USER GUIDE

HYCU SCOM Management Pack for Nutanix

Product version: 2.5
Product release date: May 2018
Document edition: First

HYCU

Legal notices

Copyright notice

Trademarks

HYCU logos, names, trademarks and/or service marks and combinations thereof are the property of HYCU or its affiliates. Other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

Citrix, the Citrix Receiver logo, StoreFront, XenApp, and XenDesktop are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

Microsoft, SharePoint, SQL Server, Windows, Windows Design 2001, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Nutanix and Prism are trademarks of Nutanix, Inc. in the United States and/or other jurisdictions.

Disclaimer

The details and descriptions contained in this document are believed to have been accurate and up to date at the time the document was written. The information contained in this document is subject to change without notice.

HYCU provides this material "as is" and makes no warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. HYCU shall not be liable for errors and omissions contained herein. In no event shall HYCU be liable for any direct, indirect, consequential, punitive, special or incidental damages, including, without limitation, damages for loss and profits, loss of anticipated savings, business interruption, or loss of information arising out of the use or inability to use this document, or any action taken based on the information contained herein, even if it has been advised of the possibility of such damages, whether based on warranty, contract, or any other legal theory.

The only warranties for HYCU products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty.

Notice

This document is provided in connection with HYCU products. HYCU may have copyright, patents, patent applications, trademark, or other intellectual property rights covering the subject matter of this document.

Except as expressly provided in any written license agreement from HYCU, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property on HYCU products. Use of underlying HYCU product(s) is governed by their respective Software License and Support Terms.

Important: Please read Software License and Support Terms before using the accompanying software product(s).

HYCU
www.hycu.com

Contents

Chapter 1

Introduction

This chapter introduces HYCU SCOM Management Pack for Nutanix and explains how it interacts with Nutanix Enterprise Cloud Platform and Microsoft System Center Operations Manager.

About HYCU SCOM Management Pack for Nutanix

HYCU SCOM Management Pack for Nutanix (SCOM MP for Nutanix) is an availability and performance management solution that extends end- to-end service monitoring capabilities of SCOM to include Nutanix infrastructure. As a SCOM add-in, SCOM MP for Nutanix is designed similarly to other Management Pack products that extend SCOM.

SCOM MP for Nutanix enables IT teams to monitor Nutanix hyperconverged infrastructure with SCOM. It provides an extensive set of features needed by IT for health, availability, infrastructure, and application performance monitoring:

- Discovery, visualization, and updates for Nutanix nodes, clusters, virtual machines, storage, data protection, and replication
- Health monitoring for Nutanix nodes, clusters, virtual machines, storage, data protection, and replication, using descriptive alerts and knowledge base
- Detection and grouping of the application specific virtual machines, by using the Application Awareness feature
- Complete, quick, and convenient overview of Nutanix environment by using intuitive high-level dashboards

SCOM MP for Nutanix enables you to do the following:

- **Monitor disk health and performance**

  Disk health and performance may not impact the VMs due to the replication and redundancy, but you need visibility to make sure the device is at its full capability. You can continually monitor disk health and performance by referencing the hardware topology view which shows a complete overview of Nutanix storage, current status, and any alerts.

- **Assure high availability of business-critical applications**

  Monitoring of replication for protection domain is the key to the service high availability. Having an up to date replica of the protection domain will maintain optimal service and reference any alerts that occur in relation to it. You can quickly identify any of the replication issues and proactively remediate by acting on alerts containing resolution steps.

- **Detect business-critical applications running on Nutanix infrastructure**

  Knowing which business critical applications are running within Nutanix cluster helps you understand the roles of each virtual machine and resources consumed. You can quickly identify application environments running on Nutanix and related virtual machines with their roles in the application dashboard, which groups related virtual machines together.

- **Monitor virtual machines**

  Nutanix infrastructure relies on the CVM (Nutanix Controller VM), which makes monitoring of CVM status vital to the flow of key resources to Nutanix clusters. You can immediately identify CVM status which contains detailed information about the health, alerts, and possible resolution steps which keep your Nutanix environment at maximum resources.

- **Monitor hardware components**

  By monitoring statuses of hardware sensors, for example, fan rotation speed sensor, CPU temperature sensor, and power supply voltage sensor, you can quickly notice conditions that might eventually cause a system halt and reduce availability at inconvenient times. Reacting to such alerts in time can help you prevent such unplanned occurrences.

- **Monitor HYCU Data Protection – a Nutanix backup and recovery solution by HYCU, Inc.**

  By monitoring availability of HYCU Data Protection backup controllers (virtual machines), you are quickly informed about their offline state, HYCU Data Protection REST web service unavailability, and other problems that render connectivity impossible. In such circumstances, raised alerts help you resolve the problem in time and guarantee that backups scheduled in HYCU Data Protection are not missed.

  By monitoring compliancy of Nutanix virtual machines protected by HYCU Data Protection, you can react in time and help in ensuring that their data protection does not deteriorate.

SCOM MP for Nutanix fully integrates topology, health, and performance data into the SCOM Operations console.

Product architecture

SCOM MP for Nutanix is installed on a SCOM management server. It uses a sophisticated component called HYCU SCOM Data Collector for Nutanix (SCOM Data Collector for Nutanix or simply Data Collector) that is installed on a SCOM management server or a proxy system. SCOM Data Collector for Nutanix connects to one or more Nutanix clusters through the Nutanix REST API interface. It optimizes the interface response by filtering redundant data from data stream, and therefore reduces load on SCOM workflows. SCOM Data Collector for Nutanix makes the product application aware through the Application Awareness feature.

The following diagram shows how SCOM MP for Nutanix connects the SCOM platform and the Nutanix infrastructure.

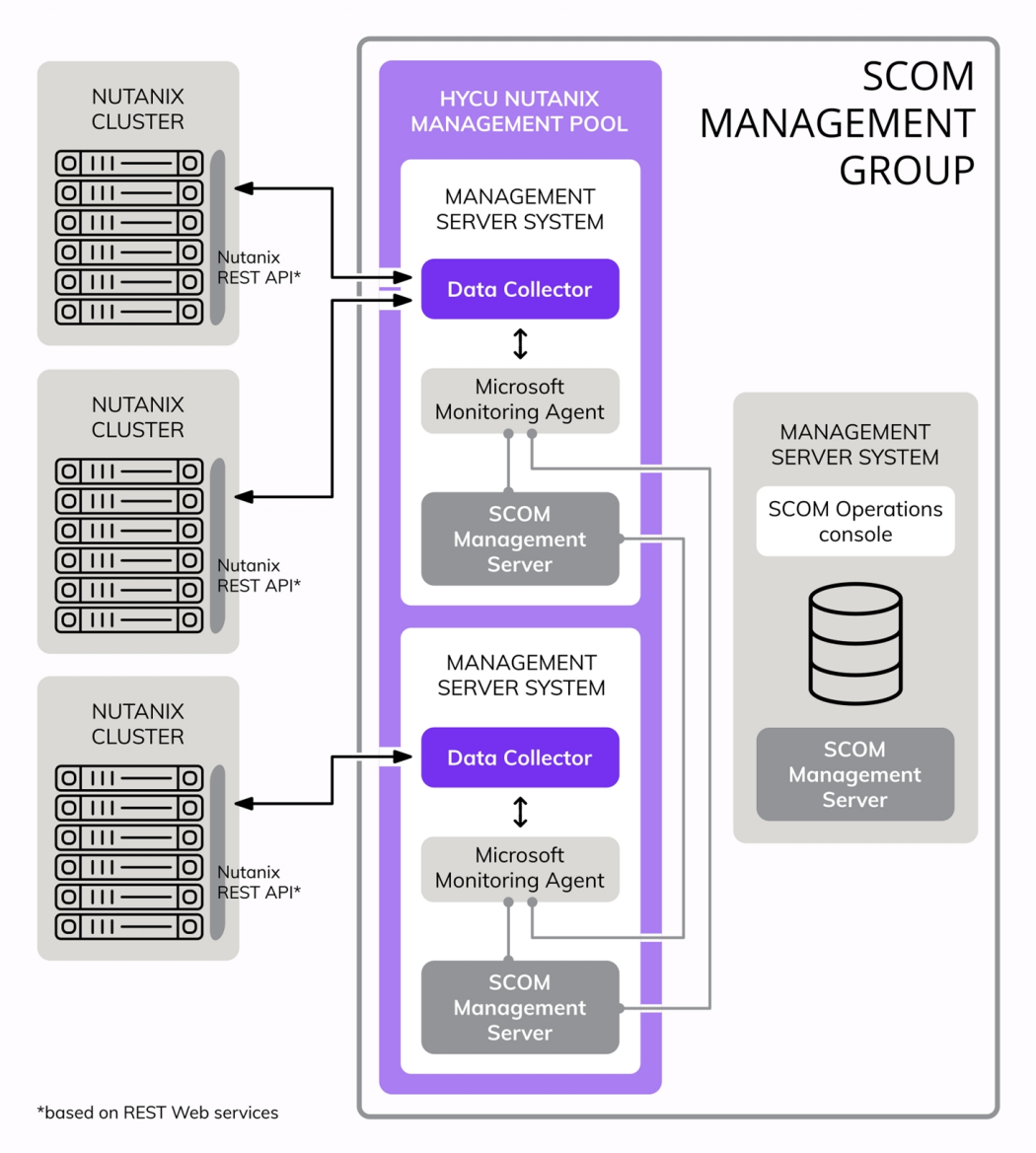

Figure 1–1: High-level overview of the SCOM MP for Nutanix environment

About Nutanix

Nutanix delivers enterprise computing and storage featuring built-in virtualization.

Nutanix hyperconverged infrastructure natively integrates servers, storage network, and storage into a single x86-based server deployed in scale-out clusters. Nodes (host systems) that are part of the enterprise-scale clusters run industry-standard or native hypervisors and the Nutanix operating system (AOS, formerly known as NOS). Each server contains x86-64 processors, memory, solid state drives (SSDs), and traditional hard disk drives (HDDs) that aggregate storage resources into a single storage pool. Capacity is added by adding nodes to the computing cluster.

Built-in virtualization allows applications and data to move freely between on-premises environments and public clouds. All data, metadata, and operations are distributed across the entire cluster combining physical and virtual storage. Such combined functionality eliminates performance bottlenecks, enables predictable scalability without limits, reduces power and space consumption, and eliminates storage complexity.

Nutanix Enterprise Cloud Platform features predictable performance, cloud-like infrastructure consumption, robust security, and application mobility for a broad range of enterprise applications without infrastructure constraints. The infrastructure is truly invisible, shifting focus back to applications.

About System Center Operations Manager

System Center Operations Manager (SCOM), a component of Microsoft System Center, is a cross-platform data center management system that allows you to monitor devices, services, and operations for many computer systems from a single console. By using SCOM you can check the following aspects of discovered objects in your monitored environment:

- Availability
- Health
- Performance
- Configuration aspects
- Security aspects

When problems are detected with any of the above conditions, SCOM can send alerts that inform you properly. They help you identify root problem causes and define effective solutions.

Chapter 2

Installation and configuration

This chapter contains instructions for installing, verifying the installation of, and configuring SCOM MP for Nutanix by using configuration wizards included in the product.

Feature overview

SCOM MP for Nutanix consists of the following components (presented as features and subfeatures by the product's Setup Wizard):

Component	Description
General components	A container with general components of the product.
Application Awareness	A component that provides identification of the applications installed on Nutanix virtual machines. It contains charts and tables with infrastructure and virtual machine-related data. It also gives you an option of generating lists of most intensive processes with regards to CPU usage or memory consumption. This is a subfeature of General components.
Dashboards	A component that provides presentation dashboards for overview of Nutanix hardware, storage, virtual machines, and data protection. This is a subfeature of General components.
Advanced Dashboards	A component that provides presentation dashboards for overview of the entire Nutanix environment. This is a subfeature of General components.
Hardware monitoring	A component that provides detailed information on current Nutanix hardware condition. This is a subfeature of General components.
HYCU Data Protection monitoring	A component that provides monitoring for HYCU Data Protection, a Nutanix backup and recovery solution by HYCU, Inc. In this scope, HYCU Data Protection backup controllers

Component	Description
	and virtual machines protected by HYCU Data Protection are monitored. This is a subfeature of General components.
Reports	A component that provides detailed information about the monitored Nutanix environment. It contains charts and tables with infrastructure and virtual machine-related data. This is a subfeature of General components.
SuperPacks	A container of dashboards that correlate information collected by SCOM MP for Nutanix and other SCOM add-ins (Management Pack products).
Citrix XenApp and XenDesktop	A component that provides dashboards for correlation of information from SCOM MP for Nutanix with information from Citrix SCOM Management Pack for XenApp and XenDesktop. It bridges the gap between the Nutanix infrastructure and Citrix as a Nutanix workload by providing dashboards for various scenarios, for example, correlating Citrix site session data with Nutanix cluster resource usage. These dashboards combine data from the Nutanix and Citrix infrastructures. This is a subfeature of SuperPacks.
Microsoft Exchange Server	A component that provides dashboards for correlation of information from SCOM MP for Nutanix with information from Microsoft Exchange Server Management Pack. This is a subfeature of SuperPacks.
Microsoft SQL Server	A component that provides dashboards for correlation of information from SCOM MP for Nutanix with information from Microsoft System Center Management Pack for SQL Server. This is a subfeature of SuperPacks.
Data Collector service	SCOM Data Collector for Nutanix. A component that collects data from Nutanix clusters and makes it available for monitoring in SCOM. It is implemented as a service which listens for requests and acts as a proxy. SCOM and SCOM Data Collector for Nutanix communicate with each other by using HTTPS or HTTP, through the default port that can be changed during product installation. SCOM Data Collector for

Component	Description
	Nutanix uses REST Web services interface to connect to Nutanix clusters. It uses filtering of redundant data to optimize interface response and reduce load on SCOM workflows. SCOM Data Collector for Nutanix makes the product application aware through the Application Awareness feature.

Installing SCOM MP for Nutanix

This section contains instructions for installing SCOM MP for Nutanix.

Installation prerequisites

Before installing SCOM MP for Nutanix, make sure that the following prerequisites are fulfilled for each cluster, virtual machine, or application that you plan to monitor:

- Versions or editions of the following products that you are using are compatible with SCOM MP for Nutanix:
  - Nutanix AOS
  - Nutanix Acropolis
  - Microsoft System Center Operations Manager

  For a list of the supported versions and editions, see the *HYCU SCOM Management Pack for Nutanix Compatibility Matrix*.
- **Nutanix Enterprise Cloud Platform prerequisites:**
  - For a Nutanix cluster, a Nutanix user account is selected.

    HYCU recommends that you select a user account that has Viewer role assigned in Nutanix Prism and can therefore only view information (and collect monitoring data).
  - *Mandatory for low-level hardware monitoring.* For a Nutanix cluster, a user account is selected that can access hardware sensors on the cluster nodes through their IPMI implementation. SCOM MP for Nutanix supports configurations with different user accounts for different cluster nodes.

    Credentials of the default IPMI user account on Nutanix cluster nodes are usually as follows:
    - User name: `ADMIN`
    - Password: `ADMIN`

    SCOM MP for Nutanix uses these credentials by default, but you can adjust that as part of product configuration. Adjustment may also be required with clusters that are based on non-Nutanix hardware.

- *Mandatory for monitoring virtual machines running Linux.* On a virtual machine that is running Linux, the operating system is configured such that:
  - SSH server is enabled and running.
  - SSH server is configured to require password authentication at logon.
  - Inbound network traffic on port 22 is enabled in the firewall.

  > ⚠ Important If these prerequisites are not fulfilled for the virtual machine:
  > - A list of the most CPU- intensive processes is not included in the User VM CPU Load alerts for this virtual machine.
  > - You cannot run the following SCOM tasks for this virtual machine: Get Processes on Selected VM Sorted By Memory, Get Processes on Selected VM Sorted By CPU.

- **Application Awareness prerequisites:**
  - On a virtual machine where applications reside:
    - A supported operating system is running.

      For a list of the supported operating systems, see the *HYCU SCOM Management Pack for Nutanix Compatibility Matrix*, section *Application Awareness*.
    - Windows Remote Management (WinRM) is enabled.
  - A user account is selected that has operating system administrative privileges on a virtual machine where applications reside.

    > 🗒 Note When planning to monitor multiple virtual machines, HYCU recommends that you select the same user account for as many virtual machines as possible.
  - For an application, an administrative application user account is selected. For example, to monitor Microsoft Exchange Server, you must know credentials of the Microsoft Exchange Server administrator user account.
- **SuperPacks prerequisites:**
  - Application Awareness prerequisites are fulfilled.
  - Appropriate third-party SCOM add-ins (Management Pack products) are installed on each involved SCOM management server, depending on the applications whose data you want to correlate.

