Cisco UCS Management Pack User Guide, Release 3.0

For Microsoft System Center 2012, 2012 SP1 and 2012 R2, Operations Manager
August 2014

Cisco Systems, Inc.
www.cisco.com

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.

Text Part Number:

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco UCS Management Pack User Guide, Release 3.0

CONTENTS

Preface 1

- Audience 1
- Conventions 1
- Related Cisco UCS Documentation 3
- Documentation Feedback 3
- Obtaining Documentation and Submitting a Service Request 3

CHAPTER 1 Overview 1-1

- About the Cisco UCS Management Pack 1-1
- System Requirements 1-1
  - Management and Gateway Servers 1-2
  - Operations Manager Windows Agents 1-2
- Supported Cisco UCS Manager Releases 1-2

CHAPTER 2 Introduction 2-1

- One Monitor per UCS Domain Fault 2-1
- Knowledge Articles in Alerts 2-2
- Installing the Management Service outside the Resource Pool 2-2
- Event Based Discovery 2-2
- Real time UCS monitoring 2-2
- Dedicated Service Machine for UCS Domain Monitoring 2-2
- Additional Features 2-2

CHAPTER 3 Deployment Guide and Sizing Information 3-1

- Deployment Guide and Sizing Information 3-1
  - Deployment Scenarios on Trusted Boundary (Domain) 3-1
  - Deployment Scenarios on Untrusted Boundary (Domain) 3-3
- Check List to Install and Configure Cisco UCS Management Pack 3-5

CHAPTER 4 Installing the Cisco UCS Management Pack 4-1

- Installing the Cisco UCS Management Pack and Cisco UCS Management Service 4-1
- Silent Installation 4-2

Installing the Cisco UCS Management Service on Multiple Servers / Agent Managed Computers 4-3
Adding a Firewall Exception for the Cisco UCS Management Service 4-4
Upgrading the Management Pack to Release 3.0 4-4
Uninstalling the Cisco UCS Management Pack 4-4
Adding a Cisco UCS Domain to SCOM 4-5
Guidelines for adding a Cisco UCS Domain to SCOM 4-5

CHAPTER 5 Configuring Administrator Accounts 5-1
Creating a Run-As Account 5-1
Associating a Run As Account with a Profile 5-2

CHAPTER 6 Configuring Fault Acknowledgment 6-1
Creating a Resolution State 6-1
Creating a Channel 6-2
Creating a Subscriber and Subscription 6-2

CHAPTER 7 Customizing Cisco UCS Management Pack 7-1
Object Discoveries 7-1
Types of Object Discovery 7-1
Overriding Object Discoveries 7-3
Monitors 7-3
Severity Mapping 7-4
Overriding the Monitor 7-4
Migrating the Cisco UCS Domain to a Different Management Service 7-5

CHAPTER 8 Monitoring Cisco UCS Domains with SCOM 8-1
About the Monitoring Pane in SCOM 8-1
Accessing the Cisco UCS folder in the Monitoring Pane 8-1
About the Cisco UCS Folder 8-1
Cisco UCS Management Service Folder 8-2
Cisco UCS Instance Folder 8-3
Hardware Inventory Folder 8-6
Logical Inventory Folder 8-7
UCS HW/Logical Component Tasks 8-8
Alert Operations 8-9
8-9

CHAPTER 9 **Troubleshooting** 9-1

Error when Adding a Cisco UCS Domain to SCOM 9-1

Cisco UCS Monitoring Not Started 9-1

Cisco UCS Monitoring Stopped 9-2

Cisco UCS Management Service Log 9-2

Logging Levels 9-2

Changing the Logging Levels 9-2

Back Up Log Files 9-3

Purge Log Files 9-3

Generating Cisco UCS Technical Support File 9-3

Preface

This preface includes the following sections:

- Audience, page 1
- Conventions, page 1
- Related Cisco UCS Documentation, page 3
- Documentation Feedback, page 3
- Obtaining Documentation and Submitting a Service Request, page 3

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x l y l z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x l y l z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Warning **Statements using this symbol are provided for additional information and to comply with regulatory and customer requirements.**

Related Cisco UCS Documentation

Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

Other Documentation Resources

An ISO file containing all B and C-Series documents is available at the following URL: http://www.cisco.com/cisco/software/type.html?mdfid=283853163&flowid=25821. From this page, click **Unified Computing System (UCS) Documentation Roadmap Bundle**.

The ISO file is updated after every major documentation release.

Follow Cisco UCS Docs on Twitter to receive document update notifications.

For more information on UCS faults, visit this URL: http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ts/faults/reference/ErrMess/UCS_SEMs.html

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Overview

This chapter includes the following sections:

- About the Cisco UCS Management Pack, page 1-1
- System Requirements, page 1-1
- Supported Cisco UCS Manager Releases, page 1-2

About the Cisco UCS Management Pack

Microsoft System Center Operations Manager (SCOM) is a cross-platform data center management server for operating systems and hypervisors. SCOM utilizes a single interface that shows state, health, and performance information of computer systems. It also provides alerts generated according to availability, performance, configuration, or identified security risks.

A management pack is a definition file that contains predefined monitoring settings that enable an agent to monitor a specific service or application in Operations Manager. These predefined settings include discovery information that allows Operations Manager to automatically detect and begin monitoring services and applications. It also consists of a knowledge base that contains error and troubleshooting information, alerts, and reports to help you correct the problems detected in the environment.

The Cisco UCS Management Pack for Microsoft System Center Operations Manager provides visibility into the health, performance, and availability of a Cisco UCS domain through a single, familiar, and easy-to-use interface. The management pack contains rules which monitor, for example, chassis, blade servers, rack servers, and service profiles across multiple Cisco UCS domains.

System Requirements

The following system requirements are for Management Servers, Gateway Servers or Operations Manager Windows Agents (trusted or untrusted domain boundary) with Cisco UCS Management Service running on them:

- Management and Gateway Servers, page 1-2
- Operations Manager Windows Agents, page 1-2

Management and Gateway Servers

System requirement for Management Server and Gateway Server are as per the Microsoft recommendations mentioned in the following page:

http://technet.microsoft.com/en-us/library/hh205990.aspx

Operations Manager Windows Agents

System requirement for Windows agents (trusted or un-trusted domain boundary) running Cisco UCS Management Service is as follows:

Hardware

- Processor Architecture: 64-bit with Quad-core or higher
- Memory: 8 GB or higher

Operating System

UCS management service must be installed only on the Windows Agents running 64-bit versions of the following operating systems:

- Windows Server 2008 R2
- Windows Server 2008 R2 SP1
- Windows Server 2012
- Windows Server 2012 R2

Note All the above operating systems must be installed with the latest patch updates.

Software

The following software components must be installed before installing UCS management service on Windows agents:

- Windows PowerShell 2.0 or higher
- .NET Framework 4 or higher

Supported Cisco UCS Manager Releases

Cisco UCS Management Pack for Microsoft System Center Operations Manager is compatible with Cisco UCS Manager, Release 2.0 or later.

Introduction

The Cisco UCS Management Pack introduces several new features, which are listed here briefly. Subsequent chapters in this document elaborate these features further.

This chapter includes the following sections:

- One Monitor per UCS Domain Fault, page 2-1
- Knowledge Articles in Alerts, page 2-2
- Installing the Management Service outside the Resource Pool, page 2-2
- Event Based Discovery, page 2-2
- Real time UCS monitoring, page 2-2
- Dedicated Service Machine for UCS Domain Monitoring, page 2-2
- Additional Features, page 2-2

One Monitor per UCS Domain Fault

This Management Pack implements one monitor per UCS Domain fault. This provides improved power of customization at the fault level, user can override parameters like change the priority and severity or enable/disable monitors right from the Operations Manager console interface. Apart from the console interface, all these customizations can also be applied using much powerful Operations Manager cmdlets. Power Shell scripts could be developed to operate on multiple monitors at a time.

Note Monitors are not implemented for informational messages from UCS Domain. Informational messages will not be captured by the Management Pack in Operations Manager.

UCSM FSM faults are transient faults, therefore not supported by this version of Cisco UCS Management Pack. For a complete list of FSM faults in the UCS Domain not supported in the Management Pack, go to the following URL:

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ts/faults/reference/2-0/UCSFaultsErrorsRef_20/UCS_FSMs.html

Note All monitors corresponding to UCSM faults of type ‘Configuration’ are disabled by default.Only the monitors with severity as ‘Critical’ are enabled by default in the Management Pack. Users can customize rest of the monitors as per their environment/requirement.

Knowledge Articles in Alerts

Knowledge articles are available for all the monitors implemented in the Management Pack. Whenever there is an alert, you can check the knowledge article associated with the alert from the Alert Details section or Health Explorer. Knowledge articles provide a short description about the alert, and also a list of steps to resolve it.

Installing the Management Service outside the Resource Pool

This release of the Management Pack supports installing the Management Service outside the Resource Pool. Once the Management Pack is imported in the Resource Pool, user can choose to install the Management Service on the Agent Managed Computer (on trusted or untrusted boundaries) or Gateway Server.

