Smart Cloud Integration Pack

For System Center Operation Manager

v1.1.0

User's Guide

Table of Contents

About this guide

This User’s Guide provides a description of the features, installation, and use of the Acer Smart Integration Pack for Microsoft® System Center. It is intended to help system administrators to efficiently monitor and manage Acer servers.

Only persons with detailed knowledge of and experience with Microsoft® System Center should attempt this installation, potential for data corruption and/or loss exists in this User's Guide’s procedures.

1. INTRODUCTION

1.1. Overview

Acer Smart Cloud Integration Manager (Acer SCIP v1.1.0) is a software product which supersedes Acer Smart Integration Manager (Acer SIP v1.0.2). It provides add-in functions to manage Acer servers in Microsoft System Center Operation Manager (SCOM).

The major user interface (UI) is the SCOM Console. Acer SCIP primarily works in the background. It provides the functions required to discover IPMI-BMC firmware embedded in Acer servers. Acer's BMC firmware runs on Acer servers to provide Out-Of-Band Management capability. After discovering Acer servers, Acer SCIP can parse the servers' SNMP traps (PET). Based on these SNMP traps (PET), Acer SCIP can determine the hardware health state of Acer servers.

Acer SCIP can also process SNMP traps from RAID Management Software. The RAID Management Software is provided by the RAID vendors and based on these traps Acer SCIP can determine the RAID status of the Acer servers.

Acer SCIP provides a PRO-Enabled Management Pack to integrate with System Center Virtual Machine Manager (SCVMM). Once the Acer server (BMC) issues the SNMP trap (PET) to Acer SCIP, Acer SCIP can generate a PRO-Tip to the SCVMM Console via the PRO-Enabled Management Pack. The SCVMM administrator can determine whether to implement the action provided by Acer or to dismiss it. The action provided by Acer will save all the virtual machines on the Hypervisor host then put the hypervisor host into "Maintenance Mode."

1.2. Feature summary

This section shows the feature summary for Acer SCIP v1.1.0 and Acer SIP v1.0.2.

Features	SIP V1.0.2	SCIP V1.1.0
Fully integrate with MSFT System Center Operation Manager	☒	☒
Discover/Manage/Monitor Acer servers (hardware)	☒	☒
Display hardware events/alerts from Acer servers	☒	☒
Utilize Out-Of-Band hardware management (Agentless)	☒	☒
Launch Acer Smart Console for hardware-specified management	☒	☒
Display RAID alerts from the host on the Acer server	☒	☒
Support distributed-management based on SCOM architecture	☒	☒
Optionally support PRO-Tip for SCVMM	☒	☒

Note: ☒ means supported.

1.3. Supported Microsoft System Center products

Acer SCIP supports SCOM and SCVMM. The detailed information is listed below.

MSFT System Center Operation Manager Family	SIP V1.0.2	SCIP V1.1.0
Microsoft System Center 2012 R2 Operations Manager	□	☒
Microsoft System Center 2012 SP1 Operations Manager	□	☒
Microsoft System Center 2012 Operations Manager	□	□
Microsoft System Center Operations Manager 2007 R2	☒	□
Microsoft System Center Operations Manager 2007 SP1	☒	□

MSFT System Center Essentials Family	SIP V1.0.2	SCIP V1.1.0
Microsoft System Center Essentials 2010	☒	□
Microsoft System Center Essentials 2007 SP1	☒	□

MSFT System Center VMM Family	SIP V1.0.2	SCIP V1.1.0
Microsoft System Center 2012 R2 Virtual Machine Manager	□	☒
Microsoft System Center 2012 SP1 Virtual Machine Manager	□	☒
Microsoft System Center 2012 Virtual Machine Manager	□	□
Microsoft System Center 2008 R2 Virtual Machine Manager	☒	□

1.4. Supported operating systems

This section shows which operating systems are supported.

Operating System	SIP V1.0.2	SCIP V1.1.0
Microsoft Windows Server 2012 R2	□	☒
Microsoft Windows Server 2012	□	☒
Microsoft Windows Server 2008 R2	☒	□
Microsoft Windows Server 2008	☒	□

1.5. Supported languages

This section shows the languages supported by Acer SCIP and Acer SIP.

Language	V1.0.2	V1.1.0
English	☒	☒

2. INSTALLATION AND DEPLOYMENT

Acer SCIP Installation Guide is attached at the end of this document. Please install Acer SCIP according to Acer SCIP Installation Guide.

3. ACER SCIP COMPONENTS AND FUNCTIONS

This chapter describes the major Acer SCIP components and their functions.

3.1. Acer Integration Manager

Acer Integration Manager is a graphic user interface (GUI) for Acer SCIP. It assists in discovering Acer servers. The Acer Integration Manager is only available for Master Acer SCIP. The following functions are available in the Integration Manager.

3.3.1. Control Integration Service

Start, stop and re-start the Integration Service.

3.3.2. Control auto discovery

Once the Integration Service is started, you can start or stop scanning for Acer servers.

3.3.3. Configure the SNMP trap destination

You can predefine the destination of SNMP trap (PET) from Acer servers (BMC) through this function.

When Acer SCIP discovers an Acer server (BMC), it configures the IPMI-BMC firmware embedded in Acer servers to send the SNMP trap to this predefined destination when an issue occurs. The predefined destination must be the IP address of the operating system that the Master Acer SCIP is installed on.

If the destination is not set as expected, Acer SCIP can't get the SNMP trap (PET).

When you change the proxy agent of the managed Acer servers via the SCOM Console, the SNMP trap (PET) destination for the IPMI-BMC firmware embedded in Acer servers changes to the new proxy agent, too. *Proxy agent* represents the SCOM Management Server.

3.3.4. Configure Credential for Microsoft SQL Server

The Acer SCIP Integration Service uses "SQL Authentication" to communicate with SQL server. While installing Acer SCIP, you will be asked to enter the account and password information. You can also change the credential after installation.

If the credential is not set properly, the Integration Service can't communicate with the SQL server.

3.3.5. Manage IP ranges for discovery

You can set up to 10 IP ranges for server discovery. Each range can cover up to 254 IP addresses, starting from xxx.xxx.xxx.1 to xxx.xxx.xxx.254. When the IP ranges are set and auto discovery starts, the Integration Service will start scanning the set IP addresses.

If no IP range is set, the Integration Service won’t scan.

3.3.6. Setup the credentials for discovery

The goal of discovery is to find Acer servers (BMC). You must enter the BMC root password first.

There is only one set of credentials in the Integration Manager UI; therefore, all Acer servers (BMC) to be discovered must have the same root account password.

If the password is not specified, the Integration Service cannot discover servers.

3.3.7. Setup discovery interval

Acer SCIP Integration Service regularly searches for new Acer servers (BMC). The default interval is 30 seconds, which can be changed as necessary.

3.3.8. List discovered Acer servers

Discovered Acer servers are listed on the Integration Manager UI. The servers' IP Address and product information will be shown.

3.3.9. Manage or un-manage Acer servers

Managed and *Un-managed* are new attributes in Acer SCIP, but they don’t exist in SCOM.

In Acer SCIP, if an Acer server is set as *Managed*, the SNMP trap (PET) from it will be processed and parsed by the Integration Service. On the other hand, Integration Service does nothing for *Un-managed* Acer servers.

Managed Acer servers will be shown on the SCOM Console, but un-managed won’t.

If you don't want to see a specific Acer server (BMC), but its IP address is within the discovery IP ranges, you can set it as un-managed.

3.2. Acer management packs

Acer provides management packs which offer integrated manageability for Acer servers with SCOM.

Management packs include:

- Acer.Server.OOB.mp
- Acer.Server.OOB.Override.xml
- Acer.Server.RAID.A.mp
- Acer.Server.RAID.L.mp
- Acer.Server.RAID.P.mp
- Acer.Server.OOB.ForwardPETToPIM.xml

3.3. Acer PRO-enabled management pack

Acer offers a management pack to generate PRO-Tip for Acer servers or for RAID to SCVMM. The PRO-enabled MP is:

- Acer.Server.OOB.PRO12.xml

3.4. Windows Task Scheduler for Acer SCIP

A task named *TimedPSActivator* will be created in the Windows Task Scheduler after installing the Master Acer SCIP. It runs the predefined PowerShell Scripts provided by Acer SCIP every two minutes to sync the Acer SCIP database with SCOM. You can modify the frequency from the Windows Task Scheduler to suit your requirements.

4. SET ACER SCIP TO WORK WITH SCOM AND SCVMM

This chapter uses scenarios to explain how to set up Acer SCIP to work with SCOM and SCVMM.

Getting Started

4.0 Check scope of SCOM authoring

Scenario 1: Discover and manage Acer servers

4.1 Discover and manage Acer servers

4.2 Set servers as *managed* in Integration Manager

4.3 Sync *managed* Acer servers to SCOM

4.4 Delete Acer servers from the SCOM UI

4.5 Change proxy agent for Acer servers

Scenario 2: Monitor Acer servers

4.6 Monitor Acer servers in the SCOM UI

4.7 Forward SNMP traps (PET) to the Integration Service

4.8 Sync parsed SNMP traps (PET) to SCOM

4.9 Use *Alert View* to view SNMP trap events

4.10 Use *Health Explore* to determine system health

4.11 Use *Event View* to view server history

4.12 Launch Acer Smart Console for further checks

Scenario 3: Monitor RAID events related to Acer servers

4.13 Associate the OS IP with the server

4.14 Process RAID events related to Acer servers

4.15 Use *Alert View* to view RAID events

4.16 Use *Health Explore* to reset system health

4.17 No RAID event(s) in *Event View*

4.18 Open RAID management for further checks

Scenario 4: Generate PRO-Tip for Acer servers

4.19 Import *Acer.Server.OOB.PRO12.xml*

4.20 Associate hypervisor with Acer servers

4.21 Monitor associations from SCOM UI

4.22 Forward SNMP traps (PET) to Integration Service

4.23 Sync parsed SNMP traps (PET)

4.24 Use *Alert View* under *Acer Server – PRO12*

4.25 Use *Health Explore* for *Acer Server – PRO12*

4.26 Use *Event View*

4.27 View PRO-Tips in SCVMM

4.28 Implement PRO-Tips on SCVMM

Scenario 5: Generate PRO-Tips for RAID on Acer servers

4.29 Import *Acer.Server.OOB.PRO12.xml*

4.30 Associate hypervisors with Acer servers

4.31 Monitor associations in the SCOM UI

4.32 Process RAID SNMP traps for PRO-Tips

4.33 Use *Alert View* for *Acer Server – PRO12*

4.34 Use *Health Explore* for *Acer Server – PRO12*

4.35 No event(s) in *Event View*

4.36 View PRO-Tips in SCVMM

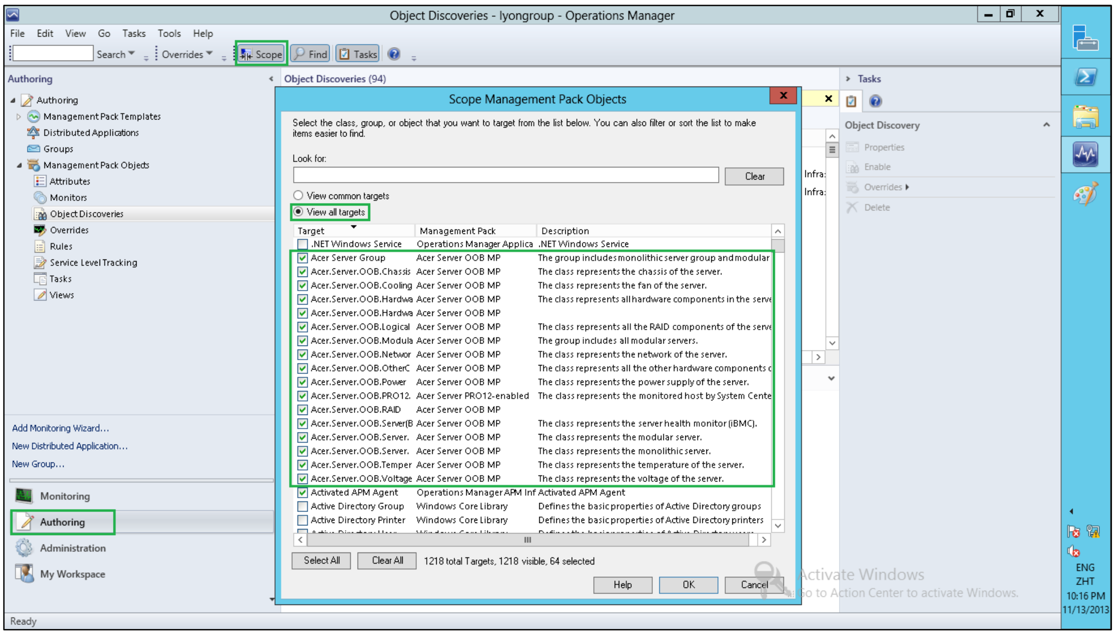
4.37 Implement PRO-Tips on SCVMM

Getting Started

4.0. Check scope of SCOM authoring

In order to make sure SCOM will carry out the discoveries, rules, monitors defined in Acer's MPs, you must first check the scope of SCOM authoring. Acer SCIP will not work correctly unless all targets in the authoring scope UI are marked.

1. Open the SCOM Console > **Authoring** > **Scope** > **View all targets**
2. Mark all the *Acer.Server.xxxxxxx* targets in the list
3. Click **OK**



Scope Management Pack Objects

Select the class, group, or object that you want to target from the list below. You can also filter or sort the list to make items easier to find.

Look for:

○ View common targets

● View all targets

Target	Management Pack	Description
□ .NET Windows Service	Operations Manager Applica	.NET Windows Service
☑ Acer Server Group	Acer Server OOB MP	The group includes monolithic server group and modular
☑ Acer.Server.OOB.Chassis	Acer Server OOB MP	The class represents the chassis of the server.
☑ Acer.Server.OOB.Cooling	Acer Server OOB MP	The class represents the fan of the server.
☑ Acer.Server.OOB.Hardwa	Acer Server OOB MP	The class represents all hardware components in the serve
☑ Acer.Server.OOB.Hardwa	Acer Server OOB MP	
☑ Acer.Server.OOB.Logical	Acer Server OOB MP	The class represents all the RAID components of the serve
☑ Acer.Server.OOB.Modula	Acer Server OOB MP	The group includes all modular servers.
☑ Acer.Server.OOB.Networ	Acer Server OOB MP	The class represents the network of the server.
☑ Acer.Server.OOB.OtherC	Acer Server OOB MP	The class represents all the other hardware components c
☑ Acer.Server.OOB.Power	Acer Server OOB MP	The class represents the power supply of the server.
☑ Acer.Server.OOB.PRO12.	Acer Server PRO12-enabled	The class represents the monitored host by System Cente
☑ Acer.Server.OOB.RAID	Acer Server OOB MP	
☑ Acer.Server.OOB.Server(B	Acer Server OOB MP	The class represents the server health monitor (iBMC).
☑ Acer.Server.OOB.Server.	Acer Server OOB MP	The class represents the modular server.
☑ Acer.Server.OOB.Server.	Acer Server OOB MP	The class represents the monolithic server.
☑ Acer.Server.OOB.Temper	Acer Server OOB MP	The class represents the temperature of the server.
☑ Acer.Server.OOB.Voltage	Acer Server OOB MP	The class represents the voltage of the server.
☑ Activated APM Agent	Operations Manager APM Inf	Activated APM Agent
□ Active Directory Group	Windows Core Library	Defines the basic properties of Active Directory groups
□ Active Directory Printer	Windows Core Library	Defines the basic properties of Active Directory printers

1218 total Targets, 1218 visible, 64 selected

Scenario 1: Discover and manage Acer servers

4.1. Discover Acer servers

In order to manage and monitor Acer servers (BMCs), the Acer servers must first be discovered using the Integration Manager UI, not by SCOM. There are two ways to discover Acer servers via the Integration Manager UI:

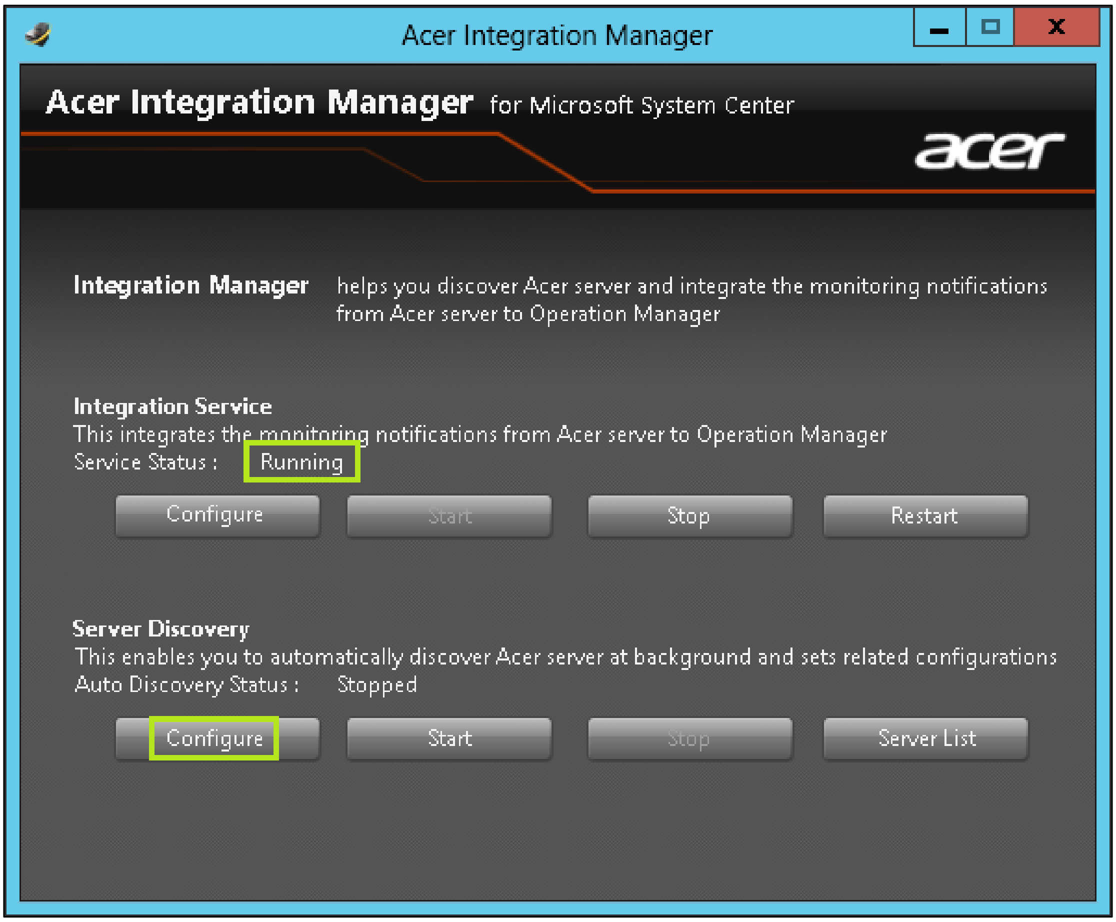
- Automatic discovery
- Add a single device

It's very important to ensure the BMC on the Acer servers is connected to the network before discovery. Refer to section 2.3.

4.1.1. Automatic discovery

Perform the following steps to discover Acer servers automatically.

1. Launch the Acer Integration Manager UI.
2. Ensure the *Integration Service* is running.
3. Click **Configuration** in the *Server Discovery* area.



Acer Integration Manager

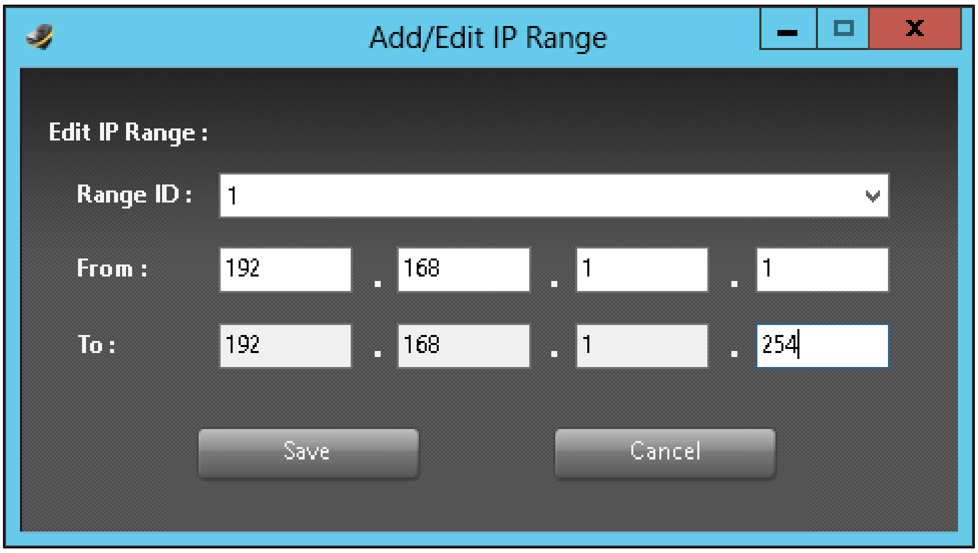
Acer Integration Manager for Microsoft System Center

Integration Manager helps you discover Acer server and integrate the monitoring notifications from Acer server to Operation Manager

Integration Service
This integrates the monitoring notifications from Acer server to Operation Manager
Service Status : Running

Server Discovery
This enables you to automatically discover Acer server at background and sets related configurations
Auto Discovery Status : Stopped

4. A *Discovery Setting* window will open: Select the *Range* tab.
5. Click **Add/Edit** to enter IP range(s) to scan. For example, scan from 192.168.1.1 to 192.168.1.254.



Add/Edit IP Range

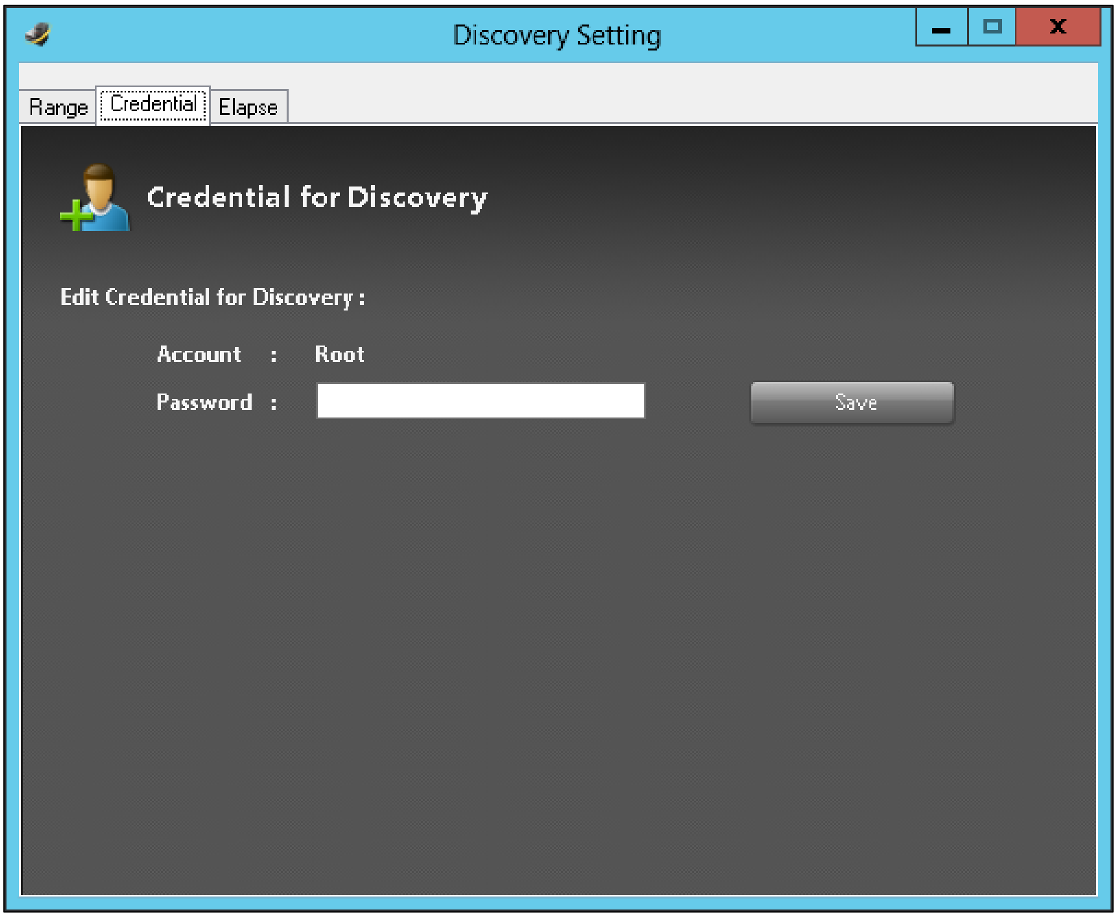
Edit IP Range :

Range ID : 1

From : 192 . 168 . 1 . 1

To : 192 . 168 . 1 . 254

6. Select the **Credential** tab.
7. Enter the root account password for the BMC firmware then save it. The default root account password for Acer BMC is "superuser".