    For a list of the required Management Pack products and links to their download webpages, see the *HYCU SCOM Management Pack for Nutanix Compatibility Matrix*, section *SuperPacks*.
- **HYCU Data Protection monitoring prerequisites:**
  - For each HYCU Data Protection instance, an administrative HYCU Data Protection user account is selected. Such account has the Protection Service property set to Built-in Administrator or Administrator.

Installation overview

The process of installing SCOM MP for Nutanix consists of four tasks:

1. Install SCOM MP for Nutanix on the SCOM management server.

   For instructions, see "Installing the product on SCOM management server" below.
2. Verify the product installation.

   For instructions, see "Verifying product installation on SCOM management server" on page 17.
3. *Mandatory if automatic import is not performed.* Manually import included management packs to SCOM management server.

   For instructions, see "Manually importing included management packs" on page 17.
4. *Mandatory if automatic import is not performed.* Verify the management packs import.

   For instructions, see "Verifying import of included management packs" on page 18.

Complete the tasks in the documented order of precedence.

Installing the product on SCOM management server

To install SCOM MP for Nutanix on the SCOM management server, do the following:

1. Go to the Nutanix Monitoring - HYCU webpage and sign in with your account credentials.

   If you do not have an account yet, apply for it at the following email address: support@hycu.com
2. When you are signed in, under Product download, click **HYCU SCOM Management Pack for Nutanix**.
3. Read through the Software License and Support Terms text. If you agree with the terms, click **Accept** and proceed.
4. In the Product download link line, click **Download** to transfer the product release archive and save it on the local system.
5. Copy the product release archive to the SCOM management server.
6. Log on to the SCOM management server with a user account that is assigned the Operations Manager Administrators user role.
7. In Windows Explorer, locate the `HYCU.SCOM.MP.Nutanix.<Version>.zip` file and extract its contents.
8. Locate the extracted `HYCU.SCOM.MP.Nutanix.msi` file and double-click it. The Setup Wizard starts.
9. Follow instructions of the Setup Wizard.
10. In the Custom Setup page, when prompted to select features for installation, consider the following points:

- By default, all features and subfeatures are selected for installation.
- The `General components` feature is required for initial deployment. It can be installed on one SCOM management server and later added to other management servers as needed. It can also be installed without its subfeatures. To install `Data Collector service` only, omit this feature completely.

  This feature includes the following subfeatures:

  - `Application Awareness`
  - `Dashboards`
  - `Advanced dashboards`
  - `Hardware monitoring`
  - `HYCU Data Protection monitoring`
  - `Reports`
- `SuperPacks` includes the following subfeatures:
  - `Citrix XenApp and XenDesktop`
  - `Microsoft Exchange Server`
  - `Microsoft SQL Server`

  > ⚠ Important Any subfeature of `SuperPacks` requires the `Application Awareness` subfeature of `General components` to be installed as well.
- `Data Collector service` should be installed on every SCOM management server that will be included in HYCU Nutanix Management Pool.

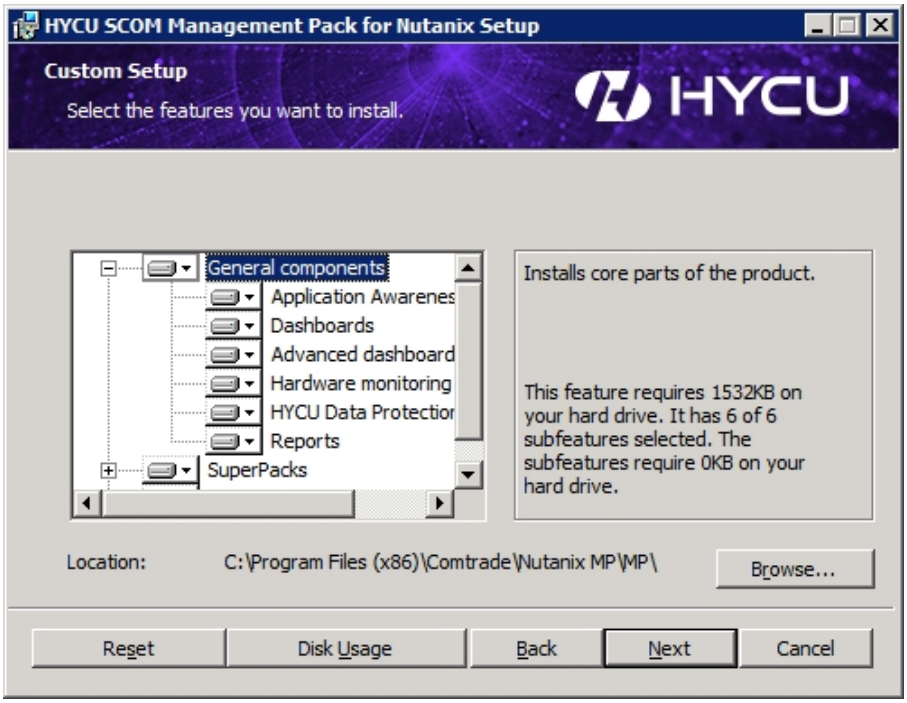

Figure 2–1: Custom Setup page of SCOM MP for Nutanix Setup Wizard

Clear selection of the features or subfeatures that you do not plan to use and click **Next**.

11. In the Data Collector Service Settings page, specify port for SCOM Data Collector for Nutanix (the `Data Collector service` feature). To use SSL encryption to secure communication, select **Use SSL encryption** option. If this option is selected, the SSL certificate of the product is imported to your system as trusted.

    Click **Next**.

12. In the Install HYCU SCOM Management Pack for Nutanix page, if you want that the management packs (included in the product) are imported into SCOM automatically, select **Automatically import included management packs**. Click **Install** to start the installation process.

    > Note Automatic import is possible only if all required management packs are available. If the import is not possible, a warning message prompts you to import the management pack manually.

13. When the installation completes, click **Finish**.

Verifying product installation on SCOM management server

To verify that the SCOM MP for Nutanix installation on the SCOM management server computer is correct, do the following:

1. Log on to the SCOM management server computer.
2. Go to **Start > Control Panel** and click **Programs and Features**.
3. Verify that the following entry is present in the Name column:

   `HYCU SCOM Management Pack for Nutanix`
4. Go to **Start > Administrative Tools** and double-click **Services**.
5. Verify that the following entry is present in the Name column:

   `HYCU SCOM Data Collector for Nutanix`
6. Right-click the entry and select **Properties**.
7. In the HYCU SCOM Data Collector for Nutanix Properties (Local Computer) window, on the General property page, verify that value of the Service status field reads `Running`.
8. If you selected to automatically import the included management packs, verify the import success. For instructions, see "Verifying import of included management packs" on the next page.

Manually importing included management packs

SCOM MP for Nutanix Setup Wizard provides automatic import of the sealed management packs that are included in the product. If the automatic import fails or you want to import

the management packs into SCOM manually, do the following:

1. Launch the SCOM Operations console and connect to the management server.
2. In the Administration view, right-click **Management Packs**, and then select **Import Management Packs**. The Import Management Packs wizard opens.
3. In the Import Management Packs wizard, click **Add** and then select Add from disk.

   When prompted to search the online catalog for dependencies, click **No**. The Select Management Packs to import window opens.
4. In the Select Management Packs to import window, browse to the installation folder of the included management packs (default path: `%ProgramFiles (x86)%\Comtrade\Nutanix MP\MP\`), select all the SCOM MP for Nutanix-related packages, and then click **Open**.
5. On the Install HYCU SCOM Management Pack for Nutanix page, click **Install**.

   The management pack packages are downloaded and imported.

   If there is a problem at any stage of the import process, select the management pack to view the status details. When the import process is complete for a management pack, the management pack status changes to `Imported`. Click **Close**.

Import is possible only if all required SCOM-default management packs are available. You can import missing management packs from the System Center Operations Manager installation directory.

Verifying import of included management packs

To verify that the management packs included in SCOM MP for Nutanix were successfully imported into SCOM, do the following:

1. Launch the SCOM Operations console and connect to the management server.
2. In the **Monitoring** view, in the console tree, verify that the elements listed in the following figures are displayed (the list may differ based on your actual selection of features for the installation):

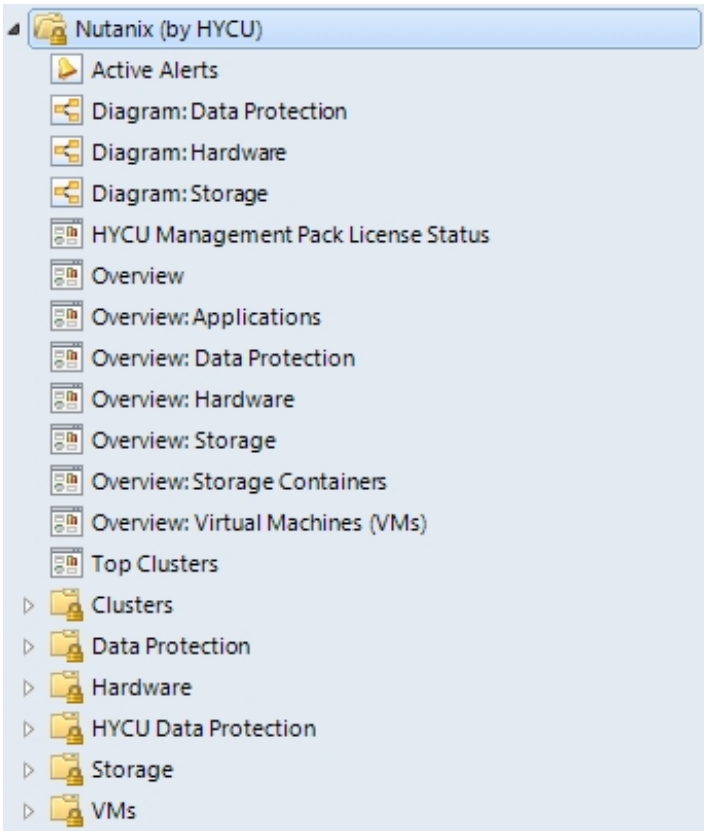

Figure 2–2: Elements of SCOM MP for Nutanix, as seen in the SCOM Operations console (part 1)

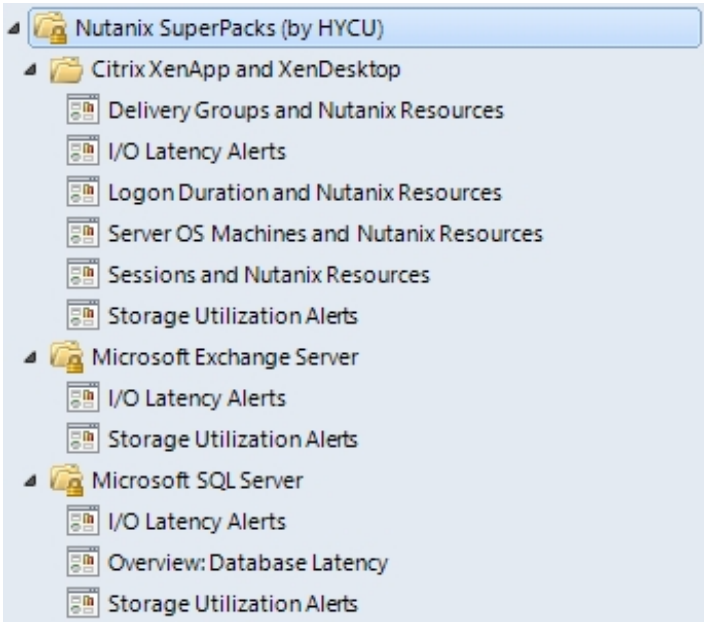

Figure 2–3: Elements of SCOM MP for Nutanix, as seen in the SCOM Operations console (part 2)

3. In the **Administration** view, expand **Administration** and click **Management Packs**.

4. Verify that the following management pack versions are listed in the results pane (the list of management packs may differ based on your actual selection of features for the installation):

   Table 2–1: Management packs included in different product features (installation components)

Feature (installation component)	Management packs	Management pack versions
General components	HYCU Management Pack for Nutanix (Core)	2.5.*x*.*x*
Application Awareness	HYCU Management Pack for Nutanix (Application Awareness)	2.5.*x*.*x*
Dashboards	HYCU Management Pack for Nutanix (Dashboards)	2.5.*x*.*x*
Advanced Dashboards	HYCU Management Pack for Nutanix (Widgets)	2.5.*x*.*x*
	HYCU Management Pack for Nutanix (Advanced Dashboards)	2.5.*x*.*x*
Hardware monitoring	HYCU Management Pack for Nutanix (Hardware Monitors)	2.5.*x*.*x*
HYCU Data Protection monitoring	HYCU Management Pack for Nutanix (HYCU Data Protection)	2.5.*x*.*x*
Reports	HYCU Management Pack for Nutanix (Reports)	2.5.*x*.*x*
SuperPacks	HYCU Management Pack for Nutanix (SuperPacks – Core)	2.5.*x*.*x*
	HYCU Management Pack for Nutanix (SuperPacks – Widgets)	2.5.*x*.*x*
Citrix XenApp and XenDesktop	HYCU Management Pack for Nutanix (SuperPacks: Citrix XenApp and XenDesktop – Resources)	2.5.*x*.*x*
	HYCU Management Pack for Nutanix (SuperPacks: Citrix XenApp and XenDesktop)	2.5.*x*.*x*
Microsoft Exchange Server	HYCU Management Pack for Nutanix (SuperPacks: Microsoft Exchange	2.5.*x*.*x*

Feature (installation component)	Management packs	Management pack versions
	Server)	
Microsoft SQL Server	HYCU Management Pack for Nutanix (SuperPacks: Microsoft SQL Server)	2.5.*x*.*x*
Data Collector service	None	None

Configuring SCOM MP for Nutanix

This section contains instructions for configuring SCOM MP for Nutanix.

Configuration overview

The process of configuring SCOM MP for Nutanix consists of five tasks:

1. Configure HYCU Nutanix Management Pool.

   For instructions, see "Configuring HYCU Nutanix Management Pool" on the next page.
2. Configure SCOM MP for Nutanix connections.

   For instructions, see "Configuring SCOM MP for Nutanix connections" on the next page.
3. *Optional.* Configure the Application Awareness feature.

   For instructions, see "Configuring the Application Awareness feature" on page 24.
4. *Optional.* Configure the SuperPacks feature.

   This feature does not have its own configuration steps, but depends on the configured Application Awareness feature. For Application Awareness configuration instructions, see "Configuring the Application Awareness feature" on page 24.
5. *Optional.* Configure low-level hardware monitoring.

   For instructions, see "Configuring low-level hardware monitoring" on page 30.
6. *Optional.* Configure HYCU Data Protection monitoring.

   For instructions, see "Configuring HYCU Data Protection monitoring" on page 32.

Complete the tasks in the documented order of precedence.

Once the product is configured, you must cover its licensing. For instructions, see "Product licensing" on page 35.

> Tip To configure product-specific SCOM accounts manually rather than by using the configuration wizards in SCOM, follow instructions in appropriate sections in Appendix A:
>
> - "Setting up action account for monitoring Nutanix infrastructure" on page 88
> - "Setting up action account for Application Awareness" on page 89
> - "Setting up action account for individual monitored applications" on page 90

Compliance with Federal Information Processing Standards (FIPS)

SCOM MP for Nutanix does not require special configuration steps for operation in environments that are compliant with the FIPS 140-2 standard. Such environments include the following:

- Microsoft Windows operating system where the security setting for FIPS compliance is enabled in the effective policy
- Microsoft System Center Operations Manager that is running in FIPS-compliant mode

Configuring HYCU Nutanix Management Pool

By default, all SCOM management servers are involved in monitoring the Nutanix infrastructure using SCOM MP for Nutanix. They are automatically added to a custom resource pool named HYCU Nutanix Management Pool. Optionally, you can define which management servers to involve by specially configuring the resource pool and manually adding the management servers to it.

To manually add a SCOM management server to HYCU Nutanix Management Pool, do the following:

1. Launch the SCOM Operations console and connect to the management server.
2. In the Administration view, expand **Resource Pools**, right-click **HYCU Nutanix Management Pool**, and then select **Manual Membership**. In the Manual Membership dialog box, click **Yes**.
3. Right-click **HYCU Nutanix Management Pool** again and select **Properties**.
4. In the HYCU Nutanix Management Pool Properties wizard, in the General Properties page, click **Next**.
5. In the Pool Membership page, click **Add** to select desired SCOM management server.
6. In the HYCU Nutanix Management Pool Properties – Member Selection dialog box, enter you search criterion, and click **Search** to retrieve a list of the available SCOM management server.
7. Under Available items, select the SCOM management server you want in the resource pool, click **Add**, and then click **OK**.
8. In the Pool Membership page, click **Next**.
9. Review your configuration and then click **Save** to save the changes.

Configuring SCOM MP for Nutanix connections

To be able to use SCOM MP for Nutanix, you must configure its connections to Nutanix clusters by using the HYCU SCOM Management Pack for Nutanix: Configuration wizard. For

Nutanix environments that consist of multiple clusters, you must repeat the configuration procedure for each cluster that you plan to monitor.

