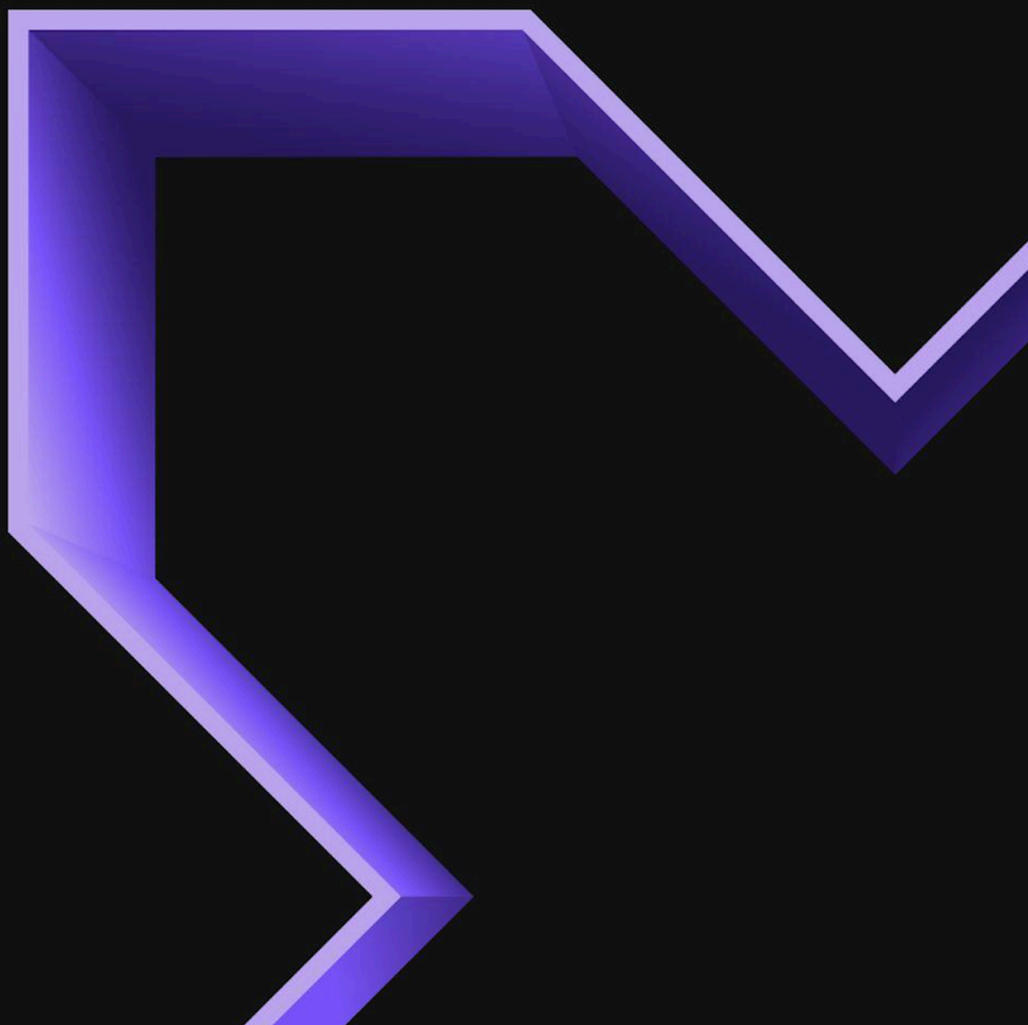
Prism Central Infrastructure Guide

Prism pc.2024.1

May 22, 2024



NUTANIX

Contents

About this Publication.....7

Prism Central Documentation Portfolio.....9

Related Documentation.....10

Getting Started.....11
- Prism Central Overview.....11
  - Logging Into Prism Central.....12
  - Prism Central Landing Page.....14
  - Application Switcher Function.....19
  - Prism Central Settings (Infrastructure).....22
  - Understanding Displayed Statistics.....24
  - Infrastructure Overview.....25
  - Admin Center Overview.....26
  - Prism Central GUI Organization.....27
- Prism Central Installation or Upgrade.....32
  - Prism Central Upgrade Methods.....33
  - Prism Central Upgrade Requirements.....34
  - Prism Central Upgrade Limitations.....36
  - Prism Central Upgrade vDisk.....37
  - Running NCC (Prism Central).....37
  - Upgrading Prism Central.....38
  - Prism Central-Managed Clusters Upgrade.....39
  - Prism Central Installation or Upgrade in Non-Nutanix ESXi Environment.....41
  - Service Manager for Installing Services and Applications.....49
- Prism Central Licensing.....51
- X-Small Prism Central.....51
- Registering or Unregistering a Cluster with Prism Central.....53
  - Unregistering from Prism Central.....54
- Application-specific Navigation Bar.....57
- Searching for Information.....60

Main Dashboard - Infrastructure.....71
- Dashboard Management.....73
  - Resetting Dashboard.....75
  - Setting Data Density.....76
  - Creating a New (Custom) Dashboard.....76
  - Modifying a Dashboard.....78
  - Sharing a Dashboard.....79
  - Generating a Dashboard Summary Report.....83
- Widgets Management.....86
  - Adding Dashboard Widgets.....89

Compute and Storage Entities..... 94
VM Management..... 94
VMs Summary View..... 95
VM Details View..... 108
Creating a VM through Prism Central (AHV)..... 121
Managing a VM through Prism Central (AHV)..... 134
Adding Multiple vGPUs to the Same VM..... 147
VM Migration Specifications..... 148
Creating a VM through Prism Central (ESXi)..... 161
Managing a VM through Prism Central (ESXi)..... 165
Nutanix Guest Tools..... 165
Storage Quality of Service (QoS)..... 186
Memory Overcommit Management..... 188
Policies for VM Management..... 188
VM Template Management..... 188
VM Template Summary View..... 189
VM Template Details View..... 190
Limitations of VM Template Feature..... 193
Creating a VM Template..... 193
Deploying VM from a Template..... 196
Managing a VM Template..... 200
Kubernetes Clusters Management..... 202
Onboarding the Kubernetes Cluster to Prism Central..... 203
Kubernetes Clusters Summary View..... 205
Kubernetes Cluster Details View..... 207
OVA Management..... 214
OVAs Summary View..... 215
Exporting a VM as an OVA..... 218
Uploading an OVA..... 219
Concatenating Upload using APIs..... 226
Deploying an OVA as VM..... 229
Downloading an OVA..... 236
Renaming an OVA..... 236
Deleting an OVA..... 237
Image Management..... 238
Images Summary View..... 239
Image Details View..... 242
Requirements..... 243
Limitations..... 243
Adding an Image..... 244
Image Upload Verification..... 259
Modifying an Image..... 260
Importing Images to Prism Central..... 261
Policies for Image Management..... 262
Catalog Management..... 262
Catalog Items Summary View..... 263
Adding a Catalog Item..... 264
Deleting a Catalog Item..... 267
Storage Container Management..... 268
Storage Containers Summary View..... 269
Storage Container Details View..... 275
Storage Components..... 280
Limitations for Storage Containers..... 290
Creating a Storage Container..... 290

Modifying a Storage Container....296
Deleting a Storage Container....300
Volume Group Management....300
Volume Groups Summary View....301
Volume Group Details View....306
Creating a Volume Group....314
Modifying a Volume Group....321
Configuring Mutual CHAP Authentication....324
Attaching Volume Groups to Guest VMs....325
Cluster RBAC for Volume Group....325
External vCenter Server Integration....326
External vCenter Datastores Summary View....327
External vCenter Datastore Details View....332
Registering External vCenter Server (Prism Central)....336
Unregistering a Cluster from the External vCenter Server (Prism Central)....339
Managing External vCenter Server Registration Changes (Prism Central)....340

Network and Security Entities....341
Subnets....341
Subnets Summary View....342
Subnet Details View....344
Network Configuration....346
Virtual Private Clouds....357
Virtual Private Clouds Summary View....357
Virtual Private Cloud Details View....359
Traffic Mirroring....363
Traffic Mirroring Summary View....365
Traffic Mirroring Details View....367
Creating a Traffic Mirroring Session....368
Disabling a Traffic Mirroring Session....372
Enabling a Traffic Mirroring Session....372
Updating a Traffic Mirroring Session....372
Deleting a Traffic Mirroring Session....373
Traffic Mirroring Session Alerts....373
Role-Based Access Control in Traffic Mirroring....374
Floating IPs....375
Floating IPs Summary View....375
Connectivity....376
Gateways Summary View....376
Gateway Details View....378
VPN Connections Summary View....380
VPN Connection Details View....381
Subnet Extensions Summary View....386
Subnet Extension Details View....388
BGP Sessions Summary View....391
BGP Session Details View....393
Security Policies....395
Security Dashboard....395

Data Protection and Recovery Entities....396
Protection Summary....396
Protection Policies....396
Recovery Plans....396
VM Recovery Points....396

VG Recovery Points....396
Consistency Groups....396

Hardware Entities....397
Cluster Management....397
Clusters Summary View....398
Cluster Details View....405
Creating a Cluster....417
Destroying a Cluster....418
Host Management....420
Hosts Summary View....420
Host Details View....424
Renaming an AHV Host....429
Expanding a Cluster through Prism Central....430
Removing a Node through Prism Central....436
Disks Summary View....438
Disk Details View....441
GPUs Summary View....444
GPU Details View....445

Activity Entities – Alert and Event Monitoring....447

Activity Entities – Tasks and Audits....448
Audits Summary View....448
Audit Details View....450
Tasks View....451

Operations Entities....453

Administration Entities....454
Availability Zones....454
Category Management....454
Categories Summary View....455
Category Details View....457
Creating a Category....457
Modifying a Category....458
Assigning a Category....459

Policies in Infrastructure....461
VM Policy Management....461
Affinity Policies Defined in Prism Central....461
NGT Policies....472
Image Policy Management....476
Image Placement Policies....476
Bandwidth Throttling Policies....484
Security Policy Management....490
Security Policies Summary View....490
Security Policy Details View....494
Storage Policy Management....495
Default Storage Policy....498

Storage Policies Summary View....500
Storage Policy Details View....503
Storage Policy Compliance....507
Storage Policy Based Replication Factor....508
Storage Policy Based Encryption....508
Creating a Storage Policy....510
Managing Storage Policies....514
Deleting a Storage Policy....516

Prism Self Service Administration....519
Prism Self Service Setup....519
Creating a VM (Self Service)....521
Creating a VM from Catalog Items (Self Service)....521
Managing a VM (Self Service)....528
Assigning a VM to a Project Member....529

Additional Operations....531
Managing Prism Central....531
Microservices Infrastructure....534
Prism Central Backup and Restore....546
Intelligent Operations....556
High Availability in Prism Central....556
Finding the Prism Central Version....557
Finding the AHV Version on Prism Central....558
Finding the AOS Version Using Prism Central....558
Expanding (Scale Out) Prism Central....559
Shutting Down or Starting Up Prism Central VM....565
Shutting down or starting up all the PC VMs in a Prism Central Configuration....565
Shutting down or starting up a single PC VM in a scale-out PC configuration....566
Keyboard Shortcuts in Prism Central....566
IP Address Reconfiguration....567
Preparing to Reconfigure the IP Address and Gateway of PC VMs....567
Reconfiguring the IP Address and Gateway of Prism Central VMs....568
Logging Out of Prism Central....570

Customer Support Services....571
Configuring Remote Connection Using CLI....571
Creating a Support Case....572
Viewing Case Status....575
Accessing the Nutanix Support Portal (Prism Central)....576
Accessing the REST API Explorer....579

Help Resources....580
Accessing Online Help (Prism Central)....580
Accessing the Nutanix Next Community....582
Glossary....582

Copyright....583

ABOUT THIS PUBLICATION

This document provides the information about how to set up the site infrastructure using Prism Central.

- For information about all the documents applicable for Prism Central, see Prism Central Documentation Portfolio on page 9.
- For information about how to access this document using online help option, see Accessing Online Help (Prism Central) on page 580.
- To access other Nutanix documents, see Nutanix support portal.

Scope of the Document

The scope of this document is limited to describe the following infrastructure-specific attributes and operations that you can perform using Prism Central:

- Monitor and Analyze system performance using exhaustive Dashboard. For more information, see Main Dashboard - Infrastructure on page 71.
- Compute and Storage Settings. For more information, see Compute and Storage Entities on page 94.
- Network and Security Settings. For more information, see Network and Security Entities on page 341.
- Data Protection and Recovery Settings. For more information, see Data Protection and Recovery Entities on page 396.
- Checking the Hardware Entities and managing Hosts. For more information, see Hardware Entities on page 397.
- Checking Alerts and Events for fault management. For more information, see Activity Entities – Alert and Event Monitoring on page 447.
- Checking ongoing and completed tasks and performing system Audits. For more information, see Activity Entities – Tasks and Audits on page 448.
- Performance Monitoring, Application Discovery, and Reports Management. For details, see Operations Entities on page 453.
- Define policies for configuration ease. For more information, see Policies in Infrastructure on page 461.
- Additional operations that include how to find the Prism Central version, AHV version, AOS version, shutdown Prism Central, perform disaster recovery, reconfigure Prism Central IP address and gateway, pair Availability Zones (AZ), logout from Prism Central, and use keyboard shortcuts. For more information, see Additional Operations on page 531.
- Prism Central self service setup. For more information, see Prism Self Service Administration on page 519.
- Customer support services from Nutanix for Prism Central. For more information, see Customer Support Services on page 571.

For a quick overview about all the infrastructure-related operations that you can perform through Prism Central, see Infrastructure Overview on page 25.

The admin-related operations are covered in the *Prism Central Admin Center Guide*. For information about how the Prism Central documentation is organized, see Prism Central Documentation Portfolio on page 9.

For a quick overview about all the admin-related operations that you can perform through Prism Central, see Admin Center Overview on page 26.

Intended Audience

The intended audience for this document are the site personnels, customer's operation teams and any tier or individual entity defined by the customer who is equipped to perform the site configurations and modifications. In addition to this, any individual with an intention to learn and develop understanding about Prism Central usage, can refer this document.

PRISM CENTRAL DOCUMENTATION PORTFOLIO

The following table describes how Prism Central documentation portfolio is organized:

Table 1: Prism Central Documentation Portfolio

Deliverable Name	Description
Prism Central Admin Center Guide	This document describes all the administrative-level tasks that you can perform from Prism Central using **Admin Center** application. For more information about **Admin Center** application, see Admin Center Overview on page 26. For more information about how to access the **Admin Center** application in Prism Central, see Application Switcher Function on page 19.
Prism Central Alerts and Events Reference Guide	This document describes how to mange alerts and events management from Prism Central. The Alerts and Events generated in Prism Central enables you to perform the fault management related operations.
Prism Central Infrastructure Guide	This document describes all the field-specific settings required to host a cluster in Prism Central. It covers all the operations that you can perform from Prism Central using **Infrastructure** application. For more information about **Infrastructure** application, see Infrastructure Overview on page 25. For more information about how to access the **Infrastructure** application in Prism Central, see Application Switcher Function on page 19.
Intelligent Operations Guide	This document describes the Prism Central intelligent operations functionality, and how to enable, disable, and perform configurations related to Intelligent Operations part of Cloud Manager module.

RELATED DOCUMENTATION

Links to Nutanix Support Portal software and documentation.

The Nutanix Support Portal provides software download pages, documentation, compatibility, and other information.

> **Note:** See Ports and Protocols for information about the ports that are used by Prism Central, Microservices Infrastructure and other Nutanix Software.
>
> On the Ports and Protocols page, select the appropriate software or application such as **Prism Central** or **Microservices Infrastructure** in the **Software Type** dropdown menu to view the ports and protocols used by that Nutanix software or application.

Documentation	Description
Release Notes | Flow Virtual Networking	Flow Virtual Networking Release Notes
Port And Protocols	Port Reference: See this page for details of ports that must be open in the firewalls to enable Flow Virtual Networking to function.
Nutanix Security Guide	Prism Element and Prism Central security, cluster hardening, and authentication.
Flow Network Security Next Gen	Flow Network Security Next-Gen is the next-generation Nutanix microsegmentation solution with an enhanced policy model, advance policy operation, and enterprise readiness features. FNG
AOS guides and release notes	Covers AOS Administration, Hyper-V Administration for Acropolis, Command Reference, Powershell Cmdlets Reference, AOS Family Release Notes, and AOS release-specific Release Notes
Life Cycle Manager Guide	How to upgrade firmware and software components.
AHV guides and release notes	Administration and release information about AHV.
Prism Central and Web Console guides and release notes	Administration and release information about Prism Central and Prism Element. Select **Release** in the Release Version selector at the top of the page.

GETTING STARTED

This section provides an overview of Prism Central that involves the following information:

- Prism Central landing page, Infrastructure dashboard and entities, statistics, application switcher, and Prism Central GUI Organization.
- Installation and upgrade specifics.
- Licensing information.
- Cluster registration and de-registration with Prism Central.
- Application-specific navigation bar and searchability attributes.
- Prism Central GUI access.

Prism Central Overview

Prism Central provides a workspace to monitor and manage multiple clusters from a centralized environment. It runs as a separate instance that consists of either a single VM or as a three-VM scale-out architecture. For more information, see Expanding (Scale Out) Prism Central on page 559.

Prism Central provides the following functionalities:

- Platform-related functionalities that include:
  - Configuration and management of administrative activities such as Licensing, Life Cycle Manager (LCM), Identity and Access Management (IAM), Projects, Prism Central UI specific settings, and admin-specific settings, which are applicable across platforms and/or for various Nutanix Apps such as NCM Self-Service, Files, Move, Objects, Database Service, Foundation Central, or Kubernetes Management. IAM, LCM, or Projects are applicable for both Nutanix Apps and platforms.
  - Discover, deploy, and manage Nutanix Apps such as *NCM Self-Service*, *Files*, *Move*, *Objects*, *VolumesDatabase Service*, *Foundation Central*, or *Kubernetes Management* and other hybrid cloud applications (preferred partner apps) from Prism Central.
  - Facilitate consumption of pre-configured and custom apps (categorized as Other Apps) that are tailored for specific needs when Calm is deployed and licensed in the Prism Central instance.
  - Alerts and Notifications related configurations. For more information, see Configuring Alerts in Prism Central information in *Prism Central Admin Center Guide*.
  - Security-related configurations.

  For more information about all the admin-related activities that you can perform using Prism Central, see Admin Center Overview on page 26.
- Cloud Infrastructure-related functionalities that include:
  - Site-specific configurations and operations.
  - Fault and performance management operations. For more information, see Prism Central Alerts and Events Reference Guide.

  For more information, see Infrastructure Overview on page 25.

- Cloud Manager-related functionalities that include accessing the Cost Governance (formerly called as Beam), NCM Self-Service and Security Central applications, and configuring Prism Intelligent Operations. For more information, see the following documentation:
  - Cost Governance
  - Self-Service
  - Security Central
  - Intelligent Operations Guide

Logging Into Prism Central

About this task

This section describes how to log into Prism Central. The Knowledge Base article KB 1661 lists the default cluster credentials.

Procedure

To log in to Prism Central, perform the following steps:

1. Open a web browser, enter http://*management_ip_addr* in the address field, and press **Enter**.
   Replace *management_ip_addr* with the Prism Central VM IP address.

   > **Note:** Prism Central supports the latest version, and the two preceding major versions of Firefox, Chrome, Safari, and Microsoft Edge browsers. The browsers must support TLS 1.2.

   The system redirects to the encrypted port (9440) and prompts you to accept the **Terms and Conditions**. The system might display an SSL certificate warning. Acknowledge the warning and proceed to the site. If user authentication is enabled and the browser does not have the correct certificate, a denied access message may appear. For the complete list of required ports, see Port Reference.
2. Click **Accept terms and conditions**. The system displays the login screen.

3. Enter your Nutanix login credentials and press **Enter** or click **Log In**.

   The login credentials might vary based on the authentication mechanism configured to access Prism Central. For more information about supported authentication mechanisms for Prism Central, see Configuring Authentication information in *Security Guide*.

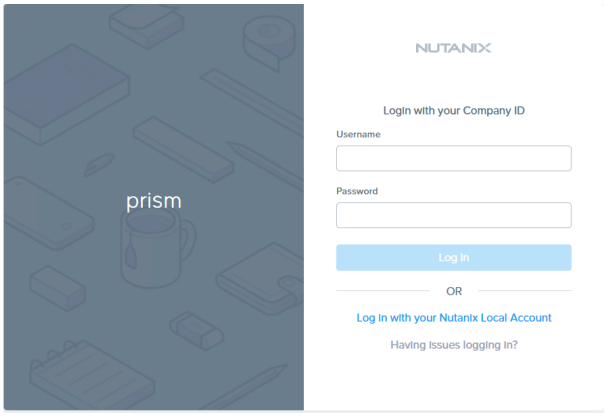


Figure 1: Login Screen

Note:

- If LDAP authentication is used, enter the user name in *username@domain* format; the *domain\username* format is not supported. The user principle name [UPN] attribute is used to find the user account in Active Directory, so your user name must be in that format.

  Note: If there is more than one LDAP/AD, the Prism Central login screen shows multiple boxes to select the configured domain names.

- The login page includes background animation that is enabled by default. You can modify it based on your requirement. For more information about how to configure Prism Central UI Settings, see *Prism Central Admin Center Guide*.
- If you are logging in as an administrator for the first time (user name admin and default password Nutanix/4u), the system prompts you to change the default password. Enter a new password in the **password** and **re-type password** fields and press **Enter**.

  Note: The system also prompts you to accept the license agreement if the EULA agreement is changed or you are logging in for the first time. In this case, enter appropriate

information in the **Name**, **Company**, and **Job Title** fields, and accept the terms and conditions for the license agreement.

The password must meet the following complexity requirements:

- At least 8 characters long
- At least 1 lowercase letter
- At least 1 uppercase letter
- At least 1 number
- At least 1 special character (allowed special characters are: "#$%&'()* +,-./:;<=>@[]^_`{|}~!)
- At least 4 characters different from the old password
- Should not be among the last 10 passwords

After you successfully change the password, the new password is synchronized across all Controller VMs and interfaces (Prism web console, nCLI, and SSH).

The default password expiration age for the `admin` user is 60 days. You can log in to PCVM with SSH and run the following commands to configure the minimum and maximum password expiration days based on your security requirement:

- `nutanix@pcvm$ sudo chage -M <MAX-DAYS> admin`
- `nutanix@pcvm$ sudo chage -m <MIN-DAYS> admin`
- After you upgrade from an AOS earlier version and then attempt to log in to Prism Central as the admin user, you are prompted to create a new admin user password.
- When you change the admin user password, ensure that you update any applications or scripts that uses the admin user credentials for authentication. Nutanix recommends that you create a service account with the admin role instead of using the admin user for authentication. For more information on authentication and roles, see Security Management Using Prism Central (PC) information in *Security Guide*.

Prism Central Landing Page

This section describes the functionalities available on the Prism Central landing page. The default application to be loaded in the Prism Central landing page is defined using the **Admin Center** application.

- For information about how to access the **Admin Center** application, see Application Switcher Function on page 19.
- For information about how to set the default landing page, see Prism Central Admin Center Guide.

Note: The **Main Dashboard** is the first page that appears after logging into Prism Central if the default landing page set is **Infrastructure**. For more information about **Main Dashboard**, see Main Dashboard - Infrastructure on page 71.

An example Prism Central landing page when **Infrastructure** is set as default landing page:

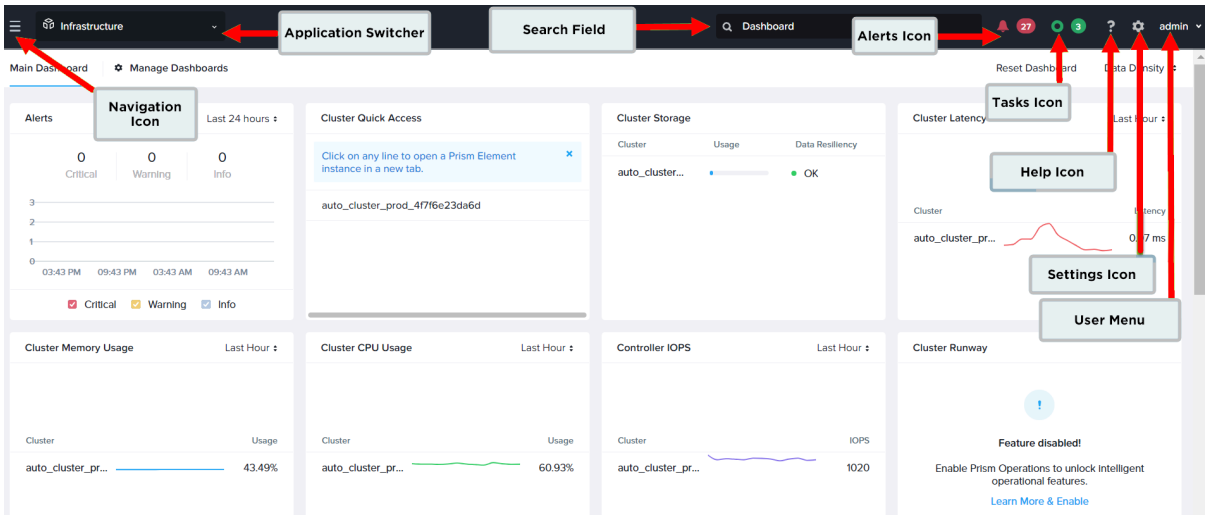


Figure 2: Prism Central Landing Page

Icons in Prism Central UI

The following table describes the list of icons used in Prism Central UI for accessibility, navigation, configuration, and observation purposes:

Table 2: Icons - Prism Central UI

Icon	Name	Description
	Alerts icon	The Alerts icon appears on the right of the Prism Central landing page. Select the Alerts icon to display the alert messages that are raised by the system. For more information about Alerts, see Prism Central Alerts and Events Reference Guide.
	Tasks icon	The Tasks icon appears next to the alerts icon on the Prism Central landing page. Select the tasks icon to view the running or completed tasks. The system displays the tasks data of the last 48 hours. You can also select **View All Tasks** at the bottom of the list to display all the tasks. For more information, see Tasks View on page 451. You can also navigate to **Activity** > **Tasks** from the **Navigation Bar** to view the **Tasks** page. **Note:** If one or more of those tasks do not complete successfully, the tasks icon turns yellow (warning) or red (failure). The tasks icon turns blue color when all the tasks are running properly or completed successfully. Select the Tasks icon to see a list of the current tasks.
	Help icon	The help icon appears on the right side of the Prism Central landing page. For more information about the help resources available in Prism Central, see Help Resources on page 17.

Icon	Name	Description
	Navigation icon	The navigation icon is used to access the **Navigation Bar** for the selected Prism Central application. For more information, see Navigation Bar on page 17.
	Search icon	The Search icon appears on the right of the Prism Central landing page. Enter a string in this field to search for relevant content in Prism Central. For more information, see Searching for Information on page 60.
	Bookmark icon	The Bookmark icon is used for quicker access to a specific page or filtered entry. When you bookmark a page or a filtered entry, the system displays that page or filtered entry under **Bookmarks** in **Navigation Bar**.
	Settings icon	The Settings icon appears on the right side of the Prism Central landing page. Click the Settings icon to view the **Prism Central Settings** page for the **Infrastructure** application. For more information about list of settings available for the **Infrastructure** application, see Prism Central Settings (Infrastructure) on page 22. **Note:** The Settings icon also appears in some entities page such as **Alerts** page to enable alert emails and specify the email addresses to which alerts should be sent. For more information, see Prism Central Alerts and Events Reference Guide. You can also access the **Prism Central Settings** page from the **Navigation Bar**.
	Add icon	The Add icon is used to add an entry in a list of allowed entries.
	Remove icon	The Remove icon is used to remove an entry from the list of allowed entries.
	Label icon	The Label icon is used to create a label for the selected entity items.
	Edit icon	The Edit icon is used to modify an existing entry.
	Delete icon	The Delete icon is used to delete an existing entry.
	Share icon	The Share icon is used to share the information with any Prism Central user.

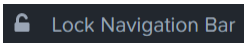
Icon	Name	Description
	Power icon	The Power icon is used to select the following VM power options in the VM console: • Power off • Power cycle • Reset • Guest shutdown • Guest reboot. For more information about the VM Power options, see Managing a VM through Prism Central (AHV) on page 134.
	Launch icon	The Launch icon is used to launch the VM console.
	Reboot icon	The Reboot icon is used to send a **Control-Alt-Delete** command to the VM console.
	Screenshot-capture icon	The Screenshot-capture icon is used to take the screenshot of the VM console display.
	Back icon	The Back icon is used to return to the previous page.

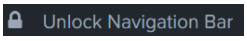
Navigation Bar

The **Navigation Bar** enables you to view and select the required configuration options for the selected application.

For information about the **Navigation Bar** applicable for a specific Prism Central application, see Application-specific Navigation Bar on page 57.

For information about the applications available in Prism Central and how to access any application, see Application Switcher Function on page 19.

You can select 

to lock and 

to unlock the **Navigation Bar**. It is a toggle. When the **Navigation Bar** is locked, it remains open all the time when you switch between multiple configurations on the Prism Central landing page.

Help Resources

The following table describes the help resources available when you select the help icon:

Table 3: Help Resources

Name	Description
Learn about search	Displays search guidelines. For more information, see Searching for Information on page 60.
Help with this page	Opens the online help that describes the current page. For more information, see Accessing Online Help (Prism Central) on page 580.

Name	Description
Online Documentation	Opens the online help at the introduction page. For more information, see Accessing Online Help (Prism Central) on page 580.
Support Portal	Opens a new browser tab (or window) at the Nutanix Support portal logon page. For more information, see Accessing the Nutanix Support Portal (Prism Central) on page 576.
Nutanix Next Community	Opens a new browser tab (or window) at the Nutanix Next Community entry page. For more information, see Accessing the Nutanix Next Community on page 582. The portal is an online community site for customers and partners to exchange ideas, tips, and information about Nutanix technologies and related data center topics.
Create Support Case	Opens the **Create a new support case** page to view or create support cases with Nutanix customer support. For more information, see Creating a Support Case on page 572.

Application Switcher

The application switcher enables you to select the relevant application to perform any task or operation. For more information, see Application Switcher Function on page 19.

User Menu (<user_name>)

The *<user_name>* indicates the user identity such as admin, nutanix, or any configured user identity who is logged into the Prism Central. It appears on the far right side of the Prism Central landing page.

For information about how to define the Prism Central users, see Controlling User Access (RBAC) information in *Security Guide*. Select *<user_name>* to display a list of options to update your user account, log off from Prism Central, and other miscellaneous tasks.

The following table describes the options available in the *<user_name>* dropdown menu.

Table 4: User Menu Options

Name	Description
Change Password	Opens the **Change Password** window to update your password. For more information, see Updating My Account in *Security Guide*.
Update Profile	Opens the **Update Profile** window to update your user name and email address. For more information, see Updating My Account in *Security Guide*.
Download Cmdlets Installer	Downloads the PowerShell installer for the Nutanix cmdlets. For information about installing the cmdlets locally and for cmdlet descriptions, For more information, see Powershell Cmdlets Reference.
Download nCLI	Downloads the Nutanix command-line interface (nCLI) as a zip file to your local system. The download occurs immediately without additional prompts after you select this option. For more information about installing the nCLI locally and for nCLI command descriptions, see Command Reference.
REST API Explorer	Opens a new browser tab (or window) at the Nutanix REST API Explorer web page. For more information, see Accessing the REST API Explorer on page 579.

Name	Description
About Nutanix	Opens the **About Nutanix** window that displays Nutanix operating system (AOS) and other version information. For more information, see Finding the Prism Central Version on page 557.
Nothing To Do?	Opens a game that is strictly for entertainment. To quit the game, select "X" at the upper right of the screen.
Sign Out	Logs you out of Prism Central. For more information, see Logging Out of Prism Central on page 570.
Adjust Contrast (Chrome only)	Displays a contrast setting box at the bottom of the screen where you can set the Prism Central display to **Normal** (default) or **High** contrast. **Note:** This option is available only when you access Prism Central using the Chrome browser.

Application Switcher Function

The Application Switcher function facilitates you to seamlessly switch between following configuration module applications:

- **Platform Services** module applications that include:
  - **Admin Center** - Select this to perform admin-related tasks, activities, and configurations. For information about the administrative tasks that you can perform using **Admin Center**, see Admin Center Overview on page 26.
  - **Apps and Marketplace** - Select this to directly access the application deployment and application management functionalities in Admin Center. For more information about the application types and deployment, see the Marketplace information in *Prism Central Admin Center Guide*. For more information about application management, see the My Apps information in *Prism Central Admin Center Guide*.

    Note: When you select **Apps and Marketplace** from the application switcher, the system redirects you to the **Admin Center** application with display of **Marketplace** menu.
- **Cloud Infrastructure** module applications that include:
  - **Infrastructure**. This document covers the complete information about **Infrastructure** application.
  - **Kubernetes Management** *(formerly called Karbon)*- Provides simplified provisioning and operations of Kubernetes clusters. Kubernetes is an open source container orchestration system for deploying and managing container-based applications. For more information, see Nutanix Kubernetes Engine documentation.
  - **Foundation Central** - Enables you to create clusters from factory-imaged nodes and re-image existing nodes that are already registered with Foundation Central, remotely from Prism Central. For more information, see Foundation Central Documentation.
- **Cloud Manager** module applications that include:
  - **Intelligent Operations** *(formerly called Prism Pro/Ultimate)*- Optimizes capacity, proactively detects performance anomalies, and automates operations tasks with ease and confidence. For more information, see Intelligent Operations Guide.
  - **NCM Self-Service** *(formerly called Calm)*- Allows you to seamlessly select, provision, and manage your business applications across your infrastructure for both the private and public clouds. Calm

provides application automation, Life Cycle Management (LCM), monitoring, and remediation to manage the heterogeneous infrastructure, for example, VMs or bare-metal servers.. For more information, see Self-Service documentation.

  - **Cost Governance***(formerly called Beam)*- Allows you to cost govern your resources using our pre-buit TCO model to govern the spending of business units or cost centers. For more information, see Cost Governance documentation
  - **Security Central***(formerly called Flow Security Central)*- A cloud based offering that provides complete visibility into the security posture and compliance of your multi-cloud environment (Nutanix, Azure and AWS). For more information, see Security Central documents.

- **Unified Storage** module applications that include:
  - **Files** - A software-defined, scale-out file storage solution that lets you share files in a centralized and protected location to eliminate the requirement of a third-party file server. For more information, see Files documentation.
  - **Objects** - A software-defined Object Store Service that is designed with an Amazon Web Services Simple Storage Service (AWS S3) compatible REST API interface capable of handling petabytes of unstructured and machine-generated data. Objects addresses storage-related use cases for backup, and long-term retention and data storage for your cloud-native applications by using standard S3 APIs. For more information, see Objects documentation.
- **Database Services** module that include:
  - **Move** - A cross-hypervisor mobility solution to move VMs with minimal downtime. For more information, see Move User Guide.
  - **Database Service** - The Nutanix Database Service (NDB) automates and simplifies database administration, bringing one-click simplicity and invisible operations to database provisioning and life-cycle management. It also enables you to perform operations such as database registration, provisioning, cloning, patching, and restore. It allows administrators to define provisioning standards with end-state driven functionality that includes network segmentation and high availability (HA) database deployments. For more information, see Nutanix Database Service User Guide.

Note:

- In a new deployment of Prism Central, the Application Switcher displays the **Admin Center**, **Infrastructure**, **Apps and Marketplace**, **Cost Governance**, and **Security Central** applications for users with the Nutanix admin role. You can view the Nutanix Apps in the Application Switcher after you enable them from the Marketplace.

  For information about how to deploy apps from Prism Central, see Nutanix Apps Deployment information in *Prism Central Admin Center Guide*.
- If you have upgraded to the current version of Prism Central, you can view all Nutanix Apps that you enabled in the previous version along with the **Admin Center**, **Infrastructure**, **Apps and Marketplace**, **Cost Governance**, and **Security Central** applications.
- For users with the non-admin role, the Application Switcher displays the applications based on the access policies. For example, a user with a system-defined consumer role can view only **Infrastructure**, **Apps and Marketplace**, and any other Nutanix Apps for which the access is provided to the user.
- You cannot add any custom applications to the Application Switcher.

Select the relevant application option to perform the configurations required at your site. The following is an example displaying the application options available through the Application Switcher function of Prism Central:

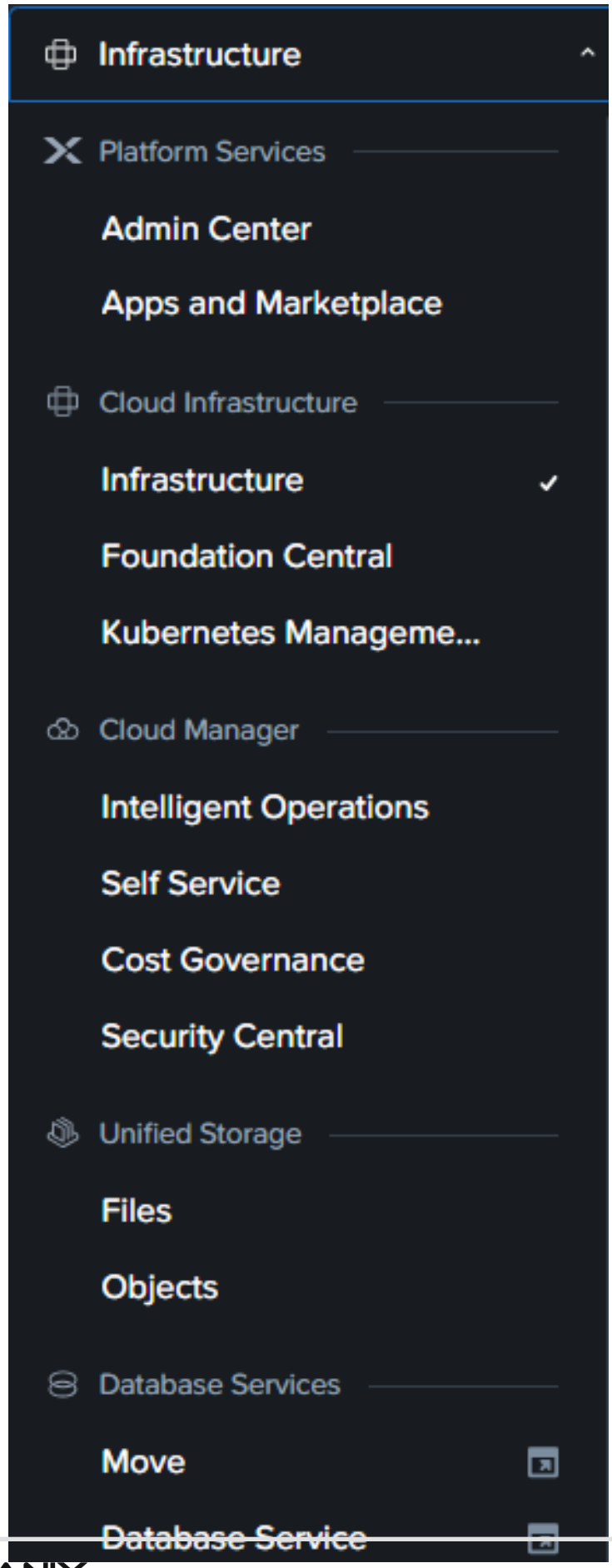


Figure 3: Application Switcher Options

Prism Central Settings (Infrastructure)

The **Settings** page of the **Infrastructure** application enables you to configure the **Prism Central Settings** for infrastructure-specific services. You can access the **Settings** page using any of the following mechanisms:

- Click the Settings icon on the Prism Central Landing page. For information about Prism Central landing page, see Prism Central Landing Page on page 14.
- Navigate to **Prism Central Settings** from the **Navigation Bar** of **Infrastructure** application. For more information about the **Navigation Bar** of Prism Central applications, see Application-specific Navigation Bar on page 57).

The **Settings** page displays a list of tasks that you can perform for the **Infrastructure** application. Click the required task to open the window or page for that task.

The following is an example displaying the tasks available under **Settings** page:

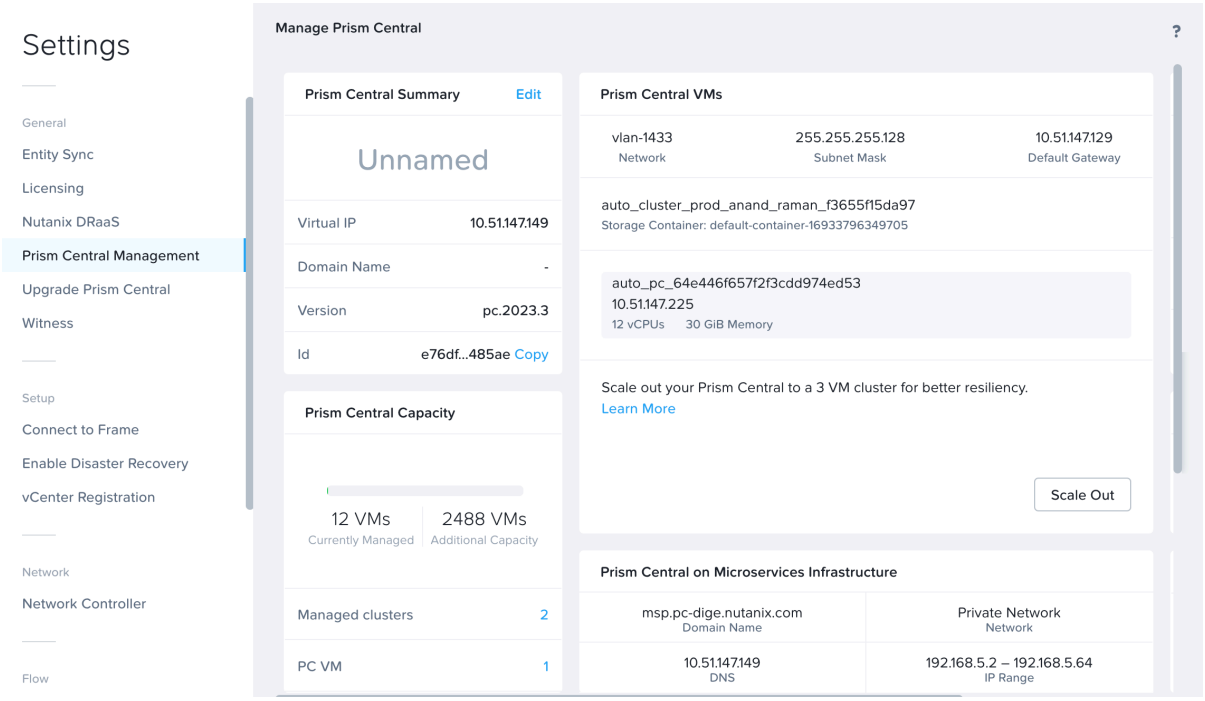


Figure 4: Settings Page - Infrastructure

The following table provides the information about all the tasks available on **Settings** page:

Table 5: Settings Page Tasks - Infrastructure

Task Category	Task Name	Description
General	Entity Sync	Opens the **Force Entity Sync** page, which synchronizes entities with the specified availability zones. For more information, see Nutanix Disaster Recovery Guide.

Task Category	Task Name	Description
	Licensing	Redirects to the **Licensing** page available under **Admin Center** application settings. For more information about how to access the Licensing page from Admin Center application, see Prism Central Admin Center Guide.
	Nutanix DRaaS	Opens the **Nutanix DRaaS** page to connect to DRaaS domain. For more information, see Nutanix Disaster Recovery Guide.
	Prism Central Management	Opens the **Manage Prism Central** page for viewing information about Prism Central and optionally expanding (scale out) Prism Central across multiple VMs. For more information, Managing Prism Central on page 531).
	Upgrade Prism Central	Opens the **Upgrade Prism Central** page to upgrade the Prism Central VM to a newer version. For more information, see Prism Central Installation or Upgrade on page 32.
	Witness	Opens the **Witness** page. The witness service continuously monitors nodes and clusters to provide an automatic mechanism to handle any system failure. For more information about how to configure **Witness** service, see Configuring a Witness (Two-node Cluster) information in *Data Protection and Recovery with Prism Element* guide.
Setup	Enable Nutanix Disaster Recovery	Opens the **Enable Nutanix Disaster Recovery** page to enable the Disaster Recovery as a Service (DRaaS) capability. For more information, see Nutanix Disaster Recovery Guide.
	Self-Service Admin Management	Opens the **Self-Service Admin Management** page available under **Identity and Access Management** > **Settings** of **Admin Center** application. For information about how to access the **Admin Center** application in Prism Central, see Application Switcher Function on page 19. For information about the **Admin Center** application in Prism Central, see Admin Center Overview on page 26.
	vCenter Registration	Opens the **vCenter Registration** window to register (or unregister) clusters with vCenter. For more information, see External vCenter Server Integration on page 326.
Network	Advanced Networking	Opens the **Advanced Networking** page to enable the advanced networking for all On-Prem AHV Clusters in the Prism Central that runs AOS 6.1 or above acropolis version.
Flow	ID Based Security	Opens the **ID Based Security** page to add Active Directory domain services configurations and to import user groups for identity-based security policies. For more information, see Flow Microsegmentation Guide.

Task Category	Task Name	Description
	Microsegmentation	Opens the **Microsegmentation** page to enable this feature, which is disabled by default. Before you can configure and use application security policies, isolation environment policies, and quarantine policies, you must enable the feature. For more information, see Flow Microsegmentation Guide.
User and Roles	Authentication	For information about User and Roles, see Security Guide.
	Local User Management	
	Role Mapping	
More Settings	For information about the settings available under **More Settings**, see Prism Central Admin Center Guide.	

Understanding Displayed Statistics

The Prism web console and Prism Central displays various statistics that are derived from the following sources:

> **Note:** Most displayed statistics appear in 30 second intervals. The values in the tables represent the most recent data point within the last 30 seconds. Prism Central collects the statistical data from each registered cluster, so the process of collecting that data could result in a longer lag time for some statistics displayed in Prism Central.

1. *Hypervisor*: Hypervisor provides usage statistics only. The support to provide usage statistics is available only in ESXi, and not in Hyper-V and AHV hypervisors. If the cluster consists of Hyper-V or AHV hypervisor, the controller provides the usage statistics.

   > **Note:** Ensure that you consider the usage statistics reported from ESXi hypervisor in both Prism Central and Prism Element, only when it matches with the usage statistics in vCenter.

2. *Controller (Stargate)*: When hypervisor statistics are unavailable or inappropriate, the Controller VM (CVM) provides the statistics from Stargate. For more information about Stargate, see Nutanix Bible. The Controller-reported statistics might differ from those reported by the hypervisor for the following reasons:

   - An NFS client might break up large I/O requests into smaller I/O units before issuing them to the NFS server, thus increasing the number of operations reported by the controller.
   - The hypervisor might read I/O operations from the cache in the hypervisor which are not counted by the controller.

3. *Disk (Stargate)*: Stargate can provide statistics from both controller and disk perspective. The controller perspective includes reading both I/O operations from memory and disk I/O operations, but the disk perspective includes only disk I/O operations.

   > **Note:** The difference in statistics derived from the sources: Hypervisor, Controller, and Disk, only applies to storage-related statistics such as IOPS, latency, and bandwidth.

The following field naming conventions are used in Prism Central to identify the information source:

- A field name with **Controller** word indicates the statistic is derived from the controller (for example *Controller IOPS*).
- A field name with **Disk** word indicates the statistic is derived from the disk (for example *Disk IOPS*).

- A field name without **Controller** or **Disk** word indicates the statistic is derived from the hypervisor. For example **IOPS**.

For VM statistics in a mixed ESXi/AHV cluster, the statistics source depends on the type of hypervisor that hosts the VM. If the Hypervisor is:

- ESXi - The hypervisor is the source for statistics.
- AHV - The controller is the source for statistics.

> **Note:**
>
> - The overview, VM, and storage statistics are derived from either the hypervisor or controller.
> - Hardware statistics are derived from disk.
> - Metrics in the analysis page are derived from any of the sources: hypervisor, controller, or disk, based on the type of metric.

The following table provides the information about the source for various statistics based on hypervisor type:

Table 6: Source for Displayed Statistics

Hypervisor Type	Statistics	Source	Analysis
ESXi	Overview, VM, and Storage	Both Hypervisor and controller	Metric dependent
		Controller for some storage statistics only	
	Hardware	Disk	
Hyper-V	Overview, VM, and Storage	Controller	
	Hardware	Disk	
AHV	Overview, VM, and Storage	Controller	
	Hardware	Disk	
Citrix Hypervisor	Overview, VM, and Storage	Controller	
	Hardware	Disk	
Mixed (ESXi + AHV)	Overview, VM, and Storage	Hypervisor	
	Hardware	Disk	

Infrastructure Overview

The **Infrastructure** application of Application Switcher Function on page 19 enables you to configure the field-specific settings required to host a cluster in Prism Central. It involves the following configurations:

- Customizable main dashboard that displays summary information across the registered clusters (see Main Dashboard - Infrastructure on page 71).

- Dashboard and configuration options to manage VMs, VM templates, OVA, image placement, catalog items, storage, volume groups, Nutanix Guest Tools (NGT), and vCenter server across the registered clusters (Compute and Storage Entities on page 94).
- Dashboard and configuration options to manage subnets, network connections, Virtual Private Clouds (VPC), floating IPs, Virtual Private Network (VPN) connections, and security policies across the registered clusters (Network and Security Entities on page 341).
- Dashboard and configuration options to manage protection policies, recovery plans, VM recovery points, VG recovery points, and consistency groups (see Data Protection and Recovery Entities on page 396).
- Hardware component dashboards with drill-down options to view detailed information about individual clusters, hosts, disks, and GPUs across the registered clusters (see Hardware Entities on page 397).
- Activity monitors for alerts and events (see Activity Entities – Alert and Event Monitoring on page 447).
- Activity monitors for audits and tasks (see Activity Entities – Tasks and Audits on page 448).
- Dashboards to manage categories and availability zones (see Administration Entities on page 454).
- Settings menu from which you can configure Prism Central functions (see Prism Central Settings (Infrastructure) on page 22).

The **Infrastructure** application also provides the following additional functionalities for cluster and field-specific health checks:

- Fault Management based on Alerts and Events Customization. For more information on Alerts and Events, see Prism Central Alerts and Events Reference Guide.
- Detailed information about the cluster health.

> **Note:** The **Services** menu available in the earlier Prism Central versions is now retired. You can use the Application Switcher Function on page 19 to access Nutanix applications and services.

Admin Center Overview

The **Admin Center** application enables you to perform the following administrative-level tasks in Prism Central:

- Enable Marketplace in Prism Central. For more information, see Enabling Marketplace information in *Prism Central Admin Center Guide*.
- Enable Prism Intelligent Operations. For more information, *Enabling Prism Intelligent Operations* in Intelligent Operations Guide.
- Discover and deploy Nutanix apps such as NCM Self-Service (formerly known as Calm), *Files*, *Move*, *Objects*, *Database Service*, *Foundation Central*, and *Kubernetes Management*.
- Discover and deploy preferred partner apps from the Marketplace.
- Discover and deploy preconfigured and custom apps (Other Apps) when NCM Self-Service (formerly known as Calm) is deployed and licensed in the Prism Central instance.
- Manage all deployed apps from a common workspace.
- Define multiple projects as per the field requirements.
- Manage Nutanix applications License.

- Define users, roles, and set up authentication mechanism for Identify and Access Management (IAM).

  Note: Prism Central provides the Self Service feature that allows you to create projects where the consumers of the IT infrastructure can provision and manage VMs in a self-service manner, without engagement of IT in day-to-day operations. The consumers of the IT infrastructure within an enterprise include individual users, development teams, test teams, and DevOps teams. Only a Prism Central administrator can create a self-service administrator role.

  For information about the roles and functions for Prism Central Self Service, see Prism Self Service Setup on page 519.

- Perform inventory and software updates as part of the Life Cycle Manager (LCM) functionality.
- Set welcome banner, language, default landing page, and other UI settings for Prism Central.
- Security management using Cluster Lockdown and SSL Certificate mechanisms.
- Define email aliases, SMTP server, and Syslog server to receive alerts and notification from Prism Central.
- Define network management guidelines for Prism Central using HTTP Proxy, Name server, NTP server, and SNMP settings.

For more information about **Admin Center**, see Prism Central Admin Center Guide.

Prism Central GUI Organization

This section provides the information about the GUI-related functionalities of Prism Central, how the Prism Central GUI is organized, and how to perform GUI-specific operations in Prism Central.

Entity Layout

In Prism Central GUI, you can access the entities from the **Navigation Bar** using the Navigation icon. For information about the **Navigation Bar**, see Prism Central Landing Page on page 14.

The entities are categorised into the following types:

- Compute and Storage Entities on page 94
- Network and Security Entities on page 341
- Data Protection and Recovery Entities on page 396
- Hardware Entities on page 397
- Activity Entities – Alert and Event Monitoring on page 447
- Activity Entities – Tasks and Audits on page 448
- Operations Entities on page 453
- Administration Entities on page 454

  Note: The **Services** menu available in the earlier Prism Central versions is now retired. You can use the Application Switcher Function on page 19 to access Nutanix applications and services.

When a list appears for the selected entity, the display may include:

- Entity tabs, **Actions** options (if any), **Group by** options, and **View by** options for the list, and a **Modify Filters** option on the far right. When you click **Modify Filters** option, the **Filters** pane appears.
- A query field that identifies the filters (if any) being applied to the list. This field displays all filter options that are currently in use. It also allows for basic filtering on the entity name.

- A table (list) of entities. The table content is determined based on the **Group by**, **View by**, and **Modify Filters** options.

  > **Note:** By default, the system displays 20 rows of entity items per page. The system also provides you an option to configure the display with a different number of rows per page between 10 to 60. To specify a different number for rows per page, click *X* **Rows**, where x indicates the number such as 10, 20, 30, 40, 50, and 60.

- An export mechanism to download the table contents in CSV format with a maximum of 1000 rows. Click **Export** to download the table contents on your local machine.

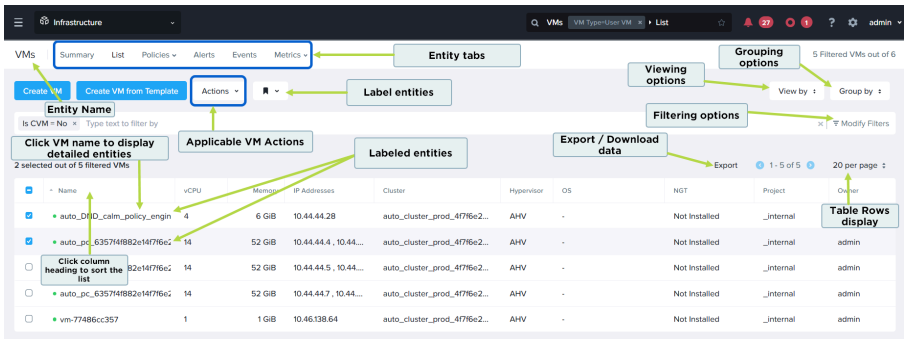


Figure 5: Entity Layout (example)

Entity Tabs

Each entity provides relevant tabs such as **Summary, List, Policies, Alerts, Events, Audit, Metrics, Scenarios, Gateway, VPN connections, Subnet Extensions,** and **BGP Sessions**, to perform entity-related configurations and observe entity related-activities.

> **Note:** For some entities, no tab appears and the relevant content appears directly in the main page of the selected entity.

Sort Function

The sort function allows you to sort the entries in alphabetic or ascending-descending order. This function appears for the Tiles and Circles views only; ordering in the Grid (tabular) view is accomplished when you click a column header.

Filters Pane

Click **Modify Filters** option to display the **Filters** pane.

The **Filters** pane include a set of fields that vary according to the selected entity. When you type the desired field values in the **Filters** pane, an entry appears in the search field for each value you enter.

> **Note:**
>
> - You can bookmark (or save) a filter using the Bookmark icon in the search field. The selected filter is saved under **Bookmarks**. To remove the bookmarked filter, navigate to **Bookmarks** from the **Navigation Bar**, and click the Bookmark icon for the saved filter.
> - Numeric filters have **To/From** fields to specify a range. You can specify the numeric values along with units in these fields. For example, the filter adjusts the scale accordingly when you type in "10 K" or "100 M".

To apply a filter, enter a value or select the checkbox of the desired value (or multiple values) for the field you want to use as a filter . You can apply filters across multiple parameters. Some parameter filters require additional context such as a constraint string or a range.

The following is an example displaying the **Filters** pane:

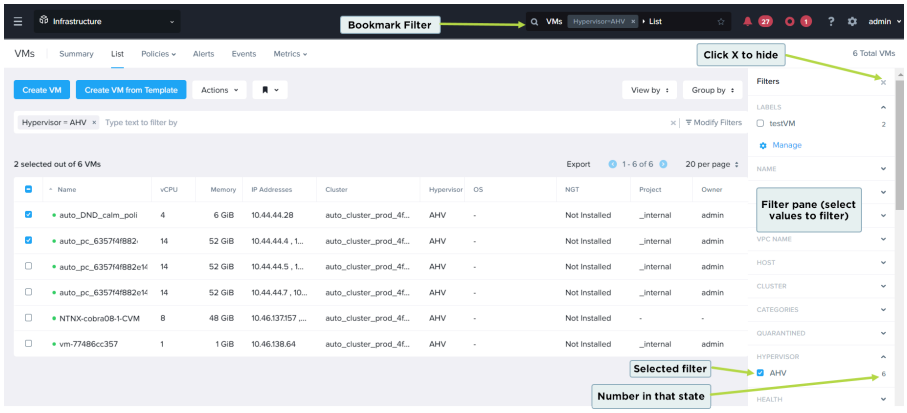


Figure 6: Filters Pane

Group by

The **Group by** option enables you to organize the entity information based on attributes such as Cluster, Hypervisor, Power State, vCPU, Health, Type, Name, and so on. The **Group by** options vary based on the selected entity.

View by

The **View by** option enables you to specify the following view types for the displayed information:

- **General** - Displays a set of general information parameters.
- **Performance**- Displays a set of performance-specific parameters.
- **Anomalous Behavior** - Displays the Anomalous behavior. For example, Anomaly count of the VMs.
- **Efficiency** - Displays a set of efficiency-related parameters. **Efficiency** is determined through the VM behavioral learning engine. For more information, see Behavioral Learning Tools information in *Intelligent Operations Guide*.
- **GPU** - Displays a set of GPU-specific parameters.
- **Data Protection** - Displays a set of data protection-related parameters.
- **Storage Configuration** - Displays a set of storage configuration-related parameters.

> **Note:** The **General** view type is available for all entities, but the other options are available only if it is applicable for an entity.

In addition to the pre-defined view types, you can also create one or more custom view types.

To create a custom view type:

1. Click the **View by** option and select **+ Add custom**.

2. In the **<entity> Columns** window that is displayed, perform the following actions:
   1. Enter a name for the custom view type in the first (top) field.
   2. Click the Add icon in the left column for each entity property to be included in the custom view type. The selected entity property appears in the right column.

      Note:

      - By default, the **Name** column is already selected.
      - A maximum of 10 entity properties are allowed in a custom **View by** option including the **Name** column.
      - To arrange the order of the selected columns, hover on the column name and click the up or down arrow as appropriate.
      - To search and filter the required entity property from the list, enter the string in the Search field above the left column.
      - To remove an entity property from the custom **View by** option, click the Remove icon associated with the entity property.

   3. Click **Save** after the entity-property list in the right column is finalized.

   The following following is an example displaying the **VM Columns** window:

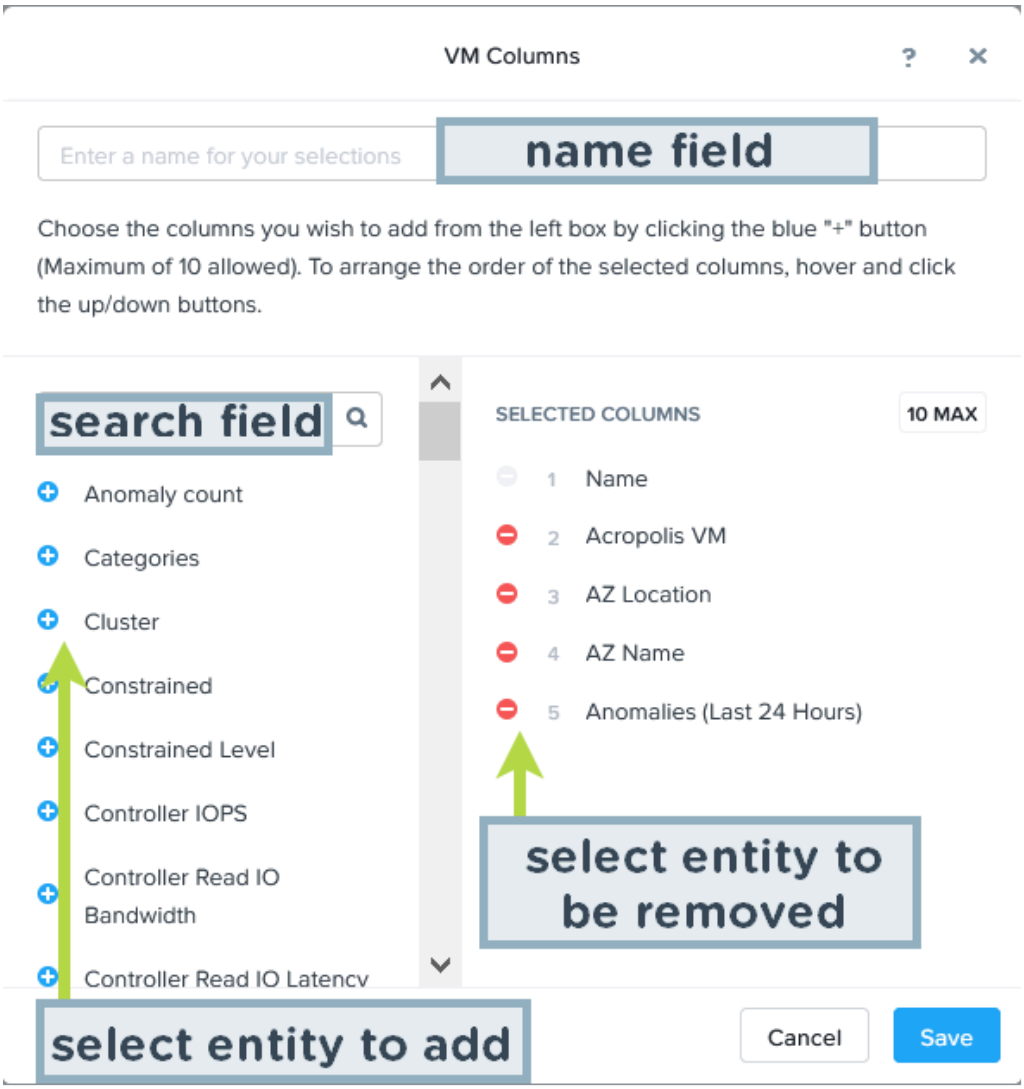


Figure 7: VM Column Window (example)

The custom view type appears (by name) in the available view types under **View By** option.

> **Note:** The custom view type appears only for the user who created it, and the administrative user and other users cannot view it.

Actions Dropdown Menu

The **Summary** page provides options to administer and categorize the entity items. The **Actions** dropdown menu is available for the selected entities in Prism Central. You can select an entity item, a set of entity items, or all entity items using the relevant checkbox available in the table list on **Summary** page. You can clear the relevant checkbox to clear a selected item from the table list.

You can also perform some administrative tasks for a cluster through Prism Element. For information about the tasks to be performed from Prism Element, see the Prism Element Web Console Guide.

> **Note:** The **Actions** dropdown list does not appear if there are no relevant actions available for the selected entity type.

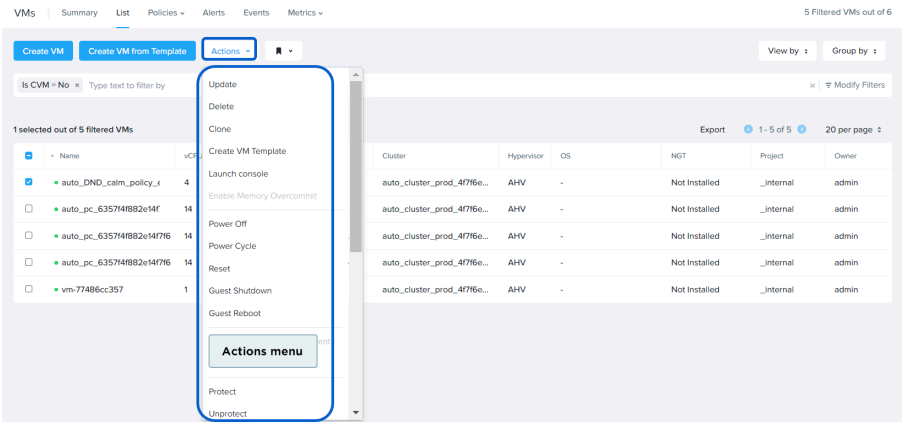


Figure 8: Action Dropdown Menu

Label

Labels enable you to create custom groupings for the entities. To add a label, click the Label icon, and enter the label name in the field. The label is applied to all the selected entity items in the table list.

Note:

- Only super admin and Prism admin roles have permissions to perform this operation.
- Labels are available for VMs and clusters only.

Export

The **Export** option enables you to download the table, that contains the entity items list to a file. Click the **Export** option available on an entity item.

Entity-Related Observation Activities

The entity-related observation activities involve the following fault and performance related statistics:

- Alarms - For information on all the alarms generated in Prism Central, see Activity Entities – Alert and Event Monitoring on page 447.
- Events - For information on all the events generated in Prism Central, see Activity Entities – Alert and Event Monitoring on page 447.
- Tasks - For information on how to observe a task and its statistics in Prism Central, see Activity Entities – Tasks and Audits on page 448.
- Audits - For information on an audit activity in Prism Central, see Activity Entities – Tasks and Audits on page 448.

Prism Central Installation or Upgrade

A Prism Central instance consists of either a single VM or as a three-VM scale-out architecture that functions as a multi-cluster monitoring and control interface. For information about the maximum tested and supported values for entities in Prism Central, see Nutanix Configuration Maximums.

Note:

- For more information on supported methods for Prism Central installation and upgrade, see Prism Central Upgrade Requirements on page 34.

- Nutanix does not support Prism Central and its managed clusters in NAT-deployed environments.

- To install or upgrade a Prism Central instance, see Prism Central Upgrade Methods on page 33.

  Note: Do not add any additional vDisks or NICs to a Prism Central VM other than what is specified in the installation or upgrade instructions.

  See Prism Central Upgrade vDisk on page 37 for information about the dedicated Prism Central upgrade vdisk that the Prism Central upgrade process deploys and uses for upgrade operations.

- To scale out an existing single VM Prism Central to multiple VMs, see Expanding (Scale Out) Prism Central on page 559.
- To upgrade one or more managed clusters through Prism Central, see Prism Central-Managed Clusters Upgrade on page 39.
- If you use a proxy server, see Prism Central Configuration When a Cluster Uses Proxy Servers information in *Prism Central Admin Center Guide*.

Prism Central Installation

A Prism Central instance consists of either a single VM or a set of VMs that functions as a multi-cluster monitoring and control interface.

You can Install a Prism Central VM using the 1-click method for both connected sites (with internet connectivity) and dark sites (without internet connectivity). For more information, see Installing Prism Central section in *Prism Web Console Guide*. This method employs the Prism Element web console from a cluster of your choice and creates the Prism Central VM in that cluster.

Prism Central Upgrade Methods

You can upgrade a Prism Central instance using the following methods:

- Upgrade directly from Prism Central web console.

  To upgrade directly from Prism Central, perform the following steps:

  1. Log in to Prism Central.
  2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Upgrade Prism Central** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
  3. Perform the steps as described in Upgrading Prism Central on page 38 section.

- Upgrade from Life Cycle Manager (LCM) tool.

  To upgrade Prism Central from LCM, perform the following steps:

  1. Log in to Prism Central.
  2. Select the **Admin Center** application from Application Switcher Function, and navigate to **LCM** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
  3. Choose either of the following upgrade methods based on the LCM connectivity status with the site:

     - *Upgrade Prism Central from LCM with Connected site* - Perform the actions as described in Performing Firmware and Software Updates in a Connected Site Setup section of *Life Cycle Manager Guide*.
     - *Upgrade Prism Central from LCM with Dark site using a web server* - Perform the actions as described in Performing Firmware and Software Updates in a Dark Site Setup section of *Life Cycle Manager Guide*.
     - *Upgrade Prism Central from LCM with Dark site using Direct Upload* - Starting with LCM 3.0, Prism Central also supports the **Direct Upload** functionality. A minimum supported version of pc.2024.1 is required to use the Direct Upload functionality on Prism Central. Perform the actions as described in Performing Firmware and Software Updates in a Dark Site Setup section of *Life Cycle Manager Guide*.

Prism Central Upgrade Requirements

- When using the 1-click method for installing Prism Central, you select from a set of preconfigured Prism Central VM sizes. The *Prism Central Scalability* section in the Prism Central Release Notes provides Prism Central VM resource and capacity specifications for the preconfigured sizes. In addition, certain optional features that you can enable such as application discovery and Self-Service (formerly Calm) require additional Prism Central VM resources (more memory and vCPUs). After installing Prism Central, you may need to increase the VM resources before enabling one or more of these optional features. The requirements for various feature combinations are listed in KB 8932.
- Ensure that all the requirements provided in Microservices Infrastructure Prerequisites and Considerations on page 535 are fulfilled for Microservices Infrastructure deployment.
- When upgrading Prism Central and AOS, upgrade Prism Central first, then upgrade AOS on the clusters managed by Prism Central. See Acropolis Upgrade Paths on the Nutanix Support portal to check the upgrade path from your current version to your target version for AOS and Prism Central.
- Nutanix does not support Prism Central and its managed clusters in NAT-deployed environments.
- Do not use the AOS binary and metadata .json files to upgrade your existing Prism Central deployment.

  Prism Central requires the use of specific Prism Central binary and metadata .json for upgrades and deployments. Using AOS files to upgrade Prism Central from any version is not supported and can result in Prism Central unavailability.

  Do not use the Prism Central AHV / ESXi / Hyper-V components on the Nutanix support portal to upgrade an existing Prism Central instance.

- You can install Prism Central in either a Nutanix cluster or a non-Nutanix environment. The following table describes the supported methods for Prism Central installation and upgrade:

Table 7: Prism Central Installation and Upgrade - Supported Methods

Environment Type	Hypervisor	Prism Central Upgrade using Upgrade Prism Central option	Prism Central Install		
			1-Click Internet with Prism Element	1-Click Internet with Prism Element	Manual installation using binaries
Nutanix (Nutanix AOS cluster) Non-Nutanix	AHV ESXi Hyper-V ESXi Hyper-V	Supported for all versions except Prism Central 2022.9	Supported for all versions except Prism Central 2022.9 Not applicable	Supported for all versions except Prism Central 2022.9 Not applicable	Not supported for Prism Central versions 2022.9, 2023.1.0.1, 2023.3, and 2023.4. **Note:** For information about installing or upgrading to Prism Central pc.2024.1 and later releases on a three-tier cluster, see Prism Central Installation or Upgrade in Non-Nutanix ESXi Environment on page 41.

However, there are some limitations when installing in a non-Nutanix environment: the 1-click method is not available, a 1-VM instance is the only option (multi-VM instances are not supported), the hypervisor must be ESXi, and some Prism Central features are not available such as Self-Service (formerly Calm) and Flow support. Additionally, the Prism Central VM supports certain software features and add-ons,

such as Nutanix Kubernetes Environment (formerly Karbon), only in a Nutanix environment. For specific requirements, see the release notes and guides for your planned or installed software components.

- To help ensure that Prism Central and each managed cluster are taking advantage of NCC features, ensure that:
  - Each node in your cluster is running the same NCC version.
  - Prism Central and each cluster managed by Prism Central are all running the same NCC version.

Before you can install Prism Central by using the 1-click method, expand Prism Central, or add a Prism Central VM, ensure you meet the following requirements:

- The specified gateway must be reachable.
- Ensure the port TCP port 2100 is open from the Prism Element cluster to the Prism Central VM IP address.
- Ensure network connectivity between the VM VLAN and portgroup of the Prism Element cluster Controller VM and the Prism Central VM VLAN and portgroup.
- No duplicate IP addresses can be used.
- The storage container used for deployment is mounted on all hypervisor hosts.
- When installing on an ESXi cluster:
  - vCenter and the ESXi cluster must be configured properly. For more information, see the vSphere Administration Guide for Acropolis.
  - vCenter must be registered in Prism.
  - DRS must be enabled in vCenter.
  - vCenter is up and reachable during the deployment.

Prism Central Upgrade Limitations

Consider the following limitations for Prism Central upgrade:

- Prism Central 2022.9 and later support maximum 200 clusters. Previous versions of Prism Central supported up to 400 clusters. A pre-upgrade check prevents upgrade attempts for existing deployments supporting more than 200 clusters. Nutanix recommends that you maintain your current Prism Central deployment at version 2022.6.x. For more information, see KB-13272.
- Prism Central 2022.9 and later versions are supported only on Prism Central instances hosted on Nutanix AOS clusters running the AHV or ESXi hypervisors. Prism Central instances hosted on Nutanix AOS clusters running Hyper-V or hosted on non-Nutanix infrastructure must not upgrade above 2022.6.x.
- If Prism Central is not registered with the AOS cluster hosting it, refer to KB-10596 for additional requirements before upgrading.
- Prism Central 2022.9 and later versions no longer support PCDRv1 (CLI-based PCDR). A pre-upgrade check blocks upgrade to Prism Central 2022.9 or later versions if a PCDRv1 setup is detected. Nutanix recommends removing the PCDRv1 configuration before upgrade and enabling PCDRv2 post-upgrade. Refer to KB-13875 and KB 9599 for further details.
- A pre-upgrade check blocks upgrade to Prism Central 2022.9 or later versions if a PCDRv2 setup (GUI-based PCDR) is detected. Nutanix recommends removing the PCDRv2 configuration, upgrading to Prism Central 2022.9 or later versions, and then re-configuring PCDRv2 once all requirements are met. Refer to KB 13666 and KB 9599 for further details.

- If a single-node Prism Central VM is upgraded to Prism Central 2022.9 or later versions, but the underlying Prism Element (PE) is not running AOS 6.6, a pre-check will prevent the scaling out of Prism Central VM from 1-node to 3-node Prism Central.
- Prism Central versions where one-click upgrade is not enabled must use the legacy one-click upgrade method available on Prism Element as the LCM bundle is not available on the portal for download. For more information, see Use Upgrade Software in the Prism Element Web Console (Legacy 1-Click Upgrade).

Prism Central Upgrade vDisk

Each Prism Central VM includes a `/home` disk partition that is used for storage during upgrade process. The Prism Central upgrade process can fail if the available disk space in this partition is near capacity.

For Nutanix clusters, the upgrade process uses a separate, dedicated vDisk of 30 GB capacity instead of the `/home` partition. Prism Central uses this dedicated vDisk to store the downloaded Prism Central software bundle, decompressing the bundle, and hosting the installer.

When you upgrade Prism Central version to the current version, the Prism Central upgrade process uses the vDisk image in the bundle to create the Prism Central upgrade vDisk. The upgrade process uses this vDisk for the upgrade operations that include any subsequent upgrade.

> **Note:** For non-Nutanix deployments, the Prism Central upgrade vDisk is not supported during Prism Central deployment. For more details, see the Prism Central Release Notes.

Requirements

- Ensure that the Prism Central instance is registered to a host in the cluster or microservices infrastructure is enabled on the Prism Central instance.
- Ensure that the Prism Element cluster hosting Prism Central is registered to this Prism Central instance.
- Ensure that the Prism Element cluster hosting Prism Central has sufficient disk resources to provide the 30 GB vDisk.

Running NCC (Prism Central)

About this task

Before doing any upgrade procedure, log on to the Prism Central VM and run the NCC checks from the ncc command line. You cannot run NCC from the Prism Central web console.

Procedure

1. Log in to the Prism Central VM through a secure shell session (SSH).
   - For single-VM deployments, use the Prism Central IP address.
   - For scale-out three-VM deployments, use the virtual IP address. If you did not configure a virtual IP address, use the Prism Central IP address of any of the Prism Central VMs.
   - If you do not know the PC VM IP address, contact your cluster administrator.
2. Run NCC.

   ```
   nutanix@pcvm$ ncc health_checks run_all
   ```

   If the check reports a status other than INFO or PASS, resolve the reported issues before proceeding. If you are unable to resolve the issues, contact Nutanix Support for assistance.

Upgrading Prism Central

About this task

This section describes how to upgrade Prism Central using the one-click **Upgrade Prism Central** method.

Before you begin

Ensure that you meet the following prerequisites before you upgrade Prism Central:

- See Prism Central Upgrade Limitations on page 36 and Prism Central Upgrade Requirements on page 34.
- See the Prism Central Release Notes for resource requirements and capacity specifications for the Prism Central VM.
- If you have enabled Objects in the Prism Central managing the cluster, ensure that the Objects VMs are healthy and running when Prism Central upgrade process enables Microservices Infrastructure or you manually enable Microservices Infrastructure.

  Caution: If the Objects VMs are not healthy and running, the task for enabling Microservices Infrastructure might fail. For information on how to start the Objects VMs, see Starting the Objects VMs in the *Objects User Guide*.

Procedure

1. Before performing any upgrade procedure, make sure that you are running the latest version of the Nutanix Cluster Check (NCC) health checks and upgrade NCC if necessary.
2. Run NCC as described in Running NCC (Prism Central) on page 37.
3. Log in to Prism Central through a web browser.
4. Select the **Infrastructure** application from Application Switcher Function, and click the Settings icon or navigate to **Prism Central Setting** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
   The system displays the **Settings** page.
5. Click **Upgrade Prism Central**, and perform the following steps to download and automatically install the Prism Central upgrade files.
   a. Do one of the following:
      » If you previously selected **Enable Automatic Download** and the software has been downloaded, click **Upgrade**, then click **Yes** to confirm.
      » If **Enable Automatic Download** is cleared, click **Download** to check if there is software available. When the download task is completed, click **Upgrade**, then click **Yes** to confirm.
   b. [Optional] To run the pre-upgrade installation checks only without upgrading, click **Upgrade** > **Pre-upgrade**. These checks also run as part of the upgrade procedure.
   The **Upgrade Software** dialog box shows the progress of your selection. When the upgrade process is complete, the Prism Central VM restarts. Wait a few minutes and log on again, as Prism Central might lose connectivity during the upgrade process.

   Note: If you are upgrading an older version of a Prism Central "large" VM that contains just a single vDisk, the upgrade process might add three new vDisks. This allows Prism Central to shard Cassandra metadata to improve performance. While the listed disk capacity of a Prism Central VM includes all the vDisks, the additional vDisks do not impact overall capacity. During the upgrade you can monitor progress ("VM disk attach" tasks) from the Tasks dashboard.

6. After the upgrade completes, run NCC as described in Running NCC (Prism Central) on page 37.
   The NCC health check pc_vm_resource_resize_check verifies that the configured amount of memory and vCPU on the Prism Central VM is adequate. If this check triggers a WARN alert, see the referenced Knowledge Base article to adjust Prism Central VM resources.

   After adjusting resources, run this check again to ensure a PASS status result: `nutanix@cvm$ ncc health_checks system_checks pc_vm_resource_resize_check`.

7. On the **LCM** page, click **Inventory** > **Perform Inventory** to enable LCM to check, update and display the inventory information.

   For more information, see Performing Inventory with the Life Cycle Manager section in *Life Cycle Manager Guide*.

Upgrading Prism Central by Uploading Binary and Metadata Files

About this task

- Do these steps to download Prism Central binary and metadata .JSON files from the Nutanix Support Portal, then upgrade through **Upgrade Software** in the Prism Central web console.
- Typically you would need to perform this procedure if your cluster is not directly connected to the Internet and you cannot download the binary and metadata .JSON files through the Prism Central web console.

Procedure

1. Log on to the Nutanix support portal and go to **Downloads** > **Prism Central**.
2. Click **Download** to save the **Prism Central Upgrade** binary and metadata .JSON files on your local media.

   You can also copy these files to a USB stick, CD, or other media.
3. Log on to the Prism Central web console.
4. Click the gear icon in the main menu and then select **Upgrade Prism Central** in the **Settings** menu.
5. Click the **upload the Prism Central binary** link.
6. Click **Choose File** for the binary and upgrade metadata (.JSON) files that you previously downloaded, browse to the file locations, and click **Upload Now**.
7. [Optional] When the file upload is completed, to run the pre-upgrade installation checks only without upgrading, click **Upgrade** > **Pre-upgrade**. These checks also run as part of the upgrade procedure.
8. When the file upload is completed, click **Upgrade** > **Upgrade Now**, then click **Yes** to confirm.
   The **Upgrade Software** dialog box shows the progress of your selection, including pre-installation and cluster health checks. After the upgrade process is completed on a Prism Central VM, the Prism Central VM restarts. This restart is not disruptive to node operations.
9. On the **LCM** page, click **Inventory** > **Perform Inventory** to enable LCM to check, update and display the inventory information.

   For more information, see Performing Inventory with the Life Cycle Manager section in *Life Cycle Manager Guide*.

Prism Central-Managed Clusters Upgrade

You can upgrade AOS on some or all of clusters registered to and managed by Prism Central through the Prism Central web console.

You can upgrade AOS on some or all of clusters registered to and managed by Prism Central. The upgrade procedure, known as 1-click centralized upgrade, enables you to upgrade each managed cluster to a specific version compatible with Prism Central. Acropolis Upgrade Paths lets you check the upgrade path from your current version to your target version for AOS, Prism Central, and Nutanix Files.

Cluster Upgrade Requirements

- Upgrade clusters through the Prism Central web console.
- You can upgrade clusters if **Available Versions** is shown in the **Upgrade Software** dialog. It will display one or more AOS versions available to apply to clusters. If no versions are available (that is, none displayed), you might have to upgrade each cluster according to procedures described in this guide. Basically, if a version is available to Prism Central, it will be available to each cluster registered.
- Prism Central and each cluster (individually also known as Prism Element) must be connected to the Internet to access the Nutanix support portal.
- Prism Central and each cluster must be configured with a domain name server. See Configuring Name Servers in the *Prism Web Console Guide* or Configuring Name Servers (Prism Central) in the *Prism Central Guide*.
- Dark-site (internet-disconnected) upgrades cannot be performed using this feature. In this case, upgrade each cluster according to procedures described in this upgrade section.
- You cannot initiate an upgrade on a cluster that has an upgrade that is in process or is not completed.

Cluster Upgrade Features

- Sequential upgrade, in order, one cluster at a time. Select the order in which clusters are upgraded. Upgrade one cluster, then the next cluster is upgraded until all upgrades are complete. The clusters waiting be upgraded are placed in a Queued status. If one cluster fails to upgrade for some reason, the upgrade is cancelled for all remaining queued clusters.
- Parallel upgrade. Upgrade all clusters at the same time. If one cluster fails to upgrade for some reason, it does not affect the upgrade status of the other clusters. The upgrade status of each cluster is independent from every other cluster.
- Labeled clusters. You can apply a label to selected clusters and upgrade just the labeled clusters. The label also enables you to filter clusters by label.

Upgrading One or More Managed Clusters

Procedure

1. Log in to the Prism Central web console.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Hardware** > **Clusters** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
3. Click the **List** tab and do one of the following:
   - » Select one or more clusters from the list.
   - » Click **Filters** and select a cluster label if you have already created a label to group specific clusters.

4. Click **Actions** > **Upgrade Software** to launch the **Upgrade Software** dialog box.

   a. **Available Versions** lists AOS versions available to apply to clusters

   b. **Upgrade Sequence** enables you to choose parallel upgrade (upgrade all selected clusters **At the same time**) or **One at a time (custom Order)** (upgrade one cluster at a time in order)

   c. List of clusters to select for upgrade order if you selected **Custom Order**

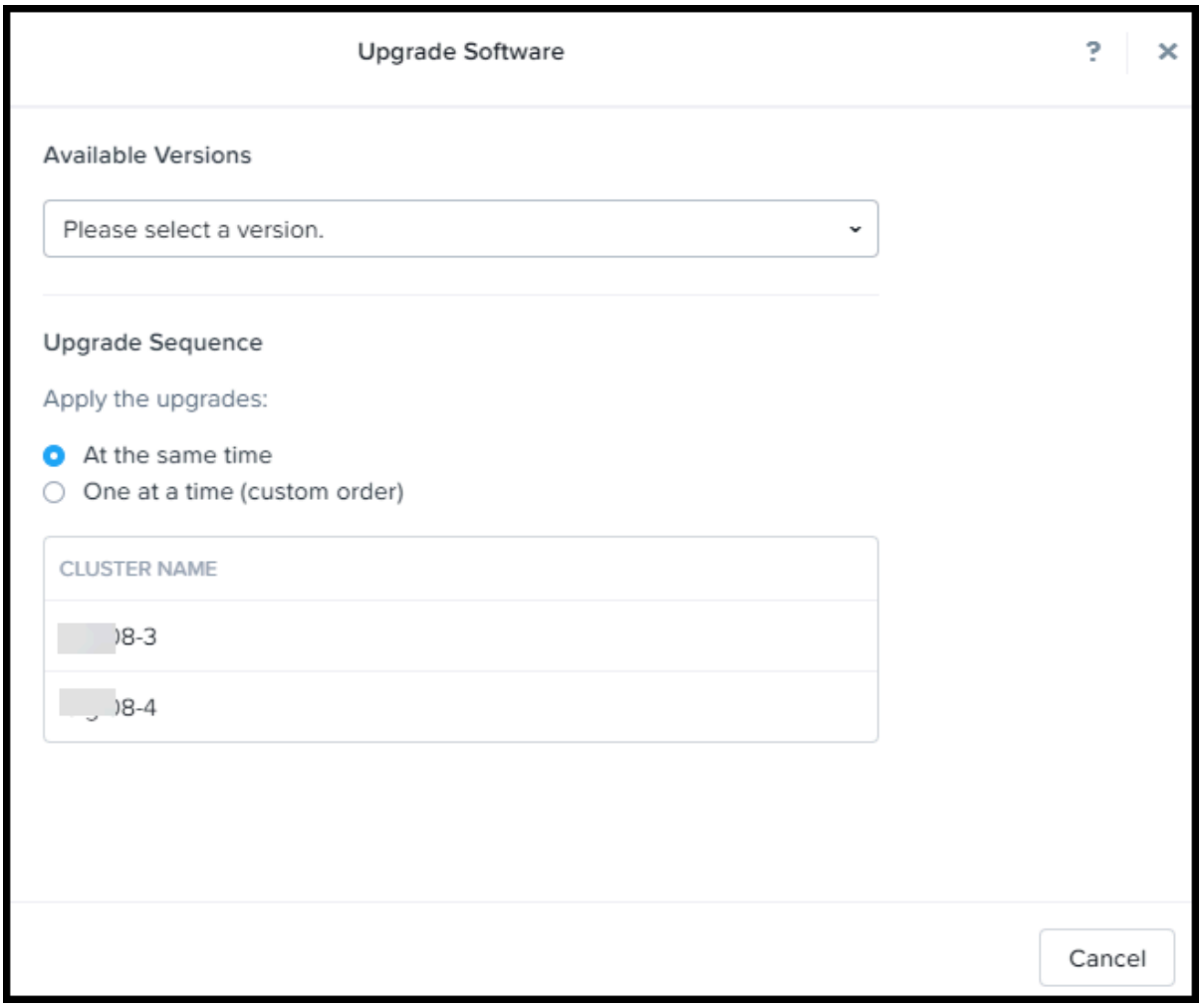


Figure 9: Upgrade Software

5. Select an AOS version and **Upgrade Sequence** choice, then click **Upgrade**.
   The upgrade begins. To view upgrade progress and status, click the blue task icon to open the **Tasks** page. The **Cluster** pane also displays **Upgrade Status**.

6. On the **LCM** page, click **Inventory** > **Perform Inventory** to enable LCM to check, update and display the inventory information.

   For more information, see Performing Inventory with the Life Cycle Manager section in

   Life Cycle Manager Guide.

Prism Central Installation or Upgrade in Non-Nutanix ESXi Environment

This section describes how to install and upgrade Prism Central virtual machine (VM) in a non-Nutanix environment with the ESXi hypervisor.

> **Note:** Use these procedures only when you install or upgrade the Prism Central VM to Prism Central pc.2024.1 or later versions.

Downloading Prism Central VM Installation Files (Manual Method)

This section describes how to download Prism Central VM installation files for manual installation (when the Prism Central 1-click deployment method is not available).

Procedure

1. Log on to the Nutanix Support portal and go to the Prism Central Downloads page.
   The page lists the latest available version. You can download previous release bits from the **Other Versions** tab.
2. Locate the **Prism Central Install on ESX(Version:** `pc version`) file, and click **Download** to get the Prism Central VM files, then save them to a folder, directory, or other location.
   The system downloads a `pc_version`.ova file, where `pc_version` is the Prism Central version. For example, the downloaded file for Prism Central pc.2024.1 is named pc.2024.1.ova.

Installing the Prism Central VM (ESXi)

About this task

A special VM runs Prism Central from which you can monitor and manage multiple clusters. To install the Prism Central VM on an ESXi hypervisor, do the following:

> **Note:** You cannot deploy a large Prism Central VM using this manual method. You can only deploy a small Prism Central VM. For a small Prism Central VM, the recommended VM size is 6 vCPUs, 26 GB of memory, and 500 GiB of storage. Contact Nutanix Support if you require a large Prism Central VM.

Procedure

1. Download and extract the Prism Central files for ESXi as described in Downloading Prism Central VM Installation Files (Manual Method) on page 42.
2. Install the downloaded OVA file as follows:
   a. Connect to vCenter or an ESXi host using the vSphere client.
   b. Select the OVA file and deploy it.
      Select an OVA file called pc.2024.1.ova and deploy it from the download location on the workstation. In the OVA filename, the version 2024.1 indicates the Prism Central version. See the vSphere documentation for instructions on how to do deploy an OVA file.

      Note:

      - Nutanix recommends a VM size of 6 vCPUs, 26 GB of memory, and 500 GiB of storage for a small Prism Central VM deployment. Contact Nutanix Support if you require a large Prism Central VM.
      - In the OVA deployment wizard using vSphere web client, Nutanix recommends that you manually select **Thin Provision** as the virtual disk format while configuring the storage. Failing to manually select **Thin Provision** creates the default thick provisioned VMDK in vSAN.

3. Power on the Prism Central VM through the vSphere Client. Click **ACTIONS** > **Power** > **Power On** to start the VM.

   > **Note:** The Prism Central VM is powered between five and six minutes if the Prism Central is either a *master* or has a version greater than or equal to *pc.2020.11*. The VM is powered in approximately three minutes for other Prism Central versions.

4. Log into the Prism Central VM through the vSphere console (user name "nutanix" and password "nutanix/4u").

5. Assign a static IP address to the Prism Central VM as follows:

   a. Open the ifcfg-eth0 file for editing.

      The following command opens the file using the vi editor:

      ```
      $ sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0
      ```

   b. Add or update the `NETMASK`, `IPADDR`, `BOOTPROTO`, and `GATEWAY` entries as needed.

      > **Note:** Use the route -n command to retrieve the NETMASK and GATEWAY information. Ensure that the selected IP address is unreachable to the console IP address.

      ```
      NETMASK="xxx.xxx.xxx.xxx"
      IPADDR="xxx.xxx.xxx.xxx"
      BOOTPROTO="none"
      GATEWAY="xxx.xxx.xxx.xxx"
      ```

      - Enter the desired netmask value in the `NETMASK` field. (Replace *xxx.xxx.xxx.xxx* with the appropriate value.)
      - Enter the appropriate static IP address (usually assigned by your IT department) for the Prism Central VM in the `IPADDR` field.
      - Enter `none` as the value in the `BOOTPROTO` field. (You might need to change the value from `dhcp` to `none` if you employ DHCP. Only a static address is allowed; DHCP is not supported.)
      - Enter the IP address for your gateway in the `GATEWAY` field.

        > **Warning:** Carefully check the file to ensure there are no syntax errors, whitespace at the end of lines, or blank lines in the file.

   c. Save the changes.

   d. Remove any existing Nutanix Controller VM entries, that is ones which include "NTNX-*<number>*-CVM", from the /etc/hosts file. (Ensure that you do not remove any other entries from the file.)

      To edit the file using vi, enter

      ```
      $ sudo vi /etc/hosts
      ```

      When the Prism Central VM starts the first time and DHCP is enabled in the network, an entry similar to the following is added to the /etc/hosts file. This entry (if present) needs to be removed from the /etc/hosts file before restarting the Prism Central VM in the next step, which generates a new entry if DHCP is enabled.

      ```
      127.0.0.1 NTNX-10-3-190-99-A-CVM
      ```

   e. Restart the Prism Central VM.

      ```
      $ sudo reboot
      ```

      > **Note:** The Prism Central VM is powered in approximately a minute.

6. Log on to the Prism Central VM again through the vSphere console and then enter the following command to create a cluster:

   ```
   $ cluster --cluster_function_list="multicluster" -s static_ip_address create
   ```

   The *static_ip_address* is the Prism Central VM IP address.

7. [optional but recommended] Log on to vCenter Server using an administrator account and do the following:

   a. Select the Prism Central VM.

   b. Right click **Edit Notes**.

   c. In the dialog box enter NutanixPrismCentral without any new line characters and then click **OK**.

   Creating a Prism Central instance through a 1-click method enables automatically certain best practice restrictions on who can manage a Prism Central VM. This step enables the same set of best practice restrictions for a manually installed Prism Central VM. (Non-administrators may not perform any operations while administrators may perform a limited set of permissions including launch console, power off or on, pause or resume, migrate, and configure VM host affinity.)

What to do next

This completes Prism Central installation. The next step is to register clusters with Prism Central. Port 9440 needs to be open in both directions between the Prism Central VM and any registered clusters. For more information about how to connect to an existing Prism Central instance, see Registering or Unregistering a Cluster with Prism Central on page 53.

Setting Up the Installation Environment

This section describes setting up the environment for installing Prism Central pc.2024.1 or later releases.

About this task

The installation environment setup involves the following phases:

- Install the Prism Central pc.2024.1 release using the OVA file. For more information, see Installing the Prism Central VM (ESXi) on page 42.
- Downloading the CSI bundle from the Nutanix portal.
- Setting up the installation tool.
- Setting up target Prism Central cluster configuration.
- Setting up the site proxy environment and defining storage policies.

Procedure

1. Log on to the Nutanix Support portal and browse to the Microservices Platform (MSP) page.
2. Download the CSI bundle and extract its contents into the /home/nutanix/data directory on the PC VM.

   The CSI bundle contains essential tools such as `CredHelper` and `setup_three_tier`.

3. Copy the `setup_three_tier` tool from the tools directory inside the CSI bundle and place it in the /home/nutanix/cluster/bin folder on the Prism Central VM.

4. SSH to the Prism Central VM and run the `setup_three_tier` tool.

   The `setup_three_tier` tool creates the Prism Central environment configuration file.

   For example:

   ```
   nutanix@pcvm$ sudo ./home/nutanix/data/vsphere_csi_bundle/tools/setup_three_tier -e
   ```

5. Create the cluster.

   You can specify additional parameters such as DNS servers and NTP servers. For example:

   ```
   nutanix@pcvm$ cluster --cluster_function_list "multicluster" -s
    198.162.146.81 --dns_servers "198.162.64.15, 198.162.64.16" --ntp_servers
    "0.centos.pool.ntp.org,1.centos.pool.ntp.org" create
   ```

6. (Optional) Configure proxy settings.

   If a proxy setup is in place, ensure to configure Microservices Infrastructure (CMSP) URLs in the allowedlist in your proxy environment to allow access to docker images and other configuration files. Microservices Infrastructure requires access to the following URLs:

   - docker.io
   - production.cloudflare.docker.com
   - nutanix.github.io
   - us-west-2.amazonaws.com
   - quay.io

7. In the vSphere client, configure the vCenter settings:

   a. Create a tag and a category. Map the category to the tag.

   b. Assign the tag to the datastore hosting the Prism Central VM.

   c. Create a new VM storage policy and assign it to the newly created tag.

      For more information, see *vSphere Tags and Attributes* information in *VMWare vSphere documentation*.

      > **Note:** Ensure that you select **Enable tag based placement rules** checkbox while defining the storage policy structure.

Configuring Prism Central VM in the Non-Nutanix ESXi Environment

This task describes how to configure Prism Central VM in the non-Nutanix environment running the ESXi hypervisor.

Before you begin

Ensure that you set up the install environment before you run the install tool (`setup_three_tier` tool). For more information, see Setting Up the Installation Environment on page 44.

Procedure

1. SSH to the Prism Central VM and run the `setup_three_tier` tool.

   The `setup_three_tier` tool accepts the user configuration and sets up the environment for PC and CMSP enablement.

   For example:

   ```
   nutanix@pcvm$ sudo ./home/nutanix/data/vsphere_csi_bundle/tools/setup_three_tier
   ```

   The system prompts you to enter the vCenter IP, vCenter port, user credentials, datacenter name, and storage policy name.

2. Enter the required details.
   The system verifies the entered data, and displays the result.

3. Check that the Prism Central ENV (pc_env_config.json) configuration file is created at /etc/nutanix.

4. Run the enable Microservices Infrastructure (CMSP) script.

   ```
   nutanix@pcvm$ python /home/nutanix/data/vsphere_csi_bundle/tools/
   enable_cmsp_3_tier.py
   ```

   To confirm if Microservices Infrastructure is enabled, run the `ecli task.list` command.

5. Upgrade the Prism Central VM compatibility (VMX version).

   a. Right-click on the Prism Central VM, and navigate to **Compatibility** > **Upgrade VM Compatibility**.

   b. Set the **Compatible with** field to the **ESXi 7.0 U2 and later**.

   c. Power on the Prism Central VM.

Setting Up the Upgrade Environment

This section describes how to set up the non-Nutanix ESXi environment to upgrade to Prism Central 2024.1 or later release.

About this task

The upgrade environment setup involves the following phases:

- Configuring Prism Central VM settings and upgrading compatibility
- Configuring vCenter Settings
- Setting up upgrade tool

Procedure

1. Access the hypervisor management interface, for example VMware vSphere client, and power off the Prism Central VM.

2. Navigate to the Prism Central VM Settings, and perform the following actions:

   - In the **Virtual Hardware** tab, perform the following settings:

     - vCPU = 6
     - vRAM = 28 GB
     - Click **ADD NEW DEVICE** to add 3 new disks with sizes as 30 GB, 100 GB, and 270 GB, and allocate the disk space based on the activities planned such as Prism Central upgrade or CMSP configuration.

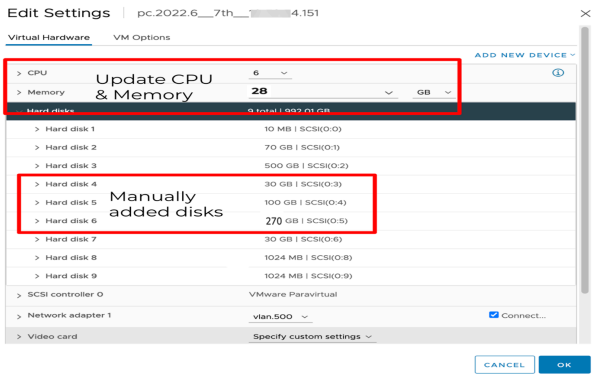


Figure 10: Virtual Hardware Settings - VSphere Client

   - Enable Disk UUID support to access and modify the Prism Central VM configuration settings in IntelliJ.

     In the **VM Options** tab, navigate to **Advanced** > **Edit Configuration**, and set **disk.EnableUUID** to *TRUE*.

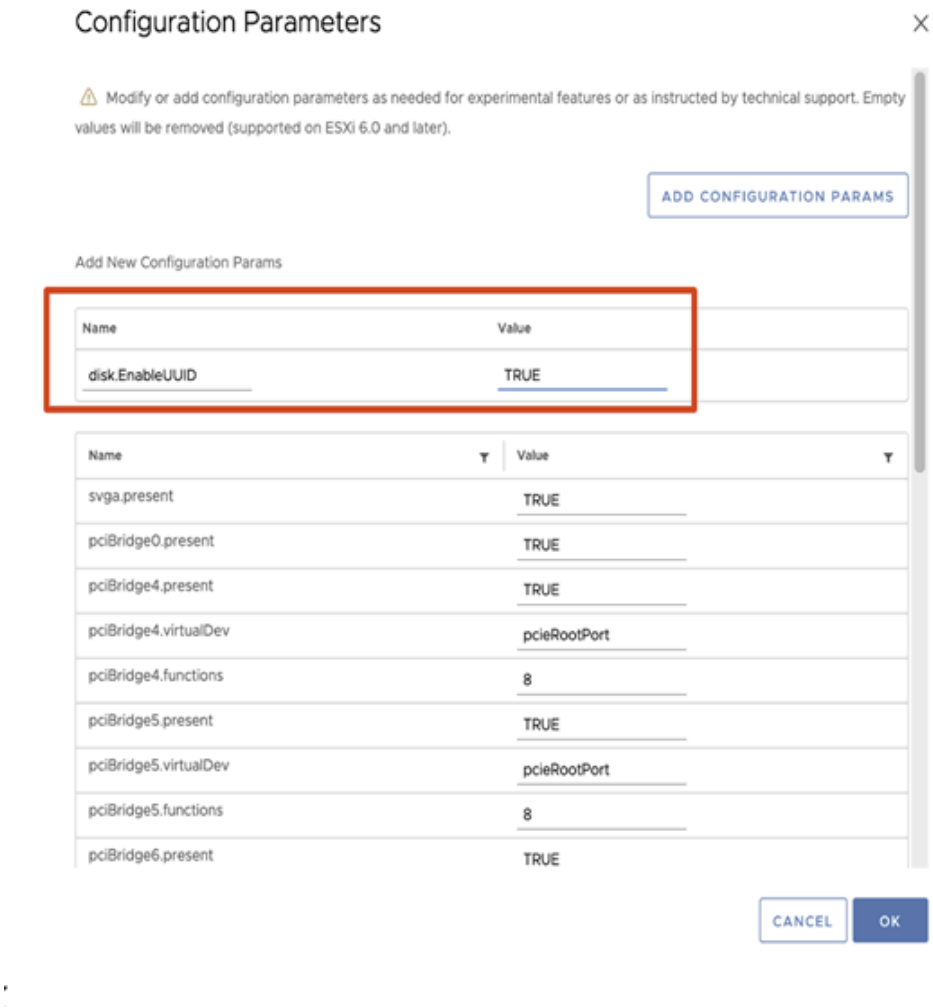


Figure 11: Enable UUID - Advanced Setting

3. Upgrade the Prism Central VM compatibility (VMX version).
   a. Right-click on the Prism Central VM, and navigate to **Compatibility** > **Upgrade VM Compatibility**.
   b. Set the **Compatible with** field to the **ESXi 7.0 U2 and later**.
   c. Power on the Prism Central VM.
4. Configure the vCenter settings.
   a. Create a tag and a category. Map the category to the tag
   b. Assign the tag to the datastore hosting the Prism Central VM
   c. Create a new VM storage policy and assign it to the newly created tag.
      For more information, see *vSphere Tags and Attributes* information in *VMWare vSphere documentation*.

> **Note:** Ensure that you select **Enable tag based placement rules** checkbox while defining the storage policy structure.

5. Set up the `setup_three_tier` tool.

   a. Log on to the Nutanix Support portal and browse to the Microservices Platform (MSP) page.

   b. Download the CSI bundle and extract its contents into the /home/nutanix/data directory on the Prism Central VM.

      The CSI bundle contains essential tools such as `CredHelper` and `setup_three_tier`.

   c. Copy the `setup_three_tier` tool from the tools directory inside the CSI bundle, and place it in the /home/nutanix/cluster/bin folder on the Prism Central VM.

Upgrading Prism Central in Non-Nutanix Environment

This section describes how to upgrade the Prism Central in the non-Nutanix environment (with ESXi hypervisor).

Before you begin

Ensure that you set up the upgrade environment before you run the upgrade tool (`setup_three_tier` tool). For more information, see Setting Up the Upgrade Environment on page 46.

Procedure

To upgrade Prism Central to pc.2024.1 and later release, perform the following steps:

1. SSH to the Prism Central VM and run the `setup_three_tier` tool.

   ```
   nutanix@pcvm$ sudo ./home/nutanix/data/vsphere_csi_bundle/tools/setup_three_tier
   ```

   The system prompts you to enter the vCenter IP, vCenter port, user credentials, datacenter name, and storage policy name.

2. Enter the required details.
   The system verifies the entered data, and displays the upgrade result.

Service Manager for Installing Services and Applications

The Service Manager feature is introduced to enable the installation of Prism Central services and application in a dark site. Service Manager enables the installation only when the Prism Central MSP Apps Bundle (`pc-app-onprem` bundle) packaged with the necessary charts and images is available in the LCM web server for the installation of the following services and applications:

- Security Dashboard
- Licensing application in Prism Central Admin Center
- Batch Service

> **Note:** Ensure that the LCM web server is reachable by all the Nutanix clusters in the dark site. For information on preparing the LCM web server, see the Life Cycle Manager Guide.

Service Manager downloads the necessary charts and images for the installation from the Prism Central MSP Apps Bundle that is placed in the LCM web server. The charts and images for the mentioned services are available in the LCM (Open Container Initiative-compliant) container registry, also called the LCM OCI registry.

Initiating Service Manager for a New Prism Central Installation

This section describes how to initiate Service Manager when you install Prism Central in a dark site for the first time.

Before you begin

Ensure that you have the following bundles in the dark site LCM web server.

- The Prism Central LCM Bundle
- The Prism Central MSP Apps Bundle that contains the necessary charts and images.

For information on preparing the LCM web server, see the Life Cycle Manager Guide.

About this task

Perform the following steps to install Prism Central with the Prism Central services and applications

Procedure

1. Install Prism Central in the dark site using the Prism Central LCM bundle.
2. Configure the LCM web server in the Prism Central Admin Center as the source for the installation bundles.

   On **Prism Central Admin Center** > **LCM** > **Settings**, select **Dark Site (Local Web Server)** in the **Source** field and provide the URL of the LCM web server in the **URL** field.
3. SSH to the Controller VM as a `nutanix` user, and run the following commands to restart the `pc_platform_bootstrap` service on the dark site cluster:

   ```
   nutanix@cvm$ genesis stop pc_platform_bootstrap
   ```

   This command stops the `pc_platform_bootstrap` service.

   ```
   nutanix@cvm$ cluster start
   ```

   This command restarts the `pc_platform_bootstrap` service.

   Restarting the `pc_platform_bootstrap`, starts the Service Manager which installs the services and applications.

Initiating Service Manager for a Prism Central Upgrade

This section describes how to initiate Service Manager when you upgrade existing Prism Central in a dark site.

Before you begin

- Ensure that you have the following bundles in the dark site LCM web server.
  - Prism Central LCM bundle
  - The Prism Central MSP Apps Bundle that contains the necessary charts and images.

  For information on preparing the LCM web server, see the Life Cycle Manager Guide.
- Install Helm 3.0 for Service manager in the dark site.
- Ensure that you have configured the LCM web server in the Prism Central Admin Center as source for the upgrade bundles.

About this task

Perform the following step to install Prism Central with the Prism Central services and applications

Procedure

- Upgrade Prism Central in the dark site using the Prism Central LCM bundle.

  When you upgrade Prism Central to pc.2024.1 or later versions, Service Manager installs the services and applications using the Prism Central MSP Apps Bundle in the LCM web server.

Prism Central Licensing

Nutanix provides licenses you can apply to enable a variety of features.

The Prism web console and Nutanix Support Portal provide the most current information on your licenses. For more information on licenses, see the License Manager Guide.

X-Small Prism Central

X-Small Prism Central is a single-node Prism Central VM that is intended for small-scale deployments with limited workload.

> **Note:** You can deploy x-small Prism Central on clusters running AOS 6.8 or later versions only. X-Small Prism Central lets you manage clusters running AOS versions earlier than AOS 6.8.

For information on the type of Prism Central deployments, see the *Prism Central Scalability* topic in the release notes for the Prism Central version to be installed.

X-Small Prism Central is ideal for users who have five or fewer clusters on their site and use only the basic or essential capabilities of Prism Central. X-Small Prism Central provides the following capabilities:

- Multi-cluster management (up to 5 clusters)
- VM management
- Host management
- Infrastructure management, monitoring, and health
- Enterprise authentication and role-based access control (RBAC)
- REST APIs
- Comprehensive search
- Pulse Insights
- Life Cycle Manager (LCM)
- Prism Central backup and restore
- Categories
- Projects
- Microservices infrastructure
- Identity and access management (IAM)

Specifications

X-Small Prism Central has the following specifications:

Table 8: X-Small PC Specifications

Number of vCPU	4
Memory	18 GB
Total Storage Capacity	100 GiB

For information about the maximum tested and supported values for x-small Prism Central, see Nutanix Configuration Maximums.

Limitations

- X-Small Prism Central does not support the scale-out Prism Central feature.

  For information on Prism Central scalability, see the *Prism Central Scalability* topic in the release notes for the Prism Central version to be installed.

- Adding entities to a x-small Prism Central deployment beyond the recommended number of VMs, clusters, or nodes results in an unsupported configuration. Nutanix recommends that you scale up to small, large, or x-large Prism Central deployment to increase its capacity. For more information, contact Nutanix Support.
- X-Small Prism Central does not allow you to enable the following features:

  - Flow Virtual Networking
  - Flow Network Security
  - Self-Service
  - Intelligent operations
  - Objects
  - Nutanix Kubernetes Engine
  - Files
  - Foundation
  - Foundation Central
  - Quotas
  - Multi-site DR (available in PRO customers)
  - Marketplace
  - Reporting and Dashboards
  - Security Dashboard

  To enable these features, you must upgrade to a small, large or x-large Prism Central deployment. For more information, contact Nutanix Support.

- X-Small Prism Central does not support nearsync and synchronous replication.

Registering or Unregistering a Cluster with Prism Central

Before you begin

- If you have never logged into Prism Central as the user admin, you need to log in and change the password before you attempt to register a cluster with Prism Central.
- Do not enable client authentication in combination with ECDSA certificates on a registered cluster since it causes interference when communicating with Prism Central.
- Ports 9440 and 80 need to be open in both directions between the Prism Central VM and all the Controller VMs (and the cluster virtual IP address if configured) in each registered cluster. For the complete list of required ports, see Ports and Protocols.
- If you have a proxy server configured and you want the cluster - Prism Central communication to go through the proxy, open the relevant ports on the proxy. If you do not want the communication to go through the proxy, add the Prism Central IP address to the proxy whitelist (allowlist) in the cluster settings. For more information about configuring proxy, see Configuring HTTP Proxy in *Prism Element Web Console Guide*. For the complete list of required ports, see Ports and Protocols.
- A cluster can register with just one Prism Central instance at a time. To register with a different Prism Central instance, first unregister the cluster.

About this task

To register a cluster with Prism Central, do the following:

Procedure

1. Log in to the Prism web console on the target cluster as the admin user.
2. In the **Actions** dropdown menu, click **Health** > **Run Checks** to run Nutanix Cluster Checks.
3. Do either of the following:
   - » In the **Home** dashboard, click **Register or create new** from the **Prism Central** widget.
   - » Click the Settings icon, and navigate to **Setup** > **Prism Central Registration** in the **Settings** page.
4. In the **Prism Central Registration** window, click **Connect**.

   The **Prism Central Registration** window provides two options: **Deploy** and **Connect**. This procedure describes how to connect to an existing Prism Central instance. For instructions on how to deploy a new Prism Central instance, see Installing Prism Central.

   A window appears outlining what services are available through Prism Element and Prism Central.
5. Click **Next** after reviewing the message.
6. Enter the following information:
   a. **Prism Central IP**: Indicates the IP address of the Prism Central VM.
   b. **Port**: The default port number is 9440. This is an optional field. For the complete list of required ports, see Ports and Protocols.
   c. **Username**: Indicates the user name for Prism Central. You can enter admin as the Prism Central user name.
   d. **Password**: Indicates the password for the Prism Central user.

7. Click **Connect** to save the values and close the window.
   The cluster is now registered with the specified Prism Central VM. After successful registration, the system allows passing information between the specified cluster and Prism Central.

   Note:

   - The user credentials provided when registering a cluster (Prism Element) with Prism Central are only used once. After registration, modifying the admin password would not impact any communication between Prism Central and the cluster.
   - On small, large, and x-large Prism Central deployments, when you register a new cluster to Prism Central, Prism Central synchronises the past 90 days of data (including multiple metrics) from the cluster. On x-small Prism Central deployments, Prism Central synchronises the past 2 hours of data (including multiple metrics) from the cluster. To view the list of metrics that are synced during registration, see the file */home/nutanix/config/arithmos/data_sender/arithmos_history.json* in the Controller VM. To view the list of metrics that are synced during a regular synchronisation between Prism Central and the cluster, see the file */home/nutanix/config/arithmos/data_sender/arithmos.json* in the Controller VM.

Unregistering from Prism Central

Before you begin

Caution: Unregistering a cluster from Prism Central is not a supported workflow. The unregistered cluster might be disallowed for re-registration with a Prism Central instance.

You can use the destroy Cluster feature of Prism Central, which implicitly unregisters the cluster. For more information, see Destroying a Cluster on page 418.

If you still want to go ahead with unregistration of the cluster, considerations the following points:

- Unregistering a cluster through the Prism web console is no longer available. This option is removed to reduce the risk of accidentally unregistering a cluster. Several features such as role-based access control, application management, micro-segmentation policies, and self-service capability require Prism Central to run your clusters. If a cluster is unregistered from Prism Central, it leads to features unavailability and configuration erasure. You can only use the following procedure from Controller VM (CVM) to unregister a cluster.
- Perform the entire registration process, followed by the cleanup process.
- Do not remove the IPs of the cluster and Prism Central from the whitelists on both sides until the unregistration process completes successfully.

If you have enabled additional applications or features in Prism Central, see the following table for recommendations before you unregister a cluster. For more information, see KB 4944.

Table 9: Unregistering a cluster with additional applications enabled

Nutanix Disaster Recovery (Leap)	Before unregistering the cluster from Prism Central, you must remove any Nutanix Disaster Recovery (Leap) configuration involving virtual machines or volume groups for the cluster being unregistered. Otherwise you will not be able to manage the snapshot creation or replication policies configured on the cluster. For more information, see KB 12749. **Note:** Do not proceed with unregistration, if the stretch config (AHV Synchronous replication) is present.
Flow Networking	You must disable Flow Networking on the cluster before unregistering it from Prism Central, using the steps mentioned in Unregistering a PE from the PC in *Flow Virtual Networking Guide*. If Flow Networking is not disabled on the cluster prior to unregistering from Prism Central, attempts to enable Flow Networking in the same cluster does not work as expected. For more information, see KB 12449.
NuCalm/App Management	You must clean up Calm entities after unregistration. Contact Nutanix Support for assistance in cleaning up the CALM entities.
Prism Self Service configuration	Changes that have been made to the Prism Self Service configuration in Prism Central are lost after unregistration. Ensure that you follow the extra cleanup steps mentioned in KB 4944.
NKE Kubernetes	Do not unregister the cluster hosting an NKE Kubernetes cluster from Prism Central. Unregistration of cluster from Prism Central will prevent the management of the NKE clusters.

About this task

To unregister a cluster from an existing Prism Central instance, perform the following steps:

Procedure

1. Log in to any CVM of the registered cluster through an SSH session.
2. Run the cluster status command and verify that all services are in a healthy state.
3. Run the following command to unregister the cluster from Prism Central.

   ```
   nutanix@cvm$ ncli multicluster remove-from-multicluster external-ip-address-or-svm-ips=pc-name-or-ip username=pc-username password=pc-password
   ```

   Replace *pc-name-or-ip* with the Prism Central name or IP address and *pc-username* and *pc-password* with the login credentials for your Prism Central administrator account. This step can take some time (though typically just a few seconds). If the password contains any special characters, ensure to enclose the password in single quotes.
4. Run the following command to verify if the cluster unregistration is completed:

   ```
   nutanix@cvm$ ncli multicluster get-cluster-state
   ```

5. Run the following command to retrieve the UUID for the cluster:

```
nutanix@cvm$ ncli cluster info
```

The following output shows the **Cluster UUID** value in the cluster information output:

```
Cluster Id          : 586dd889-84dc-422f-b8e8-8ce3cd781dcf::4100682370753502671
    Cluster Uuid             : 586dd889-84dc-422f-b8e8-8ce3cd781dcf
    Cluster Name             : PC_10.51.147.185
    Cluster Version          : pc.2024.1
    Cluster Full Version     : el8.5-release-fraser-2024.1-stable-
ca1136cd25915d9b5635483235e1fd7af3ccddfb
    External IP address      : 10.51.147.185
    Is LTS                   : false
    External Data Services... :
    Support Verbosity Level  : BASIC_COREDUMP
    Lock Down Status         : Disabled
    Password Remote Login ... : Enabled
    Timezone                 : Atlantic/Reykjavik
    NCC Version              : ncc-5.0.0
    Degraded Node Monitoring  : Enabled
```

6. Log in to the Prism Central VM through an SSH session (as the *nutanix* user) and perform the following steps:

   a. Run the unregistration clean-up script.

   ```
   [pcvm]$ python /home/nutanix/bin/unregistration_cleanup.py uuid
   ```

   Replace *uuid* with the value you obtained in step 5. This script removes all remaining registration information about that cluster and completes the unregistration process with the Prism Central VM.

   > **Note:** If you do not run the clean-up script, some artifacts continue to retain references to entities that are no longer managed by the cluster. Some artifacts that might have lost references due to the unregistration process might not be able to recover their references.

   b. Run the following command to retrieve the UUID for Prism Central:

   ```
   [pcvm]$ ncli cluster info
   ```

   Find the **Cluster UUID** value in the displayed information (see step 5), which in this case is the UUID for Prism Central.

7. Go back to the CVM, and run the unregistration_cleanup.py script to complete the unregistration process on the cluster.

```
nutanix@cvm$ python /home/nutanix/bin/unregistration_cleanup.py uuid
```

In this case the *uuid* is the Prism Central UUID obtained in step 6b.

What to do next

After unregistration process is completed, you can re-register the cluster with a new or re-created Prism Central instance.

If the clean up process is not completed successfully, perform the following actions:

- Check the logs to indicate if there are any input errors when calling the script. The logs for the unregistration cleanup script are available under ~/data/logs/unregistration_cleanup.log.
- If any error occurred during script processing, run the cluster status command and check that the cluster services are up and running. Re-run the script and check if the script processes successfully.

Note: If Prism Self Service is enabled and the unregistered cluster is set as the default cluster, you must update the default project to select a new (registered) cluster. For information about how to modify a project, see Modifying a Project information in *Prism Central Admin Center Guide*.

Application-specific Navigation Bar

Infrastructure

Select the **Infrastructure** application from the Application Switcher Function on page 19, and click Navigation icon to display the **Navigation Bar** on the left side.

The following is an example showing the **Navigation Bar** for the **Infrastructure** application:

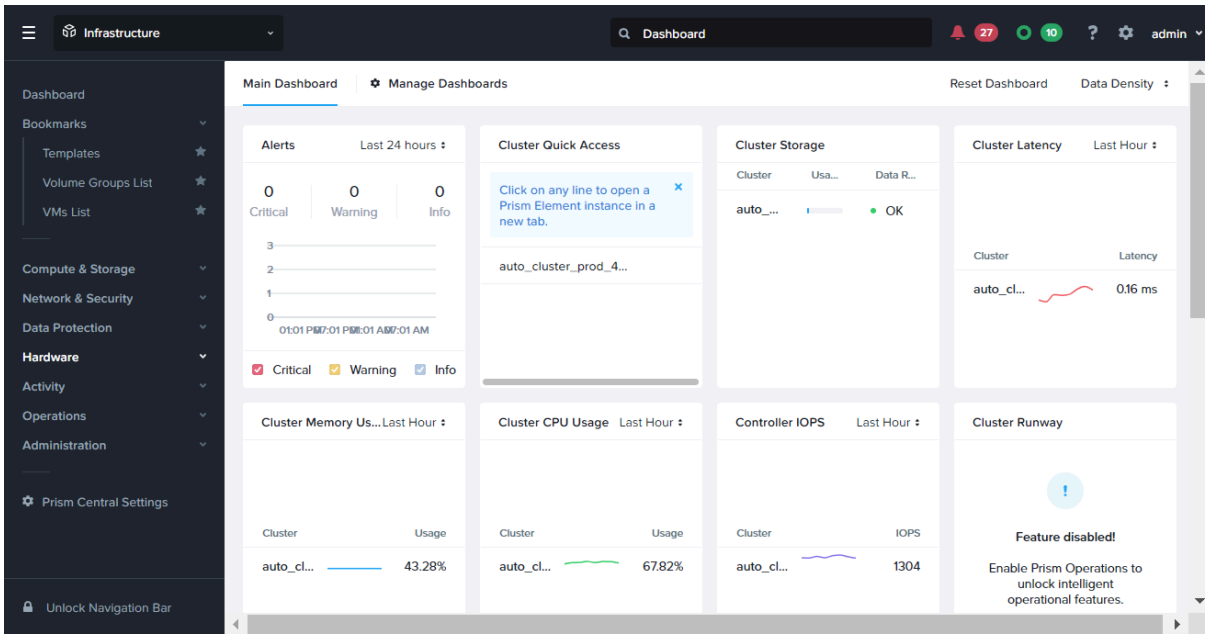


Figure 12: Navigation Bar - Infrastructure

Note:

- The **Navigation Bar** consists of **Dashboard**, **Bookmarks**, entity lists (**Compute & Storage**, **Network & Security**, **Data ProtectionHardware**, **Activity**, **Operations**, **Administration**, and **Prism Central Settings**.
- Click an entity list (for example, **Compute & Storage**) to display the entity items available in it.
- Click the entity item (for example **VMs**) to display the **Lists** page or the main page for that entity item.
- For quicker access to one or more entities in the entity list, you can bookmark the required entity to promote to the primary view of the **Navigation Bar** . Click the Bookmark icon displayed at the right of the entity name to bookmark the entity. The **Bookmarks** category appears below the **Dashboard**.

  Note: To remove a bookmarked entry, navigate to **Bookmarks**, and click the bookmark icon displayed at the right of the selected bookmarked item name.

The following table describes the entity list available in the **Navigation Bar** of the **Infrastructure** application:

Table 10: Entities - Infrastructure

Entities	Entity Items	Description
Dashboard		Displays the **Main Dashboard** (see Main Dashboard - Infrastructure on page 71).
Compute & Storage	VMs	Displays the VMs configuration page (see VM Management on page 94).
	Templates	Displays the Templates configuration page (see VM Template Management on page 188).
	OVAs	Displays the OVAs configuration page (see OVA Management on page 214).
	Images	Displays the Images configuration page (see Image Management on page 238).
	Catalog Items	Displays the Catalog configuration page (see Catalog Management on page 262).
	Storage Containers	Displays the Storage Containers configuration page (see Limitations for Storage Containers on page 290).
	Volume Groups	Displays the Volume Groups configuration page (see Volume Group Management on page 300).
	Storage Policies	Displays the Storage Policies configuration page (see Storage Policy Management on page 495).
	vCenter Datastores	Displays the vCenter Datastores configuration page (see External vCenter Server Integration on page 326).
Network & Security	Subnets	Displays the subnets configuration page (see Subnets Summary View on page 342).
	Virtual Private Clouds	Displays the virtual private clouds configuration page (see Virtual Private Clouds Summary View on page 357).
	Floating IPs	Displays the floating IPs configuration page (see Network and Security Entities on page 341).
	Connectivity	Displays the Connectivity configuration page (see Connectivity on page 376).
	Security Policies	Displays the Security Policies configuration page (see Security Policies Summary View on page 490).
	Security Dashboard	Displays the Security Dashboard (see Security Dashboard on page 395).
Data Protection	Protection Summary	Displays the Protection Summary dashboard for disaster recovery. (See Protection Summary on page 396).
	Protection Policies	Displays the Protection Policies configuration page (see Protection Policies on page 396).

Entities	Entity Items	Description
	Recovery Plans	Displays the Recovery Plans configuration page (see Recovery Plans on page 396).
	VM Recovery Points	Displays the VM Recovery Points configuration page (see VM Recovery Points on page 396).
	VG Recovery Points	Displays the VG Recovery Points configuration page (see VG Recovery Points on page 396).
	Consistency Groups	Displays the Consistency Groups configuration page (see Consistency Groups on page 396).
Hardware	Clusters	Displays the Clusters management page (see Clusters Summary View on page 398).
	Hosts	Displays the Hosts management page (see Host Management on page 420).
	Disks	Displays the Disks management page (see Disks Summary View on page 438).
	GPUs	Displays the GPUs management page (see GPUs Summary View on page 444).
Activity	Alerts	Displays the Alerts dashboard (see Prism Central Alerts and Events Reference Guide).
	Events	Displays the Events dashboard (see Prism Central Alerts and Events Reference Guide).
	Audits	Displays the Audits dashboard (see Audits Summary View on page 448).
	Tasks	Displays the Tasks dashboard (see Tasks View on page 451).
Operations	Analysis	Displays the Analysis management page (see Analysis Dashboard in *Intelligent Operation Guide*).
	Discovery	Displays the App Discovery dashboard or the enable wizard if application discovery is not enabled (see Application Discovery in *Intelligent Operation Guide*).
	Monitoring Configurations	Displays the Monitoring Integrations dashboard or the enable wizard if monitoring integrations is not enabled (see Application Monitoring in *Intelligent Operation Guide*).
	Operations Policies	Displays the Operations Policies dashboard (see Operations Policy Management in *Intelligent Operation Guide*).
	Planning	Displays the capacity Planning dashboard (see Resource Planning in *Intelligent Operation Guide*).
	Playbooks	Displays the list of playbooks (see Task Automation-Playbooks in *Intelligent Operation Guide*).
	Reports	Displays the Reports dashboard (see Reports Management in *Intelligent Operation Guide*).

Entities	Entity Items	Description
	Settings & Configurations	Displays the Settings and Configurations dashboard (see Settings & Configurations in *Intelligent Operation Guide*).
Administration	Categories	Displays the Categories dashboard (see Category Management on page 454).
	LCM	Displays the Life Cycle Manager (LCM) dashboard (see Life Cycle Manager Guide).
	Projects	Displays the Projects dashboard (see Project Overview information in *Prism Central Admin Center Guide*).
	Roles	Displays the Roles dashboard (see Security Guide).
	Users	Displays the Users dashboard (see Security Guide).
	Availability Zones	Displays the Availability Zones dashboard (see Availability Zones on page 454).
Prism Central Settings		Displays the **Settings** menu for the **Infrastructure** application (see Prism Central Settings (Infrastructure) on page 22).

Admin Center

For information about the navigation bar of **Admin Center** application, see Prism Central Admin Center Guide.

Nutanix_Apps and Other_apps

For more information about all the navigation bar of Nutanix_Apps and Other_apps that you can discover, deploy, and manage from Prism Central, refer to the application-specific documentation as described in Application Switcher Function on page 19.

Apps and Marketplace

No specific navigation bar is available for **Apps and Marketplace** option that appears in the Application Switcher. When you select **Apps and Marketplace** from the Application Switcher, the system redirects you to the **Admin Center** application with display of **Marketplace**.

Searching for Information

The **Infrastructure** application page includes a search field on the right (see Prism Central Landing Page on page 14) that allows you to find information about selected entities in various ways.

If you need help at any time to navigate Prism Central or apply a search filter, click the Help icon in the **Infrastructure** application page, and select **Learn about search**. This displays the **Search Guidelines** page that explains the search rules and options.

Search Basics

An *entity* is an object type such as a VM, cluster, node, security policy, project, report, event, alert, or audit. The search field is context-sensitive, which means it is populated automatically based on where you are in Prism Central. The first screen after logging on is the main dashboard, so *Dashboard* appears in the search field initially.

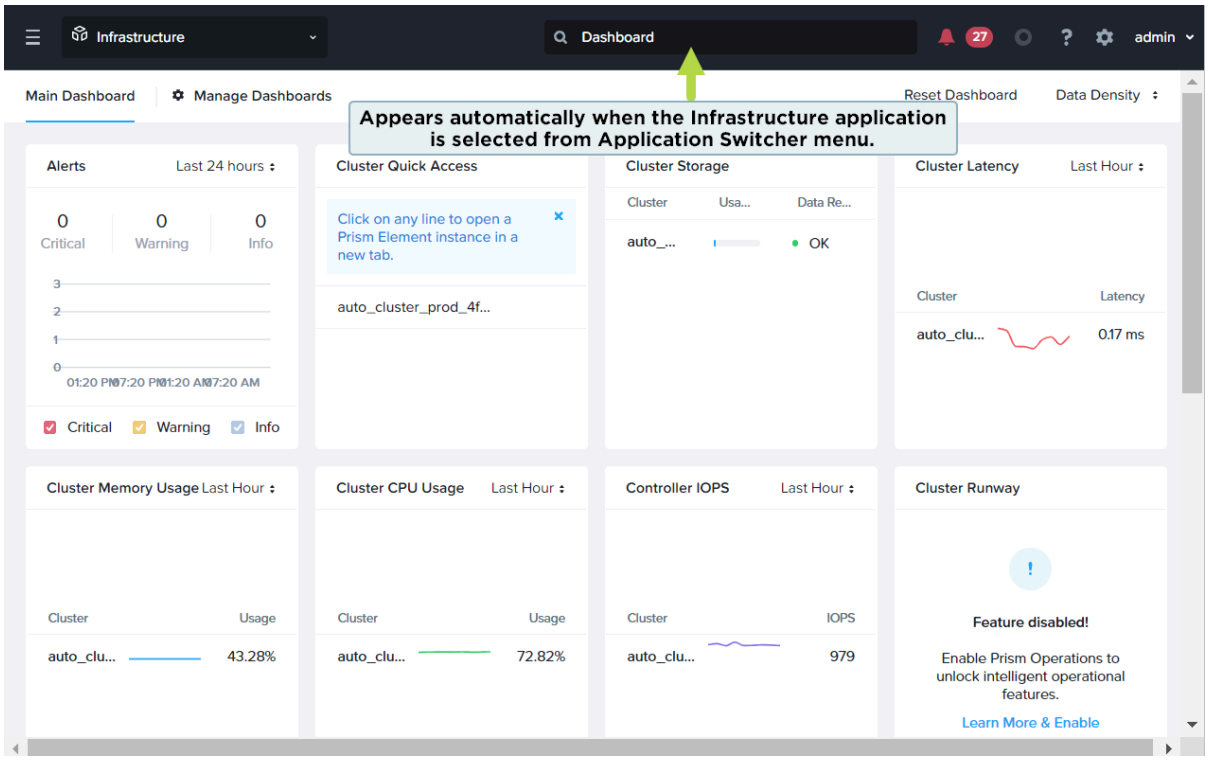


Figure 13: Search Field (Prism Central Landing page - Infrastructure)

When you navigate to different Prism Central entity pages, the search string changes automatically to match the current entity.

The following is an example showing the example of search string that appears on the VMs page:

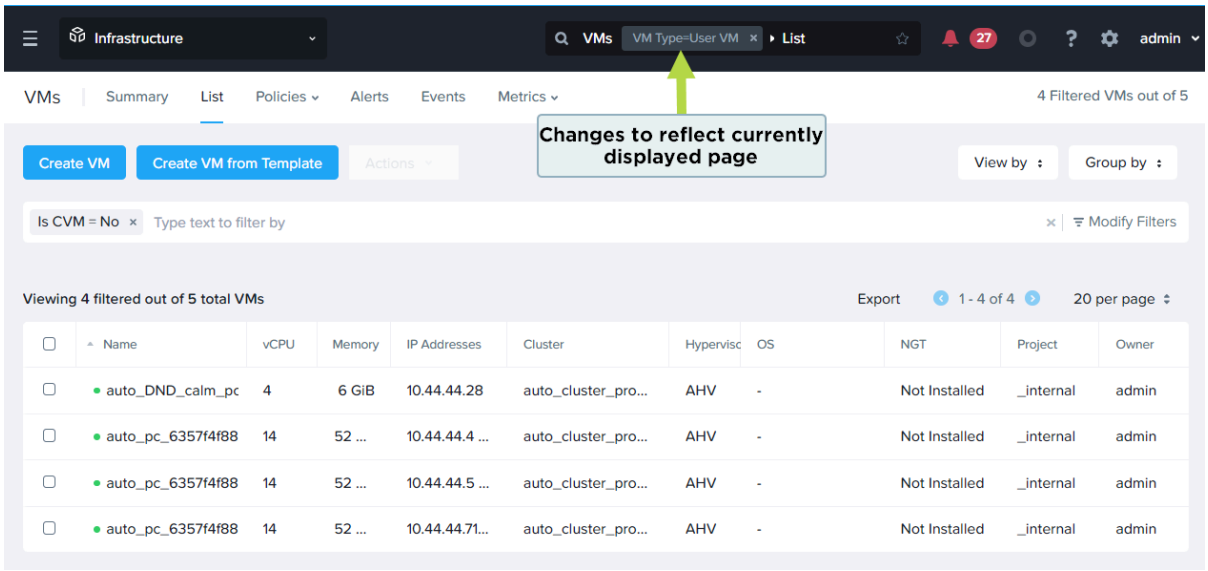


Figure 14: Search Field (Entity page)

When you enter a string in the search field, a dropdown menu appears with relevant matches across Prism Central.

Note: The search strings are case insensitive.

The following is an example showing the sample dropdown menu that appears when you enter the string *VM*:

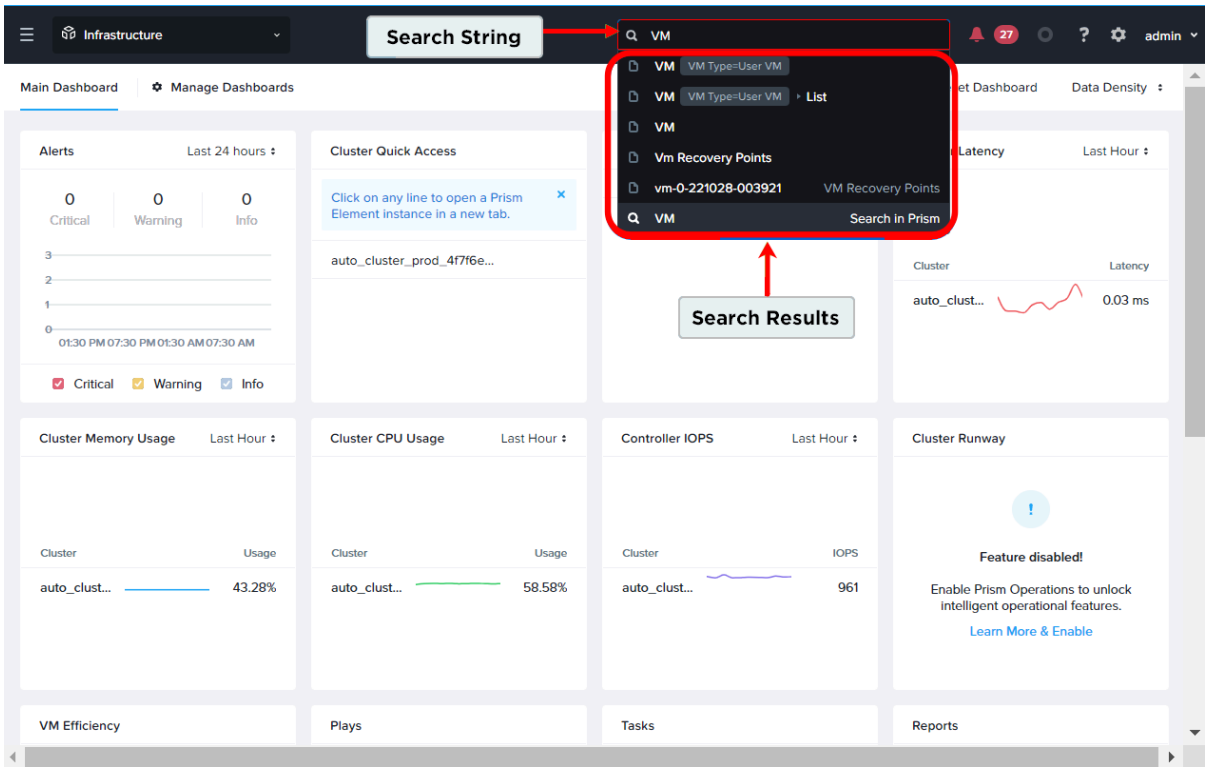


Figure 15: Search Results (for an entity type)

- *Category Value*: Select this option to display the **Category** page with any VM-related entries.
- *VM Type=User VM*: Select this option to display the filtered **Summary** page for user VMs.
- *[blank]*: Select this option to display the unfiltered **Summary** page for any user VM.
- *VM Type=User VM > List*: Select this option to display the **List** page of the user VMs.
- *VM Type=User VM > Alerts*: Select this option to display the **Alerts** page of the user VMs .
- *Search in Prism*: Select this option to search across Prism Central for any information about the target entity.

  In the following example, two tables appear in the results, a list of the top VMs and a list of the top VM-related alerts. The top VMs list includes a link to the full list of VMs, and the top alerts list includes a link

to the full list of alerts (which in this case is the same). When you click the VM or alert name, the system redirects you to the details page for that VM or alert.

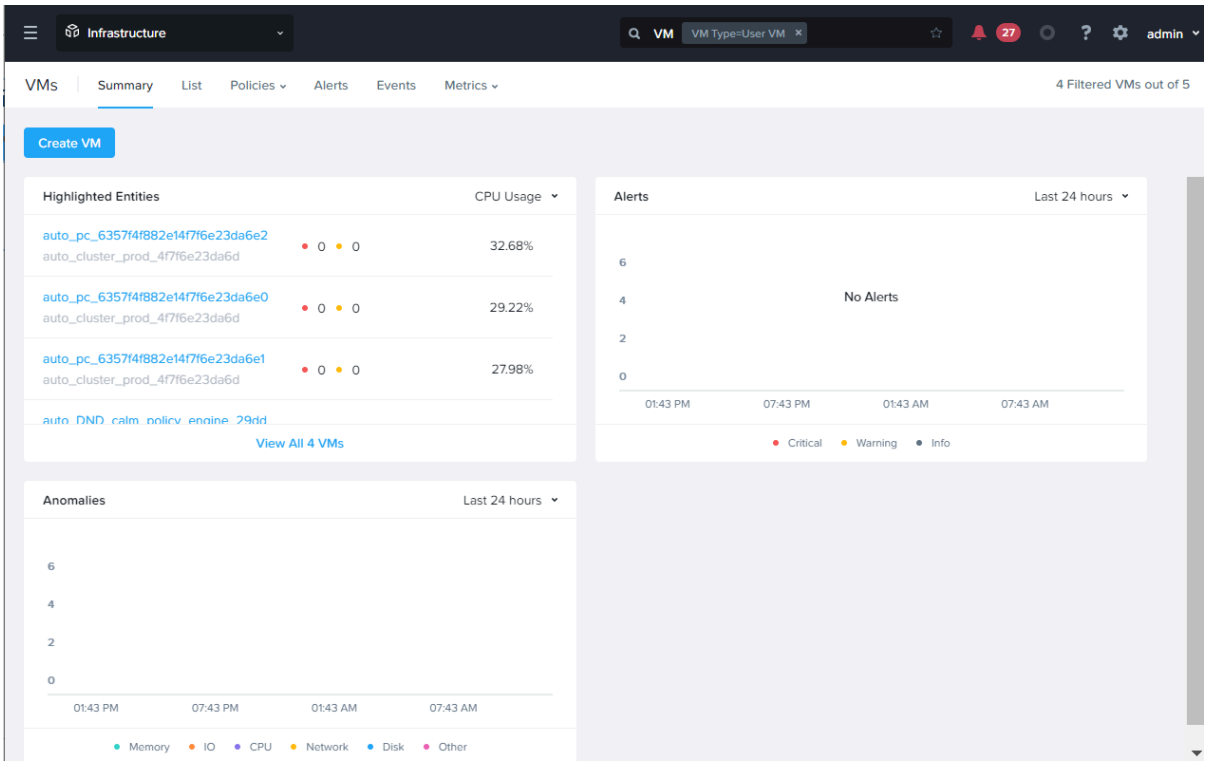


Figure 16: "Search in Prism" Results

The search is context-sensitive. You can do a quick search from your current location without entering an explicit string. For example, if you are on the user VMs summary page, clicking in the search field (or clicking the forward slash [/] character) displays the search results for user VMs. In the following example, clicking the List, Alerts, or Events entry is the same as clicking those tabs on the page. Clicking *Memory Swap* displays the Memory Swap metrics page, and *Search in Prism* displays a results page for user VMs.

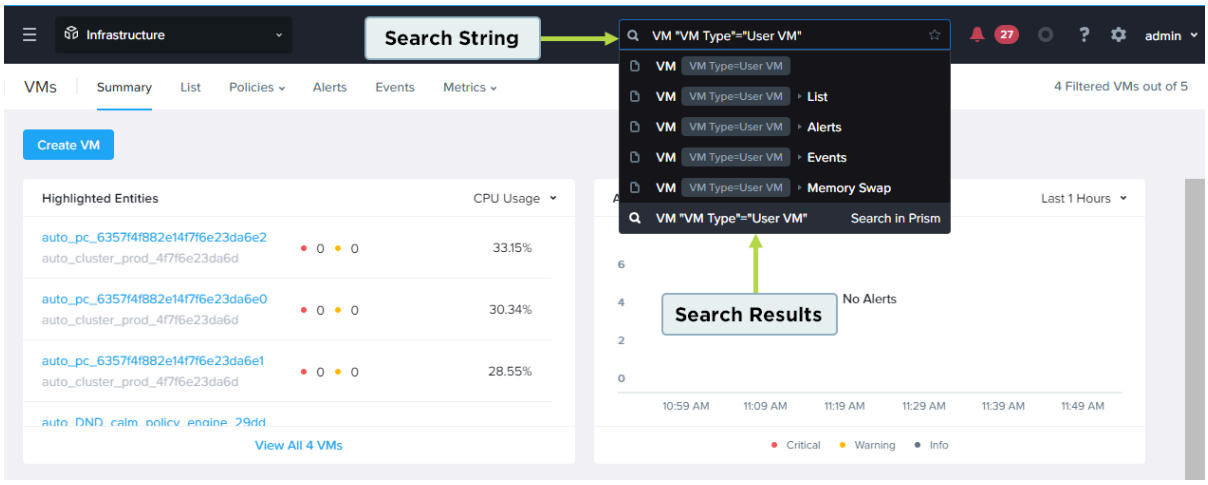


Figure 17: Search Results (for the current location)

Search provides intelligent responses based on whatever you enter in the field. For example, entering *scale out* returns a link to the Manage Prism Central page from which you can scale out Prism Central.

If you enter a more generic string such as *version*, the search engine returns results with links to pages across entities with version information.

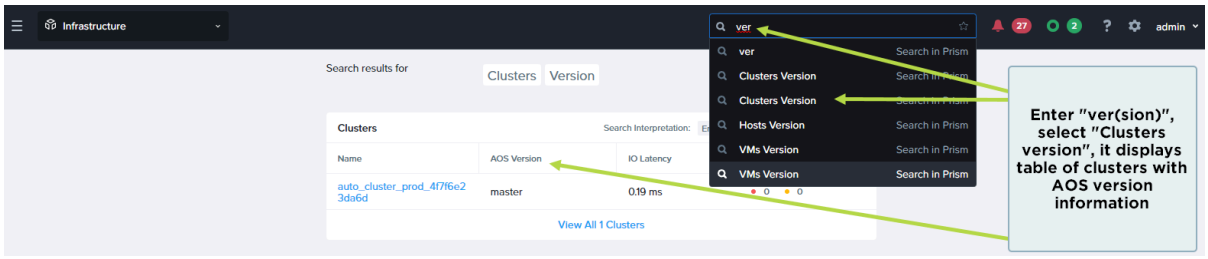


Figure 18: Search Results (for generic string)

Click the Star icon in the search field to bookmark a filtered page. This adds a bookmark for that page in the **Navigation Bar**. For more information about **Navigation Bar**, see Application-specific Navigation Bar on page 57).

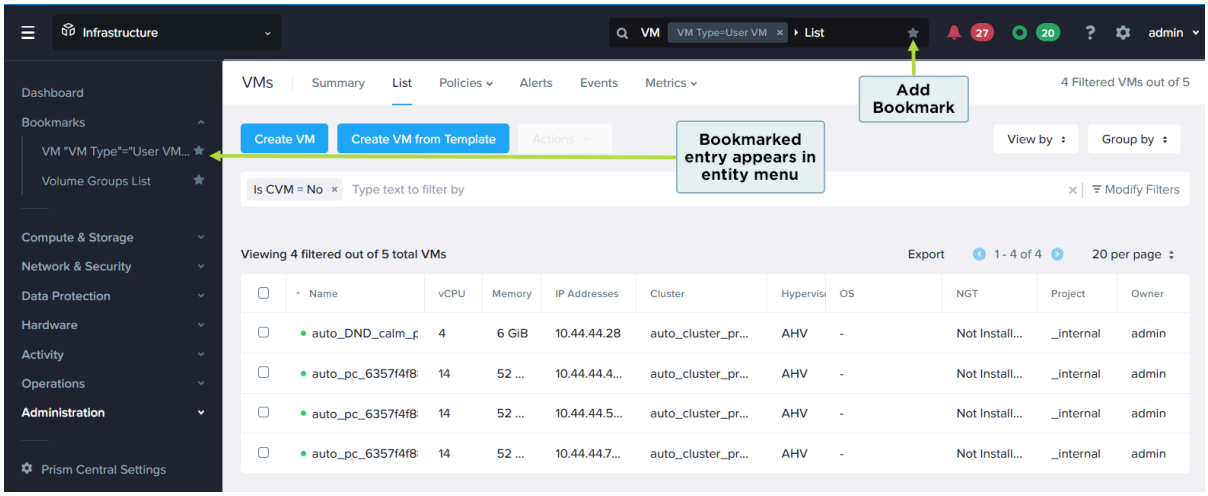


Figure 19: Bookmark Entry

On some pages, the applied filters are not reflected in the search field. For those pages, a local filters field appears. When you select one or more filters on such a page, the applied filters appear in the local filters field.

You can do the following from this field:

- Remove all filters by clicking **Clear** (on the right).
- Remove a filter by clicking *X* for that filter.
- Bookmark the filter list by clicking the Bookmark icon. You can save a maximum of 20 filter lists per entity type.
- Use a saved filter list by selecting from the dropdown menu.

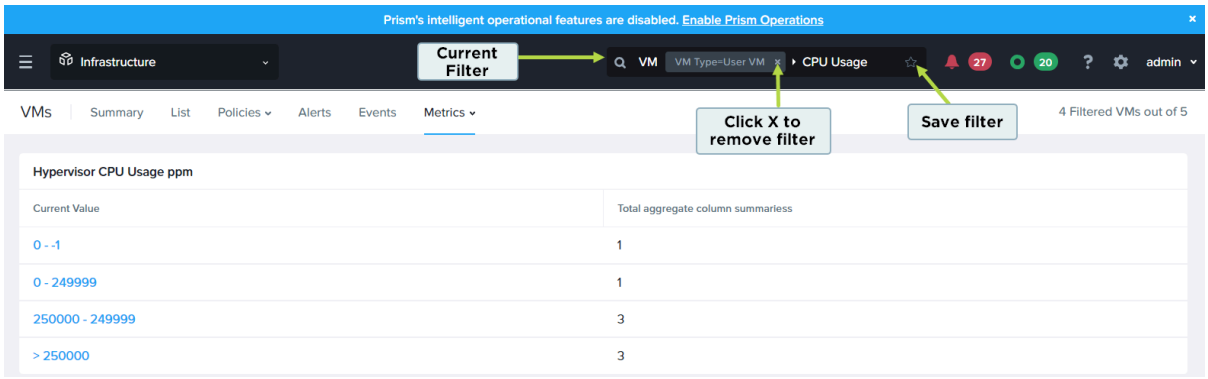


Figure 20: Local Filters Field

Query Syntax

The search field supports a range of simple and complex query options in the following syntax forms:

- [entity|metric]: Enter an entity or metric type such as `cluster`, `vm`, or `alerts` to return information about the instances of that entity or metric across the registered clusters.
- <entity> <metric>: To refine an entity search, add a metric to the query. For example, `vm iops` returns IOPS information for the VMs.
- <entity> <attribute> <metric>: To further refine the search, add an attribute for the metric. For example, `node failure alerts` returns any failure alerts about the nodes.
- [metric|attribute] operator <value>: Enter an expression for a metric or attribute to return instances that match the expression. For example, `"block model"=1050` returns information about the NX-1050 nodes. See the following "Filter Expressions" section for the supported expression operators.
- <complex expression>: Combine the syntax forms to create complex queries. For example, `clusters hypervisor = AHV "cpu usage" < 30` returns information about clusters running the AHV hypervisor with CPU usage below 30%. Complex expressions have an implied AND so only instances that satisfy all conditions are returned.
- <action expression>: In addition to search queries, you can initiate certain actions from the query bar. For example, `<vm_name> launch console` launches a console window for the specified VM (if you are allowed to do so).

The following table describes the syntax rules for search queries.

Table 11: Syntax Rules

Rule	Example
RULES THAT GO TO WELL DEFINED PAGES	
entity type	vms
entity type + metric perspective (io, cpu, memory)	vms io
entity type + alerts	vm alerts
entity type + alerts + alert filters	vm alerts severity=critical
entity type + events	vm events

Rule	Example
entity type + events + event filters	vm events classification=anomaly
entity type + filters (both metric and attribute)	vm “power state”=on
entity type + filters + metric perspective (io, cpu, memory)	vm “power state”=on io
entity type + filters + alerts	vm “power state”=on alerts
entity type + filters + alerts + (alert filters)	vm “power state”=on alerts severity=critical
entity type + filters + events	vm “power state”=on events
entity type + filters + events + event filters	vm “power state”=on events classification=anomaly
entity instance (name, ip address, disk serial, ...)	vm1, 10.1.3.4, BHTXSPWRM
entity instance + metric perspective (io, cpu, memory)	vm1 io
entity instance + alerts	vm1 alerts
entity instance + alerts + alert filters	vm1 alerts severity=critical
entity instance + events	vm1 events
entity instance + events + event filters	vm1 events classification=anomaly
entity instance + pages	vm1 nics, c1 capacity
parent instance + entity type	c1 vms
alert title search	disk bad alerts
page name search	analysis, tasks
RULES THAT ONLY GO TO SEARCH RESULT PAGES (exclusively)	
entity type + metric	vm iops
entity type + attribute	vm power state
entity instance + metric	vm1 iops
entity instance + attribute	vm1 power state
entity type + filters + metric	vm “power state”=on iops
entity type + filters + attribute	vm “power state”=on hypervisor
help text search	upgrade cluster

Keywords

The following table lists the keywords or phrases you can use when formulating a query.

- The *Object* column identifies the type of object.
  - *Entities*: Lists the entities you can specify. The list is limited. For example, you cannot search for information about remote sites or network switches.
  - *Fields*: Lists the parameters (fields) you can specify.
  - *Alerts*: Lists the alert conditions you can specify.
  - *Events*: Lists the event conditions you can specify.
  - *Actions*: Lists the actions you can specify.
- The *Entity* column specifies the entities for which you can use that keyword in a query. For example, Alert queries can apply to any entity, but Fields has multiple rows broken down by entity type (such as cluster, VM, and disk) because there are select keywords that apply to each entity type.
- The *Keywords* column is a comma-separated list of the keywords or phrases you can use in a query for the specified object/entity type.

Table 12: Search Keywords

Object	Entity	Keywords
Entities	(n/a)	vm, cluster, node, container, disk
Fields	(not specified)	cpu usage, memory usage, disk usage, free physical storage, storage logical usage, saving ratio, savings, iops, read iops, write iops, io bandwidth, read io bandwidth, write io bandwidth, io latency, read io latency, write io latency, memory capacity, hypervisor
	Cluster	cluster name, ip address, version, number of hosts, cpu count, memory capacity, runway, storage runway, cpu runway, memory runway
	VM	vm name, ip address, host ip, virtual cpus count, power state, reserved memory, os, virtual hardware version
	Disk	serial, tier, mode, iops
	Container	container name, rf, on disk deduplication, perf-tier deduplication, compression, erasure coding
	Node	host name, ip address, service vm, hypervisor name, cpu capacity, cpu model, cpu sockets count, cpu cores count, cpu thread count, serial number, block model

Object	Entity	Keywords
Alerts	(any)	alert, alert title • Severity levels: critical, warning, info • Categories (impact types): capacity, performance, configuration, availability, system indicator • Dispositions types: resolved, unresolved, acknowledged, unacknowledged
Events	(any)	event type, title
Actions	VM	clone, migrate, delete, power on, power off, suspend, create vm, launch console, create network config, resume, snapshot, update, configure vm host affinity
	Cluster	launch prism element, unregister

Filter Expressions

You can use any of the following operators in an expression.

Table 13: Query Operators

Description	Operator
contains	~
does not contain	!~
starts with (“starts with” x)	=x*
ends with (“ends with” x)	=*x
equal to	=
not equal to	!=
greater than	>
greater than or equal to	>=
less than	<
less than or equal to	<=
a metric range, for example CPU usage between 10 and 30	=[10 to 30]

The following implicit operator rules apply to expressions:

- In most cases, an AND is applied to all filters in an expression. For example, *hypervisor=AHV iops>100* means the hypervisor is AHV and IOPS are over 100.
- If the filters are on the same attribute, an OR is applied. For example, *hypervisor=AHV hypervisor=ESXi* means the hypervisor is either AHV or ESXi.

- If the filters are on the same metric, an AND is applied to create a range. For example, *iops>100 iops<500* means IOPS in the range 100-500.
- If multiple range filters are defined in a single query, an OR is applied across the ranges. For example, *iops>100 iops<500 cpu>20 cpu<40* means IOPS in the 100-500 range or CPU in the 20-40 range.

Search Units

The data for search queries comes from the following parameters.

Table 14: Data Parameters

Data Type	Unit	Parameter
bytes usage related properties	GiBiBytes	memory_capacity_bytes, storage.usage_bytes, storage.free_bytes, storage.logical_usage_bytes, data_reduction.saved_bytes, storage.usage_bytes, storage.user_container_own_usage_bytes, data_reduction.saved_bytes, memory_size_bytes
runway properties	days	capacity.runway, capacity.storage_runway, capacity.cpu_runway, capacity.memory_runway
disk capacity related properties	TebiBytes	storage.capacity_bytes, storage.user_capacity_bytes
CPU/memory usage properties	percent	hypervisor_cpu_usage_ppm, hypervisor_memory_usage

Example Queries

Here are examples of various query types.

- Entity queries:

```
<cluster_name>
<cluster_ip_address>
<disk_serial#>
VMs "Power State"=On List
VMs Hypervisor=AHV List
powered on vms "memory capacity" > 32
```

- Performance queries:

```
clusters running out of cpu
clusters hypervisor = AHV "cpu usage" < 30
vm iops
```

- Alert queries:

```
node failure alerts
<cluster_name> alerts
<cluster_name> critical availability alerts
<alert title>
Alerts "Create Time"="08-Nov-2018 9:46 AM to 08-Nov-2018 10:46 AM" Severity=Critical
```

- Action queries:

```
<vm_name> launch console
<cluster_name> launch prism element
```

```
create vm
```

- Exploration queries:

```
clusters hypervisor=AHV
vm os=Linux
<cluster_name> vms
"block model"=1050
"cpu model"=Intel
containers Rf > 2
clusters version=4.6.2
hosts iops < 1000
<cluster_name> powered off vms
disks tier=ssd
vms "cpu usage"
vms “power state”
```

MAIN DASHBOARD - INFRASTRUCTURE

The **Main Dashboard** provides a dynamic summary view of all the registered clusters in Prism Central.

To view the **Main Dashboard** at any time, select **Infrastructure** application from the Application Switcher Function on page 19, and click **Dashboard** in the **Navigation Bar** .

> **Important:** Nutanix recommends using Google Chrome web browser to access Prism Central. The display of dashboard and widgets is optimized for Google Chrome browser.

Dashboard Layout

The **Dashboard** provides a collection of widgets that appear as tiles with targeted information about the registered clusters in each tile. The **Dashboard** includes the following options:

- **Main Dashboard** tab: Displays the Infrastructure dashboard. The additional tabs appear if you create any custom dashboards.
- **Manage Dashboard**: Enables you to create a custom dashboard, edit the custom dashboard, or delete a custom dashboard. For more information about how to create a custom dashboard and modify the custom dashboard, see Creating a New (Custom) Dashboard on page 76 and Modifying a Dashboard on page 78.
- **Reset Dashboard**: Enables you to reset the dashboard to the default set of widgets.
- **Generate Report**: Enables you to generate the complete **Main Dashboard** and **Custom Dashboard** widgets as a report of all the registered clusters. For information about how to generate the dashboard report, see Generating a Dashboard Summary Report on page 83.

  > **Note:** Generating a report requires a valid license - Prism Pro, Prism Ultimate, or any edition of NCM. For more information, see License Manager Guide. The **Generate Report** option does not appear if the appropriate license is not available.

- **Add Widget**: Enables you to add a widget to the displayed dashboard. For information about how to add a widget to a dashboard, see Adding Dashboard Widgets on page 89.

  > **Note:** Adding a widget to a dashboard requires a Prism Pro license. The **Add Widgets** does not appear if Prism Pro is disabled.

- **Data Density** - Enables you to select the density of data representation in the widgets. Select one of the following three options:
  - **Light**: The information is lightly packed in the widget with more spacing between the elements.
  - **Default**: The information is moderately packed with sufficient spacing between the elements. This scheme of data density is based on user research by Nutanix.
  - **Dense**: The information is densely packed with minimal spacing between the elements for essential legibility.