Discovery Setting

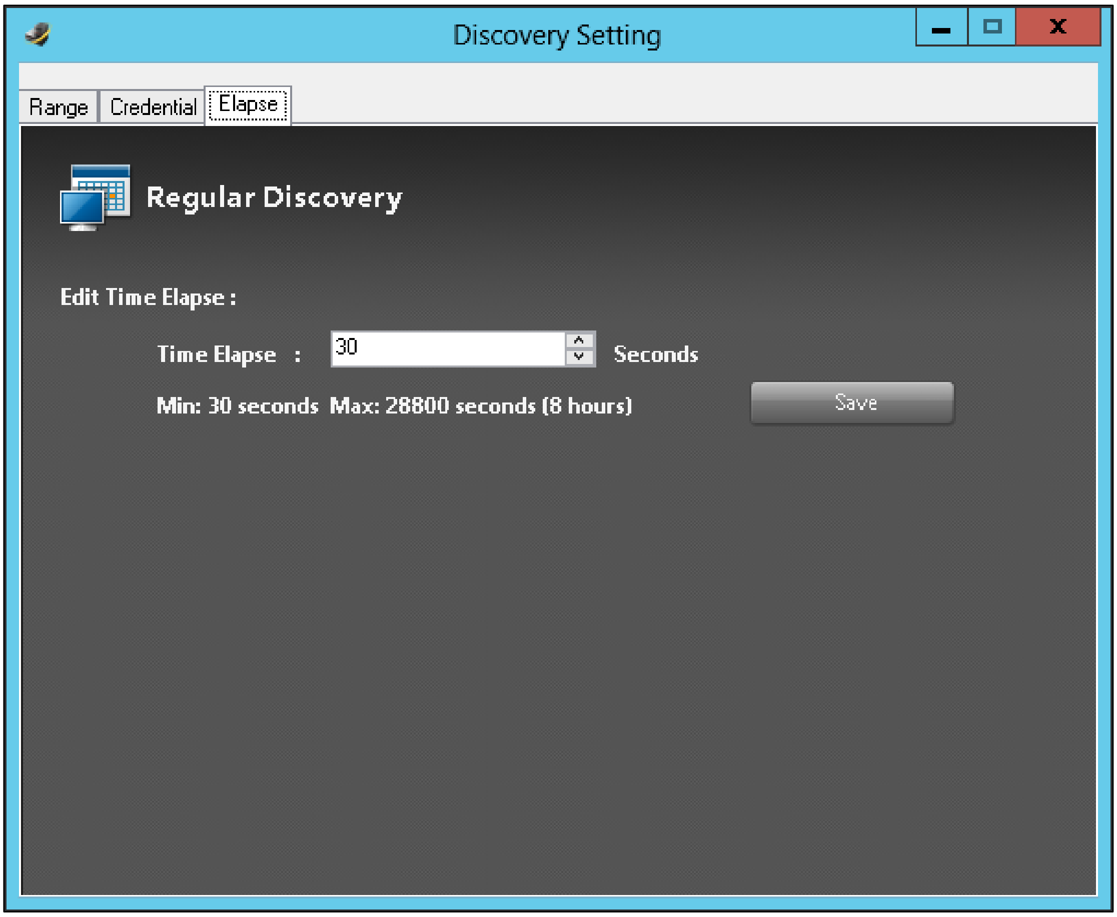
Credential for Discovery

Edit Credential for Discovery :

Account : Root

Password :

8. Select the *Elapse* tab.
9. Modify the elapse time to what you want then save it. The default is 30 seconds.

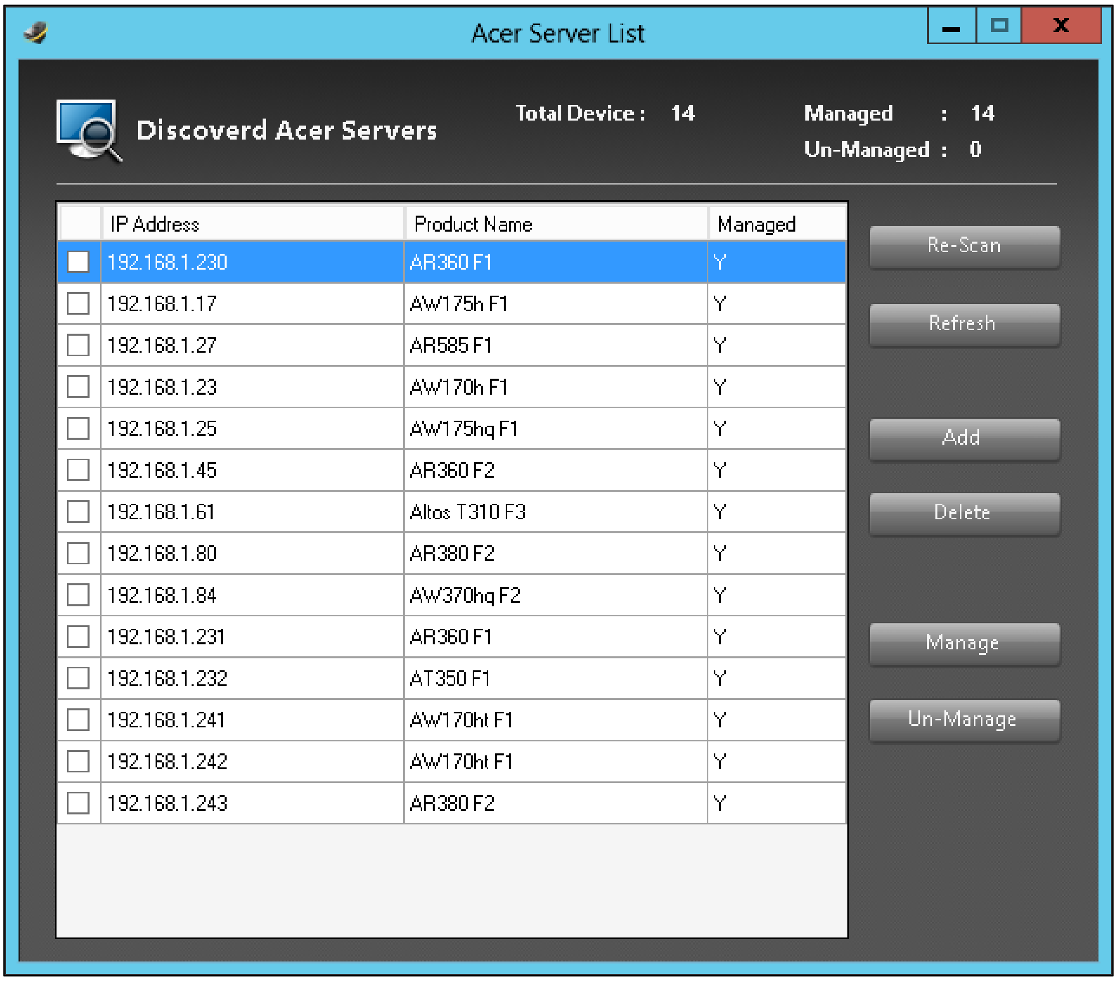


Edit Time Elapse :

Time Elapse : 30 Seconds

Min: 30 seconds Max: 28800 seconds (8 hours)

10. Close the *Configuration* window.
11. Click **Start** in the *Server Discovery* area. The status will change to *running* and discovery will run in the background.
12. Click **Server List** in the *Server Discovery* area to view the discovered Acer servers (BMC).



Total Device : 14

Managed : 14

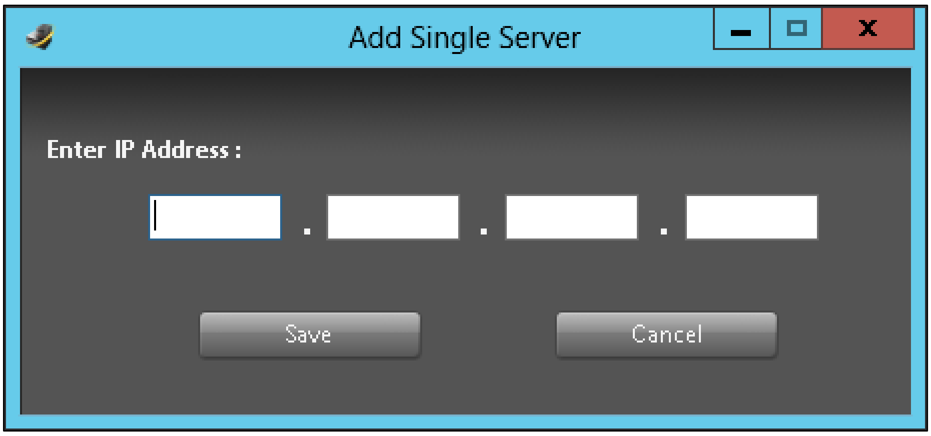
Un-Managed : 0

	IP Address	Product Name	Managed
□	192.168.1.230	AR360 F1	Y
□	192.168.1.17	AW175h F1	Y
□	192.168.1.27	AR585 F1	Y
□	192.168.1.23	AW170h F1	Y
□	192.168.1.25	AW175hq F1	Y
□	192.168.1.45	AR360 F2	Y
□	192.168.1.61	Altos T310 F3	Y
□	192.168.1.80	AR380 F2	Y
□	192.168.1.84	AW370hq F2	Y
□	192.168.1.231	AR360 F1	Y
□	192.168.1.232	AT350 F1	Y
□	192.168.1.241	AW170ht F1	Y
□	192.168.1.242	AW170ht F1	Y
□	192.168.1.243	AR380 F2	Y

4.1.2. Add a single device

Perform the following steps to add a single Acer server.

1. Launch the Acer Integration Manager UI.
2. Ensure that *Integration Service* is running.
3. Click **Configuration** in the *Server Discovery* area.
4. Select the **Credential** tab.
5. Enter the root account password for the BMC firmware then save it. The default root account password for Acer BMC is "superuser".
6. Close the *Configuration* window.
7. Click **Server List** in the *Server Discovery* area to open the *Acer Server List*.
8. Click **Add**, and enter the IP address of the Acer server (BMC), then save it.



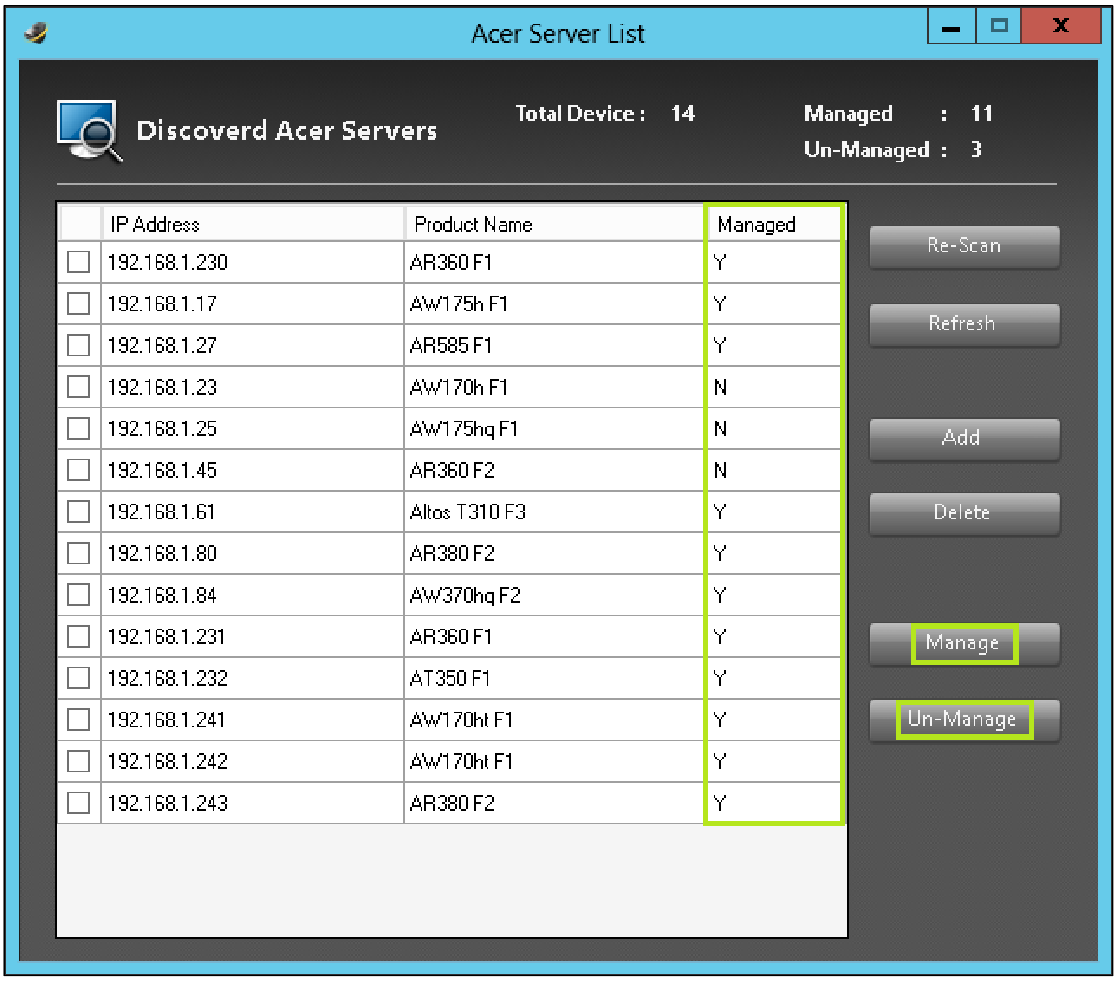
9. The specified Acer server will be added to the *Acer Server List*, provided it can be discovered and the specified credential is correct.

4.2. Set servers as *managed* in Integration Manager

Discovered Acer servers will be listed in the *Acer Server List* in the Integration Manager UI. They will be set as *managed* by default, but you can change them to *un-managed* depending on your needs.

You can follow the steps below to change the *Managed* state to Y or N. Only managed Acer servers will be synched to SCOM later by the *TimePSActivator* task.

1. Launch the Acer Integration Manager UI.
2. Click **Server List** in the *Server Discovery* area to open the *Acer Server List* showing all discovered Acer servers.
3. Mark the checkbox of the targeted Acer servers.
4. Click **Un-manage** to set the *Managed* state as N or click **Manage** to set it as Y.



Discoverd Acer Servers

Total Device : 14

Managed : 11

Un-Managed : 3

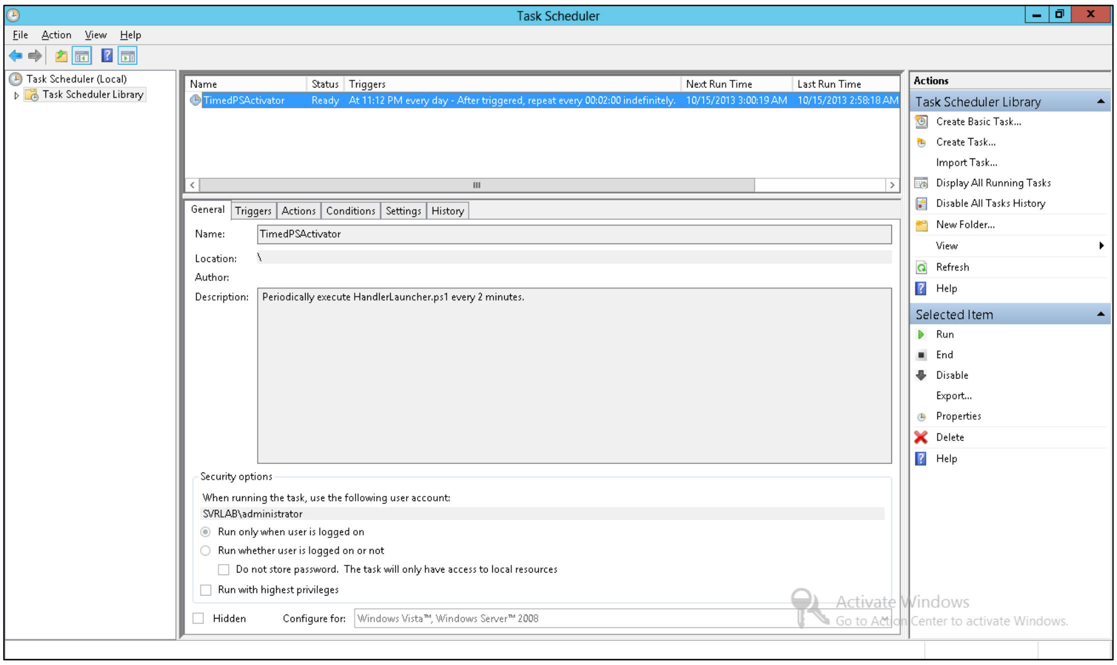
	IP Address	Product Name	Managed
□	192.168.1.230	AR360 F1	Y
□	192.168.1.17	AW175h F1	Y
□	192.168.1.27	AR585 F1	Y
□	192.168.1.23	AW170h F1	N
□	192.168.1.25	AW175hq F1	N
□	192.168.1.45	AR360 F2	N
□	192.168.1.61	Altos T310 F3	Y
□	192.168.1.80	AR380 F2	Y
□	192.168.1.84	AW370hq F2	Y
□	192.168.1.231	AR360 F1	Y
□	192.168.1.232	AT350 F1	Y
□	192.168.1.241	AW170ht F1	Y
□	192.168.1.242	AW170ht F1	Y
□	192.168.1.243	AR380 F2	Y

4.3. Sync *managed* Acer servers to SCOM

The *TimedPSActivator* task in the Windows Task Scheduler will sync managed Acer servers to SCOM regularly. The task performs synchronization every two minutes by default.

You can modify the frequency through the following steps.

1. Open **Control Panel** > **Administrative Tools** > **Task Scheduler** > **Task Scheduler Library**.



Name	Status	Triggers	Next Run Time	Last Run Time
TimedPSActivator	Ready	At 11:12 PM every day - After triggered, repeat every 00:02:00 indefinitely.	10/15/2013 3:00:19 AM	10/15/2013 2:58:18 AM

Name: TimedPSActivator

Location: \

Author:

Description: Periodically execute HandlerLauncher.ps1 every 2 minutes.

Security options

When running the task, use the following user account:

SVRLAB\administrator

● Run only when user is logged on

○ Run whether user is logged on or not

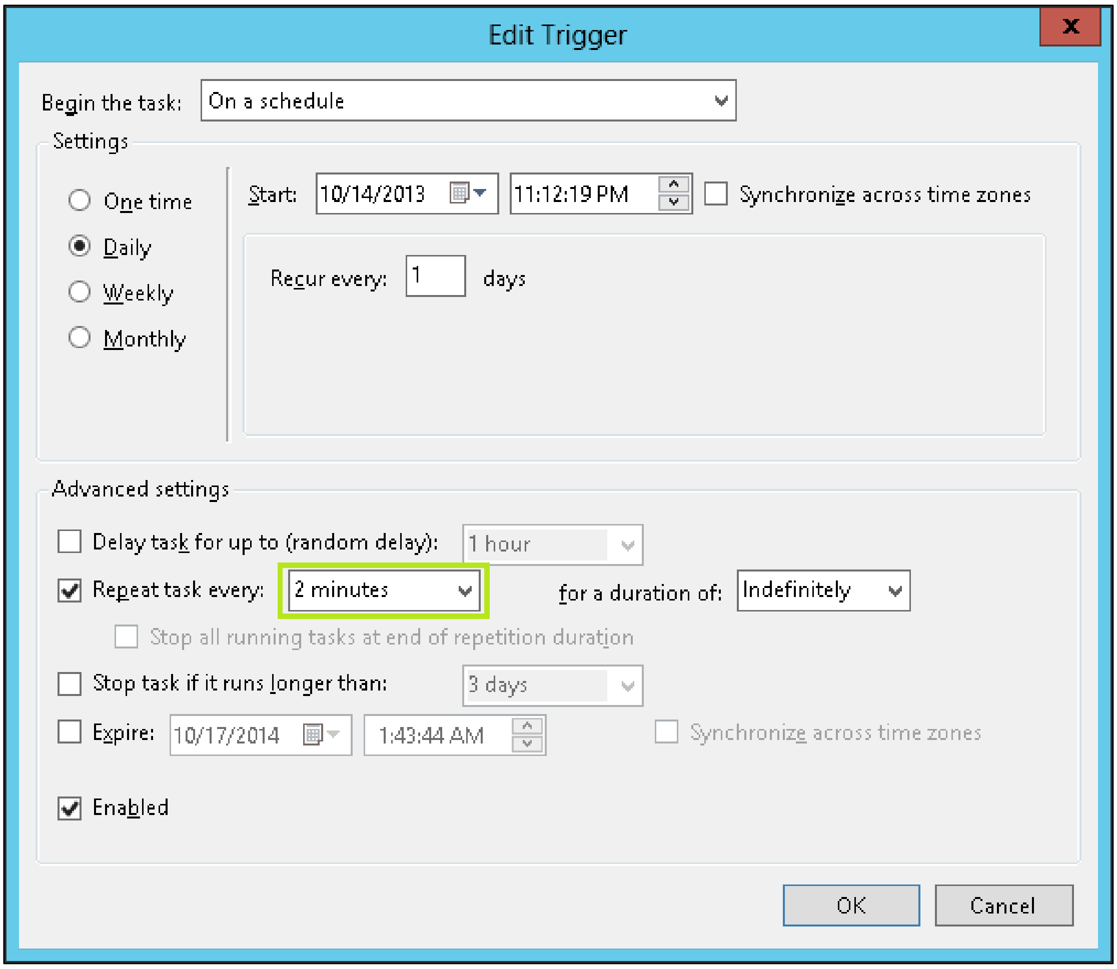
□ Do not store password. The task will only have access to local resources

□ Run with highest privileges

□ Hidden Configure for: Windows Vista™, Windows Server™ 2008

Activate Windows
Go to Action Center to activate Windows.

2. Double-click **TimedPSActivator**.
3. Select the **Triggers** tab.
4. Select the trigger rule and click **Edit**.
5. Modify the frequency to suit your needs.



Edit Trigger

Begin the task: On a schedule

Settings

○ One time
● Daily
○ Weekly
○ Monthly

Start: 10/14/2013 11:12:19 PM □ Synchronize across time zones

Recur every: 1 days

Advanced settings

□ Delay task for up to (random delay): 1 hour

☑ Repeat task every: 2 minutes for a duration of: Indefinitely

□ Stop all running tasks at end of repetition duration

□ Stop task if it runs longer than: 3 days

□ Expire: 10/17/2014 1:43:44 AM □ Synchronize across time zones

☑ Enabled

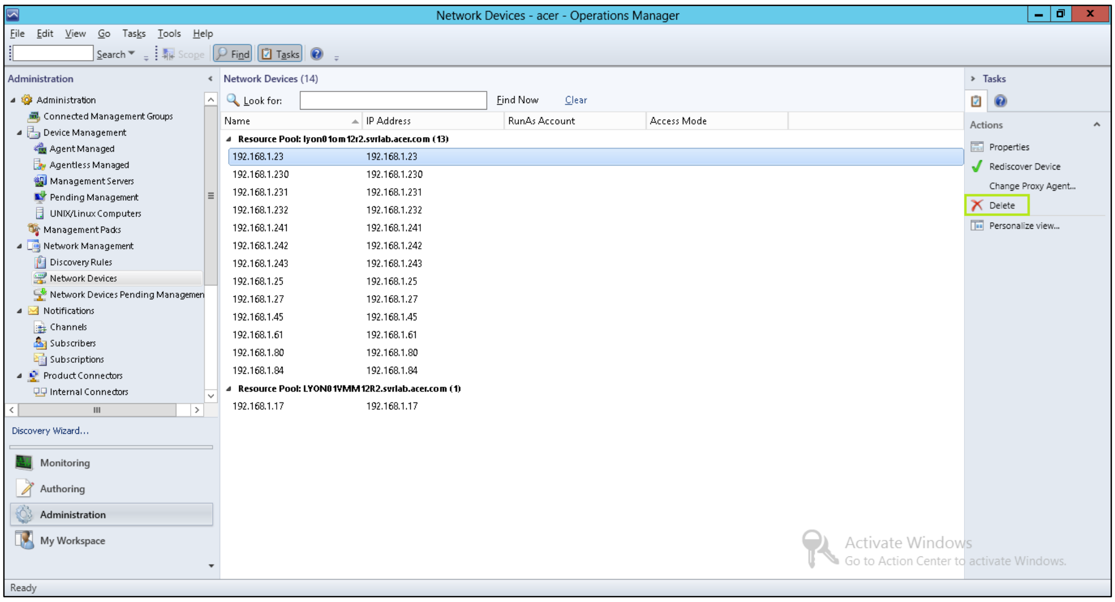
4.4. Delete Acer servers from the SCOM UI

Managed Acer servers will be synched to SCOM and the managed Acer servers shown in **SCOM** > **Administration** > **Network Devices**.

In the SCOM *Network Devices* list you can delete Acer servers. Once the servers are deleted from SCOM, they disappear from the *Network Devices* list, but they will still appear in the Integration Manager *Acer Server List*. Once the *TimedPSActivator* task completes the next synchronization, the servers' *Managed* state will be set as N.

You can follow the steps below to delete Acer servers from SCOM:

1. Open the SCOM Console.
2. Switch to **SCOM** > **Administration** > **Network Devices**.
3. Select the target Acer servers.
4. Click **Delete** in the right-hand panel.



Name	IP Address	RunAs Account	Access Mode
Resource Pool: lyon01om12r2.svrlab.acer.com (13)			
192.168.1.23	192.168.1.23		
192.168.1.230	192.168.1.230		
192.168.1.231	192.168.1.231		
192.168.1.232	192.168.1.232		
192.168.1.241	192.168.1.241		
192.168.1.242	192.168.1.242		
192.168.1.243	192.168.1.243		
192.168.1.25	192.168.1.25		
192.168.1.27	192.168.1.27		
192.168.1.45	192.168.1.45		
192.168.1.61	192.168.1.61		
192.168.1.80	192.168.1.80		
192.168.1.84	192.168.1.84		
Resource Pool: LYON01VMM12R2.svrlab.acer.com (1)			
192.168.1.17	192.168.1.17		

4.5. Change proxy agent for Acer servers

In the SCOM *Network Devices* list, you can change the proxy agent for Acer servers.