To configure SCOM MP for Nutanix connection for a Nutanix cluster, do the following:

1. Launch the SCOM Operations console and connect to the management server.
2. In the **Authoring** view, in the Authoring pane, expand **Authoring**.
3. Right-click **Management Pack Templates** and then select **Add Monitoring Wizard**.
4. In the Add Monitoring Wizard window, select **HYCU SCOM Management Pack for Nutanix: Configuration** and then click **Next**.
5. In the Template Name and Description page, specify a name and description of the template, and then specify an object where connection configuration data should be stored. Do one of the following:
   - To select an existing management pack, select it from the **Select destination management pack** drop-down list.
   - To create a new management pack, follow the steps:
     a. Click **New**.
     b. In the Create a Management Pack wizard, in the General Properties page, specify the name, version, and description. Click **Next**.
     c. In the Knowledge page, click **Create**.

   Click **Next**.
6. In the Nutanix Cluster Connection Parameters page, in the Nutanix Cluster Connection Parameters section, specify the following:
   - Fully qualified domain name or IP address of the Nutanix cluster (**Cluster**)
   - *Required if you are using special proxy configuration.* A different number for the Nutanix Prism listening port (**Port**)

     Default value: `9440`.
   - Credentials of the chosen Nutanix user account (**User name**, **Password**)

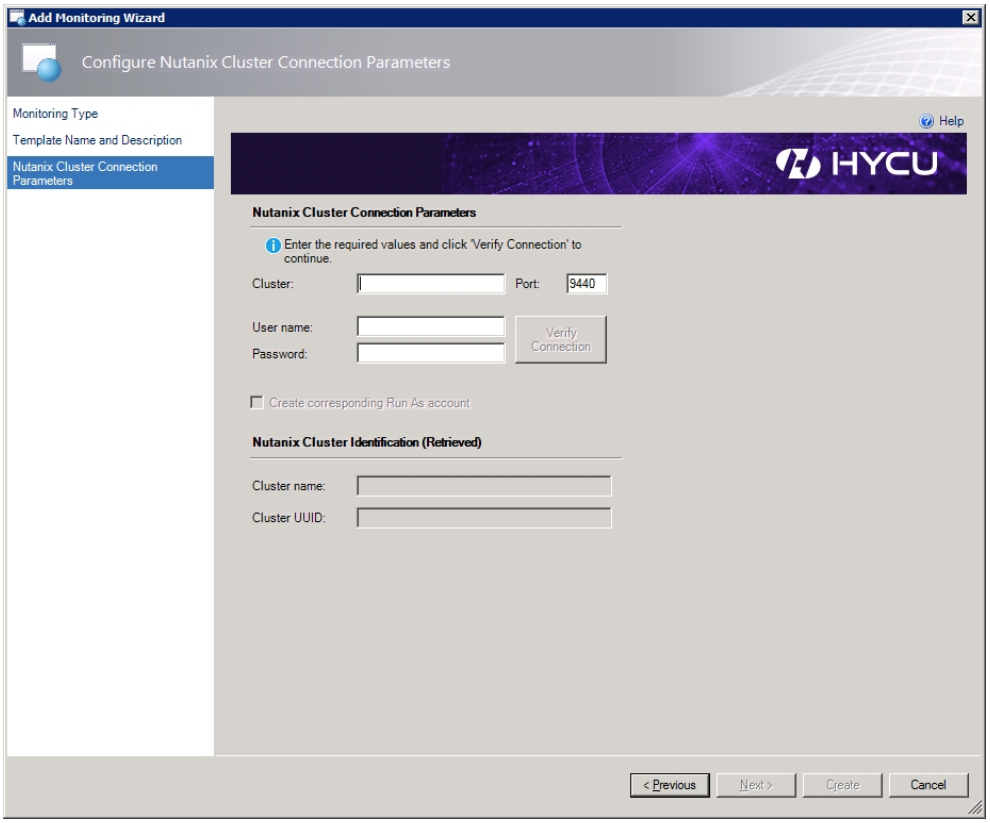

Figure 2–4: Nutanix Cluster Connection Parameters page of Add Monitoring Wizard

7. Click **Verify Connection** to test connectivity with the cluster:
   - In case of connection success (green checkmark icon appears), the cluster name and UUID (universally unique identifier) appear in the Nutanix Cluster Identification (Retrieved) section.
   - Else (red cross icon appears), correct values in the Cluster, Port, User name, and Password text boxes, and retry connecting until successful.
8. Select the **Create corresponding Run As account** option and then click **Create** to apply configuration and close the wizard.

In the **Administration** view of the SCOM Operations console, in the Administration > Run as Configuration > Accounts context, the `HYCUNutanixPrismAccount_<NutanixClusterUUID>` entry is added to the Type: Basic Authentication list.

In this instance, `<NutanixClusterUUID>` is universally unique identifier of the Nutanix cluster.

Configuring the Application Awareness feature

You must configure the Application Awareness feature of SCOM MP for Nutanix to use the following functionality:

- Inclusion of details about the current top processes on your virtual machines in alerts
- Ability to run Nutanix-specific tasks in the SCOM Operations console
- Detection and monitoring of application environments running on virtual machines

  This use case requires an additional application-specific configuration step (marked *Optional* in the configuration procedure).
- Inclusion of information on application roles in alerts and graphs

  This use case requires an additional application-specific configuration step (marked *Optional* in the configuration procedure).
- Product's SuperPacks feature.

SCOM MP for Nutanix also detects systems outside Nutanix environment that are part of application environments which include at least one Nutanix cluster node; such systems are treated as external and are not monitored.

> ⚠ Important Application discovery on virtual machines usually takes approximately 24 hours to complete. Application objects are therefore not available immediately after the product is installed. Before you start configuring Application Awareness, ensure that all virtual machines that host your applications get discovered by SCOM (appear in the SCOM Operations console).

Application Awareness configuration procedure depends on the set-up of the target application environment. The procedure distinguishes between the following:

- Application environments running on virtual machines (within the same cluster) that use *a single administrative user account*

  For the corresponding configuration procedure, see "Using single account for Application Awareness" below.
- Application environments running on virtual machines (within the same cluster) that use *multiple administrative user accounts*

  For the corresponding configuration procedure, see "Using multiple accounts for Application Awareness" on page 27.

> Note You can configure no more than one administrative user account for each virtual machine. To configure a different administrative user account, first delete configuration of the existing one.

Using single account for Application Awareness

To configure Application Awareness for environments where virtual machines within the same cluster share a single administrative user account, use the **Use single account** option. With this option, an application group with all virtual machines on the selected cluster is created.

For every Nutanix cluster with application environments that you plan to monitor, do the following:

1. Launch the SCOM Operations console and connect to the management server.
2. In the **Authoring** view, in the Authoring pane, expand **Authoring**.
3. Right-click **Management Pack Templates** and then select **Add Monitoring Wizard**.
4. In the Add Monitoring Wizard window, select **HYCU SCOM Management Pack for Nutanix: Application Awareness Configuration** and then click **Next**.
5. In the Template Name and Description page, specify a template name and description, and then specify an object where Application Awareness configuration data should be stored. Do one of the following:
   - To select an existing management pack, select it from the **Select destination management pack** drop-down list.
   - To create a new management pack, follow the steps:
     a. Click **New**.
     b. In the Create a Management Pack wizard, in the General Properties page, specify the name, version, and description. Click **Next**.
     c. In the Knowledge base, click **Create**.

   Click **Next**.
6. Select **Use single account** and then click **Next**.

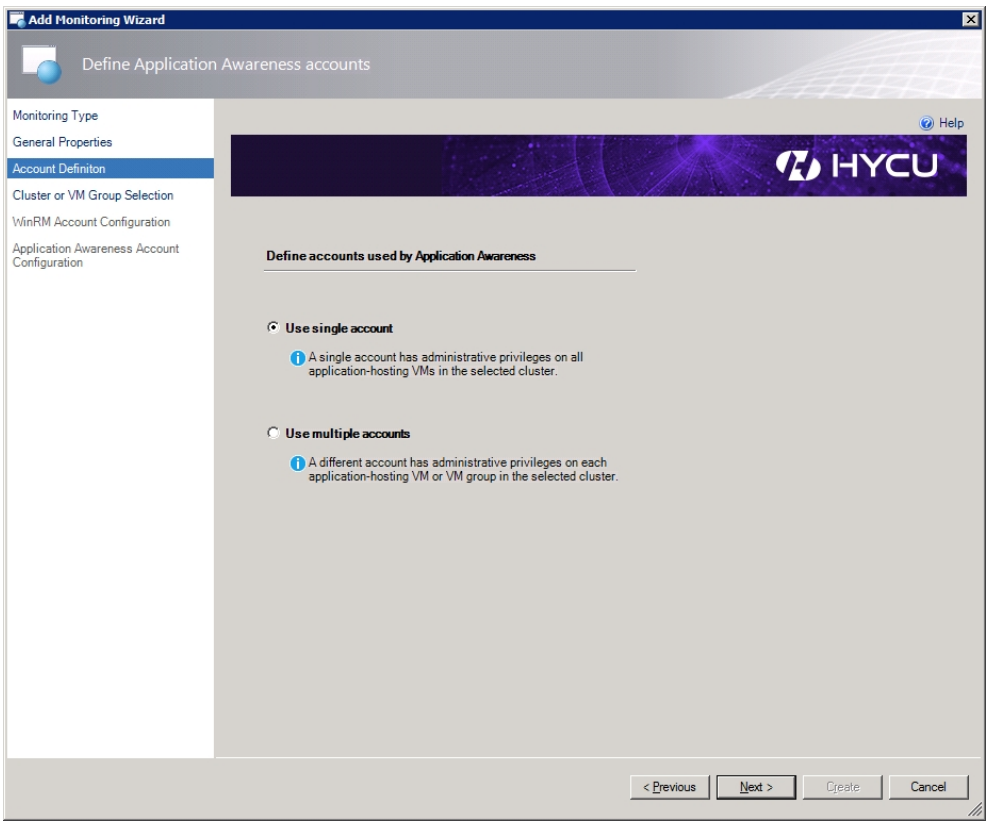

Figure 2–5: Account Definition page of Add Monitoring Wizard

7. Select the Nutanix cluster for which you create account. Click **Next**.

8. Specify credentials of the WinRM account that has access to virtual machines hosted on the same domain in the Nutanix cluster. Select **Create corresponding Run As account** and then click **Next**.

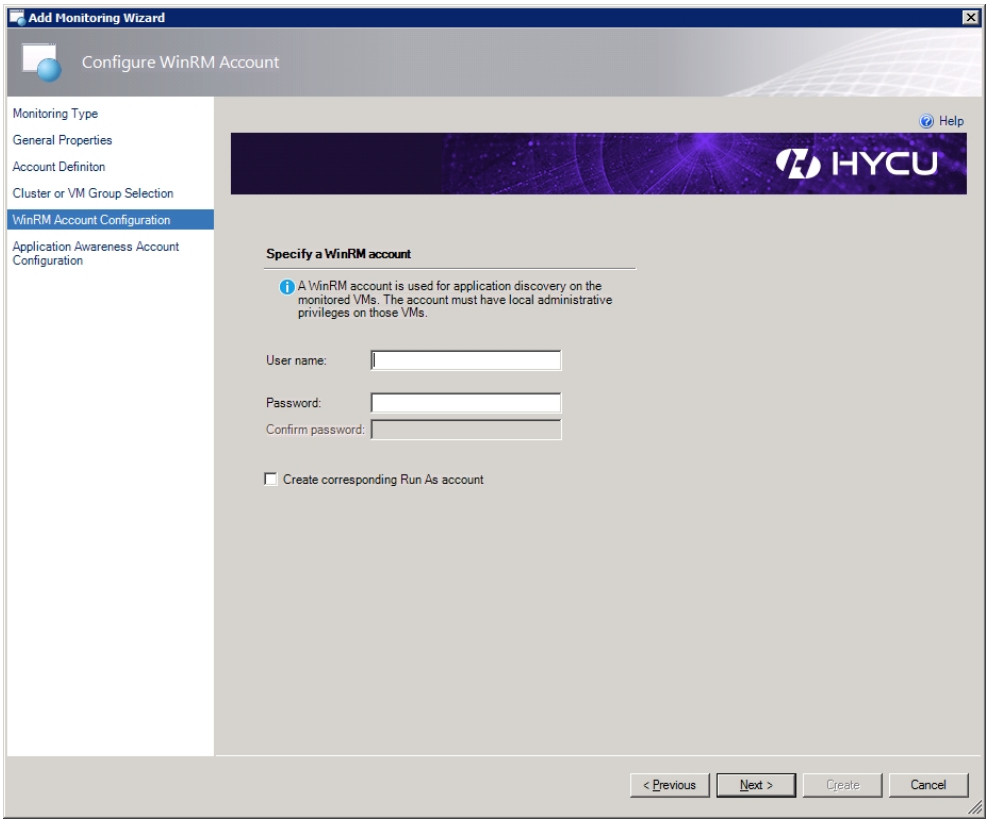

Figure 2–6: WinRM Account Configuration page of Add Monitoring Wizard

9. *Optional.* In the Application Awareness Account Configuration page, configure administrative user accounts of the monitored applications. For each application you plan to monitor, follow the steps:
   a. Click **Add**.
   b. In the Application Account Credentials dialog box, select the application from the **Application** drop-down list.
   c. In the corresponding text boxes, enter user name and password of the administrative user account of the application.
   d. Click **OK**.

   Review the list of user accounts to be configured.
10. Click **Create** to apply configuration and close the wizard.

Using multiple accounts for Application Awareness

To configure Application Awareness for environments where different administrative user accounts are configured in virtual machines within the same cluster, use the **Use multiple accounts** option.

For every Nutanix cluster with application environments that you plan to monitor, do the following:

1. Launch the SCOM Operations console and connect to the management server.
2. In the **Authoring** view, in the Authoring pane, expand **Authoring**.
3. Right-click **Management Pack Templates** and then select **Add Monitoring Wizard**.
4. In the Add Monitoring Wizard window, select **HYCU SCOM Management Pack for Nutanix: Application Awareness Configuration** and then click **Next**.
5. In the Template Name and Description page, specify a template name and description, and then specify an object where Application Awareness configuration data should be stored. Do one of the following:
   - To select an existing management pack, select it from the **Select destination management pack** drop-down list.
   - To create a new management pack, follow the steps:
     a. Click **New**.
     b. In the Create a Management Pack wizard, in the General Properties page, specify the name, version, and description. Click **Next**.
     c. In the Knowledge base, click **Create**.

   Click **Next**.
6. Select option **Use multiple accounts** and then click **Next**.

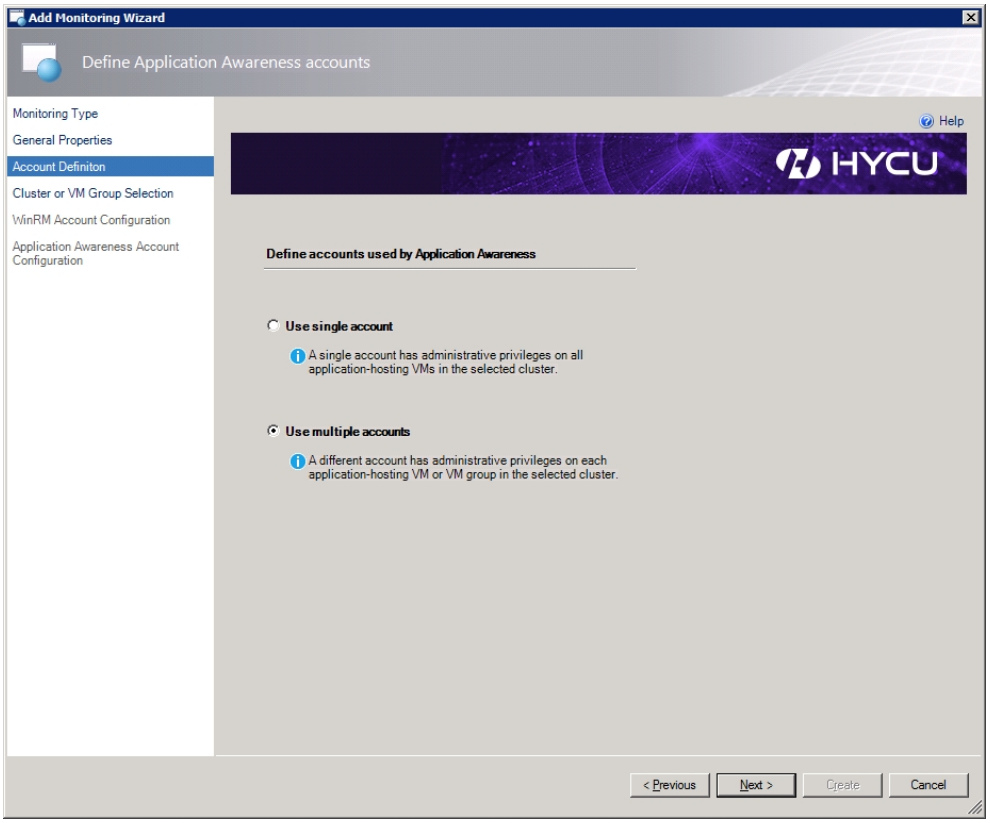

Figure 2–7: Account Definition page of Add Monitoring Wizard

7. Specify the Group name. Click **Next**.
8. Specify credentials of the WinRM account that has access to virtual machines from the domain. Select **Create corresponding Run As account** and then click **Next**.