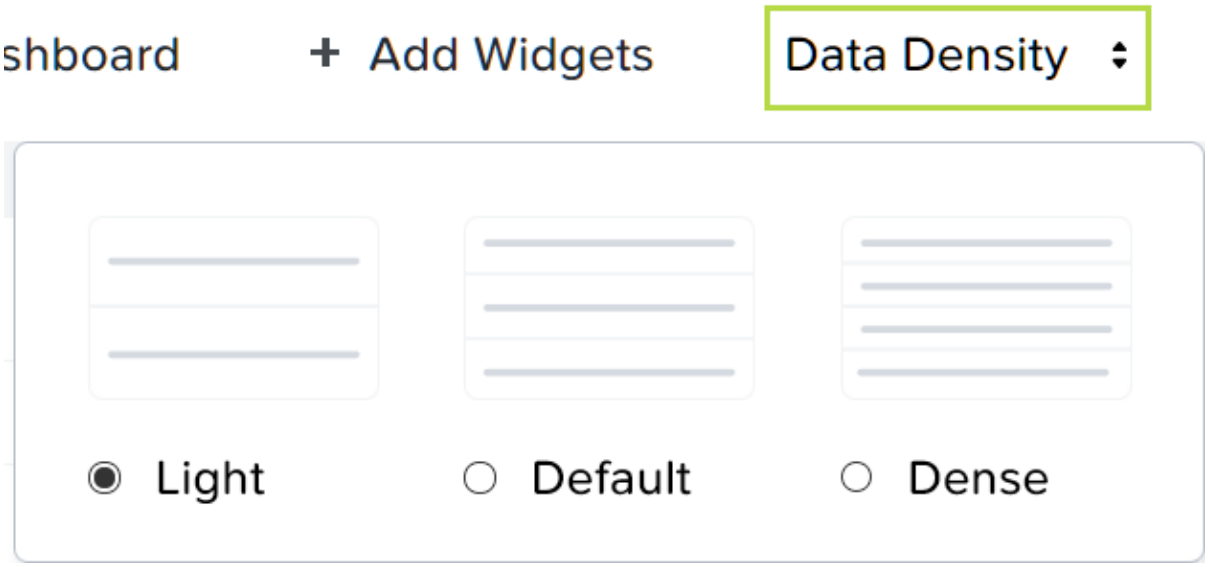


Figure 21: Data Density

> **Note:** The **Manage Dashboards** and **Add Widget** are Prism Pro license features. If Prism Pro is disabled, these options disappear, and you cannot customize or add custom dashboards. Any custom dashboards created before Prism Pro was disabled exists, but clicking the **Reset All** (which replaces the **Reset Dashboard** when custom dashboard exists) deletes all custom dashboards and returns the **Main Dashboard** to the default state.

The following is an example showing the main dashboard:

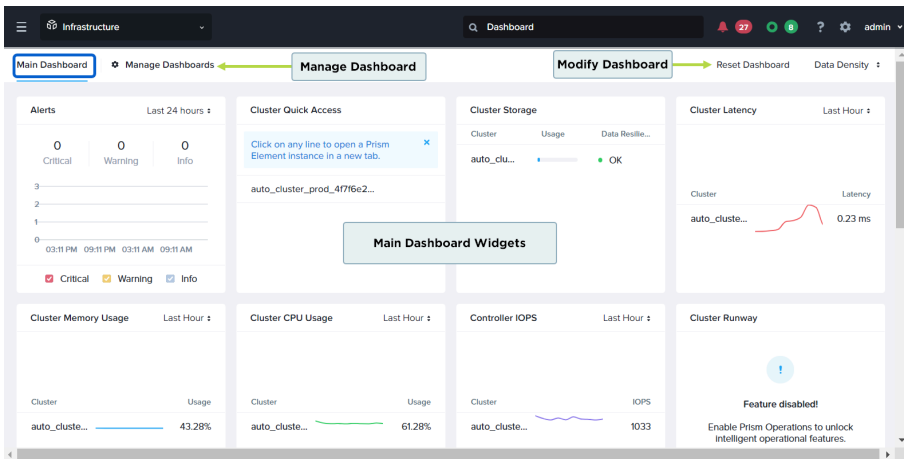


Figure 22: Main Dashboard

Dashboard Management

The **Main Dashboard** displays an array of information tiles (widgets) by default. You can customize this view by adding or deleting widgets as desired. For information about how to modify a dashboard, see Modifying a Dashboard on page 78.

The widgets are lined up in rows of four widgets per row. The default widgets are described in this section as they appear from left to right, top to bottom on the **Main Dashboard** page.

The following is an example view of the **Main Dashboard** page with the default widgets:

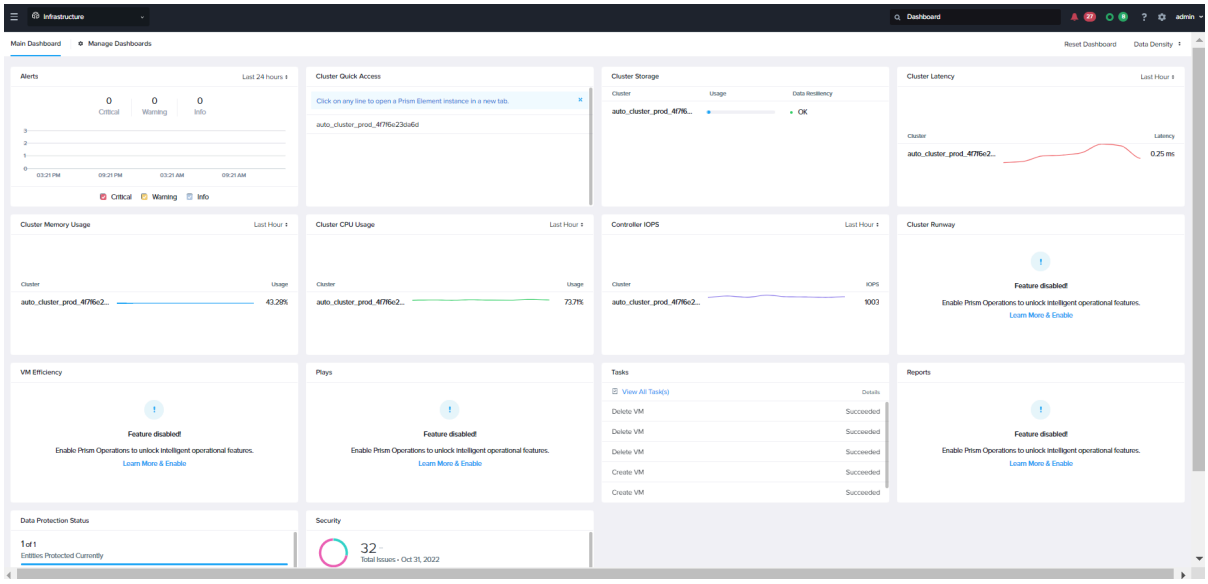


Figure 23: Main Dashboard with Default Widgets

The following is an example displaying a widget with a period (time) selection:

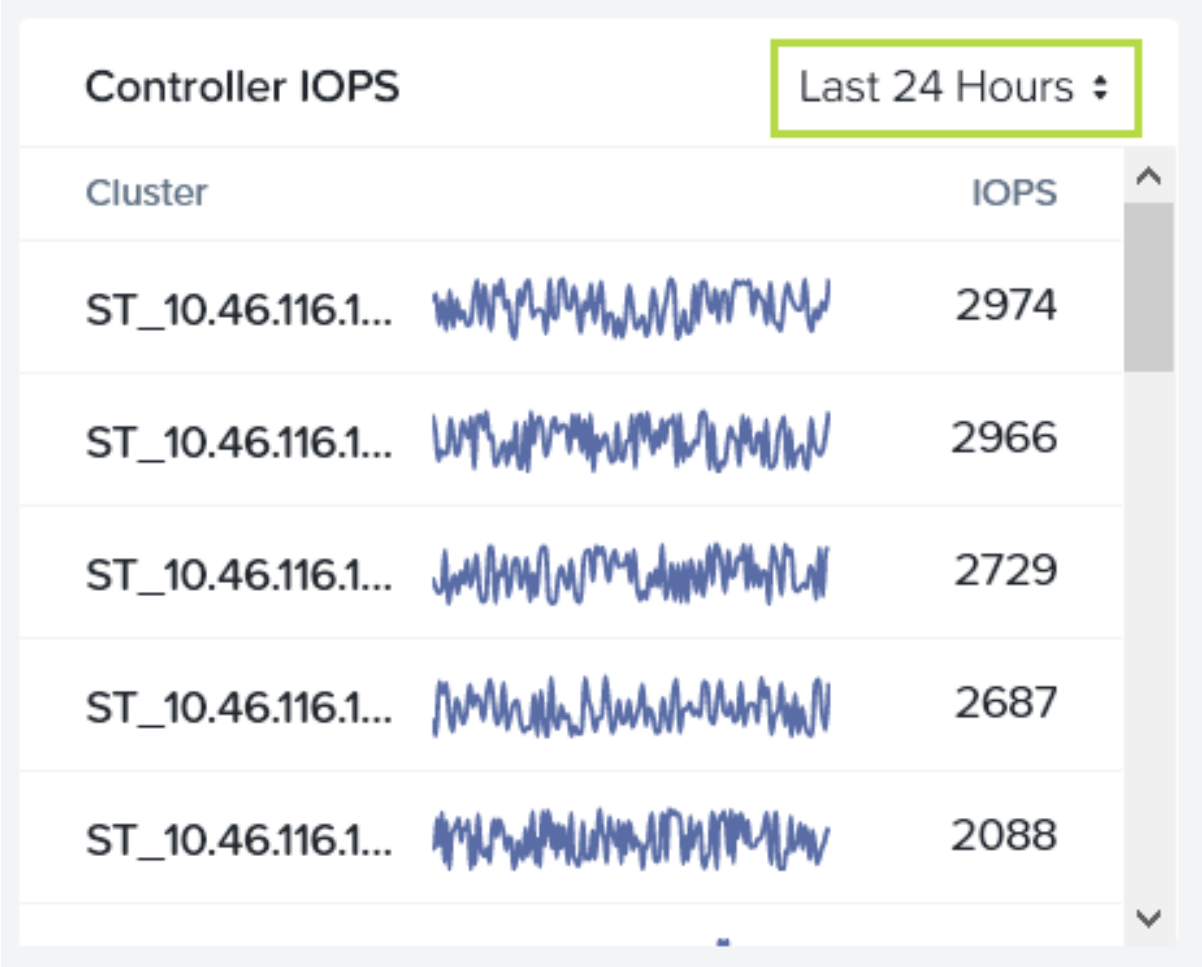


Figure 24: Sample Widget

- **Alerts**: This widget displays colored bar graph representing the alerts raised in the selected period. You can select the period on the drop down list at the top right corner of the widget. Each category of alerts is represented as a colored bar. Click any bar on the graph to see a list of the alerts represented in the bar. Click **View All Alerts** link to see all the alerts on the **Alerts** page.

  The Alerts are categorized as **Critical**, **Warning** and **Info**, and are represented as red, yellow, and blue bars respectively in the graphs.

- **Cluster Quick Access**: This widget displays a list of the clusters managed by the Prism Central. It allows you to open the Prism Element for a registered cluster in a new window when you click the name of the cluster. The cluster **Home** page appears in Prism Element. For more information about the **Home** page of Prism Central, see Prism Central Web Console Guide.

- **Cluster Storage**: This widget displays storage and resiliency information for the highest usage clusters. Each line includes the cluster name, a usage column with a bar that visually indicates how much capacity is used currently, and a data resiliency column that displays the current status (critical, warning, OK, or unknown). The cluster list is ordered by data resiliency status with critical clusters at the top of the list. Click the cluster name to see the cluster details page. Hovering the cursor over the usage bar displays a box with usage details including data reduction ratio, usage percentage, used space, total space, fault domain (disk, node, or rack), and fault tolerance level (0, 1, or 2). The data reduction ratio indicates the data savings due to data reduction techniques such as de-duplication, compression, and erasure coding. (A 1:1 ratio indicates none of these data reduction techniques are in use currently.)

- **Cluster Latency**: This widget displays the total (read and write) IO latency average for the highest latency clusters. Click *<cluster name>* to display the **Summary** page for that cluster.
- **Cluster Memory Usage**: This widget displays the percentage of total memory in use currently for the highest usage clusters. Click *<cluster name>* to display the **Summary** page for that cluster.
- **Cluster CPU Usage**: This widget displays the percentage of total CPU in use currently for the highest usage clusters (or all clusters if there are fewer than five). Click *<cluster name>* to display the **Summary** page for that cluster.
- **Controller IOPS**: This widget displays the total (read and write) controller IOPS for the highest volume clusters. Click *<cluster name>* to display the **Summary** page for that cluster. The IOPS number comes from the controller when the hypervisor is AHV or Hyper-V and from the hypervisor when the hypervisor is ESXi.
- **Cluster Runway**: This widget alerts you to potential storage, CPU, or memory resource constraints across the clusters and provides an estimated *runway* (time remaining) before the resources are maxed out based on current usage. Click *<cluster name>* to display the **Capacity** page for that cluster.
- **VM Efficiency**: This widget displays the number of VMs that are considered inefficient and are broken down by category: over-provisioned, inactive, constrained, and bully. It provides a link to the VMs dashboard. For information about these VMs, see VMs Summary View on page 95.

  For more information, see Behavioral Learning Tools information in *Intelligent Operations Guide*.
- **Plays**: This widget displays a list of plays running on the cluster. The list is categorised into completed, failed, and paused plays. The completed plays are displayed in the center widget. The number for each category is linked to the **Plays** page.
- **Tasks**: This widget displays a list of recent tasks with the current status of each task. Click the **View All Tasks(s)** link to view the **Tasks** page. For more information, see Tasks View on page 451.
- **Reports**: This widget displays a table that lists the number of total and scheduled reports with a link to the **Reports** page. For more information, see Reports Management in *Intelligent Operation Guide*.
- **Data Protection Status**: This widget displays the protection summary and recovery plans if created. If no recovery plan is created, it displays a **How to setup?** link to create a create recovery plan.
- **Security**: This widget displays the summary of **Security Dashboard**. Click the **View All Issues** link to view the **Security Dashboard** page. For more information, see Security Dashboard on page 395.

Resetting Dashboard

This section describes how to reset an existing dashboard in Prism Central.

About this task

Perform the following steps to reset a dashboard:

Procedure

1. Log in to Prism Central, and select the **Infrastructure** application from the Application Switcher Function on page 19.
   The infrastructure dashboard is displayed.
2. Click **Reset Dashboard** to reset the main dashboard to the default set of widgets.
   The system prompts you to confirm the reset dashboard action.
3. Click **OK** to confirm.
   The main dashboard is reset to default.

Setting Data Density

This section describes how to set up the data density in Prism Central.

About this task

Perform the following steps to set up the data density:

Procedure

1. Log in to Prism Central, and select the **Infrastructure** application from the Application Switcher Function on page 19.
   The infrastructure dashboard is displayed.
2. Click **Data Density** option to select the density of data representation in the widgets.
   The system prompts you to select the data density option.

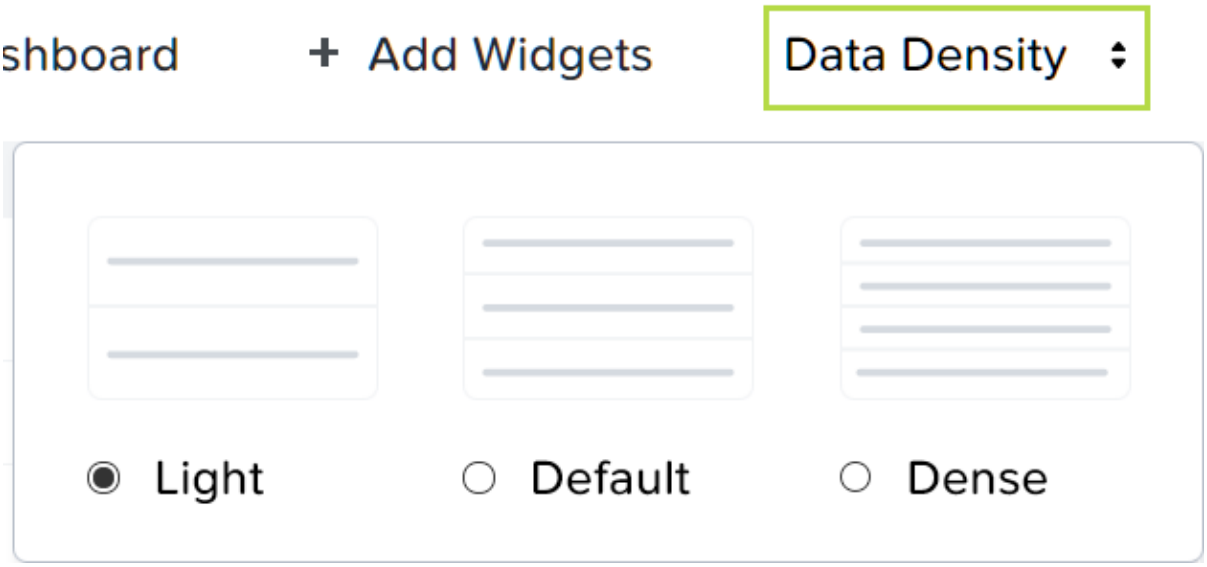


Figure 25: Data Density Options

Select one of the following three options:

Light: The information is lightly packed in the widget with more spacing between the elements.

Default: The information is moderately packed with sufficient spacing between the elements. This scheme of data density is based on user research by Nutanix.

Dense: The information is densely packed with minimal spacing between the elements for essential clarity.

Creating a New (Custom) Dashboard

About this task

The **Main Dashboard** provides a default view into the clusters, but you can add custom views by creating custom dashboards. To create a custom dashboard, do the following:

> **Note:** Creating a dashboard requires a valid NCM license. For more information, see License Manager Guide. The **Manage Dashboards** does not appear if the appropriate license is not available.

Procedure

1. Log in to Prism Central, and select the **Infrastructure** application from the Application Switcher Function on page 19.
   The infrastructure dashboard is displayed.
2. Click **Manage Dashboards**, and perform the following steps:
   a. Click **New Dashboard**.
   b. Enter a name for the dashboard in the displayed field.
   c. Click **Save**.

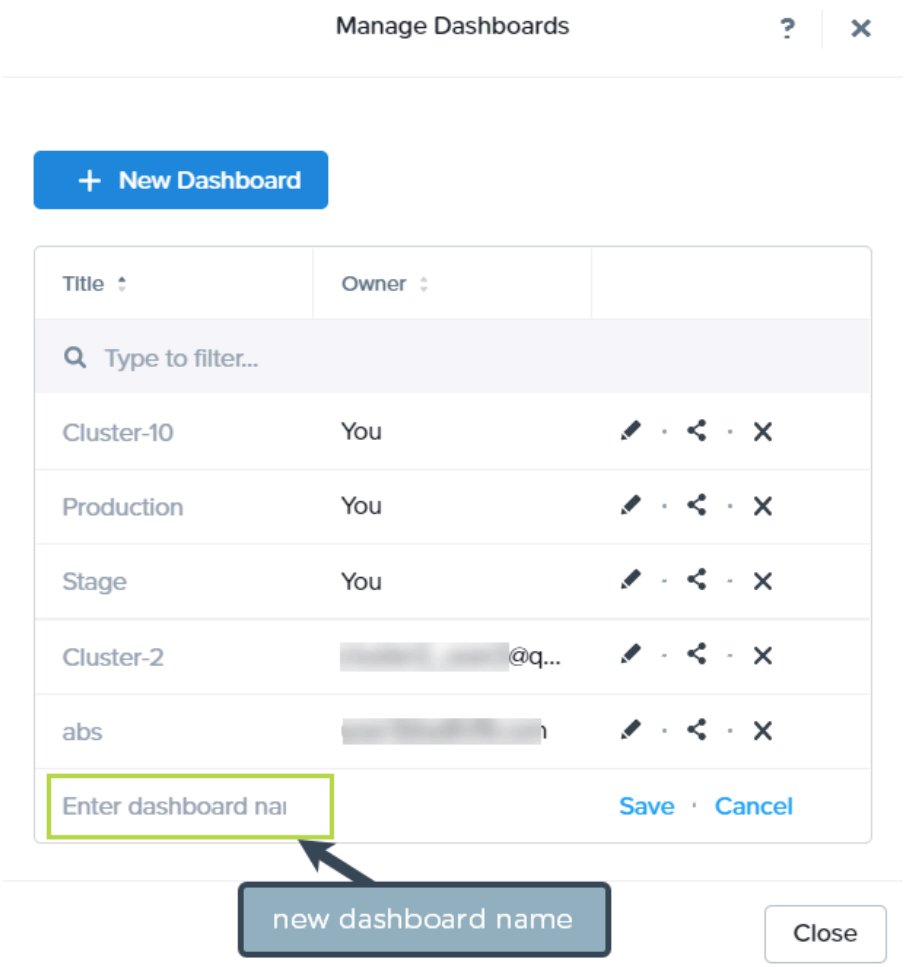


Figure 26: Manage Dashboards Windows (new dashboard)

3. Click **Close** to close the **Manage Dashboards** window.
   A new dashboard tab appears next to the **Main Dashboard** (or other custom dashboard) tab.

   Note: The new dashboard is empty (no widgets) initially.

4. Click the new dashboard tab, and then click the **Add Widgets**.
   The system displays the **Add Widgets** window.

5. In the **Add Widgets** window, select a widget and add it to the dashboard. For more information on how to add a widget, see Adding Dashboard Widgets on page 89.

   Repeat this step for all the desired widgets to be added to the new dashboard.

Modifying a Dashboard

About this task

The **Main Dashboard** provides a default view into the registered clusters, but you can customize that view at any time. To modify the Main dashboard or any other dashboard you create, do the following:

> **Note:** Customizing a dashboard requires a Prism Pro license. The **Add Widgets** and **Manage Dashboards** do not appear if Prism Pro is disabled.

Procedure

1. Log in to Prism Central, and select the **Infrastructure** application from the Application Switcher Function on page 19.
   The infrastructure dashboard is displayed.
2. Click **Main Dashboard** tab or previously added custom dashboard tab.

3. Perform either of the following operations:

   - To add a widget to the displayed **Main Dashboard** or custom dashboard, click **Add Widgets**, select a widget from the **Add Widgets** window, and add it to the **Main dashboard** or custom dashboard.

     For information about how to add a widget, see Adding Dashboard Widgets on page 89.

   - To delete a widget, click *X* in the upper right of the displayed tile. The system prompts you to confirm the delete action.

     Click **OK**. The widget disappears from the dashboard.

   - To reset the **Main Dashboard** to the default set of widgets (after you have previously added or deleted widgets), click **Reset Dashboard**. The system prompts you to confirm the reset action.

     Click **OK**. The **Main Dashboard** returns to its default view.

   - To rename a custom dashboard, perform the following steps:

     1. Click **Manage Dashboards**.
     2. Click the Edit icon for that dashboard.
     3. Enter a new name in the displayed field.
     4. Click **Save**.

   - To delete a custom dashboard, click **Manage Dashboards** and then click *X* for that dashboard. The system prompts you to confirm the delete action.

     Click **OK**. The tab for that custom dashboard disappears from the **Dashboard** page.

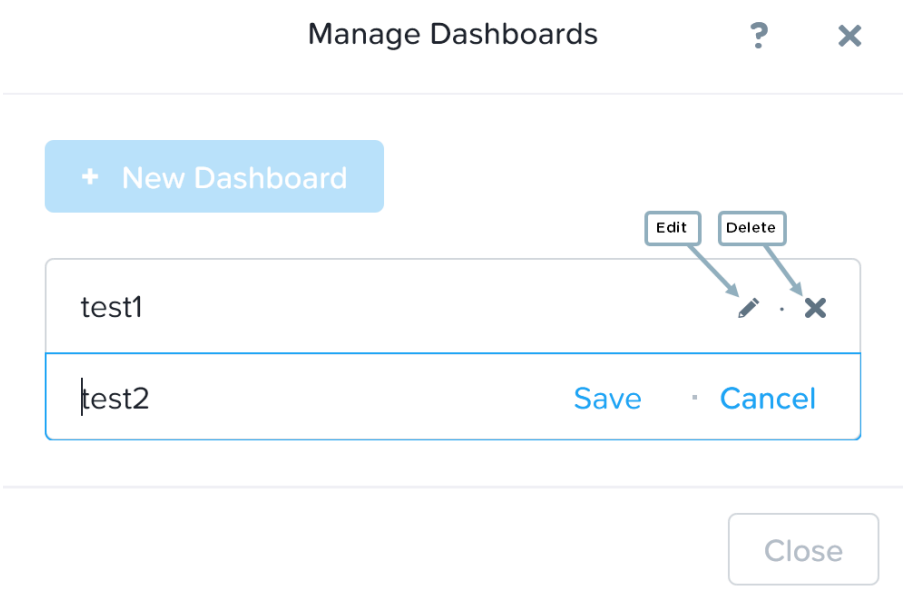


Figure 27: Manage Dashboards Window

Sharing a Dashboard

About this task

Any user with edit permission can share a custom dashboard with other users and provide view or edit access to them.

Note: Enable CMSP to use this feature.

Procedure

1. Log in to Prism Central, and select the **Infrastructure** application from the Application Switcher Function on page 19.
   The infrastructure dashboard is displayed.
2. Click **Manage Dashboard**.
   The systems displays the **Manage Dashboard** window. This window lists all the existing custom dashboards.

3. Select the custom dashboard you want to share, and click the Share icon.

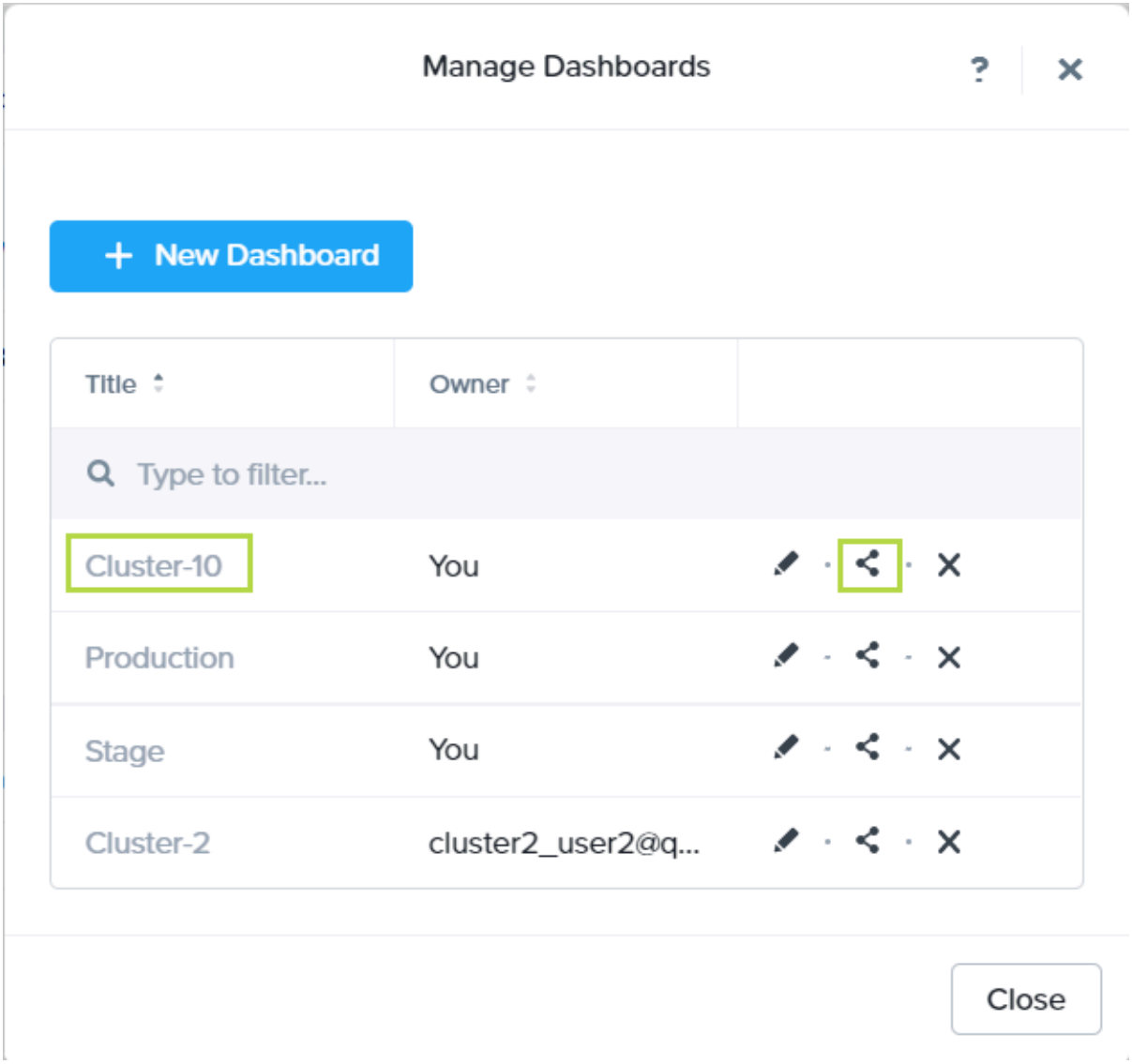


Figure 28: Manage Dashboards

The **Sharing Dashboard** window appears.

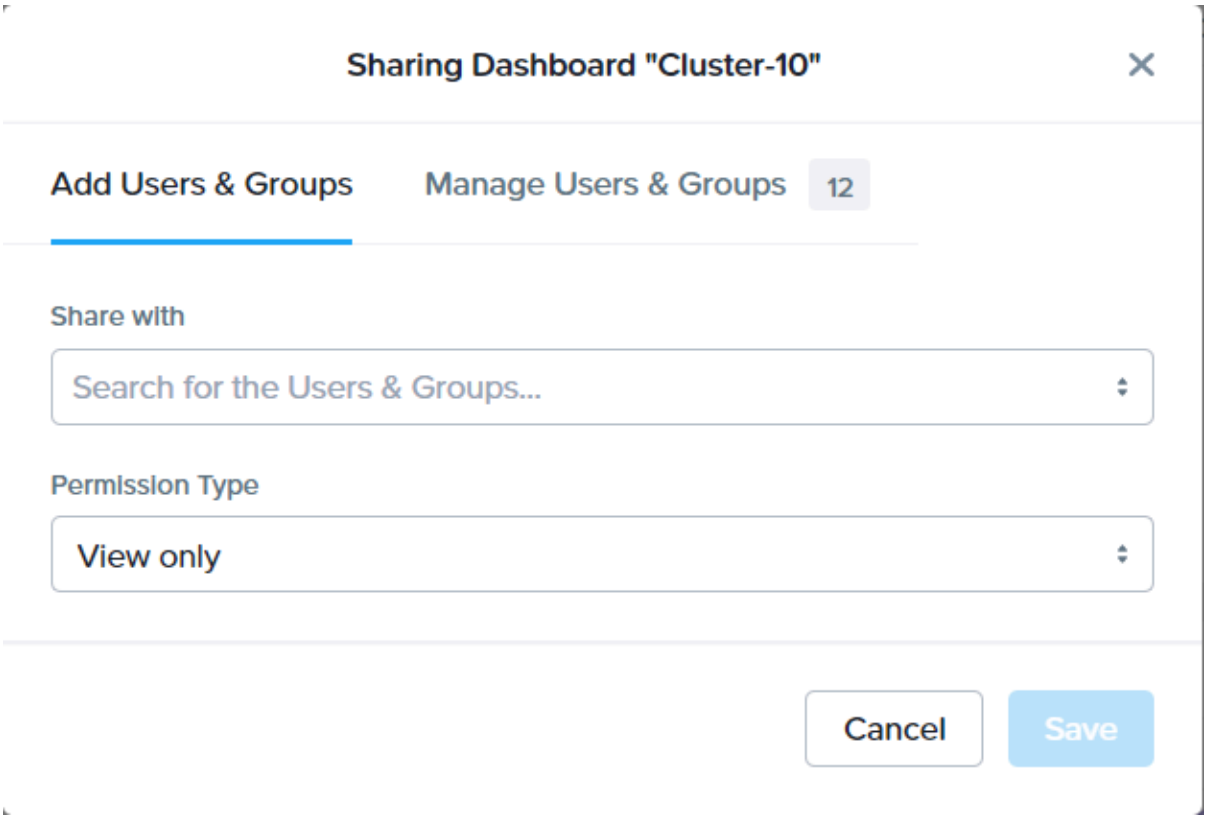


Figure 29: Sharing Dashboard

4. In the **Add Users & Groups** tab, perform the following steps:

   a. In **Share with** field, add the users or groups to share the custom dashboard. You can type a first few characters of a user or group, and as you type, a dropdown menu appears based on the typed keywords. Select the user or group to be added from the displayed list.

   > **Note:** The system also allows you to add more than one user or group.

   b. In the **Permission Type** dropdown menu, select the permission as **View only** or **Edit**.

   The system assigns the selected permission to the user or group entered in the **Share with** field.

   > **Note:**
   >
   > - Only the user with **Edit** permission can view, edit and share the custom dashboard. The user with **View only** permission can only view the custom dashboard.
   > - The **Manage Users & Groups** tab allows you to change the permission type for users or groups with whom you have shared the dashboard earlier. You can also remove the users or groups as per the requirement.

5. Click **Save**.
   A message appears that indicates the dashboard is shared successfully.

   After you share the dashboard, wait for few minutes for changes to take effect.

   > **Note:** You cannot view any information about entities in the dashboard chart without entity permissions.

Generating a Dashboard Summary Report

In Prism Central, you can monitor infrastructure widgets by visualizing the data on the dashboards. However, the data is available only in the Prism Central interface. Generating a Report feature allows you to export the infrastructure data as a report for further analysis, archival, compliance, and other purposes.

> **Note:** Generating a report requires a valid license - Prism Pro, Prism Ultimate, or any edition of NCM. For more information, see License Manager Guide. The **Generate Report** option does not appear if the appropriate license is not available.

You can generate a report in the following ways:

- Download the dashboard data as a report in PDF format or CSV format.
- Email the dashboard data as a report to the recipients in PDF format or CSV format, or both, as an attachment.
- Save the dashboard data as a report configuration to schedule, share, and export reports.

The following is an example showing the dropdown menu of the **Generate Report** option from the Main Dashboard:

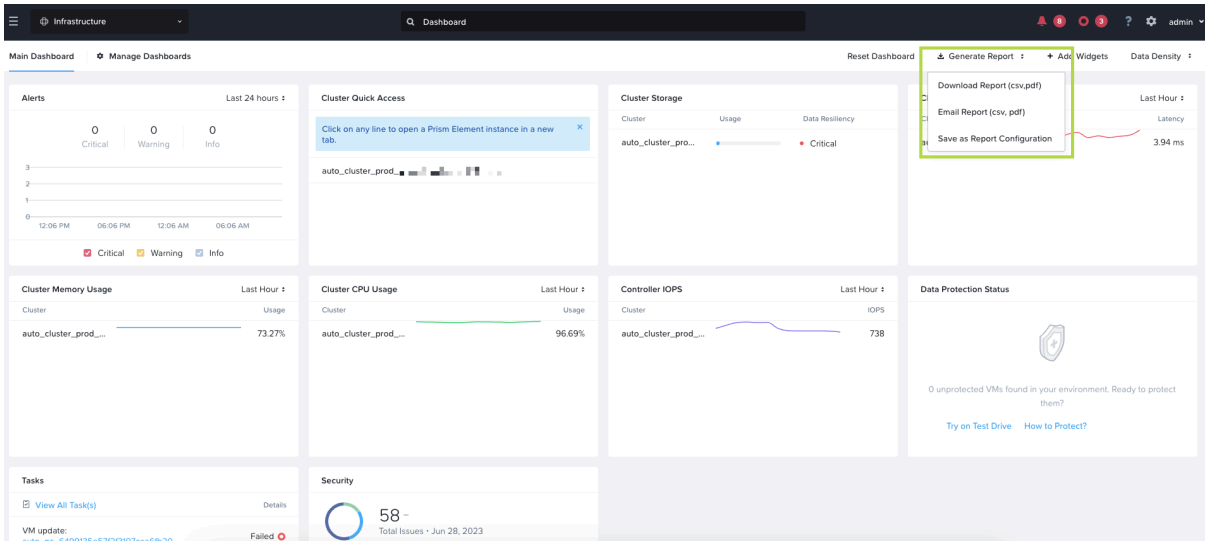


Figure 30: Main Dashboard - Generate Report Dropdown Menu

The following table describes the dropdown menu list of the **Generate Report** option:

Table 15: Generate Report Dropdown List

Options	Description
Download Report (csv, pdf)	Click this action to download the report. For more information, see Downloading a Report on page 84.
Email Report (csv, pdf)	Click this action to email the report. For more information, see Emailing a Report on page 84.

Options	Description
Save as Report Configuration	Click this action to save the report as a configuration. For more information, see Saving as a Report Configuration on page 85.

Downloading a Report

This task describes how to download the main and custom dashboard widgets data as a report, either in PDF format or CSV format.

About this task

Downloading a report has the following workflow:

- The report instance is generated in your preferred format and notified on the main and custom dashboards.
- The generated report instance is available for you to download under **Generated Reports** tab of the Reports page.

> **Important:**
>
> - You can also resend the generated report instance as an email from the **Generated Reports** tab of the Reports page. For more information, see Resending a Report Instance.
> - You must download or resend the report within 24 hours from the time you generated the report instance. After 24 hours, Prism Central removes the report instance from the **Generated Reports** tab.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from **Application Switcher** function.
   The infrastructure dashboard is displayed.
3. Click **Main Dashboard** tab or previously added custom dashboard tab.
4. Click **Generate Report**.
5. Select **Download Report (csv, pdf)** and enter the following information:
   a. **Report Name**: Enter the report name.
   b. **Report Format**: Select PDF format or CSV format.
6. Click **Download**.
   Prism Central displays a confirmation message on the dashboard screen that the report was generated.

What to do next

Select the **Intelligent Operations** application from **Application Switcher** function, and navigate to **Reports** from the **Navigation Bar**. Select **Generated Reports** tab to view and download the generated report instance. For more information, see Downloading a Report Instance.

Emailing a Report

This task describes how to email the main and custom dashboard widgets as a report.

About this task

You can email the main and custom dashboard reports as an attachment in PDF format, CSV format, or both. After you email the report, it is also available as a report instance under **Generated Reports** tab of the Reports page to resend or download the report.

> **Important:** Ensure to resend or download the report within 24 hours from the time you generated the report instance. After 24 hours, Prism Central removes the report instance from the **Generated Reports** tab.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from **Application Switcher** function.
   The infrastructure dashboard is displayed.
3. Click **Main Dashboard** tab or previously added custom dashboard tab.
4. Click **Generate Report**.
5. Select **Email Report (csv, pdf)** and enter the following information:
   a. **Recipients**: Enter the recipients (comma-separated) email address of the report.
   b. **Subject**: Enter the subject of the email.
   c. **Body**: Enter the desired text.
   d. **Report Format**: Select the **PDF** checkbox or **CSV** checkbox or both to set a report format.
6. Click **Send**.

What to do next

Select the **Intelligent Operations** application from **Application Switcher** function, and navigate to **Reports** from the **Navigation Bar**. Select **Generated Reports** tab to view and manage the generated report instance. For more information, see Managing a Report Instance from Generated Reports Tab.

Saving as a Report Configuration

This task describes how to save the main and custom dashboards data as a report configuration.

About this task

You can save the main and custom dashboards data as a report configuration. The configuration of the report that you save is available under **Configurations** tab of the Reports page to perform report management actions.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from **Application Switcher** function.
   The infrastructure dashboard is displayed.
3. Click **Main Dashboard** tab or previously added custom dashboard tab.
4. Click **Generate Report**.
5. Select **Save as Report Configuration** and enter the following information:
   - **Report Configuration Name**: Enter the report configuration name.

6. Click **Send**.

What to do next

Select the **Intelligent Operations** application from **Application Switcher** function, and navigate to **Reports** from the **Navigation Bar**. Select **Configurations** tab to view and manage the saved report configuration. For more information, see Managing a Custom Report Configuration.

Widgets Management

Widgets provides a quick access to the fault, security, and performance-related data for a cluster such as Alerts, memory usage, CPU usage, CVM IOPS, VM efficiency, Reports, Plays, canceled and succeeded Tasks, Data Protection status, and Security dashboard. Each widget provides unique information, and can be added to the dashboard based on the observation requirements.

Resize the Widgets

You can click and drag down the resize handle at the bottom of the widget to vertically resize a widget.

> **Note:** You cannot resize a widget horizontally.

The following is an example of the resize handle:

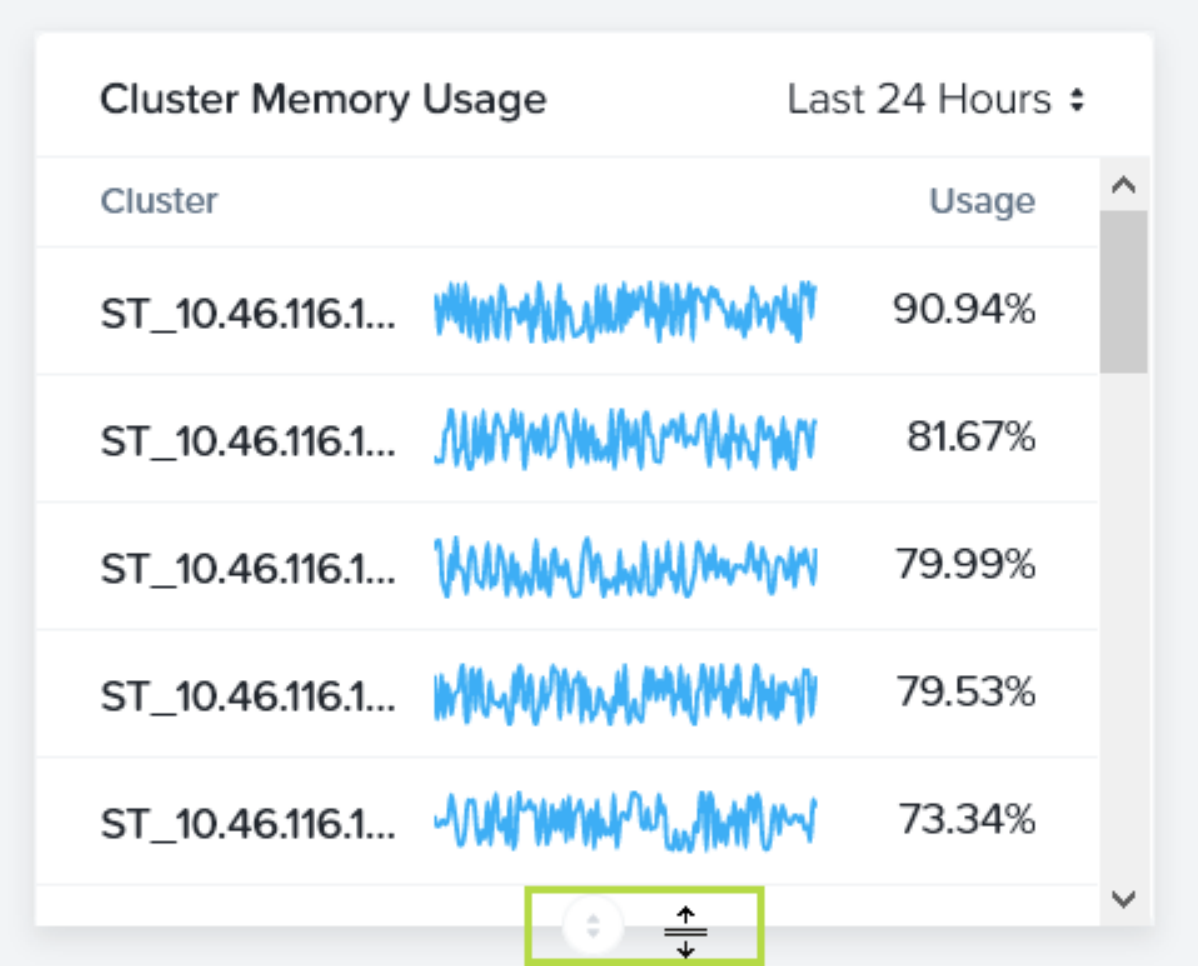


Figure 31: Vertically Resizing the Widget

When you click and drag up or down the resize handle to resize a widget, the widget placed below the resized widget shifts upward or downward.

You can resize (increase or decrease) a widget length in multiples of half of the default length of the widget, such as half, one-and-half, twice, and two-and-half times the default length. Even if you attempt to resize it in any other variation of the default length, the widget auto-sizes itself to the nearest half length.

The following is an example for widget resizing:

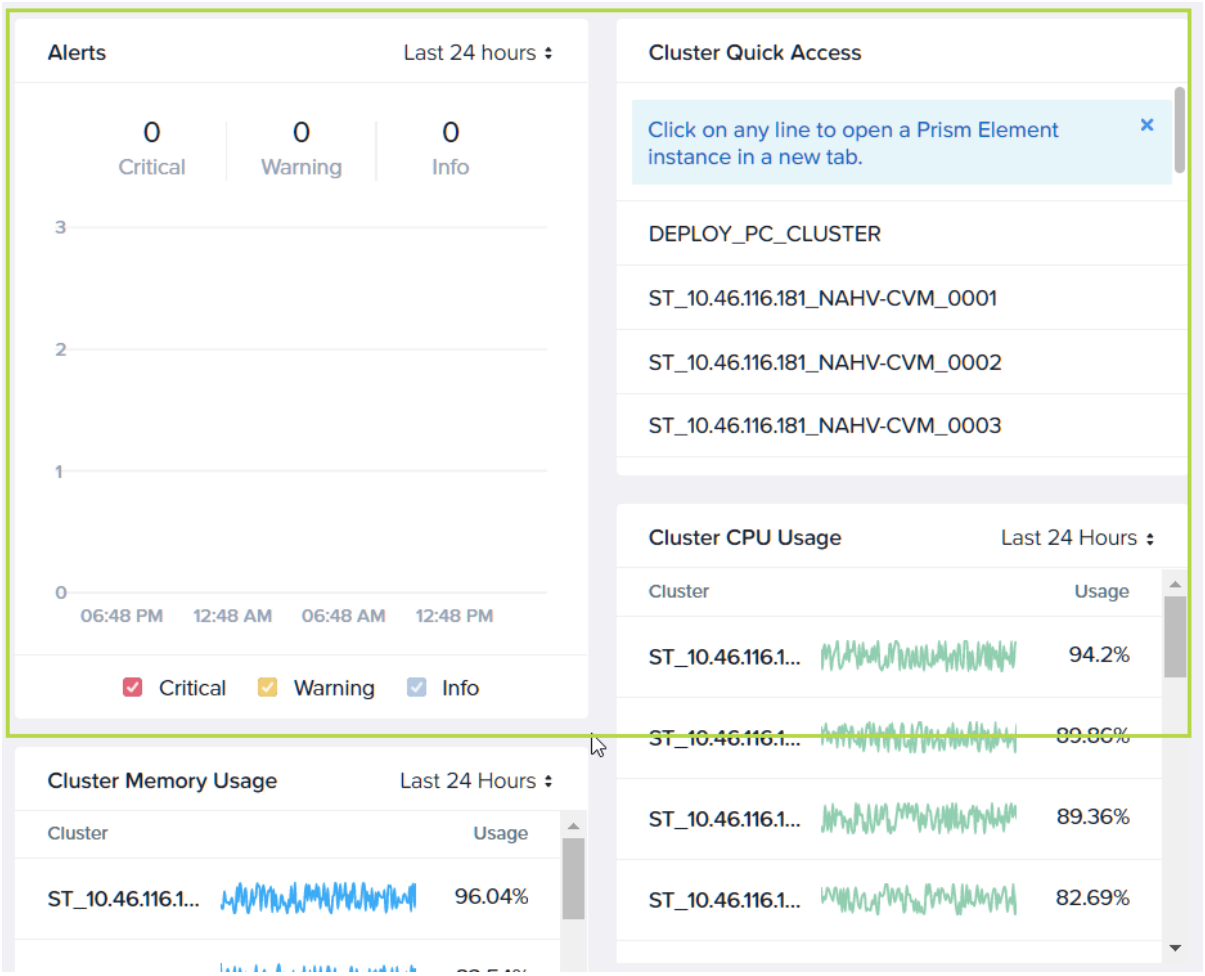


Figure 32: Widget Resize to One-and-half Times the Default Length

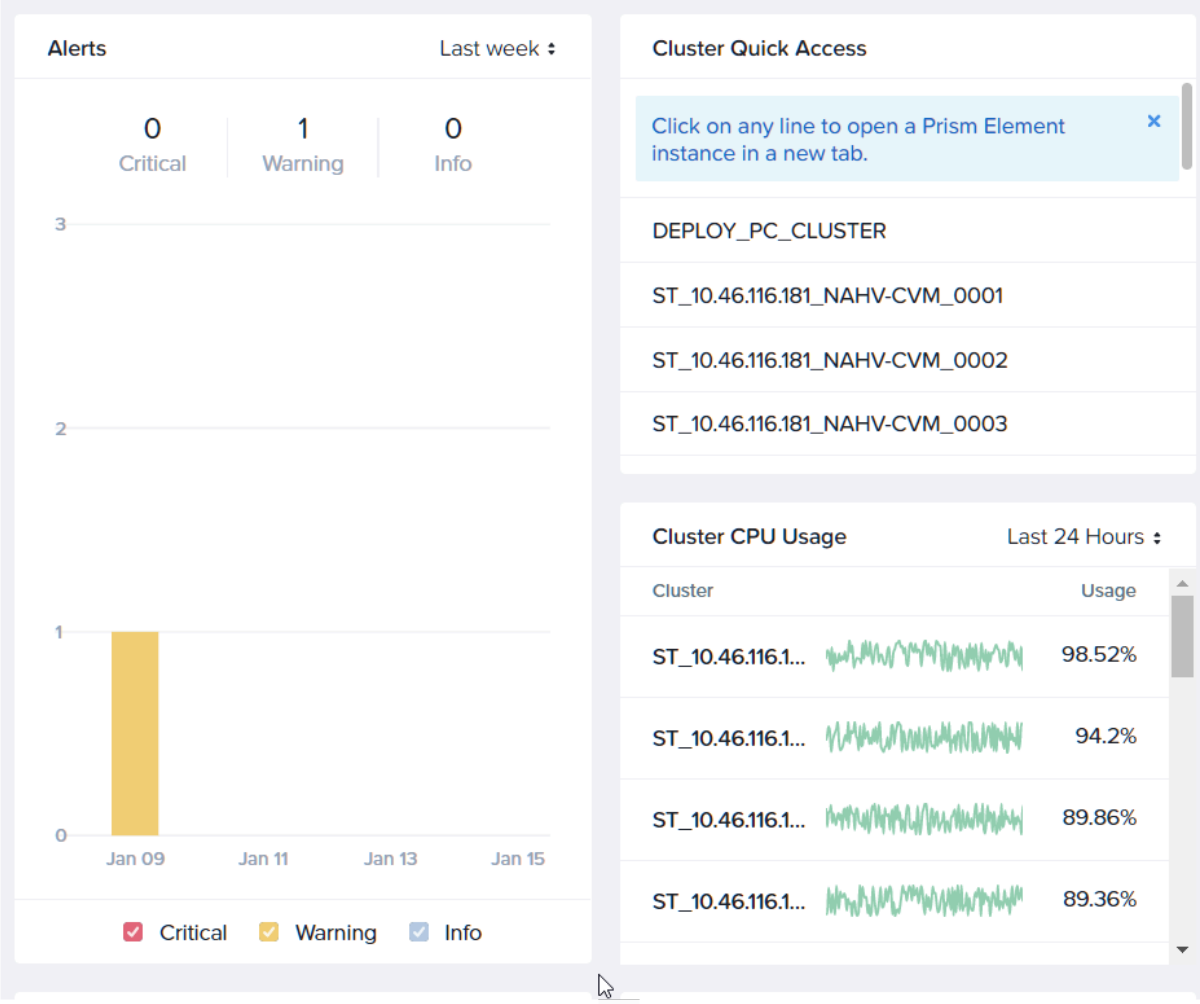


Figure 33: Widget Resize to Twice the Default Length

Drill-down or Expanding Data Elements in a Widget

You can click the data element of a widget to expand or drill-down the information presented in the widget.

Note:

- Expanding a data element in a widget is not possible in all widgets.
- In widgets that provide a list, if you select the list item or row, the system opens an entity page in Prism Central or another application such as Prism Web Console in a new browser tab. For example:
  - In the **Cluster Quick Access** widget, if you click *<cluster name>*, the system opens the Prism Element Web Console for that cluster in a new browser tab.
  - In the **Cluster Storage** widget, if you click *<cluster name>*, the system displays the cluster details view for that cluster.
- In widgets that provide numbers, if you click a number, the system opens the respective entity page in Prism Central. For example:

  In the **Reports** widget, if you click **Total Reports** or the **Scheduled Reports** number, the system displays the **Reports** page.

- In widgets that display charts, if you click the chart, the system displays an expanded or drill-down view of the chart.

  Note: If you click the entity name (such as <*cluster name*>), instead of displaying the drill-down view of the chart, the system displays the entity details page.

- The following is an example of expanding a chart in a widget.

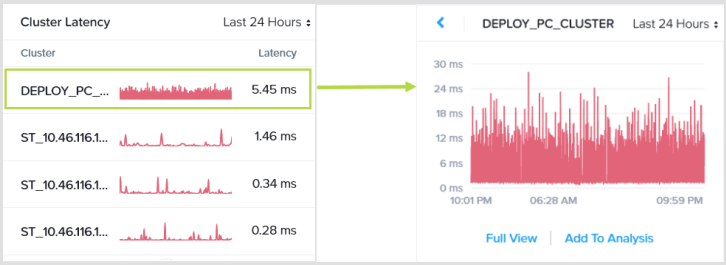


Figure 34: Widget Data Drill-down

At the bottom of the drill-down view, you can select **Full View** to open the details page of the selected entity (cluster or VM). Click **Add To Analysis** to add the chart to the **Analysis** dashboard. For more information, see Analysis Dashboard in *Intelligent Operation Guide*.

Hover Details in Drill-down Views

After you select a chart in a widget, the drill-down view of the chart is displayed. You can hover on any point on the time chart to display the parameters at that point.

In the same example as presented in the Drill-down or Expanding Data Elements in a Widget on page 88, if you hover over the chart, the sample details are displayed.

Adding Dashboard Widgets

Prism Central provides a selection of widgets that can be added to the **Main Dashboard** or a custom dashboard. Each widget provides information about a specific resource or usage topic that is displayed in a tile on the dashboard.

To add a widget to a dashboard, perform the following steps:

Note: Adding a widget to a dashboard requires a Prism Pro license. The **Add Widgets** does not appear if Prism Pro is disabled.

1. Log in to Prism Central, and select **Infrastructure** application from Application Switcher Function on page 19. The infrastructure dashboard is displayed.
2. In the **Main Dashboard** or custom dashboard, click **Add Widgets**.
3. In the **Add Widgets** window, select the desired widget from the left column.

   Note: To find a widget, enter the name in the search field. The system displays a preview of the selected widget.

4. Enter values for the configurable parameters in the right column.

   Note: The parameters vary by widget; some widgets do not have any configurable parameters.

5. Click **Add to Dashboard** (or **Add & Return to Dashboard**) to add the widget to the dashboard.

The following table describes the widgets that you can add to the **Main dashboard**:

Table 16: Widget Parameters

Widget	Description	Parameter	Values
Custom Widgets			
Custom Alerts Widget	Displays a custom list of alerts.	**Widget Name**: Enter a name for the widget. A name (which you can keep or overwrite) is provided after selecting the other options.	(user entered name or settings-based name)
		Select a Cluster: Select the cluster(s) to monitor from the dropdown menu. The default is all clusters.	All Clusters, <cluster name>
		Choose Size: Select the size (width/height dimensions) of the widget. The default is 1 x 1.	1 x 1, 2 x 1, 2 x 2, 2 x 3, 2 x 4, 4 x 4
		Severity. The default is critical.	Critical, Warning, Info
		Entity: Select the entity of interest. The default is cluster.	Cluster, Storage, VM, Hardware, DR
Top Lists Widget	Displays a list of the top performers for a selected metric.	**Widget Name**: Enter a name for the widget that you can keep or overwrite.	(user entered name or settings-based name)
		Select a Cluster: Select the cluster(s) to monitor from the dropdown menu. The default is all clusters.	All Clusters, <cluster name>
		Choose Size: Select the size (width/height dimensions) of the widget. The default is 2 x 1.	2 x 1, 2 x 2, 2 x 3
		Entity: Select the entity of interest. The default is host.	host, VM
		Metric: Select the metric of interest. The default is IOPS.	IOPS, Memory Usage, CPU Usage, Bandwidth, Latency
Custom Chart Widget	Displays a performance graph for a selected entity and metric pair.	**Widget Name**: Enter a name for the widget. The default is *New Chart Widget*.	(name)
		Entity Type: The default is host.	Host, Disk, Storage Pool, Storage Container, Virtual Machine, Virtual Disk

Widget	Description	Parameter	Values
		Entity: There is no default value. The system displays the list of entity items based on the **Entity Type** field.	(entity name)
		Metric: There is no default value. For information about metrics available for the selected entity item, see the information available in **Metrics Tab** section of that individual entity . For example, for VM-related metrics information, see **Metrics Tab**section in VMs Summary View on page 95 and VM Details View on page 108.	(metric name)
Cluster Info Widget	Displays cluster summary information about alerts, anomalies, runway, and inefficient VMs.	**Widget Name**: Enter a name for the widget. The default is *New Widget*.	(n/a)
		Select a Cluster: Select the target cluster from the dropdown menu.	(registered cluster names)
Virtual Infrastructure Widgets: These widget appears on the **Main dashboard** by default. For details, see Main Dashboard - Infrastructure on page 71.			
VM Efficiency	Displays the number of overprovisioned, inactive, constrained, and bully VMs in the cluster with links to the details.	(no customizable parameters)	(n/a)
Storage Over-provisioning	Displays the configured threshold for storage over-provisioning	Storage Over-provisioning Ratio	
Hardware Widgets: All these widgets (except **Impacted Cluster** and **Performance**) appear on the Main dashboard by default. For details, see Main Dashboard - Infrastructure on page 71.			
Cluster CPU Usage	Displays the percentage of total CPU in use currently for the highest usage clusters.	(no customizable parameters)	(n/a)
Cluster Latency	Displays the total (read and write) IO latency average for the highest latency clusters.	(no customizable parameters)	(n/a)
Cluster Memory Usage	Displays the percentage of total memory in use currently for the highest usage clusters.	(no customizable parameters)	(n/a)

Widget	Description	Parameter	Values
Cluster Quick Access	Displays a list of registered clusters. Health and alert icons appear for each cluster. Clicking the cluster line opens Prism (element) for that cluster in a separate tab or window.	(no customizable parameters)	(n/a)
Cluster Runway	Displays storage, CPU, and memory runway estimates (time remaining before the resource reaches capacity). For more information, see Capacity Runway Summary View in *Intelligent Operation Guide*.	(no customizable parameters)	(n/a)
Cluster Storage	Displays storage statistics for the highest usage clusters.	(no customizable parameters)	(n/a)
Controller IOPS	Displays the total (read and write) controller IOPS for the highest volume clusters.	(no customizable parameters)	(n/a)
Impacted Cluster	Displays information about any clusters that are impacted (performance, capacity, or other potential issues) and may need attention.	(no customizable parameters)	(n/a)
Performance	Displays latency, bandwidth, and IOPS statistics for the highest usage clusters.	(no customizable parameters)	(n/a)
Alerts	Displays colored bar graph that represents the alerts raised in the period selected. Click **View All Alerts** link to see all the alerts on the **Alerts** page. For more information about the alerts generated in Prism Central, see Prism Central Alerts and Events Reference Guide.	(no customizable parameters)	(n/a)
Activity Widgets: The **Tasks** widget appears on the **Main Dashboard** by default. For more information, see Main Dashboard - Infrastructure on page 71.			
Tasks	Displays a list of recent tasks with the current status of each task and a link to the **Tasks** page.	(no customizable parameters)	(n/a)

Widget	Description	Parameter	Values
Discovered Apps	Displays the number of applications discovered in a specified set of monitored clusters. Click the **App instances** number to display the application discovery page. Click the **Identified** or **Unidentified** number to display the application discovery page filtered for that condition. This widget displays the discovered apps information only if you enable App Discovery.	(no customizable parameters)	(n/a)
Operations Widgets: These widgets appear on the **Main Dashboard** by default. For more information, see Main Dashboard - Infrastructure on page 71.			
Plays	Displays a list of the Plays running on the cluster. The list is categorised into completed, failed and paused plays. The completed plays are displayed in the center widget. The number for each category is linked to the **Plays** page.	(no customizable parameters)	(n/a)
Reports	Displays a table that lists the number of total and scheduled reports with a link to the **Reports** page.	(no customizable parameters)	(n/a)
Nutanix Disaster Recovery Widgets: These widgets appear on the **Main Dashboard** by default. For more information, see Main Dashboard - Infrastructure on page 71.			
Data Discovery Status	Displays the Protection summary and recovery plans if created. If no recovery plan is created, it displays a **How to setup?** link to create a create recovery plan.	(no customizable parameters)	(n/a)
Security Widgets: These widgets appear on the **Main Dashboard** by default. For more information, see Main Dashboard - Infrastructure on page 71.			
Security	Displays the summary of **Security Dashboard**. Select the **View All Issues** link to view the **Security Dashboard** page. For more information, see Security Dashboard on page 395.	(no customizable parameters)	(n/a)

COMPUTE AND STORAGE ENTITIES

You can access the following entity items from the **Compute and Storage** entity of the **Infrastructure** application:

- VMs (see VM Management on page 94)
- Templates (see VM Template Management on page 188)
- Kubernetes Clusters (see Kubernetes Clusters Management on page 202)
- OVAs (see OVA Management on page 214)
- Images (see Image Management on page 238)
- Catalog Items (see Catalog Management on page 262)
- Storage Containers (see Limitations for Storage Containers on page 290)
- Volume Groups (see Volume Group Management on page 300)
- vCenter Datastores (see External vCenter Server Integration on page 326)

For information about how to access the entities items available in **Compute and Storage** entities, see Application-specific Navigation Bar on page 57.

VM Management

You can perform the following actions to manage a VM from Prism Central:

- Create and manage VMs directly from Prism Central when the hypervisor is either ESXi or AHV. For more information, see the following sections:
  - Creating a VM through Prism Central (ESXi) on page 161.
  - Managing a VM through Prism Central (ESXi) on page 165.
  - Creating a VM through Prism Central (AHV) on page 121.
  - Managing a VM through Prism Central (AHV) on page 134.
- Create and manage a VM from Prism Central using Prism Self Service. For more information, see the following sections:
  - Creating a VM (Self Service) on page 521.
  - Managing a VM (Self Service) on page 528.
  - Creating a VM from Catalog Items (Self Service) on page 521

  For more information about Prism Self service setup, see Prism Self Service Setup on page 519.
- Add multiple vGPUs to the same VM, and perform a live migration of vGPU-enabled VMs within or outside the cluster. For more information, see the following sections:
  - Adding Multiple vGPUs to the Same VM on page 147
  - Live Migration of vGPU-enabled VMs on page 154
- Export VM as an OVA. For more information, see Exporting a VM as an OVA on page 218.
- Manage NGT. For more information, see Nutanix Guest Tools Overview on page 166.

- Define the QoS for Storage. For more information, see Storage Quality of Service (QoS) on page 186.
- Perform Memory Overcommit for new and existing VMs. For more information, see Memory Overcommit Management on page 188.
- Define Affinity and NGT Policies for VM Management. For more information, see Policies for VM Management on page 188.

VMs Summary View

The **Summary** tab on the **VMs** page provides a dashboard of all the VMs across registered clusters.

To access the summary view of all VMs, perform the following steps:

1. Log in to the Prism Central web console.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment.
3. Click the **Summary** tab.

   The system displays the **Summary** view of all the VMs across registered clusters:

> **Note:** To access the summary view of all the non-nutanix VMs that are managed by an external *vCenter*, select **Non-Nutanix** environment from the dropdown menu in the **VMs** page.
>
> The **Summary**, **Alerts**, and **Events** tabs display the same information as for Nutanix-managed VMs. The **Metrics** tab displays a subset of the full list (10 of the 12 metrics). The **List** tab displays fields for name, node name, hypervisor, memory, IP addresses, power state, and cluster name. While displaying the VM name, vCenter encodes any special characters included in the VM name to utf-8.
>
> Using playbooks, you can manage the VMs in **Non-Nutanix** environment. For more information about playbooks, see Task Automation - Playbooks in *Intelligent Operations Guide*.

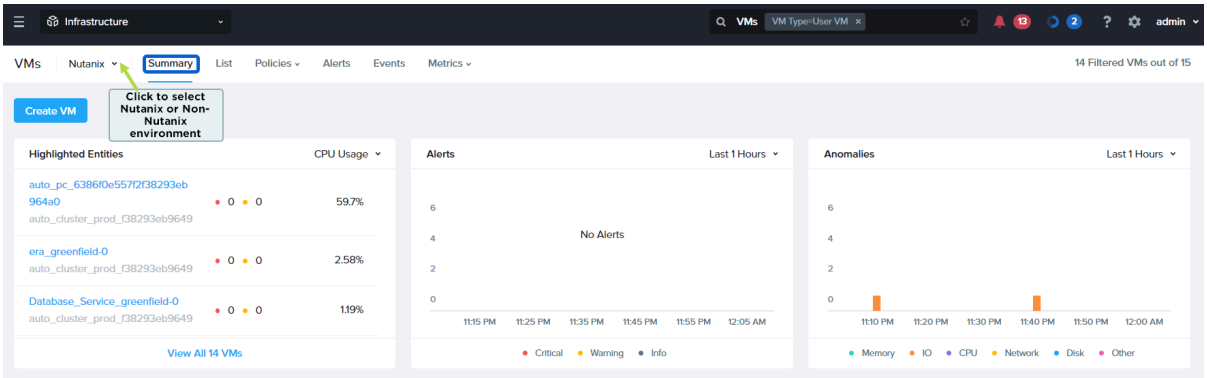


Figure 35: Summary View - All VMs

The **VMs** page includes six tabs on the left (**Summary**, **List**, **Policies**, **Alerts**, **Events**, and **Metrics**) with a display area below the selected tab.

> **Note:** This section describes the information and options that appear in the **Summary** page for all VMs. For instructions on how to view and organize that information in various ways, see Prism Central GUI Organization on page 27.

The **Summary** tab for all VMs displays the following three widgets:

- **Highlighted Entities**: Displays a list of the VMs with the highest usage of the *<parameter>* you select from the dropdown menu on the right of the widget. The *<parameter>* involves **CPU Usage**, **IO Latency**, **Memory Usage**, and **IOPS**. Click **View All XX VMs** link at the bottom to display the **List** tab.
- **Alerts**: Displays a list of VM-related alerts that are generated during the specified *<interval>* you select from the dropdown menu on the right of the widget. The *<interval>* involves **Last week**(default), **Last 24 hours**, and **Last 1 hour**. When an alert appears, you can click the graph to view a list of those alerts. Click any alert to display the details page for that alert.
- **Anomalies**: Displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified *<interval>* you select from the dropdown menu on the right of the widget. The *<interval>* involves **Last week** (default), **Last 24 hours**, and **Last 1 hour**. When an anomaly appears, you can click the graph to view a list of those anomalies. Click any anomaly to display the event page for that anomaly.

List Tab

The **List** tab displays the list of VMs across all registered clusters.

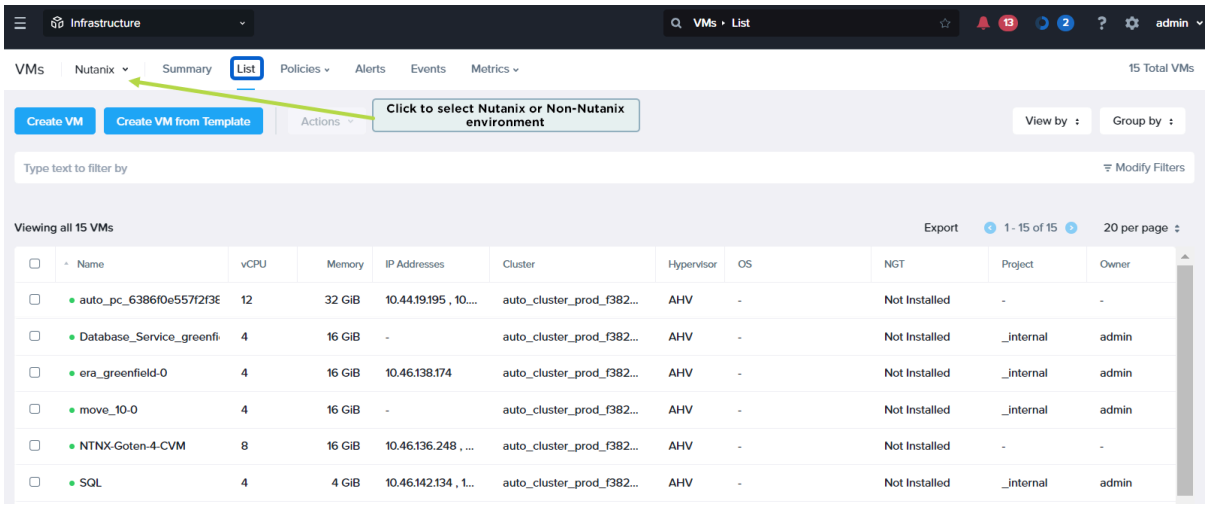


Figure 36: VMs List Tab

The following table describes the fields that appear in the VMs **List** tab.

> **Note:** The fields vary based on the **View by** and **Group by** options. A dash (-) is displayed in a field when a value is not available or applicable. For more information about **View by** and **Group by** options, see Prism Central GUI Organization on page 27.

Table 17: VMs List Tab - Field Description

Field	Description	Values
Select **General** from **View by** option.		
Name	Displays the VM name. You can click the VM name to view the detailed information for that VM. For information about VM details view, see VM Details View on page 108.	(VM name)

Field	Description	Values
vCPU	Displays the virtual CPU count of the VM.	(vCPU count)
Memory	Displays the total amount of memory available to this VM.	xxx [MB|GiB]
IP addresses	Displays one or more VM IP addresses.	(IP address)
Cluster	Displays the name of the cluster in which the VM resides.	(cluster name)
Hypervisor	Displays the hypervisor type on which the VM is running.	AHV, ESX, or Hyper-V
OS	Displays the guest operating system of the VM.	(OS)
NGT	Displays whether Nutanix Guest Tools is installed on the VM.	Installed, Not Installed
Project	Displays the name of the project to which this VM belongs.	(project name)
Owner	Displays the owner (user name) of this VM.	(user name)
Select **Performance** from **View by** option.		
Name	Displays the VM name.	(VM name)
Memory Overcommit	Displays the Memory Overcommit state of the VM.	Enabled / Disabled
Memory Usage	Displays the percentage of allocated memory capacity currently being used by this VM.	0 -100%
CPU Usage	Displays the percentage of allocated CPU currently being used by this VM	0 -100%
Read IOPS	Displays read I/O operations per second (IOPS) for this VM.	(number)
Write IOPS	Displays write I/O operations per second for this VM.	(number)
IO Bandwidth	Displays I/O bandwidth used per second for this VM.	xxx [MBps|KBps]
IO Latency	Displays the average I/O latency for this VM.	xxx [ms]
Cluster	Displays the name of the cluster in which the VM resides.	(cluster name)
Select **Anomalous Behavior** from **View by** option.		
Name	Displays the VM name.	(VM name)
Anomaly Count	Displays the Anomaly count for Memory, I/O, CPU, Network, and Disks	(Integer number)
Anomaly Disabled	Displays whether Anomaly reporting is Disabled.	Yes/No
Select **Efficiency** from **View by** option.		
Name	Displays the VM name.	(VM name)

Field	Description	Values
Efficiency	Displays the assessed efficiency of the VM. If a VM is performing in an expected range, the efficiency is listed as *Good*. If not, the type of inefficiency is displayed as determined by the VM behavioral learning engine. For more information, see Behavioral Learning Tools in *Intelligent Operations Guide*.	Good, Constrained, Overprovisioned, Inactive, Bully; (*NA* if insufficient baseline data for categorization, which is typically 21 days)
Reason	Displays the reason why a VM is considered inefficient. A dash (-) appears for a *Good* VM.	(text message)
Project	Displays the name of the project to which this VM belongs.	(project name)
Owner	Displays the owner (user name) of this VM.	(user name)
Cluster	Displays the name of the cluster in which the VM resides.	(cluster name)
Select **GPU** from **View by** option.		
Name	Displays the VM name.	(VM name)
GPU Configuration	Displays the GPU board (in case of Passthrough mode), vGPU software, type and number of vGPU instances in brackets (in case you configured the vGPU mode).	(GPU board/software-type name) Example: Passthrough - Nvidia Tesla M60 Example: vGPU - Nvidia GRID M60-8Q (2)
GPU Type	Displays the GPU configuration made as Passthrough or vGPU or if you did not configure GPU then a dash (-) appears.	[Passthrough|vGPU|-]
GPU Usage	Displays the percentage of GPU capacity being used by the VM.	(percentage)
GPU Framebuffer Usage	Displays the percentage of GPU framebuffer (RAM) capacity being used by the VM.	(percentage)
Select **Data Protection** from **View by** option.		
Name	Displays the VM name. You can click the VM name to view the detailed information for that VM. For information about VM details view, see VM Details View on page 108.	(VM name)
Categories	Displays the category mapped to the VM. For information about categories in Prism Central, see Category Management on page 454.	String (Category name)
Consistency Group	Displays the consistency group of the VM. For information about Consistency Groups in Prism Central, see Consistency Groups information in *Nutanix Disaster Recovery Guide* .	(Yes/No)
Protection Status	Displays the Protection Status of the VM.	(Protected/Unprotected)

Field	Description	Values
Sync Status	Indicates the VM synchronization status between the Availability Zones in the Disaster Recovery setup.	(Sync Status)
Protection Type	Displays the type of protection defined for the VM.	(Protection Policy/ Legacy Protection Domain)
Protection Policy	Displays the protection policy that is applicable for the VM. For more information about protection policies, see Nutanix Disaster Recovery Guide.	(String) Protection Policy Name
Recovery Plans	Displays the recovery plans that is applicable for the VM. For more information about VM recovery plans, see Nutanix Disaster Recovery Guide.	(String) Recovery Plans Name
Select **Storage Configuration** from **View by** option.		
Name	Displays the VM name.	(VM name)
Replication Factor	Displays the Replication Factor setting for the VM in the storage policy applied to the VM.	Inherit from Container or 2 or 3
Encryption	Displays the Encryption setting for the VM in the storage policy applied to the VM.	Enabled or Inherit from Cluster
Compression	Displays the Compression setting for the VM in the storage policy applied to the VM.	Inline or Post Process (if enabled) , Disabled or Inherit from Cluster
Throttled Throughput (IOPS)	Displays the throttled throughput value in terms of IOPS set for the VM in the storage policy applied to the VM.	(Integer number)
Throttled Throughput (MB/s)	Displays the throttled throughput value in terms of MB/s set for the VM in the storage policy applied to the VM.	(Integer number)
Associated Policy	Displays the name of the storage policy applied to the VM.	(String) Storage Policy Name

Field	Description	Values
Compliance State	Displays the compliance state of the VM based on realization of the storage policy applied to the VM. **Note:** The compliance state is displayed as **In Progress** until the extent groups are synchronized by the Curator service at full scan intervals. Full scan intervals are intervals of 6 hours. Depending up on the time elapsed in the full scan interval at the time when the Replication Factor was set or updated, it may take up to 6 hours for the **In Progress** state to change to **Compliant** or **Non Compliant**.	**In Progress**, **Compliant** or **Non Compliant**
Cluster	Displays the name of the cluster that the VM resides in.	(String) Cluster Name
Select **Add custom** from **View by** option.		
Acropolis VM	Displays whether the VM is running on the AHV host.	(Yes/No)
Anomalies (Last 24 hours)	Displays the sum of all the anomaly counts for 20 metrics such as memory, I/O, CPU, network, and disks in the last 24 hours.	(Integer number)
AZ Name	Displays the availability zone specified to the VM.	AZ name
Cluster UUID	Displays the UUID of the cluster in which the VM resides.	(cluster UUID)
Constrained Level	Displays the VM constrained level along with the metric that constrains the VM.	“high”:”memory”, “moderate”:cpu” or “high”:”cpu”, “moderate”:memory”
Controller IOPS	Displays the total (read and write) I/O operations per second (IOPS) for the VM.	(Integer number)
Controller Read IO Bandwidth	Displays the read I/O bandwidth of the VM.	(Integer number (KBps))
Controller Read I/O Latency	Displays the read I/O latency of the VM.	(Integer number (ms))
Controller Write IO Bandwidth	Displays the write I/O bandwidth of the VM.	(Integer number (KBps))
Controller Write IO Latency	Displays the write I/O latency of the VM.	(Integer number (ms))
Created Timestamp	Displays the date and time of VM creation.	(date and time), Timestamp in MM DD, YYYY, hh: mm AM/PM format. For example, Oct 27, 2023, 06:51 AM
Description	Displays the description specified for the VM.	(description text)

Field	Description	Values
Disk Capacity	Displays the total disk capacity of the VM.	(Integer number (GiB))
Disk Usage	Displays the disk usage percentage for the VM.	(0 - 100%)
Disk Usage Bytes	Displays the amount of used disk space.	(Integer number (GiB))
Efficiency Detail	Displays the reason why a VM is considered inefficient.	(text message)
Health	Displays the health state of the VM.	(Critical/Warning/Good)
Host	Displays the host name. This field might be blank if the VM is powered off and a host is not assigned.	(hostname)
Host IP	Displays the host IP address.	(IP address)
Host UUID	Displays the UUID of the host.	(host UUID)
Hypervisor IOPS	Displays the total (read and write) I/O operations per second (IOPS) from the hypervisor for the VM.	(Integer number)
IS CVM	Displays whether the VM is a CVM or not.	(Yes/No)
Network Adapters	Displays the number of network adapters in the VM.	(Integer number)
Network Rx Bytes	Displays the number of bytes received from the network.	(Integer number)
Network Rx Packets Dropped	Displays number of packets received from the network and dropped.	(Integer number)
Network Tx Packets Dropped	Displays number of packets sent to the network and dropped.	(Integer number)
NGT communication status	Displays the NGT communication status between CVM and guest VMs. For more information, see Nutanix Guest Agent and Controller VM Communication on page 182.	(Active/Inactive)
NGT communication type	Displays the transport channel established between CVM and guest VMs. For more information, see Verifying Communication Type Using Prism Central on page 184.	(IP-based/IP-less)
NGT Installed Version	Displays if NGT is installed in the VM. For more information, see Installing NGT on page 169.	(Installed/Not Installed/ Latest)
Overprovisioned	Displays the type of over-provisioned VMs. **Note:** This and the following field filters based on a VM efficiency algorithm, which is part of the VM behavioral learning capabilities (see Behavioral Learning Tools).	(Good/High/Moderate)
Overprovisioned level	Displays the VM overprovisioned level along with the metric that overprovisions the VM.	“high”:”memory”, “moderate”:cpu” or “high”:”cpu”, “moderate”:memory”

Field	Description	Values
Power State	Displays whether the VM is powered off or powered on.	(Off/On)
Services Enabled	Displays the name of the NGT services enabled in the VM.	(file_level_restore, vss_snapshot)
Shared Usage	Displays the shared data usage by the VM.	(Integer number (GiB))
Snapshot Usage	Displays the amount of storage used for snapshots.	(Integer number (GiB))
Total Working Set Size	Displays the total working set size of the VM. Working set is the amount of memory that a VM requires in a given time interval.	(Integer number (GiB/MiB))
Virtual NICS	Displays the name of the virtual NIC that allows the VM to connect to a network	(NIC name)
VM Type	Displays the type of VM.	(Guest, PCVM, MSP, AFS)
VPC Name	Displays the VPC Name specified for the VM.	(VPC name)
Working Set Size Read	Displays the read working set size of the VM.	(Integer number (GiB/MiB))
Working Set Size Write	Displays the write working set size of the VM.	(Integer number (GiB/MiB))

You can perform the following actions for the VMs in the **List** tab:

- Access the detailed information about an individual VM. For more information, see VM Details View on page 108.
- Filter the VMs list based on available parameter values using **Filters** pane. For more information, see Filters Pane - VMs Page on page 103.
- Export the table that contains the list of VMs and their information to a file in a CSV format. For more information, see Export on page 32.
- Group the VMs based on pre-defined criteria. For information about how to group the VMs, see Group by on page 29.
- View VMs based on pre-defined criteria or create a custom view. For information about available views and how to create a custom view, see View by on page 29.
- Assign a label to the filtered criteria. For information about how to define a label, see Label on page 32.
- Create a VM. For more information about how to create a VM, see Creating a VM through Prism Central (AHV) on page 121 or Creating a VM through Prism Central (ESXi) on page 161.
- Perform the VM-specific actions on a single or multiple VMs using the **Actions** dropdown menu. For instructions on how to perform these actions, see Managing a VM through Prism Central (AHV) on page 134 or Managing a VM through Prism Central (ESXi) on page 165.

  Note: The available actions appear in bold; other actions are grayed out. For grayed out options, a tool tip explaining the reason is provided. The available actions depend on the current state of the selected VM(s).

Filters Pane - VMs Page

The following table describes the fields available in the **Filters** pane:

Table 18: Filter Pane Fields

Parameter	Description	Values
Labels	Filters based on label name. Select one or more labels from the **Labels** dropdown menu. If there are no labels currently, the system displays a message about how to create labels.	(label names)
Name	Filters based on the VM name. Select a condition from the dropdown menu and enter a string in the field. The system returns a list of VMs that satisfy the VM name condition/string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	(VM name string)
Description	Filters based on the description specified for the VM. Enter a string in the field to filter the result. The system returns a list of VMs that satisfy the description string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	(Description string)
IP Addresses	Filters based on the IP address specified for the VM. Enter a valid IP address in the field to filter the result. The system returns a list of VMs that satisfy the IP address string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	(A Valid IP Address)
VPC Name	Filters based on the VPC Name specified for the VM. Enter a string in the field to filter the result. The system returns a list of VMs that satisfy the VPC string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	(VPC name string)
Host	Filters based on the host name. Select a condition from the dropdown menu and enter a string in the field. The system returns a list of VMs that satisfy the host name condition/string.	(host name string)

Parameter	Description	Values
Cluster	Filters based on the cluster name. Select a condition from the dropdown menu and enter a string in the field. The system returns a list of VMs that satisfy the cluster name condition/string.	(cluster name string)
Categories	Filters based on category names. Enter a category name in the field and then check the box. As you type a dropdown menu appear to help you select the correct category. A new field appears where you can add more categories to the filter. The number of VMs tagged to each selected category are displayed in the **List** tab.	(category name)
Quarantined	Filters based on the Quarantined mechanism. Select either **Strict** or **Forensics** or both the checkboxes. The system displays the number of VMs currently quarantined as Strict or Forensics.	Strict, Forensics
Hypervisor	Filters based on the hypervisor type. Select one or more of the checkboxes to filter on those hypervisors. The system displays the number of VMs currently on each hypervisor type.	AHV, ESX, Hyper-V
Health	Filters based on the VM health state (good, warning, or critical). Select one or more states to return a list of VMs in that state(s). The system displays the number of VMs currently in each state.	Critical, Warning, Good
Nutanix Guest Tools	Filters based on the NGT status. Select one or more NGT status to return a list of VMs with selected NGT status. For more information on **Nutanix Guest Tools** filters, see Installing NGT on page 169.	Installed, SSR, VSS, VSS and SSR, Not installed
Power State	Filters based on the VM power state. Select one or more states to return a list of VMs in that state(s). The system displays the number of VMs currently in each state.	On, Off, Suspended, Paused, Unknown
Is CVM	Filters based on the whether the VM is a CVM or not. The system displays the number of CVMs, if filter selected is **Yes**.	No, Yes
VM Type	Filters based on the type of VM. Select either Guest, PCVM, MSP, AFS or multiple checkboxes. The system displays the number of VMs of each type.	Guest, PCVM, MSP, AFS
Memory Overcommit	Filters based on the Memory Overcommit status. Select one or more Memory Overcommit status to return a list of VMs with selected status.	Enabled, Disabled, Not Available
Memory Usage	Filters based on the amount of memory capacity being used. Select the checkbox(es) for the desired percentage range or enter a percentage range in the ***from <low> to <high> %*** field. The system returns a list of VMs utilizing memory in that range.	([xx] to [yy]% range)

Parameter	Description	Values
CPU Usage	Filters based on the processor usage. Select the checkbox(es) for the desired percentage range or enter a percentage range in the ***From <low> to <high> %*** field. The system returns a list of VMs utilizing memory in that range.	([xx] to [yy]% range)
Read IOPS	Filters based on the read IOPS. Select the checkbox(es) for the desired range or enter a range in the ***From <low> to <high> IOPS*** field. The system returns a list of VMs with read IOPS in that range.	([xx] to [yy] IOPS range)
Write IOPS	Filters based on the write IOPS. Select the checkbox(es) for the desired range or enter a range in the ***From <low> to <high> IOPS*** field. The system returns a list of VMs with write IOPS in that range.	([xx] to [yy] IOPS range)
I/O Bandwidth	Filters based on the I/O bandwidth used. Select the checkbox(es) for the desired range or enter a range in the ***From <low> to <high> Mbps*** field. The system returns a list of VMs with I/O bandwidth usage in that range.	([xx] to [yy] Mbps range)
I/O Latency	Filters based on the average I/O latency. Select the checkbox(es) for the desired range or enter a range in the ***From <low> to <high> ms*** field. The system returns a list of VMs with average I/O latency in that range.	([xx] to [yy] ms range)
Over Provisioned	Filters for over-provisioned VMs. Select the checkbox(es) for the desired type (high and moderate). **Note:** This and the following two fields filter based on a VM efficiency algorithm, which is part of the VM behavioral learning capabilities. For more information, see Behavioral Learning Tools in *Intelligent Operations Guide*.	High, Moderate
Constrained	Filters for constrained VMs. Select the checkbox(es) for the desired type (high and moderate).	High, Moderate
Efficiency	Filters for certain VM profiles. Check the boxes for the desired profile types. There is one for efficient VMs (good) and four for inefficient VMs (bully, over-provisioned, constrained, and inactive).	Bully, Over Provisioned, Constrained, Inactive VM, Good
GPU Configuration	Filters for GPU configuration information such as model name. Enter the GPU configuration information in the field and then select the checkbox. As you type, a dropdown menu appears to help you select the correct configuration information.	(configuration info)

Parameter	Description	Values
GPU Type	Filters based on GPU operational mode. Select the checkbox for one or more of the GPU types.	vGPU, Passthrough, Passthrough(Compute)
vCPU	Filters based on the number of vCPUs allocated to the VM. Select one or more numeric checkboxes to return a list of VMs with selected number of vCPUs.	vCPU Integer value
GPU Usage	Filters based on the amount of GPU capacity being used. Enter a percentage range in the ***from <low> to <high> %*** field. The system returns a list of GPUs in that range.	([xx] to [yy]% range)
GPU Framebuffer Usage	Filters based on the amount of GPU framebuffer (RAM) capacity being used. Enter a percentage range in the ***from <low> to <high> %*** field. The system returns a list of GPUs in that range.	([xx] to [yy]% range)
Storage Configuration	Filters based on the storage policy configuration parameters set for VM. This view displays the storage configurations parameters set for the VMs by storage policies applied to the VMs. For more information about storage policies, see Storage Policies Summary View on page 500.	Storage policy name
vGPU Guest driver Version	Filters on the guest driver version. Enter the guest driver version number in the field.	(guest driver version number)
AZ Name	Filters based on the availability zone specified of the VM. Enter a string in the field to filter the result. The system returns a list of VMs that satisfy the AZ string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	AZ String
NGT Communication Status	Filters based on the NGT communication status between CVM and guest VMs. Select the communication status to filter the result. The system returns a list of VMs that satisfy the selected status.	Active, Inactive
NGT Communication Type	Filters based on the transport channel established between CVM and guest VMs. Select the required transport channel checkbox to filter the result. The system returns a list of VMs that satisfy the selected transport channel.	IP-Less, IP-Based

Policies Tab

The **Policies** tab displays **Affinity Policies** and **NGT Policies**.

For more information about how to configure **Affinity Policies** and **NGT Policies** see Affinity Policies Defined in Prism Central on page 461 and NGT Policies on page 472.

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options that are available on the **Activity** > **Alerts** page, however it only displays the VM-related alerts across the

registered clusters. For more information about alerts, see Prism Central Alerts and Events Reference Guide.

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options that are available on the **Activity** > **Events** page, however it only displays the VM-related events across the registered clusters. For more information about events, see Prism Central Alerts and Events Reference Guide.

Metrics Tab

The **Metrics** tab allows you to view performance metrics across the VMs. Click the **Metrics** tab to display dropdown menu of available metrics, and select the metric name to display the relevant performance information.

> **Note:** The **Metrics** dropdown menu is hypervisor-specific, and might vary based on the hypervisors used in the cluster.

The following table describes the dropdown menu list of the **Metrics** tab:

Table 19: Metrics Tab Fields

Metric	Description
CPU Usage	Displays a CPU usage table that lists the current values and total VMs (number). The current values are split into percentile intervals (for example, less than 25%, 25-50, 50-75, more than 75%). You can click a percentile interval to view the **Summary** tab filtered with selected VMs. **Note:** The same format also applies to the other metrics in this table with either percentile or quantity intervals.
CPU Ready Time	Displays a CPU ready time percentage usage table.
Memory Usage	Displays a memory percentage usage table.
Memory Swap	Displays memory swap-out and swap-in rate tables.
IOPS	Displays total, read, and write IOPS tables.
IO Latency	Displays total, read, and write I/O latency rate tables.
I/O Bandwidth	Displays total, read, and write I/O bandwidth rate tables.
Storage Usage	Displays total, snapshot, and shared storage size tables.
Working Set Size	Displays total, write, and read working set size tables. Working set is the amount of memory that a VM requires in a given time interval.
Network Packets Dropped	Displays tables for the number of transmitted and received packets dropped.
Network Bytes	Displays tables for the amount of transmitted and received bytes (in GiB).

Metric	Description
Disk Usage	Displays a disk usage table that lists the current values and total VMs (number). The current values are split into percentile intervals, for example, l3.68% - 4.1%, more than 4.93%. Click a percentile interval to display the **Summary** tab filtered to just those VMs. **Note:** The same format also applies to the other metrics in this table with either percentile or quantity intervals.

VM Details View

To access the details view of an individual VM, perform the following steps:

1. Log in to the Prism Central web console.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment. For information about how to access the list of VMs in **Non-Nutanix** environment (non-nutanix VMs managed by external *vCenter*), see VMs Summary View on page 95.
3. Click the target <*VM_Name*> to view the **Summary** tab of an individual VM.

   Note: Replace <*VM_Name*> with the actual VM name at your site.

The following is an example showing the **Summary** tab of an individual VM:

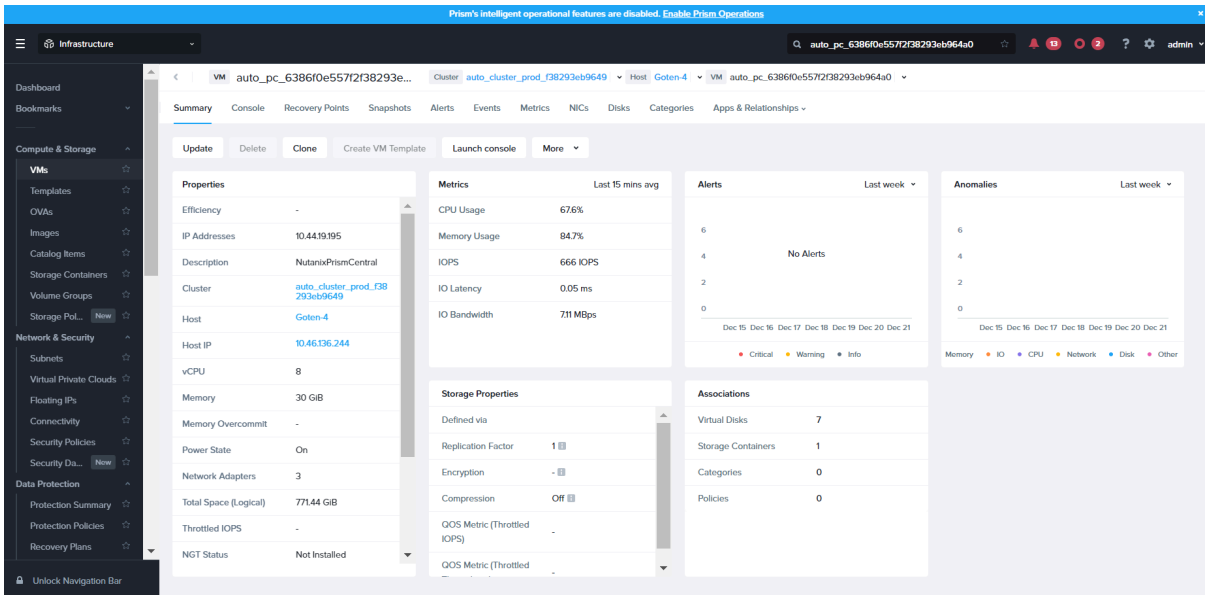


Figure 37: Summary Tab - Individual VM

Note: VirtIO must be installed in a VM for AHV to display correct VM memory statistics. For more information about VirtIO drivers, see Nutanix VirtIO for Windows in *AHV Administration Guide*.

The **Summary** tab of an individual VM provides the following widgets:

- **Properties**: Displays summary information about the VM. For information about the fields available in **Properties** widget, see Properties Widget - Parameter Details on page 109.
- **Alert**: Displays a list of related alerts that occurred during the specified interval. Select either **Last week** (default), **Last 1 hour**, or **Last 24 hours** from the dropdown menu on the top right corner of the widget.
- **Anomalies**: Displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified interval. Select either **Last week** (default), **Last 1 hour**, or **Last 24 hours** from the dropdown menu on the top right corner of the widget. When an anomaly appears, you can click the graph to display a list of those anomalies. If you click an individual anomaly, the system displays the event page for that anomaly.
- **Storage Properties** : Displays the storage properties of the VM as defined in the storage policy associated with the VM. The storage properties involve the actual values for Replication Factor, Encryption, and Compression that is applied to the VM. For information about the fields available in **Storage Properties** widget, see Storage Properties Widget - Parameter Details on page 111.
- **Associations**: Displays the other entities associated with the VM such as Virtual Disks, Storage Containers, Categories and policies (storage policies). For information about the fields available in **Associations** widget, see Associations Widget - Parameter Details on page 112.

  Note: In the **Storage Properties** widget, for any storage property, even if the "i" symbol specifies **Inherited from Cluster**, but the **Association** widget always displays the actual inherited values.

  The following is an example showing the VM Storage Properties and Associations Widget:

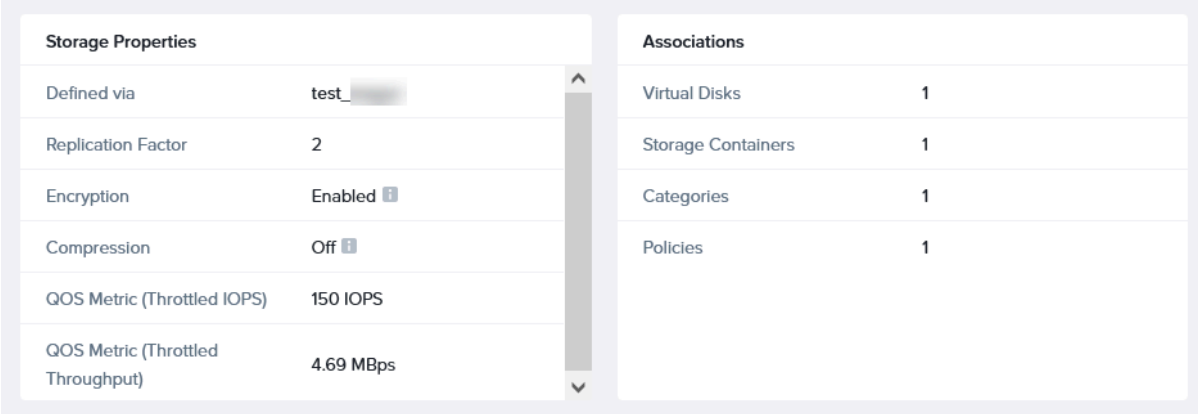


Figure 38: VM Storage Properties and Associations Widget

<*Action*> available above the widgets and under **More** dropdown menu. Click the appropriate <*Action*> to run that administrative action on the VM. The available <*Action*> appear in bold, and the other actions are grayed out. The available actions depend on the current state of the VM. For more information about how to perform any <*Action*>, see Managing a VM through Prism Central (AHV) on page 134.

Note: You can perform administrative actions on VMs in Acropolis-managed clusters only.

Properties Widget - Parameter Details

The following table describes the fields available in the **Properties** widget.

Note: A dash (-) in a field indicates that there is not enough data to evaluate or a value is not assigned.

Table 20: VM Properties - Parameter Details

Parameter	Description	Values
Efficiency	Displays the efficiency state for this VM. If the efficiency is not good, an additional field may appear that specifies the problem. For example, if the VM is constrained, a Constrained field appears that identifies the constrained resource such as the CPU or memory. **Note:** The Anomalies, Efficiency, Over provisioned, and Constrained parameters relate to the VM behavioral learning feature. For more information, see Behavioral Learning Tools in *Intelligent Operations Guide*.	Bully, Over Provisioned, Constrained, Inactive VM, Good
IP Addresses	Displays one or more IP addresses assigned to the VM.	(IP address)
Description	Displays the description specified for the VM	*<Description Text>*
Cluster	Displays the name of the cluster in which the VM resides.	(cluster name)
Host	Displays the host name. This field may be blank if the VM is powered off and a host is not assigned.	(host name)
Host IP	Displays the host IP address.	(IP address)
vCPU	Displays the number of virtual CPUs assigned to this VM.	(number)
Memory	Displays the amount of memory available to this VM.	xxx [MB|GB]
Memory Overcommit	Displays whether Memory Overcommit is enabled or disabled. For more information on Memory Overcommit feature, see Memory Overcommit	Enabled -
Power State	Displays whether the VM is powered on or powered off	On, Off
Network Adapters	Displays the number of network adapters available to this VM.	(# of adapter ports)
Total Space (Logical)	Displays the total disk capacity available to this VM.	xxx [GB|TB]
Throttled IOPS	Displays the throttled throughput value in IOPS. For more information about Throttled IOPS, see Storage Quality of Service (QoS) on page 186.	-
NGT Status	Displays if NGT is installed	Installed, Not Installed, Latest
Services Enabled	Displays the services enabled for this VM.	*<Services>* such as NCM Self-Service (formerly known as Calm), Karbon, and so on.

Parameter	Description	Values
NGT	Displays the NGT version installed on the VM	*<NGT version>* such as 21.5
NGT Cluster Version	Displays the NGT version available on the cluster	*<NGT version>* such as 21.5
Owner	Displays the VM owner name.	admin (if VM is created by Prism Central admin user.
Project	Displays the name of the project to which the VM is mapped.	*<Project Name>* such as *_Internal*for projects created by admin user.
(the following fields appear when the VM is allocated to a GPU)		
GPU Type	Displays the GPU operational mode. If it is vGPU, the following fields also appear.	vGPU, Passthrough, None
GPU Configuration	Displays the vGPU profile used.	(vGPU profile name)
Framebuffer	Displays the size of the GPU framebuffer (RAM).	xxx GiB
Virtual Slice	Displays the virtual slice applied. The "virtual slice" reflects the approximate amount of physical GPU resources that the vGPU can receive. **Note:** The Virtual Slice and vGPU Guest Driver Version fields do not appear for passthrough GPUs.	(slice amount)
vGPU Guest Driver Version	Displays the version number of the vGPU guest driver.	(version number)

Storage Properties Widget - Parameter Details

The following table describes the fields available in the **Storage Properties** widget.

Note: A dash (-) in a field indicates that there is not enough data to evaluate or a value is not assigned. For more information about the Storage properties, see Storage Policy Details View on page 503.

Table 21: Storage Properties Widget - Parameter Details

Parameter	Description	Values
Defined via	Displays the name of the storage policy that the VM is associated with.	Storage policy name
Replication Factor	Displays the Replication Factor setting for the VM in the storage policy applied to the VM.	Inherit from Container or 2 or 3

Parameter	Description	Values
Encryption	Displays the status of encryption that the storage policy applies to the VM.	Enabled or Inherit from Cluster
Compression	Displays the status and type of compression that the storage policy applies to the VM.	Inline, Post Process, Off or Inherit from Cluster
QOS Metric (Throttled IOPS)	Displays the type of QOS metric that the storage policy applies to the VM with the throttled throughput value in IOPS.	(Integer) IOPS
QOS Metric (Throttled Throughput)	Displays the type of QOS metric that the storage policy applies to the VM with the throttled throughput value in MBps.	(Integer) MBps

Associations Widget - Parameter Details

The following table describes the fields available in the **Associations** widget.

> **Note:** A dash (-) in a field indicates that there is not enough data to evaluate or a value is not assigned.

Table 22: Associations Fields

Parameter	Description	Values
Virtual Disks	Displays the number of virtual disks associated with the VM.	(number)
Storage Containers	Displays the number of storage containers associated with the VM.	(number)
Categories	Displays the number of categories associated with the VM.	(number)
Policies	Displays the number of policies like storage policies and Image Placement policies that are associated with the VM.	(number)

Entity Relationship Information

The entity relationship involves relationship between related entities like clusters, hosts, and VMs instances. It allows quick access between the related entities. You can directly navigate to a target cluster, host, or VM instance through the respective dropdown menus.

Example: Displaying Relationship between Entities

The following example indicates that VM *auto_pc_611cd08373101ab68d756c9a0* resides on host *cool-07-2* and cluster *auto_cluster_prod_rohan_bajaj_1ab68d756c98*.

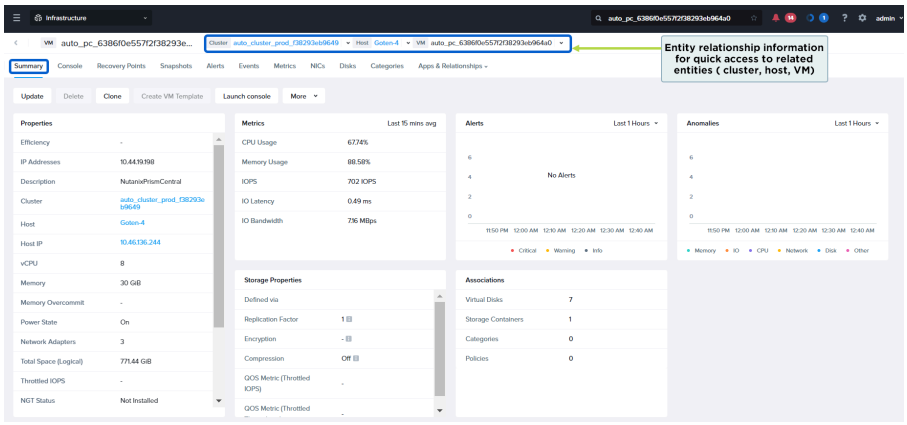


Figure 39: VM Summary: Entity Relationship Information

Example: Viewing VMs on a Cluster

Click the **VM** dropdown menu to view the list of VM instances in the selected cluster. Alternatively, you search the VM instance name residing on the target cluster.

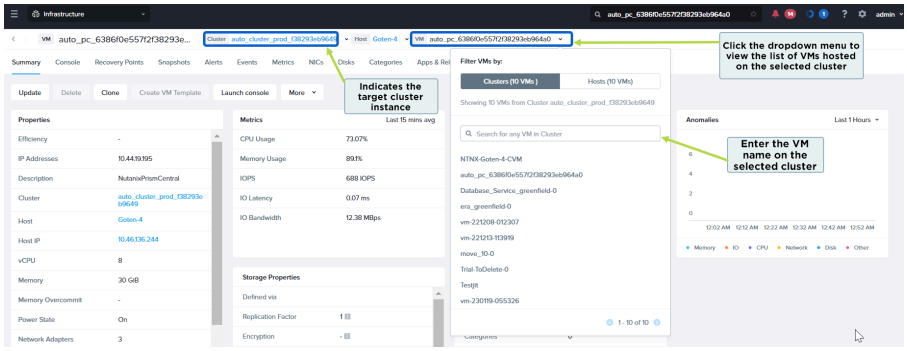


Figure 40: VMs on a Cluster

Example: Viewing VM Instances on a Host

Click the **VM** dropdown menu to view the list of VM instances on the selected host. Alternatively, you can search the VM instance name belonging to the target host.

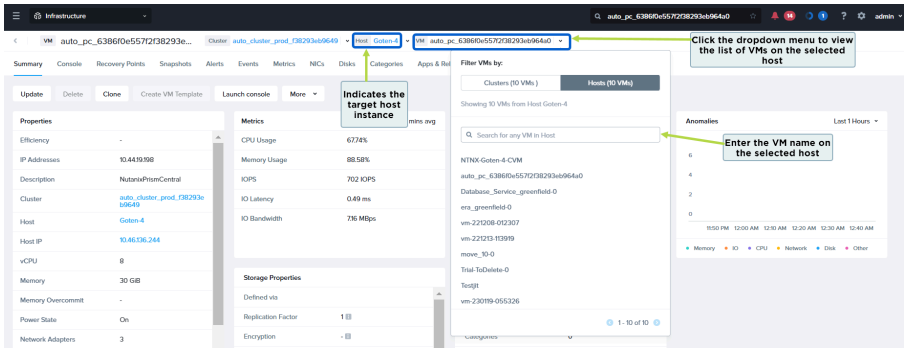


Figure 41: VMs on a Host

Note:

- The **Recent** label indicates the last accessed entity instances. The system displays a maximum of three recently accessed entity instances.
- The filtered list of VMs display only the powered-on VM instances.
- If the VMs are not filtered on a host instance, all VMs on the selected cluster are displayed.

Console Tab

The **Console** tab displays the VM console screen. There are three icons available on the top right corner of the console screen).

- Click the Reboot icon to send a **Control-Alt-Delete** command to the console.
- Click the Screenshot-capture icon to take a screen shot of the console display.
- Click the Launch icon to open the console in a new window.

Recovery Points Tab

The **Recovery Points** tab displays a list of recovery points (backup snapshots) when recovery points are created for the selected VM.

For information about how to create a recovery point, see Managing a VM through Prism Central (AHV) on page 134.

The protection policy associated with the VM also creates the VM recovery points for Disaster Recovery. For more information about VM recovery points, see Nutanix Disaster Recovery Guide.

The list is blank if there are no recovery points available. The total number of recovery points and the latest and oldest recovery points are listed on the left. A list of all recovery points appears in a table on the right with the create time, location, expiry time, and recovery point type provided for each recovery point.

You can restore or replicate a VM from a recovery point. Select the recovery point and click the required action from the **Actions** menu:

- Click **Clone** to create a new cloned VM from the selected recovery point.
- Click **Replicate** to replicate a VM from the selected recovery point either locally or remotely in a state of a chosen recovery point.
- Click **Restore** to restore the VM from the selected recovery point.
- Click **Delete** to delete the recovery point.

Snapshots Tab

The **Snapshots** tab displays information in tabular form about backup snapshots of the VM taking from Prism Element. Each line represent a snapshot, and the following information is displayed for each snapshot:

- **Create Time**: Displays the time the backup snapshot was created (completed).
- **Name**: Displays a name for the backup if one was created.

- **Action**: Displays four action links:
  - Click the **Details** link to open a window that displays the snapshot details.
  - Click the **Clone** link to clone a VM from the snapshot.
  - Click the **Restore** link to restore the VM from the snapshot. This restores the VM back to the state of the selected snapshot.
  - Click the **Delete** link to delete the snapshot.

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options as the Alerts dashboard, however it is filtered to display the alerts only for the selected VM (individual VM). For more information about alerts, see Prism Central Alerts and Events Reference Guide.

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options as the Events dashboard, however it is filtered to display the events only for the selected VM (individual VM). For more information about events, see Prism Central Alerts and Events Reference Guide.

Metrics Tab

The **Metrics** tab allows you to view usage metrics for the selected VM.

Click the **Metrics** tab to view the graphs for all the metrics . The graph is a rolling time interval performance or usage monitor. The baseline range appears as a blue band in the graph.

> **Note:** The baseline range and identified anomalies are based on sophisticated machine-learning capabilities. For more information, see Behavioral Learning Tools in *Intelligent Operations Guide*. The machine-learning algorithm uses 21 days of data to monitor and predict performance. A graph or baseline band may not appear if less than 21 days of data is available.

You can perform the following actions in the **Metrics** tab:

- Place the cursor anywhere on the horizontal axis to display the value at that time.
- Select the duration (time interval) from the dropdown menu on the right (last 1 hour, last 24 hours, or last week).
- Click the **Filters** option to select one or more appropriate metric checkboxes to display the selected metrics in the **Metrics** page. For more information, see Table 23: Metrics Tab Fields on page 116.
- From the **Actions** dropdown menu that appears on the top-right corner of each metrics widget, you can perform the following operations:
  - Select **Alert Settings** to create an alert policy for the selected metric. For more information about how to create alert policies, see Prism Central Alerts and Events Reference Guide.
  - Select **Add to Analysis** to add the selected metric to **Analysis** dashboard. For more information, see Analysis Dashboard in *Intelligent Operation Guide*.

The following table describes the metrics available in **Metrics** tab:

> **Note:** Metrics are hypervisor-dependant, and might not be available on all hypervisors.

Table 23: Metrics Tab Fields

Metric	Description
CPU Usage	Displays the percentage of CPU capacity currently being used by the VM (0–100%).
CPU Ready Time	Displays the current, high, and low percentage of CPU wait time (0–100%).
Memory Usage (%)	Displays the percentage of memory capacity currently being used by the VM (0–100%).
IOPS related metrics	Displays separate graphs for total, write, and read I/O operations per second (IOPS) for the VM.
IO Latency related metrics	Displays separate graphs for total, write, and read average I/O latency (in milliseconds) for physical disk requests by the VM.
IO Bandwidth related metrics	Displays separate graphs for total, write (only), and read (only) I/O bandwidth used per second (MBps or KBps) for physical disk requests by the VM.
Usage related metrics	Displays separate graphs for disk, snapshot, and shared data usage (in GiBs) by the VM.
Working Set Size related metrics	Displays separate graphs for total, write, and read storage usage (in GiBs) for the VM working set size.
Disk Usage (%)	Displays the disk usage percentage for the VM.
Dropped Network Packets related metrics	Displays separate graphs for the number of transmitted and received packets dropped.
Network Bytes related metrics	Displays separate graphs for the amount of transmitted and received bytes (in GiBs).

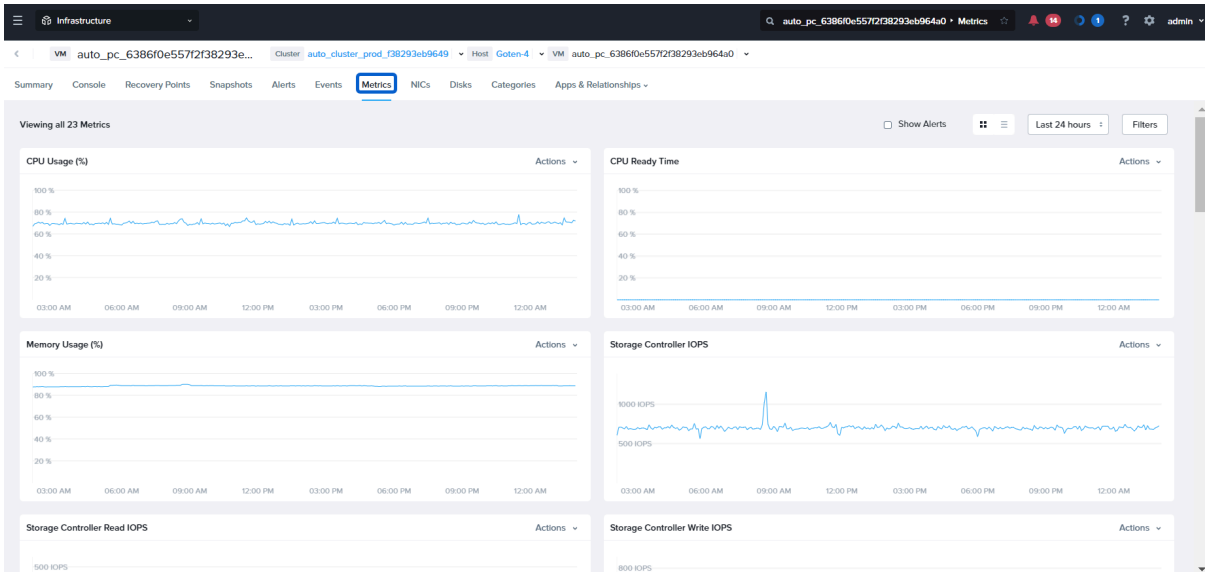


Figure 42: Metrics Tab

NICs Tab

The **NICs** tab displays information in tabular form about the virtual NICs in the VM. Each line represent a virtual NIC, and the following table describes the fields.

Table 24: NIC Fields

Parameter	Description	Values
VLAN ID	Displays the VLAN ID of the NIC.	(VLAN ID
MAC Address	Displays the virtual NIC MAC address.	(MAC address)
Network Connection State	Displays whether the NIC is connected to the network currently.	Connected, Disconnected
VPC	Displays the Virtual Private Cloud (VPC) of the NIC. For more information about VPC, see Virtual Private Clouds on page 357.	(VPC name)
Virtual Switch	Displays the virtual switch of the NIC. For more information about how to create a virtual switch, see Creating a Virtual Switch on page 349.	(Virtual Switch Name)
IP Address	Displays the virtual NIC IP address	(IP address)
Action	Displays the available actions you can perform on the NIC.	Delete

Disks Tab

The **Disks** tab displays information in tabular form about the virtual disks in the VM. Each line represents a virtual disk, and includes the following fields.

- **Disk Address**: Displays the disk address (such as ide.0 or scsi.1).
- **Capacity**: Displays the disk capacity (in MiB or GiB).

Categories Tab

The **Categories** tab displays the categories and image placement policies associated with the VM. Each VM can have a one-to-many relationship with categories and the categories can have a many-to-one relationship with image placement policies.

For more information about categories management and image placement policies, see Category Management on page 454 and Image Placement Policies on page 476.

Apps & Relationships Tab

The **Apps & Relationships** tab displays a dropdown menu with two options: **Discovered Apps** and **App Relationships**.

> **Note:** Application Discovery function needs to be enabled to view the **Discovered Apps** and **App Relationships**. For more information about Application discovery function and how to enable it in Prism Central, see Application Discovery in *Intelligent Operations Guide*.

The **Discovered Apps** page displays (up to) the top 20 applications that are communicating with other entities (usually client VMs). The discovered applications are sorted based on the number of clients communicating with the application. This menu option provides similar information as the application

discovery dashboard, except it is filtered to display the details only for this VM . For more information, see Application Discovery in *Intelligent Operation Guide*.

The **App Relationships** page displays three tabs: **Visualization**, **Incoming List**, and **Outgoing List**. All the three tabs display (up to) the top 20 results with respect to the visualization, incoming or outgoing client communication.

The **Visualization** tab displays a visual representation of the VM and the applications running on it, along with its incoming and outgoing communication with other entities. Data for last 24 hours is fetched to display the information on the visualization tab.

You can perform the following actions in **Apps & Relationships** tab:

- Hover on an entity to see the communication details with the applications.
- Hover on an application to see the incoming communication of the application with external entities and outgoing communications of the VM on which the application is running.

Note: In case of dual NIC VMs, click and expand the App listing to view the specific IP that is being used by the application.

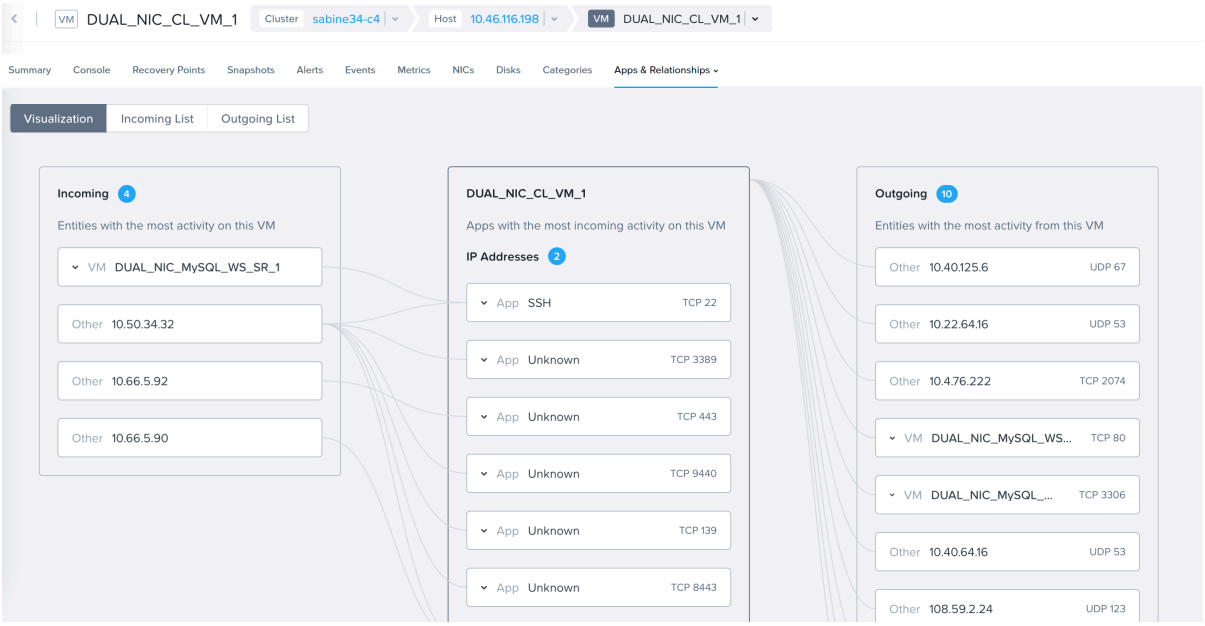


Figure 43: Visualization Tab

Incoming List: Displays a list of entities having incoming communication with this VM. Each line represents an incoming communication and includes the following fields.

Table 25: Incoming List Fields

Parameter	Description	Values
Source Entity Name	Displays the name of the communicating entity. If the entity is not identified by Prism Central (through registered PE or through vCenter using monitoring configurations feature), the name is displayed as unknown.	(VM name), Unknown

Parameter	Description	Values
Source IP Address	Displays the IP Address of the communicating entity.	(IP Address)
Destination App	Displays the name of the application that is being communicated to. If the application is not an identified one, the Destination App is displayed as Unknown.	(application name), Unknown
Destination IP Address	Displays the IP Address of the VM.	(IP address)
Destination Port	Displays the port used by the application for communication.	(port number)
Destination App Identification Status	Indicates whether the application is an identified application type. An identified application is one that is a known type.	Identified, Unidentified

Click **Modify Filters** option to view the **Filters** pane. You can use the **Filters** pane to select a filter option.

You can apply filters with multiple fields. The filters fetch the latest discovery and communication data and accordingly display the result set, to a maximum of 20 results.

The following table describes the filter options for **Incoming List**.

Table 26: Filters Pane - Incoming List

Field	Description	Values
Source Entity Name	Filters based on the source entity name. Select a condition from the dropdown menu (**Contains**, **Equal to**, **Not equal to**, **Doesn't contain**, **Starts with**, **Ends with**) and enter a string in the field.	(source entity name string)
Entity Type	Filters based on the entity type. A VM belongs to a cluster managed by Prism Central or vCenter (only if using monitoring configurations feature). An Unknown entity is one that is not identified by Prism Central.	VM, Unknown
Source IP Address	Filters based on the source IP address.(same options as Source Entity Name).	(source IP address string)
Destination App	Filters based on the destination app (same options as Source Entity Name).	(Destination App string)
Destination IP Address	Filters based on the destination IP address (same options as Source Entity Name).	(destination IP address string)
TCP Port	Filters based on the TCP port number.	(TCP port number)
UDP Port	Filters based on the UDP port number.	(UDP port number)
Time Range	Filters based on the time range.	Last 30 Mins, Last 1 Hour, Last 12 Hours, and Last 24 Hours

Outgoing List: Displays a list of entities having outgoing communication from this VM. Each line represents an outgoing communication and includes the following fields.

Table 27: Field Description - Outgoing List

Field	Description	Values
Destination Entity Name	Displays the name of the entity this VM is communicating to. If the entity is not identified by Prism Central (through registered PE or through vCenter using monitoring configurations feature), the name is displayed as unknown.	(entity name), Unknown
Destination IP Address	Displays the IP Address of the entity this VM is communicating to.	(IP address)
Destination Port	Displays the port on which this VM is communicating with the destination entity.	(port number)
Source IP Address	Displays the IP Address of the VM.	(IP address)
Source App Identification Status	Indicates whether the communicating application is an identified application type. An identified application is one that is a known type.	Identified, Unidentified

You can filter this list by opening the Filter pane to select a filter option. The following table describes the filter options for **Outgoing List**. You can apply filters with multiple fields. The filters fetch the latest discovery and communication data and accordingly display the result set, to the maximum of 20 results.

The following table describes the filter options for **Outgoing List**:

Table 28: Filter Pane - Outgoing List

Fields	Description	Values
Destination Entity Name	Filters based on the destination entity name. Select a condition from the dropdown menu (**Contains**, **Equal to**, **Not equal to**, **Doesn't contain**, **Starts with**, **Ends with**) and enter a string in the field.	(destination entity name string)
Entity Type	Filters based on the entity type. A VM belongs to a cluster managed by Prism Central or vCenter (only if using monitoring configurations feature). An Unknown entity is one that is not identified by Prism Central.	VM, Unknown
Destination IP Address	Filters based on the destination IP address. (same options as Destination Entity Name).	(destination IP address string)
TCP Port	Filters based on the TCP port number.	(TCP port number)
UDP Port	Filters based on the UDP port number.	(UDP port number)
Source IP Address	Filters based on the source IP address (same options as Destination Entity Name).	(source IP address string)

Fields	Description	Values
Time Range	Filters based on the time range.	Last 30 Mins, Last 1 Hour, Last 12 Hours, and Last 24 Hours

Creating a VM through Prism Central (AHV)

You can create virtual machines (VMs) in Acropolis-managed clusters through Prism Central.

About this task

Note:

- For instructions about how to install Nutanix VirtIO on Windows VMs, see Windows VM Provisioning in the *AHV Administration Guide*.
- If you are logged in as the self-service administrator or a project member, see Creating a VM (Self Service) on page 521.

To create a VM in an AHV cluster, perform the following steps:

Procedure

To create a VM in AHV cluster, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and go to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment. For information about how to access the list of non-nutanix VMs managed by an external *vCenter*, see VMs Summary View on page 95.

3. Click **Create VM**, and enter the following information in the **Configuration** step:

   a. **Name**: Enter a name for the VM.

   b. **Description** (optional): Enter a description for the VM.

   c. **Cluster**: Select the target cluster from the dropdown menu on which you intend to create the VM.

   d. **Number of VMs**: Enter the number of VMs you intend to create. The created VM names are suffixed sequentially.

   e. **vCPU(s)**: Enter the number of virtual CPUs to allocate to this VM.

   f. **Number of Cores per vCPU**: Enter the number of cores assigned to each virtual CPU.

   g. **Memory**: Enter the amount of memory (in GiBs) to allocate to this VM.

   h. **Enable Memory Overcommit**: Select this checkbox to enable memory overcommit for the VM.

      Before you turn memory overcommit on or off, see Memory Overcommit in the *AHV Administration Guide*. For more information on configuring memory overcommit, see Memory Overcommit Management on page 188.

      > **Note:** Ensure that the status of the **Memory Overcommit** property under **Configuration** in the **Review** tab is set as **Enabled**.

   i. **Enable Advanced Processor Compatibility**: Select this checkbox to enable advanced processor compatibility for the VM.

      After you select the **Enable Advanced Processor Compatibility** checkbox, the system provides you the option to select the required CPU generation.

      Select the required CPU generation name in the **Select CPU generation** dropdown menu.

      For more information, see Advanced Processor Compatibility in AHV section in the *AHV Administration Guide*.

      > **Note:** Advanced processor compatibility setting for VMs with automatic cluster selection configuration is not supported. For more information on automatic cluster selection, see Automatic Cluster Selection for VM Placement section in the *AHV Administration Guide*.

      The following is an example showing the **Configuration** step:

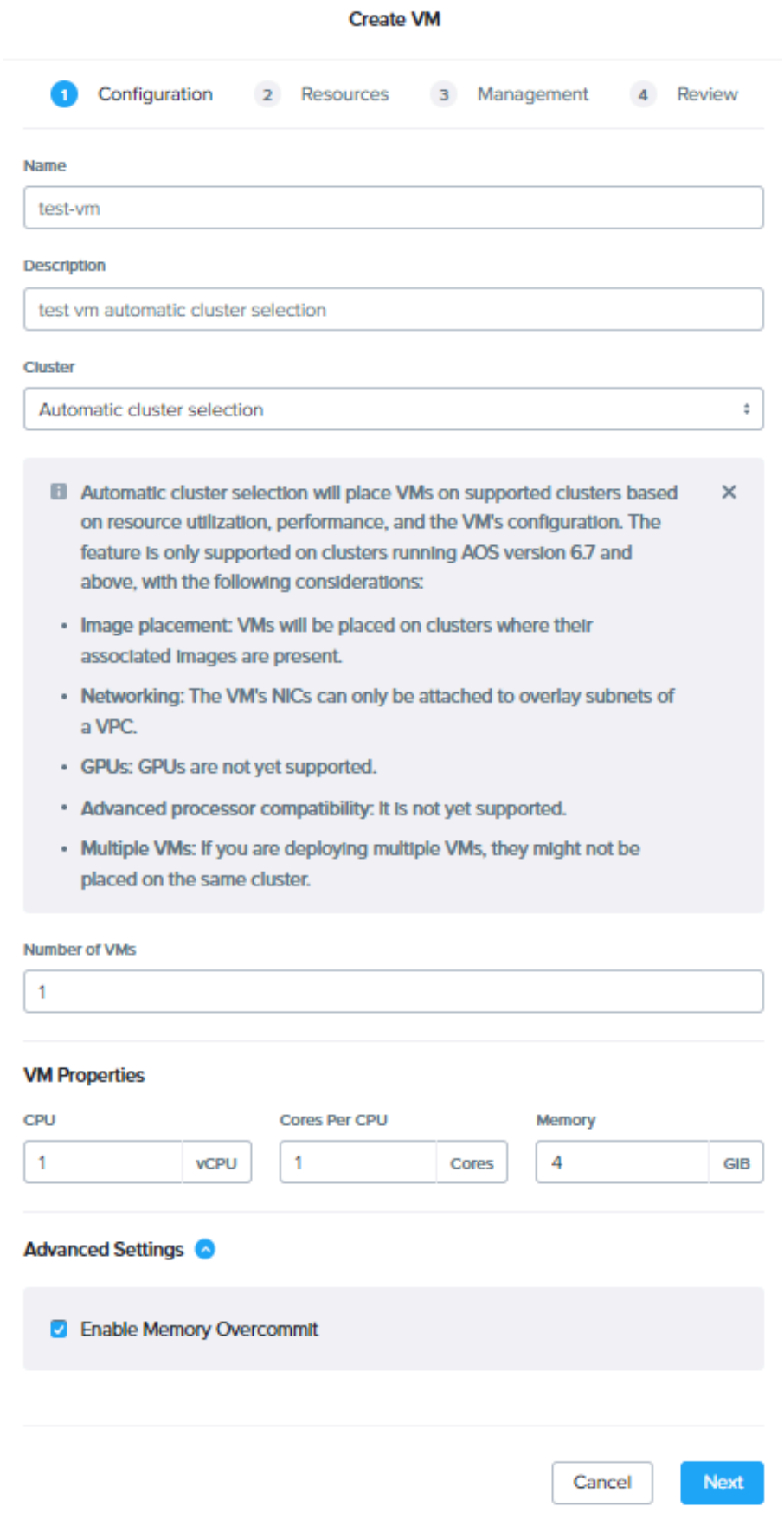


Figure 44: Create VM - Configuration

The following is an example showing the **Configuration** step:

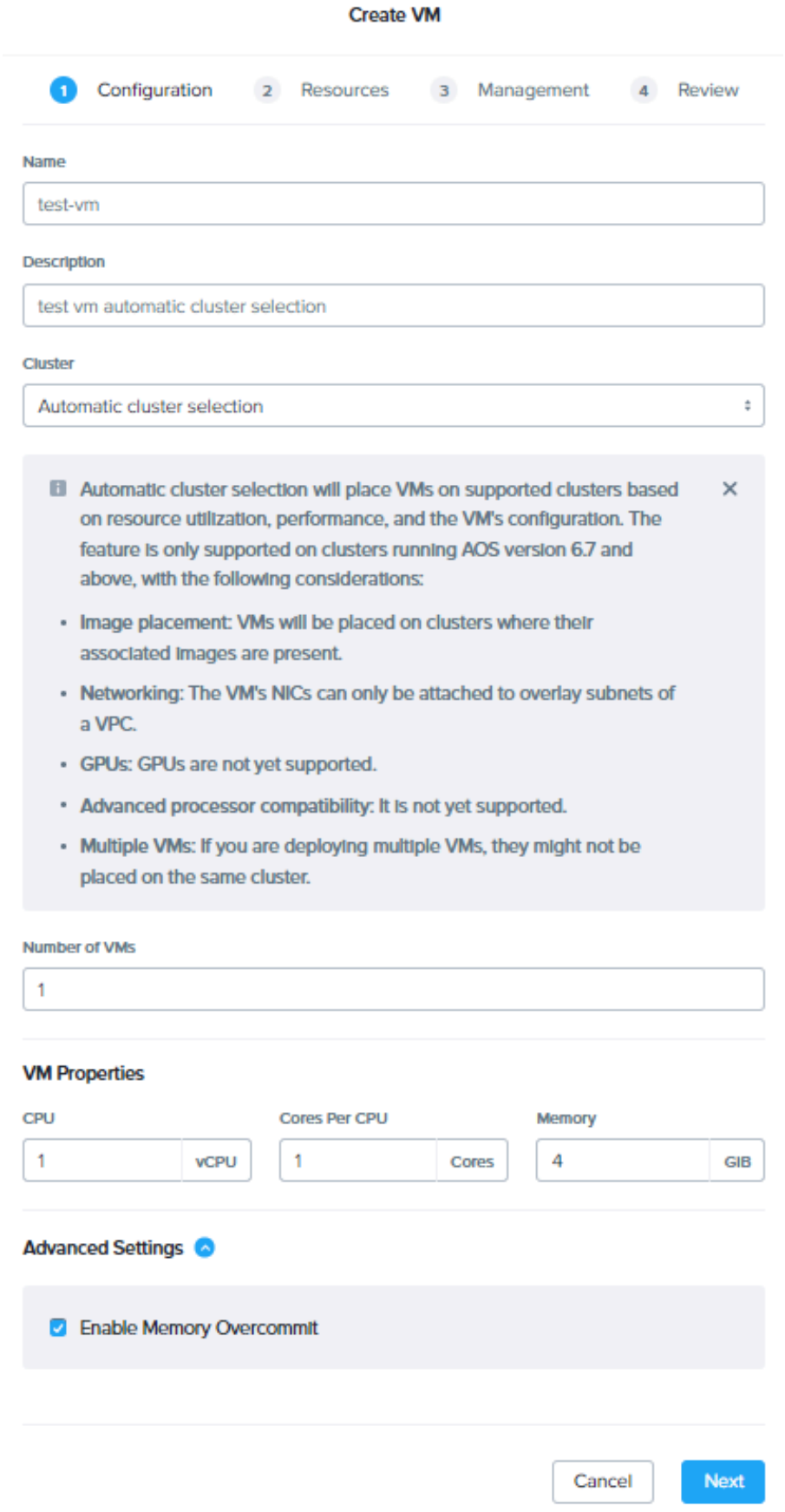


Figure 45: Create VM - Configuration

4. In the **Resources** step, perform the following actions to attach a Disk to the VM:

   Disks: Click **Attach Disk**, and enter the following information:

   The following is an example showing the **Attach Disk** window:

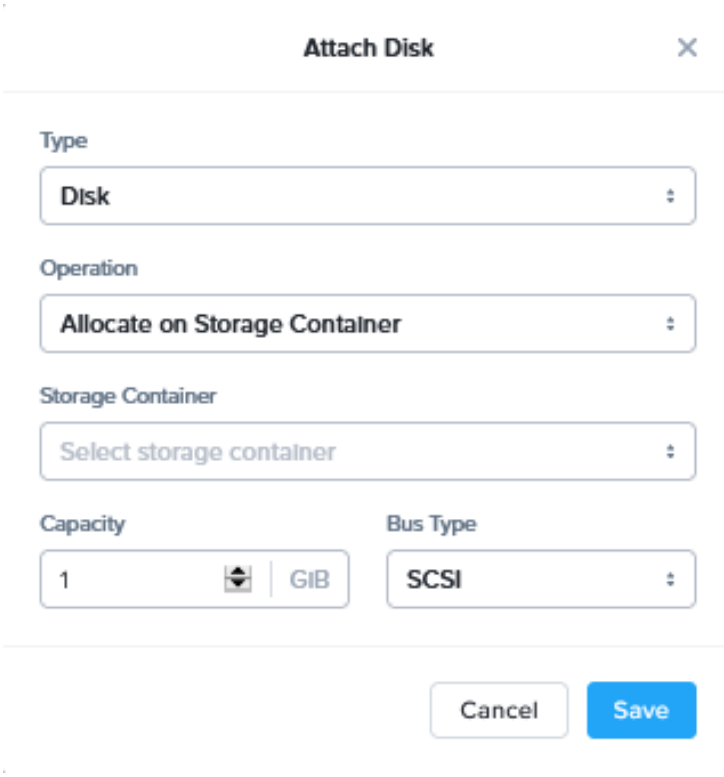


Figure 46: Attach Disk Window

   a. **Type**: Select the type of storage device, **Disk** or **CD-ROM**, from the dropdown menu.

   b. **Operation**: Specify the device contents from the dropdown menu.

      - Select **Empty CD-ROM** to create a blank CD-ROM device. A CD-ROM device is needed when you intend to provide a system image from CD-ROM.

        Note: The **Empty CD-ROM** option is available only when *CD-ROM* is selected as the storage device in the **Type** field.

      - Select **Allocate on Storage Container** to allocate space without specifying an image. Selecting this option means you are allocating space only. You have to provide a system image later from a CD-ROM or another source.

        Note: The **Allocate on Storage Container** option is available only when *Disk* is selected as the storage device in the **Type** field.

      - Select **Clone from Image** to copy an image that you have imported by using the image service feature onto the disk.

   c. If you select:

- **Allocate Storage Container** in the **Operation** field, the system prompts you to specify the **Storage Container**.

  > **Note:** If the VM is assigned to a category associated with a storage policy, then the storage container that you select might not govern the storage properties of the VM. The storage properties that the storage policy provides override the storage properties that the storage container provides.

- **Clone from Image** in the **Operation** field, the system prompts you to specify the **Image**.

d. Enter either of the following information based on your selection in the **Operation** field:

- **Storage Container**: Select the appropriate storage container.
- **Image**: Select the image you created using the image service feature. For information about Image management, see Image Management on page 238.

  > **Note:** If the image you created does not appear in the list, see KB-4892. The image transfer can trigger image bandwidth throttling if a bandwidth throttling policy is associated with the image. For more information, see Bandwidth Throttling Policies on page 484.

e. **Bus Type**: Select the bus type from the dropdown menu.

   The options displayed in the dropdown menu vary based on the storage device **Type** selected in the **Type** field.

   If the storage device **Type** is:

- **Disk**: The available choices are **SCSI**, **SATA**, **PCI**, or **SATA**.
- **CD-ROM**: The available choices are **IDE**, or **SATA**

f. **Capacity**: Enter the disk size in GiB.

g. When all the field entries are correct, click **Save** to attach the disk to the VM and return to the **Create VM** window.

Repeat this step to attach additional devices to the VM.

5. In the **Resources** tab, perform the following actions to create a network interface for the VM:

   Networks: Click **Attach to Subnet**. The **Attach to Subnet** window appears.

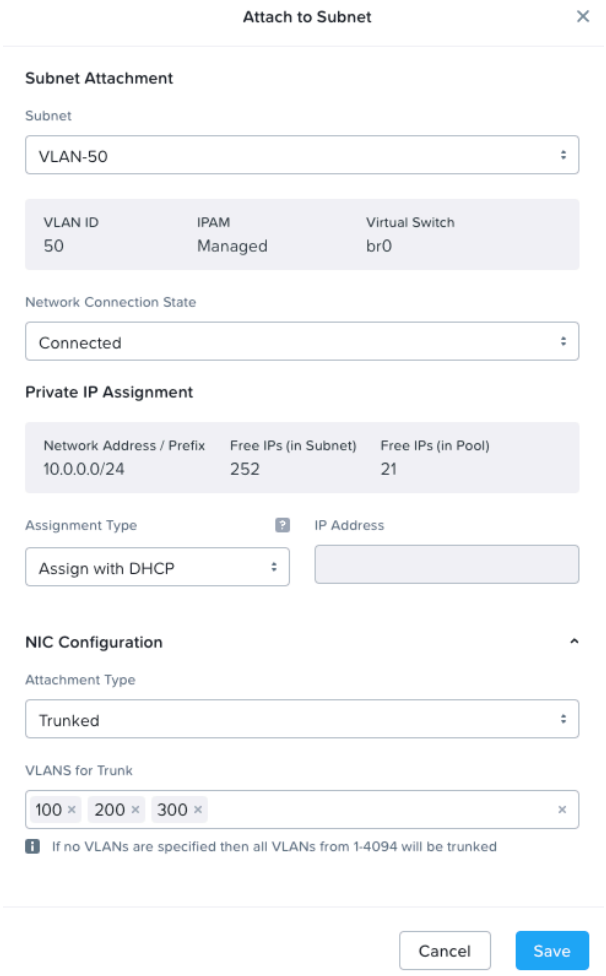


Figure 47: Attach to Subnet Window

   a. **Subnet**: Select the target subnet from the dropdown menu.

      The list includes all the defined networks. For more information on how to perform the network configuration, see Creating VLAN Connections on page 347.

   b. **VLAN ID**: This is a read-only field that displays the VLAN ID.

   c. **IPAM**: This is a read-only field that informs you if the subnet is IPAM managed or not.

   d. **Virtual Switch**: This is a read-only field that displays the name of the virtual switch associated with the subnet.

   e. **Network Connection State**: Select the state for the network after VM creation:

      - *Connected*: If the VM needs to be connected to the network to operate.
      - *Disconnected*: If the VM needs to be in disconnected state after creation.

f. **Network Address/Prefix**: This is a read-only field that displays the network IP address and prefix.

g. **Free IPs (in Subnet)**: This is a read-only field that displays the free IP addresses in the selected subnet.

h. **Free IPs (in Pool)**: This is a read-only field that displays the free IP addresses in the network IP pool.

i. **Assignment Type**: Select the IP assignment type from the dropdown menu. The options are `Assign with DHCP`, `Assign Static IP`, and `No Private IP`.

j. **IP Address**: Enter the static IP address for VLAN.
This field is enabled only if `Assign Static IP` is selected in the **Assignment Type** field.

k. **Attachment Type**: Select the NIC configuration attachment type from the dropdown menu. The options are `Access` and `Trunked`.
If you select `Trunked` attachment type, **VLANS for Trunk** field appears where you can specify the VLANs ID for the trunk.

l. **VLANS for Trunk**: Specify the VLAN ID for the trunk.
If you do not specify the VLAN ID for the trunked attachment type, then all VLANs from 1- 4094 are trunked.

> **Note:** VLANS for Trunk is available only for basic VLANs.

m. Click **Save** to create a network interface for the VM,and return to the **Create VM** window.

Repeat this step to create additional network interfaces for the VM.

6. (Optional) If you want to add Traffic Mirror Destination NICs, click **Add Mirror Destination NIC**.

> **Note:** NIC MAC Address is assigned after the creation of the VM.

You can add additional Traffic Mirror Destination NICs by clicking **Add New NIC**.

7. In the **Resources** step, perform the following actions for boot configuration.

Boot Configuration: Select one of the following firmware to boot the VM.

» **Legacy BIOS Mode**: Used to start the VM with legacy BIOS firmware.

» **UEFI BIOS Mode**: Used to start the VM with UEFI firmware. UEFI firmware supports larger hard drives, faster boot time, and provides more security features. For more information on UEFI firmware, see UEFI Support for VM information in the *AHV Administration Guide*.

If you select **UEFI BIOS Mode** for **Boot Configuration**, the system enables you to define the **Shield VM Security Settings**:

- **Secure Boot**: Select this check box to enable UEFI secure boot policies for your guest VMs. For more information on Secure Boot functionality, see Secure Boot for VMs information in *AHV Administration Guide*.
- **Attach vTPM**: Select this checkbox to enable vTPM. For information about vTPM functionality, see Securing AHV VMs with Virtual Trusted Platform Module (vTPM) information in *Security Guide*.

8. In the **Resources** step, perform the following actions to add a GPU:

   GPUs: Click **Add GPU**. The **Add GPU** dialog box appears. Do the following in the indicated fields:

   > **Note:** This step is applicable

   a. only to AHV clusters with GPU-enabled mode: Select the option for the desired mode, either **vGPU** or **Passthrough**.

   b. If you select **vGPU**, perform the following configuration settings:

   - **NVIDIA Virtual GPU License**: Select a license type from the dropdown menu. This action sets (filters the list of) available profiles. Click the Help icon for information about the license types.

     > **Note:**
     >
     > You can add multiple vGPUs to the VM only if you select the license for NVIDIA Virtual GPU software version 10.1 (440.53) or later.
     >
     > Before you add multiple vGPUs to the VM, see Multiple Virtual GPU Support and Restrictions for Multiple vGPU Support in the *AHV Administration Guide*.

   - **vGPU Profile**: Select the option for the desired profile. Click the help links (Virtual Slice column and end of line) for more information on the profiles.

     > **Note:**
     >
     > Multiple vGPUs are supported on the same VM only if you select the highest vGPU profile type. After you add the first vGPU, to add multiple vGPUs, see Adding Multiple vGPUs to the Same VM on page 147

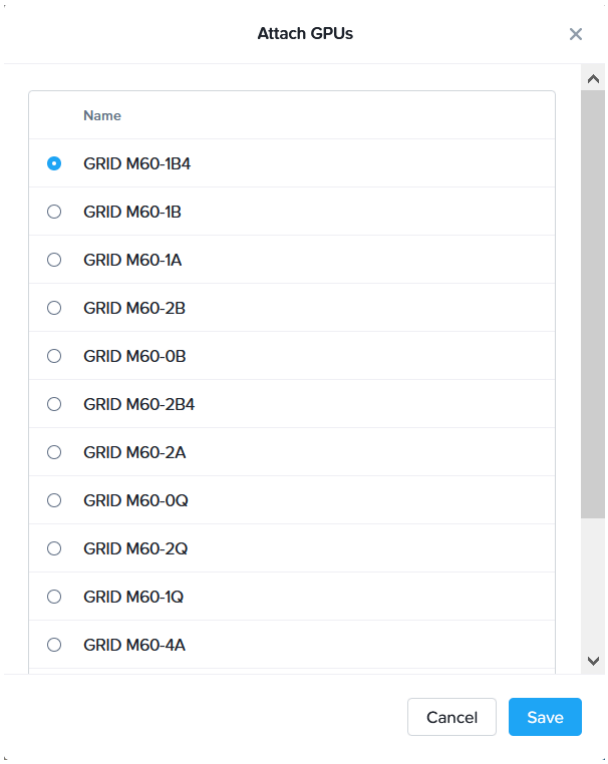


Figure 48: Attach GPUs Window: vGPU

c. If you select **Passthrough**, click the option for the desired type.

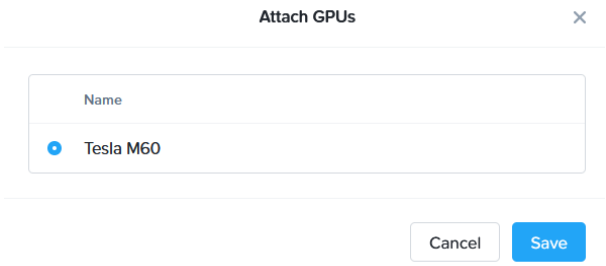


Figure 49: Attach GPUs Window: Passthrough

d. Click **Save**.

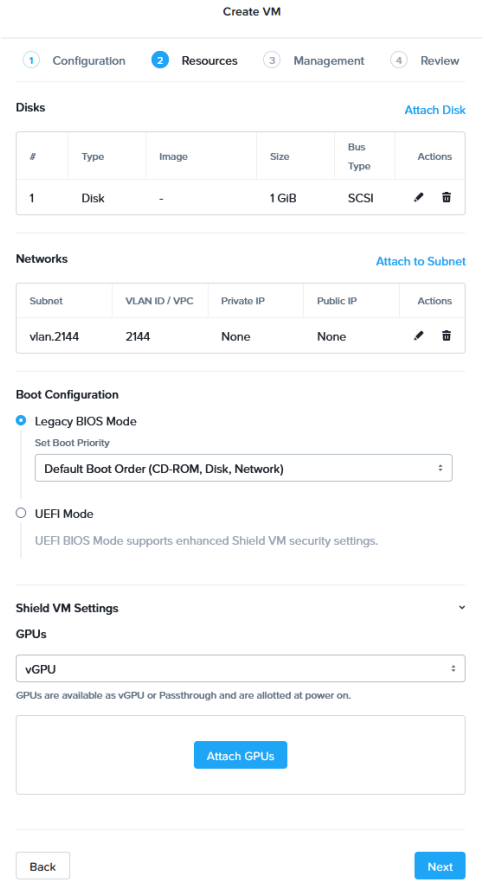


Figure 50: Create VM Window (Resources)

9. In the **Management** step, perform the following actions to define categories and timezone:

   a. Turn on the **Enable 'Default-Storage' policy** switch to apply the default storage policy to the VM that you are creating.

      The **Enable 'Default-Storage' policy** switch is turned off by default.

      For more information on the default storage policy, see Default Storage Policy on page 498.

   b. **Categories**: Search for the category to be assigned to the VM. Select the checkboxes of the categories that you want to assign to the VM.

      If you enabled the **Enable 'Default-Storage' policy** switch for the VM in the previous step, then the **Storage:$Default** is displayed in the **Categories** dropdown menu. To assign more categories to the VM, select the categories from the dropdown menu.

      > **Note:**
      >
      > Do not assign any other category that is already associated with another storage policy to the entity, such as a VM or VG, if you want to enable the **Enable 'Default-Storage' policy** switch for that entity. If you enable the **Enable 'Default-Storage' policy** switch for an entity that is already associated with another category, the **Storage: $Default** category is enabled, but the storage policy associated with the other category overrides the default storage policy.

   c. **Timezone**: Select the local timezone to use from the dropdown menu.

   d. **Use this VM as an agent VM**: Select this option to make this VM as an agent VM.

      You can use this option for the VMs that must be powered on before the rest of the VMs (for example, to provide network functions before the rest of VMs are powered on the host) and

must be powered off and migrated after rest of the VMs (for example, during maintenance mode operations).

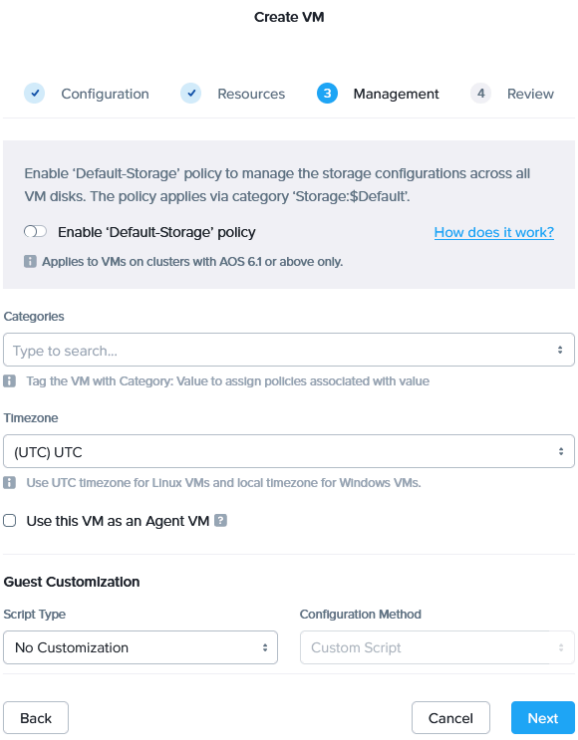


Figure 51: Create VM Window (Management)

10. In the **Management** step, perform the following actions for VM customization:

    Guest Customization: To customize the VM, select Cloud-init (for Linux VMs) or Sysprep (for Windows VMs).

    Script Type: Select the VM script customization type from the dropdown menu. The options are `No Customization`, `Sysprep(Windows)`, or `Cloud-init (Linux)`.

    Configuration Method: Select the VM script customization method from the dropdown menu. This field is activated when the **Script Type** is either `Sysprep(Windows)` or `Cloud-init (Linux)`. The options are `Custom Script` or `Guided Script`.

    The system displays the options required to configure Cloud-init and Sysprep, such as options to specify a configuration script and options to upload a script

11. To specify a user data file (Linux VMs) or answer file (Windows VMs) script for unattended provisioning, perform either of the following actions:

    » If the file is available on your local computer, click **Upload Script**, choose and upload the file.

    » Create or paste the contents of the file in the text box below **Upload Script**.

    Note: The script type supports the following file formats.

    - Sysprep: XML
    - Cloud-init (Linux): YAML, JSON, or Shell.

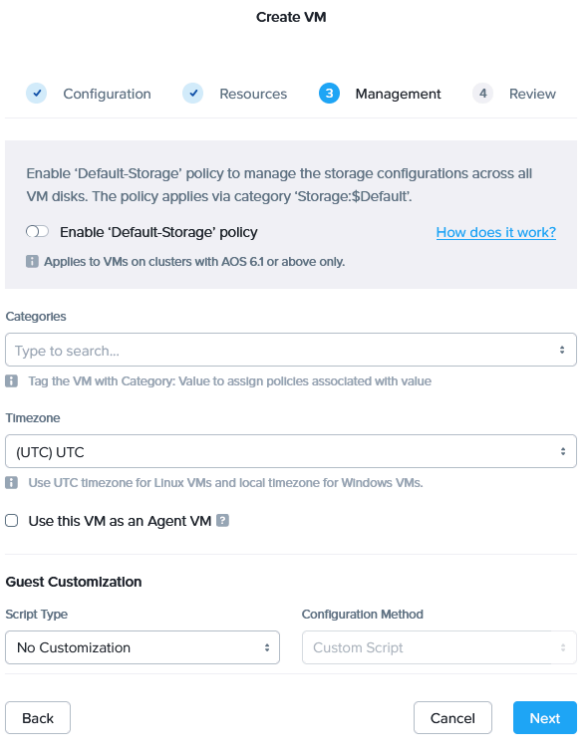


Figure 52: Create VM Window (Management)

12. In the **Review** step, when all the field entries are correct, click **Create VM** to create the VM, and close the **Create VM** window.

    The new VM appears in the VMs **Summary** page and **List** page.

Managing a VM through Prism Central (AHV)

About this task

After you create a VM, you can perform various operations to manage it based on your requirement.

Note:

- You can perform some of the available actions on a single VM at a time, while others can be performed on multiple VMs simultaneously. The available actions appear in bold; the unavailable actions are grayed out. The available actions depend on the current state of the VM and user permissions.

- You can perform only those operations for which you have permissions from the admin.
- Do not install any external software on the Prism Central VM.

To manage a VM, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment. For information about how to access the list of non-nutanix VMs managed by an external *vCenter*, see VMs Summary View on page 95.
3. Select the required action using any of the following methods:
   - Select the target VM checkbox in the **List** tab, and choose the required action from the from the **Actions** dropdown menu.
   - Right-click on the target VM in the **List** tab, and select the required action from the displayed dropdown menu.
   - Select the required action in the **Summary** page of an individual VM. For information about how to access the **Summary** page of an individual VM, see VM Details View on page 108.

The following table provides the information about all the actions that you can perform to manage the VM:

Table 29: VM Actions

Action	Description	Applicable to Multiple VMs
Update	Update the VM configuration. For more information, (see Updating a VM through Prism Central (AHV) on page 138.	No
Delete	Delete the VM.	Yes
Clone	Clone a VM. For more information, see Cloning a VM through Prism Central (AHV) on page 144.	No
Create VM Template	Create a VM template. For more information, see Creating a VM Template on page 193.	No
Launch Console	Launch the VM console. For more information, see Launching a VM Console through Prism Central (AHV) on page 146.	No
Migrate Across Clusters	On-demand migrate the VM across AHV clusters without the need to protect them in synchronous replication schedules or set up Nutanix Disaster Recovery from the Prism Central web console. For more information about on-demand VM migration, see On-Demand Cross-Cluster Live Migration on page 155.	Yes
Power On	Power on the VM.	Yes
Power Off	Power off the VM.	Yes

Action	Description	Applicable to Multiple VMs
Power Cycle	power off the VM followed by a power on.	Yes
Reset	Perform an ACPI reset action through the BIOS of the VM.	Yes
Guest Shutdown	Perform a graceful shutdown of the operating system of the VM.	Yes
Guest Reboot	Perform a graceful restart of the operating system of the VM.	Yes
Pause/Suspend	Pause or suspend the VM. This option is available only when the VM is powered on.	Yes
Resume	Resume a paused or suspended VM.	No
Disable Efficiency Measurement	Disable machine-learning capability of efficiency measurement for the VM. You can also create a category of VMs and assign the category in **Inefficiency Measurement Exclusion** policy to control this function through operations policies. For more information, see Operations Policy Management in *Intelligent Operations Guide*. **Note:** By default, the efficiency measurement function is enabled for all VMs.	Yes
Enable Efficiency Measurement	Enable machine-learning capability of efficiency measurement. **Note:** If the VM is part of the VM category that is mapped to the **Inefficiency Measurement Exclusion** operations policy, the policy takes precedence and the system does not allow you to enable efficiency measurement. For information about how to assign or remove the VM category in **Inefficiency Measurement Exclusion** policy, see Managing Operations Policies in *Intelligent Operations Guide*. You cannot enable efficiency measurement on individual VMs if the efficiency measurement is disabled on the cluster level.	Yes
Disable Anomaly Detection	Disable machine-learning capability of Anomaly Detection for the VM. You can also create a category of VMs and assign the category in **Anomaly Detection Exclusion** policy to control this function through operations policies. For more information, see Operations Policy Management in *Intelligent Operations Guide*. **Note:** By default, the anomaly detection function is enabled for all VMs.	Yes
Enable Anomaly Detection	Enable machine-learning capability of anomaly detection. **Note:** If the VM is part of the VM category that is mapped to the **Anomaly Detection Exclusion** operations policy, the policy takes precedence and the system does not allow you to enable anomaly detection. For information about how to assign or remove the VM category in **Anomaly Detection Exclusion** policy, see Managing Operations Policies in *Intelligent Operations Guide*.	Yes

Action	Description	Applicable to Multiple VMs
Protect	Assign the VM to a protection policy. Selecting **Protect** opens a window to specify the protection policy to which this VM should be assigned. You can create a protection policy for a VM or set of VMs that belong to one or more categories by enabling Nutanix Disaster Recovery and configuring the Availability Zone.	Yes
Unprotect	Remove the VM from a protection policy.	Yes
Create Recovery Point	Create VM recovery point. The VM can be restored or replicated from a recovery point either locally or remotely in a state of a chosen recovery point. In the **Create VM Recovery Point** window, enter a name for the VM recovery point. You can choose to create an app consistent VM recovery point by enabling the **App Consistent** checkbox. For more information about app consistent recovery point, see Terminology section in the *Data Protection and Recovery with Prism Element* guide.	No
Migrate	Migrate the VM within the cluster to another host or outside the cluster. In the **Migrate VM** window, choose any of the following options: • **Migrate Within Cluster** to select the target host from the dropdown menu (or select the System will automatically select a host option to let the system choose the host). • **Migrate Outside Cluster (Protected VMs)** to live migrate the VM protected with synchronous replication outside the cluster. **Note:** This option is disabled if the VM is not protected with synchronous replication schedule or VM synchronization is not completed at the recovery AZ. **Note:** Nutanix recommends to live migrate VMs when they are under light load. If they are migrated while heavily utilized, migration may fail because of limited bandwidth. For more information about VM migration, see VM Migration Specifications on page 148.	No
Add to Recovery Plan	Add the VM to a recovery plan you created previously. For more information, see the Adding Guest VMs Individually to a Recovery Plan section in the *Nutanix Disaster Recovery Guide*.	Yes
Run Playbook	Run a playbook you created previously. For more information, see Running a Playbook (Manual Trigger) in *Intelligent Operations Guide*.	Yes
Manage Categories	Assign the VM a category value. For more information, see Assigning a Category on page 459.	Yes
Install NGT	Install Nutanix Guest Tools (NGT). For more information, see Installing NGT on page 169.	Yes

Action	Description	Applicable to Multiple VMs
Manage NGT Applications	Enable or disable NGT. For more information, see Managing NGT Applications on page 172.	Yes
Upgrade NGT	Upgrade NGT. For more information, see Upgrading NGT on page 172.	Yes
Configure VM Host Affinity	This option is disabled and cannot be used to define VM-Host affinity in Prism Central. The VM-Host affinity policies can be created using VM categories and host categories. For more information about affinity policies Prism Central, see Affinity Policies Defined in Prism Central on page 461. For information about how to create an affinity policy, see Creating an Affinity Policy on page 469. It is recommended to create an affinity to multiple hosts (at least two) to protect against downtime due to a node failure.	No
Add to Catalog	Add the VM to the catalog. For more information, see Adding a Catalog Item on page 264.	No
Manage Ownership	Specify a project and user who owns the VM. In the **Manage VM Ownership** window, select the target project from the dropdown menu and enter a user name as owner of the VM.	No
Set QoS Attributes	Configure quality of service (QoS) settings. For more information, see Setting QoS for an Individual VM on page 187.	Yes
Export as OVA	Export the VM as OVA. For more information, see OVA Management on page 214 and Uploading an OVA on page 219.	No

4. Check the status of the selected action under tasks widget.

Updating a VM through Prism Central (AHV)

You can use Prism Central to update the VM configuration.

