the default schedules being weekly and daily, respectively. In case of configuration archive management, system-level periodic configuration collection and polling are disabled by default.

In CiscoWorks LMS, you can create user-defined jobs for inventory polling and collection, and configuration collection and polling on a set of devices selected as part of the job creation process. You should consider this option when servers manage a large number of devices. In this case, data collection and job creation will be much easier if you have created well-defined common device groups.

Note: One problem with this approach is that when new devices get added to the system, you have to modify the jobs to add the new devices. This modification helps update the job to include the new device list.

Periodic Polling Versus Periodic Collection

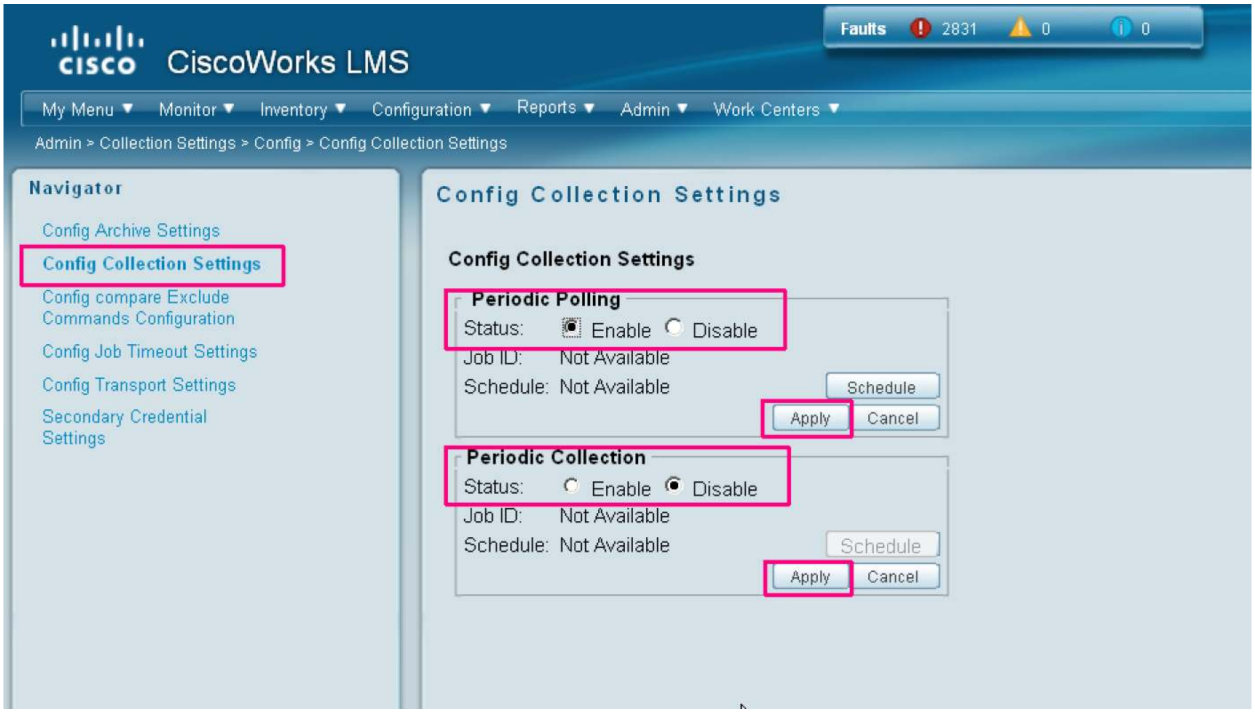
Periodic polling refers to a mechanism where LMS will poll a specific MIB variable within the device to determine if the configuration of that device has changed. If the configuration has changed, then and then only LMS will retrieve that device’s configuration file.

Periodic collection refers to a mechanism where the devices’ configurations will be retrieved on a periodic basic regardless of whether the configuration has changed.

Polling uses fewer resources than full scheduled collection because configuration files are retrieved only if the configuration MIB variable is set, so it is recommended that you chose enable the Period Polling option and disable the Periodic Collection option. It is shown in Figure 28.

Admin → Collection Settings → Config → Config Collection Settings

Figure 28. The CiscoWorks LMS Config Collection Settings Window


CiscoWorks LMS
Faults 2831 0 0
My Menu ▼ Monitor ▼ Inventory ▼ Configuration ▼ Reports ▼ Admin ▼ Work Centers ▼
Admin > Collection Settings > Config > Config Collection Settings
Navigator
Config Archive Settings
Config Collection Settings
Config compare Exclude Commands Configuration
Config Job Timeout Settings
Config Transport Settings
Secondary Credential Settings
Schedule
Apply
Cancel

Config Collection Settings

Config Collection Settings

Periodic Polling

Status: ● Enable ○ Disable

Job ID: Not Available

Schedule: Not Available

Periodic Collection

Status: ○ Enable ● Disable

Job ID: Not Available

Schedule: Not Available

Change the execution policy in default job policies for archive management and network configuration to parallel execution (choose **Admin → Collection Settings → Config → Config Transport Settings**). Remove protocols that are not used in your environment, and prioritize them.

General Observations

The UI performance of the application client can be improved by using device groups when executing application tasks, especially when a single server is managing a large number of devices.