Event Based Discovery

Event based discovery is a unique feature in this Management Pack, by which the object discoveries executes only when there is some change detected in the inventory of UCS Domain. Intelligence is built in the Cisco UCS Management Service to detect any change in inventory and raise appropriate events to trigger the Object discovery and pull the changes in Operations Manager.

Real time UCS monitoring

This Management Pack supports real time UCS monitoring, which means that any fault on the UCS Domain is captured in the Operations Manager within a few seconds.

Dedicated Service Machine for UCS Domain Monitoring

When you choose a service machine while adding a UCS Domain in the Add Monitoring Wizard, it means all the monitors, object discoveries, and rules required to monitor an UCS Domain execute on the Service Machine dedicatedly and do not use the resources on any other computer for monitoring this particular UCS Domain. The Management Servers however, will continue to analyze the return data from the Service Machine and store them in the database. A single Service Machine can also monitor multiple UCS Domains.

Note Service Machine chosen to monitor UCS Domain in Add Monitoring Wizard should have Cisco UCS Management Service installed and running on it.

Additional Features

Aside from the features listed above, the Cisco UCS Management Pack comprises the following additional features:

- A KVM Console can be launched on a Service Profile, Blade Server, or Rack Unit.
- Tech Support utility facilitates collecting logs for diagnosing an issue.
- Silent installation allows the administrator to run the installer from a script without prompting for user inputs.
- Run-As Account association in the Add Monitoring Wizard simplifies the overall process to start monitoring a UCS Domain.
- Supports more secure account distribution.

CHAPTER 3

Deployment Guide and Sizing Information

This chapter includes the following sections:

- Deployment Guide and Sizing Information, page 3-1
- Check List to Install and Configure Cisco UCS Management Pack, page 3-5

Deployment Guide and Sizing Information

Deployment Scenarios on Trusted Boundary (Domain)

Single Server Deployment of Operations Manager - Recommended Approach

The Management Group (MG1) has one management server - MS1

Step 1 Add an Agent Managed Computer - AM1.

Step 2 Run the Installer on MS1, choose custom install and import only the Management Pack on MS1.

Step 3 Run the installer on AM1 and install the Management Service only.

Step 4 While adding UCS Domain from Operations Manager Console choose AM1 as the Service Machine for monitoring UCS Domain.

Step 5 Enable monitors for faults as documented in the *Monitoring Cisco UCS Manager using Syslog* document available at the following URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/ucsm_syslog/b_Monitoring_Cisco_UCSM_Using_Syslog.pdf

Note The Agent Managed Computer's 'Health Service Private Bytes Threshold' and 'Monitoring Host Private Byte Threshold' are set to 400 MB each.

Sizing Information

The following table displays the sizing information for the above approach.

Agent Managed Computer	Hardware Specification	No. of Blades Monitored	No. of UCS Components Monitored
AM1	Quad-core CPU and 8GB RAM	80	~4500

Single Server Deployment of Operations Manager - Alternative Approach

Step 1 Run the Installer on MS1 and do a complete install, which imports the Management Pack and installs the Management Service on MS1.

Step 2 While adding UCS Domain from Operations Manager Console choose MS1 as the Service Machine for monitoring UCS Domain.

Sizing Information

The following table displays the sizing information for the above approach

Management Server	Hardware Specification	No. of Blades Monitored	No. of UCS Components Monitored
MS1	Quad-core CPU and 8GB RAM	160	~9000

Multiple Management Server Deployment of Operations Manager - Recommended Approach

The Management Group (MG1) has three management servers: MS1, MS2 and MS3

Step 1 Add an Agent Managed Computer: AM1.

Step 2 Repeat **Step 1** to add more Agent Managed Computers for monitoring the UCS Domain.

Step 3 Run the Installer on MS1/MS2/MS3, and choose **Custom Install** to import only the Management Pack.

Step 4 Run the installer on AM1 and install only the Management Service.

Step 5 Repeat **Step 4** for all the Agent Managed Computers added in **Step 2**.

Step 6 While adding the UCS Domain from the Operations Manager Console, choose AM1 as the Service Machine for monitoring UCS Domain.

Step 7 Enable monitors for faults as documented in the *Monitoring Cisco UCS Manager using Syslog* document available at the following URL:
http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/ucsm_syslog/b_Monitoring_Cisco_UCSM_Using_Syslog.pdf

Step 8 Alternatively, you could also select the Agent Managed Computer added in **Step 2** and **Step 5** as the Service Machine from the **Add Monitoring** Wizard.

Note The Agent Managed Computer's 'Health Service Private Bytes Threshold' and 'Monitoring Host Private Byte Threshold' are set to 400 MB each.

Multiple Management Server Deployment of Operations Manager - Alternative Approach

Step 1 Run the Installer on MS1/MS2/MS3 and do a complete install, which imports the Management Pack and installs the Management Service also.

Step 2 Chose other Management Servers where the Management Service should be installed. Run the installer and chose custom install and install the Management Service only.

Step 3 While adding UCS Domain from Operations Manager Console chose the Management Servers where installer was run in Step 1 or 2 as the Service Machine for monitoring UCS Domain

Sizing Information

The following table displays the sizing information for the above approach

Manageme nt Server	Hardware Specification	No. of Blades Monitored	No. of UCS Components Monitored
MS1	Quad-core CPU and 8GB RAM	160	~9000
MS2	Quad-core CPU and 8GB RAM	160	~9000
MS3	Quad-core CPU and 8GB RAM	160	~9000

Deployment Scenarios on Untrusted Boundary (Domain)

Distributed deployment of Operations Manager could have Gateway Servers which are installed on a different Domain un-trusted to the Management Group domain. These Gateway servers monitor the Agent Managed Computers locally and send the monitoring information to the connected Management Server.

The Management Group (MG1) has two management servers: MS1 and MS2. Gateway Server GW1 is connected to MS1. GW1 belongs to a different Active Directory Domain than MS1/MS2. Assuming there are multiple UCS Domain to be monitored, few UCS Domain(s) are on same network as MS1/MS2 and few other UCS Domain(s) belong to the same network as GW1.

Recommended Approach

Step 1 Add an Agent Managed Computer: AM1 to MS1/MS2.

Step 2 Add an Agent Managed Computer AM2 to GW1.

Step 3 Repeat **Step 1** and **Step 2** to add more Agent Managed Computers to monitor the Cisco UCS Domain.

Step 4 Run the Installer on MS1/MS2, choose custom install and import only the Management Pack.

Step 5 Run the installer on AM1 and install only the Cisco UCS Management Service.

Step 6 Run the installer on AM2 and install only the Cisco UCS Management Service.

Step 7 Repeat **Step 5** and **Step 6** for additional Agent Managed Computers added in **Step 3**.

Step 8 While adding Cisco UCS Domain from the Operations Manager Console choose AM1 as the Service Machine for monitoring the Cisco UCS Domain which belongs to the same network as MS1/MS2.

Step 9 While adding Cisco UCS Domain from Operations Manager Console choose AM2 as the Service Machine for monitoring Cisco UCS Domain which belongs to the same network as GW1.

Step 10 Enable monitors for faults as documented in the *Monitoring Cisco UCS Manager using Syslog* document available at the following URL:
http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/ucsm_syslog/b_Monitoring_Cisco_UCSM_Using_Syslog.pdf

Step 11 Alternatively Agent Managed Computer added in **Step 3** and **Step 7** could also be selected as Service Machine from Add Monitoring Wizard.

Sizing Information

The following table displays the sizing information for the above approach

Agent Managed Computer	Hardware Specification	No. of Blades Monitored	No. of UCS Components Monitored
AM1	Quad-core CPU and 8GB RAM	80	~4500
AM2	Quad-core CPU and 8GB RAM	80	~4500

Note The Agent Managed Computer's 'Health Service Private Bytes Threshold' and 'Monitoring Host Private Byte Threshold' are set to 400 MB each.

Alternative Approach

Step 1 Run the Installer on MS1/MS2 and do a complete install, which imports the Management Pack and installs the Management Service also.

Step 2 Run the installer on GW1 and select custom install and choose to install only the Cisco UCS Management Service.

Step 3 While adding UCS Domain from Operations Manager Console choose MS1/MS2 as the Service Machine (where the installer was run in **Step 1**) for monitoring UCS Domain which belongs to the same network as MS1/MS2.

Step 4 While adding UCS Domain from Operations Manager Console choose GW1 as the Service Machine for monitoring UCS Domain which belongs to the same network as GW1.

Note You can add Cisco UCS domains only from the SCOM Console application where Cisco UCS Management Pack installer was run to install the Management Pack or the Management Service, or both.