About this task

To update a VM, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default with all the VMs across registered clusters in the **Nutanix** environment. For information about how to access the list of non-Nutanix VMs managed by an external *vCenter*, see VMs Summary View on page 95.

3. Select the **Update** action using any of the following methods:

   - Select the target VM checkbox in the **List** tab, and choose **Update** from the from the **Actions** dropdown menu.
   - Right-click on the target VM in the **List** tab, and select **Update** from the displayed dropdown menu.
   - Click **Update** in the **Summary** page of an individual VM. For information about how to access the **Summary** page of an individual VM, see VM Details View on page 108.

   The **Update VM** window appears, which includes the same fields as the **Create VM** window. For information about how to create a VM, see Creating a VM through Prism Central (AHV) on page 121.

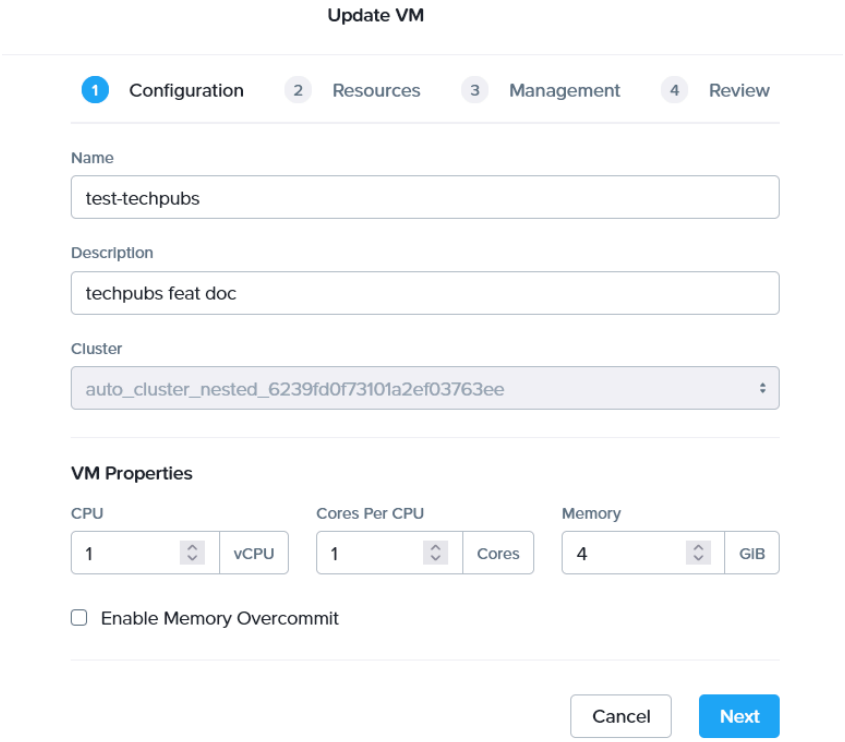


Figure 53: Update VM Window (Configuration)

Modify the VM configuration based on your requirement as indicated in the following steps, and click **Save** in the **Review** step:

4. **Enable Memory Overcommit**: Select this checkbox to enable memory overcommit for the VM.

   Before you turn memory overcommit on or off, see Memory Overcommit in the *AHV Administration Guide*. For more information on configuring memory overcommit, see Memory Overcommit Management on page 188.

   > **Note:** Verify that the status of the **Memory Overcommit** property under **Configuration** in the **Review** tab is set as **Enabled**.

5. **Disks**:

   - You can add new disks to the VM using the **Attach Disk** option. You can also modify the existing disk attached to the VM using the controls under the actions column. See Creating a VM through

Prism Central (AHV) on page 121 before you modify the disk or create a new disk for a VM. You can turn the flash mode settings for the VM and VM disks on or off.

- You can change the storage container of the disk from the **Storage Container** field:

  Note: Starting with Prism Central 2023.4, the individual VM disks can be migrated using Prism Central UI. If more granular control is required, perform the steps through acli as described in Migrating a vDisk to Another Container section in *AHV Administration Guide*.

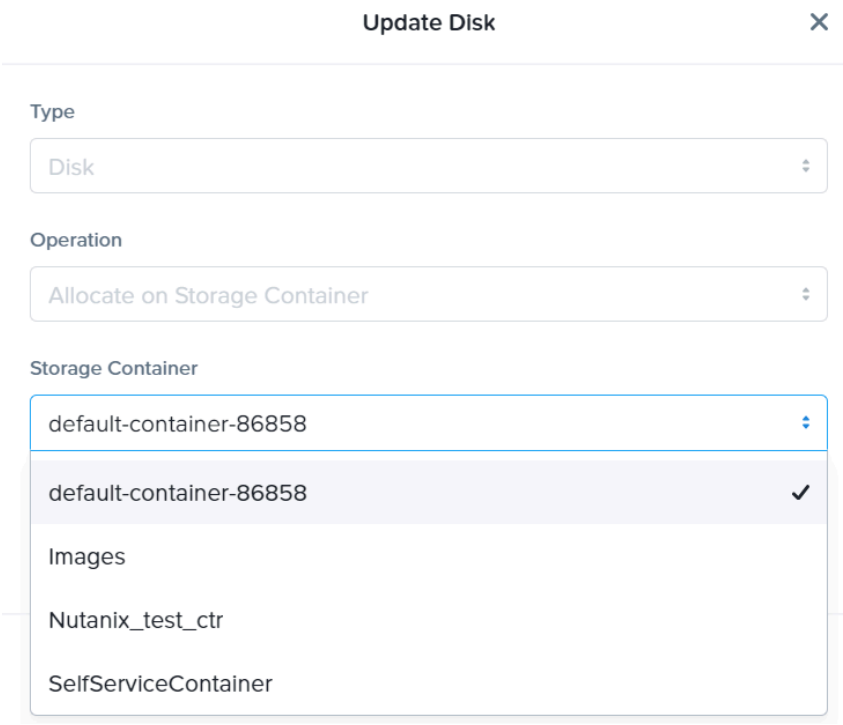


Figure 54: Storage Container Update

a. To enable flash mode on the VM, click the **Enable Flash Mode** checkbox.

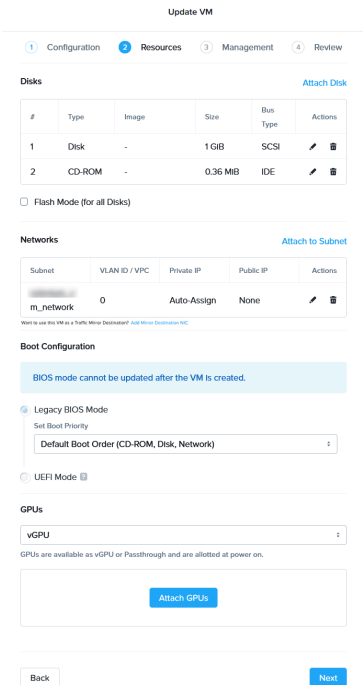


Figure 55: Update VM Window (Resources)

» After you enable this feature on the VM, the status is updated in the VM table view. To view the status of individual virtual disks (disks that are flashed to the SSD), click the update disk icon in the **Disks** pane in the **Update VM** window.

» You can turn off the flash mode feature for individual virtual disks. To update the flash mode for individual virtual disks, click the update disk icon in the **Disks** pane and deselect the **Enable Flash Mode** check box.

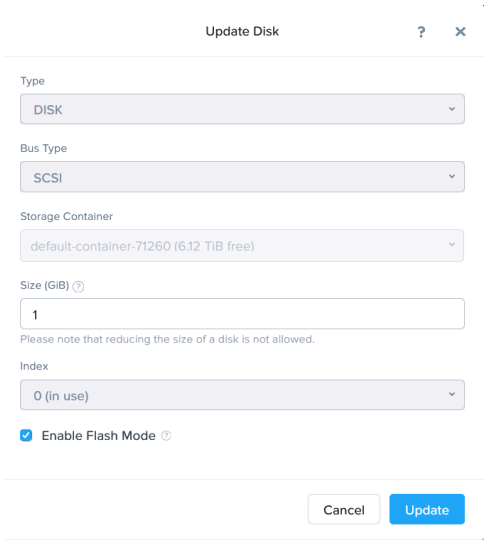


Figure 56: Update Disk Window (VM Disk Flash Mode)

Note: The flash mode setting is not supported for **CD-ROM** storage devices.

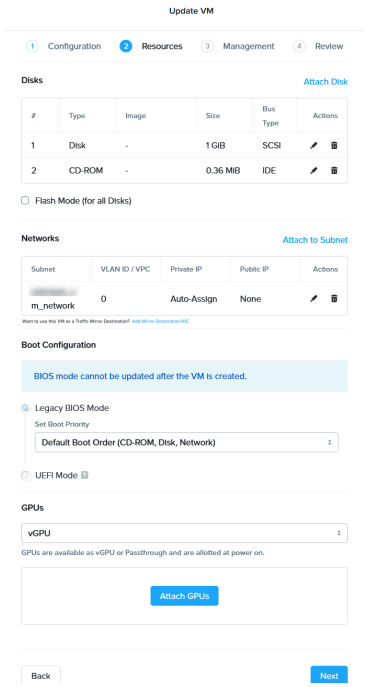


Figure 57: Update VM Window (Resources)

6. **Networks:** You can attach a new network to the VM using the **Attach to Subnet** option. You can use the **Add Mirror Destination NIC** option to use the VM as a Traffic Mirror destination. You can also modify the existing subnet and Traffic Mirror destination NICs attached to the VM. Before you modify the NIC network or create a new NIC for a VM, see Creating a VM through Prism Central (AHV) on page 121 and Limitation for VNIC Hot-Unplugging information in the *AHV Administration Guide*.

7. **Boot Configuration:** You cannot modify the BIOS mode after the VM is created. However, if you have enabled the Secure Boot option under UEFI Mode while creating the VM, you can modify this setting during the VM update.

8. **GPUs:** (For GPU-enabled AHV clusters only) You can add pass-through GPUs if a VM is already using GPU pass-through. You can also change the GPU configuration from pass-through to vGPU or vGPU to pass-through, change the vGPU profile, add more vGPUs, and change the specified vGPU license.

   Note:

   - You must shut down the VM before you perform GPU configuration-related operations.
   - Before you add multiple vGPUs to the VM, see Multiple Virtual GPU Support and Restrictions for Multiple vGPU Support information in the *AHV Administration Guide*.
   - Multiple vGPUs are supported on the same VM only if you select the highest vGPU profile type.
   - After you add the first vGPU, to add multiple vGPUs, see Adding Multiple vGPUs to the Same VM on page 147.

9. Turn on or off the **Enable 'Default-Storage' policy** switch to turn on or off the default storage policy for the VM. The switch is turned off by default.

   The default storage policy uses the **Storage:$Default** category. When you turn on the **Enable 'Default-Storage' policy** switch, the VM is associated with the **Storage:$Default** category.

   For more information on the default storage policy, see Default Storage Policy on page 498.

Cloning a VM through Prism Central (AHV)

You can use Prism Central to clone a VM.

About this task

To clone a VM, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment. For information about how to access the list of non-nutanix VMs managed by an external *vCenter*, see VMs Summary View on page 95.

3. Perform the **Clone** action using any of the following methods:

   - Select the target VM checkbox in the **List** tab, and choose **Clone** from the from the **Actions** dropdown menu.
   - Right-click on the target VM in the **List** tab, and select **Clone** from the displayed dropdown menu.
   - Click **Clone** in the **Summary** page of an individual VM. For information about how to access the **Summary** page of an individual VM, see VM Details View on page 108.

   The **Clone VM** window appears, which includes the same fields as the **Create VM** window. For information about how to create a VM, see Creating a VM through Prism Central (AHV) on page 121.

   A cloned VM inherits most the configurations (except the name) of the source VM.

   Note:

   - You can clone up to 250 VMs at a time.
   - You cannot override the secure boot setting while cloning a VM, unless the source VM already had secure boot setting enabled.

   The following is an example showing the **Clone VM** window:

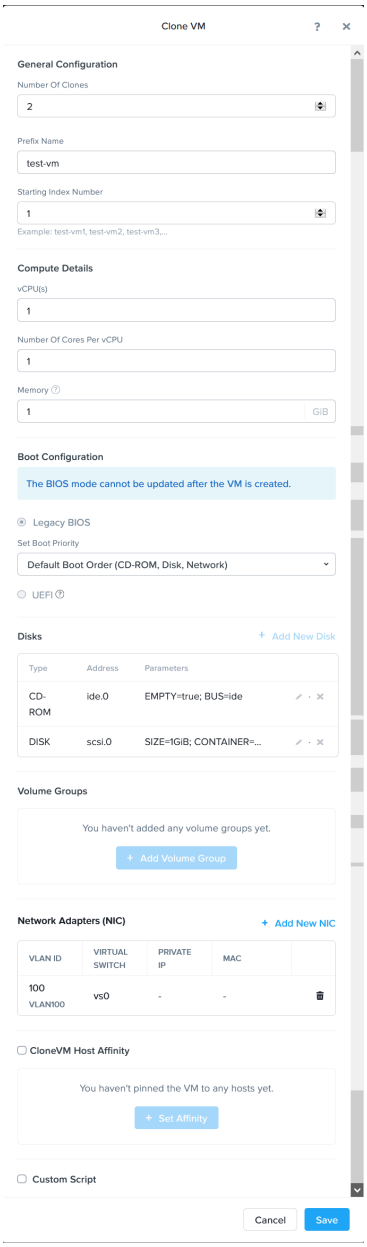


Figure 58: Clone VM Window

4. Enter a name for the clone, and click **Save**.

   You can optionally override some of the configurations before you click **Save**. For example, you can override the number of vCPUs, memory size, boot priority, NICs, or the guest customization.

   The VM clone is created successfully.

Launching a VM Console through Prism Central (AHV)

You can use Prism Central to launch a VM console.

Procedure

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment. For information about how to access the list of non-nutanix VMs managed by an external *vCenter*, see VMs Summary View on page 95.

3. Select the **Launch Console** action using any of the following methods:

   - Select the target VM checkbox in the **List** tab, and choose **Launch Console** from the from the **Actions** dropdown menu.
   - Right-click on the target VM in the **List** tab, and select **Launch Console** from the displayed dropdown menu.
   - Click **Launch Console** in the **Summary** page of an individual VM. For information about how to access the **Summary** page of an individual VM, see VM Details View on page 108.

   This opens a Virtual Network Computing (VNC) client and displays the console in a new tab or window. This option is available only when the VM is powered on. The VM power options that you access from the **Power On Actions** (or **Power Off Actions**) action link below the VM table can also be accessed from the VNC console window. To access the VM power options, click Power icon at the top-right corner of the console window.



Figure 59: Console Window (VNC)

Note:

- A VNC client may not function properly on all browsers. Some keys are not recognized when the browser is Chrome. It is observed that the VNC client works better on Firefox browser.
- To enable or disable the console support for a VM with one vGPU configured, see Enabling or Disabling Console Support for vGPU VMs.

Adding Multiple vGPUs to the Same VM

About this task

You can add multiple vGPUs of the same vGPU type when you create a new VM or update an existing VM.

- For information about how to create a VM, see Creating a VM through Prism Central (AHV).
- For information about how to update an existing VM, see Updating a VM through Prism Central (AHV).

For more information about multiple vGPU support, see Multiple Virtual GPU Support information in the *AHV Administration Guide*.

Before you begin

Ensure that the following prerequisites are met before you add multiple vGPUs to the VM:

- Select the license for NVIDIA Virtual GPU software version 10.1 (440.53) or later.
- Observe the guidelines and restrictions specified in Multiple Virtual GPU Support and Restrictions for Multiple vGPU Support.

Procedure

To add multiple vGPUs to the same VM, perform the following steps:

1. Click **Add GPU** in the **Resources** step of create VM workflow or update VM workflow. For more information, see Creating a VM through Prism Central (AHV) or Updating a VM through Prism Central (AHV)
2. In the **Add GPU** window, click **Add**.

   The License field is grayed out and you cannot select a different license when you add a vGPU for the same VM.

   The **VGPU Profile** is auto-selected. The system allows you to select additional vGPU of the same vGPU type as indicated by the message at the top of the **Add GPU** window.

   The newly added vGPU appears in the **Create VM** or **Update VM** window.
3. Repeat the steps for each vGPU addition to the VM.

VM Migration Specifications

VM migration can be performed in the following ways:

- *Live Migration* – This method is used to transfer the VM from one physical host to another host without affecting the normal functions and operations of the VM, and with minimal and often no interruption to the users of the VM.

  Live migration is supported for the following scenarios:

  - Intra-cluster live migration of guest VMs from one host to another host. For more information, see Migrating Within the Cluster on page 153.
  - Cross-cluster live migration (CCLM) of guest VMs protected with synchronous replication schedules. For more information, see Cross-Cluster Live Migration in the *Nutanix Disaster Recovery Guide*.
  - On-demand cross-cluster live migration of guest VMs across AHV clusters registered to the same or different Prism Central AZs. For more information, see On-Demand Cross-Cluster Live Migration on page 155.
- *Cold Migration* - This method is used to transfer the VM from one physical host to another host with minimal VM downtime. You can use **Nutanix Move** for Inter-cluster VM migration <Third-Party Hypervisor> to the AHV cluster. For more information, see Move User Guide.

  Note: The <Third-party hypervisors> are Xen (Amazon EC2), Microsoft Hyper-V, and VMware ESXi.

Live Migration Cases

VM live migration is applicable for the following cases:

- Maintenance activity required on the cluster - This scenario is applicable for a planned event (for example, scheduled maintenance of guest VMs) at the primary AZ when you put node into maintenance

mode. For information about how to configure a planned failover, see Cross-Cluster Live Migration section in *Nutanix Disaster Recovery Guide.*

- AHV or Firmware Upgrades - When you upgrade the AHV or Firmware, the VMs need to be live migrated to another AHV cluster.
- Load balancing or to isolate specific VMs on hosts.
- Changes in Host affinity policy.
- Acropolis Dynamic Scheduling (ADS)- If ADS detects a resource contention in the cluster, it creates a migration plan to eliminate the hotspots in the cluster by migrating VMs from one host to another. For more information about ADS, see Acropolis Dynamic Scheduling in AHV section in *AHV Administration Guide*.
- Defragmentation activity to create resources for VM power-on operation. This activity is performed when the cluster can accommodate resources for VM power-on operation after moving some VMs to another host.

Live Migration Restrictions

The following VM condition (or properties) impacts the VM Live migration.

- VM is powered off.
- VM is configured as an agent VM.

  You can select or clear the **Use this VM as an agent VM** checkbox to enable or disable this function when you create or update a VM. For more information, see Creating a VM through Prism Central (AHV).
- WSL2 is enabled. For more information about WSL2, see Windows Subsystem for Linux (WSL2) Support on AHV section in *AHV Administration Guide*.
- GPU passthrough is enabled.

  For information about how to verify if GPU passthrough is enabled for the VM, see Checking Live Migration Status of a VM on page 150.
- CPU passthrough is enabled.
- VM-Host affinity is set from the Prism Element web console with one host.

  For information about how to verify the VM-Host affinity policy from Prism Element web console, see Verifying Affinity Policy Association on page 151.
- VM Affinity policies are defined from Prism Central using VM Categories and Host categories.

  For information about how to verify the affinity policies mapped to a VM from Prism Central, see Checking Affinity Policies of a VM From Prism Central on page 152.
- Defragmentation activity to create resources for VM-power-on is in progress.

> **Note:** Starting with AOS 6.8 release, AHV supports the live migration of the guest VMs that have windows credential guard enabled. When you upgrade to AOS 6.8 or later release and enable HA reservation for the cluster, the system reserves the resources to accommodate the HA event. However, if you have the existing VMs in the cluster that have Windows Credential guard enabled, some guest VMs (both with or without windows credential guard enabled) might fail to start due to the unavailability of sufficient resources in the cluster. Ensure that you have sufficient resources available in the cluster to accommodate the HA reservation.
>
> For more information on windows credential guard, see Windows Defender Credential Guard Support in AHV in *AHV Administration Guide*.

For information on how to enable HA reservation, see Enabling High Availability for the Cluster section in *Prism Web Console Guide*.

Checking Live Migration Status of a VM

This section describes how to check whether the live migration is allowed for the VM.

Procedure

To check if a VM can be live migrated, perform the following steps:

1. Log on to the CVM as a nutanix user using SSH.
2. Run the following command:

   ```
   nutanix@cvm$ acli vm.get <VM_NAME> | grep 'allow_live_migrate
   ```

   Replace `<VM_NAME>` with the actual VM name at your site.

   The following attribute value confirms the live migration is allowed:

   ```
   allow_live_migrate: True
   ```

What to do next

If `allow_live_migrate: False` is returned for the above command, then check the status of the VM properties that restricts live migration.

The following table provides the information about the verification procedure to check the status of VM properties:

VM Properties	Verification Procedure

WSL2	Log on to the CVM as a Nutanix user using SSH, and run the following command:
	`nutanix@cvm$ acli vm.get <VM_NAME> | grep 'hardware_virtualization`
	Replace `<VM_NAME>` with the actual VM name at your site.
	The following attribute value confirms WSL2 is enabled:
	`hardware_virtualization: True`

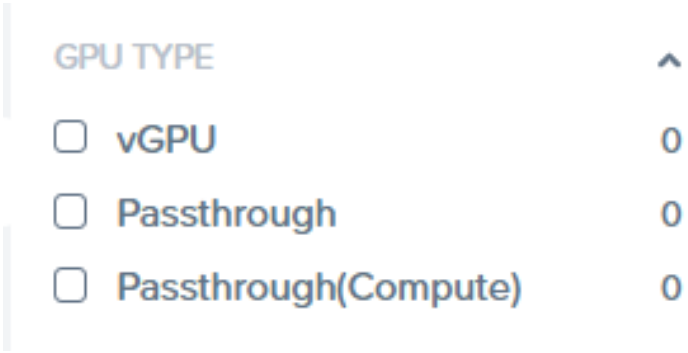
VM Properties	Verification Procedure
GPU	1. Log in to Prism Central. 2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar. The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment. 3. Apply the **GPU TYPE** filter from the **Modify Filter** option. The system displays the VMs based on the selected GPU criteria. 

Figure 60: GPU TYPE Filter

Verifying Affinity Policy Association

This section describes how to verify the VM-Host affinity from Prism Element web console and affinity policies mapped to the VM from Prism Central.

Procedure

To verify affinity policy association for a VM, perform the following checks:

- Checking VM-Host Affinity From Prism Element on page 151.
- Checking Affinity Policies of a VM From Prism Central on page 152.

Checking VM-Host Affinity From Prism Element

About this task

Using Prism Element, you can define the VM-host affinity policy that controls the placement of a VM. You can use this policy to specify that a selected VM can only run on the members of the affinity host list.

Procedure

To verify the VM-Host affinity, perform the following steps:

1. Log in to Prism element web console.
2. Navigate to **VM** > **Table**, and double-click the target VM name. The system displays the **Update VM** window.

3. Under **VM Host Affinity**, check the hosts specified for the VM.

> **Note:**
>
> VMs with Host affinity policies can only be migrated to the hosts specified in the affinity policy during an HA event. If only one host is specified, the VMs cannot be migrated.

Checking Affinity Policies of a VM From Prism Central

About this task

Using Prism Central, you can define the affinity policy based on VM Categories and Host categories.

Procedure

To verify the affinity policy associated with a VM, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.

   The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment.
3. Click the target VM name.
   The system displays the details view of the target VM.
4. Click the **Categories** tab in the target VM's details view.
   The system displays the Categories and Affinity Policy associated with the VM.

Defining Behaviour for Non-migratable VMs (GPU/CPU/PCI/Host Affinity configured VMs)

About this task

When an attempt is made for a host to enter maintenance mode, the VMs with GPU passthrough, CPU passthrough, PCI passthrough, and host affinity policies are not migrated to the other hosts in the cluster and therefore may block the attempt to enter maintenance mode.

To overcome this situation, Nutanix recommends you define either of the following behavior for these non-migratable VMs when host enters the maintenance mode:

- Automatically shutdown these non-migratable VMs.
- Set a block migration indication for these non-migratable VM.

Procedure

To define the above behaviors for non-migratable VMs, perform the following steps:

1. Log on to CVM with SSH.

2. Run the following command to put the host into maintenance mode with default action set for non-migratable VMs:

```
nutanix@cvm$ acli host.enter_maintenance_mode <Hypervisor-IP-address> [wait="{ true | false }" ]
 [non_migratable_vm_action="{ acpi_shutdown | block }"
```

   Replace:

   - `<Hypervisor-IP-address>` - with the actual host name at your site.
   - `wait`: Set the wait parameter to true to wait for the host evacuation attempt to finish.
   - `non_migratable_vm_action`: By default, this parameter is set to *block*, which means VMs with GPU, CPU passthrough, PCI passthrough, and host affinity policies are not migrated or shut down when you put a node into maintenance mode. If you want to automatically shut down such VMs for the duration of the maintenance mode, set this parameter to *acpi_shutdown*.

Migrating Within the Cluster

You can live-migrate a VM to another host within the cluster.

About this task

The **Migrate Within Cluster** option in the **Migrate VM** window allows you to migrate VMs to other hosts within the cluster.

Before you begin

Ensure that you observe the prerequisites as described in Live Migration of vGPU-enabled VMs on page 154 section, and the limitations described under Limitations for Live Migration information in *AHV Administration Guide*.

Procedure

To live migrate the VMs within the cluster, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment. For information about how to access the list of non-nutanix VMs managed by an external *vCenter*, see VMs Summary View on page 95.

3. Select the target VM checkbox in the **List** tab, and choose **Migrate** from the **Actions** dropdown menu. The system displays the **Migrate VM** window with **Migrate Within Cluster** option selected as default.

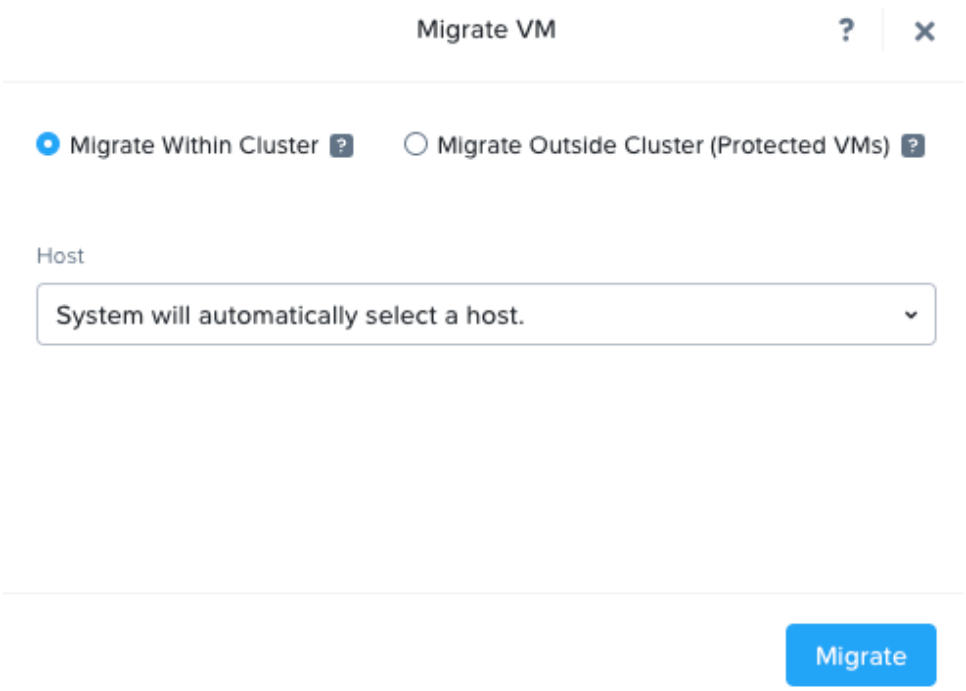


Figure 61: Migrate VM window

4. In the **Host** dropdown menu, perform either of the following actions:

   - Retain the `System will automatically select a host` default option if you want to migrate the VM to a host selected by the system.

     The system selects a host based on the GPU resources available with the host as appropriate for the VM to be migrated live.

   - Select the target host from the dropdown menu to which you want to migrate the VM.

5. Click **Migrate**.

   Prism submits the task and displays the following message:

   ```
   Successfully submitted migrate operation.
   Task details
   ```

   Task details is a link to the **Tasks** page. Click the **Task details** link to monitor the migration task in the **Tasks** page.

   The host name of the VM in the **List** view changes to the host name to which you migrated the VM.

Live Migration of vGPU-enabled VMs

You can live-migrate a vGPU-enabled VM to another host within the cluster.

> **Note:** Live migration of VMs with vGPUs is supported for vGPUs created with minimum NVIDIA Virtual GPU software version 10.1 (440.53).

You can perform live migration of VMs enabled with virtual GPUs (vGPU-enabled VMs) only on best effort basis, if the destination node is equipped to provide enough resources to the vGPU- enabled VMs. However, if the destination node is not equipped with the enough resources, the vGPU-enabled VMs are shut down and you might experience a downtime.

In a successful migration case, the vGPUs can continue to run while the VMs that are running the vGPUs are seamlessly migrated in the background.

When you perform the LCM update, the vGPU-enabled VMs are listed as Non-HA-protected VMs. LCM also migrates the Non-HA-protected VMs on best effort basis to the destination node if the following requirements are met:

- Destination node is equipped with the required resources for the VM.
- The VM GPU drivers are compatible with the AHV host GPU drivers.

If the destination node is not equipped with the enough resources or there is any compatibility issue between the VM GPU drivers and AHV host GPU drivers, the LCM forcibly shuts down the Non-HA-protected VMs.

Prerequisites

Ensure the following prerequisites are met before you live migrate the vGPU-enabled VMs:

- The VM is not powered off.
- The host affinity is not set for the VM.

  If the host affinity of the VM is set to only one host, you cannot migrate the VM. However, based on the GPU resources required, if the host affinity is set to multiple hosts with the same or similar GPU resources, you can migrate the VM among the hosts with which the affinity is set.
- You have another host in the same cluster that supports the resources necessary to support the vGPU-enabled VM that you want to live migrate.

Limitations

For limitations applicable to live migration of vGPU-enabled VMs, see Limitations for Live Migration in *AHV Administration Guide*.

On-Demand Cross-Cluster Live Migration

On-demand cross-cluster live migration (CCLM) enables you to migrate guest VMs (and all of their associated metadata like VM categories) across AHV clusters registered to the same or different Prism Central availability zones (AZs). You can live migrate (which ensures zero VM downtime) the guest VMs without the need to protect them with synchronous replication schedules or set up Nutanix Disaster Recovery from the Prism Central web console.

> **Note:** AHV Metro Availability also provides CCLM capability that is based on the Nutanix Disaster Recovery workflows. With AHV Metro CCLM, you can live migrate only the guest VMs protected with synchronous replication schedules. For more information on AHV Metro CCLM, see Cross-Cluster Live Migration in the *Nutanix Disaster Recovery Guide*.

You can live migrate a VM in the following situations:

- In an overlay subnet in a Prism Central AZ to an overlay subnet in another Prism Central AZ
- In an overlay subnet in a virtual private cloud (VPC) in a Prism Central AZ to an overlay subnet in another VPC in the same Prism Central AZ
- Within the same VPC in a Prism Central AZ

- In a VLAN subnet in a Prism Central AZ to a VLAN subnet in another Prism Central AZ
- In a VLAN subnet in a Prism Central AZ to another VLAN subnet in the same Prism Central AZ

A Layer 2 (L2) network extension creates a tunnel between the source and destination subnets so that the VMs in these subnets can communicate with each other. To ensure that dependent VMs on the source cluster and the destination cluster can communicate with the migrating VM throughout the live migration process, connect the source and the destination subnets using an L2 network extension before you live migrate a VM in the following scenarios:

- From an overlay subnet in a Prism Central AZ to an overlay subnet in another Prism Central AZ
- From an overlay subnet in a VPC in a Prism Central AZ to an overlay subnet in another VPC in the same Prism Central AZ
- From a VLAN subnet in a Prism Central AZ to a VLAN subnet in another Prism Central AZ
- From a VLAN subnet in a Prism Central AZ to another VLAN subnet in the same Prism Central AZ

> **Tip:** An L2 network extension is not required between the source and the destination subnets if you live migrate a guest VM within the same VPC subnet.

For successful live migration, Nutanix recommends that the round-trip latency between the clusters be 40 ms or less.

On-Demand CCLM Requirements

This section describes the requirements for live migrating guest VMs.

Table 30: Nutanix Software Requirements

Nutanix Software	Software Version Required
AOS	• 6.7 or later. While upgrading the AOS version from 6.6 to 6.7, ensure that the upgrade is completed before performing on-demand migration of the guest VM. • For OD-CCLM of vTPM-enabled guest VMs, 6.8 or later. Both the primary and recovery clusters must be running AOS 6.8 and later.
Prism Central	• pc.2023.3 or later. • For OD-CCLM of vTPM-enabled guest VMs pc.2024.1 or later.

Table 31: Prism Central User Requirements

Prism Central User	Permissions
Administrator	Only the administrator can perform on-demand live migration between the clusters registered to different Prism Central deployments.
Non-administrator	Non-administrators can perform on-demand live migration only between the clusters registered to the Prism Central deployment. The user must have the following permissions: • View_Prism_Central • View_Virtual_Machine • View_Subnet • View_Availability_Zone • Allow_Cross_Cluster_VM_Migration • View_Cluster

- Both the source and the destination subnet must have the same IP network prefix.
- If you did not enable the advanced processor compatibility feature for the guest VM, ensure that both the source and the destination cluster have identical CPU feature sets (set of CPU flags). Otherwise, live migration fails. For more information, see Advanced Processor Compatibility in AHV in the *AHV Administration Guide*.

  Live migration can happen even when the CPU types of the source and destination clusters do not match exactly. The destination cluster must support the superset of the CPU features of the source cluster.
- Both the primary and the recovery clusters must run on the same AHV version.
- Both the primary and the recovery clusters must have the same storage container name for the guest VMs.

  A storage container with the same name as the one on the primary cluster must exist on the recovery cluster. For example, if a *SelfServiceContainer* storage container exists on the source cluster, the destination cluster must also have a *SelfServiceContainer* storage container.

- If the primary and the recovery cluster (Prism Element) are in different subnets, open the ports listed on Ports and Protocols for communication.

  > **Tip:** If the primary and the recovery cluster (Prism Element) are in the same subnet, you do not need to open the ports manually.

  - To open the ports for communication from the primary cluster to the recovery cluster, run the following command on all CVMs of the source cluster:

    ```
    nutanix@cvm$ allssh 'modify_firewall -f -r remote_cvm_ip,remote_virtual_ip -p
     2030,2036,2073,2090 -i eth0'
    ```

    Replace *remote_cvm_ip* with the IP address of the destination cluster CVM. For multiple CVMs, replace *remote_cvm_ip* with the IP addresses of the CVMs separated by comma.

    Replace *remote_virtual_ip* with the virtual IP address of the recovery cluster.

  - To open the ports for communication from the recovery cluster to the primary cluster, run the following command on all CVMs of the destination cluster:

    ```
    nutanix@cvm$ allssh 'modify_firewall -f -r source_cvm_ip,source_virtual_ip -p
     2030,2036,2073,2090 -i eth0'
    ```

    Replace *source_cvm_ip* with the IP address of the source cluster CVM. For multiple CVMs, replace *source_cvm_ip* with the IP addresses of the CVMs separated by comma.

    Replace *source_virtual_ip* with the virtual IP address of the primary cluster.

    > **Note:**
    >
    > - Use the *eth0* interface only. *eth0* is the default CVM interface that shows up when you install AOS.
    > - For network segmentation enabled Nutanix cluster, use the *ntnx0* interface and run the following command:
    >
    >   ```
    >   nutanix@cvm$ allssh 'modify_firewall -f -r remote_cvm_ip,remote_virtual_ip
    >    -p 2030,2036,2073,2090 -i ntnx0'
    >   ```
    >
    >   Replace *remote_cvm_ip* with the IP address of the cluster CVM where you want to migrate the guest VMs. For multiple CVMs, replace *remote_virtual_ip* with the IP addresses of the CVMs separated by comma.

- The recovery cluster must have sufficient storage capacity to host the migrating guest VMs.
- The recovery cluster must be reachable from the source cluster.
- IP address management must be manually set up on both the primary and the recovery cluster.
- The guest VM to be live migrated must be powered on.

  The Prism Central web console filters out the guest VMs that are powered off.

On-Demand CCLM Limitations

Consider the following limitations before performing on-demand live migration of your guest VMs:

- On-demand live migration to Nutanix Cloud AZ (DRaaS) is not supported.
- On-demand live migration to Nutanix Cloud Cluster AZ (NC2) is not supported.

- On-demand live migration of guest VMs fails in the following scenarios:
  - Guest VMs are part of Flow Network Security policies.
  - Guest VMs are part of consistency groups.
  - Guest VMs have redundancy factor 1 (RF1).
  - GPU passthrough is enabled on guest VMs. For information on GPU passthrough verification, see Checking Live Migration Status of a VM in the *AHV Administration Guide*.
  - CPU passthrough is enabled on guest VMs. For information on GPU passthrough verification using acropolis CLI (acli), see vm in the Command Reference Guide.
  - Guest VMs are vNUMA VMs.
  - Guest VMs are in a paused state or have NVMe disks attached.
  - Memory overcommit is enabled on guest VMs.
  - Guest VMs are connected to a managed VLAN (IPAM-enabled).
  - Guest VMs are upgraded before on-demand live migration starts.

    When on-demand live migration is in progress, do not perform hotplug upgrades to the memory or CPU. Updates to NIC, disk, memory, and CPU are fatal while data is copied during migration.
  - Prism Central upgrade is in progress.
  - AHV upgrade is in progress.

    Similarly, if on-demand live migration is in progress, upgrading AHV fails.
  - LCM upgrade is in progress.
- After migrating a guest VM in an overlay subnet in a virtual private cloud (VPC) to an overlay subnet in another VPC, Prism Central does not retain the floating IP address of the guest VM if the VPCs are attached to different external subnets. Therefore, you must reassign the floating IP address to the migrated guest VM to access the guest VM from the external network.

  If the VPCs share the same external subnets, Prism Central retains the floating IP address of the guest VM.
- After migration to the recovery cluster, VM categories are not preserved if those categories do not exist on the recovery cluster.
- Data over the wire is not encrypted during the live migration.
- Automatic defragmentation on the recovery cluster is not supported.
- Guest VMs running on ESXi are not supported.

On-Demand CCLM Best Practices

Nutanix recommends the following best practices for live migrating your guest VMs (and all of their associated metadata like VM categories):

- Ensure that you set up the relevant user permissions. For more information, see On-Demand CCLM Requirements on page 156.

- Enable the advanced processor compatibility feature for the guest VM and select the oldest CPU generation to maximize the migration capability of the guest VM. For more information, see Advanced Processor Compatibility in AHV in the *AHV Administration Guide*.
- When on-demand live migration is in progress, do not protect the guest VM with a DR protection policy.
- When on-demand live migration is in progress, do not perform Nutanix software upgrades. For more information, see On-Demand CCLM Limitations on page 158.
- Do not perform on-demand live migration when Nutanix software upgrades are in progress. For more information, see On-Demand CCLM Limitations on page 158.
- When on-demand live migration is in progress, do not change IP addresses or other network configurations of the guest VMs.
- Nutanix recommends migrating up to 10 large-size and 60 small-size guest VMs in parallel.

  While no limit exists to the number of parallel migrations, the time required for successful migration depends on the guest VM size.
- When an administrator user s the guest VMs created by a non-administrator to a Nutanix cluster registered to a different Prism Central deployment, the administrator user becomes the owner of the guest VM after the VM migration. The ownership remains the same irrespective of who migrated the guest VM when the live migration happens between the Nutanix clusters registered to the same Prism Central deployment.

Performing On-Demand CCLM

If, due to a failure event (for example, scheduled maintenance of guest VMs) at the primary cluster, you must migrate your applications to another AHV cluster without VM downtime, perform an on-demand live migration to the recovery cluster.

Before you begin

See On-Demand CCLM Requirements on page 156, On-Demand CCLM Limitations on page 158, and On-Demand CCLM Best Practices on page 159.

About this task

To live migrate the guest VMs, follow these steps at the primary AZ:

Procedure

1. Log in to the Prism Central web console.
2. From **Application Switcher Function**, select the **Infrastructure** application, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**.
3. Select the guest VMs to live migrate.

   Warning: To see the guest VM configurations that cannot be migrated, see On-Demand CCLM Limitations on page 158.
4. Click **Migrate Across Clusters** from the **Actions** drop-down menu.

5. Do the following in the **Destination Cluster** tab:
   a. From the dropdown menu, under **Destination Location**, select the AZ to live migrate your guest VMs.
   b. From the dropdown menu, under **Destination Cluster**, select the AHV cluster to live migrate your guest VMs.
   c. Click **Next**.
6. Do the following in the **Network** tab:
   a. From the dropdown menu under **Destination Subnets**, select the network to map the subnet of the migrated guest VMs.
   b. Click **Next**.
7. Do the following in the **Migration Checks** tab:
   a. Review the status of the selected guest VMs after the prechecks run automatically.
      If any precheck fails, resolve the issue that is causing the failure and click **check again**.
   b. When all the **Checks** under the **Selected VMs** show OK, click **Migrate**.

   The selected guest VMs migrate to the recovery cluster with zero VM downtime.

Creating a VM through Prism Central (ESXi)

You can create virtual machines (VMs) in ESXi clusters through Prism Central.

Before you begin

Ensure that the following prerequisites are met before you create a VM in ESXi cluster:

- All the requirements, rules, and guidelines are considered, and the limitations are observed. For details, see External vCenter Server Integration on page 326.
- The vCenter Server is registered with your cluster. For more information about how to register a vCenter Server, see Registering External vCenter Server (Prism Central) on page 336.

Procedure

To create a VM in ESXi cluster, perform the following steps:

1. Log in to Prism Central.
2. Select **Infrastructure** application from Application Switcher Function, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
   The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment. For information about how to access the list of non-nutanix VMs managed by an external *vCenter*, see VMs Summary View on page 95.

3. Click **Create VM**, and enter the following information in the **Configuration** step:

   a. **Name**: Enter a name for the VM.

   b. **Description** (optional): Enter a description for the VM.

   c. **Cluster**: Select the target ESXi cluster from the dropdown list on which you intend to create the VM.

   d. **Number of VMs**: Enter the number of VMs you intend to create. The created VM names are suffixed sequentially.

   e. **vCPU(s)**: Enter the number of virtual CPUs to allocate to this VM.

   f. **Number of Cores per vCPU**: Enter the number of cores assigned to each virtual CPU.

   g. **Memory**: Enter the amount of memory (in GiBs) to allocate to this VM.

   The following is an example showing the **Configuration** step:

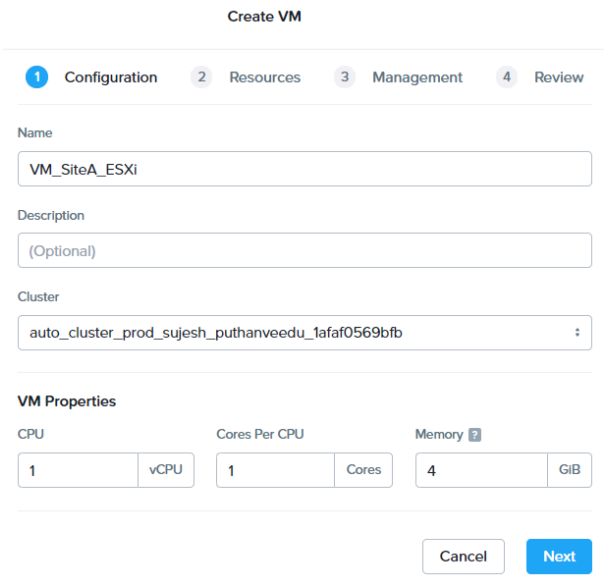


Figure 62: Create VM - Configuration

4. In the **Resources** step, perform the following actions to attach a Disk to the VM:

   Disks: Click **Attach Disk** , and enter the following information:

   a. **Type**: Select the type of storage device, **Disk** or **CD-ROM**, from the dropdown list.

   b. **Operation**: Specify the device contents from the dropdown list.

      - Select **Empty CD-ROM** to create a blank CD-ROM device. A CD-ROM device is needed when you intend to provide a system image from CD-ROM. The **Empty CD-ROM** option is available only when *CD-ROM* is selected as the storage device in the **Type** field.
      - Select **Allocate on Storage Container** to allocate space without specifying an image. Selecting this option means you are allocating space only. You have to provide a system image later from

a CD-ROM or other source. The **Allocate on Storage Container** option is available only when *Disk* is selected as the storage device in the **Type** field.

c. If you select **Allocate on Storage Container** in the **Operation** field, the system prompts you to specify the **Storage Container**. Select the appropriate storage container.

d. **Bus Type**: Select the bus type from the dropdown list.

   The options displayed in the dropdown list varies based on the storage device **Type** selected in the **Type** field.

   If the storage device **Type** is:

   - **Disk** - The available choices are **SCSI**, **SATA**, **PCI**, or **SATA**.
   - **CD-ROM** - The available choices are **IDE**, or **SATA**

e. **Path**: Enter the path to the desired system image.

f. **Capacity**: Enter the disk size in GiB.

g. When all the field entries are correct, click **Save** to attach the disk to the VM and return to the **Create VM** window.

Repeat this step to attach additional devices to the VM.

5. In the **Resources** step, perform the following actions to create a network interface for the VM:

   Networks: Click **Attach to Subnet**. The **Attach to Subnet** window appears.

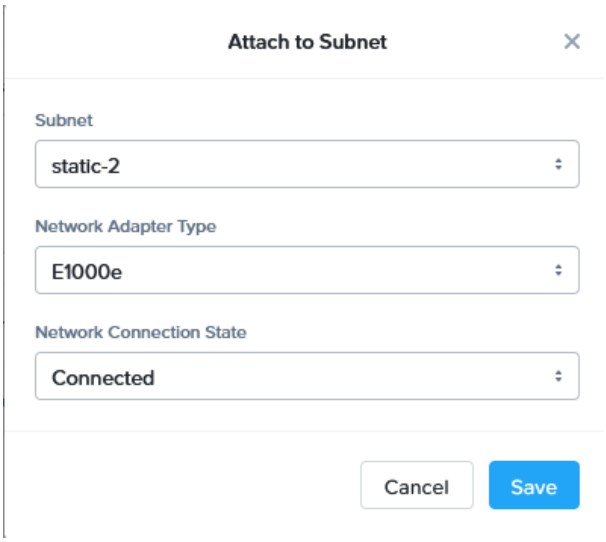


Figure 63: Attach to Subnet Window

   a. **Subnet**: Select the target subnet from the dropdown list.

      The list includes all the defined networks. For more information about how to perform the network configuration, see Creating VLAN Connections on page 347.

   b. **Network Adapter Type**: Select the network adapter type from the dropdown list.

      For information about the list of supported adapter types, see External vCenter Server Integration on page 326.

   c. **Network Connection State**: Select the state for the network after VM creation:

      - *Connected* - If the VM needs to be connected to the network to operate.
      - *Disconnected* - If the VM needs to be in disconnected state after creation.

   d. Click **Save** to create a network interface for the VM,and return to the **Create VM** window.

   Repeat this step to create additional network interfaces for the VM.

6. In the **Management** step, perform the following actions to define categories and timezone:

   a. **Categories**: Search for the category to be assigned to the VM. The policies associated with the category value are assigned to the VM.

   b. **Guest OS**: Type and select the guest operating system.

      The guest operating system that you select affects the supported devices and number of virtual CPUs available for the virtual machine. The Create VM wizard does not install the guest operating

system. For information about the list of supported operating systems, see External vCenter Server Integration on page 326.

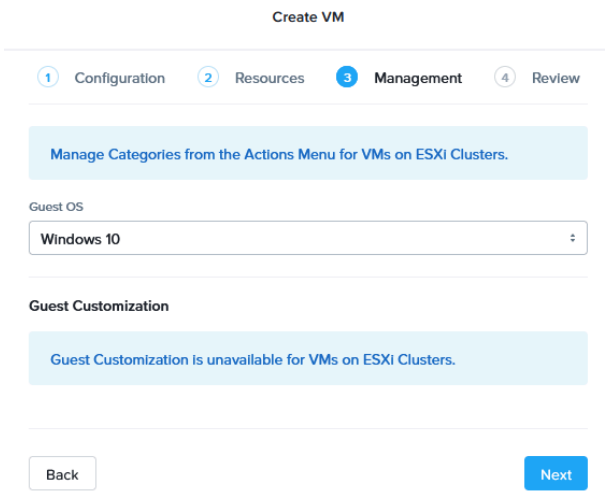


Figure 64: Create VM Window (Management)

7. In the **Review** step, when all the field entries are correct, click **Create VM** to create the VM, and close the **Create VM** window.

   The new VM appears in the VMs **Summary** page and **List** page.

Managing a VM through Prism Central (ESXi)

This section describes how to manage VMs in an ESXi cluster through Prism Central in **Nutanix** environment.

About this task

The procedure to manage VMs in an ESXi cluster in Nutanix environment is same as for AHV cluster, however the fields can vary when you create or manage a VM in an ESXi cluster. For information about the fields, see Creating a VM through Prism Central (ESXi) on page 161

About this task

To manage a non-nutanix VM on an external *vCenter*, you can use playbooks. For more information, see VMs Summary View on page 95.

> **Note:** Do not install any external software on the Prism Central VM.

Procedure

To manage a VM of an ESXi cluster in **Nutanix** environment:

- Perform the procedure and actions as described in Managing a VM through Prism Central (AHV) on page 134.

  You can perform only those operations for which you have permissions from the admin.

Nutanix Guest Tools

Nutanix Guest Tools (NGT) is a software package that comes bundled with AOS. You can install NGT in a guest virtual machine (VM) to enable advanced VM management functionalities provided by Nutanix.

Nutanix Guest Tools Overview

The NGT software package for Linux and Windows includes the following components:

- **NGT Installer**: Allows you to install NGT in a guest VM.
- **Nutanix Guest Agent (NGA) Service**: Maintains a communication channel between the Controller VM (CVM) and the guest VMs.
- **Nutanix VirtIO Package**: Includes the drivers required to run the VM on the AHV hypervisor. For more information about VirtIO drivers, see Nutanix VirtIO for Windows in *AHV Administration Guide*.
- **Python**: The NGA service is written in Python and is shipped with a dedicated installation of Python so it does not interact with the other components in the system.
- **Nutanix VSS package**: Enables Nutanix native in-guest Volume Snapshot Service (VSS) agent to take application-consistent snapshots for all the VMs that support VSS.

In addition, the NGT software package for Windows also includes the following components:

- A custom module that performs checks and fulfills all the prerequisites.
- Microsoft Visual C++ 2008/2012 x64 redistributable component
- Integration with Windows Performance Monitor for hypervisor statistics.

Installing NGT in a guest VM allows you to use the following advanced VM management features:

- **File Level Restore CLI**

  Performs self-service file-level recovery from the VM snapshots. For more information about self-service restore, see Self-Service Restore in the *Data Protection and Recovery with Prism Element* guide.

- **Nutanix VM Mobility**

  Facilitates VM migration between ESXi and AHV, in-place hypervisor conversion, and cross-hypervisor disaster recovery (CHDR) features. For more information about cross-hypervisor disaster recovery, see Nutanix Cross Hypervisor Disaster Recovery in the *Data Protection and Recovery with Prism Element* guide. For more information about in-place hypervisor conversion, see In-Place Hypervisor Conversion in the *Prism Element Web Console Guide*.

- **Application-consistent snapshots for Windows VMs**

  Enables Nutanix native in-guest Volume Snapshot Service (VSS) agent to take application-consistent snapshots for all the VMs that support VSS. This mechanism takes application-consistent snapshots without any VM stuns (temporary unresponsive VMs) and also enables third-party backup providers like CommVault and Rubrik to take application-consistent snapshots on the Nutanix platform regardless of which hypervisor is used in the cluster. For more information about Nutanix VSS-based snapshots for the Windows VMs, see the *Application-consistent Snapshots with Microsoft Volume Shadow Copy Service (VSS)* section in the Conditions for Application-consistent Snapshots topic of the *Data Protection and Recovery with Prism Element* guide.

- **Application-consistent snapshots for Linux VMs**

  Supports application-consistent snapshots for Linux VMs by running specific scripts on VM quiesce. For more information, see the Conditions for Application-consistent Snapshots information of the *Data Protection and Recovery with Prism Element* guide.

- **Static IP address preservation support after failover for Nutanix Disaster Recovery (DR)**

  This feature allows the preservation of the IP address of a guest VM (with a static IP address) for its failover (DR) to an IPAM network. For more information, see the *Networking Requirements* section in the Nutanix Disaster Recovery Requirements topic of the *Nutanix Disaster Recovery Guide*.

- **In-guest scripts execution support for Nutanix Disaster Recovery (DR)**

  In-guest scripts automate various task executions upon recovery of the VMs. For example, you can automate the task of changing the domain controller or performing the reassigning of the DNS IP address and reconnection to the database server at the recovery AZ. For more information about the tasks that can be automated using In-guest scripts, see Creating a Recovery Plan in the *Nutanix Disaster Recovery Guide*.

Nutanix Guest Tools Requirements

Ensure that the following requirements are met so that you can successfully install NGT, and use all the NGT features.

General Requirements

- NGT can be installed on VMs running Windows or Linux OS only. It cannot be installed on VMs running VMware Photon OS. For information about the supported OS for specific NGT features, see the NGT section in *Compatibility and Interoperability Matrix*.
- A virtual IP address must be configured for the Nutanix cluster. If you change the virtual IP address of the cluster, the reconfiguration impacts all the VMs in your cluster on which NGT is installed. For more information, see Virtual IP Address Impact in the *Prism Web Console Guide*.
- Network access from the virtual IP address of the cluster to the guest VMs where Prism Central-based management of NGT is required.
- Network access from the guest VM to the virtual IP address of the cluster where IP-based connectivity is used for NGT.
- VMs must have at least one empty IDE or SATA CD-ROM to attach the ISO required for the configuration and installation of NGT.
- The following ports must be accessible to use the specific NGT functionality:
  - If IP-based communication is enabled, the TCP port 2074 of the cluster virtual IP address must be accessible from the guest VMs so that the guest VMs can communicate with the CVM. For more information, see Nutanix Guest Agent and Controller VM Communication.
  - The TCP port 23578 in the guest VM must be accessible if you want to use the VSS service.

  For the complete list of required ports, see Port Reference.

Windows Requirements

In addition to the General Requirements, ensure that the following requirements are met so that you can successfully install NGT in a Windows VM:

- To install NGT, you need a local user account in the VM with administrative privileges. Domain accounts are currently not supported.
- For Windows Server Edition VMs, ensure that Microsoft Volume Shadow Copy Service (VSS) is enabled before you install NGT with the VSS application enabled. For more information about how to verify if Microsoft VSS is enabled on your server, see Microsoft documentation.

  Note:

  - Before you enable the VSS feature, upgrade the NGT version on the Windows Server Edition VMs to 2.3.2 or later. If not, the VSS snapshots will be marked as crash-consistent.
  - NGT's VSS feature is not supported on Windows Client Edition VMs or Linux VMs.

- During NGT installation a few PowerShell commands are executed. To run these commands, the PowerShell executable must be present in the PATH system variable of the environment. Otherwise, the installation of NGT might fail. For more information, see KB-7284.
- The PowerShell version on the Windows VMs must be 3.0 or later.
- Antivirus scanners might need exclusions added for the C:\Program Files\Nutanix directory for successful NGT installation.
- Windows Remote Manager Service (winrm) must be running and configured to allow SSL-based connections. The following commands are one of the many methods to configure winrm with SSL. These commands must be executed from an administrative Windows PowerShell console.

```
> $certificate = New-SelfSignedCertificate -DnsName $env:computername -
CertStoreLocation cert:\LocalMachine\My
```

```
> winrm create winrm/config/Listener?Address=*+Transport=HTTPS
 "@{Hostname=`"$env:computername`";CertificateThumbprint=`"$($certificate.ThumbPrint)`"}"
```

```
> cmd /c 'winrm set winrm/config/service/auth @{Basic="true"}'
```

```
> netsh advfirewall firewall add rule name=\"WinRM-HTTPS\" dir=in localport=5986
 protocol=TCP action=allow
```

> **Note:** Windows Remote Manager Service (winrm) is required to install NGT from Prism Central only. It is not required when you upgrade NGT or install NGT manually by logging in to the guest VM.

Linux Requirements

In addition to the General Requirements, ensure that the following requirements are met so that you can successfully install NGT in a Linux VM:

- To install NGT in bulk, ensure that any package manager configuration within the VMs works properly, as old or invalid configurations might prevent NGT package installation.
- Ensure that the VM has Python 2.6 or a later version installed.
- You must have a guest VM user account with password-based SSH, and root or passwordless SUDO access enabled.
- Ensure that the user has write permissions for the /usr/local directory as NGT is installed at this location.
- Ensure that the user has write permissions for the /mnt/nutanix/ngt directory to mount the NGT ISO at this location.
- Ensure that a minimum available disk space of 550 MB is available in the /mnt/nutanix/dir directory for copying the NGT installer when upgrading NGT.
- Ensure that the user has write access to /tmp directory for the duration of the installation.

General Notes

- NGT includes VirtIO drivers when you install it on a Windows VM. If these drivers are already installed in your guest VM, they might be replaced during the installation of NGT, depending on the version that is bundled with NGT. If the drivers were downgraded, you might need to manually reinstall VirtIO and restart the VM if prompted. For more information about VirtIO drivers, see Nutanix VirtIO for Windows in *AHV Administration Guide*. For information about the compatible VirtIO driver versions, see the *AOS - NGT - VM Mobility Matrix* section in the *NGT* tab of the Compatibility and Interoperability Matrix.
- VirtIO driver installation updates the NIC driver in the guest VM. During the update, the guest VM might lose network connectivity. The network connectivity is restored after the update is complete.

- If a VM is connected to a volume group (VG), NGT captures the iSCSI Qualified Name (IQN) of the VM and stores the information. If you change the IQN of the VM and take a snapshot of the VM before the NGT refresh cycle (currently at 5 minutes) occurs, NGT does not provide the auto restore capability because the snapshot operation cannot capture the VM-VG connection.

  Workaround:

  - **Windows VM**: In the command prompt, run the `net stop "Nutanix Guest Tools Agent" && net start "Nutanix Guest Tools Agent"` command.
  - **Linux VM**: Restart the Nutanix Guest Agent (NGA) service by running one of the following commands:
    - For guest VMs that support the **systemd** OS, run the `$ systemctl restart ngt_guest_agent` command.
    - For guest VMs that do not support the **systemd** OS, run the `$ sudo service ngt_guest_agent restart` command.
- By default, NGT client certificates expire every 1,000 days. Regenerate the certificates before they expire. For more information, see Regenerating NGT Certificates for Guest VMs information in the *Prism Element Web Console Guide*.

NGT Management in Prism Central

You can use Prism Central to perform the following operations on a guest VM or multiple guest VMs:

- Enable NGT and mount the NGT installer
- Install NGT
- Upgrade NGT
- Manage NGT applications

In addition, NGT installation through Prism Central provides the following capabilities:

- Enable Nutanix Volume Shadow Copy Service (VSS) and Self Service Restore (SSR) applications as part of the install workflow
- Select multiple VMs in Prism Central from the VM Entity browser and upgrade NGT on these VMs
- Defer restarting of the VMs to a specified later time and date after installing or upgrading NGT
- Define policies that allow you to defer restarting of the VMs to a specified later time and date

Installing NGT

The installation of NGT using Prism Central is fully automated. You do not need to manually log in to the VM to install NGT. For large-scale deployments, Nutanix recommends to use Prism Central to install NGT.

Before you begin

Ensure that all the requirements specified in Nutanix Guest Tools Requirements are met before you install NGT.

About this task

To install NGT, perform the following steps on a guest VM or multiple guest VMs at the same time in Prism Central:

Note:

- The guest VM must be powered on to install NGT in the VM.
- You cannot install NGT on VMs created on storage containers with replication factor 1.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and go to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default with VMs across all the registered clusters.

   Tip: The **NGT** status column associated with a VM displays whether the NGT is installed in the VM, whether it is the latest version, and whether an upgrade is available or not.

3. Select the target VM checkbox in which you want to install NGT, and choose **Install NGT** from the **Actions** dropdown menu.
   The system displays the **Install NGT** window.

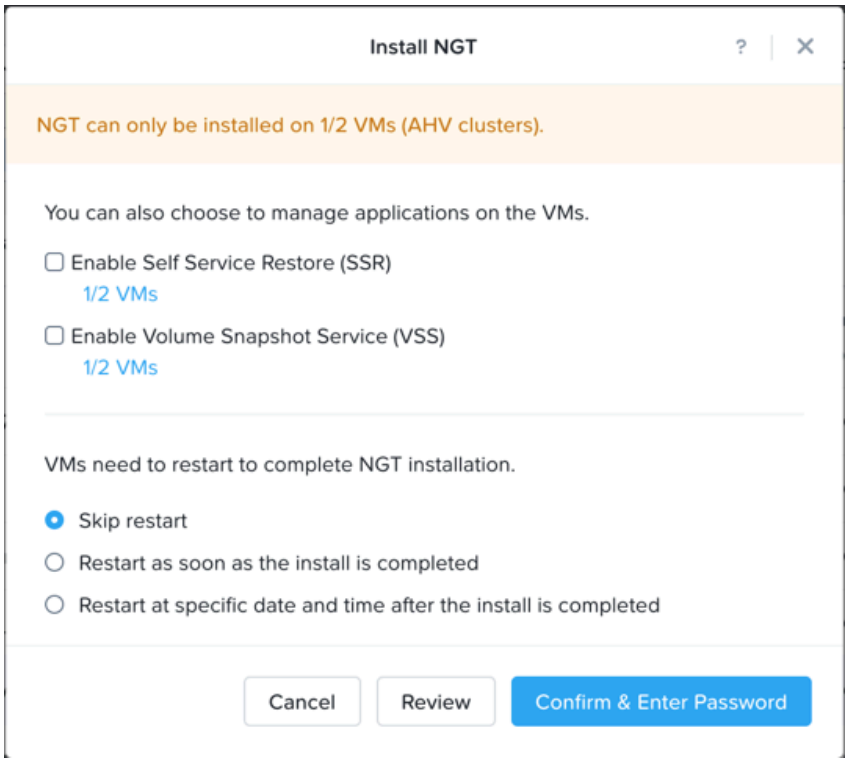


Figure 65: Installing NGT

   Note: If you select multiple VMs, this window displays the number of VMs on which you can install NGT. For example, if you select a VM on which NGT is already installed, it is skipped during this operation.

4. (Optional) To enable SSR and VSS applications, select the **Enable Self Service Restore (SSR)** and **Enable Volume Snapshot Service (VSS)** checkboxes.
   If you choose not to enable these features during the installation of NGT, you can do it later by following the instructions in Managing NGT Applications.

5. Select the restart schedule of the VM using either of the following options:

   - **Skip restart**: The VM does not restart after the installation completes.

     Note: If you select **Skip restart**, the system checks if any NGT policy is defined, and applies the restart action; **Restart as soon as the install is completed** or **Restart at specific date and time after the install is completed** based on the NGT policy (if defined). For more information about how to create an NGT policy, see Creating a NGT Policy on page 474.

   - **Restart as soon as the install is completed**: The VM restarts after the installation completes.
   - **Restart at specific date and time after the install is completed**: The VM restarts at the specific date and time that you configure in the **Date** and **Time** fields.

     Note: Nutanix recommends that you restart the VM after the NGT installation completes.

6. (Optional) Click **Review** to view your configurations.
7. Click **Confirm & Enter Password**.
8. In the **Username** and **Password** fields, enter a username and password of an account that meets the requirements specified in Nutanix Guest Tools Requirements, and is accessible to all the VMs on which NGT is being installed.

   Note: If you choose to install NGT on multiple VMs and the VMs do not have the same username and password, you can add them to a JSON file and paste the file in the box provided. Click **Download sample json** to download a sample of the JSON file.

9. Click **Done** to start the installation process.

   When the installation completes successfully on a VM, the **NGT** status column of the VM in the **List** tab displays the status as **Latest**. It takes a few minutes for the status to reflect in Prism Central because this is an asynchronous operation.

   Note: If the Nutanix Guest Tools Requirements are not met or you experience any issue with the installation process, the NGT installation fails and an alert message displays. Ensure that all the requirements are met and perform the installation process again to install NGT in the VMs.

10. (Optional) If you do not want to install NGT automatically or cannot provide the username and password of an account that meets the requirements, click **Skip and Mount** to complete the installation manually.

    Prism Central enables the NGT feature in the VM, mounts the NGT installer, and attaches an ISO to the virtual CD drive with the volume label NUTANIX_TOOLS to the selected VMs. You can then install NGT by logging in to the VM. For more information, see Installing NGT in a Windows VM or Installing NGT in a Linux VM in the *Prism Element Web Console Guide*.

    Note: If NGT is already installed in the VM, it detects the NUTANIX_TOOLS CD and reconfigures itself. Once NGT is installed and the reconfiguration is successful, the system automatically unmounts NUTANIX_TOOLS. For more information, see CD-ROM Eject Functionality of NGT.

Enabling NGT and Mounting the NGT Installer on Cloned VMs

If you have cloned a VM or multiple VMs from a VM that had NGT installed, perform the following steps to re-enable and configure NGT on the cloned VMs.

About this task

Perform the following steps to enable NGT and mount the NGT installer on cloned VMs.

Note: After you perform the following steps, you do not need to separately install NGT on the cloned VMs.

Procedure

1. Navigate to the **Install NGT** window by following the instructions mentioned in Steps 1 through 3 of Installing NGT.
2. Enable NGT and mount the NGT installer on the cloned VMs by following the instructions in Step 10 of Installing NGT (choosing **Skip and Mount**).
   NGT automatically identifies the ISO, updates the configuration, and unmounts the CD.

Managing NGT Applications

Prism Central allows you to enable or disable the Nutanix Volume Shadow Copy Service (VSS) and Self-Service Restore (SSR) applications even after NGT is installed in a guest VM.

About this task

Perform the following steps to enable the SSR and VSS applications if you have not enabled them during the NGT installation workflow. You can also disable these applications (if already enabled) after NGT is installed using this procedure.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default with VMs across all the registered clusters.
3. Select the target VM checkbox in which you want to enable or disable the SSR and VSS applications, and choose **Manage NGT Applications** from the **Actions** dropdown menu.
4. In the **Manage Applications** window, select the corresponding option to enable or disable applications.
5. Click **Confirm** to save the changes.
   When you enable an application, the **Services Enabled** field in the **Properties** widget of the **Summary** tab displays the services enabled for the VM. For example, if you enable the SSR application the **Services Enabled** field displays **SSR**.

Upgrading NGT

Prism Central allows you to upgrade NGT on the guest VMs.

Before you begin

- Ensure that all the requirements specified in Nutanix Guest Tools Requirements are met.
- Unless you upgrade AOS, you cannot upgrade NGT.
- Upgrading NGT using Prism Central is supported on VMs that have NGT version 1.2.3 or later. If the VM has an earlier version of NGT, upgrade NGT using the procedure in the Upgrading NGT topic in the *Prism Web Console Guide*.

About this task

Perform the following steps to upgrade NGT on a guest VM.

Note:

- You can upgrade NGT on a maximum of 60 VMs at the same time.
- For Linux VMs, upgrading a cluster running any NGT version prior to NGT 4.0 to NGT 4.0 or later versions, might fail. For more information, see KB-15396.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default with VMs across all the registered clusters.
3. Select the target VM checkbox in which you want to enable or disable the SSR and VSS applications, and choose **Upgrade NGT** from the **Actions** dropdown menu.
   The system displays the **Upgrade VMs** window.

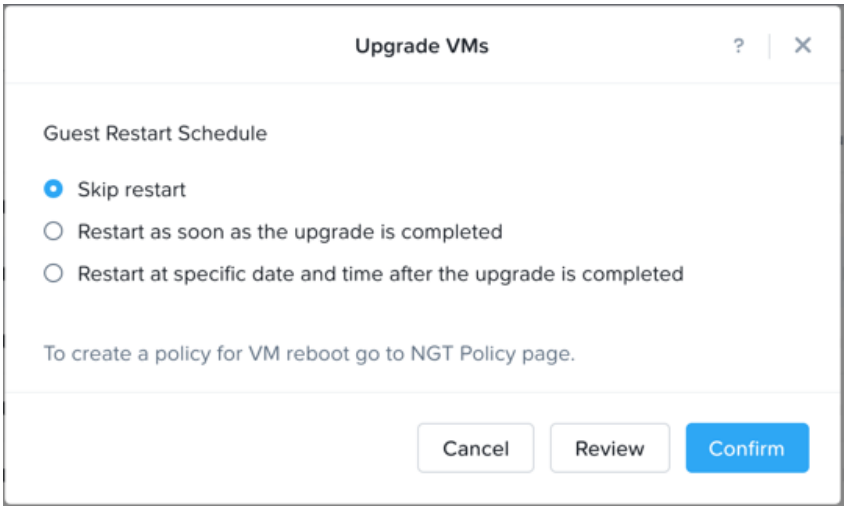


Figure 66: Upgrading NGT

4. In the **Upgrade VMs** window, select the restart schedule of the VMs using either of the following options:

   - **Skip restart**: The VM does not restart after the installation completes.
   - **Restart as soon as the install is completed**: The VM restarts after the installation completes.
   - **Restart at specific date and time after the install is completed**: The VM restarts at the specific date and time that you configure in the **Date** and **Time** fields.

   Note:

   - If you select multiple VMs to upgrade, the Upgrade VMs window displays the number of VMs on which you can upgrade NGT. For example, if you select a VM on which the latest version of NGT is already installed, that VM is skipped during this operation.
   - Nutanix recommends that you restart the VM after upgrading NGT.

5. (Optional) Click **Review** to view your configurations.

6. Click **Confirm** to start the upgrade process.

   When the upgrade is complete, the **NGT** status column associated with the VMs displays the status as **Latest**. It takes a few minutes for the status to reflect in Prism Central because this is an asynchronous operation.

   Note: If the Nutanix Guest Tools Requirements are not met or if you experience any issue with the upgrade process, the NGT upgrade fails and an alert message displays. Ensure that all the prerequisites are met and perform the upgrade process again to upgrade NGT.

Uninstalling NGT

Prism Central does not support automatic uninstallation of NGT.

You must log in to a guest VM to uninstall NGT in that VM. For more information, see Uninstalling and Removing Nutanix Guest Tools in the *Prism Element Web Console Guide*.

Note: If the NGT Status in Prism Central displays **Latest** after uninstalling NGT, follow the instructions mentioned in Step 3 of Uninstalling and Removing Nutanix Guest Tools in the *Prism Element Web Console Guide* to remove the NGT information from Prism Central.

Manage Bulk Operations for NGT

You can install or upgrade NGT in bulk on multiple guest virtual machines (VMs) using third-party endpoint management tools, such as Microsoft Intune or HCL BigFix, or automation tools, such as Ansible. Using these management tools, you can also remove NGT in bulk from guest VMs.

Bulk installation of NGT is supported on guest VMs running AOS 6.7 or later versions only.

The Nutanix Support portal lists the following NGT installer files:

- EXE file for Windows OS
- TGZ file for RPM-based Linux OS
- TGZ file for DEB-based Linux OS
- Nutanix NGT GnuPG public key

Download the latest installer files to install or upgrade NGT in bulk.

Note: Bulk installation of NGT using third-party endpoint management tools does not require Prism Central. However, you must enable and mount NGT in guest VMs using Prism Central after installing NGT in VMs. For more information, see Enable and Configure NGT.

Prepare the NGT installation files for Distribution

You can install NGT using the installer files available in the Nutanix Support portal in a single VM or, in bulk, on multiple VMs. When you prepare to install NGT in bulk on multiple VMs, download the installer files and make them available for use by the third-party endpoint management tool deployed at your site. The instructions in this document assume that the third-party endpoint management tool deployed at your site requires that you host the NGT installer files on a web server.

Hosting the files for Windows VMs

Before you begin

Ensure that the NGT version is compatible with the AOS version installed in your cluster.

Procedure

1. Go to the Nutanix Support portal, select **Downloads** > **NGT**, and download the *nutanix-guest-agent-<version>.exe* installer file for Windows, which matches the AOS version installed in your clusters.
2. Host this installation file directly on the web server.

Hosting the files for Red Hat Package Manager (RPM) based VMs

Before you begin

Ensure that the NGT version is compatible with the AOS version installed in your cluster.

Procedure

1. Go to the Nutanix Support portal, select **Downloads** > **NGT**, and download the *nutanix-guest-agent-rpm-<version>.tar.gz* installer file for RPM-based distributions, which matches the AOS version installed in your clusters.
2. Extract the *nutanix-guest-agent-rpm-<version>.tar.gz* file, and host the *NUTANIX-NGT-GPG-KEY* file and the *ngt_repo* directory on the web server.

Hosting the files for Debian (DEB) based VMs

Before you begin

Ensure that the NGT version is compatible with the AOS version installed in your cluster.

Procedure

1. Go to the Nutanix Support portal, select **Downloads** > **NGT**, and download the *nutanix-guest-agent-deb-<version>.tar.gz* installer file for DEB-based distributions, which matches the AOS version installed in your clusters.
2. Extract the *nutanix-guest-agent-deb-<version>.tar.gz* file, and host the i386 and amd64 directories on the web server.

3. (Optional) Perform the following steps to verify the DEB installer packages against the detached signatures using the *NUTANIX-NGT-GPG-KEY* file:

   a. Run the following command to import the public key:

   ```
   $ gpg --import NUTANIX-NGT-GPG-KEY
   ```

   The following is an example.

   ```
   $ gpg --import NUTANIX-NGT-GPG-KEY
   gpg: key 42DBF8BB: public key "Nutanix, Inc. (NGT Packaging)
    <security@nutanix.com>" imported
   gpg: Total number processed: 1
   gpg:               imported: 1  (RSA: 1)
   ```

   b. Run the following command to verify the DEB installer packages against the detached signatures:

   ```
   $ gpg --verify os-arch/nutanix-guest-agent.deb.asc os-arch/nutanix-guest-
   agent_version-1_os-arch.de
   ```

   Replace *os-arch* with the architecture of the OS of guest VM, and *version* with the NGA version.

   The following is an example.

   ```
   $ gpg --verify i386/nutanix-guest-agent.deb.asc i386/nutanix-guest-
   agent_4.0-1_i386.deb
   gpg: Signature made Wed 24 May 2023 01:46:29 PM UTC using RSA key ID 42DBF8BB
   gpg: Good signature from "Nutanix, Inc. (NGT Packaging) <security@nutanix.com>"
   gpg: WARNING: This key is not certified with a trusted signature!
   gpg:          There is no indication that the signature belongs to the owner.
   Primary key fingerprint: D8B0 18BD CFEB 774C D157  F0A5 11B1 600F 42DB F8BB
   ```

Install NGT in Bulk on Multiple VMs

You can install NGT in bulk on multiple Windows and Linux guest VMs using the NGT installer files available in the Nutanix Support portal.

Installing NGT in Bulk on Windows VMs

Before you begin

- Ensure that the cluster meets all NGT requirements. For more information, see Nutanix Guest Tools Requirements on page 167.
- Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.
- Review the end user license agreement (EULA) for Nutanix Guest Tools using a manual installation because the following installation procedure requires you to accept the EULA automatically.

Procedure

1. Configure the third-party endpoint management tool deployed at your site to distribute the *nutanix-guest-agent-<version>.exe* file to the VMs where NGT is installed.

   For more information, see the tool-specific documentation.

2. Configure the third-party endpoint management tool to install NGT by running one of the following commands:

   » `C:\ngtinstaller> nutanix-guest-agent-version.exe /quiet ACCEPTEULA=yes /norestart`

   Replace *version* with the NGA version.

   Use this command to ensure that VMs do not restart after you install NGT.

   > **Note:** This command might update the Nutanix VirtIO drivers if no Nutanix VirtIO drivers are installed or if a newer version is available, but the updated functionality of the VirtIO drivers is available only after a VM restart.

   » `C:\ngtinstaller> nutanix-guest-agent-version.exe /quiet ACCEPTEULA=yes`

   Replace *version* with the NGA version.

   Use this command to automatically restart the VM and to make all the updated VirtIO driver functionalities to be available in the VM.

3. (Optional) To generate the NGT logs in a location other than the %TEMP% directory, install NGT by running the following command.

   `C:\ngtinstaller> nutanix-guest-agent-version.exe /quiet ACCEPTEULA=yes /log log_file`

   Replace *version* with the NGA version, and *log_file* with the filename to write the logs.

   Ensure that the directory containing the filename that you provide has the necessary write permissions. Also, the installation process adds some events to the Windows application event log.

What to do next

After successful installation, enable and configure NGT in guest VMs. For more information, see Enable and Configure NGT.

Installing NGT in Bulk on Linux VMs

About this task

This sample procedure provides steps to install NGT on Red Hat Package Manager (RPM) based operating systems. Use this procedure as a template to install NGT on Debian-based operating systems.

Before you begin

- Ensure that the cluster meets all NGT requirements. For more information, see Nutanix Guest Tools Requirements on page 167.
- Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.

Procedure

1. To verify the package signatures, configure the third-party endpoint management tool deployed at your site to install the NUTANIX-NGT-GPG-KEY file on RPM-based operating systems.

   For more information, see the tool-specific documentation.

2. Configure the third-party endpoint management tool to set up the repositories.

   For more information, see the tool-specific documentation.

   For example, guest VMs running RedHat 8.x distribution might need a repository configuration in /etc/yum.repos.d/nutanix-guest-tools.repo similar to the following configuration:

   ```
   [NutanixGuestTools]
   name=Nutanix Guest Tools
   baseurl=http://local-web-server/ngt_repo
   enabled=1
   gpgcheck=1
   gpgkey=http://local-web-server/RPM-GPG-PUBLIC-KEY
   repo_gpgcheck=0
   ```

   Replace *local-web-server* with the name of the web server used to distribute the NGT installer files as described in Preparing the NGT installation files for the Distribution.

3. Configure the third-party endpoint management tool to install the Nutanix guest agent package by running the package manager-specific install command.

   For example, the yum install -y nutanix-guest-agent command installs Nutanix guest agent package using the yum package manager for RedHat-based distributions.

   ```
   [nutanix@localhost ~]$ yum install -y nutanix-guest-agent
   ```

   For information about the install command specific to the package manager at your site, see the package manager-specific documentation.

What to do next

After successful installation, enable and configure NGT in guest VMs. For more information, see Enable and Configure NGT.

Enable and Configure NGT

Use Prism Central to enable and configure NGT in VMs so that you can use the NGT applications such as self-service restore, volume snapshot service, and application-consistent snapshots. The initial configuration of NGT requires mounting an ISO into the CD-ROM drive of guest VMs. The NGT agent detects the ISO and performs the initial configuration, making connections to the CVM.

Enabling and Configuring NGT using Prism Central

Before you begin

- Ensure that the cluster meets all NGT requirements. For more information, see Nutanix Guest Tools Requirements on page 167.
- Ensure that you install NGT in the VMs.

  Note: Because NGT is installed, you do not require WinRM or SSH access to the VM or a local user account in the VM with administrative privileges.

Procedure

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function on page 19, and go to **Compute & Storage** > **VMs** from the **Navigation Bar**.
   The system displays the **List** tab by default with VMs across all the registered clusters.

   > **Tip:** The **NGT** status column associated with a VM displays whether the NGT is installed in the VM, whether it is the latest version, and whether an upgrade is available or not.

3. To enable and configure NGT in a VM, select the target VM checkbox and choose **Install NGT** from the **Actions** dropdown menu.
   The system displays the **Install NGT** window.

   > **Note:** The Install NGT workflow is the same for installing NGT and enabling and configuring NGT if NGT is already installed.

4. To enable SSR and VSS applications, select the **Enable Self Service Restore (SSR)** and **Enable Volume Snapshot Service (VSS)** checkboxes.
   If you choose not to enable these features during NGT configuration, you can do it later by following the instructions in Managing NGT Applications.

5. Select **Skip restart** as the restart schedule.

   > **Note:** Because NGT is already installed in the VM, a restart is not required during NGT configuration.

6. Click **Confirm and Enter Password**.

7. Click **Skip and Mount**.
   Prism Central enables the NGT feature in the VM, mounts the NGT installer, and attaches an ISO to the virtual CD drive with the volume label NUTANIX_TOOLS to the selected VMs.

   > **Note:** Because NGT is already installed in the VM, it detects the NUTANIX_TOOLS CD and reconfigures itself. After NGT is installed and the reconfiguration is successful, the system automatically unmounts NUTANIX_TOOLS. For more information, see Automatic CD-ROM Ejection on page 185.

What to do next

The Nutanix Guest Agent (NGA) service in the VMs starts periodic communication with the CVM. To verify whether the NGA service is communicating with the CVM, log in to the CVM and run the following command:

```
nutanix@cvm$ nutanix_guest_tools_cli list_vm_tools_entities include_vm_info=true
 vm_name=vm-name
```

Replace `vm-name` with the name of one of the VMs.

Upgrade NGT in Bulk on Multiple VMs

You can upgrade NGT in bulk on multiple Windows and Linux guest VMs using the NGT installer file available in the Nutanix Support portal.

Upgrading NGT in Bulk on Windows VMs

Before you begin

- Ensure that the NGT version is compatible with the AOS version installed in your cluster. For more information, see the NGT section in the *Compatibility and Interoperability Matrix*.

- Ensure that the cluster meets all NGT requirements. For more information, see Nutanix Guest Tools Requirements on page 167.
- Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.

Procedure

- Perform Step 1 to Step 3 in Installing NGT in Bulk on Windows VMs.

  The installer detects that an existing NGT version is already present on the VM and performs an upgrade.

Upgrading NGT in Bulk on Linux VMs

About this task

This sample procedure provides steps to upgrade NGT on Red Hat Package Manager (RPM) based operating systems. Use this procedure as a template to upgrade NGT on Debian-based operating systems.

Before you begin

- Ensure that the NGT version is compatible with the AOS version installed in your cluster. For more information, see the NGT section in the *Compatibility and Interoperability Matrix*.
- Ensure that the cluster meets all NGT requirements. For more information, see Nutanix Guest Tools Requirements on page 167.
- Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.

Procedure

1. To verify the package signatures, configure the third-party endpoint management tool deployed at your site to install the NUTANIX-NGT-GPG-KEY file on RPM-based operating systems.

   For more information, see the tool-specific documentation.

2. Configure the third-party endpoint management tool to set up the repositories.

   For more information, see the tool-specific documentation.

   For example, guest VMs running RedHat 8.x distribution might need a repository configuration in /etc/yum.repos.d/nutanix-guest-tools.repo similar to the following configuration:

   ```
   [NutanixGuestTools]
   name=Nutanix Guest Tools
   baseurl=http://local-web-server/ngt_repo
   enabled=1
   gpgcheck=1
   gpgkey=http://local-web-server/RPM-GPG-PUBLIC-KEY
   repo_gpgcheck=0
   ```

   Replace *local-web-server* with the name of the web server used to distribute the NGT installer files as described in Preparing the NGT installation files for the Distribution.

3. Configure the third-party endpoint management tool to upgrade the Nutanix guest agent package by running the package manager-specific upgrade command.

   For example, the yum update -y nutanix-guest-agent command upgrades Nutanix guest agent package using the yum package manager for RedHat-based distributions.

   ```
   [nutanix@localhost ~]$ yum update -y nutanix-guest-agent
   ```

   For information about the upgrade command specific to the package manager at your site, see the package manager-specific documentation.

Uninstall NGT in Bulk from Multiple VMs

You can uninstall NGT in bulk from guest VMs using the third-party management tool deployed at your site.

> **Note:** Before uninstalling NGT from a guest VM, ensure the communication link between guest VM and CVM remains active. The CVM displays that NGT is uninstalled only if the communication between CVM and guest VM is active during the uninstallation. If the communication link is down, CVM continues to display that NGT is installed on the guest VM even after the successful uninstallation of NGT. For information about how to verify that the communication link is active, see Step 4 in Enabling NGT and Mounting the NGT Installer on Cloned VMs of the *Prism Element Web Console Guide*.

Uninstalling NGT from Windows VMs

About this task

When you install NGT in a Windows VM, NGT registers an uninstaller in the VM that can be accessed manually using Add/Remove Programs in the Windows Control Panel. This uninstaller can also be used by a third-party endpoint management tool to remove NGT from the VM.

Before you begin

Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.

Procedure

- Configure the third-party endpoint management tool to uninstall the Nutanix Guest Agent package using the uninstaller registered with Add/Remove Programs in the Windows Control Panel.

  For more information, see the tool-specific documentation or Microsoft Windows documentation.

Uninstalling NGT from Linux VMs

About this task

This sample procedure provides steps to remove NGT on Red Hat Package Manager (RPM) based operating systems. Use this procedure as a template to remove NGT on Debian-based operating systems.

Before you begin

Ensure that you registered the VMs with the third-party endpoint management tool deployed at your site. For more information, see the tool-specific documentation.

Procedure

- Configure the third-party endpoint management tool to uninstall the Nutanix guest agent package in bulk by running the package manager-specific removal command.

  For example, the yum remove -y nutanix-guest-agent command uninstalls Nutanix guest agent package using the yum package manager for RedHat-based distributions.

  ```
  [nutanix@localhost ~]$ yum remove -y nutanix-guest-agent
  ```

  For information about the removal command specific to the package manager at your site, see the package manager-specific documentation.

Nutanix Guest Agent and Controller VM Communication

You can set up connectivity between the controller virtual machine (CVM) and the guest VMs using the Nutanix Guest Tools (NGT) service that runs on the CVM and the Nutanix Guest Agent (NGA) service that runs on the guest VMs in the Nutanix cluster. After you install NGT in a guest VM, the NGA service in the guest VM starts periodic communication with the CVM based on the type of communication in a VM:

- **IP-less**: Communication between NGA and CVM happens only over a serial port connected to the guest VM.
- **IP-based**: NGA communicates with the CVM over SSL by connecting to the virtual IP of the CVM on port 2074.

By default on AHV clusters, the NGA service communicates with the CVM over IP-less connections using the first serial port on the guest VM. If the CVM does not respond, NGA reverts to IP-based communication.

For more information about how to check the communication type in a guest VM, to verify whether the NGA is communicating with the CVM, or to verify whether NGA is communicating with the CVM using IP or without an IP, see Communication Type Verification.

The communication type used between NGA and the CVM is determined when the guest VM starts. NGA might select an alternative communication type following a failover event or an event that requires a VM restart, such as disaster recovery or high availability.

IP-less Communication

In IP-less communication, the NGA service in the guest VM starts periodic communication with the CVM over the first serial port on the guest VM. The NGA service communicates with the CVM by sending remote procedure calls (RPCs) over the serial port to the CVM. The communication link over the serial port becomes active when NGA receives a response from the CVM. If the CVM does not respond, NGA reverts to IP-based communication.

> **Note:**
>
> - Only AHV clusters support IP-less communication.
> - Nutanix recommends that the virtual IP port 2074 on the CVM is accessible so that NGA can revert to IP-based communication in case of any failures.

IP-less communication enhances the security of the communication link because it does not require the CVM to be accessible by the VM over the network, and identification of the VM is guaranteed by the hypervisor without in-guest certificates.

Prerequisites and Requirements

IP-less communication between the CVM and the guest VMs is established automatically when the following prerequisites and requirements are met:

- The guest VM must be running on AOS 6.6 or later, and NGT 3.0 or later versions.

- NGT is installed. For information about how to install NGT, see:
  - NGT Installation to install using Prism Element web console.
  - Installing NGT on page 169 to install using Prism Central.
- If an older version of NGT is already installed on the guest VM, you must upgrade it to the latest version. For information about how to upgrade NGT, see:
  - Upgrading NGT to upgrade using Prism Element web console.
  - Upgrading NGT on page 172 to upgrade using Prism Central.
- To switch an existing guest VM from IP-based communication to IP-less communication, Nutanix recommends that you upgrade AHV and AOS to the latest version, then restart the VM when installing or upgrading NGT on the VM. If you do not restart the VM, the serial port remains deactivated and the NGA service continues to communicate with the CVM using the virtual IP port 2074 on the CVM. After NGT is installed or upgraded, you must power cycle the VM to activate the serial port that is attached to it before IP-less communication can be used. An in-guest reboot might not be sufficient.

IP-based Communication

With IP-based communication, after you install NGT in a guest VM, the NGA service in the guest VM starts periodic communication with the CVM over SSL connections.

> **Note:** AHV, ESXi, and mixed clusters support IP-based communication.

Each Nutanix cluster is configured as a certificate authority (CA). When NGT is enabled in a VM, a certificate pair is generated specifically for that VM and it is embedded in an ISO that is configured for that VM. The security certificates are installed inside the VM as part of the installation process.

The NGA service inside the guest VM initiates an SSL connection to port 2074 of the cluster virtual IP address to communicate with the CVM. Any firewall must be configured to allow the guest VM to reach port 2074 on the cluster virtual IP address. For the complete list of required ports, see Port Reference.

NGT provides three levels of security for VM communication:

- SSL certificates that ensure a secure TCP connection between the CVM and the guest VM
- Capability-based authorization that ensures only NGT features that are supported by the cluster are enabled on the guest VM.
- NGT ensures that the communication is established only if the system or BIOS UUID of the guest VM and the UUID of the guest VM (provided by the hypervisor) stored in the CVM are the same.

Communication is successful only if all the three conditions are met. For example, if a VM that has NGT installed is cloned, the new VM cannot communicate with the CVM. You must separately enable NGT, and mount the NGT installer on the cloned VM. The NGT installer includes configuration specific to the VM, and when the VM is re-configured and is able to communicate with the CVM, it automatically unmounts the installation media. You do not need to separately install NGT again on the cloned VMs.

NGA also publishes information about the VM to the CVM, for example, guest OS type, status of VM mobility, and VSS services.

Communication Type Verification

You can verify the type of communication established between the controller VM (CVM) and the guest VMs using Prism Central or the CVM SSH (CLI) console.

Verifying Communication Type Using Prism Central

You can verify the type of communication established between the CVM and the guest VM using Prism Central.

About this task

To verify the communication type using Prism Central, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default with VMs across all the registered clusters.
3. Click **Modify Filters** option to access the list of available filters.
4. In the **NGT COMMUNICATION TYPE** filter, select the **IP-based** or **IP-less** checkbox to filter the VMs based on the NGT communication type.
   The system displays the list of VMs based on the selected options.

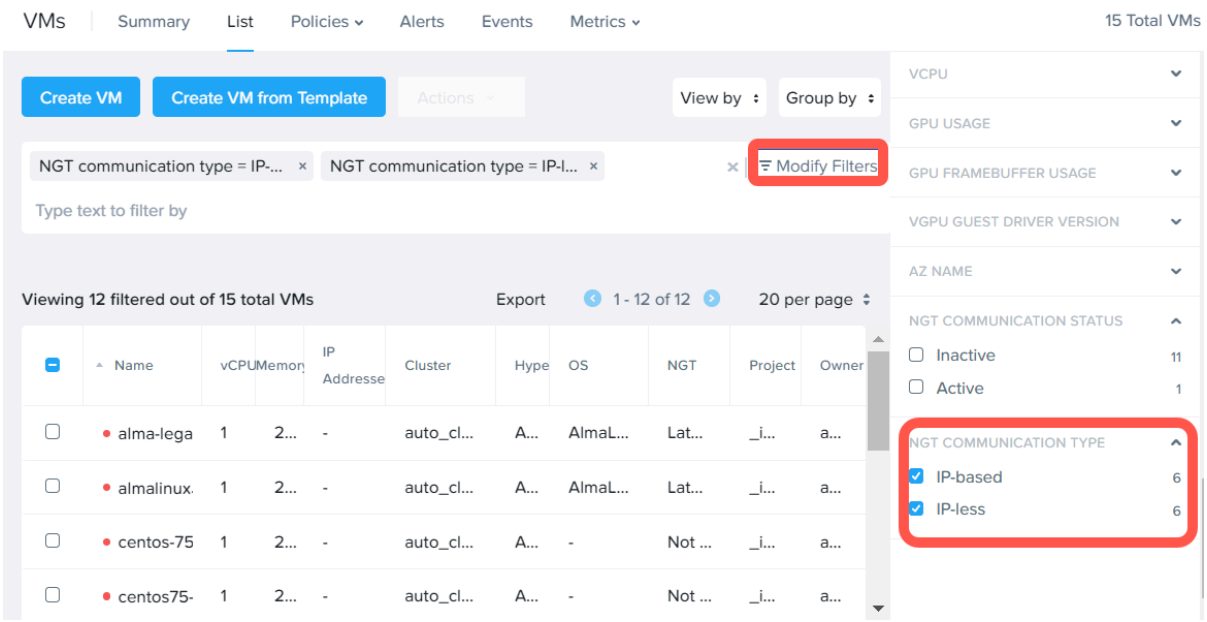


Figure 67: IP-Based and IP-Less Filter

Note: To check the VMs on which NGT is installed, select the **Installed** checkbox in the **NUTANIX GUEST TOOLS** filter. The system displays the list of VMs on which NGT is installed.

Verifying Communication Type Using CLI

You can verify the type of communication established between CVM and guest VM using CVM SSH (CLI) console.

About this task

To verify the communication type using the CVM SSH console, perform the following steps:

Procedure

1. Log in to any CVM in the cluster as a Nutanix user with SSH.
2. Run the following command:

```
nutanix@cvm $ nutanix_guest_tools_cli list_vm_tools_entities include_vm_info=true
 vm_name=vm-name
```

   Replace `vm-name` with the name of the guest VM.

   Observe the following attributes in the command output:

   - communication_link_active = true - Indicates that the NGA is communicating with the CVM.
   - communication_link_over_serial_port_active = true - Indicates that the communication between NGA and the CVM is IP-less.
   - communication_link_over_serial_port_active = false - Indicates that the communication between NGA and the CVM is over IP.

Automatic CD-ROM Ejection

After NGT is installed or re-configured in a guest VM, the CD-ROM is auto-ejected from the VM in the following stages.

1. CD-ROM is automatically ejected from the VM immediately after the installation of NGT is successfully completed.
2. NGA indicates to the controller VM (CVM) that the installation is complete and the CD-ROM is detached from the VM through the hypervisor. This operation depends on the communication between the guest VM and the CVM and may take up to 10 minutes.

   Note:

   - These operations can occur at different times. It is possible that the CD-ROM shows up as empty inside a VM, but the status in the NGT-Controller VM service Tools Mounted might display as true. If this situation occurs, unmount the CD-ROM using the Prism Element web console..
   - If the NGT software version in the ISO is more recent than the installed version in the guest VM, the CD-ROM does not eject automatically. This functionality enables the upgrade of the NGT software inside the VM.

NGT Usage in Disaster Recovery

If NGT is enabled on a guest VM that is protected by Nutanix Disaster Recovery, the snapshots of the VM include NGT relevant information along with its capabilities.

The NGT information is preserved for a restored guest VM in the following scenarios:

- Migrating the VM to the remote cluster (Planned Failover)
- Performing an in-place restore of the VM on the source cluster
- Creating a clone of the VM on the source cluster

In these scenarios, a new NGT ISO image containing only the relevant configuration information (SSL certificates, Controller VM IP address, ans so on) is created for the recovered guest VM and the image is

automatically attached to the VM. When the VM is powered on, the NGA service running on the VM copies the relevant configuration information and detaches the NGT ISO CD-ROM automatically.

The NGT information is not preserved for a restored guest VM in the following scenarios:

- Performing an out-of-place restore of the VM on the remote cluster.
- Retrieving and restoring the snapshot from the remote cluster to the source cluster.

In these scenarios, you must enable NGT again in the restored VM.

Storage Quality of Service (QoS)

Storage QoS provides administrators granular control to manage the performance of virtual machines and ensure that the system delivers consistent performance for all workloads. You can use a controllable knob to limit the IOPS that the storage layer would serve for individual virtual machines. IOPS is the number of requests the storage layer can serve in a second. You can set throttle limits on a VM to prevent noisy VMs from over-utilizing the system resources.

Note:

- Storage QoS is applicable only if you have an AOS Pro or above license. See the License Manager Guide for more information on AOS licenses.
- Setting storage QoS is not allowed when the AOS upgrade is in progress.

Terminology

Throttled IOPS

The maximum IOPS that the storage layer tries to admit over a sustained period. Applications that are running on the VM are not permitted to exceed this level. This prevents VMs from affecting a system beyond the set limits. However, if the system is in a state of flux, your application might not be throttled. To prevent application crashing due to misconfiguration, the throttled IOPS setting must not be less than one hundred. Otherwise, an error is raised.

Setting maximum IOPS on a VM may affect the cluster latency for that VM and may result in higher latency being displayed in the cluster latency charts. Performance of any other VM is not affected by this setting. You can view individual VM latency graph to ensure that the other VMs are not affected. You can also create a custom focus view to display the throttled IOPS for all the VMs.

Throughput

Throughput is the amount of data that an application sees from the storage layer underneath per second. The maximum throughput is calculated by multiplying the number of IOPS with the block size.

Calculation of the IOPS and Throughput

The default block size used for IOPS calculation is 32 KiB. If the block size is less than or equal to 32 KiB, then the system is rate limited by the number of IOPS and the bandwidth is calculated by multiplying the number of IOPS with the block size of the application. Otherwise, if the block size is greater than 32 KiB, the system is rate limited by the throughput and the number of IOPS is calculated by dividing the throughput by block size of the application.

For example, if you have set a throttle limit of 800 IOPS on a VM and the application is admitting IOPS with 8 KiB block size, then the application would see 800 IOPS and throughput of 6.25 MBps. However, if application is admitting IOPS with 64 KiB block size, then the application would see 400 IOPS and a throughput of 25 MBps.

The following table provides the information about the block size, IOPS, and throughput relationship when throttle limit is set to 800, 400, or 200 IOPS:

Table 32: Relationship between Block Size, IOPS, and Throughput

Block size	IOPS	Throughput
8 KiB	800	6.25 MBps
16 KiB	800	12.50 MBps
32 KiB	800	25 MBps
64 KiB	400	25 MBps
128 KiB	200	25 MBps

Limitations

Storage QoS has the following limitations:

- Storage QoS is not supported for an in-place restore, out-of-place restore, and snapshot operation on VM.
- While creating a clone of a VM, any QoS attributes throttle limit set on the original VM might not be applied to the new cloned VM. QoS throttle limit needs to be set on the new cloned VM separately.
- For linked clones, when you are sharing the vDisks across multiple VMs, shared disks are not a part of QoS policy and shared disks would not be throttled. Each VM might exceed the maximum limit depending on the shared vDisk usage. For example, during bootstorm in a VDI setup.
- If a VM has volume groups attached, then QoS is not applicable.
- Storage QoS is not supported for Metro Availability, synchronous replication, and Nutanix Files virtual machines.

Setting QoS for an Individual VM

About this task

Storage QoS allows you to set throttle limits on a VM to prevent noisy VMs from over-utilizing the system resources. Perform the following procedure to set the QoS for an individual VM.

Figure 68: Setting QoS for an Individual VM

A video on this topic is available https://players.brightcove.net/5850956868001/xJM5EiUJJ_default/index.html?videoId=6275779955001 on Brightcove.

To set QOS for an individual VM, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default with VMs across all the registered clusters.

3. Perform either of the following actions:

   » Select the target VM checkbox, and choose **Set QoS Attributes**from the **Actions** dropdown menu.

   > **Note:** This action is not permitted (greyed out) for the VM on which Prism Central is hosted.

   » Click the target VM to access the VM Details View on page 108, and choose **Set QoS Attributes** from the **More** dropdown menu.

4. In **Input Type** field, select either of the following options:

   » IOPS - For more information about IOPS, see *Throttled IOPS* information in Storage Quality of Service (QoS) on page 186.

   » Throughput - For more information about throughput, see *Throughput* information in Storage Quality of Service (QoS) on page 186.

   If you select:

   - **IOPS**- Enter a value for the throttled IOPS in the **Throttled IOPS** field.
   - **Throughput** - Enter a value for the throttled throughput in the **Throttled Throughput** field.

5. (Optional) Click **Show Details** to populate a table that describes the relationship between block size, IOPS, and throughput.

6. Click **Confirm** to set the defined QOS values for the target VM.

   Click **Clear Attributes** to delete all the values.

   The system stores the number of IOPS or throughput to be served by the storage layer.

   > **Note:** To edit the storage QoS setting, follow the same steps as described in this section, and enter a new value for **IOPS** or **Throughput**.

Memory Overcommit Management

The Memory Overcommit feature enables you to optimize the physical memory utilization of a VM. It allows the host to automatically detect whether the memory is under-utilized or over-utilized for a VM. Using Prism Central, you can enable the Memory Overcommit feature.

For more information about Memory Overcommit feature, and how to enable or disable it using Prism Central, see Memory Overcommit information in *AHV Administration Guide*.

Policies for VM Management

You can define the Affinity and NGT policies for managing a VM. For information about Affinity and NGT policies, see VM Policy Management on page 461.

VM Template Management

In Prism Central, you can create VM templates to manage the golden image of a VM. A VM template can be considered as a master copy of a virtual machine. It captures the virtual machine configuration and the contents of the VM including the guest operating system, and the applications installed on the VM. You can use this template to deploy multiple VMs across clusters.

> **Note:** You can create or manage a VM template only as an admin user.

VM Template Summary View

The **Templates** page displays the information about all the VM templates across registered clusters.

To access the summary view of all VM templates, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Templates** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The following is an example showing the **Templates** page with all the VM templates:

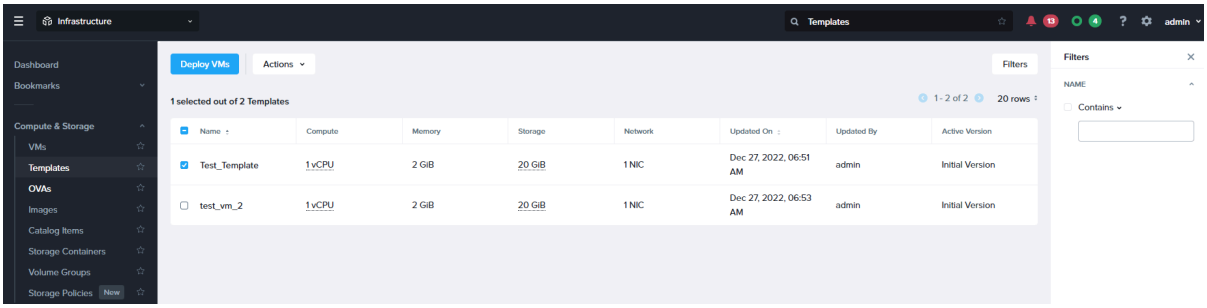


Figure 69: Summary View - All VM Templates

Table 33: Templates Page - Field Description

Field	Description	Values
Name	Displays the template name. Click the template name to view the detailed information about that template. For more information, see VM Template Details View on page 190.	*<Template name>*
Compute	Displays the virtual CPU count of the VM that is deployed using this template.	(vCPU count) x vCPU, where x is numeric digit.
Memory	Displays the total amount of memory available to the VM that is deployed using this template.	(Memory) x [MB|GiB], where x is numeric digit.
Storage	Displays total amount of storage available to the VM that is deployed using this template.	x [MB|GiB], where x is numeric digit.
Network	Displays the NIC count of the VM that is deployed using this template.	x NIC, where x is numeric digit.
Updated On	Displays the last date and time when the template has been updated.	(date and time), Timestamp in MM DD, YYYY, hh:mm AM/PM format. For example, Dec 27, 2022, 06:51 AM
Updated By	Displays the user who most recently updated the template.	<user>. For example admin

Field	Description	Values
Active Version	Displays the name of the active version of the template. An active version is the version of the template that gets deployed by default when you click **Deploy VMs**.	(version). For example, Initial Version

You can perform the following actions for the VM templates in the **Templates** page:

- Access the detailed information about an individual VM template. For more information, see VM Template Details View on page 190.
- Deploy a VM. For information about how to deploy a VM using VM template, see Deploying VM from a Template on page 196.
- Filter the VM templates list based on the template name using **Filters** pane. For more information about **Filters** pane, see Filters Pane on page 28.
- Sort the list of templates from the **Name** and **Updated On** columns. For information about sorts function, see Sort Function on page 28.
- Use the **Actions** dropdown menu to perform the available operations as described in Managing a VM Template on page 200.

VM Template Details View

The VM template details view includes two pages: **Summary** page and **Versions** page.

Summary Page

The **Summary** page of an individual VM template consists of a dashboard that provides the detailed information about the VM.

To access the **Summary** page of an individual VM template:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Templates** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
3. Click the <*VM_Template_Name*> to view the **Summary** page of an individual VM template.

> **Note:** Replace <*VM_Template_Name*> with the actual VM name at your site.

The following is an example showing the **Summary** page of an individual VM template:

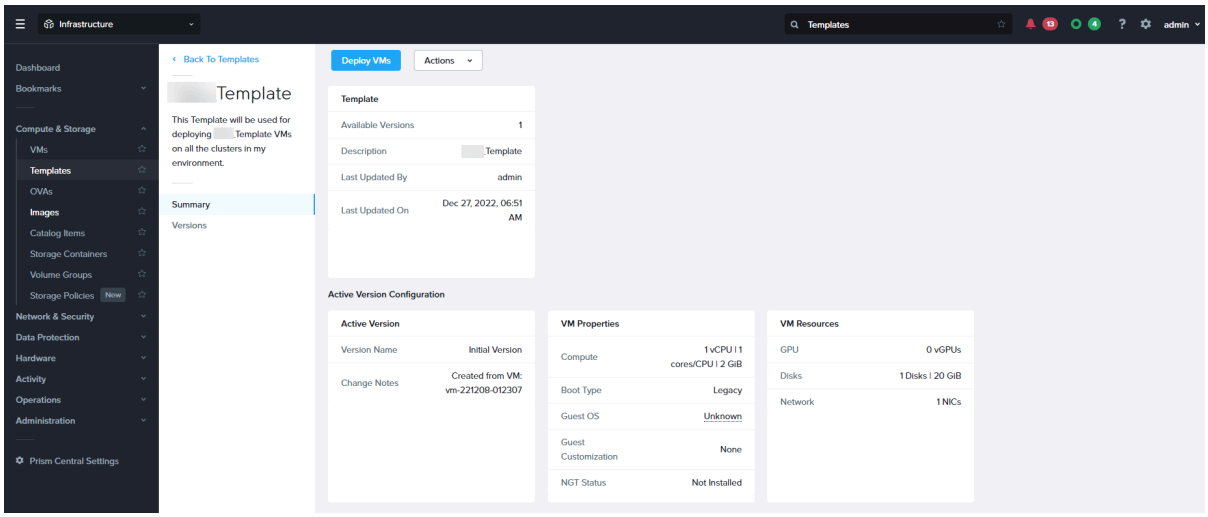


Figure 70: Summary Page - Individual VM Template

The **Summary** page provides you the options to deploy a VM using the selected VM template, and an **Actions** dropdown menu.

- For information about how to deploy a VM using the VM template, see Deploying VM from a Template on page 196.
- For information about the list of actions available under **Actions** dropdown menu, see Managing a VM Template on page 200.

The **Summary** page of an individual VM template provides the following widgets:

- **Template**: This widget displays the following parameters:
  - **Available Versions**: Number of versions available
  - **Description**: User-provided description of the template
  - **Last Updated by**: User who has last updated the template
  - **Last Updated on**: Date and time of last update to the template
- **Active Version Configuration**: This widget displays the following parameters:
  - **Version Name**: Name of the currently active version of the template
  - **Change Notes**: User-provided change notes for the active version
- **VM Properties**: This widget displays the following parameters:
  - **Compute**: Compute resources of the VM such as CPU, core per CPU, and memory
  - **Boot Type**: Boot type of the VM such as legacy or UEFI
  - **Guest OS**: Guest OS of the VM. If the source VM of the template does not have NGT installed on it, then this field is displayed as unknown.
  - **Guest Customization**: Status of the guest customization application (applied/not applied)
  - **NGT Status**: Status of the NGT installation

- **VM resources**: This widget displays the following parameters:
  - **GPU**: Number of GPU assigned to the VM
  - **Disks**: Number of disks and total disk capacity assigned to the VM
  - **Network**: Number of NICs assigned to the VM

Versions Page

To view the **Versions** page of an individual VM template, click **Versions**.

The following is an example showing the **Versions** page of an individual VM template:

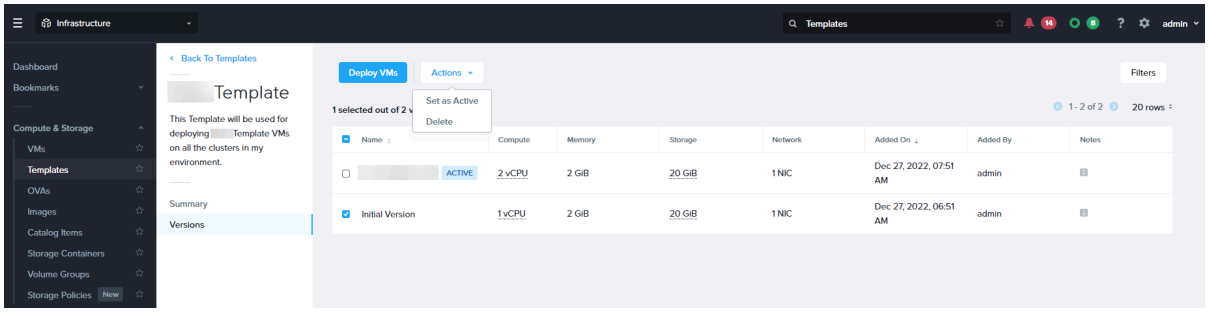


Figure 71: Versions Page - VM Template

You can perform the following actions for the VM template version in the **Versions** page:

- Deploy a VM using the selected VM template version. For information about how to deploy a VM using the selected VM template version, see Deploying VM from a Template on page 196.

  Note: By default the active version of the template always gets deployed. In the **Versions** page, you can select the specific VM template version, and make it Active for VM deployment.

- Select a version and set it as active, or delete a selected version from the **Actions** dropdown menu. For more information, see Managing a VM Template on page 200.
- Filter the VM templates list based on the template name using **Filters** pane. For more information about **Filters** pane, see Filters Pane on page 28.
- Sort the list of templates from the **Name** and **Updated On** columns. For information on sorts function, see Sort Function on page 28.

Table 34: Versions Fields

Parameter	Description	Values
Name	Displays the VM Template version name. This column also indicates if the version is an active version.	*<Template _Version_name>*
Compute	Displays the virtual CPU count of the VM that gets deployed using this version.	(vCPU count) x vCPU, where x is numeric digit.
Memory	Displays the total amount of memory available to the VM that gets deployed using this version.	(Memory) x [MB|GiB], where x is numeric digit.

Parameter	Description	Values
Storage	Displays total amount of storage available to the VM that gets deployed using this version.	x [MB|GiB], where x is numeric digit.
Network	Displays the NIC count of the VM that gets deployed using this version.	x NIC, where x is numeric digit.
Added On	Displays the last date and time when the version was added.	(date and time), Timestamp in MM DD, YYYY, hh:mm AM/PM format. For example, Dec 27, 2022, 06:51 AM
Added By	Displays the user who added the version.	<user>. For example admin
Notes	Displays the user-specified change note for the version.	<Version-specific-text> that you specify in **Change Notes** field when you update a VM template version.

You can sort the list of versions by clicking on **Name** and **Added On** columns.

Limitations of VM Template Feature

The current implementation of the VM template feature has the following limitations:

- You cannot create a VM template if any of the following conditions is applicable at your site:
  - VM is not on AHV.
  - VM is an agent or a PC VM.
  - Any volume group is attached to the VM.
  - VM is undergoing vDisk migration.
  - VM has disks located on RF1 containers.
  - VM is protected by PD-based DR.
- VM templates do not copy the following attributes from the source VMs:
  - Host affinity attributes
  - HA priority attributes
  - Nutanix Guest Tools (NGT) installation
  - Quality of service (QoS) configuration

  You must reconfigure the above-listed attributes at the deployed VMs.
- VM Template does not protect the underlying VM recovery point from deletion by a user having delete permission. VM Template deployment fails if you delete the associated VM recovery point.

Creating a VM Template

This section describes how to create a VM template in Prism Central.

About this task

To create a VM template, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab as default
3. In **List** tab, select the VM to create a VM template.

   Note: Before you select a VM to create a VM template, ensure that the VM is powered off.

4. In the **Actions** dropdown menu, select **Create VM Template**.

   You can also click **Create VM Template** in the **Summary** page of an individual VM. For information about how to access the **Summary** page of an individual VM, see VM Details View on page 108.

   The system displays the **Create template from VM** window.

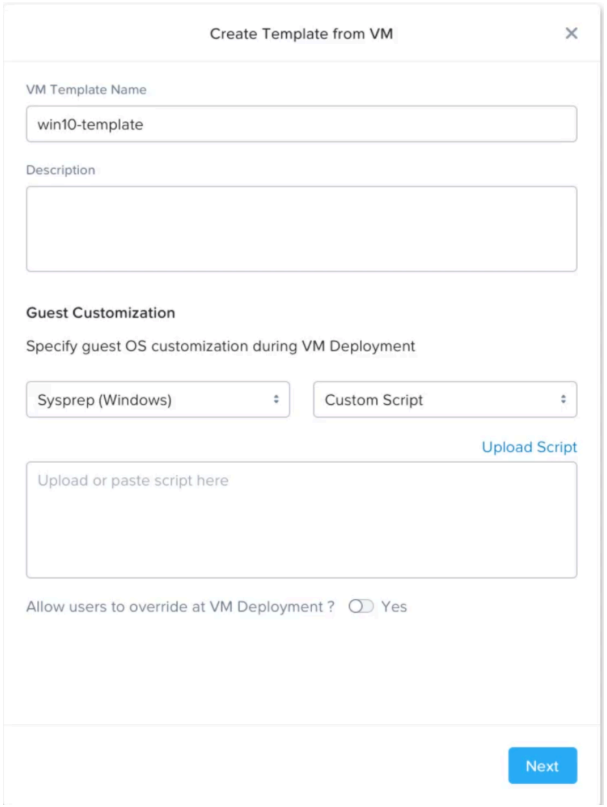


Figure 72: Create Template from VM window

5. In the **Create Template from VM** window, enter the following information:

   a. **Name** - Name of the VM Template.

   b. **Description** - Description for the VM template. Description is an optional field.

   c. For the **Guest Customization** fields, select the following options for guest operating system (OS) for the VMs that you deploy using this VM template:

      - In the **Script Type** field, select **Sysprep (Windows)** to customize the Windows OS, and **Cloud-init (Linux)** to customize the Linux OS.

        Note: If you select **No Customization** at the time of creating the template and allow the users to override the guest customization settings using **Allow users to override at VM Deployment?** toggle field, it gives the maximum customization control to the users. In this case, the users can customize the script type and the configuration method.

      - In the **Configuration Method** field, for each of these script types selected in **Script Type** field, select either upload a custom script or opt for a guided setup in the field.

        Note:

        - If you select **Custom Script**, you can either upload a script to customize the guest OS of the VMs, or you can copy-paste the script in the text box.
        - If you select **Guided Script** , enter the following information:
          - **Authentication Type**: Select one of the radio button to set the authentication type:
            - **Password**: Set a username and password for the user who uses this template to deploy the VM.
            - **SSH Key** [Cloudinit (Linux) only]: Set the SSH key for the user who use this template to deploy the VM.
          - **Locale**: Select the locale (language) from the dropdown list.
          - **Hostname**: Enter the hostname for the user who uses this template to deploy a VM
          - **License Key**: Enter the license key.

            Important: The information that you enter is used to customize the OS of the VMs that are deployed using this template.

      Note: If you opt for **Guest Customization** setup with script (custom or guided script), ensure that the script is in a valid format. The system does not validate the guest customization scripts. In the script is not in valid format, the VM deployment might succeed but the guest customization script may not work as expected. You can observe the discrepancies (if any) only after the VM gets deployed.

   d. Set the **Allow users to override at VM Deployment?** toggle field as per your requirement. This toggle field is used to enable or disable the override permission for guest customization settings.

      - If this toggle field is:
        - *Enabled*: The system allows the users (who use this VM template to deploy VM) to modify the guest OS customization settings in VM template. The users can modify the settings only

for the **Configuration Method** field. For example, the users can change the authentication information at the time of deploying a VM from VM template, or they can change from a guided setup to a custom script.

- *Disabled*: The settings that are already provided in the VM template, can be used for VM deployment.

6. Click **Next**.

   On the next page, you can review the template details.

   The system prompts you to review the configuration details, resource details, network details, and management details.

7. Click **Save** to save the inputs and create a VM template.

   The new template appears in the **Templates** page list.

   Note: Once you create a VM template, the template metadata is available in Prism Central. The template data is stored as a VM recovery point and is co-located with the source VM. If you use the VM template to deploy a VM to another cluster, the recovery point is copied to the destination cluster before deployment.

Deploying VM from a Template

Before you begin

Ensure that the VM template is available. For information about how to create a VM template, see Creating a VM Template on page 193.

About this task

After you create a VM template, you can use the VM template to deploy any number of VMs across clusters.

To deploy a VM using a VM template, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Templates** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57 .

3. Select the target VM template to deploy VMs using either of the following methods:

   - In the **Templates** page, select the target template checkbox, and click **Deploy VMs**. For more information about **Templates** page, see VM Template Summary View on page 189.
   - In the **Summary** page of an individual VM template, click **Deploy VMs**. For more information about **Summary** page of an individual VM template, see VM Template Details View on page 190.
   - In the **Versions** page of an individual VM template, select the target VM template version, and click **Deploy VMs**. For more information about **Versions** page of an individual VM template, see VM Template Details View on page 190.

     Note: In the **Versions** page, you can select any active or non-active VM template version for VM deployment.

   Note: By default, the active version of the VM template is used for VM deployment.

   The **Deploy VM from Template** window appears. By default, you see a **Quick Deploy** method. You can click**Advanced Deploy** to access the **Advanced Deploy** method in **Deploy VM from Template** window . In **Advanced Deploy** method, you can view and modify some VM properties and network settings.

4. Deploy VM using either of the following deployment methods:

   - **Quick Deploy** method:

     The is an example showing the **Quick Deploy** method:

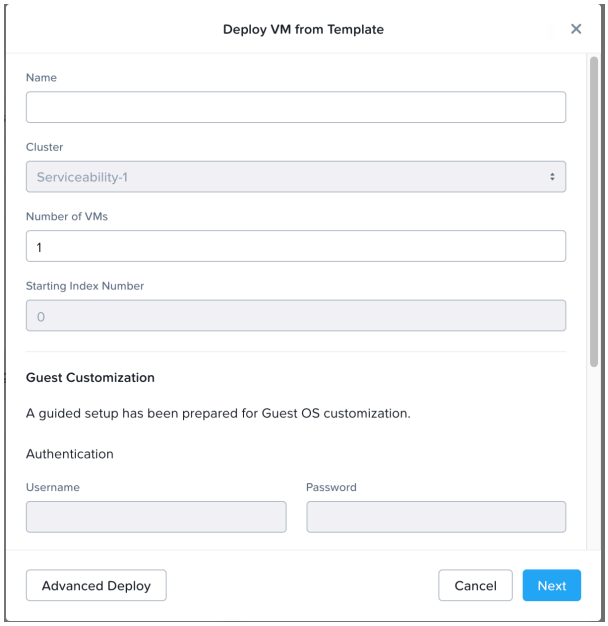


Figure 73: Deploy VM from Template - Quick Deploy Method

1. Enter the following information:

   - **Name**: Enter a name for the VM.
   - **Cluster**: Select the cluster where you want to deploy the VM.
   - **Number of VMs**: Enter the number of VMs that you want to deploy.
   - **Starting Index Number**: Enter the starting index number for the VMs when you are deploying multiple VMs simultaneously. These index numbers are used in the VM names. For example, if you are deploying two VMs and specify the starting index number as 5, the VMs are named as *vm_name*-5 and *vm_name*-6.
   - **Guest Customization**: The template can have any one of the following options for guest OS customization:

     - **No Customization**
     - **Sysprep (Windows)**, or **Cloud-init (Linux)**. For **Sysprep (Windows)**, or **Cloud-init (Linux)**, you can choose to either upload a custom script or opt for a guided setup.

       Note: These fields are enabled for modification only if the VM template allows you to override its guest customization settings while deploying the VM. The **Allow users to override at VM Deployment?** toggle field is used to enable or disable the override for guest customization settings. For information about how to set this toggle field during VM template creation, see Creating a VM Template on page 193. If the override

permission for the guest OS customization is disabled, the settings that are already provided in the template can be used for VM deployment.

2. Click **Next** to verify the configuration details of the VMs to be deployed.
3. Click **Deploy** to deploy the VMs.

- **Advanced Deploy** method:

  The following is an example showing the **Advanced Deploy** method:

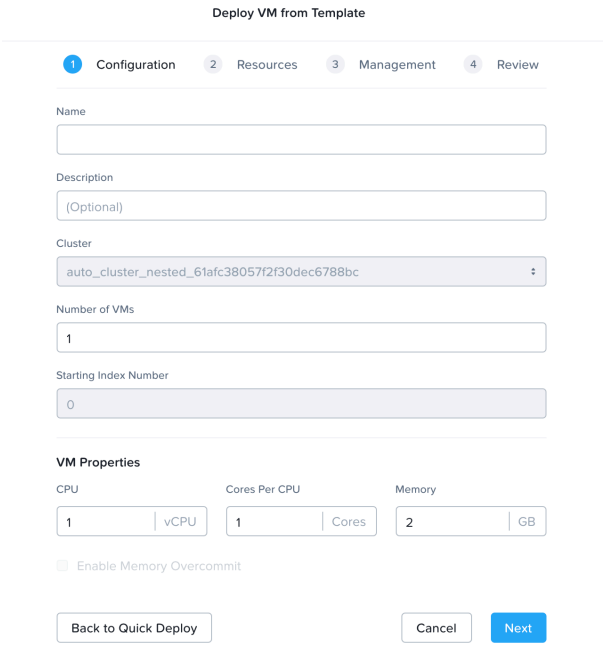


Figure 74: Deploy VM from Template - Advanced Deploy Method

1. Enter the following information:

   - **Configuration**: Provide inputs for name and description (optional) of the VM, cluster where you want to deploy the VM, Number of VMs to be deployed, and starting index number (only if deploying multiple VMs). In this tab, you can also view and modify the VM properties such as CPU, core per CPU, and memory.
   - **Resources**: Review the configuration settings for the VM resources such as disks, networks, and boot configuration. Here, you can modify the network settings but cannot modify any other settings.
   - **Management**: The fields in this tab are enabled for modification only if the VM template allows you to override its guest customization settings while deploying the VM. The **Allow users to override at VM Deployment?** toggle field is used to enable or disable the override for guest customization settings. For information about how to set this toggle field during VM template creation, see Creating a VM Template on page 193. If the override permission for

the guest OS customization is disabled, the settings that are already provided in the template can be used for VM deployment.

If guest customization has been enabled, provide inputs for authentication type, username, password, locale, and Hostname.

> **Note:** Hostname of the VM is automatically generated based on the VM names that you provide. If you are deploying a single VM, you can override the automatic generation of the hostname by specifying a hostname. If you are deploying multiple VMs, you cannot override the automatic hostname generation.

- **Review**: Review the information displayed in this tab.

2. Click **Deploy** to deploy the VMs.

Managing a VM Template

About this task

After you create a VM template, you can perform the following actions to manage the VM Template:

- Update the guest OS of the source VM specified in the VM template
- Complete guest OS update
- Cancel guest OS update
- Update the configuration of the template to create a new VM template version
- Delete the VM template.

For information about how to create a VM template, see Creating a VM Template on page 193.

To manage a VM template, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Templates** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57 .

Select the target VM template using either of the following methods:

- Select the target VM template checkbox in the **Templates** page. For more information about **Templates** page, see VM Template Summary View on page 189.
- Click the target template to view the **Summary** page of an individual VM template. For more information about **Summary** page of an individual VM template, see VM Template Details View on page 190.

3. Select the required action from the **Actions** dropdown menu:

Note: The available actions appear in bold and the unavailable actions are greyed out. The available actions depend on the current state of the template and user permissions.

The following actions are available in **Actions** drop down menu:

- **Update Guest OS**

  To update the guest OS in a VM Template, perform the following steps:

  1. Select the target VM template version on which the guest OS is to be updated in **Select a version to Update** window, and click **Proceed**.

     Note: By default the active version of the VM Template is selected for VM Template update, however the system provides you an option to select the VM Template version on which the guest OS is to be updated.

  2. Review the information displayed in the **Update Guest OS** window, and click **Proceed**.

     At this stage, the system deploys a temporary VM from the selected VM template version, and provides you an option to access the VM. You can also access the new VM from VMs **List** tab. For information about VMs **List** tab, see VMs Summary View on page 95.

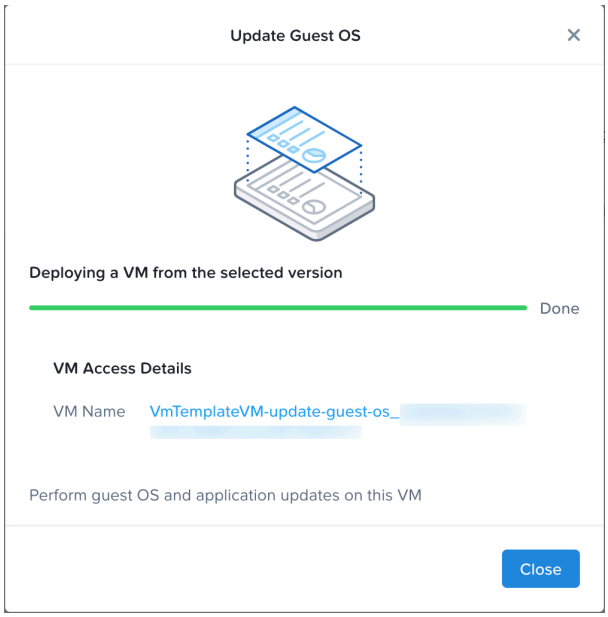


Figure 75: Update Guest OS

  3. Start the temporary VM, log on to the VM, and update the guest OS of the temporary VM. For information on how to update a VM, see Managing a VM through Prism Central (AHV) on page 134.
  4. Complete the guest OS update using the **Complete Guest OS Update** option from the **Actions** dropdown menu.

- **Complete Guest OS Update** to complete the process initiated for guest OS update. You must select this option only after successful update of the guest OS of the temporary VM.

  Note: At this stage, the system prompts you to create a new version of the VM Template with updated guest OS. Specify the details for the new version, and click **Complete Update**.

  The temporary VM automatically gets deleted after completion of the guest OS upgrade process.

- **Cancel Guest OS Update** to cancel the process initiated for guest OS update.

The temporary VM automatically gets deleted after cancellation of the guest OS upgrade process.

- **Update Configuration** to modify the VM template configuration. In **Select a version to Update** window, select the VM template version that you want to modify, and create a version on top of it.

  Perform the following steps to update the VM template configuration in **Update Template Configuration** window:

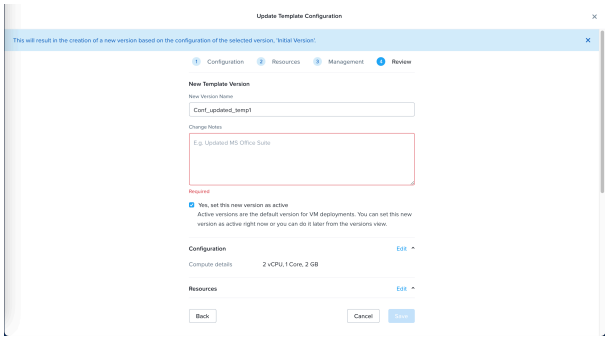


Figure 76: Update Template Configuration

1. In the **Configuration** step, view the name of the base version that you want to update, change notes for that version, cluster name, VM properties (CPU, cores per CPU), and memory). In this section, you can modify only VM properties.
2. In the **Resources** step, view the information about disks, networks, and boot configuration. In this section, you can modify only network resources.
3. In the **Management** step, modify the guest customization settings.
4. In the **Review** step, review and modify the configuration settings that you are allowed to modify. You must provide a name and change notes for the new version. You can also choose to set this new version as active version.

   > **Note:** An active version is the version of the template gets deployed by default when you click **Deploy VMs** after VM template configuration update.

5. Click **Save** to save the settings and create a new VM template version.

- **Delete Template** to delete a template. The system prompts you to confirm the delete action. Click **OK** to delete the VM template.

4. To only manage a VM template version:

   a. Select the VM template version from the **Versions** page. For information about how to access the **Versions** page of an individual VM template, see VM Template Details View on page 190.

   b. Select either of the following options from the **Actions** dropdown menu:

   - **Set as Active** to make the selected VM template version as the active version.
   - **Delete** to delete the selected VM template version.

     > **Note:** You cannot delete the active version of a VM template.

Kubernetes Clusters Management

The **Kubernetes Clusters** entity in the **Infrastructure** application allows you to see the Kubernetes clusters that you deploy on the Nutanix clusters.

To see the Kubernetes clusters in the **Kubernetes Clusters** entity in the **Infrastructure** application, you must onboard the Kubernetes clusters to Prism Central. See Onboarding the Kubernetes Cluster to Prism Central on page 203 for more information.

Before you onboard any Kubernetes clusters to Prism Central, the **Kubernetes Clusters** entity page is displayed as follows:

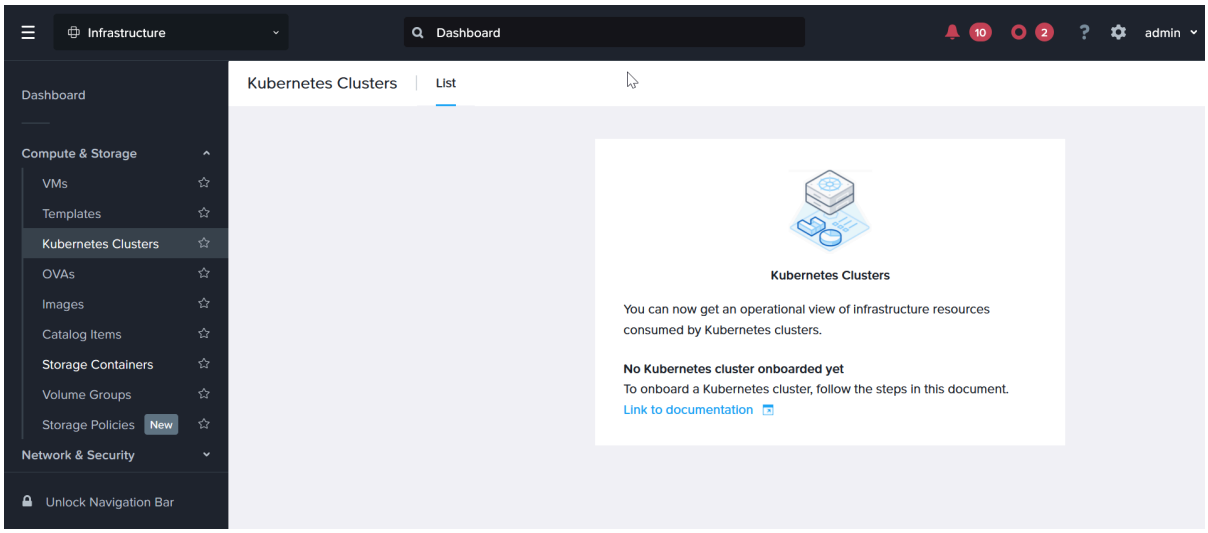


Figure 77: Kubernetes Clusters entity page before onboarding Kubernetes clusters

If you do not want to manage the Kubernetes clusters in Prism Central **Infrastructure** application, off-board the Kubernetes clusters. To off-board the cluster, use the `helm uninstall <helm-chart-name>` command. See the *What to do next* section in Onboarding the Kubernetes Cluster to Prism Central on page 203.

Kubernetes Cluster Entity Views

Prism Central provides the following views for the **Kubernetes Clusters**.

- Kubernetes Clusters Summary View on page 205
- Kubernetes Cluster Details View on page 207

Onboarding the Kubernetes Cluster to Prism Central

After creating the Kubernetes clusters with NKE Next Generation Workload Clusters (In Technical Preview) or Red Hat OpenShift, you need to onboard the clusters to Prism Central. After onboarding, you can view the Kubernetes clusters on Prism Central.

About this task

For information on NKE Next Generation Kubernetes cluster (In Technical Preview), see Next Generation Workload Cluster (Technical Preview) in the *Nutanix Kubernetes Engine Guide*.

To onboard the Kubernetes cluster to Prism Central, perform the following steps:

Procedure

1. Find the UID of the Kubernetes cluster by running the following command.

   ```
   $ kubectl --kubeconfig <kubeconfig> get ns kube-system -o json | grep uid
   ```

   Replace `<kubeconfig>` with the path to the Kubernetes `kubeconfig` file.

   Note the UID from the output of the command.

2. If you created an NKE Next Generation Kubernetes cluster, note the cluster name that you provided while creating it.

3. If you created Red Hat OpenShift Kubernetes clusters, find the infrastructure name of the Kubernetes cluster by running the following command.

   ```
   $ kubectl --kubeconfig <kubeconfig> get infrastructure cluster -o yaml |
    grep .status.infrastructureName
   ```

   Note the infrastructure name from the output of the command.

4. (Optional) To run the onboarding CLI command on your local system (laptop or desktop system), export the cluster name and the UID by running the following command.

   ```
   $ export CLUSTER_NAME=<cluster-name>
   $ export CLUSTER_UUID=<uid-of-kube-system-namespace>
   ```

   In case of Red Hat OpenShift Kubernetes clusters, export the cluster UID and the infrastructure name by running the following command.

   ```
   $ export CLUSTER_UUID=<uid-of-kube-system-namespace>
   $ export CLUSTER_INFRA_NAME=<infrastructure-name>
   ```

   Replace the following:

   - `<cluster-name>` with the name of the cluster.
   - `<uid-of-kube-system-namespace>` with the UID found and noted.
   - `<infrastructure-name>` with the infrastructure name found and noted.

5. Download the *Kubernetes Agent* (k8s-agent-1.0.0.tar) file (k8s-agent-1.0.0.tar) from the NDK Downloads page to the Kubernetes onboarding CLI folder (ndk-k8s-agent-folder) on your local system (laptop or desktop system).

6. Run the Kubernetes onboarding CLI command on your local system (laptop or desktop system) with details of the Prism Central instance and the details exported in the previous step.

   ```
   $ helm install <release-name> /<path-to-ndk-k8s-agent-folder>/ndk-k8s-
   agent-<version>/ndk-k8s-agent --set pc.endpoint=<pc-endpoint>,pc.username=<prism-
   admin user name>,pc.password=<prism-admin user password>,pc.insecure=<true-
   or-false>,k8sClusterName=<k8s-cluster-name>,k8sClusterUUID=<k8s-cluster-
   uid>,k8sDistribution=<k8s-distribution> -n ntnx-system --create-namespace
   ```

   Replace the values as follows:

   - `<release-name>` with the file name of the Kubernetes agent. For example, `nutanix-k8s-agent-1.0.426`.
   - `<path-to-k8s-agent-folder>` with the path to the folder on Prism Central where you unpacked the Kubernetes agent CLI file.
   - `<pc-endpoint>` with Prism Central IP address or virtual IP address.

- `<prism-admin user name>` with the user name that has Prism Central Admin privileges.
- `<prism-admin user password>` with the password for the Prism Admin username.
- `<k8s-cluster-name>` with the name of the Kubernetes cluster.
- `<k8s-cluster-uid>` with the UID of the Kubernetes cluster.
- `<k8s-distribution>` with the distribution used to create the Kubernetes cluster with. Specify as follows:
  - For **Nutanix Kubernetes Engine** Next-Gen—`NKE`. For information about NKE Next Generation workload clusters (currently available only for Technical review), see Next Generation Workload Cluster
  - For **Red Hat OpenShift**—`OCP`
- `<true-or-false>` with either true or false. The `pc.insecure` option is used to set certificate verification. Setting the `true` option means the certificates are not verified. Setting the `false`option means the certificates are verified.

What to do next

- You can update the parameters such as Prism Central user name and password for the Kubernetes agent by running the following command.

  ```
  $ helm upgrade <release-name> /<path-to-ndk-k8s-agent-folder>/ndk-k8s-agent-<version>/ndk-k8s-agent --set username=<prism-admin user name>,password=<prism-admin user password>
  ```

- To off-board the Kubernetes clusters, run the following command:

  ```
  helm uninstall <release-name> -n ntnx-system <namespace>
  ```

  Replace
  - `<release-name>` with the file name of the Kubernetes agent. For example, `nutanix-k8s-agent-1.0.426`.
  - `<namespace>` with the name space that was created during onboarding.

Kubernetes Clusters Summary View

The **List** tab in the **Kubernetes Clusters** summary view provides a list of the Kubernetes clusters that you onboard to the Prism Central instance. To access the **Kubernetes Clusters** summary view, perform the following steps:

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Kubernetes Clusters** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   After you onboard the Kubernetes clusters, the **List** tab displays the onboarded Kubernetes clusters as follows.

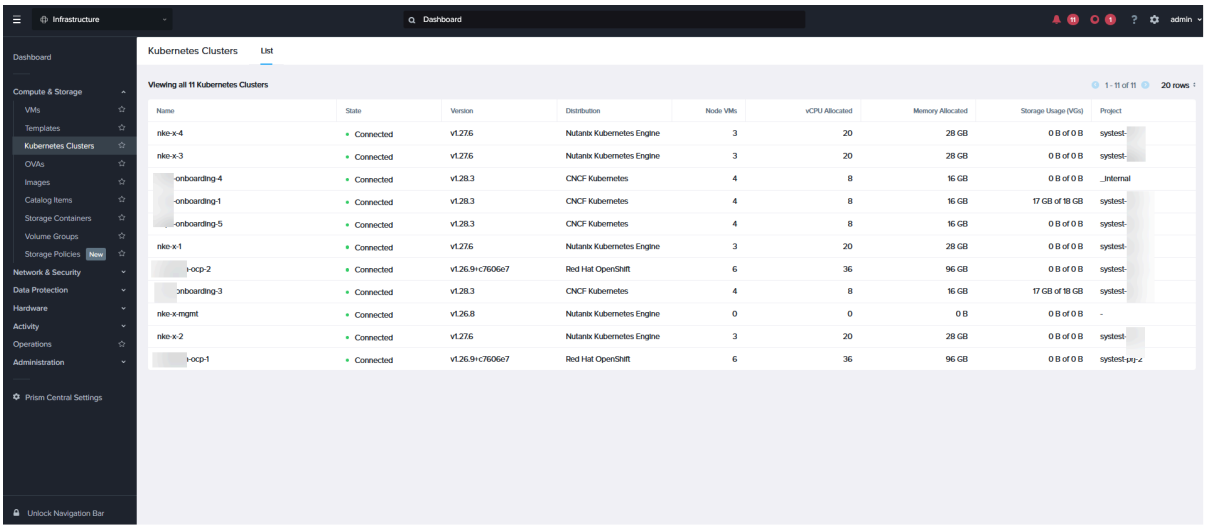


Figure 78: Kubernetes Clusters entity page after onboarding Kubernetes clusters

The following table describes the fields that appear in the **List** tab of the **Kubernetes Clusters** page. A dash (-) is displayed in a field when a value is not available or applicable.

Table 35: Kubernetes Clusters - List Tab Field Description

Field	Description	Values
Name	Displays the name of the Kubernetes cluster.	String
State	Displays the state of the connection to the Kubernetes cluster onboarding agent.	**Connected** or **Disconnected**
Version	Displays the version of Kubernetes bundle used to deploy the Kubernetes cluster.	<version>. For example, **1.27.6**
Distribution	Displays the name of the tool used to create the Kubernetes.	**CNCF Kubernetes** **Red Hat OpenShift** **Nutanix Kubernetes Engine**
Node VMs	Displays the number of Node VMs in the Kubernetes cluster.	Integer
vCPU Allocated	Displays the number of vCPUs allocated to the Kubernetes cluster.	Integer
Memory Allocated	Displays the amount of memory in GB allocated to the Kubernetes cluster.	(Decimal number) GB

Field	Description	Values
Storage Usage (VGs)	Displays the amount of Volume Group storage in bytes used by the Kubernetes cluster.	(Decimal number) B of (Decimal number) B
Project	Displays the name of the Project that manages the Kubernetes cluster. Displays `_Internal` if the Kubernetes cluster infrastructure resources are assigned to the default project VM.	String

Kubernetes Cluster Details View

The Kubernetes cluster details view displays the properties of individual Kubernetes cluster listed on the **List** tab of the **Kubernetes Clusters** summary view.

The Kubernetes cluster details view page provides information about the Kubernetes cluster on the following tabs:

- **Summary** tab—This tab is the default landing tab of the details view page.
- **Nodes** tab—This tab provides details of all the Kubernetes nodes in the Kubernetes cluster.
- **Storage** tab—This tab provides the details of the storage (Volume Groups or VGs) associated with the Kubernetes cluster.
- **Alerts** tab—This tab provides the details of the infrastructure alerts raised for the Kubernetes cluster.

To access the details view of an Kubernetes cluster, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Kubernetes Clusters** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
3. Click the **Name** of the Kubernetes cluster to view the **Summary** tab of the details view.

Summary Tab

The following is an example showing the **Summary** tab of an individual Kubernetes cluster.

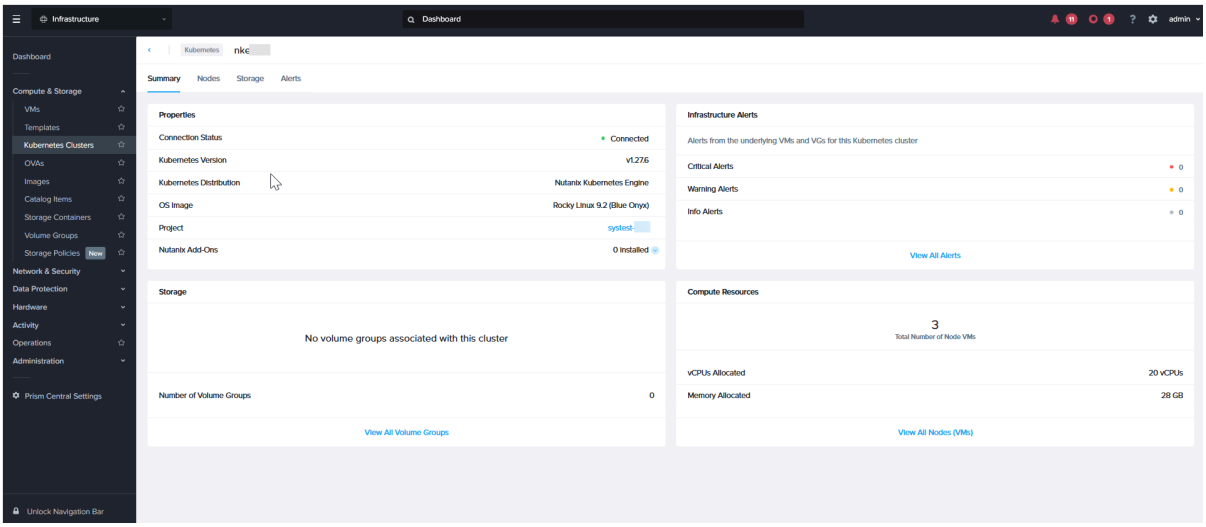


Figure 79: Kubernetes Cluster - Summary Tab

The **Summary** tab of an individual Kubernetes cluster provides the following widgets:

- **Properties**: This widget provides the following parameters.
  - **Connection Status**: The state of the connection to the Kubernetes cluster onboarding agent.
  - **Kubernetes Version**: The version of Kubernetes bundle used to deploy the Kubernetes cluster.
  - **Kubernetes Distribution**: The name of the Kubernetes distribution used to create the Kubernetes cluster.
  - **OS Image**: The distribution and version of the operating system underlying the Kubernetes cluster. For example, Ubuntu 22.04.3 LTS.
  - **Project**: The name of the project that is configured in the **Prism Central Admin Center** application, to manage the infrastructure resources utilized by the Kubernetes cluster.
  - **Nutanix Add-Ons**: The number of the Nutanix add-on packages such as Nutanix CSI or any Container Network Interface (CNI) packages.
- **Infrastructure Alerts**: This widget displays the purpose of this widget in a banner. This widget provides the following parameters for the alerts from the underlying VMs and VGs for this Kubernetes cluster.
  - **Critical Alerts**: The number of critical alerts generated in the AHV host for the VMs and VGs associated with the Kubernetes cluster.
  - **Warning Alerts**: The number of warning alerts generated in the AHV host for the VMs and VGs associated with the Kubernetes cluster.
  - **Info Alerts**: The number of informational alerts generated in the AHV host for the VMs and VGs associated with the Kubernetes cluster.

  For more information about alerts, see the Prism Central Alerts and Events Reference Guide.
- **Storage**: This widget provides the **Number of Volume Groups** associated with the Kubernetes cluster.

  It also provides a clickable link that opens the **Storage** tab in the Kubernetes cluster details view.
- **Compute Resources**: This widget provides the following parameters about the VMs associated with the Kubernetes cluster.
  - **Total Number of Node VMs**: The total number of VMs on the AHV host associated with the Kubernetes cluster.
  - **vCPUs Allocated**: The number of vCPUs allocated to the Kubernetes cluster.
  - **Memory Allocated**: The amount of memory allocated (in GB) to the Kubernetes cluster.

  The widget also provides a clickable link that opens the **Storage** tab in the Kubernetes cluster details view.

Nodes Tab

The **Nodes** tab provides information about the AHV hosts associated with the individual Kubernetes cluster. The following is an example showing the **Nodes** tab of the Kubernetes cluster.

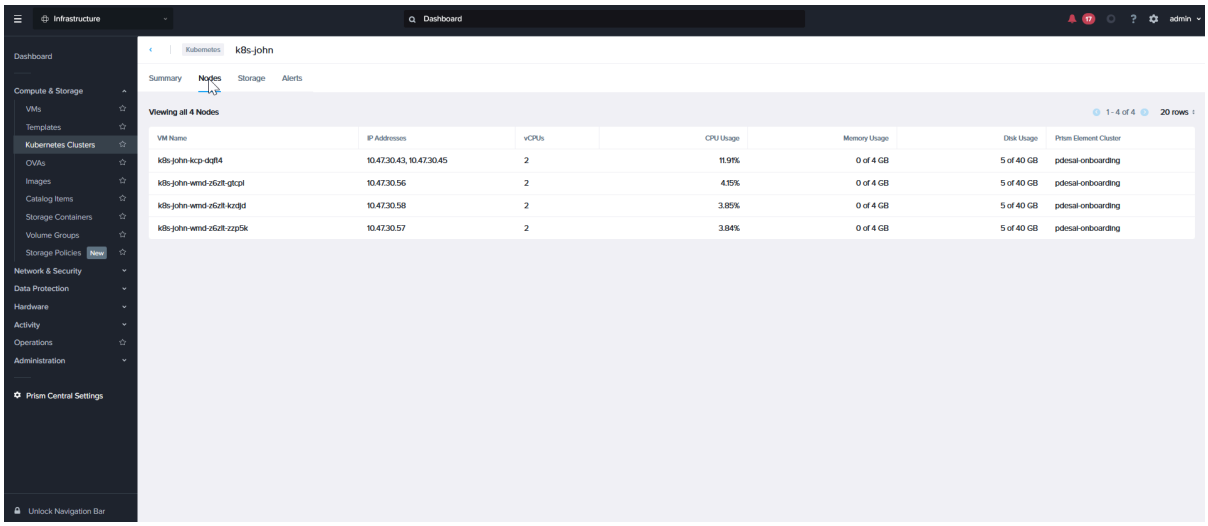


Figure 80: Kubernetes Cluster - Nodes Tab

Table 36: Nodes Tab Field Descriptions

Parameter	Description	Values
VM Name	Displays the name of the VM in the AHV host, that is associated with the individual Kubernetes cluster.	(String)
IP Addresses	Displays the IP addresses of the VM.	Comma-separated list of IP addresses in XXX.XXX.XXX.XXX without CIDR prefix.
vCPUs	Displays the number of vCPUs associated with the AHV host.	Integer
CPU Usage	Displays the CPU usage in percentage.	Decimal number with two decimal places suffixed with %.
Memory Usage	Displays the usage of the allocated memory.	<Usage> of <Allocated> memory suffixed with GB.
Disk Usage	Displays the usage of the allocated disk space.	<Usage> of <Allocated> disk space suffixed with GB.
Prism Element Cluster	Displays the name of the Prism Element cluster.	(String)

Storage Tab

The **Storage** tab provides the storage allocation and usage information associated with the individual Kubernetes cluster. The following is an example showing the **Storage** tab for the Kubernetes cluster.

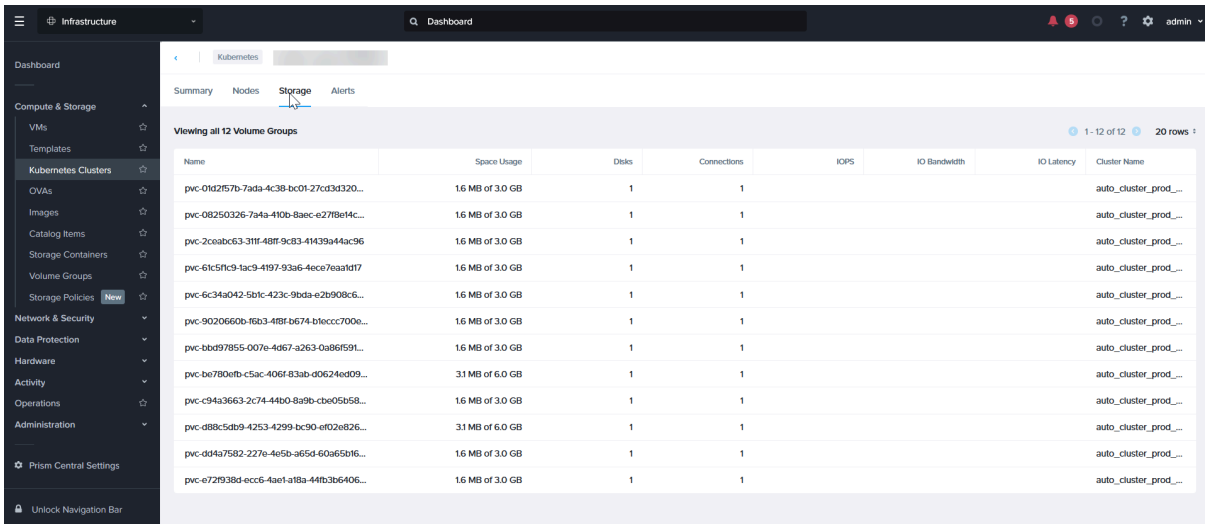


Figure 81: Kubernetes Cluster - Storage Tab

Table 37: Storage tab Field Descriptions

Parameter	Description	Values
Name	Displays the name of the Volume Group (VG).	Volume Group name
Storage usage	Displays the usage of the VG storage.	XX GB of <total> capacity GB
Disks	Displays the number of disks associated with the VG.	(Integer number)
Connections	Displays the number of connections to the VG.	(Integer number)
IOPS	Displays the IOPS of the VG.	(Integer number)
IO Bandwidth	Displays the Input Output (I/O) Bandwidth in MBps.	(Integer number)
IO Latency	Displays the I/O latency.	Time in ms
Cluster Name	Displays the name of the cluster on which the VG is located.	(Cluster name)

Alerts Tab

The **Alerts** tab provides the alerts information associated with the individual Kubernetes cluster. The following is an example showingthe **Alerts** tab for the Kubernetes cluster.

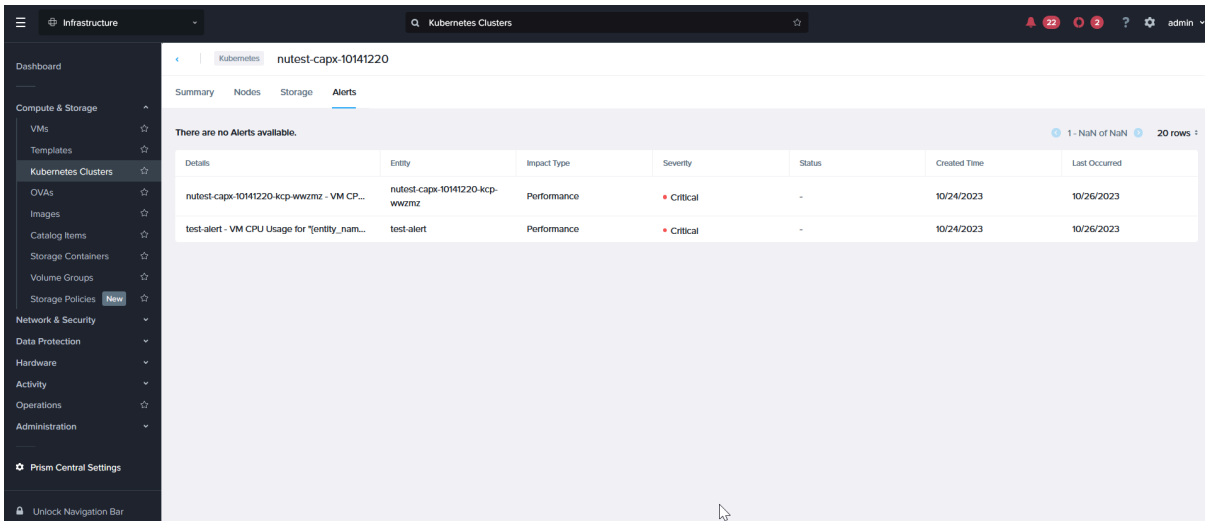


Figure 82: Kubernetes Cluster - Alerts Tab

The Alerts tab shows an extract of the entity's alert tab. For example, the alert page shows the alerts for the VM that the workload nodes are created on. This tab provides the same features and options as the Alerts dashboard, however it is filtered to display the alerts only for the selected Kubernetes cluster. For more information about alerts, see Prism Central Alerts and Events Reference Guide.

Table 38:

Parameter	Description	Values
Details	Displays the name of the entity and type of alert.	Concatenated value of entity name (for example, VM name) and the alert name.
Entity	Displays the name of the entity (VM or VG) that the alert applies to.	<entity-name>
Impact Type	Displays the category in which the alert is classified.	Availability, Capacity, Configuration, Performance, System Indicator

Parameter	Description	Values
Severity	Displays the severity level of this condition. There are three levels: Critical An actionable critical situation has been detected, and action is required immediately. The cluster can have the potential issues and can stop running, or run into irreparable issues. Warning An actionable issue has been detected, and user intervention is required. A more serious issue can occur if the alert is not resolved soon. Info (Informational) An actionable minor problem has been detected. It should be resolved relatively soon and not ignored.	Critical, Warning, Informational

Parameter	Description	Values
Status	Indicates whether the alert is resolved. Resolving an error means you set that error as fixed. The alert can return if the condition is scanned again at a future point. If you do not want to be notified about the condition again, turn off the alert for this condition. For more information about how to turn off the alert using alert policies, see Alert Policies (Prism Central). • A blank value means the alert is not resolved. • An **Acknowledged By** value means this alert is acknowledged manually by the specified user at the specified date and time. To manually acknowledge an alert, select the target alert check box and click **Acknowledge**. • An Auto Resolved (date_time) value means this alert was resolved automatically at the specified date and time. This functionality requires the auto resolve setting to be enabled for this alert type. For more information about how to set the auto resolve using alert policies, see Alert Policies (Prism Central). • A **Resolved By** user (date_time)" value means this alert is resolved manually by the specified user at the specified date and time. To manually resolve an alert, check the box for that alert and click **Resolve**.	(blank), Acknowledged By user (date_time), Auto Resolved (date_time), Resolved By user (date_time)
Created Time	Displays the date and time when the alert occurred.	(date and time)
Last Occurred	Displays the date and time when the alert is last generated (before this occurrence). If this is the first occurrence, both **Created Time** and **Last Occurred** display the same date and time.	(date and time)

OVA Management

An Open Virtual Appliance (OVA) file is a tar archive file created by converting a virtual machine (VM) into an Open Virtualization Format (OVF) package for easy distribution and deployment. OVA helps you to quickly create, move or deploy VMs on different hypervisors.

The minimum supported versions to perform OVA operations are AOS 5.18, Prism Central 2020.8, and AHV-20190916.253.

You can perform the following OVA operations in Prism Central:

> **Note:** All the following operations are supported from the **OVAs** page except exporting a VM as an OVA. You can export a VM as an OVA from the **List** tab in VMs Summary View on page 95 or from the **Summary** page in VM Details View on page 108.

- Export a VM as an OVA. For more information, see Exporting a VM as an OVA on page 218.
- Upload an OVA. For more information, see Uploading an OVA on page 219.
- Deploy an OVA file as a VM. For more information, see Deploying an OVA as VM on page 229.
- Download an OVA file to your local machine. For more information, see Downloading an OVA on page 236.
- Rename an OVA file. For more information, see Renaming an OVA on page 236.
- Delete an OVA file. For more information, see Deleting an OVA on page 237.
- Resume upload when an upload is interrupted and shows an error.