When you configure systems to manage a large number of devices, consider the following:

Administrative Tips

- On the Windows platform, Terminal Server is supported only if Windows is configured for Remote Desktop Administration (Windows 2003 and 2008).
- CiscoWorks and system log files could grow to an unmanageable size over a period of time. It is very important to trim or rotate these files periodically. You could use the Logrot utility to manage these files. Following are some of the features of the Logrot utility:
    - Not limited to rotating only CiscoWorks log files but can be used to rotate any file
    - Can be run using the command **NMSROOT/bin/perl NMSRoot/bin/logrot.pl**
    - Can be configured and scheduled from GUI at **Admin → System → Log rotation**
    - Can rotate logs while CiscoWorks is running
    - Can optionally archive and compress rotated logs
    - Can be configured to rotate logs only when they have reached a certain size
    - Has a built-in configuration that makes adding new files very easy
    - Is typically run from UNIX cron or Windows AT
- Command-line interface (CLI) commands:

  - **cmexport** is the CiscoWorks user-tracking and topology services CLI for exporting user-tracking, Layer 2 topology, and discrepancy data details into XML format.
  - Remote invocation through servlet-based **cmexport** and **utexport** can also be used in CiscoWorks user-tracking and topology services, the former command for exporting Layer 2 topology details and discrepancy and the latter for user tracking.
  - **cwcli config** is the configuration command-line tool of the CiscoWorks configuration management feature. The **cwcli netconfig** command allows you to use NetConfig from the command line.
  - **cwcli export** is a command-line tool that provides servlet access to inventory, configuration, and change audit data. This can be used for generating inventory, configuration archive, and change audit data for devices in CiscoWorks configuration management feature.

Extracting Data from CiscoWorks LMS Servers for Centralized Reporting

CiscoWorks LMS supports export of data in XML format. If you have multiple instances of any of these applications, you could use this facility to develop consolidated reports.

From version 3.2, direct access to the LMS database is also supported, which offers users great flexibility in creating applications on their own. Initially only a limited set of table views is supported. More will be open in future releases.

CiscoWorks Configuration Management Data Extracting Engine

CiscoWorks Data Extracting Engine (DEE) is a utility that allows customers to extract data for devices managed by CiscoWorks Configuration Management from the inventory database, configuration archive, and change audit data. This tool supports the following features:

- Generating inventory data in XML format: The tool has servlet access and a command-line utility that can generate inventory data for devices managed by the CiscoWorks LMS server.
- Generating configuration data in XML format: The tool generates the latest configuration data from the configuration archive in XML format. Elements in the XML file are created at the configlet level in the current configuration archive.
- Generating change audit data in XML format: The tool uses the existing change audit log data and generates the change audit log data in XML format.

The Data Extracting Engine offers a great opportunity for customers to take advantage of the information stored in CiscoWorks LMS. The XML-based data along with web-based access to data allows CiscoWorks LMS users to:

  - Integrate their applications tightly with CiscoWorks LMS
  - Consolidate information from multiple CiscoWorks LMS servers in a single location
  - Maintain custom asset-management solutions

CiscoWorks User-Tracking and Topology Data Extracting Engine

CiscoWorks user-tracking and topology DEE is a utility that allows users to extract information available in CiscoWorks LMS for user-tracking and topology information. CiscoWorks user-tracking and topology DEE provides servlet access and a command-line utility to extract information on devices discovered by the CiscoWorks Asynchronous Network Interface (ANI) server. The information that can be extracted using the CiscoWorks user-tracking and topology DEE is:

- User-tracking data in XML format: DEE generates user-tracking data for devices discovered by CiscoWorks LMS.
- Layer 2 topology data in XML format: Generates the latest Layer 2 topology data including information on neighbor devices.

- Discrepancy data in XML format: CiscoWorks discrepancy APIs are used to retrieve the latest discrepancy report data from the CiscoWorks ANI ser6ver.

Open Database Schema Support in CiscoWorks LMS 4.0

CiscoWorks LMS uses a proprietary database based on Sybase. In versions prior to LMS 3.2, there was no support for direct database access. From LMS 3.2, database access is supported. Following is a list of exposed database views by applications:

- Common Services
  - Network_Devices
  - Job_Details
- User-Tracking and Topology Services
  - End_Hosts
- Fault Management
  - Fault_Alert_History
  - Fault_Event_History
  - Fault_Event_Details
- Configuration and Inventory Management
  - Device_Inventory
  - Module_Inventory
  - Port_Inventory
  - Processor_Inventory
  - Memory_Inventory
  - Device_Credentials_Status
  - Device_Inventory_Collection_Status
  - Device_Config_Archive_Status
  - Change_Audit_History
  - Syslog
  - IP SLA Performance Management

For how to set up Open Database Connectivity (ODBC) to the database and for details of the database schema, please refer to the document *Open Database Schema Support in LMS 4.0* included on the DVD.

Summary

This white paper provides an outline and recommendations for deploying CiscoWorks LMS server. It also tries to highlight some of the best practices related to the deployment of large-scale networks and makes the user aware of the scaling characteristics of CiscoWorks LMS. Your implementation may vary - watch system resource usage, and plan accordingly. Be aware of the means to maximize performance and usability that are already available in the tools.

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

C07-629879-00 01/11