Manageme nt Server	Hardware Specification	No. of Blades Monitored	No. of UCS Components Monitored
GW1	Quad-core CPU and 8GB RAM	160	~9000
MS1	Quad-core CPU and 8GB RAM	160	~9000

Check List to Install and Configure Cisco UCS Management Pack

Serial No.	Title
1.	Ensure that logged in user has one of the following privileges on Management Server for executing installer • Domain Administrator • Domain user with local administrative privileges
2.	Ensure that logged in user has one of the following privileges on Management Server or Gateway Server or Agent Managed computers (trusted or untrusted boundaries) administrator privileges (local or domain) on gateway server or agent managed computer (trusted and untrusted boundaries). • Domain Administrator • Domain user with local administrative privileges
3.	Ensure that the computer used for installing Cisco UCS Management Pack and UCS Management Service is part of domain.
4.	Validate the Operating System of computer / server with one of the following a. Windows Server 2008 R2 b. Windows Server 2012 c. Windows Server 2012 R2

Serial No.	Title
5.	Validate the Operations Manager version with one of the following a.SCOM 2012 RTM (Updated with latest CUs) b.SCOM 2012 SP1 (Updated with latest CUs) c.SCOM 2012 R2 (Updated with latest CUs)
6.	Ensure that UCS Management Pack must be installed / imported on Management Server only through installer.
7.	Install Cisco UCS Management Service on following server(s) / computer(s) a.Agent Managed Computers (trusted boundary) - Recommended b.Management Server c.Agent Managed Computers (Untrusted boundary) - Recommended d.Gateway Server
8.	Ensure .Net framework 4.0 (minimum) is installed on server / computer used for Cisco UCS Management Service (Verified by installer also)
9.	Ensure PowerShell 2.0 (minimum) is installed on server / computer used for Cisco UCS Management Service (Verified by installer also)
10.	Ensure that the option “Allow this server to act as a proxy and discover managed objects on other computers” is enabled for following server / computer hosting Cisco UCS Management Service. a.Agent Managed Computers (trusted boundary) b.Management Server c.Agent Managed Computers (Untrusted boundary) d.Gateway Server
11.	Ensure that all server(s) / computer(s) hosting Cisco UCS Management Service are discovered in Operations Manager – Console – Administration – Device Management – (Agent Managed / Management Server).
12.	Ensure that all server(s) / computer(s) hosting Cisco UCS Management Service are visible in Operations Manager – Console – Monitoring – Cisco Unified Computing System – Cisco UCS Management Service – State View. If not visible, refer to point 12.
13.	Ensure that Operations Manager – Console – Authoring - Add Monitoring Wizard has been launched on server(s) / computers(s) hosting Cisco UCS Management Service for adding Cisco UCS domain or Management Server where management pack is imported.

Serial No.	Title
14.	If Cisco UCS domain is added on a Gateway Server or agent managed computer (untrusted boundary) is selected for service machine, ensure that Cisco UCS domain is reachable from Gateway Server or agent managed computer (untrusted boundary).
15.	Ensure that after adding Cisco UCS domain through Add Monitoring Wizard, appropriate Run As Account has been associated with correct Run As Profile.
16.	Ensure, if Run As Account distribution is set to More Secure, the computer hosting Cisco UCS Management Service must appear in Selected Computers list and it must be same as selected for monitoring Cisco UCS domain.
17.	Ensure that Operations Manager “Action Account” must have read and write privileges on TEMP (%SystemRoot%\Temp) folder.

CHAPTER 4

Installing the Cisco UCS Management Pack

This chapter includes the following sections:

- Installing the Cisco UCS Management Pack and Cisco UCS Management Service, page 4-1
- Installing the Cisco UCS Management Service on Multiple Servers / Agent Managed Computers, page 4-3
- Upgrading the Management Pack to Release 3.0, page 4-4
- Uninstalling the Cisco UCS Management Pack, page 4-4

Installing the Cisco UCS Management Pack and Cisco UCS Management Service

Prerequisites:

- The domain account with local administration rights should be used to install the Management Pack and/or the Management Service on Management Servers or Gateway Servers. This account should also be used to install the Management Service on the SCOM agent managed computers.
- You need to have .Net 4.0 installed on your computer

Step 1 Launch the Cisco UCS Management Pack Installer.

Step 2 In the **Setup Wizard** screen, click **Next**.

Step 3 In the **License Agreement** screen, do the following:

a. Review the End User License Agreement.

b. Click the **I accept the terms in the License Agreement** radio button.

c. Click **Next**.

Step 4 In the **Product Registration** screen, do the following:

a. In the **Username** field, enter your name.

b. In the **Organization** field, enter the name of your company.

c. Click the **Next** button.

The user name is required, but the organization name is optional.

Step 5 In the **Setup Type** screen, choose one of the following options and then click **Next**:

- **Custom**—To choose which components you want to install. Continue with Step 6 if you chose this option.
- **Complete**—To install all components of the Cisco UCS Management Pack. Continue with Step 7 if you chose this option.

Step 6 In the **Custom Setup Type** screen, check the check boxes for the components you want to install and then click **Next**:

- **Import Management Pack**—Imports the Cisco UCS Management Pack and related components into the management group. You can import the Cisco UCS management pack into any management server in the management group.

Note The Management Pack can be imported only on a SCOM Management Server.

- **Install Cisco UCS Management Service**—Installs the proxy agent that provides a bridge between SCOM and the Cisco UCS domain. This service maintains the Cisco UCS connections pool and provides Cisco UCS data to the management pack.

Note You can install the Cisco UCS Management Service only if you either choose to import the Management Pack also or the Management Pack is already imported in the Management Group.

Note The Cisco UCS Management Service can be installed on more than one SCOM Management Server, Gateway Server and Agent managed Computers.

Step 7 In the **Select Installation Folder** screen, accept the default installation folder or click **Browse** to navigate to a different folder, and then click **Next**.

Step 8 On the **Ready to Install** screen, click the **Install** button to start the installation.

After the Cisco UCS Management Pack is successfully installed, the **Installation Complete** screen is displayed.

Step 9 Click the **Finish** button to exit.

Silent Installation

Step 1 Run the command prompt with Administrative privilege.

Step 2 Navigate to the directory where the installer is present.

Step 3 Run the command **Cisco.Ucsm.MP.2012.v3.0.1-x64.msi /quiet**.

Note You must change the setup name according to your running release version, before executing the command.

Installing the Cisco UCS Management Service on Multiple Servers / Agent Managed Computers

You can install the Cisco UCS Management Service on more than one SCOM Management Server, Gateway Server, or Agent Managed Computers.

Note Each instance of the Cisco UCS Management Service manages the Cisco UCS domains assigned to it. There is no load balancing or high availability (HA) between instances of the Cisco UCS Management Service.

Note A domain account or local account with local administrative rights should be used to install the Management Service.

Prerequisite:

Import the Management Pack into the management group. The domain account with local administration rights should be used to install the Management Service.

Step 1 Launch the Cisco UCS Management Pack Installer.

Step 2 In the **Setup Wizard** screen, click **Next**.

Step 3 In the **License Agreement** screen, do the following:

a. Review the End User License Agreement.

b. Click the **I accept the terms in the License Agreement** radio button.

c. Click **Next**.

Step 4 In the **Product Registration** screen, do the following:

a. In the **Username** field, enter your name.

b. In the **Organization** field, enter the name of your company.

c. Click the **Next** button.

The user name is required, but the organization name is optional.

Step 5 In the **Setup Type** screen, choose **Custom** and then click **Next**:

Step 6 In the **Features to Install** screen, check the check boxes for the components you want to install and then click **Next**:

- **Install Cisco UCS Management Service**—Installs the proxy agent that provides a bridge between SCOM and Cisco UCS. This service maintains the Cisco UCS connections pool and provides Cisco UCS data to the management pack.
- Add a desktop shortcut for the Cisco UCS Management Service Configuration GUI.

Note The option to import the Cisco UCS Management Pack is disabled if you have already imported the management pack.

Step 7 In the **Select Installation Folder** screen, accept the default installation folder or click **Browse** to navigate to a different folder, and then click **Next**.

Step 8 On the **Ready to Install** screen, click the **Install** button to start the installation.

After the Cisco UCS Management Service is successfully installed, the **Installation Complete** screen is displayed.

Step 9 Click the **Finish** button to exit.

Adding a Firewall Exception for the Cisco UCS Management Service

Before you start monitoring your Cisco UCS domain, enable the following inbound rules in the Windows Firewall with Advanced Security on the computer where you run the Cisco UCS Management Service:

- File and Printer Sharing:
  - Echo-Request—ICMPv4-In
  - Echo-Request—ICMPv6-In
- Remote Service Management (RPC)
- Remote Service Management (RPC-EPMAP)

Upgrading the Management Pack to Release 3.0

The Cisco UCS Management Pack, Release 3.0 does not support direct upgrade from the Cisco UCS Management Pack, Release 2.6.2. You need to uninstall any previous release of the Management Pack.

Step 1 Uninstall the Cisco UCS Management Pack, Release 2.6.2 or earlier.

For more information on how to uninstall the Cisco UCS Management Pack, Release 2.6.2, see the Cisco UCS Management Pack User Guide at the following URL: http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/msft_tools/scom/scom_2-6/scom_2-6_user_guide/scom_2_6_userguide.pdf

Step 2 Install the Cisco UCS Management Pack, Release 3.0.

Uninstalling the Cisco UCS Management Pack

To uninstall the Cisco UCS Management Pack, complete the following steps.