  > **Note:** The resume upload action is not available in case the concatenate process of the upload is interrupted. In such a case, you need to run the Concatenate API from the **REST API Explorer** to resume the upload.

To perform any action on an OVA, select the target OVA in the **OVAs** page, and choose the required action from the **Actions** dropdown menu.

> **Note:**
>
> The **Actions** dropdown menu appears only if you select an OVA in the **OVAs** page. If the **OVAs** page is empty, then the **Actions** dropdown menu is available only after you create an OVA using **Upload OVA** or export an existing VM as an OVA.
>
> The following is an example showing the **Actions** dropdown menu in **OVAs** page.

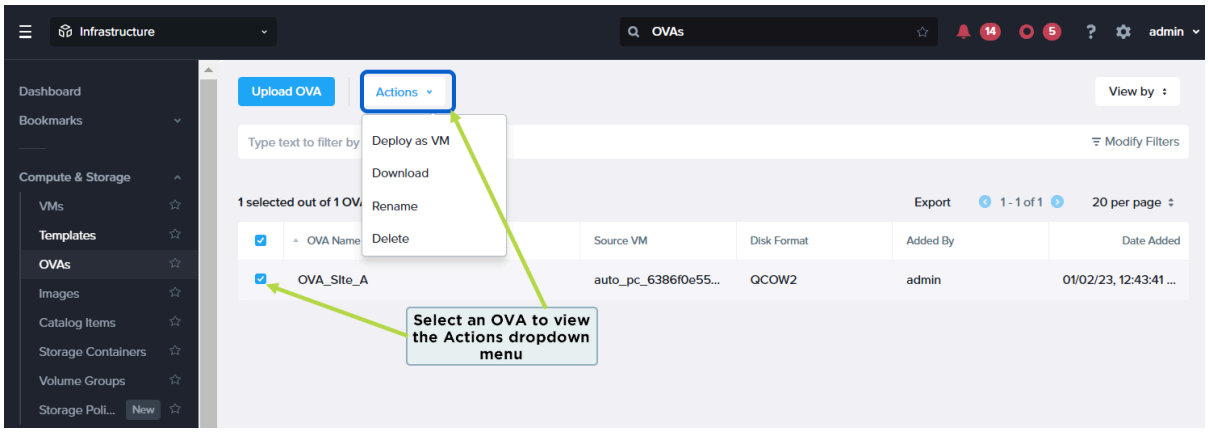


Figure 83: Actions Dropdown Menu - OVAs Page

You can check the task progress for these actions in **Tasks** page or from the Tasks icon. For information about **Tasks** page, see Tasks View on page 451.

OVAs Summary View

This section provides the information about the OVAs summary view, OVA-specific alerts, and the fields that appear in the **OVAs** page.

To access the summary view of all OVAs across registered clusters, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **OVAs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   Prism Central displays **OVAs** page that enables you to view the information about OVAs available in the cluster.

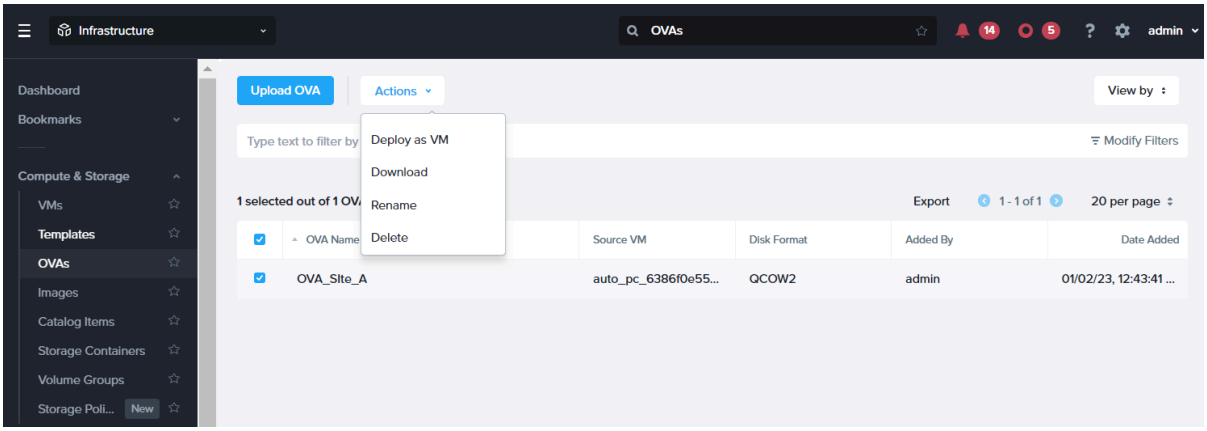


Figure 84: OVAs Page

The following table describes the fields that appear in the **OVAs** page. A dash (-) is displayed in a field when a value is not available or applicable.

Table 39: OVAs Page - Field Description

Field	Description	Values
OVA Name	Displays the name of the OVA file.	*<OVA_File Name>*
Source VM	Displays the name of source VM that was exported as an OVA. The alert indicators for the task status are displayed beside the source VM for which the task is run. See the Alert indicator table for more information.	*<Source_VM_File Name>*
Disk Format	Displays the format of the disks in the OVA.	[QCOW2|VMDK]
Added by	Indicates the user who added this OVA.	*<User_Name>*. For example, admin
Date added	Displays the date and time when the OVA was added.	(Timestamp in mm/dd/yyyy format, time in hr:min:sec [AM|PM] format) Example: 01/07/23, 3:00:20 PM

OVA Alerts

This section provides the information about the OVA specific alerts generated in Prism Central.

Table 40: OVA Alerts

OVA Alerts	Status Message sample	Description
 **Figure 85:**	`Incorrect file uploaded. Multiple OVA files present in OVA.`	Indicates the upload process failed during validation. You must fix the issue in the OVA file or upload the correct, compatible OVA file.
Figure 86:	`Upload for OVA file has not started. Please start OVA file upload using Resume Upload option.` `Uploaded OVA file has not been verified. Please start verification using Resume Upload option.`	Indicates there is an interruption in one of the three sub-tasks in the upload process. You can resume the upload. See the *Resume Upload* action procedure.
 **Figure 87:**	`OVA file upload is in progress.`	Indicates the OVA upload is in progress without any error or interrupts. Check the **Tasks** page after some time to verify the successful upload. For information on how to access **Tasks** page, see Icons in Prism Central UI on page 15 (using the Tasks icon) or Tasks View on page 451.

A sample of the error hover message is as follows:

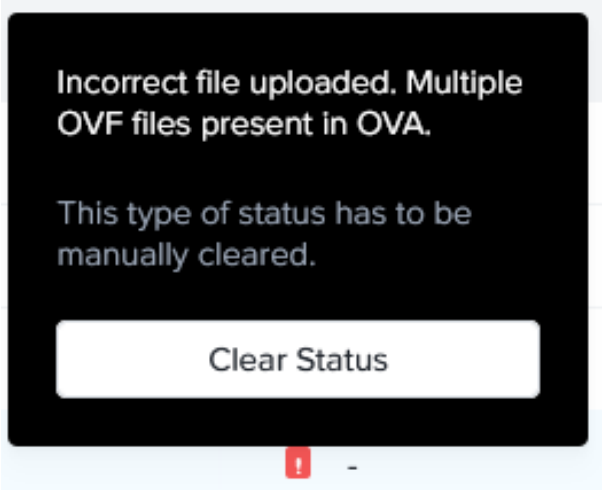


Figure 88: Sample error hover message

Filters Pane - OVAs page

You can filter the information in the **OVAs** page based on the following fields that are available in the **Filter** pane. For information about how to use **Filters** option in Prism Central, see Prism Central GUI Organization on page 27.

Table 41: Filter Pane Field Description - OVAs page

Field	Description	Values
OVA Name	Filters based on the OVA file name. It returns a list of OVAs that matches the name condition/string.	*<OVA file name >*
Source VM	Filters based on the Source VM name. It returns a list of OVAs for which the Source VM field matches the condition/string.	*<Source VM name>*
Disk Format	Filters based on the disk format. Select one or more checkbox for the OVAs of the required disk format.	VMDK, QCOW2

Exporting a VM as an OVA

Before you begin

If you intend to run the OVA in a non-Nutanix environment, ensure that you install the necessary drivers as per the requirements of the destination hypervisor.

About this task

This section describes how to export a VM an OVA.

As a Super Admin, you can select the **Export as OVA** from the **Actions** dropdown menu in the VMs **List** tab or click **Export as OVA** action in the **Summary** page of an individual VM. For information about how to access the **List** tab or **Summary** page of an individual VM, see VMs Summary View on page 95 and VM Details View on page 108.

> **Note:**
>
> - You can export a VM as an OVA with a specified disk format for the disks configured on the VM.
> - The Super Admin role was formerly called as User Admin.

To export a VM as an OVA, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment. For information about how to access the list of VMs managed by external *vCenter*, see VMs Summary View on page 95.

3. Select the target VM checkbox, and choose **Export as OVA** from the **Actions** dropdown menu.

   You can also click the target VM to access VM Details View on page 108, and select **Export as OVA** from the **More** dropdown menu.

   The system displays the **Export as OVA** window:

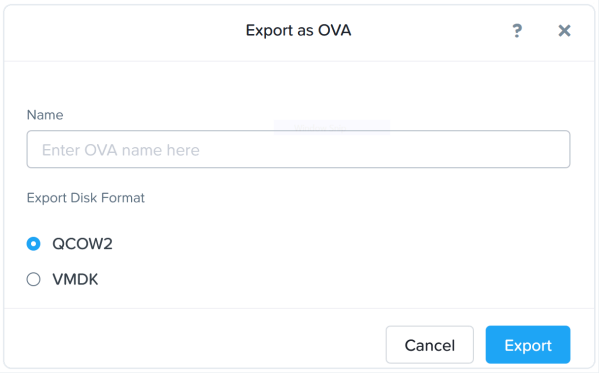


Figure 89: Export as OVA window

4. Specify the following information:

   a. Enter the name for the OVA file in the **Name** field.

   b. Select the disk format in which you want to export the OVA file in the **Export Disk Format** field.

      The default format is QCOW2. If you want to use the OVA to deploy a VM with disks formatted as VMDK, then select VMDK as the disk format.

5. Click **Export**.

   You can check the progress of the *Export as OVA* task in the **Tasks** page or from the Tasks icon. For information about **Tasks** page, see Tasks View on page 451.

   The exported OVA is available on the OVA dashboard.

Uploading an OVA

About this task

This section describes how to upload an OVA in Prism Central.

You can upload an OVA from the following sources:

- *From a local folder*: When you upload an OVA from a local source, you can upload it to only one target cluster.
- *From a URL*: When you upload an OVA from a URL, you can upload it to multiple clusters. The upload operation runs concurrently on all the selected clusters.

Select the appropriate upload source based on your requirement; a single cluster upload or multiple-cluster upload option.

Note:

- Prism Central supports the upload of up to three OVA files concurrently from local folders. Prism Central queues other OVA files that you upload until one or more of the concurrent uploads are completed.

- There is no restriction on the number of concurrent uploads for OVA uploads from URL.
- For OVA upload from local folders, the upload process can be interrupted due to the following reasons:
  - Network issues when the upload is running.
  - You close the browser window or tab in which the upload is running.
- The concatenate and validate operations of the OVA upload operation fail when an error occurs in the upload services because the checksum provided for the OVA file when it was created is incorrect.

  If the upload process is interrupted due to any reason, you can resume the process. If the validation operation is interrupted due to a concatenation error, you must run the concatenate API to resume concatenation and validation. See Concatenating Upload using APIs on page 226.

Prism Central uses indicators to display the status of OVAs that you may have tried to upload. The status message is displayed when you hover the mouse or pointing device cursor on the indicator. See *OVA Alerts* section in OVAs Summary View on page 215.

To upload an OVA, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **OVAs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **OVAs** page

3. Click **Upload OVA**.
   The system displays the **Upload OVA** window.

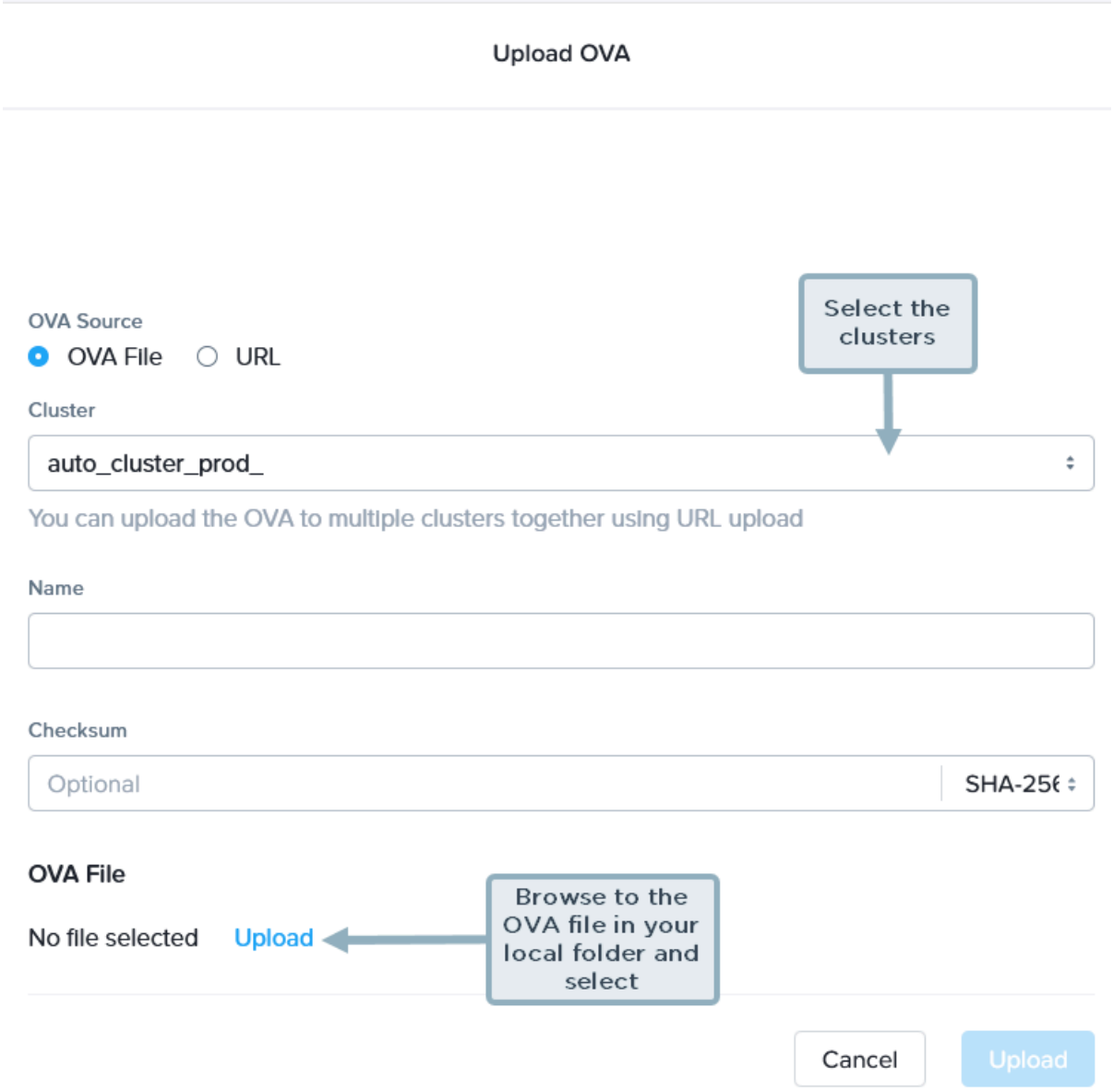


Figure 90: Upload OVA window

4. Specify the following field information in the **Upload OVA** window:

   a. **OVA Source**: Select the OVA source. For example, **OVA File** to upload from a local folder or **URL** to upload from a URL.

      If you choose **URL** in the **OVA Source** field, you can select multiple clusters in the **Select AHV Cluster** field. One cluster gets selected by default in the **Select AHV Cluster** field.

   b. **Name**: Enter the name for the OVA file.

      By default, Prism Central uses the file name of the OVA file that you upload, if you do not specify OVA file name in the **Name** field.

   c. (Optional) **Checksum**: Enter the checksum value of the OVA file based on the selected encryption as SHA-1 or SHA-256 hash algorithm.

   d. Based on your selection in the **OVA Source** field, perform the following relevant action:

      - **OVA File**: Click **Select File** to navigate to the location of the OVA file in your local folder and open it.
      - **OVA URL**: Enter the source URL from where you want to upload the OVA file.

        Note: Only NFS and HTTP protocols are supported.

        To specify one or more URLs, enter the appropriate URL address in the field using the following syntax for either NFS or HTTP:

        ```
        nfs://[hostname|IP_addr]/path
        http://[hostname|IP_addr]/path
        ```

        Enter either the name of the host (*hostname*) or the host IP address (*IP_addr)* and the path to the file. If you use a *hostname*, the cluster must be configured to point at a DNS server that

can resolve that name (see Configuring Name Servers for Prism Central in *Prism Central Admin Center Guide*). A file uploaded through NFS must have 644 permissions.

The following is an example showing the OVA URL field:

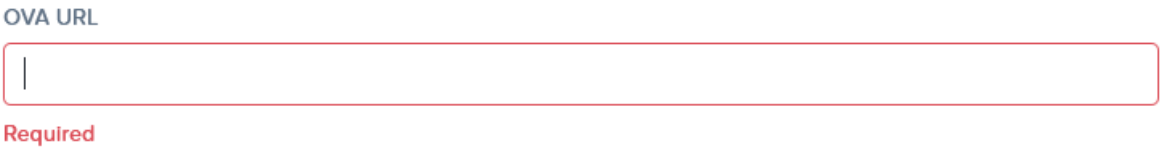


Figure 91: OVA URL field

> **Note:**
>
> Ensure that the URL that you provide is not redirected to another URL. The upload fails for redirected URLs.

Prism Central adds the URL to a list on the page and clears the **OVA URL** text box for another URL.

e. Click **Upload**.

The OVA upload starts. Wait until the **Continue in Background** option is displayed.

> **Note:** The **Continue in Background** option is not displayed for uploads from URL.

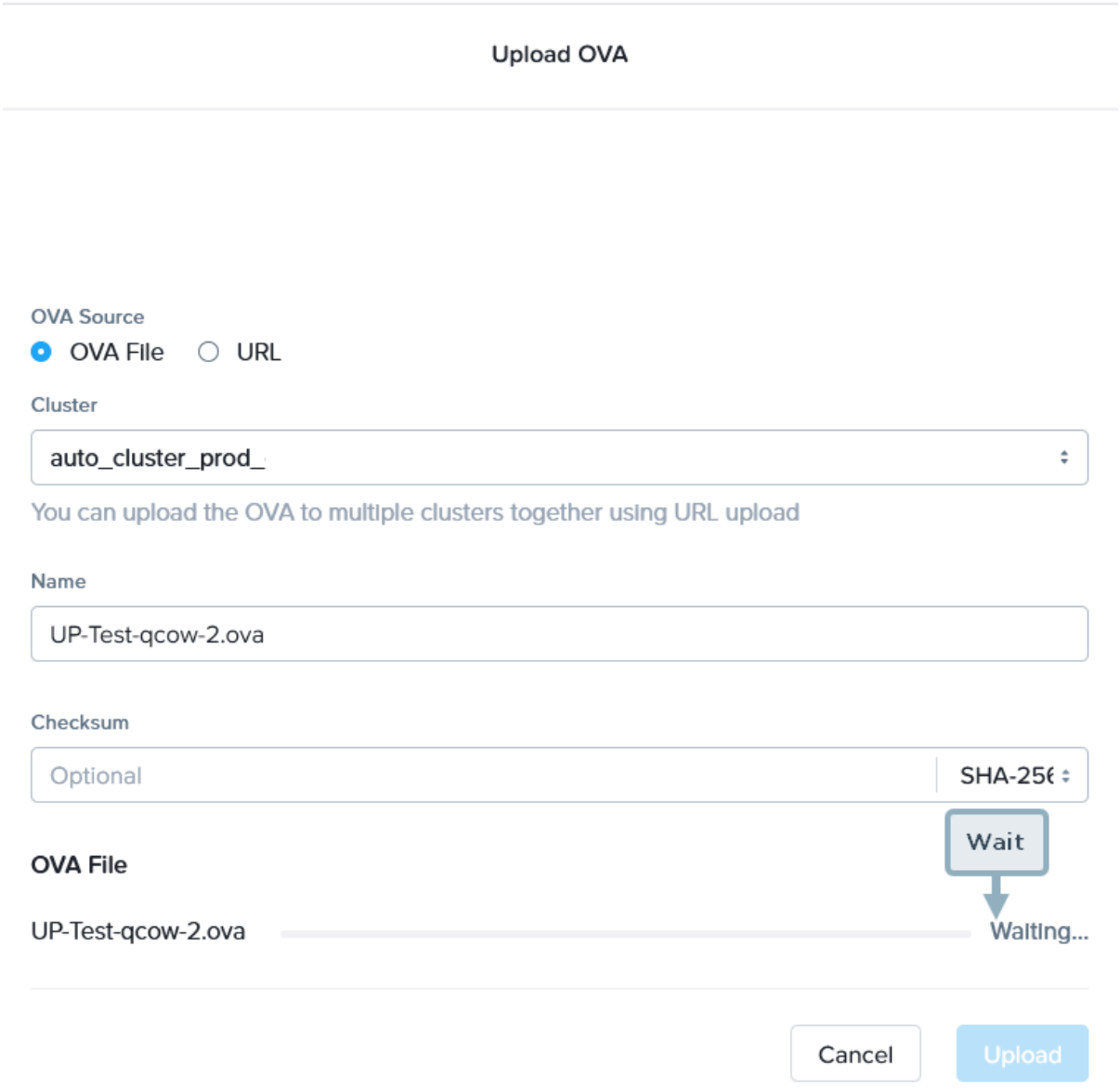


Figure 92: Upload OVA - Waiting

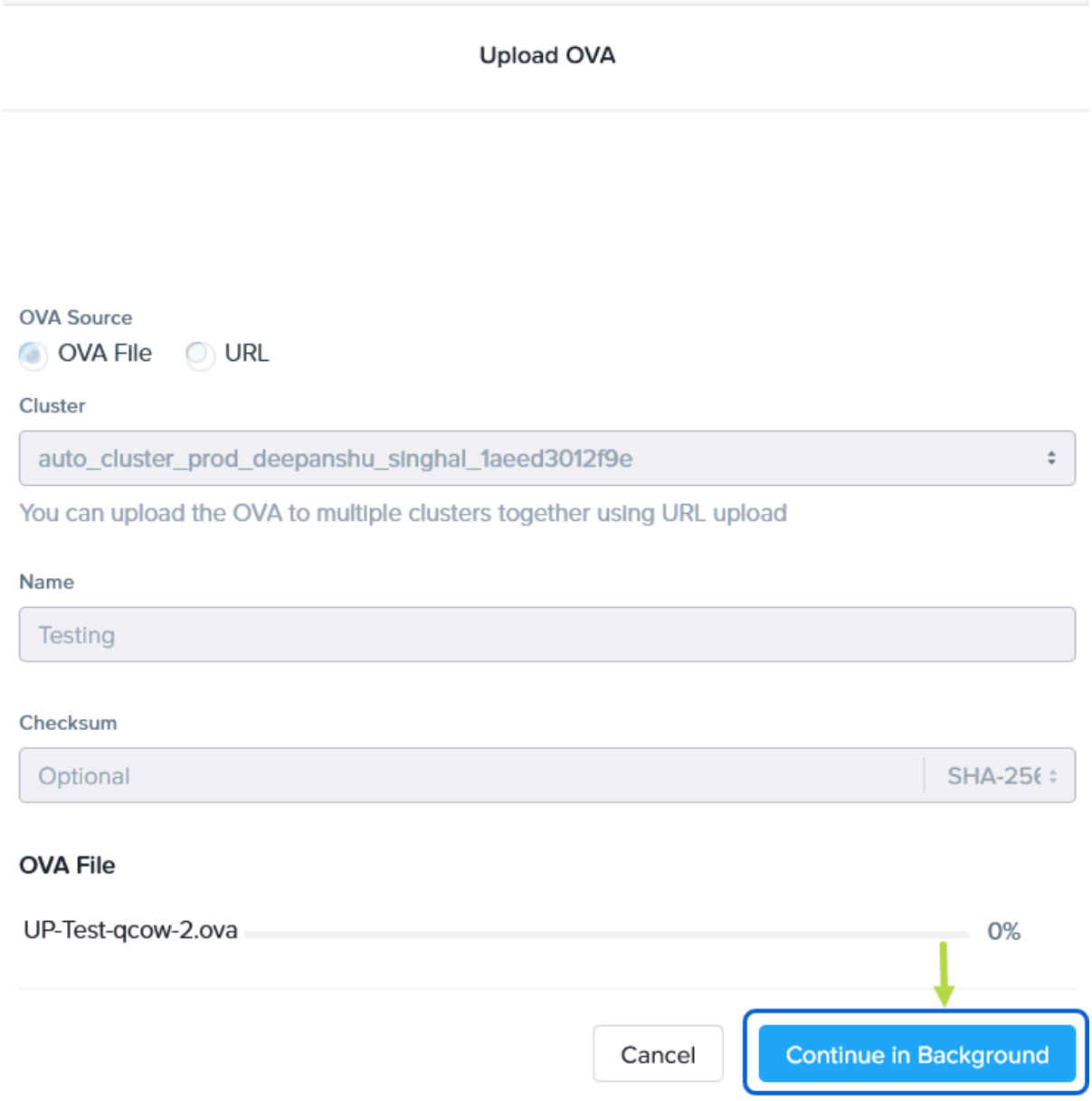


Figure 93: Continue in Background button

When the upload task is successfully completed, the system displays the following message:

```
Upload of the file is successfully completed. Verification of file is progressing in
 background. Please track it from Tasks page.
```

5. To resume an upload process that was interrupted, select the target OVA in the **OVAs** page, and choose **Resume Upload** from the **Actions** dropdown menu.

   The status message appears when you hover the mouse over the status icons for each OVA. The status message provides the indication about whether you can use the **Resume Upload** option to resume the upload.

   Note:

   Check the reason for failure of **OVA Validate** task in the **Tasks** page. If the upload process is interrupted due to concatenation and validation failure resulted from an incorrect checksum, the **Resume Upload** option is not available.

   Upload the OVA again in case the upload process was interrupted due to a checksum error.

Concatenating Upload using APIs

About this task

This section describes how to run the concatenation API using the **REST API Explorer** in Prism Central.

During an OVA upload, the OVA file is chunked and the chunks are uploaded. After upload, during the validation phase, the chunks are concatenated and validated.

When the OVA upload process is interrupted due to the concatenation error, you need to run the concatenation API to resume the upload process.

To run the concatenation API successfully, you need to perform the following actions:

- Derive the UUID of the OVA for which the upload is interrupted. The UUID is derived using the name of the OVA. For more information, see *Step 1* to *Step 4* in the following procedure.
- Run the concatenation API. For more information, see *Step 5* to *Step 6* in the following procedure.

Procedure

To run the concatenation API, perform the following steps:

1. Log in to Prism Central.
2. Select **REST API Explorer** from the *<user>* dropdown menu in the upper-right corner.

   The **REST API Explorer** opens in a new browser tab and displays a list of the objects that can be managed by the API.

3. In the **REST API Explorer** browser tab, navigate to **ovas** > **Post /ovas/list**, and click **Try it Out**.The **Post /ovas/list** helps you filter the OVAs and get the details of the details of the interrupted OVA.

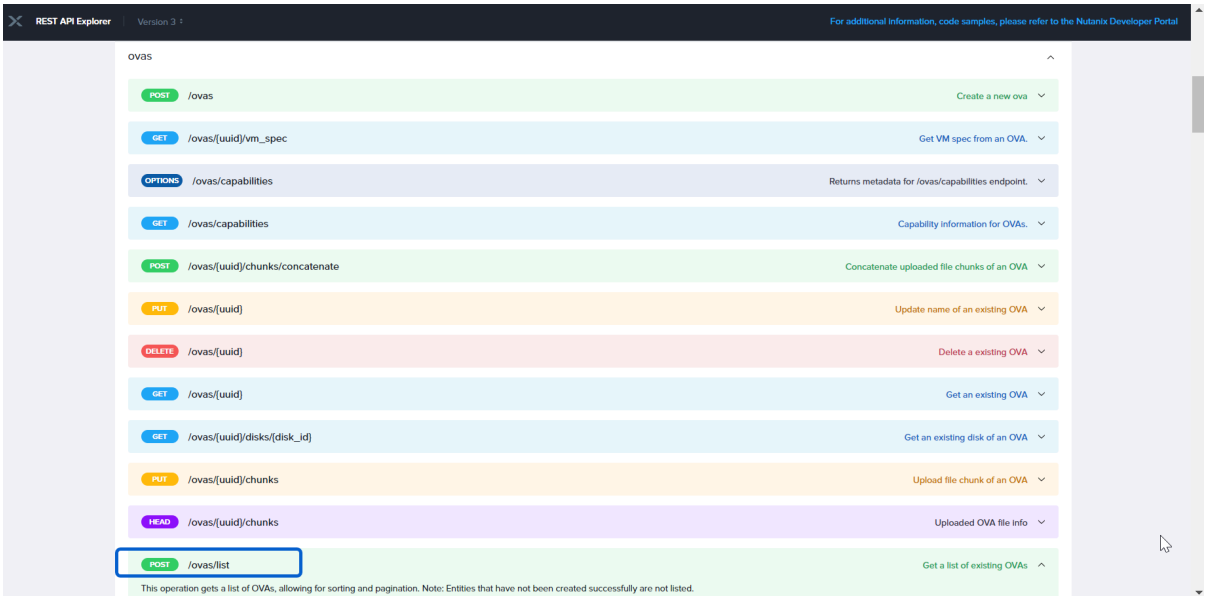


Figure 94: REST API Explorer

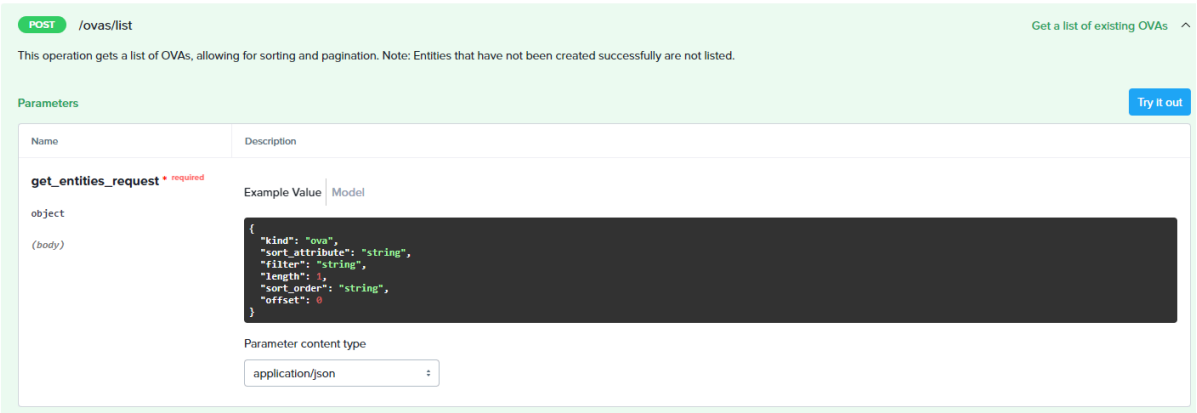


Figure 95: REST API Explorer -Try it Out

4. Enter the name of the OVA in the **"filter"** field of **get_entities_request** API in the following format, and click **Execute**.

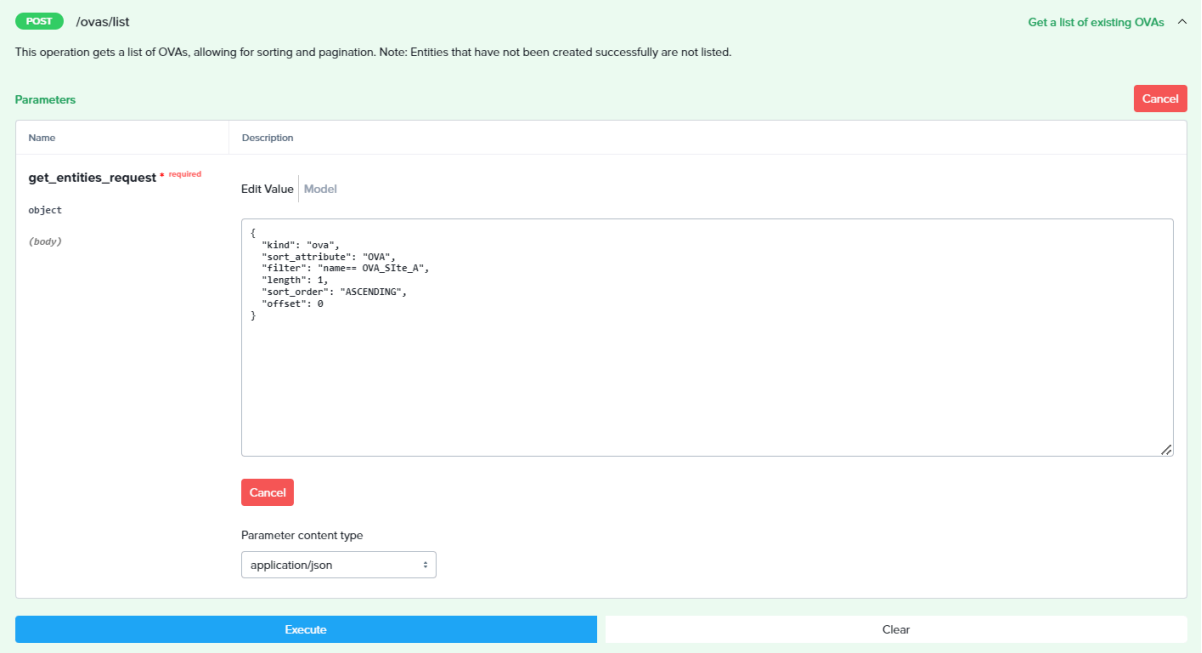


Figure 96: Parameter Filter

In the **Response Body** box, the UUID of the queried OVA is listed. Note or copy the UUID.

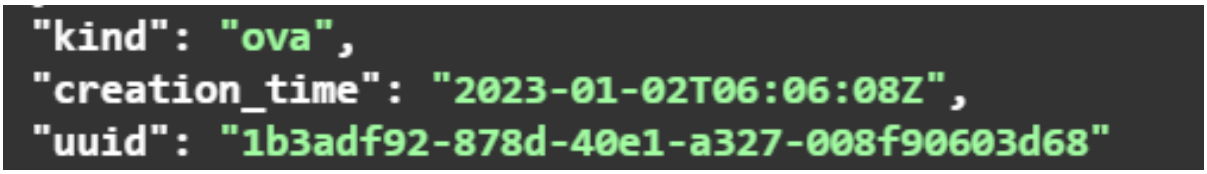


Figure 97: OVA Upload UUID

5. In the **REST API Explorer** browser tab, navigate to **ovas** > **Post /ovas/{uuid}/chunks/concatenate**, and click **Try it Out**.

6. Enter the UUID of the OVA in the **uuid** field, and click **Execute**.

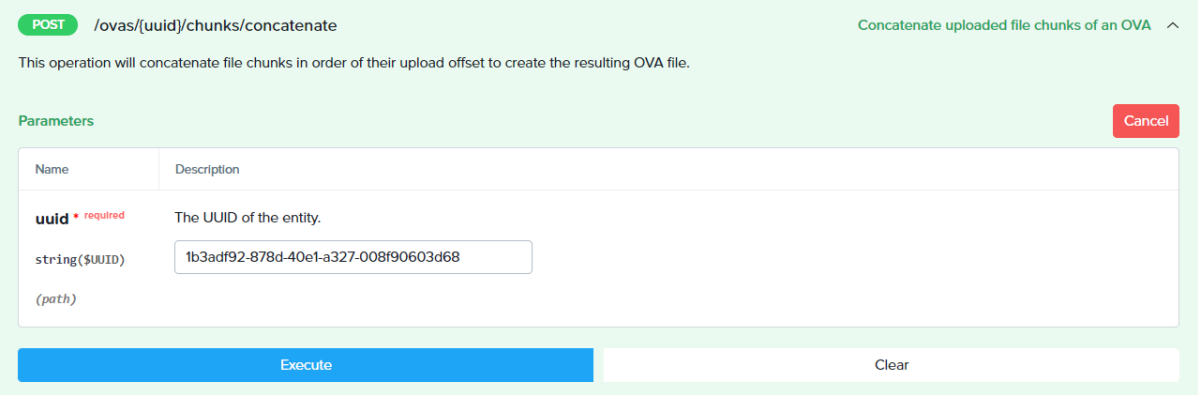


Figure 98: OVA Upload UUID

The **Response Code** field displays 202 indicating that the concatenation and validation request has been accepted.

Deploying an OVA as VM

About this task

This section describes how to deploy an OVA as VM.

> **Note:**
>
> For the OVAs that are not created from AHV, ensure that the pre-installed VirtIO drivers are available for them. For more information about VirtIO drivers, see Nutanix VirtIO for Windows in *AHV Administration Guide*.

To deploy an OVA as a VM, perform the following steps:

> **Note:** You can navigate back and forth between the steps using **Back** and **Next**.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **OVAs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **OVAs** page

3. Select the target OVA, and choose **Deploy as VM** from the **Actions** dropdown menu.
   The system displays the **Deploy as VM** window.

   You need to use the steps in the **Deploy as VM** window to configure the deployment.

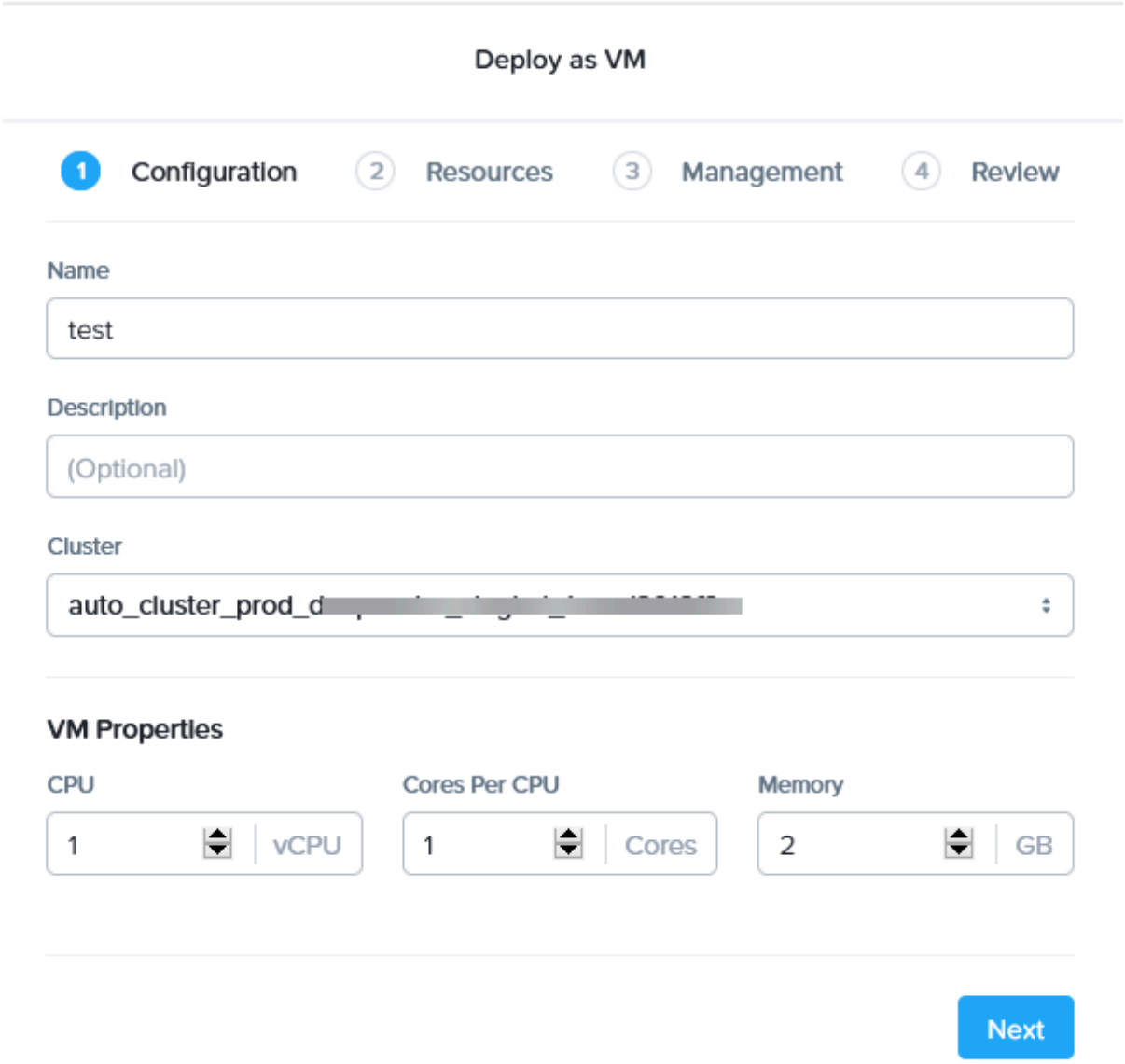


Figure 99: Deploy as VM - Configuration Step

4. In the **Deploy as VM** window, specify the following information in the **Configuration** step:

   a. **Name**: Enter the name of the VM that needs to be deployed.

   b. **Description**: Enter that description such as Backup VM for Prism.

   c. **Cluster**: Select one of the following options from the dropdown menu:

      - Target cluster on which you intend to place the guest VM.

        Only the clusters for which you have access and where OVAs are available, are displayed in the **Cluster** dropdown menu. By default, Prism Central selects a cluster in the dropdown menu for deployment.

      - **Automatic cluster selection**, if you intend to place the guest VM on a system-selected cluster. For more information, see Automatic Cluster Selection for VM Placement section in the *AHV Administration Guide*.

        > **Note:** Automatic cluster selection configuration for VMs with GPU specifications is not supported.

   d. **CPU**, **Cores Per CPU** and **Memory** in **VM Properties**: Specify the CPU and memory requirements as required.

   e. Click **Next**.
   The system displays the **Resources** step.

5. Specify the following information in the **Resources** step:

> **Note:**
> You can add new disks, NICs and GPUs.

a. **Boot Configuration**: Select **UEFI Mode** only if your hardware supports UEFI boot mode, else select **Legacy BIOS Mode**.

b. **Set Boot Priority**: The default priority is already set.

c. **Attach Disk**: Used to attach additional disks in addition to the disks already available in the OVA.

In the **Attach Disk** window, specify the required information, and click **Save**.

For more information about how to attach a disk, see Creating a VM through Prism Central (AHV) on page 121.

d. **Attach to Network**: Used to attach the network.

In the **Attach to Network** window, select **Subnet** and **Network Connection State** from the dropdown menus.

For more information about how to configure network, see Creating a VM through Prism Central (AHV) on page 121.

e. Click **Add GPU** to add GPU resources.

> **Note:**
> - Automatic cluster selection configuration for VMs with GPU specifications is not supported. If you have selected the **Automatic cluster selection** option in step 4.c on page 231, the system does not provide you the option to add GPU.
> - If the selected cluster has GPU resources, then you can add multiple vGPUs to the same VM. Addition of multiple vGPUs is based on the installed GPU resources.

- For information about how to add multiple GPUs, see Adding Multiple vGPUs to the Same VM on page 147.
- For information about multiple vGPU support, see Multiple Virtual GPU Support information in *AHV Admin Guide*.

f. Click **Next**.
The system displays the **Management** step.

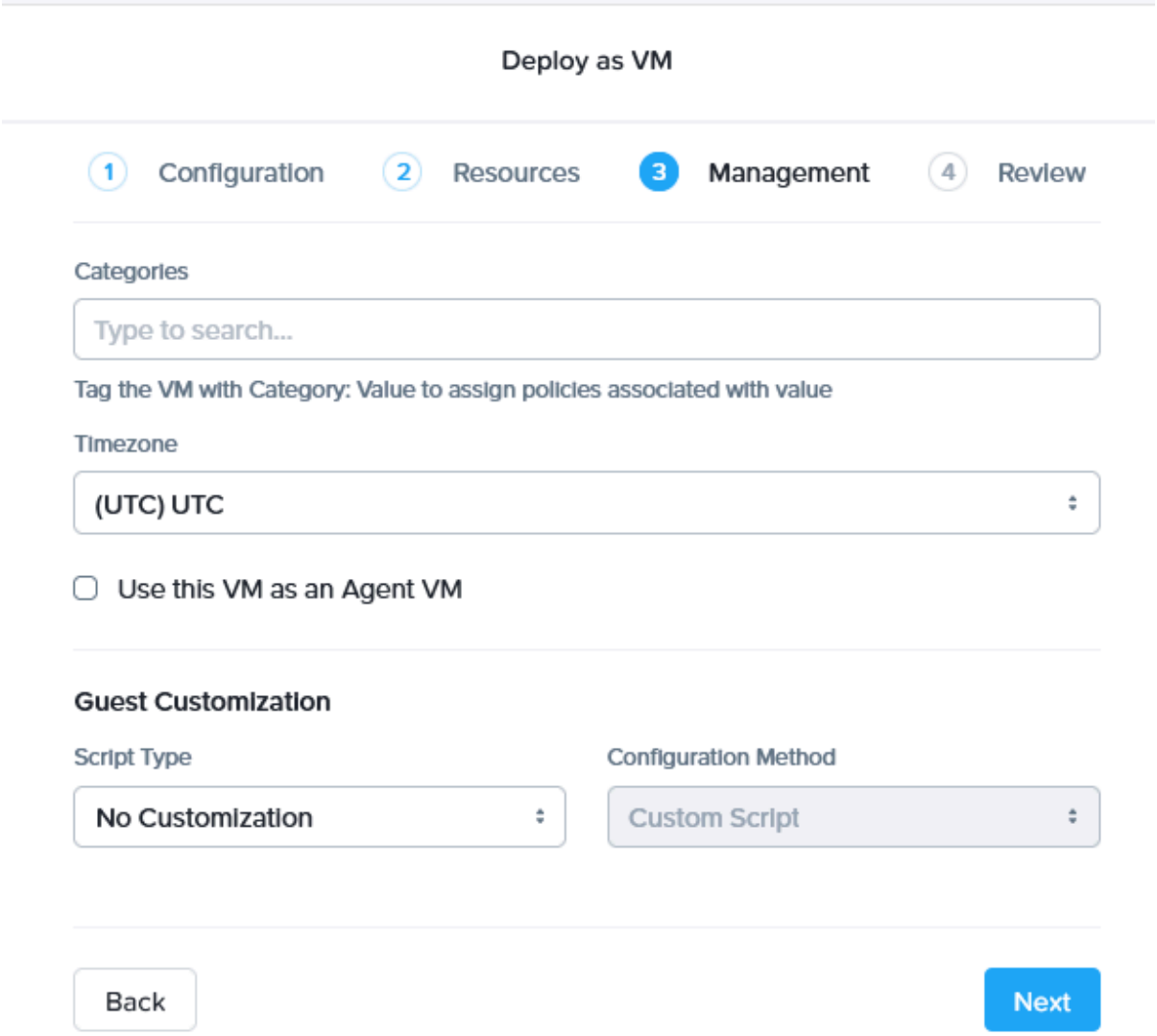


Figure 100: Deploy as VM - Management Step

g. **Categories**: Select the category to be mapped to the VM. Type in this field to display a list of available categories. For more information about categories, see Category Management on page 454.

h. **Timezone**: Select the appropriate timezone as per your requirement.

i. **Use this VM as an Agent VM**- Select this checkbox if you want to use the deployed VM as an agent VM.

j. **Guest Customizations**: Used to customize the VM. Select Cloud-init (for Linux VMs) or Sysprep (for Windows VMs).

   Script Type: Select the VM script customization type from the dropdown menu. The options are `No Customization`, `Sysprep(Windows)`, or `Cloud-init (Linux)`.

   Configuration Method: Select the VM script customization method from the dropdown menu. This field is activated when the **Script Type** is either `Sysprep(Windows)` or `Cloud-init (Linux)`. The options are `Custom Script` or `Guided Script`.

The system displays the options required to configure Cloud-init and Sysprep, such as options to specify a configuration script and option to upload script.

k. To specify a user data file (Linux VMs) or answer file (Windows VMs) script for unattended provisioning, perform either of the following actions:

   » If the file is available on your local computer, click **Upload Script**, choose and upload the file.

   » Create or paste the contents of the file in the text box below the **Upload Script**.

   Note: The script type supports the following file formats.

   - Sysprep: XML
   - Cloud-init (Linux): YAML, JSON, or Shell.

l. Click **Next**.
The system displays the **Review** step.

Deploy as VM

1 Configuration 2 Resources 3 Management 4 Review

Configuration

Name	test
CPU	1 vCPU
Cores Per CPU	1 Cores
Memory	2 GB

Resources

Disks

#	Type	Image	Size	Bus Type
1	Disk	-	0.94 GiB	SCSI
2	Disk	-	0.94 GiB	SCSI

Boot Configuration: Default Boot Order (CD-ROM, Disk, Network)

Networks

Subnet	Private IP
pc_network	Auto-Assign

Management

Categories	None
Timezone	UTC
Guest Customization	No Customization

6. Review the deployment configuration in the **Review** step, and Click **Launch** .
   You can check the progress of the deployment task in the **Tasks** page or from the Tasks icon. For information about **Tasks** page, see Tasks View on page 451.

Downloading an OVA

This section describes how to download an OVA on your local machine from Prism Central.

About this task

To download an OVA, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **OVAs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **OVAs** page.
3. Select the OVA to be downloaded, and choose **Download** from the **Actions** dropdown menu.
   The system displays the **Download** window.

   The following is an example showing the **Download** window:

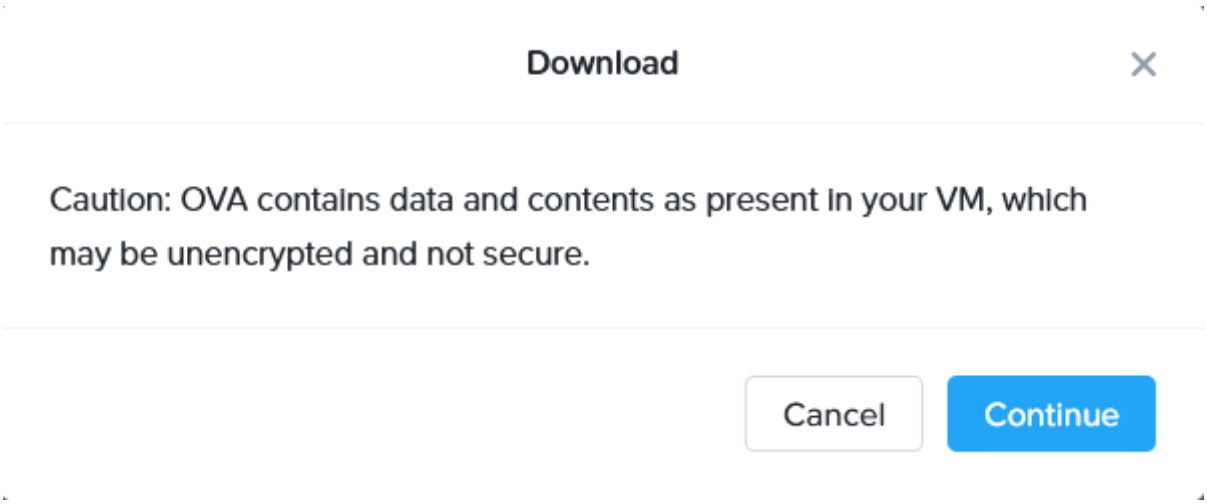


Figure 102: Download window

Note: You can download up to five OVAs in parallel.

4. To confirm the download action, click **Continue**. To cancel the download action, click **Cancel**.

   The downloaded file is saved in a local folder based on your browser's download settings.

   Once the download starts, it continues even after you sign out from the console, as the TCP connection does not break. However, if you close the browser or the internet connection is interrupted, the download fails as the TCP connection breaks.

Renaming an OVA

This section describes how to rename an OVA in Prism Central.

About this task

To rename an OVA, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **OVAs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **OVAs** page
3. Select the OVA to be renamed, and choose **Rename** from the **Actions** dropdown menu.
   The system prompts you to update the new name for the OVA file.

   The following is an example showing the **Rename** window:

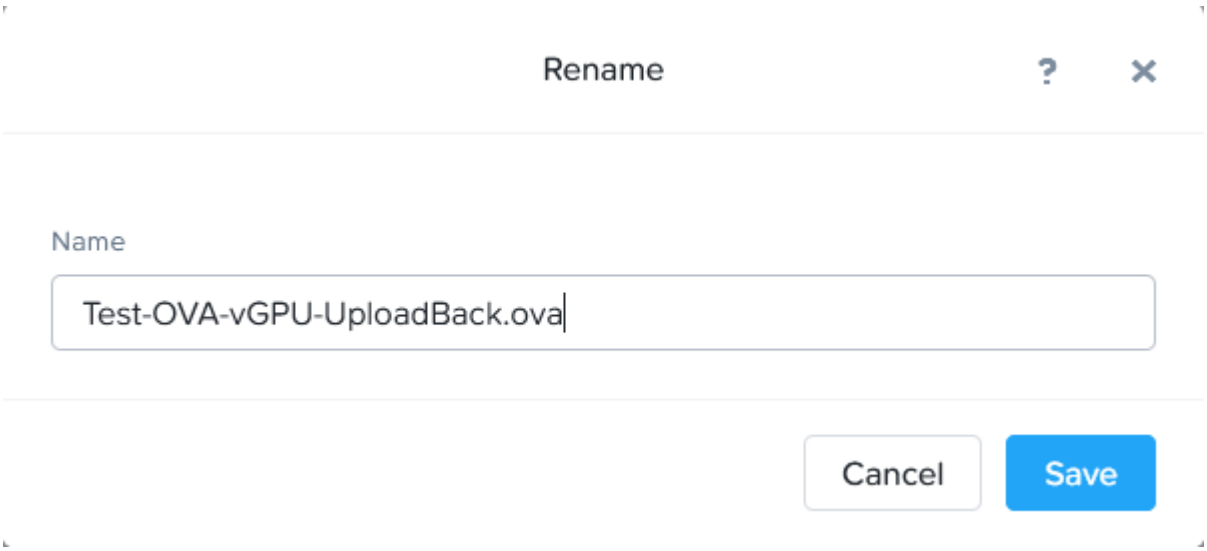


Figure 103: Rename window

4. Delete the old name and enter the new name in the **Name** field.
5. To confirm the rename action, select **Save**.
   To cancel the rename action, select **Cancel**.

Deleting an OVA

This section describes how to delete an OVA in Prism Central.

About this task

To delete an OVA, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **OVAs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **OVAs** page.

3. Select the OVA to be renamed, and choose **Delete** from the **Actions** dropdown menu.
   The system prompts you to confirm the delete action.

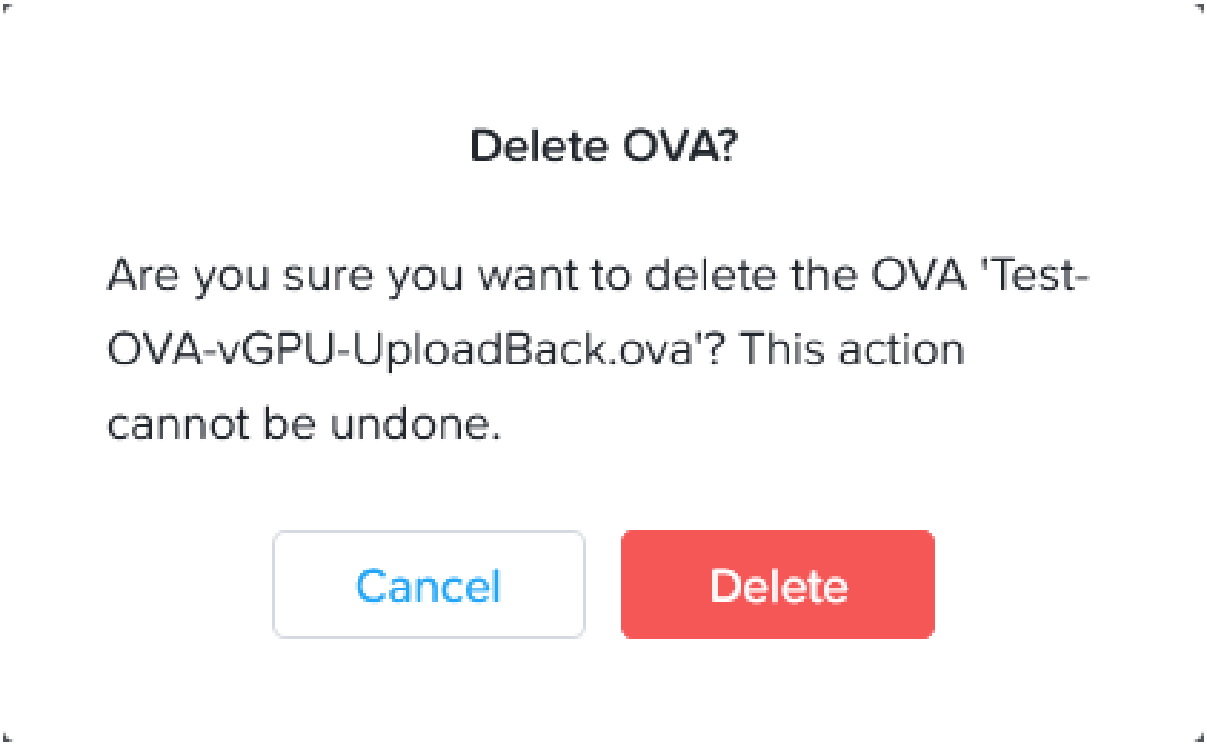


Figure 104: Delete OVA window

4. To confirm the delete action, select **Delete**.
   To cancel the delete action, select **Cancel**.

> **Note:** The **Delete** action deletes the OVA permanently. You cannot recover a deleted OVA.

Image Management

Prism Central provides a centralized location to manage the images you require on registered AHV clusters. You can upload images to the clusters and maintains an inventory of the images on it.

> **Note:**
>
> - You can configure policies that govern the image placement process. These policies allow you to specify the clusters on which the images need to be uploaded. For more information about the image placement policies, see Image Placement Policies on page 476.
> - You can also update the uploaded images. For more information, see Modifying an Image on page 260

Figure 105: Image Management Demo

A video on this topic is available https://youtu.be/UlqM8jjvr4s on YouTube.

Image Source

In Prism Central, you can add images from the following sources:

- Workstation. For more information, see Adding Images from a Workstation on page 244.
- URLs to images on a remote server. For more information, see Adding Images from a Remote Server on page 249.
- VM disk. For more information, see Adding Images from a VM Disk on page 253.

For information about these sources, see Adding an Image on page 244.

Image Placement Methods

When you add images, the system provides you the following image placement methods:

- Select target clusters during images upload, and place image directly on the target clusters.
- Specify target clusters using image placement policies, and place images on the target clusters based on image placement policies.

  In this case, you can select the image categories, and the system uploads images to all the registered clusters mapped to the image categories in image placement policy. For information about image placement policies, see Image Placement Policies on page 476.

  > **Note:** You can also suspend or resume the image placement policies based on your requirement. For more information, see Suspending or Resuming Enforcement of an Image Placement Policy on page 258

For information about how to add images, see Adding Images from a Workstation on page 244 and Adding Images from a Remote Server on page 249.

Images Import from Registered Clusters to Prism Central

In addition to the sources defined in Image Source on page 239, you can also import images from registered AHV clusters. You can import images only from registered clusters that are running AOS 5.8 or later. For more information, see Importing Images to Prism Central on page 261.

Images Summary View

The **List** tab in **Images** page displays the information about all the images across registered clusters.

> **Note:** This section describes the information and options that appear in the **Images** page.
>
> - See Prism Central GUI Organization on page 27 for instructions on how to view and organize that information in various ways.
> - See Image Management on page 238 for information about how to add and manage images through Prism Central.
> - See Image Placement Policies on page 476 for information about image placement policies.
> - See Bandwidth Throttling Policies on page 484 for information about bandwidth throttling policies.

To access the summary view of all images, perform the following steps:

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The system displays the **List** tab by default.

   The following is an example showing the **List** tab in **Images** page:

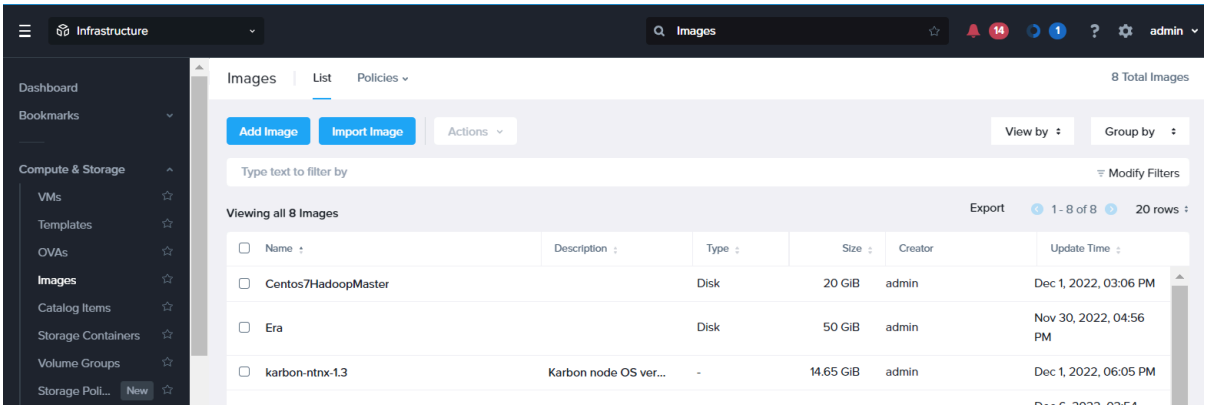


Figure 106: List tab - Images

The following table describes the fields that appear in the **List** tab in **Images** page:

> **Note:** A dash (-) is displayed in a field when a value is not available or not applicable.

Table 42: Images Page - Field Description

Parameter	Description	Values
Name	Displays the image name. Click the image name to view the detailed information about that image. For more information, see, Image Details View on page 242	<Image name>
Description	Indicates which user uploaded this image.	(text string)
Type	Displays the image type.	ISO, Disk
Size	Displays the image size.	x [MB|GB], where x is numeric digit.
Creator	Displays who created the image.	<user>. For example admin

You can perform the following actions for the images in the **List** tab:

- Access the detailed information about an individual image. For more information, see Image Details View on page 242.
- Filter the images list based on available parameter values using **Filters** pane. For more information about **Filters** pane, see Filters Pane - Images on page 241.
- Export the table that contains the list of images and their information to a file in a CSV format. For more information about **Export** option, see Export on page 32.

- Group the images based on pre-defined criteria. For information about how to group the images, see Group by on page 29.
- View images based on pre-defined criteria or create a custom view. For information about available views and how to create a custom view, see View by on page 29.
- Perform the following image-specific actions on a single or multiple images using the **Actions** dropdown menu:
  - **Update** - Used to update the image file attributes. For details, see Modifying an Image on page 260.
  - **Delete** - Used to delete the image. Select the image(s), and choose **Delete** from the **Actions** dropdown menu.
  - **Add Image to Catalog** - Used to add an image to the catalog. For more information, see Modifying an Image on page 260.

    For information on how to manage the catalogs, see Catalog Management on page 262.
  - **Manage Categories** - Used to assign a category to the images. For information about how to manage image categories , see Modifying an Image on page 260.
  - **Download Image** - Used to download the image. Select the image, and choose **Download Image** from the **Actions** dropdown menu.

    The downloaded image does not have any file extension. If you download an .ISO image, you must rename the file to append .ISO extension before using the image. A downloaded disk image is in raw format and you must manually convert it using *qemu-img* or similar tool before using the disk image.

    The Image download speed is dependent on the following factors:
    - Bandwidth between Prism Element where image is stored and Prism Central
    - Bandwidth between Prism Central and client system

    Note: You can also perform these actions from the **Summary** page of an individual image. For more information, see Image Details View on page 242.

Filters Pane - Images

You can filter the information in the **Images** page based on the following fields that are available in the **Filters** pane. For information about how to use **Filters** option in Prism Central, see Prism Central GUI Organization on page 27.

Table 43: Filter Pane Field Description - Images page

Field	Description	Values
Name	Filters based on the image name. It returns a list of storage containers that satisfy the name condition/ string.	*<Image name >*
Description	Filters based on the image description.	(description string)
Type	Filters based on the image type. Check the box(es) for the desired image types.	Disk, ISO

Policies Tab

The **Policies** tab displays **Placement Policies** and **Bandwidth Throttling Policies**.

- For information about how to configure **Placement Policies**, see Image Placement Policies on page 476.
- For information about how to configure **Bandwidth Throttling Policies**, see Bandwidth Throttling Policies on page 484.

Image Details View

To access the details view of an individual image, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The system displays the **List** tab by default.
3. Click the <*Image_Name*> to view the **Summary** tab of an individual image.

> **Note:** Replace <*Image_Name*> with the actual image name at your site.

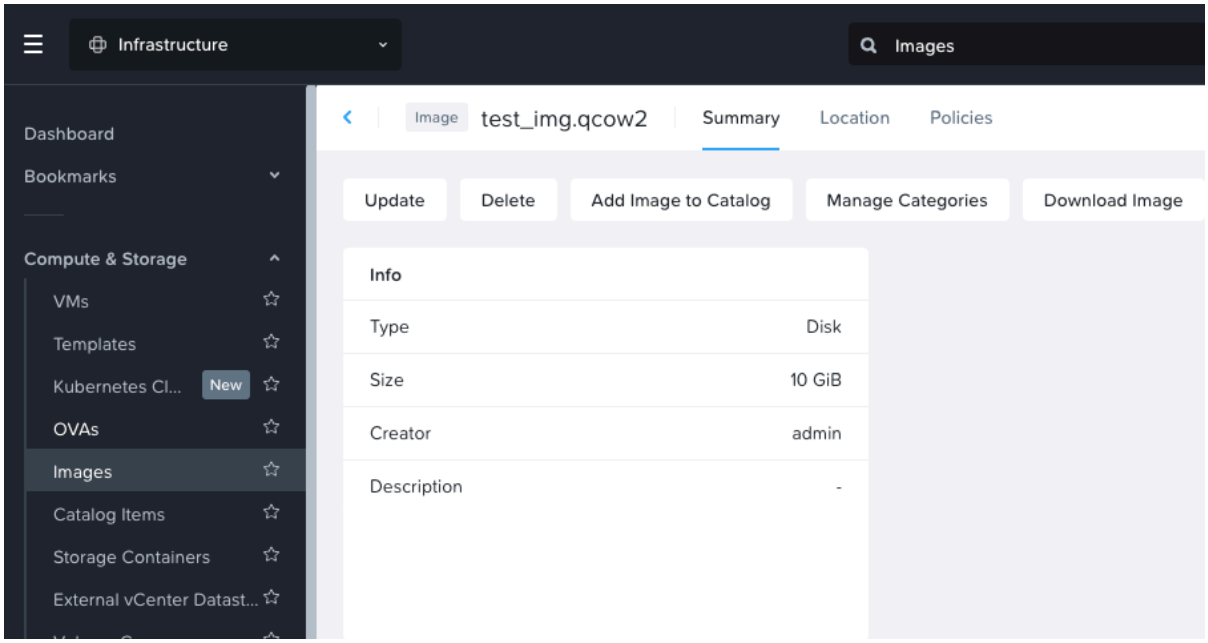


Figure 107: Image Details View (Summary Tab)

For information about the fields available in **Info** widget, see Images Summary View on page 239.

Location Tab

The following table describes the information displayed in the **Location** tab

Table 44: Location Tab -Field Description

Field	Description	Values
Name	Displays the name of the cluster in which the image is stored. Each row represents another cluster that contains the image.	*<Cluster name>*
AOS Version	Displays the AOS version running in the cluster.	*AOS version number*
Hypervisor	Displays the name of the hypervisor running in the cluster.	AHV, ESXi, Hyper-V
Host Count	Displays the number of hosts in the cluster.	(integer)
VM Count	Displays the number of VMs in the cluster	(integer)

Policies Tab

The **Policies** tab lists the policies that apply to the selected image. For information about the image-related policies, see Image Policy Management on page 476.

- For information about how to configure **Placement Policies** for images, see Image Placement Policies on page 476.
- For information about how to configure **Bandwidth Throttling Policies** for images, see Bandwidth Throttling Policies on page 484.

Requirements

You must meet the following requirements to access the image management feature in Prism Central:

- The version of both Prism Central and AOS on registered clusters is 5.8 or later.
- Clusters is registered with Prism Central with AHV installed in it.
- The port 2007 must be open for the image service.

Limitations

The following limitations apply to the image management feature in Prism Central:

- You cannot update images that another Prism Central instance managed earlier. However, the images are displayed in Prism Central, and you can use the images to create VMs or delete the images you no longer need.
- You cannot choose a container when uploading images from Prism Central. Prism Central uploads images to the container named `SelfServiceContainer`.
- When you upload images from a workstation and place the images on multiple clusters during the initial image upload, the uploaded image becomes active (in Prism Element) on only one of the selected clusters and remains inactive on the other clusters registered to Prism Central.
- If you add a new cluster that contains images to an existing Prism Central, you must first import the images to Prism Central and then use the image placement policies to push the images to any other cluster already registered with Prism Central.
- If an image is not active on a cluster, as an admin user it is possible that you are unable to use Prism Central to create that VM on that cluster. The cluster on which you want to create the VM cannot check

out the image from a remote cluster. In this scenario, you must upload the image manually to the cluster on which you want to create the VM.

When you create a VM, Prism Central uses API v2 workflows. API v2 does not have the checkout workflow. The image checkout workflow is used to copy an image on demand from cluster B to cluster A if the image does not exist or is inactive on cluster A.

Note:

You can remove this limitation using an image placement policy. Assign a category to the image that is available on multiple remote clusters, and apply the image placement policy to the image category. When you apply the image placement policy to a image, Prism Central propagates the image to all the clusters that are included in the image placement policy. Prism Central can then checkout the image from the remote cluster where the image is active and create the VM.

The system can take up to 15 minutes to switch the image propagation from an alternative cluster. For example, if an image is located on clusters A and B. As a result of an image placement policy you applied to that image, cluster A starts copying the image to cluster C. During the copy operation, if cluster A becomes unavailable, the system takes up to 15 minutes to switch to cluster B, and starts copying the image from cluster B to cluster C.

Adding an Image

This section describes how to add an image in Prism Central.

About this task

You can add the images in Prism Central from any of the following sources:

Procedure

- Workstation, see Adding Images from a Workstation on page 244.
- Remote Server, see Adding Images from a Remote Server on page 249.
- VM disk, see Adding Images from a VM Disk on page 253.

Adding Images from a Workstation

This section describes how to add (or upload) the images in Prism Central from the workstation that you use to access Prism Central.

About this task

You can select multiple images, and add them as part of a single operation.

Note:

- By default, the system selects all the clusters. The system also provides you the option to clear the cluster as per your requirement.
- The image becomes active (in Prism Element) on the selected cluster and inactive on other clusters registered to Prism Central.
- Image placement policies, if applied, take effect after a short duration.
- Most modern browsers impose file size limitations that affect this upload method. If you intend to upload images larger than 2 GB, Nutanix recommends you to upload the images from a remote server.

- The browser type, and CPU and RAM utilization on the workstation limit the number of concurrent uploads. Concurrent uploads that exceeds the default limit of the browser are queued or throttled by the browser and can consume more time.
- Large file uploads, and high CPU and memory utilization can slow down the browser.

To upload an image from a workstation, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default.

3. Click **Add Image**.
   The system displays the **Add Images** window.

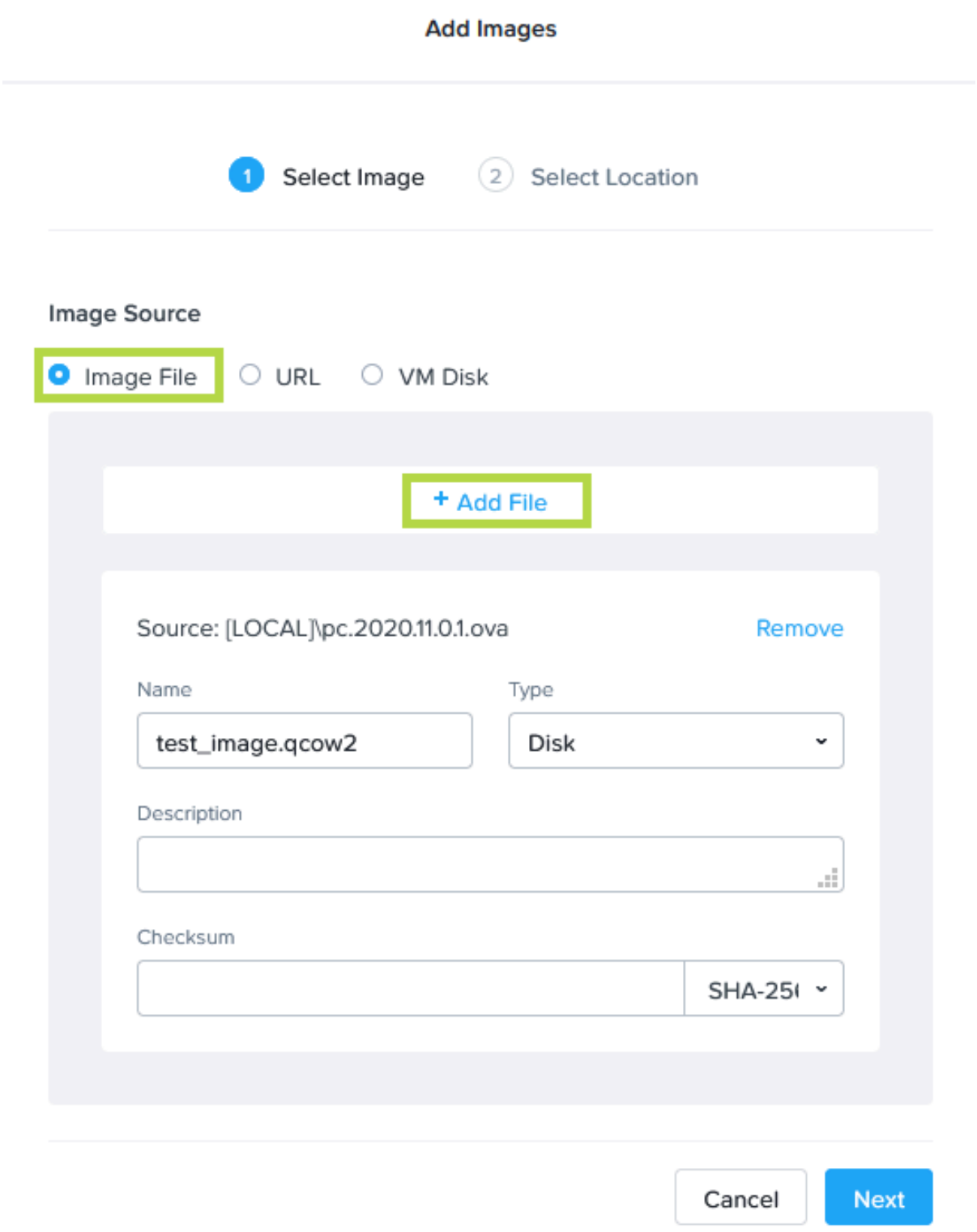


Figure 108: Add Images: File

4. Specify the following information in the **Select Image** step:

   a. **Image Source** - Select **Image File** radio button.

   b. Click **Add File**. The system displays the file attributes.

   c. Browse to the location of the image file, and then click **Open**.

   d. Specify the following attributes for the image file:

      - **Image Name** - Enter the image name. By default, the system pre-fills the name of the file you selected, however you can change the image name as per your requirement.

        Note: Ensure that the name of the image is unique across all the images in Prism Central.

      - **Image Type** - Select the type of image.
      - **Image Description** - Enter the description for the image file.
      - **Checksum** - Select the hashing algorithm.

   e. Repeat step b to step d if you want to add multiple image files.

      To remove an image file entry, locate the entry and click **Remove**.

   f. Click **Next** after you add all the image files.
      The system displays the **Select Location** step.

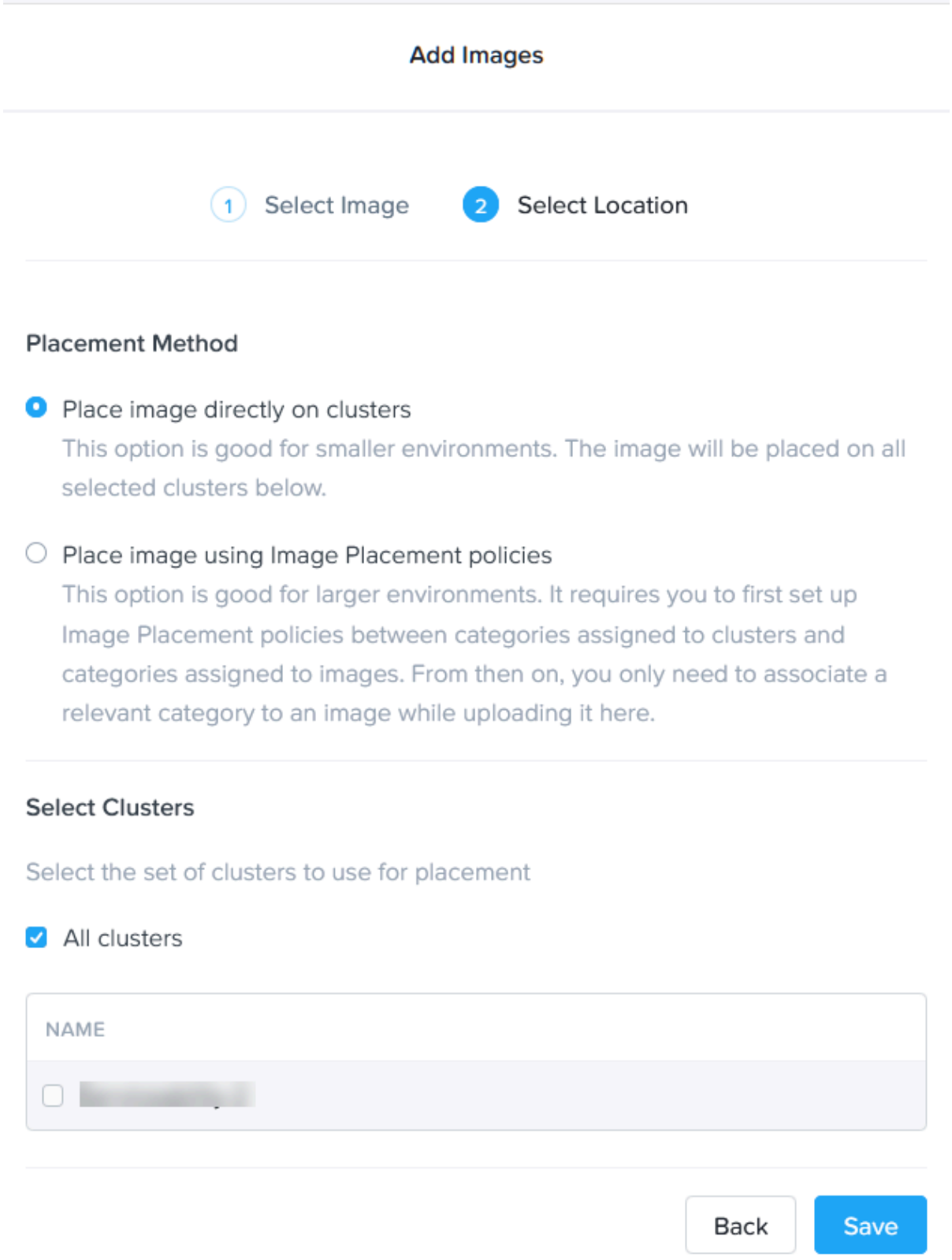


Figure 109: Add Images: Select Location

5. Specify the following information in the **Select Location** step:

   a. **Placement Method** - Select one of the following placement methods:.

      - **Place image directly on clusters**- Used to place the images directly o the selected clusters.
      - **Place image using Image Placement policies** - Used to delegate image placement decisions to configured policies and assign categories to the images

   b. If you select:

      - **Place image directly on clusters** - Specify the following information:

        Select Clusters - Select the clusters in which you want to add the image file in the **Name** column.

        Note:

        - By default, the system selects all the registered clusters.
        - If you want to add the images to all registered clusters, ensure that you select all the clusters in the **Name** column.
        - If you want to upload to only a subset of the registered clusters, clear all clusters in the **Name** column, and only select the clusters you want from the list.

      - **Place image using Image Placement policies** - Specify the following information:

        Select Image Categories - Click inside the search box and select the category you want from the list. You can also type the name of the category to reduce the list to matching names.

        Note:

        - To select multiple categories, click Add icon beside each category name that you want to include in the categories.
        - To remove a category, click Remove icon beside each category name that you want to remove from the selected categories.
        - For information about how to create a category and assign a category value to an image, see Creating a Category on page 457 and Associating Images with Categories on page 479.

6. Click **Save**.
   The system adds the image files in batches and takes some time to enforce the image placement policies (if selected).

   Note: You can also suspend or resume the image placement policies based on your requirement. For details, see Suspending or Resuming Enforcement of an Image Placement Policy on page 258.

Adding Images from a Remote Server

You can add an image from a remote server to registered Nutanix clusters. To add an image from a remote server, you need the URL of the image. You can also specify URLs to multiple images as part of a single operation. When you specify image URLs, Prism Central adds the images to all registered clusters. Adding the image from a remote server also allows you to overcome file size limitations imposed by modern browsers. The file size limitation is usually 2 GB.

About this task

To add an image from a remote server, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default.
3. Click **Add Image**.
   The system displays the **Add Images** window.

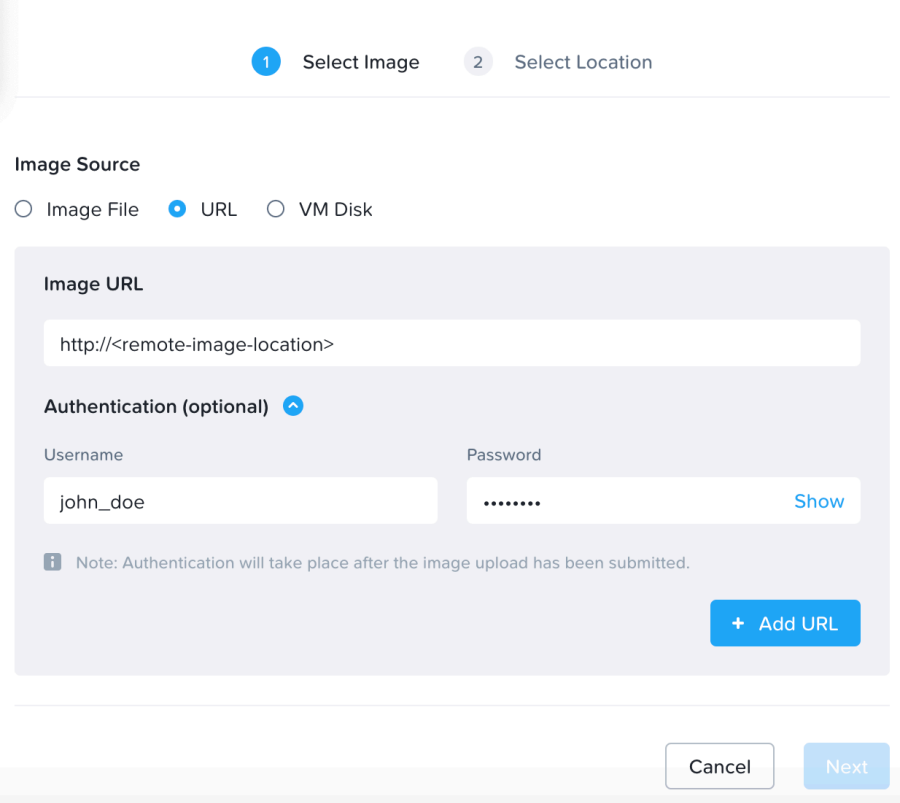


Figure 110: Add Images: URL

4. Specify the following information in the **Select Image** step:
   a. **Image Source** - Select **URL** radio button.
   b. **Enter Image URL** - Enter the appropriate URL address in the field using the following syntax for either NFS or HTTP, and then click **Upload File**.

      Note: The system supports only NFS and HTTP protocols.

      ```
      nfs://[hostname|IP_addr]/path
      http://[hostname|IP_addr]/path
      ```

      Enter either the name of the host (*hostname*) or the host IP address (*IP_addr*) and the path to the file. If you use a *hostname*, the cluster must be configured to point at a DNS server that can resolve

that name. For more information, see Configuring Name Servers for Prism Central in *Prism Central Admin Center Guide*.

> **Note:** A file uploaded through NFS must have 644 permissions.

c. Optionally, if the remote image location requires authentication credentials, enter the **Username** and **Password**, then click **Next**.

> **Note:** The authentication is validated after the image upload request is submitted.

d. Specify the following attributes for the image file:

- **Image Name** - Enter the image name. By default, the system pre-fills the name of the file you selected, however you can change the image name as per your requirement.

  > **Note:** Ensure that the name of the image is unique across all the images in Prism Central.

- **Image Type** - Select the type of image.
- **Image Description** - Enter the description for the image file.

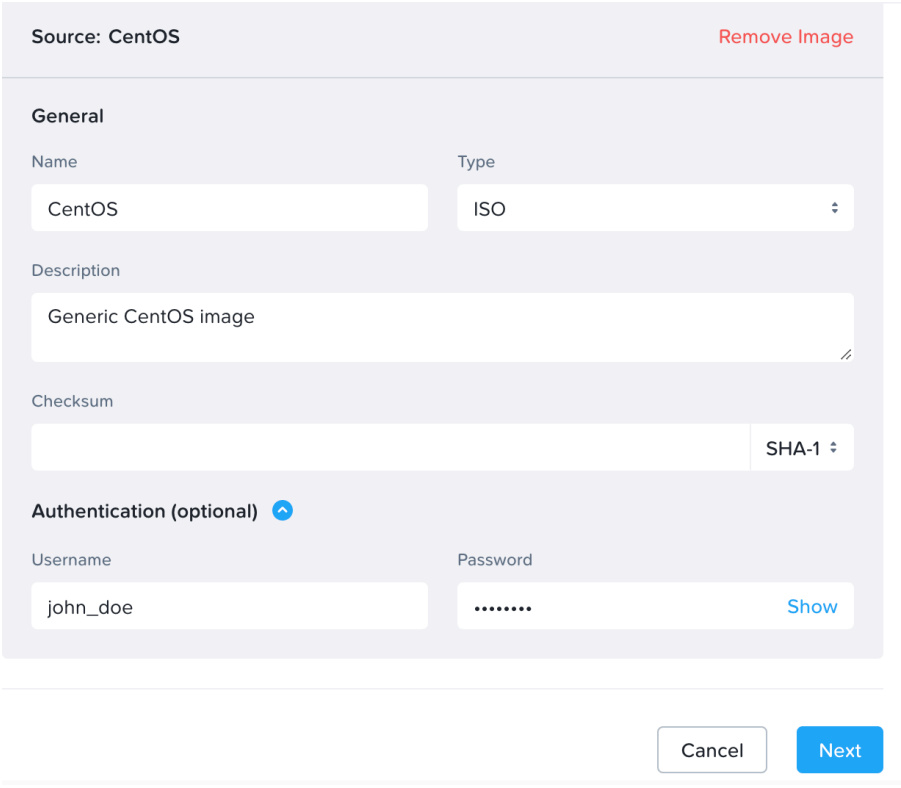


Figure 111: Add Image Attributes: URL

e. Repeat step b to step c if you want to add multiple image files.

To remove an image file entry, locate the entry and click **Remove**.

f. Click **Next** after you add all the image files.
The system displays the **Select Location** step.

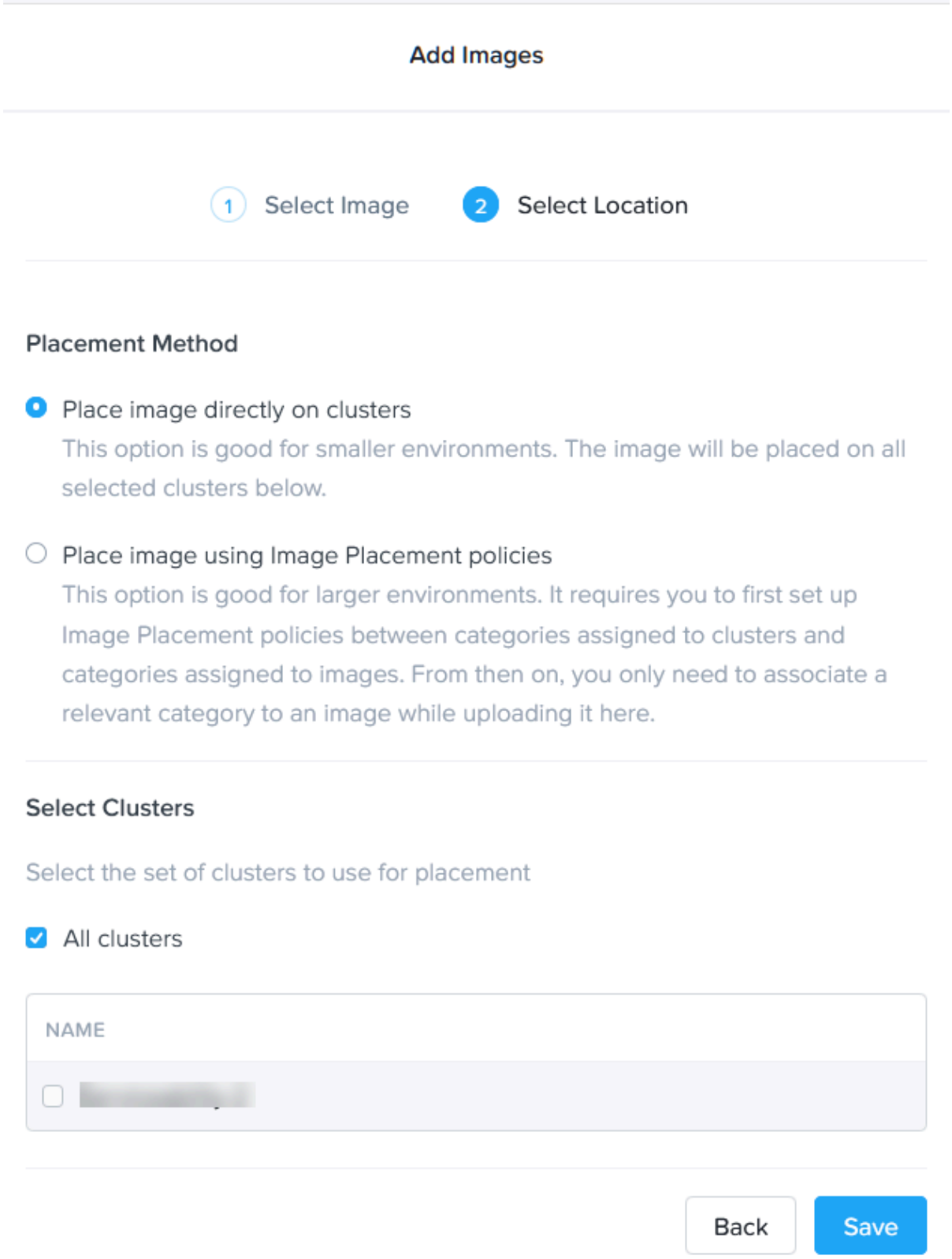


Figure 112: Add Images: Select Location

5. Specify the following information in the **Select Location** step:

   a. **Placement Method** - Select one of the following placement methods:.

   - **Place image directly on clusters**- Used to place the images directly o the selected clusters.
   - **Place image using Image Placement policies** - Used to delegate image placement decisions to configured policies and assign categories to the images

   b. If you select:

   - **Place image directly on clusters** - Specify the following information:

     Select Clusters - Select the clusters in which you want to add the image file in the **Name** column.

     Note:

     - By default, the system selects all the registered clusters.
     - If you want to add the images to all registered clusters, ensure that you select all the clusters in the **Name** column.
     - If you want to upload to only a subset of the registered clusters, clear all clusters in the **Name** column, and only select the clusters you want from the list.

   - **Place image using Image Placement policies** - Specify the following information:

     Select Image Categories - Click inside the search box and select the category you want from the list. You can also type the name of the category to reduce the list to matching names.

     Note:

     - To select multiple categories, click Add icon beside each category name that you want to include in the categories.
     - To remove a category, click Remove icon beside each category name that you want to remove from the selected categories.
     - For information about how to create a category and assign a category value to an image, see Creating a Category on page 457 and Associating Images with Categories on page 479.

6. Click **Save**.
   The system adds the image files in batches and takes some time to enforce the image placement policies.

   Note: You can also suspend or resume the image placement policies based on your requirement. For more information, see Suspending or Resuming Enforcement of an Image Placement Policy on page 258.

Adding Images from a VM Disk

This section describes how to add an image from a VM disk on the registered cluster..

About this task

Figure 113: Adding Images from a VM Disk

A video on this topic is available https://players.brightcove.net/5850956868001/xJM5EiUJJ_default/index.html?videoId=6271311948001 on Brightcove.

Before you begin

Ensure that the following prerequisites are met before you add an image from a VM disk.

- The source VM belongs to an AHV cluster.
- The source VM on which the disk resides is in the powered-off state.
- To place the image on clusters associated with relevant categories, you must first set up the image placement policies between categories assigned to clusters and categories assigned to images.

  For information about how to create a category and assign a category value to an image, see Creating a Category on page 457 and Associating Images with Categories on page 479.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default.

3. Click **Add Image**.
   The system displays the **Add Images** window.

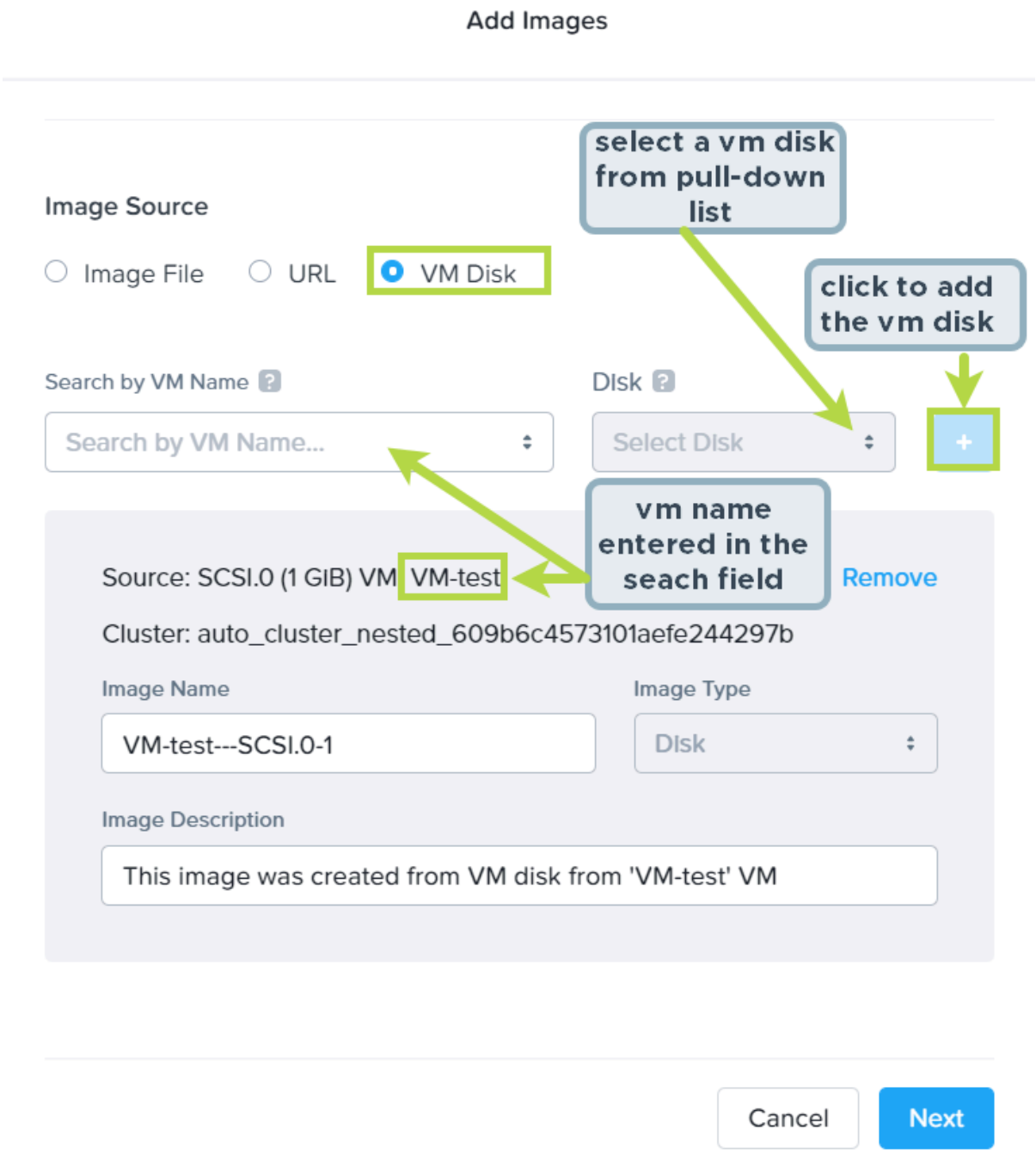


Figure 114: Add Images: VM Disk

4. Specify the following information in the **Select Image** step:

   a. **Image Source** - Select **VM Disk** radio button.

   b. **Search by VM Name** - Click inside this field text box, and select the target VM from the displayed list. The list displayed consists of all the powered-off VMs in the cluster.
   The system adds the VM to a list and populates the list of disks attached to this VM in the **Disks** dropdown list.

   c. Select the target disk from the **Disks** dropdown list, and click the Add icon,
   The system displays the disk, and cluster information of the VM source.

   d. Specify the following attributes for the image file:

      - **Image Name** - Enter the image name. By default, the system pre-fills the name of the file you selected, however you can change the image name as per your requirement.

        Note: Ensure that the name of the image is unique across all the images in Prism Central.

      - **Image Type** - Select the type of image.
      - **Image Description** - Enter the description for the image file.

   e. Repeat step b to step d if you want to add multiple image files.

      To remove an image file entry, locate the entry and click **Remove**.

   f. Click **Next** after you add all the image files.
      The system displays the **Select Location** step.

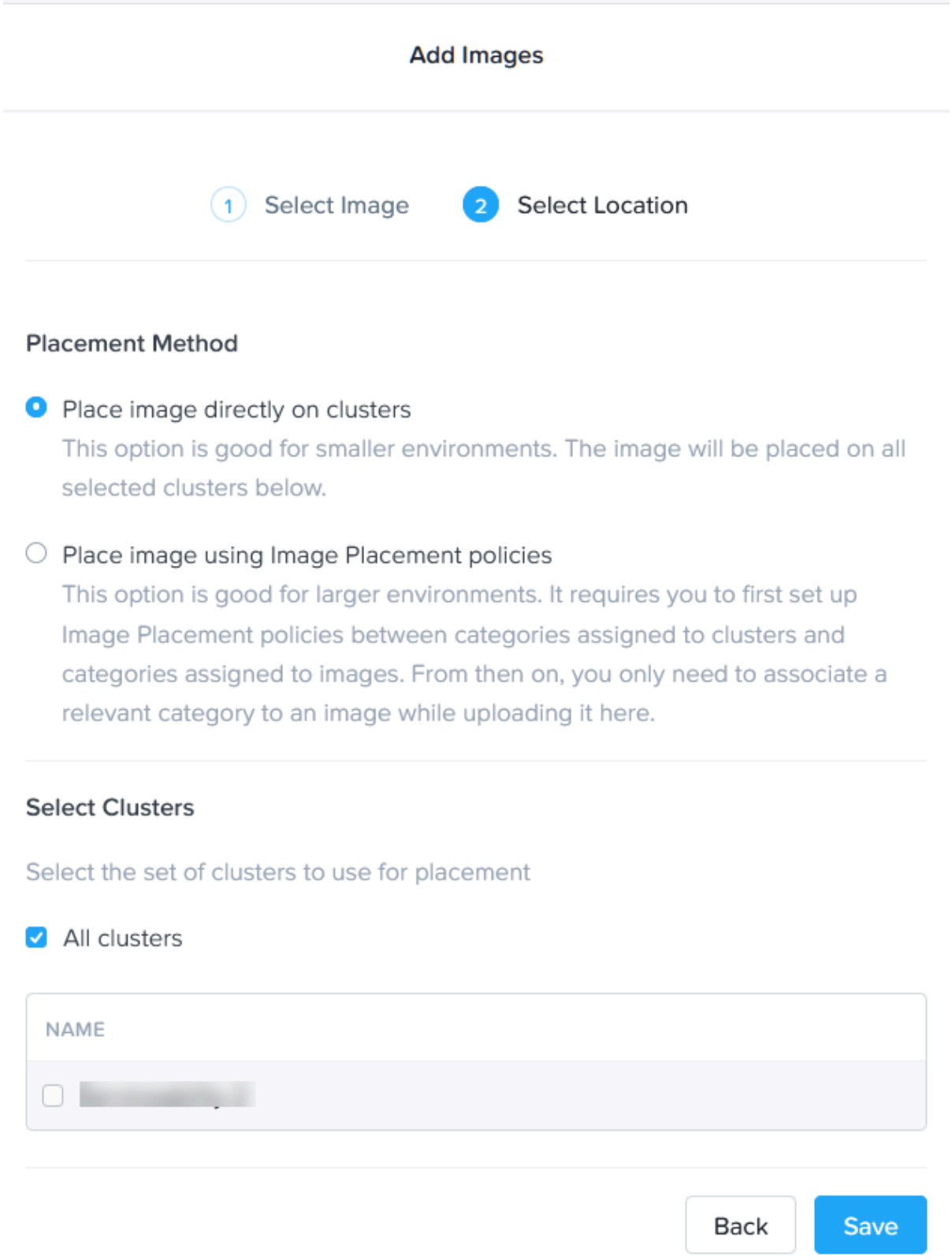


Figure 115: Add Images: Select Location

5. Specify the following information in the **Select Location** step:

   a. **Placement Method** - Select one of the following placement methods:

      - **Place image directly on clusters**- Used to place the images directly o the selected clusters.
      - **Place image using Image Placement policies** - Used to delegate image placement decisions to configured policies and assign categories to the images

   b. If you select:

      - **Place image directly on clusters** - Specify the following information:

        Select Clusters - Select the clusters in which you want to add the image file in the **Name** column.

        > **Note:**
        >
        > - By default, the system selects all the registered clusters.
        > - If you want to add the images to all registered clusters, ensure that you select all the clusters in the **Name** column.
        > - If you want to upload to only a subset of the registered clusters, clear all clusters in the **Name** column, and only select the clusters you want from the list.

      - **Place image using Image Placement policies** - Specify the following information:

        Select Image Categories - Click inside the search box and select the category you want from the list. You can also type the name of the category to reduce the list to matching names.

        > **Note:**
        >
        > - To select multiple categories, click Add icon beside each category name that you want to include in the categories.
        > - To remove a category, click Remove icon beside each category name that you want to remove from the selected categories.
        > - For information about how to create a category and assign a category value to an image, see Creating a Category on page 457 and Associating Images with Categories on page 479.

6. Click **Save**.
   The system adds the image files in batches and takes some time to enforce the image placement policies.

   > **Note:** You can also suspend or resume the image placement policies based on your requirement. For more information, see Suspending or Resuming Enforcement of an Image Placement Policy on page 258.

Suspending or Resuming Enforcement of an Image Placement Policy

This section describes how to suspend or resume the enforcement of an Image Placement Policy in Prism Central.

Before you begin

The minimum supported versions to suspend or resume the enforcement of an image placement policy in Prism Central are AOS 6.6 for Prism Element (with bundled AHV version) and PC 2022.9 for Prism Central.

About this task

Enforcement of placement policy involves copying images between clusters using image data transfer tasks that are typically long-running tasks and consume a considerable amount of network bandwidth. If you need to manage your local bandwidth and resources while the enforcement of the image placement policy is still going on, you can suspend the enforcement of the image placement policy, and can resume the enforcement at a later point of time.

To suspend or resume the enforcement of an image placement policy, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default.
3. Select **Placement Policies** in the **Policies** tab.

   The following is an example showing the placement policies view:

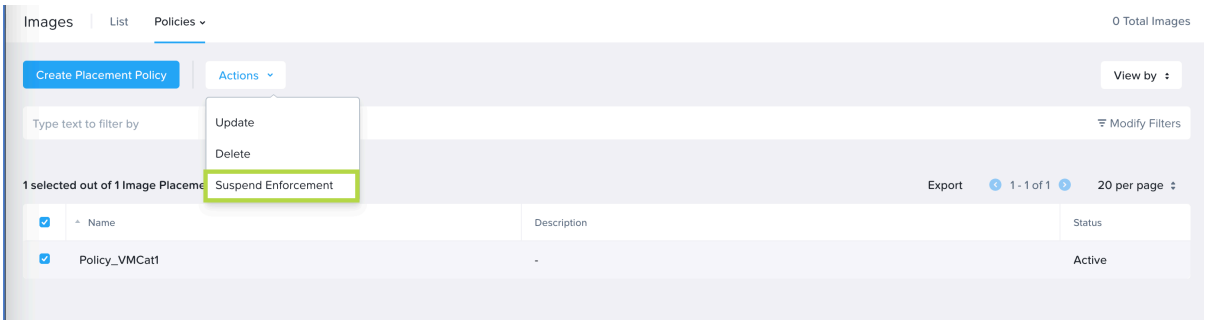


Figure 116: Placement Policy View

4. Select the target policy checkbox for which you want to suspend or resume enforcement, and choose **Suspend Enforcement** or **Resume Enforcement** from the **Actions** dropdown menu.
   The policy enforcement is suspended or resumed based on the selected action.

Image Upload Verification

This section describes how to verify whether an image upload to multiple clusters succeeded.

When you add an image and select multiple clusters for initial placement of the image using the **Place image directly on clusters**, the status message box shows that the task is successful. The status message displays the successful completion of the task even if the image is successfully uploaded to only one cluster. Nutanix recommends you to go to the **Tasks** page and check whether the Image upload and Image update subtasks succeeded for all the clusters that you selected. It is possible that the Image upload or update subtasks for some of the clusters are failed.

Nutanix recommends that you use **Place image using Image Placement policies** option when you add images to multiple clusters. Image Placement policy based placement ensures that images propagate successfully to multiple clusters in a single operation.

For information about Image Placement policy, see Image Placement Policies on page 476 section.

For information about how to place the image on the registered clusters using image placement policies, see Adding an Image on page 244 section.

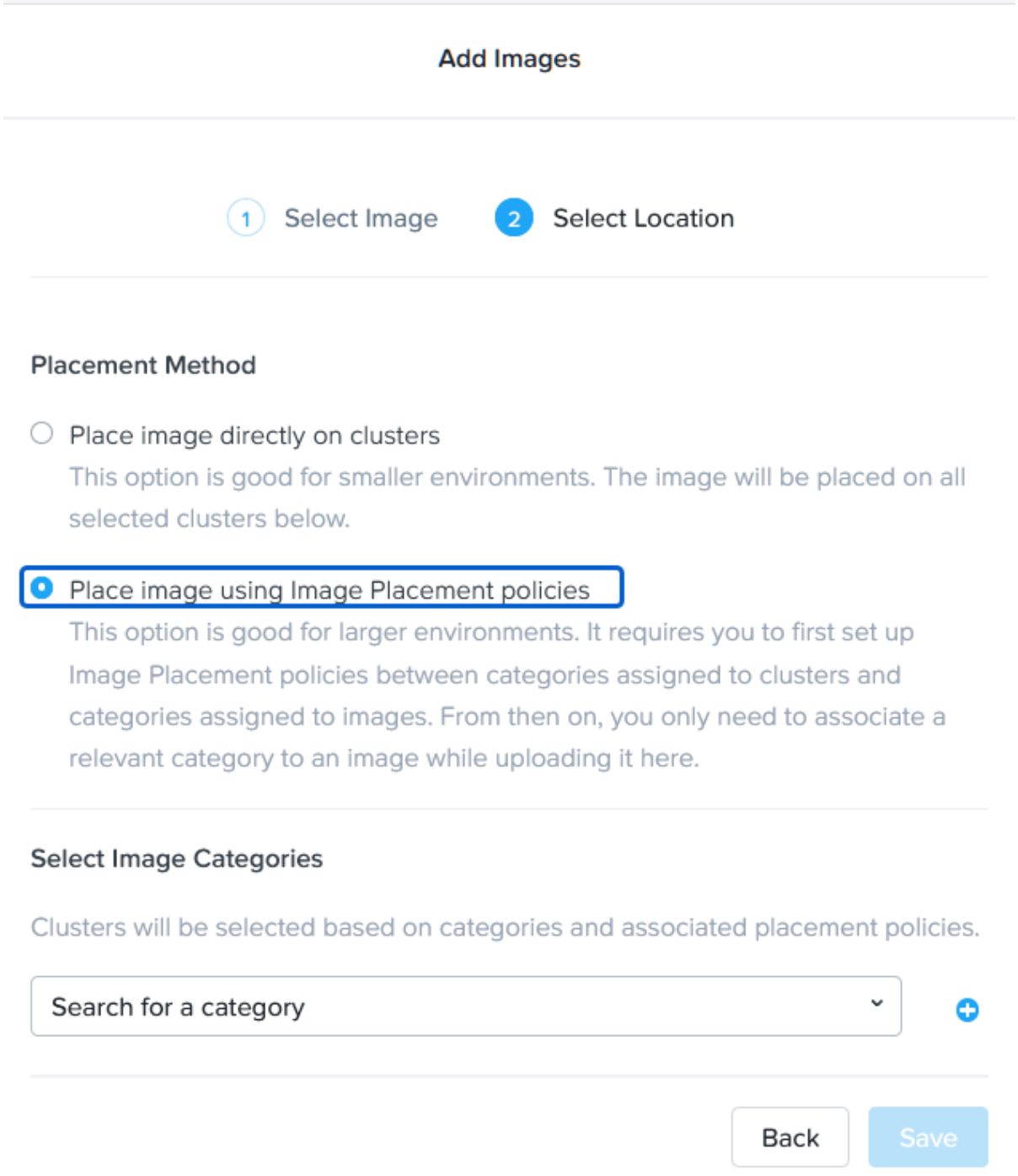


Figure 117: Image Placement Method selection for multiple clusters

Modifying an Image

This section describes how to modify images in Prism Central.

About this task

You can perform the following actions to modify the images in Prism Central:

- Update the image attributes.
- Delete the image
- Add image to Catalog.
- Manage image categories

To modify an image (delete, update, or add to catalog), perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default.
3. Select the target image checkbox, and choose any one of following actions from the **Actions** dropdown menu:
   - **Delete** to delete the image file.
   - **Update** to edit the image file.In the **Edit Image** window, update the image name, image description, or image type as desired, and click **Save**. For field details, see Adding an Image on page 244.
   - **Add Image to Catalog** to add an image to the catalog. For more information on how to add an image to the catalog, see Catalog Management on page 262.
   - **Manage Categories** to manage the image categories. In **Manage Categories** window, perform the following steps:
     1. Use the Add icon and Remove icon available under **Set Categories** field to add or remove the categories for the selected image.
     2. Click **Save**.

     For information about how to create an image category, see Creating a Category on page 457.

Importing Images to Prism Central

This section describes how to import images from registered clusters and manage the images centrally from Prism Central.

About this task

An image imported to Prism Central continues to reside on the cluster that owns it. Prism Central only creates and stores image metadata locally, and it uses that metadata when you perform an action on the image. After you import an image, the image remains visible on the cluster from which you imported it, however the system never allows you to update the image on the cluster. You can update the image only from Prism Central.

There is no impact on the following images when you import images in Prism Central:

- Any images that you choose not to import.
- Any images that you add subsequently to the cluster from its web console. These images remain editable on the cluster until you import them to Prism Central.

You can import the images in Prism Central using any of the following criteria in a single operation:

- All images from all registered clusters
- All images from a selection of clusters
- Selection of images from some of the clusters.

To import images from registered clusters, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default.
3. Click **Import Image**.
   The system displays the **Import Image** window.
4. In the **Import Images** window, select one of the following options:
   - » **All Images** - To import all images from all registered clusters.
   - » **Images On a Cluster** - To import all images from a selection of registered clusters.
   - » **Select Images** - To import specific images from a given cluster. Click the link provided for the cluster, select the images that you want to import, and click **Done**.

     Repeat this step for all the clusters from which you want to import the specific images.
5. Click **Save** to begin import.
   Prism Central imports the metadata of the selected images and marks the images as read-only entities on the clusters.

   The image continues to stay in the container that hosted the disk before importing the image.

Policies for Image Management

You can define the Image Placement and Bandwidth Throttling policies for managing images. For information about Image Placement and Bandwidth Throttling policies, see Image Policy Management on page 476.

Catalog Management

Prism Central provides a catalog service to store VM snapshots and images. A Prism Central or self-service administrator creates this catalog of objects for self-service users (who have permissions to create a VM) to use them to deploy VMs in a project.

Note:

- The catalog service is a self-service feature that appears in Prism Central only when Prism Self-Service is enabled. For information about Prism Self-Service, see Prism Self Service Setup on page 519.
- You can create a custom role and enable or disable the Marketplace Item permissions to manage the Catalog Item entity permissions. For example, if you select **No Access** permission for the Marketplace Item entity for the custom role, the user with the custom role cannot access the **Catalog Item** page. For information about how to create a custom role with

access to catalog items entity, see Creating A Custom Role information in the *AOS Security Guide*.

Catalog Items Summary View

To access the summary view of all the catalog items, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Catalog Items** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The system displays **Catalog Items** page that enables you to view the catalog items available for all the projects in the cluster.

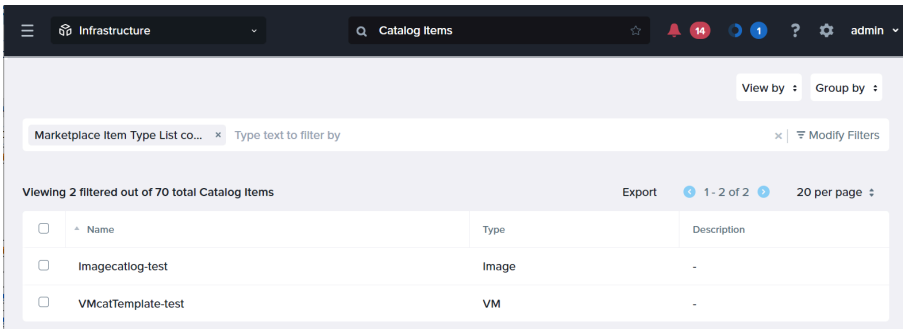


Figure 118: Catalog Items Page

The following table describes the fields that appear in the **Catalog Items** page. A dash (-) is displayed in a field when a value is not available or not applicable.

Table 45: Catalog Items Page - Field Description

Parameter	Description	Values
Name	Displays the catalog item name.	*<Catalog_Item_Name>*
Type	Displays the type of catalog item (Image or VM).	Image, VM
Description	Indicates the description for the catalog item	(description string)

Filters Pane - Catalog Items page

You can filter the information in the **Catalog Items** page based on the following fields that are available in the **Filter** pane. For information about how to use **Filters** option in Prism Central, see Prism Central GUI Organization on page 27.

Table 46: Filter Pane Field Description - Catalog Items page

Parameter	Description	Values
Name	Filters based on the catalog item name. It returns a list of catalog items that satisfy the name condition/ string.	*<Catalog_Item_Name>*

Parameter	Description	Values
Description	Filters based on the description. It returns a list of catalog items whose description field satisfy the condition/string.	(description string)
Type	Filters based on the item type. Select one or more checkbox for the catalog items of the required types.	VM, Image

Adding a Catalog Item

This section describes how to add a VM snapshot or Image as a catalog item in Prism Central.

About this task

You can add the following entities as catalog items:

- *VM* - When you add a VM as the catalog item, a VM snapshot is created. The VM snapshot is available to users across all the self-service projects in the cluster. Users who have the requisite permissions can create VMs from the snapshot.
- *Image* - When you add an image as the catalog item, the image is available to users across all the self-service projects in the cluster. Users who have the requisite permissions can create VMs from the image.

> **Note:** After you add a VM or Image as the catalog item, a copy of these entities (VM snapshot or image) is added to the catalog. There is no impact to the catalog items (VM snapshot or image) even if the VM or image is deleted in Prism Central.

To add a VM snapshot or image as the catalog item, perform the following steps:

> **Note:** Nutanix recommends to power off the VM before you add a VM snapshot to the catalog.

Procedure

1. Log in to Prism Central.
2. Perform any of the following actions based on the type of catalog item you want to add:
   - » *Image* - Navigate to the **Images** page. For information about how to access the **Images** page, see Images Summary View on page 239.
   - » *VM* - Navigate to the **List** tab of the **VMs** page. For information about how to access the VMs **List** tab, see VMs Summary View on page 95.

3. To add an image, perform the following actions:

   a. Select the target image checkbox, and choose **Add Image to Catalog** from the **Actions** dropdown menu.
   The system displays the **Add Image to Catalog** window.

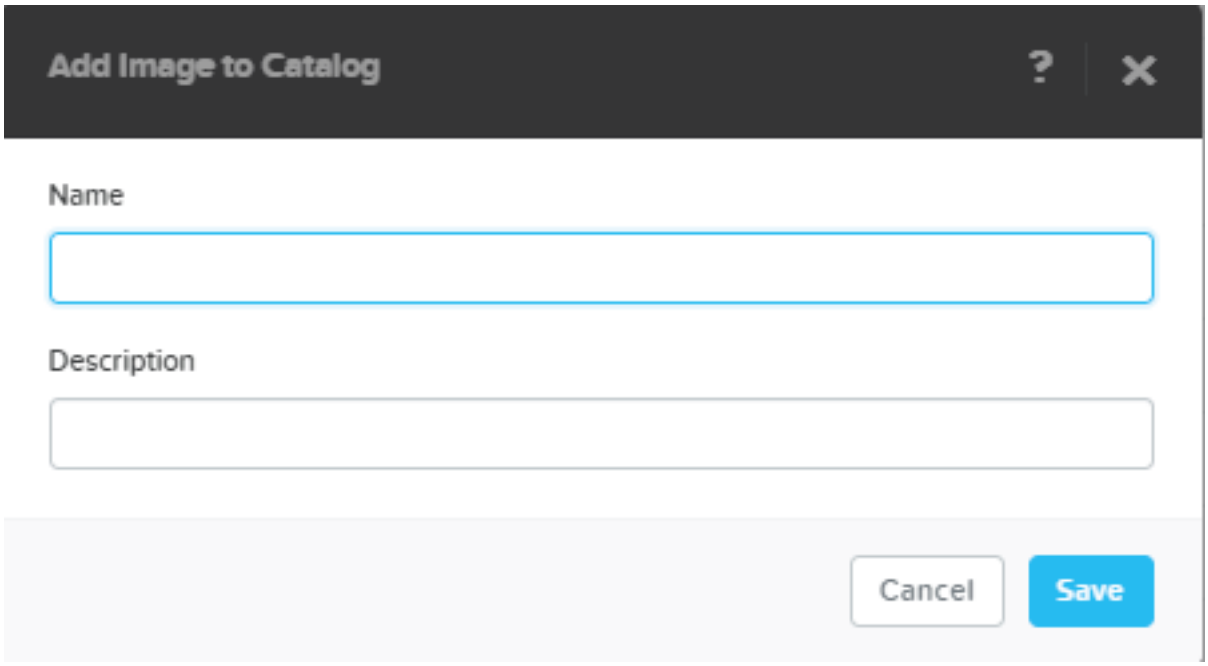


Figure 119: Add Image to Catalog Window

   b. Enter the following information in the **Add Image to Catalog** window:

      - **Name** - Enter a name for the image.
      - **Description** - Enter a description of the image.

   c. Click **Save**.
   The image is added as the catalog item.

4. To add a VM, perform the following actions:

   a. Select the target VM checkbox, and choose **Add to Catalog** from the **Actions** dropdown menu. The system displays the **Add VM to Catalog** window.

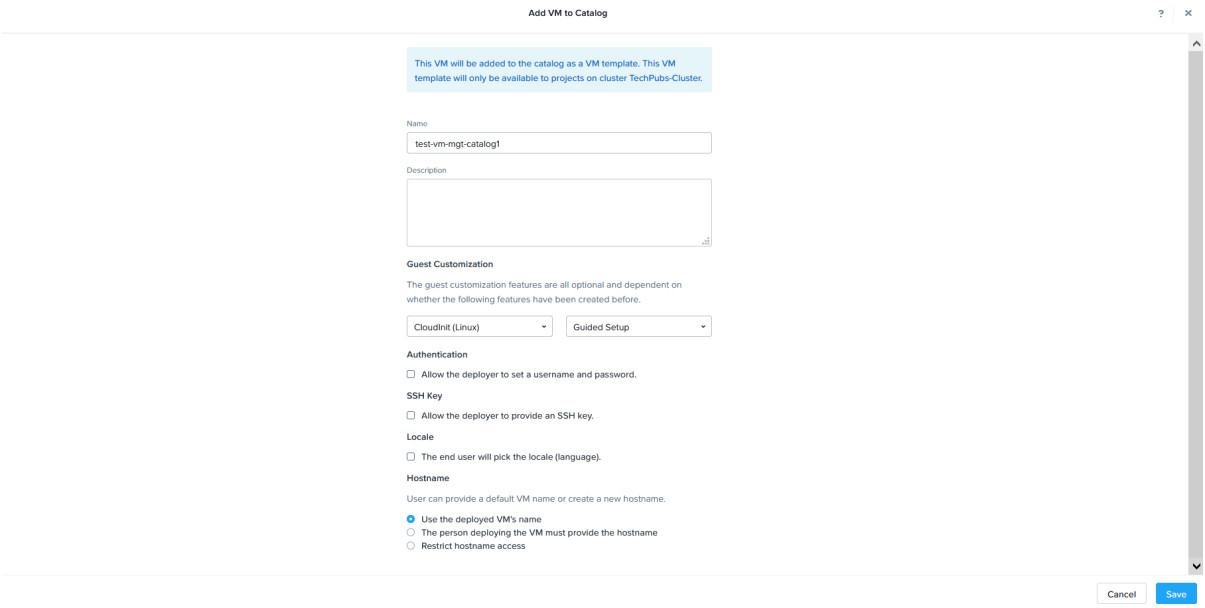


Figure 120: Add VM to Catalog Page

   b. Enter the following information in the **Add VM to Catalog** window:

      - **Name** - Enter a name for the VM.
      - **Description** (optional) - Enter a description of the VM.
      - **Guest Customization** - For the **Guest Customization** fields, select the following options for guest operating system (OS) for the VMs that you deploy using this VM template:.

        - In the **Script Type** field, select **Sysprep (Windows)** to customize the Windows OS, and **Cloud-init (Linux)** to customize the Linux OS.

          Note: If you select **No Customization** at the time of creating the template and allow the users to override the guest customization settings using **Allow users to override at VM**

Deployment? toggle field, it gives the maximum customization control to the users. In this case, the users can customize the script type and the configuration method.

- In the **Configuration Method** field, for each of these script types selected in **Script Type** field, select either upload a custom script or opt for a guided setup in the field.

Note:

- If you select **Custom Script**, you can either upload a script to customize the guest OS of the VMs, or you can copy-paste the script in the text box.
- If you select **Guided Setup** , enter the following information:
  - **Authentication**: Select the checkbox to allow the user who deploys the VM to set a username and password.
  - **SSH Key** [Cloudinit (Linux) only]: Select the checkbox to allow the user who deploys the VM to provide an SSH key.
  - **Locale**: Select the checkbox to allow the end user to specify the locale (language).
  - **Hostname**: Select the appropriate radio button to specify the host name source: the deployed VM name, a name provided by the person deploying the VM, or restricted hostname access.
  - **License Key**: Specify the license key source. Check the **Enter License Key** radio button and enter the key in the field to set the license key, check the **Allow end user to input License Key** radio button to let the user do it, or check the **No License Key** radio button to not require a license key.

    Important: The information that you enter is used to customize the OS of the VMs that are deployed using this template.

c. Click **Save**.
The VM snapshot is added as the catalog item.

Deleting a Catalog Item

This section describes how to delete a catalog item in Prism Central.

About this task

VM snapshots and images deleted from a catalog makes those items unavailable to project members.

To delete a VM snapshot or image from the catalog items, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Catalog Items** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57
The system displays **Catalog Items** page that enables you to view the catalog items available for all the projects across the registered clusters.
3. Select the target VM snapshot or Image catalog item, and click **Delete Catalog Item**.
The selected catalog item is deleted from all the projects in the cluster.

Storage Container Management

Storage Management (Prism Central)

Storage in a Nutanix cluster is organized into several components that allow you to manage capacity and performance. Nutanix clusters include storage pool, storage container, volume group, and virtual disk components. Prism Element allows you to manage all aspects of storage for a cluster, but you can also manage storage components directly from Prism Central.

A storage pool is created during cluster configuration. There is one storage pool per cluster. Storage efficiency features that include compression, deduplication, erasure coding, and replication factor are enabled at the storage container level.

The **Storage Containers** page displays information about all the storage containers across the registered clusters.

Note:

- A storage pool and three storage container are created automatically when the cluster is created.
- A storage container is created only if you have configured the Controller VMs (CVMs) with enough memory. The CVM allocation requirements differ depending on the models and features that are used at your site. For more information about the minimum CVM requirements, see Controller VM (CVM) Field Specifications information in *Acropolis Advanced Administration Guide*.
- The NutanixManagementShare, SelfServiceContainer, and a default-container are created by default.
  - The NutanixManagementShare storage container is a built-in storage container for Nutanix clusters for use with the Nutanix Files and Self-Service Portal (SSP) features. This storage container is used by Nutanix Files and SSP for file storage, feature upgrades, and other feature operations. The NutanixManagementShare storage container is not intended to be used as storage for vDisks, including Nutanix Volumes.
  - SelfServiceContainer is a built-in storage container within a Nutanix cluster that is used for storage by VMs created using Image service features such as Self-Service and OpenShift. SelfServiceContainer can also be used like any other container for regular VMs, volume groups, and images. General requirements for using container-level configurations such as compression, deduplication, erasure coding, and replication factor in SelfServiceContainer are the same as any other container.

    Important: To ensure proper operation of these features, do not delete these storage containers. Nutanix also recommends that you should not delete these storage containers even if you are not using these features.

- The **Summary** tab in the **Storage Containers** page displays information about storage containers across the registered clusters. For details, see Storage Containers Summary View on page 269.
- The **Summary** tab in the individual storage container page displays the detailed information about the selected storage container. For more information, see Storage Container Details View on page 275.
- For information about storage management tasks that are performed through Prism Element, see the Storage Management chapter in the *Prism Web Console Guide*.

You can perform the following actions to manage a storage container from Prism Central:

- Create and manage storage directly from Prism Central when the hypervisor is either ESXi, Hyper-V or AHV. For more information, see the following sections:
  - Creating a Storage Container on page 290
  - Modifying a Storage Container on page 296
  - Deleting a Storage Container on page 300
- Enable inline erasure coding. For more information, see Enabling Inline Erasure Coding on page 289

Storage Containers Summary View

The **Summary** tab in **Storage Containers** page provides the information about all the storage containers across the registered clusters.

To access the summary view of all storage containers, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Storage Containers** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
3. Click the **Summary** tab.

   The system displays **Summary** page for all storage containers.

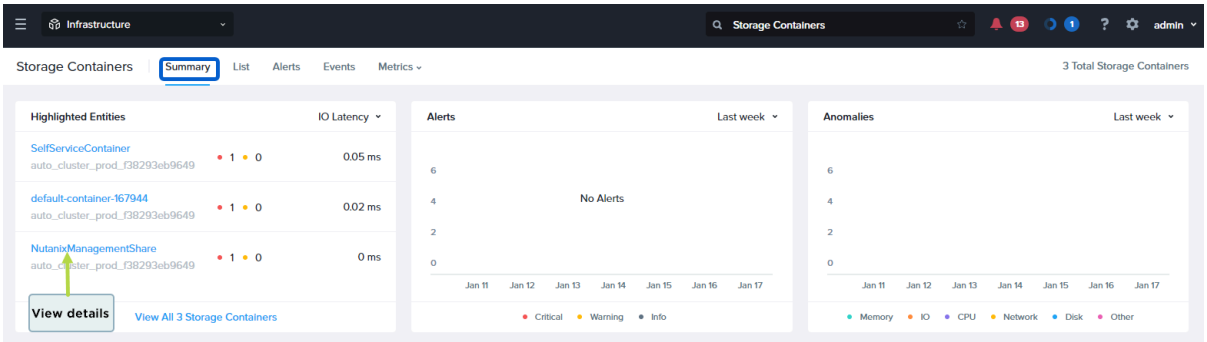


Figure 121: Summary Page - All Storage Containers

The **Storage Container** page includes five tabs on the left (**Summary**, **List**, **Alerts**, **Events**, and **Metrics**) with a display area below the selected tab.

The **Summary** tab of all storage containers displays the following widgets:

- **Highlighted Entities**: Displays a list of the storage containers with the highest usage of the *<parameter>* you select from the dropdown menu on the right of the widget. The *<parameter>* involves **IO Latency**, **IOPS**, and **Bandwidth**. Click **View All XX Storage Containers** link at the bottom to display the **List** tab.
- **Alerts**: Displays a list of alerts related to storage container that are generated during the specified *<interval>* you select from the dropdown menu on the right of the widget. The *<interval>* involves **Last week**(default), **Last 24 hours**, and **Last 1 hour**. When an alert appears, you can click the graph to view a list of those alerts. Click any alert to display the details page for that alert.
- **Anomalies**: Displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified *<interval>* you select from the dropdown menu on the right of the widget. The *<interval>* involves **Last week**(default), **Last 24 hours**, and **Last 1 hour**. When an anomaly appears, you can click the graph to view a list of those anomalies. Click any anomaly to display the event page for that anomaly.

Lists Tab

The **List** tab displays the list of storage containers across all clusters.

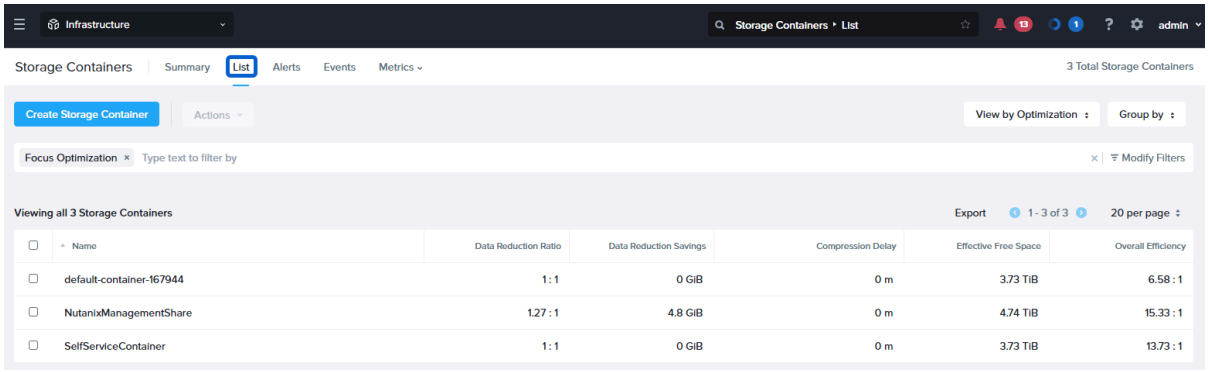


Figure 122: Storage Containers List Tab

The following table describes the fields that appear in the **List** tab of **Storage Containers** page:

> **Note:** The fields vary based on the **View by** and **Group by** options. A dash (-) is displayed in a field when a value is not available or applicable. For more information about **View by** and **Group by** options, see Prism Central GUI Organization on page 27.

Table 47: Storage Containers List Tab - Field Description

Field	Description	Values
Select **General** from **View by** option.		
Name	Displays the name of the storage container. You can click the storage container name to view the detailed information for that storage container. For information about storage container details view, see Storage Container Details View on page 275.	*<Storage _Container_Name>*
Physical Usage	Displays the amount of used physical storage space. A bar also appears that graphically indicates the amount of used and free storage space available in the storage container. When you hover the cursor over the bar, the system displays a window that lists the used space, free space, and total space in the storage container.	xxx [GiB|TiB]
Replication Factor	Displays the replication factor, which is the number of maintained data copies. The replication factor is specified when the storage container is created.	Integer
Compression	Displays whether compression is enabled.	[Off|On]

Field	Description	Values
Cache Deduplication	Displays whether "fingerprint on write" is enabled, which allows data duplication compression when data is read. Data duplication (commonly referred to as dedup) is a specialized data compression technique used to eliminate the duplicate copies of repeating data. If you set this parameter to **On**, the system applies deduplication compression to the data in both memory and solid state storage (SSD).	[None, On, Off]
Capacity Deduplication	Displays whether capacity deduplication is enabled, which allows data duplication compression on hard disks (HDD). Performance tier deduplication is a prerequisite for capacity deduplication.	[Off|On]
Erasure Coding	Displays whether erasure coding is enabled or not. For more information about Erasure Coding, see Erasure Coding on page 285.	[Off|On]
Cluster Name	Displays the name of the cluster in which the storage container resides. You can click the cluster name to view the detailed information for that cluster. For information about cluster details view, see Cluster Details View on page 405.	*<Cluster_Name>*
Select **Performance** from **View by** option.		
Name	Displays the name of the storage container. You can click the storage container name to view the detailed information for that storage container. For information about storage container details view, see Storage Container Details View on page 275.	*<Storage _Container_Name>*
Free Space (Physical)	Displays the amount of free physical space available in the storage container.	xxx [GiB|TiB]
Used Space (Physical)	Displays the amount of used physical space in the storage container.	xxx [GiB|TiB]
Total Space (Physical)	Displays the total amount of physical storage space in the storage container.	xxx [TiB]
IOPS	Displays the current I/O operations per second (IOPS) for the storage container. The controller IOPS, I/O bandwidth, and I/O latency fields record the I/O requests serviced by the Controller VM (CVM). The I/O can be served from memory, cache (SSD), or disk.	[0 - unlimited]
IO Bandwidth	Displays I/O bandwidth used per second for Controller VM-serviced requests in this storage container.	xxx [MBps|KBps]
IO Latency	Displays the average I/O latency for Controller VM-serviced requests in this storage container.	xxx [ms]
Select **Optimization** from **View by** option.		

Field	Description	Values
Name	Displays the name of the storage container. You can click the storage container name to view the detailed information for that storage container. For information about storage container details view, see Storage Container Details View on page 275.	*<Storage _Container_Name>*
Data Reduction Ratio	Displays the capacity optimization (as a ratio) that results from the combined effects of deduplication, compression, and erasure coding.	*xx*:1
Data Reduction Savings	Displays the amount of storage capacity saved from the combined effects of deduplication, compression, and erasure coding.	xxx [GiB|TiB]
Compression Delay	Displays the time delay to perform compression on the data.	xx [m]
Effective Free Space	Displays the amount of physical free space after data reduction.	xxx [GiB|TiB]
Overall Efficiency	Displays the capacity optimization (as a ratio) that results from the combined effects of data reduction (deduplication, compression, and erasure coding), cloning, and thin provisioning.	*xx*:1

You can perform the following actions for the storage containers in the **Lists** tab:

- Access the detailed information about an individual storage container. For more information, see Storage Container Details View on page 275.
- Filter the storage containers list based on available parameter values using **Filters** pane. For more information about **Filters** pane, see Filters Pane - Storage Containers Page on page 272.
- Export the table that contains the list of storage containers and their information to a file in a CSV format. For more information about **Export** option, see Export on page 32.
- Group the storage containers based on pre-defined criteria. For information about how to group the storage containers, see Group by on page 29.
- View storage containers based on pre-defined criteria or create a custom view. For information about available views and how to create a custom view, see View by on page 29.
- Create a storage container. For more information about how to create a storage container, see Creating a Storage Container on page 290.
- Perform the actions specific to storage container on a single or multiple storage containers using the **Actions** dropdown menu. For instructions on how to perform these actions, see Modifying a Storage Container on page 296 or Deleting a Storage Container on page 300.

> **Note:** The **Actions** dropdown menu is grayed out unless you select a storage container or if you select multiple storage containers.

Filters Pane - Storage Containers Page

The following table describes the fields available in the **Filters** pane:

Table 48: Filter Pane Fields

Parameter	Description	Values
Name	Filters based on the storage container name. Select a condition from the dropdown list and enter a string in the field. The system returns a list of storage containers that satisfy the storage container name condition/string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	(storage container name string)
Cluster Name	Filters based on the cluster name. Select a condition from the dropdown list and enter a string in the field. The system returns a list of storage containers that satisfy the cluster name condition/ string.	(cluster name string)
Cache Deduplication	Filters based on the cache deduplication setting. Select the checkbox(es) for the desired settings to return a list of storage containers with those settings. The number of storage containers currently in each setting are displayed in the **List** tab.	On, Off, None, Inline, Post Process
Replication Factor	Filters based on the replication factor. Select the checkbox(es) for the desired replication factor (1, 2, 3). Only existing RF values appear. For example, if all containers are at RF 2, just a single checkbox for RF 2 appears. The number of storage containers currently in each setting are displayed in the **List** tab.	1, 2, 3
Capacity Deduplication	Filters based on the capacity deduplication setting. Select the checkbox(es) for the desired settings to return a list of storage containers with those settings. The number of storage containers currently in each setting are displayed in the **List** tab.	On, Off, None, Inline, Post Process
Erasure Coding	Filters based on the erasure coding setting. Select the checkbox(es) for the desired settings to return a list of storage containers with those settings. The number of storage containers currently in each setting are displayed in the **List** tab.	On, Off
Free Space (Physical)	Filters based on the available storage space for a storage container. Select the checkbox(es) for the desired range or enter an amount range in the "**From <low> to <high> GiB|TiB**" field. It returns a list of storage containers with available capacity in that range.	([xx] to [yy] GiB |TiB range)

Parameter	Description	Values
Health	Filters based on the storage container health state. Select one or more states checkboxes to return a list of storage containers in those states. The number of storage containers currently in each state is displayed in the **List** tab.	Critical, Warning, Good
Used Space (Physical)	Filters based on the used storage space for a storage container. Select the checkbox(es) for the desired range or enter an amount range in the "**From <low> to <high> GiB|TiB**" field. It returns a list of storage containers with used storage in that range.	([xx] to [yy] GiB |TiB range)
Total Space (Physical)	Filters based on the total available capacity for a storage container. Select the checkbox(es) for the desired range or enter an amount range in the "**From <low> to <high> GiB|TiB**" field. It returns a list of storage containers with maximum capacity in that range.	([xx] to [yy] GiB|TiB range)
IOPS	Filters based on the current IOPS. Check the box for the desired range or enter a range in the "**From <low> to <high> iops**" field. It will return a list of storage containers with IOPS in that range.	([xx] to [yy] IOPS range)
IO Bandwidth	Filters based on the I/O bandwidth used. Check the box for the desired range or enter a range in the "**From <low> to <high> MBps**" field. It will return a list of storage containers with I/O bandwidth usage in that range.	([xx] to [yy] MBpS range)
IO Latency	Filters based on the average I/O latency. Check the box for the desired range or enter a range in the "**from <low> to <high> ms**" field. It returns a list of storage containers with average I/O latency in that range.	([xx] to [yy] ms range)

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options that are available on the **Activity** > **Alerts** page, however it only displays the alerts related to storage containers across the registered clusters. For more information about alerts, see *Prism Central Alerts and Events Reference Guide*.

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options that are available on the **Activity** > **Events** page, however it only displays the events related to storage containers across the registered clusters. For more information about events, see *Prism Central Alerts and Events Reference Guide*.

Metrics Tab

The **Metrics** tab allows you to view performance metrics across the storage containers. Click the **Metrics** tab to display dropdown menu of available metrics, and select the metric name to display the relevant performance information.

> **Note:** The **Metrics** dropdown menu is hypervisor-specific, and might vary based on the hypervisors used in the cluster.

The following is an example showing the dropdown menu of the **Metrics** tab:

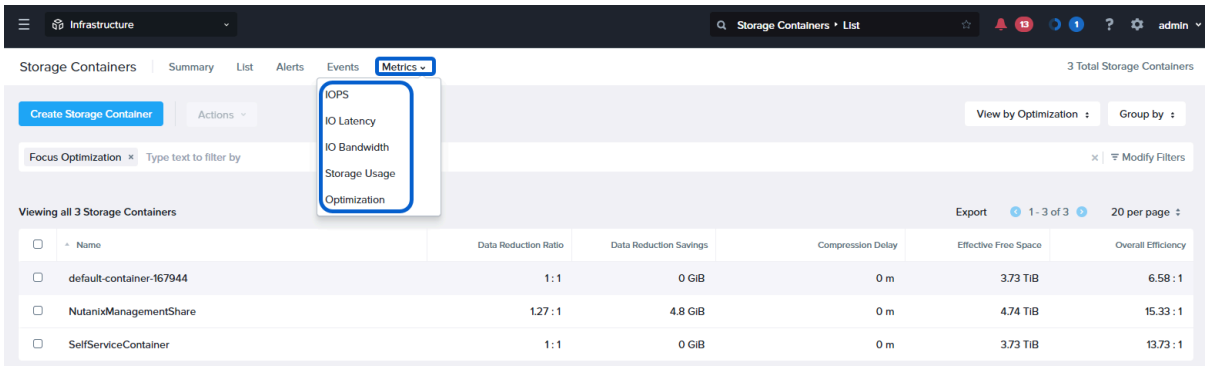


Figure 123: Storage Containers Metrics Tab

Table 49: Metrics Tab Fields

Metric	Description
IOPS	Displays total, read, and write IOPS graphs listing current values and total containers (number). The current values are split into intervals (for example, less than 700, 700-1400, 1400-2000, more than 2000). **Note:** The same format also applies to the other metrics in this table.
IO Latency	Displays total, read, and write I/O latency rate graphs.
IO Bandwidth	Displays total, read, and write I/O bandwidth rate graphs.
Storage Usage	Displays storage usage graph.
Optimization	Displays replication factor, data reduction ratio, and overall efficiency graphs.

Storage Container Details View

To access the details view of an individual storage container, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Storage Container** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   By default, the system displays the **List** tab with storage containers across all the registered clusters.
3. Click the target <*Storage_Container_Name*> to view the **Summary** tab of an individual storage container.

   > **Note:** Replace <*Storage_Container_Name*> with the actual storage container name at your site.

The following is an example showing the **Summary** tab of an individual storage container:

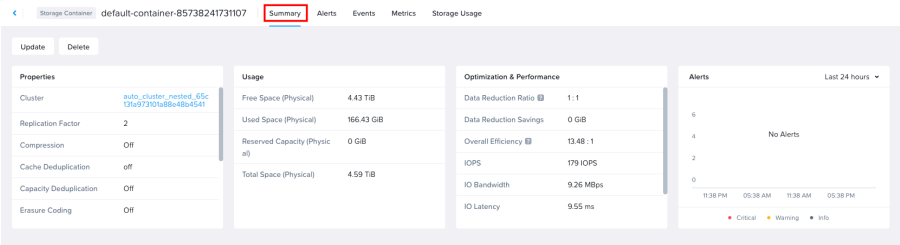


Figure 124: Summary Tab - Individual Storage Container

The **Summary** tab of an individual storage container provides the following widgets:

- **Properties** - Displays summary information about the storage container. For information about the fields available in **Properties** widget, see Storage Properties Widget - Parameter Details on page 111.
- **Alert**- Displays a list of related alerts that occurred during the specified interval. Select either **Last week** (default), **Last 1 hour** or **Last 24 hours** from the dropdown menu on the top right corner of the widget.
- **Anomalies** - Displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified interval. Select either **Last week** (default), **Last 1 hour** or **Last 24 hours** from the dropdown menu on the top right corner of the widget. When an anomaly appears, you can click the graph to display a list of those anomalies. If you click an individual anomaly, the system displays the event page for that anomaly.
- **Usage** - Displays usage data for the storage container. For information about the fields available in **Usage** widget, see Storage Properties Widget - Parameter Details on page 111.
- **Optimization & Performance** - Displays optimization and performance data for the storage container. For information about the fields available in **Optimization & Performance** widget, see Storage Properties Widget - Parameter Details on page 111.

<*Action*> available above the widgets. Click the appropriate <*Action*> to run that administrative action on the storage container. For more information about how to perform any <*Action*>, see Modifying a Storage Container on page 296 and Deleting a Storage Container on page 300.

Storage Container Widgets - Field Details

The following table describes the fields in the **Properties**, **Usage**, and **Optimization & Performance** widgets. A dash (-) in a field indicates that there is not enough data to evaluate or a value is not assigned. The displayed fields vary by hypervisor.

Table 50: Storage Container Widgets - Field Description

Field	Description	Values
Properties widget		
Cluster	Displays the name of the cluster in which the storage container resides. You can click the name to view the detailed information about the cluster. For more information, see Cluster Details View on page 405.	(cluster name)

Field	Description	Values
Replication Factor	Displays the replication factor, which is the number of maintained data copies. The replication factor is specified when the storage container is created.	[1-3]
Compression	Displays whether compression is enabled.	[Off|On]
Cache Deduplication	Displays whether "fingerprint on write" is enabled, which allows data duplication compression when data is read. Data duplication (commonly referred to as dedup) is a specialized data compression technique used to eliminate the duplicate copies of repeating data. If you set this parameter to **On**, the system applies deduplication compression to the data in both memory and solid state storage (SSD).	[None, On, Off]
Capacity Deduplication	Displays whether capacity deduplication is enabled, which allows data duplication compression on hard disks (HDD). Performance tier deduplication is a prerequisite for capacity deduplication.	[On, Off]
Erasure Coding	Displays whether erasure coding is enabled or not. For more information about Erasure Coding, see Erasure Coding on page 285.	[Off|On]
Filesystem allowlists	Displays the IP addresses for file systems that are allowed.	[IP addresses]
Compression Delay	Displays the delay (number of minutes) before data changes are compressed. A zero value indicates that compression is immediate (not delayed).	xx min
Thick Provision	Displays the reserved storage capacity for thick provisioned VMs.	xxx [GiB|TiB]
Effective Free Space	Displays the amount of logical free space after data reduction (logical free space x data reduction ratio).	xxx [GiB|TiB]
Usage widget		
Free Space (Physical)	Displays the amount of physical free space available in the storage container.	xxx [GiB|TiB]
Used Space (Physical)	Displays the amount of physical used space in the storage container.	xxx [GiB|TiB]
Reserved Capacity (Physical)	Displays the amount of physical reserved space in the storage container.	xxx [GiB|TiB]
Total Space (Physical)	Displays the amount of physical total space in the storage container.	xxx [GiB|TiB]
Optimization & Performance widget		
Data Reduction Ratio	Displays the capacity optimization (as a ratio) that results from the combined effects of deduplication, compression, and erasure coding.	*xx*:1

Field	Description	Values
Data Reduction Savings	Displays the amount of storage capacity saved from the combined effects of deduplication, compression, and erasure coding.	xxx [GiB|TiB]
Overall Efficiency	Displays the capacity optimization (as a ratio) that results from the combined effects of data reduction (deduplication, compression, and erasure coding), cloning, and thin provisioning.	*xx*:1
IOPS	Displays the current I/O operations per second (IOPS) for the storage container. The controller IOPS, I/O bandwidth, and I/O latency fields record the I/O requests serviced by the Controller VM (CVM). The I/O can be served from memory, cache (SSD), or disk.	[0 - unlimited]
IO Bandwidth	Displays I/O bandwidth used per second for Controller VM-serviced requests in this storage container.	xxx [MBps|KBps]
IO Latency	Displays the average I/O latency for Controller VM-serviced requests in this storage container.	xxx [ms]
Erasure Coding	Displays whether erasure coding is enabled or not. For more information about Erasure Coding, see Erasure Coding on page 285.	[Off|On]

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options as the Alerts dashboard, however it is filtered to display the alerts only for the selected storage container (individual storage container). For more information about alerts, see Prism Central Alerts and Events Reference Guide.

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options as the Events dashboard, except it is filtered to display just events for this storage container. For more information about events, see Prism Central Alerts and Events Reference Guide.

Metrics Tab

The **Metrics** tab allows you to view usage metrics for the storage container. Click the **Metrics** tab to view graphs for all the metrics. The graph is a rolling time interval performance or usage monitor. The baseline range appears as a blue band in the graph.

> **Note:** The baseline range and identified anomalies are based on sophisticated machine-learning capabilities. For more information, see Behavioral Learning Tools in *Intelligent Operations Guide*. The machine-learning algorithm uses 21 days of data to monitor and predict performance. A graph or baseline band may not appear if less than 21 days of data is available.

You can perform the following actions in the **Metrics** tab:

- Place the cursor anywhere on the horizontal axis to display the value at that time.
- Select the duration (time interval) from the dropdown list on the right (last 1 hour, last 24 hours, last week, last 21 days).

- From the **Actions** dropdown menu that appears on the top-right corner of each metrics widget, you can perform the following operations:
  - Select **Add to Analysis** to add the selected metric to **Analysis** dashboard. For more information, see Analysis Dashboard in *Intelligent Operation Guide*.
  - Choose **Select Analysis Session** to assign the metric to a target session.
- Click the **Filters** option to select one or more appropriate metric checkboxes to display the selected metrics in the **Metrics** page.

The following table describes the metrics available in **Metrics** tab:

> **Note:** Metrics are hypervisor-dependant, and might not be available on all hypervisors.

Table 51: Metrics Tab Fields

Metric	Description
Storage Controller IOPS	Displays the graph for total I/O operations per second (IOPS) for the storage controller.
Storage Controller Read IOPS	Displays the graphs for Read I/O operations per second (IOPS) for the storage controller.
Storage Controller Write IOPS	Displays the graph for Write I/O operations per second (IOPS) for the storage controller.
Storage Controller Latency	Displays the graph for total latency (in milliseconds) for storage controller
Storage Controller Read Latency	Displays the graph for read I/O latency (in milliseconds) for storage controller.
Storage Controller Write Latency	Displays the graph for write I/O latency (in milliseconds) for storage controller.
Storage Controller I/O Bandwidth	Displays the graph for total I/O bandwidth used per second (MBps or KBps) by storage controller.
Storage Controller Read I/O Bandwidth	Displays the graph of bandwidth used per second (MBps or KBps) for Read I/O operations by storage controller
Storage Controller Write I/O Bandwidth	Displays the graph of bandwidth used per second ((MBps or KBps) for Write I/O operations by storage controller.

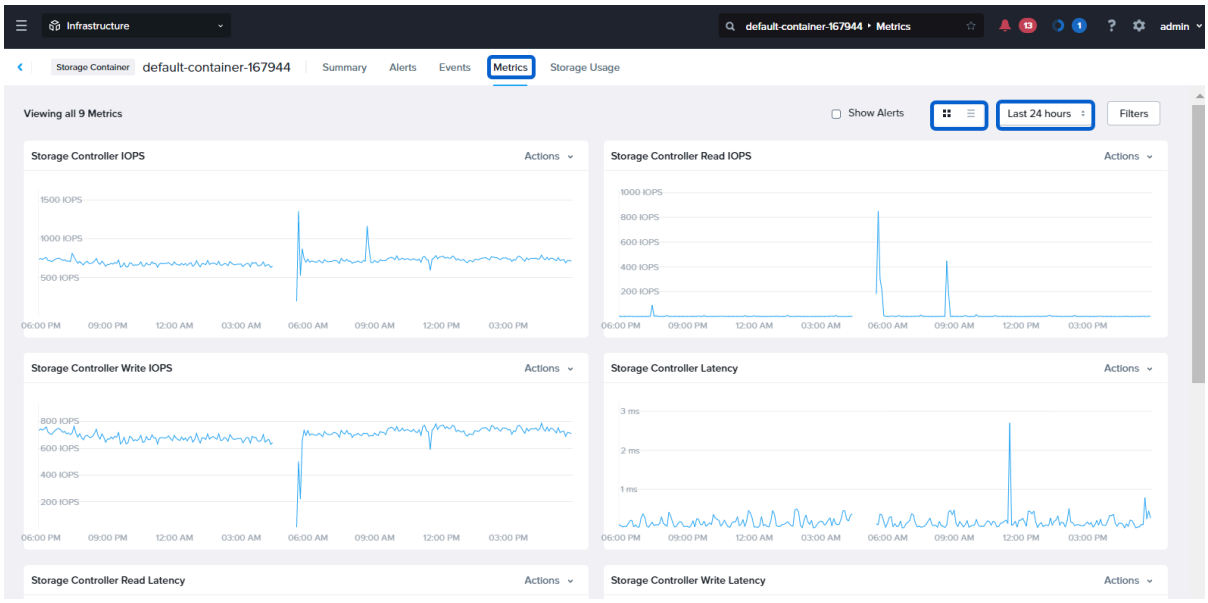


Figure 125: Metrics Tab

Storage Usage Tab

The **Storage Usage** tab displays the following graphs:

- **Usage Summary** graph - It displays a rolling time interval monitor of storage container storage usage that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in-depth analysis, you can add the monitor to the analysis page by clicking the blue link in the upper right of the graph.
- **Tier-wise Usage** graph - It displays a pie chart divided into the percentage of container storage space used by each disk tier (SSD and DAS-SATA).

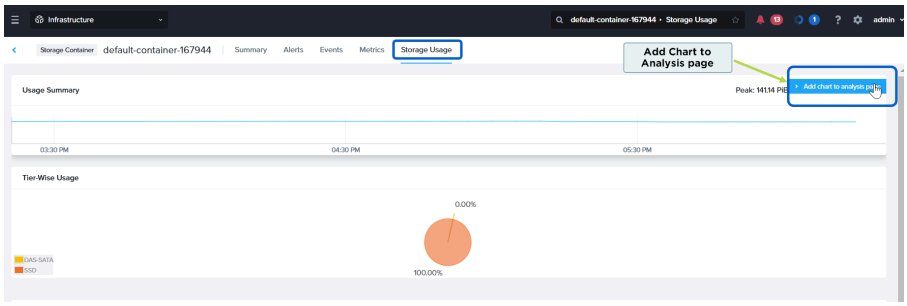


Figure 126: Storage Container Usage Tab

Storage Components

Storage in a Nutanix cluster is organized into the following components.

Storage Tiers

Each type of storage hardware (SSD-PCIe (NVMe), SSD (SATA SSD), and HDD) is placed in a storage tier. You can determine the tier breakdown for disks in a storage pool through the web console . For more information, see Storage Table View information in *Prism Element Web Console Guide*.

Storage Pools

Storage pools are groups of physical disks from one or more tiers. Storage pools provide physical separation because a storage device can only be assigned to a single storage pool at a time. Nutanix recommends creating a single storage pool for each cluster. This configuration allows the cluster to dynamically optimize capacity and performance. Isolating disks into separate storage pools provides physical separation, but can create an imbalance of these resources if the disks are not actively used. When you expand your cluster by adding new nodes, the new disks can also be added to the existing storage pool. This scale-out architecture allows you to build a cluster that grows with your needs.

When you create a cluster, a default predefined storage pool is available. This pool includes the total capacity of all the disks on all the hosts in the cluster.

Storage Containers

A storage container is a subset of available storage within a storage pool. Storage containers are created within a storage pool to hold virtual disks (vDisks) used by virtual machines. For more information, see Creating a Storage Container. By default, storage is thinly provisioned, which means that the physical storage is allocated to the storage container as needed when data is written, rather than allocating the predefined capacity when the storage container is created. Storage efficiency features such as compression, deduplication, and erasure coding are enabled at the container level.

The NutanixManagementShare storage container is a built-in storage container for Nutanix clusters for use with the Nutanix Files and Self-Service Portal (SSP) features. This storage container is used by Nutanix Files and SSP for file storage, feature upgrades, and other feature operations. To ensure proper operation of these features, do not delete this storage container. Nutanix also recommends that you do not delete this storage container even if you are not using these features. The NutanixManagementShare storage container is not intended to be used as storage for vDisks, including Nutanix Volumes.

SelfServiceContainer is a built-in storage container within a Nutanix cluster that is used for storage by VMs created using Image service features such as Self-Service and OpenShift. SelfServiceContainer can also be used like any other container for regular VMs, volume groups, and images. General requirements for using container-level configurations such as compression, deduplication, erasure coding, and replication factor in SelfServiceContainer are the same as any other container.

Volume Groups

A volume group is a collection of logically related virtual disks (or volumes). A volume group is attached to VM either directly or using iSCSI. You can add vDisks to a volume group, attach them to one or more consumers, include them in disaster recovery policies, and perform other management tasks. You can also detach a volume group from one VM and attach it to another, possibly at a remote location to which the volume group is replicated.

You manage a volume group as a single unit. When a volume group is attached to a VM, the VM can access all of the vDisks in the volume group. You can add, remove, and resize the vDisks in a volume group at any time.

Each volume group is identified by a UUID, a name, and an iSCSI target name. Each disk in the volume group also has a UUID and a SCSI index that specifies ordering within the volume group. A volume group can be configured for either exclusive or shared access.

You can backup, protect, restore, and migrate volume groups. You can include volume groups in protection domains configured for asynchronous data replication (Async DR), either exclusively or with VMs. However, volume groups cannot be included in a protection domain configured for metro availability, in a protected vStore, or in a consistency group for which application consistent snapshots are enabled.

vDisks

A vDisk is created within a storage container or volume group to provide storage to the virtual machines. A vDisk shows up as a SCSI device when it is mapped to a VM.