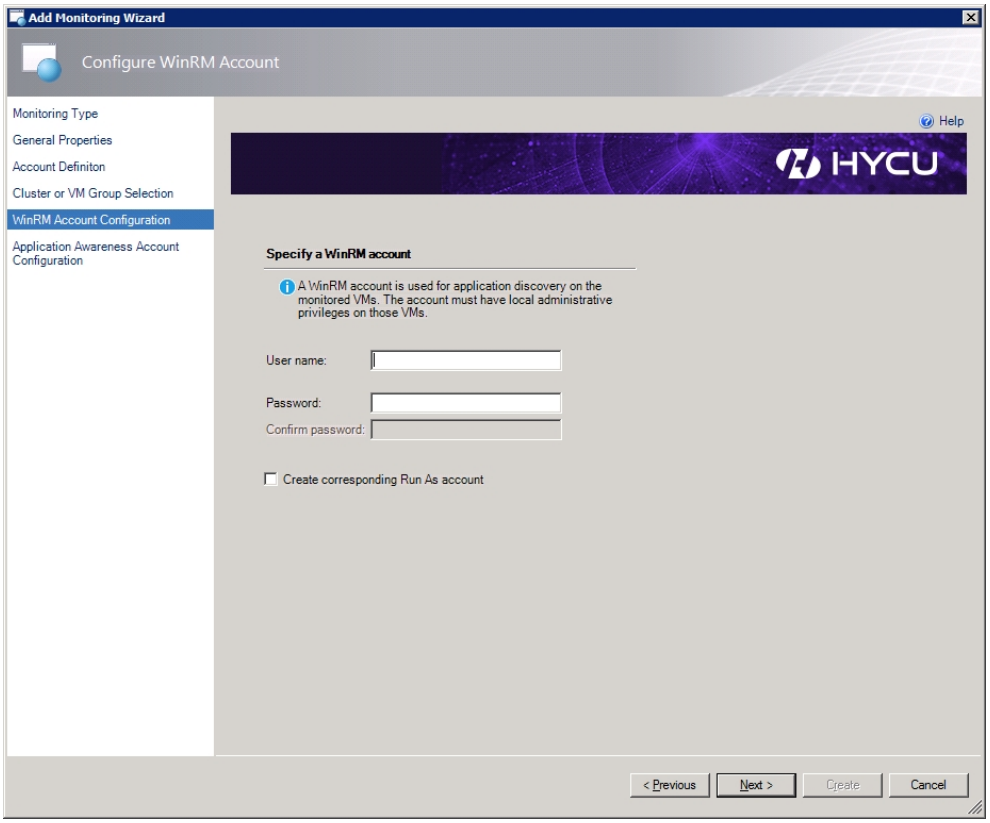

Figure 2–8: WinRM Account Configuration page of Add Monitoring Wizard

9. *Optional.* In the Application Awareness Account Configuration page, configure administrative user accounts of the monitored applications. For each application you plan to monitor, follow the steps:
   a. Click **Add**.
   b. In the Application Account Credentials dialog box, select the application from the **Application** drop-down list.
   c. In the corresponding text boxes, enter user name and password of the administrative user account of the application.
   d. Click **OK**.

   Review the list of user accounts to be configured.
10. Click **Create** to apply configuration and close the wizard.

Configuring low-level hardware monitoring

Hardware monitors of SCOM MP for Nutanix use Intelligent Platform Management Interface (IPMI) to collect low-level monitoring data from Nutanix cluster nodes: fan rotation speed, temperature, power supply voltage. To retrieve such data, interface implementation on a node is queried by a third-party tool (ipmiutil), after authenticating with valid credentials. SCOM MP for Nutanix comes preconfigured to use the default IPMI user account credentials on Nutanix cluster nodes. To supply SCOM MP for Nutanix with

non-default credentials, reconfigure a dedicated SCOM Run As profile so that a proper Run As account is added to it.

To configure a new Run As account for hardware monitoring through IPMI, do the following:

1. Launch the SCOM Operations console and connect to the management server.
2. In the **Administration** view, expand **Run As Configuration** and select **Profiles**.
3. In the Profiles list, double-click **HYCU SCOM Management Pack for Nutanix: IPMI Monitoring Account**.
4. In the Run As Profile Wizard window, click **Run As Accounts**. In the Run As Accounts page, click **Add**.
5. In the Add a Run As Account dialog box, click **New** to open Create Run As Account Wizard.
6. In the Create Run As Account Wizard window, click **Next**.
7. In the General Properties page, from the **Run As account type** drop-down list, select **Basic Authentication**.
8. In the **Display name** text box, enter account name as it will be displayed in the SCOM Operations console. Click **Next**.
9. In the Credentials page, enter valid IPMI account credentials in the respective text boxes. Click **Next**.
10. In the Distribution Security page, make your selection as appropriate and then click **Create**.
11. Upon notification about successful Run As account creation, click **Close** to close the wizard.
12. In the Add a Run As Account dialog box, click **A selected class, group, or object**. From the **Select** drop-down list, select **Object**.
13. In the Object Search dialog box, from the **Look for** drop-down list, select **Nutanix Node**, and then click **Search**.
14. In the Available items list, select the Nutanix cluster node you want to associate with the Run As account, and then click **Add**. Click **OK** to close the Object Search dialog box.
15. Click **OK** to close the Add a Run as Account dialog box.
16. In the Run As Profile Wizard window, review your configuration and then click **Save** to save your changes.
17. Upon warning about Run As credentials distribution, in the More-secure Run As accounts list, click the newly created account.
18. Use controls in the Run As Account properties dialog box and Computer Search window to distribute credentials of the Run As account to each member of HYCU Nutanix Management Pool.

Configuring HYCU Data Protection monitoring

To enable monitoring of HYCU Data Protection, a Nutanix backup and recovery solution by HYCU, Inc., you must set up connection to your HYCU Data Protection environment by using the HYCU SCOM Management Pack for Nutanix: HYCU Data Protection Configuration wizard. To monitor multiple HYCU Data Protection backup controllers, repeat the configuration procedure for each HYCU Data Protection backup controller that you plan to monitor.

> ⚠ Important Before you start, ensure that all Nutanix clusters visible from the corresponding HYCU Data Protection user interface are discovered by SCOM and present in the product's Table: Clusters view in the SCOM Operations console.

To configure HYCU Data Protection monitoring, do the following:

1. Launch the SCOM Operations console and connect to the management server.
2. In the **Authoring** view, in the Authoring pane, expand **Authoring**.
3. Right-click **Management Pack Templates** and then select **Add Monitoring Wizard**.
4. In the Add Monitoring Wizard window, select **HYCU SCOM Management Pack for Nutanix: HYCU Data Protection Configuration** and then click **Next**.
5. In the Template Name and Description page, specify a name and description of the template, and then specify an object where HYCU Data Protection monitoring configuration data should be stored. Do one of the following:
   - To select an existing management pack, select it from the **Select destination management pack** drop-down list.
   - To create a new management pack, follow the steps:
     a. Click **New**.
     b. In the Create a Management Pack wizard, in the General Properties page, specify the name, version, and description. Click **Next**.
     c. In the Knowledge page, click **Create**.

   Click **Next**.
6. In the HYCU Data Protection Connection Parameters page, in the HYCU Data Protection Connection Parameters section, specify the following:
   - Fully qualified domain name or IP address of the HYCU Data Protection backup controller (**Backup controller**)
   - *Required if a non-default port number is configured for the HYCU Data Protection web user interface.* Different listening port number of the HYCU Data Protection web interface (**Port**)

     Default value: 8443.
   - Credentials of the chosen HYCU Data Protection user account (**User name**,

Password)

Preconfigured administrative user account has the following credentials: `admin`, `admin`.

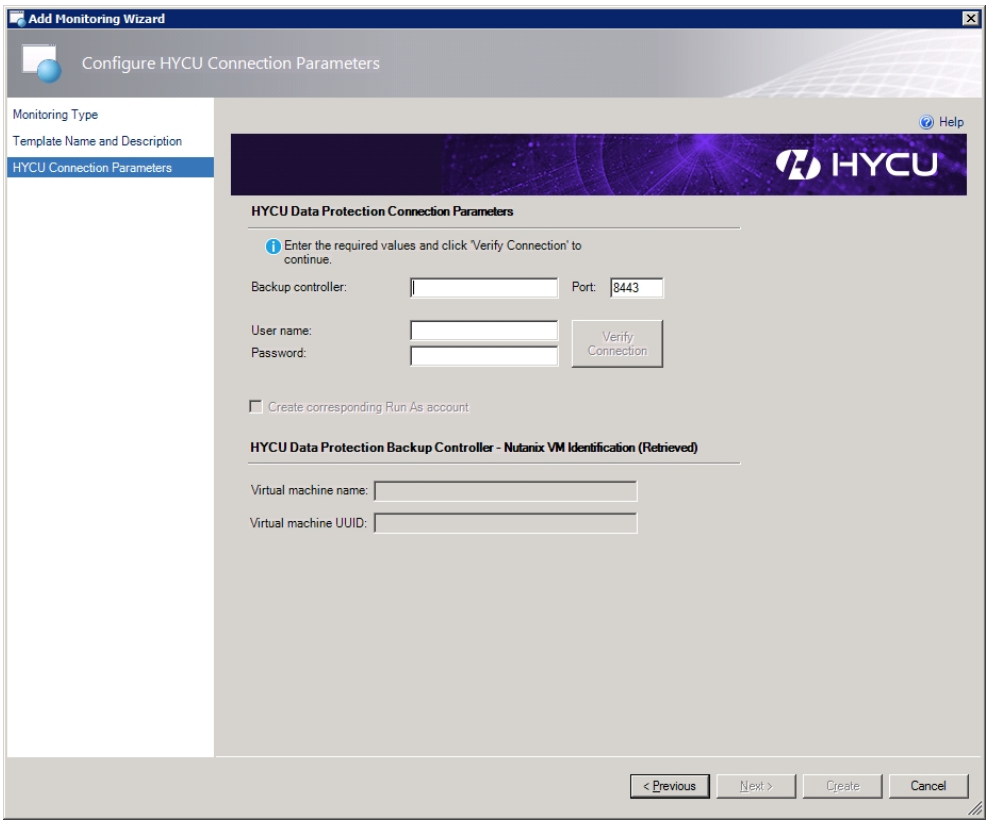

Figure 2–9: HYCU Data Protection Connection Parameters page of Add Monitoring Wizard

7. Click **Verify Connection** to test connectivity with the HYCU Data Protection backup controller:
   - In case of connection success (green checkmark icon appears), the HYCU Data Protection backup controller (virtual machine) name and UUID appear in the HYCU Data Protection Backup Controller - Nutanix VM Identification (Retrieved) section.
   - Else (red cross icon appears), correct values in the Backup controller, Port, User name, and Password text boxes, and retry connecting until successful.
8. Select the **Create corresponding Run As account** option and then click **Create** to apply configuration and close the wizard.

In the **Administration** view of the SCOM Operations console, in the **Administration > Run as Configuration > Accounts** context, the `HYCUDataProtectionAccountInfo_<VMuuid>` entry is added to the Type: Basic Authentication list.

In the above instance, `<VMuuid>` is the virtual machine UUID of the respective HYCU Data Protection backup controller.

Chapter 3

Upgrade

This chapter provides information on how to perform an in-place upgrade of SCOM MP for Nutanix from an earlier product version. During the in-place upgrade, entire configuration of SCOM MP for Nutanix in SCOM is preserved, and the included management packs are upgraded.

> ⚠ Important For a limitation related to upgrading, see the *HYCU SCOM Management Pack for Nutanix Release Notes*, section *Limitations*.

Upgrading SCOM MP for Nutanix

To upgrade the product, do the following:

1. Follow instructions in chapter *Installation and configuration*, section "Installing SCOM MP for Nutanix" on page 13.
2. Launch the SCOM Operations console and connect to the management server.
3. In the **Administration** view, expand **Administration > Run As Configuration** and then click **Profiles**.
4. In the Profiles list, double-click **Data Warehouse Account**. The Run As Profile Wizard starts.
5. Click **Run As Accounts**. In the Run As accounts list, identify the account name that is used for the Data Set target. You will need this name later.
6. Click **Add**. The Add a Run As Account dialog box appears.
7. In the Run As Account list, select the account name that you identified in step 5.
8. Select the **A selected class, group, or object** option. From the **Select** drop-down list, select **Class**.
9. In the Class Search dialog box, click **Search**. In the Available items list, select **HYCU Nutanix Accessor**, and then click **Add**.
10. Click **OK** to close the Object Search dialog box. Click **OK** to close the Add a Run As Account dialog box.
11. Click **Save** to save your changes, and then click **Close** to close the Run As Profile Wizard.

Chapter 4

Product licensing

This chapter explains different types of product licenses and provides instructions about how to obtain the license keys and activate your licenses.

Overview

After SCOM MP for Nutanix is installed and configured, you must perform specific tasks to ensure product licensing is covered. You must provide the product with a valid license activation key for every monitored Nutanix cluster. There are three license types available:

- Software evaluation licenses

  Software evaluation licenses are time-limited and are used for product evaluation. For information on requesting and activating licenses of this type, see "Software evaluation licensing" below.

- Perpetual licenses

  Perpetual (permanent) licenses are issued after product purchase and have no expiration date. For information on requesting and activating licenses of this type, see "Perpetual licensing" on the next page.

- Subscription-based licenses

  Subscription-based licenses are issued after product purchase and are time-limited. To ensure continuity of operation, you should renew them before they expire. For information on requesting and activating licenses of this type, see "Subscription-based licensing" on page 37.

> **Note** The system where SCOM MP for Nutanix is installed does not require Internet connectivity when the product license is activated (the license key is applied).

Software evaluation licensing

To evaluate the product before making a purchase, send a request through the HYCU website (preferred) or contact HYCU Sales at the info@hycu.com email address.

Software evaluation licenses are time-limited and expire 45 days after their issue date.

After you receive a software evaluation license key by email, apply the license key in your environment. To do so, copy the `license.dat` file to the `%ProgramData%\Comtrade\Nutanix MP\License` folder on each management server in

the SCOM resource pool you are using to monitor Nutanix clusters; these SCOM management servers should also have SCOM Data Collector for Nutanix (the `Data Collector service` feature of SCOM MP for Nutanix) installed.

Perpetual licensing

Perpetual licenses for SCOM MP for Nutanix are based on the number of CPU sockets and are issued for a specific Nutanix cluster. The number of purchased perpetual licenses should be equal to the number of CPU sockets within monitored Nutanix nodes. A perpetual license can be used only for monitoring the cluster for which it is issued.

Perpetual licensing procedure

Prerequisites

- You have purchased product licenses and own an entitlement order.
- You have identified which SCOM management servers are involved in monitoring your Nutanix infrastructure. Each such SCOM management server has the following characteristics;
  - It is included in the dedicated SCOM resource pool (`HYCU Nutanix Management Pool`).
  - SCOM Data Collector for Nutanix (the `Data Collector service` feature of SCOM MP for Nutanix) is installed on it.

To obtain a perpetual license key and activate the license for a specific SCOM management server, do the following:

1. Make sure that a license request file (`license.req`) exists locally in the *%ProgramData%*`\Comtrade\Nutanix MP\License` folder. The file is created automatically after discovery of your Nutanix environment completes.

   ### Example

   Contents of a license request file:

   ```
   CN      Customer Company
   PID     nutanixmp
   ND      00052DB8-098A-DCE0-6D8F-0CC47AB05798
   NRP     18
   VER     V1N
   HSUD
   ADCD74F0359FB4B6EA683AEDCFCEE9745E164D3C9BC216754562712B3583D326
   NEXT    NODE
   CN      Customer Company
   PID     nutanixmp
   ND      00052DC5-E8CB-811F-3BB6-0CC47A55B2AC
   NRP     24
   ```

```
VER     V1N
HSUD
BB6141BDECD6075AA860B4B32D2D4CC3BFC20019716666B5B1A8B43DC8295271
NEXT    NODE
```

2. Open a web browser and go to the Licensing Portal | HYCU website to submit a license request.
3. If you already have a licensing portal account, click **Sign in** and enter your user name and password. Else, create it first by filling in the request form on the website.
4. To generate the perpetual license key, click **Activate perpetual licenses**, enter your purchase order number (PO number), and then click **Next**.
5. To upload the license request file, click **Choose file**, select the license request file, and then click **Send request**.
6. In the Activate perpetual licenses page, review the list of clusters and the number of required CPU sockets within each cluster for which you want to activate perpetual license.
7. Click **Activate licenses**.