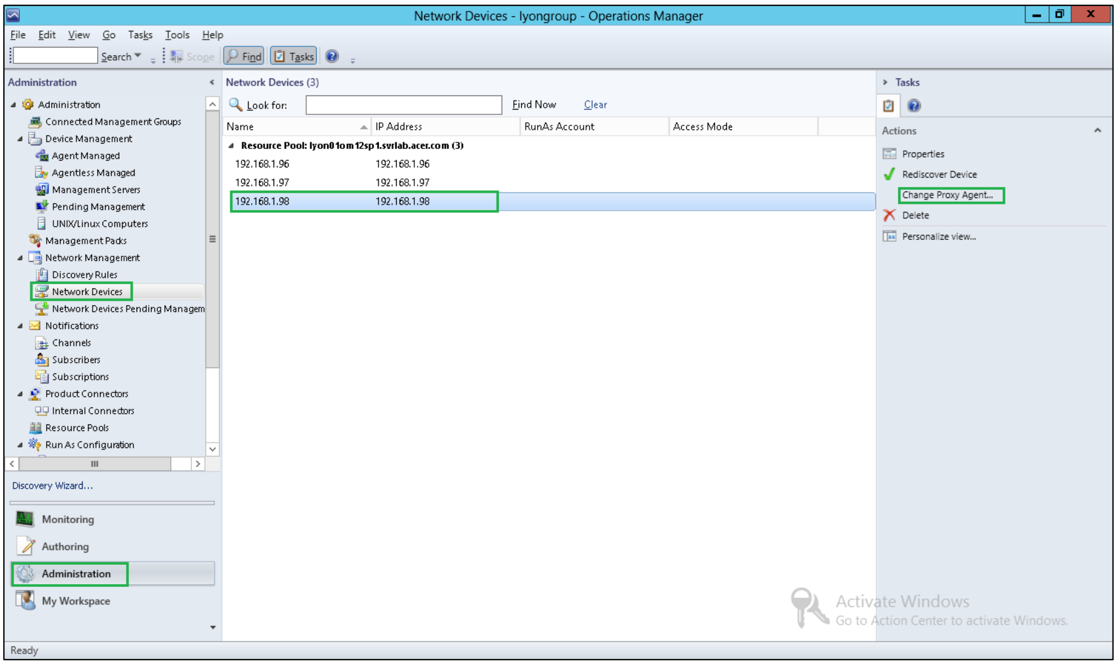
The proxy agent is the SCOM Management Server (MS) and can be modified only in a distributed deployment environment. The purpose in changing the proxy agent is to balance the management loading between SCOM Management Servers.

By default, the proxy agent of managed Acer servers is set as the SCOM MS that has the Master Acer SCIP installed, but managers can modify it. In that way, some Acer servers are processed by a specific SCOM MS, and others are handled by another SCOM MS.

Once the proxy agent of the Acer servers is changed, the *TimedPSActivator* task will perform a synchronization to inform the Acer Integration Service. The Integration Service will configure the Acer servers to send the SNMP traps to the new proxy agent when a hardware event occurs.

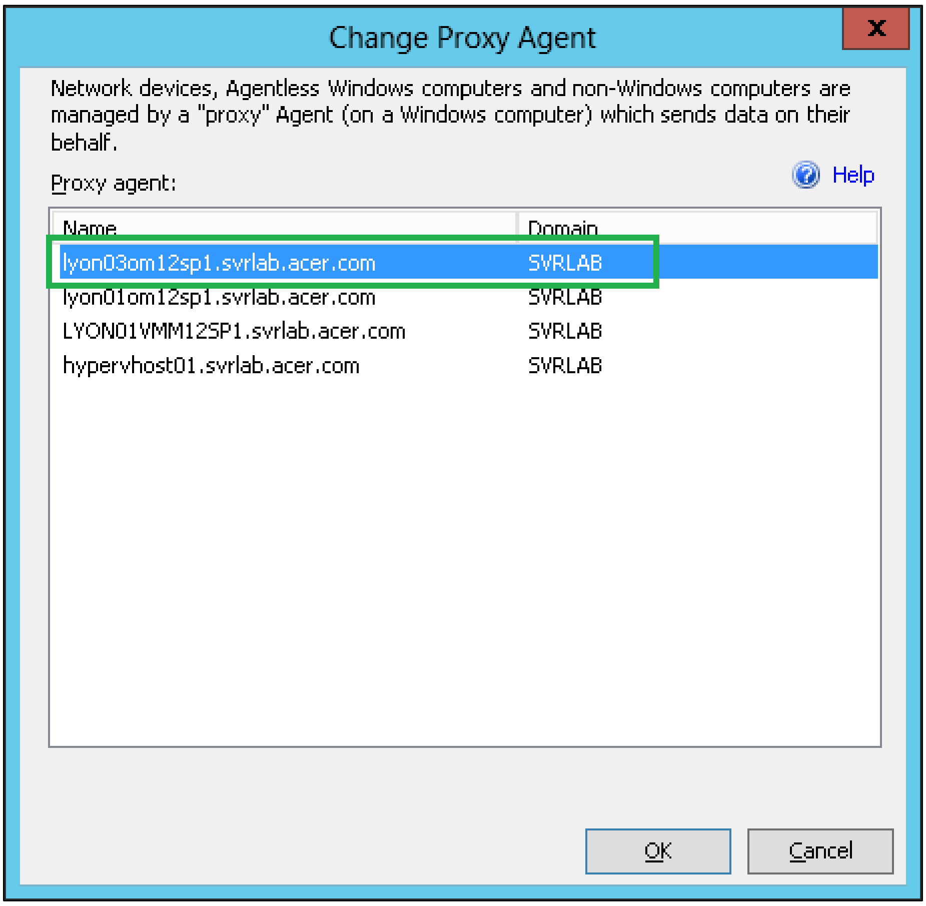
You can modify the proxy agent using the following steps:

1. Open the SCOM Console.
2. Go to **Administration** > **Network Devices**.
3. Select the target device.
4. Click **Change Proxy Agent** in the right-hand panel.



Name	IP Address	RunAs Account	Access Mode
Resource Pool: lyon01om12sp1.svrlab.acer.com (3)			
192.168.1.96	192.168.1.96		
192.168.1.97	192.168.1.97		
192.168.1.98	192.168.1.98		

5. Select a Management Server as the new proxy agent.
6. Click **OK**.

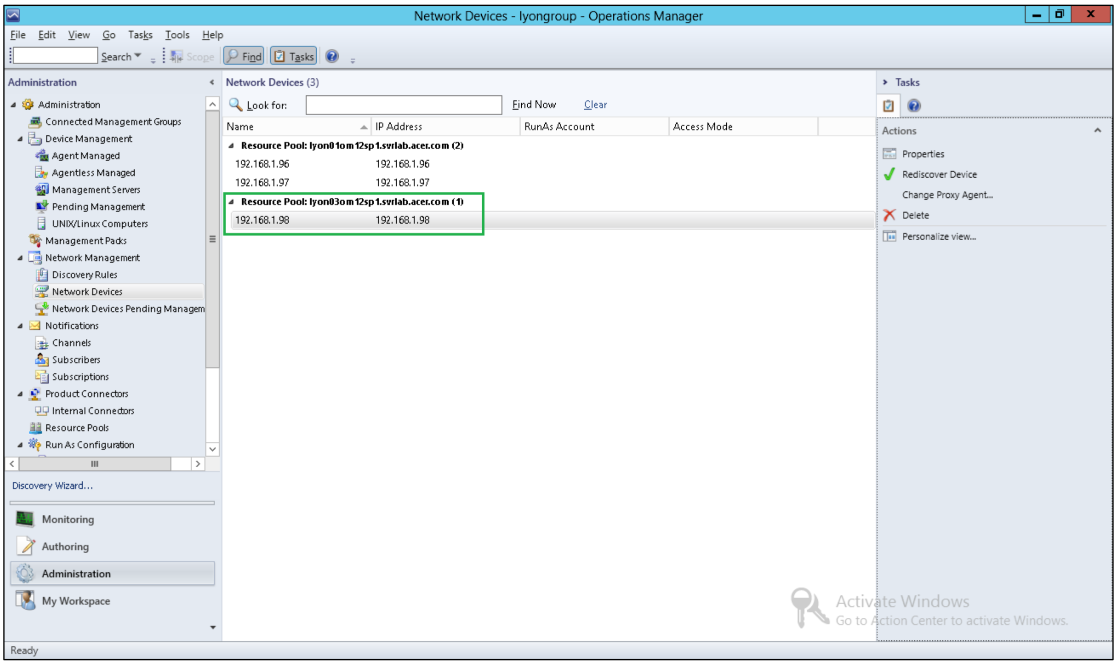


Network devices, Agentless Windows computers and non-Windows computers are managed by a "proxy" Agent (on a Windows computer) which sends data on their behalf.

Proxy agent:

Name	Domain
lyon03om12sp1.svrlab.acer.com	SVRLAB
lyon01om12sp1.svrlab.acer.com	SVRLAB
LYON01VMM12SP1.svrlab.acer.com	SVRLAB
hypervhost01.svrlab.acer.com	SVRLAB

7. The target device is now managed by the new Management Server.



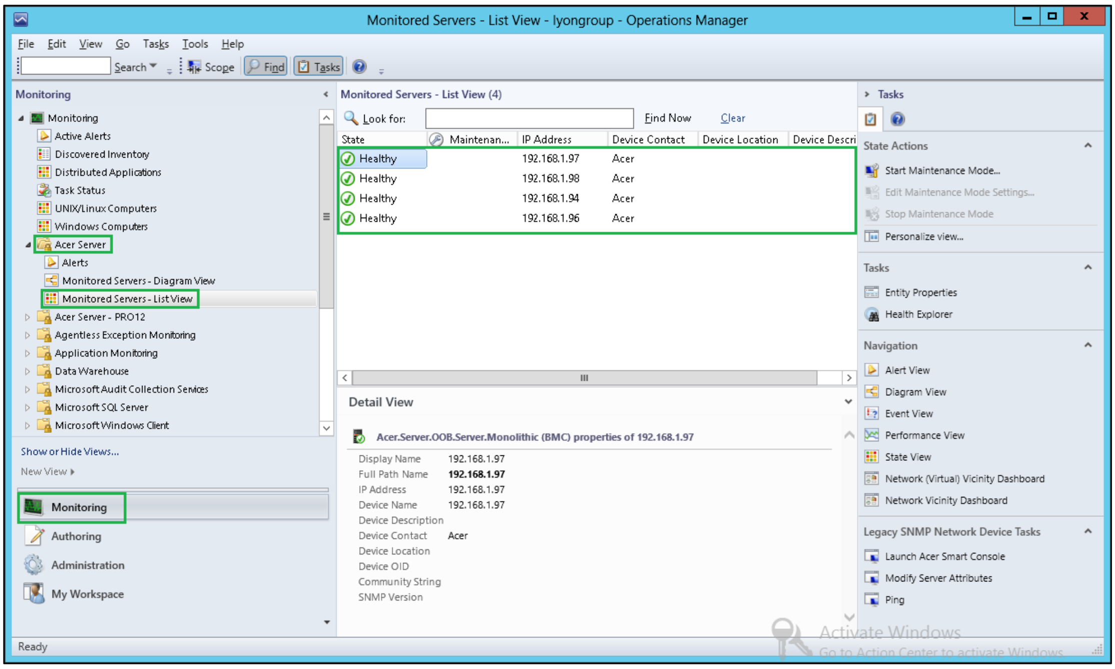
Name	IP Address	RunAs Account	Access Mode
Resource Pool: lyon01om12sp1.svrlab.acer.com (2)			
192.168.1.96	192.168.1.96		
192.168.1.97	192.168.1.97		
Resource Pool: lyon03om12sp1.svrlab.acer.com (1)			
192.168.1.98	192.168.1.98		

Scenario 2: Monitor Acer servers

4.6. Monitor Acer servers in the SCOM UI

Once managed Acer servers are shown in **SCOM** > **Administration** > **Network Devices**, the discovery rule in *Acer.Server.OOB.mp* will search for servers using the *System Contact* attribute. The action interval of this discovery rule is set as four hours by default. To change it, please refer to the SCOM Operating Guide.

Acer servers will be presented under *Acer Server Group* in *Monitoring*. Under these conditions, Acer SCIP and SCOM monitor the servers through SNMP traps from Acer servers (BMC).



State	Maintenan...	IP Address	Device Contact	Device Location	Device Descri
✓ Healthy		192.168.1.97	Acer		
✓ Healthy		192.168.1.98	Acer		
✓ Healthy		192.168.1.94	Acer		
✓ Healthy		192.168.1.96	Acer		

Acer.Server.OOB.Server.Monolithic (BMC) properties of 192.168.1.97

Display Name	192.168.1.97
Full Path Name	**192.168.1.97**
IP Address	192.168.1.97
Device Name	192.168.1.97
Device Description	
Device Contact	Acer
Device Location	
Device OID	
Community String	
SNMP Version	

4.7. Forward SNMP traps (PET) to the Integration Service

When IPMI-BMC firmware embedded in Acer servers detects a hardware event, it will send an asserted SNMP trap (PET) to the proxy agent (SCOM MS). The built-in SCOM MS SNMP trap listener will receive it, and the *ForwardPETToPIM Management Pack* (MP) will forward these SNMP traps (PET) to the Acer Integration Service.

4.8. Sync parsed SNMP traps (PET) to SCOM

After the Acer Integration Service parses the SNMP trap (PET), the *TimedPSActivator* task will perform synchronization to insert these parsed events into the SCOM UI.

4.9. Use *Alert View* to view SNMP trap events

You can open the *Alert View* for the connected Acer servers to see any current SNMP trap (PET) event(s) and asses the servers' current status.

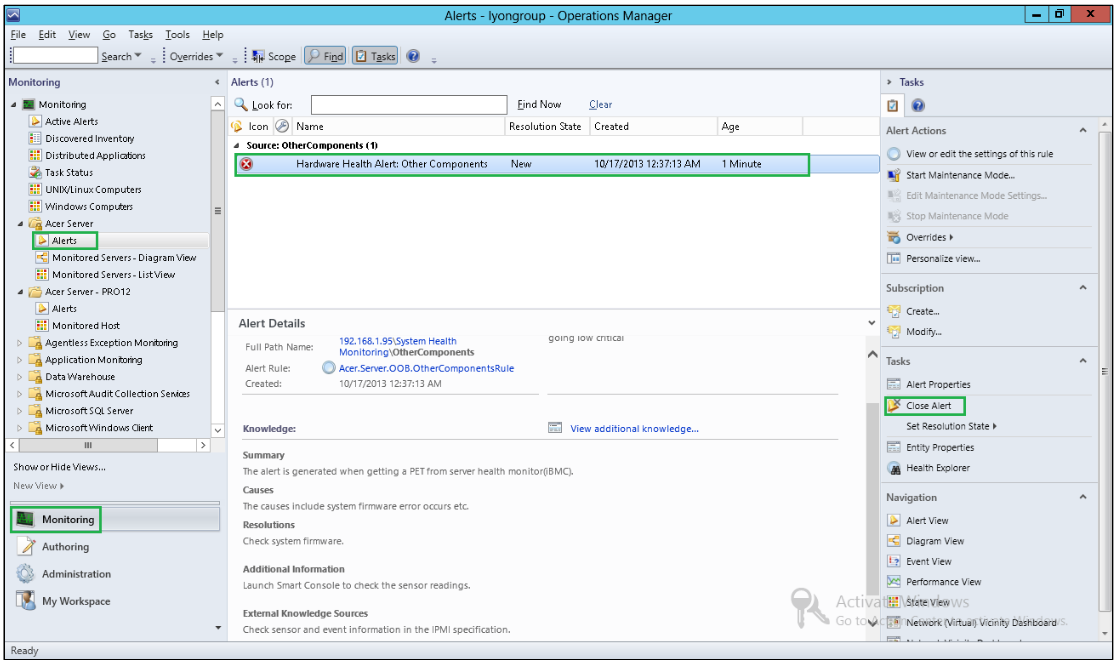
When the detected hardware issue is repaired, the Acer server (BMC) sends a "de-asserted" SNMP trap (PET) to its proxy agent (SCOM MS). The processing is the same as described in section 4.7 and 4.8, and closes the previous asserted alert information in the *Alert View*.

4.9.1. Close alerts manually

Generally alerts from Acer servers (BMC) are generated in the *Alert View* and then closed automatically. However, in some cases you may want to close the alerts from Acer servers (BMC) manually.

Follow the steps below:

1. Open the SCOM Console.
2. Go to **Monitoring** > **Acer Server** > **Alerts**.
3. Select the target alert.
4. Click **Close Alert** in the right-hand panel.



Icon		Name	Resolution State	Created	Age
Source: OtherComponents (1)					
⊗		Hardware Health Alert: Other Components	New	10/17/2013 12:37:13 AM	1 Minute

Alert Details

Full Path Name: 192.168.1.95\System Health Monitoring\OtherComponents

going low critical

Alert Rule: Acer.Server.OOB.OtherComponentsRule

Created: 10/17/2013 12:37:13 AM

Knowledge: View additional knowledge...

Summary

The alert is generated when getting a PET from server health monitor(iBMC).

Causes

The causes include system firmware error occurs etc.

Resolutions

Check system firmware.

Additional Information

Launch Smart Console to check the sensor readings.

External Knowledge Sources

Check sensor and event information in the IPMI specification.

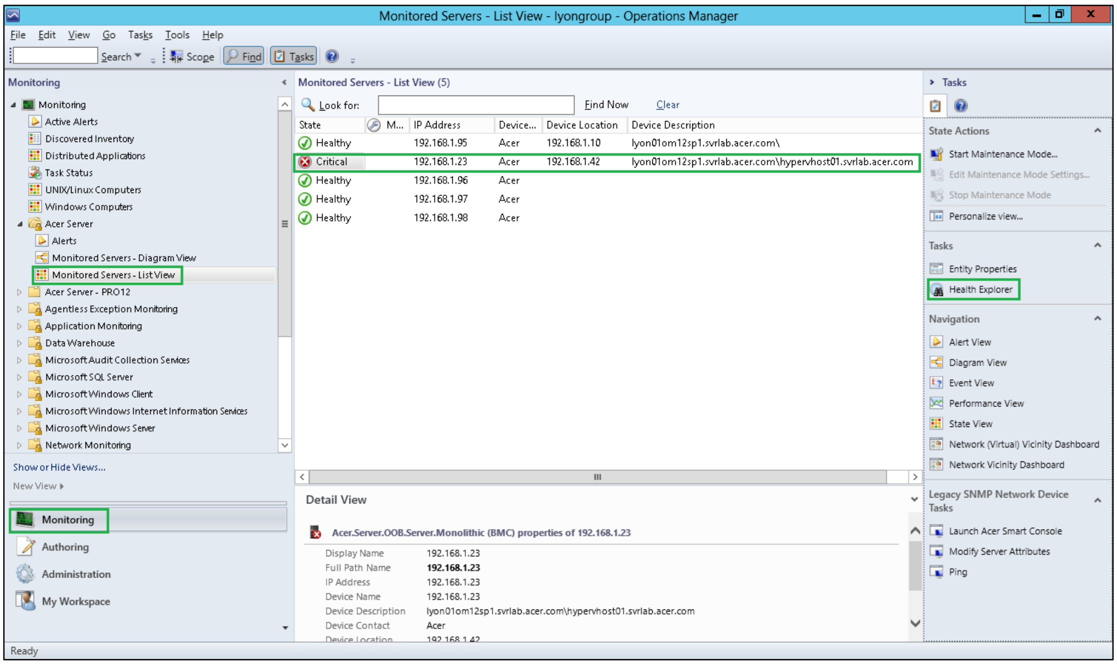
4.10. Use *Health Explore* to determine system health

Normally, alerts from Acer servers (BMC) will be shown in in *Alert View* and closed automatically. The health status of the servers will also be recovered, so you don't need to reset the health status of the Acer servers manually.

4.10.1. Reset health status manually

If you need to reset health status of Acer servers (BMC) in particular cases, follow the steps below:

1. Open the SCOM Console.
2. Go to **Monitoring** > **Acer Server** > **Monitored Servers – List View**.
3. Select the target Acer servers.
4. Click **Health Explore** in the right-hand panel.



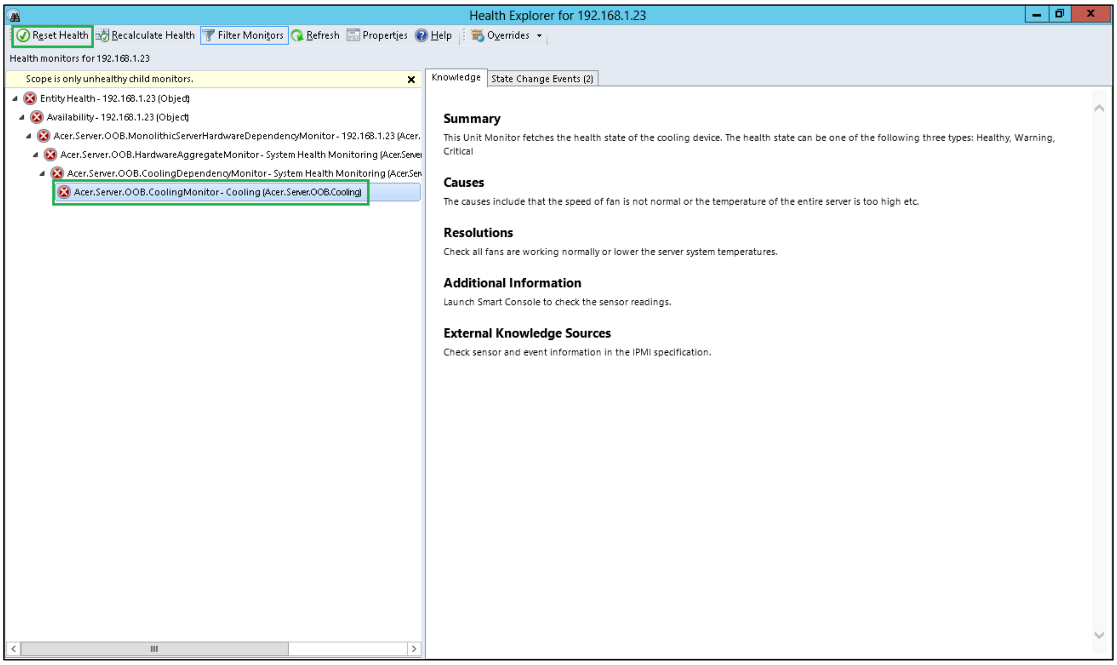
State	M...	IP Address	Device...	Device Location	Device Description
Healthy		192.168.1.95	Acer	192.168.1.10	lyon01om12sp1.svrlab.acer.com\
Critical		192.168.1.23	Acer	192.168.1.42	lyon01om12sp1.svrlab.acer.com\hypervhost01.svrlab.acer.com
Healthy		192.168.1.96	Acer		
Healthy		192.168.1.97	Acer		
Healthy		192.168.1.98	Acer		

Detail View

Acer.Server.OOB.Server.Monolithic (BMC) properties of 192.168.1.23

Display Name	192.168.1.23
Full Path Name	**192.168.1.23**
IP Address	192.168.1.23
Device Name	192.168.1.23
Device Description	lyon01om12sp1.svrlab.acer.com\hypervhost01.svrlab.acer.com
Device Contact	Acer
Device Location	192.168.1.42

5. The *Health Explore* window will open.
6. Select the target device.
7. Click **Reset Health** in the function bar at the top of the window.



Health monitors for 192.168.1.23

Scope is only unhealthy child monitors.

- Entity Health - 192.168.1.23 (Object)
  - Availability - 192.168.1.23 (Object)
    - Acer.Server.OOB.MonolithicServerHardwareDependencyMonitor - 192.168.1.23 (Acer.
      - Acer.Server.OOB.HardwareAggregateMonitor - System Health Monitoring (Acer.Server
        - Acer.Server.OOB.CoolingDependencyMonitor - System Health Monitoring (Acer.Ser
          - Acer.Server.OOB.CoolingMonitor - Cooling (Acer.Server.OOB.Cooling)

Summary

This Unit Monitor fetches the health state of the cooling device. The health state can be one of the following three types: Healthy, Warning, Critical

Causes

The causes include that the speed of fan is not normal or the temperature of the entire server is too high etc.

Resolutions

Check all fans are working normally or lower the server system temperatures.

Additional Information

Launch Smart Console to check the sensor readings.

External Knowledge Sources

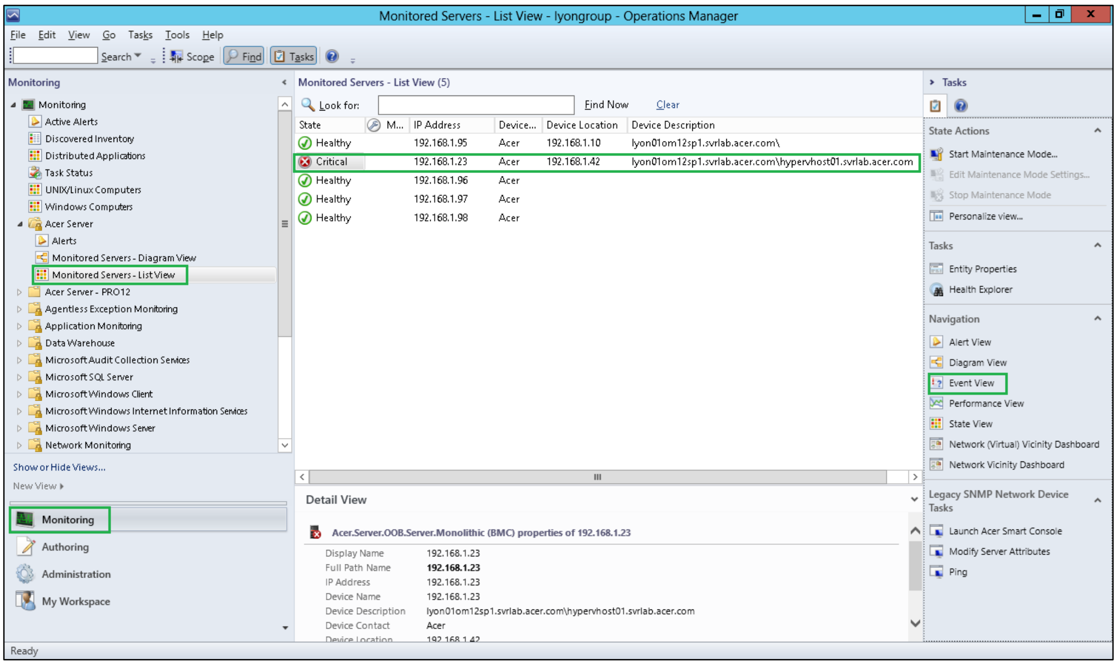
Check sensor and event information in the IPMI specification.