Containers for VMware and Hyper-V (Datastores/SMB Shares)

In vSphere, a datastore is a logical container for files necessary for VM operations. Nutanix provides the choice by supporting both iSCSI and NFS protocols when mounting a storage volume as a datastore within vSphere. NFS has many performance and scalability advantages over iSCSI, and it is the recommended datastore type.

In Hyper-V environments, storage containers are mounted as an SMB share.

> **Note:** Using a Nutanix storage container as a general-purpose NFS or SMB share is not recommended. For NFS and SMB file service, use Nutanix Files.

NFS Datastores. The Distributed Storage Fabric (DSF) reduces unnecessary network chatter by localizing the data path of guest VM traffic to its host. This boosts performance by eliminating unnecessary hops between remote storage devices that is common with the pairing of iSCSI and VMFS. To enable vMotion and related vSphere features (when using ESX as the hypervisor), each host in the cluster must mount an NFS volume using the same datastore name. The Nutanix web console and nCLI both have a function to create an NFS datastore on multiple hosts in a Nutanix cluster.

To correctly map the local ESX datastore to the Nutanix container:

- Map the NFS share with 192.168.5.2 (internal IP address) and not the Controller VM IP address or cluster virtual IP address.
- The name of the datastore should be same as the name of the container.

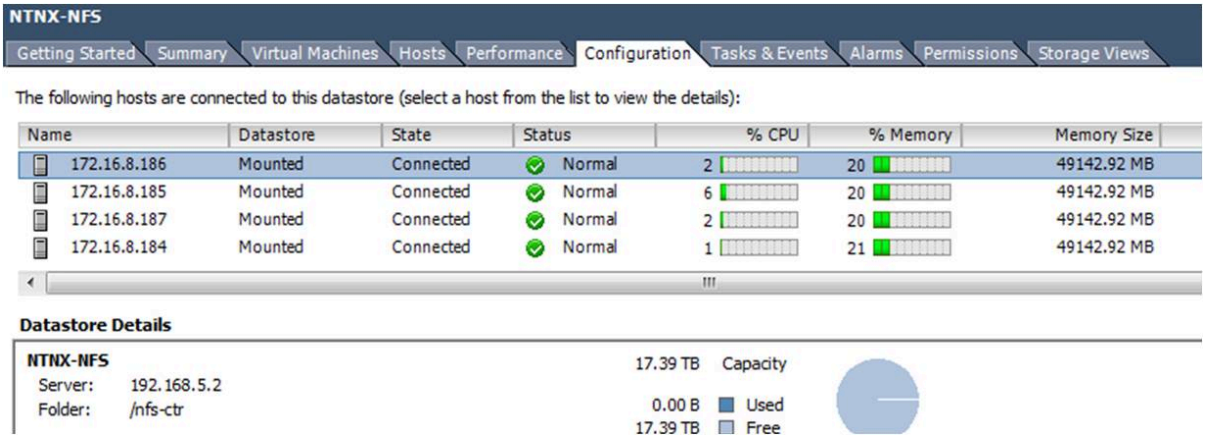


Figure 127: vSphere Configuration of NFS Datastore

SMB Library Share. The Nutanix SMB share implementation is the Hyper-V equivalent of an NFS Datastore with feature and performance parity with a vSphere configuration. The registration of a Nutanix storage container as an SMB Library share can be accomplished through a single powershell script, or through the Virtual Machine Manager GUI.

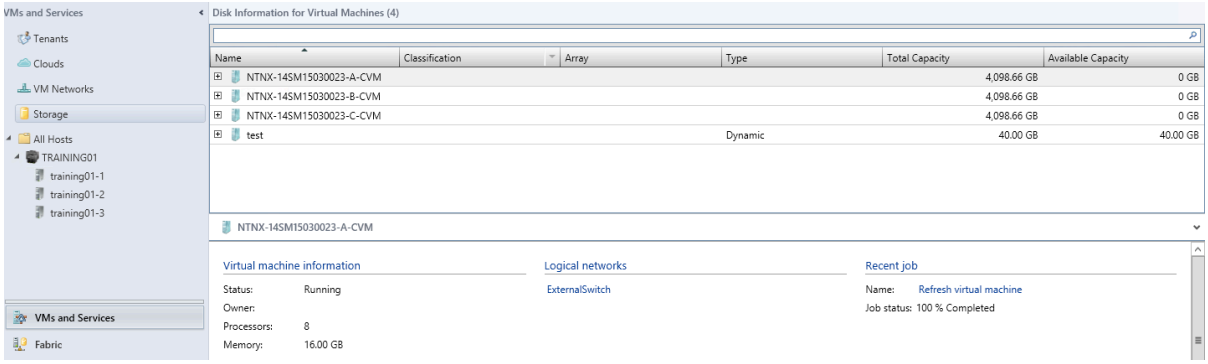


Figure 128: Hyper-V Configuration of an SMB Share

Compression

You can enable compression on a storage container. Compression can save physical storage space and improve I/O bandwidth and memory usage—which may have a positive impact on overall system performance.

> **Note:** If the metadata usage is high, compression is automatically disabled. If compression is automatically disabled, an alert is generated.

The following types of compression are available:

Post-process compression

Data is compressed after it is written. The delay time between write and compression is configurable, and Nutanix recommends a delay of 60 minutes.

Inline compression

Data is compressed as it is written. When you create a new storage container, inline compression is enabled by default for all license tiers. It is set to a delay of 0, compressing data immediately as it is written.

Data Reduction Ratios and Data Reduction Savings

You can view data reduction ratios and data reduction savings in Prism Central for any of the following entities:

- *For the entire cluster*

  Navigate to **Summary** tab in the **Clusters** page, and observe the **Data Reduction**column entry for the target cluster in **Storage Usage** widget. For information about how to access the **Clusters** page, see Clusters Summary View.

  > **Note:** The **Data Reduction Savings** for the entire cluster is visible only in the **Storage** dashboard in Prism Element. For more information, see Storage Overview View information in *Prism Element Web Console Guide*.

- *For an individual Storage Container*

  Navigate to the **Summary** tab of an individual storage container, and observe the **Data Reduction Ratio** and **Data Reduction Savings** fields in **Optimization & Performance** widget. For information about how to navigate to the **Summary** tab of an individual storage container, see Storage Container Details View.

Deduplication

Deduplication reduces space usage by consolidating duplicate data blocks on Nutanix storage. You can enable either cache deduplication only or both cache and capacity deduplication on a storage container.

Important:

- Deduplication is only supported on clusters with a minimum of three nodes.
- If deduplication enabled on storage containers having protected VMs, the system lowers the replication speed.
- Turning deduplication on for VAAI clone or linked clone environments is not recommended.

Cache Deduplication

You can enable cache deduplication of read cache to optimize performance. Cache deduplication means deduplication performed on the data in memory.

Note: Cache deduplication is not enabled by default.

Important: Nutanix recommends that you configure the Controller VMs with at least 24 GiB of RAM for Cache Deduplication.

Capacity Deduplication

You can enable capacity deduplication of persistent data to reduce storage usage. Capacity deduplication means deduplication performed on the data in hard disk storage (HDD).

Note:

- Capacity deduplication is not enabled by default. You can enable capacity deduplication only if cache deduplication is enabled.
- Capacity deduplication is available if you have purchased a Nutanix Cloud Infrastructure (NCI) Starter or higher license.

Important: Nutanix recommends that you configure the Controller VMs with at least 32 GiB of RAM and 300 GiB SSDs for the metadata disk for Capacity Deduplication.

How to enable Deduplication

Deduplication is enabled at the storage container level in Prism Central. For information about how to enable deduplication, see Creating a Storage Container (AHV) for AHV, Creating a Storage Container (ESXi) for ESXi or Creating a Storage Container (Hyper-V) for Hyper-V.

Deduplication Best Practices

The following table provides the scenarios where deduplication is recommended and where it is not recommended:

Enable deduplication	Do not enable deduplication
• Full clones • Physical-to-virtual (P2V) migration • Persistent desktops	• *Linked clones or Nutanix VAAI clones*: Duplicate data is managed efficiently by DSF so deduplication has no additional benefit • *Server workloads*: Redundant data is minimal so may not see significant benefit from deduplication

Erasure Coding

Erasure coding increases the usable capacity on a cluster. Instead of replicating data, erasure coding uses a parity information to rebuild data in the event of a disk failure. The capacity savings of erasure coding is in addition to deduplication and compression savings.

> **Important:** Erasure coding is supported on clusters with a minimum of 4 nodes when using RF2 and a minimum of 6 nodes when using RF3.

If you have configured redundancy factor 2, two data copies are maintained. For example, consider a 6-node cluster with 4 data blocks (a b c d). In this example, we start with 4 data blocks (a b c d) configured with redundancy factor 2.

The white text represents the data blocks and the green text represents the copies.

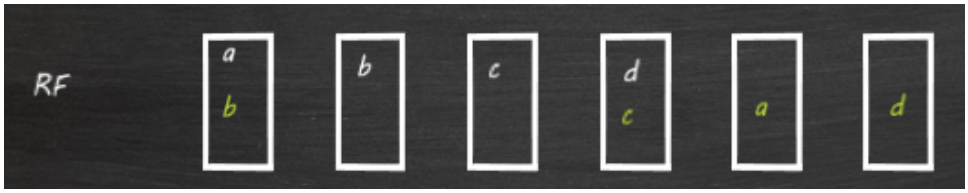


Figure 129: Data copies before Erasure Coding

When the data becomes cold, the erasure code engine performs an exclusive OR operation to compute parity “P” for the data.



Figure 130: During Computing Parity

After parity is computed, the data block copies are removed and replaced with the parity information. Redundancy through parity results in data reduction because the total data on the system is now a+b+c+d +P instead of 2 × (a+b+c+d).

> **Note:** Each block in the stripe is placed on a separate node to protect from a single node failure.

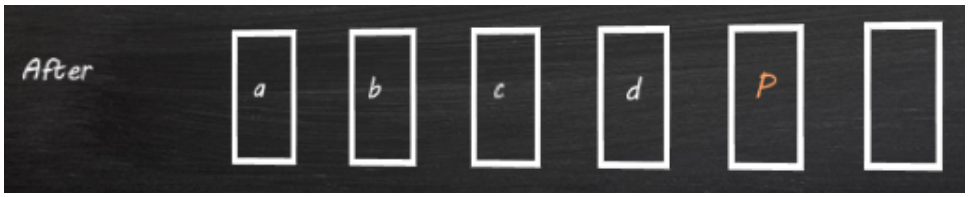


Figure 131: After Computation of Parity

If the node that contains data block c fails, block c is rebuilt using the rest of the erasure coded stripe (a b d and P) as displayed in the following example:

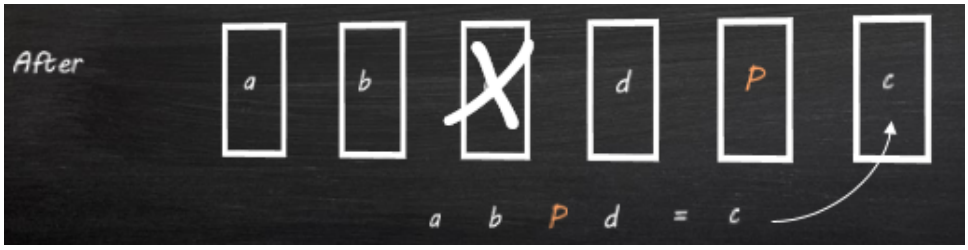


Figure 132: Post Node Failure

Block c is then placed on a node that does not have any other members of this erasure coded stripe.

> **Note:** When the cluster is configured for the redundancy factor 3, two parity blocks are maintained so that the erasure coded data has the same resiliency as the replicated data. An erasure coded stripe with two parity blocks can handle the failure of two nodes.

Example of Data Reduction Savings from Erasure Coding

The space savings from the erasure coding depends on the cluster size, redundancy setting, and percentage of cold data.

You can view the data reduction savings from Erasure coding using any of the following methods:

- Access the Storage Container Details View, and observe the following fields:
  - **Erasure Coding** value as *On* in the **Properties** widget.
  - **Data Reduction Savings** in the **Optimization & Performance** widget.
- Access the Storage Containers Summary View, and observe the **Data Reduction Savings** column for the target storage container using any of the following methods:
  - Click the **Lists** tab, and filter the storage containers based on the **Erasure Coding** value as *On*. The system displays the results in the **Lists** page.

    For information about how to use filters, see Filters Pane.
  - Select **Optimization** from the **View by** option and **Erasure Coding** from the **Group by** option. The system displays the results in the **Lists** page with **Erasure Coding: Off** and **Erasure Coding: On**.

In a 6-node cluster configured with RF2, erasure coding uses a stripe size of 5 where 4 nodes are for data and 1 node is for parity. The sixth node in the cluster ensures that if a node fails, another node is available for rebuild. With a stripe of 4 data to 1 parity, the and percentage of cold data. You can view the erasure coding usage savings from the storage container summary.

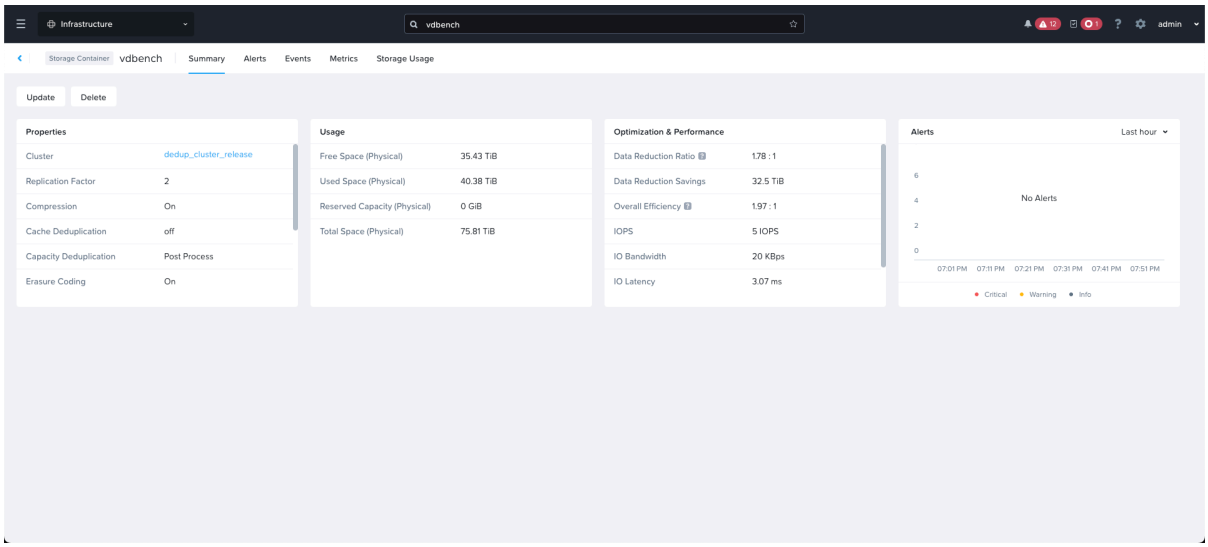


Figure 133: Storage Container Summary: Usage Savings Screen

Erasure coding stripe size adapts to the size of the cluster starting with the minimum 4 nodes with a maximum of 5 node stripe width. The following is an example displaying the various configurations of cluster size, possible stripe widths, and approximate savings that might occur when erasure coding is enabled.

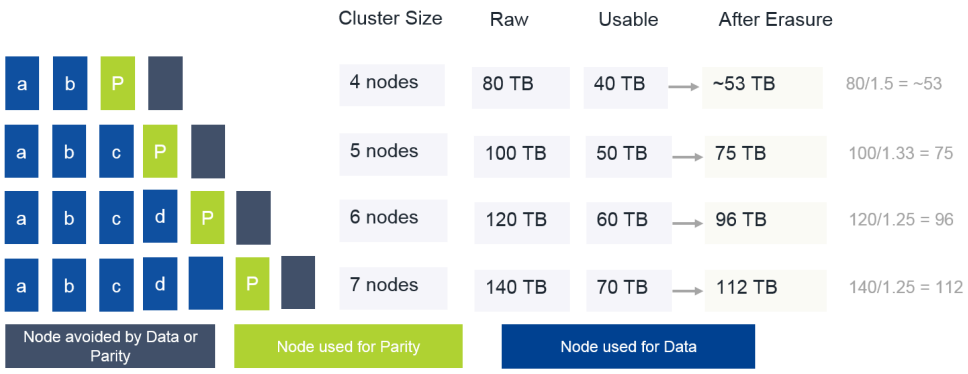


Figure 134: Example of Space Saving from Erasure Coding on 20 TiB Nodes

Erasure Coding Best Practices and Requirements

Nutanix recommends the following best practices and requirements to implement Erasure Coding:

- A cluster must have at least four nodes/blocks/racks to enable erasure coding. The cluster can have all four flash nodes or a combination of flash and hybrid nodes, or all hybrid nodes. If erasure coding is enabled on a storage container, a minimum of four blocks for RF2 or six blocks for RF3 is required to maintain block awareness.
- The following table provides the information about the recommended minimum configuration for multiple node removal operations:

Table 52: Minimum Recommended Configuration for Erasure Coding

Desired Awareness Type	FT Level	Min. Units	Simultaneous Failure Tolerance
Node	1	4 nodes	1 node
Node	2	6 nodes	2 nodes
Block	1	4 blocks	1 block
Block	2	6 blocks	2 blocks
Rack	1	4 racks	1 rack
Rack	2	6 racks	2 racks

> **Note:** Ensure that you maintain a cluster size that is at least one node greater than the combined strip size (data + parity) to allow space to rebuild the strips if a node fails.

- AOS dynamically calculates the erasure coding strip sizes depending on the number of nodes, blocks, and racks. The maximum supported and recommended strip sizes are (4,1) or (4,2) depending on the nodes, blocks, and racks. Nutanix recommends that you to not change the strip size. Greater strip sizes increases the space savings, however, it increases the cost of rebuild.
- Erasure coding effectiveness (data reduction savings) might reduce on workloads that have many overwrites outside of the erasure coding window. The default value for erasure coding window is seven days for write cold.
- Read performance is affected during rebuild and the amount depends on cluster strip size and read load on the system.
- Erasure coding is an asynchronous process, and hence the time taken to calculate and display space savings depends on the type and coldness of data. A minimum of two full curator scans are required to calculate the data savings.
- Ensure that you have RF+1 storage heavy or storage only nodes for all-flash clusters with storage heavy nodes. For example, if you have a four-node RF2 cluster, then you must add a minimum of three storage heavy nodes for optimum performance.

Inline Erasure Coding

Inline erasure coding creates erasure coding strips by erasure coding data without waiting for the data to become write cold.

There are two types of inline erasure coding:

- *Same vDisk strips*: Strips that are created using the data blocks from the same vDisk. Nutanix recommends that you configure inline erasure coding type as same vDisk strips for workloads that do not require data locality.
- *Cross vDisk strips*: Strips that are created using the data blocks across multiple vDisks. Nutanix recommends that you configure inline erasure coding type as cross vDisk strips for workloads that require data locality.

By default, same vDisk strips are created when you enable inline erasure coding.

> **Note:** Inline erasure coding with same vDisk strips can be enabled for clusters running AOS version 5.18 or higher; and with cross vDisk strips can be enabled for clusters running AOS version 6.6 or higher.

Enabling Inline Erasure Coding

Inline erasure coding can be enabled only using nCLI. Inline erasure coding is added as a storage container parameter in Zeus.

Before you begin

Caution:

- Nutanix recommends that you enable inline erasure coding for Object storage containers only. To enable inline erasure coding for any other type of storage container, contact Nutanix Support.
- Erasure coding must be enabled on the container to enable inline erasure coding. For information about how to enable erasure coding, see Creating a Storage Container on page 290.

Procedure

To enable inline erasure coding, perform the following actions:

- Run the following nCLI command:

  ```
  ncli> container create name=container_name sp-id=storage_pool_id erasure-code=on
   inline-ec-enabled=true
  ```

  Replace *container_name* and *storage_pool_id* with the storage container name and storage pool ID on which you want to enable erasure coding.

  - To explicitly configure inline erasure coding type, run the following nCLI commands:
    - For inline erasure coding type: *Same vDisk strips*

      ```
      ncli> container create name=container_name sp-id=storage_pool_id erasure-
      code=on inline-ec-enabled=true inline-ec-type=same-vdisk-strips
      ```

    - For inline erasure coding type: *Cross vDisk strips*

      ```
      ncli> container create name=container_name sp-id=storage_pool_id erasure-
      code=on inline-ec-enabled=true inline-ec-type=cross-vdisk-strips
      ```

  - To change an existing inline erasure coding type, run the following ncli commands:
    - To change to *Same vDisk strips*:

      ```
      ncli> container edit inline-ec-enabled=true inline-ec-type=same-vdisk-strips
       id=container_id
      ```

    - To change to *Cross vDisk strips*:

      ```
      ncli> container edit inline-ec-enabled=true inline-ec-type=cross-vdisk-strips
       id=container_id
      ```

  Replace *container_id* with the ID of the storage container.

Capacity Reservation Best Practices

Capacity reservation allows you to guarantee that a storage container has a minimum amount reserved that is unavailable to other storage containers.

By default, each storage container has access to all of the unused storage in the storage pool. If a storage pool consists of multiple storage containers, one storage container might take all the remaining storage space and leave others with no available space. To make sure that there is space available for a storage container, you can enable capacity reservation.

The following best practices are applicable for capacity reservation:

- Reserve capacity for a storage container only if the storage pool consists of multiple storage containers. Unless there is a specific reason to have multiple storage containers, Nutanix recommends you to configure a single storage pool with a single storage container.
- Do not reserve more than 90% of the total space in the storage pool.
- When you set an advertised capacity for a storage container, be aware that some extra space should be allocated beyond the projected size of any VMs placed in the container. This extra space is to allow room for data that is not yet garbage collected. The extra space is based on the workload and can be substantial, for example, 10% or more of the storage capacity in some cases.

Limitations for Storage Containers

Replication Factor 1 (RF1) containers are not supported in Prism Central. You can create RF1 containers only from Prism Element.

> **Note:** From Prism Central, you cannot update or delete the created RF1 containers that are created using Prism Element.

Creating a Storage Container

This section describes how to create a storage container in a cluster.

Before you begin

Ensure that the following prerequisites are met before you create a storage container in AHV cluster:

- The AHV cluster is configured to synchronize time with NTP servers. For information about how to configure the NTP server, see Configuring NTP Servers for Prism Central in *Prism Central Admin Center Guide*.
- The time on the Controller VMs and Files is synchronization to the current time. If the time on the Controller VMs and Files is ahead of the current time, cluster services might fail to start.

About this task

AOS automatically creates the following type of access to the storage container for each hypervisor:

- *AHV* - Storage container is accessible transparently for AHV.
- *ESXi* - Storage container is accessible as an NFS datastore. In this case, the access to the storage container requires access to the vSphere APIs. Ensure that you have appropriate license of vSphere to access the APIs.
- *Hyper-V* - Storage container is accessible as an SMB share.

Procedure

To create a storage container, follow these steps:

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Storage Containers** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab as default.

3. Click **Create Storage Container**, and enter the following information:

   The following is an example showing the **Create Storage Container** window:

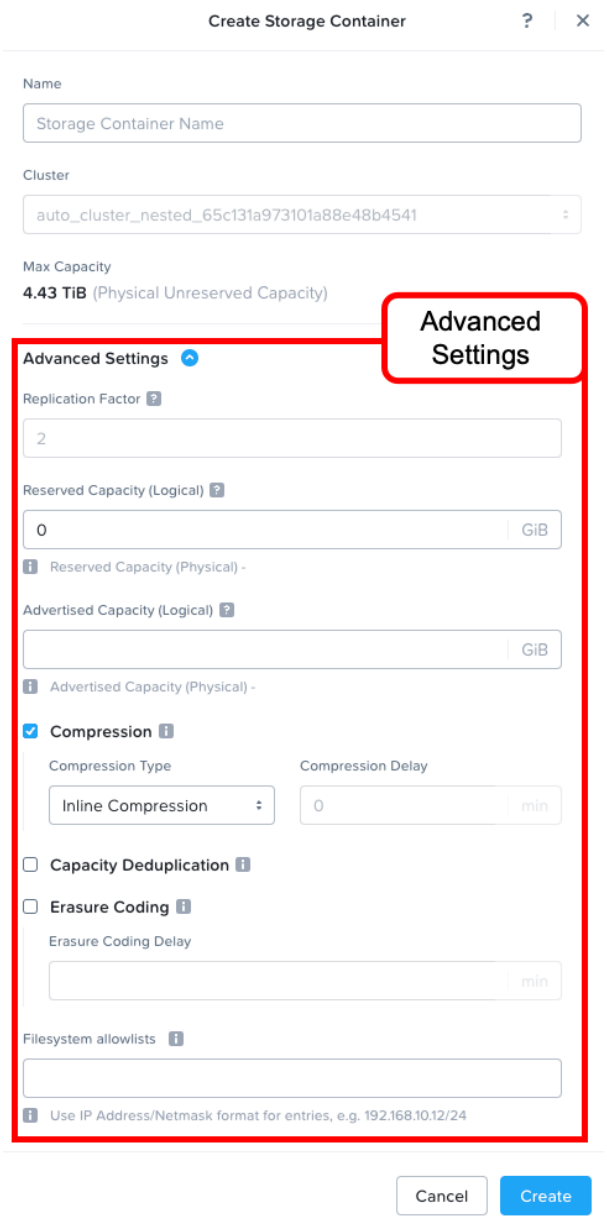


Figure 135: Create Storage Container (AHV)

- **Name**: Enter a name for the storage container.

  Note: This entity has the following naming restrictions.

  - Container Name Length: Maximum length is 75 characters.
  - Supported Characters: Uppercase and lowercase standard Latin letters (A-Z and a-z), Simplified Chinese, decimal digits (0-9), dots (.), hyphens (-) , hash (#), and underscores (_).

- Case Sensitivity: Container names are case sensitive.

- **Clusters**: Select a cluster from the dropdown list.
  - If you select an ESXi cluster in the **Clusters** dropdown list, the system prompts you to specify the **NFS Datastore**.

    The following is an example showing the **Create Storage Container** windows for *ESXi* cluster:

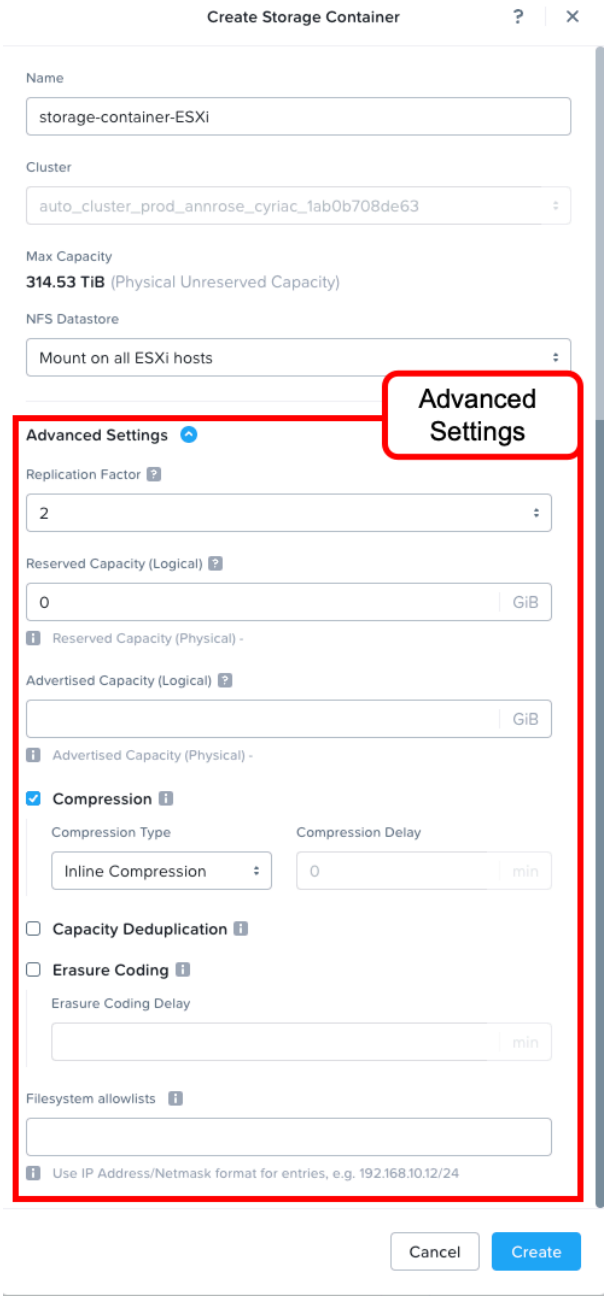


Figure 136: Create Storage Container (ESXi)

  - If you select a Hyper-V cluster in the **Clusters** dropdown list, the system prompts you to specify any of the following mechanisms to make this storage container a default store for VM configuration and virtual hard disk files on Hyper-V:

- **Make default on all Hyper-V hosts** - Used to make this storage container as a default store location for all the Hyper-V hosts.
- **Make default on particular Hyper-V hosts** - Used to make this storage container as default store for selected Hyper-V hosts.

The following is an example showing the **Create Storage Container** windows for *Hyper-V* cluster:

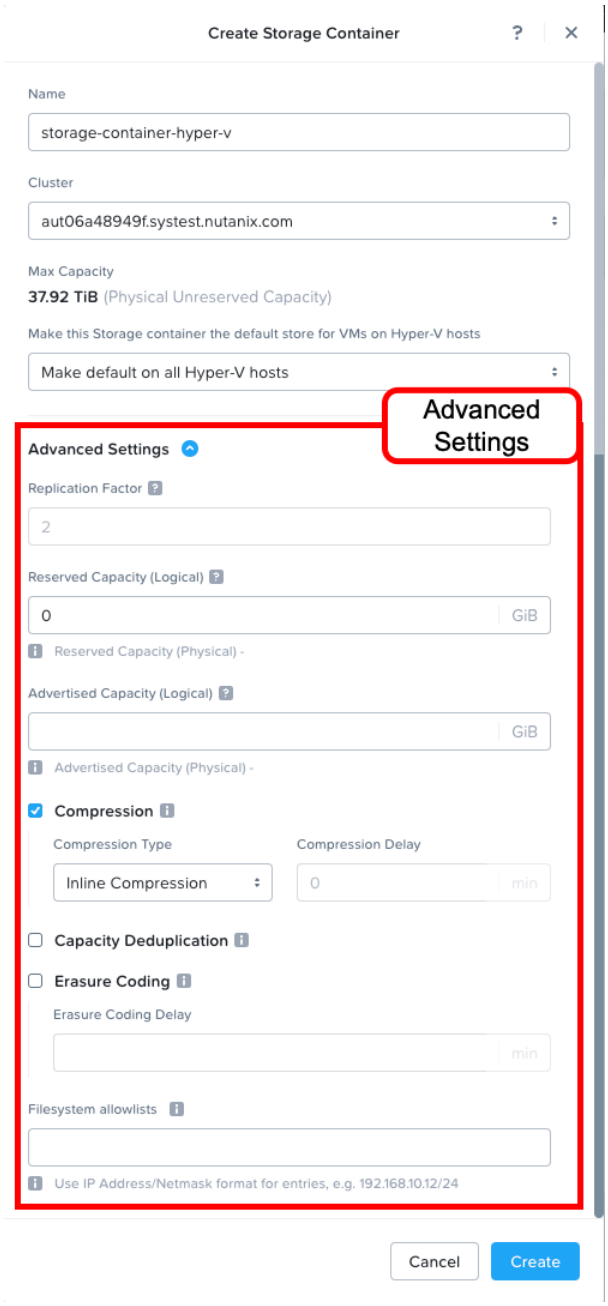


Figure 137: Create Storage Container (Hyper-V)

- **Max Capacity** *(Read-Only)*: Displays the amount of free physical space available in the selected cluster. For example, 3.48 TiB (Physical Unreserved Capacity).

4. Click **Advanced Settings** to configure the following additional parameters:

   - **Replication Factor**: Displays the number of data copies to maintain in the cluster.

     Nutanix supports a replication factor of 2 or 3. Setting the RF to 3 adds an extra layer of data protection at the cost of storing an additional copy of the data.

     > **Note:** You cannot change the replication factor of the storage container from Prism Central. The replication factor can be set only through the Prism Element. For more information about how to set replication factor, see Increasing the Cluster Fault Tolerance Level information in *Prism Web Console Guide*.

   - **Reserved Capacity (Logical)**: Enter the capacity (in GiB) to reserve storage space for this storage container.

     You can reserve space for a storage container to ensure a minimum storage capacity is available. If you reserving space for a storage container, the reserved space is no longer available to other storage containers even if it is unused. For more information, see Capacity Reservation Best Practices on page 289.

     Reserved Capacity (Physical)*(Read-Only)*: Displays the amount of physical capacity that is reserved based on the logical reserved capacity value.

   - **Advertised Capacity (Logical)**: Enter the capacity (in GiB) to reserve the maximum storage space for this storage container.

     This field is used to set an advertised capacity, which is the maximum storage size that the storage container can use. This can be set to any value, but if you configure **Reserved Capacity**, ensure that you set the advertised capacity greater than or equal to the **Reserved Capacity** for the storage container. The hypervisor ensures that the storage does not go beyond the advertised capacity of the storage container.

     Advertised Capacity (Physical) *(Read-Only)*: Displays the amount of physical capacity that is advertised based on the logical advertised capacity value.

   - **Deduplication**: Select the **Deduplication** checkbox, and choose any of the following options in the **Type** dropdown menu to optimize performance.:

     - **Inline Deduplication of Read Caches** - Used to perform deduplication on the data in memory. This option is primarily recommended for full-clone, persistent desktops, and physical to virtual migration use cases. For more information, see Cache Deduplication on page 284 information.
     - **Inline Deduplication of Read Caches + Post Process Deduplication** - Used to perform post-process deduplication of persistent data. This option is primarily recommended for full clone, persistent desktops, and physical to virtual migration use cases that need both storage capacity savings and performance savings from deduplication. For more information, see Capacity Deduplication on page 284 information.

   - **Compression**: Select the **Compression** checkbox. All data in the storage container is compressed when you configure **Compression**. For more information about data compression, see Compression on page 283.

     By default, **Inline compression** is selected in the **Type** field and **0** is selected in the **Delay** field (In Minutes) which indicates that the data is compressed immediately as it is written.

     To configure the delay time between the write and compression, under **Type** field, select **Post Process Compression** from the dropdown menu. For post-process compression, where data is

compressed after it is written, Nutanix recommends that you set a delay of 60 minutes to delay the compression activity for 60 minutes after the initial write operation.

- **Erasure Coding**: Select the **Erasure Coding** checkbox to enable erasure coding. Erasure coding increases the effective or usable capacity on a cluster. For more information about erasure coding, see Erasure Coding on page 285.
- **Filesystem allowlists**: Enter the comma-separated IP address and netmask value in the form `ip_address/ netmask`.

  A allowlist is a set of addresses that are allowed access to this storage container. Allowlists are used to allow appropriate traffic when unauthorized access from other sources is denied. If you set an allowlist at storage container level, the system overrides any global allowlist for this storage container.

  Setting an allowlist helps you provide access to the container via NFS. Some manual data migration workflows might require the allowlist to be configured temporally, while some third-party backup vendors might require the allowlist to be configured permanently to access the container via NFS.

  Caution:

  - User authentication is not available for NFS access, and the IP address in the allowlist has full read or write access to the data on the container.
  - Nutanix recommends to allow single IP addresses (with net mask such as 255.255.255.255) instead of allowing subnets (with netmask such as 255.255.255.0).

5. Click **Create**.
   The system creates a storage container in AHV cluster.

Modifying a Storage Container

A storage container is a defined subset of available storage within a storage pool that can be modified as conditions change.

About this task

Storage Containers can be modified to change how the data in that storage container is handled. For example, apply compression to the storage container.

Note: You cannot rename a storage container if any of the following conditions is met:

- The cluster is the AHV cluster.
- Storage container include vdisks.

To modify a storage container, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Storage Containers** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab as default.

3. Select the target storage container checkbox, and choose **Update** from the **Actions** dropdown menu. The system displays the **Update Storage Container** window:

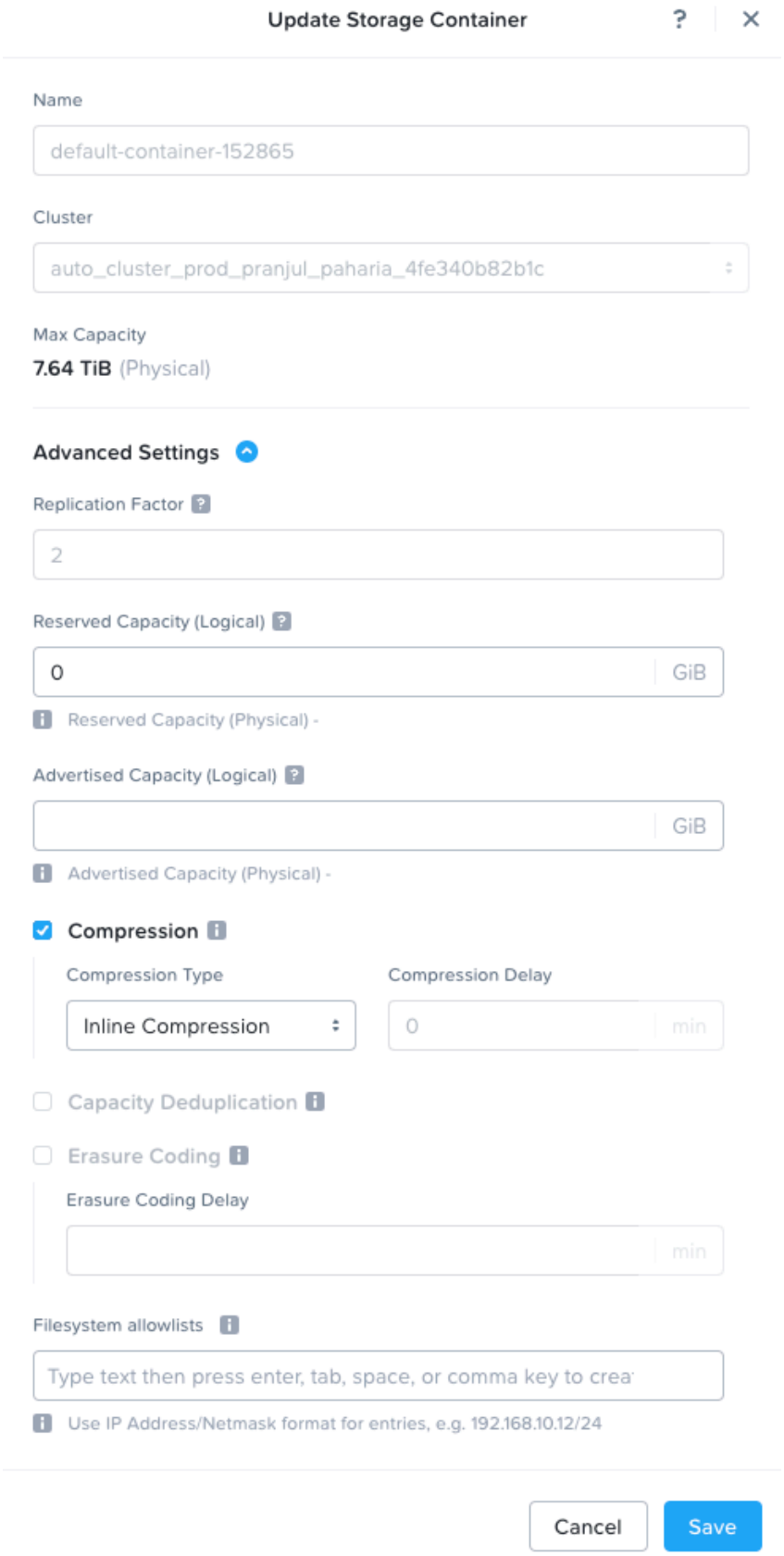


Figure 138: Update Storage Container (AHV)

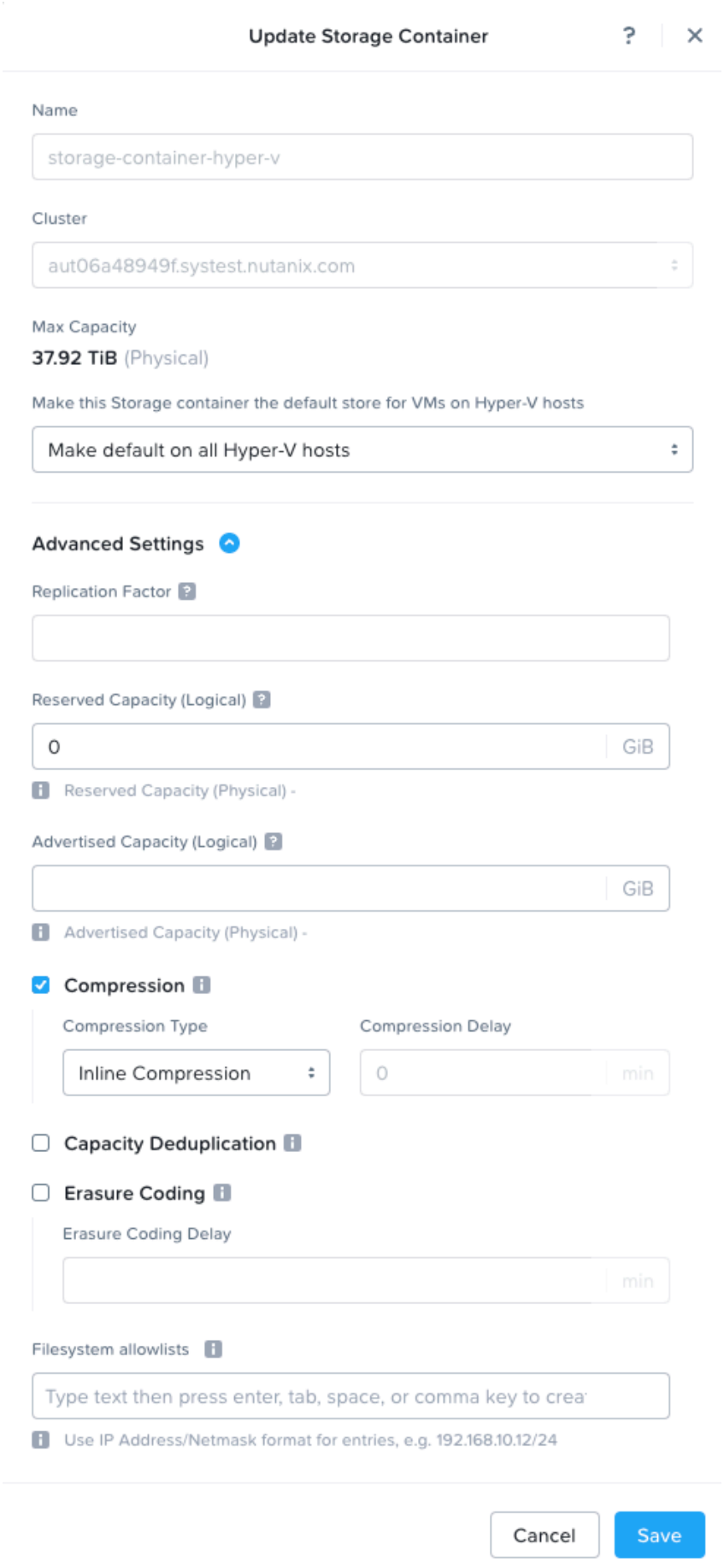


Figure 139: Update Storage Container (Hyper-V)

4. Update the storage container configuration as per your requirement, and click **Save**.
   The fields that appear in **Update Storage Container** and **Create Storage Container** windows are same. For field details, see Creating a Storage Container on page 290.

   Note:

   - If the compression policy is changed from compressed to uncompressed (or vice versa), the existing compressed (uncompressed) data in the storage container will be uncompressed (compressed) as a background process when the next data scan detects the data that needs this change.
   - You cannot change the RF of the storage container from Prism Central. The RF can be set only through Prism Element. For more information about how to set RF, see Increasing the Cluster Fault Tolerance Level section in the *Prism Web Console Guide*).

Deleting a Storage Container

A storage container is a defined subset of available storage within a storage pool that can be deleted.

About this task

Note: A SelfServiceContainer storage container is created on the target cluster and used by Prism Self Service for storage and other feature operations. To ensure proper operation of these features, do not delete this storage container. For more information about Prism Self Service, see Prism Self Service Administration on page 519.

To delete a storage container, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Storage Containers** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab as default.
3. Select the target storage container checkbox, and choose **Delete** from the **Actions** dropdown menu.
   The system prompts you to confirm the delete action.
4. Click **Delete**.
   The selected storage container is deleted from the cluster.

Volume Group Management

Volumes act as one or more targets for client Windows or Linux operating systems running on a bare metal server or as guest VMs using iSCSI initiators. You can use any storage available in any new or existing Nutanix cluster for Volumes.

Note: Do not use volumes to create an iSCSI datastore to Hyper-V or ESXi hosts. This configuration is not supported.

- The **Summary** tab on the **Volume Groups** page displays information about volume groups across the registered clusters. For more information, see Volume Groups Summary View on page 301.
- The **Summary** tab on the individual volume group page displays the detailed information about the selected volume group. For more information, see Volume Group Details View on page 306.

- For more information about volumes and volume groups, see Volumes Guide.

You can create and update volume groups directly from Prism Central web console.

- For information about how to create a volume group, see Creating a Volume Group on page 314.
- For information about how to modify a volume group, see Modifying a Volume Group on page 321.

You can configure CHAP secret password from the Prism Central web console. For more information, see Configuring Mutual CHAP Authentication on page 324

You can attach volume groups to guest VMs from the Prism Central web console. For more information, seeAttaching Volume Groups to Guest VMs on page 325

You can also define the Cluster Role Based Access Control (RBAC) for a volume group. For details, see Cluster RBAC for Volume Group on page 325

Volume Groups Summary View

The **Summary** tab in **Storage Containers** page provides the information about all the storage containers across the registered clusters.

To access the summary view of all volume groups, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Volume Groups** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The system displays the **List** tab by default with all the volume groups across registered clusters.
3. Click the **Summary** tab.

   The system displays **Summary** page for all volume groups.

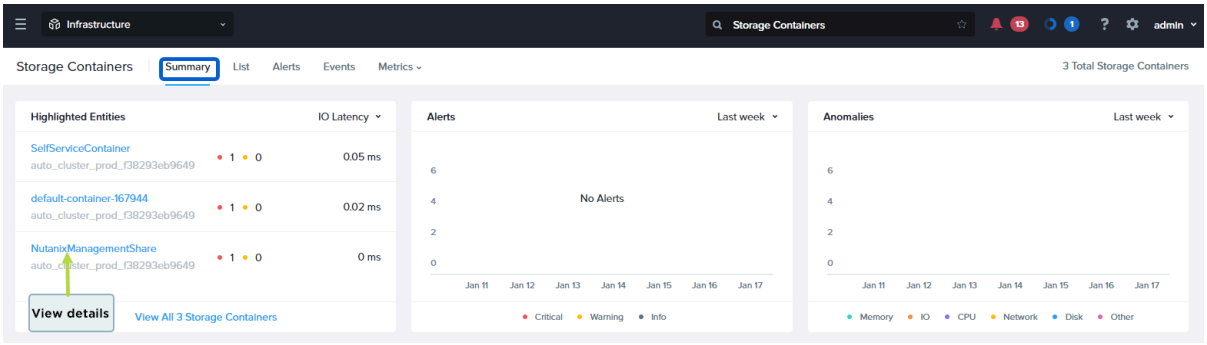


Figure 140: Summary Page - All volume Groups

The **Storage Container** page includes five tabs on the left (**Summary**, **List**, **Alerts**, **Events**, and **Metrics**) with a display area below the selected tab.

The **Summary** tab of all storage containers displays the following widgets:

- **Highlighted Entities**: Displays a list of the storage containers with the highest usage of the <*parameter*> you select from the dropdown menu on the right of the widget. The <*parameter*> involves **IO Latency**, **IOPS**, and **Bandwidth**. Click **View All XX Storage Containers** link at the bottom to display the **List** tab.
- **Alerts**: Displays a list of alerts related to storage container that are generated during the specified <*interval*> you select from the dropdown menu on the right of the widget. The <*interval*> involves **Last**

week(default), **Last 24 hours**, and **Last 1 hour**. When an alert appears, you can click the graph to view a list of those alerts. Click any alert to display the details page for that alert.

- **Anomalies**: Displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified *<interval>* you select from the dropdown menu on the right of the widget. The *<interval>* involves **Last week**(default), **Last 24 hours**, and **Last 1 hour**. When an anomaly appears, you can click the graph to view a list of those anomalies. Click any anomaly to display the event page for that anomaly.

List Tab

The **List** tab displays the list of volume groups across all clusters.

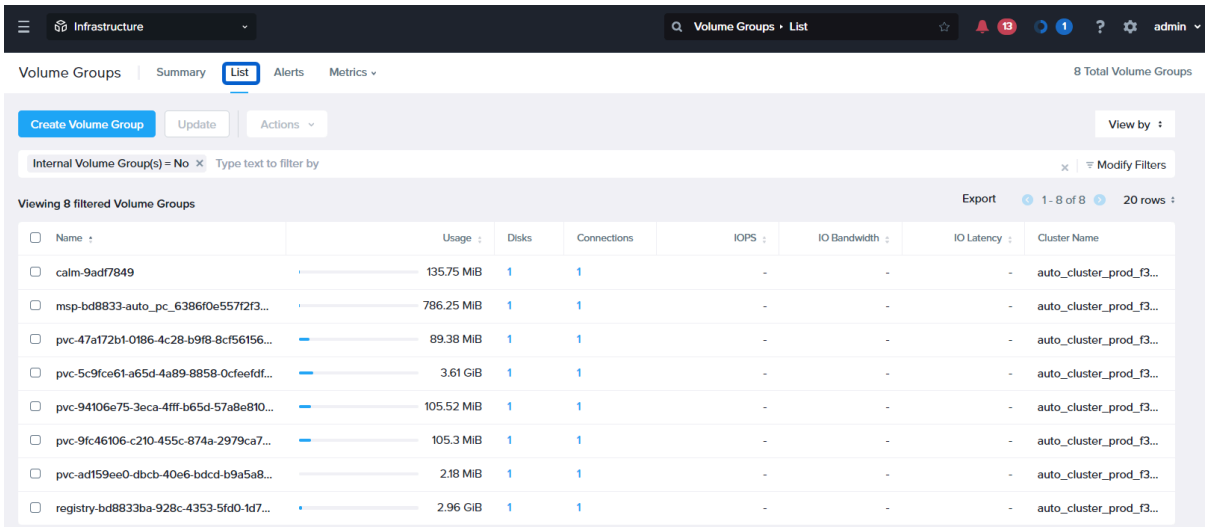


Figure 141: Volume Groups List Tab

The following table describes the fields that appear in the **List** tab of **Volume Groups** page:

> **Note:** The fields vary based on the **View by** and **Group by** options. A dash (-) is displayed in a field when a value is not available or applicable. For more information about **View by** and **Group by** options, see Prism Central GUI Organization on page 27.

Table 53: Volume Groups List Tab - Field Description

Parameter	Description	Values
Select **General** from **View by** option.		
Name	Displays the name of the volume group. You can click the volume group name to view the details page for that volume group. For information about volume group details, see Volume Group Details View on page 306. **Note:** An exclamation point appears if the cluster is running a pre-6.0 AOS version, which indicates the available information and actions are limited.	*<Volume _Group_Name>*

Parameter	Description	Values
Usage	Displays the amount of used storage space. A bar also appears that graphically indicates the amount of used and free storage space available in the volume group. When you hover the cursor over the bar, the system displays a window that lists the used space, free space, and total space in the volume group.	xxx [GiB|TiB]
Disks	Displays the number of virtual disks in the volume group. You can click the number to view the **Virtual Disks** tab in the Volume Group Details View on page 306.	(integer)
Connections	Displays the number of external client connections to the volume group. You can click the number to view the **Connections** tab in the Volume Group Details View on page 306.	(integer)
IOPS	Displays the current I/O operations per second (IOPS) for the volume group. The controller IOPS, I/O bandwidth, and I/O latency fields record the I/O requests serviced by the Controller VM. The I/O can be served from memory, cache (SSD), or disk.	[0 - unlimited]
IO Bandwidth	Displays I/O bandwidth used per second for Controller VM-serviced requests in this volume group.	xxx [MBps|KBps]
IO Latency	Displays the average I/O latency for Controller VM-serviced requests in this volume group.	xxx [ms]
Cluster Name	Displays the name of the cluster in which the volume group resides. You can click the cluster name to view the cluster details. For information about cluster details, see Cluster Details View on page 405.	(cluster name)
Select **Data Protection** from **View by** option.		
Name	Displays the name of the volume group. You can click the volume group name to view the details page for that volume group. For information about volume group details, see Volume Group Details View on page 306. **Note:** An exclamation point appears if the cluster is running a pre-6.0 AOS version, which indicates the available information and actions are limited.	*<Volume _Group_Name>*
Category	Displays the category of the volume group. For information about categories in Prism Central, see Category Management on page 454.	String (Category name)

Parameter	Description	Values
Consistency Group	Displays the consistency group of the volume group. For information about Consistency Groups in Prism Central, see Consistency Groups information in *Nutanix Disaster Recovery Guide* .	Yes/No
Protection Status	Displays the Protection Status of the volume group.	Protected/Unprotected
Protection Type	Displays the type of protection defined for the volume group.	Protection Policy
Protection Policy	Displays the protection policy that is applicable for the VM. For more information about protection policies, see Nutanix Disaster Recovery Guide.	(String) Protection Policy Name
Recovery Plan	Displays the recovery plans that is applicable for the volume group. For more information about VG recovery plans, see Nutanix Disaster Recovery Guide.	(String) Recovery Plans Name

You can perform the following actions for the storage containers in the **Lists** tab:

- Access the detailed information about an individual volume group. For more information, seeVolume Group Details View on page 306.
- Filter the volume groups list based on available parameter values using **Filters** pane. For more information about **Filters** pane, see Filters Pane - Volume Groups Page on page 304.
- Export the table that contains the list of volume groups and their information to a file in a CSV format. For more information about **Export** option, see Export on page 32.
- Group the volume groups based on pre-defined criteria. For information about how to group the storage containers, see Group by on page 29.
- View volume groups based on pre-defined criteria or create a custom view. For information about available views and how to create a custom view, see View by on page 29.
- Create a volume group. For more information about how to create a storage container, see Creating a Volume Group on page 314.
- Perform the actions specific to storage container on a single or multiple storage containers using the **Actions** dropdown menu. For instructions on how to perform these actions, seeModifying a Volume Group on page 321.

> **Note:** The **Actions** dropdown menu is grayed out unless you select a volume group.

Filters Pane - Volume Groups Page

The following table describes the fields available in the **Filters** pane:

Table 54: Filter Pane Fields - Volume Groups

Parameter	Description	Values
Name	Filters based on the volume group name. Select a condition from the dropdown menu and enter a string in the field. The system returns a list of storage containers that satisfy the storage container name condition/string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	(volume group name string)
Usage	Filters on the used storage space for a volume group. Check the box for the desired range or enter an amount range in the "**from <low> to <high> GiB**" field. It returns a list of volume groups with used storage in that range.	([xx] to [yy] GiB range)
Cluster Name	Filters based on the cluster name. Select a condition from the dropdown menu and enter a string in the field. The system returns a list of storage containers that satisfy the cluster name condition/string.	(cluster name string)
Category	Filters based on category names. Enter a category name in the field and then check the box. As you type a dropdown menu appear to help you select the correct category. A new field appears where you can add more categories to the filter. The number of volume groups tagged to each selected category are displayed in the **List** tab.	(category name)
IOPS	Filters based on the current IOPS. Check the box for the desired range or enter a range in the ***From <low> to <high> iops*** field. It returns a list of volume groups with IOPS in that range.	([xx] to [yy] IOPS range)
IO Bandwidth	Filters based on the I/O bandwidth used. Check the box for the desired range or enter a range in the ***From <low> to <high> MBps*** field. It returns a list of volume groups with I/O bandwidth usage in that range.	([xx] to [yy] MBpS range)
IO Latency	Filters based on the average I/O latency. Check the box for the desired range or enter a range in the ***from <low> to <high> ms*** field. It returns a list of volume groups with average I/O latency in that range.	([xx] to [yy] ms range)
Internal Volume Group(s)	Filters based on the volume group names specified	Yes | No

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options that are available on the **Activity** > **Alerts** page, however it only displays the alerts related to storage containers across the registered clusters. For more information about alerts, see *Prism Central Alerts and Events Reference Guide*.

Metrics Tab

The **Metrics** tab allows you to view performance metrics across the volume groups. Click the **Metrics** tab to display dropdown menu of available metrics, and select the metric name to display the relevant performance information.

> **Note:** The **Metrics** dropdown menu is hypervisor-specific, and might vary based on the hypervisors used in the cluster.

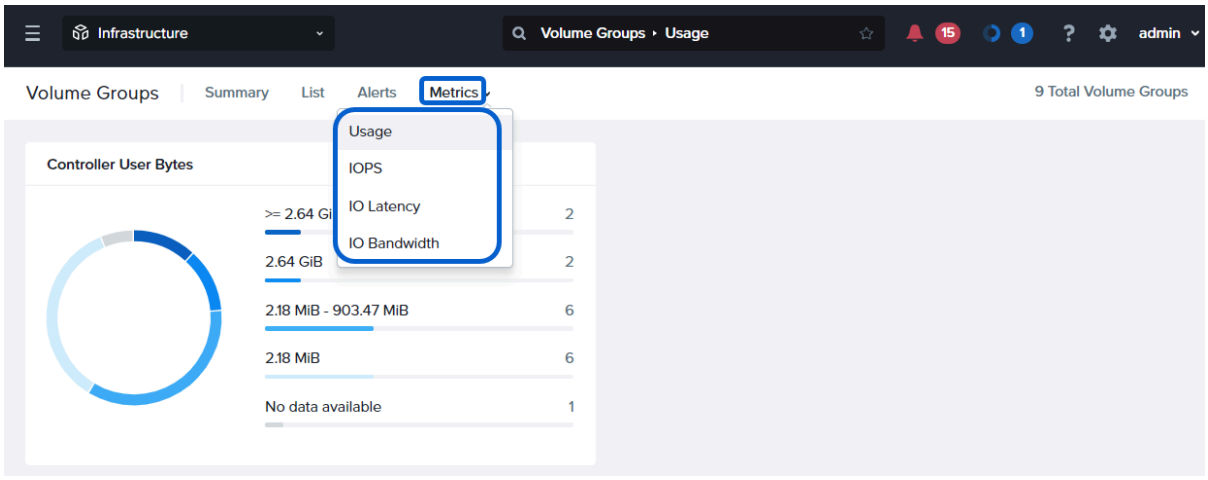


Figure 142: Volume Groups Metrics Tab

Table 55: Metrics Tab Fields

Metric	Description
Usage	Displays volume group usage graph.
IOPS	Displays total, read, and write IOPS graphs listing current values and total volume groups (number). The current values are split into intervals (for example, less than 700, 700-1400, 1400-2000, more than 2000). **Note:** The same format also applies to the other metrics in this table.
IO Latency	Displays total, read, and write I/O latency rate graphs.
IO Bandwidth	Displays total, read, and write I/O bandwidth rate graphs.

Volume Group Details View

To access the details view of an individual volume group, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Volume groups** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The system displays the **List** tab by default with all the volume groups across registered clusters.

3. Click the target <*Volume_Group_Name*> to view the **Summary** tab of an individual volume group.

> **Note:** Replace <*Volume_Group_Name*> with the actual storage container name at your site.

The following is an example showing the **Summary** tab of an individual volume group:

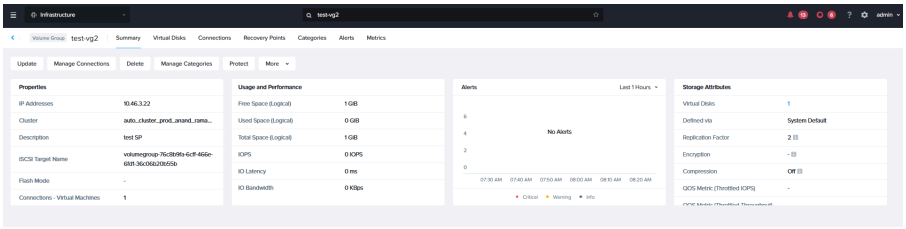


Figure 143: Summary Tab - Individual Volume Group

The **Summary** tab of an individual volume group provides the following widgets:

- **Properties** - Displays summary information about the volume group. For information about the fields available in **Properties** widget, see Table 56: Volume Group Widgets - Field Description on page 307.
- **Usage and Performance** - Displays the usage and performance data for the volume group. For information about the fields available in **Usage and Performance** widget, see Table 56: Volume Group Widgets - Field Description on page 307.
- **Alert**- Displays a list of related alerts that occurred during the specified interval. Select either **Last week** (default), **Last 1 hour** or **Last 24 hours** from the dropdown menu on the top right corner of the widget.

<*Action*> available above the widgets. Click the appropriate <*Action*> to run that administrative action on the volume group. For more information about how to perform any <*Action*>, see Modifying a Volume Group on page 321.

Volume Group Widgets - Parameter Details

The following table describes the fields available in the **Properties** and **Usage and Performance** widgets. A dash (-) in a field indicates that there is not enough data to evaluate or a value is not assigned. The displayed fields vary by hypervisor.

Table 56: Volume Group Widgets - Field Description

Parameter	Description	Values
Properties widget		
IP Addresses	Displays the IP address assigned to the volume group.	(IP address)
Cluster	Displays the name of the cluster in which the volume group resides. You can click the name to view the detailed information about the cluster. For more information, see Cluster Details View on page 405).	(cluster name)
Flash Mode	Displays whether Flash Mode is enabled for the volume group.	[Enabled, Disabled]

Parameter	Description	Values
Virtual Disks	Displays the number of virtual disks in the volume group. You can click the numeric value to view the **Virtual Disks** tab.	(integer)
Connections - External Clients	Displays the number of external client connections to the volume group. You can click the numeric value to view the **Connections** tab.	(integer)
iSCSI Target Name	Displays the name of the iSCSI target.	(ISCSI name)
Cluster	Displays the name of the cluster in which the volume group resides. You can click the cluster name to view the cluster details. For more information, see Cluster Details View on page 405.	(cluster name)
Usage and Performance Widget		
Free Space (Logical)	Displays the amount of logical (effective) free space available in the volume group. **Note:** Logical space accounts for the volume group replication factor. RF1 means the logical and physical spaces are the same, RF2 means the logical space is half the physical space, and RF3 means the logical space is a third of the physical space.	xxx [GiB|TiB]
Used Space (Logical)	Displays the amount of logical used space in the volume group.	xxx [GiB|TiB]
Total Space (Logical)	Displays the amount of logical total space in the volume group.	xxx [GiB|TiB]
IOPS	Displays the current I/O operations per second (IOPS) for the volume group. The controller IOPS, I/O bandwidth, and I/O latency fields record the I/O requests serviced by the Controller VM (CVM). The I/O can be served from memory, cache (SSD), or disk.	[0 - unlimited]
IO Bandwidth	Displays I/O bandwidth used per second for Controller VM-serviced requests in this volume group.	xxx [MBps|KBps]
IO Latency	Displays the average I/O latency for Controller VM-serviced requests in this volume group.	xxx [ms]
Storage Attributes		
Virtual Disks	Displays the number of virtual disks associated with the VG.	(integer)

Parameter	Description	Values
Defined via	Displays the entity that defines the storage attributes of the VG. The storage attributes of the VG could be inherited from the storage properties of the cluster or applied by a Storage Policy. See Storage Policy Management on page 495 for more information.	(System Default, <Name of Storage Policy>
Replication Factor	Displays the Replication Factor selected.	Inherit from Container or 2 or 3
Encryption	Displays the encryption mode selected.	Enabled or Inherit from Cluster
Compression	Displays the compression mode selected.	Inline or Post Process (if On) Off Inherit from Cluster
Throttled Throughput (IOPS)	Displays the throttled throughput value in terms of IOPS.	(Integer number)
Throttled Throughput (MB/s)	Displays the throttled throughput value in MBps.	(Integer number)

For information about Storage Policies, see Storage Policy Management on page 495.

Virtual Disks Tab

Click the **Virtual Disks** tab to view a list of virtual disks for the volume group.

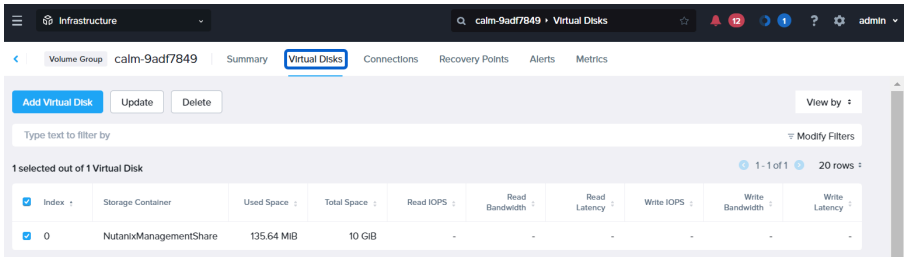


Figure 144: Virtual Disks Tab

You can perform the following actions for the virtual disks in the **Virtual Disks** tab:

- Filter the Virtual Disks list based on available field values using **Filters** pane. For more information about how to use the **Filters** pane, see Filters Pane on page 28.
- View Virtual Disks based on pre-defined criteria or create a custom view. For information about available views and how to create a custom view, see View by on page 29.

- Add, update, and delete a virtual disk. For more information about how to manage a virtual disk, see Modifying a Volume Group on page 321.

> **Note:** The available actions appear in bold; other actions are grayed out. For grayed out options, a tool tip explaining the reason is provided. The available actions depend on the current state of the selected VM(s).

The following table describes the fields that appear in the list. A dash (-) is displayed in a field when a value is not available or applicable:

Table 57: Virtual Disks - Field Description

Fields	Description	Values
Select **General** from **View by** option.		
Index	Displays the index number assigned to the virtual disk.	(integer)
Storage Container	Displays the name of the storage container in which the virtual disk is located.	(container name)
Used Space	Displays the amount of used space in the virtual disk.	xxx [GiB|TiB]
Total Space	Displays the total amount of storage space in the virtual disk.	xxx [GiB|TiB]
Read IOPS	Displays the current read I/O operations per second (IOPS) for the virtual disk.	[0 - unlimited]
Read Latency	Displays the average read I/O latency for the virtual disk.	xxx [ms]
Read Bandwidth	Displays read I/O bandwidth used per second for the virtual disk.	xxx [MBps|KBps]
Write IOPS	Displays the current write I/O operations per second for the virtual disk.	[0 - unlimited]
Write Latency	Displays the average write I/O latency for the virtual disk.	xxx [ms]
Write Bandwidth	Displays write I/O bandwidth used per second for the virtual disk.	xxx [MBps|KBps]
Select **+Add Custom** from **View by** option to create a custom view with the following additional fields:		
IOPS	Displays the current total I/O operations per second for the virtual disk.	
IO Bandwidth	Displays the total I/O bandwidth used per second for the virtual disk.	
IO Latency	Displays the average I/O latency for the virtual disk.	
Nutanix File Path	Displays the path of the storage file in Nutanix File server. For information about Nutanix Files, see Nutanix Files User Guide.	File path. For example `/home/nutanix/`

The following table describes the **Filters** pane of **Virtual Disks** tab:

Table 58: Filters Pane - Virtual Disks Tab

Field	Description	Values
Storage container	Filters based on the Storage Container name. Select a condition from the dropdown menu and enter a string in the field. The system returns a list of virtual disks that satisfy the Storage container name condition/string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	(storage container name string)
[Total|Used] Space	Filters based on the total or used storage space for a virtual disk. Enter an amount range in the **From : <low> To: <high> GiB** field. The system returns a list of virtual disks with total or used storage in that range.	([xx] to [yy] GiB range)
[Read|Write] IOPS	Filters based on the current read or write IOPS. Enter a range in the **From : <low> To: <high> IOPS** field. It returns a list of virtual disks with IOPS in that range.	([xx] to [yy] range)
[Read|Write] Bandwidth	Filters based on the read or write I/O bandwidth used. Enter a range in the **From : <low> To: <high> MBps** field. It returns a list of virtual disks with I/O bandwidth usage in that range.	([xx] to [yy] range)
[Read|Write] Latency	Filters on the average I/O latency. Enter a range in the **From : <low> To: <high> ms** field. It returns a list of virtual disks with average I/O latency in that range.	([xx] to [yy] range)

Connections Tab

Click the **Connections** tab to view a list of external client connections to the volume group.

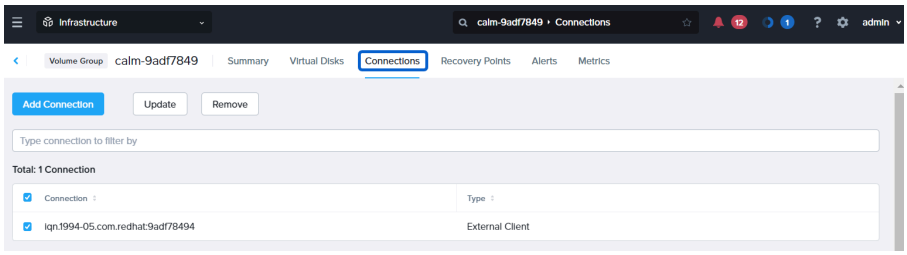


Figure 145: Connections Tab

You can add, update, and delete an external connection for the volume group. For more information about how to manage a volume group connection, see Modifying a Volume Group on page 321.

Note: The available actions appear in bold; other actions are grayed out. For grayed out options, a tool tip explaining the reason is provided. The available actions depend on the current state of the selected VM(s).

The following table describes the fields that appear in the list. A dash (-) is displayed in a field when a value is not available or applicable:

Table 59: Connections - Field Description

Field	Description	Values
Connection	Displays the IP address or IQN of the external client.	(IP or IQN address)
Type	Displays the type of connection.	external client

Recovery Point Tab

Click the **Recovery Point** tab to view a list of recovery points created with the selected volume group.

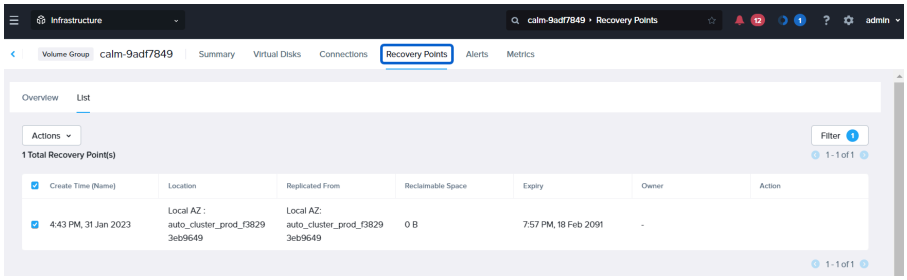


Figure 146: Recovery Points Tab

You can clone, revert, replicate, and delete a recovery point of the volume group. For more information about how to manage a volume group recovery points, see Nutanix Disaster Recovery Guide.

The following table describes the fields that appear in the list. A dash (-) is displayed in a field when a value is not available or applicable:

Table 60: Recovery Point - Field Description

Field	Description	Values
Create Time (Name)	Displays the name of the VG recovery point. By default, the system displays the VG recovery point creation time as the name when you create a VG recovery point, however you can change it as per your requirement.	(Name)
Location	Displays the location where the VG recovery point is created in *AZ location:Cluster name* format.	Local AZ : auto_cluster_prod_f38293eb9649
Replicated From	Displays the location from where the VG recovery point is replicated in *AZ location:Cluster name* format.	

Field	Description	Values
Reclaimable Space	Displays the space that can be reclaimed for the VG group recovery point.	(Integer) B. For example, 0 B
Expiry	Displays the expiry time of the VG group recovery point.	Timestamp in hh:mm AM/PM, DD MM YYYY. For example, 7:57 PM, 18 Feb 2091
Owner	Displays the owner name.	-
Action	Displays the applicable actions for the VG recovery point.	-

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options as the Alerts dashboard, however it is filtered to display the alerts only for the selected volume group (individual volume group). For more information about alerts, see Prism Central Alerts and Events Reference Guide.

Metrics Tab

The **Metrics** tab allows you to view usage metrics for the storage container. Click the **Metrics** tab to view graphs for all the metrics. The graph is a rolling time interval performance or usage monitor. The baseline range appears as a blue band in the graph.

> **Note:** The baseline range and identified anomalies are based on sophisticated machine-learning capabilities. For more information, see Behavioral Learning Tools in *Intelligent Operations Guide*. The machine-learning algorithm uses 21 days of data to monitor and predict performance. A graph or baseline band may not appear if less than 21 days of data is available.

You can perform the following actions in the **Metrics** tab:

- Place the cursor anywhere on the horizontal axis to display the value at that time.
- Select the duration (time interval) from the dropdown menu on the right (Last 1 hour, Last 24 hours, and Last week).
- From the **Actions** dropdown menu that appears on the top-right corner of each metrics widget, you can perform the following operations:
  - Select **Add to Analysis** to add the selected metric to **Analysis** dashboard. For more information, see Analysis Dashboard in *Intelligent Operation Guide*.
  - Choose **Select Analysis Session** to assign the metric to a target session.
- Click the **Filters** option to select one or more appropriate metric checkboxes to display the selected metrics in the **Metrics** page.

The following table describes the metrics available in **Metrics** tab:

> **Note:** Metrics are hypervisor-dependant, and might not be available on all hypervisors.

Table 61: Metrics Tab Fields

Metric	Description
Usage	
Controller IOPS	Displays the graph for total I/O operations per second (IOPS) for the controller.
Controller Read IOPS	Displays the graph for Read I/O operations per second (IOPS) for the controller.
Controller Write IOPS	Displays the graphs for Write I/O operations per second (IOPS) for the controller.
Controller AVG I/O Latency	Displays the graph for average latency of total I/O operations (in milliseconds) for controller
Controller AVG Read I/O Latency	Displays the graph for average latency of Read I/O operations (in milliseconds) for controller
Controller AVG Write I/O Latency	Displays the graph for average latency of Write I/O operations (in milliseconds) for controller
Controller I/O Bandwidth	Displays the graph for total I/O bandwidth used per second (MBps or KBps) by controller.
Controller Read I/O Bandwidth	Displays the graph of bandwidth used per second (MBps or KBps) for Read I/O operations by controller
Controller Write I/O Bandwidth	Displays the graph of bandwidth used per second ((MBps or KBps) for Write I/O operations by controller.

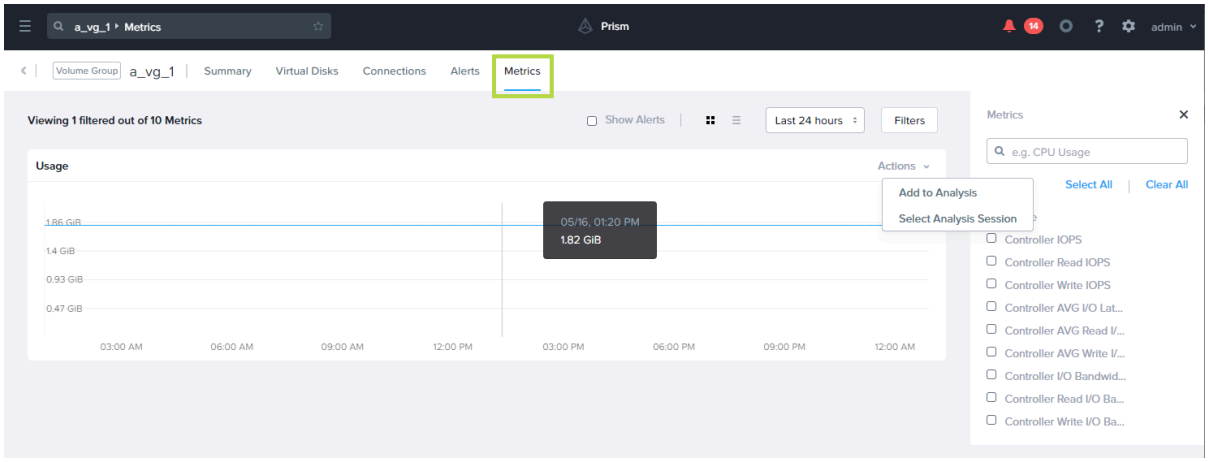


Figure 147: Metrics Tab

Creating a Volume Group

This section describes how to create a volume group in Prism Central.

Procedure

To create a volume group, perform the following steps:

1. Log in to Prism Central.

2. Select **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Volume Groups** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default with all the volume groups across registered clusters.

3. Click **Create Volume Group**. The system displays the **Create Volume Group** window - **Configuration** step.

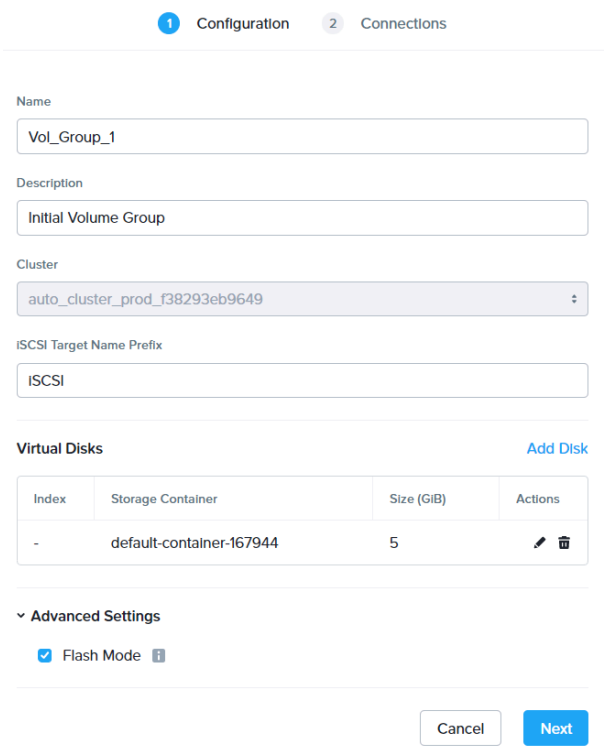


Figure 148: Create Volume Group: Configuration Step

a. In the **Configuration** step, perform the following actions:

- **Name**: Enter a name for the volume group.
- **Description**: Enter an optional description for the volume group.
- **Cluster**: Select the cluster from the dropdown menu in which you want to create the volume group.

  The list includes all clusters registered with the Prism Central.
- **iSCSI Target Name Prefix**: Enter the iSCSI target name prefix.
- **Virtual Disks**: Click **Add Disk**. In the **Add Virtual Disk** window, select the target storage container from the **Storage Container** dropdown menu, enter the disk size (in GiBs) in the **Size** field, and then click **Add**.

  The following is an example showing the **Add Virtual Disk** window:

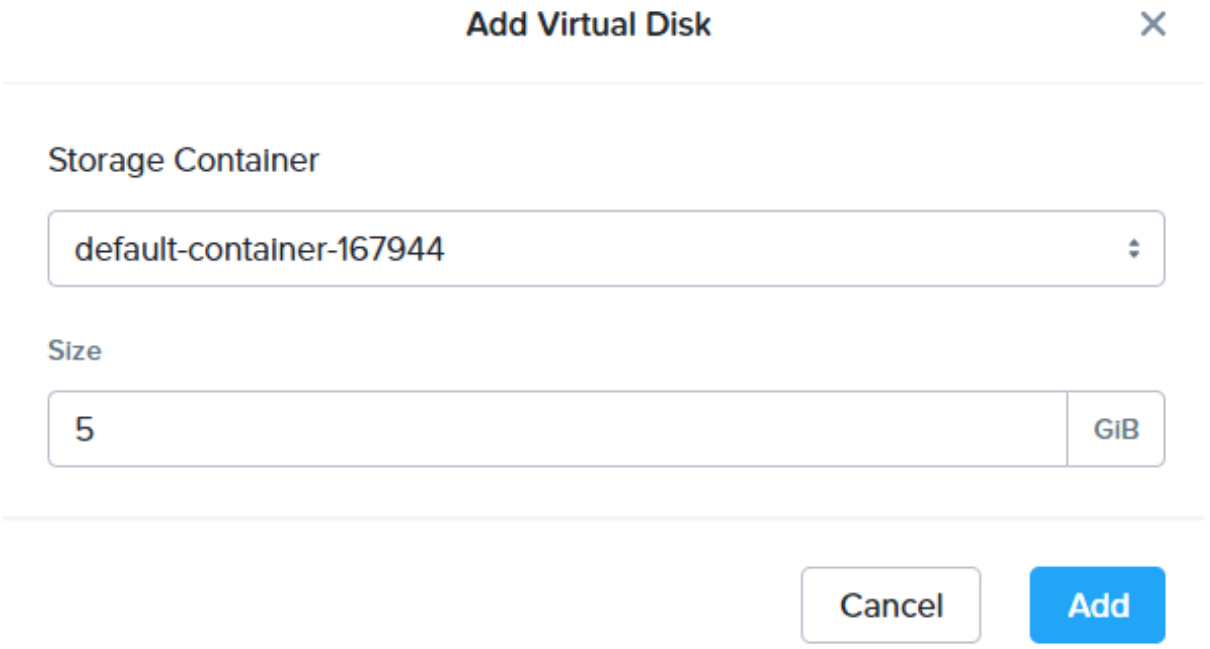


Figure 149: Add Virtual Disk Window

Repeat this action to add additional disks.

To edit or delete a disk, click Edit icon or Delete icon available under **Actions** column.

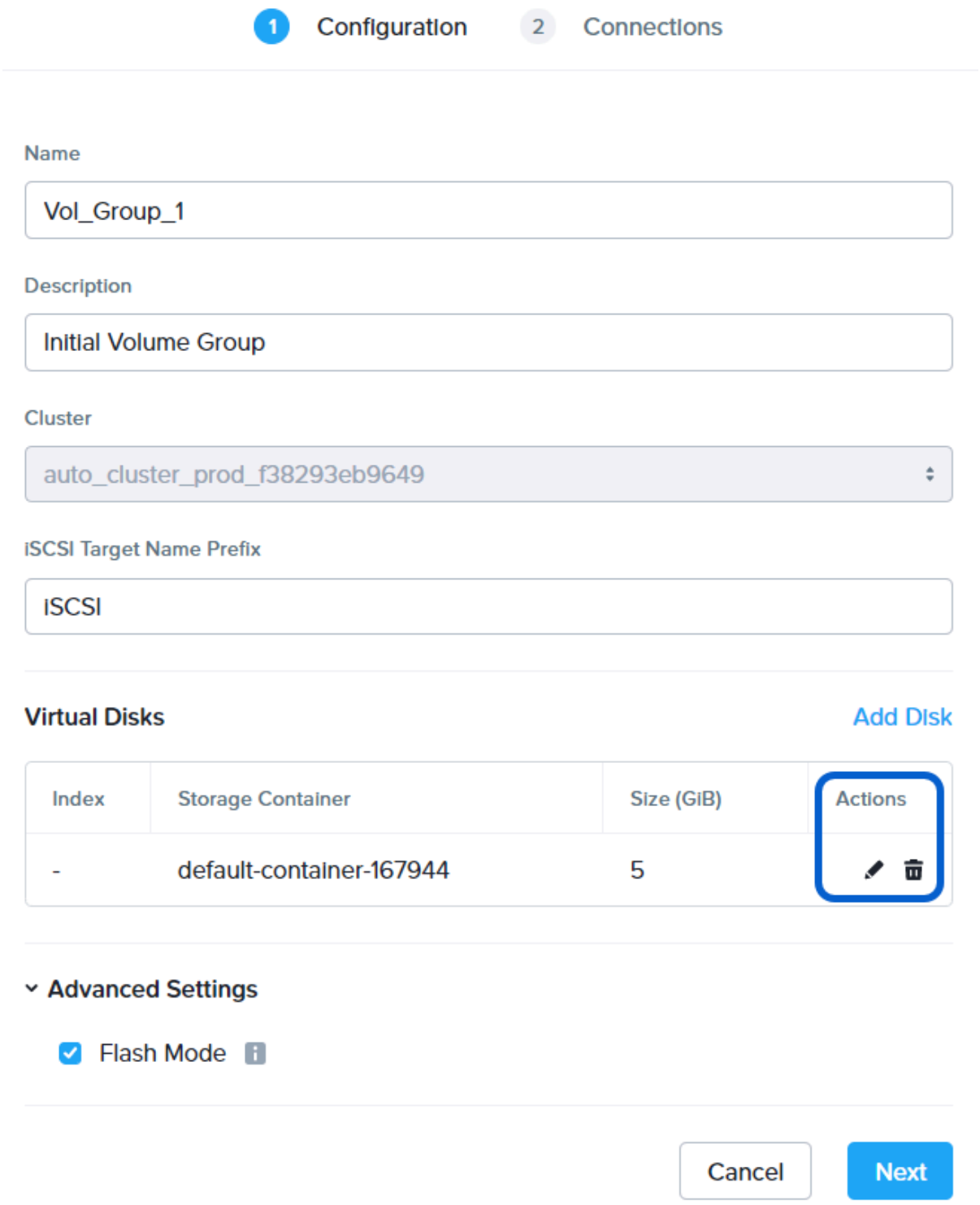


Figure 150: Edit Virtual Disk window

- **Advanced Settings** (optional): Select the **Flash Mode** checkbox to ensure no down migration of data occurs from the flash tier.

b. Click **Next**. The system displays the **Connections** step in **Create Volume Group** window.

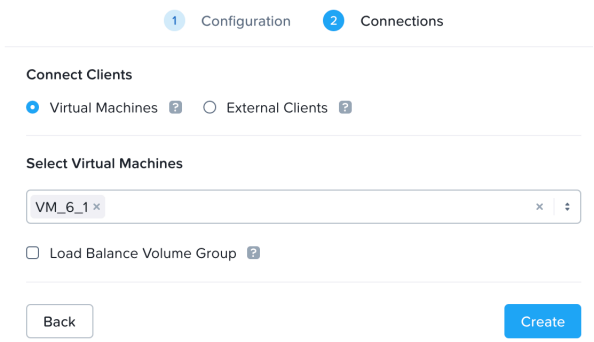


Figure 151: Connections - Virtual Machines

c. In the **Connections** step, perform the following actions:

- **Connect Clients**: Select either of the following options based on your requirement:
  - **Virtual Machines** - Allows you to configure direct attachment to VMs on the same cluster. If you select this option, set the following attributes:
    - **Select Virtual Machines**: Select one or more VMs using the dropdown menu.
    - (Optional) **Load Balance Volume Group**: Select the checkbox to enable load balancing between the selected VMs. Virtual disks in the volume group are evenly distributed between the CVMs instead of being hosted locally.

      Note: You cannot change the load balance configuration once you attach the VMs.
  - **External Clients** - Allows you to configure access to external clients or clients not residing on the same cluster.

    The following is an example showing the **External Clients** selection window:

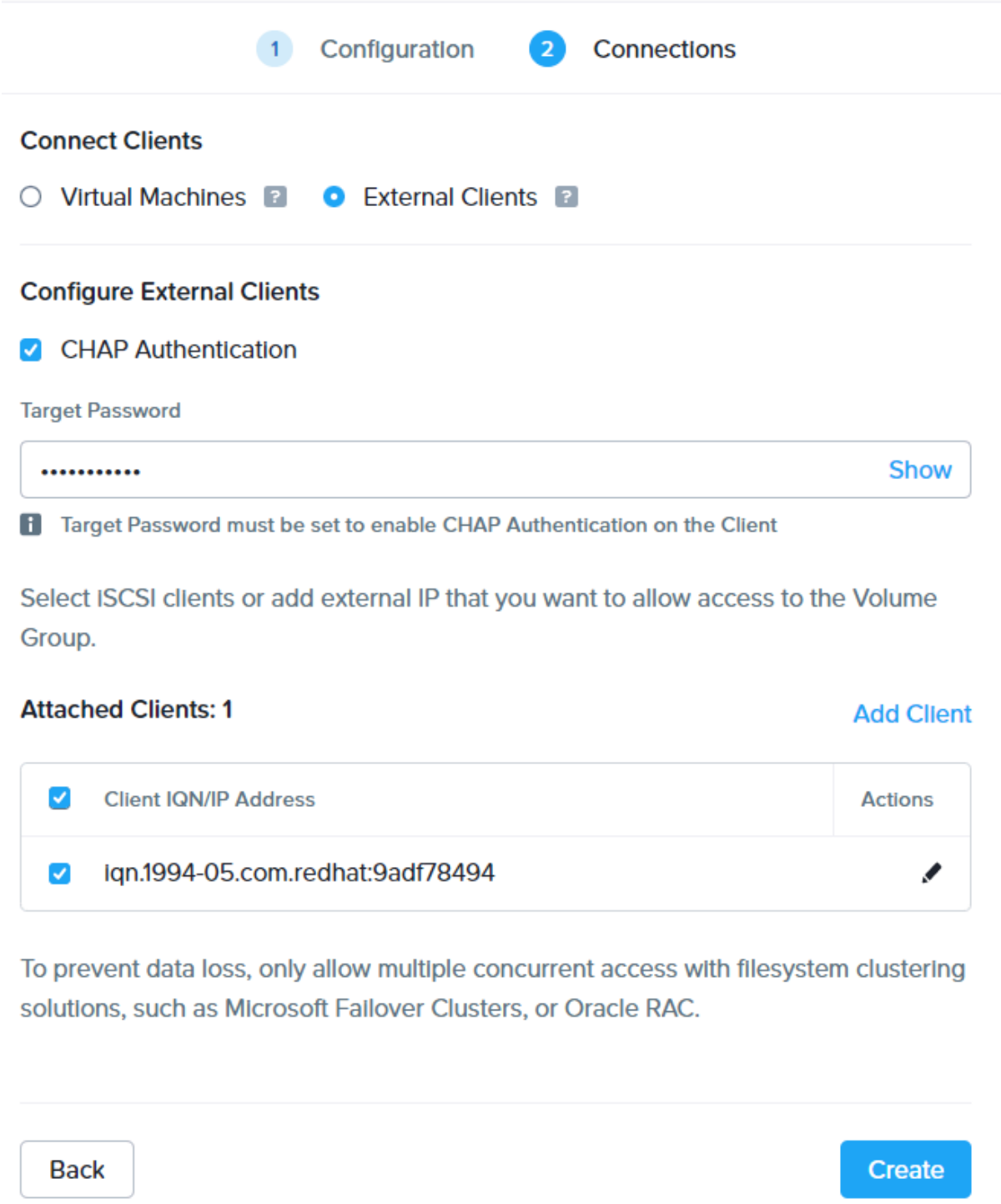


Figure 152: Connections - External Clients

If you select this option, set the following attributes:

- **Configure External Clients**: Select the **CHAP Authentication** checkbox to enable the Challenge Handshake Authentication Protocol (CHAP) on the external client, and enter the target password in the indicated field.

- **Attached Clients**: Configure the external clients as desired. The configured clients appears in a table.
  - To attach (detach) a client, select (clear) the box for that client in the table.
  - To add a client, click the **Add Client** link. In the **Add External Client** window, enter the client IP address or IQN designator name in the **Client IQN/IP Address** field, select the **CHAP Authentication** checkbox , and enter password in the **Client Password** field, and then click **Add**. The added client appears in the table.
  - To update a client, click the Edit icon for that client in the table. The **Edit External Client** window appears. Select (clear) the checkbox to enable (disable) the CHAP authentication, and then click **Save**.

    Note: The system does not allow you to change the client IQN/IP address.

d. Click **Create**.

Modifying a Volume Group

This section describes how to modify volume groups from the Prism Central web console.

About this task

You can perform the following actions to modify the volume groups from the Prism Central web console.

- Update the volume group settings.
- Delete the volume group
- Manage volume group connections.
- Manage volume group virtual disks.
- Manage volume group categories
- Configure mutual CHAP authentication.
- Attach volume groups to guest VMs.
- Manage the following operations related to Nutanix Disaster Recovery setup.
  - Protect the volume group.
  - Create recovery points for the volume group.
  - Add volume group or volume group category to a recovery plan.

  For more information about the operations related to Nutanix Disaster Recovery setup, see Nutanix Disaster Recovery Guide.

Procedure

To modify a volume group, perform the following steps:

1. Log in to the Prism Central web console.
2. Select **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Volume Groups** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default with all the volume groups across registered clusters.

3. Select the target volume group checkbox, and click **Update**. The system displays the **Update Volume Group** window - **Configuration** step.

4. Modify the volume group settings as required in **Configuration** and **Connections** steps, and click **Save**. For field details, see Creating a Volume Group on page 314.

   To delete a volume group, you can select the target volume group and choose **Delete** from the **Actions** dropdown menu.

   > **Note:** If there are active connections, you must first remove the connections before deleting the volume group.

   You can perform the following actions to manage connections, virtual disks, and categories associated with the volume group:

   - To only update volume group connections, you can select the target volume group checkbox, and choose **Manage Connections** from the **Actions** dropdown menu. For field details, see Creating a Volume Group on page 314.

     The following is an example showing the **Manage Connections** window:

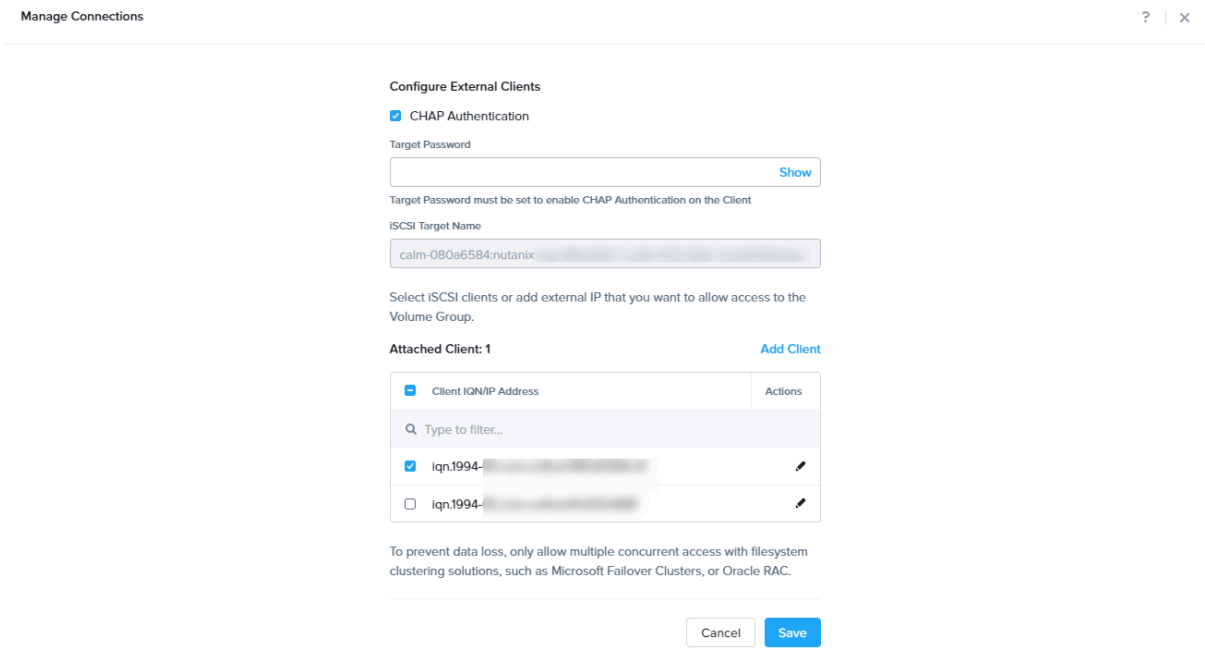


Figure 153: Manage Connections Window - Volume Group

   - To only add, update and remove volume group connections, navigate to **Connections** tab of the target volume group from Volume Group Details View on page 306 , and perform the following action:

     - Click **Add Connection** to add a volume group connection.
     - Select the target volume group connection, and click **Update** to update the volume group connection.
     - Select the target volume group connection, and click **Remove** to delete the volume group connection.

     For field details, see Creating a Volume Group on page 314.

- To only update, add, and remove virtual disks attached to a volume group, navigate to **Virtual Disks** tab of the target volume group from Volume Group Details View on page 306, and perform the following actions:

  - Click **Add Virtual Disk** to add a virtual disk to the volume group.
  - Select the target volume group virtual disk, and click **Update** to update the volume group virtual disk.
  - Select the target volume group virtual disk, and click **Delete** to delete the volume group virtual disk.

  For field details, see Creating a Volume Group on page 314.

- To update volume group categories, you can select the target volume group checkbox, and choose **Manage Categories** from the **Actions** dropdown menu.

  In **Manage Categories** window, perform the following steps:

  1. Use the Add icon and Remove icon available under **Set Categories** field to add or remove the categories for the selected volume group
  2. Click **Save**.

  For information about how to create a volume group category, see Creating a Category on page 457.

Configuring Mutual CHAP Authentication

About this task

You must set the CHAP secret password in the Prism Central web console and then set the same password in the guest VMs hosting your initiators. It is important to use the same password as the target CHAP password; otherwise, the target CHAP password changes, and VM clients connecting to the target experience a loss of connectivity (in both clustered and non-clustered applications).

To set up mutual CHAP authentication in the Prism Central web console, do the following.

Procedure

1. Log in to the Prism Central web console.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute & Storage** > **Volume Groups** from the **Navigation Bar**.
3. Select a volume group to configure CHAP authentication and click **Update**.
4. In the **Connections** tab, select **CHAP Authentication**, enter the **Target Password** and then click **Save**.
5. Go to the **List** tab under **Compute & Storage** > **Volume Groups** and from the **View by** drop-down menu, select **General**.
6. Click the volume group and do the following under the **Connections** tab.
   a. Select the iSCSI client and click **Update** on the top.
   b. In the **Edit Connections** window, select **CHAP authentication** and enter the **Client Password**.

   Note: The client password must be different from the target password, and length should be between 12 and 16 characters.

What to do next

Log in to the guest VM and configure CHAP on it. To set up mutual CHAP authentication in the Windows guest VMs, see Configuring CHAP Authentication in the *Volumes Guide*.

When you update the target password on the volume group, ensure that you update the associated recovery plan also with the new target password. If you do not update the new target password in the recovery plan, the new target password on the volume group is not retained after the failover.

Attaching Volume Groups to Guest VMs

Procedure

1. Log in to the Prism Central web console.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute & Storage** > **Volume Groups** from the **Navigation Bar**.
3. Select the volume group and click **Manage Connections** from the **Actions** drop-down menu.
4. To connect different clients for clustered applications to synchronously replicated volume groups, click **Connect different clients**.

   Note: Clustered applications generally span over Nutanix clusters. Therefore, for volume groups protected with synchronous replication, you should have more external clients on the primary or the replicated volume groups.

5. Select the IQN or the IP Address of the volume groups you want to attach.
6. Click **Save**.

   Note: Alternatively, you can select the volume group, click **Update** from the **Actions** drop-down menu, and then click **Connect different clients** to attach the clients to the replicated volume groups.

   You can use the **Primary** and **Replicated** tabs in the **Update Volume Groups** page to connect an external client either with the primary instance or the replicated instance of the Volume Group. Thus, you can switch between **Primary** and **Replicated** tabs for client connections.

   Attaching a Guest VM to a volume group protected with a synchronous replication schedule.

   Select external clients and attach them using the add client option.

   In the **Add External Client** window, add the Client IQ or IP address and, if necessary, the CHAP authentication client password.

   The volume groups are connected to the guest VM. To view the connected volume groups, go to the **List** tab under **Compute & Storage** > **Volume Groups** and then select General from the **View by** drop-down menu on the right.

   For both the primary and dormant volume group attachment, log on to the guest VM, discover the iSCSI targets, and establish connections. To complete the iSCSI connections, refer to Windows Clients or Linux Clients.

Cluster RBAC for Volume Group

Cluster role-based access control (RBAC) for Volume Group feature enables a super-admin user to provide Prism Admin and Prism Viewer roles access to one or more clusters registered with Prism Central. A user with a Prism Admin role can view and update the entities like volume groups, virtual disks, and storage containers from the allowed clusters. However, a user with a Prism Viewer role can only view the entities.

Cluster RBAC is currently supported on an on-prem Prism Central instance hosted in a Prism Element cluster running AHV. After you enable the Micro Services Infrastructure feature on Prism Central, the Cluster RBAC feature is then automatically enabled.

Cluster RBAC for Volume Group feature is supported on AHV and ESXi clusters.

> **Note:** Prism Central supports Cluster RBAC for VG feature from PC.2022.6 release.

Table 62: List of Permissions for Prism Admin and Prism Viewer Roles

Role	Privileges
Prism Admin	Full administrator privileges except for creating or modifying the user accounts
Prism Viewer	View-only privileges

For information about how to configure cluster RBAC for volume group, see Configuring Cluster RBAC for Volume Group information in *Security Guide*.

External vCenter Server Integration

The VM management through Prism Central for ESXi provides a unified management interface for all of the external vCenter server instances. All the external vCenter server instances that are registered or not registered with any of the clusters are auto-discovered and displayed. If you have not registered the external vCenter server in Prism Element, you can register the clusters to the external vCenter server instances directly from Prism Central.

During the registration process, you have an option to select the ESXi clusters that you want to manage using Prism Central. For more information about registering external vCenter server, see Registering External vCenter Server (Prism Central) on page 336. After you successfully register external vCenter server instances, you can perform the following operations directly from Prism Central.

- Create, clone, update, and delete VMs.
- Create and delete NICs.
- Attach and delete disks.
- Power operations: Power on or off, reset, suspend, resume.
- Open and launch VM console.
- Enable and disable NGT.

> **Note:** Managing VMware guest tools is not supported through Prism Central.

> **Note:**
>
> - You can perform the power operations and launching of VM console even when external vCenter server is not registered.
> - If you are creating VM through Prism, configuration changes to the VM when it is powered on is enabled by default and it depends on the guest operating system that is deployed on the VM.

Rules and Guidelines

- Ensure that all the hosts in the cluster are managed by a single external vCenter server.
- Ensure that DRS is enabled on all the external vCenter server instances.
- Ensure that you are running ESXi and external vCenter server 5.5 or later releases.
- Ensure that you have homogeneous network configuration for all the external vCenter server instances. For example, network should have either 1G or 10G NICs.
- Ensure that you unregister the external vCenter server from the cluster before changing the IP address of the external vCenter server. After you change the IP address of the vCenter Sever, you must register the external vCenter server again with the new IP address.
- The **vCenter Registration** page displays the registered vCenter Server. If for some reason the **Host Connection** field changes to *Not Connected*, it implies that the hosts are being managed by a different external vCenter server. In this case, there will be new vCenter entry with host connection status as Connected and you need to register to this external vCenter server. For more information about registering external vCenter server again, see Managing External vCenter Server Registration Changes (Prism Central) on page 340.

  Caution: If multiple external vCenter servers are managing the hosts of a single Nutanix cluster, you will not be able to perform the VM management operations. Move all the hosts into one external vCenter server.

Requirements and Limitations

- The E1000, E1000e, PCnet32, VMXNET, VMXNET 2, VMXNET 3 network adapter types (NICs) are supported.
- Only SCSI and IDE disks are supported. SATA and PCI disks are not supported.
- Creating a VM by using a template is not supported.
- Creating a VM by using image service is not supported.
- If a VM is deleted, all the disks that are attached to the VM get deleted.
- Network configuration (creation of port groups or VLANs) is not supported.

External vCenter Datastores Summary View

The **Summary** tab on the **External vCenter Datastores** page provides a dashboard of external vCenter datastores across registered vCenter instances.

To access the summary view of all external vCenter datastores, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **External vCenter Datastores** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The system displays the **Lists** tab by default.

3. Click the **Summary** tab.

   The system displays the **Summary** view of all the external vCenter datastores in the registered external vCenter server:

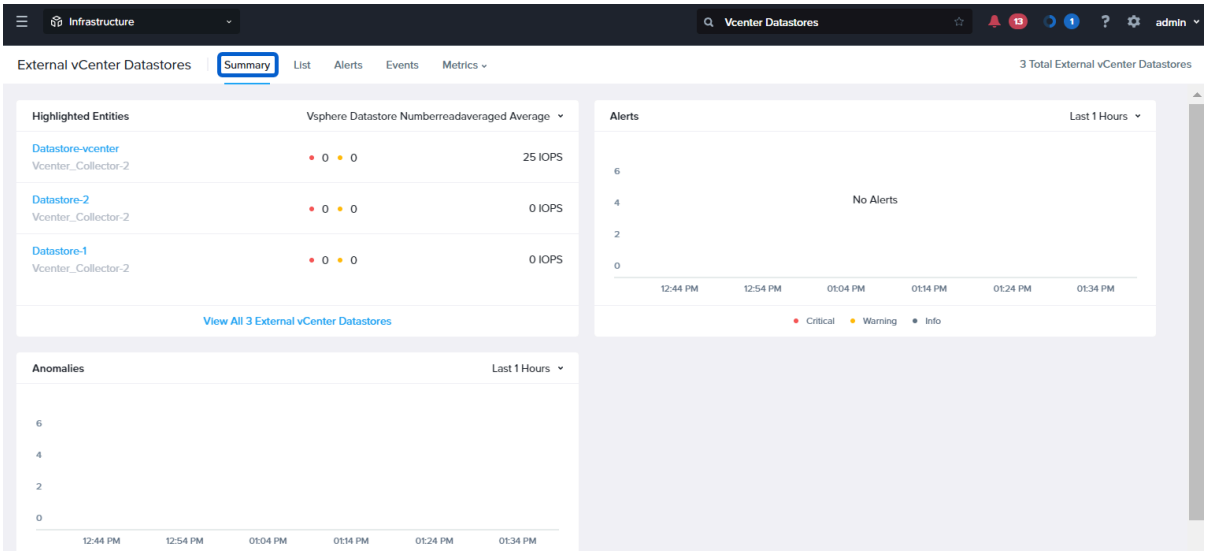


Figure 154: Summary View - All External vCenter Datastores

The **External vCenter Datastores** page includes five tabs on the left (**Summary**, **List**, **Alerts**, **Events**, and **Metrics**) with a display area below the selected tab.

> **Note:** This section describes the information and options that appear in the **Summary** page for all external vCenter datastores. For instructions about how to view and organize that information in various ways, see Prism Central GUI Organization on page 27.

The **Summary** tab for all external vCenter datastores displays the following three widgets:

- **Highlighted Entities**: Displays a list of the external vCenter datastores with the highest usage of the *<parameter>* you select from the dropdown menu on the right of the widget. The *<parameter>* involves only **vSphere Datastore Numberreadaveraged Average**. Click **View All XX External vCenter Datastores** link at the bottom to display the **List** tab.
- **Alerts**: Displays a list of external vCenter datastore-related alerts that are generated during the specified *<interval>* you select from the dropdown menu on the right of the widget. The *<interval>* involves **Last week**(default), **Last 24 hours**, and **Last 1 hour**. When an alert appears, you can click the graph to view a list of those alerts. Click any alert to display the details page for that alert.
- **Anomalies**: Displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified *<interval>* you select from the dropdown menu on the right of the widget. The *<interval>* involves **Last week**(default), **Last 24 hours**, and **Last 1 hour**. When an anomaly appears, you can click the graph to view a list of those anomalies. Click any anomaly to display the event page for that anomaly.

List Tab

The **List** tab displays the list of external vCenter datastores across all clusters.

To access the **List** tab of all external vCenter datastore:

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **External vCenter Datastores** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The system displays the **List** tab by default with external vCenter datastore across all the registered clusters.

   Note: You can use the **View by** and **Group by** options to create your own customized view and add the necessary columns to that view. For more information on how to **View by** and **Group by** options, see Prism Central GUI Organization on page 27.

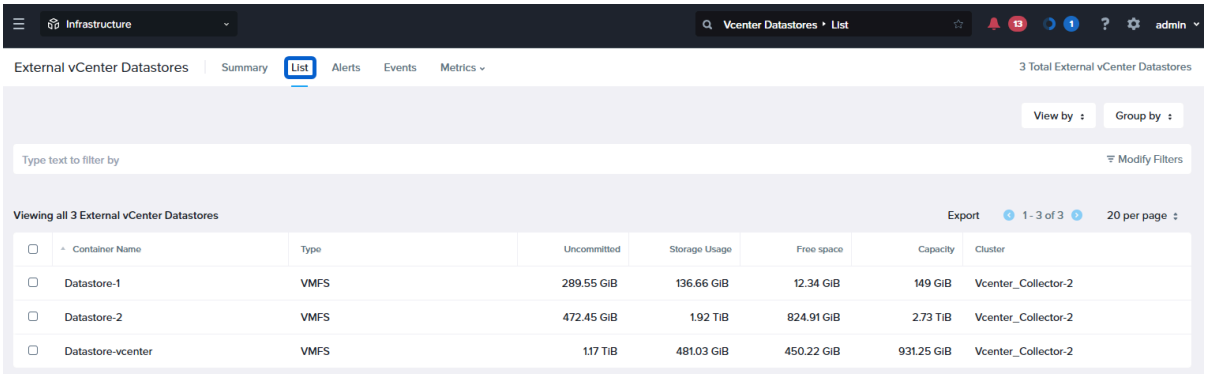


Figure 155: External vCenter Datastores - List Tab

The following table describes the fields that appear in the external vCenter datastore **List** tab.

Note: The fields vary based on the **View by** and **Group by** options. A dash (-) is displayed in a field when a value is not available or applicable. For more information about **View by** and **Group by** options, see Prism Central GUI Organization on page 27.

Table 63: External vCenter Datastores List Tab - Field Description

Field	Description	Values
Container Name	Displays the name of the datastore container. You can click the container name to view the detailed information for that container. For more information about datastore container details view, see External vCenter Datastore Details View on page 332.	(container name)
Type	Displays the file system type.	VMFS, NFS
Uncommitted	Displays the amount of uncommitted disk space.	xx [GiB|TiB]
Storage Usage	Displays the amount of used storage space.	xx [GiB|TiB]
Free Space	Displays the amount of free storage space.	xx [GiB|TiB]
Capacity	Displays the total amount of storage capacity.	xx [GiB|TiB]
Cluster	Displays the name of the cluster in which the datastore resides.	(cluster name)

You can perform the following actions for the external vCenter datastores in the **Lists** tab:

- Access the detailed information about an individual external vCenter Datastore. For details, see External vCenter Datastore Details View on page 332.
- Filter the external vCenter datastores list based on available parameter values using **Filters** pane. For more information about **Filters** pane, see Filters Pane - External vCenter Datastores Page on page 330.
- Export the table that contains the list of external vCenter datastores and their information to a file in a CSV format. For more information about **Export** option, see Export on page 32.
- Group the external vCenter datastores based on pre-defined criteria. For information about how to group the external vCenter datastores, see Group by on page 29.
- View external vCenter datastores based on pre-defined criteria or create a custom view. For information about available views and how to create a custom view, see View by on page 29.

Filters Pane - External vCenter Datastores Page

The following table describes the fields available in the **Filters** pane:

Table 64: Filter Pane Fields

Parameter	Description	Values
Container Name	Filters based on the container name. Select a condition from the dropdown menu and enter a string in the field. The system returns a list of containers that satisfy the container name condition/ string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	(name string)
Cluster	Filters on the cluster name. Enter a string in the field to display a list of clusters that satisfy the name string.	(cluster name)
Storage Usage	Filters on the amount of used storage space. Check the box(es) for the desired range or enter a range in the "**from <low> to <high> TiB**" field. The number of containers in each range is displayed on the right of the line.	([xx] to [yy] range)
Capacity	Filters based on the amount of total storage capacity.	([xx] to [yy] range)
Free Space	Filters based on the amount of free storage space.	([xx] to [yy] range)
Uncommitted	Filters based on the amount of uncommitted storage space.	([xx] to [yy] range)
Type	Filters based on file system type.	VMFS, NFS

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options that are available on the **Activity** > **Alerts** page, however it only displays the vCenter Datastore-related alerts

across the registered clusters. For more information about alerts, see *Prism Central Alerts and Events Reference Guide*.

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options that are available on the **Activity** > **Events** page, however it only displays the vCenter Datastore-related events across the registered clusters. For more information about events, see *Prism Central Alerts and Events Reference Guide*.

Metrics Tab

The **Metrics** tab allows you to view performance metrics across the external vCenter datastores. Click the **Metrics** tab to display dropdown menu of available metrics, and select the metric name to display the relevant performance information.

> **Note:** The **Metrics** dropdown menu is hypervisor-specific, and might vary based on the hypervisors used in the cluster.

The following is an example showing the dropdown menu of the **Metrics** tab:

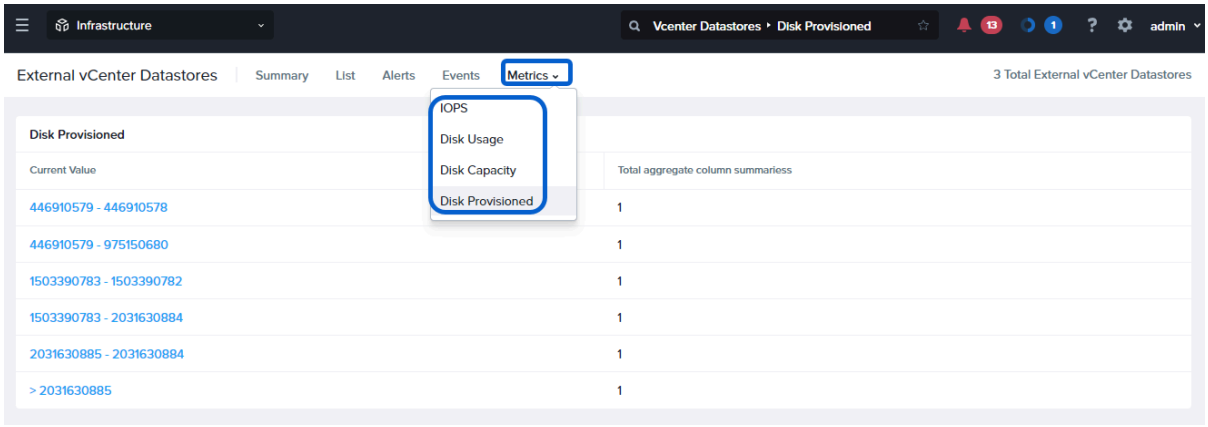


Figure 156: External vCenter Datastores Metrics Tab

The following table describes the dropdown menu of the **Metrics** tab:

Table 65: Metrics Tab Dropdown Menu

Metric	Description
IOPS	Displays the number of read and write IOPS for the listed number of containers. You can click the IOPS value to view the **Summary** tab with a filtered list of containers for the selected IOPS value. The **Total aggregate column summaries** field displays the number of containers for which the IOPS value is applicable.
Disk Usage	Displays the disk usage amount for the listed number of containers. You can click the disk usage amount to view the **Summary** tab with a filtered list of containers for the selected disk usage amount. The **Total aggregate column summaries** field displays the number of containers for which the disk usage value is applicable.

Metric	Description
Disk Capacity	Displays the disk capacity for the listed number of containers. You can click the disk capacity to view the **Summary** tab with a filtered list of containers for the selected disk capacity. The **Total aggregate column summaries** field displays the number of containers for which the disk capacity value is applicable.
Disk Provisioned	Displays the provisioned disk space for the listed number of containers. You can click the provisioned value to view the **Summary** tab with a filtered list of containers for the selected provisioned value. The **Total aggregate column summaries** field displays the number of containers for which the disk provisioned value is applicable.

External vCenter Datastore Details View

Summary Tab

The **Summary** tab of an individual external vCenter datastore consists of a dashboard that provides the detailed information about the external vCenter datastore.

To access the **Summary** tab of an individual external vCenter datastore:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Storage Container** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   By default, the system displays the **List** tab with external vCenter datastores across all the registered clusters.
3. Click the target <*vCenter_Datastore_Name*> to view the **Summary** tab of an individual external vCenter datastore.

> **Note:** Replace <*vCenter_Datastore_Name*> with the actual external vCenter datastore name at your site.

The following is an example showing the **Summary** tab of an individual external vCenter datastore:

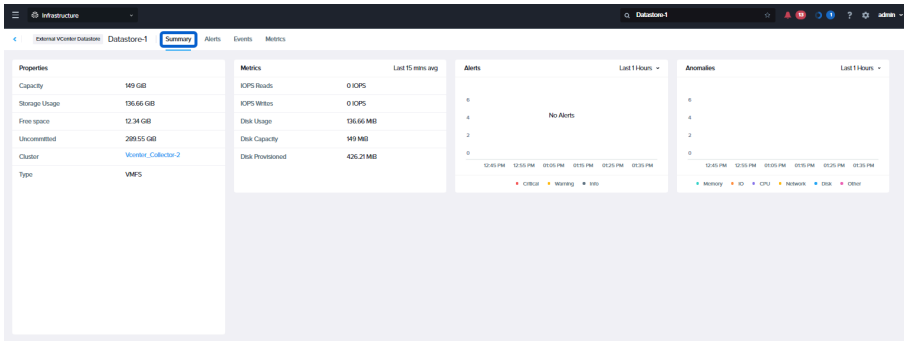


Figure 157: Summary Tab - Individual External vCenter Datastore

The **Summary** tab of an individual external vCenter datastore provides the following widgets:

- **Properties** - Displays summary information about the external vCenter datastore. For information about the fields available in **Properties** widget, see External vCenter Datastore Widgets - Parameter Details on page 333.
- **Alerts**- Displays a list of related alerts that occurred during the specified interval. Select either **Last week** (default), **Last 1 hour** or **Last 24 hours** from the dropdown menu on the top right corner of the widget.
- **Anomalies** - Displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified interval. Select either **Last week** (default), **Last 1 hour** or **Last 24 hours** from the dropdown menu on the top right corner of the widget. When an anomaly appears, you can click the graph to display a list of those anomalies. If you click an individual anomaly, the system displays the event page for that anomaly.
- **Metrics** - Displays the average metrics information for **Last 15 minutes avg** for the external vCenter datastore (container) that includes **IOPS Read**, **IOPS Writes**, **Disk Usage**, **Disk Capacity**, and **Disk Provisioned** fields. For information about the fields available in **Metrics** widget, see External vCenter Datastore Widgets - Parameter Details on page 333.

External vCenter Datastore Widgets - Parameter Details

The following table describes the fields in the **Properties** and **Metrics** widgets. A dash (-) in a field indicates that there is not enough data to evaluate or a value is not assigned. The displayed fields vary by hypervisor.

Table 66: External vCenter Datastore Widgets - Field Description

Field	Description	Values
Properties widget		
Capacity	Displays the total amount of storage capacity.	xx [GiB|TiB]
Storage Usage	Displays the amount of used storage space.	xx [GiB|TiB]
Free Space	Displays the amount of free storage space.	xx [GiB|TiB]
Uncommitted	Displays the amount of uncommitted disk space.	xx [GiB|TiB]
Cluster	Displays the name of the cluster in which the datastore resides. Click on the cluster name to displays details about that cluster.	(cluster name)
Type	Displays the file system type.	VMFS, NFS
Metrics widget		
IOPS Reads	Displays the average number of read IOPS for the selected container in last 15 minutes.	Integer (IOPS)
IOPS Writes	Displays the average number of write IOPS for the selected container in last 15 minutes.	Integer (IOPS)
Disk Usage	Displays the average disk usage amount for the selected container in last 15 minutes.	Integer (MiB)
Disk Capacity	Displays the total disk capacity for the selected container.	Integer (GiB)

Field	Description	Values
Disk Provisioned	Displays the average provisioned disk space for the selected container in last 15 minutes.	Integer (MiB)

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options as the Alerts dashboard, however it is filtered to display the alerts only for the selected external vCenter datastore (individual external vCenter datastore). For more information about alerts, see *Prism Central Alerts and Events Reference Guide*.

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options as the Events dashboard, except it is filtered to display just events for this external vCenter datastore. For more information about events, see Prism Central Alerts and Events Reference Guide.

Metrics Tab

The **Metrics** tab allows you to view usage metrics for the external vCenter datastore. Click the **Metrics** tab to view graphs for all the metrics. The graph is a rolling time interval performance or usage monitor. The baseline range appears as a blue band in the graph.

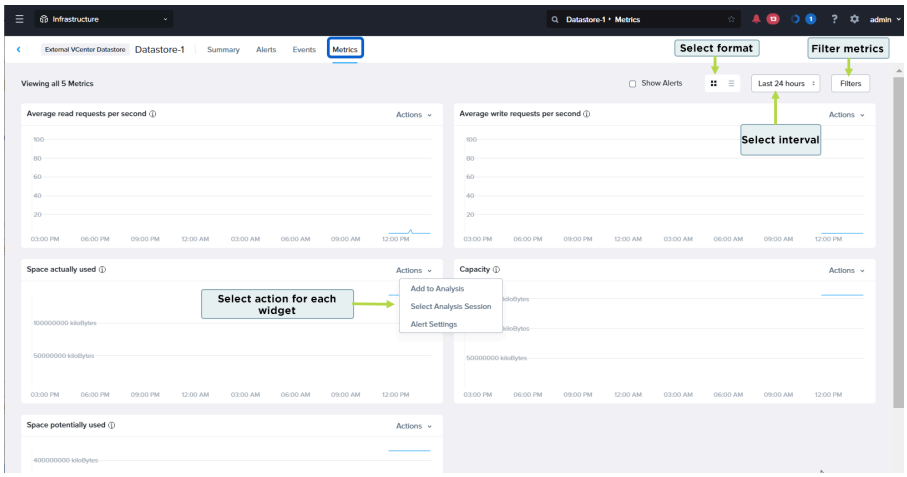


Figure 158: Metrics Tab

Note: The baseline range and identified anomalies are based on sophisticated machine-learning capabilities. For more information, see Behavioral Learning Tools) in *Intelligent Operations Guide*. The machine-learning algorithm uses 21 days of data to monitor and predict performance. A graph or baseline band may not appear if less than 21 days of data is available.

You can perform the following actions in the **Metrics** tab:

- Place the cursor anywhere on the horizontal axis to display the value at that time.
- Select the duration (time interval) from the dropdown menu on the right (last 1 hour, last 24 hours, last week, last 21 days).

- From the **Actions** dropdown menu that appears on the top-right corner of each metrics widget, you can perform the following operations:
  - Select **Add to Analysis** to add the selected metric to **Analysis** dashboard. For more information, see Analysis Dashboard in *Intelligent Operation Guide*.
  - Choose **Select Analysis Session** to add the metric to an existing or new analysis session. The system displays the **Select A Session** window.

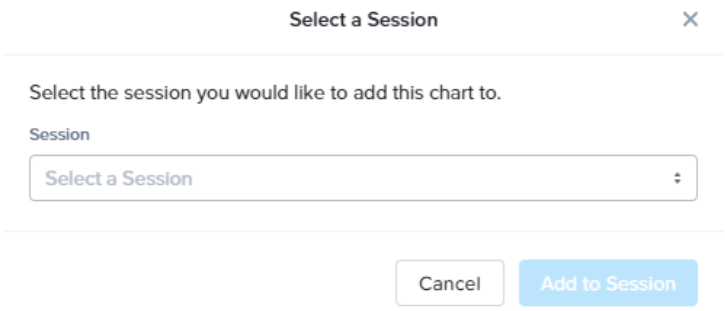


Figure 159: Session Window

    Select the target session from the **Session** dropdown menu, and then click **Add to Session**.
  - Select **Alert Settings** to create a custom alert policy for the metric. For more information about how to create a custom alert policy, see Prism Central Alerts and Events Reference Guide.
- Click the **Filters** option to select one or more appropriate metric checkboxes to display the selected metrics in the **Metrics** page.

The following table describes the metrics available in **Metrics** tab:

> **Note:** Metrics are hypervisor-dependant, and might not be available on all hypervisors.

Table 67: Metrics Tab Fields

Metric	Description
Average read requests per second	Average number of read commands issued per second to the external vCenter datastore during the collection interval.
Average write requests per second	Average number of write commands issued per second to the external vCenter datastore during the collection interval.
Space actually used	Amount of space actually used by the virtual machine or the external vCenter datastore. It might be less than the amount provisioned at any given time, depending on whether the virtual machine is powered-off, whether snapshots have been created or not, and other such factors. Available from a datastore and virtual machine target entities.
Capacity	Configured size of the external vCenter datastore. Available from an external vCenter datastore entity only.

Metric	Description
Space potentially used	Amount of storage set aside for use by an external vCenter datastore or a virtual machine. Files on the external vCenter datastore and the virtual machine can expand to this size, but not beyond it. Available from an external vCenter datastore and virtual machine target entities.

Registering External vCenter Server (Prism Central)

All the external vCenter server instances that are registered to Prism Element are listed in Prism Central. If you do not want to manage your cluster through Prism Central, you have an option to de-select the clusters from Prism Central.

Before you begin

Ensure that you have external vCenter server extension privileges as these privileges provide permissions to perform external vCenter server registration for the Nutanix cluster.

About this task

Important: Observe the following points about registering the external vCenter server with Prism Central:

- Nutanix does not store external vCenter server credentials.
- Whenever a new node is added to a cluster, vCenter Sever registration for the new node is automatically performed.

Procedure

To register an external vCenter server, perform the following steps:

1. Log in to Prism Central.
2. Select **Infrastructure** application from the Application Switcher Function on page 19.

3. Navigate to **Prism Central Settings** > **Setup** > **vCenter Registration** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   You can also click the Settings icon, and navigate to **Setup** > **vCenter Registration**.

   The system displays the **vCenter Registration** page.

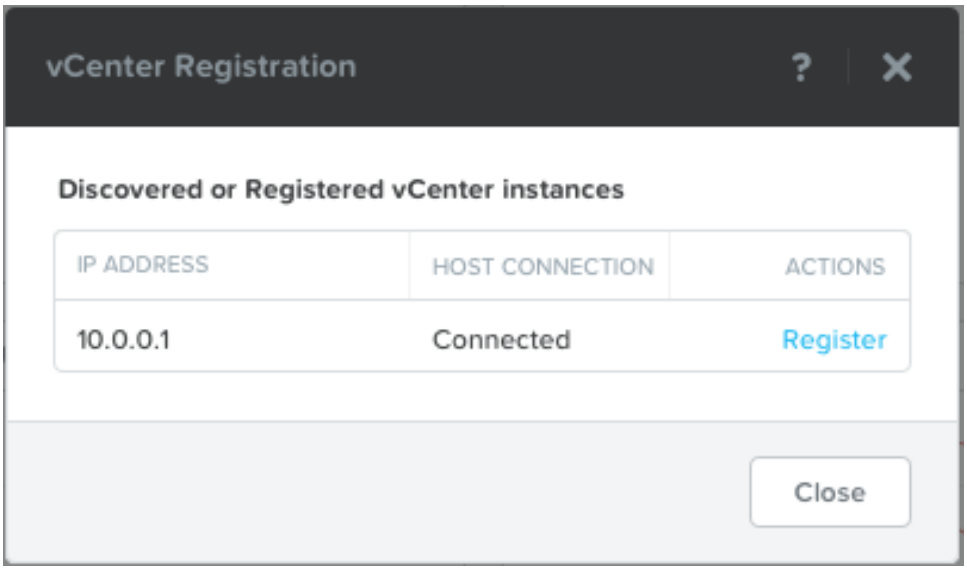


Figure 160: vCenter Registration

- The **vCenter Registration** window lists all the external vCenter server instances that are registered or not registered with the clusters.
- If you have not registered the external vCenter server in Prism Element, you can register the clusters to the external vCenter server instances directly from Prism Central.

4. Click **Register** to register the external vCenter server.

   - The external vCenter server that is managing the hosts in the cluster is auto-discovered and its IP address is auto-populated in the **IP Address** field.
   - The port number field is also auto-populated with 443. Do not change the port number. For the complete list of required ports, see Port Reference.

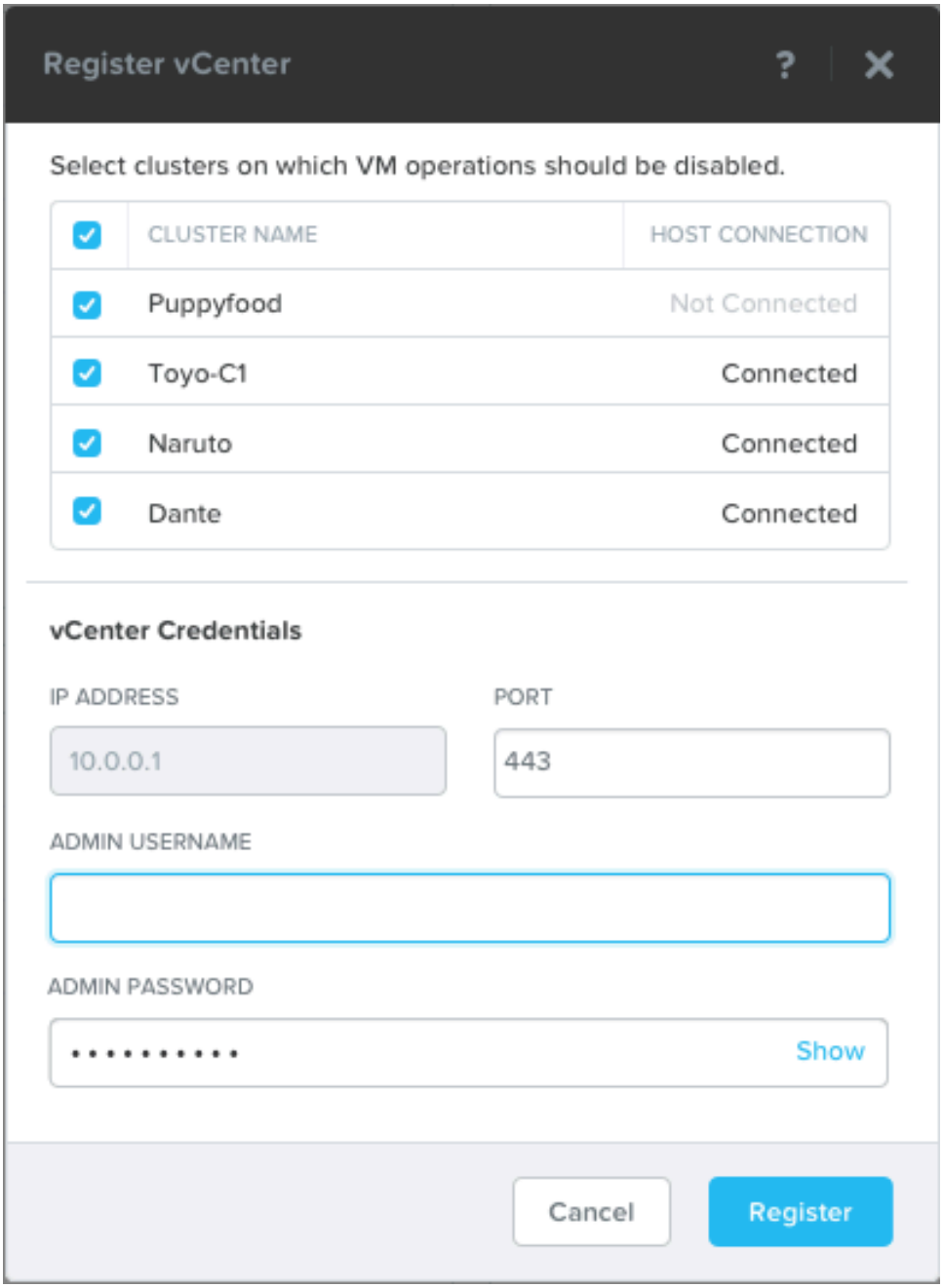


Figure 161: Cluster Selection

5. Specify the following information in the **Register vCenter** window:

   - Select the checkbox(es) of the clusters that you want to manage from Prism Central. You can also clear the checkbox(es) of the clusters that you do not want to manage from Prism Central.
   - Enter the administrator user name and password of the external vCenter server in the **Admin Username** and **Admin Password** fields.

6. Click **Register** to register the external vCenter server in Prism Central with selected clusters.

   During the registration process a certificate is generated to communicate with the external vCenter server. If the registration is successful, a relevant message is displayed in the **Tasks** page. For more information about how to access **Tasks** page, see Tasks View on page 451.

   The system displays the **Host Connection** field as *Connected*, which implies that all the hosts are managed by the registered external vCenter server.

Unregistering a Cluster from the External vCenter Server (Prism Central)

This section describes how to unregister your clusters from the external vCenter server.

About this task

- Ensure that you unregister the external vCenter server from the cluster before changing the IP address of the external vCenter server. After you change the IP address of the vCenter Sever, you should register the external vCenter server again with the new IP address with the cluster.
- The **vCenter Registration** page displays the registered external vCenter server. If the system displays the **Host Connection** field as *Not Connected* for any external vCenter server instance, it implies that the clusters (hosts) are managed from a different external vCenter server. In this case, the system also displays a new external vCenter server instance with **Host Connection** field as *Connected* and you need to register to this external vCenter server instance. For more information about how to reregister a external vCenter server, see Managing External vCenter Server Registration Changes (Prism Central) on page 340.

Procedure

To unregister the cluster from the external vCenter server, perform the following steps:

1. Log in to Prism Central.
2. Select **Infrastructure** application from the Application Switcher Function on page 19.
3. Navigate to **Prism Central Settings** > **Setup** > **vCenter Registration** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   You can also click the Settings icon, and navigate to **Setup** > **vCenter Registration**.

   The system displays the **vCenter Registration** page.
4. Click the Edit icon under **Actions** field, and clear the checkbox(es) of the clusters that you want to unregister from the external vCenter server.
5. Enter the administrator user name and password of the external vCenter server in the **Admin Username** and **Admin Password** fields, and Click **Unregister**.

   If the credentials are correct, the selected clusters are unregistered from the external vCenter server, and a relevant message is displayed in the **Tasks** dashboard. For information about how to access the Tasks dashboard, see Tasks View on page 451.

Managing External vCenter Server Registration Changes (Prism Central)

This section describes how to unregister an existing external vCenter server instance and reregister a new external vCenter server instance.

About this task

> **Important:** After you change the IP address of the vCenter Sever or if the system displays the **Host Connection** field as *Not Connected* , it implies that current external vCenter server is not managing the clusters (hosts). In this case, you must reregister the new external vCenter server instance with Prism Central.

Procedure

To re-register the external vCenter server with Prism Central, perform the following steps:

1. Log in to Prism Central.
2. Select **Infrastructure** application from the Application Switcher Function on page 19.
3. Navigate to **Prism Central Settings** > **Setup** > **vCenter Registration** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   You can also click the Settings icon, and navigate to **Setup** > **vCenter Registration**.

   The system displays the **vCenter Registration** page.
4. Click **Unregister** under **Actions** field to unregister the external vCenter server from Prism Central.
5. Click **Register** to reregister the new external vCenter server instance.

   For more information about how to register a external vCenter server with Prism Central, see Registering External vCenter Server (Prism Central) on page 336.

NETWORK AND SECURITY ENTITIES

You can access the following networking and security entity items from the **Network and Security** entity of the **Infrastructure** application. For information about how to access the entity items available in **Network and Security** entity, see Application-specific Navigation Bar on page 57.

- **Subnets**: This page displays the subnets and the operations you can perform on subnets. For more information, see Subnets on page 341.
- **Virtual Private Clouds**: This page displays the VPCs and the operations you can perform on VPCs. For more information, see Virtual Private Clouds Summary View on page 357.
- **Floating IPs**: This page displays a list of floating IP addresses that you are using in the network. It allows you to request for floating IP addresses from the free pool of I addresses available to the clusters managed by the Prism Central instance. For more information, see Floating IPs Summary View on page 375.
- **Connectivity**: This page allows you to manage the following networking capabilities. For more information, see Connectivity on page 376.
  - **Gateways**: This page provides a list of network Gateways you have created and configured, and the operations you can perform on the network Gateways. For more information, see Gateways Summary View on page 376.
  - **VPN Connections**: This page provides a list of VPN connections you have created and configured, and the operations you can perform on the VPN connections. For more information, see VPN Connections Summary View on page 380.
  - **Subnet Extensions**: This page provides a list of subnets that you have extended at the Layer 2 level using VPN (point-to-point over Nutanix VPN) or VTEP (point-to-multi-point including third party). For more information, see Subnet Extensions Summary View on page 386.
  - **BGP Sessions**: This page provides a list of BGP sessions you have created and configured, and the operations you can perform on the BGP sessions. For more information, see BGP Sessions Summary View on page 391.
- **Security Policies**: This page provides a list of security policies you configured using Flow Segmentation. For more information, see Security Policies on page 395.
- **Security Dashboard**: This page provides dynamic summary of the security posture across all registered clusters. For more information, see Security Dashboard on page 395.

For information about how to configure network connections, see Network Configuration on page 346.

Subnets (Overlay IP subnets), Virtual private clouds, floating IPs, and Connectivity are Flow virtual networking features. These features support flexible app-driven networking that focuses on VMs and applications instead of virtual LANs and network addresses. Flow virtual networking powers network virtualization to offer a seamless network experience with enhanced security. It is disabled by default. It is a software-defined network virtualization solution providing overlay capabilities for the on-premise AHV clusters.

Security policies drives the Flow Segmentation features for secure communications. For more information, see Flow Microsegmentation Guide.

Subnets

You can perform the following actions to manage a subnet from Prism Central.

- Creating a Subnet

- Updating a Subnet
- Deleting a subnet
- Creating a subnet extension
- Assigning a category value to a subnet
- Migrating VMs between VLAN and VPC networks

Subnets Summary View

The **Subnets** page displays the list of subnets across all the registered clusters.

To access the **Subnets** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Network & Security** > **Subnets** from the **Navigation Bar**.

   The **Subnets** page opens displaying the **List** tab. This tab provides information about all the subnets configured for the registered clusters.

   > **Note:** For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

The following table describes the fields that appear in the **Subnets** page.

> **Note:** The fields vary based on the **View by** and **Group by** options. A dash (-) is displayed in a field when a value is not available or applicable. For more information, see the View by on page 29 and Group by information.

Table 68: Subnets – Field Description

Field	Description	Values
Name	Displays the subnet name.	(subnet name)
External Connectivity	Displays whether or not the subnet has external connectivity configured.	(Yes/No)
Type	Displays the subnet type.	VLAN or VLAN`Basic` or Overlay
VLAN ID	Displays the VLAN identification number.	(ID number)
VPC	Displays the name of the VPC in which the subnet is used.	(Name of VPC)
Virtual Switch	Displays the virtual switch that is configured for the VLAN you selected. The default value is the default virtual switch `vs0`. **Note:** The virtual switch name is displayed only if you add a VLAN ID in the VLAN ID field.	(virtual switch name)
IP Prefix	Displays the IPv4 address of the network with the prefix.	(IPv4 Address/Prefix)

Field	Description	Values
Cluster	Displays the name of the cluster for which this subnet is configured.	(cluster name)
Hypervisor	Displays the hypervisor that the subnet is hosted on.	(Hypervisor)

You can perform the following actions from the **Subnets** page:

- Click the name of a subnet to open the subnet details page, which displays the detailed information about the subnet. For more information, see Subnet Details View on page 344.
- Create a subnet by clicking **Create Subnet**. For more information, see Creating a Subnet in the *Flow Virtual Networking Guide*.
- Migrate VMs between VLAN network and VPC network by clicking **Migrate**. For more information, see Migrating VMs between VLAN Backed and VPC Subnets in the *Flow Virtual Networking Guide*.
- Configure network connections for a cluster by clicking **Network Config**. For more information, see Network Configuration.
- Group the subnets based on pre-defined criteria. For more information, see Group by on page 29.
- View subnets based on a pre-defined criteria or create a custom view. For more information, see View by on page 29.
- Filter the subnets list based on a variety of parameter values using the **Filters** pane. For more information, see Filters Pane - Subnets page.
- Perform the following subnet-specific actions on a single or multiple subnets using the **Actions** dropdown menu. The **Actions** dropdown appears when one or more subnets are selected.

Table 69: Subnet Actions

Action	Description
Update	Click this action to update the subnet. For more information, see Updating a Subnet in the *Flow Virtual Networking Guide*.
Extend	Click this action to create a subnet extension. For more information, see Layer 2 Virtual Subnet Extension Over VTEP in the *Flow Virtual Networking Guide*.
Manage Categories	Click this action to associate the subnet with a category or change the categories that the subnet is associated with. For more information, see Assigning a Category on page 459.
Delete	Click this action to delete the subnet. For more information, see Deleting Subnets, Policies, or Routes in the *Flow Virtual Networking Guide*.

Filters Pane - Subnets page

You can filter the information in the **Subnets** page based on the following fields that are available in the **Filters** pane. For information about how to use the Filters pane, see the Filters Pane information.

Table 70: Filter Pane Field Description - Subnets page

Field	Description	Values
Name	Filters based on the subnet name. It returns a list of subnets that satisfy the name condition/string.	(Subnet name string)
External Connectivity	Filters based on whether the subnet has external connectivity configured or not.	(Yes/No)
Type	Filters based on the subnet type.	(VLAN/VLAN (External)/ Overlay
VLAN ID	Filters based on VLAN identification number.	(ID number)
VPC	Filters based on the name of the VPC in which the subnet is used.	(Name of VPC)
Cluster	Filters based on the name of the cluster for which this subnet is configured.	(cluster name)
Hypervisor	Filters based on the hypervisor that the subnet is hosted on.	ESXi/AHV/Hyper-V/XenServer/Mixed Hypervisor/Null Hypervisor

Subnet Details View

The Subnet details page consists of a dashboard that provides the detailed information about the subnet.

The details page has the **Summary**, and **Throughput** tabs.

To access the details page of an individual subnet:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Network & Security** > **Subnets** from the **Navigation Bar**.

   Prism Central displays the **Subnets** page that contains information about all the subnets configured for the registered clusters.
3. Click a subnet to open the details page of the subnet.

   The **Summary** tab opens displaying the detailed information about the subnet in widgets.

> **Note:** For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

Summary Tab

The **Summary** tab provides detailed information about the subnet in widgets. A dash (-) is displayed in a field when a value is not available or applicable.

The **Summary** tab has the following widgets:

Widget Name	Information provided
Properties	Provides the following: • Type — Displays the type of network like VLAN or Overlay. • VLAN ID — Displays the VLAN ID. This parameter is displayed only for VLAN networks. • VPC — Displays the VPC name. This parameter is displayed only for Overlay networks. • Cluster — Displays the cluster that the VLAN network is configured on. This parameter is displayed only for VLAN networks. • IP Address Prefix — Displays the IP address prefix configured for the network. This parameter is displayed for both VLAN and Overlay networks.
IP Address Pools	Provides the following: • The IP address Pool Range assigned to the network. • The total number of used and available IPs in the cluster. • Used IPs in Subnet — Displays the number of used IPs in the subnet. • Used IPs in Pools — Displays the number of used IPs in the pool. • Free IPs in Pools — Displays the number of free IPs in the pool. • Free IPs in Subnet — Displays the number of free IPs in the subnet.
Domain Settings	Provides the following DHCP settings configured for a VM in a subnet: • Domain Name Servers — Displays the total number of DNS IP addresses. • Domain Search — Displays the VLAN domain name. • Domain Name — Displays the domain name. • TFTP Server Name — Displays the name of the TFTP server where you host the host boot file. • Boot File Name — Displays the name of the boot file that the VMs need to download from the TFTP host server.

The **Summary** tab provides the following options, at the top of the page. For more information, see the *Subnet Actions* table in Subnets Summary View on page 342.

- **Update**
- **Extend**
- **Manage Categories**
- **Delete**

Throughput Tab

The **Throughput** tab provides a graphical representation of the throughput of the subnet.

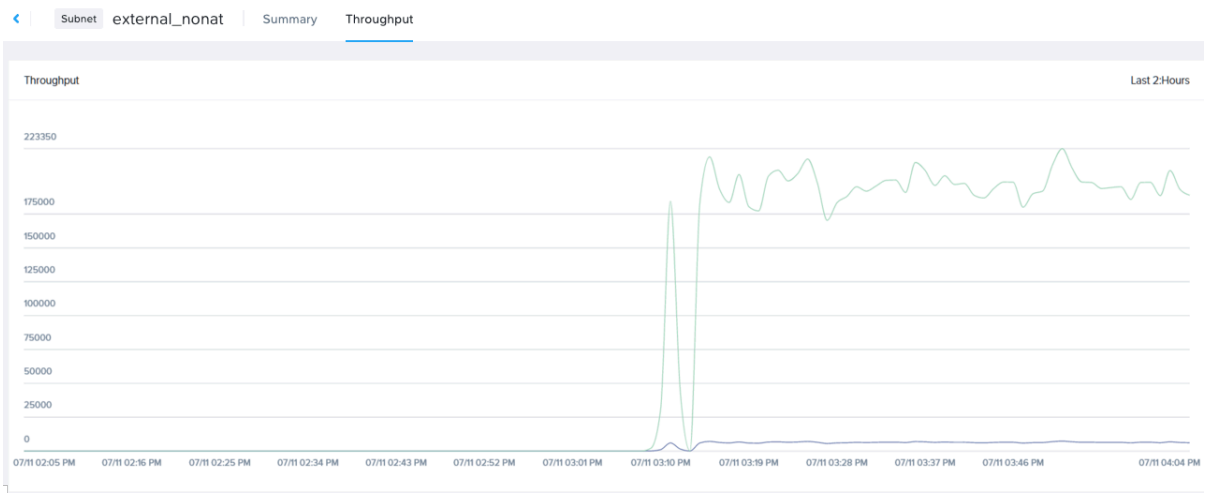


Figure 162: Subnet Details View - Throughput tab sample

Network Configuration

Each VM network interface is bound to a virtual network, and each virtual network is bound to a single VLAN. The **Network Configuration** window displays information about the configured virtual networks.

To access the **Network Configuration** window:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Network & Security** > **Subnets** from the **Navigation Bar**.

   This displays the **Subnets** page.
3. Click **Network Config**.

   This displays the **Network Configuration** window.

The **Network Configuration** window includes three tabs.

- The **Subnets** tab displays a list of the configured VLAN subnets.
- The **Internal Interfaces** tab displays a list of LAN interfaces.
- The **Virtual Switch** tab displays a list of virtual switches configured, including the default system-generated virtual switch vs0.

The following table describes the fields in each tab.

Table 71: Network Configuration – Field Description

Parameter	Description	Values
Subnets Tab		
Subnet Name	Displays the name of the subnet.	(name)
Virtual Switch	Displays the name of the virtual switch in the form vs#, for example vs0 for virtual switch 0 which is the default virtual switch.	(vs<number>)

Parameter	Description	Values
VLAN ID	Displays the VLAN identification number for the network in the form vlan.#, for example vlan.27 for virtual LAN number 27.	(ID number)
Used IP Addresses	Displays the number of IP addresses in the subnet that are used, for example IP address of a VM or any other entity. This parameter is applicable only when you have configured a managed network or subnet.	(number of IP addresses)
Free IPs in Subnets	Displays the number of free or unused IP addresses in the subnet. This parameter is applicable only when you have configured a managed network or subnet.	(number of IP addresses)
Free IPs in Pool	Displays the number of free or unused IP addresses in the configured pool. This parameter is applicable only when you have configured a managed network or subnet.	(number of IP addresses)
Actions	Action link for editing or deleting a network configuration.	(Edit/Delete)
Internal Interfaces Tab		
Descriptive Name	Displays a name for the LAN.	(LAN name)
Subnet (Gateway IP / Prefix Length)	Displays the subnet that the internal interface belongs to in the form `<IP Address>`/<number (prefix)>	(IP Address/prefix number)
Features	Displays the features available on the internal interfaces.	
Interface	Displays the interface designation such as eth0 or eth1.	(interface name)
Virtual Switch		
Name	Displays the name of the switch in the form vs#	(vs<number>)
Bridge	Displays the name of the bridge associated with the virtual switch in the form br#, for example br0 for the default bridge.	(br<number>)
MTU (bytes)	Displays the MTU set for the virtual switch in bytes. The default MTU is 1500.	(number)
Bond Type	Displays the uplink bond type associated with the virtual switch. For more information, see the *Bond Types* table in Creating a Virtual Switch on page 349.	(<bond_type>)

LAG and LACP on the ToR Switch

For more information, see Enabling LACP and LAG (AHV Only) on page 354.

Creating VLAN Connections

Prism Central allows you to create a VLAN connection for a selected cluster.

About this task

To create one or more VLAN connections (subnets), perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Network & Security** > **Subnets** from the **Navigation Bar**.
   This displays the **Subnets** page.
3. Click **Network Config**.
   This displays the **Network Configuration** window.
4. In the **Subnets** tab of the **Network Configuration** window, click **Create Subnet**.

   This displays the **Create Subnet** window.
5. Perform the following in the indicated fields:
   a. **Subnet Name**: Enter a name for the subnet.
   b. **Virtual Switch**: Select the virtual switch for the subnet from the dropdown menu.

      You can associate the default virtual switch vs0 or create a virtual switch. For information on how to create a virtual switch, see Creating a Virtual Switch on page 349.

      For more information about virtual switch, see Layer 2 Network Management in the *AHV Administration Guide*.
   c. **VLAN ID**: Enter the number of the VLAN.
      Enter just the number in this field, for example 1 or 27. Enter 0 for the native VLAN. The value appears as vlan.1 or vlan.27 in displays.
   d. **Enable IP Address Management**: Select the checkbox to have the cluster control IP addressing in the subnet.
      Selecting this checkbox displays additional fields. If the checkbox is not selected, no network management is attempted and it is assumed that the management for this virtual LAN is handled outside the cluster.
   e. **Network IP Prefix**: Enter the IP address of the gateway for the network and prefix with the network prefix (CIDR notation, for example, 10.1.1.0/24).
   f. **Gateway IP Address**: Enter the VLAN default gateway IP address.
   g. **DHCP Settings**: Select this checkbox to display the fields for defining a domain.
      Selecting this checkbox displays fields to specify DNS servers and domains. Clearing this checkbox hides those fields.
   h. **Domain Name Servers (Comma Separated)**: Enter a comma-delimited list of DNS servers.
   i. **Domain Search (Comma Separated)**: Enter a comma-delimited list of domains.
   j. **Domain Name**: Enter the VLAN domain name.
   k. **TFTP Server Name**: Enter the host name or IP address of the TFTP server from which virtual machines can download a boot file. Required in a Pre-boot eXecution Environment (PXE).
   l. **Boot File Name**: Name of the boot file to download from the TFTP server.

6. To define a range of addresses for automatic assignment to virtual NICs, click **+ Create Pool** (under **IP Address Pools**) and enter the following in the **Add IP Pool** window that is displayed:

   Note: If no pool is provided, the user must assign IP addresses to VMs manually.

   a. Enter the starting IP address of the range in the **Start Address** field.

   b. Enter the ending IP address of the range in the **End Address** field.

   c. Click **Submit** to close the window and return to the **Create Subnet** window.

7. To configure a DHCP server, select the **Override DHCP server** checkbox and enter an IP address in the **DHCP Server IP Address** field.

   This address (reserved IP address for the Acropolis DHCP server) is visible only to VMs on this network and responds only to DHCP requests. If this checkbox is not selected, the **DHCP Server IP Address** field is not displayed and the DHCP server IP address is generated automatically. The automatically generated address is `network_IP_address_subnet.254`, or if the default gateway is using that address, `network_IP_address_subnet.253`.

8. Click **Save** to configure the network connection, close the **Create Subnet** window, and return to the **Network Configuration** window.

Modifying VLAN Connections

Prism Central allows you to modify an existing VLAN connection for a selected cluster.

About this task

Perform the following steps to modify an existing VLAN connection (defined on an Acropolis managed cluster):

Procedure

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Network & Security** > **Subnets** from the **Navigation Bar**.
   This displays the **Subnets** page.

3. To modify a VLAN connection, select the checkbox associated with the VLAN connection and click **Update** from the **Actions** dropdown menu.
   This displays the **Update Subnet** window which contains the same fields as the **Create Subnet** page (see Creating VLAN Connections on page 347).

4. Modify the field values and click **Update** to save the changes, and return to the **Subnets** page.

Perform the following steps to delete an existing VLAN connection.

5. To delete a VLAN connection, select the checkbox associated with the VLAN connection and click **Delete** from the **Actions** dropdown menu.

6. In the prompt window that is displayed, click **Delete**. The VLAN connection is removed from the list.

Creating a Virtual Switch

You can create a Virtual Switch (VS) using the **Create Virtual Switch** window in Prism Central.

About this task

Perform the following steps to create a virtual switch.

For more information about virtual switch, see the Layer 2 Network Management section in the *AHV Administration Guide*.

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Network & Security** > **Subnets** from the **Navigation Bar**.
   This displays the **Subnets** page.
3. Click **Network Config**.
   This displays the **Network Configuration** window.
4. Select the **Virtual Switch** tab, and then click **Create VS**.
5. In the **Create Virtual Switch** window that is displayed, provide the necessary information in the **General** step.

Field	Description
Virtual Switch Name	Enter a name for the virtual switch.
Description	Provide a description for the virtual switch that helps identify the virtual switch.
Physical NIC MTU (bytes)	MTU must be a value in the range 1280 to 9216 inclusive.
Select Configuration Method	Select one of the two methods that you can use to implement the VS configuration: • **Standard (Recommended)**: This method ensures no disruptions occur to the workloads by putting the hosts in maintenance mode and migrating the VMs out of the host before applying the configuration. This process requires a longer duration of time to complete. The time required depends on the number and configuration of VMs. In this method, the VS configuration is deployed in the rolling update process. • **Quick**: This method interrupts the workloads running on the hosts. Use this method only if you are not running production workloads because it may result in network interruptions. In this method, the VS configuration is deployed in a rolling update process but the nodes are not put in maintenance mode before modifying the VS configuration on the node.

6. Click **Next** to go to the **Uplink Configuration** step.

   In the **Uplink Configuration** step, provide the following details:

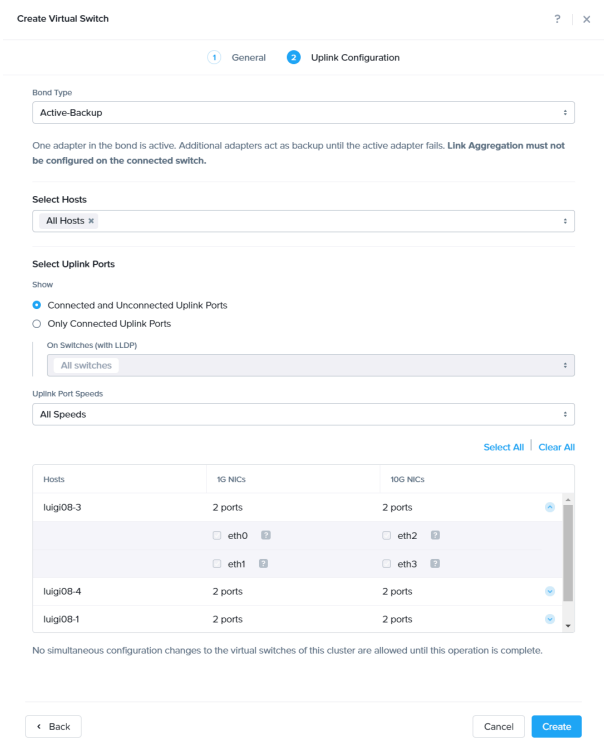


Figure 163: Create Virtual Switch - Uplink Configuration tab

Field	Description and Value
Bond Type	Select an appropriate bond type. For information about the bond types, see the *Bond Types* table.
Select Hosts	Select the hosts that can host VMs.
Select Uplink Ports	Select the criteria that need to be satisfied for the uplink ports. The available uplink ports that satisfy the criteria are displayed in the (Host port) table at the bottom of this tab.
Show	(Port Type) Select one of the following: **Connected and Unconnected Uplink Ports**: Select this option to use ports that are not currently connected but may be connected later. **Only Connected Uplink Ports**: Select this option to use only the connected ports. You must also select the switches with LLDP in the **On Switches (with LLDP)** dropdown menu.
Uplink Port Speeds	Select a speed to display the ports that have the selected speed. You can select **10G** or **All Speeds**. The speeds displayed depend on the NIC type that is installed on the host. Based on your selection the columns in the (Host Port) table change dynamically to display the ports with the speeds you selected.

Field	Description and Value
(Host Port) table	Based on your selections in **Select Uplink Ports**, a table displays the hosts that have the uplink ports that satisfy the selected criteria. Select the ports you need for this configuration from the list. Click the down arrow on the right side of the table to display the ports listed for each host. **Note:** A port listing is greyed out if it is unavailable because it is already associated with another virtual switch. Click **Select All** to select all the ports available and listed. Click **Clear All** to clear all the ports available and listed.

Table 72: Bond Types

Bond Type	Use Case	Maximum VM NIC Throughput	Maximum Host Throughput
Active-Backup	Recommended. Default configuration, which transmits all traffic over a single active adapter.	10 GB	10 GB
Active-Active with MAC pinning Also known as balance-slb	Works with caveats for multicast traffic. Increases host bandwidth utilization beyond a single 10 Gb adapter. Places each VM NIC on a single adapter at a time. Do not use this bond type with link aggregation protocols such as LACP.	10 GB	20 GB
Active-Active Also known as LACP with balance-tcp	LACP and link aggregation required. Increases host and VM bandwidth utilization beyond a single 10 Gb adapter by balancing VM NIC TCP and UDP sessions among adapters. Also used when network switches require LACP negotiation. The default LACP settings are: • Speed—Fast (1s) • Mode—Active fallback-active-backup • Priority—Default. This is not configurable.	20 GB	20 GB

Bond Type	Use Case	Maximum VM NIC Throughput	Maximum Host Throughput
No Uplink Bond	No uplink or a single uplink on each host. Virtual switch configured with the No uplink bond uplink bond type has 0 or 1 uplinks. When you configure a virtual switch with any other bond type, you must select at least two uplink ports on every node.	-	-

Note: The Maximum VM NIC Throughput and Maximum Host Throughput values are not restricted to the value provided in this table. The values in the table are indicated for an assumption of 2 x 10 Gb adapters.

For more information about uplink configuration, see Virtual Switch Workflow in the *AHV Administration Guide*.

7. Click **Create** to create the virtual switch.

   Click **Cancel** to exit without creating the virtual switch.

   Click **Back** to go back to the **General** step.