   Within a few minutes, you should receive an email from HYCU Customer Support with a license activation file (`license.dat`) attached.
8. Save the license activation file to the same location where the license request file resides, that is, into the *%ProgramData%*`\Comtrade\Nutanix MP\License` folder.

Repeat the procedure for each qualified SCOM server. Once you complete the process, your perpetual licenses are activated and you can start using SCOM MP for Nutanix.

> Tip To speed up the process for large monitoring environments, merge contents of license request files from individual SCOM management servers, and save the result into a master license request file. Then upload this file to the licensing portal.

Subscription-based licensing

Subscription-based licenses for SCOM MP for Nutanix are based on the number of CPU sockets and are issued for a specific Nutanix cluster. The number of purchased subscription-based licenses should be equal to the number of CPU sockets within monitored Nutanix nodes. A subscription-based license can be used only for monitoring the cluster for which it is issued.

Subscription-based licenses are time-limited.

Subscription-based licensing procedure

Prerequisites

- You have purchased product licenses and own an entitlement order.
- You have identified which SCOM management servers are involved in monitoring your Nutanix infrastructure. Each such SCOM management server has the following characteristics;
  - It is included in the dedicated SCOM resource pool (`HYCU Nutanix Management Pool`).
  - SCOM Data Collector for Nutanix (the `Data Collector service` feature of SCOM MP for Nutanix) is installed on it.

To obtain a subscription-based license key and activate the license for a specific SCOM management server, do the following:

1. Make sure that a license request file (`license.req`) exists locally in the *`%ProgramData%`*`\Comtrade\Nutanix MP\License` folder. The file is created automatically after discovery of your Nutanix environment completes.

   ### Example

   Contents of a license request file:

   ```
   CN      Customer Company
   PID     nutanixmp
   ND      00052DB8-098A-DCE0-6D8F-0CC47AB05798
   NRP     18
   VER     V1N
   HSUD
   ADCD74F0359FB4B6EA683AEDCFCEE9745E164D3C9BC216754562712B3583D326
   NEXT    NODE
   CN      Customer Company
   PID     nutanixmp
   ND      00052DC5-E8CB-811F-3BB6-0CC47A55B2AC
   NRP     24
   VER     V1N
   HSUD
   BB6141BDECD6075AA860B4B32D2D4CC3BFC20019716666B5B1A8B43DC8295271
   NEXT    NODE
   ```

2. Request the license activation file from HYCU Customer Support; attach the license request file to an email and send it to the following address: support@hycu.com
3. Wait for an email in reply. The email should have a license activation file (`license.dat`) attached.

4. Copy the license activation file to the same location where the license request file resides, that is, into the *%ProgramData%*\Comtrade\Nutanix MP\License folder.

Repeat the procedure for each qualified SCOM server. Once you complete the process, your subscription-based licenses are activated and you can start using SCOM MP for Nutanix.

> Tip To speed up the process for large monitoring environments, merge contents of license request files from individual SCOM management servers, and save the result into a master license request file. Then send this file in the email attachment.

License management

This section provides guidelines for the following cases:

- Your monitored environment grows beyond the licensed and you must add new licenses
- You want to modify the monitored set of Nutanix clusters and you must update your licensing scheme

Adding licenses

When your environment monitored with SCOM MP for Nutanix grows, you must purchase additional licenses to enable monitoring of additional Nutanix clusters or nodes.

To add new SCOM MP for Nutanix licenses, do the following:

1. Determine how many licenses you must add to the already purchased ones:
   a. Search for the number of currently licensed CPU sockets in the *%ProgramData%*\Comtrade\Nutanix MP\License\license.req file in the line starting with the NRP string (for example, NRP 24).
   b. Calculate the difference between numbers of actual CPU sockets and currently licensed CPU sockets.
2. Purchase the required number of additional licenses.
3. After you receive an entitlement order, obtain the license activation keys and apply them to activate your additional licenses.

   For instructions, see "Perpetual licensing procedure" on page 36 or "Subscription-based licensing procedure" on the previous page.

Modifying the set of monitored Nutanix clusters

After your licenses are activated, you may want to modify the set of Nutanix clusters that are monitored by SCOM MP for Nutanix. As each product license is issued for a specific cluster, you must update your licensing scheme in such cases.

To arrange license management activities, contact your HYCU sales representative at the info@hycu.com email address.

Chapter 5

Uninstallation

This chapter contains instructions on how to completely uninstall SCOM MP for Nutanix from your environment.

To uninstall SCOM MP for Nutanix, complete these tasks:

1. Remove management packs included in SCOM MP for Nutanix. For details, see "Removing included management packs" below.
2. Uninstall SCOM MP for Nutanix from SCOM management servers. For details, see "Uninstalling SCOM MP for Nutanix from management servers" on the next page.

Removing included management packs

To remove management packs included in SCOM MP for Nutanix and other product references from the SCOM management server, do the following:

1. Launch the SCOM Operations console and connect to the management server.
2. In the Administration view, click **Management Packs**.
3. Remove SCOM MP for Nutanix references (stored configuration data) from the object you selected during product configuration (see "Configuring SCOM MP for Nutanix" on page 21):
   - If you created a new management pack and you used this management pack exclusively for storing product configuration data, right-click the management pack and then select **Delete**.
   - If you used an existing management pack when configuring the product (for example, `Microsoft.SystemCenter.SecureReferenceOverride`), remove dependencies on the product configuration from it:
     a. Export the management pack.
     b. Make a copy of the file you exported the management pack to.
     c. Edit the file copy and remove all dependencies on the SCOM MP for Nutanix configuration from it. Search for `Comtrade` and delete the containing references, then save your changes.
     d. Delete the management pack from SCOM.
     e. Import back the management pack from the edited file copy.
4. In the Management Packs pane, right-click the management pack you want to remove

and then click **Delete**. Remove the included management packs in the following order:

a. `HYCU Management Pack for Nutanix (SuperPacks: Microsoft SQL Server)`
b. `HYCU Management Pack for Nutanix (SuperPacks: Microsoft Exchange Server)`
c. `HYCU Management Pack for Nutanix (SuperPacks: Citrix XenApp and XenDesktop)`
d. `HYCU Management Pack for Nutanix (SuperPacks: Citrix XenApp and XenDesktop - Resources)`
e. `HYCU Management Pack for Nutanix (SuperPacks - Widgets)`
f. `HYCU Management Pack for Nutanix (SuperPacks - Core)`
g. `HYCU Management Pack for Nutanix (HYCU Data Protection)`
h. `HYCU Management Pack for Nutanix (Application Awareness)`
i. `HYCU Management Pack for Nutanix (Advanced Dashboards)`
j. `HYCU Management Pack for Nutanix (Widgets)`
k. `HYCU Management Pack for Nutanix (Dashboards)`
l. `HYCU Management Pack for Nutanix (Reports)`
m. `HYCU Management Pack for Nutanix (Hardware Monitors)`
n. `HYCU Management Pack for Nutanix (Core)`

Uninstalling SCOM MP for Nutanix from management servers

To uninstall SCOM MP for Nutanix, perform the following procedure on all SCOM management servers that are part of HYCU Nutanix Management Pool (a SCOM resource pool designated to monitor Nutanix clusters):

1. In Windows Control Panel, select **Programs > Programs and Features**.
2. Locate and right-click the **HYCU SCOM Management Pack for Nutanix** entry, then select **Uninstall**.

   > Note A warning dialog box may appear informing you that other users are logged in to this computer. You cannot completely remove this program if another user is currently running it.

3. In the Setup Wizard, follow instructions until the uninstallation process completes.

Setup Wizard cannot remove the files that were placed to the installation directories after the installation, for example, license files or configuration files. You can delete such files after Setup Wizard completes the uninstallation process.

> Note To manually delete any files from the installation directories after the SCOM MP for Nutanix uninstallation, first make sure that these files are not used by other

programs and their deletion does not cause issues.

Chapter 6

Usage

This chapter contains reference information about elements of the management packs that are included in SCOM MP for Nutanix, describes specifics of the product's feature set and advises on available configuration options.

The following basic topics are covered in this chapter:

Furthermore, SCOM MP for Nutanix includes the SuperPacks feature with application-specific dashboards that correlate information from SCOM MP for Nutanix and other SCOM add-ins (Management Pack products). The following sections discuss this feature:

Discoverable object types

SCOM MP for Nutanix can discover object types listed in the following table.

Table 6–1: Object types that SCOM MP for Nutanix can discover

Icon	Object type	Description
	HYCU Nutanix Accessor	A HYCU accessor node which serves as an entry point to Nutanix infrastructure. It contains Nutanix clusters and cluster groups.
	Nutanix Cluster Group	An organizational unit that contains all discovered Nutanix clusters.

Icon	Object type	Description
	Nutanix Cluster	A Nutanix cluster discovered by SCOM MP for Nutanix.
	HYCU Nutanix Management Pool	A SCOM resource pool that contains objects managed by SCOM MP for Nutanix.
	Nutanix Data Protection Group	An organizational unit that contains one or more Nutanix protection domain groups and the corresponding remote site groups.
	Nutanix Protection Domain Group	An organizational unit that contains one or more Nutanix data protection domain subgroups.
	Nutanix Protection Domain SubGroup	An organizational unit that represents a Nutanix cluster and contains Nutanix data protection domains of this cluster.
	Nutanix Protection Domain	A group of VMs and files to be replicated together on a defined schedule. A protection group can protect a full container or selected individual VMs and files.
	Nutanix Replication Link	A connection from the data protection domain to its remote site.
	Nutanix Remote Site Group	An organizational unit that contains Nutanix remote site subgroups.
	Nutanix Remote Site Subgroup	An organizational unit that represents a Nutanix cluster and contains Nutanix remote sites of this cluster.
	Nutanix Remote Site	A remote Nutanix cluster or public cloud which can be leveraged as a target for backup or data replication purposes.
	Nutanix Node Group	An organizational unit for one or more Nutanix node subgroups; it contains all discovered Nutanix nodes for a single cluster.
	Nutanix Node SubGroup	An organizational unit that represents one cluster and contains one or more Nutanix blocks of this cluster.
	Nutanix Block	An object that contains one, two, or four server nodes.

Icon	Object type	Description
	Nutanix Node	A physical Nutanix node (host system) configured in the Nutanix cluster.
	Disk SubGroup	A group of discovered disks (HDD and SSD devices) for a single Nutanix node.
	HDD	A hard disk drive (HDD) in the Nutanix environment. It is primarily used for bulk storage and stores: – Curator Reservation (curator storage) – Extent Store (persistent storage)
	SSD	A solid state drive (SSD) in the Nutanix environment. It stores the following key items: – Nutanix Home (CVM core) – Cassandra (metadata storage) – OpLog (persistent write buffer) – Unified Cache (SSD cache portion) – Extent Store (persistent storage)
	Nutanix Storage Pool Group	A group of all discovered Nutanix storage pools of all clusters.
	Nutanix Storage SubGroup	An organizational unit that represents a Nutanix cluster and contains one or more Nutanix storage pools of this cluster.
	Nutanix Storage Pool	A group of physical storage devices of the cluster, including PCIe SSD, SSD, and HDD units. A storage pool may span multiple Nutanix cluster nodes (host systems) and is expanded as the cluster scales. Most often a single storage pool is leveraged.
	Nutanix Storage Container	A logical segmentation of the storage pool. It contains a group of VMs or files (vDisks).
	Nutanix VM	A virtual machine discovered in the Nutanix environment.
	Nutanix User VM Group	A group of all discovered Nutanix user virtual machines.
	Nutanix User VM	A user virtual machine discovered in the Nutanix environment.

Icon	Object type	Description
	Nutanix VM SubGroup	A group of discovered VMs for a single Nutanix cluster.
	Nutanix Controller VM (CVM)	A Nutanix virtual machine that runs Nutanix software and serves all I/O operations for the hypervisor and all VMs running on a node (host system). A CVM status contains information on health and alerts, and provides possible resolution steps that help to keep the Nutanix environment at maximum throughput.
	External VM	A user VM that is configured outside Nutanix environment. It is part of an application environment that includes at least one Nutanix cluster node. Such system is detected, but is not monitored.
	Application Group	Group of all applications subgroups.
	Base Application Group Class	Base group of the applications/VMs running on Nutanix VMs.
	Nutanix Entity	Abstract base class holding Nutanix related properties.
	Group of Citrix Delivery Group Machines	Group of all Citrix Delivery Controller machines from a Citrix Site.
	Citrix Site Server OS Machines Group	Group of all Server OS Machines from a Citrix Site.
	Nutanix Disk Base Class	Base class for SSD and HDD objects.
	License for HYCU SCOM Management Pack for Nutanix	Class for monitoring the HYCU license.
	Nutanix VM SplitGroup	Group of VMs from hosted on one cluster, grouped by last hexadecimal letter of the UUIDs.
	Base Application Class	Base class for all application classes.
	Base Citrix Application Class	Base class for all Citrix applications.

Icon	Object type	Description
	Citrix Delivery Controller	Citrix Delivery Controller application role.
	Citrix Role	All Citrix application roles except Delivery Controller and StoreFront.
	Citrix Site	Group of all VMs that are part of a Citrix site.
	Citrix StoreFront	Citrix StoreFront application role.
	Microsoft Exchange Server	Microsoft Exchange Server application.
	Microsoft Exchange Servers Group	Group of Microsoft Exchange Server hosts.
	Microsoft SharePoint Server	Microsoft SharePoint Server application.
	Microsoft SharePoint Servers Group	Group of the Microsoft SharePoint Server hosts.
	Microsoft SQL Server	Microsoft SQL Server application.
	Microsoft SQL Servers Group	Group of Microsoft SQL Server hosts.
	HYCU Nutanix Application VM Group Base	Group of all virtual machines with applications.
	Sensor Group	Group of all hardware sensor groups.
	Hardware Sensor	Base class for hardware sensors.
	Fan Group	Group of all fan subgroups.
	Fan SubGroup	Subgroup of fans.
	Fan Sensor	Hardware fan sensor.

Icon	Object type	Description
	Temperature Group	Group of all temperature subgroups.
	Temperature SubGroup	Subgroup of temperature sensors.
	Temperature Sensor	Hardware temperature sensor.
	Voltage Group	Group of all voltage subgroups.
	Voltage SubGroup	Subgroup of voltage sensors.
	Voltage Sensor	Power supply voltage sensor.
	Power Supply Group	Group of all power supply subgroups.
	Power Supply SubGroup	Subgroup of power supply sensors.
	Power Supply	Power supply presence sensor.
	Power Consumption Group	Group of all power consumption subgroups.
	Power Consumption SubGroup	Subgroup of power consumption sensors.
	Power Consumption	Power consumption sensor.
	HYCU Data Protection Backup Controller Group	A group that contains all discovered HYCU Data Protection backup controllers (virtual machines).
	HYCU Data Protection Backup Controller (Virtual Machine)	A virtual machine with the Nutanix backup and recovery solution by HYCU, Inc. (HYCU Data Protection backup controller).
	HYCU Data Protection Monitoring Configuration Object	Representation of an object that is created with the HYCU SCOM Management Pack for Nutanix: HYCU Data Protection Configuration wizard.
	HYCU Data Protection VM SubGroup	Group of VMs discovered through the same HYCU Data Protection backup controller.

Monitors

SCOM MP for Nutanix provides monitors listed in the table that follows. The monitors have default thresholds that you can fine tune to better suit conditions in your environment. For instructions on changing the default thresholds, see "Tuning thresholds for performance monitors and rules" on page 74. Monitors that are disabled by default and monitors whose alerts are disabled by default are specially marked.