Step 1 In the SCOM application, click the **Go** tab in the menu bar.

Step 2 Select **Administration** from the drop-down menu.

Step 3 In the **Administration** column, click **Management Packs**.

A list of management packs appears on the right panel.

Step 4 Choose **Cisco UCSM Management Pack 2012** and choose **Properties**.

Step 5 Click on the **Dependencies** tab.

Step 6 Make a list of all the entries under **Management Packs that depend on this Management Pack**.

Step 7 Click **Cancel**. The SCOM Operations Manager screen appears. Choose the management pack and click **Delete** to delete all the dependent management packs individually.

Step 8 Open Control Panel. Select **Program and Features.**

Step 9 Remove **Cisco UCS Management Pack (v3.0)**.

Note **Step 8** through **Step 9** should be performed on all the Management Servers and Gateway Servers and Agent Managed Computers where the Management Service was installed.

Alternatively, you could complete the following steps to remove the Cisco UCS Management Service:

Step 1 Run the installer a second time.

Step 2 Click **Next**. The Maintenance screen appears.

Step 3 Click **Remove**.

Ready to Remove screen appears.

Step 4 Click **Remove** to completely remove the Cisco UCS Management Service.

Note The installer tries to remove the management pack from the management group, even if only service is installed on that machine. In case you were unable to remove the management pack, the installer continues to uninstall the components, but you need to manually remove the management pack from the SCOM Console.

Adding a Cisco UCS Domain to SCOM

Guidelines for adding a Cisco UCS Domain to SCOM

You can only add Cisco UCS domains on servers (trusted domain) where either management pack is imported or the Cisco UCS Management Service is installed. We recommend that you follow the guidelines below when you configure SCOM to monitor Cisco UCS domains through the Add Monitoring wizard.

Complete the following steps to add a Cisco UCS domain to SCOM.

Step 1 In the SCOM application, click the **Go** tab in the menu bar.

Step 2 From the drop-down menu, choose **Authoring**.

Step 3 In the **Authoring** column, choose **Cisco Unified Computing Systems**.

Step 4 In the **Tasks** panel, click the **Add Monitoring** wizard.

Step 5 On the **Select Monitoring Type** page of the **Add Monitoring** wizard, choose Cisco Unified Computing Systems from the **Select the Monitoring Type** list and click **Next**.

Step 6 On the **General Information** page of the **Add Monitoring** wizard, do the following:

a. In the **IP Address/Hostname** field, enter the IP address or hostname of the Cisco UCS domain.

This is the virtual IP address that you use to access the Cisco UCS Manager in that domain.

b. In the Port Number field, enter the port number that is used to connect to the Cisco UCS domain.

This is the port number specified in the HTTP or HTTPS configuration for the Cisco UCS domain.

c. In the **Connection Mode** check box, do one of the following:

- Check the check box for secure (HTTPS) connections.
- Uncheck the check box for non-secure (HTTP) connections using default port 80.

d. Choose the Machine Type (Management Server, Gateway Server, or an Agent Managed Computer) and Service Machine where the Management Service is running.

e. Click **Test Connection** to verify that SCOM can connect to the Cisco UCS domain.

If you receive an error after you click **Test Connection**, contact your Network Administrator.

For secure connections, if there is an issue with the server certificate and a security alert dialog box is displayed, review the warnings and follow the instructions in the dialog box.

f. In the **Authentication** dialog box, enter the **Username** and **Password** and click **OK**.

If the Cisco UCS domain is configured for domain authentication, you must enter the user name in the following format: <*username@domainname*>.

g. If the connection is successful and a message box is displayed, click **OK**.

Note The dialog box validates the state of Management Service if the Management Server or Agent Managed Computer (trusted boundary) within the same active directory as the operations console machine is chosen. You can additionally start the Management Service if it stops. If you are a console user trying to add the UCS Domain, you should have Local Administration rights on the Management Server or Agent Managed Computer. This is required to find out the state of the Management Service and remotely start the Management Service.

Note When you choose a Gateway Server or Agent Managed Computer (un-trusted boundary) you have the option to proceed even when the test connection to UCS Domain fails due to connectivity problem. You need to make sure that the Cisco UCS management service is running on the Gateway Server or Agent Managed Computer (untrusted boundary).

h. Click **Next**.

Step 7 On the **Instance Name** page of the **Add Monitoring** wizard, do the following:

a. In the **Name** field, accept the default Cisco UCS domain name that was added to the field.

We recommend that you do not change the default Cisco UCS domain name.

b. In the **Description** field, enter a description of the Cisco UCS domain.

c. In the **Management Pack** section, continue with the default settings. Or check the **create new** check box to save the current Cisco UCS domain in a different Management Pack and then do one of the following:

- From the drop-down list, choose the existing management pack.

Note We recommend that you use the existing management pack with its predefined timers and configuration. The Default Management Pack is the first management pack that is displayed in the list when creating an override. Do not save anything new to the default management pack.

- Click **New** to create and define a new management pack for this Cisco UCS domain.

d. Click **Next**.

Step 8 The **Run As Account Summary** screen appears.

Step 9 Check the **Associate Run-As Account** check box to associate a run-as account to the UCS Domain.

Step 10 Click **Add**.

Step 11 Choose an existing account from the drop down or click **New** to add a new run-as account for this UCS Domain.

Note The new account you created from this dialog box has the distribution policy set to a less secure account. You can configure this to a more secure distribution policy subsequently.

Step 12 Click **Next**.

Step 13 On the **Configuration Summary** page, review the summary and click **Create**.

The template for monitoring the Cisco UCS domain is created.

Note To enable monitoring of Cisco UCS, you must associate Run As Profile, which is created by this management pack, with the Run As account.

If a **Run-As** account is not associated in **Step 9**, you can manually create the account and associate it to a profile from the SCOM Console application.

Note The **Add Monitoring** Wizard is available on systems where either the Management Pack or Management Service is installed using the installer.

CHAPTER 5

Configuring Administrator Accounts

This chapter includes the following sections:

- Creating a Run-As Account, page 5-1
- Associating a Run As Account with a Profile, page 5-2

Creating a Run-As Account

Note Create a Run As account only if you did not associate a Run As account to a profile in the **Adding a Cisco UCS Domain to SCOM** section.

SCOM uses Run As accounts to establish a connection to a Cisco UCS domain.

Step 1 In the SCOM application, click the **Go** tab in the menu bar.

Step 2 Select **Administration** from the drop-down menu.

Step 3 In the **Administration** column, click **Accounts under Run As Configuration**. In the **Tasks** column**,** click **Create Run As Account**.

Step 4 On the **Introduction** page of the **Create Run as Account wizard**, click **Next**.

Step 5 On the **General Properties** page of the **Create Run As Account wizard**, do the following:

a. From the **Run as Account Type** drop-down menu, choose **Simple Authentication**.

b. In the **Display Name** field, enter a name for the Run As account.

c. In the **Description** field, enter a description of the account.

d. Click **Next**.

Step 6 In the **Credentials** page of the **Create Run As Account wizard**, enter the **Account Name**, **Password**, and **confirm Password**.

Note If the Cisco UCS domain is configured for domain authentication, you must enter the user name in the following format: <*username@domainname*>. These credentials are used for all communication with the Cisco UCS domain.

Step 7 Click **Next**.

Step 8 In the **Distribution Security** page of the **Create Run As Account wizard**, do the following:

a. In the **Select a Distribution Security Option** field, click the **More Secure** radio button.

b. Click **Create**.

Step 9 On the **Completion** page of the **Create Run As Account wizard**, click **Close**.

The Administrator Run As account is created.

Step 10 Distribute the Run-As account to the Service Machine and do the following:

a. Open the **Properties** pane of the newly created account and go to the **Distribution** tab of the **Run As Account Properties** dialog box. Click **Add**.

b. In the **Computer Search** window, select **Search by computer name** (default) and click **Search**.

c. A list of root management server, management server(s) and Operations Manager agent managed windows computers is displayed.

d. Select the windows computer which is same as the Service Machine you selected in **Step 6** ‘h’ in the **Adding a Cisco UCS Domain to SCOM** section.

Associating a Run As Account with a Profile

Step 1 In the SCOM application, click the **Go** tab in the menu bar.

Step 2 Select **Administration** from the drop-down menu.

Step 3 In the Administration column, click **Profiles**.

Step 4 From the list of a profiles, right-click on the profile that you want to associate with the Run As account and choose **Properties**.

Step 5 On the **Introduction** page of the **Run As Profile** wizard, click **Run As Accounts** in the **Navigation** pane.

Step 6 On the **Run As Accounts** page of the **Run As Profile** wizard, click **Add**.

Step 7 In the **Run As Account** dialog box, do the following:

a. From the **Run As Account** drop-down list, choose the Run As account you want to associate with the profile.

b. In the **This Run As Account will be Used to Manage the Following Objects** field, click one of the following radio buttons:

- All Targeted Objects—Choose this option if you are monitoring a Cisco UCS domain for the first time.
- A Selected Class, Group, or Object—Choose this option if you have monitored a Cisco UCS domain before and already know which objects interest you.

c. Click **OK**.