4.11. Use *Event View* to view server history

You can open *Event View* for a single Acer server to see the historical SNMP trap (PET) events to see the system's history.

Follow the steps below:

1. Open the SCOM Console.
2. Go to **Monitoring** > **Acer Server** > **Monitored Servers – List View**.
3. Select the target Acer server.
4. Click **Event View** in the right-hand panel.



State	M...	IP Address	Device...	Device Location	Device Description
Healthy		192.168.1.95	Acer	192.168.1.10	lyon01om12sp1.svrlab.acer.com\
Critical		192.168.1.23	Acer	192.168.1.42	lyon01om12sp1.svrlab.acer.com\hypervhost01.svrlab.acer.com
Healthy		192.168.1.96	Acer		
Healthy		192.168.1.97	Acer		
Healthy		192.168.1.98	Acer		

Detail View

Acer.Server.OOB.Server.Monolithic (BMC) properties of 192.168.1.23

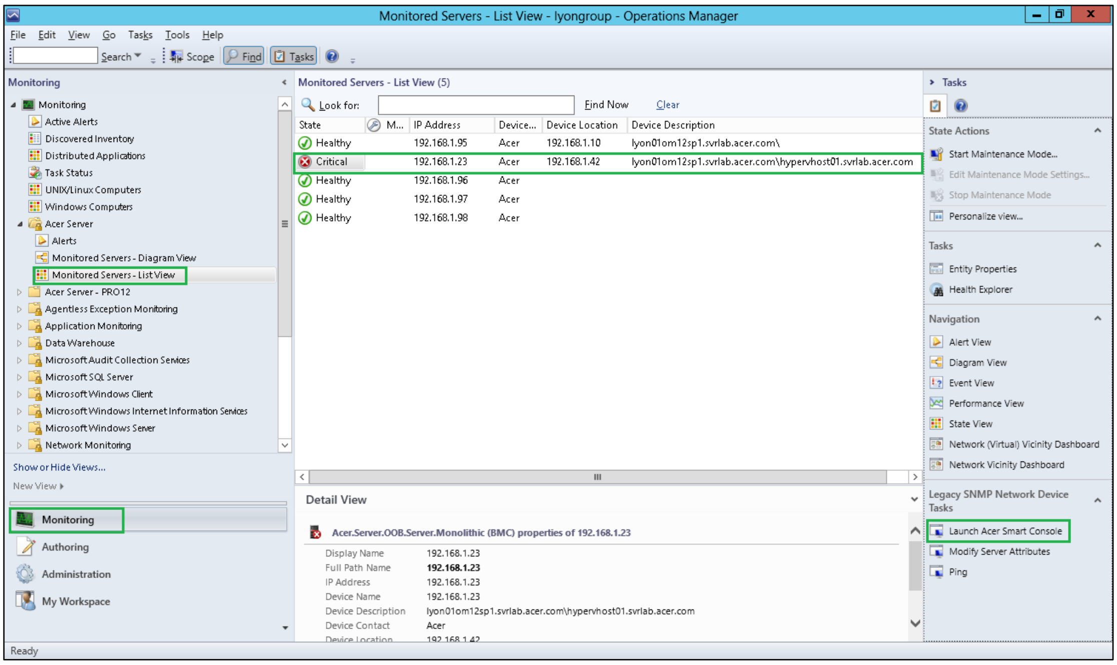
Display Name	192.168.1.23
Full Path Name	**192.168.1.23**
IP Address	192.168.1.23
Device Name	192.168.1.23
Device Description	lyon01om12sp1.svrlab.acer.com\hypervhost01.svrlab.acer.com
Device Contact	Acer
Device Location	192.168.1.42

4.12. Launch Acer Smart Console for further checks

When an alert appears in the SCOM Console *Alert View*, you can open Acer Smart Console to further check on the hardware status.

Follow the steps below:

1. Open the SCOM Console
2. Go to **Monitoring** > **Acer Server** > **Monitored Servers – List View**.
3. Select the target Acer servers.
4. Click **Launch Acer Smart Console** in the right-hand panel.



State	M...	IP Address	Device...	Device Location	Device Description
Healthy		192.168.1.95	Acer	192.168.1.10	lyon01om12sp1.svrlab.acer.com\
Critical		192.168.1.23	Acer	192.168.1.42	lyon01om12sp1.svrlab.acer.com\hypervhost01.svrlab.acer.com
Healthy		192.168.1.96	Acer		
Healthy		192.168.1.97	Acer		
Healthy		192.168.1.98	Acer		

Acer.Server.OOB.Server.Monolithic (BMC) properties of 192.168.1.23

Display Name	192.168.1.23
Full Path Name	**192.168.1.23**
IP Address	192.168.1.23
Device Name	192.168.1.23
Device Description	lyon01om12sp1.svrlab.acer.com\hypervhost01.svrlab.acer.com
Device Contact	Acer
Device Location	192.168.1.42

Scenario 3: Monitor RAID events related to Acer servers

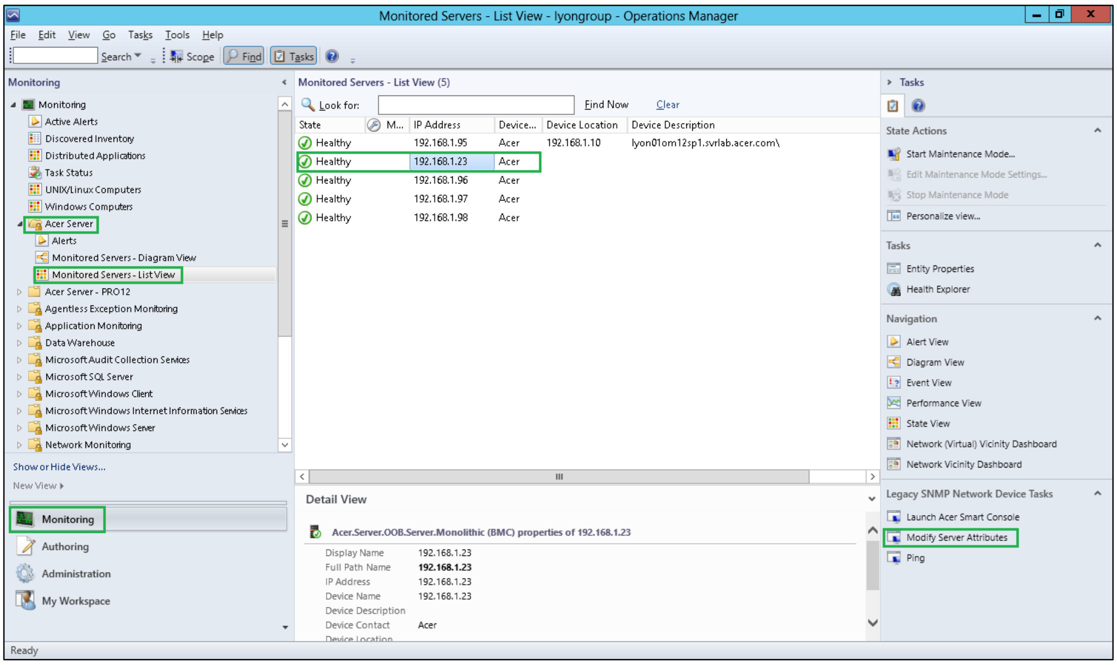
4.13. Associate the OS IP with the server

You must associate the OS IP address with its particular server (BMC) through the *Modify Server Attribute* function.

The RAID SNMP trap is sent by the RAID Management Software which is installed on an operating system (OS) running on an Acer server. The OS has its own IP address which may be different from the server's. In order to allow SCOM to know which Acer servers (BMC) the RAID SNMP trap was sent from, you must associate the OS IP address with its Acer server (BMC).

To associate the OS IP address with its server (BMC), please follow the steps below:

1. Open the SCOM Console.
2. Go to **Monitoring** > **Acer Server** > **Monitored Servers – List View**.
3. Select the target Acer servers.
4. Click **Modify Server Attributes** in the right-hand panel.



Monitored Servers - List View (5)

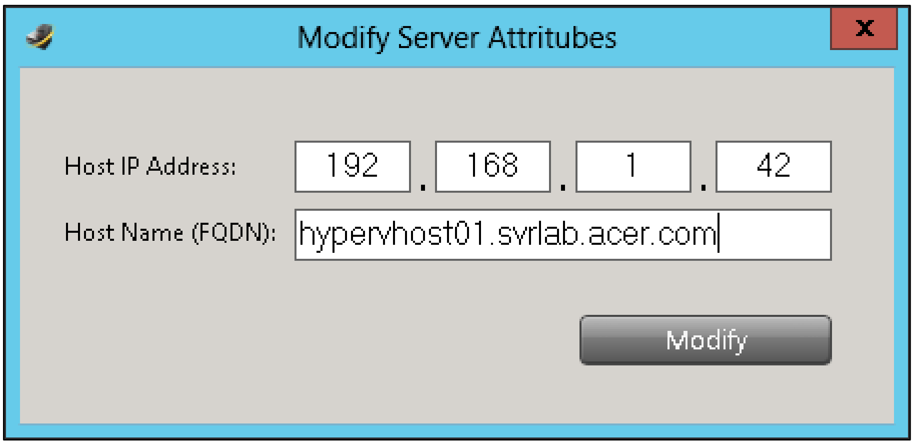
State	M...	IP Address	Device...	Device Location	Device Description
Healthy		192.168.1.95	Acer	192.168.1.10	lyon01om12sp1.svrlab.acer.com\
Healthy		192.168.1.23	Acer		
Healthy		192.168.1.96	Acer		
Healthy		192.168.1.97	Acer		
Healthy		192.168.1.98	Acer		

Detail View

Acer.Server.OOB.Server.Monolithic (BMC) properties of 192.168.1.23

Display Name	192.168.1.23
Full Path Name	**192.168.1.23**
IP Address	192.168.1.23
Device Name	192.168.1.23
Device Description	
Device Contact	Acer
Device Location	

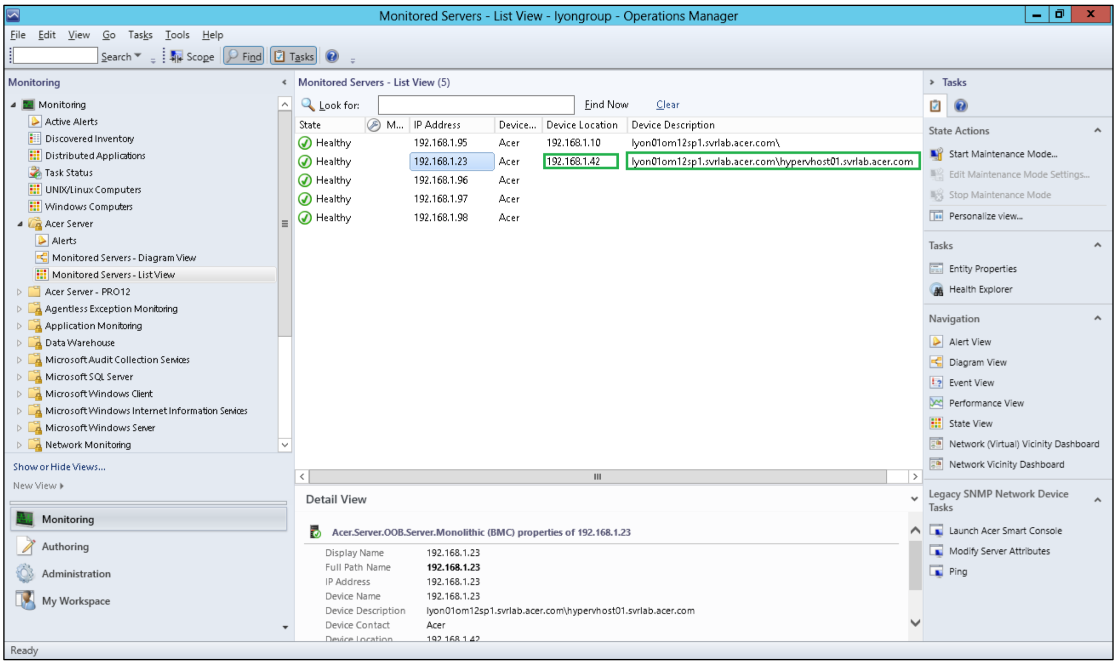
5. Enter the IP address and FQDN of the Host running on the Acer server.
6. Click **Modify**.



Host IP Address: 192 . 168 . 1 . 42

Host Name (FQDN): hypervhost01.svrlab.acer.com

7. Click **OK**.
8. The Host IP address and FQDN will be written into the device's attributes.



Monitored Servers - List View (5)

Look for: Find Now Clear

State	M...	IP Address	Device...	Device Location	Device Description
Healthy		192.168.1.95	Acer	192.168.1.10	lyon01om12sp1.svrlab.acer.com\
Healthy		192.168.1.23	Acer	192.168.1.42	lyon01om12sp1.svrlab.acer.com\hypervhost01.svrlab.acer.com
Healthy		192.168.1.96	Acer		
Healthy		192.168.1.97	Acer		
Healthy		192.168.1.98	Acer		

Detail View

Acer.Server.OOB.Server.Monolithic (BMC) properties of 192.168.1.23

Display Name	192.168.1.23
Full Path Name	**192.168.1.23**
IP Address	192.168.1.23
Device Name	192.168.1.23
Device Description	lyon01om12sp1.svrlab.acer.com\hypervhost01.svrlab.acer.com
Device Contact	Acer
Device Location	192.168.1.42

4.14. Process RAID events related to Acer servers

When SCOM's build-in SNMP trap listener receives a RAID SNMP trap, SCOM examines the source IP address of the SNMP trap according to the rules defined in *Acer.Server.RAID.x.mp*. Only RAID SNMP traps from Acer servers are processed.

4.15. Use *Alert View* to view RAID events

You can open the *Alert View* for the affected Acer server(s) to view current RAID SNMP trap events to see what happened to the RAID.

Each RAID alert must be closed manually.

4.15.1. Close alerts manually

Follow the steps in 4.9.1 to close RAID alerts.

4.16. Use *Health Explore* to reset system health

After closing the RAID alert(s), you must manually reset the health status of the affected Acer server(s).

4.16.1. Reset health status manually

Follow the steps in 4.10.1 to reset the health status of the RAID monitor.

4.17. No RAID event(s) in *Event View*

Unlike SNMP traps (PET) from Acer servers (BMC), RAID SNMP traps from RAID Management Software don't generate data in the SCOM *Event View*.

4.18. Open RAID management for further checks

In order to troubleshoot RAID events, you can open the RAID Management Software Console as provided by LSI, Adaptec or Promise.

Scenario 4: Generate PRO-Tip for Acer servers

4.19. Import *Acer.Server.OOB.PRO12.xml*

Acer.Server.OOB.PRO12.xml is to generate PRO-Tip to VMM MS for hypervisors that are running on Acer servers. By default, this MP is not imported when Acer SCIP is installed. You must import it manually.

Acer.Server.OOB.PRO12.xml is in \Program Files (x86)\Acer\Acer SCIP\MP\ on the master Acer SCIP.

4.20. Associate hypervisor with Acer servers

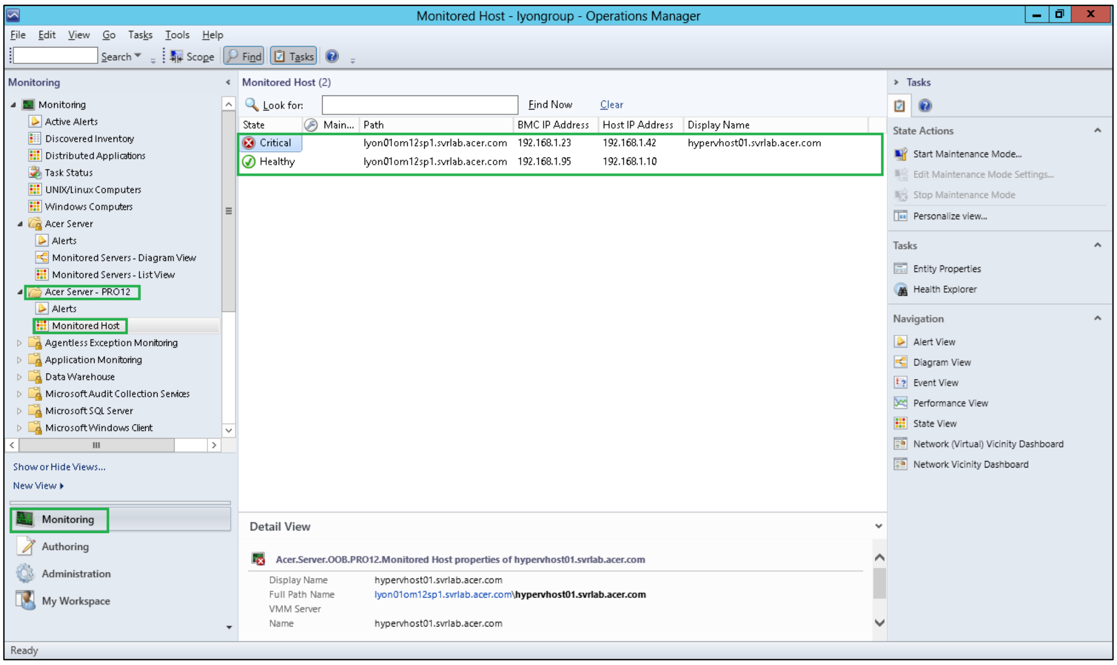
You must associate the hypervisor with Acer servers (BMC) through the *Modify Server Attribute* function.

When hypervisor is running on an Acer server and a hardware event occurs, SCOM can identify which Acer server is associated with the hypervisor according to the predefined relationship.

To associate a hypervisor with an Acer server (BMC), please follow the steps in 4.13.

4.21. Monitor associations from SCOM UI

After the hypervisor computer name has been assigned to the Acer servers through the *Modify Server Attribute* function, the discovery rule in the *Acer.Server.OOB.PRO12* MP will search for them from **SCOM** > **Administration** > **Network Devices**. The associations between each hypervisor and its Acer server are picked up. The discovery rule will create an associated item in the *Acer Server – PRO12* group under *Monitoring* to represent each combination of one hypervisor and one Acer server (BMC), and Acer SCIP and SCOM begin monitoring them.



Monitored Host (2)

Look for: Find Now Clear

State	Main...	Path	BMC IP Address	Host IP Address	Display Name
Critical		lyon01om12sp1.svrlab.acer.com	192.168.1.23	192.168.1.42	hypervhost01.svrlab.acer.com
Healthy		lyon01om12sp1.svrlab.acer.com	192.168.1.95	192.168.1.10	

Detail View

Acer.Server.OOB.PRO12.Monitored Host properties of hypervhost01.svrlab.acer.com

Display Name	hypervhost01.svrlab.acer.com
Full Path Name	lyon01om12sp1.svrlab.acer.com\hypervhost01.svrlab.acer.com
VMM Server	
Name	hypervhost01.svrlab.acer.com

4.22. Forward SNMP traps (PET) to Integration Service

The processing procedure is the same as 4.7.

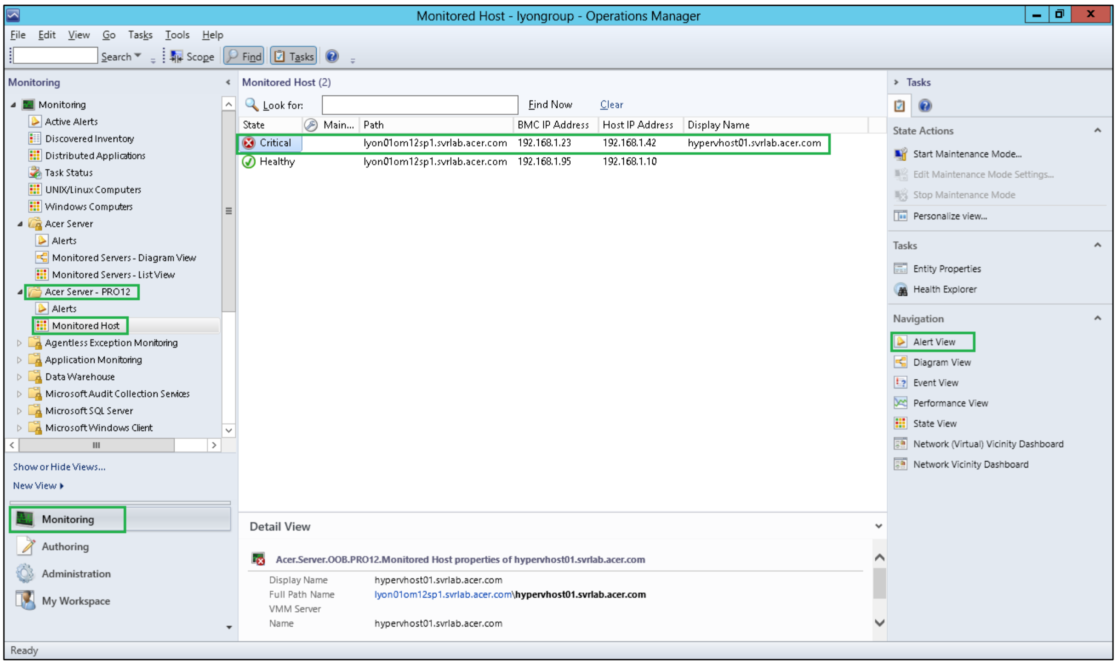
4.23. Sync parsed SNMP traps (PET)

The processing procedure is the same as 4.8.

4.24. Use *Alert View* under *Acer Server – PRO12*

At the beginning, the health status of associated items is always *good* or *healthy* in the *Acer Server – PRO12* group, no matter what health status of the servers actually is.

As time passes, the parsed SNMP traps (PET) are inserted into SCOM, and as the traps are related to certain associated items, the health status may change to *warning* or *critical*. When the health statue of an item changes to *warning* or *critical* from *good*, or changes to *critical* from *warning*, an alert will be generated in the *Alert View* for the *Acer Server – PRO12* group.



Monitored Host (2)

Look for: Find Now Clear

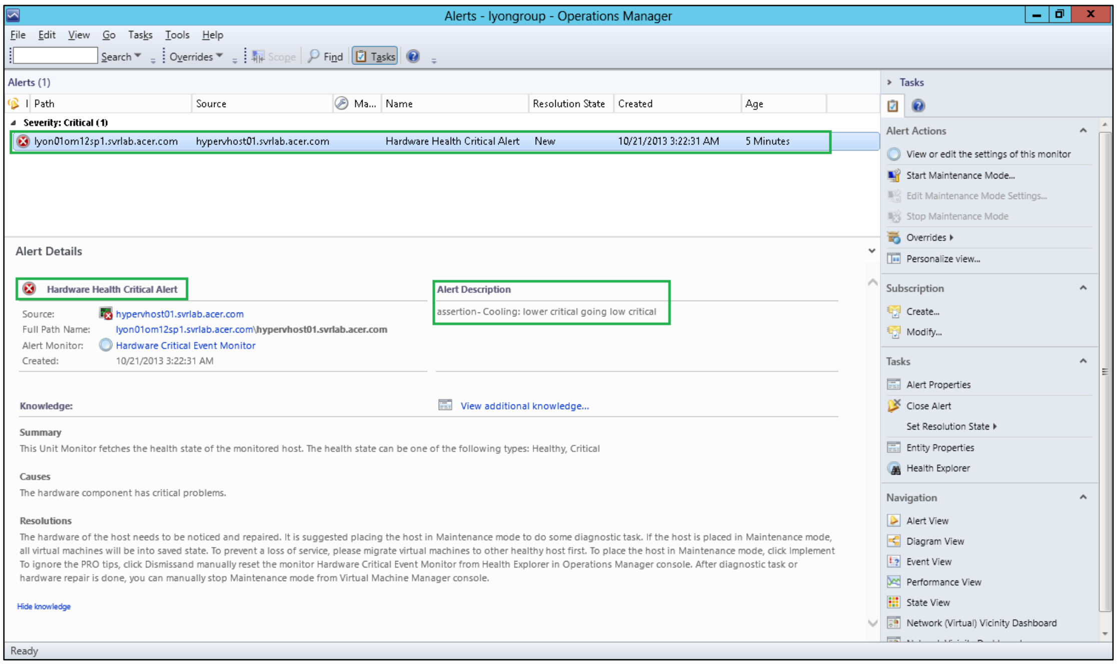
State	Main...	Path	BMC IP Address	Host IP Address	Display Name
Critical		lyon01om12sp1.svrlab.acer.com	192.168.1.23	192.168.1.42	hypervhost01.svrlab.acer.com
Healthy		lyon01om12sp1.svrlab.acer.com	192.168.1.95	192.168.1.10	

Detail View

Acer.Server.OOB.PRO12.Monitored Host properties of hypervhost01.svrlab.acer.com

Display Name	hypervhost01.svrlab.acer.com
Full Path Name	lyon01om12sp1.svrlab.acer.com\hypervhost01.svrlab.acer.com
VMM Server	
Name	hypervhost01.svrlab.acer.com

You can open the *Alert View* for the associated item in the *Acer Server – PRO12* group to see what instigated the status change.