Table 6–2: SCOM MP for Nutanix monitors

Monitor name (disablement indicator)	Description	Default values
Cluster Memory Usage Monitor	Memory usage monitor for a Nutanix cluster.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:00 Warning Threshold – 80 Critical Threshold – 90
Cluster CPU Load Monitor	CPU load monitor for a Nutanix cluster.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:00 Warning Threshold – 60 Critical Threshold – 75 Number of Samples – 3
Cluster I/O Latency Monitor (monitor disabled by default)	Input/output latency monitor for a Nutanix cluster.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:00 Warning Threshold – 5 Critical Threshold – 10 Number of Samples – 3
HYCU SCOM Management Pack for Nutanix License Status	License status monitor for the product.	Update Interval in Seconds – 900 Timeout in Seconds – 300 Warning days before expiration day – 14
Cluster REST Monitor	REST response monitor for a Nutanix cluster.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:00

Monitor name (disablement indicator)	Description	Default values
Container Usage Monitor	Usage monitor for a Nutanix container.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:02 Warning Threshold – 75 Critical Threshold – 90
Container Controller Average I/O Latency Monitor (monitor disabled by default)	Controller average input/output latency monitor for a Nutanix container.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:02 Warning Threshold – 10 Critical Threshold – 20 Number of Samples – 3
HDD Usage Monitor	Usage monitor for Nutanix physical HDD units.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:04 Warning Threshold – 75 Critical Threshold – 90
HDD Average I/O Latency Monitor	Average input/output latency monitor for Nutanix physical HDD units.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:04 Warning Threshold – 350 Critical Threshold – 400 Number of Samples – 3
SSD Average I/O Latency Monitor	Average input/output latency monitor for Nutanix physical SSD units.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:04 Warning Threshold – 35 Critical Threshold – 45 Number of Samples – 3
Node Ping Status	Node availability monitor.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01

Monitor name (disablement indicator)	Description	Default values
Node Memory Usage Monitor	Memory usage monitor for a Nutanix node.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Warning Threshold – 80 Critical Threshold – 90
Node CPU Load Monitor	CPU load monitor for a Nutanix node.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Warning Threshold – 60 Critical Threshold – 75 Number of Samples – 3
Node I/O Latency Monitor	Input/output latency monitor for a Nutanix node.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Warning Threshold – 70 Critical Threshold – 150 Number of Samples – 3
Storage Pool Usage Monitor	Usage monitor for a Nutanix storage pool.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Warning Threshold – 75 Critical Threshold – 90
Storage Pool Average I/O Latency Monitor (monitor disabled by default)	Average disk input/output latency monitor for a Nutanix storage pool.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Warning Threshold – 5 Critical Threshold – 10 Number of Samples – 3
Storage Pool SSD vs HDD Storage Usage Monitor	Performance monitor for SSD versus HDD storage average usage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01

Monitor name (disablement indicator)	Description	Default values
		Warning Threshold – 5 Critical Threshold – 20 Number of Samples – 3
VM Memory Usage Monitor	Memory usage monitor for a virtual machine.	Update Interval in Seconds – 300 Timeout in Seconds – 280 Synchronization Time – 12:02 Warning Threshold – 80 Critical Threshold – 90 Number of Samples – 6
User VM CPU Load Monitor	CPU load monitor for a user virtual machine.	Update Interval in Seconds – 300 Timeout in Seconds – 280 Synchronization Time – 12:02 Warning Threshold – 80 Critical Threshold – 90 Number of Samples – 6
VM I/O Latency Monitor	Input/output latency monitor for a virtual machine.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:02 Warning Threshold – 120 Critical Threshold – 150 Number of Samples – 3
CVM CPU Load Monitor	CPU load monitor for the controller VM.	Update Interval in Seconds – 300 Timeout in Seconds – 280 Synchronization Time – 12:02 Warning Threshold – 60 Critical Threshold – 75 Number of Samples – 3
VM Availability Monitor	Monitor of the VMs removed from the Nutanix cluster.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:02
Power Supply Status	Monitor of the status of power supply on a	Update Interval in Seconds – 300

Monitor name (disablement indicator)	Description	Default values
	Nutanix node.	Synchronization Time – (not set) Debug – false
Power Consumption Status	Monitor of the status of power consumption sensor on a Nutanix node.	Update Interval in Seconds – 300 Synchronization Time – (not set) Debug – false
Temperature Status	Monitor of the status of temperature sensor on a Nutanix node.	Update Interval in Seconds – 300 Synchronization Time – (not set) Debug – false
Fan Status	Monitor of the status of fan sensor on a Nutanix node.	Update Interval in Seconds – 300 Synchronization Time – (not set) Debug – false
Voltage Status	Monitor of the status of voltage sensor on a Nutanix node.	Update Interval in Seconds – 300 Synchronization Time – (not set) Debug – false
HYCU Data Protection Backup Controller Availability	Monitors availability of a HYCU Data Protection backup controller.	Update Interval in Seconds – 300 Synchronization Time – (not set) Debug – false
HYCU Data Protection Backup Controller Response Time	REST query response time monitor for a HYCU Data Protection backup controller.	Update Interval in Seconds – 300 Synchronization Time – (not set) Debug – false Number of Samples – 3 Warning Threshold in Milliseconds – 5000 Critical Threshold in Milliseconds – 8000
VM Compliancy with HYCU Data Protection Backup Policy (alert disabled by default)	Monitors if a Nutanix virtual machine is compliant with the assigned HYCU Data Protection backup policy.	Update Interval In Seconds – 300 Synchronization Time – (not set) Debug – false

Monitor name (disablement indicator)	Description	Default values
VMs Compliancy with HYCU Data Protection Backup Policies	Monitors if there are some Nutanix virtual machines that are not compliant with the assigned HYCU Data Protection backup policies.	Update Interval In Seconds – 300 Synchronization Time – (not set) Debug – false Threshold – 1
Last HYCU Data Protection VM Backup Status	Monitors status of the last HYCU Data Protection backup job that was run for a virtual machine.	Update Interval In Seconds – 300 Synchronization Time – (not set) Debug – false Backup Count – 1000 Job Count – 300
Nutanix Cluster Storage Running Out	Alerts, based on analysis of past usage, when current usage of the Nutanix cluster storage nears its capacity.	Update Interval In Seconds – 86400 Synchronization Time – (not set) Timeout in Seconds – 300 Warning Threshold – 60 Critical Threshold – 30 Analysis Period in Days – 30

Rules

SCOM MP for Nutanix provides rules listed in the table that follows. The rules have default thresholds that you can tune to better suit conditions in your environment. For instructions on changing the default thresholds, see "Tuning thresholds for performance monitors and rules" on page 74.

Table 6–3: SCOM MP for Nutanix rules

Rule name	Description	Default values
VM Group Populator	This rule populates VM groups with VMs (members) that have valid credentials.	Spread Initialization Time – 7200 Timeout in Seconds – 900 Update Interval in Seconds – 21600
Cluster CPU Usage [%]	This rule collects cluster CPU load, expressed as a percentage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:00

Rule name	Description	Default values
		Tolerance Type – Absolute Tolerance – 10 Maximum Sample Separation – 3
Cluster Controller I/O Bandwidth [MBps]	This rule collects total cluster disk input/output bandwidth from the controller, expressed in megabytes per second.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:00 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Cluster Memory Usage [%]	This rule collects cluster memory usage, expressed as a percentage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:00 Tolerance Type – Absolute Tolerance – 10 Maximum Sample Separation – 3
Cluster Controller Average I/O Latency [ms]	This rule collects total cluster average disk input/output latency from the controller, expressed in milliseconds.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:00 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Cluster Storage Logical Usage [B]	This rule collects logical usage of cluster storage, expressed in bytes.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:00 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Cluster Replication RX Bandwidth [MBps]	This rule collects cluster replication received bandwidth, expressed in	Update Interval in Seconds – 300

Rule name	Description	Default values
	megabytes per second.	Timeout in Seconds – 120 Synchronization Time – 12:00 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Cluster Content Cache Hits [%]	This rule collects the percentage of cluster-wide content cache hits.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:00 Tolerance Type – Absolute Tolerance – 10 Maximum Sample Separation – 3
Cluster Content Cache Hits [count]	This rule collects the number of cluster-wide content cache hits.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:00 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Cluster PreReduction Storage Usage [B]	This rule collects cluster pre-reduction space usage, expressed in bytes.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:00 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Cluster Compression Savings [B]	This rule collects the cluster compression saved space, expressed in bytes.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:00 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3

Rule name	Description	Default values
Cluster Deduplication Savings [B]	This rule collects cluster deduplication saved space, expressed in bytes.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:00 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Cluster Storage SSD Usage [B]	This rule collects cluster storage usage in the SSD tier, expressed in bytes.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:00 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Cluster Storage HDD Capacity [B]	This rule collects cluster storage capacity of the HDD tier, expressed in bytes.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:00 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Cluster Storage SSD Capacity [B]	This rule collects cluster storage capacity of the SSD tier, expressed in bytes.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:00 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Cluster Storage HDD Usage [B]	This rule collects cluster storage usage in the HDD tier, expressed in bytes.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:00 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation –

Rule name	Description	Default values
		3
Cluster Erasure Savings [B]	This rule collects cluster erasure saved space, expressed in bytes.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:00 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Cluster Storage Usage Free [%]	This rule collects cluster free storage, expressed as a percentage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:00 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Cluster Replication TX Bandwidth [MBps]	This rule collects cluster replication transmitted bandwidth, expressed in megabytes per second.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:00 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Cluster Controller IOPS [count]	This rule collects the number of total cluster disk input/output operations per second on the controller.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:00 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Cluster Storage Usage [%]	This rule collects cluster storage usage, expressed as a percentage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:00 Tolerance Type – Percentage Tolerance – 10

Rule name	Description	Default values
		Maximum Sample Separation – 3
Container Reserved Space [%]	This rule collects container reserved space, expressed as a percentage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:02 Tolerance Type – Absolute Tolerance – 10 Maximum Sample Separation – 3
Container Space Usage [%]	This rule collects container reserved space usage, expressed as a percentage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:02 Tolerance Type – Absolute Tolerance – 10 Maximum Sample Separation – 3
Container Unreserved Space Usage [%]	This rule collects container unreserved space usage, expressed as a percentage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:02 Tolerance Type – Absolute Tolerance – 10 Maximum Sample Separation – 3
Container Controller IOPS [count]	This rule collects the number of container controller input/output operations per second.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:02 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Container Controller I/O Bandwidth [kBps]	This rule collects container controller input/output bandwidth, expressed in kilobytes per second.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:02

Rule name	Description	Default values
		Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Container Controller Average I/O Latency [ms]	This rule collects container controller average input/output latency, expressed in milliseconds.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:02 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Container Deduplication Saving Ratio [%]	This rule collects container deduplication ratio, expressed as a percentage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:02 Tolerance Type – Percentage Tolerance – 5 Maximum Sample Separation – 3
Container User Usage [B]	This rule collects container user usage, expressed in bytes.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:02 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Container Erasure Coding Saving Ratio [%]	This rule collects container erasure coding ratio, expressed as a percentage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:02 Tolerance Type – Percentage Tolerance – 5 Maximum Sample Separation – 3
Container Compression Saving Ratio [%]	This rule collects container compression ratio, expressed as a percentage.	Update Interval in Seconds – 300

Rule name	Description	Default values
		Timeout in Seconds – 120 Synchronization Time – 12:02 Tolerance Type – Percentage Tolerance – 5 Maximum Sample Separation – 3
Node CPU Usage [%]	This rule collects node CPU usage, expressed as a percentage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Absolute Tolerance – 10 Maximum Sample Separation – 3
Node Memory Usage [%]	This rule collects node memory usage, expressed as a percentage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Absolute Tolerance – 10 Maximum Sample Separation – 3
Node Average Disk I/O Latency [ms]	This rule collects node average disk input/output latency, expressed in milliseconds.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Node Content Cache Hits [count]	This rule collects the number of content cache hits on a node.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3

Rule name	Description	Default values
Node Disk I/O Bandwidth [MBps]	This rule collects node disk input/output bandwidth, expressed in megabytes per second.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Node Disk IOPS [count]	This rule collects the number of node disk input/output operations per second.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Node Content Cache Hits [%]	This rule collects the percentage of content cache hits on a node.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Absolute Tolerance – 10 Maximum Sample Separation – 3
Disk Usage [%]	This rule collects disk usage, expressed as a percentage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:04 Tolerance Type – Absolute Tolerance – 10 Maximum Sample Separation – 3
Disk Free Space [%]	This rule collects total free disk space, expressed as a percentage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:04 Tolerance Type – Absolute Tolerance – 10 Maximum Sample Separation –

Rule name	Description	Default values
		3
Disk IOPS [count]	This rule collects the number of total disk input/output operations per second.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:04 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Disk I/O Bandwidth [MBps]	This rule collects total disk input/output bandwidth, expressed in megabytes per second.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:04 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Average Disk I/O Latency [ms]	This rule collects average disk input/output latency, expressed in milliseconds.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:04 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Remote Site Bytes – Transmitted [count]	This rule collects the number of remote site transmitted bytes.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Remote Site Bytes – Received [count]	This rule collects the number of remote site received bytes.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Percentage Tolerance – 10

Rule name	Description	Default values
		Maximum Sample Separation – 3
Remote Site Replication Bandwidth – Received [MBps]	This rule collects received replication bandwidth of remote site, expressed in megabytes per second.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Remote Site Replication Bandwidth – Transmitted [MBps]	This rule collects transmitted replication bandwidth of remote site, expressed in megabytes per second.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Storage Pool Average Disk I/O Latency [ms]	This rule collects storage pool average disk input/output latency, expressed in milliseconds.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Storage Pool Unreserved Disk Space Usage [%]	This rule collects storage pool unreserved disk space usage, expressed as a percentage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Absolute Tolerance – 10 Maximum Sample Separation – 3
Storage Pool Disk IOPS [count]	This rule collects the number of storage pool disk input/output operations per second.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01

Rule name	Description	Default values
		Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Storage Pool Disk I/O Bandwidth [MBps]	This rule collects storage pool disk input/output bandwidth, expressed in megabytes per second.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Storage Pool Usage [%]	This rule collects storage pool usage, expressed as a percentage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Absolute Tolerance – 10 Maximum Sample Separation – 3
Storage Pool SSD Disk Usage [%]	This rule collects storage pool SSD unit usage, expressed as a percentage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Absolute Tolerance – 10 Maximum Sample Separation – 3
Storage Pool SATA Disk Usage [%]	This rule collects storage pool HDD unit usage, expressed as a percentage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Absolute Tolerance – 10 Maximum Sample Separation – 3
Storage Pool Free Disk Space [%]	This rule collects storage pool unreserved free disk space, expressed as a	Update Interval in Seconds – 300

Rule name	Description	Default values
	percentage.	Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Storage Pool Reserved Disk Space [%]	This rule collects storage pool reserved disk space, expressed as a percentage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Absolute Tolerance – 10 Maximum Sample Separation – 3
Storage Pool SSD vs HDD Usage [%]	This rule collects storage pool SSD versus HDD usage ratio, expressed as a percentage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Absolute Tolerance – 10
Protection Domain Bytes – Transmitted [count]	This rule collects the number of protection domain transmitted bytes.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Protection Domain Bytes – Received [count]	This rule collects the number of protection domain received bytes.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Protection Domain Replication Bandwidth – Transmitted [MBps]	This rule collects transmitted replication	Update Interval in Seconds – 300

Rule name	Description	Default values
	bandwidth of the Nutanix protection domain, expressed in megabytes per second.	Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Protection Domain Replication Bandwidth – Received [MBps]	This rule collects received replication bandwidth of the Nutanix protection domain, expressed in megabytes per second.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Pending Replications [count]	This rule collects the number of replications waiting to be executed.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Absolute Tolerance – 0 Maximum Sample Separation – 12
Ongoing Replications [count]	This rule collects the number of ongoing replications.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Absolute Tolerance – 0 Maximum Sample Separation – 12
Duration Of The Last Replication [s]	This rule collects duration of the last replication, expressed in seconds.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3

Rule name	Description	Default values
Time Since The Last Replication [H]	This rule collects duration of the time period since the last replication, expressed in hours.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:01 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
User Virtual Machine CPU Usage [%]	This rule collects virtual machine CPU load, expressed as a percentage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:02 Tolerance Type – Absolute Tolerance – 10 Maximum Sample Separation – 3
User Virtual Machine Memory Usage [%]	This rule collects virtual machine memory usage, expressed as a percentage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:02 Tolerance Type – Absolute Tolerance – 10 Maximum Sample Separation – 3
User Virtual Machine Controller Average I/O Latency [ms]	This rule collects virtual machine controller average input/output latency, expressed in milliseconds.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:02 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
User Virtual Machine Controller IOPS [count]	This rule collects the number of user virtual machine controller input/output operations per second.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:02 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation –

Rule name	Description	Default values
		3
User Virtual Machine Controller I/O Bandwidth [MBps]	This rule collects virtual machine controller input/output bandwidth, expressed in megabytes per second.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:02 Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Controller Virtual Machine Memory Usage [%]	This rule collects controller virtual machine memory usage, expressed as a percentage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:02 Tolerance Type – Absolute Tolerance – 10 Maximum Sample Separation – 3
Controller Virtual Machine CPU Usage [%]	This rule collects controller virtual machine CPU load, expressed as a percentage.	Update Interval in Seconds – 300 Timeout in Seconds – 120 Synchronization Time – 12:02 Tolerance Type – Absolute Tolerance – 10 Maximum Sample Separation – 3
Temperature [°C]	This rule collects hardware temperature, expressed in degrees Celsius.	Debug – false Update Interval in Seconds – 300 Synchronization Time – (not set) Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Power Supply Voltage [V]	This rule collects power supply voltage, expressed in volts.	Debug – false Update Interval in Seconds – 300 Synchronization Time – (not set) Tolerance Type – Percentage Tolerance – 10

Rule name	Description	Default values
		Maximum Sample Separation – 3
Fan Speed [rpm]	This rule collects fan speed, expressed in revolutions per minute.	Debug – false Update Interval in Seconds – 300 Synchronization Time – (not set) Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3
Power Supply Consumption [W]	This rule collects power consumption, expressed in watts.	Debug – false Update Interval in Seconds – 300 Synchronization Time – (not set) Tolerance Type – Percentage Tolerance – 10 Maximum Sample Separation – 3

Reports

SCOM MP for Nutanix provides reports listed in the table that follows. The reports are available in the SCOM Operations console in the Reporting view, in the following folders:

- HYCU SCOM Management Pack for Nutanix (HYCU Data Protection)
- HYCU SCOM Management Pack for Nutanix (Reports)

To generate and view a report, double-click its name. You can export reported data from SCOM in various formats: XML, CSV (comma delimited), PDF, MHTML (web archive), Excel, TIFF file, Word.

