



Monitor the Cisco Unified Computing System

Using Sentry Software Monitoring for
BMC ProactiveNet Performance Management

White Paper
September 2010



Contents

What You Will Learn	3
Overview	3
Key Features	3
Inventory	4
Monitoring of Critical Devices.....	4
Environment Monitoring	4
Diagnostics	4
Capacity Reports for Capacity Planning	5
Power Consumption and Temperature Monitoring.....	5
About the Bundle.....	5
About BMC PATROL	5
About BMC PATROL Console	5
About BMC PATROL Agent.....	5
About Hardware Sentry KM for PATROL	6
Architecture.....	6
Centralized Remote Monitoring With One Agent	6
Distributed Monitoring With Several Agents.....	7
Monitoring a Cisco UCS Server Running Windows.....	9
Principle	9
Prerequisites	10
With a PATROL Agent Installed on the Monitored System	10
From the Centralized PATROL Console and Agent.....	10
Monitoring a Cisco UCS Server Running Linux	13
Principle	13
Prerequisites	13
With a PATROL Agent Installed on the Monitored System	14
From the Centralized PATROL Console and Agent.....	16
Monitoring a Cisco UCS Server running VMware ESXi and ESX 4.0.....	19
Principle	19
Prerequisites	19
Installation.....	19
Configuration.....	19
Monitoring a Cisco UCS Server through its IMC.....	22
Principle	22
Prerequisites	22
Installation.....	22
Configuration.....	22
Monitoring a Cisco UCS B-Series Blade Chassis	25
Principle	25
Prerequisites	26
Installation.....	26
Configuration.....	26
Conclusion	28

What You Will Learn

This document details the BMC architecture for Cisco Unified Computing System monitoring and provided specific guidance for using the Sentry Software Monitoring for BMC ProactiveNet Performance Management – Hardware Monitoring – Cisco UCS Edition capabilities with Microsoft Windows, Linux, and VMware ESX on Cisco UCS B-Series and C-Series servers.

Overview

Sentry Software Monitoring for BMC ProactiveNet Performance Management – Hardware Monitoring – Cisco UCS Edition (BPPM for UCS) brings critical hardware information into your BPPM environment for all your Cisco Unified Computing System components. It enables an easy and cost-effective centralized management of all your Cisco UCS hardware components through a single solution.

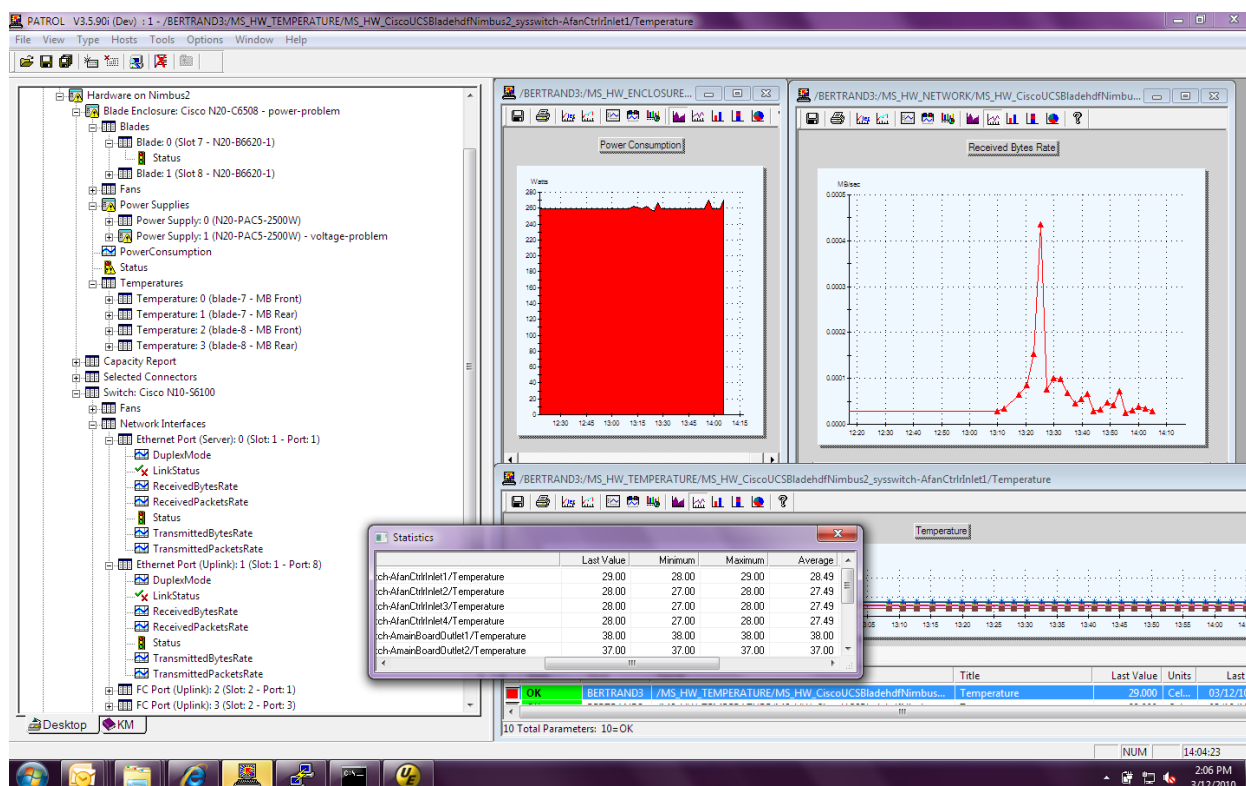
No configuration, automatic detection and centralized monitoring management of all hardware components help maximize the performance and productivity of Cisco UCS components, enabling you to build a strong, reliable foundation to base your business-critical systems on.

- Maximizes server uptime and availability
- Lowers Total-Cost-of-Ownership thanks to unmatched visibility into the realm of power consumption
- Simplifies and rationalizes the IT infrastructure management with a single hardware monitoring solution for UCS blade and rack-mount systems
- Integrates hardware management tools in your BSM strategy

Furthermore, BPPM for the Cisco Unified Computing System integrates transparently within the BMC Business Service Management (BSM) architecture, enabling complete lifecycle support for Cisco Unified Computing System operations in heterogeneous environments with BMC.

Key Features

The solution provides a rich set of monitoring features for the entire Cisco Unified Computing System product line, including the Cisco UCS B-Series blade and C-Series rack-mount servers.



Inventory

- Automatically discovers all internal components of the monitored environment
- Provides critical metrics (health, performance and events) for each components

Monitoring of Critical Devices

- RAID controllers, physical/logical disks, and volume availability
- Memory module and processors (CPU)
- Error correcting code (ECC) errors
- Network adaptors and bandwidth utilization, and data traffic

Environment Monitoring

- Temperature and fans
- Internal voltages and power supplies
- Status and color of each LED on the front and back panels

Diagnostics

- Details about each monitored component to facilitate its replacement should a failure occur (vendor, model, serial number, part number, field-replaceable unit [FRU] number, and location in the chassis)
- Full hardware health reports displaying detailed information about failures, their consequences, and how to fix them
- Ethernet traffic report on each port in MBps or the total amount of data that transited, in and out, in gigabytes per hour or per day

Capacity Reports for Capacity Planning

- Details about the capacity of the monitored system: number of physical CPUs, amount of memory, overall size of disks and volumes, and number of connected ports

Power Consumption and Temperature Monitoring

- Live monitoring (in watts) for each switch, blade chassis, and individual blade and rack-mount server
- Energy use reports (in kilowatt hours) on an hourly or daily basis

About the Bundle

Sentry Software Monitoring is a bundle comprised of the following components:

- BMC PATROL Console
- BMC PATROL Agent
- Hardware Sentry KM for PATROL

This combination of software products will let you set-up a comprehensive monitoring for your Cisco UCS environment.

About BMC PATROL

PATROL is a systems, applications, and event management tool for database and system administrators. It provides an object-oriented graphical workspace where you can view the status of every vital resource in the distributed environment you are managing.

PATROL both monitors and manages the resources in your environment using the information it gets from files you load from the console called knowledge modules. If PATROL detects a problem with a computer or application it is monitoring, these modules provide the "knowledge" for PATROL to attempt to fix the problem. If the problem escalates or requires your attention, PATROL displays every resource affected by the problem in a warning or alarm condition.

About BMC PATROL Console

The PATROL Console is your main interface with PATROL Agents. It provides an object-oriented graphical workspace where you can monitor the status of vital resources in the distributed enterprise you are managing. The PATROL main window represents devices and components as object icons.

If PATROL detects a problem with a managed device, it displays the affected resources in a warning or an alarm condition.

About BMC PATROL Agent

The PATROL Agent monitors various parts of the systems using specific Knowledge Modules (KMs). A PATROL Agent is typically installed on each managed computer and runs autonomously on those computers.

A PATROL Agent accepts requests from the PATROL Console and initiates actions based on those requests. A PATROL Agent loads information from Knowledge Modules and then gathers statistics and sends alerts and requested information to the PATROL Console.

A PATROL Agent can also use Knowledge Module information to react to system or application conditions that arise on monitored host computers. A PATROL Agent runs any menu commands or user-defined commands and tasks that you enter through the PATROL Console.

About Hardware Sentry KM for PATROL

Hardware Sentry KM for PATROL is a module loaded by the PATROL Agent and the PATROL Console that automatically detects all the various hardware components of your Cisco UCS environment, collects critical metrics, such as inventory, uptime, performance, and system health.

In effect, Hardware Sentry KM runs on the PATROL Agent and its interface is displayed on the PATROL Console.

In the BPPM for the Cisco UCS bundle, the Hardware Sentry KM module is automatically installed and loaded with the PATROL Agent and the PATROL Console.

Architecture

Hardware Sentry KM – Cisco UCS Edition is a specialized version for Cisco UCS of the multiplatform Hardware Sentry KM for PATROL.