Step 8 On the **Run As Accounts** page of the **Run As Profile** wizard, click **Save**.

Step 9 On the **Completion** page of the **Run As Profile** wizard, click **Close**.

CHAPTER 6

Configuring Fault Acknowledgment

You can use the operations console to acknowledge faults in a Cisco UCS domain. This configuration helps to communicate with Cisco UCS for acknowledging alerts from the Operations Manager Console. You can configure this from any management server in the same management group.

This chapter includes the following sections:

- Creating a Resolution State, page 6-1
- Creating a Channel, page 6-2
- Creating a Subscriber and Subscription, page 6-2

Creating a Resolution State

A resolution state can be assigned to and is visible on all faults. However, you can only acknowledge Cisco UCS faults.

Step 1 In the SCOM application, click the **Go** tab in the menu bar.

Step 2 Choose **Administration** from the drop-down menu.

Step 3 Click the **Settings** node.

Step 4 In the right panel, double-click **Alerts**.

Step 5 On the **Alert Resolution States** tab, click **New**.

Step 6 In the **Add Alert Resolution** dialog box, do the following:

a. In the **Resolution State** field, enter a name for the resolution state.

We recommend that you use a name that enables you to easily recognize the resolution state, such as UCS Acknowledged.

b. From the **Unique ID** drop-down menu, choose an ID for the resolution state.

The resolution state ID can be any available value between 1 and 254. The ID of 0 is reserved for the New state, and the ID of 255 is reserved for the Closed state.

c. Click **OK**.

Creating a Channel

Step 1 In the SCOM application, click the **Go** tab in the menu bar.

Step 2 Choose **Administration** from the drop-down menu.

Step 3 Right-click the **Channels** node and choose **New Channel > Command**.

Step 4 On the **Description** page of the **Command Notification Channel** wizard, do the following:

a. In the **Channel Name** field, enter a name for the channel.

b. In the **Description** field, enter a description of the channel.

c. Click **Next**.

Step 5 On the **Settings** page of the **Command Notification Channel** wizard, do the following:

a. In the Full Path of the Command File field, enter the path to the command file.

For example, enter the following path:

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
```

b. In the **Command Line Parameters** field, enter the command line parameters for the channel.

-Command "& 'C:\ProgramData\Cisco\UCSM\Script\AcknowledgeFault.ps1'" -getDescription '$Data[Default='Not Present']/Context/DataItem/AlertDescription$' -getAlertSource '$Data[Default='Not Present']/Context/DataItem/ManagedEntityPath$\$Data[Default='Not Present']/Context/DataItem/ManagedEntityDisplayName$'

Note The Command line parameters must be configured correctly for acknowledging the UCS faults from SCOM.

c. In the **Startup Folder for the Command Line** field, enter the startup folder name.

C:\ProgramData\Cisco\UCSM\Script

Note Verify the path and location of the script first.

Step 6 Click **Finish**.

Ensure that the script AcknowledgeFault.ps1 exists at the path specified in **Step 5** on each and every Management Server or SCOM Agent Machine hosting Cisco UCS Management Service.

Creating a Subscriber and Subscription

Step 1 In the SCOM application, click the **Go** tab in the menu bar.

Step 2 Choose **Administration** from the drop-down menu.

Step 3 Expand the **Notifications** node.

Step 4 Right-click **Subscriptions** and choose **New Subscription**.

Step 5 On the **Description** page of the **Notification Subscription** wizard, do the following:

a. In the **Subscription Name** field, enter a name for the subscription.

b. In the **Description** field, enter a description of the channel.

c. Click **Next**.

Step 6 On the **Criteria** page of the **Notification Subscription** wizard, do the following:

a. In the **Conditions** pane, check the **With Specific Resolution State** check box.

b. In the **Criteria Description** pane, click the **Specific** link.

c. In the **Resolution State** wizard, check the **UCS Acknowledge** check box in the **Resolution States to Search For** pane, and click **OK**.

d. Click **Next**.

Step 7 On the **Subscribers** page of the **Notification Subscription** wizard, click **New** to create a new subscriber.

Step 8 On the **Description** page of the **Notification Subscribers** wizard, do the following:

a. In the **Subscriber Name** field, enter the SCOM 2012 Administrator Action account as the subscriber.

b. In the **Description** field, enter a description of the subscriber.

c. Click **Next**.

Step 9 On the **Schedule** page of the **Notification Subscribers** wizard, do the following:

a. Click one of the following radio buttons to choose the notification schedule you want to use:

- **Always Send Notifications**—Sends notifications at all times on all days.
- **Notify Only During the Specified Times**—Enables you to specify the days and times during which you want SCOM to send notifications.

b. Click **Next**.

Step 10 On the **Addresses** page of the **Notification Subscribers** wizard, click **Add** to add an address where you want to have notifications sent.

Step 11 On the **General** page of the **Subscriber Address** wizard, do the following:

a. In the **Address Name** field, enter a name that you can use to identify the notification address.

b. Click **Next**.

Step 12 On the **Channel** page of the **Subscriber Address** wizard, do the following:

a. From the **Channel Type** drop-down list, choose **Command**.

a. From the **Command Channel** drop-down list, choose **Ack Channel**.

b. Click **Next**.

Step 13 On the **Schedule** page of the **Subscriber Address** wizard, do the following:

a. Click the **Always Send Notifications** radio button.

b. Click **Finish**.

The subscriber address is created and displayed in the **Subscriber Address** pane of the **Addresses** page of the **Notification Subscribers** wizard.

Step 14 On the success notification page of the **Notification Subscribers** wizard, click **Close**.

The subscriber address is displayed in the **Selected Subscribers** pane of the **Addresses** page of the **Notification Subscribers** wizard.

Step 15 On the **Subscribers** page of the **Notification Subscription** wizard, click **Next**.

Step 16 On the **Channels** page of the **Notification Subscription** wizard, click **Add** to add the channel that you have just created.

Step 17 In the **Channel Search** dialog box, do the following:

a. Click the channel you just created in the **Available Channels** pane.

If that channel is not visible in the **Available Channels** pane, you can search for it in the **Filter By** field.

b. Click **Add** to add the channel to the **Selected Channels** pane.

c. Click **OK**.

Step 18 On the **Channels** page of the **Notification Subscription** wizard, do the following:

a. In the Alert Aging field, click the **Send Notifications Without Delay** radio button.

b. Click **Next**.

Step 19 On the **Summary** page of the **Notification Subscription** wizard, do the following:

a. Review the details of your subscription in the **Confirm Notification Subscription Settings** pane.

b. If all the details are correct, check the **Enable This Notification Subscription** check box.

If one or more of the details are incorrect, click **Previous** and correct the misconfiguration.

c. Click **Finish**.

Step 20 On the success notification page of the **Notification Subscription** wizard, click **Close**.

Customizing Cisco UCS Management Pack

For each UCS Domain added for monitoring in Operations Manager, a Management Pack Template is created under the **Management Pack Templates** tab in the Cisco Unified Computing System. It is very crucial to understand the components of the Management Pack to perform any customization.

This chapter includes the following sections:

- Object Discoveries, page 7-1
- Monitors, page 7-3
- Severity Mapping, page 7-4
- Overriding the Monitor, page 7-4
- Migrating the Cisco UCS Domain to a Different Management Service, page 7-5

Object Discoveries

Every component of the Cisco UCS domain comprises an object discovery that the management pack monitors. To view the list of object discoveries in the pack, complete the following steps:

Step 1 In the SCOM application, click the **Go** tab in the menu bar.

Step 2 Choose **Authoring** from the drop-down menu.

Step 3 In the **Authoring** column, choose **Authoring** > **Management Pack templates** > **Cisco Unified Computing System**.

Step 4 Choose the template pack. Right click and choose **View Management Pack Objects** > **Object Discoveries**.

Note Several discoveries are disabled by default. Override the discoveries to enable them or change other parameters.

Types of Object Discovery

Object discoveries are of two types:

- Interval based
- Event Based

Interval Based Object Discovery

Interval based discoveries execute at a defined interval to fetch the information from the Management Service.

Interval based discovery occurs at only two levels: Cisco UCS Instance Discovery and Organization Discovery.

Cisco UCS Instance (Object Discovery)

This is the top level Object Discovery and the first discovery to run for an UCS Domain. It discovers an instance of Cisco UCS Domain into Operations Manager. This discovery runs to fetch the inventory and monitoring information from Cisco UCS Domain using the Cisco UCS Management Service.

Following are the set of Overrides available for this Object Discovery:

- CacheClass: Defines the managed object for an inventory or monitoring information to be collected from the UCS Domain.
- Discovery Level: Defines the level up to which Organizations and Service Profiles from the UCS Domain should be discovered in the Operations Manager.
- Enabled: Defines the enabled state of the object discovery.
- Interval Seconds: Defines the interval of execution.
- IsAssociated: Defines whether or not the associated or unassociated Service Profiles should be discovered in SCOM. The default value is 'True' which means only an associated service profile must be discovered in the Operations Manager.
- Logging Level: Defines if the logging is enabled or disabled for this object discovery.
- Timeout Seconds: Defines the timeout period for the discovery script to execute.

Note By default the Cisco UCS Instance discovery is programmed to execute every two hours (7200 seconds) to fetch any modifications from the Cisco UCS Domain.

Organization Discovery

Organization Discovery enables discovery of logical components in the UCS Domain. Following are the set of overrides available for object discovery:

- Enabled: Defines the enabled state of the object discovery.
- Interval Seconds: Defines the interval of execution.
- Timeout Seconds: Defines the timeout period for the discovery script to execute.

Event Based Discovery

The Cisco UCS Instance Discovery script executes at a default scheduled interval of 7200 seconds and detects the modification in the UCS Domain inventory. Any modification in UCS components triggers a windows event. This event triggers the Cisco UCS management pack to execute the discovery of modified UCS components.

Event based discovery occurs only when there is any modification in UCS components.

Following are the overrides available for an Event based Object Discovery.

- Enable Logging – Enables event logging for the discovery.
- Enabled – Enables or disables the Object Discovery.

- Timeout Seconds – Defines the timeout period for the discovery script to execute.

Overriding Object Discoveries

Complete the following steps to override the object discoveries:

Step 1 On the **Object Discovery** page, choose the object and right-click **Override**.

Step 2 Choose **Override** > **Override the Object Discovery** > **For All Objects of Class**.

Step 3 In the Override Properties page, do the following:

a. Check the **Override** checkbox.

b. Modify the override value.

c. Click **Apply/Ok**.

Note When an object discovery is enabled using override, make sure all its target class discoveries till the top level (Cisco UCS Instance) are also enabled. If not, enable them. When an object discovery is disabled using override, all the class discoveries targeted at this class till the leaf level are also not monitored by the Operations Manager

Note If you enabled an object discovery from the Disabled state, for all such object discoveries, discovery events should be generated using the Generate Discovery Event task from Cisco UCS Instance Tasks. This is used to retrieve old updates from the Management Service when the discovery was turned off.

Monitors

The Cisco UCS management pack has monitors for each UCS fault, and each monitor is event based two-state monitor. Depending on the number of UCS components on which a fault can occur, there could be multiple monitors per UCS fault.

For example, Fault F0174 can occur on the following UCS components:

```
sys/chassis-[id]/blade-[slotId]/board/cpu-[id]
sys/rack-unit-[id]/board/cpu-[id]
```

Therefore there would be two monitors in the management pack corresponding to these 2 UCS components, and the naming convention is as follows:

- F0174 sys_chassis_id_blade_slotId_board_cpu_id Monitor
- F0174 sys_rack_unit_id_board_cpu_id Monitor

Note Currently, the Cisco UCS management pack does not support display of informational, clear faults from the Cisco UCS Domain in Operations Manager.

Note UCSM FSM faults are transient faults and therefore are not supported by this version of management pack. For a complete list of FSM faults not supported in the Management Pack, go to the following URL: http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ts/faults/reference/2-0/UCSFaultsErrorsRef_20/UCS_FSMs.html

All monitors of corresponding UCSM faults of type Configuration are disabled by default

Severity Mapping

This section describes the mapping between the severity of faults in the UCS Domain and the alert severity monitors in Operations Manager.

The following table shows the mapping of severity levels between the Cisco UCS Manager and Monitors.

Table 7-1 Default Severity Mapping

Severity Level	Cisco UCSM (Severity)	Monitors (Alert Severity)
1	Critical, Major	Critical
2	Minor, Warning	Warning

Note Only monitors with alert severity as Critical are enabled by default. Therefore, only Critical and Major faults from the UCS Domain are shown as Alerts (Critical) in Operations Manager.

Complete the following steps to view the list of Monitors in the Management Pack:

Step 1 In the SCOM application, click the **Go** tab on the menu bar.

Step 2 Choose **Authoring** from the drop-down menu.

Step 3 In the Authoring column, choose **Authoring** > **Management Pack templates** > **Cisco Unified Computing System**.

Step 4 Choose the template pack and right-click to choose **View Management Pack Objects** > **Monitors**.

Overriding the Monitor

Complete the following steps to override the Monitors:

Step 1 On the **Monitors** page, choose a target and expand it.

Step 2 Go to Entity **Health** > **Availability**. A list of monitors corresponding to the target is displayed. Alternatively search the monitor by fault code, and right-click to choose **Monitor**.

Step 3 Choose **Override** > **Override the Monitor** > **For All Objects of Class**.

Step 4 On the **Override Properties** page, do the following:

a. Check the Override checkbox.

b. Modify the Override value.

The following parameters are available to override Monitors:

- Alert On State
- Alert Priority: Defines the priority of the alert generated by this monitor.
- Alert Severity: Defines the severity of the alert generated by this monitor.
- Auto-Resolve Alert: Defines whether or not to auto-resolve the alert generated by this monitor.
- Enabled: Defines the enabled state of the monitor.
- Generate Alert: Defines where or not the monitor should generate an alert.

Note When a Monitor is enabled using override, make sure all its target class discoveries till the top level (Cisco UCS Instance) are also enabled.

Migrating the Cisco UCS Domain to a Different Management Service

In a deployment where multiple SCOM Management Servers and Agent Managed Computers are present, Cisco UCS Management Service could be installed on more than one computer to monitor multiple UCS Domains. This helps in sharing the load of monitoring multiple UCS Domain among different Management Servers and Agent Managed Computers. While doing so, sometimes it may be required to assign the monitoring of UCS Domain from one Cisco UCS Management Service to another Management Service.

Complete the following steps to migrate the UCS Domain to different Cisco UCS Management Service:

Step 1 In the SCOM application, click the **Go** tab on the menu bar.

Step 2 Choose **Authoring** from the drop-down menu.

Step 3 Select **Management Pack Templates > Cisco Unified Computing System**.

Step 4 Right-click one of the UCS instances and select **Properties**.

Step 5 Select a different machine type and/or service machine from the drop down list.

Step 6 Click **OK/Apply**.

Monitoring Cisco UCS Domains with SCOM

This chapter includes the following sections:

- About the Monitoring Pane in SCOM, page 8-1
- Accessing the Cisco UCS folder in the Monitoring Pane, page 8-1
- About the Cisco UCS Folder, page 8-1

About the Monitoring Pane in SCOM

After you install and configure the Cisco UCS Management Pack, you can use the Monitoring pane of the operations manager to display a summary and components of a monitored Cisco UCS domain. The Cisco Unified Computing System folder and views in the Monitoring pane provide a complete view of the health of the Cisco UCS domains.

Accessing the Cisco UCS folder in the Monitoring Pane

Step 1 In the left pane of the SCOM application, click the **Monitoring** tab.

Step 2 Expand the **Cisco Unified Computing System** folder.

About the Cisco UCS Folder

The Cisco Unified Computing System folder displays active alert, state view and state summary for all discovered Cisco UCS domains and hardware components. The folder also provides additional views of components, which show monitoring data collected from Cisco UCS domains.

This folder contains the following sub-folders and views that display global aspects of all the monitored Cisco UCS domains:

- Cisco UCS Management Service Folder, page 8-2
- Cisco UCS Instance Folder, page 8-3
- Hardware Inventory Folder, page 8-6

Management Pack Events

This view shows any alert related to execution of monitoring scripts in Operations Manager, some of the common errors are listed in the table below:

Table 8-1 Common Errors

Serial No.	Error Code	Error Description	What to Check
1	19900	Service Connection Error	Verify the Service Machine entry in the **Add Monitoring** Wizard
2	19900	Service not found or not running.	Check if the Management Service is up and running on the Service Machine.
3	19900	Connection to the Cisco UCS Management Service failed.	Verify the account is associated to the profile and the account is authorized to make a connection to the UCS Domain.

Cisco UCS Management Service Folder

This folder contains following views related to Cisco UCS Management Service.

- Alert View—Displays alerts related to service
- Performance View—Contains counters related to performance
- State View—Displays the health state of the service

Start Service

If the Management Service used to monitor Cisco UCS Domain is stopped, an alert gets generated in the **Alert** View. Use the Start Service task to remotely start the Management Service from the Operations Manager Console.

Stop Service

If the Management Service is no longer used to monitor Cisco UCS Domain, then the Management Service could be stopped from Operations Manager Console.

Complete the following steps to start or stop the Management Service:

Step 1 In the SCOM application, click the **Go** tab in the menu bar.

Step 2 Choose **Monitoring** from the drop-down menu.

Step 3 Expand the Cisco Unified Computing System folder to display the folders and views.

Step 4 Expand **Cisco UCS Management Service** and go to **State** View.

Step 5 Select the Management Service, and from the **Tasks** pane, click **Start Service** or **Stop Service**.

Note It is crucial for the Cisco UCS domain monitoring added in the Operations Manager, that the Cisco UCS Management Service be in a healthy state. Make sure to capture alerts early in the Alert View and resolve them.

Cisco UCS Instance Folder

The Cisco UCS Instance folder contains a sub-folder for each Cisco UCS domain monitored by SCOM. Each Cisco UCS domain folder contains the following sub-folders that display alerts and information about the health and components of the domain:

- Diagram View —Displays a graphical view of a set of Cisco UCS managed objects and shows how they relate to each other.
- <UCS Name> Alert View—Displays active alerts in the Cisco UCS domain.
- <UCS Name> State View— Display health status and other inventory information about Cisco UCS domain.
- State Summary View—Provides alert view and state view in a single panel, also known as the dashboard view. This view summarizes all related information about the Cisco UCS domain.
- Hardware Inventory Folder —Different views and sub-folders under the hardware inventory folder provide a detailed insight on health state, inventory and fault information about various hardware components present in the UCS Domain.
- Logical Inventory Folder — Different views and sub-folders under the logical inventory folder provide a very detailed insight on health state and inventory information about various logical components present in the UCS Domain.

Cisco UCS Instance Tasks

The Cisco UCS Management Pack provides capability to launch following tasks on each UCS Domain Instance being monitored by Operations Manager. These tasks are available under **Tasks** > **Cisco UCS Instance Tasks** when a UCS Domain is selected from <UCS Name> State View in the Cisco UCS Instance Folder.

Generating Discovery Events

Generating discovery events generates windows events for the selected classes, which results in the corresponding Object discovery to retrieve updates from the Management Service about that particular class object. This feature is used to manually run the Object Discoveries to retrieve updates about the class in Operations Manager.

Note Generating discovery events is a mandatory task when any disabled object discovery is enabled using object discovery override. This operation retrieve old updates about the class from Management Service and updates them in the Operations Manager.

Complete the following steps to generate discovery events:

Step 1 In the SCOM application, click the **Go** tab in the menu bar.

Step 2 Choose **Monitoring** from the drop-down menu.

Step 3 Expand the Cisco Unified Computing System folder to display the folders and views.

Step 4 Select **State Summary** and click **Cisco UCS Domain** from Cisco UCS Instance State View.

Step 5 Click **Cisco UCS Instance Tasks** > **Generate Discovery Events** from right panel.

Step 6 When the **Generate Discovery Events** task launches, click **Override**.

Step 7 Change the New Value to **True** for one or more classes, to generate discovery events from them.

Step 8 Click **Run**.

Note Generate Discovery Events is an Agent Task, and executes on the computer where the Management Service is hosted to monitor the UCS Domain. The operation results in the corresponding Object Discovery to run and retrieve the latest updates from the Management Service.

Launch UCS GUI

The default browser is launched and redirected to the selected UCS home page.

Note In order to launch the UCS GUI, network connectivity should be available between the computer where the Operations Manager Console application is running and the UCS Domain.

Complete the following steps to launch the UCS GUI:

Step 1 In the SCOM application, click the **Go** tab in the menu bar.

Step 2 Choose **Monitoring** from the drop-down menu.

Step 3 Expand the Cisco Unified Computing System folder to display the folders and views. Select **State Summary** and click **Cisco UCS Domain** from the Cisco UCS Instance State View.

Step 4 Click **Cisco UCS Instance Tasks** > **Launch UCS GUI** from the right panel.

Load UCS Fault Data

The Cisco UCS Management Service collects faults from the UCS Domain using event channel subscription and generates windows events. The Cisco UCS Management Pack reads the windows events and displays them in the Operations Console. This activity is automatically handled by Cisco UCS Management Service and Management Pack.

Loading the UCS fault data manually refreshes the event channel subscription and moves the updated faults from UCS Domain into the Operations Console.

Complete the following steps to load the UCS Fault Data:

Step 1 In the SCOM application, click the **Go** tab in the menu bar.

Step 2 Choose **Monitoring** from the drop-down menu.

Step 3 Expand the Cisco Unified Computing System folder to display the folders and views. Select State Summary and click **Cisco UCS Domain** from Cisco UCS Instance State View.

Step 4 Click **Cisco UCS Instance Tasks** > **Load UCS Fault Data** from the right panel.

Step 5 Click **Run**.

Note Load UCS Fault Data is an Agent task, and executes on the computer where the Management Service is hosted to monitor the UCS Domain

Load UCS Inventory Data