What to do next

Important:

You can migrate or convert the bridges other than br0 in the cluster to virtual switches after you upgraded the minimum or compatible version of AOS and AHV. You can convert the other bridges only on Prism Web Console or using aCLI. You can convert only one bridge at a time. You need to repeat the workflow for every bridge to be converted to a virtual switch.

For more information about converting the bridges other than br0, see Migrating Bridges after Upgrade in *Prism Element Web Console Guide*.

- If you select the **Active-Active** NIC-teaming policy, you must enable LAG and LACP on the corresponding ToR switch for each node in the cluster one after the other. For more information, see Enabling LACP and LAG (AHV Only) on page 354.

Updating a Virtual Switch

You can update an existing Virtual Switch (VS) using the **Edit Virtual Switch** window in Prism Central.

About this task

Perform the following steps to update an existing virtual switch.

For more information about virtual switch, see Layer 2 Network Management in the *AHV Administration Guide*.

Procedure

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Network & Security** > **Subnets** from the **Navigation Bar**.
   This displays the **Subnets** page.
3. Click **Network Config**.
   This displays the **Network Configuration** window.
4. Select the **Virtual Switch** tab, and click the *Edit* icon associated with the virtual switch you want to update.
   This displays the **Edit Virtual Switch** window.
5. Update the necessary information for the virtual switch by following all the instructions mentioned in Steps 5 through 7 of Creating a Virtual Switch on page 349.

What to do next

> **Important:**
>
> You can migrate or convert the bridges other than br0 in the cluster to virtual switches after you upgraded the minimum or compatible version of AOS and AHV. You can convert the other bridges only on Prism Web Console or using aCLI. You can convert only one bridge at a time. You need to repeat the workflow for every bridge that you want to convert to a virtual switch.
>
> For more information about converting the bridges other than br0, see Migrating Bridges after Upgrade in *Prism Element Web Console Guide*.

- If you select the **Active-Active** NIC-teaming policy, you must enable LAG and LACP on the corresponding ToR switch for each node in the cluster one after the other. For more information, see Enabling LACP and LAG (AHV Only) on page 354.

Enabling LACP and LAG (AHV Only)

This section describes the procedure to enable LAG and LACP in AHV nodes and the Top-of-Rack (ToR) switch or any switch that is directly connected to the Nutanix node.

Procedure

To enable LACP and LAG, perform the following steps:

1. Login to Prism element and navigate to **Settings** > **Network Configuration** > **Virtual Switch**.
   You can also login to Prism Central, select the **Infrastructure** application from Application Switcher Function, and navigate to **Network & Security** > **Subnets** > **Network Configuration** > **Virtual Switch** from the navigation bar.
   The system displays the **Virtual Switch** tab.
2. Click the Edit icon ( ) for the target virtual switch on which you want to configure LACP and LAG.
   The system displays the **Edit Virtual Switch** window.
3. In the **General** tab, choose **Standard (Recommended)** option in the **Select Configuration Method** field, and click **Next**.

   > **Note:** The **Standard** configuration method puts each node in maintenance mode before applying the updated settings. After applying the updated settings, the node exits from maintenance mode. For more information, see Virtual Switch Workflow.

4. In the **Uplink** Configuration tab, select `Active-Active` in the **Bond Type** field, and click **Save**.

   > **Note:** The `Active-Active` bond type configures all AHV hosts with the fast setting for LACP speed, causing the AHV host to request LACP control packets at the rate of one per second from the physical switch. In addition, the `Active-Active` bond type configuration sets LACP fallback to `Active-Backup` on all AHV hosts. You cannot modify these default settings after you have configured them in Prism, even by using the CLI.

   This completes the LAG and LACP configuration on the cluster. At this stage, cluster starts the Rolling Reboot operation for all the AHV hosts. Wait for the reboot operation to complete before you put the node and CVM in maintenance mode and change the switch ports.

   For more information about how to manually perform the rolling reboot operation for an AHV host, see Rebooting an AHV Node in a Nutanix Cluster.

Perform the following steps on each node, one at a time:

5. Put the node and the Controller VM into maintenance mode.

   > **Note:** Before you put a node in maintenance mode, see Verifying the Cluster Health and carry out the necessary checks.

   The Step 6 in Putting a Node into Maintenance Mode using Web Console section puts the Controller VM in maintenance mode.

6. Change the settings for the interface on the switch that is directly connected to the Nutanix node to match the LACP and LAG settings made in the Edit Virtual Switch window above.

   For more information about how to change the LACP settings of the switch that is directly connected to the node, refer to the vendor-specific documentation of the deployed switch.

   Nutanix recommends you perform the following configurations for LACP settings on the switch:

Table 73: Nutanix Recommendations for LACP Settings

Nutanix Recommendations	Description
Enable LACP fallback	Nutanix recommends you enable LACP fallback to set up a workaround for the port, using which the port establishes a link before the switch receives the LACP Bridge Protocol Data Units (BPDUs). The LACP fallback helps avoid link failures if either AHV host or switch that is connected to the AHV node does not negotiate LACP. LACP fallback provides seamless discovery of new nodes in an active or passive capacity setup and reduces the impact on the node operation. When LACP fallback is enabled, you can have a minimal business impact as VMs and applications remain healthy in case of an LACP status mismatch between the AHV host and the ToR switch port. As LACP fallback ensures connectivity during initial deployment, so it is crucial when you do not have LACP in discoveryOS. **Caution:** When LACP fallback occurs, the port runs in fallback mode, and this might lead to an unbalanced utilization of ports and lack of redundancy in your site deployment. Based on your internal networking policies, you can decide whether LACP fallback is helpful for you, and enable or disable it.
Consider the LACP time options *(slow and fast)*	If the switch has a fast configuration, Nutnaix recommends you set the LACP time to fast on AHV host. Nutanix recommends the LACP time to match on both; switch and AHV host, for L2 failure detection at the same time on the switch and AHV host. If the switch has a fast configuration, set the LACP time to fast on AHV host. When the LACP time setting matches on AHV host and switch, the detachment of a failed interface occurs at the same time, and both switch and the AHV host do not use the failed interface. When the LACP time is set to: • *fast* - Failure detection occurs faster within 3 seconds • *slow* - Failure detection occurs slowly and takes up to 90 seconds The matching LACP time helps to prevent the outage.

7. Verify that LACP negotiation status is `Negotiated`.

   Perform the SSH to the CVM as a nutanix user, and run the following commands:

   ```
   nutanix@CVM$ ssh root@[AHV host IP] "ovs-appctl bond/show bond-name"
   ```

   ```
   nutanix@CVM$ ssh root@[AHV host IP] "ovs-appctl lacp/show bond-name”
   ```

   - Replace the following attributes in the above commands:
     - `bond-name` with the actual name of the uplink port such as br0-up in the above commands.
     - `[AHV host IP]` with the actual AHV host IP at your site.
   - Search for the string `negotiated` in the status lines.

8. Remove the node and Controller VM from maintenance mode. For more information, see Exiting a Node from the Maintenance Mode using Web Console.

   The Controller VM exits maintenance mode during the same process.

What to do next

Do the following after completing the procedure to enable LAG and LACP in all the AHV nodes the connected ToR switches:

- Verify that the status of all services on all the CVMs are Up. Run the following command and check if the status of the services is displayed as **Up** in the output:

  ```
  nutanix@cvm$ cluster status
  ```

- Log in to the Prism Element web console of the node and check the **Data Resiliency Status** widget displays **OK**.

Virtual Private Clouds

You can manage the virtual private clouds (VPCs) you have created and configured, from the **Virtual Private Clouds** page.

Virtual Private Clouds Summary View

The **Virtual Private Clouds** page displays the list of virtual private clouds (VPCs) across all the registered clusters.

To access the **Virtual Private Clouds** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Network & Security** > **Virtual Private Clouds** from the **Navigation Bar**.

   The **Virtual Private Clouds** page opens displaying the **List** tab. This tab provides a list of virtual private clouds you have created and configured, and the operations you can perform on them.

   > **Note:** For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

The following table describes the fields that appear in the **Virtual Private Clouds** page.

> **Note:** The fields vary based on the **View by** and **Group by** options. A dash (-) is displayed in a field when a value is not available or applicable. For more information, see the View by on page 29 and Group by information.

Table 74: Virtual Private Clouds – Field Description

Field	Description
Name	Displays the name of the VPC. The **Name** of a VPC is suffixed with `Transit VPC` when you configure the VPC as a transit VPC.
Associated External Subnets	Displays the external subnet that the VPC is assigned to.
Categories	Displays the number of categories associated with the VPC.
Externally Routable IP Addresses	Displays the externally routable IP address.
Hypervisor	Displays the hypervisor that the VPC is hosted on.
Inter VN Traffic	Displays the traffic flowing between the virtual networks or VPCs.
Internet Traffic	Displays the traffic flowing to and from the Internet.
IPv4 Gateway	Displays the IPv4 gateway IP address.
IPv4/Subnet	Displays the IPv4 network IP with subnet prefix. For example, 10.20.30.0/24.
On-Prem Traffic	Displays the traffic flowing in the on-premises network.
VLAN ID	Displays the VLAN identification number. VLAN ID is a parameter used for Transit VPC networking in Nutanix Cloud Cluster with Microsoft Azure.

You can perform the following actions for the VPCs from the **Virtual Private Clouds** page:

- Click the name of a VPC to open the VPC details page, which displays the detailed information about the VPC. For more information, see Virtual Private Cloud Details View on page 359.
- Create a VPC by clicking **Create VPC**. For more information, see Creating Virtual Private Cloud in the *Flow Virtual Networking Guide*.
- Update or delete an existing VPC using the **Actions** dropdown menu. The **Actions** dropdown appears when one or more VPCs are selected. For more information, see Updating Virtual Private Cloud or Deleting a Virtual Private Cloud in the *Flow Virtual Networking Guide*.
- View VPCs based on pre-defined criteria or create a custom view. For more information about the **View by** option, see View By information.
- Filter the VPC list based on a variety of parameter values using **Filters** pane. For more information, see Filters Pane - Virtual Private Clouds Page.

Filters Pane - Virtual Private Clouds Page

You can filter the information in the **Virtual Private Clouds** page based on the following fields that are available in the **Filters** pane. For information about how to use the Filters pane, see the Filters Pane information.

Table 75: Filter Pane Field Description - Virtual Private Clouds page

Field	Description	Values
Name	Filters based on the VPC name. It returns a list of IP addresses that satisfy the name condition/string.	(Virtual private cloud name string)
Associated External Subnets	Filters based on the external subnet that the VPC is assigned to.	(External Subnet)

Virtual Private Cloud Details View

The Virtual Private Cloud (VPC) details page consists of a dashboard that provides the detailed information about the VPC.

The details page has the **Summary**, **Subnets**, **Policies**, **Routes**, and **Metrics** tabs.

To access the details page of an individual VPC:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Network & Security** > **Virtual Private Clouds** from the **Navigation Bar**.

   Prism Central displays the **Virtual Private Clouds** page that contains information about all the VPCs configured for the registered clusters.
3. Click a VPC to open the details page of the VPC.

   The **Summary** tab opens displaying the detailed information about the VPC in widgets.

> **Note:** For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

Summary Tab

The **Summary** tab provides detailed information about the VPC in widgets.

The **Summary** tab has the following widgets:

Widget Name	Information provided
External Connectivity	Provides the following: • Associated External Subnets — Displays the number of external subnets associated with the VPC. • Externally Routable IP Addresses — Displays the external routable IP addresses associated with the VPC.
Transit VPC	Displays **Yes** if the VPC is a Transit VPC. Displays **No** if the VPC is not a Transit VPC.
Domain Name Servers (DNS)	Displays the IP address or the FQDN of the DNS servers used by the VPC.
Associations	Provides the following: • Subnets (Overlay) — Displays the number of subnets associated with the VPC. • Policies — Displays the number of policies associated with the VPC. • Routes — Displays the number of routes associated with the VPC.

Widget Name	Information provided
Floating IP Addresses	Provides the following: • Assigned Floating IPs — Displays the floating IP addresses assigned to the VPC. • Available Floating IPs — Displays the available floating IP addresses that can be assigned to the VPC.

Subnets Tab

The **Subnets** tab displays the list of subnets added to the VPC.

The following table describes the fields that appear in the **Subnets** tab.

Table 76: Subnets Tab – Field Description

Field	Description
Name	Displays the subnet name.
IP Range	Displays the IP address range configured for the subnet.
DHCP IP Pool	Displays the IP address pool range assigned to the subnet.
Default Gateway IP	Displays the IP address used as the default gateway by the entities in the subnet.
Actions	Action link for editing or deleting the subnet.

You can perform the following actions for a subnet from the **Subnets** tab:

- Click the name of the subnet to open the subnet details page, which displays the detailed information about the subnet. For more information, see Subnet Details View on page 344.
- Create a subnet by clicking **Create Subnet**. For more information, see Creating a Subnet in the *Flow Virtual Networking Guide*.
- Update an existing subnet using the **Delete** option associated with the subnet. For more information, see Updating a Subnet in the *Flow Virtual Networking Guide*.
- Delete an existing subnet using the **Delete** option associated with the subnet. For more information, see Deleting Subnets, Policies, or Routes in the *Flow Virtual Networking Guide*.

Policies Tab

The **Policies** tab displays information about the security-based traffic shaping policies you configured.

The following table describes the fields that appear in the **Policies** tab.

> **Note:** The fields vary based on the **View by** option. A dash (-) is displayed in a field when a value is not available or applicable. For more information, see the View by on page 29 information.

Table 77: Policies Tab – Field Description

Field	Description
Description	Displays the user-provided description of the policy.
Action	Displays the appropriate action for the implementation of the policy. • Permit: Permits traffic and services based on the parameters set. • Deny: Denies traffic and service based on the parameters set. • Re-route: Sends matching traffic to the next-hop IP address specified by the Reroute IP.
Priority	Displays the traffic priority.
Rule	Displays the **Permit** or **Deny** rule set for the priority.
Rule Type	Displays whether the rule is system generated or user defined.
Traffic	Displays the traffic type that the priority and rule should be applied to.
Virtual Network	Displays the ID of the subnet.
Source	Displays the source IP or subnet for which you want to manage traffic.
Destination	Displays the destination IP or subnet for which you want to set the priority.
Source Subnet	Displays the subnet IP and prefix designated as the source for the policy.
Destination Subnet	Displays the subnet IP and prefix designated as the destination for the policy.
Reroute Address	Displays the IP address to which the traffic is re-routed.
Bidirectional Policy	Displays whether the policy is bidirectional or not.
Protocol	Displays the type of protocol for which the policy is configured.
Protocol Number	Displays the protocol number for which the policy is configured.
ICMP Type	Displays the type of ICMP message associated with the policy.
ICMP Code	Displays the ICMP code of the policy.
Byte Count	Displays the total number of traffic bytes that matches the given policy. The count is updated periodically.
Packet Count	Displays the total number of traffic packets that matches the given policy. The count is updated periodically.

You can perform the following actions for a policy from the **Policies** tab:

- Create a policy by clicking **Create Policy**. For more information, see Creating a Policy in the *Flow Virtual Networking Guide*.

- Perform the following actions using the **Actions** dropdown menu. The **Actions** dropdown appears when one or more policies are selected.
  - **Update**: Update the policy. For more information, see Updating a Subnet in the *Flow Virtual Networking Guide*.
  - **Delete**: Delete the policy. For more information, see Deleting Subnets, Policies, or Routes in the *Flow Virtual Networking Guide*.
  - **Clear Counters**: Reset the counters for the selected policy.
  - **Clear All Counters**: Reset the counters for all the policies.
- View policies based on pre-defined criteria or create a custom view. For more information about the **View by** option, see View By information.

Routes Tab

The **Routes** tab displays the list of static routes added to the VPC.

The following table describes the fields that appear in the **Routes** tab.

> **Note:** The fields vary based on the **View by** option. A dash (-) is displayed in a field when a value is not available or applicable. For more information about the View by option, see View by on page 29 information.

Table 78: Routes Tab – Field Description

Field	Description
Destination Prefix	Displays the IP address and prefix of the destination.
Next Hop	Displays the next hop network or subnet for the traffic exiting the VPC.
Priority	Displays the traffic priority.
Type	Displays the type of route, local or static.
Status	Displays the status of the route, whether it is active or not

You can perform the following actions for a route from the **Routes** tab:

- View routes based on pre-defined criteria or create a custom view. For more information about the View by option, see View by on page 29 information.
- Perform the following actions using the **Manage Static Routes** option:
  - **Add Static Route**: Create a static route. For more information, see Creating Static Routes in the *Flow Virtual Networking Guide*.
  - Update an existing static route. For more information, see Updating Static Routes in the *Flow Virtual Networking Guide*.
  - Delete a static route. For more information, see Deleting Subnets, Policies or Routes in the *Flow Virtual Networking Guide*.

Metrics Tab

The **Metrics** tab displays detailed information about the VPC metrics.

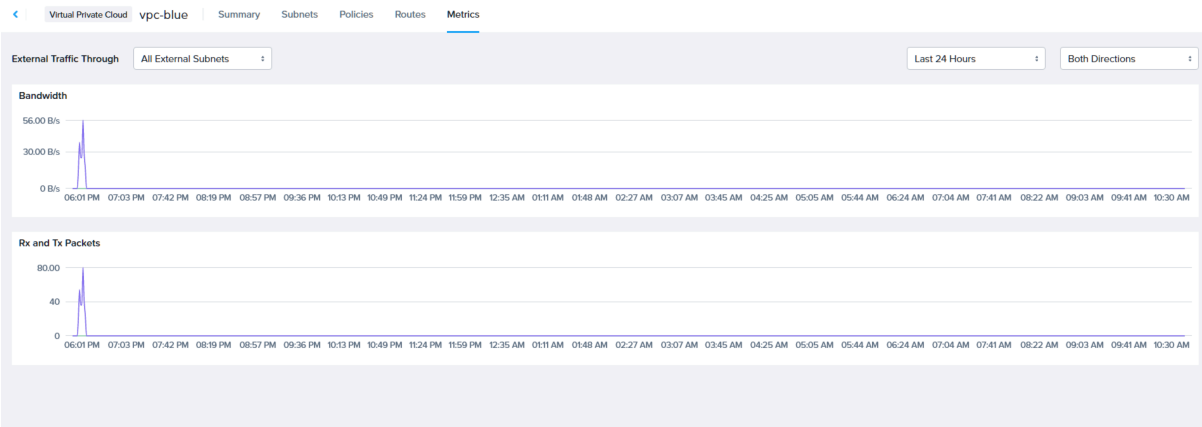


Figure 164: Metrics Tab

The following table describes the fields that appear in the **Metrics** tab.

Table 79: Metrics Tab – Field Description

Field	Description
External Traffic Through	Select **All External Networks** (default) or **(name_of_external_network_associated_with_the_VPC)** from the dropdown menu. The page displays the metrics based on your selection.
Last (time_period)	Select the period for which you want to display the metrics. The dropdown menu provides the following options: • **Last 24 Hours (default)** • **Last One Hour** • **Last Week**
Direction of traffic	Select the direction of traffic for which you want to display the metrics. The dropdown menu provides the following options: • **Both directions** (default) — Includes both directions, Ingress and Egress. • **Ingress** — Traffic entering the externally connected subnet. • **Egress** — Traffic leaving the externally connected subnet.
Bandwidth	Displays graphically the bandwidth utilization of the VPC on a timeline as set in the **Last (time_period)** parameter.
Rx and Tx Packets	Displays graphically the received and transmitted packet volume on a timeline as set in the **Last (time_period)** parameter.

Traffic Mirroring

Traffic Mirroring enables you to mirror traffic from the interfaces of the AHV hosts to the virtual NIC (vNIC) of guest VMs. Traffic Mirroring mirrors the packets from a set of source ports to a set of destination ports.

You can mirror inbound, outbound, or bidirectional traffic flowing on a set of source ports. You can then use the mirrored traffic for security analysis and to gain visibility of traffic flowing through the set of source ports. Traffic Mirroring is a useful tool for troubleshooting packets and necessary for compliance.

Prism Central allows you to select the following entity types for source and destination:

- Source:
  - Individual host ports
  - Bonded host ports
  - Virtual machines

    Note: You can only select up to 4 entities in total for all the source type entities.
- Destination: Virtual Machines

    Note: You can select up to two destination type entities.

Source Ports

Prism Central supports the following types of source ports in a Traffic Mirroring session:

- A bond port that is already mapped to a virtual switch (vs) such as vs0, vs1, or any other vs that you created
- A non-bond port that is already mapped to a vs such as vs0, vs1, or any other vs that you created
- An uplink port that is not assigned to any vs or bridge on the host
- A virtual port attached to a VM

Important Considerations

Consider the following before you create Traffic Mirroring sessions:

- Prism Central supports Traffic Mirroring from physical and VM interfaces. Therefore, a source port can be a physical or VM interface.
- Prism Central supports Traffic Mirroring to destination guest VMs running on the same AHV host (to which the source ports belong) or on a remote AHV host.
- VM interface port/bond supports Traffic Mirroring to a destination on a remote host.
- Physical source port/bond interface does not support Traffic Mirroring to a destination on a remote host.
- In a single Traffic Mirroring session, if both remote and local host destinations are available, the physical source port/bond interface is mirrored only to the local destination, while the VM interface port/bond is mirrored to both remote and local destinations.
- Nutanix does not support Traffic Mirroring on Nutanix clusters connected to AWS or Azure.
- Prism Central supports different types of source ports in one session. For example, you can create a session with br0-up (bond port) and eth5 (single uplink port) on the same host as two different source ports in the same session. You can have two different bond ports in the same session.
- Delete the Traffic Mirroring session before you delete the Traffic Mirroring destination VM or vNIC. Otherwise, the state of the Traffic Mirroring session is displayed as an error.
- If you migrate a destination VM, delete the vNIC, or if the physical port is down, the Traffic Mirroring session displays an error status.

- If all vNICs are migrated to the same host, the traffic mirror session displays active status. However, if the session has physical NICs (pNICs), the Traffic Mirroring session displays an error status.
- You cannot configure the direction of the traffic if the ports are not managed by a virtual switch.
- You can select one source VM vNIC for a single Traffic Mirroring session.
- You can select one destination VM vNIC for a single Traffic Mirroring session.

Traffic Mirroring Session Scale

Traffic Mirroring session supports the following scale:

Table 80: Traffic Mirroring Session Scale

Entities	Scale
Source ports or entities	4 entities per Traffic Mirroring session
Destination ports or entities	2 entities per Traffic Mirroring session
Maximum number of Traffic Mirror sessions	1,000 per cluster
Maximum number of Active Sessions	2 per host

Traffic Mirroring Summary View

The Traffic Mirroring page displays information about all the Traffic Mirroring sessions created across registered clusters.

To access the summary view of all the Traffic Mirroring sessions, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Network & Security** > **Traffic Mirroring** from the **Navigation Bar**.

   The **Traffic Mirroring** page opens displaying the **List** tab. This tab provides information about all the Traffic Mirroring sessions configured for the clusters.

   > **Note:** For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

The following table describes the fields that are displayed in the **List** tab.

> **Note:** The fields vary based on the **View by** option. A dash (-) is displayed in a field when a value is not available or applicable. For more information, see the View by on page 29 information.

Table 81: Traffic Mirroring - Field Description

Field	Description	Values
Name	Displays the Traffic Mirroring session name.	(Traffic Mirroring session name)
Source (Ingress)	Traffic entering the source.	(source VM, MAC address)
Source (Egress)	Traffic leaving the source.	(source VM, MAC address)
Destinations	Displays the destination virtual machine with MAC address.	(destination VM, MAC address)

Field	Description	Values
State	Displays the current operational status of the Traffic Mirroring session.	(Enabled, Disabled)

You can perform the following actions from the **List** tab:

- Click the name of a Traffic Mirroring session to open the details page, which displays detailed information about the Traffic Mirroring session.
- Create a Traffic Mirroring session by clicking **Create Mirror Session**. For more information, see Creating a Traffic Mirroring Session on page 368.
- Download the table of Traffic Mirroring sessions in CSV format by clicking **Export**.
- View the reports based on pre-defined criteria or create a custom view. For more information, see View by on page 29.
- Filter the Traffic Mirroring session list based on a variety of parameter values using the **Modify Filters** pane. For more information, see
- Perform the following actions on a Traffic Mirroring session using the **Actions** dropdown menu.

Table 82: Traffic Mirror Session Actions

Action	Description
Disable Session	Click this action to disable the Traffic Mirroring session. For more information, see Disabling a Traffic Mirroring Session on page 372.
Enable Session	Click this action to enable the Traffic Mirroring session. For more information, see Enabling a Traffic Mirroring Session on page 372.
Update	Click this action to update the Traffic Mirroring session. For more information, see Updating a Traffic Mirroring Session on page 372.
Delete	Click this action to delete the Traffic Mirroring session. For more information, see Deleting a Traffic Mirroring Session on page 373.

Filters Pane - List Tab

You can filter the information in the **List** tab based on the following fields available in the **Filters** pane. For information about how to use the **Filters** pane, see the Filters Pane information.

Table 83: Filter Pane Field Description - Traffic Mirroring Session

Field	Description	Values
Name	Filters based on the application instance name. Select the checkbox, and choose a condition from the dropdown menu (**Contains**, **Equal to**, **Not Equal to**, **Doesn't contain**, **Starts with**, **Ends with**, or) and enter a string in the field.	(Traffic Mirroring Session name string)
State	Filters based on the state of the Traffic Mirroring session. Select the checkbox for Enabled, or Disabled, or both.	Enabled, Disabled

Traffic Mirroring Details View

The Traffic Mirroring details page consists of dashboard widgets that provide detailed information about the Traffic Mirroring sessions.

To access the details page of an individual Traffic Mirroring session, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Network & Security** > **Traffic Mirroring** from the **Navigation Bar**.

   The **Traffic Mirroring** page opens displaying the **List** tab. This tab provides information about all the Traffic Mirroring sessions configured for the clusters.
3. Click the name of a Traffic Mirroring session to open the details page.

   The **Summary** tab opens displaying the detailed information about the Traffic Mirroring session in widgets.

The **Summary** page has the following widgets:

Table 84: Traffic Mirroring Session Summary Tab Widgets

Widget	Parameters
Entities	• Cluster: Displays the cluster name. • Virtual Switch for Mirrored Traffic: Displays the virtual switch used for Traffic Mirroring.
Source: Host Ports ((Individual)	• Hosts: Displays the host name. • Ports: Displays the host port details. • Direction: Displays the traffic direction of the host port.

Widget	Parameters
Source: Virtual Machines	• VM: Displays the name of the source virtual machine. • MAC Address: Displays the MAC address of the source virtual machine.
Statistics	• Status: Displays the operational status of the Traffic Mirroring session. • Packet Count: Displays the packet count mirrored and received from the destination. • Packet Byte Count: Displays the packet byte count derived from the packet count.
Destination: Virtual Machines	• VM: Displays the name of the destination virtual machine. • MAC Address: Displays the MAC address of the destination virtual machine.
Source: Host Ports(Bonds)	• Hosts: Displays the host name. • Bonds: Displays the bond name. • Ports: Displays the details of the bonds on the host port. • Direction: Displays the direction of the traffic on the host port bonding.

You can perform the following actions from the Summary tab:

- Disable an existing Traffic Mirroring session by clicking **Disable Session**.
- Update an existing Traffic Mirroring session by clicking **Update**.
- Delete an existing Traffic Mirroring session by clicking **Delete**.

Creating a Traffic Mirroring Session

Prism Central allows you to create a Traffic Mirroring session to mirror inbound, outbound, or bidirectional traffic on a set of source ports.

Before you begin

Ensure that you configure the traffic mirror type on the vNIC of the destination VM. For more information about adding a traffic mirror type vNIC to the destination VM, see Creating a VM through Prism Central (AHV) on page 121.

About this task

Follow these steps to create a Traffic Mirroring session that replicates the traffic from a set of source ports to a set of destination ports:

Procedure

1. Log in to Prism Central.
2. From the Application Switcher Function on page 19, select the **Infrastructure** application and from the navigation bar, select **Network & Security** > **Traffic Mirroring**.
   The **Traffic Mirroring** page opens displaying the **List** tab. This tab provides information about all the Traffic Mirroring sessions configured for the registered clusters.
3. Click **Create Mirror Session**.
4. In the **General** tab, enter the following information:
   a. **Name**: Enter a name for the Traffic Mirroring session.
   b. **Description**: Enter an optional description for the Traffic Mirroring session.
   c. **Cluster**: From the dropdown menu, select the cluster.
   d. **Virtual Switch for mirrored traffic**: From the dropdown menu, select the virtual switch where the Traffic Mirroring session is to be created.
      Nutanix recommends using a non-default Virtual Switch with Maximum Transmission Unit (MTU) set between 1600-9000 for Traffic Mirroring to a destination on the remote host. For more information, see Configuring Virtual Switch for VPC Traffic Types.
5. Click **Next**.

6. In the **Source & Destination** tab, follow these steps to select the individual host ports:

   a. From the **Source Type(s)** dropdown menu, select **Host Ports (Individual)**.

   b. On the **Hosts Ports (Individual)** panel, click **Select Host Ports**.
   Select Host Ports (Individual) window appears.

   c. Click the down arrow icon next to the host name.
   The system displays **NICs** associated with the host along with the drop-down menu to select the **Traffic Direction**.

   d. Under **NICs**, select the checkbox of the Ethernet port to mirror the traffic for.

   e. Under **Traffic Direction**, select the direction of the traffic from the dropdown menu.
   The **Traffic Direction** dropdown menu provides the following options:

   - **Both** (default): Includes both directions, Ingress and Egress.
   - **Ingress**: Traffic entering the source port.
   - **Egress**: Traffic leaving the source port.

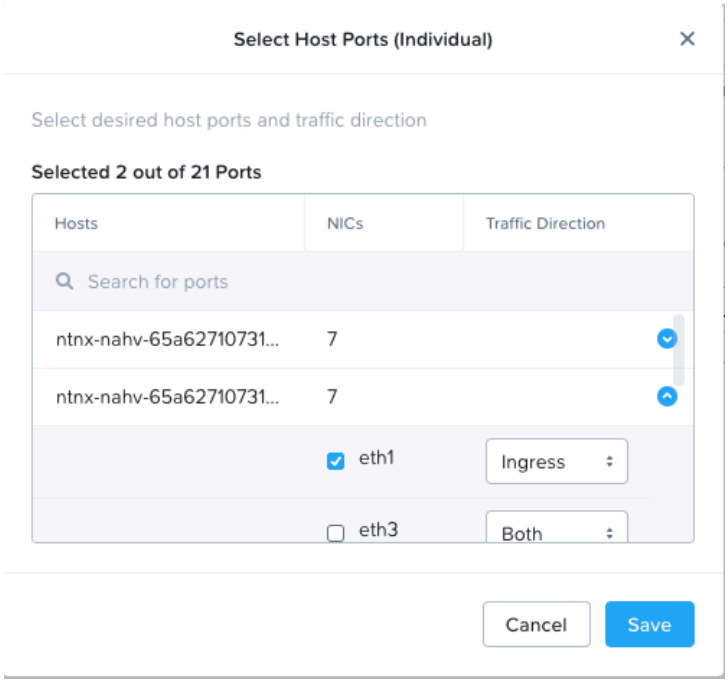


Figure 165: Individual Host Ports - Source

> **Note:** Traffic direction is unavailable if the ports are not managed by a virtual switch (vs).

   f. Click **Save**.

7. In the **Source & Destination** tab, follow these steps to select the bonded host ports:

   a. From the **Source Type(s)** dropdown menu, select **Host Ports (Bond)**.

   b. On the **Hosts Ports (Bond)** panel, click **Select Host Ports**.
   Select Host Ports (Bond) window appears.

   c. Click the down arrow icon next to the host name.
   The system displays **Bonds** and **Ports** associated with the host along with a drop-down menu to select the **Traffic Direction**.

   d. Under **Bonds**, select the checkbox of the bonded port to mirror the traffic for.

   e. Under **Traffic Direction**, select the direction of the traffic from the dropdown menu.
   The **Traffic Direction** dropdown menu provides the following options:

      - **Both** (default): Includes both directions, Ingress and Egress.
      - **Ingress**: Traffic entering the source port.
      - **Egress**: Traffic leaving the source port.

   f. Click **Save**.

8. In the **Source & Destination** tab, follow these steps to select the host virtual machines:

   a. From the **Source Type(s)** dropdown menu, select the **Virtual Machines** from the dropdown menu.

   b. On the **Virtual Machines** panel, click **Select Virtual Machines**.
   Select Virtual Machines window appears.

   c. Under **Virtual Machine**, select the source virtual machine from the dropdown menu.

   d. Under **MAC Address**, select the MAC address from the dropdown menu.

   e. Under **Direction**, select the direction of the traffic.
   The **Traffic Direction** dropdown menu provides the following options:

      - **Both** (default): Includes both directions, Ingress and Egress.
      - **Ingress**: Traffic entering the source VM.
      - **Egress**: Traffic leaving the source VM.

   f. (Optional) To add an additional VM, click **Add VM**.

   g. Click **Save**.

9. In the **Source & Destination** tab, follow these steps to select the destination virtual machines:

   a. Under destination, click **Select Virtual Machines**.
   Select Virtual Machines window appears.

   b. Under **Virtual Machine**, select the destination virtual machine from the dropdown menu.

   c. Under **MAC Address**, select the MAC address from the dropdown menu.

   d. (Optional) To add an additional VM, click **Add VM**.

   e. Click **Save**.

10. Click **Next**.

11. In the **Summary** tab, verify the Traffic Mirroring session details and do one of the following:

    » To create a session, click **Create Session**.

    » To create and enable a session, click **Create and Enable Session**.

Disabling a Traffic Mirroring Session

Prism Central allows you to disable an existing Traffic Mirroring session.

About this task

You can disable a Traffic Mirroring session to stop mirroring the traffic to the destination VM.

Procedure

1. Log in to Prism Central.
2. From the Application Switcher Function on page 19, select the **Infrastructure** application and from the navigation bar, select **Network & Security** > **Traffic Mirroring**.
   The **Traffic Mirroring** page opens displaying the **List** tab. This tab provides information about all the Traffic Mirroring sessions configured for the registered clusters.
3. Select the checkbox of the Traffic Mirroring session you want to disable.
4. From the **Actions** dropdown menu, select **Disable Session**.
   Prism Central displays the **Disable Session** window.
5. Click **Disable Session**.

Enabling a Traffic Mirroring Session

Prism Central allows you to enable a Traffic Mirroring session.

About this task

You can enable a Traffic Mirroring session that you have created to start mirroring the traffic to the destination VM.

Procedure

1. Log in to Prism Central.
2. From the Application Switcher Function on page 19, select the **Infrastructure** application and from the navigation bar, select **Network & Security** > **Traffic Mirroring**.
   The **Traffic Mirroring** page opens displaying the **List** tab. This tab provides information about all the Traffic Mirroring sessions configured for the registered clusters.
3. Select the checkbox of the Traffic Mirroring session you want to enable.
4. From the **Actions** dropdown menu, select **Enable Session**.
   Prism Central displays the**Enable Session** window.
5. Click **Enable Session**.

Updating a Traffic Mirroring Session

Prism Central allows you to update a Traffic Mirroring session.

About this task

Update a Traffic Mirroring session to modify parameters such as name, description, cluster, host, source and destination types.

Procedure

1. Log in to Prism Central.
2. From the Application Switcher Function on page 19, select the **Infrastructure** application and from the navigation bar, select **Network & Security** > **Traffic Mirroring**.
   The **Traffic Mirroring** page opens displaying the **List** tab. This tab provides information about all the Traffic Mirroring sessions configured for the registered clusters.
3. Select the checkbox of the Traffic Mirroring session you want to update.
4. From the **Actions** dropdown menu, select **Update**.
   Prism Central displays the **Update Mirror Session** window, which includes the same fields as the **Create Mirror Session** window. For information about creating a Traffic Mirroring Session, see Creating a Traffic Mirroring Session on page 368.
5. Modify the Traffic Mirroring session based on your requirements and click **Update Session**.

Deleting a Traffic Mirroring Session

Prism Central allows you to delete a Traffic Mirroring session.

About this task

You can delete a Traffic mirroring session to permanently remove from the Traffic Mirroring session page list.

Procedure

1. Log in to Prism Central.
2. From the Application Switcher Function on page 19, select the **Infrastructure** application and from the navigation bar, select **Network & Security** > **Traffic Mirroring**.
   The **Traffic Mirroring** page opens displaying the **List** tab. This tab provides information about all the Traffic Mirroring sessions configured for the registered clusters.
3. Select the checkbox of the Traffic Mirroring session you want to delete.
4. From the **Actions** dropdown menu, select **Delete**.
   Prism Central displays the **Delete Session** window.
5. Click **Delete Session**.

Traffic Mirroring Session Alerts

Prism Central generates the Traffic Mirroring session alerts for the following inconsistent state scenarios:

> **Note:** For more information about the Alerts generated in Prism Central, see Prism Central Alerts and Events Reference Guide.

Table 85: Traffic Mirror Session Alerts List

Alert Title	Possible Cause
Inconsistent SPAN Session State Detected	This alert occurs when a VM NIC is removed from the destination VM.
Inconsistent SPAN Session State Detected	This alert occurs when a destination VM is migrated to another host.
Inconsistent SPAN Session State Detected	This alert occurs when a destination VM is powered off.

Role-Based Access Control in Traffic Mirroring

Prism Central supports role-based access control (RBAC) that allows you to configure and provide customized access to the users based on their assigned roles for the Traffic Mirroring entity. For more information on configuring RBAC, see Controlling User Access (RBAC).

From the Prism Central roles dashboard, you can define and assign the following roles to users or user groups:

- Predefined built-in roles (system roles)
- Custom roles

Any user with the following predefined built-in roles can configure the Traffic Mirroring functionality:

- Network Infra Admin
- Prism Admin

For more information on predefined built-in and custom roles, see Built-in Role Management and Custom Role Management in the *Security Guide*.

Traffic Mirroring Permissions

The following table lists all of the permissions that you can add to a custom role and assign that custom role to the user to perform various Traffic Mirroring tasks.

Table 86: Traffic Mirroring Permissions

Traffic Mirroring Permissions
Create Traffic Mirror
Delete Traffic Mirror
Update Traffic Mirror
View Traffic Mirror
View Traffic Mirror Stats
View Cluster
View Cluster Networking Capabilities
View Host
View Uplink Bond
View VM

Floating IPs

You can access the floating IP addresses you have created and configured, from the **Floating IPs** page.

For information about floating IP addresses and their role in flow virtual networking, see the *SNAT and Floating IP Address* section in the Essential Concepts topic of the *Flow Virtual Networking Guide*.

> **Note:** Floating IP addresses are not reachable (Pings fail) unless you associate them to primary or secondary IP addresses of VMs. For more information, see Assigning Secondary IP Addresses to Floating IPs in the *Flow Virtual Networking Guide*.

Floating IPs Summary View

The **Floating IPs** page displays the list of floating IP addresses across all the registered clusters.

To access the **Floating IPs** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Network & Security** > **Floating IPs** from the **Navigation Bar**.

   The **Floating IPs** page opens displaying the **List** tab. This tab provides a list of floating IPs you have created and configured, and the operations you can perform on the IPs.

> **Note:** For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

The following table describes the fields that appear in the **Floating IPs** page.

> **Note:** The fields vary based on the **View by** option. A dash (-) is displayed in a field when a value is not available or applicable. For more information, see the View by on page 29 information.

Table 87: Floating IPs – Field Description

Parameter	Description	Values
Floating IP Address	Displays the floating IP address assigned.	(IP address)
External Subnet	Displays the name of the external subnet that the IP address is assigned to.	(Name of the assigned subnet)
Association Status	Displays the status of association between the IP address and the external subnet and VPC.	Associated
VPC	Displays the name of the VPC associated with the IP address.	(Name of the associated VPC)
VM Name	Displays the name of the VM associated with the IP address.	(Name of the assigned VM)
Private IP	Displays the private IP address assigned to the same VM. This private IP address is assigned from the internal private subnet that the network controller creates when you crate a network gateway.	(IP address)

You can perform the following actions for the floating IP addresses from the **Floating IPs** page:

- Request a floating IP address by clicking **Request Floating IP**. For more information, see Requesting Floating IPs in the *Flow Virtual Networking Guide*.
- Update or delete an existing floating IP address using the **Actions** dropdown menu. The **Actions** dropdown appears when one or more addresses are selected.
  - **Update**: Assign or change the assignment of the floating IP address. You can assign the floating IP address to a IP address such as a private IP address in a VPC or the primary IP address of a VM or a secondary IP address created on a VM.
  - **Delete**: Delete the floating IP address. The deleted IP address returns to the IP address pool as unused. Before you delete a floating IP address, ensure that it is not assigned to a private IP address or a VM. Change the assignment to None if it is already assigned, using the **Update** option.
- View floating IP addresses based on pre-defined criteria or create a custom view. For more information about the **View by** option, see View By information.
- Filter the floating IP addresses list based on a variety of parameter values using **Filters** pane. For more information, see Filters Pane - Floating IPs Page.

Filters Pane - Floating IPs Page

You can filter the information in the **Floating IPs** page based on the following fields that are available in the **Filters** pane. For information about how to use the Filters pane, see the Filters Pane information.

Table 88: Filter Pane Field Description - Floating IPs page

Field	Description	Values
Floating IP Address	Filters based on the floating IP address assigned. It returns a list of IP addresses that satisfy the string.	(Floating IP address)
External Subnet	Filters based on the external subnet that the IP address is assigned to.	(External Subnet)

Connectivity

You can access network gateways, VPN connections, subnet extensions, and BGP sessions from the `Connectivity` page.

To access the **Connectivity** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Connectivity** page opens displaying the **Gateways** tab. This tab provides a list of network Gateways you have created and configured, and the operations you can perform on the network Gateways.

- To view the VPN connections, click the **VPN Connections** tab.
- To view the subnets extended across the clusters, click the **Subnet Extensions** tab.
- To view the BGP sessions created for the clusters, click the **BGP Sessions** tab.

Gateways Summary View

The **Gateways** page displays a list of gateways created for the clusters managed by Prism Central.

To access the **Gateways** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways you have created and configured, and the operations you can perform on the network gateways.

   > **Note:** For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

The following table describes the fields that appear in the **Gateways** page.

Table 89: Gateway – Field Description

Parameter	Description	Values
Name	Displays the name of the gateway.	(Name of gateway)
Type	Displays the gateway type.	(Local or Remote)
Service	Displays the service that the gateway uses.	(VPN or VTEP)
Service IP	Displays the IP address used by the service.	(IP address)
Status	Displays the operational status of the gateway.	(Up or Down)
Attachment Type/Vendor	Displays the type of subnet associated with the gateway.	(VLAN or Overlay-VPC name)
Connections	Displays the number of service connections (such as VPN connections) configured and operational on the gateway.	(Number)

You can perform the following actions for a gateway from the **Gateways** page:

- Click the name of a gateway to open the gateway details page, which displays the detailed information about the gateway. For more information, see Gateway Details View on page 378.
- Create a local or remote gateway with VPN or VTEP service by clicking the **Create Gateway** dropdown menu. For more information, see Creating a Network Gateway in the *Flow Virtual Networking Guide*.
- Update or delete an existing gateway using the **Actions** dropdown menu. The **Actions** dropdown menu appears when one or more gateways are selected. For more information, see Updating a Network Gateway or Deleting a Network Gateway in the *Flow Virtual Networking Guide*.
- Filter the gateway list based on various parameter values using the **Filters** pane. For more information, see Filters Pane - Gateways Page.

Filters Pane - Gateways Page

You can filter the information in the **Gateways** page based on the following fields that are available in the **Filters** pane. For information about how to use the Filters pane, see the Filters Pane information.

Table 90: Filter Pane Field Description - Gateways page

Field	Description	Values
Name	Filters based on the gateway name. It returns a list of gateways that satisfy the name condition/string.	(Gateway name string)
Service IP	Filters based on IP address used by the service.	(IP address)
Status	Filters based on the operational status of the gateway.	(Up or Down)

Gateway Details View

The **Summary** page of an individual gateway consists of a dashboard that provides the detailed information about the gateway.

To access the **Summary** page of an individual gateway:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways that you have created and configured.
3. Click a gateway to view the **Summary** page of the gateway.

> **Note:** For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

The gateway **Summary** page has the following widgets:

Table 91: Gateway Widgets

Parameter	Description	Values
Properties widget		
Type	Displays the gateway type.	(Local or Remote)
Attachment Type	Displays the network entity like VLAN or VPC that the gateway is attached to.	(VLAN or VPC)
VPC or Subnet (VLAN)	Displays the name of the attached VPC or VLAN subnet.	(Name of VLAN or VPC)
Vendor (Applicable only if you select remote gateway)	Displays the name of the vendor of the gateway appliance at the remote site.	(Name of Vendor)
Floating or Private IP Address	Displays the Floating (for VPC) or Private (for VLAN) IP address assigned to the gateway.	(IP Address)
External IP (Applicable only if you select remote gateway)	Displays the IP address assigned to the remote gateway.	(IP Address that you assigned to the remote gateway.)
Status	Displays the operational status of the gateway.	(Up or Down)
Gateway Version	Displays the version of the Nutanix gateway appliance deployed.	(Version)

Parameter	Description	Values
Cluster	Displays the name of the cluster on which the gateway is created.	(Cluster name)
Gateway VM	Displays the name of the VM on which the gateway is created.	(Name of VM - actionable link. Click the name-link to open the VM details page of the gateway VM.)
Service Configuration widget		
Service	Displays the service used by the gateway.	(VPN or VTEP or BGP)
VPN Service Configuration		
External Routing	Displays the type of routing associated with the gateway for external traffic routing.	(Static or eBGP with ASN)
Internal Routing	Displays the type of routing associated with the gateway for internal traffic routing.	(Static or eBGP with ASN)
VPN Connections	Displays the total number of VPN connections associated with the gateway.	(Number - actionable link. Click the link to open the VPN connection details page for the associated VPN connection.)
View VPN Connections	Click this link to open the VPN Connections tab.	-
VTEP Service Configuration		
VXLAN (UDP) Port	Displays the VXLAN (UDP) Port for the gateway.	(Number)
Subnet Extensions	Displays the total number of subnet extensions associated with the gateway.	(Number - actionable link. Click the link to open the subnet extensions details page for the associated subnet extension.)
View Subnet Extensions	Click this link to open the **Subnet Extensions** tab.	-
BGP Service Configuration		
ASN	Displays the ASN of the EBGP route.	(Number)
BGP Sessions	Displays the total number of BGP sessions associated with the gateway.	(Number - actionable link. Click the link to open the BGP sessions details page for the associated BGP session.)
Serviced VPC	Displays VPC service used by the gateway.	(Name of VPC)
View BGP Sessions	Click this link to open the **BGP Sessions** tab.	-

You can perform the following actions for a gateway from the **Summary** tab:

- Update an existing gateway by clicking **Update**. For more information, see Updating a Network Gateway in the *Flow Virtual Networking Guide*.

- Delete the gateway by clicking **Delete**. For more information, see Deleting a Network Gateway in the *Flow Virtual Networking Guide*.

VPN Connections Summary View

The **VPN Connections** page displays a list of VPN connections created for the clusters managed by Prism Central.

A VPN connection represents the VPN IPSec tunnel established between local gateway and remote gateway. When you create a VPN connection, you must select two gateways between which you want to create the VPN connection.

To access the **VPN Connections** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways.
3. Click the **VPN Connections** tab.

   The **VPN Connections** page opens displaying the list of VPN connections created for the clusters.

> **Note:** For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

The following table describes the fields that appear in the **VPN Connections** page.

Table 92: VPN Connections – Field Description

Parameter	Description	Values
Name	Displays the name of the connection.	(gateway name)
IPSec Status	Displays the connection status of IPSec tunnel.	(Connected or Not Connected)
EBGP Status	Displays the status of the EBGP gateway connection.	(Established or Not Established)
Local Gateway	Displays the name of the local gateway used for the connection.	(Name of local gateway)
Remote Gateway	Displays the name of the remote gateway used for the connection.	(Name of remote gateway)
Dynamic Routing Priority	Displays the dynamic routing priority assigned to the connection for throughput management. You can assign any value in the range of 100-1000. Nutanix Flow Virtual Networking assigns the first VPN connection the value 500 by default. Thereafter, subsequent VPN connections are assigned values decremented by 50. For example, the first connections is assigned 500, then the second connection is assigned 450, the third one 400 and so on.	(Number in the range of 100-1000. User assigned.)

You can perform the following actions for a VPN connection from the **VPN Connections** page:

- Click the name of a VPN connection to open the VPN connection details page, which displays the detailed information about the connection. For more information, see VPN Connection Details View on page 381.
- Create a VPN connection by clicking **Create VPN Connection**. For more information, see Creating a VPN Connection in the *Flow Virtual Networking Guide*.
- Update or delete an existing VPN connection using the **Actions** dropdown menu. The **Actions** dropdown appears when one or more VPN connections are selected. For more information, see Updating VPN Connection or Deleting a VPN Connection in the *Flow Virtual Networking Guide*.
- Filter the VPN connection list based on various parameter values using the **Filters** pane. For more information, see Filters Pane - VPN Connections Page.

Filters Pane - VPN Connections Page

You can filter the information in the **VPN Connections** page based on the following fields that are available in the **Filters** pane. For information about how to use the Filters pane, see the Filters Pane information.

Table 93: Filter Pane Field Description - VPN Connections page

Field	Description	Values
Name	Filters based on the VPN connection name. It returns a list of VPN connections that satisfy the name condition/string.	(VPN connection name string)
EBGP Status	Filters based on the status of the EBGP gateway connection.	(Established or Not Established)
IPSEC Status	Filters based on the connection status of IPSec tunnel.	(Connected or Disconnected)

VPN Connection Details View

The VPN Connection details page provides detailed information about a VPN connection.

The details page has the **Summary**, **Throughput**, **IPSec Logging**, and **Routing Protocol Logging** tabs.

To access the details page of an individual VPN connection:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways you have created and configured.
3. Click the **VPN Connections** tab.

   The **VPN Connections** page opens displaying the list of VPN connections created for the clusters.
4. Click the name of a VPN connection to open the details page of the connection.

   The **Summary** tab opens displaying the detailed information about the VPN connection in widgets.

> **Note:** For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

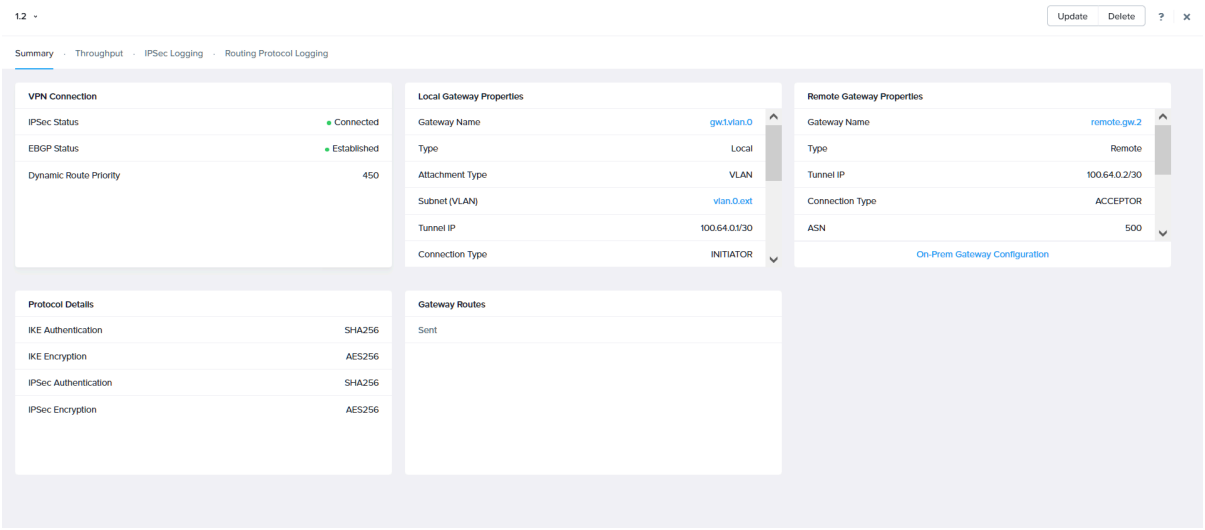


Figure 166: VPN Connection Details

Summary Tab

The **Summary** tab provides detailed information about a VPN connection in widgets.

The following table describes the fields that appear in the **Summary** tab.

Table 94: VPN Connection Summary Tab - Field Description

Parameter	Description	Values
VPN Connection widget		
IPSec Status	Displays the connection status of IPSec tunnel.	(Connected or Not Connected)
EBGP Status	Displays the status of the EBGP gateway connection.	(Established or Not Established)
Dynamic Routing Priority	Displays the dynamic routing priority assigned to the connection for throughput management. You can assign any value in the range of 100-1000. Flow Virtual Networking assigns the first VPN connection the value 500 by default. Thereafter, subsequent VPN connections are assigned values decremented by 50. For example, the first connections is assigned 500, then the second connection is assigned 450, the third one 400 and so on.	(Number in the range of 100-1000. User assigned.)
Local Gateway Properties widget		
Gateway Name	Displays the name of the local gateway used for the connection.	(Name of local gateway)
Type	Displays the type of gateway.	(Local)
Attachment Type	Displays the network entity like VLAN or VPC that the gateway is attached to.	(VLAN or VPC)

Parameter	Description	Values
VPC or Subnet (VLAN)	Displays the name of the attached VPC or VLAN subnet.	(Name of VLAN or VPC)
Tunnel IP	Displays the Tunnel IP address of the local gateway.	(IP Address)
Connection Type	Displays the connection type you selected while creating the VPN connection. The connection type may be Initiator or Acceptor of a VPN connection between the local and remote gateways. T	(Initiator or Acceptor)
External Routing	Displays the type of routing associated with the gateway for external traffic routing.	(Static or eBGP with ASN)
Internal Routing	Displays the type of routing associated with the gateway for internal traffic routing.	(Static or eBGP with ASN)
Floating or Private IP Address	Displays the Floating (for VPC) or Private (for VLAN) IP address assigned to the gateway.	(IP Address that you assigned to the local gateway with /30 prefix when you configured the VPN connection.)
Status	Displays the operational status of the gateway.	(Up or Down)
Cluster	Displays the name of the cluster on which the gateway is created.	(Cluster name)
Gateway VM	Displays the name of the VM on which the gateway is created.	(Name of VM - actionable link. Click the name-link to open the VM details page of the gateway VM.)
Remote Gateway Properties widget		
Gateway Name	Displays the name of the remote gateway used for the connection.	(Name of remote gateway)
Type	Displays the type of gateway.	(Remote)
Tunnel IP	Displays the Tunnel IP address of the remote gateway.	(IP Address)
Connection Type	Displays the connection type you selected while creating the VPN connection. The connection type may be Initiator or Acceptor of a VPN connection between the local and remote gateways. T	(Initiator or Acceptor)
External Routing	Displays the type of routing associated with the gateway for external traffic routing.	(Static or eBGP with ASN)
ASN	Displays the ASN of the EBGP route. This information is only displayed if you configured EBGP as the External Routing protocol.	(Number)
Vendor	Displays the name of the vendor of the gateway appliance at the remote site.	(Name of vendor of gateway appliance)

Parameter	Description	Values
External IP	Displays the IP address assigned to remote the gateway.	(IP Address that you assigned to the remote gateway with /30 prefix when you configured the VPN connection.)
Status	Displays the operational status of the gateway.	-
Protocol Details widget		
Service	Displays the service used by the gateway.	(VPN or VTEP)
Gateway Routes widget	Displays the status of the routes used by the gateways.	(Sent)

You can perform the following actions from the **Summary** tab:

- View the detailed information of a VPN connection. For the list of available parameters, see the *VPN Connection Summary Tab* table above.
- Update an existing VPN connection by clicking **Update**. For more information, see Updating VPN Connection in the *Flow Virtual Networking Guide*.
- Delete an existing VPN connection by clicking **Delete**. For more information, see Deleting a VPN Connection in the *Flow Virtual Networking Guide*.

Throughput Tab

The **Throughput** tab provides a graphical representation of the throughput of the VPN connection.

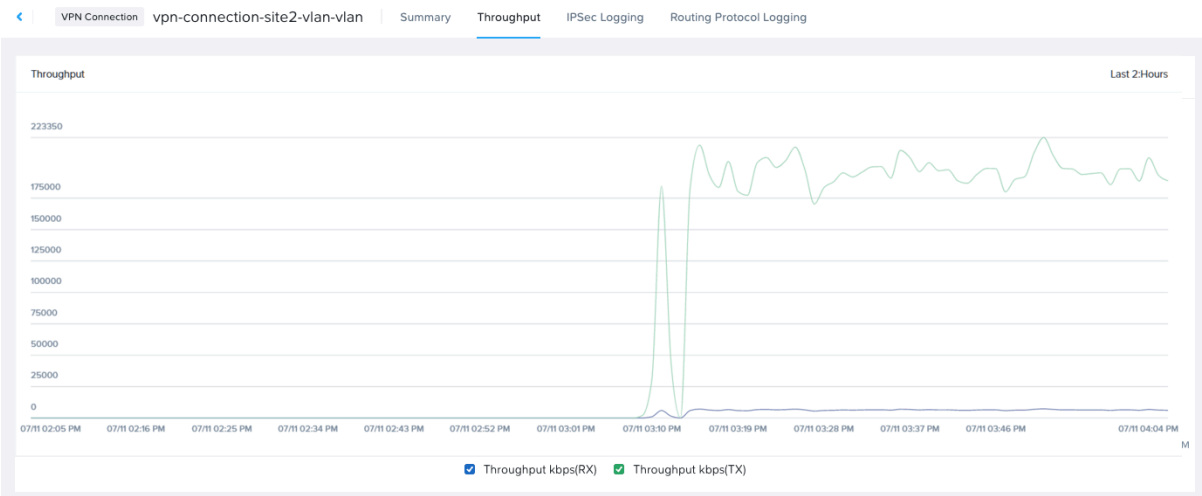


Figure 167: VPN Connections Details View - Throughput tab sample

IPSec Logging

The **IPSec Logging** tab provides logs for the IPSec tunnel.

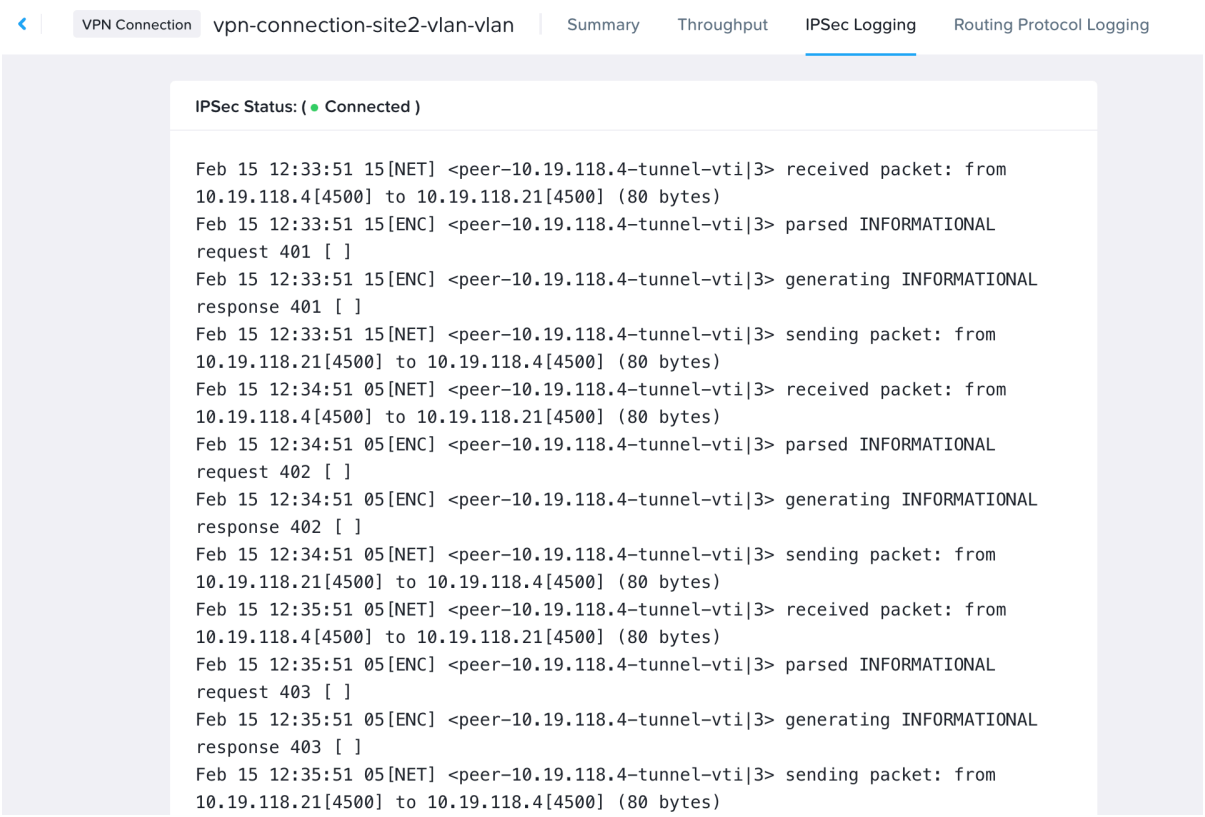


Figure 168: IPSec Logs tab sample for a VPN

Routing Protocol Logging

The **Routing Protocol Logging** tab provides logs for the routing protocol used in the VPN connection.

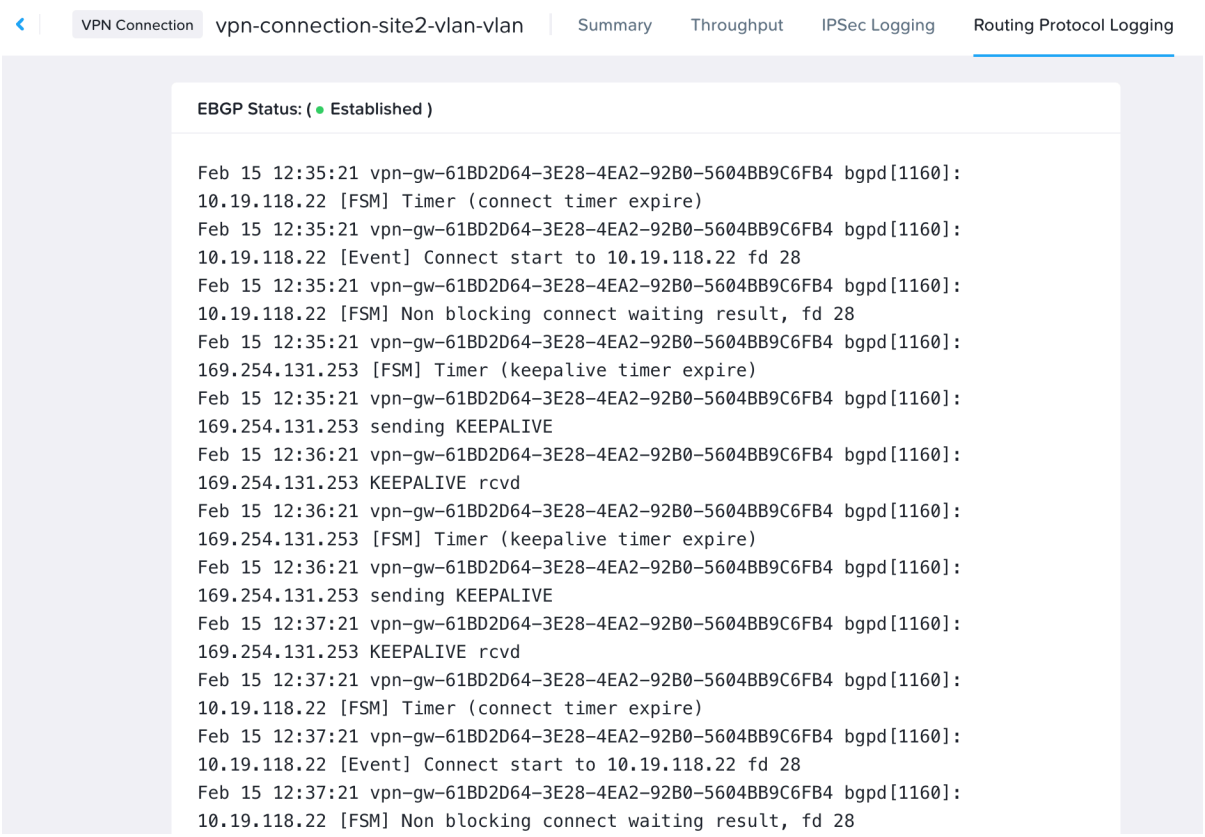


Figure 169: Routing Protocol Logs tab sample for a VPN

Subnet Extensions Summary View

The **Subnet Extensions** page displays a list of subnet extensions created for the clusters managed by Prism Central.

To access the **Subnet Extensions** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways.
3. Click the **Subnet Extensions** tab.

   The **Subnet Extensions** page opens displaying the list of subnet extensions created for the clusters.

> **Note:** For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

The following table describes the fields that appear in the **Subnet Extensions** page.

Table 95: Subnet Extensions – Field Description

Parameter	Description	Values
Name	Displays the name of the subnet extension.	(Name of subnet extension)

Parameter	Description	Values
Type	Displays the subnet extension type.	(**Across Availability Zones** or **To a Third Party Data Center**)
Extension Over	Displays the service that the subnet extension uses.	(VPN or VTEP)
Extension Uses	Displays the name of the local network gateway that the subnet extension uses.	(Name of local network gateway)
Local Subnet	Displays the name of the local subnet that the subnet extension uses.	(Name of local subnet)
Remote Site	Displays the name of the remote network gateway that the subnet extension uses.	(Name of remote network gateway)
Connection Status	Displays the status of the connection that is created by the subnet extension. **Note: Not Available** status indicates that Prism Central is unable to ascertain the status.	(Not Available, Connected, or Disconnected)
Interface Status	Displays the status of the interface that is used by the subnet extension.	(Connected or Down)

You can perform the following actions for a subnet extension from the **Subnet Extensions** page:

- Click the name of a subnet extension to open the subnet extension details page, which displays the detailed information about the extension. For more information, see Subnet Extension Details View on page 388.
- Extend a subnet **Across Availability Zones** or **To a Third Party Data Center** by clicking the **Create Subnet Extension** dropdown menu. You can extend a subnet using **VPN** or **VTEP** service. For more information, see Layer 2 Virtual Network Extension in the *Flow Virtual Networking Guide*.
- Update or delete existing subnet extension using the **Actions** dropdown menu. The **Actions** dropdown appears when one or more subnet extensions are selected. For more information, see Updating an Extended Subnet or Removing an Extended Subnet in the *Flow Virtual Networking Guide*.
- Filter the subnet extension list based on various parameter values using the **Filters** pane. For more information, see Filters Pane - Subnet Extensions Page.

Filters Pane - Subnet Extensions Page

You can filter the information in the **Subnet Extensions** page based on the following fields that are available in the **Filters** pane. For information about how to use the Filters pane, see the Filters Pane information.

Table 96: Filter Pane Field Description - VPN Connections page

Field	Description	Values
Name	Filters based on the subnet extension name. It returns a list of subnet extensions that satisfy the name condition/string.	(Subnet extension name string)

Field	Description	Values
Connection Status	Filters based on the status of the connection that is created by the subnet extension.	(Connected or Disconnected)
Interface Status	Filters based on the status of the interface that is used by the subnet extension.	(Connected or Not Available)

Subnet Extension Details View

The Subnet Extension details page provides detailed information about a subnet extension.

The details page has the **Summary**, **Address Table**, and **Throughput** tabs.

To access the details page of an individual subnet extension:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways you have created and configured.

   > **Note:** For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

3. Click the **Subnet Extensions** tab.

   The **Subnet Extensions** page opens displaying the list of subnet extensions created for the clusters.
4. Click a subnet extension to open the details page of the extension.

   The **Summary** tab opens displaying the detailed information about the extension in widgets.

Summary Tab

The **Summary** tab provides detailed information about the subnet extension in widgets.

The subnet extension **Summary** tab has the following widgets:

Table 97: Subnet Extension Summary Tab Widgets

Parameter	Description	Values
Properties widget		
Type	Displays the subnet type.	(VLAN or Overlay)
VLAN ID	(For VLAN subnets only) Displays the VLAN ID of the VLAN subnet that is extended.	(VLAN ID number)
VPC	(For Overlay subnets only) Displays the name of the VPC subnet that is extended.	(Name of VPC)
Cluster	(For VLAN subnets only) Displays the cluster that the VLAN subnet belongs to.	(Name of cluster)
IP Address Prefix	Displays the network IP address with prefix, of the VLAN subnet that is extended.	(IP Address with prefix)
Virtual Switch	(For VLAN subnets only) Displays the virtual switch on which the VLAN subnet is configured.	(Virtual Switch name such as vs0 or vs1)
IP Address Pools widget		

Parameter	Description	Values
Pool Range	Displays the range of IP addresses in the pool configured in the subnet that is extended.	(IP address range)
(Interactive Graphic Pie Chart)	Displays a dynamic pie chart that displays the statistic you hover on. Displays the following IP address statistics outside the pie chart, that you can hover on: • Total number of IP addresses available. • Used IP addresses in the subnets • Used IP addresses in the IP address pools • Free IP addresses in the subnets • Free IP addresses in the IP address pools	(IP Address statistics)
Subnet Extension widget		
Subnet Extension (properties) - Common		
Type	Displays the subnet extension type.	(**Across Availability Zones** or **To a Third Party Data Center**)
Interface Status	Displays the status of the interface that is used by the subnet extension.	(Connected or Down)
Connection Status	Displays the status of the connection that is created by the subnet extension. **Not Available** status indicates that Prism Central is unable to ascertain the status.	(Not Available, Connected, or Disconnected)
Local IP Address	Displays the IP address that you entered in the **Local IP Address** field while creating the subnet extension.	(IP Address)
Local Subnet	Displays the name of the local subnet that the subnet extension uses.	(Name of local subnet)
Subnet Extension (properties) - (Only for **Across Availability Zones** type)		
Local Availability Zone	(Only for **Across Availability Zones** type) Displays the name of the local AZ that is hosting the subnet that is extended.	(Name of the local Availability Zone)
Remote Availability Zone	(Only for **Across Availability Zones** type) Displays the name of the remote AZ that the subnet is extended to.	(Name of the remote Availability Zone)
Remote Subnet	(Only for **Across Availability Zones** type) Displays the name of the remote subnet that the subnet extension connects to.	(Name of remote subnet)
Remote IP Address	(Only for **Across Availability Zones** type) Displays the IP address that you entered in the **Remote IP Address** field while creating the subnet extension.	(IP Address)

Parameter	Description	Values
Subnet Extension (properties) - (Only for **To a Third Party Data Center** type)		
Local Gateway	(Only for **To a Third Party Data Center** type) Displays the name of the local gateway used for the subnet extension.	(Name of local gateway)
Remote Gateway	(Only for **To a Third Party Data Center** type) Displays the name of the remote gateway used for the subnet extension.	(Name of remote gateway)

You can perform the following actions from the **Summary** tab:

- View the detailed information of a subnet extension. For the list of available parameters, see the *Subnet Extension Details - Summary Tab Fields* table above.
- Update an existing subnet extension by clicking **Update**. For more information, see Updating an Extended Subnet in the *Flow Virtual Networking Guide*.
- Delete an existing subnet extension by clicking **Delete**. For more information, see Removing an Extended Subnet in the *Flow Virtual Networking Guide*.

Address Table Tab

The **Address Table** tab provides MAC Address information only when the subnet extension uses VTEP service. The tab provides the following information:

- **MAC Address**: This provides the MAC addresses of devices connected to the remote VTEP endpoint in the subnet extension.
- **Remote VTEP Endpoint**: This provides the IP address of the remote VTEP endpoint in the subnet extension.

Throughput Tab

The **Throughput** tab provides a graphical representation of the throughput of the subnet extension.

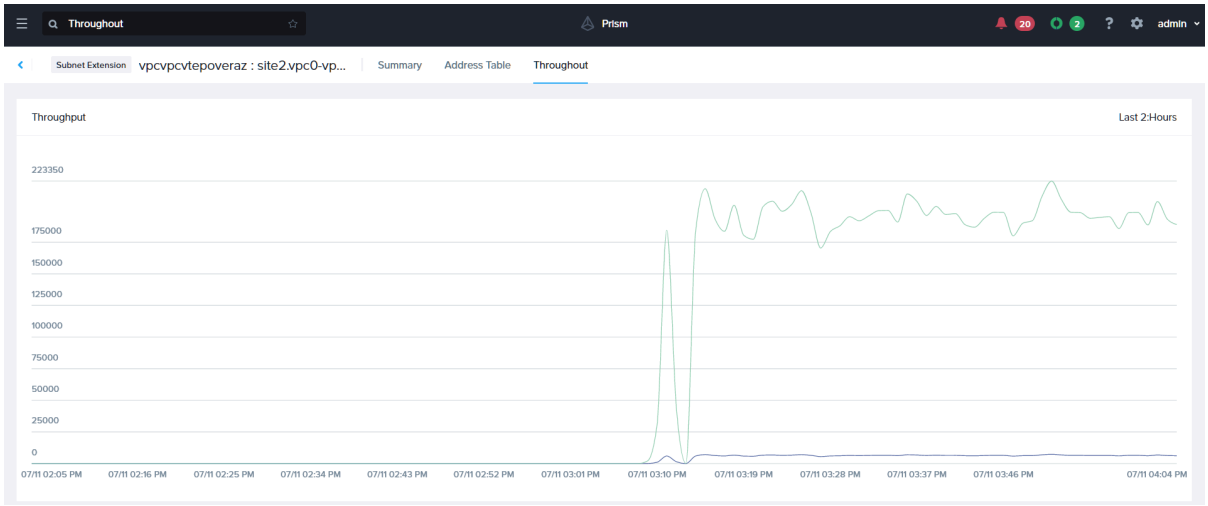


Figure 170: Subnet Extension Details View - Throughput tab sample for VTEP Extension

BGP Sessions Summary View

The **BGP Sessions** page displays a list of BGP sessions created for the clusters managed by Prism Central.

To access the **BGP Sessions** page:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways.

   > **Note:** For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

3. Click the **BGP Sessions** tab.

   The **BGP Sessions** page opens displaying the list of BGP sessions created for the clusters.

The following table describes the fields that appear in the **BGP Sessions** page.

Table 98: BGP Sessions – Field Description

Parameter	Description	Values
Name	Displays the name of the BGP session.	(Name of BGP session)
Serviced VPC	Displays the name of the VPC that the BGP session services.	(Name of VPC)
Local Gateway	Displays the name of the local BGP gateway that the BGP session uses.	(Name of local BGP gateway)
Remote Gateway	Displays the name of the remote BGP gateway that the BGP session uses.	(Name of remote BGP gateway)
Session Status	Displays the status of the eBGP session. • Displays **Established** if the session is **Up**. • Displays **Active** when the network controller is attempting to establish the session.	**Established** or **Active**

Parameter	Description	Values
Route Priority	Displays an integer number that denotes the route priority. When the route priority is assigned dynamically, then the network controller assigns integer numbers (usually between 600 and 800 starting with 700) in descending order with steps of 5. For example, the first session is assigned 700 as route priority and then when you create the second session, the controller assigns it a route priority of 695 and a third session is assigned 690. Greater the number, greater is the route priority. With dynamically assigned priority, the priority is assigned in the order of reducing priority to the order of BGP sessions created. The BGP session created first gets the highest priority 700, the second session get the second highest priority 695 and so on. You can manually assign a route priority as well by assigning any number between 300 and 900.	(Integer Number)

You can perform the following actions for a gateway from the **BGP Sessions** page:

- Click the name of a BGP session to open the details page, which displays the detailed information about the BGP session. For more information, see BGP Session Details View on page 393.
- Create a BGP session by clicking **Create BGP Session**. For more information, see Creating a BGP session in the *Flow Virtual Networking Guide*.
- Update or delete an existing BGP session using the **Actions** dropdown menu. The **Actions** dropdown menu appears when one or more BGP sessions are selected. For more information, see Updating a BGP session or Deleting a BGP session in the *Flow Virtual Networking Guide*.
- Filter the gateway list based on various parameter values using the **Filters** pane. For more information, see Filters Pane - BGP Sessions Page.

Filters Pane - BGP Sessions Page

You can filter the information in the **BGP Sessions** page based on the following fields that are available in the **Filters** pane. For information about how to use the Filters pane, see the Filters Pane information.

Table 99: Filter Pane Field Description - BGP Sessions page

Field	Description	Values
Name	Filters based on the BGP session name. It returns a list of BGP sessions that satisfy the name condition/ string.	(BGP session name string)
Session Status	Filters based on the status of the eBGP session.	(Established or Down)

BGP Session Details View

The BGP Session details page provides detailed information about a BGP session.

The details page has the **Summary**, **Routes**, and **BGP Logs** tabs.

To access the details page of an individual BGP session:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Network & Security** > **Connectivity** from the **Navigation Bar**.

   The **Gateways** page opens displaying the list of network gateways you have created and configured.

   > **Note:** For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

3. Click the **BGP Sessions** tab.

   The **BGP Sessions** page opens displaying the list of BGP sessions created for the clusters.
4. Click the name of a BGP session to open the details page of the session.

   The **Summary** tab opens displaying the detailed information about the BGP session in widgets.

Summary Tab

The **Summary** tab provides detailed information about the BGP session in widgets.

The BGP session **Summary** tab has the following widgets:

Table 100: BGP Session Summary Tab Widgets

Parameter	Description	Values
Properties widget		
Session Status	Displays the overall status of the BGP session.	(Up or Down)
eBGP Status	Displays the eBGP status of the BGP session.	**Established** or **Active**
Route Priority	Displays an integer number that denotes the route priority. For more information about Route Priority, see BGP Sessions Summary View on page 391.	(Integer Number)
Local Gateway widget		
Local Gateway	Displays the name of the local BGP gateway.	(Name)
eBGP ASN	Displays the ASN of the local BGP gateway used by the session. It would be an integer number in the 1-65000 range. **Note:** Make sure that this ASN does not conflict with any of the other on-premises BGP ASNs.	(Number)
Remote Gateway widget		
Remote Gateway	Displays the name of the remote BGP gateway.	(Name)

Parameter	Description	Values
eBGP ASN	Displays the ASN of the remote BGP gateway used by the session. It would be an integer number in the 1-65000 range. **Note:** Make sure that this ASN does not conflict with any of the other on-premises BGP ASNs.	(Number)

You can perform the following actions from the **Summary** tab:

- View the detailed information of a BGP session. For the list of available parameters, see the *BGP Session Details - Summary Tab Fields* table above.
- Update an existing BGP session by clicking **Update**. For more information, see Updating a BGP session in the *Flow Virtual Networking Guide*.
- Delete an existing BGP session by clicking **Delete**. For more information, see Deleting a BGP session in the *Flow Virtual Networking Guide*.

Routes Tab

The **Routes** tab provides a list of the routes used by the BGP session with the corresponding **Next Hop** details. It has the following lists:

- **Advertised** (default): The **Routes** tab opens in the **Advertised** list. The **Advertised** list provides a list of the advertised routes with the corresponding **Next Hop** details.
- **Received**: This list provides list of the routes received from remote with the corresponding **Next Hop** details.

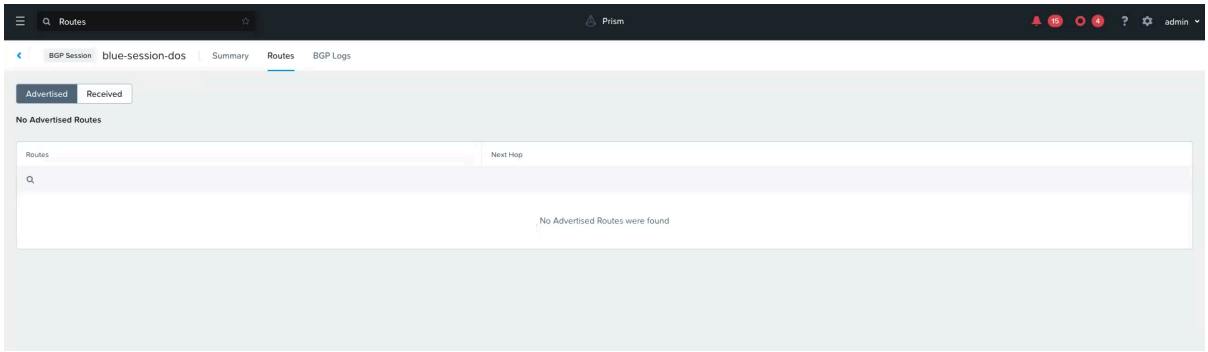


Figure 171: BGP Session Details View - Routes Advertised tab sample for a BGP session

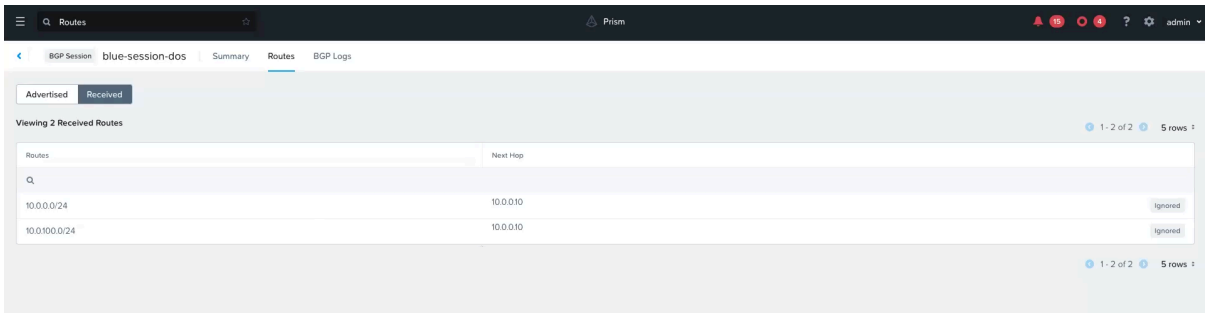


Figure 172: BGP Session Details View - Routes Received tab sample for a BGP session

BGP Logs Tab

The **BGP Logs** tab provides detailed live logs for the BGP session. This information can be very useful in monitoring and debugging a BGP session.

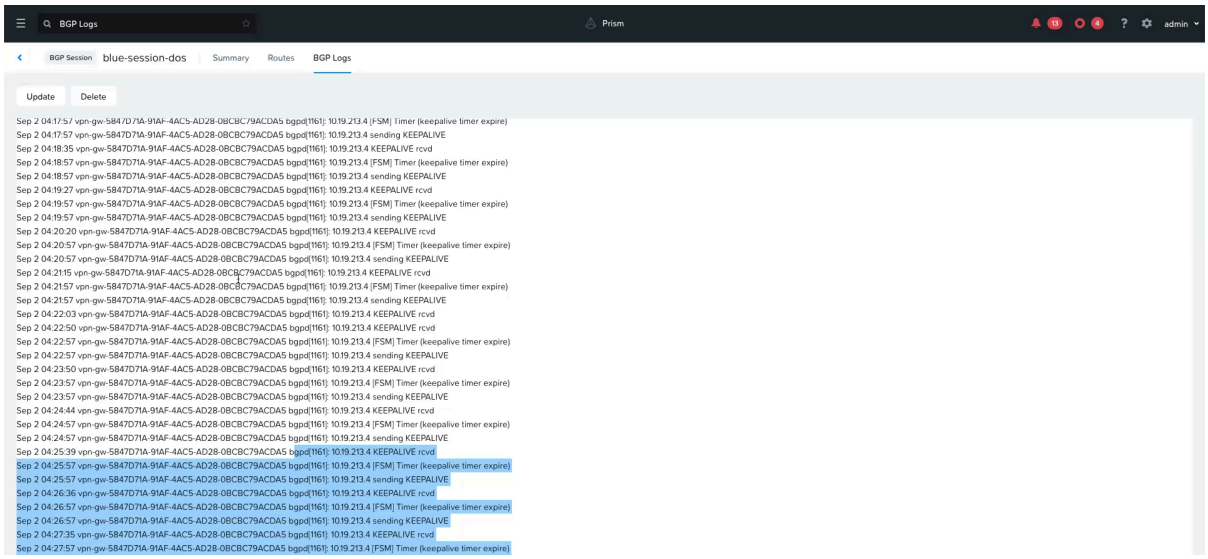


Figure 173: BGP Session Details View - BGP Logs tab sample for a BGP session

Security Policies

Security policies are defined using Nutanix Flow that provides a policy-driven security framework to inspect traffic within the data center.

For information about how to create and apply security policies, see Flow Microsegmentation Guide.

For information about how to view security policies in Prism Central, see Security Policies Summary View on page 490 or Security Policy Details View on page 494.

Security Dashboard

The Security Dashboard provides dynamic summary of the security posture across all registered clusters. The Security Dashboard allows you to view the most critical security parameters like cluster-based issue summary, STIG policy compliance, security hardening, and identified vulnerabilities. For more information, see Security Dashboard in the *Nutanix Security Guide*.

DATA PROTECTION AND RECOVERY ENTITIES

You can access dashboards for the following data protection types from the **Data Protection** entity of the **Infrastructure** application. For information about how to access the entity items available in **Data Protection** entity, see Application-specific Navigation Bar on page 57.

- Protection Summary on page 396
- Protection Policies on page 396
- Recovery Plans on page 396
- VM Recovery Points on page 396
- VG Recovery Points on page 396
- Consistency Groups on page 396

Protection Summary

Protection Summary provides a detailed information about the Nutanix Disaster Recovery entities in an AZ, and helps you to generate DR reports for the specified time. It also enables you to monitor the health of your DR deployments and the activities performed on the Nutanix Disaster Recovery entities. For more information about **Protection Summary**, see Nutanix Disaster Recovery Guide.

Protection Policies

A Protection policies is a configurable policy that takes recovery points of the protected entities (guest VMs, volume groups, and consistency groups) in equal time intervals, and replicates those recovery points to the recovery AZs. For more information about protection policies, see Nutanix Disaster Recovery Guide.

Recovery Plans

The Recovery plans are used in automated Disaster Recovery (DR) configurations to orchestrate the recovery of the protected entities to different Nutanix clusters at the same or different AZs. For more information about recovery plans, see Recovery Plans View information in *Nutanix Disaster Recovery Guide*.

VM Recovery Points

The protection policy associated with the VM creates the VM recovery points. For more information about VM recovery points, see Nutanix Disaster Recovery Guide.

VG Recovery Points

VG Recovery Points lists the recovery points of all the protected volume groups (generated over time) on the local cluster. For more information about VG recovery points, see Nutanix Disaster Recovery Guide.

Consistency Groups

A consistency group is a collection of the entities that are treated as a single group and backed up collectively in a recovery point. For information about Consistency Groups, see Consistency Groups information in *Nutanix Disaster Recovery Guide* .

HARDWARE ENTITIES

You can access dashboards for the following hardware components from the **Hardware** entity of the **Infrastructure** application. For information about how to access the entity items available in **Hardware** entity, see Application-specific Navigation Bar on page 57.

- Clusters (see Clusters Summary View on page 398)
- Hosts (see Hosts Summary View on page 420)
- Disks (see Disks Summary View on page 438)
- GPUs (see GPUs Summary View on page 444)

Cluster Management

In Prism Central, the clusters dashboard allows you to view summary information about all the registered clusters and access the detailed information about each cluster. For more information, see Clusters Summary View on page 398 and Cluster Details View on page 405.

The **Actions** menu appears when a cluster is selected. The following table provides the information about all the actions that you can perform to manage the clusters:

> **Note:** The available actions appear in bold; other actions are disabled. For disabled options, you can see a tool tip explaining the reason. The available actions depend on the current state of the selected clusters.

Table 101: Cluster Actions

Action	Description	Applicable to Multiple Clusters
Launch Prism Element	Launch Prism element for that cluster in a separate tab or window (depending on your browser settings). **Note:** When you access a cluster from Prism Central, you log in through your Prism Central user account, not a cluster user account. As a result, the cluster user configuration options are different (more limited) than when logging directly into the cluster. The options that appear in the Prism Element main menu user dropdown list are **REST API Explorer**, **About Nutanix**, **Support Portal**, **Help**, **Nutanix Next Community**, and **Sign Out**.	No
Upgrade Software	Upgrade the AOS version on the cluster. For more information, see Prism Central Installation or Upgrade on page 32.	Yes
Rack Configuration	Configure the rack awareness feature. This option appears only for clusters that satisfy the conditions for rack awareness. For instructions on configuring rack awareness, see Rack Fault Tolerance in *Prism Element Web Console Guide*.	No
Manage Categories	Configure and manage cluster categories.	No
Enable Efficiency Measurement	Enable efficiency measurement for the cluster.	Yes

Action	Description	Applicable to Multiple Clusters
Disable Efficiency Measurement	Disable efficiency measurement for the cluster.	Yes
Enable Anomaly Detection	Enable Anomaly Detection for the cluster.	Yes
Disable Anomaly Detection	Disable Anomaly Detection for the cluster.	Yes
Run Playbook	Run or create a new playbook for the cluster entity type.	Yes
Manage & Backup Keys	Download the encryption keys for the cluster. If the cluster goes down, you can access your data with the backup key.	No
Enable Data-at-Rest Encryption	Enable Data-at-Rest Encryption for the cluster.	Yes
Manage KMS Types	Manage the Key Management Solution (KMS) for the cluster.	No
Enable Data-in-transit Encryption	Enable Data-in-transit Encryption for the cluster.	Yes
Disable Data-in-transit Encryption	Disable Data-in-transit Encryption for the cluster.	Yes
Manage Rebuild Capacity	Manage Rebuild Capacity for a cluster having a minimum of three nodes. For more information about rebuild capacity, see Rebuild Capacity Reservation in Prism Element Web Console Guide.	No
Manage Recycle Bin	Manage Recycle Bin for the cluster. You can choose to retain the deleted VMs and volume groups for a specific retention time (1 to 7 days). This feature is supported for clusters running AOS 6.6.1 and later.	No
Manage Redundancy State	Manage redundancy state for the cluster based on your cluster configuration. The redundancy factor determines the cluster's readiness to recover from an unexpected hardware failure. Set this factor to define the number of failures that your cluster can tolerate.	No
Maintenance Resiliency	Disable the default cluster resiliency preference setting of *Smart*. If you clear the *Smart* checkbox, the system changes the cluster resiliency preference to *Immediate*. For more information on cluster resiliency preference, see Cluster Resiliency Preference section in *Web Console Guide*. **Note:** Starting with AOS 6.8 release, the cluster resiliency preference is set as *Smart* by default.	No
Expand Cluster	Expand a cluster. For information on expanding a cluster, see Expanding a Cluster through Prism Central on page 430	No
Destroy Cluster	Destroy a cluster. For information on destroying a cluster, see Destroying a Cluster on page 418.	Yes

Clusters Summary View

The **Summary** tab on the **Clusters** page provides a dashboard of all the registered clusters.

To access the summary view of all the clusters, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Hardware** > **Clusters** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The system displays the **List** tab by default with all the registered clusters in **Nutanix** environment.
3. Click the **Summary** tab. The system displays **Summary** page for all the clusters.

> **Note:** To access the summary view of all the non-nutanix clusters managed by *vCenter*, select **Non-Nutanix** from the dropdown menu in **Clusters** page.
>
> The **Summary**, **Alerts**, and **Events** tabs display the same information as for Nutanix-managed clusters. The **Metrics** tab displays CPU usage, memory usage, and VM operations. The **List** tab displays fields for name, host count, VM count, storage usage, and storage capacity.

Using playbooks, you can manage the clusters in **Non-Nutanix** environment. For more information about playbooks, see Task Automation - Playbooks in *Intelligent Operations Guide*.

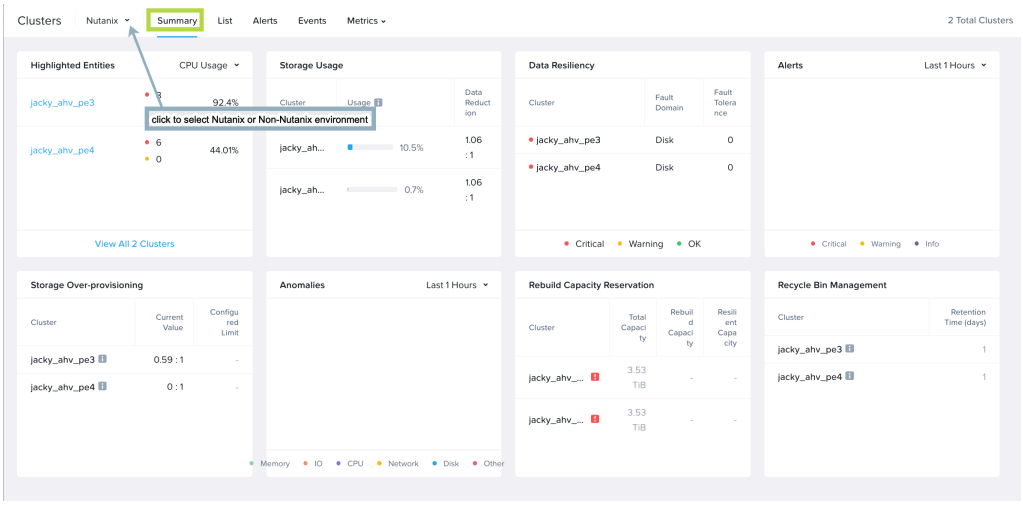


Figure 174: Summary Page - All Clusters

The **Summary** page for all clusters displays information about all the registered clusters and allows you to access detailed information about each cluster.

The **Clusters** page includes the following tabs on the left: **Summary**, **List**, **Alerts**, **Events**, and **Metrics** with a display area below the selected tab.

> **Note:** This section describes the information and options that appear in the **Summary** page for all clusters. For instructions on how to view and organize that information in various ways, see Prism Central GUI Organization on page 27.

The **Summary** tab for all the clusters displays the following widgets:

- **Highlighted Entities**: Displays a list of clusters with the highest usage of the parameter you select from the dropdown menu on the right of the widget. The options are **CPU Usage**, **IO Latency**, **IOPS**, and **Memory Usage**. Click the **View all XX Clusters** link at the bottom to display the **List** tab (following section).
- **Storage Usage**: Displays a list of clusters along with the percentage usage (with respect to total usable capacity of the cluster) and data reduction. Total usage is calculated as the sum of used capacity and

free reserved capacity. Data reduction ratio displays the ratio of how much the data size is reduced by enabling compression, deduplication, and erasure coding. Placing the cursor anywhere on the horizontal axis displays a breakdown view of the storage capacity usage.

- **Data Resiliency**: Displays a list of clusters along with the fault domain and the current state of the fault tolerance. Fault tolerance of a cluster can have any one of the following states:
  - OK: This state indicates that the fault tolerance domain is highly resilient to safely handle a node or a disk (in single or two node clusters) failure.
  - Warning: This state indicates that the fault tolerance level is almost reaching to 0. Warning state is displayed if the cluster is not fault tolerant at the configured domain, but is fault tolerant at a lower domain. For example, if you have configured rack as the configured domain and the cluster can no longer handle any rack failures due to some reason but can still handle node (lower domain) failures, then fault tolerance state is displayed as Warning.
  - Critical: This state indicates that the fault tolerance level is 0, and the fault tolerance domain cannot handle a node or a disk (in single or two node clusters) failure.
  - Computing: This state indicates that the new fault tolerance level is being calculated. This state is displayed soon after a node or disk failure, before rebuild is initiated.
- **Alerts**: Displays a list of cluster-related alerts that occurred during the specified interval. Select either **Last 24 hours** (default), **Last 1 Hours**, or **Last week** from the dropdown menu. When an alert appears, you can click on the graph, which then displays a list of those alerts. Clicking on an alert displays the details page for that alert.
- **Storage Over-provisioning**: Displays a list of the clusters along with the storage over-provisioning ratio (calculated based on the provisioned storage and the available raw storage). The current value and state of storage over-provisioning ratio is displayed according to the configured limits.
- **Rebuild Capacity Reservation**: Displays a list of clusters with their total capacity, rebuild capacity, and resilient capacity. For more information about rebuild capacity, see Rebuild Capacity Reservation section in Prism Element Web Console Guide.
- **Recycle Bin Management**: Displays a list of clusters with their retention time in days. For more information on Recycle Bin, see Recycle Bin in the *Prism Element Web Console Guide*.
- **Anomalies**: Displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified interval. Select either **Last 24 hours** (default), **Last 1 Hours**, or **Last week** from the dropdown menu. When an anomaly appears, you can click on the graph, which then displays a list of those anomalies. Clicking on an anomaly displays the event page for that anomaly.

Lists Tab

The **List** tab displays the list of clusters.

To access the **Lists** tab of all clusters:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Hardware** > **Clusters** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The system displays the **List** tab by default with clusters.

   > **Note:** You can use the **View by** and **Group by** options to create your own customized view and add the necessary columns to that view. For more information on how to **View by** and **Group by** options, see Prism Central GUI Organization on page 27.

The following table describes the fields that appear in the clusters **List** tab.

Note: The fields vary based on the **View by** and **Group by** options. A dash (-) is displayed in a field when a value is not available or applicable. For more information about **View by** and **Group by** options, see Prism Central GUI Organization on page 27.

Table 102: Clusters List Fields

Parameter	Description	Values
View by **General** Fields		
Name	Displays the cluster name. Clicking on the name displays the details page for that cluster. For more information, see Cluster Details View on page 405.	(cluster name)
AOS Version	Displays the version number of AOS running on the cluster.	(version number)
Upgrade Status	Displays the current upgrade status. There are various stages from scheduled to succeeded (or failed).	Pending, Downloading, Queued, PreUpgrade, Upgrading, Succeeded, Failed, Cancelled, Scheduled
Hypervisors	Displays the hypervisor type running in the cluster. In the case of a mixed cluster such as one running ESXi or Hyper-V that also includes NX-6035C nodes running AHV, both hypervisor types are listed.	AHV, ESX, Hyper-V
Host Count	Displays the number of hosts (nodes) in the cluster.	(number of nodes)
VM Count	Displays the total number of VMs in the cluster (in any state).	(number of VMs)
Cluster Runway	Displays the predicted runway (time period) before the cluster requires additional resources. For more information, see the *Capacity Tab* section in Cluster Details View on page 405.	(number of days)
Inefficient VMs	Displays the number of inefficient VMs in the cluster. For more information, see Behavioral Learning Tools in *Intelligent Operations Guide*.	(number)
View by **Performance** Fields		
Name	Displays the cluster name.	(cluster name)
CPU Usage	Displays the percentage of CPU capacity in the cluster currently being used.	0 -100%
Memory Usage	Displays the percentage of memory capacity in the cluster currently being used.	0 -100%
IOPS	Displays total (both read and write) I/O operations per second (IOPS) for this cluster.	(number)

Parameter	Description	Values
IO Bandwidth	Displays total I/O bandwidth used per second in this cluster.	xxx [MBps|KBps]
IO Latency	Displays the average I/O latency in this cluster.	xxx [ms]
View by **Capacity** Fields		
Name	Displays the cluster name.	(cluster name)
Cluster Runway	Displays the predicted runway (time period) before the cluster requires additional resources. For more information, see the *Capacity Tab* section in Cluster Details View on page 405.	(number of days)
CPU Runway	Displays the predicted CPU runway (time period) before the cluster requires additional resources.	(number of days)
Memory Runway	Displays the predicted memory runway (time period) before the cluster requires additional resources.	(number of days)
Storage Runway	Displays the predicted storage memory runway (time period) before the cluster requires additional resources.	(number of days)
View by **Encryption** Fields		
Name	Displays the cluster name.	(cluster name)
Data-at-Rest Encryption	Displays the cluster encryption type.	Not Encrypted, Software, Hardware, Software and Hardware
KMS Type	Displays the key management system (KMS) type.	Not Set, Native (Local), Native (Remote), External
Data-in-Transit Encryption	Displays the cluster encryption type.	Not Encrypted, Software, Hardware, Software and Hardware
Host Count	Displays the number of hosts (nodes) in the cluster.	(number of nodes)

You can perform the following actions for the clusters in the **Lists** tab:

- Create a cluster. For information about how to create a cluster, see Creating a Cluster on page 417.
- Access the detailed information about an individual cluster. For more information, see Cluster Details View on page 405.
- Filter the clusters list based on available parameter values using **Filters** pane. For more information about **Filters** pane, see the following section *Filters Pane - Clusters Page*.
- Export the table that contains the list of clusters and their information to a file in a CSV format. For more information about **Export** option, see Export on page 32.
- Group the clusters based on pre-defined criteria. For information about how to group the clusters, see Group by on page 29.

- View clusters based on pre-defined criteria or create a custom view. For information about available views and how to create a custom view, see View by on page 29.
- Assign a label to the filtered criteria. For information about how to define a label, see Label on page 32.
- Perform the cluster-specific actions on a single or multiple clusters using the **Actions** dropdown menu. For more information, see Cluster Management on page 397.

Filters Pane - Clusters Page

The following table describes the fields available in the **Filters** pane:

Table 103: Filters Pane

Parameter	Description	Values
Labels	Filters on label name. Select one or more labels from the dropdown list. (If there are no labels currently, a message about how to create labels is displayed.)	(label names)
Name	Filters on the cluster name. Select a condition from the dropdown list (**Contains**, **Doesn't contain**, **Starts with**, **Ends with**, or **Equal to**) and enter a string in the field. It will return a list of clusters that satisfy the name condition/string.	(cluster name string)
AOS Version	Filters on AOS version. Select one or more versions to return a list of clusters running those version(s). The number of clusters currently running each version is displayed on the right of the line.	(Acropolis version numbers across clusters currently)
Hypervisors	Filters on the hypervisor type. Select one or more hypervisors to return a list of clusters running those hypervisor(s). The number of clusters currently running each hypervisor is displayed on the right of the line.	AHV, ESXi, Hyper-V, XenServer
Health	Filters on the cluster health state (good, warning, or critical). Select one or more states to return a list of clusters in that state(s). The number of clusters currently in each state is displayed on the right of the line.	Critical, Warning, Good
CPU Usage	Filters on the amount of total CPU being used. Check the box for the desired range or enter a percentage range in the **from <low> to <high>** % field. It will return a list of clusters utilizing total CPU in that range (0-100%).	([xx] to [yy]% range)
Memory Usage	Filters on the amount of total memory being used. Check the box for the desired range or enter a percentage range in the **from <low> to <high>** % field. It will return a list of clusters utilizing total memory in that range (0-100%).	([xx] to [yy]% range)

Parameter	Description	Values
IOPS	Filters on the total (both read and write) IOPS. Check the box for the desired range or enter a range in the **from <low> to <high> iops** field. It will return a list of clusters with total IOPS in that range.	([xx] to [yy] range)
IO Bandwidth	Filters on the total I/O bandwidth used. Check the box for the desired range or enter a range in the **from <low> to <high> bps** field. It will return a list of clusters with total I/O bandwidth usage in that range.	([xx] to [yy] range)
IO Latency	Filters on the average I/O latency. Check the box for the desired range or enter a range in the **from <low> to <high> ms** field. It will return a list of clusters with average I/O latency in that range.	([xx] to [yy] range)
Upgrade Status	Filters on the current upgrade status. There are various stages from scheduled to succeeded (or failed).	Pending, Downloading, Queued, PreUpgrade, Upgrading, Succeeded, Failed, Cancelled, Scheduled
Categories	Filters on the category type. Search for the category name. For example, ADGroup:$Default	(category name string)
Data-at-rest Encryption Type	Filters on the encryption type. Check the box for the desired encryption type. It will return a list of clusters with the corresponding encryption type applied.	Not Encrypted, Software, Hardware, Dual
Data-at-rest Encryption Scope	Filters on the encryption scope. Check the box for the entities where encryption is applied on. It will return a list of clusters with the corresponding encryption scope applied.	Cluster, Entity
KMS Type	Filters on the key management system (KMS) type.	Not Set, Native (Local), Native (Remote), External
Data-in-Transit Encryption	Filters on the encryption type. Check the box for the desired encryption type. It will return a list of clusters with the corresponding encryption type applied.	Not Enabled, Enabled

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options that are available on the **Activity** > **Alerts** page, however it only displays the cluster-related alerts. For more information about alerts, see *Prism Central Alerts and Events Reference Guide*.

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options that are available on the **Activity** > **Events** page, however it only displays the cluster-related events. For more information about events, see *Prism Central Alerts and Events Reference Guide*.

Metrics Tab

The **Metrics** tab allows you to view usage metrics across the clusters. Click the **Metrics** tab to display dropdown menu of available metrics, and select the metric name to display the relevant performance information.

> **Note:** The **Metrics** dropdown menu is hypervisor-specific, and might vary based on the hypervisors used in the cluster.

Table 104: Metrics Tab Fields

Metric	Description
CPU Usage	Displays a CPU usage table listing current values and total clusters (number). The current values are split into percentile intervals (for example, less than 25%, 25-50, 50-75, more than 75%). Clicking on a percentile interval displays the Summary tab filtered to just those clusters. **Note:** The same format also applies to the other metrics in this table with either percentile or quantity intervals.
Memory Usage	Displays a memory percentage usage table.
IOPS	Displays total, read, and write IOPS tables.
IO Latency	Displays total, read, and write I/O latency rate tables.
IO Bandwidth	Displays total, read, and write I/O bandwidth rate tables.

Cluster Details View

Summary Tab

The **Summary** tab of an individual cluster consists of a dashboard that provides the detailed information about the cluster.

To access the **Summary** tab of an individual cluster:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Hardware** > **Clusters** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The system displays the **List** tab by default with all the registered clusters in **Nutanix** environment. For information about how to access the list of clusters in **Non-Nutanix** environment (non-nutanix clusters managed by external *vCenter*), see Clusters Summary View on page 398.
3. Click the target <*cluster_name*> to view the **Summary** tab of an individual cluster.

   > **Note:** Replace <*cluster_name*> with the actual cluster name at your site.

The **Summary** tab of an individual cluster provides the following widgets:

- **Properties** - Displays summary information about the cluster. For information about the fields available in **Properties** widget, see Cluster Properties Widget on page 408.
- **Metrics** - Displays the cluster metrics such as CPU usage, Memory usage, IOPS, IO latency, and IO bandwidth.

- **Alert** - Displays a list of related alerts that occurred during the specified interval. Select either **Last week** (default),**Last 1 hour**, or **Last 24 hours** from the dropdown menu on the top right corner of the widget.
- **Anomalies** - Displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified interval. Select either **Last week** (default), **Last 1 hour**, or **Last 24 hours** from the dropdown menu on the top right corner of the widget. When an anomaly appears, you can click the graph to display a list of those anomalies. If you click an individual anomaly, the system displays the event page for that anomaly.
- **VM Efficiency** - Displays the number of VMs that are considered inefficient, broken down by category (over-provisioned, inactive, constrained, and bully). For more information, see Behavioral Learning Tools in *Intelligent Operations Guide*.
- **Tier-wise Usage**: Displays a pie chart divided into the percentage of storage space used by each disk tier in the cluster. Disk tiers can include SSD, HDD, and SSD-NVMe depending on the hardware model type.
- **Storage Over-provisioning** - Displays the storage over-provisioning ratio (calculated based on the provisioned storage and the available raw storage) in the cluster. You can configure a ratio limit to alert the administrator when the ratio changes excessively. If the ratio reaches 70% of the configured limit, the widget displays a warning alert in yellow color. The widget displays Critical alert in red color if the ratio exceeds 90%. Note that the time taken for the Storage Over-provisioning Ratio widget to reflect the changes made in the cluster varies according to the recent storage operations or activities performed.
- **Data Resiliency Status** - Displays the current resiliency status of the cluster. The information includes the current failure domain (rack, block, or node) and the level of fault tolerance (FT 1 or FT 2). The widget indicates if any of the current fault domain changes from its configured state. If a data rebuild is triggered after a component failure, the widget also displays a rebuild progress indicator that enables you to track the estimated time until full resiliency has been restored to the cluster.
- **Storage Summary** - Displays information about the physical storage space utilization (in GiB or TiB) and resilient capacity of the cluster. Placing the cursor anywhere on the horizontal axis displays a breakdown view of the storage capacity usage. You can also configure a threshold warning for the

resilient capacity utilization in the cluster by clicking the gear icon at the top right corner. For more information, see Configuring a Warning Threshold for Resilient Capacity.

The View Details link displays the resiliency status and storage information of all the individual nodes in the cluster.

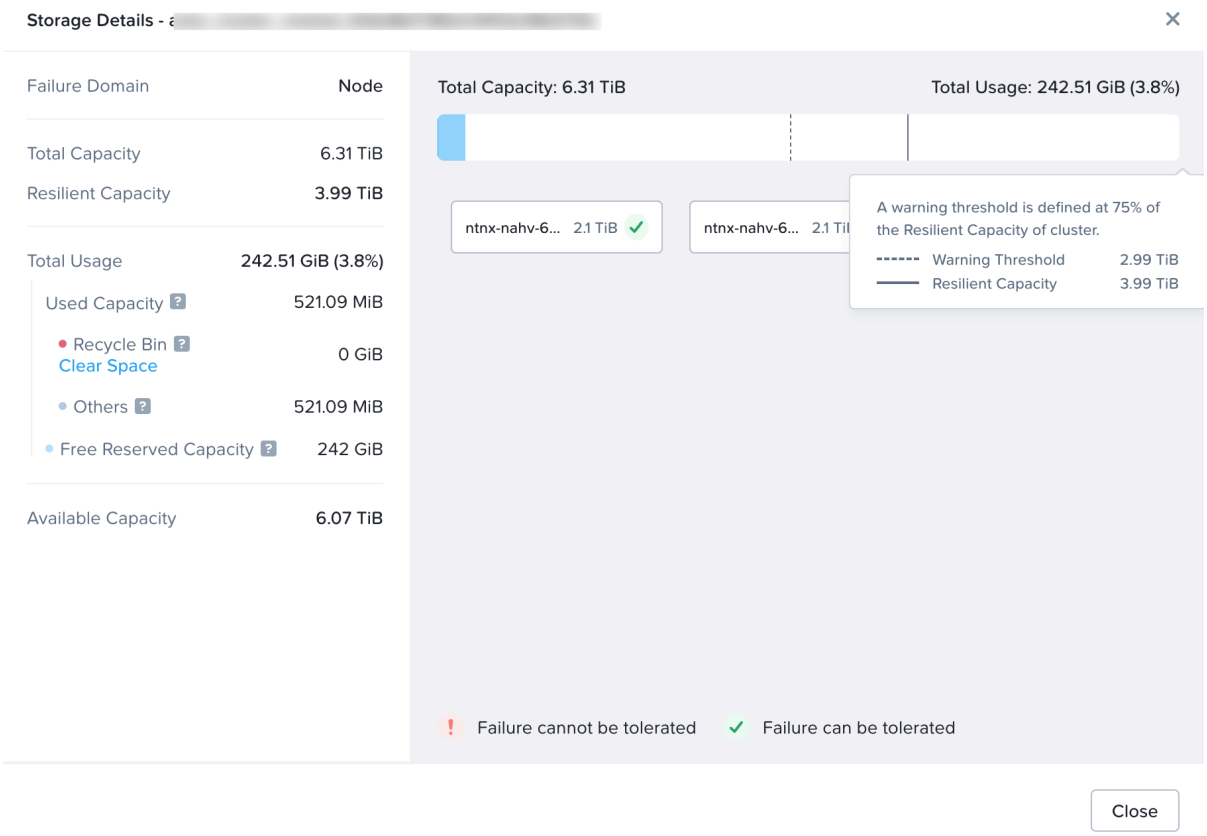


Figure 175: Storage Summary - View Details

The Storage Details page is divided into two sections: The right section displays a diagrammatic representation of the number of nodes present in the cluster along with the respective storage capacity used. You can view the warning threshold and resilient capacity of each of the nodes. The left section provides detailed storage information of the cluster as follows.

Table 105: Storage Information

Parameter	Description	Values
Failure Domain	Displays the entity (node, block, or rack) whose failure the cluster can tolerate while still running the guest VMs and responding to commands through the management console.	node, block, or rack
Total Capacity	Displays the total capacity of all the disks on all the hosts in the cluster.	xxx [GB|TB]

Parameter	Description	Values
Resilient Capacity	Displays the total resilient capacity of the cluster. Resilient capacity is the storage capacity available in the cluster after accounting for the storage space needed to rebuild and restore in case of any component failure.	xxx [GB|TB]
Total Usage	Displays the sum of all the storage space used by the cluster. The total used capacity is calculated based on the following: • Used Capacity: The amount of used storage space in the cluster (by user data). • Snapshots: The total storage capacity in the cluster consumed by snapshots (sum of both local and remote. • Recycle Bin: The total storage capacity in the cluster consumed by the VMs deleted by the user. • Other: The total storage capacity occupied by VMs, VG disks, and images. • Free Reserved Capacity:The total capacity that can be used by selected storage containers.	xxx [GB|TB]
Available Capacity	Displays the available storage capacity on all the disks on all the hosts in the cluster.	xxx [GB|TB]

In addition to the above-mentioned widgets, some actions (only the applicable ones appear) also appear on the **Summary** tab. You can perform the cluster-specific actions on a single or multiple clusters using these actions. The first four actions are: **Launch Prism Element**, **Upgrade Software**, **Rack Configuration**, and **Manage Categories**. The rest of the actions appear in the **More** dropdown menu. For more information, see Cluster Management on page 397.

Cluster Properties Widget

The following table describes the fields in the **Properties** widget. A dash (-) in a field indicates that there is not enough data to evaluate or a value is not assigned. The displayed fields vary by hypervisor.

Table 106: Cluster Properties Fields

Parameter	Description	Values
Health	Displays the cluster health state (good, warning, or critical).	Critical, Warning, Good
Storage Usage	Displays the amount of storage used in the cluster	xxx [GiB|TiB]
Storage Capacity	Displays the total amount of storage capacity in this cluster.	xxx [GiB|TiB]

Parameter	Description	Values
Cluster Runway	Displays the predicted runway (time period) before the cluster requires additional resources (see the Capacity Tab section below).	(number of days)
VM Count	Displays the number of VMs in the cluster.	(number of VMs)
AOS Version	Displays the version number of AOS running on the cluster.	(version number)
Host Count	Displays the number of hosts (nodes) in the cluster.	(number of hosts)
Upgrade Status	Displays the status of the last (or current) upgrade attempt.	(status condition)
IP Address	Displays the virtual IP address for the cluster (if defined).	(IP address)
Hypervisors	Displays the hypervisor type running in the cluster. In case of a mixed cluster such as one running ESXi or Hyper-V that also includes NX-6035C nodes running AHV, both hypervisor types are listed.	AHV, ESX, or Hyper-V

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options as the Alerts dashboard, except it is filtered to display just alerts for this cluster. For more information, see Alerts Summary View (Prism Central) in *Prism Central Alerts and Events Reference Guide*.

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options as the Events dashboard, except it is filtered to display just events for this cluster. For more information, see Events Summary View (Prism Central) in *Prism Central Alerts and Events Reference Guide*.

Metrics Tab

The **Metrics** tab allows you to view usage metrics for the cluster. Click the **Metrics** tab and then the desired metric name (see following table) to display a graph for that metric below the tab. The graph is a rolling time interval performance or usage monitor. The baseline range appears as a blue band in the graph.

> **Note:** The baseline range and identified anomalies are based on sophisticated machine-learning capabilities. For more information, see Behavioral Learning Tools in the *Intelligent Operations Guide*. The machine-learning algorithm uses 21 days of data to monitor and predict performance. A graph or baseline band may not appear if less than 21 days of data is available.

- Place the cursor anywhere on the horizontal axis to display the value at that time.
- Select the duration (time interval) from the dropdown list on the right (last 1 hour, last 24 hours, last week, last 21 days).
- [I/O-based metrics] Check the appropriate box(es) to have the graph display total, read, or write usage (or any combination of the three).
- Click **Alert Settings** to configure an alert for this metric. For more information, see Creating Custom Alert Policies in *Prism Central Alerts and Events Reference Guide*.

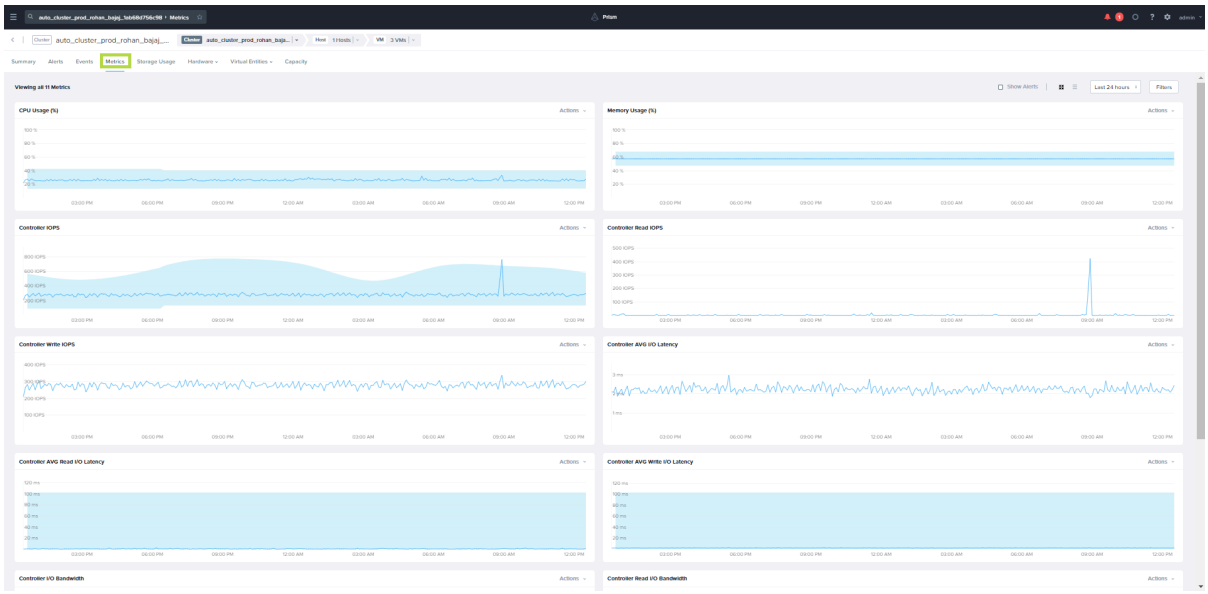


Figure 176: Cluster Metrics Tab

The following table describes the available metrics. Some metrics are not available on all hypervisors.

Table 107: Metrics Tab Fields

Metric	Description
CPU Usage	Displays the percentage of CPU capacity currently being used by the cluster (0–100%).
Memory Usage	Displays the percentage of memory capacity currently being used by the cluster (0–100%).
IOPS	Displays separate graphs for total, write, and read I/O operations per second (IOPS) for the cluster.
I/O Latency	Displays separate graphs for total, write, and read average I/O latency (in milliseconds) for physical disk requests by the cluster.
I/O Bandwidth	Displays separate graphs for total, write, and read I/O bandwidth used per second (MBps or KBps) for physical disk requests by the cluster.

Storage Usage Tab

The **Storage Usage** tab displays the following graphs:

- The **Cluster-wide Usage Summary** graph displays a rolling time interval monitor of total storage usage across the cluster that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in-depth analysis, you can add the monitor to the analysis page by clicking the blue link in the upper right of the graph.
- The **Tier-wise Usage** graph displays a pie chart divided into the percentage of storage space used by each disk tier (SSD and DAS-SATA) across the cluster.

Hardware and Virtual Entities Tabs

Clicking these tabs displays a list of hardware and virtual entity types that exist in this cluster. Clicking a hardware entry such as **Hosts** or a virtual entity such as **Containers** displays the information you would see on the **List** tab summary page for that the specified hardware or virtual entity except filtered to just those in this cluster. See Hardware Entities on page 397 and Compute and Storage Entities on page 94 for more information.

Capacity Tab

The **Capacity** tab displays current and historical usage information and provides resource planning tools. It includes the following sections:

> **Note:**
>
> - The capacity planning feature requires a Prism Pro license. Without a Prism Pro license, the **Capacity** tab is disabled.
> - Capacity planning requires a minimum of 21 days of data from a cluster to calculate the baseline runway estimates. No estimates appear when insufficient data is available. In addition, it takes a day after registering a cluster for the data to appear in Prism Central.
> - Capacity planning checks the past 90 days of data for monthly seasonality, it also uses up to 365 days of past data (when available) for calculating and adjusting the baseline accordingly if it finds a seasonality pattern.
> - For a Non-Nutanix cluster, the vCenter datastores dashboard appears only when at least one vCenter instance has been registered. For more information, see Application Monitoring in *Intelligent Operation Guide*.

- A **<cluster_name> Runway** area (upper left) that displays the current cluster runway overall and broken down by CPU, memory, and storage. *Runway* refers to how long the cluster can continue to run normally, based on the current consumption rate, before the existing resources are used to capacity. The overall runway value is the same as the lowest value for any single resource (storage, CPU, or memory). For example, if the storage runway is 14 days while the CPU and memory runways are 45 days, the overall runway is 14 days (the storage value).

  A plus sign in any runway value, for example the 89+ in the Cluster Capacity Tab figure, indicates that the predicted runway is more than that number of days, but the estimation stopped at that number.

  > **Note:** Prism Central version 2023.3 onwards, Storage Runway feature is not available for vCenter clusters.

  - Clicking **Storage Runway** displays a storage usage graph and table (to the right).
  - Clicking **CPU Runway** displays a CPU usage graph and table.
  - Clicking **Memory Runway** displays a memory graph and table.

- Click **Optimize Resource** (middle left to open the **Optimize Resources** window, which identifies areas to improve cluster resource allocation or capacity. Recommendations might include

  - Table of *inefficient* (over-provisioned, inactive, constrained, and bully) VMs based on the VM behavioral learning engine. Click the appropriate link to see a list of the VMs in that state. For more information, see Behavioral Learning Tools in *Intelligent Operations Guide*.
  - An add node recommendation. The recommendation is based on the current (historical) CPU, memory, and storage usage demand across the cluster.

  Click the **Get Report** link to run the Cluster Efficiency report. For more information, see Reports Management in the *Intelligent Operation Guide*.

- **Get Started** (lower left). Click **Get Started** to open the resource planning scenario page. From this page you can create *what if* scenarios to test future workloads against current or hypothetical storage, CPU, and memory resource capacity. For more information, see Creating a Scenario in *Intelligent Operations Guide*.
- **Ignore Time Window** (upper right). Click **Ignore Time Window** to open the **Ignore Time** window. On this page, you can specify the time window you want to ignore while calculating the capacity runway. You should ignore any one-time intentional cluster usage that can adversely affect the cluster runway calculation, such as when a workload is transferred to another cluster due to planned maintenance. You should set the Ignore Time window slightly wider than the usage spike you want to ignore. For example, if the spike is from March 5th to March 7th, you should set a window from March 4th to March 8th.

  Once defined, the Ignore Time window is disregarded from the time series data for CPU, memory, and storage usage for a Nutanix or vCenter cluster, thus making the runway prediction more accurate. It takes a couple of hours for the runway to get updated after you define an Ignore Time window. You can add multiple Ignore Time windows for each cluster.

- A usage history graph (middle right). The graph displays storage, CPU, or memory usage depending on which is selected in the left column. Placing the cursor anywhere on the horizontal axis displays the value(s) at that time. A (solid red) maximum capacity line appears near the top of the graph, and an additional (dotted red) effective capacity line appears on the storage graph. A (vertical) Today line is displayed to indicate where the current date is located on the graph. When there is an alert or event, a bell icon appears either on the Today line or at the starting point of the alert. Clicking the bell icon (red for critical alert, orange for warning alert, or gray for event) displays more information about that alert or event.
- A table (lower right) that displays usage information. The information in the table varies depending on which runway (storage, CPU, or memory) is selected.

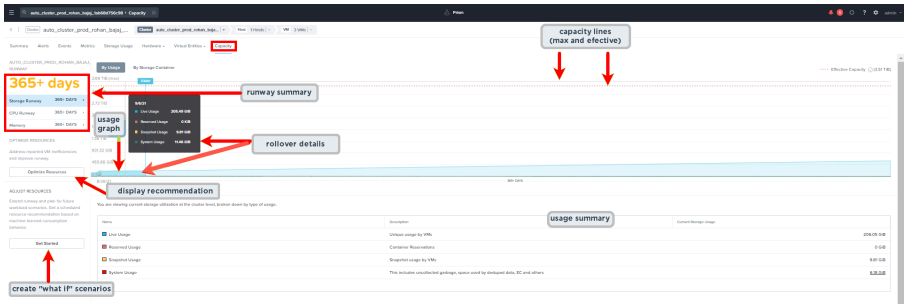


Figure 177: Cluster Capacity Tab (Nutanix Cluster)

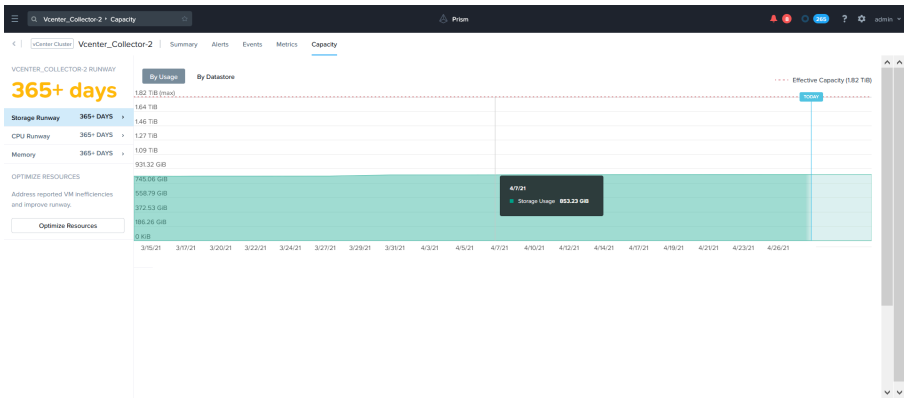


Figure 178: Cluster Capacity Tab (Non-Nutanix Cluster)

Capacity Tab: Storage View

When **Storage Runway** is selected, the graph and table display storage usage information. The maximum and effective storage capacity values (in TiBs) for the cluster appear above the graph. Effective capacity of a cluster is computed based on the configured reservations (from the capacity configurations settings) and the replication factor for all the containers in the cluster.

The storage view includes two tabs:

- Click the **By Usage** button to see cluster-wide storage information (see previous figure).
- Click **By Storage Container** to see storage information per storage container. You can select all storage containers from the dropdown list (upper left of graph) or a single storage container from the dropdown list or by clicking the storage container name in the table.

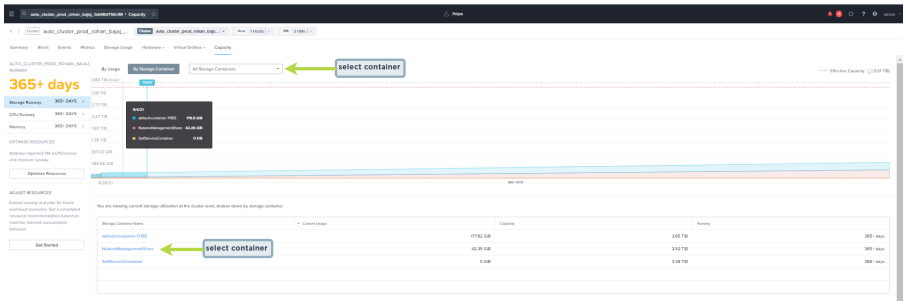


Figure 179: Storage Container View (Nutanix Cluster)

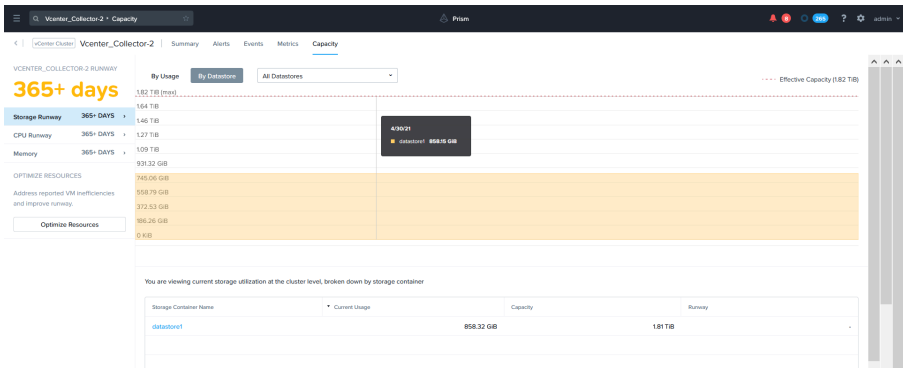


Figure 180: Storage Container View (Non-Nutanix Cluster)

The following table describes the fields in the storage table.

Table 108: Capacity Tab: Storage Fields

Parameter	Description	Values
By Usage tab (cluster-wide)		
Name	Displays a descriptive name for a type of storage. There are four types: • Live Usage: The amount of live storage. • Snapshot Usage: The amount of storage used for snapshots. • System Usage: The amount of storage for everything else (total usage - (reserved + snapshot + live)). System usage includes garbage, parity, and other miscellaneous uses. • Reserved Usage: The amount of storage reserved for thick provisioned VMs (ESXi).	Live Usage, Reserved Usage, Snapshot Usage, System Usage
Current Storage Usage	Displays the amount of used storage space in the cluster or storage container.	xxx [GB|TB]
By Storage Container tab: All Storage Containers		
Storage Container Name	Displays the name of the storage container.	(storage container name)
Current Usage	Displays the amount of storage space used by the storage container currently.	xxx [GB|TB]
Capacity	Displays the total amount of storage capacity available to the storage container.	xxx [TB]
By Storage Container tab: <storage container name>		
Storage Container Name	Displays one of the following: • If All Storage Containers is selected, the storage container names are displayed. Click a name to see the details for that storage container. • If a single storage container is selected, it displays the four storage types described for the Name field in the By Usage tab (Live Usage, Reserved Usage, Snapshot Usage, and System Usage).	(storage container name) OR Live Usage, Reserved Usage, Snapshot Usage, System Usage
Current Storage Usage	Displays the amount of used storage space in the cluster or storage container.	xxx [GB|TB]

Capacity Tab: CPU View

When **CPU Runway** is selected, the graph and table display CPU usage information. The maximum and effective CPU capacity values (in GHz) for the cluster appear above the graph. The CPU view includes two tabs:

- Click **Overall** to see cluster-wide CPU information.
- Click **By Host** to see CPU information per host. You can select all hosts from the dropdown list (upper left of graph) or a single host from the dropdown list or by clicking the host name in the table.

The following table describes the fields in the CPU table. Entries for (up to) the top 10 VMs (overall tab) or hosts appear in the CPU table.

Table 109: Capacity Tab: CPU Fields

Parameter	Description	Values
Overall tab		
VM Name	Displays the VM name. There is a line for each VM in the cluster.	(VM name)
CPU Usage (%)	Displays the percent of CPU capacity used by the VM currently.	(0–100%)
Num vCPUs	Displays the number of vCPUs allocated to the VM.	(1-max)
By Host tab: All Hosts		
Host Name	Displays the name of the host.	(host name)
Average CPU Usage over last 1 hour	Displays the average host CPU usage during the last hour.	xxx [GHz]
Current CPU Capacity	Displays the CPU capacity of the host.	xxx [GHz]
Runway	Displays the current runway (estimated time interval that current CPU capacity is sufficient for the workload).	(number of days)
By Host tab: <host name>		
VM Name	Displays the VM name. There is a line for each VM in the cluster.	(VM name)
CPU Usage (%)	Displays the percent of CPU capacity used by the VM.	(0–100%)
Num vCPUs	Displays the number of vCPUs allocated to the VM.	(1-max)

Capacity Tab: Memory View

When **Memory Runway** is selected, the graph and table display memory usage information. The maximum and effective memory capacity values (in GiBs) for the cluster appear above the graph. The memory view includes two tabs:

- Click **Overall** to see cluster-wide memory information.
- Click **By Host** to see memory information per host. You can select all hosts from the dropdown list (upper left of graph) or a single host from the dropdown list or by clicking the host name in the table.

The following table describes the fields in the memory table. Entries for (up to) the top 10 VMs (overall tab) or hosts appear in the memory table.

Table 110: Capacity Tab: Memory Fields

Parameter	Description	Values
Overall tab		
VM Name	Displays the VM name. There is a line for each VM in the cluster.	(VM name)
Memory Usage	Displays the amount of memory used by the VM.	xxx [GiB]
Memory Usage (%)	Displays the percentage of memory capacity used by the VM.	(0–100%)
By Host tab: All Hosts		
Host Name	Displays the name of the host.	(host name)
Average Memory Usage over last 1 hour	Displays the average host memory usage during the last hour.	xxx [GiB]
Runway	Displays the current runway (estimated time interval that current memory capacity is sufficient for the workload).	(number of days)
Current Memory Capacity	Displays the memory capacity of the host.	xxx [GiB]
By Host tab: <host name>		
VM Name	Displays the VM name. There is a line for each VM in the cluster.	(VM name)
Memory Usage	Displays the amount of memory used by the VM.	xxx [GiB]
Memory Usage (%)	Displays the percentage of memory capacity used by the VM currently.	(0–100%)

Security Dashboard Tab

The Security Dashboard provides dynamic summary of the security posture across all registered clusters. The Security Dashboard allows you to view the most critical security parameters like cluster-based issue summary, STIG policy compliance, security hardening, and identified vulnerabilities. For more information, see Security Dashboard in the *Nutanix Security Guide*.

Entity Relationship Widget

The entity relationship widget shows the relationship between related entities like clusters, hosts, and VMs instances. The widget allows quick access between the related entities. You can directly navigate to a target cluster, host, or VM instance through the respective dropdown menus.

Example: Viewing Cluster Instances

Click the **Cluster** dropdown menu to view the list of cluster instances. Alternatively, you search a cluster name.

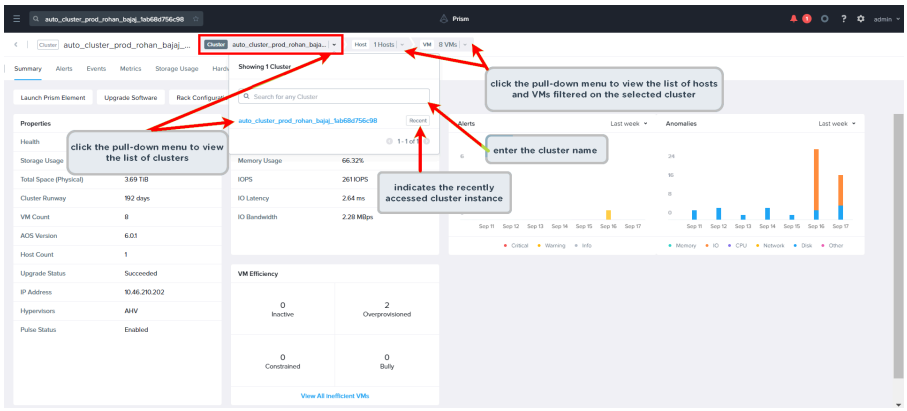


Figure 181: Clusters

Note:

- The **Recent** label indicates the last accessed entity instances. The widget displays a maximum of three recently accessed entity instances.
- The filtered list of VMs display only the powered-on VM instances.
- If the VMs are not filtered on a host instance, all VMs on the selected cluster are displayed.

Creating a Cluster

Before you begin

Ensure that you meet the following prerequisites:

- All hosts are running AOS 6.7 or later versions.
- All hosts are reimaged with the same set of AOS and hypervisor versions. For information about reimaging the hosts using Foundation Central, see Run Foundation Central.
- All hosts are reachable.
- All hosts are in the same subnet.

About this task

To create a cluster through Prism Central, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Hardware** > **Clusters**.
   The system displays the **List** tab with all the registered clusters in your **Nutanix** environment.
3. Click **Create Cluster**.
4. Review the **Create Cluster Prerequisites**, and click **Next**.

5. Enter the following details in the **Create Cluster** wizard:

   a. In the **Select Host** section, enter the CVM IP of the hosts that you want to use for cluster creation, separated by a comma or a space and click **Discover Hosts**.
   The list of discovered hosts, along with their details, is displayed at the bottom of the wizard.

   b. In the **Configure** section, enter the following details:

      - **Cluster Name**: Name for the cluster.
      - **Cluster external IP**: [Optional] External IP address for the cluster.
      - **Redundancy Factor**: [Optional] Redundancy factor for the cluster. The default value is **RF2**. Following are some important considerations while selecting the redundancy factor for your cluster:
        - A one-node cluster supports RF2 mirroring inside single node.
        - A two-node cluster supports RF2 mirroring inside each node and RF2 across clusters.
        - Clusters with more than three nodes do not support any mirroring inside nodes.
        - You can choose RF3 only if the cluster has a minimum of five nodes.
      - **DNS Server(s) IP**: [Optional] IP address of DNS server, separated by a comma or a space if you are entering multiple IP addresses.
      - **NTP Server(s) IP**: [Optional] IP address of NTP server, separated by a comma or a space if you are entering multiple IP addresses.
      - **Container Name**: [Optional] Name of the container that you want to be associated with the cluster.
      - **Cluster Domain Fault Tolerance**: [Optional] Select the fault tolerance domain for the cluster. The default value is **Disk** for a single node cluster, and **Node** for multiple-nodes cluster. You can choose **Disk**, **Block**, or **Rack** as the fault tolerance domain.
      - **Enable Backplane Segmentation**: [Optional] Enable backplane segmentation. Backplane segmentation separates the CVM-to-CVM traffic from other kinds of traffic. This is applicable only if you have at least three hosts. If you enable backplane segmentation, you need to enter a few mandatory parameters such as subnet, netmask, and ports. For more information about backplane segmentation, see Segmented and Unsegmented Networks.

   c. Click **Next**.
   In the **Review** section, the pre-checks are run to validate that the hosts meet all the requirements mentioned under the Prerequisites. If the pre-checks are successful, the configuration details of the cluster are displayed for review.

   d. Click **Create Cluster**.
   Cluster creation operation might take some time. Under **Recent Tasks**, you can verify that a cluster create task was initiated.

What to do next

You can register the newly created cluster with Prism Central. For more information, see Registering or Unregistering a Cluster with Prism Central on page 53.

Destroying a Cluster

Before you begin

Ensure the following prerequisites:

- The minimum supported versions for destroying a cluster through Prism Central are version 6.8 for Prism Element (with bundled AHV version) and version pc.2024.1 for Prism Central.
- You need to reclaim your license before destroying a cluster.

About this task

> **Caution:** Destroying a cluster is irreversible. Upon successful completion of this operation, the cluster is unregistered, and all the nodes go back to the available node pool. All cluster settings, user VMs, and data policies are permanently deleted, and all Prism Central configurations for categories and policies applied to the cluster are lost. Nutanix recommends performing all the preparatory actions before destroying a cluster.

To destroy a cluster through Prism Central, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Hardware** > **Clusters** .
   The system displays the **List** tab with all the registered clusters in your **Nutanix** environment.
3. Select the cluster to destroy and click **Actions** > **Destroy Cluster**.

   > **Note:** You cannot destroy a cluster that is hosting a Prism Central Instance.

4. Review the **Destroy Cluster Prerequisites** and click **Next**.
   The pre-checks are run to validate that the cluster meets all the requirements mentioned under the Prerequisites. The result of the pre-checks and the cluster details are displayed for review.

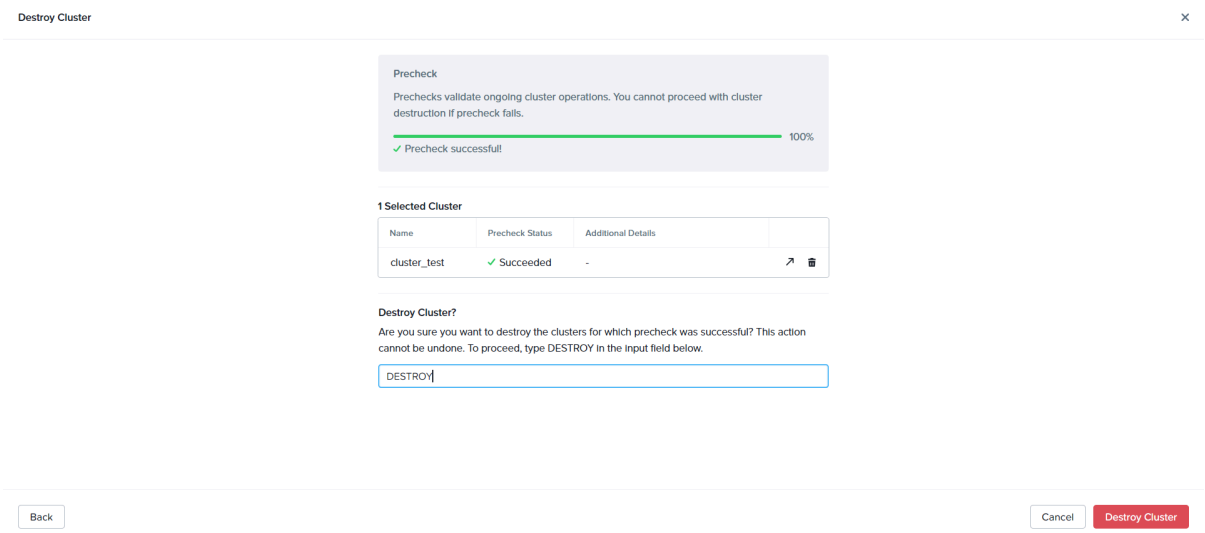


Figure 182: Destroy Cluster

5. Under **Destroy Cluster?**, type DESTROY to confirm the destroy cluster operation.
   Note that this is a case-sensitive input, and you need to enter the word in upper-case.

6. Click **Destroy Cluster**.

   Destroy Cluster operation might take some time. Under **Recent Tasks**, you can verify that a cluster destroy task has been initiated.

Host Management

In Prism Central, the hosts dashboard allows you to view summary information about hosts across registered clusters and access detailed information about each host. For more information, see Hosts Summary View on page 420 and Host Details View on page 424.

You can perform the following actions to manage hosts in Prism Central:

- Assign a category to the host. For more information, see Assigning a Category on page 459.
- Run playbook to perform operations on host. For more information, see Task Automation - Playbooks in *Intelligent Operations Guide*.
- Rename an AHV host. For more information, see Renaming an AHV Host on page 429.

Hosts Summary View

The **Summary** tab on the **Hosts** page provides a dashboard of the hosts across all the registered clusters.

To access the summary view of all the hosts, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Hardware** > **Hosts** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The system displays the **List** tab by default with all the hosts across registered clusters in **Nutanix** environment. For information about how to access the list of hosts in **Non-Nutanix** environment (non-nutanix hosts managed by external *vCenter*), see Host Details View on page 424.
3. Click the **Summary** tab. The system displays **Summary** page for all the hosts.

   > **Note:** To access the summary view of all the hosts managed by *vCenter*, select **Non-Nutanix** environment from the dropdown menu in **Hosts** page.
   >
   > The **Summary**, **Alerts**, and **Events** tabs display the same information as for Nutanix-managed clusters. The **Metrics** tab displays a subset of the full list (5 of the 7 metrics). The **List** tab displays fields for name, host IP, VM count, memory capacity, and cluster name.

   Using playbooks, you can manage the hosts in **Non-Nutanix** environment. For more information about playbooks, see Task Automation - Playbooks in *Intelligent Operations Guide*.

Clicking the **Summary** tab displays the following three widgets:

- **Suggested**: Displays a list of the hosts with the highest usage of the parameter you select from the dropdown menu on the right of the widget. The options are **CPU Usage**, **Memory Usage**, **IO Latency**, and **IOPS**. Click the **View all XX Hosts** link at the bottom to display the **List** tab (following section).
- **Alert**: Displays a list of host-related alerts that occurred during the specified interval. Select either **Last 24 hours** (default) or **Last week** from the dropdown menu.
- **Anomalies**: Displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified interval. Select either **Last 24 hours** (default) or **Last week** from the dropdown menu. When an anomaly appears, you can click on the graph, which then displays a list of those anomalies. Clicking on an anomaly displays the event page for that anomaly.

List Tab

Clicking the **List** tab, which appears by default when you first open the page, displays a list of the hosts across the registered clusters. The following table describes the fields that appear in the hosts list. The fields vary based on the **Focus** menu selection, which is either **General** or **Performance**. A dash (-) is displayed in a field when a value is not available or applicable.

Table 111: Hosts List Fields

Parameter	Description	Values
General Focus Fields		
Name	Displays the name of the host. Clicking on the name displays the details page for that host. For more information, see Host Details View on page 424.	(host name)
Host IP	Displays the IP address assigned to the hypervisor running on the host.	(IP address)
CVM IP	Displays the IP address assigned to the Controller VM.	(IP address)
Hypervisor	Displays the hypervisor type running on the host.	AHV, ESX, or Hyper-V
Memory Capacity	Displays the memory capacity of the host.	xxx [MB|GB]
Cluster	Displays the name of the cluster in which the host resides.	(cluster name)
Performance Focus Fields		
Name	Displays the name of the host.	(host name)
CPU Usage	Displays the percentage of CPU capacity currently being used by this host.	0 - 100%
Memory Usage	Displays the percentage of memory capacity currently being used by this host.	0 -100%
IOPS	Displays I/O operations per second (IOPS) for this host.	[0 - unlimited]
Disk IO Bandwidth	Displays I/O bandwidth used per second for this host.	xxx [MBps|KBps]
IO Latency	Displays the average I/O latency (in milliseconds) for this host.	xxx [ms]
Cluster	Displays the name of the cluster in which the host resides.	(cluster name)

You can filter the hosts list based on a variety of parameter values. The following table describes the filter options available when you open the Hosts view **Filter** pane. To apply a filter, select a parameter and check the box of the desired value (or multiple values) you want to use as a filter. You can apply filters across multiple parameters. Some parameter filters require additional context such as a constraint string or a range.

Table 112: Filters Pane - Hosts Page

Parameter	Description	Values
Name	Filters on the host name. Select a condition from the dropdown menu (**Contains**, **Doesn't contain**, **Starts with**, **Ends with**, or **Equal to**) and enter a string in the field. It will return a list of hosts that satisfy the name condition/string.	(host name string)
Cluster	Filters on the cluster name. Enter a string in the field. It will return a list of hosts that reside in the clusters which satisfy the name string.	(cluster name string)
Health	Filters on the host health state (good, warning, or critical). Select one or more states to return a list of hosts in that state(s). The number of hosts currently in each state is displayed on the right of the line.	Critical, Warning, Good
Categories	Filters on category names. Enter a category name in the field and then check the box. As you type a dropdown menu appear to help you select the correct category. A new field appears where you can add more categories to the filter. The number of hosts tagged to each selected category is displayed on the right of the line.	(category name)
Hypervisor	Filters on the hypervisor type. Select one or more hypervisors to return a list of clusters running those hypervisor(s). The number of clusters currently running each hypervisor is displayed on the right of the line.	AHV, ESXi, Hyper-V
Memory Capacity	Filters on the host memory capacity. Check the box for the desired range or enter an amount range in the *from <low> to <high> GiB* field. It will return a list of hosts with memory capacity in that range.	([xx] to [yy] GiB range)
CPU Usage	Filters on the amount of CPU being used. Check the box for the desired range or enter a percentage range in the *from <low> to <high> %* field. It will return a list of hosts utilizing CPU in that range (0-100%).	([xx] to [yy]% range)
Memory Usage	Filters on the amount of total memory being used. Check the box for the desired range or enter a percentage range in the *from <low> to <high> %* field. It will return a list of clusters utilizing total memory in that range (0-100%).	([xx] to [yy]% range)
GPUs	Filters for GPU configuration information such as model name. Select a condition from the dropdown menu (**Contains**, **Doesn't contain**, **Starts with**, **Ends with**, or **Equal to**) and enter a string in the field. As you type a dropdown menu appears to help you select the correct configuration information. It will return a list of hosts that satisfy the GPU condition/string.	(configuration info)

Parameter	Description	Values
IOPS	Filters on the IOPS. Check the box for the desired range or enter a range in the *from <low> to <high> iops* field. It will return a list of hosts with IOPS in that range.	([xx] to [yy] range)
IO Bandwidth	Filters on the I/O bandwidth used. Check the box for the desired range or enter a range in the *from <low> to <high> bps* field. It will return a list of hosts with I/O bandwidth usage in that range.	([xx] to [yy] range)
IO Latency	Filters on the average I/O latency. Check the box for the desired range or enter a range in the *from <low> to <high> ms* field. It will return a list of hosts with average I/O latency in that range.	([xx] to [yy] range)

You can perform the following actions for the hosts in the **List** tab:

- Access the detailed information about an individual host. For more information, see Host Details View on page 424.
- Filter the host list based on available parameter values using **Filters** pane. For more information about **Filters** pane, see Filters Pane - Hosts Page.
- Export the table that contains the list of hosts and their information to a file in a CSV format. For more information about **Export** option, see Export on page 32.
- Group the hosts based on pre-defined criteria. For information about how to group the clusters, see Group by on page 29.
- View hosts based on pre-defined criteria or create a custom view. For information about available views and how to create a custom view, see View by on page 29.
- Perform the host-specific actions on a single or multiple hosts using the **Actions** dropdown menu. For more information, see Host Management on page 420 .

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options as the Alerts dashboard, except it is filtered to display just host-related alerts across the registered clusters. For more information, see Alerts Summary View (Prism Central) in *Prism Central Alerts and Events Reference Guide*.

Audits Tab

The **Audits** tab displays a table of audits. This tab provides the same features and options as the Audits dashboard, except it is filtered to display just host-related events across the registered clusters. For more information, see Audits Summary View on page 448.

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options as the Events dashboard, except it is filtered to display just host-related events across the registered clusters. For more information, see Events Summary View (Prism Central) in *Prism Central Alerts and Events Reference Guide*.

Metrics Tab

The **Metrics** tab allows you to view usage metrics across the hosts. Clicking the **Metrics** tab displays a list of available metrics; click the metric name to display the relevant information to the right. The following table describes the available metrics. (Some metrics are not available on all hypervisors.)

Table 113: Metrics Tab Fields

Metric	Description
CPU Usage	Displays a CPU usage table listing current values and total hosts (number). The current values are split into percentile intervals (for example, less than 25%, 25-50, 50-75, more than 75%). Clicking on a percentile interval displays the Summary tab filtered to just those hosts. **Note:** The same format also applies to the other metrics in this table with either percentile or quantity intervals.
Memory Swap	Displays memory swap-out and swap-in rate tables.
Memory Usage	Displays a memory percentage usage table.
IOPS	Displays total, read, and write IOPS tables.
IO Latency	Displays total, read, and write I/O latency rate tables.
IO Bandwidth	Displays total, read, and write I/O bandwidth rate tables.
Network Packets Dropped	Displays the number of network packets that have been received and then dropped.

Host Details View

Summary Tab

The **Summary** tab of an individual host consists of a dashboard that provides the detailed information about the host.

To access the **Summary** tab of an individual host:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Hardware** > **Hosts** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   By default, the system displays the **List** tab with all the hosts.
3. Click the target <*host_name*> to view the **Summary** tab of an individual host.

   Note: Replace <*host_name*> with the actual host name at your site.

The **Summary** tab of an individual host provides the following widgets and actions:

- **Properties**: Displays summary information about the host. For more information, see the Host Properties on page 425 table.
- **Alert**: Displays a list of related alerts that occurred during the specified interval. Select either **Last week** (default),**Last 1 hour**, or **Last 24 hours** from the dropdown menu on the top right corner of the widget.

- **Metrics**: Displays the metrics information: **CPU Usage**, **Memory Usage**, **IOPS**, **IO Latency**, and **IO Bandwidth**.
- **Anomalies**: Displays a graph of memory, I/O, CPU, networking, disk, or other anomalies that occurred during the specified interval. Select either **Last week** (default), **Last 1 hour**, or **Last 24 hours** from the dropdown menu on the top right corner of the widget. When an anomaly appears, you can click the graph to display a list of those anomalies. If you click an individual anomaly, the system displays the event page for that anomaly.
- **Rename**: Renames an AHV host. For more information, see Renaming an AHV Host on page 429.
- **Manage Categories**: Manages categories for the host. For more information, see Category Management on page 454.
- **Run Playbook**: Runs a playbook. For more information, see Running a Playbook (Manual Trigger) in *Intelligent Operations Guide*.

The host name and the following set of tabs appear on the left: **Summary**, **Alerts**, **Events**, **Metrics**, **Usage**, **Hardware**, and **Virtual Entities**. Click a tab to display that information on the right. Click the **Back to Hosts** link to return to the summary view.

Host Properties

The following table describes the fields in the **Properties** widget. A dash (-) in a field indicates there is not enough data to evaluate or a value is not assigned. The displayed fields vary by hypervisor.

Table 114: Host Properties Fields

Parameter	Description	Values
Memory Capacity	Displays the total memory capacity for this host.	xxx [MB|GB]
Disk Capacity	Displays the total amount of disk capacity on this host.	xxx [GB|TB]
Cluster	Displays the name of the cluster in which the host resides. Clicking the name displays the details page for that cluster . For more information, see Cluster Details View on page 405.	(cluster name)
Host IP	Displays the host IP address.	(IP address)
Hypervisor	Displays the hypervisor name.	(hypervisor name)
VM Count	Displays the number of VMs running on this host.	(number)
Block Model	Displays the block model number.	(model series number)
Serial Number	Displays the block serial number.	(block serial number)
CPU Capacity	Displays the total CPU capacity for this host.	xxx [GHz]
CVM IP	Displays the IP address assigned to the Controller VM.	(IP address)
IPMI Address	Displays the IP address of the Intelligent Platform Management Interface (IPMI) port. An IPMI port is used for the hypervisor host console.	(IP address)

Parameter	Description	Values
Node Serial	Displays the node serial number. The node serial is a unique number passed through from the manufacturer. (The form can vary because it is determined by each manufacturer.)	(manufacturer serial number)
Oplog Disk %	Displays the percentage of the operations log (oplog) capacity currently being used. The oplog resides on the metadata disk.	[0 - 100%]
Oplog Disk Size	Displays the current size of the operations log. (The Oplog maintains a record of write requests in the cluster.) A portion of the metadata disk is reserved for the Oplog, and you can change the size through the nCLI.	xxx [GB]
Monitor Enabled	Displays whether the host is high availability (HA) protected. A **Yes** value means HA is active for this host. A **No** value means VMs on this host are not protected (will not be restarted on another host) if the host fails. Normally, this value should always be **Yes**. A **No** value is likely a sign of a problem situation that should be investigated.	[Yes|No]
Disks	Displays the number of disks in each storage tier in the host. Tier types vary depending on the Nutanix model type.	DAS-SATA: (number), SSD-SATA: (number), SSD-PCIe: (number)
GPUs	Displays the number and type of GPUs in the host. For example, if the host contains four Tesla M10 GPUs, this field displays "Tesla M10 (4)".	(GPU type and number)
Datastore(s)	Displays the names of any datastores.	(names)

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options as the Alerts dashboard, except it is filtered to display just alerts for this host. For more information, see Alerts Summary View (Prism Central) in *Prism Central Alerts and Events Reference Guide*.

Audits Tab

The **Audits** tab displays a table of audits. This tab provides the same features and options as the Audits dashboard, except it is filtered to display just host-related events across the registered clusters. For more information, see Audits Summary View on page 448.

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options as the Events dashboard, except it is filtered to display just events for this host. For more information, see Events Summary View (Prism Central) in *Prism Central Alerts and Events Reference Guide*.

Metrics Tab

The **Metrics** tab allows you to view usage metrics for the host. Click the **Metrics** tab and then the desired metric name (see following table) to display a graph for that metric on the right. The graph is a rolling time interval performance or usage monitor. The baseline range appears as a blue band in the graph.

Note: The baseline range and identified anomalies are based on sophisticated machine-learning capabilities. For more information, see Behavioral Learning Tools in *Intelligent Operations Guide*. The machine-learning algorithm uses 21 days of data to monitor and predict performance. A graph or baseline band may not appear if less than 21 days of data is available.

- Place the cursor anywhere on the horizontal axis to display the value at that time.
- Select the duration (time interval) from the dropdown list on the right (last 1 hour, last 24 hours, last week, last 21 days).
- [I/O-based metrics] Check the appropriate box(es) to have the graph display total, read, or write usage (or any combination of the three).
- Click **Alert Settings** to configure an alert for this metric. For more information, see Creating Custom Alert Policies in *Prism Central Alerts and Events Reference Guide*.

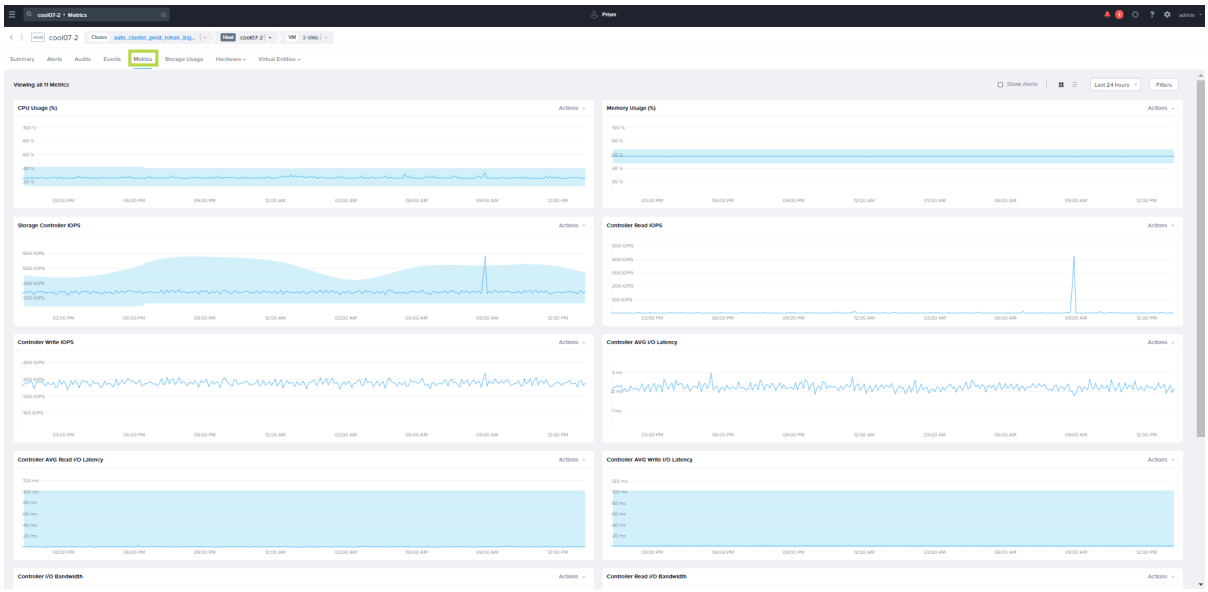


Figure 183: Host Metrics Tab

The following table describes the available metrics. Some metrics are not available on all hypervisors.