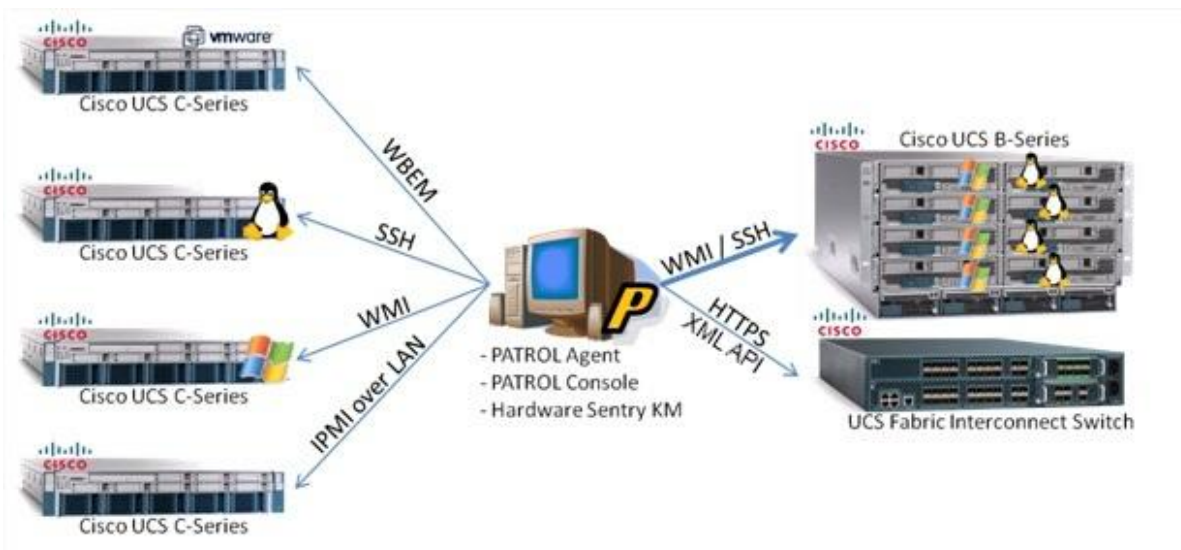
Hardware Sentry KM is a Knowledge Module for PATROL: it runs on top of a PATROL Agent and the metrics it collects (health, performance and events) are displayed in a PATROL Console.

In the traditional BMC PATROL architecture, a PATROL Agent needs to be installed on each managed server. Hardware Sentry KM, however, is able to monitor systems remotely. This means the user can choose between two main architectures:

Centralized Remote Monitoring With One Agent

One PATROL Agent runs one instance of Hardware Sentry KM and is used to monitor several Cisco UCS systems. The PATROL Agent, PATROL Console and Hardware Sentry KM can be installed on the very same machine.

Figure 1. Architecture Overview



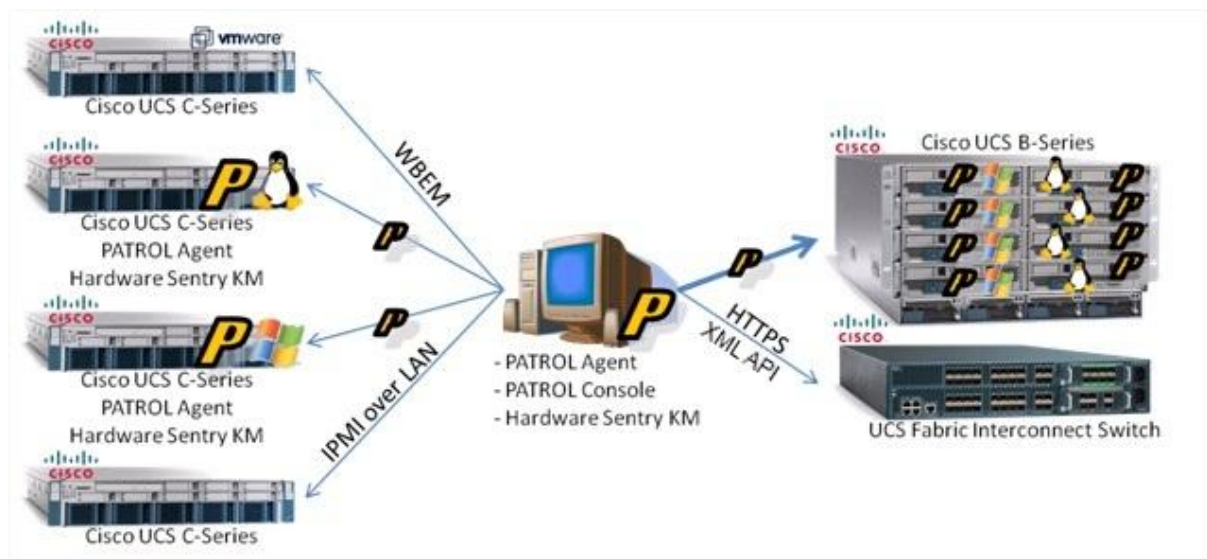
The main advantage of this architecture is that the products need to be installed on a single system. Everything else is done remotely.

However, this architecture may not scale well over 100 managed servers and will require the installation of additional agents at a later time.

Distributed Monitoring With Several Agents

A PATROL Agent with Hardware Sentry KM is installed on each server to be monitored (Windows and Linux systems). The PATROL Console is installed on a separate machine. It is recommended to also install a PATROL Agent and Hardware Sentry KM with the console, in order to remotely monitor systems where a PATROL Agent cannot be installed (for example, VMware ESX, Fabric Interconnect Switch).

Figure 2. Distributed Monitoring Architecture



The main benefit of this architecture is that it scales very well over thousands of monitored systems. It implies, however, the deployment of the PATROL Agent and Hardware Sentry KM on all systems.

Health and Performance Metrics

Monitoring UCS B-Series platform

Sentry's hardware monitoring solution integrates Cisco UCS Manager into BMC Performance Manager: every metric and status that is available in UCS Manager's GUI is made available in the BMC framework, and thus can be leveraged for reporting, proactive alerting, event correlation, service impact management, etc.

In order to cover the entire UCS B-Series platform, Sentry's hardware monitoring solution connects to the switch (through Cisco's native UCS XML API) to gather all metrics related to the main chassis and the switch. The product is also able to connect to blade servers individually in order to gather internal metrics are not available through UCS Manager: storage subsystem, network traffic, a few environmental parameters. Various instrumentation standards are leveraged on the B-Series blade servers to assess the health of their internal hardware components: IPMI, WMI, and SSH.

Cisco UCS Switch Monitored Elements

	Parameters	Units	Default Alert Conditions
Powering	Status	n/a	Warning (Degraded) Alarm (Failed)
Cooling	Speed	Rotation Per Minute (RPM)	Warning (Degraded) Alarm (Failed)
	Speed Percent	n/a	n/a
	Status	n/a	n/a
Temperature	Status	n/a	Warning (Degraded) Alarm (Failed)
	Temperature	Celcius degrees (C°)	n/a

Voltage	Status	n/a	Warning (Degraded) Alarm (Failed)
	Voltage	miliVolts (mV)	n/a
Port Status	Status	n/a	Warning (Degraded) Alarm (Failed)
Blade Status	Status	n/a	Warning (Degraded) Alarm (Failed)
Link Failure Detection	Link Status	n/a	Triggers a warning if the network interface is not connected 0 = OK; 1= Unplugged
Link Downgrade Detection	Link Speed	Megabits per second	n/a
Traffic Report	Transmitted Packet Rate	Packets per second	n/a
	Received Packet Rate	Packets per second	n/a
	Transmitted Byte Rate	Megabytes per second	n/a
	Transmitted Packet Rate	Packets per second	n/a
Power Consumption	PowerConsumption	Watts	

Cisco UCS Chassis Monitored Elements

	Parameters	Units	Default Alert Conditions
Powering	Status	n/a	Warning (Degraded) Alarm (Failed)
Cooling	Speed	Rotation Per Minute (RPM)	Warning (Degraded) Alarm (Failed)
	Speed Percent	n/a	
	Status	n/a	
Temperature (Internal/External)	Status	n/a	Warning (Degraded) Alarm (Failed)
	Temperature	Celcius degrees (C°)	
Blade Status	Status	n/a	Warning (Degraded) Alarm (Failed)

Monitoring C-Series Rack-mount Servers

Cisco rack-mount servers are high-performance standard PC servers, running Windows or Linux, instrumented with a few standard protocols: IPMI, WMI or SNMP and some LSI-specific components.

On Windows, Sentry's hardware monitoring solution will rely on WMI, Microsoft's IPMI WMI provider to monitor the environment (temperature, fans, power supplies, disks, LEDs, etc.). The monitoring of the NICs is done through the Windows NDIS provider for WMI or through the Windows SNMP MIB-2 Agent.

On Linux, Sentry's hardware monitoring solution will rely on the OpenIPMI driver and ipmitool, an official Linux utility, to monitor the environment (temperature, fans, power supplies, disks, LEDs, etc.). The monitoring of the NICs is done through some Linux commands or through the Linux SNMP MIB-2 Agent.

It is possible to monitor a Cisco UCS C-Series rack-mount server out-of-band through its "Integrated Management Controller" (IMC), using remote IPMI. The IMC needs to be properly configured on the network and remote IPMI enabled. While less detailed than the in-band monitoring, this solution still gives a complete picture of the hardware health of the C-Series server.