Alerts (1)

I	Path	Source	Ma...	Name	Resolution State	Created	Age
Severity: Critical (1)							
	lyon01om12sp1.svrlab.acer.com	hypervhost01.svrlab.acer.com		Hardware Health Critical Alert	New	10/21/2013 3:22:31 AM	5 Minutes

Alert Details

Hardware Health Critical Alert

Source: hypervhost01.svrlab.acer.com
Full Path Name: lyon01om12sp1.svrlab.acer.com\hypervhost01.svrlab.acer.com
Alert Monitor: Hardware Critical Event Monitor
Created: 10/21/2013 3:22:31 AM

Alert Description
assertion- Cooling: lower critical going low critical

Knowledge: View additional knowledge...

Summary
This Unit Monitor fetches the health state of the monitored host. The health state can be one of the following types: Healthy, Critical

Causes
The hardware component has critical problems.

Resolutions
The hardware of the host needs to be noticed and repaired. It is suggested placing the host in Maintenance mode to do some diagnostic task. If the host is placed in Maintenance mode, all virtual machines will be into saved state. To prevent a loss of service, please migrate virtual machines to other healthy host first. To place the host in Maintenance mode, click Implement To ignore the PRO tips, click Dismissand manually reset the monitor Hardware Critical Event Monitor from Health Explorer in Operations Manager console. After diagnostic task or hardware repair is done, you can manually stop Maintenance mode from Virtual Machine Manager console.

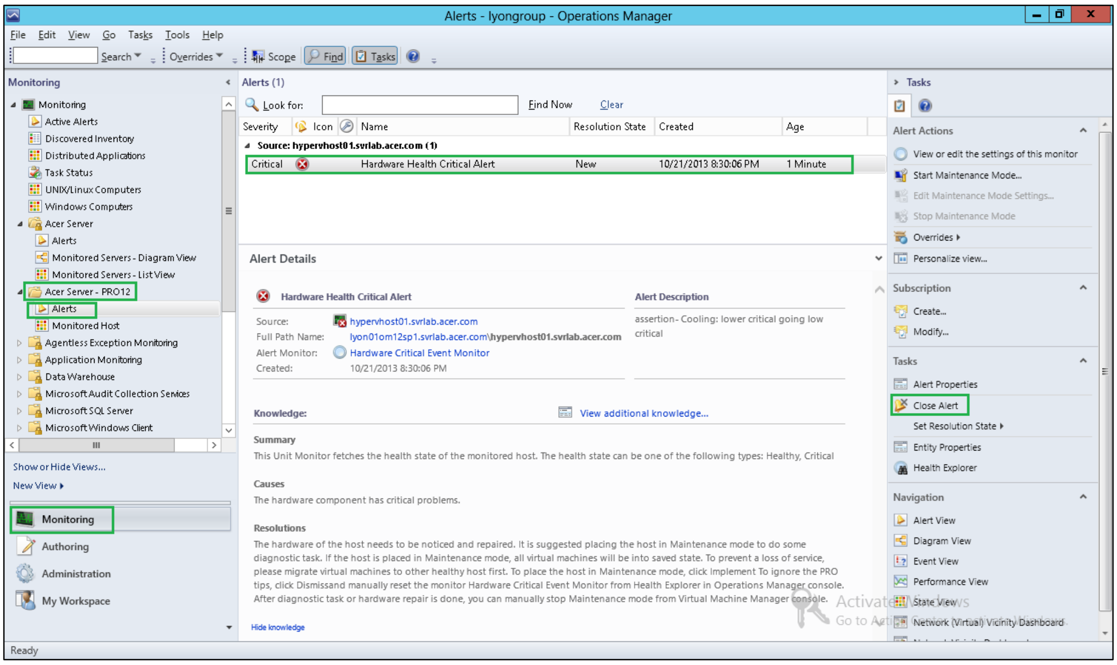
Hide knowledge

Normally, implementing PRO-Tip in the SCVMM Console will close the alerts in *Acer Server – PRO12*, or you can close them manually.

4.24.1. Close alerts manually

Follow the steps below:

1. Open the SCOM Console.
2. Go to **Monitoring** > **Acer Server – PRO12** > **Alerts**.
3. Select the target alert(s).
4. Click **Close Alert** in the right-hand panel.



Severity	Icon	Name	Resolution State	Created	Age
Source: hypervhost01.svrlab.acer.com (1)					
Critical	☒	Hardware Health Critical Alert	New	10/21/2013 8:30:06 PM	1 Minute

Alert Details

Hardware Health Critical Alert

Source: hypervhost01.svrlab.acer.com
Full Path Name: lyon01om12sp1.svrlab.acer.com\hypervhost01.svrlab.acer.com
Alert Monitor: Hardware Critical Event Monitor
Created: 10/21/2013 8:30:06 PM

Alert Description

assertion- Cooling: lower critical going low critical

Knowledge: View additional knowledge...

Summary

This Unit Monitor fetches the health state of the monitored host. The health state can be one of the following types: Healthy, Critical

Causes

The hardware component has critical problems.

Resolutions

The hardware of the host needs to be noticed and repaired. It is suggested placing the host in Maintenance mode to do some diagnostic task. If the host is placed in Maintenance mode, all virtual machines will be into saved state. To prevent a loss of service, please migrate virtual machines to other healthy host first. To place the host in Maintenance mode, click Implement To ignore the PRO tips, click Dismissand manually reset the monitor Hardware Critical Event Monitor from Health Explorer in Operations Manager console. After diagnostic task or hardware repair is done, you can manually stop Maintenance mode from Virtual Machine Manager console.

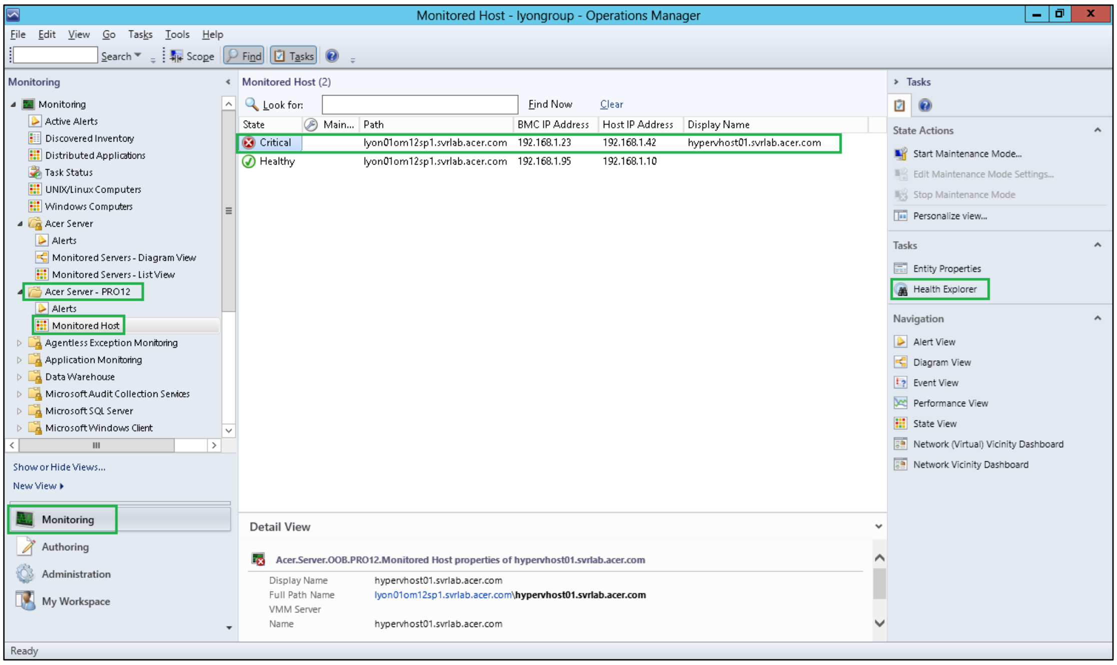
Hide knowledge

4.25. Use *Health Explore* for *Acer Server – PRO12*

Normally, implementing PRO-Tip in the SCVMM Console can reset the health status of associated items in the *Acer Server – PRO12* group, but you may want to reset the health status of associated items for particular cases.

4.25.1. Reset health status manually

1. Open the SCOM Console.
2. Go to **Monitoring** > **Acer Server – PRO12** > **Monitored Host**.
3. Select the target host(s).
4. Click **Health Explore** in the right-hand panel.



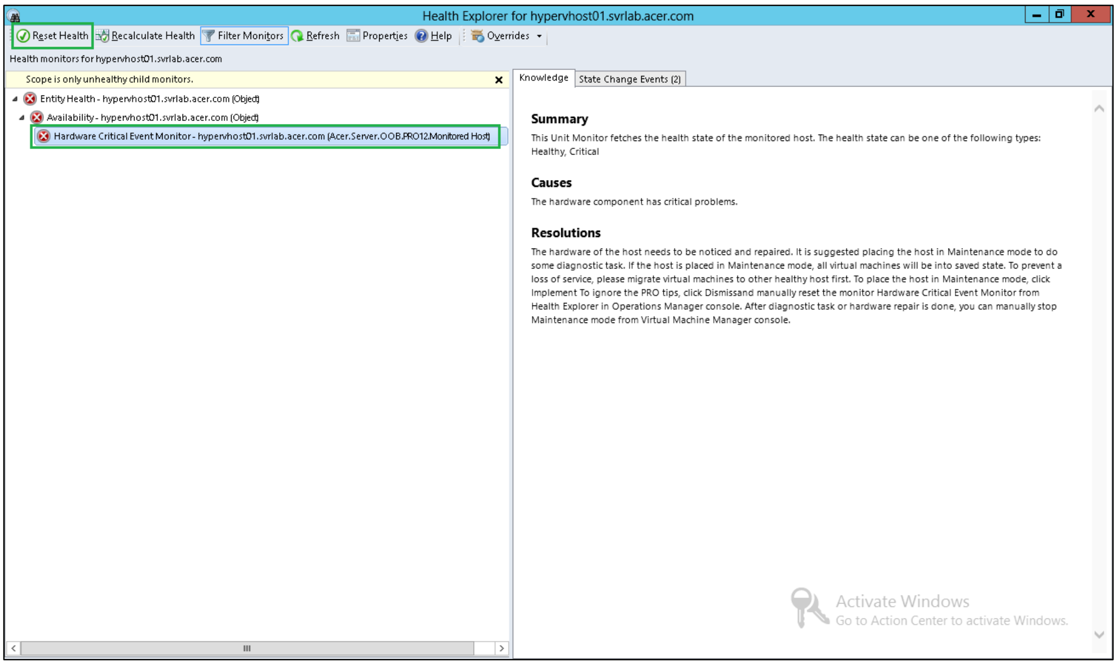
State	Main...	Path	BMC IP Address	Host IP Address	Display Name
Critical		lyon01om12sp1.svrlab.acer.com	192.168.1.23	192.168.1.42	hypervhost01.svrlab.acer.com
Healthy		lyon01om12sp1.svrlab.acer.com	192.168.1.95	192.168.1.10	

Detail View

Acer.Server.OOB.PRO12.Monitored Host properties of hypervhost01.svrlab.acer.com

Display Name	hypervhost01.svrlab.acer.com
Full Path Name	lyon01om12sp1.svrlab.acer.com\hypervhost01.svrlab.acer.com
VMM Server	
Name	hypervhost01.svrlab.acer.com

5. Select the target monitor(s).
6. Click **Reset Health** in the function bar.



Health monitors for hypervhost01.svrlab.acer.com

Scope is only unhealthy child monitors.

- Entity Health - hypervhost01.svrlab.acer.com (Object)
  - Availability - hypervhost01.svrlab.acer.com (Object)
    - Hardware Critical Event Monitor - hypervhost01.svrlab.acer.com (Acer.Server.OOB.PRO12.Monitored Host)

Summary

This Unit Monitor fetches the health state of the monitored host. The health state can be one of the following types: Healthy, Critical

Causes

The hardware component has critical problems.

Resolutions

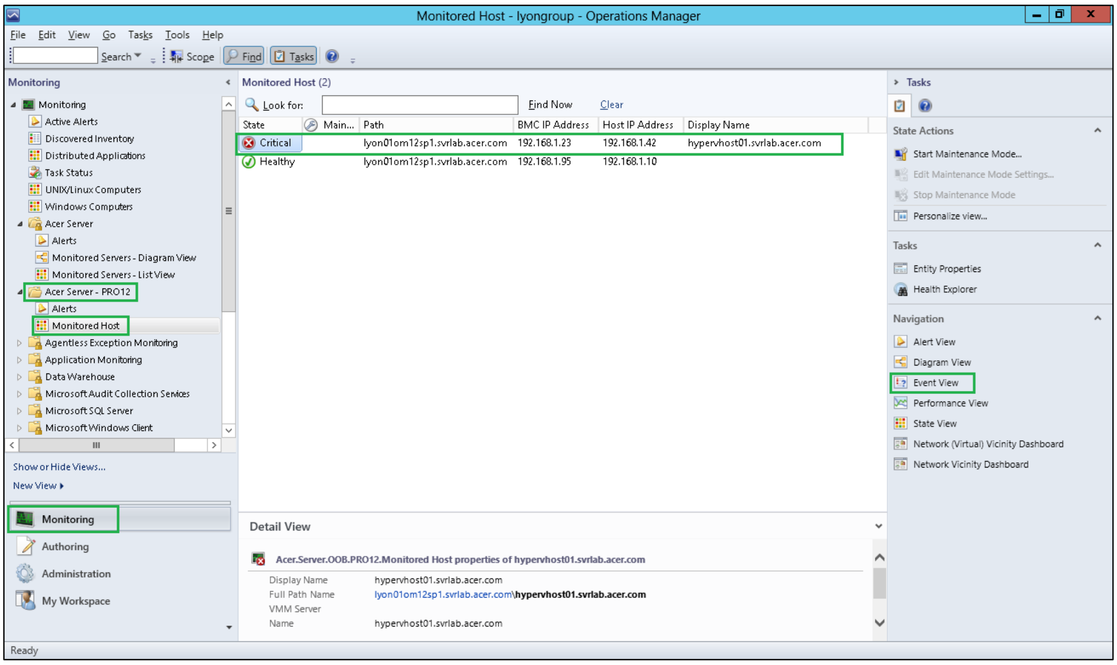
The hardware of the host needs to be noticed and repaired. It is suggested placing the host in Maintenance mode to do some diagnostic task. If the host is placed in Maintenance mode, all virtual machines will be into saved state. To prevent a loss of service, please migrate virtual machines to other healthy host first. To place the host in Maintenance mode, click Implement To ignore the PRO tips, click Dismissand manually reset the monitor Hardware Critical Event Monitor from Health Explorer in Operations Manager console. After diagnostic task or hardware repair is done, you can manually stop Maintenance mode from Virtual Machine Manager console.

4.26. Use *Event View*

You can open *Event View* for a single pair of associated items to see the historical SNMP trap (PET) events.

Follow the steps below:

1. Open the SCOM Console.
2. Go to **Monitoring** > **Acer Server – PRO12** > **Monitored Host**.
3. Select the target host.
4. Click **Event View** in the right-hand panel.



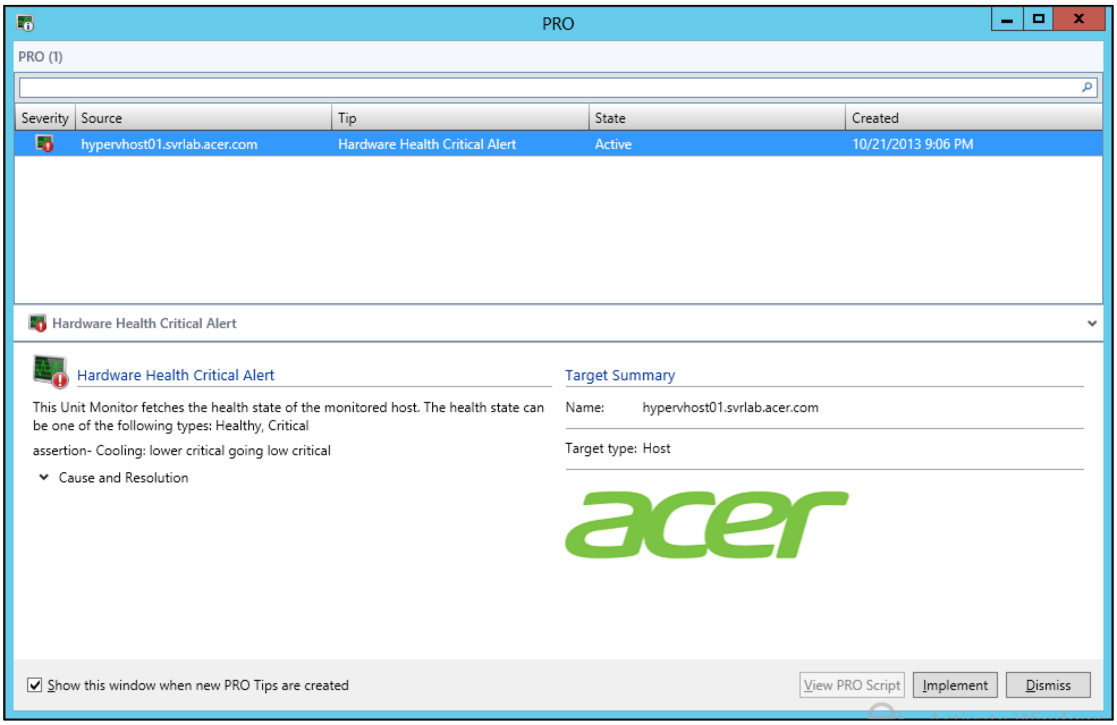
State	Main...	Path	BMC IP Address	Host IP Address	Display Name
Critical		lyon01om12sp1.svrlab.acer.com	192.168.1.23	192.168.1.42	hypervhost01.svrlab.acer.com
Healthy		lyon01om12sp1.svrlab.acer.com	192.168.1.95	192.168.1.10	

Acer.Server.OOB.PRO12.Monitored Host properties of hypervhost01.svrlab.acer.com

Display Name hypervhost01.svrlab.acer.com
Full Path Name lyon01om12sp1.svrlab.acer.com**hypervhost01.svrlab.acer.com**
VMM Server
Name hypervhost01.svrlab.acer.com

4.27. View PRO-Tips in SCVMM

When health status of an associated item changes to *warning* or *critical* from *good*, or changes to *critical* from *warning*, an alert will be generated in *Alert View* for the *Acer Server – PRO12* group, and a PRO-Tip will appear in the SCVMM *PRO* window. You can log into the SCVMM Console to see the *PRO* window.



Severity	Source	Tip	State	Created
	hypervhost01.svrlab.acer.com	Hardware Health Critical Alert	Active	10/21/2013 9:06 PM

Hardware Health Critical Alert

This Unit Monitor fetches the health state of the monitored host. The health state can be one of the following types: Healthy, Critical

assertion- Cooling: lower critical going low critical

Cause and Resolution

Target Summary

Name: hypervhost01.svrlab.acer.com

Target type: Host

☑ Show this window when new PRO Tips are created

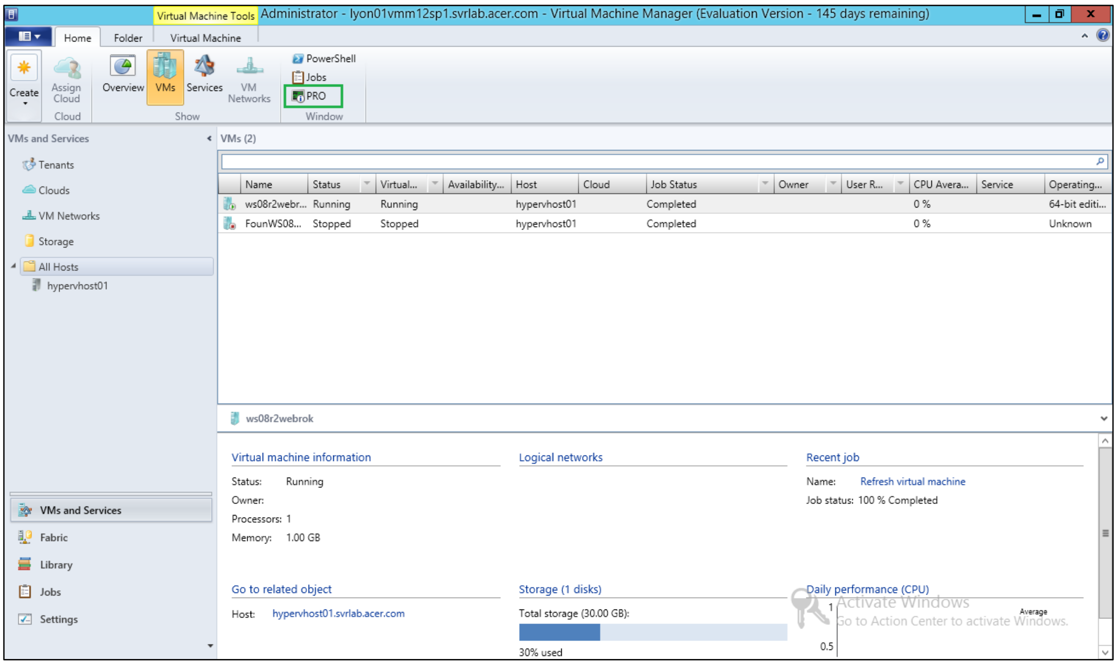
4.28. Implement PRO-Tips on SCVMM

Log into the SCVMM Console. When a PRO-Tip appears in the SCVMM *PRO*, it means an issue has been detected on one or more Acer servers. You can decide to **Implement** or **Dismiss** the PRO-Tip.

Implementing the PRO-Tip will put the hypervisor into maintenance mode; dismissing the PRO-Tip will ignore it and no action will be taken.

Follow the steps below to implement a PRO-Tip:

1. Open the SCVMM Console.
2. Click **PRO** in the top panel.



Name	Status	Virtual...	Availability...	Host	Cloud	Job Status	Owner	User R...	CPU Avera...	Service	Operating...
ws08r2webr...	Running	Running		hypervhost01		Completed			0 %		64-bit editi...
FounWS08...	Stopped	Stopped		hypervhost01		Completed			0 %		Unknown

ws08r2webrok

Virtual machine information
Status: Running
Owner:
Processors: 1
Memory: 1.00 GB

Logical networks

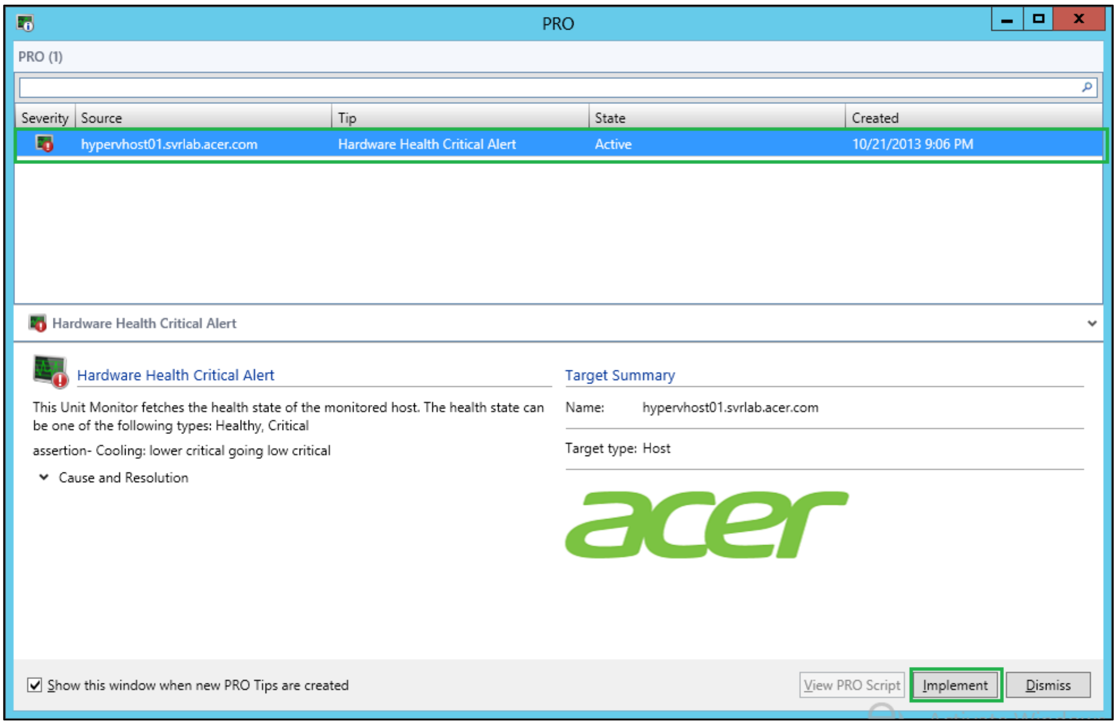
Recent job
Name: Refresh virtual machine
Job status: 100 % Completed

Go to related object
Host: hypervhost01.svrlab.acer.com

Storage (1 disks)
Total storage (30.00 GB):
30% used

Daily performance (CPU)

3. Select the target PRO-Tip.
4. Click **Implement** at the bottom.



Severity	Source	Tip	State	Created
	hypervhost01.svrlab.acer.com	Hardware Health Critical Alert	Active	10/21/2013 9:06 PM

Hardware Health Critical Alert

This Unit Monitor fetches the health state of the monitored host. The health state can be one of the following types: Healthy, Critical

assertion- Cooling: lower critical going low critical

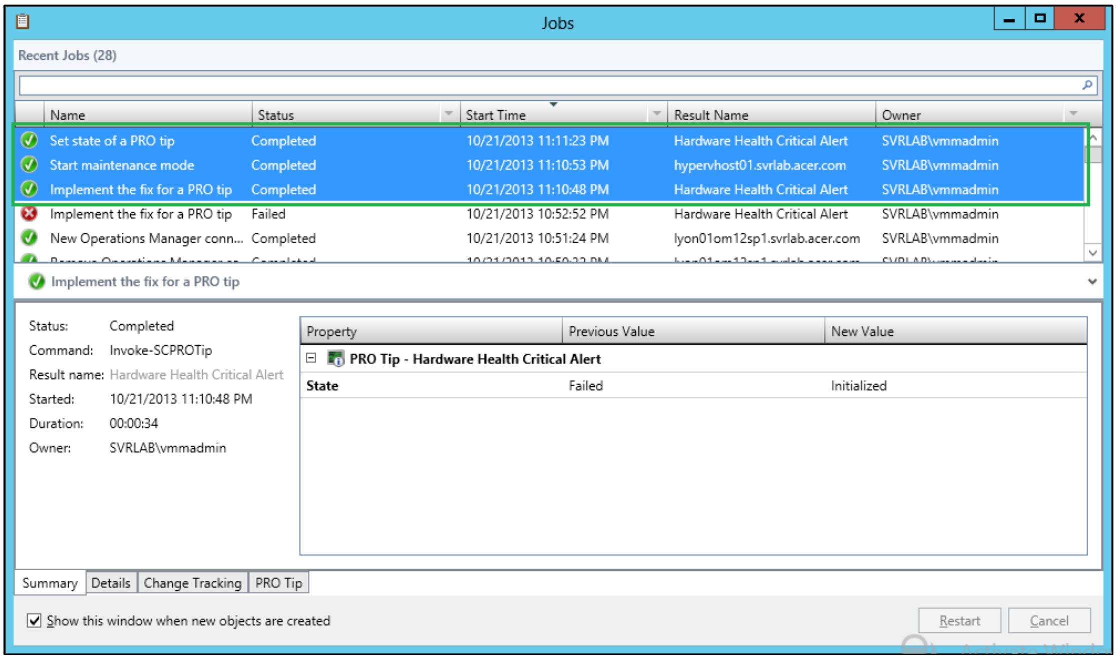
Target Summary

Name: hypervhost01.svrlab.acer.com

Target type: Host

☑ Show this window when new PRO Tips are created

5. Open the *Jobs* window.
6. The jobs *Implement the fix for a PRO-Tip*, *Start maintenance mode* and *Set state of a PRO-Tip* run sequentially.