Table 115: Metrics Tab Fields

Metric	Description
CPU Usage	Displays the percentage of CPU capacity currently being used by the host (0 - 100%).
Memory Usage	Displays the percentage of memory capacity currently being used by the host (0 - 100%).
Controller IOPS	Displays graph for total I/O operations per second (IOPS) for the host.
Controller Read IOPS	Displays graph for read I/O operations per second (IOPS) for the host.

Metric	Description
Controller Write IOPS	Displays graph for write I/O operations per second (IOPS) for the host.
Controller AVG I/O Latency	Displays graph for average I/O latency (in milliseconds) for physical disk requests by the host.
Controller AVG Read I/O Latency	Displays graph for average read I/O latency (in milliseconds) for physical disk requests by the host.
Controller AVG Write I/O Latency	Displays graph for average write I/O latency (in milliseconds) for physical disk requests by the host.
Controller I/O Bandwidth	Displays graph for I/O bandwidth used per second (MBps or KBps) for physical disk requests by the host.
Controller I/O Read Bandwidth	Displays graph for read I/O bandwidth used per second (MBps or KBps) for physical disk requests by the host.
Controller I/O Write Bandwidth	Displays graph for write I/O bandwidth used per second (MBps or KBps) for physical disk requests by the host.

Storage Usage Tab

The **Storage Usage** tab displays the following graphs:

- The **Usage Summary** graph displays a rolling time interval monitor of host storage usage that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in depth analysis, you can add the monitor to the analysis page by clicking the blue link in the upper right of the graph.
- The **Tier-wise Usage** graph displays a pie chart divided into the percentage of host storage space used by each disk tier (SSD and DAS-SATA).

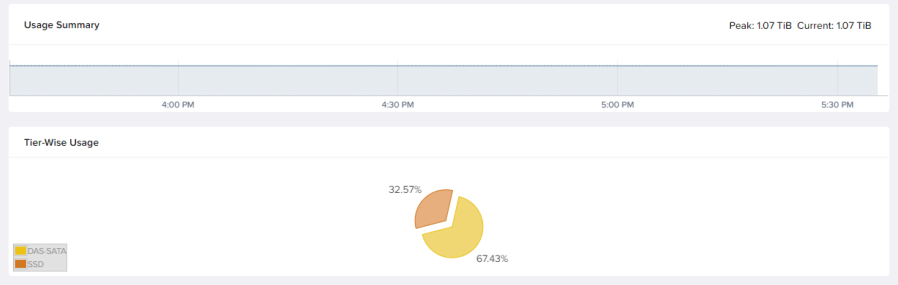


Figure 184: Host Usage Tab

Hardware and Virtual Entities Tabs

Clicking these tabs displays a list of hardware and virtual entity types that exist on this host. Clicking a hardware entry such as **Disks** or a virtual entity such as **VMs** displays the information you would see on the **List** tab summary page for that the specified hardware or virtual entity except filtered to just those on this host. For more information, see Hardware Entities on page 397 and Compute and Storage Entities on page 94 topics.

Entity Relationship Widget

The entity relationship widget shows the relationship between related entities like clusters, hosts, and VMs instances. The widget provides quick access between the related entities. You can directly navigate to a target cluster, host, or VM instance through the respective dropdown menus.

Example: Viewing Hosts on a Cluster

Click the **Host** dropdown menu to view the list of host instances on the selected cluster. Alternatively, you can search the host instance name belonging to the target cluster.

Note:

- The **Recent** label indicates the last accessed entity instances. The widget displays a maximum of three recently accessed entity instances.
- The filtered list of VMs display only the powered-on VM instances.
- If the VMs are not filtered on a host instance, all VMs on the selected cluster are displayed.

Renaming an AHV Host

You can rename an AHV host from Prism Central.

About this task

The minimum supported versions to rename an AHV host from Prism Central are version 6.6 for Prism Element (with recommended AHV version) and version 2022.9 for Prism Central. For information about the recommended AHV version based on the AOS release and hardware model, see Compatibility and Interoperability Matrix.

To rename an AHV host from Prism Central, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Hardware** > **Hosts** .
   The system displays the **List** tab by default with all the hosts across registered clusters.
3. Select the target host checkbox, and choose **Rename** from the **Actions** dropdown menu.
   The system displays the **Rename Host** window.
4. Enter a new name for the host in the **New Host Name** field, and click **Save**.

   You must adhere to the following rules for the host name:

   - Allowed characters are: uppercase letters (A-Z), lowercase letters (a-z), decimal digits (0-9), dots (.), and hyphens (-).
   - The host name must start and end with a number or letter.
   - A minimum of one character and a maximum of 63 characters are allowed.
   - Successive dots are not allowed. Each dot-separated string must follow the first two rules.

   Note: Once the AHV host rename task is complete, it might take a few minutes for the changes to propagate from the host to Prism Central.

Expanding a Cluster through Prism Central

A cluster is a collection of nodes. You can expand a cluster by adding new nodes to the cluster after connecting them to the network on the same subnet as the cluster. The cluster expansion process compares the AOS version on the existing and new nodes and performs any upgrades necessary for all the nodes to run the same AOS version.

Before you begin

Ensure that the following prerequisites are met before you add a node to the cluster:

- Review the relevant sections in Prerequisites for adding a node before attempting to add a node to the cluster. The process for adding a node varies depending on several factors. This section covers specific considerations based on your AOS, hypervisor, encryption, and hardware configuration.
- Check the Health of the cluster. If any health checks are failing, resolve them before adding any nodes. As a final check, run NCC to ensure that the cluster is healthy.
- Allow any current expand cluster operations to complete.
- All nodes are in the correct metadata state by checking the Hardware dashboard. If any nodes show Metadata store disabled on the node or Node is removed from metadata store, enable the metadata store by clicking **Enable Metadata Store**.
- Follow the SSDs' requirements for Hybrid HCI Node and All-Flash HCI Node specified in HCI Node Field Requirements in the *Acropolis Advanced Administration Guide*.

About this task

You can add new nodes to a cluster using Prism Central or Prism Element web console. For information about expanding a cluster through Prism Element web console, see Expanding a Cluster in the *Prism Element Web Console Guide*.

The minimum supported versions to add new hosts using Prism Central web console is Prism Central version 2023.3.

To add one or more nodes to an existing cluster through Prism Central, do the following:

Procedure

1. Log in to Prism Central.
2. From the Application Switcher Function on page 19, select the **Infrastructure** application, and navigate through **Navigation Bar** to **Hardware** > **Clusters**.
   For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab with all the registered clusters in your **Nutanix** environment.
3. Select the cluster that you want to expand, and click **Expand Cluster**.
   The system searches for hosts in the entire network and all the discovered hosts are listed in the **Expand Cluster** page.
4. (Optional) Click **Discover Hosts Manually** to discover any hosts that are not listed after automatic host discovery, and enter the hostname or CVM IP.

   > **Note:** ESXi or AHV compute-only nodes and hosts with deactivated IPv6 support are not discovered automatically. You must initiate manual host discovery for such hosts.

5. In the **Select Host** page, select the hosts that you want to add to the cluster, and click **Next**.

6. In the **Choose Host Type** page, select **Host Type** from the dropdown menu for each of the hosts you have selected, and then click **Next**.

   You can select any one of the following host types:

   - **HCI**: Standard host in the cluster.
   - **Storage**: Host optimized for storage usage. This type of host allows seamless expansion of storage capacity of your cluster.
   - **Compute**: Host optimized for computing purposes (CPU and memory).

7. In the **Configure Host** page, enter or update the host details such as hostname, CVM IPv4, CVM IPv6, hypervisor IPv4, hypervisor IPv6, IPMI IPv4, IPMI IPv6. Click **Next**.

   Host name is required for the Hyper-V clusters, while it is optional for AHV and ESXi clusters.

8. (Optional) In the **Networking** page, select the **Active Uplink**and **Backup Uplink** for each host and click **Next**. To configure the switches, expand the row containing each host.

9. In the **Software Check** page, review the AOS and hypervisor versions and their compatibility status.

   The new hosts must run the same AOS and hypervisor versions as the cluster. If the host's AOS version is lower than the cluster's AOS version, an upgrade is performed.

   If there is a version mismatch between the new host and ESXi or Hyper-V cluster, you are prompted to upload the ISO in the ~/software_downloads/hypervisor_installer directory in any one CVM of the cluster using wget command. If the ~/software_downloads/hypervisor_installer directory does not exist on the CVM, you must create the directory and then upload the ISO file. After you upload the ISO file, enter the ISO file name in the text box under **hypervisor Compatibility** and click **Validate**. The system checks for the file and displays a message.

10. Click **Next**.

11. Review the model and serial information displayed for all the selected hosts, and click **Expand Cluster**.

12. (Optional) You can click **Run Prechecks** before clicking **Expand Cluster** to know any issues that you must fix before proceeding with the Expand Cluster operation.

    Under Recent tasks list, you can verify that the **Expand Cluster** operation has started. The operation might take some time if it involves the re-imaging or a software upgrade at the node.

Prerequisites for expanding a Cluster through Prism Central

The process for expanding a cluster varies depending on the AOS version, hypervisor host type, data-at-rest encryption status, and certain hardware configuration factors.

AOS Considerations

The following apply to any cluster:

- Ensure that the total number of nodes per cluster does not exceed the Cluster Maximums defined in Maximum System Values in *Prism Element Web Console Guide*. Note that the maximum number of nodes per cluster differ per the hypervisor type and in case it is a pure hypervisor cluster (cluster with only one type of hypervisor) or mixed hypervisor cluster (cluster with more than one type of hypervisor).
- The expand cluster process does not support compute-only node preparation.

- The expand cluster discovery step (finding nodes to add) requires that IPv6 multicast packets are allowed through the physical switch. Therefore, the expand cluster process does not work when IPv6 is disabled in your network. If IPv6 is not enabled currently, do one of the following:
  - Enable IPv6 in your network and retry the expand cluster operation.
  - If enabling IPv6 is not an option, the expand cluster procedure allows you to enter the IP addresses of nodes to add manually and run discovery using IPv4. This requires that you have the IP addresses before starting the expand cluster operation.
- If the Controller VM memory on a new node is less than the current nodes in the cluster, the expand cluster process increases the memory on the new node to the same base value as the current nodes. The new Controller VM is upgraded to a maximum of 32 GB.

  The Controller VM is upgraded to a maximum of 28 GB for ESXi nodes with 64 GB or less of total physical memory. With total physical memory greater than 64 GB, the existing Controller VM memory is increased by 4 GB.
- A new node is reimaged automatically before being added under certain conditions. The following table describes those conditions.

Table 116: Node Imaging Criteria

Configuration	Description
Same AOS and hypervisor versions	The node is added to the cluster without reimaging it.
Same hypervisor version but different AOS version	The node is automatically reimaged before it is added. However, if the AOS version on the node is higher than the version on the cluster, you can upgrade the cluster to the higher version. If you do not upgrade the base cluster to match the node AOS version, the node is reimaged automatically to match the lower AOS version of the cluster. For more information about how to upgrade your cluster, see the Life Cycle Manager Guide.
Same AOS version but different hypervisor version	The node is automatically reimaged before it is added.

Note: If you are expanding a cluster (now) on which the network is segmented only by traffic type (management and backplane), see Network Segmentation During Cluster Expansion in the *Security Guide*.

AHV Considerations

The following apply to clusters running AHV:

- If the Controller VMs in the cluster reside in a VLAN configured network, the discovery process still finds any factory-prepared nodes regardless of their current VLAN status (configured or not configured).
- Network configuration has the following restrictions and requirements:
  - You cannot migrate management from br0 to other bridges.
  - You can only have the Controller VM management interface (eth0) and hypervisor management interface deployed on the br0 bridge.

ESXi Considerations

The following apply to clusters running ESXi:

- Before adding a host running ESXi 7.0U2 and later versions, with Trusted Platform Module (TPM) 2.0 enabled, to a cluster, Nutanix recommends that you backup the recovery key created when encrypting the host with TPM. For information on how to generate and backup the recovery key, see *KB 81661* in the *VMware documentation*. Ensure that you use this recovery key to restore the host configuration encrypted by TPM 2.0 if it fails to start after adding the host to your cluster. For information on how to restore an encrypted host, see *KB 81446* in the *VMware documentation*. If you don't have the recovery key, and if the host fails to start, contact Nutanix Support.
- If the ESXi root user password was changed from the default, the expand cluster operation might fail. In this case, reset the ESXi root user password to the default, and then retry the expand cluster procedure. For default cluster credentials, see KB 1661.
- While expanding a Nutanix cluster running NSX enabled ESXi hosts, add the newly imaged node to the Nutanix cluster where the host and CVM management network are configured with a standard vSwitch, and then add the node in NSX manager. Otherwise, the cluster expansion operation fails with the following error. For information on expanding a cluster, see Expanding a Cluster in *Prism Element Web Console Guide*.

  ```
  Failed to get VLAN tag of node <MAC Address of the node>
  ```

- If network segmentation is not enabled, expand cluster supports mixed (ESXi + storage-only) node clusters. However, when network segmentation is enabled, you cannot use expand cluster for a mixed cluster.
- Network configuration has the following restrictions and requirements:
  - You cannot configure the network when either a target node or the base cluster has LACP enabled. Prepare LACP nodes offline using a Foundation VM.
  - You cannot migrate management from vSwitch0 to another standard vSwitch.
  - Management interfaces must either be on a VSS or a DVS; a mixed setup is not supported.
  - If on VSS, the Controller VM management interface (eth0) and the hypervisor management interface must be deployed on vSwitch0 and connected to port group VM Network and Management Network, respectively.
  - If on DVS, all Controller VM management interfaces and all host management interfaces must be connected to the same distributed virtual switch and same port group. (However, the Controller VM interfaces can be connected to a different DVS port group than the host management interfaces.)
  - Segmented network interfaces (backplane, volume, DR) must be on same vSwitch type (VSS or DVS) as the management.
  - If network segmentation is enabled on the base cluster and the backplane is deployed on a separate vSwitch than management, you can create vSwitches (VSS or DVS) and prepare the required Controller VM interfaces. (Manual switch configuration is required for expand now but is integrated into the expand later work flow.)
  - If the base cluster is on DVS and you are doing an expand later, you can migrate the target nodes from the default vSwitch0 to that DVS.
- If the Controller VMs in the cluster reside in a VLAN configured network, you must first configure the new nodes in the same VLAN before attempting to add them. Otherwise, the discovery process does not find these nodes. For more information about VLAN configuration instructions, see Discovering Nodes in a VLAN-Segmented Network in the *Field Installation Guide*.

- To expand a cluster (now) configured with DVS for Controller VM external communication, ensure that you do the following:
  - Expand DVS with the new node.
  - Make sure both the host and the CVM are configured with DVS.
  - Make sure that host to CVM and CVM to CVM communications are working.
  - Follow the cluster expansion procedure.
- After adding the new nodes, note the following:
  - The common Nutanix datastores are mounted on the new nodes by default after cluster expansion.
  - The target storage containers must be set to mount on the new hosts. You can check the mount status from the **Storage** dashboard. For more information, see Storage Table View in *Prism Element Web Console Guide*. Click the **Storage Container** tab, select the target storage container, click the **Update** button, and verify that **Mount on all ESXi Hosts** (or the new hosts are checked in **Mount/Unmount on the following ESXi Hosts**) is selected in the **NFS DATASTORE** field.
  - If an added node has an older processor class than the existing nodes in the cluster, cluster downtime is required to enable EVC (enhanced vMotion compatibility) with the lower feature set as the baseline. For an indication of the processor class of a node, see the **Block Serial** field in the **Hardware** dashboard. For more information, see Hardware Diagram View or Hardware Table View in *Prism Element Web Console Guide*. For more information on enabling EVC, see vSphere EVC Settings in the *vSphere Administration Guide for Acropolis*.

    Caution: If you mix processor classes without enabling EVC, vMotion/live migration of VMs is not supported between processor classes. If you add the host with the newer processor class to vCenter Server before enabling EVC, cluster downtime is required to enable EVC later because all VMs (including the Controller VM) must be shut down.
  - Add the new nodes to the appropriate vCenter Server cluster. If an added node has a newer processor class (for example, Haswell) than the existing nodes in the cluster (Ivy Bridge or Sandy Bridge), enable EVC with the lower feature set as the baseline before adding the node to vCenter.
  - If you are adding multiple nodes to an existing EVC-enabled vCenter cluster, which requires powering off the Controller VM for each node to complete the addition, add just one node at a time and wait for data resiliency to return to *OK* before adding the next node to vCenter.

    Caution: Adding multiple nodes to vCenter simultaneously can cause a cluster outage when all the Controller VMs are powered off at the same time.
  - If you are adding a node to a cluster where HA is enabled with APD and VMCP is enabled, you must enable APD and APD timeout on the new host.
  - If you are adding new nodes to vCenter EVC configured cluster, ensure the following requirements.
    - Enabling EVC requires ESXi version 6.0 or above.
    - All ESXi nodes should be on same version and build.

Hyper-V Considerations

The following apply to clusters running Hyper-V:

- Network preparation is not supported. To bypass this step and prepare the nodes otherwise, click the **Skip Networking** button when you get to the **Networking** tab. In addition, imaging to AHV or ESXi is not possible if the node or base cluster is Hyper-V.

- If the Controller VMs in the cluster reside in a VLAN configured network, you must first configure the new nodes in the same VLAN before attempting to add them. Otherwise, the discovery process does not find these nodes. For more information about VLAN configuration instructions, see Discovering Nodes in a VLAN-Segmented Network in the *Field Installation Guide*.
- After adding the new nodes, if you manage your Hyper-V cluster by using Microsoft System Center VM Manager (SCVMM), do not use the Prism web console or Microsoft Failover Cluster Manager to add the new node to the failover cluster. Instead, use SCVMM to add the node to the Hyper-V cluster and then perform the following steps in the SCVMM user interface.
  1. Open the SCVMM user interface.
  2. Refresh the cluster in SCVMM. The new node is displayed under the failover cluster in the **Pending** state.
  3. Right-click the node and select **Add to host cluster**.
  4. Choose a run-as account that has the local administrator permissions on the new node.
  5. Click **OK**. The SCVMM agent is installed on the node and file shares are registered to the new node.
  6. Update the networking and other settings of the node to match your standard configuration.

For Microsoft Windows Server 2012 R2 deployments, after adding the node to the cluster in SCVMM, ensure that node disks are not added as clustered resources. Open the Failover Cluster Manager and click **Storage** > **Disks** to check.

Nutanix Clusters Considerations

The following apply to clusters hosted on a cloud platform:

- When expanding a cluster on AWS, the nodes are not added to the Cassandra ring (wait in a queue) until there are enough nodes to extend the ring. In addition, new nodes are added to the Cassandra ring only when they are do not break domain awareness. (Other services remain unaffected.)

Hardware Considerations

Note the following when it applies to the nodes you are adding:

- Ensure that you use the minimum version of Foundation required by your hardware platform. To determine whether Foundation needs an upgrade for a hardware platform, see the respective system specifications guide. If the nodes you want to include in the cluster are of different models, determine which of their minimum Foundation versions is the most recent version, and then upgrade Foundation on all the nodes to that version.
- When adding partially populated all-SSD nodes to an existing cluster, the minimum number of partially populated all-SSD nodes added must be equal to the maximum RF in the cluster.
- If you are adding a node with a different processor class to the cluster, ensure that there are no running VMs on the node and the host has the following configuration:
  - ESXi: Verify that EVC is enabled on the cluster.
  - Hyper-V: If you want to move the VMs between the nodes, ensure that you have selected the **Migrate to a physical computer with a different processor version** option for each VM by browsing to **Settings** > **Processor** > **Compatibility** in the **Action** pane of the Hyper-V Manager.

    Note: Do not shut down more than one Controller VM at the same time.

- If you expand a cluster by adding a node with older generation hardware to a cluster that was initially created with later generation hardware, power cycle (do not reboot) any guest VMs before migrating them to the added older generation node or before upgrading the cluster.

  Guest VMs are migrated during hypervisor and firmware upgrades (but not AOS upgrades).

  For example, if you are adding a node with G4 Haswell CPUs to a cluster that also has newer G5 nodes with Broadwell CPUs, you must power cycle guest VMs hosted on the G5 nodes before you can migrate the VMs to the node with G4 CPUs. Power cycling the guest VMs enables them to discover a CPU set compatible with older G4 processors.

  In rare cases, certain CPU features might be deprecated in the new generation of CPUs. For example, Intel introduced MPX in Skylake class of CPUs and deprecated it with Ice Lake. In such cases, introduction of Ice Lake (newer) CPUs to an all-Skylake cluster can cause problems with existing VMs that are running with MPX. Such VMs must be power cycled.

  Power cycle guest VMs from the Prism web console VM dashboard. Do not perform a Guest Reboot; a VM power cycle is required in this case.

- If you physically add a node to a block (for example, a single node shipped from Nutanix is placed into an empty slot in an existing chassis), log on to the Controller VM for that node, and update the following parameters in the /etc/nutanix/factory_config.json file:

  - rackable_unit_serial: Set it to the same value as the other Controller VMs in the same block.
  - node_position: Set it to the physical location of the node in the block (A, B, C, D).

  After changing the configuration file, restart Genesis with the `genesis restart` command.

Limitations for Expanding a Cluster through Prism Central

Consider the following limitations before you expand a cluster through Prism central.

- Encryption and Rack Awareness functionalities are not yet supported for expanding a cluster through Prism Central.
- Expand cluster functionality does not have an option to upload the hypervisor image through Prism Central web console. If there is a version mismatch between the new host and ESXi or Hyper-V cluster, you are prompted to upload the ISO in the ~/software_downloads/hypervisor_installer directory in any one CVM of the cluster using wget command, and enter the file details in the Prism Central web console.

Removing a Node through Prism Central

You can remove a node from a cluster using Prism Central.

Before you begin

Review Prerequisites for Removing a Node through Prism Central on page 437 before attempting to remove a node from a cluster.

About this task

The minimum supported version to remove a host using Prism Central web console is pc.2023.3.

To remove a host from a cluster using Prism Central web console, perform the following steps:

Procedure

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Hardware** > **Hosts** .
   The system displays the **List** tab by default with all the hosts across registered clusters.
3. Select the target host checkbox, and choose **Remove Host** from the **Actions** dropdown menu.
   The system displays the **Remove Host** window. As a result of successful execution of remove host operation, the host gets detached from the cluster and the VMs on the selected host are migrated to other hosts. Some VMs might be automatically powered off due to lack of resources.
4. In the **Remove host** window, click **Run Precheck** to run the prechecks for remove host operation. The system checks several points including the space availability for VMs of the node to be removed, fault tolerance, upgrade status on the node. If any of the prechecks fail, fix the issue and then click **Remove** to remove the host.
   You can verify the progress of the remove host operation under recent tasks list.

   Caution: Do not shut down the CVM or put the CVM into maintenance mode while the node removal is in progress.

Prerequisites for Removing a Node through Prism Central

Consider the following set of prerequisites before you remove a node from a cluster:

- For information about reclaiming or rebalancing your cluster licenses after node removal, see the License Manager Guide.
- Removing a node (host) takes some time because data on that node must be migrated to other nodes before it can be removed from the cluster. You can monitor progress through the dashboard messages. Removing a node implicitly removes all the disks in that node.
- (Hyper-V only) Initiating a removal of a node running Hyper-V fails if the node is running as a part of a Hyper-V failover cluster and the following message appears.

  ```
  Node node id is a part of a Hyper-V failover cluster failover cluster name. Please
   drain all the roles, remove the node from the failover cluster and then mark the
   node for removal.
  ```

  If this message is displayed in either nCLI or in web interface, as a cluster administrator, you must use the management tools provided by Microsoft such as *Failover Cluster Manager* to drain all the highly-available roles off the node. Then remove the node from the failover cluster followed by removing the node from the AOS cluster.
- (ESXi only) Before removing the node, ensure that there are no guest VMs running on the respective ESXi host. Note that CVM should be running on the node to initiate the node removal.
- (ESXi only) Temporarily disable DRS on the cluster before the node removal. The DRS must be re-enabled after the node is removed. Update the HA configuration to exclude the node you want to remove.

- (ESXi only) As a cluster administrator, you must use the management tools provided by VMware to first migrate all the guest VMs off the node/host, then remove the node from the AOS cluster of ESXi hosts. After that disconnect and remove the node (host) from the vCenter server.

  > **Caution:** Ensure that you migrate the guest VMs before removing a host or node. Verify that the target cluster has enough available compute capacity before actually migrating the VMs. Removing a node or host without first migrating the guest VMs may result in loss of service.

  1. Migrate the guest VMs that need to be migrated.
  2. Click **Remove Host** from Prism.
  3. After successful removal from the AOS cluster, put the host in maintenance mode.

     > **Caution:** When you put the host in maintenance mode, the maintenance mode process powers down or migrates all the VMs that are running on the host.

     For more information, see Node Maintenance in the *vSphere Administration Guide for Acropolis*.
  4. Remove the host from the vCenter server.

Limitations for Removing a Node through Prism Central

Consider the following limitations before you remove a node from a cluster.

- For an RF1 or RF2 enabled cluster, the minimum number of nodes to support node removal is four. You cannot remove a node from a cluster that has less than four nodes.
- For an RF3 enabled cluster, the minimum number of nodes to support node removal is five. You cannot remove a node from an RF3-enabled cluster that has less than five nodes.
- You can remove only one node at a time.

Disks Summary View

Summary View of All Disks

The **Summary** tab on the **Disks** page provides a dashboard of the disks across all the registered clusters.

To access the **Summary** view of all the disks:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Hardware** > **Disks** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
3. Click the **Summary** tab. The system displays **Summary** page for all the disks.

Clicking the **Summary** tab displays the following three widgets:

- **Highlighted Entities**: Displays a list of the disks with the highest usage of the parameter you select from the dropdown menu on the right of the widget. The options are **IO Bandwidth**, **IOPS**, **IO Latency**, and **Disk Usage**. Click the **View all XX Disks** link at the bottom to display the **List** tab (following section).
- **Alert**: Displays a list of disk-related alerts that occurred during the specified interval. Select either **Last 24 hours** (default) or **Last week** from the dropdown menu.
- **Anomalies**: Displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified interval. Select either **Last 24 hours** (default) or **Last week** from the dropdown menu. When an anomaly appears, you can click on the graph, which then displays a list of those anomalies. Clicking on an anomaly displays the event page for that anomaly.

Detailed View of an Individual Disk

For information about how to access the detailed view of an individual host, see Disk Details View on page 441.

List Tab

Clicking the **List** tab, which appears by default when you first open the page, displays a list of the disks across the registered clusters. The following table describes the fields that appear in the disks list. The fields vary based on the **Focus** menu selection, which is either **General** or **Performance**. A dash (-) is displayed in a field when a value is not available or applicable.

Table 117: Disks List Fields

Parameter	Description	Values
General Focus Fields		
Serial Number	Displays the disk serial number.	(serial number)
Host	Displays the name of the host in which this disk resides.	(host name)
Tier	Displays the disk type (tier name). Nutanix models can contain disk tiers for PCIe solid state disks (SSD-PCIe), SATA solid state disks (SSD-SATA), and direct attach SATA hard disk drives (DAS-SATA) depending on the model type.	[SSD-PCIe | SSD-SATA | DAS-SATA]
Mode	Displays the operating state of the disk.	online, offline
Disk Usage	Displays the percentage of disk space used and total capacity of this disk.	[0 - 100%] of xxx [GB| TB]
Cluster	Displays the name of the cluster in which the host resides.	(cluster name)
Performance Focus Fields		
Serial Number	Displays the disk serial number.	(serial number)
Disk Usage	Displays the percentage of disk space used and total capacity of this disk.	[0 - 100%] of xxx [GB| TB]
Disk Capacity	Displays the total physical space on the drive.	xxx [GB|TB]
IOPS	Displays I/O operations per second (IOPS) for this disk.	[0 - unlimited]
IO Bandwidth	Displays I/O bandwidth used per second for this disk.	xxx [MBps|KBps]
IO Latency	Displays the average I/O latency (in milliseconds) for this disk.	xxx [ms]
Cluster	Displays the name of the cluster in which the disk resides.	(cluster name)

You can filter the disks list based on a variety of parameter values. The following table describes the filter options available when you open the **Filter** pane. To apply a filter, select a parameter and check the box

of the desired value (or multiple values) you want to use as a filter. You can apply filters across multiple parameters. Some parameter filters require additional context such as a constraint string or a range.

Table 118: Filter Pane Fields

Parameter	Description	Values
Serial Number	Filters on the disk serial number. Select a condition from the dropdown list (**Contains**, **Doesn't contain**, **Starts with**, **Ends with**, or **Equal to**) and enter a string in the field. It will return a list of disks that satisfy the serial number condition/string.	(serial number string)
Host	Filters on the host name. Enter a string in the field. It will return a list of disks in the hosts that satisfy the host name condition/string.	(host name string)
Cluster	Filters on the cluster name. Enter a string in the field. It will return a list of disks in the clusters that satisfy the cluster name condition/string.	(cluster name string)
Mode	Filters on whether the disk is online or offline. Check the box for one or both of these modes. The number of disks currently in each state is displayed on the right of the line.	Online, Offline
Tier	Filters on whether the disk is in the solid state (SSD-SATA) or hard disk (DAS-SATA) tier. Check the box for one or both of these modes. The number of disks currently in each tier is displayed on the right of the line.	DAS-SATA, SSD-SATA
Health	Filters on the disk health state (good, warning, or critical). Select one or more states to return a list of disks in that state(s). The number of disks currently in each state is displayed on the right of the line.	Critical, Warning, Good
Disk Usage	Filters on the used capacity. Enter a percentage range in the "**from <low> to <high>** %" field. It will return a list of disks with used capacity in that range (0-100%).	([xx] to [yy]% range)
Disk Capacity	Filters on the total capacity. Enter an amount range in the "**from <low> to <high> GiB**" field. It will return a list of disks with total capacity in that range.	([xx] to [yy] GiB range)
IOPS	Filters on the IOPS. Enter a range in the "**from <low> to <high> iops**" field. It will return a list of disks with IOPS in that range.	([xx] to [yy] range)
IO Bandwidth	Filters on the I/O bandwidth used. Enter a range in the "**from <low> to <high> bps**" field. It will return a list of disks with I/O bandwidth usage in that range.	([xx] to [yy] range)
IO Latency	Filters on the average I/O latency. Enter a range in the "**from <low> to <high> ms**" field. It will return a list of disks with average I/O latency in that range.	([xx] to [yy] range)

You can group the disks list in the following ways:

- The **Color** dropdown menu allows you to color code the disk entries by tier type, mode, or health state. (You can only choose one.) A legend appears at the bottom to indicate what each color means in that grouping.
- The **Group** dropdown menu allows you to group the disk entries by host, tier type, mode, cluster, or health state. (You can only choose one.)
- [Tiles and Circles views only] The **Sort** dropdown menu allows you to group the disk entries by the information parameters (fields), which vary depending on whether you selected the **General** or **Performance** focus. (You can only choose one parameter.)

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options as the Alerts dashboard, except it is filtered to display just disk-related alerts across the registered clusters. For more information, see Alerts Summary View (Prism Central) in *Prism Central Alerts and Events Reference Guide*.

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options as the Events dashboard, except it is filtered to display just disk-related events across the registered clusters. For more information, see Events Summary View (Prism Central) in *Prism Central Alerts and Events Reference Guide*.

Metrics Tab

The **Metrics** tab allows you to view usage metrics across the hosts. Clicking the **Metrics** tab displays a list of available metrics; click the metric name to display the relevant information to the right. The following table describes the available metrics.

Table 119: Metrics Tab Fields

Metric	Description
IOPS	Displays total, read, and write IOPS tables listing current values and total disks (number). The current values are split into intervals (for example, less than 20, 20-40, 40-60, more than 60). Clicking on an interval displays the Summary tab filtered to just those disk. **Note:** The same format also applies to the other metrics in this table.
IO Latency	Displays total, read, and write I/O latency rate tables.
IO Bandwidth	Displays total, read, and write I/O bandwidth rate tables.

Disk Details View

Summary Tab

The **Summary** tab of an individual disk consists of a dashboard that provides the detailed information about the disk.

To access the **Summary** tab of an individual disk:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Hardware** > **Disks** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   By default, the system displays the **List** tab with all the disks.
3. Click the target <*disk_name*> to view the **Summary** tab of an individual disk.

   Note: Replace <*disk_name*> with the actual host name at your site.

Summary Tab

The **Summary** tab of an individual disk provides the following widgets:

- A **Properties** widget that displays summary information about the disk. For more information, see the Table 120: Disk Properties Fields on page 442 table.
- An **Alert** widget that displays a list of related alerts that occurred during the specified interval. Select either **Last 24 hours** (default) or **Last week** from the dropdown menu.
- An **Anomalies** widget that displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified interval. Select either **Last 24 hours** (default) or **Last week** from the dropdown menu. When an anomaly appears, you can click on the graph, which then displays a list of those anomalies. Clicking on an anomaly displays the event page for that anomaly.

The following table describes the fields in the **Properties** widget. A dash (-) in a field indicates there is not enough data to evaluate or a value is not assigned. The displayed fields vary by hypervisor.

Table 120: Disk Properties Fields

Parameter	Description	Values
Disk Usage	Displays the amount of used space on the drive.	xxx [GB|TB]
Cluster	Displays the name of the cluster in which the disk resides.	(cluster name)
Host	Displays the name of the host in which the disk resides.	(host name)
Host IP	Displays the IP address of the host.	(IP address)
Tier	Displays the disk type (tier name). Nutanix models can contain disk tiers for PCIe solid state disks (SSD-PCIe), SATA solid state disks (SSD-SATA), and direct attach SATA hard disk drives (DAS-SATA) depending on the model type.	[SSD-PCIe | SSD-SATA | DAS-SATA]
Mode	Displays whether the disk is currently online or offline.	[online|offline]
Disk Capacity	Displays the total physical space on the drive.	xxx [GB|TB]

Parameter	Description	Values
Status	Displays the operating status of the disk. Possible states include the following: • **Normal**. Disk is operating normally. • **Data migration initiated**. Data is being migrated to other disks. • **Marked for removal, data migration is in progress**. Data is being migrated in preparation to remove disk. • **Detachable**. Disk is not being used and can be removed.	Normal; Data migration initiated; Marked for removal, data migration is in progress; Detachable
Self Encryption Drive	Displays whether this is a self-encrypted drive.	Not Present, Present

Alerts Tab

The **Alerts** tab displays a table of alerts. This tab provides the same features and options as the Alerts dashboard, except it is filtered to display just alerts for this disk. For more information, see Alerts Summary View (Prism Central) in *Prism Central Alerts and Events Reference Guide*.

Events Tab

The **Events** tab displays a table of events. This tab provides the same features and options as the Events dashboard, except it is filtered to display just events for this disk. For more information, see Events Summary View (Prism Central) in *Prism Central Alerts and Events Reference Guide*

Metrics Tab

The **Metrics** tab allows you to view usage metrics for the disk. Click the **Metrics** tab and then the desired metric name (**IOPS**, **IO latency**, and **IO Bandwidth**) to display a graph for that metric on the right. The graph is a rolling time interval performance or usage monitor. The baseline range (based on the machine-learning algorithm) appears as a blue band in the graph.

> **Note:** The machine-learning algorithm uses 21 days of data to monitor and predict performance. A graph or baseline band may not appear if less than 21 days of data is available.

- Check the appropriate box(es) to have the graph display total, read, or write usage (or any combination of the three).
- Place the cursor anywhere on the horizontal axis to display the value at that time.
- Select the duration (time interval) from the dropdown list on the right (last 1 hour, last 24 hours, last week, last 21 days).
- Click **Alert Settings** to configure an alert for this metric. For more information, see Creating Custom Alert Policies in *Prism Central Alerts and Events Reference Guide*.

Storage Usage Tab

The **Usage** tab displays the following graph:

- The **Usage Summary** graph displays a rolling time interval monitor of disk storage usage that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. For more in depth analysis, you can add the monitor to the analysis page by clicking the blue link in the upper right of the graph.

GPUs Summary View

Summary View of All GPUs

The **Summary** tab on the **GPUs** page provides a dashboard of the GPUs across all the registered clusters.

To access the **Summary** view of all the GPUs:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Hardware** > **GPUs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
3. Click the **Summary** tab.

   The system displays **Summary** page for all the GPUs.

The following table describes the fields that appear in the GPUs list. A dash (-) is displayed in a field when a value is not available or applicable.

Table 121: GPU List Fields

Parameter	Description	Values
Type	Displays the GPU model type.	Tesla M10, Tesla M60, Tesla M60 compute
Cluster	Displays the name of the cluster in which the GPU resides.	(cluster name)
Mode	Displays the mode in which the GPU is operating.	None, vGPU, passthrough
Allocation	Indicates the number of VMs allocated to the GPU.	"No VM allocated", "*x* of *y* VMs allocated"

You can filter the GPUs list based on several parameter values. The following table describes the filter options available when you open the GPUs view **Filter** pane. To apply a filter, select a parameter and check the box of the desired value (or multiple values) you want to use as a filter. You can apply filters across multiple parameters. Some parameter filters require additional context such as a constraint string or a range.

Table 122: Filter Pane Fields

Parameter	Description	Values
Type	Filters on the GPU model type. Select a condition from the dropdown menu (**Contains**, **Doesn't contain**, **Starts with**, **Ends with**, or **Equal to**) and enter a string in the field. It returns a list of GPUs that satisfy the type condition/string.	Tesla M10, Tesla M60, Tesla M60 compute
Host	Filters on the host name. Enter a string in the field. It returns a list of GPUs in the selected hosts.	(host name string)

Parameter	Description	Values
Cluster	Filters on the cluster name. Enter a string in the field. It returns a list of GPUs in the selected clusters.	(cluster name string)
Mode	Filters on the GPU operation mode. Check the box for one or more of these modes. The number of GPUs currently in each mode is displayed on the right of the line.	None, vGPU, Passthrough

You can group the GPUs list in the following ways:

- The **Group** dropdown menu allows you to group the GPU entries by cluster, host, or mode. (you can only choose one.)
- The **Sort** dropdown menu allows you to group the GPU entries by type, cluster, mode, or allocation. (you can only choose one parameter.)

Clicking the **Summary** tab displays the following three widgets:

- **Highlighted Entities**: Displays a list of the disks with the highest usage of the parameter you select from the dropdown menu on the right of the widget. The options are **IO Bandwidth**, **IOPS**, **IO Latency**, and **Disk Usage**. Click the **View all XX Disks** link at the bottom to display the **List** tab (following section).
- **Alert**: Displays a list of disk-related alerts that occurred during the specified interval. Select either **Last 24 hours** (default) or **Last week** from the dropdown menu.
- **Anomalies**: Displays a graph of memory, I/O, CPU, networking, or disk anomalies that occurred during the specified interval. Select either **Last 24 hours** (default) or **Last week** from the dropdown menu. When an anomaly appears, you can click on the graph, which then displays a list of those anomalies. Clicking on an anomaly displays the event page for that anomaly.

Detailed View of an Individual GPU

For information about how to access the detailed view of an individual host, see GPU Details View on page 445.

GPU Details View

Summary Tab

The **Summary** tab of a GPU consists of a dashboard that provides the detailed information about the GPU.

To access the **Summary** tab of an individual GPU:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Hardware** > **GPUs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   By default, the system displays the **List** tab with GPUs across all the registered clusters.
3. Click the target <*GPU_name*> to view the **Summary** tab of an individual GPU.

> **Note:** Replace <*GPU_name*> with the actual GPU name at your site.

Clicking the **Summary** tab displays the following:

- A section on the left that displays summary information about the GPU. For more information, see the Table 123: GPU Summary Fields on page 446 table.
- A section of the right that displays GPU performance metrics. The graphs are rolling time interval performance monitors that can vary from one to several hours depending on activity moving from right to left. Placing the cursor anywhere on the horizontal axis displays the value at that time. This section includes the following graphs:
  - **GPU Usage**: Displays the percentage of GPU capacity being used.
  - **GPU Framebuffer Usage**: Displays the percentage of GPU framebuffer (RAM) capacity being used.
- **Action** on the upper right (which appears regardless of which tab is selected):
  - Click the Help icon to open a help page in a separate tab or window.
  - Click the X icon to close the details page.

The following table describes the GPU summary information fields. A dash (-) is displayed in a field when a value is not available or applicable.

Table 123: GPU Summary Fields

Parameter	Description	Values
GPU Type	Displays the GPU type for this entry.	Tesla M10, Tesla M60, Tesla M60 compute
Cluster Name	Displays the name of the cluster in which the GPU resides.	(cluster name)
Host	Displays the name of the host in which the GPU resides.	(host name)
Mode	Displays the GPU operational mode. If it is vGPU, an additional field appears that displays the vGPU profile used.	None, vGPU, Passthrough
Allocation	Displays the number of VMs allocated to this GPU. This field does not appear if no VMs are allocated.	"*x* of *y* VMs allocated"
Framebuffer (RAM) Per GPU	Displays the framebuffer (RAM) size per GPU.	xx GiB
ID	Displays the GPU ID number.	(ID number)

VMs Tab

Clicking the **VMs** tab displays a table of VMs allocated (attached) to the GPU. The table includes the following fields:

- **Name**: Displays the VM name. Click the name to display the details page for that VM. For more information, see VM Details View on page 108.
- **GPU Usage**: Displays the percentage of GPU capacity used by this VM.
- **GPU Framebuffer Usage**: Displays the percentage of GPU framebuffer (RAM) capacity used by this VM.

ACTIVITY ENTITIES – ALERT AND EVENT MONITORING

For information about Alerts and Events in Prism Central, see Prism Central Alerts and Events Reference Guide.

ACTIVITY ENTITIES – TASKS AND AUDITS

You can access dashboards for the following activity monitors from the **Activity** entity of the **Infrastructure** application. For information about how to access the entity items available in **Activity** entity, see Application-specific Navigation Bar on page 57.

- Audits (see Audits Summary View on page 448)
- Tasks (see Tasks View on page 451)

Audits Summary View

The **Audits** summary view provides a dashboard of the actions performed across the registered clusters.

Note:

- The retention period for audit entries is four weeks by default.
- Audit information appears only for those registered clusters running AOS 5.10 or later.
- Audit logs with default values are generated when updates to VMs are initiated, either by Prism Central **Self Service** users or by using Nutanix v3 API calls for the first time.
- For all Prism Central related events, see Prism Central Logs in *Prism Central Alerts and Events Reference Guide*. Additionally, you can refer to the Audit Log Events in *Prism Central Alerts and Events Reference Guide* for the complete list of captured audit events.

To access the **Audits** summary view, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Activity** > **Audits** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The system displays the **Audits** dashboard.

The following table describes the fields that appear in the audits list. A dash (-) is displayed in a field when a value is not available or applicable.

Table 124: Recovery Plans Fields

Parameter	Description	Values
Action Description	Describes the action taken such as "deleted VM `vm-name`" or "added disk `disk-name`"	(action description)
User Name	Displays the name of the user who requested the action.	(user name)
Entity Affected	Displays the entity name. Click the name to go to the details page for that entity.	(entity name)
Entity Type	Displays the entity type such as VM or host.	(entity type)

Parameter	Description	Values
Operation Type	Displays the type of operation that took place. The possible operation types depend on the entity type and can include create, update, delete, and power state change.	(operation type)
Request Time	Displays the time the user requested the action.	(time and date)
Cluster	Displays the name of the cluster in which the action took place. Click the cluster name to display the details page for that cluster.	(cluster name)

To filter the list, click **Modify Filters** (upper right). This displays a pane for selecting filter values. The following table describes the filter options available. You can apply multiple filters together. For example, if you want to filter by a particular VM name, you can filter by *entity type* = *VM* and then use the *name contains* filter.

Table 125: Filter Pane Fields

Field	Description	Values
User IP	Enter a user IP address and then click **Add** to filter for actions requested by that user. You can add multiple user IP addresses.	(IP address)
Cluster	Enter a cluster name in the field to filter for actions in the cluster.	(cluster name)
Entity Type	Check the boxes of one or more entities to filter for actions on those entity types.	VM, Storage Container, Catalog Item, Image, Cluster, Host, Disk, GPU, Security Policy, NGT Policy, Project, Role, User, Category, Availability Zone, Protection Policy, Recovery Plan, Recoverable Entity, Report
Operation Type	Check the boxes of one or more operations to filter on those operations.	Create, Update, Delete, Power State Change
Request Time	Check an interval box to filter for actions that were requested during that time period. For the custom interval option (**from** *xxx* **to** *xxx*), click in each field and select a date from the pop-up calendar.	Last 1 hour, Last 24 hours, Last week, From *xxx* to *xxx*
Cluster	Enter a cluster name in the field to filter for actions in the cluster. **Note:** Entering *Prism Central* in the cluster filter criteria does not populate any result.	(cluster name)

Field	Description	Values
User IP	Enter a user IP address and then click the **Add** to filter for actions requested by that user. You can add multiple user IP addresses.	(IP address)

Audit Details View

The details page of an individual action provides the detailed information about the action.

To access the details page of an action:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Activity** > **Audits** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
3. Click the target <*action_name*> to view the details page of an individual action.

> **Note:** Replace <*action_name*> with the actual action description at your site.

The details page includes the following:

- The action description (upper left). You can switch from one action details page to another by selecting from the dropdown list.
- A section on the left that displays summary information about the action (see following table).
- A section on the right that displays a table of information specific to that action. The table shows the attributes that were changed during the action and the current value that is set for the attribute. The attributes vary depending on the specifics of the action (see following examples).

The following table describes the action summary information fields. A dash (-) is displayed in a field when a value is not available or applicable.

Table 126: Action Summary Fields

Parameter	Description	Values
Action Description	Displays the action description.	(description)
User Name	Displays the name of the user who requested the action.	(user name)
Target Entity	Displays the name of the entity that was the action target. Click the entity name to display the details for that entity.	(entity name)
Affected Entities	Displays the names of the entities that were affected by the action. Click an entity name to displays the details page for that entity.	(one or more entity names)
Operation Type	Displays the type of operation that took place. The possible operation types depend on the entity type and can include create, update, delete, and power state change.	(operation type)
Request Time	Displays the time the user requested the action.	(time and date)
User IP	Displays the IP address of the user.	(IP address)

Parameter	Description	Values
Cluster	Displays the name of the cluster in which the action took place. Click the cluster name to display the details page for that cluster.	(cluster name)
Status	Displays the status of the action.	Succeeded, Failed

Tasks View

The **Tasks** page provides a dashboard that displays information about all tasks across the registered clusters.

> **Note:** From Prism Central version pc.2024.1 onwards, you can view a task if you have the view permission for any one of the clusters affected by the task.

To access the **Tasks** dashboard:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Activity** > **Tasks** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
3. The system displays the **Tasks** dashboard.

An icon appears in the main menu when there are current tasks (running or completed within the last 48 hours). The icon appears blue when a task runs normally, yellow when it generates a warning, or red when it fails. Clicking the icon displays a dropdown menu of current tasks.

You can see the tasks dashboard by doing one of the following:

- Clicking the **View All Tasks** link at the bottom of the current tasks dropdown menu.
- Clicking the **View All Tasks** link in the Tasks widget in the main dashboard.
- Selecting **Activity** > **Tasks** from the **Navigation Bar**.

You can do the following in the Tasks dashboard:

- Filter the list by entering a criteria in the **Modify Filter** field.
- Filter the list by clicking **Modify Filters**. This displays a filter pane on the right of the screen. Click on one or more of the states to filter the list to just tasks in those states. The states are Aborted, Canceled, Failed, Queued, Running, Paused, Skipped, Succeeded, and Scheduled. The number of tasks in each state currently appear to the right of the state name. Click the X icon (upper right) to close the filter pane.
- Download the task list in CSV format by clicking the download icon (on the right above the table).

The following table describes the fields in the tasks list. Each task appears in the list for a minimum of one hour after completion, but how long that task remains in the list depends on several factors. In general, the maximum duration is two weeks. However, tasks are rotated off the list as new tasks arrive, so a task might disappear from the list much sooner when activity is high. In some cases a task appears for longer than two weeks because the last task for each component is retained in the listing.

Table 127: Tasks List Fields

Parameter	Description	Values
Task	Specifies which type of operation the task is performing.	(name of operation such as upgrade)
Entity Affected	Lists the entity name or describes the operation. If this is a live link, click it to either see more details or go to the entity details page.	(name or description)
Cluster	Specifies the cluster name(s) on which the task is running. A dash (-) appears when the task applies to Prism Central rather than one of the registered clusters.	(cluster names)
Progress	Indicates the current percentage complete for the task.	0%-100%
Status	Indicates the task status, which can be pending, running, completed, or failed.	Succeeded, Running,Failed, Queued
Created On	Displays when the task began.	xx [seconds| minutes| hours| days] ago
Duration	Displays how look the task has been running or took to complete.	xx [seconds| minutes| hours| days]

OPERATIONS ENTITIES

Starting from Prism Central version 2023.3, NCM Intelligent Operations (formerly AIOps) now has a new user interface. The following Operations Entities have been moved from Prism Central Infrastructure app to the new user interface created for NCM Intelligent Operations:

- Analysis
- App Discovery
- Monitoring Configurations
- Operations Policies
- Planning
- Playbooks
- Reports
- Settings and Configurations

The documentation for the above-mentioned entities has been moved to the newly created *Intelligent Operations Guide*. For more information, see Intelligent Operations Guide.

ADMINISTRATION ENTITIES

You can manage the following entity items from the **Administration** entity of the **Infrastructure** application:

- Users, Roles, and Projects. For more information about how to manage users, roles, and projects in Prism Central, see Prism Central Admin Center Guide.
- LCM. For information about LCM, see LCM Documentation.
- Availability Zones. For information about Availability Zones in Prism Central, see Availability Zones on page 454.
- Categories. For information about how to manage Categories in Prism Central, see Category Management on page 454.

For information about how to access the entities items available in **Administration** entity, see Application-specific Navigation Bar on page 57.

Availability Zones

Nutanix Disaster Recovery works with sets of physically isolated locations called availability zones (AZs). For information about Availability Zones in Prism Central, see Nutanix Disaster Recovery Guide .

Category Management

A category is a grouping of entities into a key-value pair. Typically, new entities are assigned to a category based on some criteria. Policies can then be tied to those entities that are assigned (grouped by) a specific category value.

For example, you might have a Department category that includes values such as engineering, finance, and HR. In this case, you could create one backup policy that applies to engineering and HR and a separate (more stringent) backup policy that applies to just finance. Categories allow you to implement a variety of policies across entity groups, and Prism Central allows you to view any established relationships quickly.

The following hypothetical example illustrates the relationship of four policies (Backupbasic, Engenvironment, Hourly alerts, and Daily backup) tied to three departments (Eng, Fin, and HR) that apply to 30+ VMs in each department.

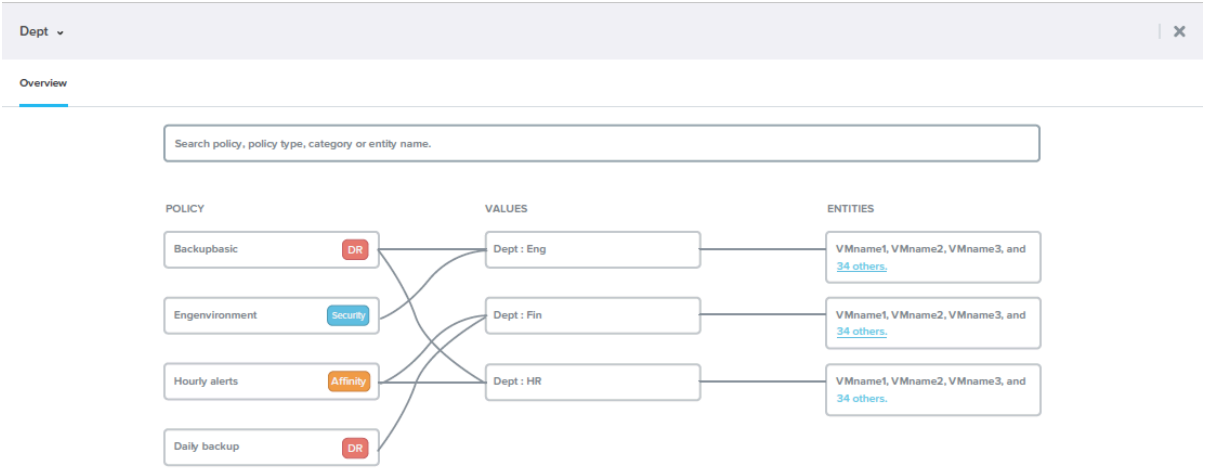


Figure 185: Dept Details View (example)

Important:

The **Storage: $Default** category is used to assign the default storage policy to an entity such as a VM or a VG. You cannot associate any other storage policy with this category. Nutanix recommends that you do not associate any other policy with the **Storage: $Default** category or make any other changes to this category.

For more information on the default storage policy, see Default Storage Policy on page 498.

Categories Summary View

The **Categories** summary view provides a dashboard of the existing categories.

To access the **Categories** dashboard:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Administration** > **Categories** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
3. The system displays the **Categories** dashboard.

The following table describes the fields that appear in the categories list. A dash (-) is displayed in a field when a value is not available or applicable.

Table 128: Categories List Fields

Parameter	Description	Values
Name	Displays the name of the category.	(category name)
Value	Displays the values defined for the category. Click **Show more** (right of line) to see a line for each value. (Click**Show fewer** to collapse the list.) You may see an icon with a "showing X of Y" message to indicate there are additional values; click the icon to display the full list.	(value names)

Parameter	Description	Values
Associated Entities	Lists the number of entities assigned to this category. **Note:** For a non-admin user, Prism Central displays the list of associated entities only when you expand the row. Prism Central does not display the cumulative list of associated entities for a non-admin user.	(number)
Associated Policies	Lists the number of policies assigned to this category.	(number)

You can filter the category list based on several parameter values. The following table describes the options available when you click **Modify Filters**, which displays the Categories view **Filters** pane. To apply a filter, select a parameter and check the box of the desired value (or multiple values) you want to use as a filter. You can apply filters across multiple parameters.

Table 129: Filter Pane Fields

Parameter	Description	Values
Name	Filters on the category name. Select a condition from the dropdown list and enter a string in the field. It will return a list of categories that satisfy the name condition/string. **Note:** In this and the Value field, the condition menu options are **Contains**, **Does not contain**, **Starts with**, **Ends with**, and **Equal to**.	(name string)
Entities	Filters on the entity type. Check the box for one or more entity types.	VM, Host, App, Blueprint, Cluster, Image, Marketplace Item, Reports, Subnet
Policies	Filters on the policy type. Check the box for one or more entity types.	Security Policy, Affinity Policy, Image Placement Policy, NGT Policy, Protection Policy, QoS Policy

Click **New Category** to create a category. For more information, see Creating a Category on page 457.

Perform the following category-specific actions on a category using the **Actions** dropdown menu. The **Actions** dropdown appears when one or more categories are selected.

- **Update**: Click this action to modify an existing category. For more information, see Modifying a Category on page 458.
- **Delete**: Click this action to modify an existing category.

Category Details View

The details page of an individual category provides the detailed information about the category.

To access the details page of a category:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Administration** > **Categories** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
3. Click the target <*category_name*> to view the details page of an individual category.

   Note: Replace <*category_name*> with the actual category name at your site.

A category details page includes the following:

- Category name (upper left). You can switch from one category to another by selecting a different category name from the dropdown list in the upper left of the screen.
- Action buttons (upper right).
  - Click **Update** to update the category definition. For more information, see Modifying a Category on page 458.
  - Click **Delete** to delete the category.

    The actions are grayed out if not allowed. For example, you cannot delete system categories.
  - Click the Help icon to open a help page in a separate tab or window.
  - Click the X icon to close the details page.
- **Policies** (left), **Values** (middle), and **Entities** (right) columns that list the values defined for the category plus the policies and entities associated with that category. The list does not include the policies that are associated with multiple categories. Placing the cursor over a policy, value, or entity displays lines that graphically indicate the association among the three parameters.

Creating a Category

About this task

To create a category, do the following:

Procedure

1. Log in to Prism Central.
2. Select **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Administration** > **Categories** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
3. Go to the categories dashboard and click **New Category**.
   The **Create Category** page appears.

4. Do the following in the indicated fields:

   a. **Name**: Enter a name for the new category.

      > **Note:** The **Name** and **Values** fields are case sensitive.

   b. **Purpose** (optional): Enter a description of the category purpose.

   c. **Values**: Enter a category value. To add a second (and subsequent) value, click the plus sign (+) to the right. This opens another line; enter the next value in the new field.

      Repeat this step for all the values you want to include in the category. For example, if the category name is Departments, values might include Engineering, HR, Sales, Marketing, and so on.

      Duplicate values are discarded. Character case is considered when determining duplicates. For example, multiple instances of the value `Sales` are considered duplicates and all instances but one are dropped; the values `Sales` and `sales` are considered unique and are accepted.

   d. Click **Save**.

      This creates the category and closes the page. The new category now appears in the category list.

Modifying a Category

About this task

You can update or delete a custom (user-defined) category. System (built-in) categories cannot be modified or deleted.

> **Note:** You cannot delete a category if it is used in an existing policy. All associations with existing policies must be removed before a category can be deleted.

To update or delete an existing category, do the following:

Procedure

1. Log in to Prism Central.
2. Select **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Administration** > **Categories** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
3. Go to the categories dashboard and select the desired category from the list.
4. Do one of the following:

   » To modify that category, select **Update** from the **Actions** dropdown menu. The **Update Category** page appears, which includes the same fields as the **Create Category** page. For more information, see Creating a Category on page 457. Update the field values as desired and then click the **Save** button.

   » To delete that category, select **Delete** from the **Actions** dropdown menu. You are prompted to verify the delete (click the **OK** button). The category is then deleted and removed from the list.

Assigning a Category

About this task

You can assign a category value to an entity of the following types: cluster, VM, host, volume group, catalog, image, report, subnet, blueprint, app, and marketplace item. To assign a category value to one or more entities, do the following:

Procedure

1. Log in to Prism Central.
2. Select **Infrastructure** application from Application Switcher Function on page 19, and navigate to the dashboard of the entity that you want to assign a category to.
3. Select all the entities that you want to tag with the same category value.
   - Cluster: Go to the **List** tab in the clusters dashboard and select the checkboxes for the target clusters. For more information, see Clusters Summary View on page 398.
   - VM: Go to the **List** tab in the VMs dashboard and select the target VMs. For more information, see VMs Summary View on page 95.
   - Host: Go to the **List** tab in the hosts dashboard and select the target hosts. For more information, see Hosts Summary View on page 420.
   - Volume group: Go to the **List** tab in the volume groups dashboard and select the target volume groups. For more information, see Volume Groups Summary View on page 301.
   - Catalog: Go to the catalog items dashboard and select the target catalog items. For more information, see Catalog Items Summary View on page 263.
   - Image: Go to the **List** tab in the images dashboard and select the target images. For more information, see Images Summary View on page 239.
   - Report: Go to the reports dashboard and select the target reports. For more information, see Reports Summary View in *Intelligent Operations Guide*)
   - Subnet: Go to the subnets dashboard and select the target subnets. For more information, see Subnet Details View on page 344.
   - Blueprint, App, or Marketplace item: For information, see Marketplace Manager section of the *NCM Self-Service Administration and Operations Guide*.
4. Select **Manage Categories** from the **Actions** dropdown menu.
   This displays the **Manage [Cluster|VM|Image|Subnet] Categories** page.

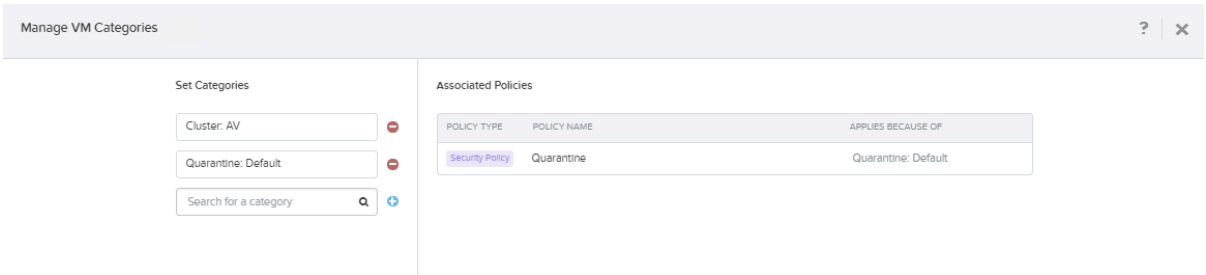


Figure 186: Manage VM Categories Page

5. In the **Manage [Cluster|VM|Image|Subnet] Categories** page, do the following:

   a. Enter a category name in the **Set Categories** field, select the target value from the list, and then click the plus sign (+) to the right of the field to assign that category value to the selected entities.

      The **Set Categories** field acts like a search field; it provides a list of matching categories as you enter a string. Select the desired category value when you see it in the list. Any policies associated with the selected category value appear in the **Associated Polices** section to the right.

   b. Repeat the first step to assign a value for a second category.

      You can repeat this step for as many categories as desired. To illustrate, in the figure above the VMs are assigned two values, *AV* from the *Cluster* category and *Default* from the *Quarantine* category. In this example *Cluster:AV* has no policies associated with it currently, but *Quarantine:Default* is associated with the Quarantine security policy.

      > **Note:** Categories support multi-cardinality, which means you can assign multiple category values to the same entity. In this case you can assign multiple values to the same VM.

   c. Click **Save** to save the category assignment.

POLICIES IN INFRASTRUCTURE

This section describes the policies framework in Prism Central.

Policies are used to define the systematic configuration guidelines for the following requirements:

- Controlled management of **VMs**, **Images**, **Storage**, and **Network & Security** entities. For more information, see the following sections:
  - VM Policy Management on page 461 for VM-related policies.
  - Image Policy Management on page 476 for image-related policies.
  - Storage Policy Management on page 495 for storage-related policies.
  - Security Policy Management on page 490 for policies related to network security framework setup.
- System services customization. For more information, see Operations Policy Management in *Intelligent Operations Guide*.
- Disaster Recovery setup. For information about how to create the protection policies in Disaster Recovery setup, see Nutanix Disaster Recovery Guide.

VM Policy Management

In Prism Central, you can create and manage the following types of policies for the VMs:

- Affinity Policies (see Affinity Policies Defined in Prism Central on page 461)
- NGT Policies (see NGT Policies on page 472)

Affinity Policies Defined in Prism Central

In Prism Central, you can define the category-based VM-Host affinity policies, where a set of VMs can be affined (correlated) to run only on a particular set of hosts. Category-based affinity policy enables you to easily manage affinities for a large number of VMs. In case of any changes to the affined hosts, you only need to update the category of the host, and it updates the affinity policy for all the affected VMs.

This policy checks and hard enforces where a VM can be hosted when you start or migrate the VM. If there are no resources available on any of the affined hosts, the VM is not started.

> **Note:**
>
> If you create a VM-Host affinity policy for a VM that is configured for asynchronous replication, you must create similar categories and corresponding policies on the remote site as well. If you define similar categories and policies on the remote site, the system applies the affinity policies when the VMs are migrated to the remote site.

For information about how the category-based VM-Host affinity policies are handled during disaster recovery, see Affinity Policies Handling - PC Based DR Solution with Physically Isolated Locations.

Affinity Policies Summary View

The affinity policies summary view enables you to access a list of all the user-defined affinity policies across registered clusters.

To access the summary view of all affinity policies:

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.

   The system displays the **List** tab by default.
3. Select **Affinity Policies** in the **Policies** tab dropdown menu.

   The system displays a summary view of affinity policies across all registered clusters.

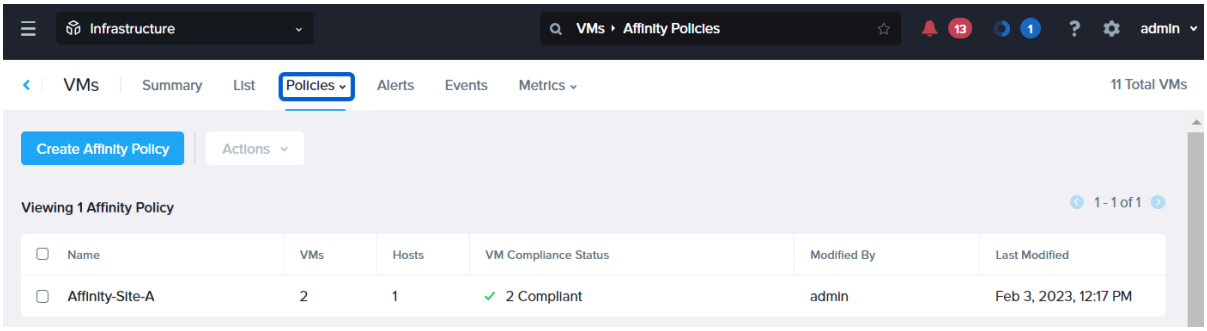


Figure 187: Summary View - All Affinity Policies

Table 130: Affinity Policies Page - Field Description

Parameter	Description	Values
Name	Displays the affinity policy name.	(name)
VMs	Displays the count of VMs associated with the selected affinity policy.	(number of VMs)
Hosts	Displays the count of hosts associated with the selected affinity policy.	(number of hosts)
VM Compliance Status	Displays the compliance status of the VMs associated with this policy. If the policy is being applied and the compliance status is not yet known, the status is displayed as Pending. If a VM is part of multiple VM-Host affinity policies, the oldest policy is applied on the VM. For rest of the policies, the VM is displayed as non-compliant.	(number of VMs Compliant/Non Compliant/Pending)
Modified By	Displays the name of the user who modified the selected affinity policy last time.	(user)
Last Modified	Displays the date and time when the selected affinity policy is modified last time.	(date & time)

You can perform the following actions for the affinity policies in the **Affinity Policies** summary view:

- Access the detailed information about an individual affinity policy. For more information, see Affinity Policies Details View on page 463.
- Create an affinity policy. For more information, see Creating an Affinity Policy on page 469.
- Use the **Actions** dropdown menu to update, delete, or re-enforce an affinity policy. For more information, see Managing Affinity Policies on page 470.

Affinity Policies Details View

The affinity policy details view allows you access the detailed information about an individual affinity policy. It includes four tabs: **Summary**, **Categories**, **Entities**and **Audit**.

To access the details view of an individual affinity policy, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.

   The system displays the **List** tab by default.
3. Select **Affinity Policies** in the **Policies** tab.

   The system displays a summary view of affinity policies across all registered clusters.
4. Click the target *<Affinity_Policy_Name>* to view the **Summary** tab of an individual affinity policy.

> **Note:** Replace *<Affinity_Policy_Name>* with the actual affinity policy name at your site.

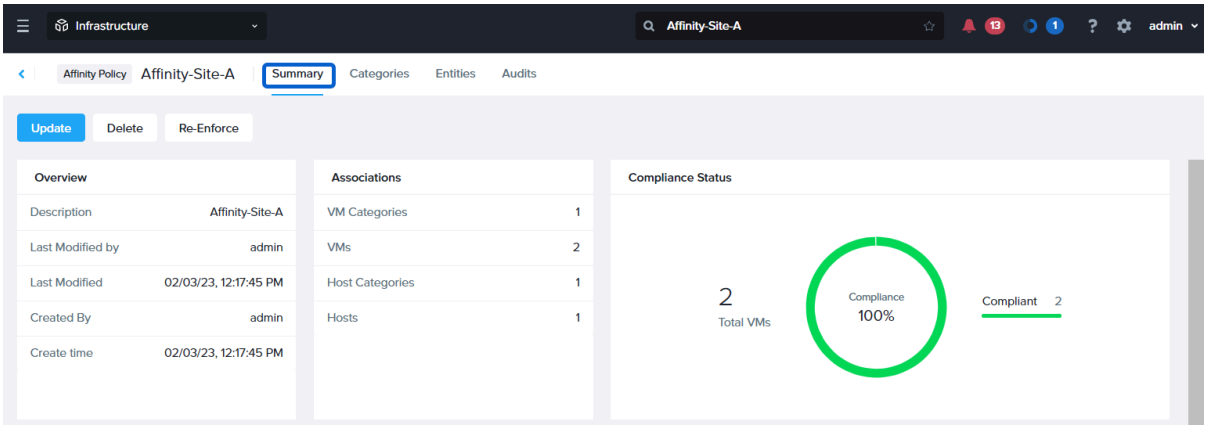


Figure 188: Affinity Policies Details view

The **Summary** tab of an individual affinity policy provides the following widgets:

- **Overview** - Displays an overview information about the affinity policy.
- **Associations**- Displays the associated VM and Host entities and their categories.
- **Compliance Status** - Displays the compliance status of the VMs associated with this policy. If the policy is being applied and the compliance status is not yet known, the status is displayed as Pending. If a VM is part of multiple VM-Host affinity policies, the oldest policy is applied on the VM. For rest of the policies, the VM is displayed as non-compliant.

For information about the fields available in the widgets, see Affinity Policy Widgets - Field Details on page 463.

<Action> available above the widgets. Click the appropriate *<Action>* to run that administrative action on the affinity policy. For more information about how to perform any *<Action>*, see Managing Affinity Policies on page 470.

Affinity Policy Widgets - Field Details

The following table describes the fields in the **Overview**, **Associations**, and **Compliance Status** widgets.

Table 131: Affinity Policy Widgets - Field Description

Field	Description	Values
Overview widget		
Description	Displays the affinity policy description specified while creating the affinity policy.	(description)
Last Modified By	Displays the name of the user who modified the affinity policy last time.	(user)
Last Modified	Displays the date and time when the policy is modified last time.	(date & time)
Created By	Displays the name of the user who created the affinity policy	(user)
Create time	Displays the date and time when the affinity policy is created.	(date & time)
Associations widget		
VM Categories	Displays the count of VM categories mapped to the selected affinity policy.	(number of VM categories)
VMs	Displays the count of VMs associated with the selected affinity policy.	(number of VMs)
Host Categories	Displays the count of host categories mapped to the selected affinity policy.	(number of host categories)
Hosts	Displays the count of hosts associated with the selected affinity policy.	(number of hosts)
Compliance Status widget		
Total VMs	Displays the total number of VMs in the selected affinity policy.	(total number of VMs)
Compliance	Displays the compliance status in percentage .	Integer %
Compliant, In Progress, or Non compliant	Displays the number of VMs that are compliant and non-compliant with the affinity policy. If the compliance check is in progress, the system displays the compliance status as *In progress*.	Compliant, In Progress, or Non compliant

Categories Tab

The **Categories** tab displays the VMs and hosts categories information.

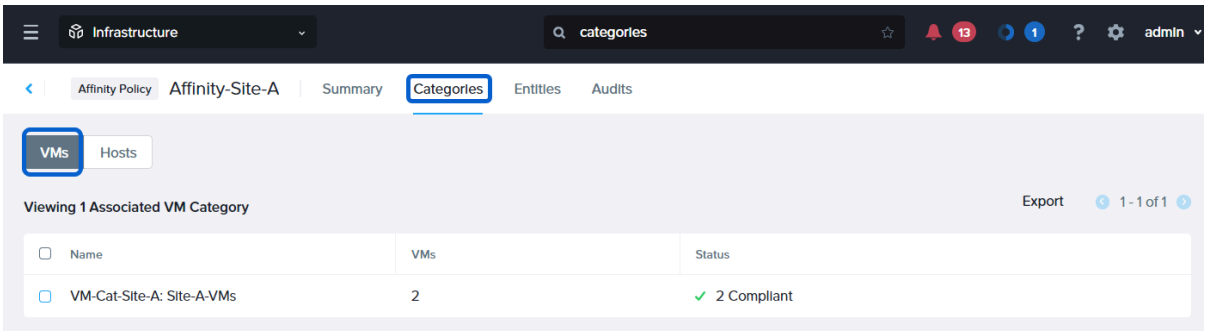


Figure 189: Affinity Policies - Categories (VMs)

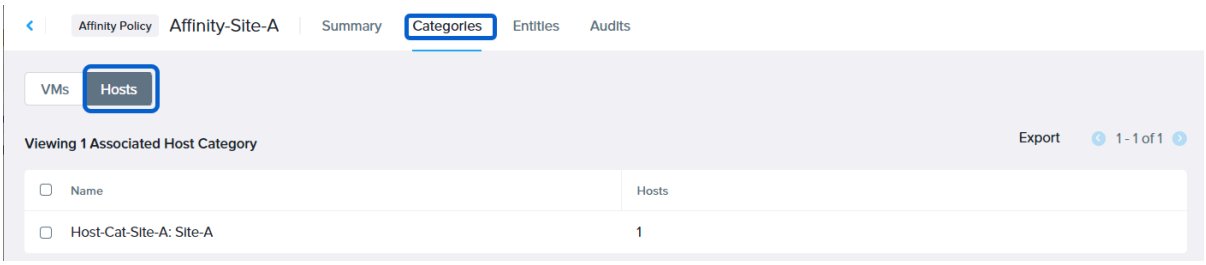


Figure 190: Affinity Policies - Categories (Hosts)

The following table describes the information displayed in the **Categories** tab

Table 132: Categories Tab -Field Description

Field	Description	Values
VMs tab		
Name	Displays the VM category name and its value.	(VM Category Name: Value)
VMs	Displays the count of VMs associated with the selected affinity policy.	(number of VMs)
Status	Displays the compliance status.	(number of VMs Compliant|Non-compliant|Pending
Host tab		
Name	Displays the host category name and its value.	(host category Name: Value)
Hosts	Displays the count of hosts associated with the selected affinity policy.	(number of hosts)

You can export the table that contains the list of VM categories and host categories and their information to a file in a CSV format. For more information about **Export** option, see Export on page 32.

Entities Tab

The **Entities** tab displays the VMs and hosts entity-related information.

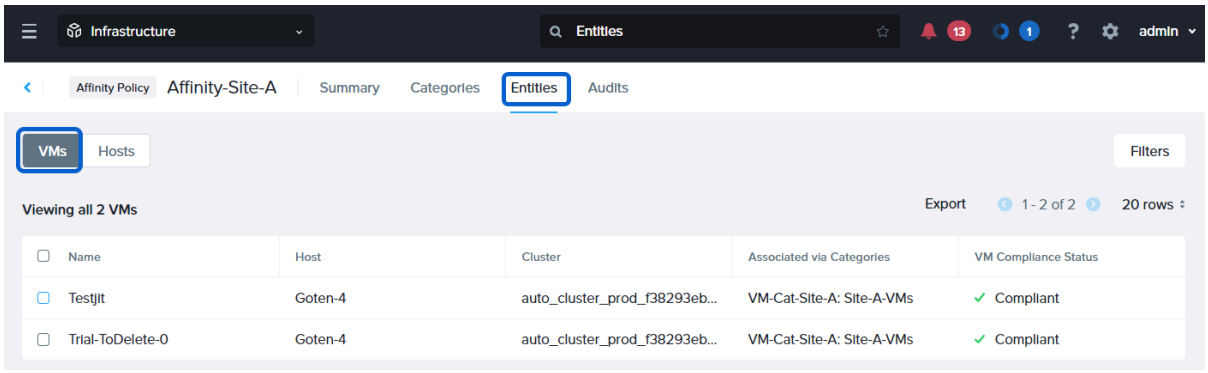


Figure 191: Affinity Policies - Entities (VMs)

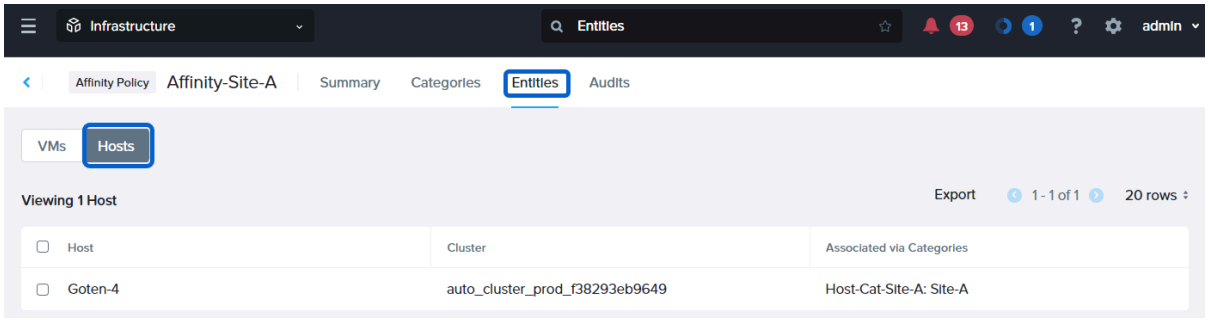


Figure 192: Affinity Policies - Entities (Hosts)

The following table describes the information displayed in the **Entities** tab

Table 133: Entities Tab -Field Description

Field	Description	Values
VMs tab		
Name	Displays the VM name associated with the selected affinity policy.	(VM name)
Host	Displays the host name associated with the selected affinity policy.	(host name)
Cluster	Displays the name of the cluster (on which the host resides) associated with the selected affinity policy.	(cluster name)
Associated via Categories	Displays the VM category name and its value.	(VM category name: Value)
Compliance Status	Displays the VM compliance status with the selected affinity policy.	Compliant|Non-compliant|Pending
Host tab		
Host	Displays the name of the host associated with the selected affinity policy.	(host name

Field	Description	Values
Cluster	Displays the name of the cluster (on which the host resides) associated with the selected affinity policy.	(cluster name)
Associated via Categories	Displays the host Category name and its value.	(host category name: Value)

You can export the table that contains the list of VM entities and host entities related information to a file in a CSV format. For more information about **Export** option, see Export on page 32.

Audits Tab

The **Audits** tab displays the user action-related information for the affinity policies.

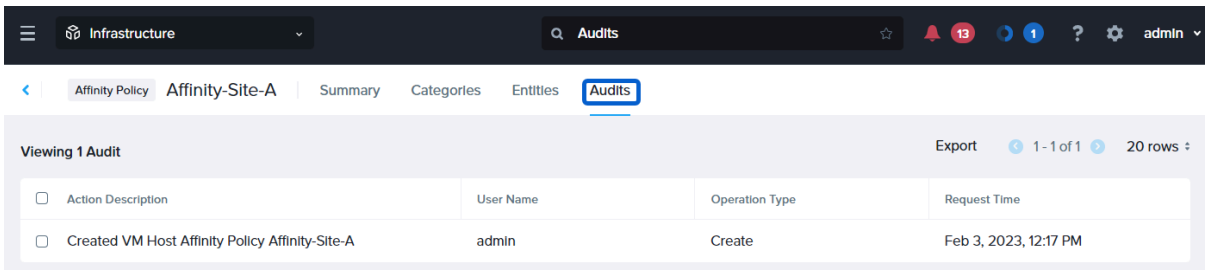


Figure 193: Affinity Policies - Audits

The following table describes the information displayed in the **Audits** tab

Table 134: Audits Tab -Field Description

Field	Description	Values
Action Description	Displays the user-action for affinity policies.	(action description)
User Name	Displays the name of the user who performed the action.	(host name)
Operation Type	Displays the type of operation performed by the user for affinity policies. For example, Create	(cluster name)
Request Time	Displays the date and time of the user action.	(date and time)

You can export the table that contains the list of user actions related information to a file in a CSV format. For more information about **Export** option, see Export on page 32.

Limitations of Affinity Policies

Affinity policies created in Prism Central have the following limitations:

- The minimum supported versions for VM-Host affinity policies are version 6.1 for Prism Element and version 2022.1 for Prism Central.

- Host category attach or detach takes around five minutes to get reflected in the applicable affinity policies.

  When you assign a category to a host and map the host category to the affinity policy, you can observe that the host count gets updated immediately in the Entities tab. However, the system takes approximately 5 minutes to update the host count in Affinity Policies Summary View on page 461.

  The delay in host count update is due to the usage of different APIs to derive the host count in Entities tab and Affinity Policies Summary View on page 461.

  For information about how to create a category, see Creating a Category.

  For information about how to assign a category to host, see Associating Hosts with Categories on page 469

  For information about how to create the affinity policy and map the host category to the affinity policy, see Creating an Affinity Policy on page 469.

Affinity Policy Configuration Workflow

About this task

To set up an affinity policy, perform the following steps:

Procedure

1. Create categories for the following entities:

   a. VMs

   b. Hosts

   For information about how to create a category, see Creating a Category.

2. Apply the VM categories to the VMs and host categories to the hosts.
   For information about how to associate a category to the VMs, see Associating VMs with Categories.
   For information about associating categories with hosts, see Associating hosts with Categories.

3. Create the affinity policy. For details, see Creating an Affinity Policy.

Associating VMs with Categories

About this task

To associate categories to VMs, perform the following steps:

Procedure

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
   The system displays the **List** tab by default.

3. Select the target VMs checkboxes that you want to associate with a category, and choose **Manage Categories** from the **Actions** dropdown menu.
   The system displays the **Manage VM Categories** window.

4. Type the name of the category in **Set Categories** field.
   The system displays the list of matching categories based on the typed entry.

5. Use the Add icon and Remove icon to add and remove the required categories.

> **Note:** If the VM category you selected is already part of any affinity policy, the system displays the associated affinity policy details.

6. Click **Save**.

Associating Hosts with Categories

About this task

To associate categories with hosts, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Hardware** > **Hosts** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
   The system displays the **List** tab by default.
3. Select the target host checkboxes that you want to associate with a category, and choose **Manage Categories** from the **Actions** dropdown menu.
   The system displays the **Manage Host Categories** window.
4. Type the name of the category in **Set Categories** field.
   The system displays the list of matching categories based on the typed entry.
5. Use the Add icon and Remove icon to add and remove the required categories.
6. Click **Save**.

Creating an Affinity Policy

About this task

This section describes how to create an affinity policy in Prism Central.

Before you begin

Ensure that the following prerequisites are met before you create an affinity policy:

- VM and Host categories are created. For information about how to create a category, see Creating a Category on page 457.
- VMs are associated with VM categories, and hosts with host categories. For details, see Associating VMs with Categories on page 468 and Associating Hosts with Categories on page 469.

> **Note:**
>
> - The system also allows you to associate VMs with VM category and hosts with host category after creation of affinity policy.
> - If you have configured any legacy affinity policy (non-category-based affinity policy) associated with the VMs, you must first remove those legacy affinity policies to allow the creation of category-based affinity policies associated with the same VMs.

Procedure

To create an affinity policy, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
   The system displays the **List** tab by default.
3. Select **Affinity Policies** in the **Policies** tab dropdown menu, and click **Create Affinity Policy**.
   The system displays the **Create Affinity Policy** window.
4. Specify the following information in the **Create Affinity Policy** window:
   - **Name**: Enter the affinity policy name.
   - (optional) **Description**: Enter the description for the affinity policy.
   - **VM Categories**:Type the name of the VM category. The system displays the list of matching categories based on the typed entry. Use the Add icon and Remove icon to add and remove the required categories.
   - **Host Categories**:Type the name of the host category. The system displays the list of matching categories based on the typed entry. Use the Add icon and Remove icon to add and remove the required categories.

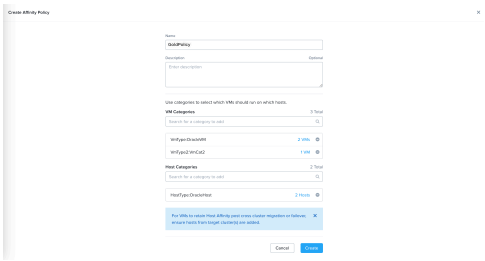


Figure 194: Create Affinity Policy

5. Click **Create**.

Managing Affinity Policies

This section describes how to manage the existing affinity policies in Prism Central.

About this task

You can perform the following actions to manage the existing affinity policies in Prism Central:

- Update an affinity policy.
- Delete an affinity policy.
- Re-enforce an affinity policy.

Procedure

To manage the affinity policies, perform the following steps:

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
   The system displays the **List** tab by default.
3. Select **Affinity Policies** in the **Policies** tab dropdown menu.
   The system displays the affinity policies created across registered clusters.
4. Select the target affinity policy checkbox, and choose **Update** from the **Actions** dropdown menu.
5. Update the fields in the **Update Affinity Policy** window as per your requirement, and click **Save**. For field details, see Creating an Affinity Policy on page 469.

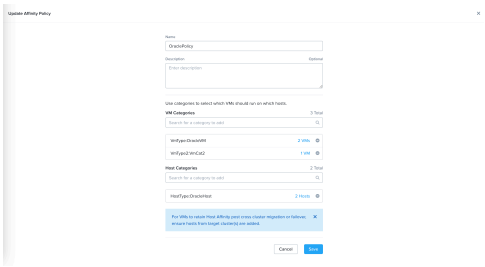


Figure 195: Update Affinity Policy

To delete the affinity policy, select the target affinity policy checkbox and choose **Delete** from the **Actions** dropdown menu. The system prompts you to confirm the delete action. Click **Delete** to confirm the delete affinity policy action.

To re-enforce the affinity policy, select the target affinity policy checkbox and choose **Re-enforce** from the **Actions** dropdown menu. The system prompts you to confirm the action. Click **Re-enforce** to apply the updated affinity policy.

Role Based Access Control for Affinity Policies

This section describes the Role Based Access Control (RBAC) requirements and limitations for affinity policies. For information about RBAC, see Controlling User Access (RBAC) in *Security Guide*.

Role Based Access Control Requirements for Affinity Policies

Before you allocate the Affinity Policy-Related Permissions on page 471, ensure that the following basic permissions are allocated to the admin user or a custom user to access the affinity policies framework in Prism Central:

- View VM
- View category

Affinity Policy-Related Permissions

In addition to the basic permissions to view VM and categories as specified in Role Based Access Control Requirements for Affinity Policies on page 471, you can also assign the following permissions to the admin or custom user to manage the affinity policies in Prism Central:

Table 135: Affinity Policy-Related Permissions

Permission	Description
Create_VM_Host_Affinity_Policy	Admin or custom user can create Affinity Policies.
View_VM_Host_Affinity_Policy	Admin or custom user can view affinity policies.
Update_VM_Host_Affinity_Policy	Admin or custom user can update the existing affinity policies.
Reenforce_VM_Host_Affinity_Policy	Admin or custom user can re-enforce the existing affinity policies.
Delete_VM_Host_Affinity_Policy	Admin or custom user can delete affinity policies.

These permissions also facilitate the admin or custom user to manage the legacy affinity policies (affinity policies that are defined in the Prism Element) from Prism Central.

Role-Based Access Control Limitations for Affinity Policies

The following table describes the limitations that apply to RBAC for affinity policies:

Table 136: RBAC - Limitations for Affinity Policies

Permission Assigned to the Admin or Custom user	Admin or Custom User Action	System Behavior	Limitation
Create_VM_Host_Affinity_Policy Update_VM_Host_Affinity_Policy	Admin or custom user creates or updates the affinity policy.	The system applies the affinity policy to all the VMs associated with the mapped VM categories.	The system does not check whether the admin or the custom user has permission to access the VMs or hosts mapped in the affinity policy.
Update VM Categories	Admin or custom user updates a VM category (for example, attaches a VM to a VM category).	The system applies the affinity policy to which the VM category is assigned.	The system does not check whether the admin or the custom user has permission to create or update the affinity policy.
Update Host Categories	Admin or custom user updates a Host category (for example, attaches a host to a Host category).	The system applies the affinity policy to which the host category is assigned.	The system does not check whether the admin or the custom user has permission to create or update the affinity policy.

NGT Policies

NGT policies are used to define the VM reboot action after you install or upgrade the NGT.

If a restart is required post installation or upgrade, you can define a policy on when the restart should happen. You can use these policies when you have different set of VMs which you would like to be restarted at different times, for example if they are in different time zones or if their down times are expected to be different. Policy workflow are defined on the categories. You have to attach the category to the VM and then you can create a policy for the VM.

Important: The NGT policies are applied only when you select **Skip restart** option during installation or upgradation of NGT. However, if you select a different restart option during installation or upgradation of NGT, the NGT policy is not applied. For more information about how to install and upgrade NGT, see NGT Management in Prism Central on page 169.

NGT Policies Summary View

The NGT policies summary view enables you to access a list of all the user-defined Nutanix Guest tools (NGT) policies (VM reboot policies) across registered clusters.

To access the NGT policies summary view, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The system displays the **List** tab by default.
3. Select **NGT Policies** in the **Policies** tab dropdown menu.

   The system displays a view of NGT policies across all registered clusters.

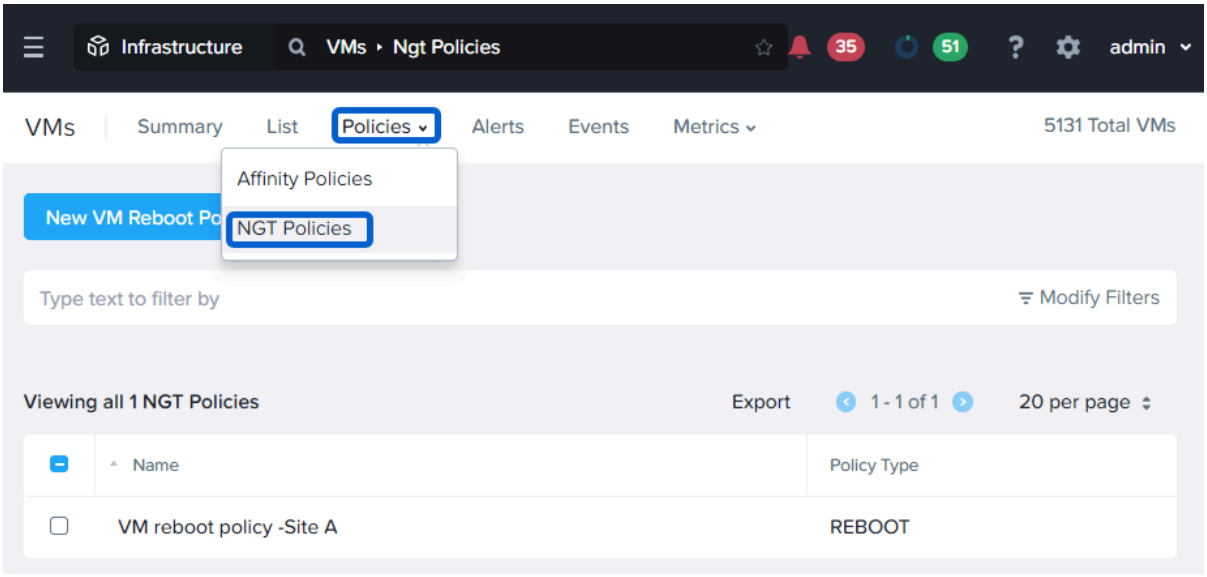


Figure 196: NGT Policies

Table 137: NGT Policies Page - Field Description

Field	Description	Values
Name	Displays the NGT policy name.	(name)
Policy Type	Displays the type of NGT policy.	REBOOT

You can perform the following actions for the NGT policies in the **NGT Policies** summary view:

- Create an NGT policy. For more information, see Creating a NGT Policy on page 474.
- Filter the NGT policies list based on the NGT policy name using **Filters** pane. For more information about **Filters** pane, see Filters Pane on page 28.

- Use the **Actions** dropdown menu to update and delete an NGT policy. For more information, see Managing NGT Policies on page 475.

Creating a NGT Policy

This section describes how to create a NGT Policy (VM reboot policy).

Procedure

To create a NGT policy, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default.
3. Select **NGT Policies** in the **Policies** tab dropdown menu, and click **New VM Reboot Policy**.
   The system displays the **New VM Reboot Policy** window.
4. Specify the following information in the **Create Affinity Policy** window:
   - **Policy Name**: Enter the NGT policy (VM reboot policy) name.
   - (optional) **Policy Description**: Enter the description for the NGT policy.
   - **Guest Restart Schedule**: Select one of the following guest VM restart schedules:
     - **Restart as soon as the install/upgrade is completed**: Select this option if you want to restart the VMs of the selected category right after the install process is completed.
     - **Restart at specific day and time after the upgrade is completed**: Select this option and choose the date and time on which you want to the restart to happen.

       Note: The VMs restart depends on the Prism Element timezone settings.
     - **Add Category**: Click **Add Category** and select the category that you want to apply to the NGT policy. Type the name of the VM category. The system displays the list of matching categories

based on the typed entry. Use the Add icon and Remove icon to add and remove the required categories.

For information about how to create a VM category, see Creating a Category on page 457.

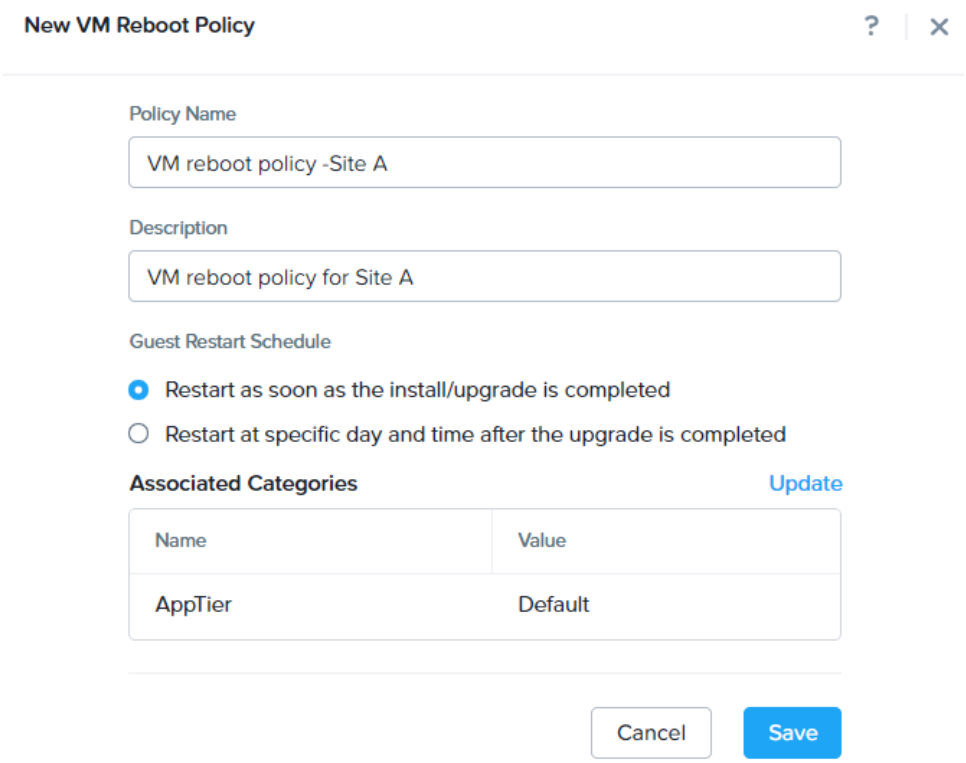


Figure 197: Create VM Reboot Policy

5. Click **Save**.

> **Note:** Any VM reboot policy you create using this procedure is overridden if you choose to restart the VM during installation or upgradation of NGT by using a different option compared to the option configured in the policy for VM restart. If you choose not to restart the VM during installation or upgradation of NGT, the system continues to apply the existing reboot policy for the VM.. For example, if you select the **Restart as soon as the install/upgrade is completed** option as part of the NGT policy, and if you select the **Restart at specific date and time after the install is completed** option during installation or upgradation of NGT, the **Restart at specific date and time after the install is completed** setting take precedence and the VM is restarted at the scheduled date and time. However, if you select the **Skip restart** option during installation or upgradation of NGT, the VM reboot policy takes precedence and the VM restart occurs immediately after an installation or upgrade.

The policy is created and saved in the NGT Policies pane.

Managing NGT Policies

This section describes how to manage the existing NGT policies (VM reboot policies) in Prism Central.

About this task

You can perform the following actions to manage the existing NGT policies in Prism Central:

- Update an NGT policy.
- Delete an NGT policy.

Procedure

To modify a NGT policy, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default.
3. Select the target NGT policy checkbox, and choose **Update** from the **Actions** dropdown menu.
   The system displays the NGT policies created across registered clusters.
4. Update the fields in the **Update VM Reboot Policy** window as per your requirement, and click **Save**. For field details, see Creating an Affinity Policy on page 469.

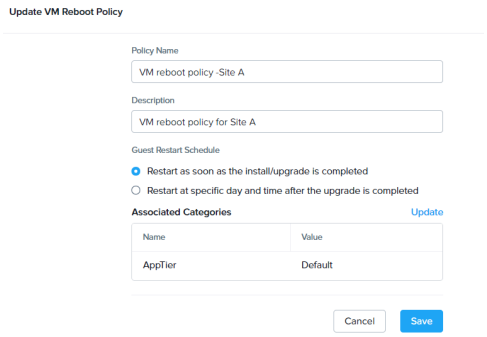


Figure 198: Update VM Reboot Policy

To delete an NGT policy, select the target NGT policy checkbox and choose **Delete** from the **Actions** dropdown menu. The system prompts you to confirm the delete action. Click **Delete** to confirm the delete NGT policy action.

Image Policy Management

In Prism Central, you can create and manage the following types of policies for the images:

- Image Placement Policies (see Image Placement Policies on page 476)
- Bandwidth Throttling Policies (see Bandwidth Throttling Policies on page 484)

Image Placement Policies

Prism Central enables you to upload VM images from your workstation or from a remote server. It also enables you to manually specify a subset of registered clusters as targets for those images. However, image placement decisions are often driven by compliance requirements, policies, and regulations. For example, you might have to confine a VM image to a Nutanix cluster in a specific location. Or, a cluster in one region might require a Windows VM image with a specific set of applications while a cluster in another region might require a Linux VM with its own set of applications.

Prism Central enables you to configure policies that govern which clusters receive the images that you upload. These policies, called image placement policies, map images to target clusters using categories associated with both those entities. For example, an image placement policy states that the Linux images associated with the `OS:Linux` and `distribution:Centos` categories must be uploaded to the clusters associated with the `Location:SFO` category.

Image placement policies also specify how strictly the policy must be enforced. Soft enforcement allows clusters not identified by the policy to use the images, when required, by checking them out. Hard enforcement disallows such usage. By using both soft and hard enforcement on the same category of clusters, you can address more specific use cases. For more information, see Sample Scenarios and Configurations on page 483.

Image placement policies maintain a state of compliance across the clusters registered with Prism Central. They detect and correct violations introduced by changes in category assignments and updates to their configuration (including a switch from soft enforcement to hard enforcement). For more information, see Sample Scenarios and Configurations on page 483.

Image Placement Policies Summary View

The image placement policies summary view allows you to access a list of all the user-defined image placement policies across registered clusters.

To access the summary view of all image placement policies:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The system displays the **List** tab by default.
3. Select **Placement Policies** in the **Policies** tab dropdown menu.

   The system displays a summary view of image placement policies across all registered clusters.

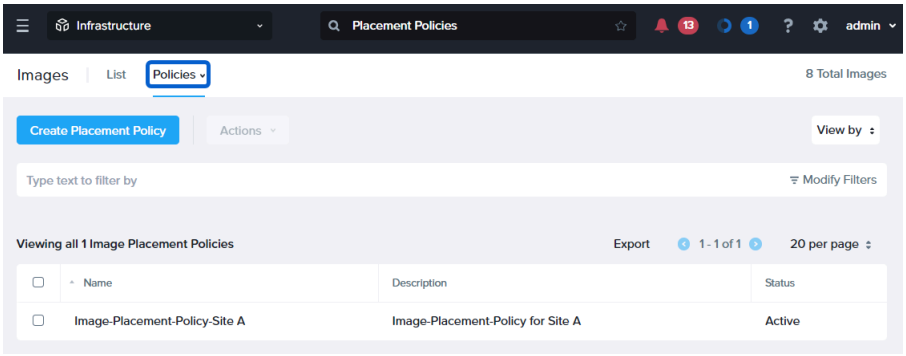


Figure 199: Summary View - All Image Placement Policies

Table 138: Image Placement Policies Page - Field Description

Field	Description	Values
Name	Displays the image placement policy name.	(name)
Description	Displays the purpose of the image placement policy.	(text string)
Status	Displays the status of the image placement policy.	Active|Suspended

You can perform the following actions in the **Image Placement Policies** summary view:

- Access the detailed information about an individual image placement policy. For more information, see Image Placement Policy Details View on page 478.
- Create an image placement policy. For more information, see Creating an Image Placement Policy on page 480.

- Use the **Actions** dropdown menu to update, delete, suspend enforcement (if status is active) or resume enforcement (if status is suspended). For more information, see Managing Image Placement Policies on page 481.
- Filter the image placement policies list using **Filters** pane. For more information about **Filters** pane, see Filters Pane on page 28.

  For more information about fields, see Table 138: Image Placement Policies Page - Field Description on page 477.
- Export the table that contains the list of image placement policies and their information to a file in a CSV format. For more information about **Export** option, see Export on page 32.
- View image placement policies based on pre-defined criteria or create a custom view. For information about available views and how to create a custom view, see View by on page 29.

Image Placement Policy Details View

To access the details view of an individual image placement policy, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The system displays the **List** tab by default.
3. Select **Placement Policies** in the **Policies** tab.

   The system displays a summary view of image placement policies across all registered clusters.
4. Click the target <*Image_Placement_Policy_Name*> to access the details view individual image placement policy.

> **Note:** Replace <*Image_Placement_Policy_Name*> with the actual image placement policy name at your site.

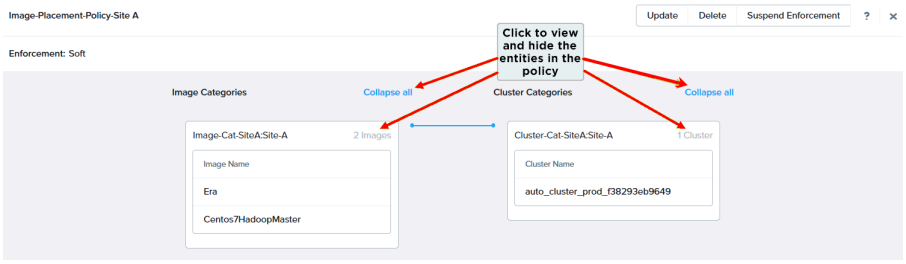


Figure 200: Image Placement Policy Details view

The details view of an individual image placement policy provides the following information:

- Policy name that appears in the upper left. You can switch from one policy to another by selecting the policy name from the dropdown menu.
- Policy enforcement status appears below the name and indicates whether the enforcement is hard or soft.
- Two columns that specify the target images (on the left) and target clusters (on the right). Click **Expand all** (or **Collapse all**) to display (or hide) the list of images or clusters.

<*Action*> available in the top right corner. Click the appropriate <*Action*> to run that administrative action on the image placement policy. For more information about how to perform any <*Action*>, see Managing Image Placement Policies on page 481.

Configuration Workflow

About this task

To set up an image placement policy, perform the following steps:

Procedure

1. Create categories for the following entities:
   a. Clusters (for example, create categories based on cluster location or region)
   b. Images (for example, create categories based on operating system and size)
   For information about how to create a category, see Creating a Category.
2. Apply the cluster categories to clusters and image categories to images.
   For information about how to associate categories with a Nutanix cluster, see Associating Clusters with Categories on page 479.
   For information about how to associate categories with an image, see Associating an Image with Categories.
3. Configure the image placement policy. For more information, see Configuring an Image Placement Policy.

Associating Clusters with Categories

About this task

To associate categories with a registered Nutanix cluster, perform the following steps:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Hardware** > **Clusters** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default.
3. Select the target cluster checkboxes that you want to associate with a category, and choose **Manage Categories** from the **Actions** dropdown menu.
   The system displays the **Manage Cluster Categories** window.
4. Type the name of the category in **Set Categories** field.
   The system displays the list of matching categories based on the typed entry.
5. Use the Add icon and Remove icon to add and remove the required categories.
6. Click **Save**.

Associating Images with Categories

About this task

To associate categories with an image, perform the following steps:

Procedure

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default.
3. Select the target image checkbox(es) that you want to associate with a category, and choose **Manage Categories** from the **Actions** dropdown menu.
   The system displays the **Manage Image Categories** window.
4. Type the name of the category in **Set Categories** field.
   The system displays the list of matching categories based on the typed entry.
5. Use the Add icon and Remove icon to add and remove the required categories.
6. Click **Save**.

Creating an Image Placement Policy

About this task

This section describes how to create an image placement policy in Prism Central.

Before you begin

Ensure that the following prerequisites are met before you create an image placement policy:

- Cluster and Image categories are created. For information about how to create a category, see Creating a Category on page 457.
- Images are associated with the Image categories, and clusters with the cluster categories. For more information, see Associating Images with Categories on page 479 and Associating Clusters with Categories on page 479.

  Note: The system also allows you to associate images with image category and clusters with cluster category after creation of image placement policy.

- Review existing image placement policies to avoid causing conflicts. For information about issues caused by conflicting policies, see How Prism Central Handles Conflicting Policies on page 482

Procedure

To create an affinity policy, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default.
3. Select **Placement Policies** in the **Policies** tab dropdown menu, and click **Create Placement Policy**.
   The system displays the **Create Image Placement Policy** window.

4. Specify the following information in the **Create Image Placement Policy** window:

   - **Policy Name**: Enter the image placement policy name.
   - (optional) **Description**: Enter the description for the image placement policy.
   - **Assign Images With All Of The Following Categories**: Type the name of the image category. The system displays the list of matching categories based on the typed entry. Use the Add icon and Remove icon to add and remove the required categories.
   - **To Clusters With All Of The Following Categories**: Type the name of the cluster category. The system displays the list of matching categories based on the typed entry. Use the Add icon and Remove icon to add and remove the required categories.
   - **Policy Enforcement**: Select one of the following mechanisms for policy enforcement:
     - **Soft** - The images are uploaded to the set of clusters identified by the image placement policy, and no restriction is placed on using those images on clusters outside the identified set. For example, if clusters A, B, and C are registered with Prism Central, and an image placement policy with a soft enforcement policy uploads an image to clusters A and B, you can use the image to create a VM on cluster C. The checkout to cluster C is not blocked.
     - **Hard** - The images are uploaded to the set of clusters identified by the image placement policy, however you cannot use the image to create a VM on any cluster outside the identified set. For example, if clusters A, B, and C are registered with Prism Central, and an image placement policy with a hard enforcement policy uploads an image to clusters A and B, the image is available only on clusters A and B. Cluster C cannot check out the image.

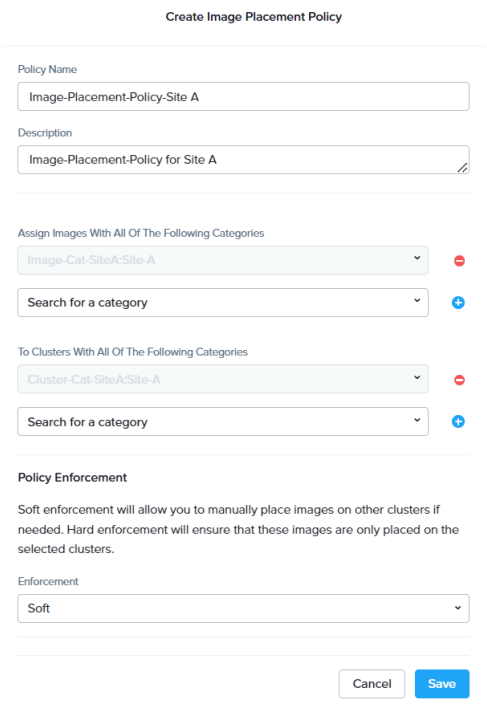


Figure 201: Create Image Placement Policy

5. Click **Save**.

Managing Image Placement Policies

This section describes how to manage the image placement policies in Prism Central.

About this task

You can perform the following actions to manage the image placement policies in Prism Central:

- Update an image placement policy.
- Delete an image placement policy.
- Suspend Enforcement
- Resume Enforcement

Updates to an image placement policy can result in a policy violation. Prism Central attempts to correct the violation by running a series of actions. For example, if you change the cluster category such that the policy now identifies a different set of clusters as targets, Prism Central first copies the images to the clusters in the new category, and then removes the images from the clusters in the previously mentioned category. If you change the policy enforcement setting from Soft to Hard, and if any clusters that are not identified as targets had previously checked out the images, Prism Central corrects the violation by deleting the images from those clusters. An update to a policy might also result in a conflict with one or more of the other policies that apply to the same category of images.

For more information about how Prism Central handles conflicting policies, see How Prism Central Handles Conflicting Policies on page 482.

Procedure

To update an image placement policy, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default.
3. Select **Placement Policies** in the **Policies** tab dropdown menu.
   The system displays the placement policies across all the registered clusters.
4. Select the target image placement policy checkbox, and choose **Update** from the **Actions** dropdown menu.
5. Update the fields in the **Update Image Placement Policy** window as per your requirement, and click **Save**. For field details, see Creating an Image Placement Policy on page 480.

   To delete the image placement policy, select the target image placement policy checkbox and choose **Delete** from the **Actions** dropdown menu. The system prompts you to confirm the delete action. Click **Delete** to confirm the delete action.

   To suspend enforcement of the image placement policy (if Active), select the target image placement policy checkbox and choose **Suspend Enforcement** from the **Actions** dropdown menu. The system prompts you to confirm the **Suspend Enforcement** action. Click **Confirm** to suspend the policy enforcement.

   To resume enforcement of the image placement policy (if Suspended), select the target image placement policy checkbox and choose **Resume Enforcement** from the **Actions** dropdown menu. The system prompts you to confirm the **Resume Enforcement** action. Click **Confirm** to resume the policy enforcement.

How Prism Central Handles Conflicting Policies

Policies are said to be in conflict if they identify the same category of images but their resulting cluster placements are different.

For example, the following policies are conflicting policies if they apply to the same category of images:

- Policy P1, which identifies clusters C1 and C2 as target clusters, and the policy enforcement setting is Soft.
- Policy P2, which identifies clusters C3 and C4 as target clusters, and the policy enforcement setting is Hard.

Prism Central handles such conflicts in the following manner:

- Prism Central ignores conflicting policies and does not perform any action on the images. If policy P1 was configured first, Prism Central stops enforcing P1 as soon as P2 is configured, and it does not enforce P2 either. When there is a policy conflict, the conflict is noted in the **Policies** tab of the details view for that image.
- Prism Central continues to enforce other policies that are not in conflict. For example, if policies P3 and P4 apply to the same categories of images as P1 and P2, Prism Central continues to enforce P3 and P4 as long as they are not in conflict with P1 and P2.

Sample Scenarios and Configurations

The following table describes how to configure image management policies to achieve a desired result. The examples use a Prism Central instance to which three clusters A, B, and C and registered (possibly among other clusters).

Table 139: Sample Scenarios and Configurations

Desired Result	Image Placement Policy Configuration
The images must be available on any one of the clusters (A, B, or C) and can be checked out to the other two clusters and to any other clusters that might be registered with Prism Central now or in the future.	Create an image placement policy that identifies any one of the clusters (A, B, or C) as the target cluster (by the use of categories) and set the policy enforcement to Soft.
The images must be available on all of the clusters A, B, and C and can be checked out to any other clusters that are registered with Prism Central now or in the future.	Create an image placement policy that identifies clusters A, B, and C as the target clusters (by the use of categories) and set the policy enforcement to Soft.
The images must be available on all of the clusters A, B, and C and cannot be checked out to any other clusters that are registered with Prism Central now or in the future.	Do the following: • Create an image placement policy that identifies clusters A, B, and C as the target clusters (by the use of categories) and set the policy enforcement to Soft. (This policy ensures that the images are available on all of the three clusters) • Create a second image placement policy that identifies clusters A, B, and C as the target clusters (by the use of categories) and set the policy enforcement to Hard. (This policy makes sure that the images are available only on these three clusters)

Desired Result	Image Placement Policy Configuration
The images must be available only on cluster A and cannot be checked out to clusters B and C now, and the images also cannot be checked out to any other clusters that are registered with Prism Central in the future.	Create an image placement policy that identifies cluster A as the target cluster (by the use of categories) and set the policy enforcement to Hard.
The images are available on cluster A and must now be available on clusters B and C. Cluster A can use the images if required. The policy enforcement is currently Soft.	Do the following: • Dissociate the categories specified in the image placement policy from cluster A and associate them with clusters B and C. • Do not update the image placement policy (no changes are required). Prism Central takes the following corrective actions: 1. Prism Central copies the images to clusters B and C. If clusters B and C had checked out the images before the reassignment of categories to the clusters, the images are not copied. 2. Additionally, because the Soft policy enforcement setting is retained, Prism Central does not remove the image from cluster A.
The images are available on cluster A and must now be available only on clusters B and C. Cluster A must not be permitted to use the images. The policy enforcement is currently Soft.	Do the following: • Dissociate the categories specified in the image placement policies from cluster A and associate them with clusters B and C. • Change the policy enforcement setting in the image placement policy to Hard. Prism Central takes the following corrective actions: 1. Prism Central copies the images to clusters B and C. If clusters B and C had checked out the images before the reassignment of categories to the clusters, the images are not copied. 2. To honor the Hard policy enforcement setting, Prism Central removes the image from cluster A.

Bandwidth Throttling Policies

Prism Central uses the bandwidth throttling policy feature to manage the usage of bandwidth when you create a new image or transfer an image from one cluster to another cluster using Prism Central. The bandwidth throttling policy allows you to limit the bandwidth consumed during image creation using the URL option in specific clusters. For information about how to add a image using the URL option, see Adding Images from a Remote Server on page 249..

Without bandwidth throttling policy, an image creation from the remote server consumes as much bandwidth as available. High bandwidth consumption for creating a new image limits the bandwidth availability for the other cluster operations.

Bandwidth Throttling Policies Summary View

The bandwidth throttling policies summary view allows you to access a list of all the user-defined bandwidth-throttling policies across registered clusters.

Summary View of all Bandwidth Throttling Policies

To access the bandwidth throttling summary view, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The system displays the **List** tab by default.
3. Select **Bandwidth Throttling Policies** in the **Policies** tab dropdown menu.

   The system displays a view of bandwidth throttling policies across all registered clusters.

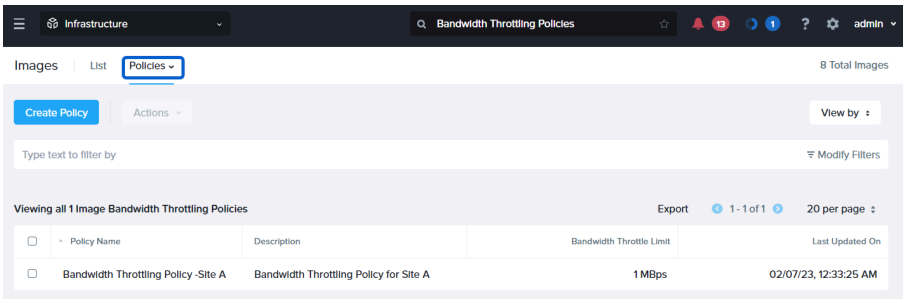


Figure 202: Bandwidth Throttling Policies

Table 140: Bandwidth Throttling Policies Page - Field Description

Field	Description	Values
Policy Name	Displays the policy name.	(name)
Description	Describes the purpose of the policy.	(description)
Bandwidth Throttle Limit	Describes the bandwidth throttle limit configured for the policy in MBps	xx MBps
Last Updated On	Describes the date and time when the bandwidth throttling policy was created or updated.	(date and time)

You can perform the following actions for the bandwidth throttling policies in the **Bandwidth Throttling Policies** summary view:

- Access the detailed information about an individual bandwidth throttling policy. For more information, see Bandwidth Throttling Policy Details View on page 486.
- Create a bandwidth throttling policy. For more information, see Creating a Bandwidth Throttling Policy on page 487.
- Filter the bandwidth throttling policies list using **Filters** pane. For more information about **Filters** pane, see Filters Pane on page 28

  For more information about fields, see Table 140: Bandwidth Throttling Policies Page - Field Description on page 485.
- Export the table that contains the list of bandwidth throttling policies and their information to a file in a CSV format. For more information about **Export** option, see Export on page 32.

- View bandwidth throttling policies based on pre-defined criteria or create a custom view. For information about available views and how to create a custom view, see View by on page 29.
- Use the **Actions** dropdown menu to update and delete a bandwidth throttling policy. For more information, see Managing Bandwidth Throttling Policies on page 489.

Bandwidth Throttling Policy Details View

To access the details view of an individual bandwidth throttling policy, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The system displays the **List** tab by default.
3. Select **Bandwidth Throttling Policies** in the **Policies** tab.

   The system displays a summary view of bandwidth throttling policies across all registered clusters.
4. Click the target *<Bandwidth_Throttling_Policy_Name>* to access the details view individual bandwidth throttling policy.

> **Note:** Replace *<Bandwidth_Throttling_Policy_Name>* with the actual bandwidth throttling policy name at your site.

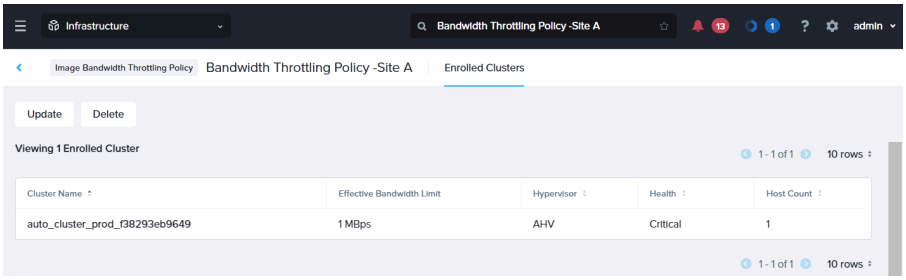


Figure 203: Bandwidth Throttling Policy Details view

The details view of an individual bandwidth throttling policy provides the following information:

- Policy name that appears in the upper left.
- **Enrolled Cluster** tab that displays the following cluster information:
  - **Cluster Name** - Displays the name of the cluster that is configured with bandwidth throttling policy.
  - **Effective Bandwidth Limit** - The selected cluster uses the **Effective Bandwidth Limit** configured to add a new image next time. In a scenario where multiple bandwidth throttling policies are applied to the same cluster, the minimum of all the applicable bandwidth throttling policies is enforced on the cluster.

    For example, you have a cluster named **PE-123**, and you have created multiple bandwidth throttling policies with different **Bandwidth Limit**, then during the cluster association with the bandwidth throttling policy (step 6), the cluster is associated with the bandwidth throttling policy which has the least **Bandwidth Limit** configured on it.
  - **Hypervisor** - Displays the Hypervisor name.
  - **Health** - Displays the cluster health.
  - **Host Count** - Displays the number of hosts in the cluster

<*Action*> available above the detailed view column. Click the appropriate <*Action*> to run that administrative action on the bandwidth throttling policy. For more information about how to perform any <*Action*>, see Managing Bandwidth Throttling Policies on page 489 .

Requirements for Bandwidth Throttling Policy

Ensure that the following prerequisites are met to configure the bandwidth throttling policy feature in Prism Central:

- Prism Central release 2021.9 or later and AOS version 6.0 or later are deployed at your site.
- The clusters are registered with Prism Central.
- A cluster category is created and associated with the cluster.

  For information about how to create a cluster category, see Creating a Category on page 457.

  For information about how to associate a category to a cluster, see Assigning a Category on page 459.
- AHV Hypervisor is deployed at your site.

  Note: The bandwidth throttling policy is not supported with ESXi and Hyper-V hypervisors.

Limitations with Bandwidth Throttling Policy

The following limitations apply to the bandwidth throttling policies:

- Prism Central enforces bandwidth throttling policy only for new images created by using the URL option on clusters registered with Prism Central. For information about how to add a image using the URL option, see Adding Images from a Remote Server on page 249..
- You cannot enforce a bandwidth throttling policy if you create an image directly from a Prism Element.
- The least applicable bandwidth throttling policy on the source and destination cluster is enforced when you transfer an image from one cluster to another cluster.

Creating a Bandwidth Throttling Policy

About this task

This section describes how to create a bandwidth throttling policy in Prism Central.

Perform the following procedure to create a new bandwidth throttling policy.

Before you begin

Ensure that the following prerequisites are met before you create a bandwidth throttling policy in Prism Central:

- Requirements that are described in Requirements for Bandwidth Throttling Policy on page 487 are followed.
- Limitations that are described in Limitations with Bandwidth Throttling Policy on page 487 are observed.

Procedure

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default.
3. Select **Bandwidth Throttling Policies** in the **Policies** tab dropdown menu, and click **Create Policy**.
   The system displays the **Create Image Bandwidth Throttling Policy** window.

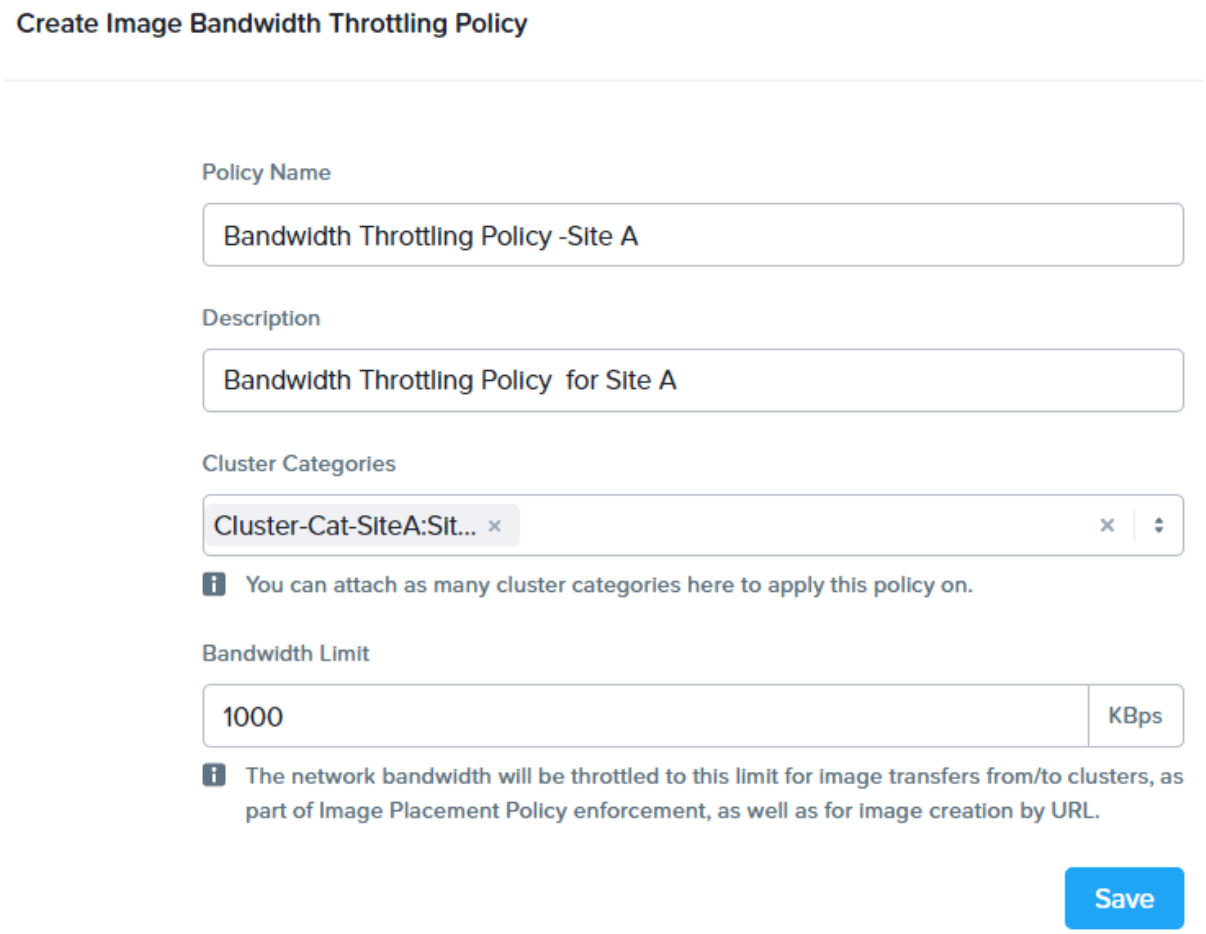


Figure 204: Create Bandwidth Throttling Policy

4. Specify the following information in the **Create Image Bandwidth Throttling Policy** window:

   - **Policy Name**: Enter the image placement policy name.
   - (optional) **Description**: Enter the description for the image placement policy.
   - **Cluster Categories**: Type the name of the cluster category. The system displays the list of matching categories based on the typed entry. Use the Add icon and Remove icon to add and remove the required categories.

     For more information about categories, see Category Management on page 454 .
   - **Bandwidth Limit**: Enter the bandwidth throttling value in KBps. The system considers this value when you add the image using the URL option and while enforcing image placement policy to transfer image transfer from one cluster to another.

     > **Note:** The bandwidth limit task is serialized on each cluster to strictly enforce the bandwidth limit on each cluster. For example, when you create a new image, only one image create task runs on the cluster at a time. The second image creation task configured with another bandwidth limit can start only after completion of the first image creation task.

5. Click **Save**.

Managing Bandwidth Throttling Policies

This section describes how to manage the bandwidth throttling policies in Prism Central.

About this task

You can perform the following actions to manage the bandwidth throttling policies in Prism Central:

- Update an bandwidth throttling policy
- Delete an bandwidth throttling policy.

Procedure

To manage the bandwidth throttling policies, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Images** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default.
3. Select **Bandwidth Throttling Policies** in the **Policies** tab dropdown menu.
   The system displays the bandwidth throttling policies across all the registered clusters.
4. Select the target bandwidth throttling policy checkbox, and choose **Update** from the **Actions** dropdown menu.
5. Update the information as per your requirement in the **Update Image Bandwidth Throttling Policy** window, and click **Save**. For more information about fields, see Creating a Bandwidth Throttling Policy on page 487.

   To delete the bandwidth throttling policy, select the target bandwidth throttling policy checkbox and choose **Delete** from the **Actions** dropdown menu. The system prompts you to confirm the delete action. Click **Delete** to confirm the delete action.

Security Policy Management

Security policies inspect traffic that originates and terminates within a data center and help eliminate the need for additional firewalls within the data center.

Security policies are defined using Nutanix Flow which provides a policy-driven security framework. You can enable Nutanix Flow using the Flow-specific settings from the **Prism Central Settings** page. For more information, see Prism Central Settings (Infrastructure) on page 22.

For information about how to create and apply security policies, see Flow Microsegmentation Guide.

For information about how to view the security policies across all clusters in prism Central, see Security Policies Summary View on page 490.

For information about how to view the detailed information about an individual security policy, see Security Policy Details View on page 494.

Security Policies Summary View

The Security policies summary view allows you to access a list of all the user-defined security policies across registered clusters.

To access the security summary view, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Network & Security** > **Security Policies** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The system displays the **Policies** tab by default with consolidated view of security policies across all registered clusters.
3. Select **Security Policies** in the **Policies** tab dropdown menu.

   The system displays a view of security policies across all registered clusters.

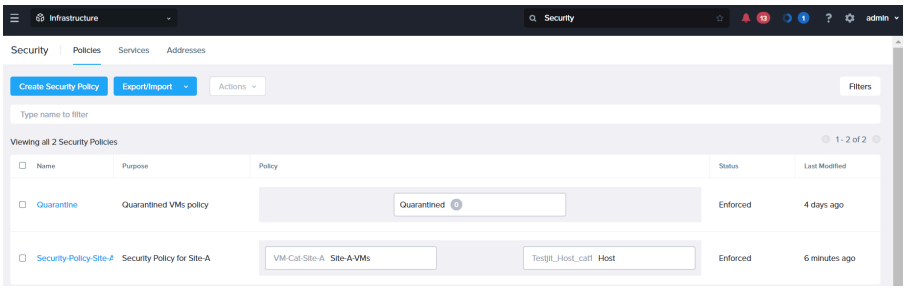


Figure 205: Security Policies

Table 141: Security Policies Page - Field Description

Field	Description	Values
Name	Displays the security policy name. The policy is one of three types: application, quarantine, or isolation.	(name), Application, Quarantine, Isolation
Purpose	Describes the purpose of the security policy.	(text string)
Policy	Displays a high-level view of the policy configuration.	(boxed text)

Field	Description	Values
Status	Displays the current status of the security policy as either Enforced or in Monitoring mode.	Enforced, Monitoring
Last Modified	Displays the time-line for the security policy. Last modified time-line or the creation time-line if the policy has never been modified.	Time-line. For example, 4 days ago, 6 minutes ago

You can perform the following actions for the security policies in the **Security Policies** summary view:

- Access the detailed information about an individual security policy. For more information, see Security Policy Details View on page 494.
- Create, import, or export a security policy. For more information, see Flow Microsegmentation Guide.
- Filter the security policies list using **Filters** pane. For more information about **Filters** pane, see Filters Pane - Security Policies Page on page 493
- Use the **Actions** dropdown menu to update, delete, enforce (if initial selection is monitoring), or monitor (if initial selection is enforce) a security policy. For more information, see Flow Microsegmentation Guide.

Services Tab

Service is a group of protocol-port combination. You can use any of the default services or create a custom service.

The **Services** tab displays the list of all system and user-defined (custom) services.

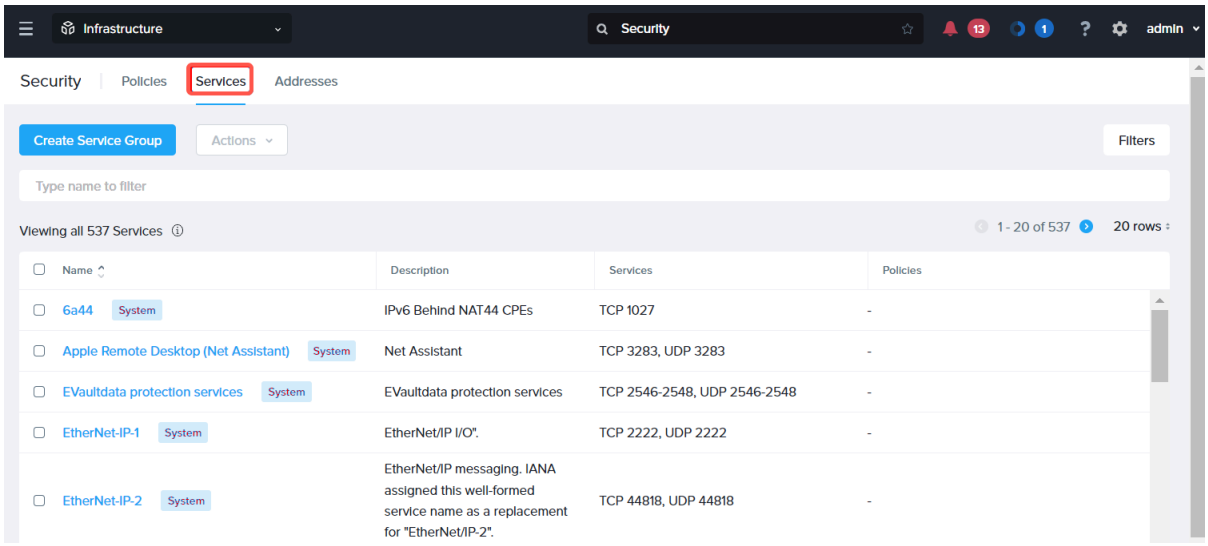


Figure 206: Security Services Tab

The following table describes the fields that appear in the **Services** tab of **Security**page:

Table 142: Security Services Tab - Field Description

Field	Description	Values
Name	Displays the service name.	(service name)
Description	Displays the description of the service.	(description, string)
Services	Displays the protocol and port combination of the service	(Protocol-Port combination) For example, TCP 1027
Policies	Displays the security policies in which the services are attached.	(policy name)

You can perform the following actions for the services in the **Services** tab:

- Filter the services list based on the available field values using **Filters** pane. For more information about **Filters** pane, see Filters Pane - Security Policies Page on page 493.
- Create a service group. For more information about how to create a service group, see Flow Microsegmentation Guide.
- Use the **Actions** dropdown menu to update, delete, or clone a service. For more information, see Flow Microsegmentation Guide.

> **Note:** The **Actions** dropdown menu is grayed out unless you select a service or if you select multiple services.

Addresses Tab

Address Group is a way to group one or many IP address or range. It can be used when you define security policies.

The **Addresses** tab displays the list of all user-defined addresses.

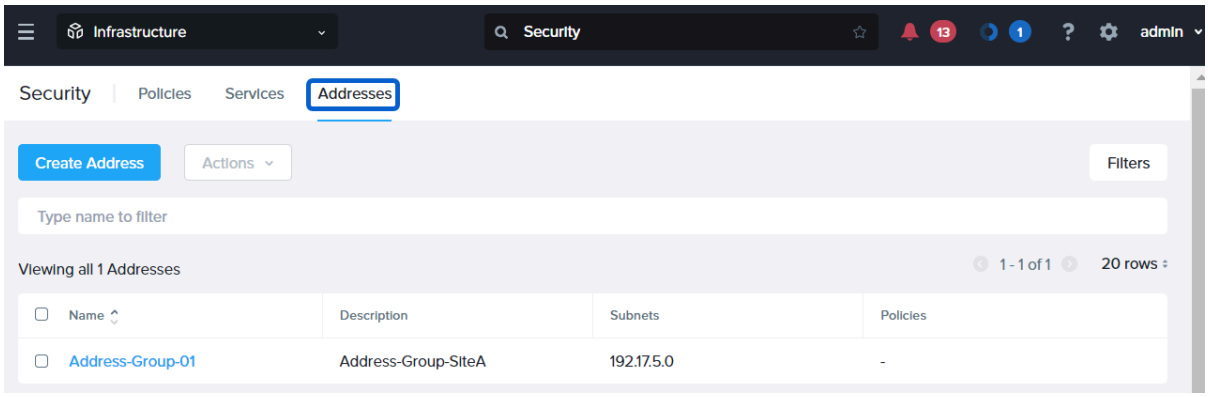


Figure 207: Security Addresses Tab

The following table describes the fields that appear in the **Addresses** tab of **Security**page:

Table 143: Security Addresses Tab - Field Description

Field	Description	Values
Name	Displays the address group name.	(address group name)
Description	Displays the description of the address group.	(description, string)
Subnets	Displays the subnet information	(subnet IP)
Policies	Displays the security policies in which the addresses are used.	(policy name)

You can perform the following actions for the addresses in the **Addresses** tab:

- Filter the services list based on the available field values using **Filters** pane. For more information about **Filters** pane, see Filters Pane - Security Policies Page on page 493.
- Create Address. For more information about how to create a address, see Flow Microsegmentation Guide.
- Use the **Actions** dropdown menu to update or delete an address. For more information, see Flow Microsegmentation Guide.

  Note: The **Actions** dropdown menu is grayed out unless you select a address or if you select multiple addresses.

Filters Pane - Security Policies Page

The following table describes the fields available in the **Filters** pane:

Table 144: Filter Pane Fields - Security Policies

Field	Description	Values
Filter pane fields in **Policies** tab.		
Name	Filters based on the security policy name. Select a condition from the dropdown menu and enter a string in the field. The system returns a list of security policies that satisfy the security policy name condition/string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	(security policy name string)
Type	Filters on the security policy type. Select the checkbox for one or more of the policy types (application, quarantine, isolation, and VDI).	Application, Quarantine, Isolation, VDI
Status	Filters on the security policy status. Select the checkbox for Enforced, or Monitoring, or both.	Enforced, Monitoring
Filter pane fields in **Services** tab.		

Field	Description	Values
Name	Filters based on the service name. Select a condition from the dropdown menu and enter a string in the field. The system returns a list of services that satisfy the service name condition/ string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	(service name)
Description	Filters based on the description of the service.	(description, string)
Protocol	Filters based on the service protocol; TCP, UDP, and ICMP.	TCP|UDP|ICMP
Filter pane fields in **Addresses** tab.		
Name	Filters based on the address name. Select a condition from the dropdown menu and enter a string in the field. The system returns a list of addresses that satisfy the address name condition/ string. **Note:** In this field, the condition menu options are **Contains**, **Doesn't contain**, **Starts with**, **Ends with**, and **Equal to**.	(address name)
Description	Filters based on the description of the address.	(description, string)

Security Policy Details View

To access the details view of an individual security policy, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Network & Security** > **Security Policies** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The system displays the **Policies** tab by default with consolidated view of security policies across all registered clusters. .
3. Select **Security Policies** in the **Policies** tab dropdown menu.

   The system displays a view of security policies across all registered clusters.

4. Click the target <*Security_Policy_Name*> to access the details view individual security policy.

Note: Replace <*Security_Policy_Name*> with the actual security policy name at your site.

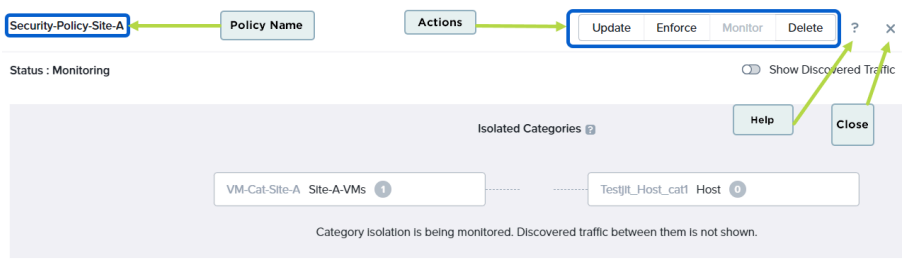


Figure 208: Security Policy Details view

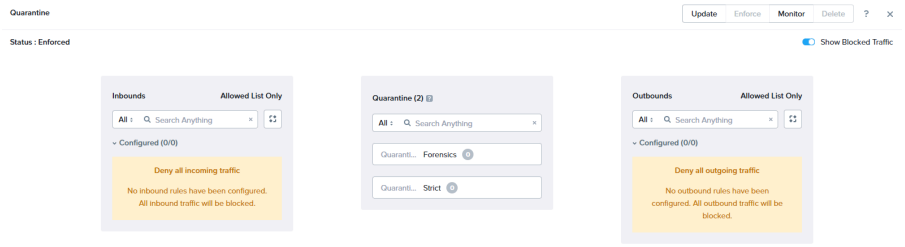


Figure 209: Security Policy Details View: Enforced Policy Example

You can perform the following actions in the **Security Policies** details view:

- Use toggle **Show Blocked Traffic** to view or hide the blocked traffic data. This toggle is available when policy status is **Enforced**.
- Use toggle **Show Discovered Traffic** to view or hide the discovered traffic data. This toggle is available when policy status is **Monitoring**.
- Update, delete, enforce (if initial selection is monitoring), or monitor (if initial selection is enforce) a security policy. For more information, see Flow Microsegmentation Guide.
- Click the Help icon to open a help page in a separate tab or window.

The available actions appear in bold; other actions are grayed out. For grayed out options, the system displays a tool tip with the reason.

Storage Policy Management

Storage Policies in Prism Central let you manage the storage attributes like Replication factor, encryption, compression, and QoS of entities like Virtual Machines (VMs) and Volume Groups (VGs). A single storage policy can manage the attributes of several entities that are associated with various Categories. You can configure entity-centric storage policies to manage the storage attributes of the entities as required.

When you install or upgrade the Prism Central instance to Prism Central pc.2024.1 or later versions, Prism Central configures a predefined or default storage policy.

For more information on the default storage policy, see Default Storage Policy on page 498.

A storage policy uses categories to associate with entities such as VMs and VGs. Using a storage policy, you can manage parameters of the entities such as Replication Factor, encryption, type of data compression (such as Inline, No compression, or Post Process compression), and IOPS or Throughput throttling to be applied to the entities. When you apply storage policies to the entities using categories,

the attributes are configured for the entities, and the entity data is transformed to comply with the storage policy. This mechanism is described in Storage Policy Compliance on page 507.

Important Considerations

- Prism Central supports storage policies only on AHV.
- Prism Central supports Data-at-rest encryption at the entity level with storage policies. In other words, when Prism Central applies a storage policy on an entity such as a VM or VG, it applies the policy even if data-at-rest encryption is not enabled on the cluster. Storage policies support entity-centric data-at-rest encryption only if the encryption on the underlying clusters is enabled during deployment.

  > **Note:** After you enable encryption using storage policies, you cannot turn it off. However, you can delete the storage policy on which the encryption is enabled. In such cases, any new data written into the entities is not encrypted. The data that was written prior to the deletion of the storage policy remains encrypted.

- Prism Central supports storage policies for VMs and volume groups (VGs).
- Prism Central applies storage policies to Categories. You need to tag the VMs and VGs in Categories. You might also attach VGs to VMs. When you apply different storage policies through different categories to a VG and VM tagged to each other, the storage policies are applied independently. The storage policy applied to the tagged VG does not affect the tagged VM and vice versa.
- The storage policy engine takes 30 minutes or more to apply a newly created storage policy to the associated entities like VMs. The time taken depends on the number of entities associated with the storage policy.
- Storage policies use categories to associate with entities like VMs and VGs. You cannot associate an entity such as a VM or a VG directly with the storage policy. Create a category for the entities, and then assign the category with the storage policy.

  When you associate a category with a storage policy, Prism Central associates all the entities that are associated with that category with the storage policy.

  For information about how to create a category and assign a category to a VM or VG, see Category Management on page 454.
- A cloned entity like a cloned VM or VG inherits the category and the attached storage policy of the original entity from which it is cloned. Thus, the storage policy engine applies the storage policy that is associated with the inherited category to the cloned entities.
- A cloned entity like a cloned VM does not inherit the compliance state of the storage policy applied to the entity from which it is cloned. The cluster runs a full compliance cycle to establish compliance with the storage policy of the cloned entity. In this case, the system displays the **Compliance State** of the cloned entity as **In Progress**, and not inherit the **Compliant** state.

  For example, if VM1 has a storage policy applied to it and is in a **Compliant** state and VM2 is cloned from VM1, then VM2 does not automatically inherit the **Compliant** state of VM1.
- Shared data between the encrypted VMs and unencrypted VMs is encrypted.
- Shared data between a VM with Replication Factor 2 and another VM with Replication Factor 3 configurations complies with Replication Factor 3. In other words, in such a case, the shared data has three copies.
- For disaster recovery, when you use a snapshot or recovery point of a VM on which you have applied a storage policy, the snapshot restores the category of the VM and, therefore, the storage policy as well.

  > **Note:** The recovery point or snapshot of a VG does not restore the category, and therefore the storage policy, of the VG.

Requirements

Ensure that you meet the following requirements to complete the built-in pre-checks and successfully create a storage policy.

> **Note:** The storage policy engine performs the pre-checks based on these requirements in the sequence listed below. For example, suppose you repeat an existing storage policy name for a new storage policy. In that case, the policy engine fails the storage policy creation, generates the failure message stating, Duplicate name , and stops other checks. The engine triggers the storage policy creation only after all the pre-checks are validated.

1. A unique name is assigned to every storage policy. Prism Central displays an error if the storage policy name matches any existing storage policy entry.
2. A *defined* (non-default) value for at least one storage policy attribute or property. For example, for **Compression** the default value is **Inherit from Cluster**, so you might instead select **On** with **Inline** as the value. You could select or provide a defined value for any one ore more properties of the storage policy.

   For the list of properties that you can configure during creation or updating of a storage policy, see Creating a Storage Policy on page 510.
3. The throttled IOPS value is set greater than 99 (to enable rate-limiting or throttling) or equal to -1 (to clear the throttling) in the storage policies.
4. The Replication Factor you set is supported by the Fault Tolerance of the cluster that hosts the VMs or VGs.

   For example, if the Fault Tolerance of the cluster is FT1, then select the Replication Factor **2** in the policy.

Limitations

- Prism Central does not support storage policies for entities running on ESXi and Hyper-V.
- Prism Central does not support storage policies for Nutanix Disaster Recovery with on-premises recovery AZ (on-prem recovery cluster managed by a Prism Central or Nutanix Disaster Recovery with multiple Prism Central deployments. For more information, see Nutanix Disaster Recovery Guide.
- Nutanix supports storage policies for Nutanix Disaster Recovery with th single Prism Central. However, the storage properties defined for the container are applied to the snapshots replicated to the replication cluster. In other words, the snapshot data replicated to the remote site is transformed based on the settings defined for the remote site containers. The storage policies are applied only after the VM failover.
- You can associate multiple categories with one storage policy. However, you can associate one category with only one storage policy. After associating a category with one storage policy, you cannot associate the same category with another storage policy. When you associate the same category with another storage policy, Prism Central adds the category to the **Associated Categories** list but displays an alert (an exclamation mark) and turns off the **Save** button until you remove the category. The following message pops up when you hover on or click the alert (exclamation mark):

  ```
  This category has an existing storage policy (<name of storage policy>)
   associated with it.
  ```

- You can create a maximum of 100 storage policies irrespective of the type of Prism Central deployed (whether x-large, large, small, or x-small Prism Central with scale-out or single instance).

  For information on Prism Central scalability and the type of Prism Central deployments, see the *Prism Central Scalability* topic in the release notes for the Prism Central version to be installed.
- You cannot create or apply a storage policy for a snapshot. Prism Central applies a storage policy to a live vDisk and the entire chain of snapshots of that vDisk.

- Prism Central does not encrypt the snapshots of the vDisk that are in the storage if the live vDisk is deleted before AOS applies the storage policy to the vDisk.
- Role-based access control (RBAC) can be configured for **Storage Policies**. Prism Central supports only Super Admin, Prism Admin, or Prism Viewer roles for Storage Policies. Prism Central does not support granular RBAC for Storage Policies. Do not attempt to configure permissions using APIs. Use **Super Admin** role permissions for **Storage Policies** operations.

  You can create custom roles to assign specific permissions such as create, update, delete, or view permissions.
- If two entities that share data have different Replication Factor, then the higher Replication Factor is applied to the shared data.
- If two entities share data and one or both entities have a storage policy with encryption enabled, then the shared data is encrypted.
- If two entities share data and only one of the entities has a storage policy with compression enabled, then the shared data is not compressed.
- Suppose you associate an entity with multiple storage policies. In that case, the policy engine sorts the storage policy list using a method based on the policy name and applies the highest-ranking policy from the sorted list to the entity. The highest-ranking storage policy is the one with the lexicographically smallest name in the list. Suppose you add another storage policy later, and this newly added policy becomes the highest-ranking policy in the newly sorted list. In that case, the engine continues to apply the previously applied storage policy. To apply the newly added storage policy to the entity, remove the association of the entity with the previously applied storage policy.

Default Storage Policy

Storage Policies in Prism Central lets you manage the storage attributes like Replication factor, encryption, compression, and QoS of entities like Virtual Machines (VMs) and Volume Groups (VGs). You can configure custom entity-centric storage policies to manage the storage attributes of the entities as required.

When you install or upgrade the Prism Central instance to pc.2024.1 or later versions, Prism Central configures a predefined or default storage policy. The default storage policy only defines the Replication Factor (RF) and Compression parameters. It allows the values for the other parameters to be taken from the cluster storage settings.

The default storage policy requires a minimum Prism Central version of pc.2024.1. AOS 6.8 and later versions fully support the default storage policy. Older versions of AOS do not fully support the default storage policy, even if they support storage policies broadly.

The **Storage Policies** dashboard in Prism Central provides an introductory dialog that describes the **Default Storage Policy**.

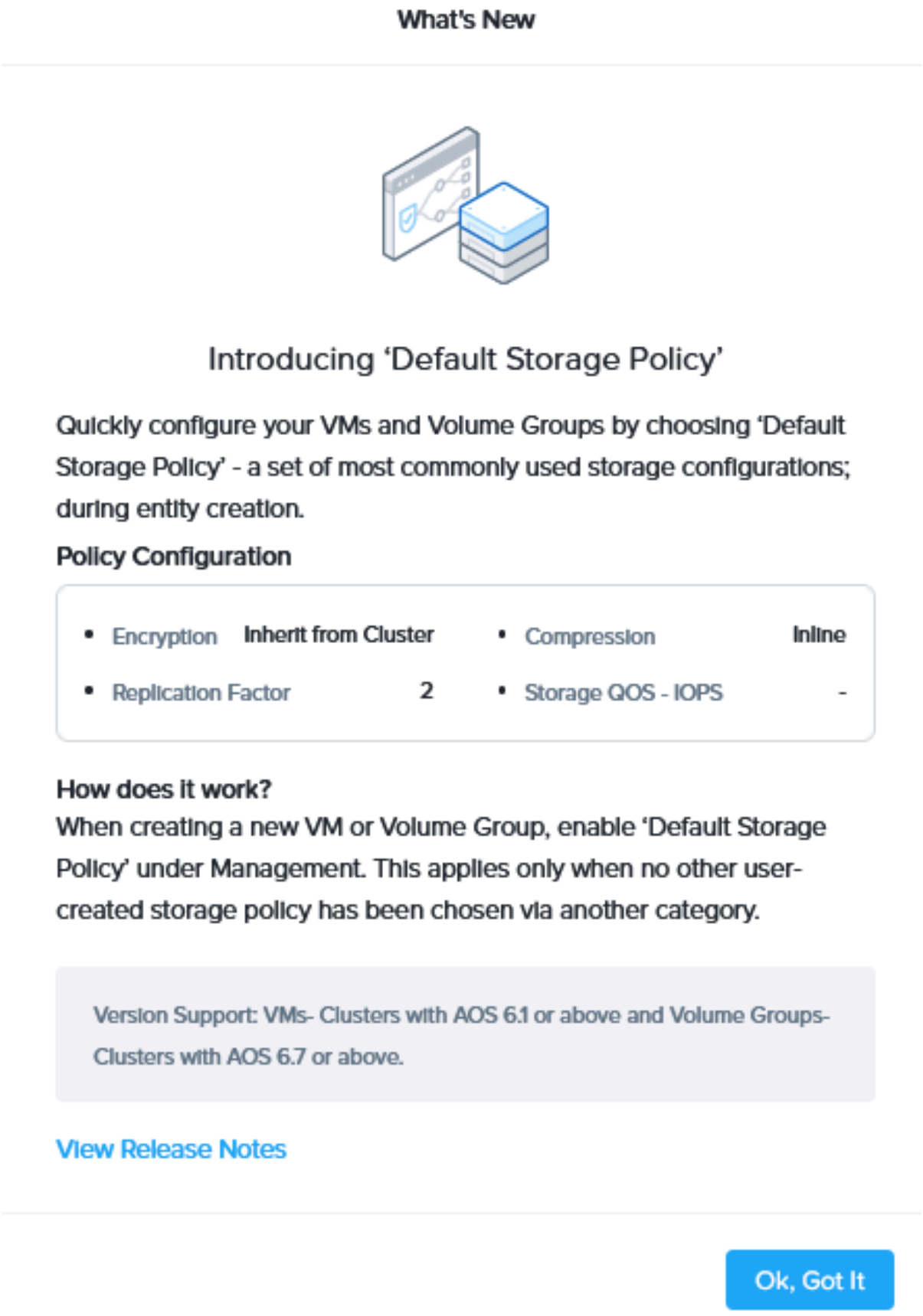


Figure 210: Introducing 'Default Storage Policy'

You can apply the default storage policy to any entity, such as VMs and VGs, by enabling the **Enable 'Default-Storage' policy** toggle switch when you create or update a VM or VG. The default storage policy is associated with the **Storage:$Default** category. When you turn on the **Enable 'Default-Storage' policy** toggle switch, the default storage policy is applied, like any other storage policy, to the VM or VG that is associated with the **Storage:$Default** category.

The standard configuration of the default storage policy is as follows:

- Replication Factor (RF) is set to **2**.
- Encryption is set to **Inherit from Cluster**.
- Compression is set to **Inline**.
- No values are set for QoS.

Limitations for Default Storage Policy

- If the name of an existing storage policy conflicts with the **Default Storage** policy during its creation, Prism Central creates the **Default Storage** policy but does not issue any alert. Rename the existing policy. The **Default Storage** policy cannot be updated.
- When you create or update an entity like a VM or a VG,
  - The default storage policy (**Enable 'Default-Storage' policy** toggle switch) is not enabled for the entity by default.
  - If you assign a category associated with a non-default storage policy to an entity and also enable the **Enable 'Default-Storage' policy** toggle switch, the non-default storage policy gets precedence over the default storage policy. The default storage policy is not applied to the entity in such a case.
- **Storage: $Default Category**

  The **Storage: $Default** category is used to assign the default storage policy to an entity such as a VM or a VG. You cannot associate any other storage policy with this category. Nutanix recommends that you do not associate any other policy with the **Storage: $Default** category or make any other changes to this category.

  Do not assign any other category that is already associated with another storage policy to the entity, such as a VM or VG, if you want to enable the **Enable 'Default-Storage' policy** switch for that entity. If you enable the **Enable 'Default-Storage' policy** switch for an entity that is already associated with another category, the **Storage: $Default** category is enabled, but the storage policy associated with the other category overrides the default storage policy.
- **Edit the Default Storage Policy**

  You cannot edit the default storage policy. You can only apply it to an entity by associating the entity with the **Storage: $Default** category, enabling the **Enable 'Default-Storage' policy** switch for that entity, and ensuring that no other categories with storage policies are applied to that entity, thus overriding the default storage policy.

Storage Policies Summary View

The Storage policies summary view allows you to access a list of all the user-defined storage policies across registered clusters.

> **Note:** The **Storage Policies** page is available if you are logged on as a view-only user. However, you cannot create a storage policy or modify an existing one.

To access the storage policies summary view, perform the following steps:

1. Log in to Prism Central.

2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Storage Policies** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The system displays the **List** tab by default with a summary view of storage policies across all registered clusters. When you open the **Storage Policies** page for the first time, Prism Central displays the **Introducing 'Default Storage Policy'** page. Select **OK, Got it** to go to the **List** tab of the **Storage Policies** summary view.

   For more information on the default storage policy, see Default Storage Policy on page 498.

Table 145: Storage Policies Page - Field Description

Field	Description	Values
Name	Displays the name of the Storage Policy. You can click the name to view the details page of the selected storage policy. The default storage policy (see Default Storage Policy on page 498) is named **Default Storage** and marked `SYSTEM`.	(Name of storage policy)
Replication Factor	Displays the Replication Factor selected.	Inherit from Container or 2 or 3
Encryption	Displays the encryption mode selected.	Enabled or Inherit from Cluster
Compression	Displays the compression mode selected.	Inline or Post Process (if On) Off Inherit from Cluster
Throttled Throughput (IOPS)	Displays the throttled throughput value in terms of IOPS.	(Integer number)
Throttled Throughput (MB/s)	Displays the throttled throughput value in MBps.	(Integer number)
Total Categories	Displays the total number of categories that are associated with the storage policy.	(Integer number)

Field	Description	Values
Realized Entities	Indicates the number of entities to which the storage policy is applied. **Note:** A single storage policy can be applied to multiple entities. Multiple storage policies cannot be applied to a single entity.	(Integer number)

You can perform the following actions for the storage policies in the **Storage Policies** summary view:

- Access the detailed information about an individual storage policy. For more information, see Storage Policy Details View on page 503.
- Create a storage policy. For more information, see Creating a Storage Policy on page 510.
- Update, clone, or delete a storage policy. For more information, see Managing Storage Policies on page 514.

  Note: You cannot update or delete the **Default Storage** policy. You can only clone the **Default Storage** policy. Cloning the default storage policy does not create another default policy. It creates another non-default storage policy that you can modify to suit the needs of your deployment.

- Filter the storage policies list using **Filters** pane. For more information on **Filters** pane, see Filters Pane on page 28.

  For field details, see Table 145: Storage Policies Page - Field Description on page 501.
- Export the table that contains the list of storage policies and their information to a file in a CSV format. For more information on **Export** option, see Export on page 32.
- Use the **Actions** dropdown menu to update, clone, or delete a storage policy. For more information, see Managing Storage Policies on page 514.

Associations Tab

The **Associations** tab displays the compliance state of the storage policies across the registered clusters.

The following table describes the fields that appear in the **Associations** tab of **Storage**page:

Note: A dash (-) is displayed in a field when a value is not available or applicable.

Table 146: Storage Associations Tab - Field Description

Parameter	Description	Values
Name	Indicates the name of the Storage Policy. You can click the name to view the details page of the selected storage policy.	(Name of storage policy)
Associated Categories	Displays the number of categories associated with the storage policy.	(Integer number)
Unrealized Entities		

Parameter	Description	Values
VMs	Displays the number of VMs that the system considers for compliance check and to apply the storage policy.	(Integer number)
VGs	Displays the number of VGs that the system considers for compliance check and to apply the storage policy.	(Integer number)
Realized Entities		
VMs	Indicates the number of VMs to which the storage policy is applied.	(Integer number)
VGs	Indicates the number of VGs to which the storage policy is applied.	(Integer number)
Compliance for Realized Entities	Provides a link to a dialog window that displays the state of compliance of the VMs and VGs covered by the policy.	(Integer) **in Progress** (Integer) **Non Compliant** (Integer) **Compliant**

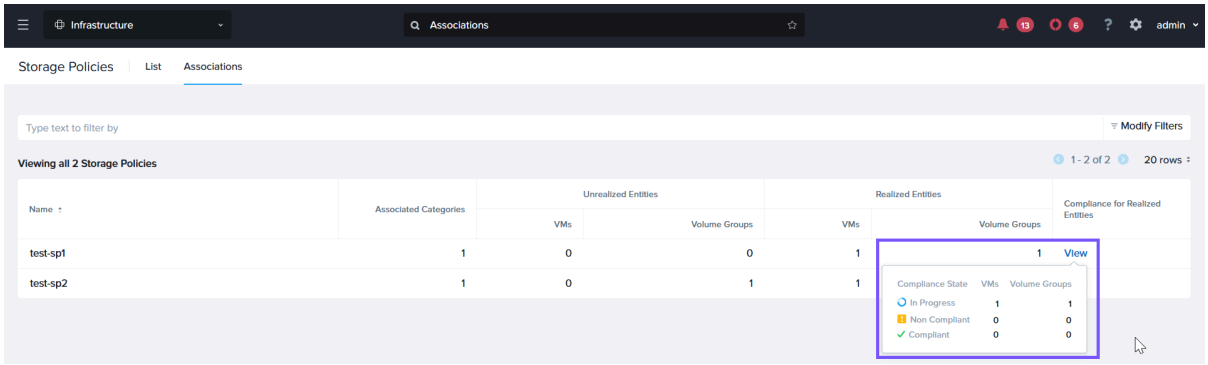


Figure 211: Storage Policy Compliance Pop-up Window

You can filter the storage policies list based on the storage policy name using **Filters** pane in the **Associations** tab. For more information, see Filters Pane on page 28.