Cisco UCS B-Series Monitored Elements

	Parameters	Units	Default Alert Conditions
Processor Status	Status	n/a	Warning (Degraded) Alarm (Failed)
	Error Count	Error	n/a

	Parameters	Units	Default Alert Conditions
Memory Status	Predicted Failure	Failure	Trigger a warning if a CPU failure is predicted to happen
	Status	n/a	Warning (Degraded) Alarm (Failed)
	Error Count	Error	n/a
	Predicted Failure	Failure	Trigger a warning if a memory failure is predicted to happen
Temperature	Status	n/a	Warning (Degraded) Alarm (Failed)
	Temperature	Celcius degrees (C°)	
Voltage	Status	n/a	Warning (Degraded) Alarm (Failed)
	Voltage	miliVolts (mV)	n/a
Full Network Monitoring	Status	n/a	Warning (Degraded) Alarm (Failed)
	Bandwidth Utilization	%	n/a
	Duplex Mode	n/a	0 = Half-Duplex; 1 = Full Duplex
	Link Status	n/a	Triggers a warning if the network interface is not connected 0 = OK; 1= Unplugged
	Link Speed	Megabits per second	n/a
	Transmitted Packet Rate	Packets per second	n/a
	Received Packet Rate	Packets per second	n/a
	Transmitted Byte Rate	Megabytes per second	n/a
	Received Byte Rate	Megabytes per second	n/a
	Error Percent	%	n/a
Disk Controller	Battery Status	n/a	Warning (Degraded) Alarm (Failed)
	Controller Status	n/a	Warning (Degraded) Alarm (Failed)
Disks	Status	n/a	Warning (Degraded) Alarm (Failed)
	Predicted Failure	Failure	Triggers a warning if a failure is predicted
	Error Count	Error	n/a

Monitoring a Cisco UCS Server Running Windows

Principle

Cisco UCS servers are instrumented with a baseboard management controller (BMC) following the Distributed Management Taskforce (DMTF) Intelligent Platform Management Interface (IPMI) standard.

On Windows systems, Hardware Sentry KM uses the Microsoft IPMI driver and the IPMI Windows Management Interface (WMI) provider to discover the hardware components of the server and check their status.

WMI is therefore the only instrumentation layer and protocol Hardware Sentry KM uses in this case, either locally or remotely.

Prerequisites

The Cisco UCS server must be running one of the following versions of Windows:

- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003 R2

On Windows Server 2003 R2, the monitoring of the server requires the prior installation of the “Hardware Management” component of the “Management and Monitoring Tools” group in the “Add/Remove Windows Components” Control Panel applet. Note that versions of Windows prior to Windows Server 2003 R2 do not offer full IPMI support, so the data that may be gathered through the operating system may be limited.

On Windows 2008, the “Hardware Management” component is installed and configured by default.

With a PATROL Agent Installed on the Monitored System

Installation

Follow the standard procedure to install the following components:

- PATROL Agent
- Hardware Sentry KM – UCS Edition

Configuration

Add the hostname or IP address of the monitored system in the PATROL Console.

Nothing needs to be specifically configured at the level of Hardware Sentry KM: it automatically discovers all the hardware elements of the server and monitors them.

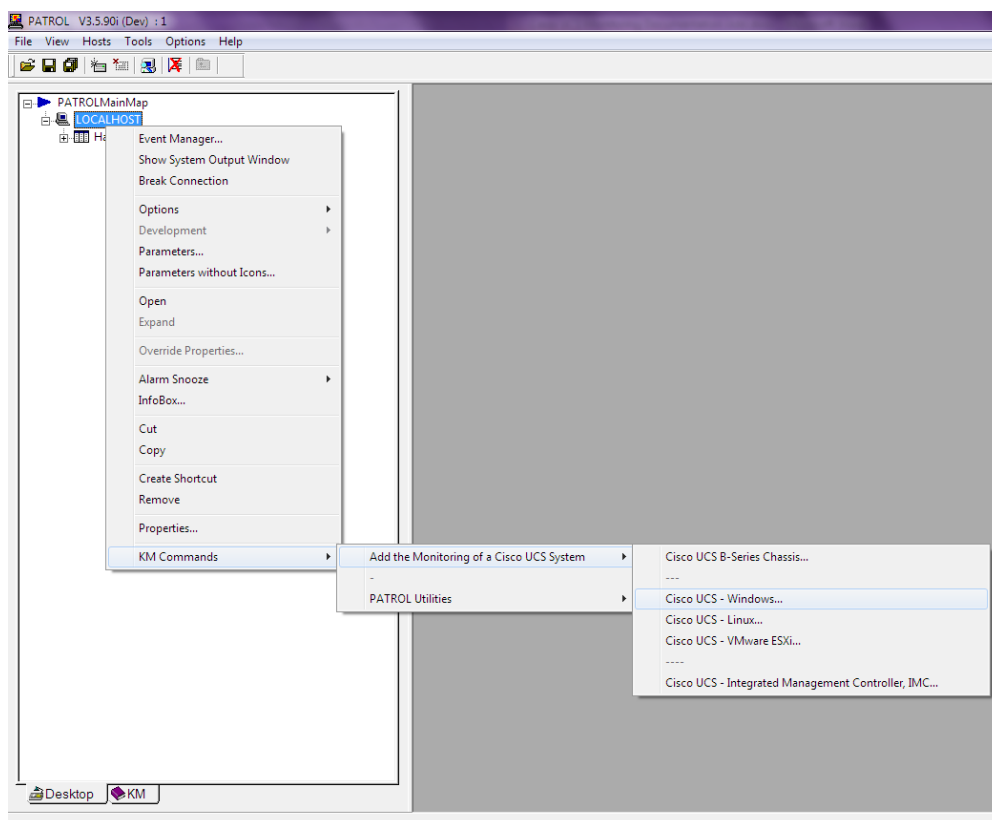
From the Centralized PATROL Console and Agent

Installation

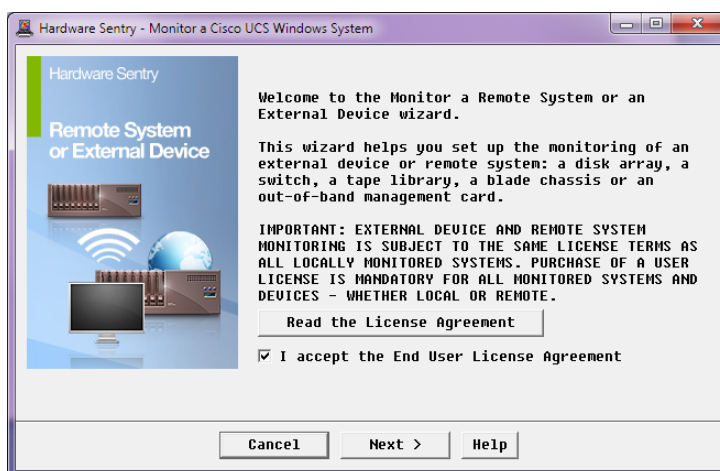
Nothing additional needs to be installed.

Configuration

In the PATROL Console, right-click the icon corresponding to the main PATROL Agent > KM Commands > Add the Monitoring of a Cisco UCS System > Cisco UCS – Windows....



The Monitor a Cisco UCS Windows System appears. Check the box to accept the condition of the software license agreement of this product.



In the next step, enter the system name as it will be displayed in the PATROL Console. Specify its IP address or fully qualified name if it is different from the display name used above.

Hardware Sentry - Monitor a Cisco UCS Windows System

Cisco UCS Server Identification

System Name: (Name displayed in the consoles)
ucsWindows01

IP address or fully qualified name: (Leave blank to use the System Name above)
172.16.8.244

< Back Next > Help

Then enter the username and password to connect to the system. The specified credentials need to be member of the Local Administrators group.

Hardware Sentry - Monitor a Cisco UCS Windows System

WMI Credentials

Please provide a user account valid on ucsWindows01 in order to perform WMI queries.

Login: (valid on ucsWindows01) Please specify a login with administrative privileges on ucsWindows01.
dom\patrol If the specified account is local to ucsWindows01, you will have to specify it accordingly as shown below: ucsWindows01\<username>

Password: *****

Note: You can leave these fields blank if "patrol" is a user account valid on ucsWindows01. Otherwise, you need to specify a user account allowed to make WMI queries on ucsWindows01.

< Back Next > Help

Click Finish in the final step.

Hardware Sentry - Reinitialize

Hardware Sentry

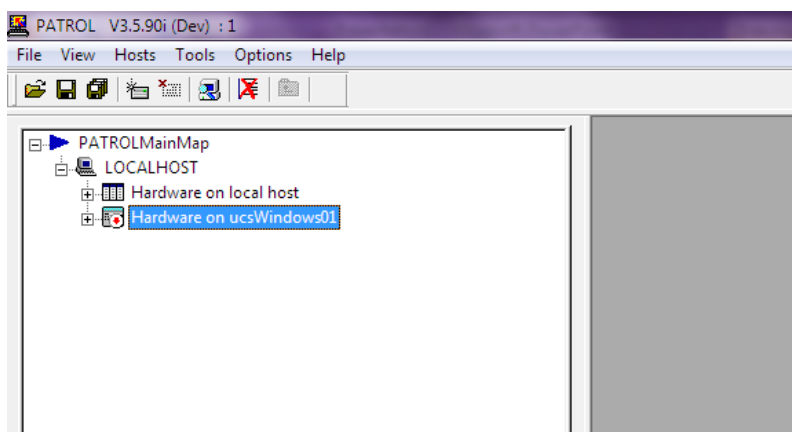
Reinitialize Hardware Sentry

Hardware Sentry needs to be reinitialized for the new settings to be taken into account. It will destroy all previously discovered objects and trigger a new platform detection on localhost as well as a full discovery of the environment.

Click on the Finish button to apply the new settings and reinitialize Hardware Sentry.

< Back Finish Help

A new icon is created in the PATROL Console, corresponding to the monitoring of the hardware of this Cisco UCS Windows server.



After a couple minutes, Hardware Sentry KM has completed its initial discovery of the system and displays the internal components of the server in the console.

Monitoring a Cisco UCS Server Running Linux

Principle

Cisco UCS servers are instrumented with a baseboard management controller (BMC) following Intel's IPMI standard.

On Linux systems, Hardware Sentry KM uses the Linux built-in OpenIPMI driver and the `ipmitool` utility to monitor the hardware components of the server and check their status. It also uses the `ethtool` utility to monitor the traffic on the network cards.

For the remote monitoring of a Linux system, Hardware Sentry KM uses the SSH protocol to execute the `ipmitool` and `ethtool` commands and analyze their respective outputs.