Table 6–4: SCOM MP for Nutanix reports

Report name	Description
HYCU Data Protection – Noncompliant Virtual Machines	This report provides a list of the monitored Nutanix virtual machines that are not compliant with the assigned HYCU Data Protection backup policies, and information on the assigned HYCU Data Protection backup policy and protection status for each of them. The following HYCU Data Protection compliancy statistics for monitored VMs are also included: noncompliant and compliant VM count per HYCU

Report name	Description
	Data Protection backup policy and in total. The data is presented in tables and charts.
Nutanix Enterprise Cloud Platform – Infrastructure Capacity Planning	This report provides a retrospective on usage of Nutanix cluster resources (storage, memory, CPU) for each selected cluster. It helps you predict, based on analysis of past usage, the date of complete consumption of each resource type. You can use this information to upsize the running-out resources in time. Note that predicted run-out dates heavily depend on the fluctuations in usage that happened during the period selected for analysis. The data is presented in tables and graphs.
Nutanix Enterprise Cloud Platform – Resource Consumption	This report provides information on current resource consumption for Nutanix clusters and detailed data on the Nutanix nodes and their hardware configuration, CPU capacity, CPU cores, memory size, storage capacity, and VM count per each cluster and in total. It also depicts the Nutanix resource utilization per cluster. You can use this report to quickly get a list of the available hardware resources used in your Nutanix clusters. The data is presented in tables and charts.
Nutanix Enterprise Cloud Platform – Resource Optimization	This report helps you optimize usage of Nutanix cluster resources. It first analyzes virtual machines' usage of the allocated resources (CPU, memory) through the chosen past period. Based on the analysis, it identifies virtual machines with excessive resources and virtual machines that went short of resources. The report then lists such oversized and undersized virtual machines together with a recommendation for optimal resource allocation. The data is presented in tables and charts.
Nutanix Enterprise Cloud Platform – Storage and Virtual Machine Density	This report lists utilization of the Nutanix storage pools and containers, sorts them by number of VMs that are hosted on them, displays some past utilization trends and the SSD–HDD ratio, which prompts you whether you must add more SSD units to the system or not. It helps you identify which

Report name	Description
	containers are inactive and can be deleted to release their reserved space for other containers.

Tasks

Through its Application Awareness feature, SCOM MP for Nutanix provides Nutanix virtual machine-related tasks. The tasks are available in the SCOM Operations console in the Monitoring view, in the Tasks pane, when a virtual machine is selected in the Table User VMs table.

Table 6–5: SCOM MP for Nutanix tasks

Task name	Description
Processes on VM By CPU Usage	A list of the currently running top processes by CPU usage on a VM. With this information, you can immediately recognize the process that causes high resource consumption and decide, whether there is some unwanted software on a VM causing this high resource consumption or if this is a consequence of a bigger load for applications running on it and more resources should be assigned to the VM.
Processes on VM By Memory Usage	A list of the currently running top processes by memory usage on a VM. With this information, you can immediately recognize the process that causes high resource consumption and decide, whether there is some unwanted software on a VM causing this high resource consumption or if this is a consequence of a bigger load for applications running on it and more resources should be assigned to the VM.
Open Nutanix Prism Home Page	Opens the Nutanix Prism Home page in the system default web browser.
Open Nutanix Prism Alerts Page	Opens the Nutanix Prism Alerts page in the system default web browser.
Open Nutanix Prism Hardware Page	Opens the Nutanix Prism Hardware page in the system default web browser.
Open Nutanix Prism Container Table	Opens the Nutanix Prism Container table in the system default web browser.
Open Nutanix Prism Disk Table	Opens the Nutanix Prism Disk table in the system default web browser.
Open Nutanix Prism	Opens the Nutanix Prism Host table in the system default web

Task name	Description
Host Table	browser.
Open Nutanix Prism Data Protection Page	Opens the Nutanix Prism Data Protection page in the system default web browser.
Open Nutanix Prism Async DR Table	Opens the Nutanix Prism Async DR table in the system default web browser.
Open Nutanix Prism Remote Site Table	Opens the Nutanix Prism Remote Site table in the system default web browser.
Open Nutanix Prism Storage Page	Opens the Nutanix Prism Storage page in the system default web browser.
Open Nutanix Prism Storage Pool Table	Opens the Nutanix Prism Storage Pool table in the system default web browser.
Open Nutanix Prism VM Page	Opens the Nutanix Prism VM page in the system default web browser.
Open Nutanix Prism VM Table	Opens the Nutanix Prism VM table in the system default web browser.

Tuning thresholds for performance monitors and rules

Some monitors and rules have default thresholds that might need additional tuning to suit your environment. You should evaluate monitors and rules to determine whether the default thresholds are appropriate. If a default threshold is not appropriate, baseline the relevant performance counters and then adjust the thresholds by overriding them.

For the detailed procedure on how to override the monitor or rule default values, see the SCOM documentation. For an example on how to override a monitor, see "Override default values in monitors and rules" below. For a list of the monitors and rules which default parameters you can adjust, see "Monitors" on page 50 and "Rules" on page 55.

Override default values in monitors and rules

There are several approaches on how to change the default thresholds in monitors and rules. You can make changes from different contexts and for different sets of objects. For the detailed and up to date procedures on how to override the monitor or rule default values, see the SCOM documentation.

For example, to change the default monitor thresholds for all objects of the same class, do the following:

1. Launch the SCOM Operations console and connect to the management server.
2. In the **Authoring** view, expand **Authoring** and then click **Monitors**. A list of the available monitors appears.
3. In the **Look for** text box, type the name of the monitor you want to update and then click **Find Now**.
4. In the results pane, right-click the monitor you want to update and then select **Overrides > Override the Monitor > For all objects of class**.
5. In the Override Properties window, locate and select the parameter you want to override.
6. For the selected parameter, change the default value in the **Override Value** column.
7. From the **Management pack** drop-down list, select an existing management pack (for example, `Microsoft.SystemCenter.SecureReferenceOverride`) or create a new one, and then click **Apply** to apply a new threshold value.
8. Click **OK**.

SuperPacks: Citrix XenApp and XenDesktop

The Citrix XenApp and XenDesktop (SuperPacks) dashboards are available in the SCOM Operations console in the Monitoring view, in the Nutanix SuperPacks (by HYCU) folder.

Table 6–6: Citrix XenApp and XenDesktop (SuperPacks) dashboards

Dashboard name	Description
Delivery Groups and Nutanix Resources	The dashboard displays Citrix delivery groups with the corresponding available load and average logon duration. For each delivery group, top 10 server or desktop OS machines per CPU, memory, IOPS, and I/O latency are listed to enable detecting of any excessive machine resource usage. All information on the dashboard is the latest snapshot of the environment. With this dashboard, you are able to detect potential resource issues for the delivery groups and remediate the situation by, for example, giving more resources to the server and desktop OS machines.
Logon Duration and Nutanix Resources	The dashboard displays how Citrix site logon duration and number of logons is related to the Nutanix cluster resource usage parameters like CPU, Memory, I/O latency, etc. during the last 24 hours. It helps you to detect any potential resource bottlenecks during the logon storm.

Dashboard name	Description
I/O Latency Alerts	The dashboard displays alerts generated due to poor I/O latency detected in the monitored Nutanix infrastructure. It also presents lists of Nutanix storage pools and Nutanix containers with impact on performance of Citrix server OS or desktop OS machines, together with a list of such OS machines. A graph is included that shows I/O latency for each depicted storage pool or container through the last 24 hours.
Storage Utilization Alerts	The dashboard displays alerts generated due to high storage utilization detected in the monitored Nutanix infrastructure. It also presents lists of Nutanix storage pools and Nutanix containers with impact on performance of Citrix server OS or desktop OS machines, together with a list of such OS machines. A graph is included that shows storage utilization for each depicted storage pool or container through the last 24 hours.
Server OS Machines and Nutanix Resources	The dashboard displays all server OS machines for the selected Citrix site with Citrix load information. In addition, the top 10 server or desktop OS machines per CPU, memory, IOPS, and I/O latency are listed with the basic Nutanix cluster resource usage information. All information on the dashboard is the latest snapshot of the environment. With this dashboard you can detect any server OS machines with excessive resource usage.
Sessions and Nutanix Resources	The dashboard displays how Citrix site sessions are related to the Nutanix cluster resource usage parameters like CPU, memory, I/O latency, etc. during the last 24 hours. It helps you to detect any potential resource bottlenecks during normal usage and allows you to plan resources based on the real usage pattern.

SuperPacks: Microsoft Exchange Server

The Microsoft Exchange Server (SuperPacks) dashboards are available in the SCOM Operations console in the Monitoring view, in the Nutanix SuperPacks (by HYCU) folder.

Table 6–7: Microsoft Exchange Server (SuperPacks) dashboards

Dashboard name	Description
I/O Latency Alerts	The dashboard displays alerts generated due to poor I/O latency detected in the monitored Nutanix infrastructure. It also presents lists of Nutanix storage pools and Nutanix containers with impact on performance of computers that host Microsoft Exchange Server, together with a list of such computers. A graph is included that shows I/O latency for each depicted storage pool or container through the last 24 hours.
Storage Utilization Alerts	The dashboard displays alerts generated due to high storage utilization detected in the monitored Nutanix infrastructure. It also presents lists of Nutanix storage pools and Nutanix containers with impact on performance of computers that host Microsoft Exchange Server, together with a list of such computers. A graph is included that shows storage utilization for each depicted storage pool or container through the last 24 hours.

SuperPacks: Microsoft SQL Server

The Microsoft SQL Server (SuperPacks) dashboards are available in the SCOM Operations console in the Monitoring view, in the Nutanix SuperPacks (by HYCU) folder.

Table 6–8: Microsoft SQL Server (SuperPacks) dashboards

Dashboard name	Description
Overview: Database Latency	The dashboard displays application groups of the Microsoft SQL Server deployments on Nutanix infrastructure. It also presents member computers, Nutanix storage pools, and Nutanix containers associated with the selected application group. A graph is included that shows database disk read/write latency through the last 24 hours. Additional graphs show I/O latency for the selected storage pool and the selected container through the last 24 hours.
I/O Latency Alerts	The dashboard displays alerts generated due to poor I/O latency detected in the monitored Nutanix infrastructure. It also presents lists of Nutanix storage pools and Nutanix containers with impact on performance of computers that host Microsoft SQL Server, together with a list of such computers. A graph is included that shows I/O latency for

Dashboard name	Description
	each depicted storage pool or container through the last 24 hours.
Storage Utilization Alerts	The dashboard displays alerts generated due to high storage utilization detected in the monitored Nutanix infrastructure. It also presents lists of Nutanix storage pools and Nutanix containers with impact on performance of computers that host Microsoft SQL Server, together with a list of such computers. A graph is included that shows storage utilization for each depicted storage pool or container through the last 24 hours.

Chapter 7

Troubleshooting

If you encounter problems with using SCOM MP for Nutanix, you can often solve them yourself. This chapter contains information that may help you in such cases.

General troubleshooting guidelines

When investigating an issue, first verify that:

- All installation prerequisites are fulfilled and the product is configured according to the provided instructions.
- You are not running into a known product limitation. For a list of the limitations, see the *HYCU SCOM Management Pack for Nutanix Release Notes*.
- Your issue is not related to third-party software or hardware (Nutanix or Microsoft). Otherwise, contact the respective vendor for assistance.
- You have the latest operating system and software application patches installed on the affected systems. Else, install the patches and check if the issue persists.
- The affected systems are not running out of memory or storage space.

Product log files

SCOM MP for Nutanix records its actions and occurrences of unexpected behavior (errors) into the log files. You can use the logged information to investigate issues.

Log file location

In SCOM MP for Nutanix, there are two sources of log entries:

- Data Collector
- Other product components

Data Collector creates and maintains its log files in the `%ProgramData%\Comtrade\Nutanix MP\Logs` directory. The log file names contain the log file creation date, for example, `2017-04-10.txt`. A log file is archived once its size reaches one gigabyte (1 GB). For each day, a maximum of five (5) log files are preserved.

Log entries of other product components are added to the operating system event log, into its `Applications and Services Logs > Operations Manager` section.

Log severity levels

Log entries (event records) have different severity levels. SCOM MP for Nutanix defines six different severity levels.

Table 7–1: Log severity levels in SCOM MP for Nutanix

Severity level	Log entry meaning
Fatal	Severe error
Error	Error, most often a consequence of an exception
Warn	Warning, typically alerting about a non-critical (recoverable) or temporary issue
Info	Informational message
Debug	Debugging data; a log entry used for troubleshooting
Trace	Tracing data; a voluminous log entry used for troubleshooting complex issues

By default, the severity level for log entries from either source is set to `Info`, which means only information messages, warnings, errors, and fatal errors are logged. You can change the level for troubleshooting purposes.

> Note When a particular log severity level is set, it causes messages with higher severity level to be recorded as well. For example, if the severity level is set to `Warn`, warnings, errors, and fatal errors are logged, but information, debugging, and tracing messages are not.

To change the severity level, do the following:

1. In the **Start** menu, type `regedit` in the **Search** text box, and then click the **Search** icon.
2. In the results list, click `regedit` or `regedit.exe`.
3. In the User Account Control dialog box, click **Yes**.
4. In the Registry Editor window, navigate to **HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > ConnectorSvc**.
5. Depending on the source of log entries for which you are changing the severity level, do the following:
   - Right-click the **ConnectorLoggingLevel** value and select **Modify**.
   - Right-click the **NutanixMPLoggingLevel** value and select **Modify**.
6. In the **Value data** text box, type a value from the Severity level column of table 10.

> Caution HYCU recommends that you back up Windows Registry before making any changes to it.

7. Click **OK**.
8. If you adjusted the severity level for entries originating from Data Collector, using the **Services** administrative tool of the operating system, restart the **HYCU SCOM Data Collector for Nutanix** service.

Problems and solutions

This section lists symptoms of common problems that you may encounter while using SCOM MP for Nutanix, together with proposed actions – resolution steps.

HYCU Nutanix MP Accessor node for Nutanix Cluster is not visible

Symptom

When setting up credentials of HYCU SCOM Management Pack for Nutanix: Monitoring Account, the HYCU Nutanix MP Accessor node for your Nutanix cluster does not show up in the list of the discovered objects.

Action

Do both of the following:

- Manually retrigger the `Nutanix Accessor Role Discovery` task to make sure the discovery is run.
- On the SCOM management server computer, inspect the Operations Manager event log for discovery related errors and take appropriate actions.

SCOM MP for Nutanix discovers nothing

Symptom

Nothing is discovered by SCOM MP for Nutanix after the product (including the monitoring user accounts) is configured.

Action

Do both of the following:

- On the SCOM management server computer, inspect the Operations Manager event log for discovery related errors and act accordingly.
- Verify that the Nutanix Accessor objects were successfully discovered as follows:
  1. Launch the SCOM Operations console and connect to the management server.
  2. In the **Monitoring** view, in the Monitoring pane, expand **Monitoring** and click **Discovered Inventory**.
  3. Right-click into the blank area of the Results pane and select **Change Target Type**.
  4. In the Select Items to Target window, select **View all targets** and then enter the

string `Accessor` into the **Look for** text box.

5. Locate and select the **HYCU Nutanix Accessor** target and then click **OK**.
6. Verify that the Nutanix Accessor node matches the listed Nutanix Cluster. If the Accessor node is missing, follow instructions in section "HYCU Nutanix MP Accessor node for Nutanix Cluster is not visible" on the previous page.

Graphs "User Virtual Machine CPU Load" and "User Virtual Machine Memory Usage" are empty

Symptom

Two graphs from the User VM Performance folder do not contain any data: `User Virtual Machine CPU Load`, `User Virtual Machine Memory Usage`. In the Operations Manager event log, an event with the Event ID 22402 is logged.

Action

Increase values of the `Update Interval` and `Timeout Seconds` parameters in the respective monitors: `User VM CPU Load Monitor`, `User VM Memory Usage Monitor`. Note that value of the `Timeout Seconds` parameter should be less or equal to value of the `Update Interval` parameter.