The Cisco UCS Management Pack collects inventory updates from the UCS Domain periodically (the default interval is two hours). Use this task to manually load any updates from UCS Domain.

Complete the following steps to load the UCS Inventory Data:

Step 1 In the SCOM application, click the **Go** tab in the menu bar.

Step 2 Choose **Monitoring** from the drop-down menu.

Step 3 Expand the Cisco Unified Computing System folder to display the folders and views. Select State Summary and click **Cisco UCS Domain** from Cisco UCS Instance State View.

Step 4 Click **Cisco UCS Instance Tasks** > **Load UCS Inventory Data** from right hand panel.

Step 5 Click **Override** to override any task parameter. The following overrides are available.

- **a.** TimeOut Seconds: Time out period for the task to complete execution.
- **b.** Organization Discovery Level: Defines the level up-to which Organizations and Service Profiles from UCS Domain should be discovered in operations Manager.
- **c.** Enable Logging: Defines if the logging is enabled/disabled for this object discovery.
- **d.** Cache Class: Defines the Managed Object for which inventory or Monitoring information to be collected from UCS Domain.
- **e.** Associated Service Profiles: Defines whether the associated or unassociated Service Profiles need to be discovered in SCOM. Default value is “True” which means only an associated service profile needs to be discovered in the Operations Manager.

Step 6 Click **Run**.

Note Load UCS Inventory Data is a SCOM Agent Task and executes on the Service Machine monitoring UCS Domain.

Ping UCS

The Ping UCS task pings to the UCS domain to check the connectivity between the Operations Manager console and the Cisco UCS domain.

Follow the steps outline below to Ping UCS Domain

Step 1 In the SCOM application, click the **Go** tab in the menu bar.

Step 2 Choose **Monitoring** from the drop-down menu.

Step 3 Expand the Cisco Unified Computing System folder to display the folders and views. Select State Summary and click **Cisco UCS Domain** from Cisco UCS Instance State View.

Step 4 Click **Cisco UCS Instance Tasks** > **Ping UCS** from right hand panel.

Ping UCS Continuously (ping -t)

The Ping UCS Continuously task continuously pings to the UCS Domain to check the connectivity between the Operations Manager Console and the Cisco UCS Domain.

Complete the following steps to ping the UCS Domain continuously:

Step 1 In the SCOM application, click the **Go** tab in the menu bar.

Step 2 Choose **Monitoring** from the drop-down menu.

Step 3 Expand the Cisco Unified Computing System folder to display the folders and views. Select State Summary and click **Cisco UCS Domain** from Cisco UCS Instance State View.

Step 4 Click **Cisco UCS Instance Tasks** > **Ping UCS Continuously (ping –t)** from right hand Panel.

Hardware Inventory Folder

The Hardware Inventory folder displays a diagram view of the Cisco UCS hardware in the Cisco UCS domain, such as chassis, blade servers, fabric interconnects, and rack mount servers. Each type of hardware has its own folder with alert view, state view, and state summary for that hardware.

Different views and folders under Hardware Inventory provide an insight to health state, inventory and fault information about various hardware components of UCS Domain.

The following are the views and folders present under the hardware inventory:

- Diagram View: shows the entire hardware component under UCS Domain in a hierarchical fashion. User can click any component and the details view will give additional information about the component. User can also choose to launch the Alert View and Diagram view to see the alerts or component with-in the selected component.
- Chassis
  - Blade
  - Fan Module
  - Fan
  - IO Module
  - Port
  - PSU
- Fabric Interconnect
  - Fan
  - Fan Module
  - PSU
  - Storage Item
  - Switch Card
  - Port
  - SWVlanPortNS
- Rack Mount

- FEX
  - Fan
  - IO Module
  - Power Supply Unit
- Rack Unit
  - Fan Module
  - Interface Card
  - Inventory
  - PSU

Each of the above folders has three views:

- Alert View: Shows the alerts on all the instance of the component.
- State View: Shows the inventory about all the instances of the component.
- State Summary: Shows the State View and Alert View in a single pane.

Logical Inventory Folder

Different views and folders under Logical Inventory provide an insight to health state, inventory and fault information about various logical components of UCS Domain. Following views and folder are present under logical Inventory:

- Diagram View: Displays the entire logical component under UCS Domain in a hierarchical fashion. You can click any component and the details view provides additional information about the component. You can also choose to launch the Alert View and Diagram view from the right panel to see the alerts or component within the selected component.
- Organization: State View lists all the organizations and sub-organizations available in the UCS Domain. Hierarchy of the organizations can be seen from the Diagram View. Alert View shows all the alerts related to organizations and sub-organizations and the State Summary shows the State View and the Alert View in a single pane.
  - Firmware Packs and Items

    Firmware Items: Lists the state summary of various firmware items.

    Firmware Packs: Lists the state summary of various firmware Packs.
  - Pools: Lists the state summary of various Pools like: Mac Pool, Server Pool, UUID Pool etc.
  - Service Profiles. Alert View and State View shows the alerts and inventory related to the service profiles. State Summary shows the Alert View and State View in a single pane.

Note By default the management pack discovers only the root level organization and its components (Service Profiles/Pools), in order to discover sub-organizations; override the Discovery level under Cisco UCS Instance Object Discovery.

Note By default the management pack discovers only associated service profiles. In order to discover the non-associated service profiles, override the IsAssociated parameter under Cisco UCS Instance Object Discovery.

This folder displays Logical Inventory View of UCS which contains Organization, Service Profiles, Pools, Firmware Packs and Items. It consists of Organizations folder which contains different views for the Organization, that is, Alert View, State View, and State Summary view. It also contains sub folders for Sub-Organizations, Service Profiles, Firmware Packs and Items, and Pools, each containing the different views for respective items. All the sub-organizations have a similar content structure.

UCS HW/Logical Component Tasks

KVM Console Task

The Cisco UCS Management Pack provides capability to launch KVM console from the Operations Console. KVM console launch action is available for following UCS components:

- Blade Server (Hardware Component)
- Rack Unit Server (Hardware Component)
- Service Profile (Logical Component)

Complete the following steps to launch the KVM console:

Step 1 In the SCOM application, click the **Go** tab in the menu bar.

Step 2 Choose **Monitoring** from the drop-down menu.

Step 3 Expand the Cisco Unified Computing System folder to display the folders and views.

Step 4 Expand the Cisco UCS Instance(s) folder.

Step 5 Expand <UCS Name> folder of UCS Domain on which KVM Console should be launched. Depending upon KVM Console should be launched on Blade/Rack/Service Profile, follow one of the following steps:

a. Blade Server: Go to **HW Inventory** > **Chassis** > **Blade** > **Blade State View**. Select the blade server and click **Tasks** > **Blade Tasks** > **Launch KVM**.

b. Rack Unit Server: Go to **HW Inventory** > **Rack Mount** > **Rack Unit** > **Rack Unit State View**. Select the rack unit server and click **Tasks** > **Rack Unit Tasks** > **Launch KVM**.

c. Service Profile: Go to **Logical Inventory** > **Organization** > **Service Profiles** > **Service Profile State** View. Select the service profile and click **Tasks** > **Service Profile Tasks** > **Launch KVM**.

Note The KVM console requires Java Version 1.6 Update (14). To launch the KVM console, you must have valid Cisco UCSM user credentials with administrator or user role privileges, and must be associated with the Cisco UCS Domain Profile.

Caution The KVM console cannot be launched on a Blade/Rack Unit/Service Profile, if the connection to the UCS Domain is established using a proxy server.

Caution The KVM console being a console task cannot be launched on a Blade/Rack Unit/Service Profile, when there is no direct connectivity between Operations Console machine and the Service Machine where the Cisco UCS Management Service is running. This could occur when the Operations Console machine belongs to a different Active Directory Domain than the Service Machine.

Alert Operations

Acknowledge UCS Faults

This operation could be performed on an Operation Manager alert created by the Management Pack due to a fault on UCS Domain. Using this operation, user can acknowledge an UCS Domain fault from the Operations Manager Console itself.

Prerequisites: Required configuration as explained under the Configuring Faults Acknowledgments section must be completed before performing this operation.

Complete the following steps to acknowledge a UCS fault from Operations Manager Console:

Step 1 Select an alert in Operations Manager which belongs to a UCS Domain.

Step 2 Right click on the alert and choose **Set Resolution State**.

Step 3 Click **UCS Acknowledged** (configured resolution state).

View Knowledge Article of Alerts

Knowledge Articles provide more information about an alert generated in Operations Manager. This Management Pack supports knowledge articles for every UCS fault generated as alert in Operations Manager. Knowledge articles will help the user to get additional information about the alert like Fault Cause, Explanations and Resolution steps. Resolution Steps should be followed to resolve the alerts.

Complete the following steps to view the knowledge articles of generated alerts:

Step 1 Select an alert in Operations Manager which belongs to a UCS Domain.

Step 2 Right click on the alert and choose **Properties**.

Step 3 On the properties window, click the **Product Knowledge** tab.

Clearing of Alerts

Alerts generated in Operations Manager due to UCS Domain faults will get closed automatically in Operations Manager when the fault is cleared from UCS Domain. There is no manual activity required to clear an alert in the Operations Manager console.

CHAPTER 9

Troubleshooting

This chapter includes the following sections:

- Error when Adding a Cisco UCS Domain to SCOM, page 9-1
- Cisco UCS Monitoring Not Started, page 9-1
- Cisco UCS Monitoring Stopped, page 9-2
- Cisco UCS Management Service Log, page 9-2

Tip For troubleshooting issues with SCOM, see the knowledge base articles available from Support for Microsoft System Center 2012.

Error when Adding a Cisco UCS Domain to SCOM

Problem SCOM displays an error message when you attempt to add a Cisco UCS domain. This error message is displayed if the required library, Cisco.UCS.MP.UI.dll, is not present on the current machine.

Solution Adding a UCS Domain using Operations Manager Console is allowed from the computers where the installer was run to import the Management Pack or install the Management Service or both.

Cisco UCS Monitoring Not Started

Scenario 1

Problem After successfully adding Cisco UCS Domain and assigning appropriate Run-As-Account to Run-As-Profile, Cisco UCS Domain is not monitored.

Solution Look for event 19900 in the Management Pack Events under Monitoring > Cisco Unified Computing System. Disable LAN proxy or “choose Bypass proxy server for local addresses” from LAN Settings on computer hosting Cisco UCS Management Service. Discovery of UCS instance is scheduled every hour hence it will take approximately one hour to discover UCS instance.

To modify the proxy using Internet Explorer:

Step 1 Open Internet Explorer

Step 2 Go to **Tools** > **Internet Options** > **Connections** > **LAN Settings** > **Proxy Server**

Step 3 Disable **Use a proxy server for your LAN**

Scenario 2

Problem After successfully adding Cisco UCS Domain and assigning appropriate Run-As-Account to Run-As-Profile, Cisco UCS Domain is not monitored, and the following error message (example shown below) is displayed in the Event Data section of the Management Pack Events:

```
Example:
DN: Miscellaneous Error: Could not load file or assembly
'file:///C:\Windows\TEMP\dfeyvn4h.dll' or one of its dependencies. The system cannot find
the file specified.
```

Solution SCOM Action Account user and its group should have read/write permission to "C:\windows\temp" folder.

Cisco UCS Monitoring Stopped

Problem Monitoring stops and an alert message appears which makes the service machine critical.

Solution Go to the **Alert Details** section and click **Start the Service**, and then **Run the task**. This ensures the Management Service is up and running. You can also verify the same from the services.msc dialog box.

Cisco UCS Management Service Log

This version of the Cisco UCS Management Pack supports Cisco UCS Management Service logging.

Logs are present at:

"%PROGRAMDATA%\Cisco\UCSM\Log"

Under the above location there are separate logs for each Cisco UCS Domain being monitored.

Logging Levels

- Exception: Logs any exceptions occurred while monitoring the UCS Domain.
- Error: Logs any errors or exceptions occurred while monitoring the UCS Domain.
- Information: Logs Errors, Exceptions and informational messages to the log file.

Note Default logging level is set to: Error.

Changing the Logging Levels

Log on to the computer hosting the Cisco UCS Management Service, and complete the following steps to change the logging level:

Step 1 Open the **PowerShell** window.

Step 2 Use the **$wcf = New-WebServiceProxy http://localhost:8732/SCOMUcsAgent** command to connect to the agent.

Step 3 To get the current log, use the **$wcf.GetLoggingType("UCSM")** command.

Step 4 To change logging, enter (Info, Error, Exception) and use the **$wcf.UpdateLoggingType("UCSM","Info")** command.

Back Up Log Files

The Cisco UCS Management Service backs up log files greater than 10 MB. Once a log file size reaches 10 MB the Management Service stops writing to that file and creates a new file. If the Management Service is re-started then it checks the size of the existing active file and if it is less than 10 MB it starts appending to that file.

Purge Log Files

Any file whose last modified date and time is greater than 30 days is purged automatically. However, currently, this duration of 30 days is not configurable.

Generating Cisco UCS Technical Support File

Step 1 Launch a command prompt.

Step 2 Change the directory to Cisco UCS Management Pack installation folder (default location :- C:\Program Files\Cisco\Cisco UCS Management Pack\UcsAgent.

Step 3 Verify that file "Cisco.UCS.TechSupport.exe" is available.

Step 4 Use the following syntax to generate tech support zip file.

a. Run Cisco.UCS.TechSupport.exe without any parameter.

This generates the tech support file at default location (C:\ProgramData\Cisco\UCSM)

b. Run Cisco.UCS.TechSupport.exe <FolderName> to generate the tech support file at user defined location.

Note The tech support file can be generated per Cisco UCS Management Service guidelines. The tech support Utility is available on all the computers where Cisco UCS Management Service is installed. You should log on to the computer and run the command to generate the Tech Support file for the local Cisco UCS Management Service.

Note It is recommended to change the logging level to 'Informational' and wait for one to two days before generating the tech support file, this helps to capture required information for debugging the problem.