Prerequisites

The Cisco UCS server can run any popular distribution of Linux, given that:

- The OpenIPMI driver is installed and properly loaded
- `ipmitool` is properly installed and accessible from the `$PATH` variable

Check the interoperability matrix http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html for all the supported platforms on UCS Servers.

Note: The OpenIPMI driver can be activated with the following commands:

```
/sbin/chkconfig ipmi on
/sbin/service ipmi start
```

The `ipmitool` packages can be found at this address: <http://ipmitool.sourceforge.net>, or with the vendor of your Linux distribution.

By default, both the `ipmitool` and `ethtool` utilities require root privilege. It is possible to configure Hardware Sentry KM with the root password or to use the `sudo` utility to execute the commands that require root privilege.

If the `sudo` option is preferred, the `sudo` utility must have been properly configured to allow the PATROL Agent's default account to execute the `ipmitool` and `ethtool` commands as root. This can be done by an authorized administrator only in the `/etc/sudoers` file by adding the following line:

```
patrol ALL=NOPASSWD:/sbin/ethtool,/usr/bin/ipmitool
```

With a PATROL Agent Installed on the Monitored System

Installation

Follow the standard procedure to install the following components:

- PATROL Agent
- Hardware Sentry KM – UCS Edition

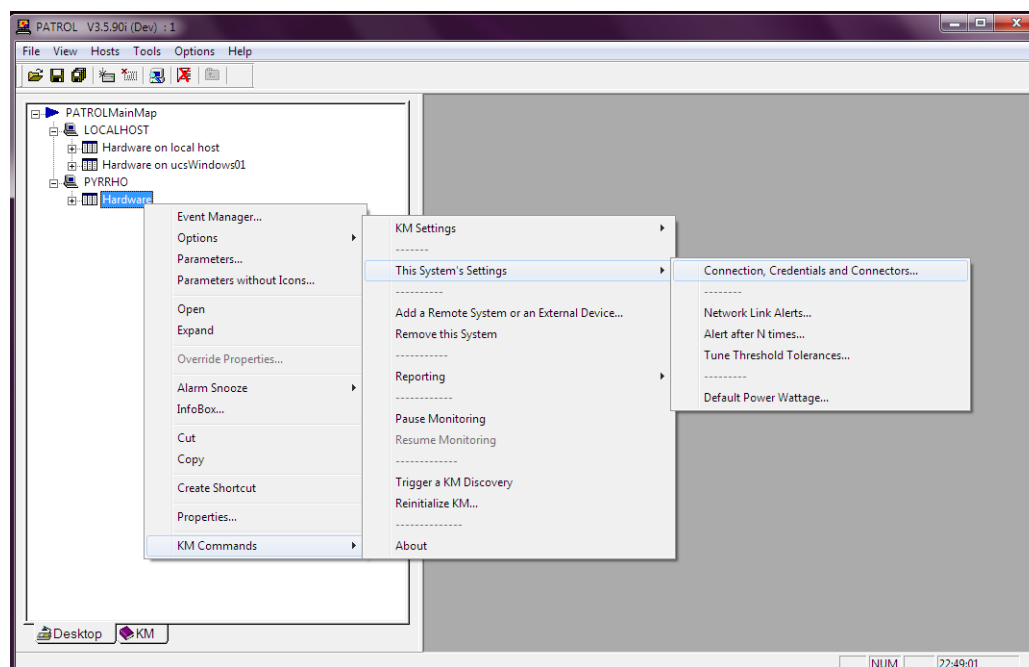
Note: The Linux distribution needs to be one supported by this version of the PATROL Agent. Please refer to the PATROL Agent's Installation Guide for further information.

Configuration

Add the hostname or IP address of the monitored system in the PATROL Console.

Without further configuration, Hardware Sentry KM is not able to properly monitor the Cisco UCS server running Linux because it needs root privilege in order to access the hardware information.

To configure Hardware Sentry KM with the root credentials or to use sudo, [right-click] on the main “Hardware” icon under the icon of the newly added PATROL Agent in the Console > KM Commands > This System's Settings > Connection, Credentials and Connectors....



In the wizard, enter the root credentials or specify that Hardware Sentry KM should use the sudo utility in order to execute ipmitool and ethtool.

Hardware Sentry - SNMP Community and Command Execution Credentials on pyrrho.internal.sentrysof...

SNMP Community and Command Execution Credentials

Use the following SNMP community for SNMP queries:

Leave this field empty if you want Hardware Sentry to automatically detect the SNMP community ().

Use the following account to execute external commands:

Username:

Password:

Leave the above fields empty if you want Hardware Sentry to use the PATROL Agent default account (patrol).

Sudo options To execute external commands, Hardware Sentry may use the "sudo" utility rather than impersonation.

Cancel Next > Help

For the sudo options, click the Sudo options button. In the new windows, check the boxes for both `ipmitool` and `ethtool`, and click Accept.

Sudo options

Sudo options

The following programs may be executed by Hardware Sentry to gather hardware information. Some of these programs may require privileged access.

Check the corresponding boxes if you want Hardware Sentry to use the "sudo" utility to run these commands:

☒ ethtool

☒ ipmitool

Enter the command line to execute the "sudo" utility:

Leave the field empty to use the default /usr/bin/sudo path.

Using the "sudo" utility for a given set of commands may be more secure than impersonating every command executed by Hardware Sentry.

You must have installed "sudo" on this computer and configured the "/etc/sudoers" file to allow the PATROL Agent to execute the selected commands as root.

Accept Cancel

Warning! It is important not to provide Hardware Sentry KM with the root password and in the same time instruct the KM to also use the sudo utility.

Click Next and leave all other options to their default until the end of the wizard, and click Finish. Hardware Sentry KM reinitializes itself and after a couple minutes discovers all the internal components of the Cisco UCS server.

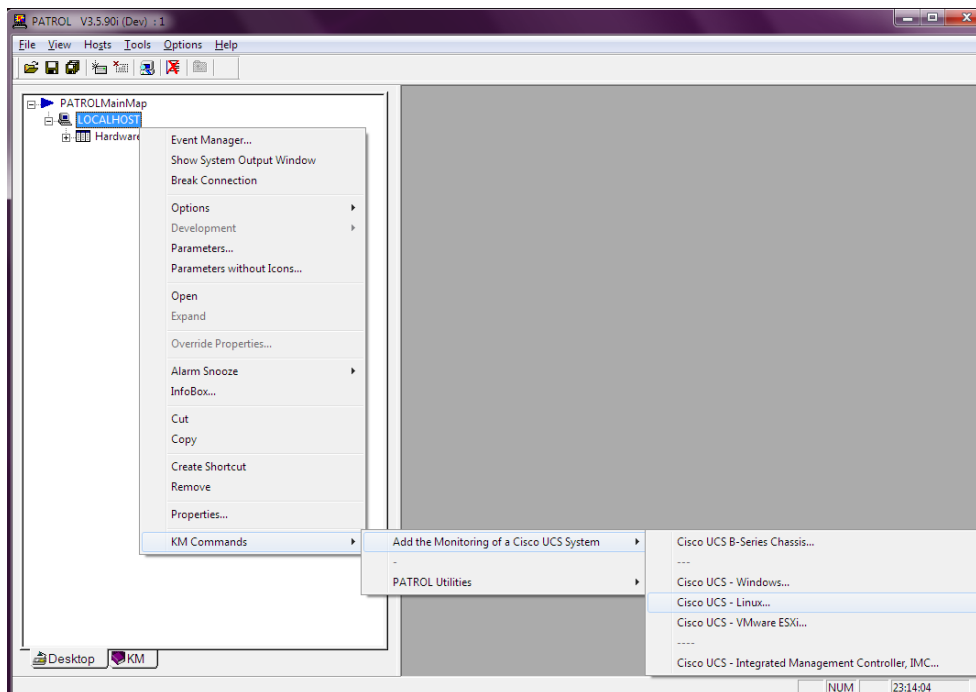
From the Centralized PATROL Console and Agent

Installation

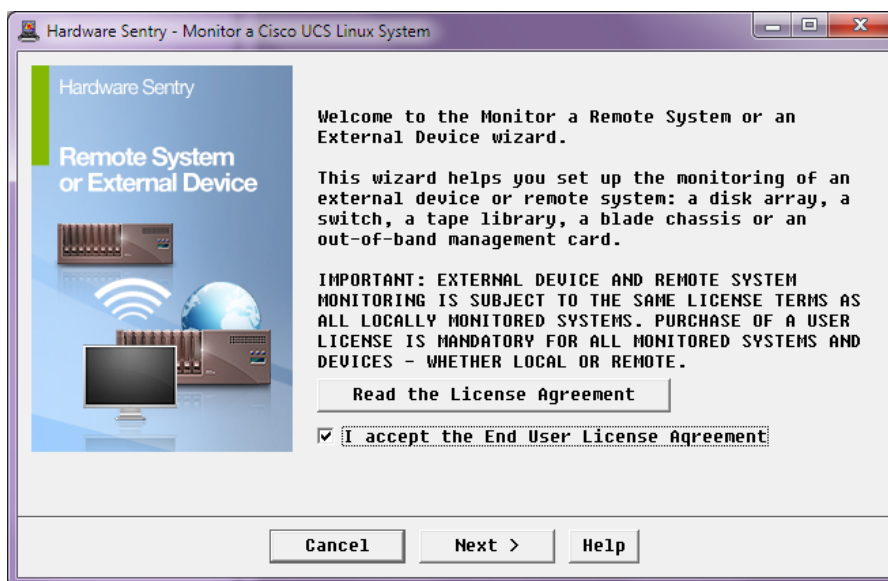
Nothing additional needs to be installed.