Nutanix Cluster Storage Running Out monitor does not generate alerts

Symptom

The Nutanix Cluster Storage Running Out monitor does not generate alerts, even when current usage of the Nutanix cluster storage is already near the storage capacity.

Inspection with the Event Viewer utility reveals existence of the following message in the operating system event log, in its `Applications and Services Logs > Operations Manager` section:

```
OleDb Module encountered a failure 0x80004005 during execution and will
post it as output data item. Unspecified error
: Login failed for user '<DomainName>\<UserName>'

Workflow name: Comtrade.Nutanix.Monitor.Storage.Prediction.Usage
Instance name: <InstanceName>
Instance ID: {<InstanceUUID>}
Management group: <ManagementGroupName>
```

This problem occurs only after upgrade from an earlier product version.

Action

Complete the upgrade process by following steps 2 to 11 of the upgrade procedure, as documented in chapter *Upgrade*, section "Upgrading SCOM MP for Nutanix" on page 34.

Applications hosted on some virtual machines are not discovered by Application Awareness

Symptom

In the Monitoring view of the SCOM Operations console, in `Table: User VMs` in the Monitoring > Nutanix (by HYCU) > VMs folder, indicators of discovered applications are missing for some VMs. When you run the `Processes on VM By CPU Usage` task for such virtual machine, it reports the following error:

```
Unable to connect to the remote virtual machine since AppAwareness WinRM
Account is not set.
```

Action

Do the following:

1. In the SCOM Operations console, switch to the Authoring view.
2. In the console tree, expand **Authoring > Management Pack Templates** and then select **HYCU SCOM Management Pack for Nutanix: Application Awareness Configuration**.
3. Check if management pack templates exist for this monitoring scenario:
   - If the templates do not exist, see section "Configuring the Application Awareness feature" on page 24 for instructions on how to configure an appropriate WinRM account.
   - If the templates already exist, proceed to the next step.
4. In the SCOM Operations console, switch to the **Administration** view.
5. In the console tree, expand **Administration > Run As Configuration > Accounts**.
6. In the results pane, in the Type: Basic Authentication list, check each configured **HYCUNutanixAppAwarenessAccount_<*Name*>** account for correct credentials:
   a. Double-click the account to open the Run As Account Properties dialog box, then click the **Credentials** tab.
   b. Verify the user name and re-enter the password. If the target VM is a member of a domain, ensure the user name is specified in the `<UserName>@<DomainName>` format.
   c. Click **OK** to save your changes.
7. Wait until the next discovery cycle and check if the applications are discovered as expected.

HYCU Data Protection-protected VMs: missing property values, failed monitors, spurious alerts, failed workflows

Symptom

While monitoring HYCU Data Protection-protected VMs, you notice any of the following:

- In the SCOM Operations console, in the Table: User VMs view, some virtual machines do not have populated values for their compute, memory, and storage-related properties. Monitors for the same properties are failing, resulting in absence of the corresponding alerts. Healthy state of the problematic VMs reads `Unmonitored`.
- Spurious virtual machine availability alerts are raised whose description contains the following information:

```
The virtual machine '{0}' has been removed from Nutanix cluster.

For more information, log on Nutanix Prism instance associated with the
respective Nutanix cluster. Use the following URL:
https://{1}:9440
```

- HYCU Data Protection virtual machine-related workflows fail. Their error report includes the following text:

```
Cannot bind argument to parameter 'ClusterIp' because it is an empty
string.
```

Listed symptoms are induced by the same root cause: Nutanix clusters that are visible to HYCU Data Protection, but are still undiscovered in SCOM.

Action

Do the following:

1. Configure connections to the Nutanix clusters that are visible from the corresponding HYCU Data Protection user interface, but have not been discovered in SCOM yet. For instructions, see section "Configuring SCOM MP for Nutanix connections" on page 22.
2. Wait until the next discovery cycle completes.

Getting assistance

Depending on the required type of assistance, do the following:

- If you need assistance with product evaluation, contact your HYCU account owner or sales representative.
- If you already purchased the product, you have a valid support agreements, and:

- You need assistance with *product licensing*, see section "Licensing assistance" below.
- You have *an issue with the product or your monitored environment*, see section "Support" below.

Licensing assistance

Depending on the service that you need, refer to the following:

- To generate license request files and activate them, follow instructions in chapter "Product licensing" on page 35.
- To change license scope and arrange any license management activities, contact your HYCU sales representative at the info@hycu.com email address.
- To redesignate licenses (deactivate existing licenses), go to the Licensing Portal | HYCU website. Sign in to your account and follow the License Redesignation steps.
- For any licensing-related issues or questions about the licensing process, send an email with detailed issue description (expected behavior, symptoms, screen shots, log files, and similar) or list of questions to info@hycu.com.

> **Note** Make sure to include your company name and purchase order (PO) number in communication with HYCU Customer Support.

Support

If you have an issue with the product or your monitored environment, collect the following data before contacting the Customer Support department:

1. General information:
   - Your company name
   - Purchase order (PO) number
2. Basic information about the environment such as:
   - Host operating system
   - Microsoft System Center Operations Manager version
   - Nutanix AOS version
   - Version of the installed SCOM MP for Nutanix (the product)
   - Whether you are still evaluating the product or already using a purchased license
   - Whether the product is installed in a development or production environment
3. Additional information such as:
   - Whether the product was installed or it was upgraded from an earlier version
   - Time when the product was installed
   - Time when the product was most recently reconfigured
   - Time when you first noticed issue symptoms
   - Versions of the monitored applications
   - Operating systems on which monitored applications are running

  - Whether the host operating system or monitored environment were updated recently

4. Detailed explanation of the issue, including:
   - Expected behavior
   - Issue symptoms
   - Screen shots of the user interfaces
   - List of troubleshooting actions that you have already taken

The above data is required by HYCU Customer Support so that a support engineer can efficiently investigate the issue from the very beginning. Pack collected support information into an archive, and do one of the following:

- *Preferred.* On the HYCU webpage, submit your request (support case) and include the archive attached.
- Send an email with the attached archive to support@hycu.com.

> ⚠ Important If the email attachment is too large or the email is getting rejected by the company email server, deliver the archive by using Comtrade File Sharing Facility.

To deliver data by using Comtrade File Sharing Facility, do the following:

1. Open a web browser and go to the Comtrade File Sharing Facility website.
2. Click **SHARE A FILE NOW** and then click **Browse**.
3. In the Choose File to Upload dialog box, browse to and select your archive file, and then click **Open**.
4. Repeat step 3 for each additional file you want to send.
5. On the Comtrade File Sharing Facility webpage, click **Upload Now** and then allow file processing to finish.
6. In the **To:** text box, type `support@hycu.com` and leave other text boxes blank.
7. At the bottom of the webpage, type the given anti-spam verification code in the corresponding text box.
8. Click **Process Details Now**.

Getting additional information and latest updates

For additional information about SCOM MP for Nutanix, visit the SCOM MP for Nutanix | HYCU webpage.

For the latest product version and most up-to-date documentation, go to the Nutanix Monitoring webpage.

Before contacting HYCU Customer Support

If you cannot solve your issue, report it. Before contacting HYCU Customer Support, make sure that:

- You perform the general checks. For details, see section "General troubleshooting guidelines" on page 79.
- You verify that your problem is not documented in this chapter. For more information, see section "Problems and solutions" on page 81.
- You collect relevant data that might be required to send to HYCU Customer Support: a description of your problem, configuration specification of your environment, and similar information. For details, see section "Customer Support" on page 93.

The HYCU Customer Support team will provide you with further instructions. Among other things, you may be asked to perform diagnostic operations in your environment and collect specific data from your systems and send it to HYCU.

> Note The HYCU Customer Support team is not qualified to solve the issues related to third-party software or hardware.

For information on how to reach HYCU Customer Support, see part "HYCU Customer Support and information " on page 93.

Appendix A

Manual configuration

This appendix includes instructions for setting up product-specific SCOM accounts manually, that is, not by using the provided configuration wizards.

For instructions for wizard-guided configuration, see following sections:

- "Configuring SCOM MP for Nutanix connections" on page 22
- "Configuring the Application Awareness feature" on page 24.

Setting up action account for monitoring Nutanix infrastructure

Before manually setting up action account for monitoring Nutanix infrastructure, make sure that the Application Awareness prerequisites listed in "Configuring SCOM MP for Nutanix" on page 21 are fulfilled.

To set up Nutanix monitoring action account (`HYCU SCOM Management Pack for Nutanix: Monitoring Account`), do the following:

1. Launch the SCOM Operations console and connect to the management server.
2. In the **Administration** view, expand **Run As Configuration**, and then click **Profiles**.
3. In the results pane, double-click **HYCU SCOM Management Pack for Nutanix: Monitoring Account**.
4. In the Run As Profile Wizard window, click **Run As Accounts**. In the Run As Accounts page, click **Add**.
5. In the Add a Run As Account dialog box, click **New** to open Create Run As Account Wizard.
6. In the Create Run As Account Wizard window, click **Next**.
7. In the General Properties page, from the **Run As account type** drop-down list, select **Basic Authentication**.
8. In the **Display name** text box, enter account name as it will be displayed in the SCOM Operations console. Click **Next**.
9. In the Credentials page, enter valid Nutanix Prism user account credentials in the respective text boxes. Click **Next**.
10. In the Distribution Security page, make your selection as appropriate and then click

Create.

11. Upon notification about successful Run As account creation, click **Close** to close the wizard.
12. In the Add a Run As Account dialog box, click **A selected class, group, or object**. From the **Select** drop-down list, select **Object**.
13. In the Object Search dialog box, from the **Look for** drop-down list, select **HYCU Nutanix Accessor**, and then click **Search**.
14. In the Available items list, select the Nutanix cluster you want to associate with this account, and then click **Add**. Click **OK** to close the Object Search dialog box.

    > Note If a name of the cluster node is listed instead of the cluster name, select the node name.

15. Click **OK** to close the Add a Run as Account dialog box.
16. In the Run As Profile Wizard window, review your configuration and then click **Save** to save your changes.
17. Upon warning about Run As credentials distribution, in the More secure Run As accounts list, click the newly created account.
18. Use controls in the Run As Account properties dialog box and Computer Search window to distribute credentials of the Run As account to each member of HYCU Nutanix Management Pool.

Setting up action account for Application Awareness

Before manually setting up action account for Application Awareness, make sure that the Application Awareness prerequisites listed in "Configuring SCOM MP for Nutanix" on page 21 are fulfilled.

To set up Application Awareness action account (`HYCU SCOM Management Pack for Nutanix: AppAwareness WinRM Account`) and enable application discovery and monitoring, do the following:

1. Launch the SCOM Operations console and connect to the management server.
2. In the **Administration** view, expand **Run As** Configuration, and then click **Profiles**.
3. In the results pane, double-click **HYCU SCOM Management Pack for Nutanix: AppAwareness WinRM Account**.
4. In the Run As Profile Wizard window, click **Run As Accounts**. In the Run As Accounts page, click **Add**.
5. In the Add a Run As Account dialog box, click **New** to open Create Run As Account Wizard.
6. In the Create Run As Account Wizard window, click **Next**.

7. In the General Properties page, from the **Run As account type** drop-down list, select **Basic Authentication**.
8. In the **Display name** text box, enter account name as it will be displayed in the SCOM Operations console. Click **Next**.
9. In the Credentials page, enter valid local administrative user account credentials in the respective text boxes. Click **Next**.
10. In the Distribution Security page, make your selection as appropriate and then click **Create**.
11. Upon notification about successful Run As account creation, click **Close** to close the wizard.
12. In the Add a Run As Account dialog box, click **A selected class, group, or object**. From the **Select** drop-down list, select one of the following:
    - **Object**, to use the user account in all your environments in the single domain in the cluster.

      In the Object Search window, search for **HYCU Nutanix Accessor**, then select the cluster you want to associate with this account, click **Add**, and then click **OK**.

      > Note If a name of the cluster node is listed instead of the cluster name, select the node name.

    - **Groups**, to use the user account in a specific domain within the cluster.

      In the Group Search window, search for the group that was created with the HYCU SCOM Management Pack for Nutanix: Application Awareness Configuration wizard to associate with this account. Select a group created with a template and then click **OK**.
13. Click **OK** to close the Add a Run as Account dialog box.
14. In the Run As Profile Wizard window, review your configuration and then click Save to save your changes.
15. Upon warning about Run As credentials distribution, in the More secure Run As accounts list, click the newly created account.
16. Use controls in the Run As Account properties dialog box and Computer Search window to distribute credentials of the Run As account to each member of HYCU Nutanix Management Pool.

Setting up action account for individual monitored applications

To complete configuration of Application Awareness, you must perform additional configuration steps for each application that you plan to monitor. For a list of the supported applications, see the *HYCU SCOM Management Pack for Nutanix Compatibility Matrix*.

> ⚠ Important To configure different application administrative user accounts for use in different environments, make sure that application objects are already discovered and available. Application discovery on virtual machines usually takes approximately 24 hours to complete. Application objects are therefore not available immediately after the product is installed.

To set up action accounts for individual monitored applications, do the following:

1. Launch the SCOM Operations console and connect to the management server.
2. In the **Administration** view, expand **Run As Configuration**, and then click **Profiles**.
3. Depending on the application you plan to monitor, double-click one of the following:
   - **HYCU SCOM Management Pack for Nutanix: AppAwareness Citrix Admin Account**
   - **HYCU SCOM Management Pack for Nutanix: AppAwareness Microsoft Exchange Server Admin Account**
   - **HYCU SCOM Management Pack for Nutanix: AppAwareness Microsoft SharePoint Admin Account**
   - **HYCU SCOM Management Pack for Nutanix: AppAwareness Microsoft SQL Server Admin Account**
   - **HYCU SCOM Management Pack for Nutanix: HYCU Data Protection Monitoring Account**
   - **HYCU SCOM Management Pack for Nutanix: IPMI Monitoring Account**
   - **HYCU SCOM Management Pack for Nutanix: Monitoring Account**
4. In the Run As Profile Wizard window, click **Run As Accounts**. In the Run As Accounts page, click **Add**.
5. In the Add a Run As Account dialog box, click **New** to open Create Run As Account Wizard.
6. In the Create Run As Account Wizard window, click **Next**.
7. In the General Properties page, from the Run As account type drop-down list, select **Basic Authentication**.
8. In the **Display name** text box, enter account name as it will be displayed in the SCOM Operations console. Click **Next**.
9. In the Credentials page, enter valid application administrative user account credentials in the respective text boxes. Click **Next**.
10. In the Distribution Security page, make your selection as appropriate and then click **Create**.
11. Upon notification about successful Run As account creation, click **Close** to close the wizard.
12. In the Add a Run As Account dialog box, click **A selected class, group, or object**. From the **Select** drop-down list, select one of the following:

- **Object**, to use the user account in all your environments in the single domain in the cluster.

  In the Object Search window, search for **HYCU Nutanix Accessor**, then select the cluster you want to associate with this account, click **Add**, and then click **OK**.

  > Note If a name of the cluster node is listed instead of the cluster name, select the node name.

- **Groups**, to use the user account in a specific domain within the cluster.

  In the Group Search window, search for the group that was created with the HYCU SCOM Management Pack for Nutanix: Application Awareness Configuration wizard to associate with this account. Select a group created with a template and then click **OK**.

13. Click **OK** to close the Add a Run as Account dialog box.
14. In the Run As Profile Wizard window, review your configuration and then click **Save** to save your changes.
15. Upon warning about Run As credentials distribution, in the More secure Run As accounts list, click the newly created account.
16. Use controls in the Run As Account properties dialog box and Computer Search window to distribute credentials of the Run As account to each member of HYCU Nutanix Management Pool.

HYCU Customer Support and information

Use the communication channels listed in this section if you need:

- Help with the product licensing process
- Assistance while using the product
- Additional information about this product
- Information about other HYCU products

Customer Support

Should you require additional information or assistance while using the product, contact the vendor that shipped it.

If you have purchased the product directly from HYCU, and are experiencing a problem, search for a solution on the following webpage:
support.hycu.com

In the absence of an article addressing your problem, ask HYCU Customer Support for assistance: on the webpage, click **Submit a request** and fill in the request form. You must be signed in with a valid account prior to submission. Apply for an account at the following email address:
support@hycu.com

Important: Before submitting a request to the Customer Support department, perform a health check on all systems that are in failed (critical, red) state and have the following information ready:

- Symptoms
- Sequence of events leading to the problem
- Commands and options that you used
- Messages you have received (a description with the date and time)

For a complete list of pieces of required support information, check troubleshooting sections in the product documentation.

Company website and video channel

For more information about our company and other products we offer, visit HYCU website at:
www.hycu.com

For additional product-related information, watch videos on the HYCU channel on YouTube:
www.youtube.com/c/HYCUInc

General information

For questions related to product business or purchase of this or other HYCU products, send an email to:
info@hycu.com

Feedback

For comments or suggestions about this product, including its documentation, send an email to:
info@hycu.com

We will be glad to hear from you!

www.hycu.com

HYCU