Name	Status	Start Time	Result Name	Owner
Set state of a PRO tip	Completed	10/21/2013 11:11:23 PM	Hardware Health Critical Alert	SVRLAB\vmmadmin
Start maintenance mode	Completed	10/21/2013 11:10:53 PM	hypervhost01.svrlab.acer.com	SVRLAB\vmmadmin
Implement the fix for a PRO tip	Completed	10/21/2013 11:10:48 PM	Hardware Health Critical Alert	SVRLAB\vmmadmin
Implement the fix for a PRO tip	Failed	10/21/2013 10:52:52 PM	Hardware Health Critical Alert	SVRLAB\vmmadmin
New Operations Manager conn...	Completed	10/21/2013 10:51:24 PM	lyon01om12sp1.svrlab.acer.com	SVRLAB\vmmadmin
Remove Operations Manager co...	Completed	10/21/2013 10:50:22 PM	lyon01om12sp1.svrlab.acer.com	SVRLAB\vmmadmin

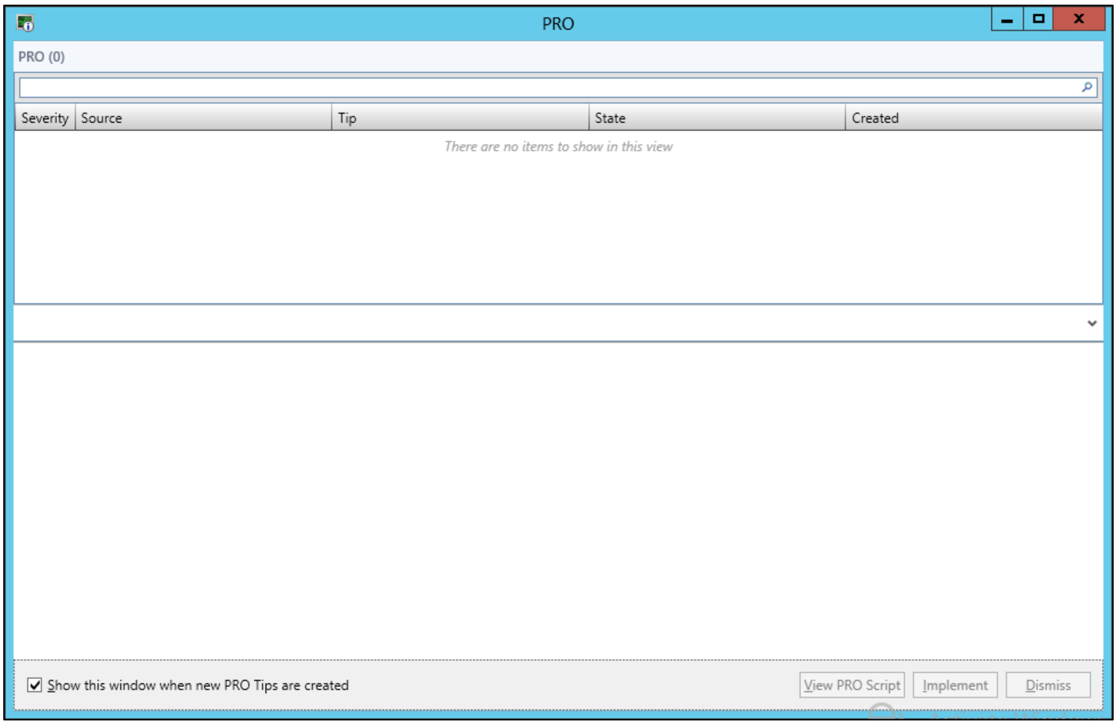
Implement the fix for a PRO tip

Status: Completed
Command: Invoke-SCPROTip
Result name: Hardware Health Critical Alert
Started: 10/21/2013 11:10:48 PM
Duration: 00:00:34
Owner: SVRLAB\vmmadmin

Property	Previous Value	New Value
⊟ PRO Tip - Hardware Health Critical Alert		
State	Failed	Initialized

☑ Show this window when new objects are created

7. The implemented PRO-Tip will be deleted after the jobs are complete.


PRO

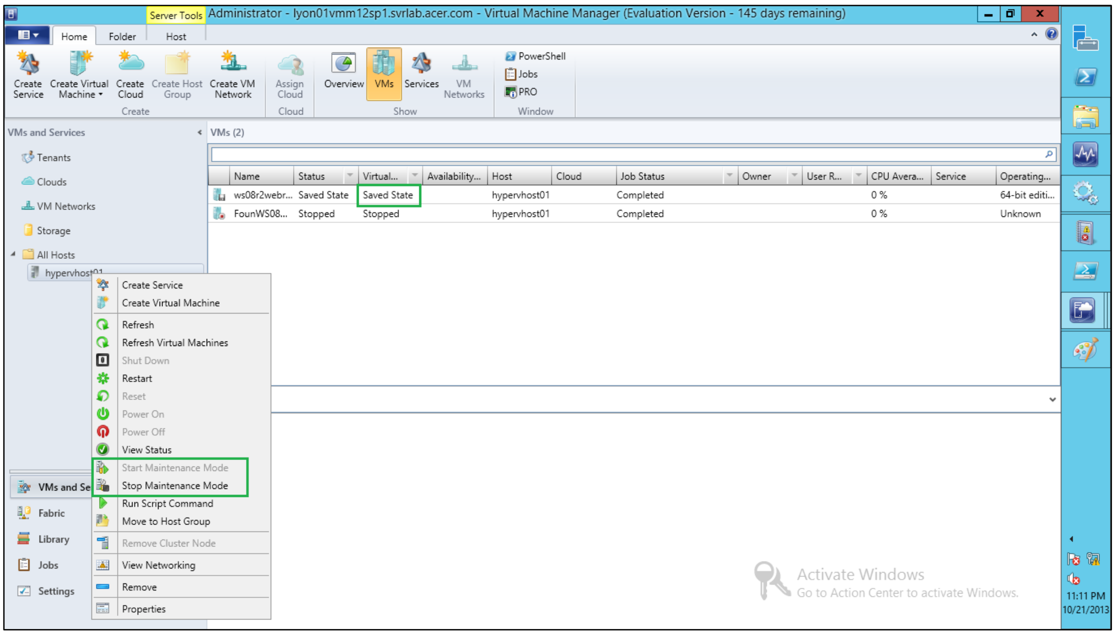
PRO (0)

Severity	Source	Tip	State	Created

There are no items to show in this view

☑ Show this window when new PRO Tips are created

8. The most will be put into maintenance mode.


Administrator - lyon01vmm12sp1.svrlab.acer.com - Virtual Machine Manager (Evaluation Version - 145 days remaining)

VMs (2)

	Name	Status	Virtual...	Availability...	Host	Cloud	Job Status	Owner	User R...	CPU Avera...	Service	Operating...
	ws08r2webr...	Saved State	Saved State		hypervhost01		Completed			0 %		64-bit editi...
	FounWS08...	Stopped	Stopped		hypervhost01		Completed			0 %		Unknown

Scenario 5: Generate PRO-Tips for RAID on Acer servers

4.29. Import *Acer.Server.OOB.PRO12.xml*

The procedure is the same as 4.19.

4.30. Associate hypervisors with Acer servers

The procedure is the same as 4.20.

4.31. Monitor associations in the SCOM UI

The procedure is the same as 4.21.

4.32. Process RAID SNMP traps for PRO-Tips

When SCOM's built-in SNMP trap listener receives a RAID SNMP trap, SCOM examines the source IP address of the SNMP trap according to the rules defined in *Acer.Server.OOB.PRO12.xml*. Only LSI, Adaptec and Promise RAID SNMP traps and events from Acer servers will be processed.

4.33. Use *Alert View* for *Acer Server – PRO12*

At the beginning, the health status of associated items is always *good* or *healthy* in the *Acer Server – PRO12* group, no matter what health status of the RAID on the servers actually is.

As time passes, the parsed RAID SNMP traps' health status may change to *warning* or *critical*. When the health statue of an item changes to *warning* or *critical* from *good*, or changes to *critical* from *warning*, an alert will be generated in the *Alert View* for the *Acer Server – PRO12* group.

You can open the *Alert View* of the associated items in the *Acer Server – PRO12* group to see what instigated the status change. Normally implementing the PRO-Tips from the SCVMM Console will close the alert, or you can close them manually by following the steps in 4.24.1.

4.34. Use *Health Explore* for *Acer Server – PRO12*

The procedure is the same as 4.25.

4.35. No event(s) in *Event View*

There are no RAID events shown in *Event View* for the *Acer Server – PRO12* group.

4.36. View PRO-Tips in SCVMM

The procedure is the same as 4.27.

4.37. Implement PRO-Tip on SCVMM

The procedure is the same as 4.28

Smart Cloud Integration Pack

For System Center Operation Manager

v1.1.0

Installation Guide

Table of Contents

About this guide

This User’s Guide provides a description of the features, installation, and use of the Acer Smart Integration Pack for Microsoft® System Center. It is intended to help system administrators to efficiently monitor and manage Acer servers.

Only persons with detailed knowledge of and experience with Microsoft® System Center should attempt this installation, potential for data corruption and/or loss exists in this User's Guide’s procedures.

1. INTRODUCTION

This document shows you how to install Acer Smart Cloud Integration Pack (SCIP) in an SCOM environment. Contents cover the environment requirements, supported operating systems, supported SCOM, prerequisites and related settings.

Acer SCIP is a software product provided by Acer to integrate manageability for Acer servers with Microsoft System Center Operation Manager. With Acer SCIP, SCOM can monitor SNMP traps from Acer servers, RAID SNMP traps from the RAID management software on Acer servers. The facility to generate PRO-Tips in the SCVMM console is optional.

2. MICROSOFT SYSTEM CENTER OPERATION MANAGER DEPLOYMENT

This chapter includes parts or articles from the *Deploying System Center 2012 – Operations Manager* document from Microsoft. Detailed steps and complete information can be found in the original document.

2.1. Single-server deployment

The single-server management group scenario combines all the management group roles that can coexist into a single instance of the Windows Server operating system running as a member server in an Active Directory domain. This instance can be on dedicated hardware or on a virtual machine.

The Operations console can be deployed to computers other than the single server, and the web console is accessed via a browser. Agents are then typically deployed to a limited number of devices depending on the capacity of the server that System Center 2012 – Operations Manager is deployed on.

You deploy Operations Manager in a single-server management group when you want to use it for evaluation, testing, and management pack development, usually in nonproduction or preproduction environments.

2.2. Distributed deployment

The distributed management group installation will form the foundation of 99 percent of Operations Manager deployments. It allows for the distribution of features and services across multiple servers to allow for scalability. It can include all Operations Manager server roles and supports the monitoring of devices across trust boundaries through the use of a gateway server.

3. PREREQUISITES

To run Acer SCIP properly requires some advance setup. This chapter describes those prerequisites in detail. Before installing Acer SCIP, you should read this chapter carefully.

3.1. Software installation requirements

3.1.1. SCOM, SCVMM

You need to deploy SCOM and get it ready before installing Acer SCIP. Please refer to the *Deploying System Center 2012 – Operations Manager* document from Microsoft.

- Supported System Center families
  - Microsoft System Center 2012 R2 Operations Manager / Microsoft System Center Virtual Machine Manager 2012 R2
  - Microsoft System Center 2012 SP1 Operations Manager / Microsoft System Center Virtual Machine Manager 2012 SP1
- Supported operating systems
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows Server 2012

Please refer to: http://technet.microsoft.com/en-us/library/hh457006.aspx

3.1.2. Microsoft SQL Server 2012

You need to deploy the SQL server and get it ready before installing Acer SCIP. Please refer to *Install SQL Server 2012* from Microsoft.

Additionally, it is necessary to configure the following manually:

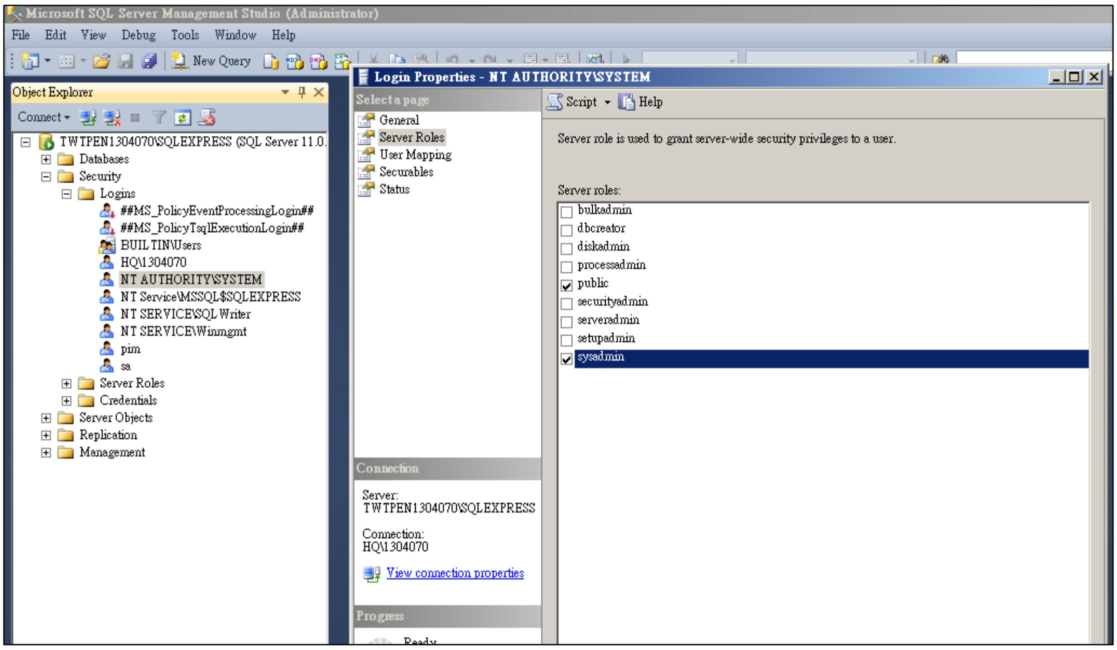
3.1.2.1. Add the *sysadmin* role to the SQL Server

- After installing SCOM and Microsoft SQL Server, you need to add the *sysadmin* role to NT AUTHORITY\SYSTEM in *Microsoft SQL Logins*. This allows the SCIP Integration Service to access the SQL Server.

  Step 1. Open **Microsoft SQL Server Management Studio** > choose the target SQLSERVER instance > **Security** > **Logins** > **NT AUTHORITY\SYSTEM**

  Step 2. Open the NT AUTHORITY\SYSTEM properties

  Step 3. Log into **Properties** > **Server Roles** > check **sysadmin** and save.



Server: TWTPEN1304070\SQLEXPRESS

Connection: HQ\1304070

Server role is used to grant server-wide security privileges to a user.

Server roles:

- □ bulkadmin
- □ dbcreator
- □ diskadmin
- □ processadmin
- ☑ public
- □ securityadmin
- □ serveradmin
- □ setupadmin
- ☑ sysadmin

3.1.2.2. Create a new user to log into the SQL server

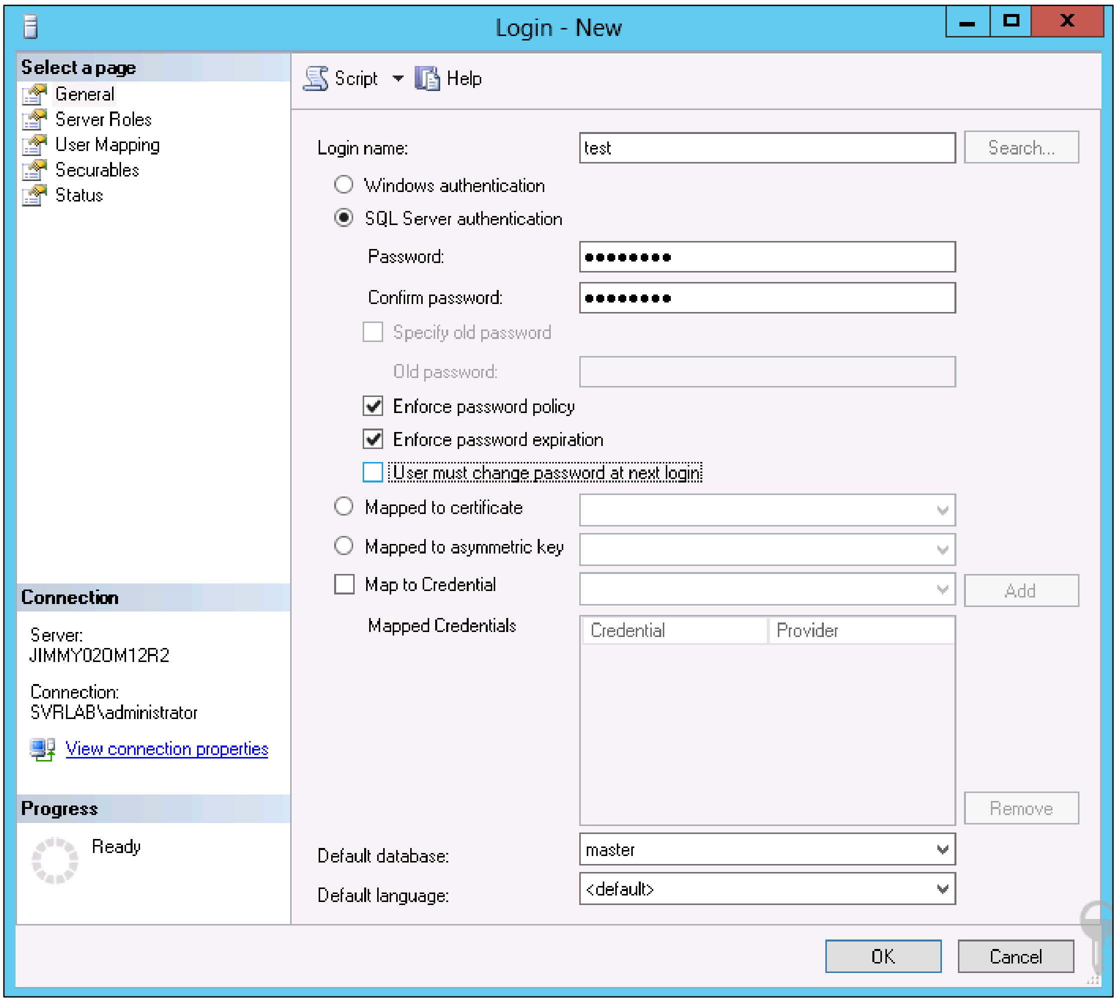
You need to create a group account and password, so that Acer SCIP can use a pre-created user to communicate with the SQL server. If the login information is not correct, Acer SCIP cannot be installed.

To create the new login:

Step 1. Open SQL Server 2012

Step 2. Right-click on **Security/Logins** > **New Login…**

Step 3. Enter the *Login name*, select the radio button for *SQL Server authentication*. Enter the *Password* and *Confirm password* and uncheck *User must change password at next login*.



Login name: test

○ Windows authentication

● SQL Server authentication

Password: ••••••••

Confirm password: ••••••••

□ Specify old password

Old password:

☑ Enforce password policy

☑ Enforce password expiration

□ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

□ Map to Credential

Mapped Credentials

Credential	Provider

Default database: master

Default language: <default>

Connection

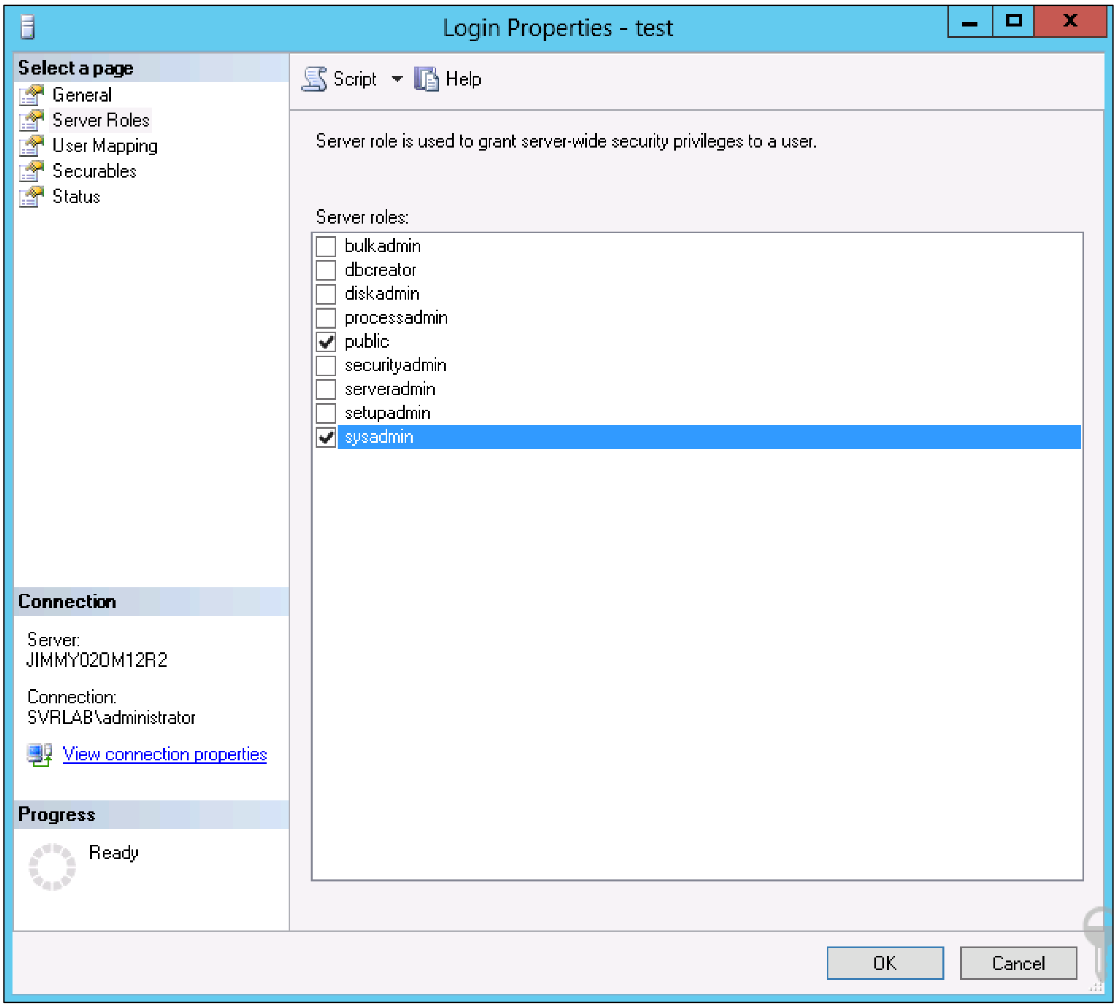
Server:
JIMMY020M12R2

Connection:
SVRLAB\administrator

Progress

Ready

Step 4. Select **Server Roles** and check *Sysadmin*, click **OK**.



Server role is used to grant server-wide security privileges to a user.