Configuration

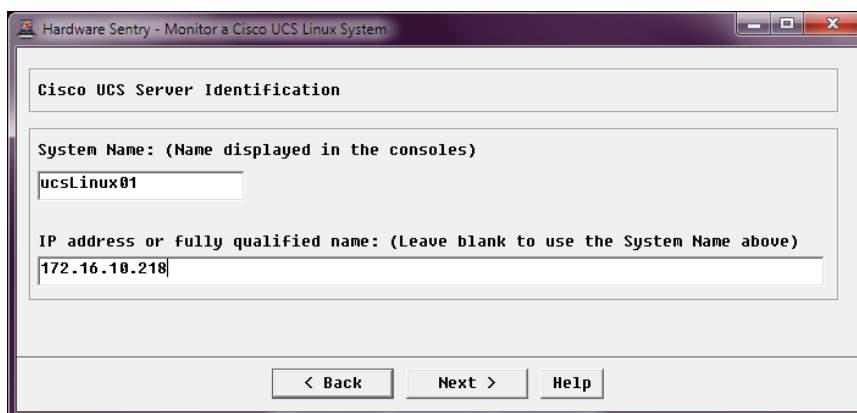
In the PATROL Console, [right-click] on the icon corresponding to the main PATROL Agent > KM Commands > Add the Monitoring of a Cisco UCS System > Cisco UCS – Linux....



The Monitor a Cisco UCS Linux System appears. Check the box to accept the condition of the software license agreement of this product.

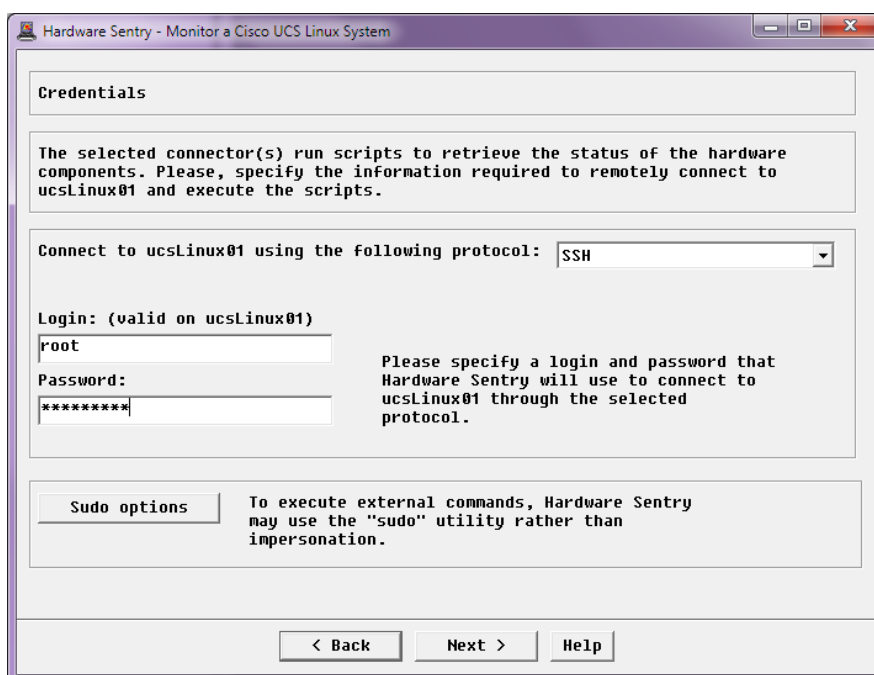


In the next step, enter the system name as it will be displayed in the PATROL Console. Specify its IP address or fully qualified name if it is different from the display name used above.



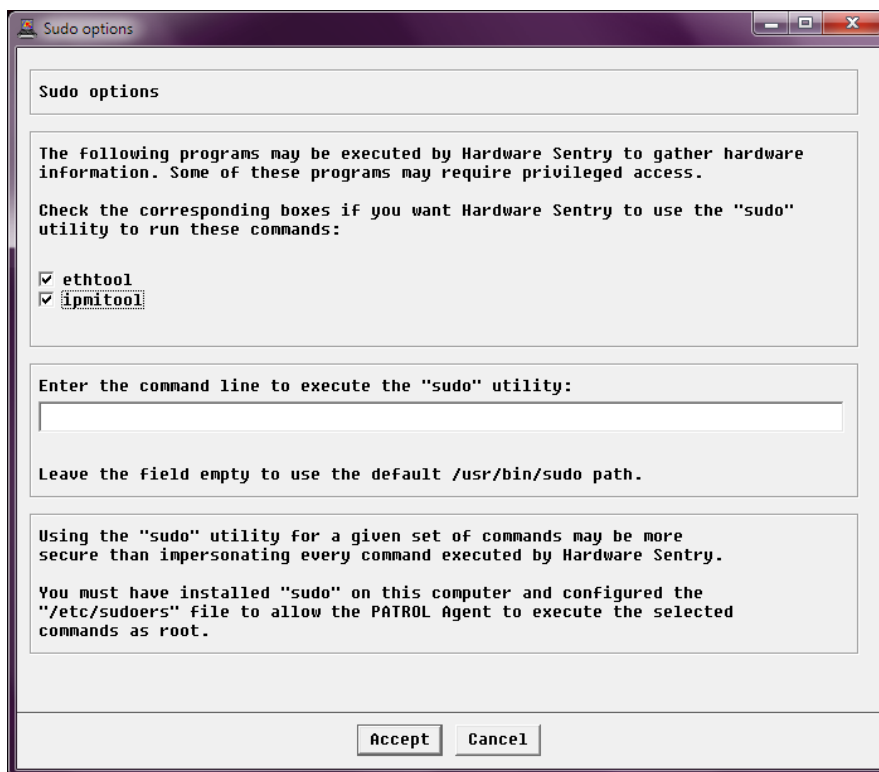
The screenshot shows a window titled "Hardware Sentry - Monitor a Cisco UCS Linux System". The main section is "Cisco UCS Server Identification". It contains two text input fields: "System Name: (Name displayed in the consoles)" with the value "ucslinux01" and "IP address or fully qualified name: (Leave blank to use the System Name above)" with the value "172.16.10.210". At the bottom are three buttons: "< Back", "Next >", and "Help".

In the wizard, enter the root credentials or specify that Hardware Sentry KM should use the sudo utility in order to execute ipmitool and ethtool.



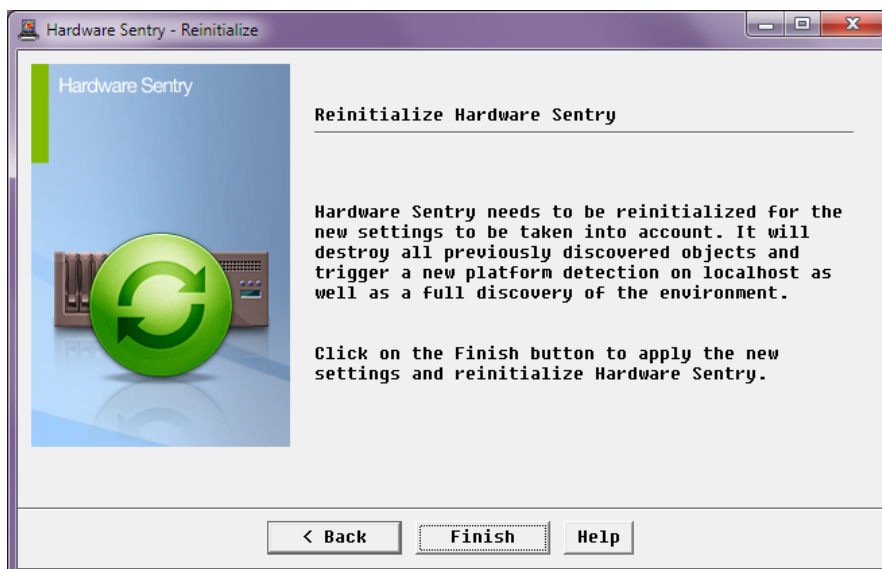
The screenshot shows a window titled "Hardware Sentry - Monitor a Cisco UCS Linux System". The main section is "Credentials". It contains a text box with the instruction: "The selected connector(s) run scripts to retrieve the status of the hardware components. Please, specify the information required to remotely connect to ucslinux01 and execute the scripts." Below this is a dropdown menu labeled "Connect to ucslinux01 using the following protocol:" with "SSH" selected. There are two text input fields: "Login: (valid on ucslinux01)" with the value "root" and "Password:" with the value "*****". To the right of the password field is a note: "Please specify a login and password that Hardware Sentry will use to connect to ucslinux01 through the selected protocol." At the bottom left is a button labeled "Sudo options". To its right is a text box with the instruction: "To execute external commands, Hardware Sentry may use the 'sudo' utility rather than impersonation." At the bottom are three buttons: "< Back", "Next >", and "Help".

For the sudo options, click the Sudo options button. In the new windows, check the boxes for both ipmitool and ethtool, and click Accept.

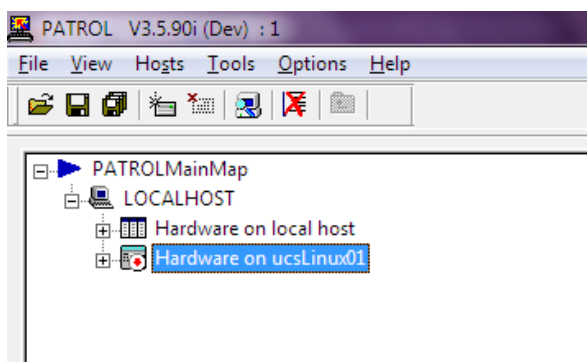


Warning! It is important not to provide Hardware Sentry KM with the root password and in the same time instruct the KM to also use the sudo utility.

Click Next and leave all other options to their default until the end of the wizard, and click Finish. Hardware Sentry KM reinitializes itself and after a couple minutes discovers all the internal components of the Cisco UCS server.



A new icon is created in the PATROL Console, corresponding to the monitoring of the hardware of this Cisco UCS Linux server.



After a couple minutes, Hardware Sentry KM has completed its initial discovery of the system and displays the internal components of the server in the console.

Monitoring a Cisco UCS Server running VMware ESXi and ESX 4.0

Principle

Cisco provides a specific version of the VMware ESX 4.0 firmware so that it can properly handle the underlying hardware instrumentation of Cisco UCS servers.

VMware ESX 4.0 exposes a WBEM interface that offers a subset of the CIM model following the SMASH standard (WBEM, CIM and SMASH are all standards defined by the DMTF, see dmtf.org for more information). The Hardware Sentry KM communicates with this SMASH interface on ESX to monitor the hardware of Cisco UCS servers running VMware ESX 4.0.

Monitoring of VMware ESXi 4.0 is done remotely as nothing can be installed on those servers.

Prerequisites

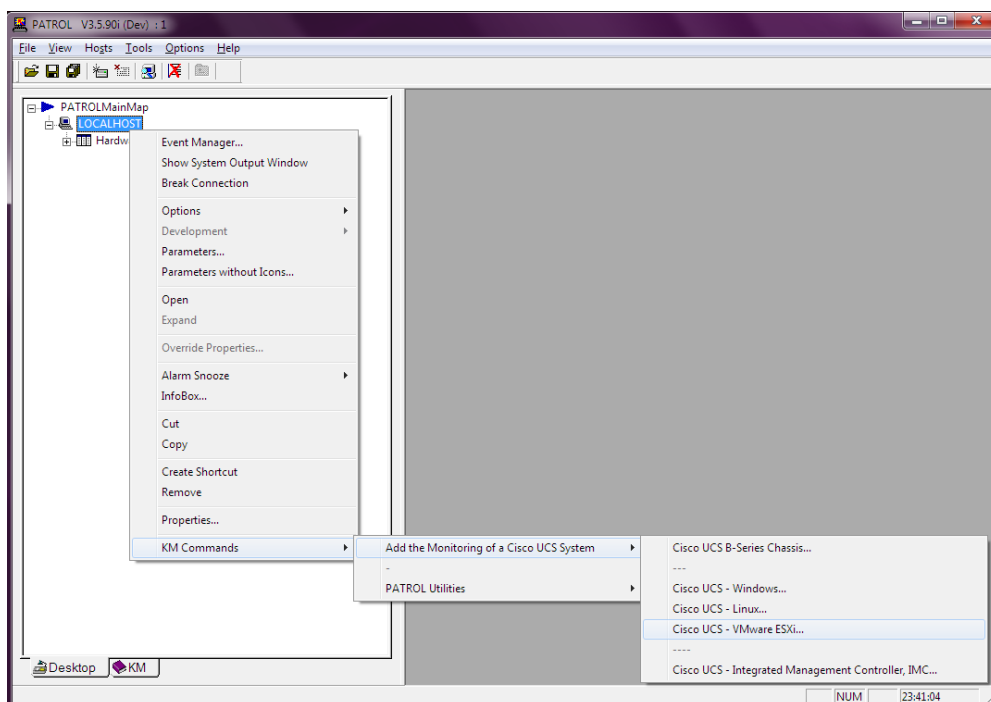
Supported versions of VMWare ESXi or ESX on Cisco UCS.

Installation

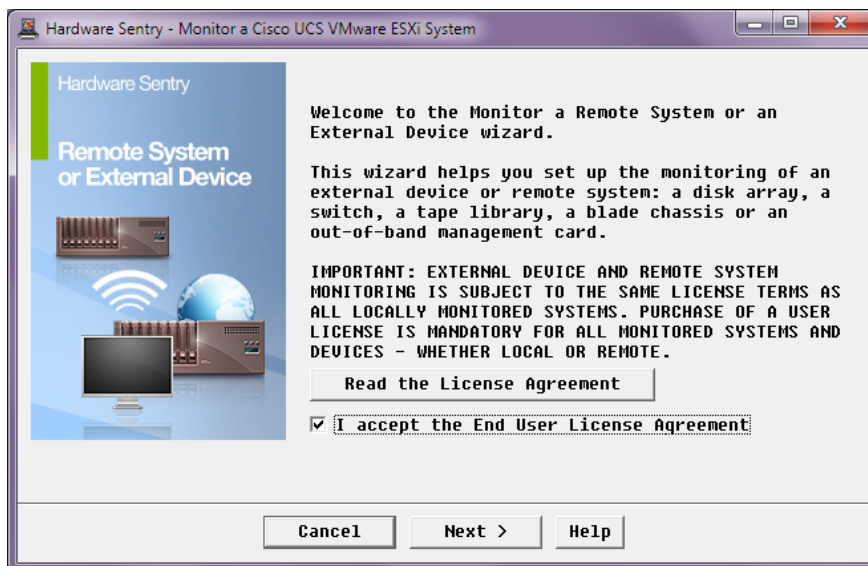
Nothing additional needs to be installed. Everything will be performed from the central PATROL Agent and Console.

Configuration

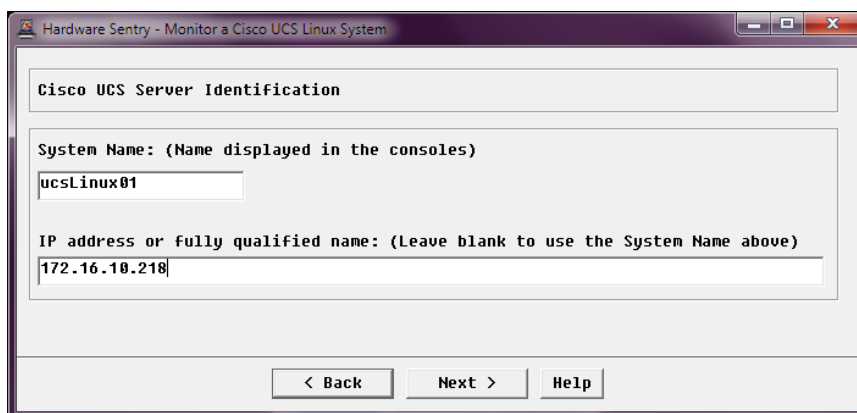
In the PATROL Console, right-click on the main PATROL Agent icon > KM Commands > Add the Monitoring of a Cisco UCS System > Cisco UCS – VMware ESXi...



Monitor a Cisco UCS VMware ESXi System appears. Check the box to accept the condition of the software license agreement of this product.

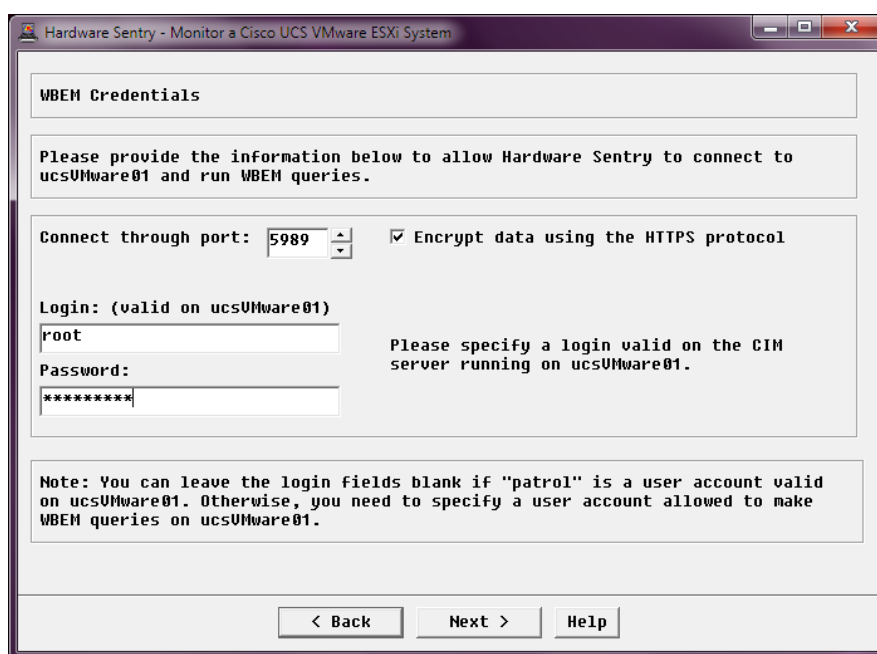


In the next step, enter the system name as it will be displayed in the PATROL Console. Specify its IP address or fully qualified name if it is different from the display name used above.



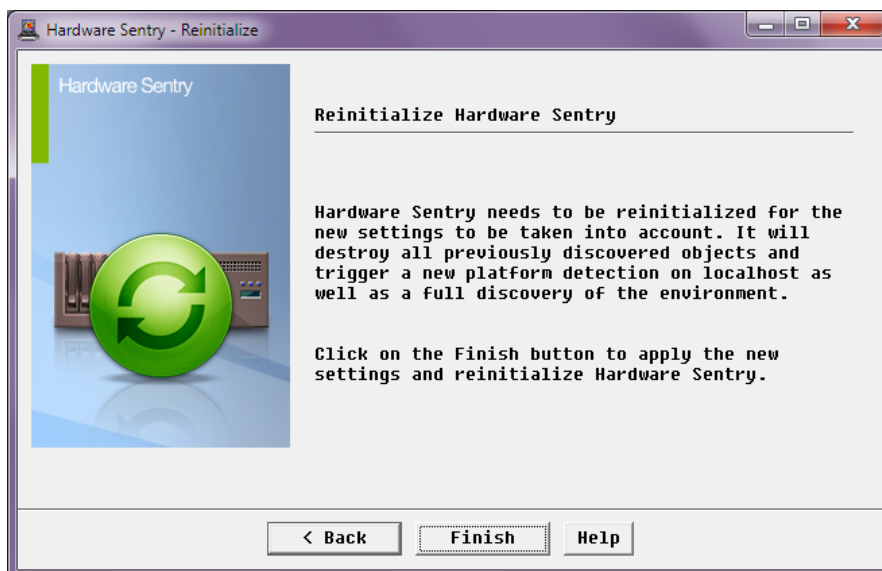
The screenshot shows a window titled "Hardware Sentry - Monitor a Cisco UCS Linux System". The main section is "Cisco UCS Server Identification". It contains two text input fields: "System Name: (Name displayed in the consoles)" with the value "ucsLinux01" and "IP address or fully qualified name: (Leave blank to use the System Name above)" with the value "172.16.10.210". At the bottom are three buttons: "< Back", "Next >", and "Help".