Server roles:

□ bulkadmin
□ dbcreator
□ diskadmin
□ processadmin
☑ public
□ securityadmin
□ serveradmin
□ setupadmin
☑ sysadmin

Server:
JIMMY020M12R2

Connection:
SVRLAB\administrator

Note: To check whether this user is valid or not, you can exit and re-open the SQL server console using the information you just entered.

3.1.2.3. Configure fixed TCP port for listening

Acer SCIP support Single-Server / Distributed Deployment architecture, so Microsoft SQL Server will be set a specific and fixed port for listening incoming connections. If not to do, Acer SCIP might connect to remote Microsoft SQL Server so that Acer PIM Service is fail.

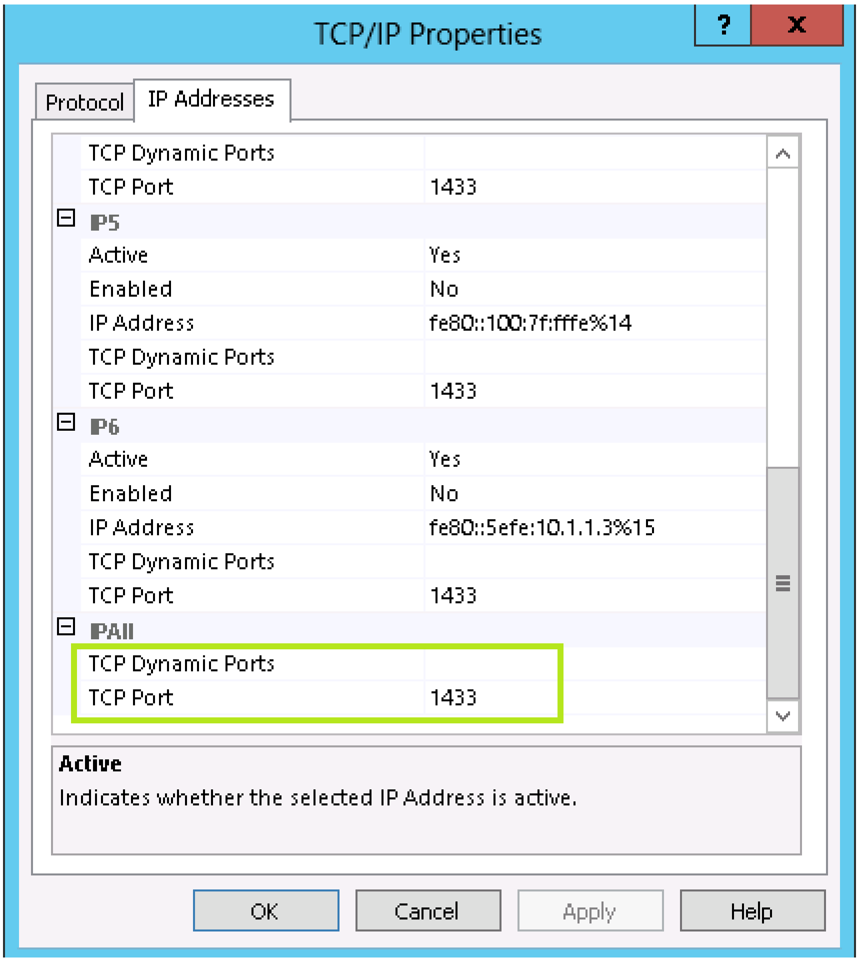
Steps to configure:

Step 1. Click “Start” -> enter metro mode -> select “SQL Server Configuration Manager” and click

Step 2. Select “Protocols for [**instance name** user created]” -> Select Protocol Name is “TCP/IP” and double click

Step 3. Select IP Address panel -> configure “IPALL” group setting -> clear TCP Dynamic Ports -> type port number “1433” into TCP Port

Step 4. Click “Apply” -> click “OK”.



TCP Dynamic Ports	
TCP Port	1433
⊟ **IP5**	
Active	Yes
Enabled	No
IP Address	fe80::100:7f:fffe%14
TCP Dynamic Ports	
TCP Port	1433
⊟ **IP6**	
Active	Yes
Enabled	No
IP Address	fe80::5efe:10.1.1.3%15
TCP Dynamic Ports	
TCP Port	1433
⊟ **IPAll**	
TCP Dynamic Ports	
TCP Port	1433

Active

Indicates whether the selected IP Address is active.

Note: It’s suggestion for restarting SQL Server service after configuring.

3.1.3. Download and install Python 2.7.x 32-bit for Windows

Acer Integration Service was developed using python, and you need to download and install python 2.7.x 32-bit (x86) for Windows. Python can be downloaded from http://www.python.org/getit/

Note: Follow the standard Windows install procedure for python 2.7.x.

3.1.4. Install pyodbc-3.0.7.win32-py2.7.exe for Windows

Download and install the Python ODBC module *pyodbc-3.0.7.win32-py2.7.exe* for Windows. Pyodbc for Windows can be downloaded from https://code.google.com/p/pyodbc/downloads/list

Ensure you install the pyodbc module after installing Python 2.7.x.

Note: Follow the standard Windows install procedure for pyodbc.

3.1.5. Download and install Python Launcher for Windows

Download and install Python Launcher for Windows 32-bit (launchwin.msi). It can be found from https://bitbucket.org/vinay.sajip/pylauncher/downloads

Note: Follow the standard Windows install procedure for the launcher.

3.2. Firewall policy requirements

Check and open following firewall ports on Windows:

- UDP 162 (Operation Manager SNMP Trap listener)
- TCP 9898 (for Acer SCIP RESTfull communication)
- UDP 51622 (for forwarding SNMP Traps to Acer SCIP)

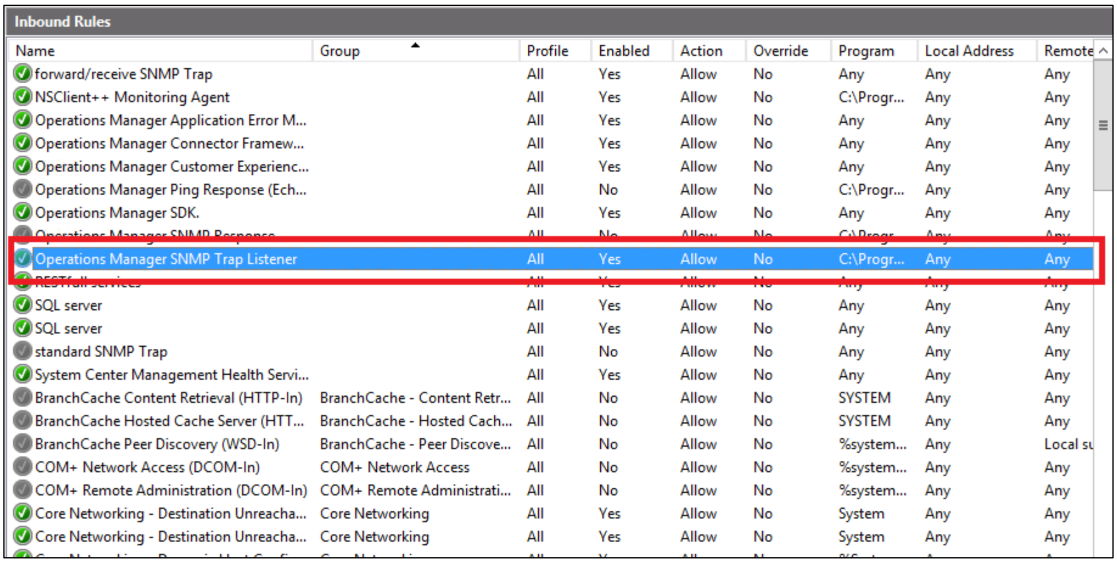
3.2.1 Enable the Operations Manager SNMP Trap Listener rule

SCOM has a built-in SNMP Trap listener and this rule must be enabled in order for SCOM to receive SNMP traps (PET) from Acer servers.

To enable the rule, follow the steps below:

Step 1. Open the Windows **Control Panel** on the server > **System and Security** > **Windows Firewall** > **Advanced settings** > **Inbound Rules**.

Step 2. Right-click on the *Operations Manager SNMP Trap Listener* rule, then **Enable** it.



Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote
✓ forward/receive SNMP Trap		All	Yes	Allow	No	Any	Any	Any
✓ NSClient++ Monitoring Agent		All	Yes	Allow	No	C:\Progr...	Any	Any
✓ Operations Manager Application Error M...		All	Yes	Allow	No	Any	Any	Any
✓ Operations Manager Connector Framew...		All	Yes	Allow	No	Any	Any	Any
✓ Operations Manager Customer Experienc...		All	Yes	Allow	No	Any	Any	Any
Operations Manager Ping Response (Ech...		All	No	Allow	No	C:\Progr...	Any	Any
✓ Operations Manager SDK.		All	Yes	Allow	No	Any	Any	Any
Operations Manager SNMP Response		All	No	Allow	No	C:\Progr...	Any	Any
✓ Operations Manager SNMP Trap Listener		All	Yes	Allow	No	C:\Progr...	Any	Any
✓ RESTfull services		All	Yes	Allow	No	Any	Any	Any
✓ SQL server		All	Yes	Allow	No	Any	Any	Any
✓ SQL server		All	Yes	Allow	No	Any	Any	Any
standard SNMP Trap		All	No	Allow	No	Any	Any	Any
✓ System Center Management Health Servi...		All	Yes	Allow	No	Any	Any	Any
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow	No	SYSTEM	Any	Any
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allow	No	SYSTEM	Any	Any
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow	No	%system...	Any	Local su
COM+ Network Access (DCOM-In)	COM+ Network Access	All	No	Allow	No	%system...	Any	Any
COM+ Remote Administration (DCOM-In)	COM+ Remote Administrati...	All	No	Allow	No	%system...	Any	Any
✓ Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow	No	System	Any	Any
✓ Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow	No	System	Any	Any

3.2.2 *Create new rule – TCP 9898*

Acer Integration Manager UI uses TCP port 9898 to communicate with the Acer Integration Service.

To create the rule allowing this, follow the steps below:

Step 1. Open **Control Panel** > **System and Security** > **Windows Firewall** > **Advanced settings** > right-click on **Inbound Rules** > **New Rule…**

Step 2. Select **Port** and click **Next**.

Step 3. Select **TCP** > **Specific local ports:**

Step 4. Enter **9898** in the text box and click **Next**.

Step 5. Select **Allow the connection**.

Step 6. Mark the **Domain** and click **Next**.

Step 7. Give it a name, such as *TCP 9898 for Acer SCIP*, and click **Finish**.

3.2.3 *Create new rule – UDP 51622*

When SCOM's built-in SNMP Trap listener receives an SNMP trap from an Acer server, Acer's MP will forward the SNMP trap to the local UDP 51622 port, which is monitored by the integration service.

To create the rule:

Step 1. Open **Control Panel** > **System and Security** > **Windows Firewall** > **Advanced settings** > right-click on **Inbound Rules** > **New rule…**

Step 2. Select **Port** and click **Next**.

Step 3. Select **UDP** > **Specific local ports:**

Step 4. Enter **51622** in the text box and click **Next**.

Step 5. Select **Allow the connection**.

Step 6. Mark the **Domain** and click **Next**.

Step 7. Give it a name, such as *UDP 51622 for Acer SCIP*, and click **Finish**.

3.2.4 Create new rule – TCP 1433

SQL Server is a Winsock application that uses sockets network library, through TCP/IP communications. SQL Server listens for incoming connections on a specific port, and the default port for SQL Server is 1433.

To create the rule allowing this, follow the steps below:

Step 1. Open **Control Panel** > **System and Security** > **Windows Firewall** > **Advanced settings** > right-click on **Inbound Rules** > **New rule…**

Step 2. Select **Port** and click **Next**.

Step 3. Select **TCP** > **Specific local ports:**

Step 4. Enter **1433** in the text box and click **Next**.

Step 5. Select **Allow the connection**.

Step 6. Mark the **Domain** and click **Next**.

Step 7. Give it a name, such as *TCP 1433 for Microsoft SQL Server*, and click **Finish**.

3.3. Runtime environment requirements

3.3.1. Add python installation path to Windows environment variable

Steps to add environment variable:

Step 1. Open **Control Panel** > **System and Security** > **System** > **Advanced system settings** > **Advanced** > **Environment Variables**

Step 2. Select **System Variables** > **Path**, and click **Edit**.

Step 3. Add **python installation path** to *Variable Value*.

Note:

1. When you change a system environment variable, it usually requires rebooting the system to take effect.
2. About typing "**python installation path**", please **omitting** the last backslash. (Whether there is or not, meaning of the expression is the same.

3.3.2. Check the Windows .NET Framework

Ensure the following .NET framework version is installed:

- NET framework 4.5 on Windows Server 2012 R2
- NET framework 4.5 on Windows Server 2012

By default, .NET framework 4.5 is installed when Windows Server 2012 or 2012 R2 is installed.

3.3.3. Check Windows PowerShell

Ensure the following Power Shell version is installed:

- PowerShell 4.0 on Windows Server 2012 R2
- PowerShell 3.0 on Windows Server 2012

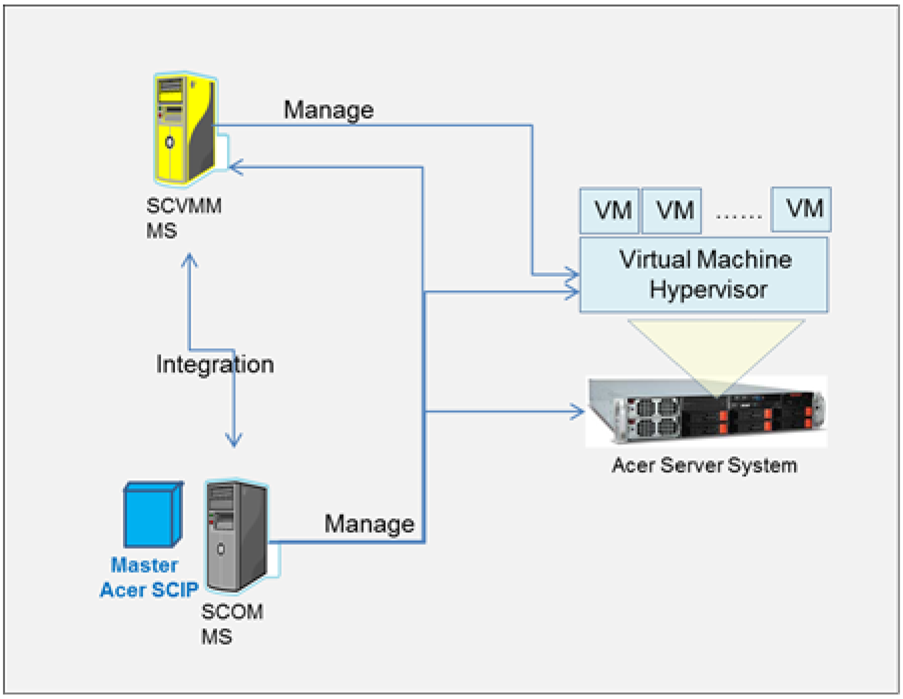
By default, PowerShell 4.0 is installed when Windows Server 2012 R2 is installed. PowerShell 3.0 is installed when Windows Server 2012 is installed.

3.3.4. Set up monitoring for Acer servers

Acer SCIP discovers and manages IPMI-BMC embedded in Acer servers. Acer SCIP and SCOM can also receive and parse SNMP Traps (RAID) from RAID Management Software on Acer servers. Please refer to your Acer server User's Guide to ensure the RJ45 network cables are correctly fitted to allow network access of the IPMI-BMC and that the operating system can communicate with SCOM.

3.3.5. *Set up Acer SCIP, SCOM and SCVMM for PRO-Tips*

To use PRO-Tips, you need to integrate the SCOM Management Server (MS) with SCVMM MS and import *Acer.Server.OOB.PRO12.xml* into the SCOM MS.

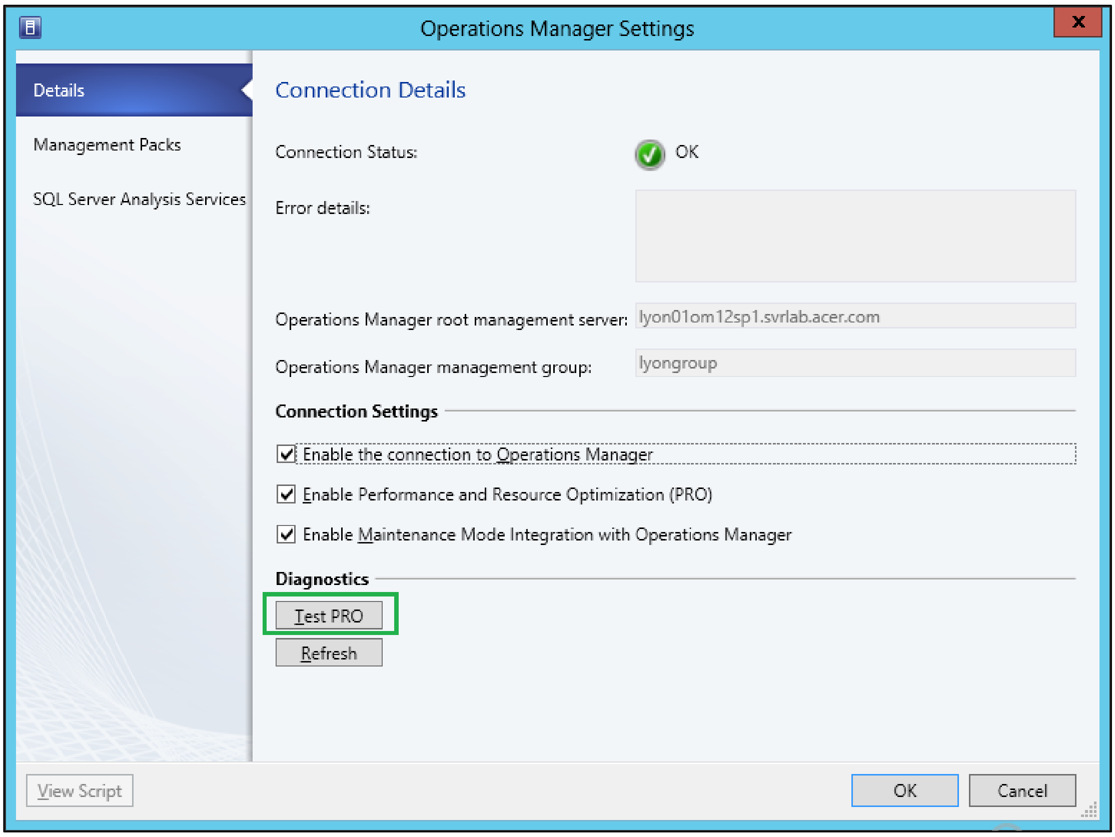


To integrate the SCOM Management Server with the SCVMM Management Server, please refer to http://technet.microsoft.com/en-us/library/hh427287.aspx. Please follow the steps in this referenced document carefully. If the integration between SCOM MS and SCVMM MS is not correct, the PRO-Tip function will not work.

Notes:

You need to:

- Run SCOM to discover SCVMM and Virtual Machine Hosts, then install the SCOM agent on the SCVMM and Virtual Machine Hosts. In **Administration - > Device Management > Agent Managed** of the SCOM Console, the SCVMM and VM Hosts must be listed and have "good" health.
- Install the SCOM Console on the SCVMM Management Server.
- Configure **Settings > System Center Settings > Operation Manager Server > Properties** of the SCVMM Console, and try **Diagnostics > Test RPO**. If this function works correctly, then the integration is complete.



Connection Details

Connection Status: ✓ OK

Error details:

Operations Manager root management server: lyon01om12sp1.svrlab.acer.com

Operations Manager management group: lyongroup

Connection Settings

☑ Enable the connection to Operations Manager

☑ Enable Performance and Resource Optimization (PRO)

☑ Enable Maintenance Mode Integration with Operations Manager

Diagnostics

In the SCOM Console, fully import *Acer.Server.OOB.PRO12.xml.*

3.4. Requirements for monitored servers

3.4.1. Setup RAID management software for RAID monitoring

RAID is monitored by the RAID vendor's Management Software. Therefore, RAID Management Software must be installed and configured in advance in order to send out the SNMP Traps (RAID) to SCOM. Only LSI, Adaptec and Promise RAID SNMP Traps are supported by Acer SCIP.

Follow concept below to install and setup RAID Management Software:

Step 1. Install correct RAID Management Software on OS running on Acer servers

Step 2. Install and enable SNMP service of OS running on Acer servers

Step 3. Set SCOM's IP address as one of trap destination of SNMP service.

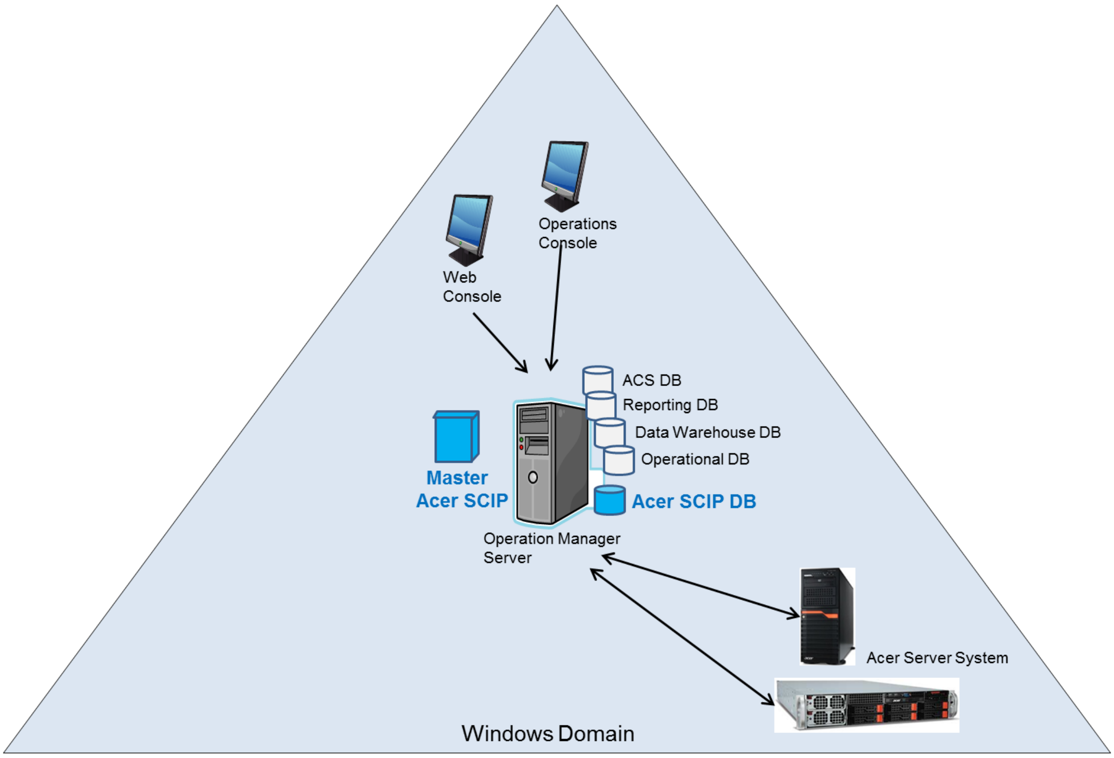
Please refer to Appendix 6.1.

4. INSTALL ACER SCIP

This chapter guides you through installing Acer SCIP and setting up the required environment.

4.1. Install the Master Acer SCIP in a single-server deployment

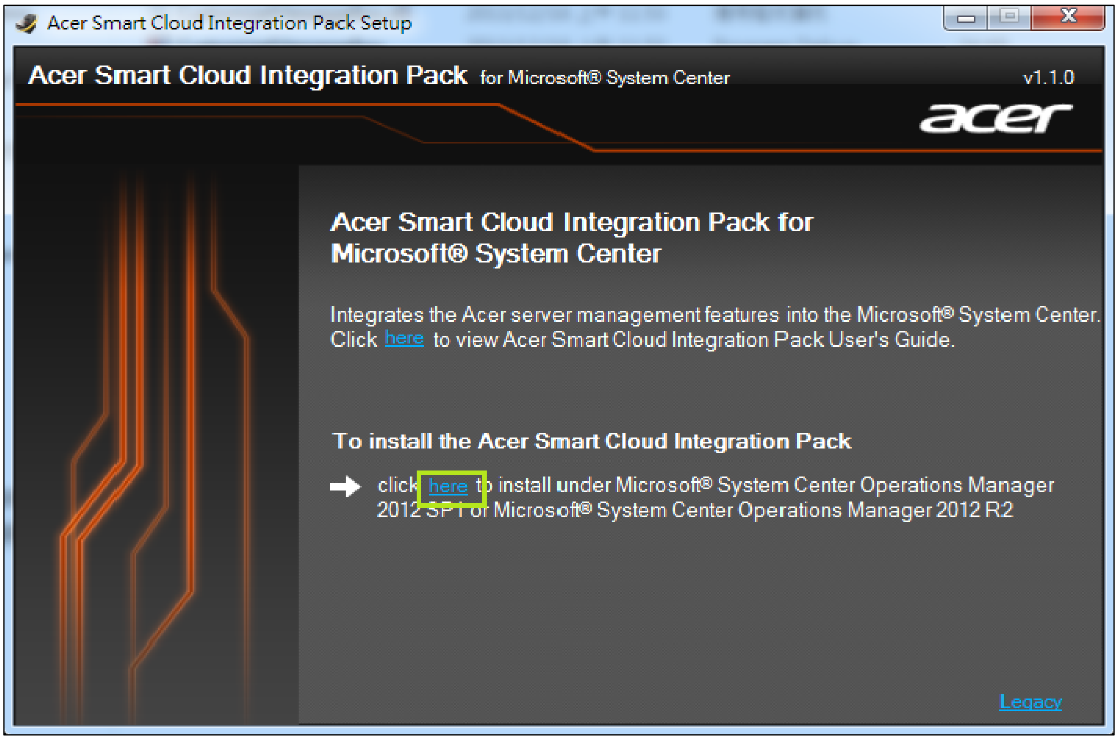
For single-server deployment install the Master Acer SCIP on the Operations Manager Server, as illustrated below.