Specify the WBEM credentials to connect to the VMware ESXi system. These are the same as the one use to connect with the VMware vSphere Client.



The screenshot shows a window titled "Hardware Sentry - Monitor a Cisco UCS VMware ESXi System". The main section is "WBEM Credentials". It contains a text area with the instruction: "Please provide the information below to allow Hardware Sentry to connect to ucsVMware01 and run WBEM queries." Below this are two input fields: "Connect through port:" with a dropdown menu showing "5989" and a checkbox labeled "Encrypt data using the HTTPS protocol" which is checked. Below these are two more input fields: "Login: (valid on ucsVMware01)" with the value "root" and "Password:" with the value "*****". To the right of the password field is a text label: "Please specify a login valid on the CIM server running on ucsVMware01." At the bottom is a text area with a note: "Note: You can leave the login fields blank if 'patrol' is a user account valid on ucsVMware01. Otherwise, you need to specify a user account allowed to make WBEM queries on ucsVMware01." At the bottom are three buttons: "< Back", "Next >", and "Help".

In the last step, click Finish and Hardware Sentry KM reinitializes itself and after a couple minutes discovers all the internal components of the Cisco UCS server.



A new icon is created in the PATROL Console, corresponding to the monitoring of the hardware of this Cisco UCS VMware ESXi server.

Monitoring a Cisco UCS Server through its IMC

Principle

Cisco UCS C-Series servers (rack-mount) are equipped with an Integrated Management Controller (or IMC) which accessible out-of-band with its own IP address on the network.

The Cisco IMC is actually an enhanced Baseboard Management Controller (BMC) following Intel's IPMI instrumentation standard. The Cisco IMC has a Web interface which lets administrators configure the underlying hardware and visualize its status. It is also supports the IPMI-over-LAN protocol (RCMP+ on port UDP/623).

Hardware Sentry KM is able to connect to the Cisco IMC directly using the IPMI-over-LAN protocol and access the hardware information of the Cisco UCS C-Series server.

The main benefit of interrogating the Cisco IMC is that it does not depend on the operating system. Even when the main system is turned off or crashed, the Cisco IMC is still able to provide information about the hardware. This is what is called "out-of-band" monitoring, as opposed to "in-band" monitoring when going through the operating system.

Prerequisites

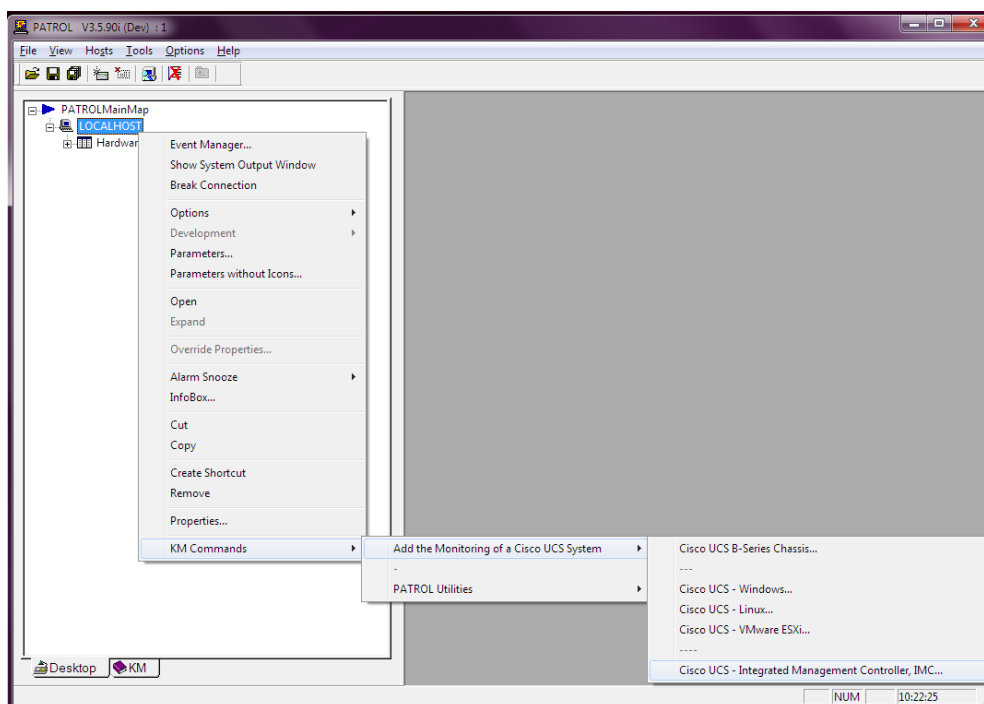
The Cisco IMC must have been configured to operate on the network and be accessible through the IPMI-over-LAN protocol.

Installation

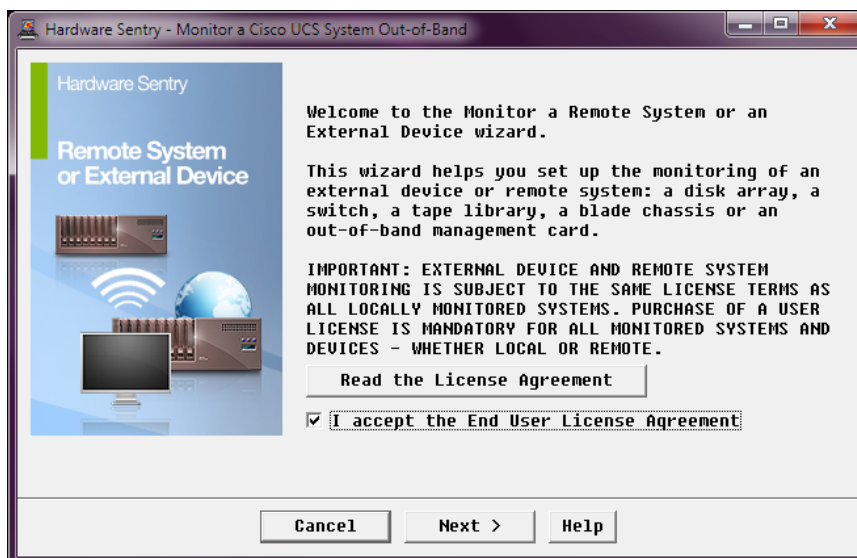
Nothing additional needs to be installed. Everything will be performed from the central PATROL Agent and Console.

Configuration

In the PATROL Console, right-click on the main PATROL Agent icon > KM Commands > Add the Monitoring of a Cisco UCS System > Cisco UCS – Integrated Management Controller, IMC...



The Monitor a Cisco UCS VMware System Out-of-Band appears. Check the box to accept the condition of the software license agreement of this product.



In the next step, enter the system name as it will be displayed in the PATROL Console. Specify its IP address or fully qualified name if it is different from the display name used above.

Hardware Sentry - Monitor a Cisco UCS System Out-of-Band

Cisco UCS Integrated Management Controller (IMC) Identification

System Name: (Name displayed in the consoles)
ucsIMC01

IP address or fully qualified name: (Leave blank to use the System Name above)
172.16.11.173

Note: Please specify the name or IP address of the IMC out-of-band management card.

< Back Next > Help

Specify the credentials to connect to the Cisco Integrated Management Controller. User level privilege is sufficient for Hardware Sentry KM to gather the hardware information from the Cisco IMC.

Note: These are not the same as the credentials used to connect to the operating system.

Hardware Sentry - Monitor a Cisco UCS System Out-of-Band

IPMI over LAN Credentials

Please provide the information below to allow Hardware Sentry to connect to ucsIMC01 through the IPMI-over-LAN protocol (UDP/623).

Login: (valid on ucsIMC01)
admin

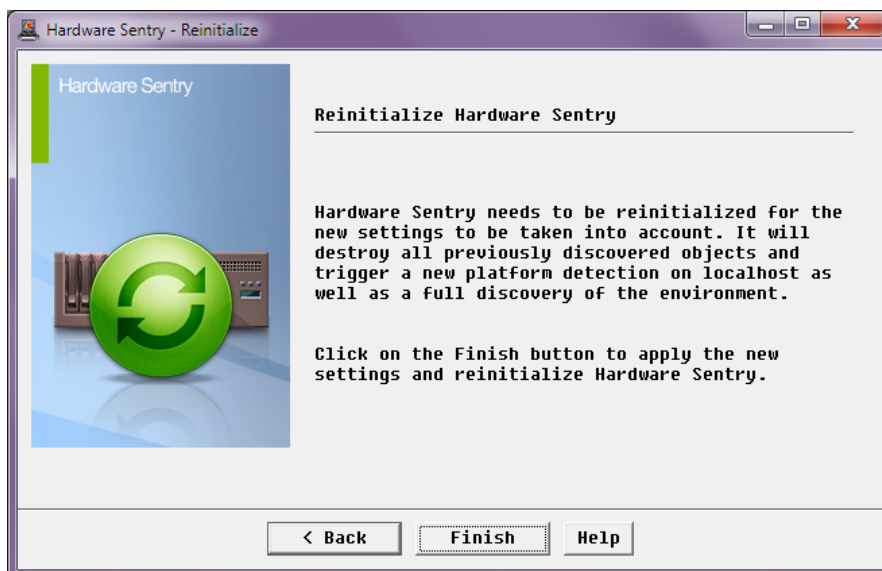
Password:

Specify a username and password able to connect to the system management chip (the Baseboard Management Controller, BMC) through the IPMI-over-LAN interface.

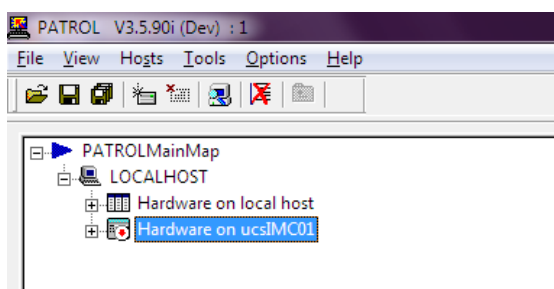
Note: The specified credentials need to be explicitly enabled for remote connection on ucsIMC01. This can be done in-band from the managed system, or from its BIOS interface. The required privilege level is 'USER'.

< Back Next > Help

In the last step, click Finish and Hardware Sentry KM reinitializes itself and after a couple minutes discovers all the internal components of the Cisco UCS server.



A new icon is created in the PATROL Console, corresponding to the monitoring of the hardware of this Cisco UCS server.



After a couple minutes, Hardware Sentry KM has completed its initial discovery of the system and displays the internal components of the server in the console.

Monitoring a Cisco UCS B-Series Blade Chassis

Principle

The Cisco UCS B-Series infrastructure consists of:

- A main chassis (UCS 5108) with the blade servers (B-Series)
- One or two (for HA) Fabric Interconnect Switches (6120 or 6140).

The switches are responsible for linking of the blade servers to the LAN and to a SAN (optional). The switch is capable of handling both traffics on the same backplane (actually everything is 10 Gb/s Ethernet, and SAN traffic is encapsulated into Ethernet frames).

The switch is also responsible for the management of the entire platform. UCS Manager, the Cisco built-in administration tool, is actually a Web application running on the switch itself. It gives visibility on the health of the main chassis (temperature, cooling, powering), the health of the interconnect switches (temperature, cooling, powering, connectivity) and an overall status of each blade server.

In order to cover the entire UCS B-Series platform, Hardware Sentry KM connects to the switch (through Cisco's native UCS XML API) to gather all metrics related to the main chassis and the switch.

Note: The KM also needs to connect to each blade server individually in order to gather internal metrics are not available through UCS Manager: storage subsystem, network traffic, a few environmental parameters. Please refer to the previous “Monitoring a Cisco UCS server” sections for more details.

Prerequisites

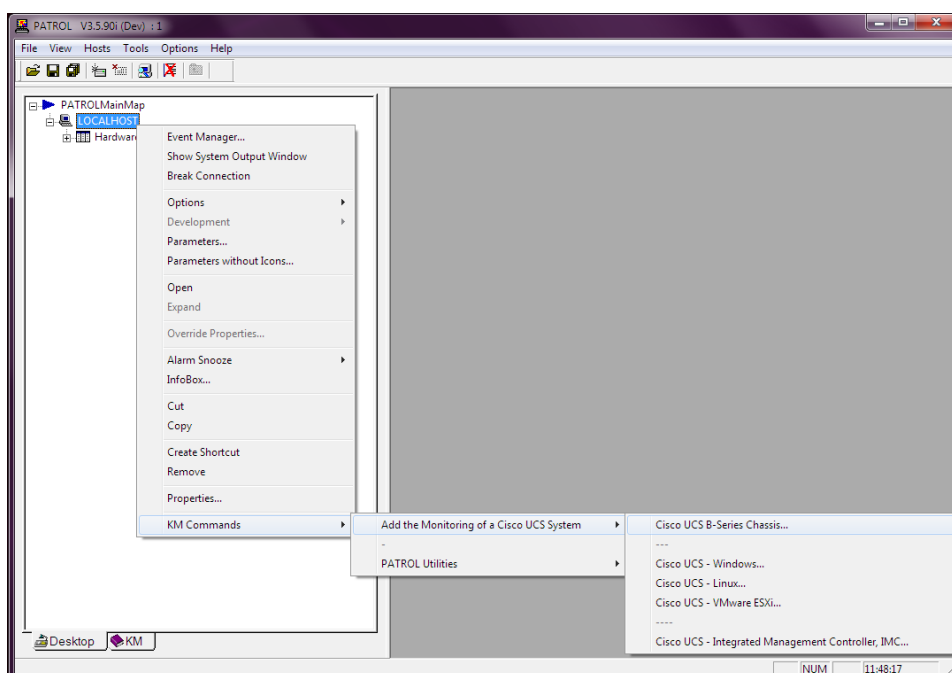
The only requirement is to have a login and password able to connect to the UCS Manager with operator privilege.

Installation

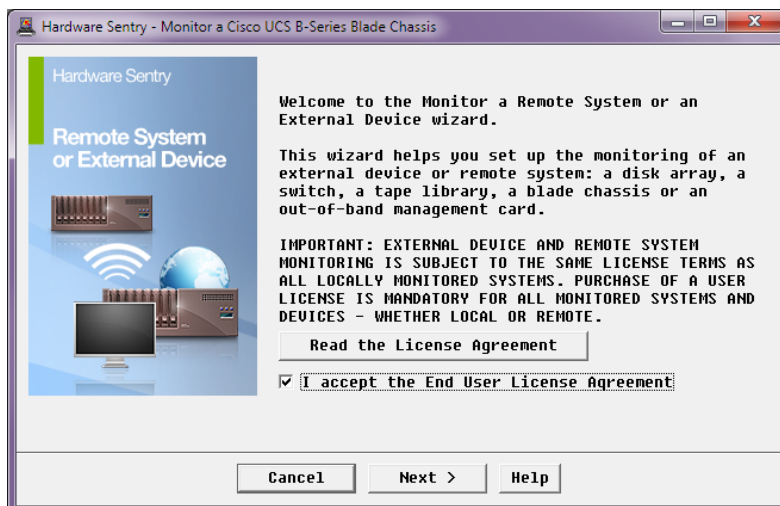
Nothing additional needs to be installed. Everything will be performed from the central PATROL Agent and Console.

Configuration

In the PATROL Console, right-click the main PATROL Agent icon > KM Commands > Add the Monitoring of a Cisco UCS System > Cisco UCS – Cisco UCS B-Series Chassis....



The Monitor a Cisco UCS B-Series Blade Chassis appears. Check the box to accept the condition of the software license agreement of this product.



In the next step, enter the system name as it will be displayed in the PATROL Console. Specify its IP address or fully qualified name if it is different from the display name used above.

Cisco UCS B-Series Chassis Identification

System Name: (Name displayed in the consoles)
ucsBladeChassis01

IP address or fully qualified name: (Leave blank to use the System Name above)
10.20.30.16

Note: Please specify the name or IP address of the Cisco UCS Fabric Interconnect Switch, i.e. where the UCS Manager Web/Java interface runs.

< Back Next > Help

Specify the credentials to connect to the Fabric Interconnect Switch. Operator level privilege is sufficient for Hardware Sentry KM to gather the hardware information from the Cisco UCS Manager through the Cisco UCS XML API.

Cisco UCS Credentials

Please provide the information below to allow Hardware Sentry to connect to ucsBladeChassis01 (the Cisco UCS Fabric Interconnect Switch) and send native UCS XML API requests to it.

☒ Encrypt data using the HTTPS protocol

Login: (valid on ucsBladeChassis01)
admin

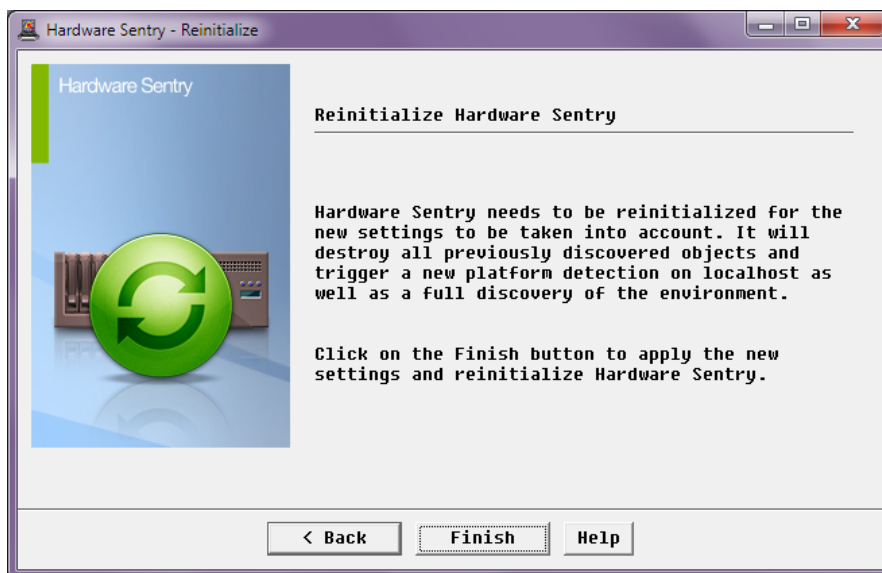
Password:

Please specify a login able to connect to the Cisco UCS Manager running on the Fabric Interconnect Switch (ucsBladeChassis01).

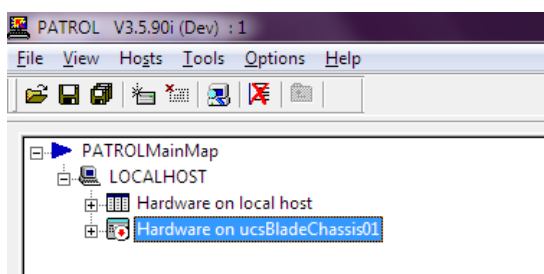
Note: The credentials specified need to have sufficient privileges to be able to make native UCS XML API calls, in read-only mode.

< Back Next > Help

In the last step, click Finish and Hardware Sentry KM reinitializes itself and after a couple minutes discovers all the internal components of the Cisco UCS B-Series Blade Chassis.



A new icon is created in the PATROL Console, corresponding to the monitoring of the hardware of this Cisco UCS server.



After a couple minutes, Hardware Sentry KM has completed its initial discovery of the system and displays the internal components of the server in the console.

Conclusion

The close collaboration established between BMC, Sentry Software and Cisco teams has made possible the development of a solution specifically dedicated to the monitoring of Cisco UCS environment. Sentry Software Monitoring for BMC ProactiveNet Performance Management – Hardware Monitoring – Cisco UCS Edition transforms the way you manage the hardware health of your Cisco UCS infrastructure and helps you take incremental steps towards the objectives of your BSM strategy.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)