Installing the Master Acer SCIP:

Step 1. Double-click **Setup.exe** in the Acer SCIP installation folder.

Step 2. Click **here** to install Acer SCIP for SCOM 2012 SP1 or 2012 R2.


Acer Smart Cloud Integration Pack Setup
Acer Smart Cloud Integration Pack for Microsoft® System Center
v1.1.0
acer

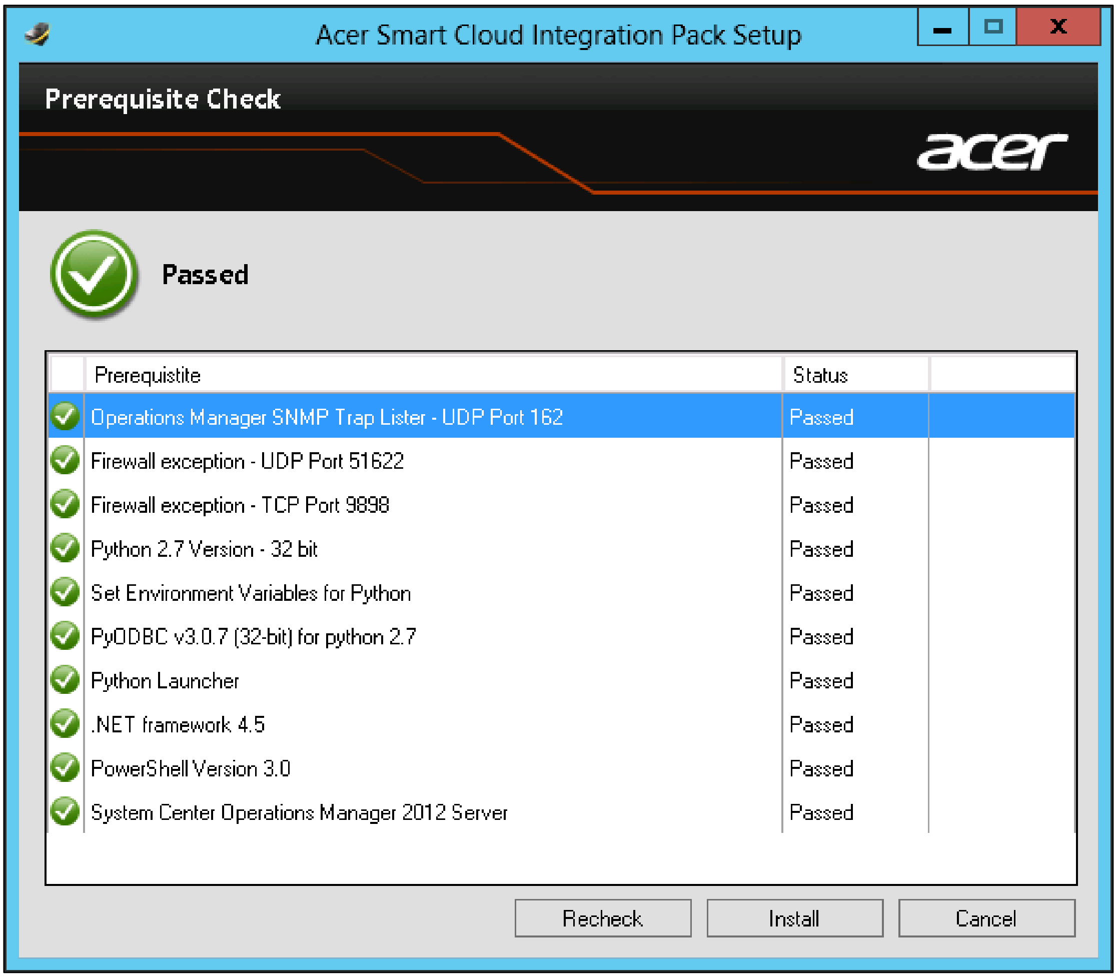
Acer Smart Cloud Integration Pack for Microsoft® System Center

Integrates the Acer server management features into the Microsoft® System Center. Click here to view Acer Smart Cloud Integration Pack User's Guide.

To install the Acer Smart Cloud Integration Pack

click here to install under Microsoft® System Center Operations Manager 2012 SP1 or Microsoft® System Center Operations Manager 2012 R2

Step 3. The installation package will complete the prerequisite checks and ensure the environment is suitable.



Acer Smart Cloud Integration Pack Setup

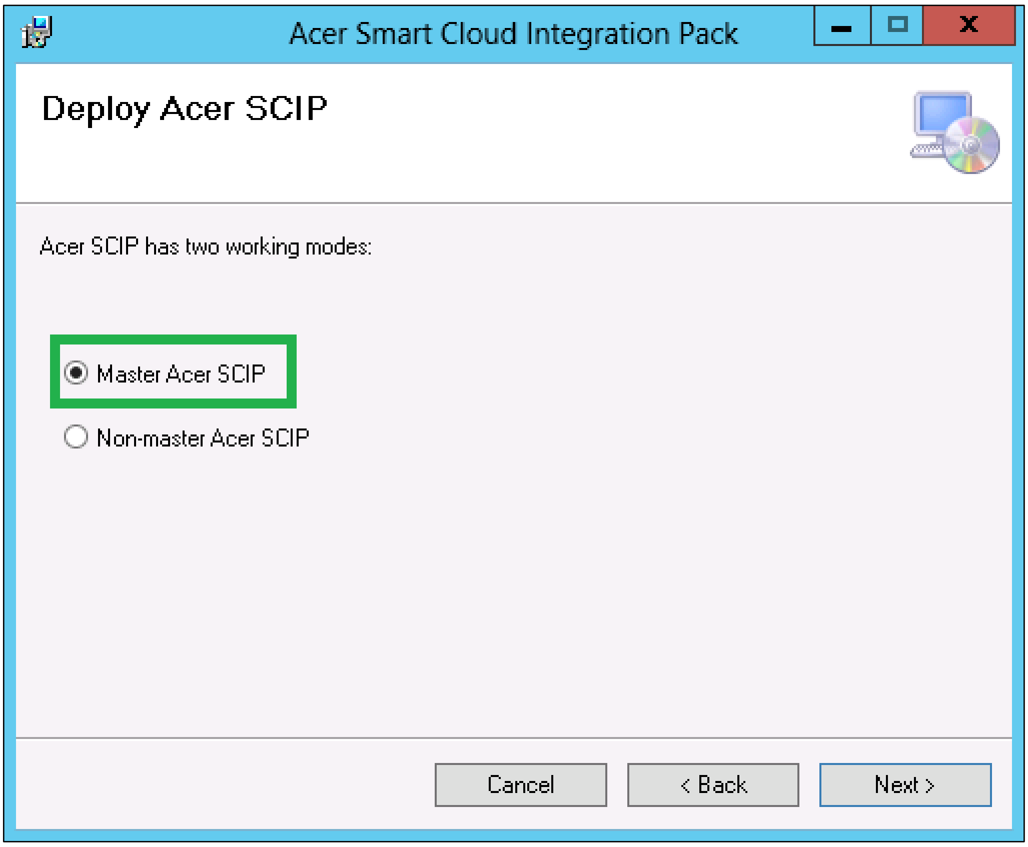
Prerequisite Check

Passed

	Prerequistite	Status
✓	Operations Manager SNMP Trap Lister - UDP Port 162	Passed
✓	Firewall exception - UDP Port 51622	Passed
✓	Firewall exception - TCP Port 9898	Passed
✓	Python 2.7 Version - 32 bit	Passed
✓	Set Environment Variables for Python	Passed
✓	PyODBC v3.0.7 (32-bit) for python 2.7	Passed
✓	Python Launcher	Passed
✓	.NET framework 4.5	Passed
✓	PowerShell Version 3.0	Passed
✓	System Center Operations Manager 2012 Server	Passed

Step 4. Click **Run** in the next two windows.

Step 5. Select **Master Acer SCIP** and click **Next**.



Deploy Acer SCIP

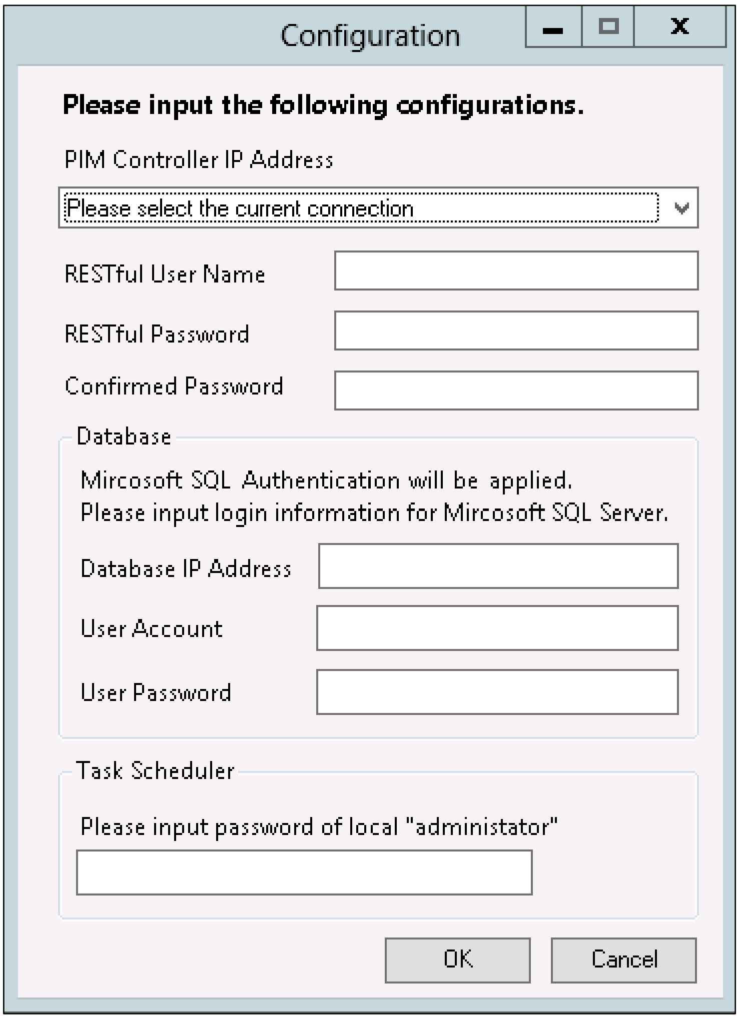
Acer SCIP has two working modes:

● Master Acer SCIP

○ Non-master Acer SCIP

Step 6. Click **Next** to confirm the installation.

Step 7. Select an IP address to be the Acer Integration Service's IP. This IP address is used to define the Acer server SNMP Trap (PET) destination.



Configuration

Please input the following configurations.

PIM Controller IP Address

Please select the current connection

RESTful User Name

RESTful Password

Confirmed Password

Database

Mircosoft SQL Authentication will be applied.
Please input login information for Mircosoft SQL Server.

Database IP Address

User Account

User Password

Task Scheduler

Please input password of local "administator"

Step 8. Enter a name for the RESTful User Name. Enter a password for RESTful connection. (Name and password are determined by you.)

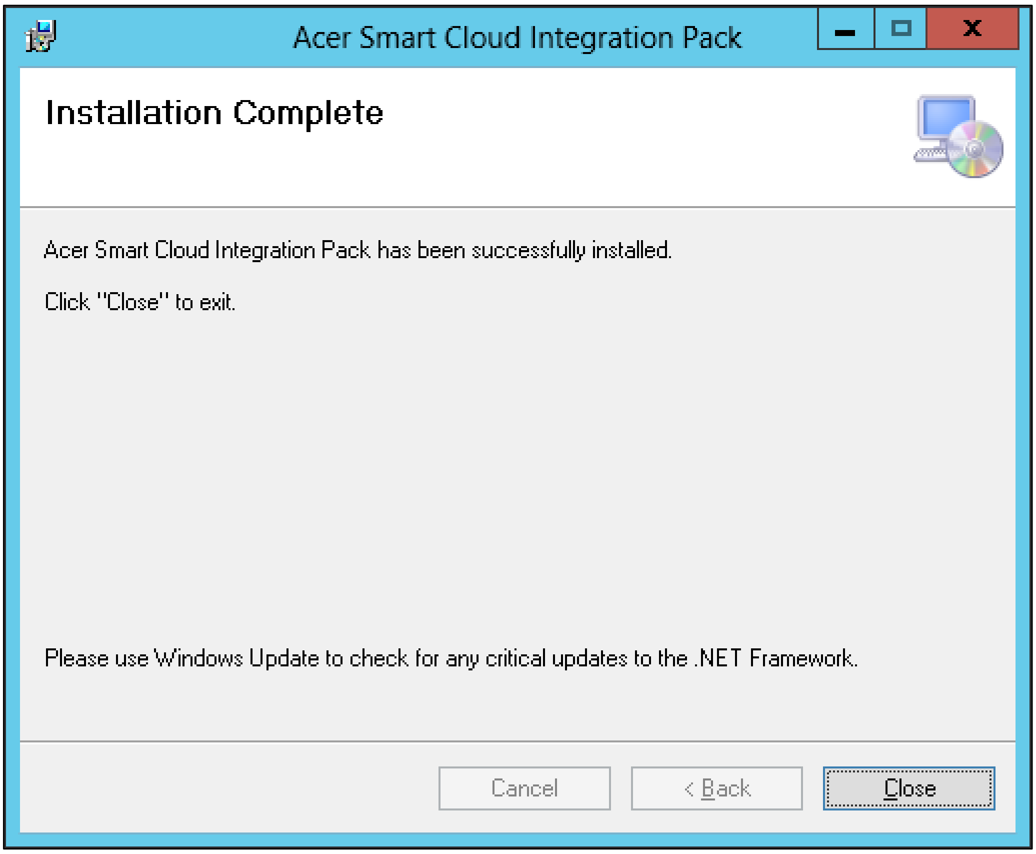
Step 9. Enter the IP address for the SQL Server.

Step 10. Enter the exact pre-created User Account and User Password of **SQL Authentication** way.

Step 11. Enter the *local administrator* password.

Step 12. Click **OK** to start installing Acer SCIP.

Step 13. When the installation is complete you will be informed. Click **Close** to finish the installation.


Acer Smart Cloud Integration Pack

Installation Complete

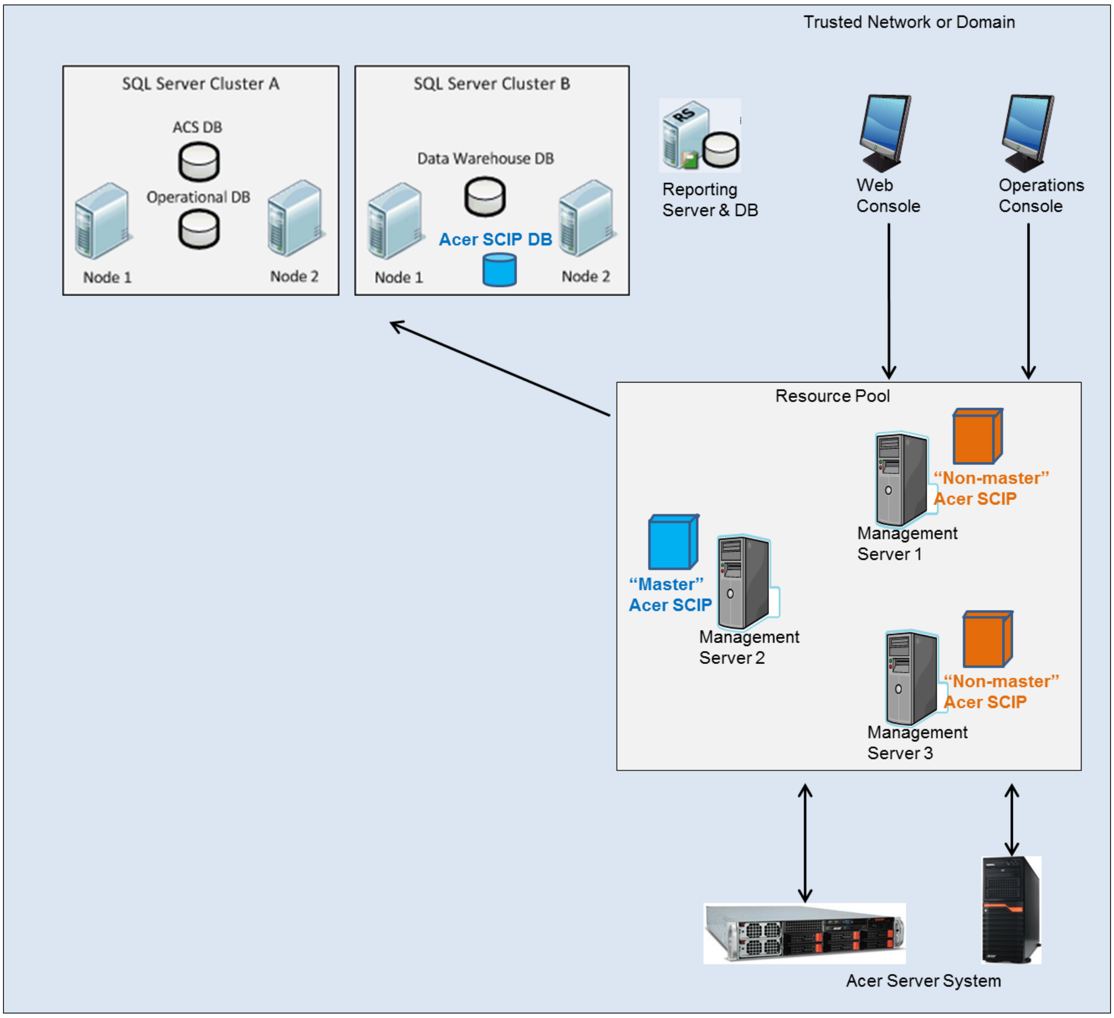
Acer Smart Cloud Integration Pack has been successfully installed.

Click "Close" to exit.

Please use Windows Update to check for any critical updates to the .NET Framework.

4.2. Install Acer SCIP in a distributed deployment environment

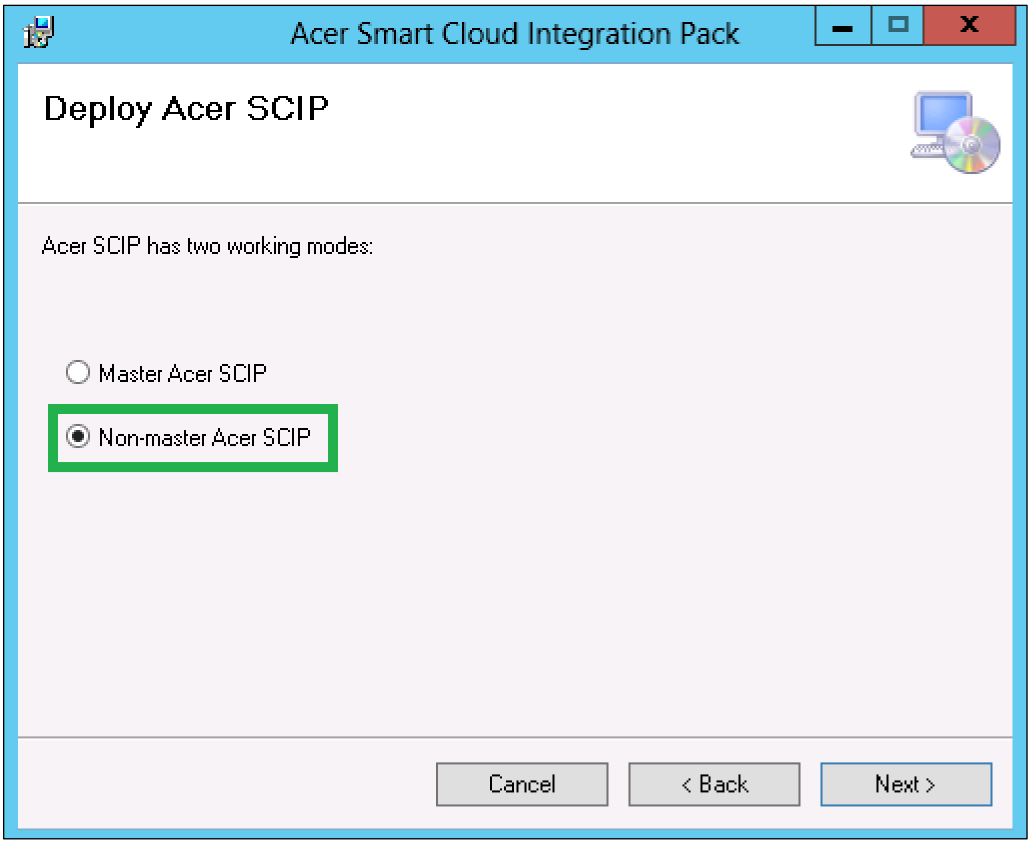
In a distributed deployment environment there may only be one master Acer SCIP on one Operations Manager Server. You may then install non-master Acer SCIP on other the Operations Manager Servers, as illustrated below.



To install the master Acer SCIP, please refer to section 4.1.

To install the non-master Acer SCIP:

All steps are the same as those in section 4.1., except step #5, where you should select *non-master Acer SCIP*.



Acer Smart Cloud Integration Pack

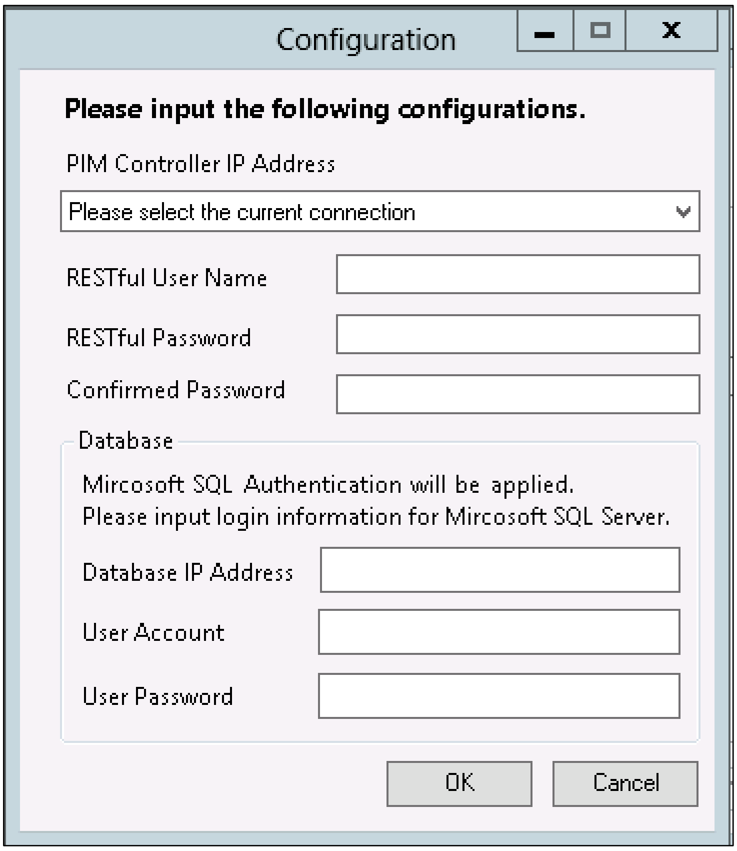
Deploy Acer SCIP

Acer SCIP has two working modes:

○ Master Acer SCIP

● Non-master Acer SCIP

Note: The non-master Acer SCIP Server does not create the required task(s) in the Task Scheduler. Its configuration form is shown below:



Configuration

Please input the following configurations.

PIM Controller IP Address

Please select the current connection

RESTful User Name

RESTful Password

Confirmed Password

Database

Mircosoft SQL Authentication will be applied.
Please input login information for Mircosoft SQL Server.

Database IP Address

User Account

User Password

5. UNINSTALL ACER SCIP

5.1. Uninstall the Master Acer SCIP in a single-server deployment

To uninstall the master Acer SCIP you need to remove:

- The Acer SCIP programs, files, and folders.
- Acer PIM service from Windows Services.
- Management packs from SCOM MS.
- Databases and tables from the SQL server.
- Related alerts and devices from the SCOM Console.

Follow the steps below to uninstall the Master Acer SCIP:

Step 1. Log into the OS which has the master Acer SCIP installed.

Step 2. Open **Control Panel** > **Programs and Features**.

Step 3. Select **Acer Smart Cloud Integration Pack** and click **Uninstall**.

Step 4. Follow the prompts.

Step 5. Choose whether you want to drop the database or not.

Step 6. Choose whether you want to remove the imported management packs for Acer SCIP or not.

5.2. Uninstall Acer SCIP in Distributed Deployment

In a distributed deployment environment, one master and many non-master Acer SCIPs might be installed. Please first uninstall all non-master Acer SCIPs, and then uninstall the master Acer SCIP.

Follow the steps below to uninstall non-master Acer SCIPs:

Step 1. Log into one OS which has a non-master Acer SCIP installed.

Step 2. Open **Control Panel** > **Programs and Features**.

Step 3. Select **Acer Smart Cloud Integration Pack** and click **Uninstall**.

Step 4. Follow the prompts.

Step 5. Repeat on each OS that has a non-master Acer SCIP installed until all non-master Acer SCIPs are uninstalled

Step 6. Refer to section 8.1 to uninstall the master Acer SCIP.

6. Appendix

6.1. Installing the SNMP Trap service

To install:

Step 1. Click **Administrative Tools** > **Server Manager**.

Step 2. Click **Features** in the side pane > **Add Features**.

Step 3. Select **SNMP Services** > **Next** > **Install**.