For more information about Storage Policies, see Storage Policy Management on page 495.

- For information about creating or updating storage policies, see Creating a Storage Policy on page 510.
- For information about deleting storage policies, see Deleting a Storage Policy on page 516.

Storage Policy Details View

To access the details page for a storage policy, go to the storage policy **List** tab (see Storage Policy Management on page 495) and click the name of the storage policy you want to view the details of. You

can also access the details page by clicking the name of the storage policy wherever that name appears, such as in a dashboard widget or search result.

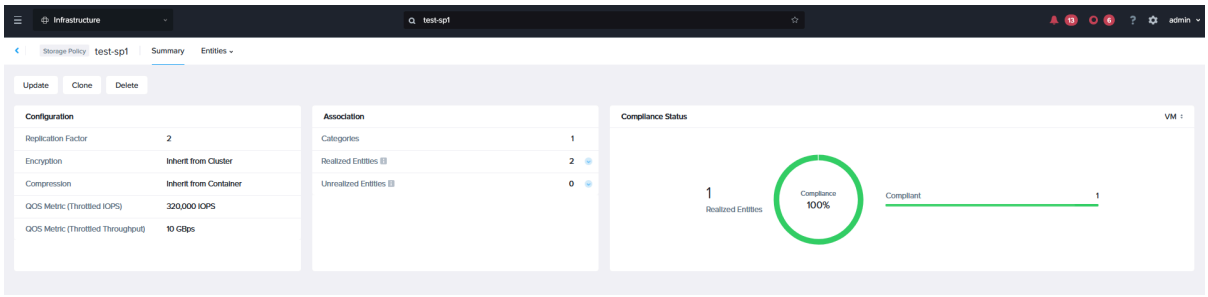


Figure 212: Storage Policies details view

The storage policy details page includes the following tabs:

- **Summary**—displayed by default when you open the storage policy details page. This tab provides information about the storage policy summarized into widgets.
- **Entities**—displays the list of entities including VMs and VGs associated with the storage policy.

The **Summary** tab of an individual storage policy provides the following widgets:

- **Configuration** - Displays the configuration attributes of the storage policy.
- **Associations**- Displays the count of associated realized and unrealized VMs, VGs,and their categories.
- **Compliance Status** - Displays the compliance status of the entities associated with this policy. If the policy is being applied and the compliance status is not yet known, the status is displayed as **In Progress**. For information about the fields available in the widgets, see Storage Policy Widgets- Field Details on page 504.

<*Action*> available above the widgets. Click the appropriate <*Action*> , such as **Update**, **Clone**, or **Delete** to run that administrative action on the storage policy. For more information about how to perform any <*Action*>, see Managing Storage Policies on page 514.

Storage Policy Widgets- Field Details

The following table describes the fields in the **Configuration**, **Associations**, and **Compliance Status** widgets.

Table 147: Storage Policy Widgets- Field Description

Field	Description	Values
Configuration widget		
Replication Factor	Indicates the Replication Factor selected.	Inherit from Container or 2 or 3
Encryption	Indicates the encryption mode selected.	Enabled or Inherit from Cluster

Field	Description	Values
Compression	Indicates the compression mode selected.	Inline or Post Process (if On) Off Inherit from Cluster
QoS Metric (Throttled IOPS)	Indicates the throttled throughput value in terms of IOPS.	(Integer number)
QoS Metric (Throttled Throughput)	Indicates the throttled throughput value in MBps.	(Integer number)
Associations widget		
Categories	Displays the count of VM and VG categories mapped to the selected storage policy.	(number of VM and VG categories)
Realized Entities	Indicates the number of entities that the storage policy is applied to. The storage policy acts on these entities and defines their storage properties.	(Integer number)
Non-realized Entities	Indicates the number of entities that the storage policy is not applied to. The storage policy is associated with these entities but does not act on them. When a storage policy is not applied to an entity like a VM or a VG, then the entity is listed as **Non-realized Entity**.	(Integer number)
Compliance Status widget		
Realized Entities	Indicates the number of entities that the storage policy is applied to. **Note:** A single storage policy can be applied to multiple entities. Multiple storage policies cannot be applied to a single entity.	(Integer number)
Compliance State	Indicates the number of entities in each of the following compliance states: • In Progress: Indicates the number of entities that the policy has already been applied to and data transformation of entity's data (compliance) is in progress. • Compliant: Indicates the number of entities that are in compliance. • Non Compliant: Indicates the number of entities that are not in compliance	Compliant, In Progress, or Non compliant

Entities Tab

The **Entities** tab enables you to view the realized and non-realized VMs for the selected storage policy:

- Select **Realized** from the **Entities** tab dropdown menu to view the entities that the storage policy is applied to.

- Select **Unrealized** from the **Entities** tab dropdown menu to view the entities that the storage policy is not applied to.

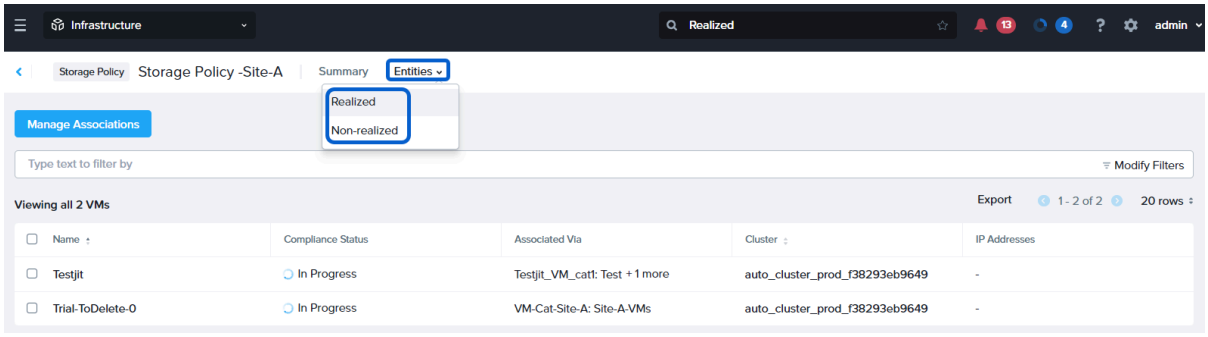


Figure 213: Entities Tab

The following table describes the fields that appear in the **Entities** tab of storage policies details view:

Table 148: Entities Tab - Field Details

Field	Description	Values
Name	Indicates the name of the entity like VMs and VGs.	(entity name such as the name of the VM or VG)
Compliance Status	Indicates the compliance status of the entity as **In Progress**, **Compliant** or **Non Compliant**.	In Progress | Compliant | Non Compliant
Associated Via	Indicates the categories to which the entity and the storage policy are concurrently associated. The storage policy is associated with the entity because the storage policy is associated with this category that is associated with the entity. For example, StoragePolicy1 is associated with CategoryA which is in turn associated with VM1. The category displayed in **Associated via** is CategoryA. The other categories associated with VM1 but not associated with StoragePolicy1 are not displayed here.	(category name)
Cluster	Indicates the name of the cluster on which the entity resides.	(cluster name)
IP Addresses	Indicates the IP addresses configured for the entity.	(IP address)

You can perform the following actions for the storage policies in the **Entities** tab:

- Filter the storage policies list using **Filters** pane. For more information, see Filters Pane on page 28.

  For field details, see Table 148: Entities Tab - Field Details on page 506.
- Export the table that contains the list of storage policies and their information to a file in a CSV format. For more information about this option, see Export on page 32.

Storage Policy Compliance

When you create a policy like a storage policy and apply it to entities like VMs and VGs, there is no way to know whether the application configured or transformed the entities to the parameters set in the policy. You need a mechanism to track the application of the policy and the changes made to the entities in alignment with the parameters set in the policies. Compliance provides that mechanism to track the application of policies and the transformation of the entities and provide feedback on the status at an entity level.

The compliance process begins when you associate a storage policy to a category and, therefore, to entities that the category is assigned to. The association applies the storage policies to the entities that the category is assigned to. For the several reasons, a storage policy is not applied to an entity.

After application, the parameters of the entities such as replication factor, encryption, and compression are transformed according to the configuration of the storage policy. Such transformation (compliance) does not occur for some entities that the category may be assigned to, any of the following, but not restricted to, reasons:

- Incompatible hypervisor: The node is running a hypervisor or version that does not support storage policies. Only AHV supports storage policies.
- Incompatible AOS version: The cluster is running an AOS version that does not support storage policies.
- Multiple storage policies applied: When you apply multiple storage policies to an entity, only one is applied. Other storage policies report that entity as non compliant.

Compliance, thus, tracks the process from application to transformation and reports the status in the storage policy **Summary** tab. AOS applies the storage policy parameters in a specific order that **Compliance** also uses to report status. This order of implementation and tracking of the storage policy parameters is as follows:

- Replication Factor: Replication Factor indicates data availability which is the most factor for an entity.
- Encryption: Encryption indicates data security which is the second most important factor for an entity.
- Compression: There may be cases where compression may not be possible for an entity. So in such a case, if Replication Factor and Encryption parameters are applied and entity data is transformed accordingly, then the compliance engine reports the state for the entity as **Compliant**.
- Throughput: This parameter has lower priority in implementation and compliance reporting. The implementation is similar to the Compression parameter.

Compliance reports the states separately for VMs and VGs, even if the VMs or VGs are tagged to each other. For example, if VM1 is tagged to VG1. VM1 is associated with Category1 and VG1 is associated with Category2. storage policies SP1 and SP2 are associated to Category1 and Category2 respectively. **Compliance** reports the states of VM1 and VG1 separately. It reports the states separately even if VM1 and VG1 are associated to the same Category1, and hence storage policy SP1.

Compliance reports the following states:

Realized Entities

The compliance engine reports this state when a storage policy is applied to the entity. Application of storage policy means that the parameters set in the storage policy are identified for the entity that it is applied to. So when the system reads the storage policy and identifies the Replication Factor, Encryption, Compression and throttled throughput QOS metric parameters for the entity, the compliance engine reports the entity as **Realized Entity**.

Non-realized Entities

There may be several reasons why a storage policy could not be applied to (realized on) an entity. For example, storage policies cannot be applied to ESXi VMs (non-Nutanix entity).

In Progress

Compliance engine reports this state when the one or more parameters set in the storage policy are applied to an entity and the entity data is being transformed to comply with those parameters.

Compliant

The compliance engine reports this state when the transformation of the entity data is complete and all the high priority parameters like Replication Factor and Encryption have been set for the entity in accordance with the settings in the storage policy.

Non Compliant

The compliance engine reports this state when the transformation of the entity data could not be completed and one or more high priority parameters like Replication Factor and Encryption could not be set for the entity in accordance with the settings in the storage policy. **Non Compliant** also indicates unknown state of transformation.

The compliance states are displayed on the storage policy details page. For more information, see Storage Policy Details View on page 503.

Storage Policy Based Replication Factor

Replication Factor is the number of replication copies of any data made on the cluster. For example if you have a Replication Factor of 2 for a container, then the data in that container is written twice on nodes in different fault tolerance domains. This is dependent on how you have configured the fault tolerance domains.

You can use a storage policy to apply Replication Factor to entities like VMs and VGs. When you apply a storage policy to an entity, the Replication Factor defined in the storage policy is applied to the entity. Storage policy compliance checks whether the entity data is compliant with the Replication Factor setting in the storage policy.

Limitations

Configuring Replication Factor for entities using storage policies is not possible in some cases.

- Storage Policies do not support setting Replication Factor of 1. You can only use a storage policy to set Replication Factor (RF) 2 or 3.
- Prism Central does not support Policy based replication factor configuration for entities on storage containers which have Erasure Coding or Deduplication enabled.
- A storage policy Replication Factor setting is not applied when the RF setting in the storage policy is higher than the Replication Factor setting in the cluster.

  For example, if the RF of a cluster is 2, but a storage policy with RF 3 is applied to an entity in that cluster, the entity is reported as **Realized** but **Non-compliant**.
- Shared data between a VM with Replication Factor 2 and another VM with Replication Factor 3 configurations complies with Replication Factor 3. In other words, the shared data has 3 copies.
- A cloned entity like a cloned VM or VG inherits the category, and the storage policy attached thereto, of the original entity that it is cloned from. Thus, the storage policy engine applies the storage policy that is associated with the inherited category to the cloned entities.

Storage Policy Based Encryption

Storage policies allow you to make data-at-rest encryption choices at the entity level.

Deployments can continue to have data-at-rest encryption capabilities scoped for the entire cluster. Storage policy provides the additional option to control the encryption scope decisions at the entity (VM or VG) level.

Note: Prism Central does not support Policy based encryption for storage containers on which Erasure Coding or Deduplication is enabled.

The Key Manager System (KMS) choice is configured as a cluster-wide setting, leveraging either Nutanix Built-in Native Key manager or leveraging a third party Key Manager. As part of the Key manager configuration, the scope of encryption-at-rest is defined either as Cluster-wide or specific entity-scoping. Entity-scoping means that the encryption-at-rest scope is defined at the container or the data policy level.

Important:

- When you select the cluster, you can manage the KMS type by clicking **Actions** > **Manage KMS Type**.
- From Prism Central, if you try to configure storage policy based encryption for any single VM or Category entity without enabling **Entity Encryption** on that cluster, the entity is marked as **Non Compliant**, and Prism Central does not transform the entity data to be encrypted.

  Log on to Prism Central and perform the following steps:

  1. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Hardware** > **Clusters**
  2. Select the target cluster, and choose **Enable Data-at-Rest Encryption** from the **Actions** dropdown menu.
  3. In the **Data-at-Rest Encryption** window, specify the following information:

     - **Select Encryption Type** - Select **Entity Encryption** and click **Save Encryption Type**.
     - **Select Key Management Server (KMS)** - Select **Native KMS (Local)** and click **Enable Encryption**.

     The system prompts you to confirm the action.
  4. Enter **SET** in the **Type SET to Confirm** window, and click **Set Encryption**

When a storage policy is used, AOS data for the VM or VG is encrypted on the disk for all the vDisks attached to the VM or VG. The main features include:

- Once encryption is enabled in a policy, it cannot be disabled. If the VM or VG moves out of the policy or the policy is deleted, then the new writes to the VM or VG are unencrypted and existing data remains encrypted.
- The system automatically generates a unique key for each storage container.
- Multi-tenant requirements having a unique key per tenant can be fulfilled by ensuring that the set of VMs belonging to each tenant is mapped to its own container. Nutanix recommends having only 50 tenants or less per cluster.
- Encryption can be enabled for new and existing VMs or VGs.
- Storage policies supports Volume Group. For any VG attached to a VM that is associated with a storage policy enabling encryption, the data stored in the VG is encrypted only if the storage policy associated with the VG also enables encryption. In other words, data encryption in a VG attached to a VM is independent of the storage policy associated with the VM. It is not derived from the storage policy applied to the VM that the VG is attached to.
- Unencrypted VM needs to remain unencrypted during the cloning process.
- Shared data between the encrypted entities and unencrypted entities is encrypted.

For information about containers, see the Storage Management section in the *Prism Web Console Guide*.

For information about configuring key manager, see the Security Guide.

Creating a Storage Policy

You can create or update a storage policy in Prism Central only.

Before you begin

Ensure that you have created the necessary categories and assigned the entities such as VMs and VGs to the categories.

For more information about how to create a category, see Creating a Category on page 457.

For more information about how to assign a category to the entity, see Assigning a Category on page 459.

About this task

Prism Central provides a two-step framework to create a storage policy that involves the following steps:

- **Configuration** step - Enables you to configure the data replication (Replication Factor), data security (Encryption), data reduction (Compression) and QoS (IOPS or Throughput throttling) aspects of the storage policy.
- **Association** step - Enables you to associate the storage policy with categories that the entities (like VM or VG) are associated with.

Procedure

To create a storage policy, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Storage Policies** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.

   The system displays the **List** tab by default with summary view of storage policies across all registered clusters.

3. Click **Create Storage Policy**.
   The system displays the **Create Storage Policy** window with the **Configuration** step.

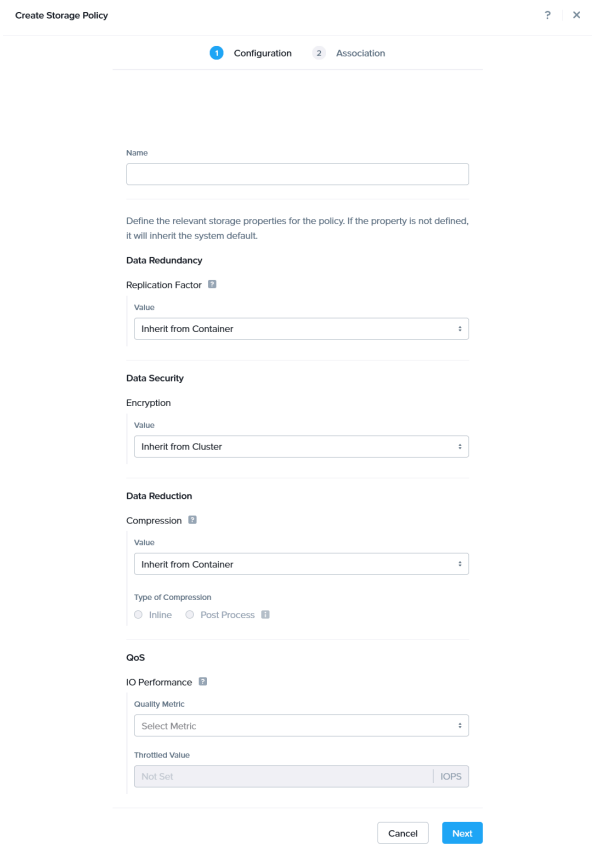


Figure 214: Create Storage Policy - Configuration Step

Configure the following fields in the **Configuration** step. Select a defined (non-default) value for a least one of the properties.

Table 149: Configuration Step - Field Description

Field	Description and Values
Name	Enter a unique name for the storage policy. **Note:** Do not repeat a name previously used for another storage policy. The built-in pre-check fails if you enter a non-unique name.
Data Redundancy	

Field	Description and Values
Replication Factor	Select one of the following values from the dropdown list. • **Inherit from Container** (default)—the category or entity inherits the Replication Factor (RF2 or RF 3) configuration from the container. This is the default value for Replication Factor. • **2**—to enable Replication Factor 2 (RF2—Original plus 1 copy) through the storage policy. • **3**—to enable Replication Factor 3 (RF3—Original plus 2 copies) through the storage policy. **Note:** The Replication Factor selected must be supported by the Fault Tolerance of the cluster. For example, if the Fault Tolerance of the cluster is FT1, then selecting Replication Factor **3** in the policy leads to non-compliance.
Data Security	
Encryption Value	Select one of the following values from the dropdown list. • **Enabled**—to enable encryption through the storage policy. **Note:** After you enable encryption using storage policies, you cannot disable it. • **Inherit from Cluster** (default)—the category or entity inherits the encryption configuration from the cluster. This is the default value for Encryption.
Data Reduction	
Compression Value	Select one of the following values from the dropdown list. • **On**—to enable compression. If you select **On** then you must select the type of compression that you want to apply. You can select **Inline** compression (default) or **Post Process** compression. If you select **Post Process**, the data is compressed with some delay (up to 3600 seconds) that is set by the system default. • **Off**—to disable compression. • **Inherit from Cluster** (default)—the category or entity inherits the compression configuration from the cluster. This is the default value for compression.
IO Performance (Also see the *Relationship between Block Size, IOPS and Throughput* table for information about how Throttle IOPS or Throughput is calculated based on block size)	
Quality Metric	Select one of the following values from the dropdown list. • **Throughput** • **IOPS**

Field	Description and Values
Throttled Value	Provide a numeric value. **Note:** For **IOPS** the value must be greater than 99 or equal to -1 (minus 1).

Throttle IOPS or Throughput Relationship: Set the Throttle IOPS or Throughput based on the block size. Nutanix uses a fixed block size of 32k. For example, with a block size of 32K, if you set a Throttle IOPS value of 1000 IOPS, the Throttle Throughput would be 31.25 MBps. See the table.

Table 150: Relationship between Block Size, IOPS and Throughput

Block Size	IOPS	Throughput (MBps)
8k	1000	7.81
16K	1000	15.63
32K	1000	31.25
64K	500	31.25
128K	250	31.25

4. Click **Next**.

   If you did not select or enter an appropriate value and the pre-checks failed, the relevant error is displayed below the field that failed the pre-check. Select or enter an appropriate value, and click **Next** again.

   The system displays the **Association** step.

5. In the **Association** step, select the category or categories you want to associate with the storage policy in the **Add Category** field.

   Type the first 2-3 characters of the category name you want to associate with in the **Add Category** field. The system displays a dropdown list of the matching categories based on the typed entry.

   Use the Add icon and Remove icon to add and remove the required categories in the**Associated Categories** list.

   > **Note:** You can add multiple categories for one storage policy. When you associate a category with one storage policy, you cannot associate the same category with another storage policy.

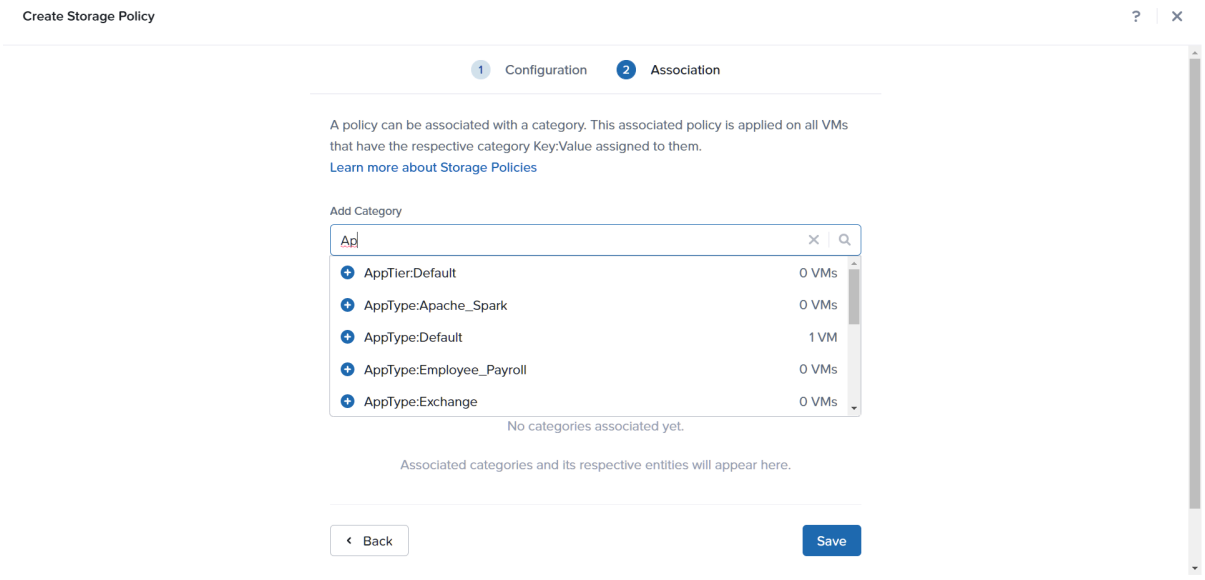


Figure 215: Create Storage Policy - Association Step

6. Click **Save** to save the storage policy.

Managing Storage Policies

This section describes how to update, clone, and delete the storage policies in Prism Central

About this task

You can perform the following actions to manage the Storage policies in Prism Central:

- Update a Storage policy.

  > **Note:** You cannot update the **Default Storage** policy.

- Clone a Storage policy.

  > **Note:** You can clone the **Default Storage** policy.

- Delete a Storage policy.

  > **Note:** You cannot delete the **Default Storage** policy.

  When you delete a storage policy, the entities associated with the deleted storage policy return to their default state, or the configurations from any other storage policy associated with the category are

applied to the entities. Nutanix recommends that you remove all the categories and entities associated with the storage policy.

When a storage policy is deleted, it is marked for removal in the database. Prism Central stops displaying that storage policy. The process stops applying the storage attributes of the policy and instead applies the storage attributes configured for the container. However, the VM continues to display the storage policy as if it still applies until the next system scan occurs and the policy is removed from the VM information. A Kanon service scan occurs every 1800 seconds and refreshes the information.

- Manage associations.

  Note: You cannot update the category association of the **Default Storage** policy. The **Default Storage** policy is associated with the **Storage:$Default** category.

Procedure

To update a storage policy, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **Storage Policies** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default.
3. Select the target storage policy check box, and choose **Update** from the **Actions** dropdown menu.
4. Update the information as per your requirement in the **Update Storage Policy** window, and click **Save**. For field details, see Creating a Bandwidth Throttling Policy on page 487.

   To delete the storage policy, select the target storage policy check box and choose **Delete** from the **Actions** dropdown menu. The command prompt prompts you to confirm the deletion action. Click **Delete** to confirm the delete action.

   Note: You can also click **Preview changes** to view the categories and entities that are affected by the deletion of the storage policy.

   To clone the storage policy, select the target storage policy check box and choose **Clone** from the **Actions** dropdown menu. The system displays the **Create copy of <Storage Policy-Name>** window with the same values populated in it as specified for the selected storage policy.

   Note: The **<Storage Policy-Name>** indicates the actual name of the storage policy you selected to clone.

   During cloning, the categories to which the original storage policy is attached are removed. The clone storage policy does not inherit the categories from the original storage policy.

   Enter the field details as per your requirement, and click **Save**. For field details, see Creating a Storage Policy on page 510.

   To update the category associations only in an existing storage policy, navigate to the **Entities** tab in Storage Policy Details View on page 503and click **Manage Associations**. Type the first 2-3

characters of the category name in the **Add Category** field and use the Add icon and Remove icon to add and remove the required categories in the**Associated Categories** list.

> **Note:** You can associate multiple categories with one storage policy. When you associate a category with only one storage policy. You cannot associate one category with multiple storage policies
>
> The **Storage: $Default** category is associated with the **Default Storage** policy. Do not associate the **Storage: $Default** category with any other storage policy.

Deleting a Storage Policy

You can delete a storage policy. When you do so, the entities associated with the deleted storage policy return to their default state or the configurations from any other storage policy that is associated with the category are applied to the entities.

Before you begin

Nutanix recommends that you remove all the categories and entities associated with the storage policy.

About this task

When a storage policy is deleted, it is marked for removal in the database. Prism Central stops displaying that storage policy. The process stops applying the storage attributes of the policy and instead applies the storage attributes configured for the container. However, the VM continues to display the storage policy as if it still applies, until the next system scan occurs and removes the policy from VM information.

Remove associations of the storage policy to categories in the **Categories** or **Entities** tabs of the storage policy details page.

Delete a storage policy from the **Storage Policies** dashboard or the **Summary** tab of the storage policy details page.

Do the following to delete a storage policy:

Procedure

1. Click the name of the storage policy. On the storage policy details page, click **Delete**.
   The **Delete <storage-policy-name>** dialog box is displayed as follows:

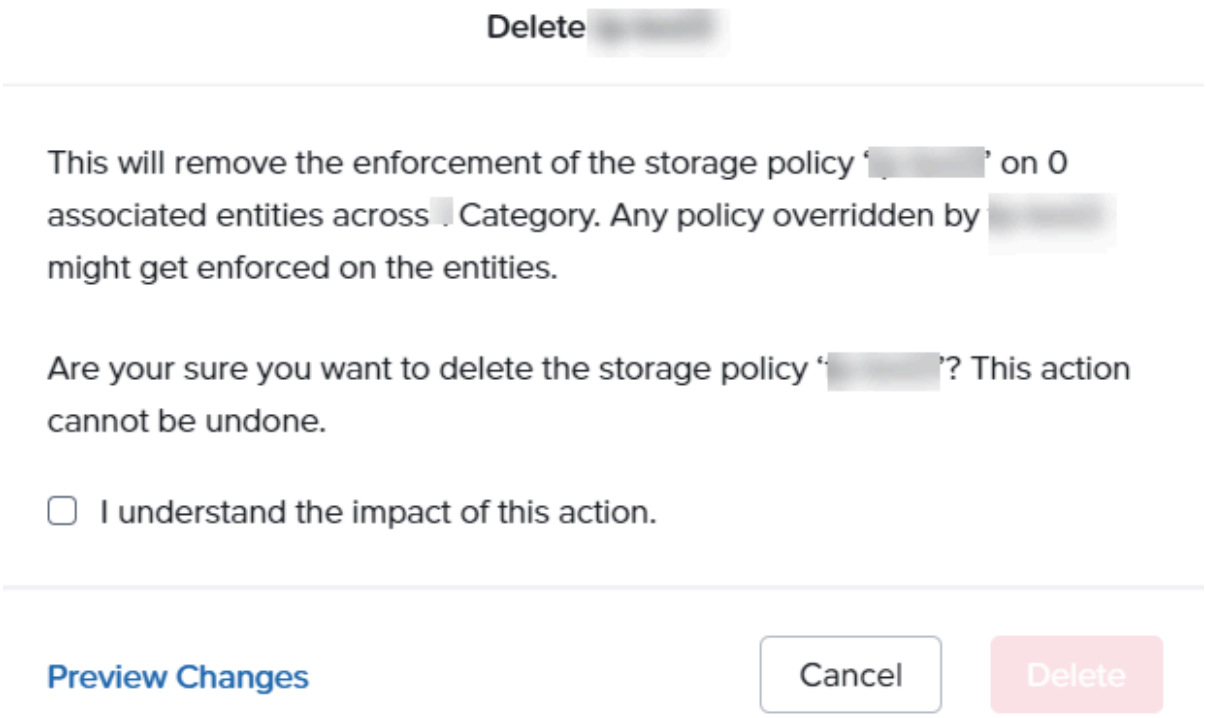


Figure 216: Delete Storage Policy

2. (Optional) Click **Preview Changes** to view the **Changes Preview** dialog box.
   The **Changes Preview** dialog box lists the categories and entities that are affected by the deletion of the storage policy.

   Tip: If you have already removed all the associations of the storage policy, then the list of categories and entities is empty.

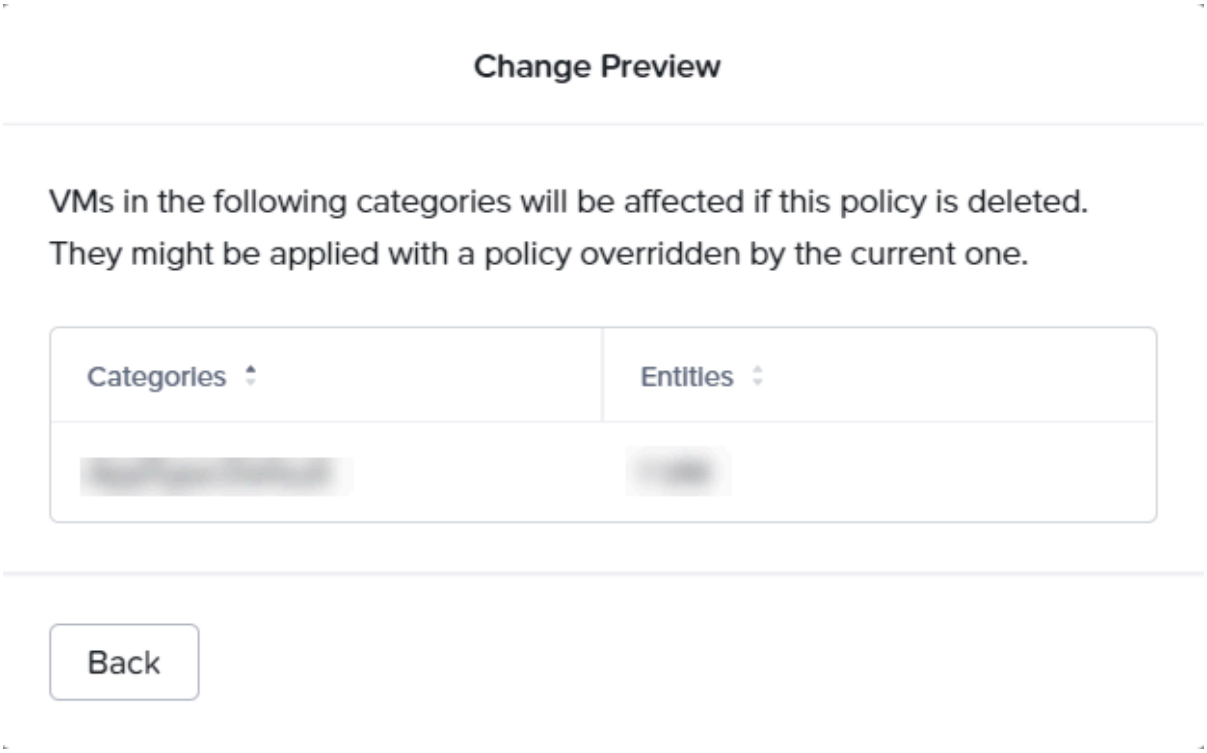


Figure 217: Change Preview

   After you preview the impact, click **Back** to go back to the **Delete <storage-policy-name>** window.

3. Select the **I understand the impact of this action.** checkbox.
   The **Delete** is enabled only after you select the **I understand the impact of this action.** checkbox.
4. Click **Delete**.

PRISM SELF SERVICE ADMINISTRATION

This section describes how to configure and administer Prism Self Service.

The Prism Self Service feature allows you to create projects where consumers of IT infrastructure within an enterprise—individual users or teams such as development, test, and DevOps—can provision and manage VMs in a self-service manner, without having to engage IT in day-to-day operations.

For information about user roles and configuration workflow for Prism Self Service, see Prism Self Service Setup on page 519.

Prism Self Service Setup

Prism Self Service represents a special view within Prism Central. While Prism Central enables infrastructure management across clusters, Prism Self Service allows end users to consume that infrastructure in a self-service manner. Prism Self Service uses the resources provided by a single AHV cluster.

> **Important:** Prism Self Service is only supported with AHV hypervisor, and not supported with other hypervisors.

> **Note:** A SelfServiceContainer storage container is created on the target cluster and used by Prism Self Service for storage and other feature operations. To ensure proper operation of these features, do not delete this storage container. For more information about storage containers, see Storage Container Management on page 268

Prism Self Service Roles

There are three roles to consider when configuring Prism Self Service:

1. *Prism Central administrator*. The Prism Central administrator adds an Active Directory that includes the pool of self-service users and (optionally) creates one or more self-service administrators. Prism Central administrators also create VMs, images, and network configurations that may be consumed by self-service users.
2. *Self-service administrator*. The self-service administrator performs the following tasks:

   - Creates a project for each team that needs self service and adds users and groups to the projects.
   - Configures roles for project members. A project member can access only the entities or perform only the actions defined in the role assigned to that project member.
   - Publishes VM templates and images to the catalog.
   - Monitors resource usage by various projects and its VMs and members, and then adjusts resource quotas as necessary.

   It is optional to configure a separate self-service administrator because a Prism Central administrator can perform any of these tasks. However, if you would like to authorize users to administer end-user VM or application provisioning, you can use this role to give them access to virtual infrastructure without giving them access to physical infrastructure.

   > **Caution:** Self-service administrators have full access to all VMs running on the Nutanix cluster, including infrastructure VMs not tied to a project. Self-service administrators can assign infrastructure VMs to project members, add them to the catalog, and delete them even if they do not have administrative access to Prism Central. Consider these privileges when appointing self-service administrators, and

make sure to communicate to self-service administrators the need to exercise caution when working with infrastructure VMs.

After a Prism Central administrator has designated a user as a self-service administrator, the Prism Central administrator cannot limit the user's privileges. Therefore, if you plan to delegate self-service administration responsibilities to an Active Directory group, be sure that you want to delegate the responsibility to all the users in the group. If the user group is large or includes users that must not have self-service administrator privileges, Nutanix recommends that you create a separate Active Directory group for the users to whom you want to delegate self-service administration responsibilities.

3. *Project user*. These are the users assigned to a project by a self-service administrator. They can perform any action that the self-service administrator grants them. The permissions are determined by the roles assigned to the users and groups in the project. When project users log in, they see a custom self-service GUI interface that shows only what the role permissions allow. Project users create and manage only what they need.

Prism Self Service Workflow

To configure Prism Self Service, perform the following tasks:

Table 151: Prism Self Service Workflow

Sequence	Tasks	Description
1	Specify an Active Directory for Prism Self Service.	For more information, see Adding an Authentication Directory (Prism Central) information in *Security Guide*.
2	Add one or more self-service administrators.	For more information, see Managing Prism Self Service Admins information in *Prism Central Admin Center Guide*.
3	Create a project for each team that needs self service and add users and groups to the projects.	For more information, see Project Overview information in *Prism Central Admin Center Guide*.
4	Configure roles for project members. You can also allow project members to create their own VMs	For more information, see Controlling User Access (RBAC) in *Security Guide*. **Note:** Role Based Access Control (RBAC) is an independent feature, so you can configure RBAC without configuring self service or creating projects. However, projects allow you to enforce RBAC in a more granular way.
5	Add VM templates and images to the catalog.	For more information, see Catalog Management on page 262.
6	Create VMs as needed and assign them to project members as appropriate.	For information about how to create a VM, see Creating a VM (Self Service) on page 521 and Creating a VM from Catalog Items (Self Service) on page 521. For information about how to assign a VM to a project member, see Assigning a VM to a Project Member on page 529.

Sequence	Tasks	Description
7	Monitor resource usage for the projects and adjust resource quotas as needed.	For more information, see the following information in *Prism Central Admin Center Guide*: • Project Details View - To monitor resource usage for a project. • Quota Policy Overview - To define the resource quotas.

Creating a VM (Self Service)

About this task

When you are logged in to Prism Central as a self-service administrator or a project member, you can create a VM if you have the required permissions to create a VM.

Procedure

In Prism Central Self Service framework, you can create a VM in the following two ways:

- Using the workflow that an admin user follows. For more information, see Creating a VM through Prism Central (AHV) on page 121.
- Using a source file (image or VM template) that is stored in the Prism Central catalog. For more information, see Creating a VM from Catalog Items (Self Service) on page 521.

  For information about Prism Self Service, see Prism Self Service Administration on page 519.

Creating a VM from Catalog Items (Self Service)

This section describes how to create a VM from catalog items.

About this task

When you are logged on as a self-service administrator or a project member with permission to create a VM, you can create a VM based on a source file stored in the Prism Central catalog. For information about how to add a source file (image or VM template) to a catalog, see Adding a Catalog Item on page 264.

For information about Prism Self Service, see Prism Self Service Administration on page 519.

> **Note:** If you are not logged in as a self-service administrator or a project member and you want to create a VM without the source file stored in the Prism Central catalog, you can follow the procedure as described in Creating a VM through Prism Central (AHV) on page 121.

Procedure

To create a VM from catalog items, perform the following steps:

1. Log in to Prism Central as a self-service administrator or a project member.

2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
The system displays the **List** tab by default with all the VMs across registered AHV clusters.

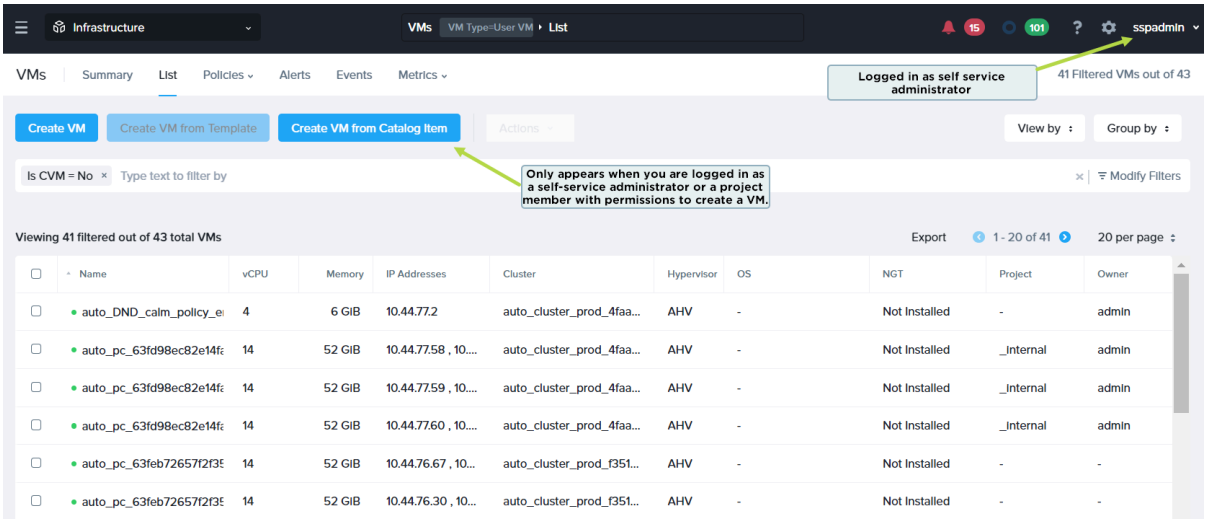


Figure 218: VM Summary View - Self Service Administrator login

3. Click **Create VM from Catalog Item**.

> **Note:** The **Create VM from Catalog Item** option only appears if you are logged in as self-service administrator or a project member with permissions to create a VM.

The system displays the **Create VM from Catalog Item** page.

4. In **Catalog Type**, select one of the following source for the VM:

» **VM Template** - Used to create a VM from a VM template in the catalog.

A VM template includes all the configuration information required to create a VM. You can use a template to quickly deploy a VM without specifying all the configuration information.

» **Image**- Used to create a VM from a mounted disk image.

Disk images can be CD-ROM images such as installer ISO images or images of hard drives that contain pre-installed applications and data. Disk images enable you to share data with other VMs, however you need to specify configuration information for the VM that you create using the disk image.

5. In **Catalog Item** field, perform either of the following actions based on the source you select in the **Catalog Type** field:

   - If **VM Template** is selected as the source in the **Catalog Type** field, select the target VM template in the **Catalog Item** field. The available VM templates from the catalog are listed. If the target VM image does not appear in the list, you can search for it by name in the search field.

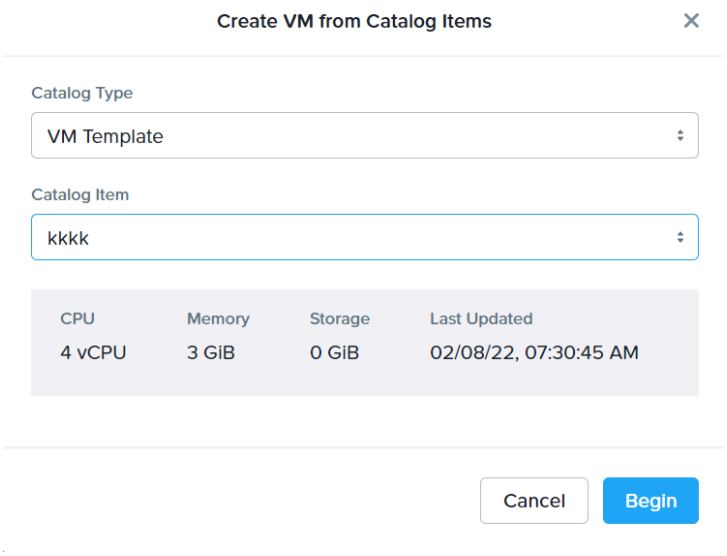


Figure 219: Create VM from Catalog Items

   - If **Image** is selected as the source in the **Catalog Type** field, select one or more of the disk images. The available disk images from the catalog are listed. If the target disk image does not appear in the list, you can search for it by name in the search field.

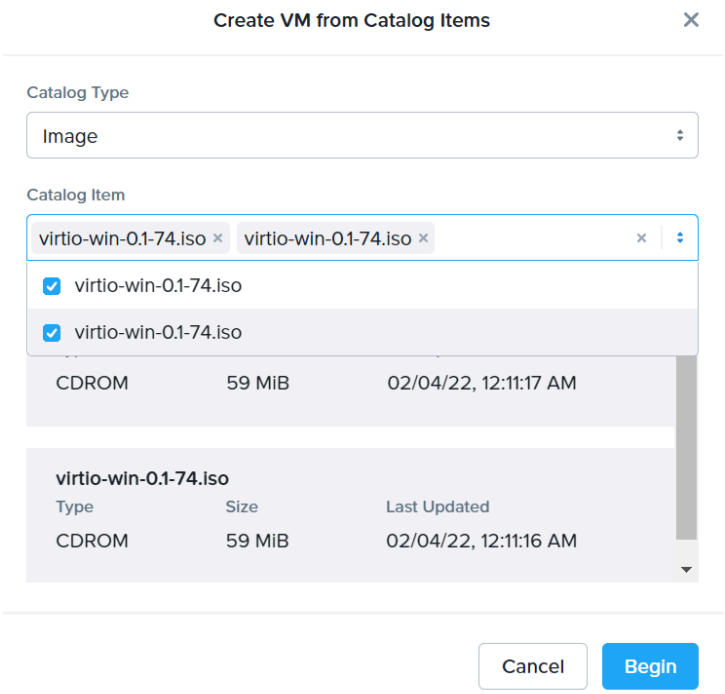


Figure 220: Create VM Window (Configuration)

6. Click **Begin**.

   The **Create VM** page appears.

7. In the **Configuration** step, specify the following information:

   a. **Name**: Enter a name for the VM.

   b. **Project**: Select the project associated with this VM from the dropdown menu.

   c. **Cluster**: Select the target cluster from the dropdown menu on which you intend to create the VM.

   d. **Number of VMs**: Enter the number of VMs you intend to create. The VM names are suffixed with sequential numbers (1 to 5).

   e. **vCPU(s)**: Enter the number of virtual CPUs to allocate to this VM.

   f. **Number of Cores per vCPU**: Enter the number of cores assigned to each virtual CPU.

   g. **Memory**: Enter the amount of memory (in GB) to allocate to this VM.

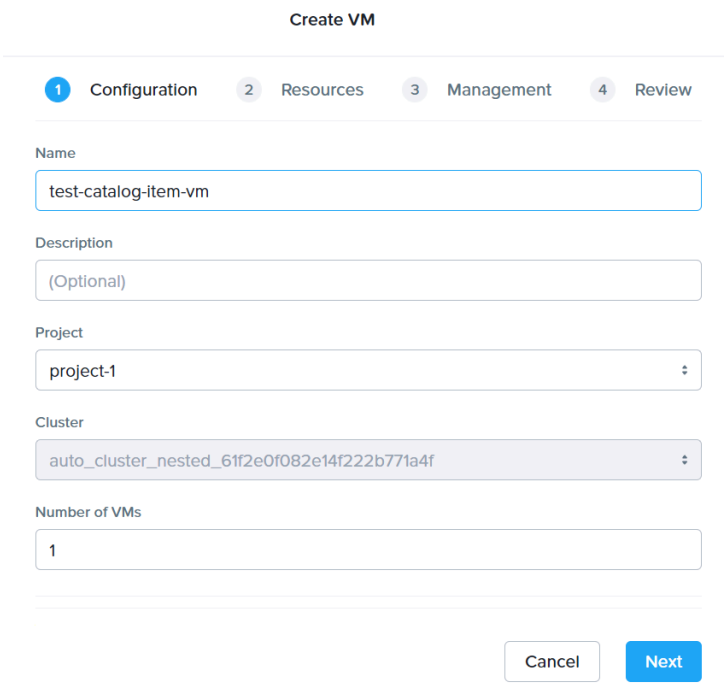


Figure 221: Create VM Window (Configuration)

8. In the **Resources** step, specify the following information.

   - **Disks**: Displays the disks and CD-ROMs attached to this VM.

     - If **VM Template** is selected as the source in **Catalog Type** field, the system displays a fixed list of devices. Select the device from which you want to boot the VM.
     - If **Image** is selected as the source in **Catalog Type** field, there are **+ New Disk** and **+ New CDROM** links above the list.

       - Click **+ New Disk** to add a disk. The system displays a new line at the bottom of the list. Specify the disk size and then click **Save** at the end of line to add the disk. The name and type field values are entered automatically.
       - Click **+ New CDROM** to add a CD-ROM. The system displays a new line at the bottom of the list. Click **Save** at the end of line to add the CD-ROM. All the field values are entered automatically.

       Repeat this action until you have added all the desired disks and CD-ROMs. When the list is complete, select the device from which you want to boot the VM.

9. In the **Resources** step, perform the following actions to configure the network interface for the VM:

   a. Click **Attach to Subnet**. The system displays the **Attach to Subnet** window.

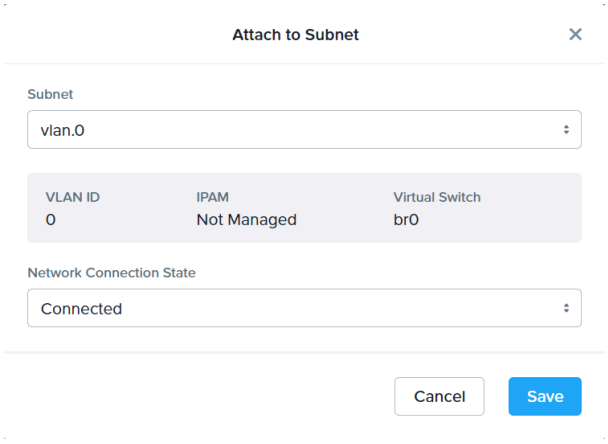


Figure 222: Attach to Subnet Window

   b. Select the target subnet from the **Subnet Name** dropdown menu.

      The list includes all defined networks. For more information, see Network Configuration for VM Interfaces information in *Prism Web Console Guide*.

   c. **VLAN ID**: This is a read-only field that displays the VLAN ID.

   d. **IPAM**: This is a read-only field that informs you if the subnet is IPAM managed or not.

   e. **Virtual Switch**: This is a read-only field that displays the name of the virtual switch associated with the subnet.

   f. Select the state for the network that you want it to operate in after VM creation in **Network Connection State** field. The options are `Connected` or `Disconnected`.:

   g. Click **Save** to create a network interface for the VM. The system returns to the **Create VM** window.

   h.

   Repeat this step to create additional network interfaces for the VM.

10. In the **Resources** step, perform the following action to specify boot configuration for the VM:

    Select one of the following firmware to boot the VM in **Boot Configuration** field:

    » **Legacy BIOS Mode**: Select legacy BIOS to boot the VM with legacy BIOS firmware.

    » **UEFI BIOS Mode**: Select UEFI to boot the VM with UEFI firmware. UEFI firmware supports larger hard drives, faster boot time, and provides more security features. For more information about UEFI firmware, see the UEFI Support for VM section in the *AHV Administration Guide*.

11. (Optional) In the **Management** step, perform the following action to assign a VM category.

    Enter the category name or select one from the **Categories**dropdown menu. The policies associated with the category value are assigned to the VM.

    This field acts like a search field; it provides a list of matching categories as you enter a string. Select the desired category value when you see it in the list. You can repeat this step for as many categories as desired.

12. In the **Management** step, perform the following actions for guest customization:

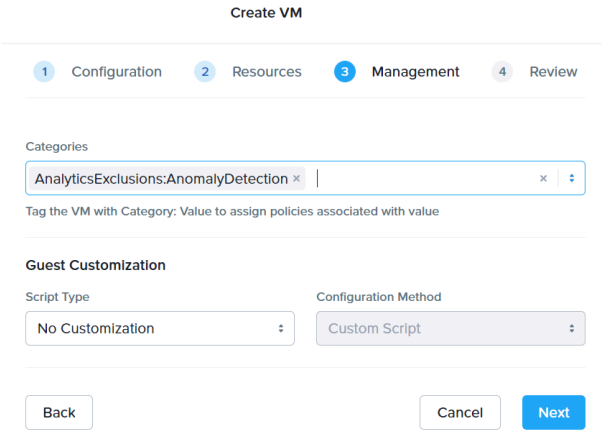


Figure 223: Create VM Window (Management)

- Select Cloud-init (for Linux VMs) or Sysprep (for Windows VMs) in the **Guest Customization** dropdown menu.
- Select the VM script customization type from the **Script Type** dropdown menu. The options are `No Customization`, `Sysprep(Windows)`, or `Cloud-init (Linux)`.
- Select the VM script customization method in the **Configuration Method** dropdown menu. This field is activated when the **Script Type** is either `Sysprep(Windows)` or `Cloud-init (Linux)`. The options are `Custom Script` or `Guided Script`.

The system displays the fields required to configure Cloud-init and Sysprep, such as options to specify a configuration script and the option to upload a script.

13. To specify a user data file (Linux VMs) or answer file (Windows VMs) the script for unattended provisioning, perform one of the following actions:

» If the file is available on your local computer, click **Upload Script**, and select and upload the file.

» Create or paste the contents of the file in the text box below the **Upload Script**.

> **Note:** The script type supports the following file formats.
>
> - Sysprep: XML
> - Cloud-init (Linux): YAML, JSON, or Shell.

14. In the **Review** step, Click **Create VM** to create the VM and close the **Create VM** window.
The system displays the new VM in the VMs Summary View on page 95.

Managing a VM (Self Service)

About this task

After you log in to Prism Central as a self-service administrator or a project member you can perform various actions on the VM to manage the VM configuration.

For information about all the actions, see Managing a VM through Prism Central (AHV) on page 134.

Note:

- The system allows you to perform only those actions for which you have permission.
- The available actions appear in bold; other actions are grayed out. The available actions depend on the current state of the VM and your permissions.

Procedure

You can perform these actions using any of the following methods:

- Select the target VM in the **List** tab of the **VMs** page, and choose the required action from the **Actions** dropdown menu. For more information, see VMs Summary View on page 95.
- Right-click on the target VM in the **List** tab of the **VMs** page, and select the required action from the **Actions** dropdown menu.
- Go to the details page of the target individual VM, and perform the required action. For more information, see VM Details View on page 108.

Assigning a VM to a Project Member

This section describes how to assign a VM to a project member.

About this task

A VM is assigned to a member within the scope of a particular project. You can assign a VM to only one project member.

Procedure

To assign a VM to a project member, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Compute & Storage** > **VMs** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default with all the VMs across registered clusters in **Nutanix** environment. For information about how to access the list of non-nutanix VMs managed by an external *vCenter*, see VMs Summary View on page 95.
3. Select the **Manage Ownership** action using any of the following methods:
   - Select the target VM checkbox in the **List** tab, and choose the **Manage Ownership** from the from the **Actions** dropdown menu.
   - Right-click on the target VM in the **List** tab, and select **Manage Ownership** from the displayed dropdown menu.
   - Select the **Manage Ownership** action from the **More** dropdown menu in VM Details View on page 108.

   The system displays the **Manage VM Ownership** window.

4. Enter the following information in the **Manage VM Ownership** window, and click **Save**.

   - **Project**: Select the target project from the dropdown menu.
   - **User**: Enter a user name. A list of matches appears as you enter a string; select the user name from the list when it appears.

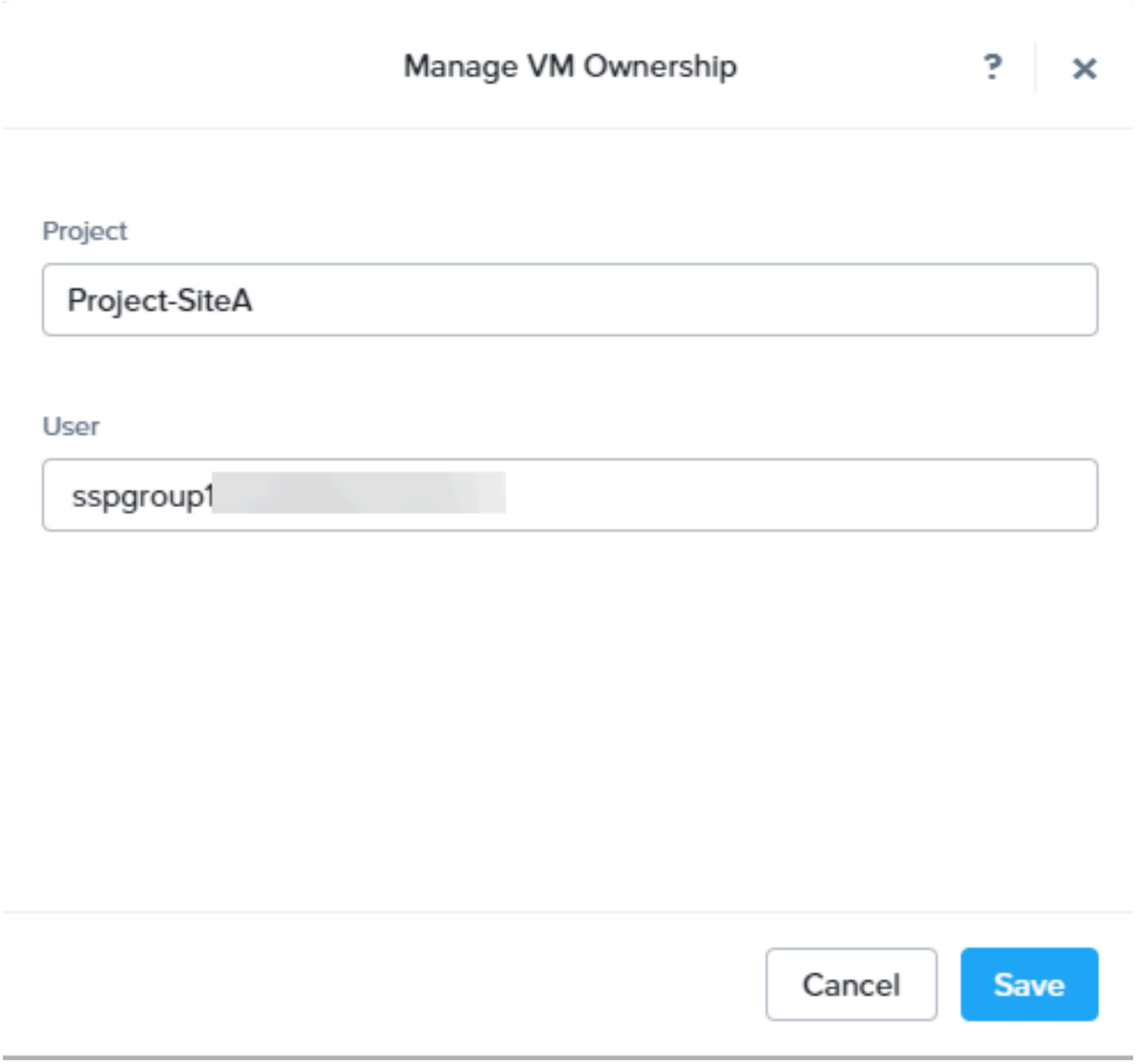


Figure 224: Assign VM to a Project Member

The selected VM is assigned to the project member.

ADDITIONAL OPERATIONS

After installing Prism Central, you can perform the following additional operations:

> **Note:** For information about how to install Prism Central, see Prism Central Installation or Upgrade on page 32.

- Log in and out through any supported browser. For more information, see Logging Into Prism Central on page 12 and Logging Out of Prism Central on page 570.
- Monitor the status of this Prism Central instance. For more information, see Managing Prism Central on page 531.
- Check version information. For more information, see Finding the Prism Central Version on page 557.
- Modify login page and automatic log off settings. For more information, see Configuring Prism Central UI Settings in *Prism Central Admin Center Guide*.
- Register clusters with this Prism Central instance. For more information, see Registering or Unregistering a Cluster with Prism Central on page 53.
- Expand Prism Central from a single VM to a multi-VM instance. For more information, see Expanding (Scale Out) Prism Central on page 559.
- Shutdown or Start Up a Prism Central VM. For more information, see Shutting Down or Starting Up Prism Central VM on page 565.
- Protect Prism Central with up to three AHV or ESXi clusters registered to it. For more information, see Backing up Prism Central on page 548.
- Recover Prism Central from Prism Element running on the registered AHV or ESXi cluster. For more information, see Restoring Prism Central (1-Click Recovery) on page 552.

Managing Prism Central

Prism Central consists of one or more VMs treated as a single instance that monitors and manages registered clusters. You can view information about the Prism Central VMs by clicking the gear icon in the main menu and then selecting **Prism Central Management** from the **Settings** menu (see Prism Central Settings (Infrastructure) on page 22). This displays the **Manage Prism Central** page.

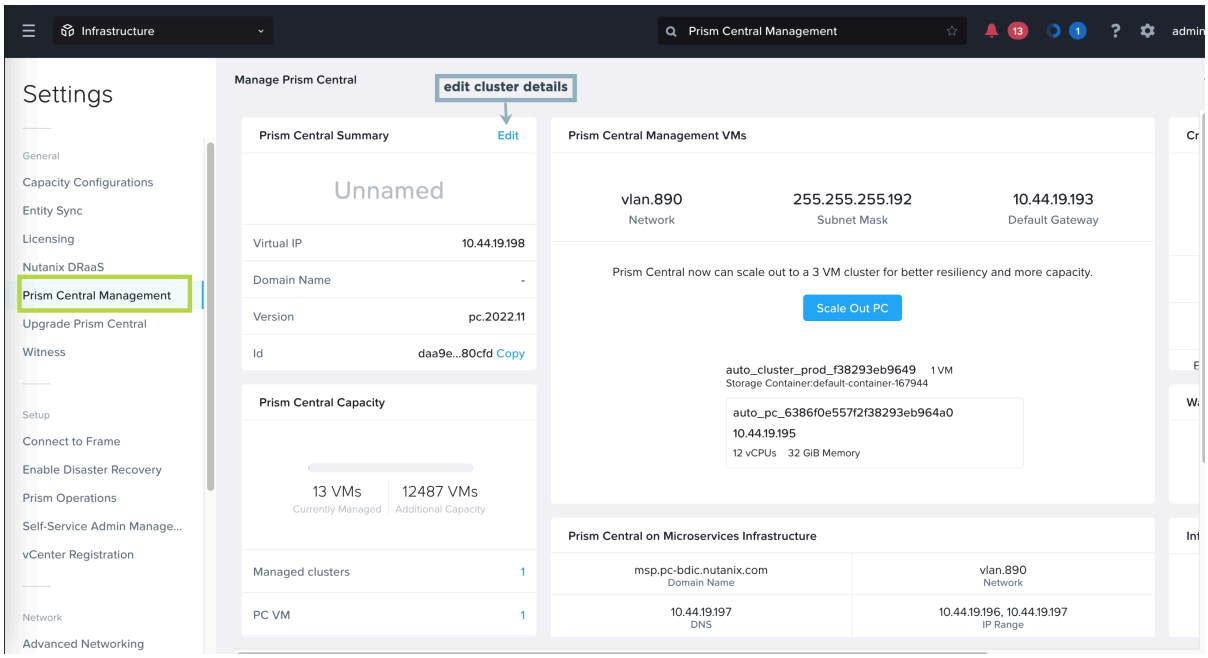


Figure 225: Manage Prism Central Page (1-VM instance)

The **Prism Central Management** page contains the following widgets:

- A **Prism Central Summary** widget on the upper left that displays fields for
  - Cluster name, which is **Unnamed** by default.
  - Domain name. A dash appears if a domain name is not specified.
  - Version. This is the Prism Central version number.
  - ID number. Click the copy link to copy the ID number so you can paste it elsewhere.
- A **Prism Central Capacity** widget on the lower left that displays fields for
  - Number of VMs monitored currently by this Prism Central instance.
  - Number of additional VMs (remaining capacity) this Prism Central instance can monitor.
  - Number of clusters registered to this Prism Central instance; click the number to display the clusters page. For more information, see Clusters Summary View on page 398.
  - Number of VMs that comprise this Prism Central instance; click the number to display the VMs page. For more information, see VMs Summary View on page 95.
- A **Prism Central VMs** widget in the middle that displays network address information (network name, subnet mask, and default gateway address) at the top and information below about each VM in the Prism Central instance (VM name and name of storage container in which it is located, IP address, number of vCPUs, and memory size). In addition, single VM instances include a **Scale Out PC** option to scale out this Prism Central instance . For more information, see Expanding (Scale Out) Prism Central on page 559.
- An **Alerts** widget on the right that displays a list of Prism Central-related alerts broken into Critical, Warning, and Info sections. For more information about alerts, see Prism Central Alerts and Events Reference Guide.

When the Prism Central instance consists of three VMs, the display changes slightly. The **Scale Out PC** option disappears, and a new **Add PCVM** option appears (top right). Prism Central instances are limited to a maximum of three VMs, but if you lose one of those VMs for any reason, you can add a replacement by clicking **Add PCVM**. The system displays the **Add PC VMs** page (similar to the **Scale Out PC** page) from which you can add the new VM.

> **Note:** Verify that the prerequisites in Expanding (Scale Out) Prism Central on page 559 are satisfied before adding a Prism Central VM.

To add or change the Prism Central domain name or virtual IP, click the **Edit** link in the **Prism Central Summary** widget. The **Cluster Details** window appears. Do the following:

1. In the **Cluster Name** field, enter a name for the cluster (default "Unnamed"). After naming the cluster, the field no longer appears when subsequently opening the window. Naming the cluster is optional.
2. In the **FQDN** field, enter the fully qualified domain name (FQDN) for the Prism Central cluster. This requires an administrator to configure the domain name in the DNS server to resolve to all the external IPs of the Prism Central VMs.
3. In the **Virtual IP** field, enter an IP address that will be used as a virtual IP for the cluster. This is relevant if you have a multi-VM Prism Central.

   > **Note:** FQDN and virtual IP settings in Prism Central are mutually exclusive. Do not enter a virtual IP in this field if you specified a FQDN in the previous field. A virtual IP provides resiliency but not load balancing. A FQDN does both.

4. When the fields are correct, click **Update** to save the changes and close the window.

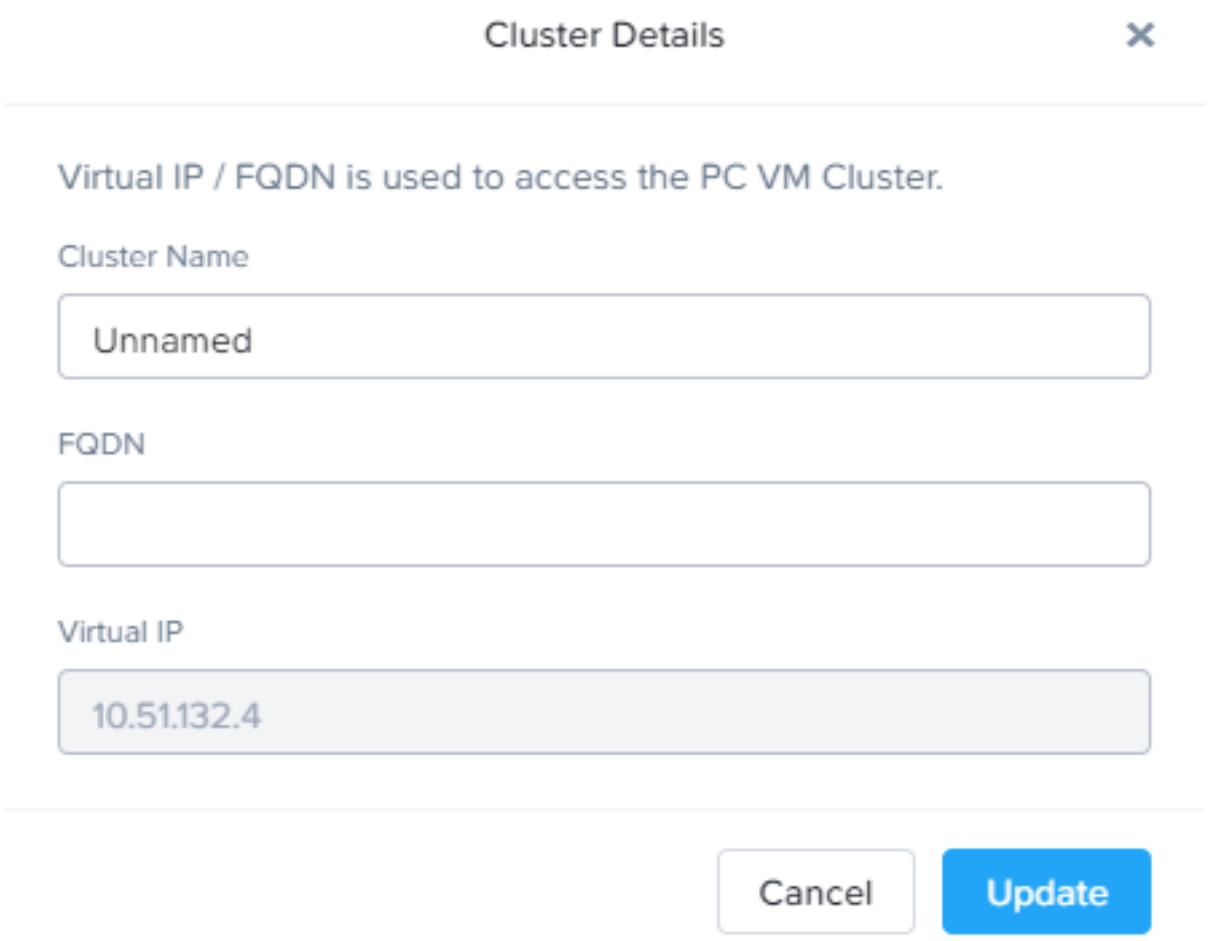


Figure 226: Cluster Details

Microservices Infrastructure

Microservices Infrastructure (sometimes referred to as MSP) provides a common framework and services to deploy the container-based services associated with Prism Central based components like Flow Virtual Networking and Objects. It deploys services like Identity and Access Management (IAM), Load Balancing (LB), and Virtual Private Networking (VPN). Such services are packaged in containers as microservices and the control plane for the microservices platform enables microservices infrastructure.

Microservices Infrastructure is enabled by default when you install or upgrade Prism Central to the *minimum supporting Prism Central version* or later, subject to some requirements.

> **Caution:** You cannot disable Microservices Infrastructure after it is enabled (whether by default or manually).

For information about upgrading Prism Central to a version that enables Microservices Infrastructure by default, see Prism Central Installation or Upgrade on page 32.

minimum supporting Prism Central version

The term *minimum supporting Prism Central version* in this section means Prism Central version that enables Microservices Infrastructure by default. The *minimum supporting Prism Central version* is pc.2022.9.

minimum supporting AOS versions

The term *minimum supporting AOS versions* in this section means AOS version that support deployment of a new Prism Central with default enabling of Microservices Infrastructure.

- The *minimum supporting AOS version*s for upgrading Prism Central are AOS 6.1.x, 6.5.x and 6.6.
- The *minimum supporting AOS version* for installing or deploying Prism Central is AOS 6.6.

minimum supporting versions

The term *minimum supporting versions* in this section means Prism Central version that enables Microservices Infrastructure by default and AOS version that supports default enabling of Microservices Infrastructure.

Hosting Prism Element Cluster (hosting PE cluster)

The Prism Element cluster that hosts a Prism Central (PC) instance is mentioned as hosting PE cluster. A PE cluster can host a number of PC instances. Such a hosting PE cluster is only registered to on PC instance and not to all the PC instances that it hosts.

Enabled by default

Microservices Infrastructure is enabled by default when you install or upgrade Prism Central to *minimum supporting Prism Central version* with *minimum supporting AOS version* and all the requirements are fulfilled.

Enable manually

When any or some of the requirements are not fulfilled in the clusters at the time you install or upgrade Prism Central (to *minimum supporting Prism Central version*), Microservices Infrastructure is not enabled by default. Manually enable Microservices Infrastructure after you ensure that the deployment complies with the requirements.

In certain cases, you may need to manually enable Microservices Infrastructure. For example, the Prism Central instance (upgrading to *minimum supporting Prism Central version*) is not registered to the hosting PE cluster. In such a case, the upgrade process fails to enable Microservices Infrastructure by default. You need to register the PC instance with the host PE cluster or establish trust between the PC instance and the hosting PE cluster. To establish trust between the hosting PE cluster, enable Microservices Infrastructure in the PC instance. The trust setup workflow is integrated in the workflow that enables Microservices Infrastructure.

Important: Upgrading Prism Central to a version that enables Microservices Infrastructure by default takes up to 40 minutes longer than a normal Prism Central upgrade.

Caution: If you have enabled Objects in the Prism Central managing the cluster, ensure that the Objects VMs are healthy and running when Prism Central upgrade process enables Microservices Infrastructure or you manually enable Microservices Infrastructure. If the Objects VMs are not healthy and running, the task for enabling Microservices Infrastructure might fail. To start the Objects VMs, see Starting the Objects VMs in the *Objects User Guide*.

Microservices Infrastructure Prerequisites and Considerations

The Prism Central and cluster deployment must fulfil some prerequisites for Microservices Infrastructure to be enabled by default. These prerequisites apply to manually enabling Microservices Infrastructure as well.

Make sure you meet the prerequisites listed before you enable the Microservices Infrastructure.

Note: Microservices Infrastructure uses several ports and protocols for its operations. For information about the ports that are used by Microservices Infrastructure and need to be open in the firewalls accordingly, see Ports and Protocols. Also, see the *Firewall Access to URLs* section in this topic for more information

about the ports, protocols, IP addresses, and subnets that Microservices Infrastructure uses and need to be managed in the firewalls.

On the Ports and Protocols page, select **Microservices Infrastructure** in the **Software Type** dropdown menu.

Microservices Infrastructure Prerequisites

- **Only if you have Prism Central Disaster Recovery (PC DR) enabled**

  If you have enabled PC DR in Prism Central, then do the following:

  1. Disable PC DR in Prism Central. For more information, see Disabling Prism Central Backup and Restore on page 555.

     Note: When you disable PC DR, you cannot enable it again after the Prism Central upgrade until you upgrade at least one Prism Element in the Prism Central cluster (Availability Zone) to *minimum supporting AOS version*.

  2. Upgrade Prism Central to *minimum supporting Prism Central version* (pc.2022.9 or later version that enables Microservices Infrastructure by default).
  3. Upgrade at least one Prism Element in the Prism Central cluster (Availability Zone) to *minimum supporting AOS version*.
  4. Enable Prism Central Disaster Recovery.

- **Minimum AOS Versions**
  - Nutanix supports fresh installation or deployment of Prism Central clusters with CMSP enabled by default on AOS versions. With a minimum Prism Central version of PC.2023.3, fresh installation or deployment is supported on AOS versions 6.5.3.x and later, and 6.6 and later.
  - To upgrade a PC instance to *minimum supporting Prism Central version*, the hosting PE cluster must run *minimum supporting AOS version* 6.5.x or 6.6. If the hosting PE cluster is not running a *minimum supporting AOS version*, then upgrade the AOS version to a *minimum supporting AOS version*.

    This requirement of *minimum supporting AOS version* is not applicable if the Prism Central instance is registered to the hosting PE cluster.
  - When upgrading a PC instance to *minimum supporting Prism Central version*:
    - If the PC instance is not registered to the hosting PE cluster, then register the PC instance to the hosting PE cluster and then run the upgrade workflow.
    - If the PC instance cannot be registered to the hosting PE cluster, enable Microservices Infrastructure to establish trust between the PC instance and the hosting PE cluster.
  - If the PC instance is not registered to the hosting PE cluster or Microservices Infrastructure is not enabled (with trust setup) on the PC instance, then the PC upgrade fails.

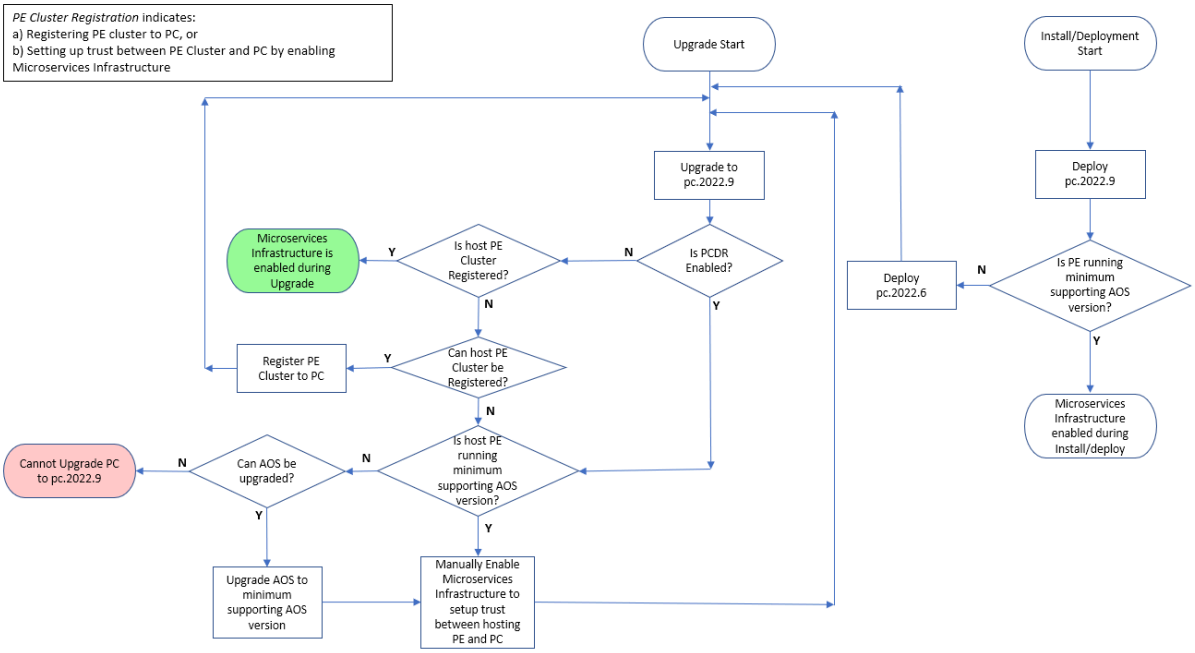


Figure 227: Upgrade/Install Minimum Supporting Prism Central - Process

- **Hypervisor**

  Clusters running AHV or ESXi only support Microservices Infrastructure. For ESXi clusters, enter your vCenter credentials (user name and password) and a network for deployment.

- **Prism Element Cluster and Prism Central IP Addresses**

  Ensure that you have configured virtual IP address and iSCSI data services IP address on the Prism Element that hosts Prism Central. For more information, see Modifying Cluster Details information in the *Prism Element Web Console Guide*).

  Note:

  - You can only change these IP addresses of Prism Central or Prism Element cluster after Microservices Infrastructure is enabled (whether enabled by default or manually enabled). You cannot remove any of these IP addresses. If you remove the current IP address, you must add another IP address before you save the configuration.
  - If a Prism Central instance (on which Microservices Infrastructure is enabled or will be enabled during upgrade) manages multiple Prism Element clusters, configure the iSCSI Data Service IP address on the Prism Element cluster hosting the Prism Central instance. Ensure that the iSCSI Data Service IP address is configured on the hosting Prism Element cluster before you install the or upgrade to the Prism Central that enables Microservices Infrastructure by default.

- **Cold Migration and CLI-based Prism Central Disaster Recovery Support**

  Cold Migration and CLI-based Prism Central Disaster Recovery of Prism Central VMs are not supported.

- **Name and NTP Servers**

  Ensure that you have configured at a minimum, one Name server and one NTP server in both the host Prism Element cluster and Prism Central.

  Warning: Do not remove the Name and NTP server configurations when Microservices Infrastructure is enabled.

- **Prism Central Memory**

  KB 8932 lists the Prism Central VM memory requirements. If your Prism Central VM resources do not meet the recommended amount, manually increase the memory.

- **Prism Central Registration and Trust Configuration**

  Ensure that you have registered the Prism Central instance to the Prism Element cluster. For more information, see Registering or Unregistering a Cluster with Prism Central on page 53.

  Note: If you unregister the Prism Element cluster from the Prism Central instance after you enable Microservices Infrastructure, then trust is automatically configured between the Prism Element cluster and the Prism Central instance. There is no impact to Prism Central. This behavior is supported with a

minimum Prism Central version of pc.2022.1 with Prism Element cluster running minimum AOS versions 6.1 or 6.5.

If you do not want to register the Prism Central instance with the Prism Element, then you must complete the trust configuration procedure to enable Microservices Infrastructure.

The workflow to enable Microservices Infrastructure includes steps to set up trust between the unregistered Prism Central and the Prism Element. For more information, see Configuring Trust Between Prism Central and Host Cluster.

Trust setup is supported on Prism Element cluster running minimum AOS versions 6.1 or 6.5 and Prism Central running minimum version pc.2022.1.

Note: Ensure that Prism Element cluster is running a minimum version of AOS 6.5 or AOS 6.6 before upgrading the AOS or Prism Central, for which trust is already set up.

If the Prism Element cluster is running a version of AOS older than *minimum supporting AOS version* and the Prism Central is not registered to the host Prism Element, then, before initiating the Prism Central upgrade, register Prism Central with the Prism Element cluster to enable Microservices Infrastructure by default.

If you upgrade the Prism Central version even though it is not registered to the Prism Element cluster, you need to enable Microservices Infrastructure manually after the upgrade is complete.

- **Default Private VXLAN**

  If the Prism Central that you want to upgrade is registered to the Prism Element cluster, then the upgrade process enables Microservices Infrastructure by default using private VXLAN network. If the private VXLAN is used, the ports 9440, 3205, and 3260 are required to be opened from Prism Central to all the Controller VM IP addresses and Controller VM virtual IP addresses in the clusters managed by the Prism Central, and the iSCSI Data Services IP (DSIP) addresses configured for the clusters managed by the Prism Central.

- **Firewall Access to URLs**

  Microservices infrastructure requires access to the following URLs:

  - *.docker.io
  - *.production.cloudflare.docker.com
  - *.nutanix.github.io

  Microservices Infrastructure requires the following IP address ranges or subnets open (in the firewall) to access the Prism Element Controller VM IP addresses, Controller VM virtual IP addresses, and the Prism Central VIP addresses of port 0, for ICMP traffic. Microservices Infrastructure also requires these IP address ranges or subnets to access the Prism Element Controller VM IP addresses and Controller VM virtual IP addresses, the Prism Element iSCSI Data Services IP (DSIP), and the Prism Central virtual IP addresses on ports 9440, 3205, and 3260. Therefore, ports 0, 3205, 3260 and 9440 must be open in the firewall for these IP address ranges or subnets to reach the all the Prism Element Controller VM IP addresses and Controller VM virtual IP addresses, Prism Element iSCSI Data Services IP (DSIP) address, and the Prism Central virtual IP addresses as required.

  The firewall must also allow any specific IP address range or subnets that are or might be configured as the private networks for Microservices infrastructure.

  Note: Do not use the IP addresses in the subnet 10.200.32.0/24 for operational purposes such as DNS or CVM networks. This prevents any negative impact and maintain seamless operations in the networking.

  For more information, see Ports and Protocols to see the access requirements for all the Nutanix software.

Table 152: Subnets for Microservices Infrastructure

Subnet	Purpose
10.100.0.0/16	Reserved for Kubernetes pod network
10.200.32.0/24	Reserved for Kubernetes services network

- **Prism Central Service Domain Name**.

  During the Microservices Infrastructure deployment process, a DNS service is deployed within Prism Central. This DNS service is utilized for discovery of available Prism Central Microservices.

  Ensure that the following caveats are considered when selecting a Prism Central Domain Name:

  - This value refers to the Prism Central Service Domain, and should not exactly match any FQDN currently in use, as this will complicate configuration of forwarding or redirection of queries.
  - The top-level domain cannot exceed 6 characters.
  - The top-level domain cannot end with "test".
  - The subdomain cannot exceed 16 characters.
  - The selected FQDN must contain at least three labels.
  - All labels within the FQDN must be at least two characters long.
  - If Prism Central has a proxy configuration, then ensure that the domain name is added to the allow-list with a * preceding the domain name (*.defined_domian_name).

    For example, if you use the domain name test.nutanix.com, then allow-list *.test.nutanix.com.

  The following are examples of valid domain configurations:

  - my.cluster.domain
  - my.test.cluster.test.domain
  - test.nutanix.com

  The following are examples of domains not supported:

  - my.cluster.test
  - my.cluster.domain.test

Limitations

The following limitations apply after Microservices Infrastructure is enabled (whether by default or manually):

- **Hypervisor Support**

  Nutanix does supports Microservices Infrastructure only on an on-premise Prism Central (PC) deployment hosted on an AOS cluster running AHV or ESXi. Clusters running other hypervisors are not supported.

- **Nutanix Move**

  Moving a Prism Central enabled with Microservices Infrastructure from ESXi host to AHV host using Nutanix Move is not supported.

- **Scale-out and Single PCVM deployments**

  Scaleout three-node Prism Central VMs deployment: Small, large, or x-large Prism Central VMs are supported. Reverting the deployment to a single Prism Central VM deployment is not supported.

  Single Prism Central VM deployment: Small, large, or x-large Prism Central VM are supported. You can expand a single PCVM deployment to a scaleout three-node PC deployment on a minimum Prism Central version of pc.2022.1 and minimum AOS version of 6.1. Expanding a single node Prism Central with Microservices Infrastructure is supported only on a minimum Prism Central version of pc.2022.1 and minimum AOS version of 6.1.

  For information on Prism Central scalability and the type of Prism Central deployments, see the *Prism Central Scalability* topic in the release notes for the Prism Central version to be installed.

- **IP Address Restrictions**

  Ensure that the IP addresses in subnet that you configure for Microservices Infrastructure do not conflict with the IP addresses in the management subnet.

  > **Note:** Do not use the IP addresses in the subnet 10.200.32.0/24 for operational purposes such as DNS or CVM network.

Trust Configuration and Manually Enable Microservices Infrastructure

The following two workflows are closely associated with each other:

- Trust setup between the Prism Central that Microservices Infrastructure is enabled in, and the Prism Element cluster that hosts the Prism Central.
- Manually enabling Microservices Infrastructure in Prism Central.

The trust configuration workflow occurs as the starting point in the workflow to manually enable microservices infrastructure (see Enabling Microservices Infrastructure Manually on page 543).

The steps to manually enable Microservices Infrastructure follows the trust configuration steps.

The starting point for the workflows is the **Enable Now** in the **Prism Central on Microservices Infrastructure** widget on the **Prism Central Management** page in **Prism Central Settings**page.

Configuring Trust Between Prism Central and Host Cluster

If Prism Central is not registered to the host cluster Prism Element, it must have a trust relationship setup with the Prism Element cluster.

Before you begin

Ensure that you have satisfied these requirements.

- The Prism Central instance is deployed with a minimum Prism Central version of pc.2022.1. The Prism Element cluster is deployed with a minimum AOS version of 6.1 (STS versions) or 6.5 (LTS versions). If required, upgrade the AOS version of the Prism Element cluster AOS version of the host cluster before you manually enable microservices infrastructure.
- Add the domain used (like *.prism-central.cluster.local) by the Prism Central to the allow-list.
- Ensure that requirements provided in Microservices Infrastructure Prerequisites and Considerations on page 535 are met.

About this task

If the Prism Central instance is not registered to the Prism Element cluster that hosts it, then after you click **Continue** on the **Important Information** window, Prism Central displays the **Enable Microservices Infrastructure** window with the trust configuration parameters.

Procedure

1. Go to the **Prism Central Management** page (see Managing Prism Central on page 531).
2. In the **Prism Central on Microservices Infrastructure** widget, click **Enable Now**.

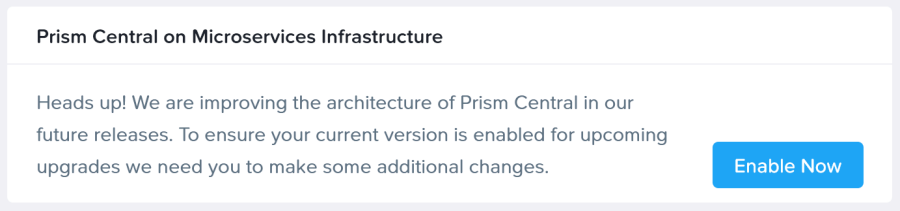


Figure 228: Prism Central on Microservices Infrastructure widget

3. Read the information and then click **Continue**.
4. On the **Enable Microservices Infrastructure** window, provide the following information:
   - Virtual IP Address or FQDN of the host Prism Element.
   - Admin user name used to log on to the host Prism Element.
   - Password for the admin user name provided to log on to the host Prism Element.

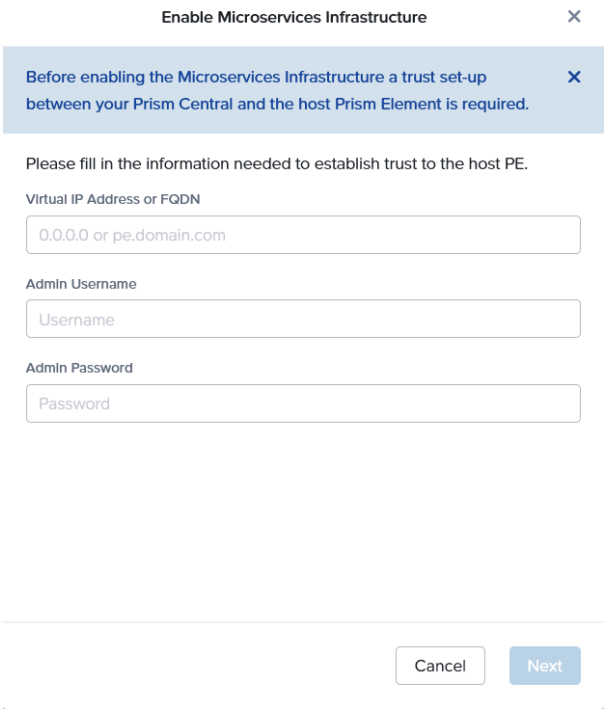


Figure 229: Enable Microservices Infrastructure - Trust setup

5. Click **Next**.
   The **Enable Microservices Infrastructure** main dialog box provides the parameters to enable microservices infrastructure.

6. Complete manually enabling microservices infrastructure. See Enabling Microservices Infrastructure Manually on page 543.

Enabling Microservices Infrastructure Manually

The microservices infrastructure enabled by default. This topic provides the procedure to enable microservices infrastructure manually.

Before you begin

Ensure that all the requirements provided in Microservices Infrastructure Prerequisites and Considerations on page 535 are fulfilled before enabling the microservices infrastructure.

If the Prism Central instance is not registered to the Prism Element cluster hosting the Prism Central, then set up trust between the Prism Central and the Prism Central cluster by completing the steps provided in Configuring Trust Between Prism Central and Host Cluster on page 541.

> **Caution:** If you have enabled Objects in the Prism Central managing the cluster, ensure that the Objects VMs are healthy and running when Prism Central upgrade process enables Microservices Infrastructure or you manually enable Microservices Infrastructure. If the Objects VMs are not healthy and running, the task for enabling Microservices Infrastructure might fail. To start the Objects VMs, see Starting the Objects VMs in the *Objects User Guide*.

About this task

To enable the microservices infrastructure, do the following:

Procedure

1. Read the information, and then click **Continue**.

   > **Important:** If the Prism Central deployment is not registered with the Prism Element, then the **Enable Microservices Infrastructure** window provides the parameters for establishing trust between Prism Central and Prism Element that hosts the Prism Central instance.
   >
   > Complete the steps mentioned in Configuring Trust Between Prism Central and Host Cluster on page 541. Then, the main **Enable Microservices Infrastructure** dialog box is displayed.

   The main **Enable Microservices Infrastructure** dialog box is also displayed if the Prism Central instance is already registered with the host Prism Element.

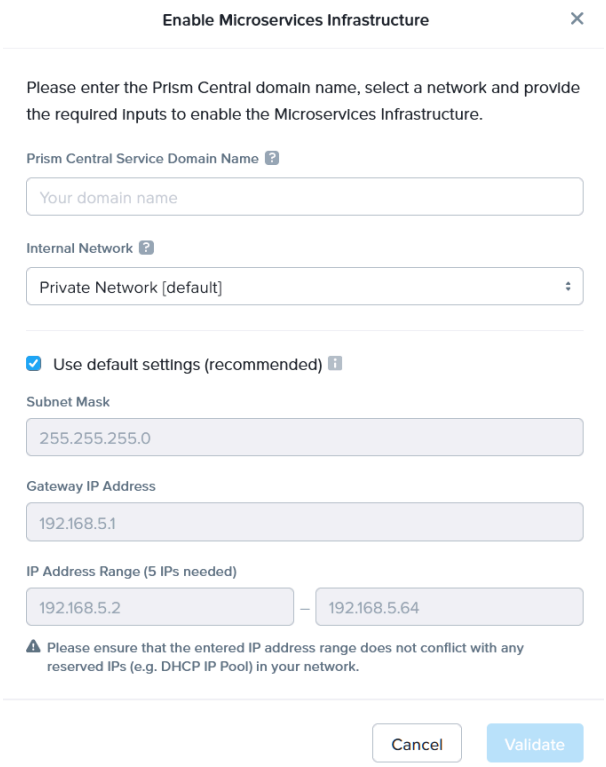


Figure 230: Enable Microservices Infrastructure

2. Provide the following information in the main **Enable Microservices Infrastructure** box.

   - **Prism Central Service Domain Name**: Enter a domain name for the service. See **Prism Central Service Domain Name** restrictions in Microservices Infrastructure Prerequisites and Considerations on page 535.
   - **Internal Network**: Select the network to use for Prism Central micro services communication from the dropdown list.

     The default selection **Private Network [default]** is a pre-configured private VxLAN network. Instead, if you want microservices infrastructure to use a different network, you can select the network (managed or unmanaged) from the drop-down list. If the network you want microservices

infrastructure to use does not appear in the list, you must first configure it. For more information, see Network Configuration on page 346.

- The **Use default settings (recommended)** checkbox is available only when you have retained the default selection (**Private Network [default]**) for **Internal Network** in the preceding step. This checkbox is checked by default. Do one of the following:

  - Retain the check mark for the **Use default settings (recommended)** checkbox and click **Validate**. (Go to step 3 on page 545.)

    Retaining the check mark for the **Use default settings (recommended)** checkbox allows Prism Central to use the **Private Network [default]** with the default values for **Subnet Mask**, **Gateway IP Address** and **IP Address Range**.

  - Clear the **Use default settings (recommended)** checkbox, if you want Prism Central to use the **Private Network [default]** setting with specific (non-default or custom) values for **Subnet Mask**, **Gateway IP Address** and **IP Address Range**.

Configure the **Internal Network** for microservices infrastructure if you did one of the following:

- Selected a managed or unmanaged network other than **Private Network [default]** for **Internal Network**.

  If you selected a managed network, the values in the **Subnet Mask**, **Gateway IP Address** and **IP Address Range** fields are already configured. If you selected an unmanaged network, you must enter the necessary values in the respective fields.

- Cleared the **Use default settings (recommended)** checkbox with the **Private Network [default]** selection for **Internal Network**.

Enter the values for the following parameters to configure **Internal Network**:

Parameter	Description
Subnet Mask	Enter the subnet mask.
Gateway IP Address	Enter the IP address for the gateway.
IP Address Range	Enter a range of IP addresses that the network can use. Enter a range of at least 10 available (unreserved) addresses for a 3-VM (scale out) Prism Central instance or at least 5 addresses for a 1-VM Prism Central instance. The addresses must be consecutive or sequential. For a managed network, the range of addresses for microservices infrastructure must be outside the range of reserved IP addresses (for example, DHCP IP Pool) in the selected network.

3. After you check that the values entered for all the fields are correct, click **Validate**.
   The system checks the settings. When the settings are confirmed, a Validation was successful message appears and the **Validate** changes to **Enable**.

4. Click **Enable**.
   The process begins, which takes about 45 minutes. You can monitor progress from the tasks dashboard (see Tasks View on page 451). When the microservices infrastructure is enabled, the contents of the enable box in the **Manage Prism Central** page changes to display configuration information such as the domain name, the used IP addresses, and the service domain's DNS IP address.

What to do next

After the tasks are completed, including the **IAM Migration & Bootstrap** task, log out of Prism Central. Wait at least 15 minutes before logging on to Prism Central.

Enabling Microservices Infrastructure (dark site)

Manually enabling the Microservices Infrastructure when there is no Internet access (dark site) requires some extra steps from the standard procedure.

About this task

To enable the Microservices Infrastructure at a dark site, do the following:

Procedure

1. From a device that has public Internet access, log on to the Nutanix support portal, select **Downloads** > **LCM** from the entity menu (hamburger icon), and then download the LCM Dark Site Bundle tar file.
2. Set up a local web server, upload LCM Dark Site Bundle to the server, and extract the files in a directory in the base of the web server.

   For more information, see the Local Web Server Setup section in the *Life Cycle Manager Guide*. Set the following file types in the LCM web server when you are using Windows Web Server: .json, .xz, .qcow2, .sign, .gz

   For the mime types associated with the above file types, see the Local Web Server Setup section in the *Life Cycle Manager Guide*.
3. In the Nutanix support portal **Downloads** page, select **Microservices Platform (MSP)**, download the **Upgrade (Darksite)** bundle to the web server base directory you used in step 2, and extract the files.

   Note: With a minimum Prism Central version of pc.2023.4, to upgrade Microservices Infrastructure in a darksite, download and use the **Prism Central LCM Bundle**. Do not download Microservices Infrastructure **Upgrade (Darksite)** bundle for dark site upgrades.
4. Now follow the standard procedure for enabling the Microservices Infrastructure through Prism Central (see Enabling Microservices Infrastructure Manually on page 543).

Prism Central Backup and Restore

Prism Central Backup and Restore (PCBR) is a robust solution for protecting your Prism Central instances (including scale-out configurations) against unforeseen events such as natural disasters, network outages, or power failures. The feature enables you with the following automated backup solutions to ensure the resilience of your instances and service configurations across both on-prem environments and public cloud platforms such as AWS.

Continuous Backup

: Enables almost real-time backup of your Prism Central instances (and various service configurations within it) to up to three AHV or ESXi clusters registered to the same on-prem Prism Central, ensuring minimal data loss and swift recovery after disruptions.

Point in Time Backup

: Enables scheduled backups of your Prism Central instances (and various service configurations within it) to one S3 object-based storage (bucket) on AWS, allowing for recovery to specific points in time and protection against ransomware attacks and datacenter failures.

You can configure continuous or point-in-time backup for your deployment (and various service configurations within it) in the following combinations to up to four locations. You can also configure continuous and point-in-time backup together for your deployment.

Backup Type	Number of Backup Targets Supported
On-prem	Upto three AHV or ESXi clusters
Cloud	One S3 object-based storage. An S3 bucket can be used to back up multiple Prism Central deployments.
Hybrid (On-prem + Cloud)	A combination of up to three AHV or ESXi clusters and one S3 object-based storage.

The 1-Click recovery restores the important service configurations along with the entire Prism Central deployment, minimizing downtime and operational impact.

The following services can be backed up and data associated with them recovered.

- Nutanix Disaster Recovery (formerly known as Leap)
- Flow Network Security (formerly known as Flow Microsegmentation)
- Networking (such as AHV-based VLAN and Virtual Switch configurations)
- Flow Virtual Networking (Virtual Private Clouds (VPCs), and virtual networks using Networking Controller (ANC) and Networking Gateway)
- Intelligent Operations
- VM management
- Cluster management
- Categories
- Licensing
- Reporting templates

Although the following services continue to run, their data is not backed up and therefore not recoverable.

- NCM Self-Service (formerly known as Calm)

  Important: To do a planned restore of a NCM Self-Service-enabled Prism Central instance to a recovery cluster, perform the following steps.

  1. Manually backup the NCM Self-Service-related entities in Prism Central at the primary cluster. For more information, see Backing up Calm Data in *Calm Administration and Operations Guide*.
  2. Restore Prism Central in the recovery cluster.

     Caution: Before you restore the Prism Central instance in a recovery cluster, ensure the Prism Central backup is synched at least once with the recovery cluster you select to restore the Prism Central instance.

  3. Restore the NCM Self-Service-related in the new Prism Central instance at the recovery cluster. For more information, see Restoring Calm Data in *Calm Administration and Operations Guide*.

- LCM
- Nutanix Kubernetes Engine (formerly known as Karbon)

- Objects
- Files
- Catalog
- Images
- VM templates

> **Note:** Migration of Prism Central VMs using vMotion is not supported.

For Nutanix Disaster Recovery Jobs (RPJs) in progress, see this Note. Metrics older than 90 days also cannot recovered.

This document walks you through the GUI-based PCBR solution.

Implementation Considerations

Unsupported Backup Methods

Protecting your Prism Central instances using protection domain-based disaster recovery, protection policy-based workflows, third-party backup software, or any unsupported methods renders those instances unrecoverable.

Backup Suspension During Upgrades

For enabled Prism Central Backup and Restore (PCBR), the system pauses the backup of Prism Central configuration data when Prism Central upgrade is initiated. The backup resumes after the upgrade process is complete.

Testing

Nutanix strongly recommends against testing 1-Click PCBR. It must be manually triggered only when the Prism Central instance becomes unavailable due to an unplanned event like a natural calamity, network outage, or power failure.

Backing up Prism Central

You can protect or back up a Prism Central instance to its registered Nutanix clusters, AWS S3 object-based storage, or Nutanix clusters and AWS S3 object-based storage together that fulfill the requirements. The system enables you to back up a Prism Central instance to at most three AHV or ESXi clusters and one S3 object-based storage. Clusters running Hyper-V are not supported.

Before you begin

Ensure that the following requirements are met before protecting or backing up the Prism Central instance.

- To back up a Prism Central instance to AWS S3 object-based storage, which is called point-in-time backup in the Prism Central web console, the Prism Central instance must run on a minimum version of pc. 2024.1 or later.

  > **Note:** All current versions of Prism Central support backing up to Nutanix clusters, which is called continuous backup in the Prism Central web console.

- The Prism Central instance must have an NTP configuration to synchronize time between the Prism Central instance and the registered clusters. For more information on NTP configuration, see Configuring NTP Servers (Prism Central) in the *Prism Central Admin Center Guide*.
- The Nutanix clusters used to back up the Prism Central instance must be running a minimum version of AOS 6.0 or later.

- For continuous backup, at least one cluster used to back up the Prism Central instance must be running AOS 6.5.3.1 or later because the Prism Central instance can be restored only on clusters running AOS 6.5.3.1 or later. For more information, see Restoring Prism Central (1-Click Recovery) on page 552.
- For point-in-time backup, at least one cluster used to back up the Prism Central instance must be running AOS 6.8 or later because the Prism Central instance can be restored only on clusters running AOS 6.8 or later. For more information on the supported AOS versions, see Compatibility and Interoperability Matrix.
- To configure an AWS bucket for point-in-time backup, perform the operations noted in Amazon S3 Object Lifecycle and Policies on page 550.
- The Nutanix clusters used to back up the Prism Central instance must be registered to Prism Central instance you want to back up.
- The Nutanix cluster hosting the Prism Central instance must be registered to the Prism Central instance you want to back up.

  If the cluster is not registered to the Prism Central instance, enabling Prism Central Backup and Restore fails.

About this task

To protect or back up a Prism Central instance, perform the following steps.

Procedure

1. Log in to the Prism Central web console.
2. Click the Settings icon and navigate to **General** > **Prism Central Management** from the **Settings** menu. For more information, see Prism Central Settings (Infrastructure).
   The **Prism Central Management** page appears. This page provides information about this Prism Central instance.

   > **Tip:** The **Whats's New** page appears when you go to the **Prism Central Management** page for the first time.

3. Select one of the following in the **Prism Central Backup and Restore** widget.

   » **Continuous Backup**. To enable real-time backup of your Prism Central instances (and various service configurations within it) to the clusters registered to the same on-prem Prism Central, ensuring minimal data loss and swift recovery after disruptions.

   > **Note:** The RPO and RTO for recovery from a continuous backup is 5 minutes and 90 minutes, respectively. You can recover the Prism Central instance only from the latest backup.

   » **Point-in-Time Backup**. To enable scheduled backups of your Prism Central instances (and various service configurations within it) to S3 object-based storage on AWS, allowing for recovery to specific points in time.

   > **Note:** The RPO and RTO for recovery from a point-in-time backup is 2 hours and 90 minutes, respectively. You can recover the Prism Central instance from any available restore points.

4. Click **Protect Now**.

   > **Note:** The **Protect Now** option is available only when one or more clusters are registered to the Prism Central instance, or you want to configure S3 buckets on AWS.

   The **Protect Prism Central** window appears. This window shows the services data that will be backed up and those that will not be backed up.

5. Click **Continue**, and do one of the following according to the backup type you selected in step 3.

   - For continuous backup, select one or more clusters to back up the Prism Central instance.

     > **Note:** You can select a maximum of 3 clusters.

   - For point-in-time backup, specify the following details in the **Protect Prism Central** window.

     > **Note:** Perform the operations noted in Amazon S3 Object Lifecycle and Policies on page 550 before you proceed to specify the following details.

     - **AWS Region Name**. Enter an AWS region name. For more information, see *AWS documentation*.
     - **AWS Bucket Name**. Enter a bucket name. For more information, see *AWS documentation*.
     - (Optional for NC2 environments) **Access Key**. Enter your access key.
     - (Optional for NC2 environments) **Secret Access Key**. Enter your secret access key.

     > **Note:** The first restore point is created immediately, and then restore points are created every 2 Hours (RPO). Up to 30 days of restore points are supported for restoring the Prism Central instance.

6. Click **Proceed**.
   The system synchronizes Prism Central configuration data to the selected clusters or S3 object-based storage. While the configuration data is synchronizing, the **Status** is shown Sync in Progress. The **Status** turns to Synced when the configuration data is synchronized. For continuous backup, the first backup creation on the selected clusters takes at least 30 minutes. After the first backup, the system synchronizes Prism Central configuration data with the selected clusters every 30 minutes. For point-in-time backup, the process of taking the first backup starts immediately when you submit the S3 bucket details and takes at least 15 minutes. After the first backup, the system synchronizes Prism Central configuration data with the S3 bucket every 2 hours.

7. (optional) If you want to back up the Prism Central instance to more Nutanix clusters or S3 buckets, click **+ Add Backup** in the **Prism Central Backup and Restore** widget.
   However, the number of entities backing up the Prism Central instance must be at most four— to three on-prem clusters and one S3 object-based storage. You can use a cluster only once to back up the same Prism Central instance.

8. (optional) If you want to remove a Nutanix cluster or a bucket from backing up the Prism Central instance, click **Remove** in front of the cluster, type Remove (not case sensitive), and click **Remove**.

Amazon S3 Object Lifecycle and Policies

About this task

When you have created an Amazon S3 bucket in a suitable region to store the backup data, you must perform the following configurations for it.

Procedure

1. Enable versioning.

   A version of the file is created each time the system writes the seed data file on the new key path to the bucket. The previous version becomes noncurrent, and the currently written file becomes current. For more information on the current and noncurrent items and how to enable bucket versioning, see *Amazon S3 documentation*)

2. Enable Object lock for objects to enable WORM (write-once-read-multiple) configuration and to create point-in-time snapshots of Prism Central configuration.

   Configure Object lock when you create a bucket. To ensure that the backup data put into the bucket is retained for some time and deleted at that time, the system retains the data for 31 days. Configure the retention mode as Governance. For more information on how to enable object lock, see *Amazon S3 documentation*.

3. Configure an object lifecycle rule to auto-delete older backup data.

   To enable the automatic deletion of objects after a certain time as they become stale, configure an object lifecycle rule from the Amazon S3 console that applies to all objects in the bucket. For more information on how to configure a lifecycle rule, see *Amazon S3 documentation*.

   > **Note:** Configure a maximum time of 31 days for deleting noncurrent objects. Nutanix recommends setting the deletion of expired object delete markers, the expiration of the current version of objects, and the deletion of incomplete multipart uploads to a day.

   The rule you created is listed as the following.

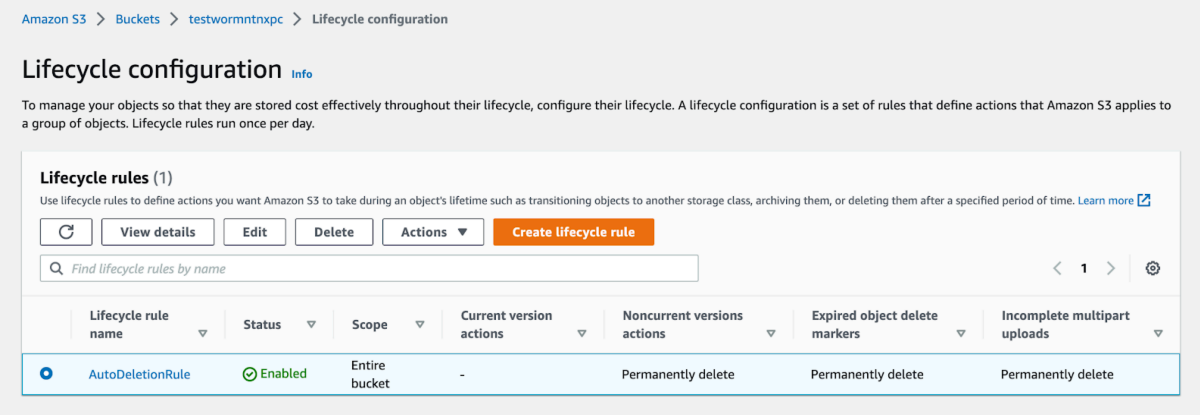


Figure 231: Lifecycle Configuration

4. By default, public access is blocked for buckets in the AWS console. To enable access, log on as the root user of the AWS account and navigate to the IAM service.

   For more information, see *AWS S3 documentation*.

5. Create a user from the Amazon S3 console. Do not provide console access to this user since an access key is to be generated for this user to enable programmatic access from outside of AWS.

   a. When the user is created, create a policy with an identifiable name and paste the following JSON in the text box.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetObjectVersion",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion"
            ],
            "Resource": "arn:aws:s3:::Bucket_name"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:GetLifecycleConfiguration"
            ],
            "Resource": "arn:aws:s3:::Bucket_name"
        }
    ]
}
```

Replace *Bucket_name* with the name of your Amazon S3 bucket.

b. Find the policy created in the previous step and attach it with the user you created in step 6.

c. Create an access key with a descriptive name and then select **Application running outside AWS** from the AWS console.

d. Save the access key. Nutanix recommends downloading the CSV file. The same key needs to be input on the Prism Central web console while configuring this S3 bucket as the target endpoint for storing your Prism Central configuration backups.

For more information, see *AWS S3 documentation*.

Restoring Prism Central (1-Click Recovery)

If you have protected or backed up your Prism Central instance, you can use an AHV or ESXi cluster to restore the Prism Central instance. For continuous backups (backups stored on on-prem Nutanix clusters), you can recover the Prism Central instance from a registered cluster only. For point-in-time backups (backups stored on Amazon S3), you can recover the instance on a registered cluster, or you can recover it on a cluster that is not registered with any Prism Central instance.

Before you begin

Ensure that the Nutanix cluster you use to restore the Prism Central instance meets the following requirements.

- Registered to the protected Prism Central instance.
- To restore from a continuous backup, the cluster must run AOS 6.5.3.1 or later. For more information on the supported AOS versions, see Compatibility and Interoperability Matrix.
- To restore from a point-in-time backup, the cluster must run AOS 6.8 or later. For more information on the supported AOS versions, see Compatibility and Interoperability Matrix.
- Configured with ISCSI data service IP address for efficient recovery of Nutanix Disaster Recovery or NCM Self-Service configurations.

> **Note:** The Nutanix cluster takes about 10 minutes to stabilize the Prism Central instance after the recovery task on the Prism Element web console is displayed as complete. This is because Microservices Infrastructure causes the system to rotate certificates after the restoration and restart services like IAM and Flow Virtual Networking.

About this task

To restore a Prism Central instance, perform the following steps.

Procedure

1. Log in to any Prism Element web console registered to the Prism Central instance you want to restore

   The Prism Element dashboard shows the Prism Central widget, which contains Prism Central information (IP address and connection status). If this is a fresh Prism Element that you created and you have yet to register to a Prism Central instance, it won't appear. Instead, you see the **Register or Deploy Prism Central**.

2. Click the Settings icon and navigate to **Data Resiliency** > **Restore Prism Central** from the **Settings** menu. For more information, see Settings Menu in the `Prism Element Web Console Guide`.
   The **Restore Prism Central** page appears. This page provides you options to restore the Prism Central instance from Prism Element cluster or S3-compatible object storage.

3. Select from where you want to restore the Prism Central instance and click **Restore Now**.

   > **Note:** If you configured only continuous backup, the **Restore Now** option is available only when Prism Central is in a disconnected state (shown **Disconnected** in the Prism Element web console.

   The **Restore Prism Central** window appears. This window shows the service data that will be recovered and those that will not.

4. Click **Continue** and specify the following information according to the source from where you want to recover.

   » To recover from a continuous backup, see Restore Prism Central-Field Information for Continuous Backup on page 554.

   » To recover from a point-in-time backup, see Restore Prism Central-Field Information for S3-based Object Storage on page 554.

   The Prism Central instance is restored in 60 to 90 minutes, depending on the configuration data of the hosts. The restoration involves the deployment of Prism Central and the restoration of its configuration data from the backup, which could take anywhere between 60 and 120 minutes, depending on the size of the data. The restored Prism Central instance takes an additional 30 to 40 minutes to show all the guest VMs, disks, and metrics. Wait to perform any actions on the restored Prism Central instance until all the recovery tasks are completed on the cluster. You can see the restoration status and the related processes in the **Tasks** window.

What to do next

Consider the following after the Prism Central restoration.

- Use the newly restored Prism Central instance only.

  If the old Prism Central instance becomes available, shut down or delete the old instance because running the old Prism Central instance can cause data corruption.

  > **Note:** If the Prism Central restoration fails, contact Nutanix Support. Do not bring up the old Prism Central instance.

- Reset the credentials.

  Prism Central restores with the default credentials. Nutanix recommends changing the default credentials. For information about changing the default credentials, see Logging Into Prism Central in the *Prism Central Infrastructure Guide*.

  > **Note:** If you have both S3-compatible object storage and Nutanix on-prem clusters configured as backup targets and you recovered the Prism Central instance through an on-prem cluster. In that case, you must reconfigure the s3 bucket credentials after the recovery through the **Prism Central Backup and Restore** widget in **Settings** > **Prism Central Management**.

  > **Note:** widget on the Prism Central Management page.

- Reconfigure the proxy server. For information on how to configure the HTTP proxy through the Prism Central web console, see Configuring an HTTP Proxy in the *Prism Central Admin Center Guide*

  If the old Prism Central instance had a proxy server, reconfigure the proxy server so that the recovered Prism Central instance maps to the correct IP address.

- Reconfigure the fully qualified domain name (FQDN).

  If the old Prism Central instance had an FQDN, reconfigure the FQDN so that the recovered Prism Central instance maps to the correct IP address.

- Recovery Plan Jobs (RPJ) in progress: Perform the steps mentioned in KB-10962.

  If the old Prism Central instance had a failover task running (Nutanix Disaster Recovery) or protection policy with guest VMs protected with synchronous replication schedule, perform the steps mentioned in KB 10962 to ensure that all the failover tasks stuck in the running state are terminated and a script is executed for efficient recovery of the Prism Central instance.

Restore Prism Central-Field Information for Continuous Backup

Procedure

1. Select the cluster where you want to restore the Prism Central instance.
2. Verify the version of Prism Central instance that would restore on the selected cluster.
3. Select the network where you want to restore and install Prism Central instances.
   The **Subnet Mask**, **Gateway**, and **DNS Address(s)** fields show the relevant information associated with the selected network.
4. Enter details (name, IP address) for the Prism Central instance you want to restore and click **Save**.
5. Review the summary and click **Recover**.

Restore Prism Central-Field Information for S3-based Object Storage

Procedure

1. In **Connect** tab, specify the following details, and click **Next**.
   a. **AWS Region Name**. Enter an AWS region name. For more information, see `AWS documentation`.
   a. **AWS Bucket Name**. Enter a bucket name. For more information, see `AWS documentation`.
   b. (Optional for NC2 environments) **Access Key**. Enter your access key.
   c. (Optional for NC2 environments) **Secret Access Key**. Enter your secret access key.

2. In **Source** tab, select the Prism Central backup you want to restore, and click **Next**.
   An S3 bucket can be used to back up multiple Prism Central instances. The instances are listed as the `PC_<IP_ADDRESS>` or the FQDN if configured.
3. In **Restore Point** tab, specify the date for the point-in-time backup, and then select one of the available restore points to restore the Prism Central instance. Click **Next**.
4. In **Installation** tab, verify the cluster IP address where Prism Central instance was hosted originally and the version of your instance, and click **Next**.
5. In **Configuration** tab, specify the networking details.

   Note: If you are restoring the Prism Central instance from the same cluster (Prism Element web console) where the Prism Central instance was hosted, details like **vLAN**, **Subnet Mask**, **Gateway IP**, **DNS Address(es)**, **NTP Address(es)**, **Container**, and **Virtual IP** are populated automatically. You must configure these details if you are trying to restore the Prism Central instance from a different AZ or a cluster. Click **Next**.
6. In the **Microservices** tab, specify the Prism Central service domain name, internal network, and the required input to enable Microservices Infrastructure (CMSP). Nutanix recommends using the default settings for **Subnet Mask**, **Gateway IP Address**, and **IP Address Range**.

   Note: Ensure that the IP address range does not conflict with the reserved DHCP IP address pool in your network.
7. In **Summary** tab, review the information you configured in the previous steps, and click **Restore**.

Disabling Prism Central Backup and Restore

About this task

The following procedure to disable Prism Central Backup and Restore is the same for continuous and point-in-time backup types.

Caution: You can enable Prism Central Backup and Restore only if any one of the Nutanix clusters (Prism Element) registered to the Prism Central instance is running minimum AOS version 6.5.3.1 . For point-in-time backups, you can enable Prism Central Backup and Restore only if any one of the clusters registered to the Prism Central instance is running a minimum AOS version 6.8.

Procedure

1. Log in to the Prism Central web console.`
2. Click the Settings icon and navigate to **General** > **Prism Central Management** from the **Settings** menu. For more information, see Prism Central Settings (Infrastructure) on page 22).
   The **Manage Prism Central** page appears. This page provides information about this Prism Central deployment.
3. Click **Remove** for the target clusters listed in the **Nutanix Disaster Recovery** widget.

What to do next

When Prism Central Backup and Restore is disabled, the Prism Central resources are unprotected. To ensure recovery of the Prism Central instance in case of a disaster, enable it again after completing the required tasks that require Prism Central Backup and Restore to be disabled.

Intelligent Operations

Intelligent Operations allows you to run your IT operations efficiently using intelligent operational features that include:

- Cluster activity analysis.
- Application discovery in a cluster.
- Application monitoring in a cluster.
- Resource capacity and usage planning.
- Task automation using playbooks.
- Resource and activity related reports generation for Nuatnix and non-Nutanix environments

You can enable Intelligent Operations from **Admin Center** application. For more information, see Enabling Intelligent Operations in *Intelligent Operations Guide*.

Starting from Prism Central version 2023.3, NCM Intelligent Operations (formerly AIOps) now has a new user interface. The following Operations Entities have been moved from Prism Central Infrastructure app to the new user interface created for NCM Intelligent Operations:

- Analysis
- App Discovery
- Monitoring Configurations
- Operations Policies
- Planning
- Playbooks
- Reports
- Settings and Configurations

The documentation for the above-mentioned entities has been moved to the newly created *Intelligent Operations Guide*. For more information, see Intelligent Operations Guide. You can also find the Intelligent Operations Release Notes under Nutanix Cloud Manager on the documentation portal.

High Availability in Prism Central

Prism Central supports high availability using the following functionalities:

- **VM high availability: Migrates and restarts the Prism Central VM (PCVM) from a failed node to another node.**

  When a node that hosts a PCVM fails, Acropolis migrates and restarts the PCVM in another node that has enough data resources and entities required to run the PCVM.

  > **Note:** Prism Central supports VM high availability only if your deployment meets the following requirements:
  >
  > - PCVM runs pc.2024.1 or later
  > - The cluster (Prism Element) runs AOS 6.8 or later
  > - AHV version is 20230302.100173 or later.

  Both single VM Prism Central and three VM scale-out Prism Central deployments support high availability using the VM high availability feature in Acropolis.

  For information on high availability, see VM High Availability in Acropolis in the *Prism Element Web Console Guide*. For information on how to enable high availability in a PCVM, see Enabling High Availability for the Cluster in the *Prism Element Web Console Guide*.

- **Scale-out: Scales out a single VM Prism Central deployment to a three-VM deployment with a fault tolerance of one PCVM.**

  Prism Central supports high availability by scaling out a single VM Prism Central deployment to a three-VM deployment with a fault tolerance of one PCVM. For information on how to scale out a Prism Central deployment across multiple VMs, see Expanding (Scale Out) Prism Central.

  In a scale-out Prism Central deployment, if one PCVM fails, the other two PCVMs perform the load balancing for the failed PCVM, and the Prism Central stays active. If two or all three PCVMs fail, then Prism Central is considered inactive.

  For information on the configurations, requirements, specifications, and limitations of scalability, see the *Prism Central Scalability* topic in the release notes for the Prism Central version to be installed.

Finding the Prism Central Version

About this task

You can check the version of your Prism Central instance using the Prism Central user interface or by running the following command.

```
nutanix@cvm$ ncli cluster info
```

Do the following to check the Prism Central version in the UI.

Procedure

1. Log in to Prism Central.
2. Click the user icon in the main menu and then select the **About Nutanix** option from the dropdown menu.

   An **About Nutanix** window appears that includes the AOS version number. It also includes a link to Nutanix patent information.
3. Click **Close** to close the window.

Finding the AHV Version on Prism Central

About this task

You can see the installed AHV version in Prism Central.

Procedure

To view the AHV version installed on any host in the clusters managed by Prism Central, perform the following steps:

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function, and navigate to **Hardware** > **Hosts** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar.
   The system displays the **List** tab by default with all the hosts across registered clusters.
3. Click the target host name for which you want to see the hypervisor version.
   The system displays the Host Details View with **Summary** tab.
4. Observe the Hypervisor Version field in the **Properties**widget to view the hypervisor version.

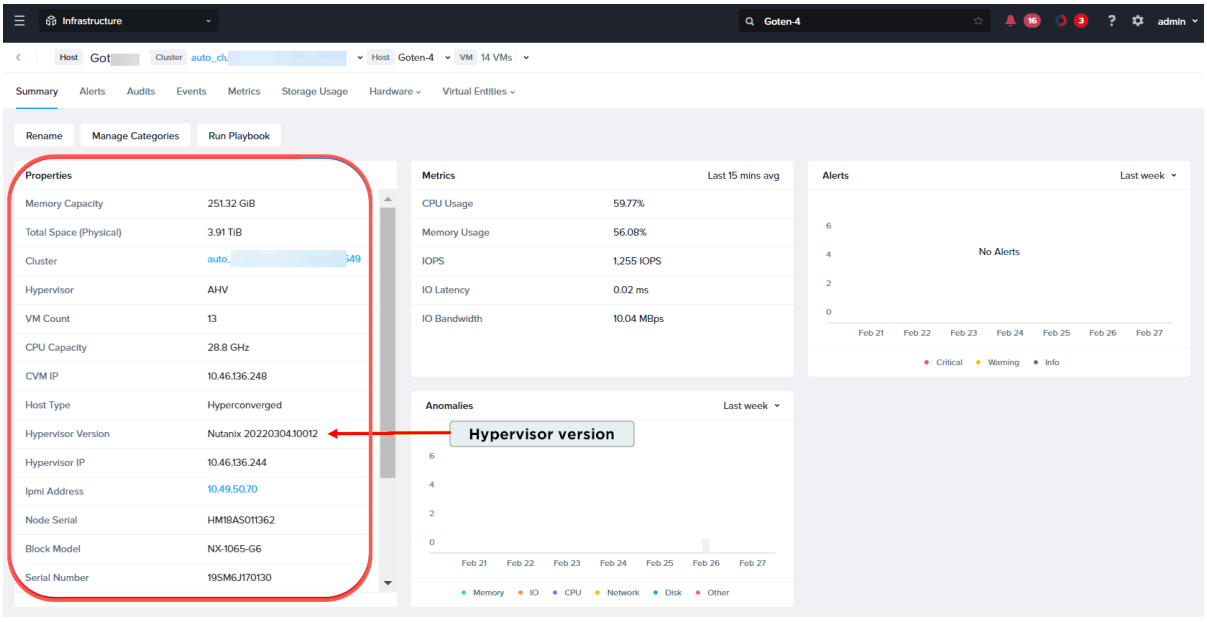


Figure 232: Hypervisor Version in Host Detail View

Finding the AOS Version Using Prism Central

To view the Nutanix AOS version running in the Prism Central, do the following:

Procedure

1. Log in to Prism Central.
2. Select the **Infrastructure** application from Application Switcher Function on page 19, and navigate to **Hardware** > **Clusters** from the **Navigation Bar**. For information about the **Navigation Bar**, see Application-specific Navigation Bar on page 57.
   The system displays the **List** tab by default with all the registered clusters in **Nutanix** environment.

3. In the **List** tab, the AOS version of the cluster is listed against the cluster name.

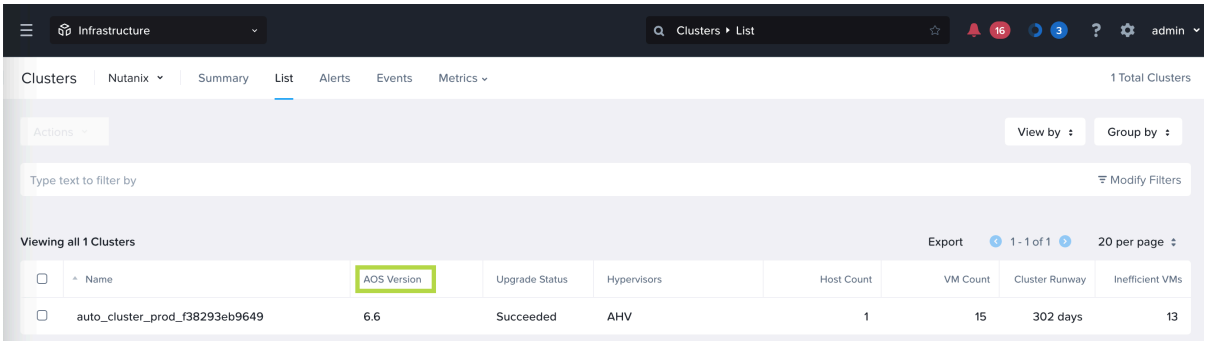


Figure 233: AOS Version in a Cluster

Expanding (Scale Out) Prism Central

Before you begin

The following requirements must be met before you can expand Prism Central or add a Prism Central VM:

- The specified gateway must be reachable.
- No duplicate IP addresses can be used.
- The container used for deployment is mounted on the hypervisor hosts.
- For Prism Central versions lower than 2023.3, the hosting cluster should be registered with Prism Central.
- When installing on an ESXi cluster:
  - vCenter and ESXi cluster must be configured properly. For more information about vCenter and ESXi configuration, see the vCenter Configuration topic in *vSphere Administration Guide for Acropolis*.
  - vCenter must be registered in Prism.
  - DRS must be enabled in vCenter.
  - vCenter is up and reachable during the deployment.

About this task

If Prism Central is just a single VM currently, you can expand it to three VMs. This increases both the capacity and resiliency of Prism Central (at the cost of maintaining two additional VMs). For information on Prism Central scalability, see the *Prism Central Scalability* topic in the release notes for the Prism Central version to be installed.

To expand this Prism Central instance across multiple VMs, do the following:

Note:

- Scaling out of Prism Central VM not registered with the hosting Prism Element is not supported if any of the portfolio products such as Self-Service or Disaster Recovery is enabled on Prism Central.
- All the scale out Prism Central VMs must run on the same cluster. For example, running two VMs in cluster_1 and one VM in cluster_2 is not supported.

- If you have configured application monitoring on a single node Prism Central setup, and you scale out to 3 nodes running Prism Central version PC.2023.4, you must power off and then again power on the newly added nodes.

Procedure

1. Log in to Prism Central.
2. Click the Settings icon and then select **Prism Central Management** from the **Settings** menu. For more information, see Prism Central Settings (Infrastructure) on page 22.
   The **Manage Prism Central** page appears. This page provides information about this Prism Central instance.

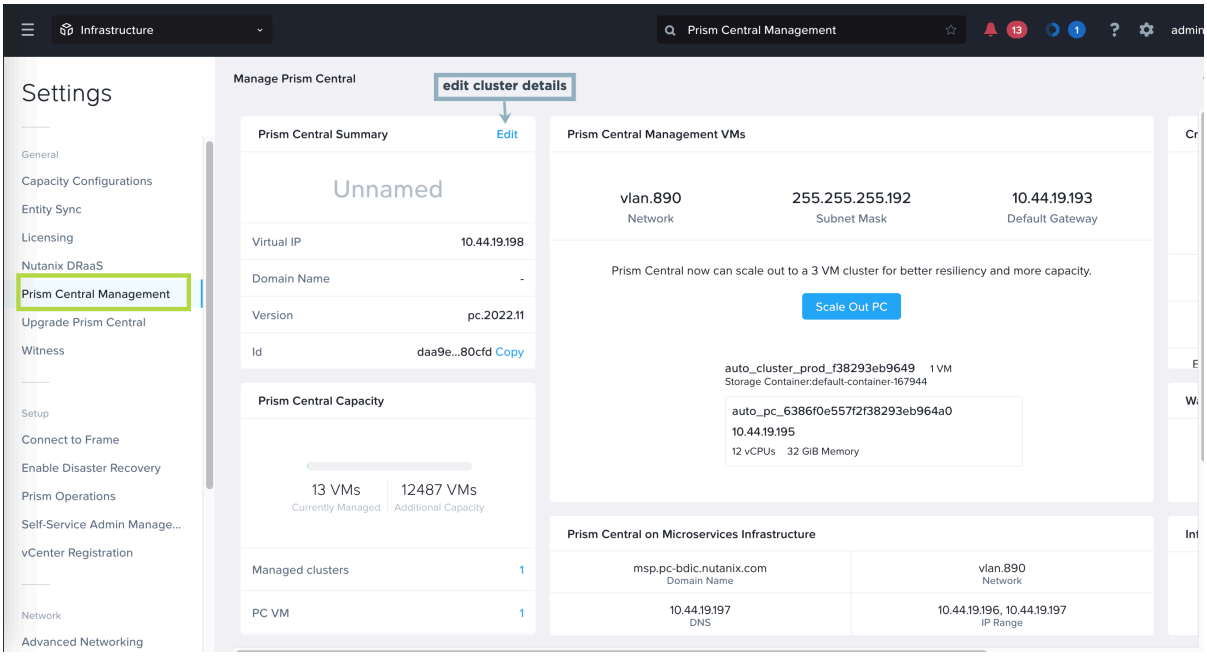


Figure 234: Manage Prism Central Page

3. To expand this Prism Central instance from one to three VMs, click **Scale Out PC** to display the **Scale Out PC** page and do the following:

> **Note:** A pop-up window appears explaining that scale out is a one-way process. Click **Continue** to display the **Scale Out PC** page. Once you scale out a Prism Central instance from a single VM to multiple VMs, you cannot revert back. Deleting any of the Prism Central VMs may result in data loss.

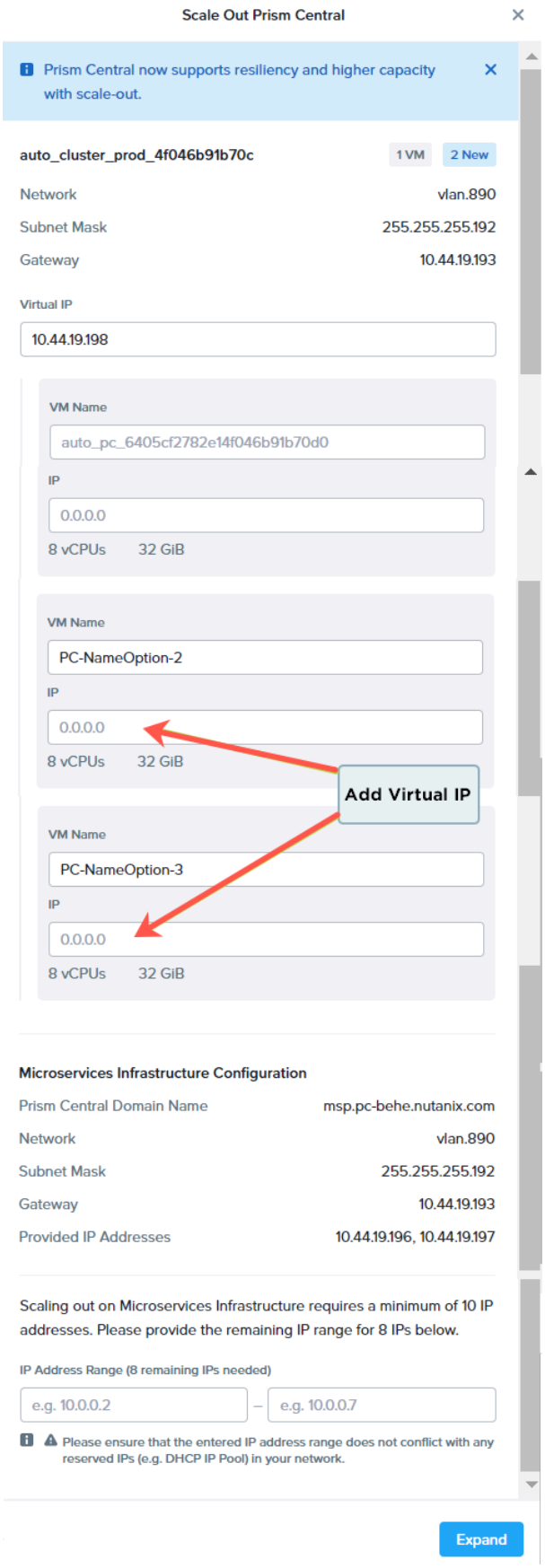


Figure 235: Scale Out PC Page

Note: The Prism Central VM image is deployed from the target cluster. If the required image cannot be accessed, typically because there is no Internet access (such as at a dark site), a pop-up error message appears. In this case you have the option to manually download and deploy the image as follows:

1. Log on to the Nutanix customer support portal, click **Downloads** > **Prism Central**, and click the download link for the target version to save the Prism Central binary .TAR and

metadata .JSON files on your local media. The binary .TAR file is from the Prism Element bundle, used for 1-click deployment.

2. Log on (using SSH) to any Controller VM in the cluster specified in the error message and copy the Prism Central binary .TAR and metadata .JSON files to the Controller VM.
3. Run the following command to deploy the Prism Central image:

   ```
   nutanix@cvm$ ncli software upload software-type=PRISM_CENTRAL_DEPLOY file-path=file_path meta-file-path=metadata_file_path
   ```

   The *file_path* is the full (absolute) path to the .TAR file, and the *metadata_file_path* is the full path to the .JSON file. After this step completes, you can continue the scale out procedure.

a. Review the **Network**, **Subnet Mask**, and **Gateway** fields, which display the network name, subnet mask value, and gateway IP address applied to this Prism Central instance.

   The values in these three fields are read-only and cannot be changed.

   Note: The scale-out process uses the IP addresses from the network configured. If you used the default network configuration being the Private Network [default] while enabling microservices infrastructure, Prism Central displays and uses Private Network [default] details in this section.

b. [optional] To specify a virtual IP address for Prism Central, click the **Add Virtual IP** link.

   This displays the **Add PC Virtual IP** window. A virtual IP can be used as a single point of access for Prism Central. Enter the IP address in the Virtual IP field, and then click **Update**.

c. Specify IP addresses for the two new Prism Central VMs.

   1. Click the pencil icon for one of the new VMs. (The VM names are set automatically.) The **IP field** opens for editing. Enter the IP address and then click the green check mark icon to save that address.



Figure 236: Edit IP Field

   2. Repeat this step for the second new VM.

   The vCPU count and memory size in the new VMs are fixed and match the current Prism Central VM values; you cannot change these values.

d. When all the parameters are correct, click **Expand**.

   This starts the process of creating the new VMs and deploying this Prism Central instance. You can monitor progress from the **Tasks** page. For more information, see Tasks View on page 451.

What to do next

In some cases, especially when using NCM Self-Service (formerly known as Calm), a version mismatch with a linked product could occur after expanding Prism Central. To fix this situation, perform a life cycle manager (LCM) inventory after completing the Prism Central expansion procedure. For instructions on how to perform an LCM inventory, see the LCM documentation.

Shutting Down or Starting Up Prism Central VM

About this task

A Prism Central VM (PC VM) is managed like any other VM in a cluster through the Prism Element web console for the cluster in which the Prism Central VM is running. However, shutting down a PC VM requires extra caution.

> **Note:**
>
> Prism Central supports features that could be damaged by shutting down the PC VM abruptly. You must follow the steps carefully to avoid any issues.

Procedure

- To shut down the PC VM in single VM configuration, or to shut down all the three PC VMs in a scale out configuration, see Shutting down or starting up all the PC VMs in a Prism Central Configuration on page 565.
- To shut down a single PC VM in a scale-out Prism Central configuration, see Shutting down or starting up a single PC VM in a scale-out PC configuration on page 566.

Shutting down or starting up all the PC VMs in a Prism Central Configuration

About this task

To shut down the PC VM in single VM configuration, or to shut down all the three PC VMs in a scale out configuration, perform the following steps:

Procedure

1. SSH to the IP address of the PC VM that you want to shut down.
2. Stop the cluster.

   ```
   nutanix@pcvm$ cluster stop
   ```

3. Check the status of the services running on the cluster.

   ```
   nutanix@pcvm$ cluster status
   ```

   The command output should show the following three services still running: Zeus, Scavenger, and VipMonitor.

4. To shut down a PC VM, log on to the web console of the host and go to the VM dashboard (see VM Dashboard in Prism Element Web Console Guide). In the VM Table view, select the PC VM you want to shut down (one at a time), and then select **Power Off Actions >> Power Off** or **Power Off Actions >> Guest Shutdown** from the action links.

   Alternatively, you can SSH to the IP address of the PC VM and run the command to shut down the PC VM.

   ```
   nutanix@pcvm$ sudo shutdown -h now
   ```

   You must run this command for each PC VM that you want to shut down.

5. To power on a PC VM, log on to the web console of the host and go to the VM Dashboard (see VM Dashboard). In the VM Table view, select the PC VM you want to power on (one at a time), and then select **Power On**.

6. Once all the PC VMs are powered on, check the status of the services from any one of the PC VMs.

```
nutanix@pcvm$ cluster status
```

   In the command output, verify that all the three services (Zeus, Scavenger, and VipMonitort) are running.

7. Once all the three services start running, start the cluster from any one of the PC VMs.

```
nutanix@pcvm$ cluster start
```

Shutting down or starting up a single PC VM in a scale-out PC configuration

About this task

To shut down or start up a single PC VM in a scale-out PC configuration, perform the following steps:

Procedure

1. SSH to the IP address of the PC VM.
2. Run the following command to gracefully stop all the services:

```
nutanix@pcvm$ genesis stop all
```

3. Now log on to the web console of the host and go to the VM dashboard (see VM Dashboard in *Prism Element Web Console Guide*).
4. In the VM Table view, select the PC VM you want to shut down, and then select **Power Off Actions >> Power Off** or **Power Off Actions >> Guest Shutdown** from the action links.

   Alternatively, you can SSH to the IP address of the PC VM and run the command to shut down the PC VM.

```
nutanix@pcvm$ sudo shutdown -h now
```

5. To power on a PC VM in a scale-out PC configuration, log on to the web console of the host and go to the VM Dashboard (see VM Dashboard). In the VM Table view, select the PC VM you want to power on (one at a time), and then select **Power On**.
6. Restart the genesis service:

```
nutanix@pcvm$ genesis restart
```

7. Check the status of the services running on the cluster.

```
nutanix@pcvm$ cluster status
```

8. Start the services in the PC VM:

```
nutanix@pcvm$ cluster start
```

Keyboard Shortcuts in Prism Central

You can use the following keyboard shortcuts to invoke important menu options or views in Prism Central:

Table 153: Keyboard Shortcuts for Prism Central Menu Options

Shortcut Key	Menu Option/View
s	Settings Menu
f	Spotlight (search bar)
u	User Menu
h	Help menu (? menu)
p	Recent tasks

You can use the arrow keys to select a particular menu option.

IP Address Reconfiguration

You can use this procedure to reconfigure the IP address and gateway of single Prism Central instances as well as Prism Central VMs in a Scale out Prism Central (clustered PC VMs or PC cluster).

> **Note:** Reconfiguring the IP address and gateway of Prism Central VMs does not require additional steps when using Nutanix Disaster Recovery (formerly Leap).

Preparing to Reconfigure the IP Address and Gateway of PC VMs

Perform the tasks described in this topic before you start the IP address reconfiguration procedure.

About this task

You must perform the following tasks while the Prism Central VMs are still on the existing IP addresses.

Procedure

1. Coordinate Prism Central downtime, because the features and functionality of Prism Central will be unavailable for the entire duration of the IP address reconfiguration procedure.
2. Create a table to map the existing IP addresses with the new IP addresses of the Prism Central VMs for your reference.
3. Use SSH to log on to any running Prism Central VM in the PC cluster or the single PC VM if you do not have a PC cluster.
4. Verify if the PC VM or PC cluster is in a stable state.

   ```
   nutanix@pcvm$ cluster status
   ```

   This command is valid even if you only have a single PC VM and do not have a PC cluster.
5. Run the NCC health checks to make sure that the PC cluster is in a healthy state.
6. If you want to reconfigure the IP addresses of the entities in the AOS clusters (such as IP addresses of CVMs and hypervisor hosts), on which the PC is hosted, reconfigure those IP addresses first before you reconfigure the IP addresses of the PC VMs.
7. Stop the PC VM or PC cluster.

   ```
   nutanix@pcvm$ cluster stop
   ```

   This command is valid even if you only have a single PC VM and do not have a PC cluster.

   Wait to proceed until an output showing all the services as DOWN is displayed, except the Zeus and Scavenger services.

Reconfiguring the IP Address and Gateway of Prism Central VMs

Before you begin

Ensure that you have completed the tasks described in Preparing to Reconfigure the IP Address and Gateway of PC VMs on page 567.

About this task

The procedure to reconfigure the IP addresses of PC VMs differs depending on whether or not IP Address Management (IPAM) is enabled in an AHV cluster. The procedure to reconfigure the IP addresses of PC VMs in an ESXi cluster is the same as the procedure of an AHV cluster in which IPAM is disabled.

IP Address Management (IPAM) is a feature of AHV that allows it to assign IP addresses automatically to VMs by using DHCP. For more information, see IP Address Management section in the *AHV Administration Guide*.

In this document, managed network refers to an AHV network that has IPAM enabled, and unmanaged network refers to an AHV network that does not use IPAM.

Note:

- Reconfiguration of PC VM IP addresses is not supported for Prism Central scale-out deployments used in Nutanix Cloud Clusters (NC2) on AWS or Azure environment.
- Do not reconfigure the IP address of the PC VM if any Nutanix Kubernetes Engine (NKE) or Objects are deployed on the cluster since changing the PC VM IP address is not supported for NKE or Objects after deployment.

Perform the following procedure to reconfigure the IP address of a single PC VM or PC VMs in a PC cluster.

Procedure

1. Log in as `nutanix` user and run the *external_ip_reconfig* script.

```
nutanix@pcvm$ external_ip_reconfig
```

2. Follow the prompts to type the new netmask, gateway, and external IP addresses.

   A message similar to the following is displayed when the procedure begins:

   ```
   External IP reconfig started
   ```

   A message similar to the following is displayed if the procedure is completed successfully:

   ```
   External IP reconfig finished successfully. Restart all the CVMs and start the
    cluster.
   ```

   The message indicates that you must restart the CVMs. In this case, you are reconfiguring the IP addresses of the PC VMs, so you must restart the PC VMs and not the CVMs.

   > **Note:**
   >
   > If your PC VMs are running in a managed network of an AHV cluster, do not start the PC VMs yet but proceed to step 3.
   >
   > If your PC VMs are in an unmanaged network of an AHV cluster or are in an ESXi cluster, skip steps 3, 4, and 5, and proceed to step 6 directly.
   >
   > Perform steps 3, 4, and 5 only if the new IP address is in a different IP address range than the previous IP address range and your PC VM is in a managed network of an AHV cluster.

   A message similar to the following is displayed if the procedure fails:

   ```
   External IP reconfig Failed
   ```

   If the procedure fails, run the following command to check the log for troubleshooting purposes:

   ```
   nutanix@pcvm$ cat ~/data/logs/ip_reconfig.log
   ```

3. (Optional) Use SSH to log onto any CVM of the AOS cluster that is hosting the PC cluster or PC VM.

   > **Note:** Perform this step only if the new IP address is in a different IP address range than the previous IP address range and your PC VM is in a managed network of an AHV cluster.

4. (Optional) Update the NIC attached to the PC VM with the new IP address of the PC VM.

   > **Note:** Perform this step only if the new IP address is in a different IP address range than the previous IP address range and your PC VM is in a managed network of an AHV cluster.

   ```
   nutanix@cvm$ acli vm.nic_update pc-vm-name pc-vm-mac request_ip=true ip=pc-vm-ip
   ```

   Replace the variables with their appropriate values as follows:

   - *pc-vm-name*: Name of the Prism Central VM whose IP address you modified.
   - *pc-vm-mac*: MAC address of the Prism Central VM whose IP address you modified (press **Tab** after you type the name of the PC VM to automatically populate the MAC address).
   - *pc-vm-ip*: New IP address of the Prism Central VM.

5. (Optional) Log on to the Prism Element web console and modify the IP address range in the IP pool for the PC network to work with the modified IP address of Prism Central VMs. In the Prism Element web console, perform the following:

   Note: Perform this step only if the new IP address is in a different IP address range than the previous IP address range and your PC VM is in a managed network of an AHV cluster.

   a. In the **VM** dashboard, click the **Table** view.

   b. Select a **PC VM** and click **Update**.

   c. In the **Update VM** dialog box, scroll down to the **Network Adaptors (NIC)** section.

   d. In the **VLAN Name** column, note the names of the networks attached to your PC VM.

   e. Click **Close**.

   f. Click the gear icon in the top-right corner, and under **Settings**, click **Network Configuration**.

   g. In the **Network Configuration** dialog box, identify the network names you noted in step d.

   h. Select each network and click the pencil icon next to the network.

   i. Under **IP Address Pools**, modify the IP address range if the new IP address of the PC VM is in a different IP address range than the previous IP address range.

6. Restart each Prism Central VM in the PC cluster or the single PC VM if you do not have a PC cluster.

7. Once the PC VMs are powered on, use SSH to log on to each PC VM or the single PC VM if you do not have a PC cluster and verify if the output of the following verification script displays the new IP addresses:

   ```
   nutanix@pcvm$ python cluster/bin/external_ip_reconfig_verify.py
   ```

8. Start the PC cluster.

   ```
   nutanix@pcvm$ cluster start
   ```

9. Perform the steps mentioned in KB-15469.

10. Perform the following verification steps:

    a. Log on to the Prism Element web console of every cluster attached to the PC VM whose IP address you changed.

    b. On the **Home** page, verify if the **PC Registration** status is displayed as **OK**. This might take a few minutes after the PC VM or PC cluster is powered on.

Logging Out of Prism Central

Procedure

To log off from Prism Central, select **Sign Out** from the user menu that appears on the far right side of the Prism Central landing page. You are logged out immediately after selecting the option (no prompt or message).

CUSTOMER SUPPORT SERVICES

Nutanix provides customer support services in several ways.

- Nutanix customer support can monitor your clusters and provide assistance when problems occur through the Pulse mechanism. For more information, see Pulse Health Monitoring information in *Prism Central Admin Center Guide*.
- Nutanix customer support maintains a portal that you can access to request assistance, download various product updates, and view documentation. For more information, see Accessing the Nutanix Support Portal (Prism Central) on page 576.
- If you need help, you can create a support ticket directly from Prism Central. For more information, see Creating a Support Case on page 572.
- Nutanix technical support can remotely assist with problems in a Prism Central (PC) VM by logging into the faulty PCVM through an SSH connection. For more information, see Configuring Remote Connection Using CLI on page 571.

Configuring Remote Connection Using CLI

You can enable a remote support connection tunnel for a maximum of 72 hours using CLI.

About this task

If you face an issue in your Prism Central (PC) VM and the Nutanix Support team needs access to it to troubleshoot the issue, you can open a support tunnel for the Nutanix Support team to give remote access to your VM. The Nutanix Support team ensures that the connection to your PCVM through the support tunnel is secure and compliant by consolidating connectivity, authentication, authorization, audit, and recorded sessions.

Use the following procedure to enable the remote support connection tunnel.

Procedure

1. SSH into CVM or PCVM .
2. Start ncli.

```
nutanix@cvm$ ncli

<ncli>
```

3. Run the cluster start-remote-support with the duration parameter set as required.

   The duration parameter must be set in minutes even if you need a duration of hours.

```
ncli> ncli cluster start-remote-support duration=<minutes>
```

   Add duration that you want to enable the remote support connection tunnel for, in minutes. For example, if you want to keep the connection open for 24 hours, enter `duration=1440`.

> **Note:** You can keep the remote support connection tunnel between 0-72 hours.

Creating a Support Case

About this task

Nutanix customer support maintains a portal where you can get assistance by opening a support case and viewing the status of your open cases (see Accessing the Nutanix Support Portal (Prism Central) on page 576). However, you can also create a support case directly from Prism Central. To create a support case or view information about your open cases, do the following:

> **Note:** A support portal connection is required before you can create a case (see Prism Central Licensing on page 51). In addition, at least one cluster must be registered with Prism Central. Also, this feature is available only to customers who get support directly from Nutanix (such as NX and SX model customers), not customers who get initial support from third parties.

Procedure

1. Click the Help icon in the main menu and select **Create Support Case** from the dropdown menu.

   The **Create new support case** page appears. One of the following appears on this page:

   - If there are no open cases currently, a blank page with fields for creating a case appears.
   - If you have one or more open support cases, summary information about those cases appears (see Viewing Case Status on page 575). To create a case from this page, click the **Create new support case** button (upper right). The blank page with fields for creating a case will appear.

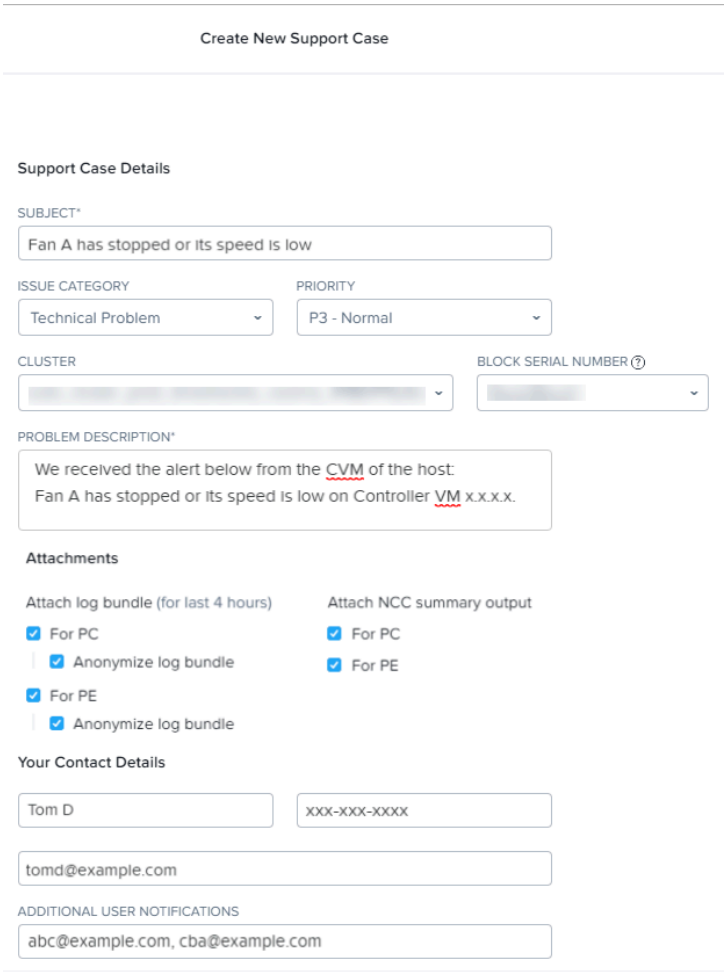


Figure 237: Create New Support Case Page

2. Do the following in the indicated fields:

   a. **Subject**: Enter a title that briefly describes the issue.

   b. **Issue Category**: Select the type of issue from the dropdown menu.

      The types are **Technical Problem**, **Question**, **Comment/Feedback**, **Scheduled Upgrade/ Maintenance**, **RFE** (request for enhancement), **Licensing**, **Non Technical issue**, and **Technical Problem - Foundation**.

   c. **Priority**: Select the priority for this issue from the dropdown menu.

      There are four priority levels based on the severity of the problem plus a request for enhancement option. Select the appropriate priority based on the following descriptions.

      - **P1 - Emergency**. System is not available and productivity has been halted. Product is unusable in its current state.
      - **P2 - Critical**. System is available but experiencing issues which have a direct impact on productivity. Major inconvenience.
      - **P3 - Normal**. System is having an occasional issue that has been identified as needing to be resolved, but the issue has not greatly affected productivity. Minor inconvenience.
      - **P4 - Low**. Questions about documentation, processes, or procedures. General requests about information.
      - **RFE - Request for Enhancement**. Feature requests for the product which would improve the experience or functionality for the customer.

   d. **Cluster**: Select the target cluster from the dropdown menu.

   e. **Block Serial Number**: Select the serial number of the asset (node) in question from the dropdown menu.

      If you need more information, see the "Installed Base" page on the Nutanix support portal for a list of your assets and the corresponding serial numbers.

   f. **Tell Us More**: Enter a description of your issue in the text box.

      Include any relevant details that might help Nutanix customer support analyze and resolve your issue.

   g. **Attach log bundle (for last 4 hours)**: Check this box to attach log files from the last four hours to the case. If you want the attached logs to be anonymized (personally identifiable information removed), check the **Anonymize log bundle** box.

      - **For PC**: Check this box to attach Prism Central log files from the last four hours to the case. If you want the attached logs to be anonymized (personally identifiable information removed), check the **Anonymize log bundle** box.
      - **For PE**: Check this box to attach Prism Element log files from the last four hours to the case. If you want the attached logs to be anonymized (personally identifiable information removed), check the **Anonymize log bundle** box.

      > **Note:** If the target cluster is not connected to the Internet, such as in a dark site, a log bundle or NCC summary report (following step) cannot be attached to the case through this method.

   h. **Attach NCC summary output**

      - **For PC**: When this box is checked, NCC is run, and the summary output of Prism Central is attached. This ensures that the NCC (health checks) results reflect the current state.

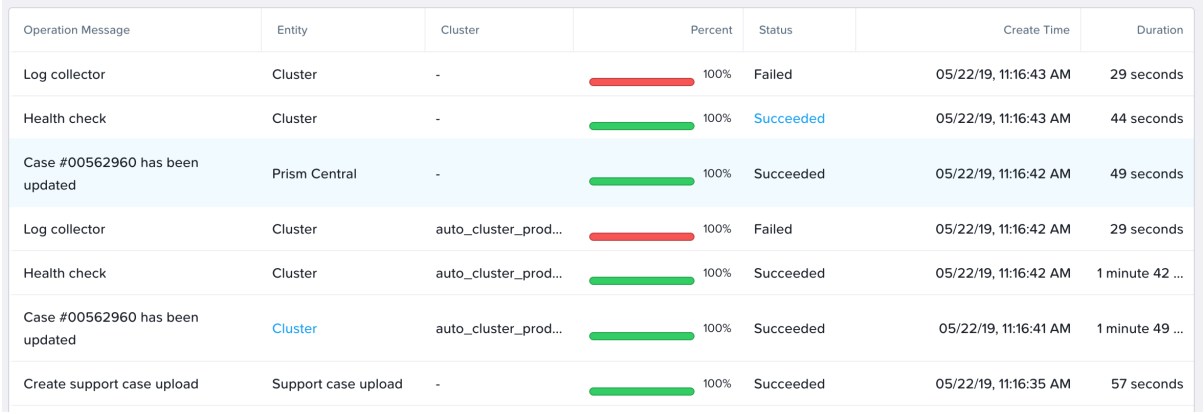
- **For PE**: When this box is checked, NCC is run, and the summary output of Prism Element is attached. This ensures that the NCC (health checks) results reflect the current state.

i. **Your Contact Details**: Enter your name, phone number, and e-mail address in the indicated fields. Case updates are sent to your e-mail address. You can also have the case updates sent to (up to two) additional users by entering their e-mail addresses in the **Additional User Notification** field.

3. When the entered information is completed, click **Submit**.

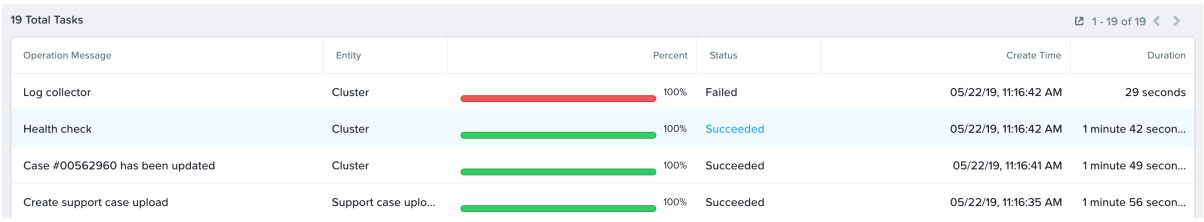
   This submits the case to Nutanix customer support for review and response. The speed of response reflects the priority of the issue, where P1 and P2 issues have a higher priority and more rapid response than less critical issues, but Nutanix customer support strives to handle all cases as quickly as possible.

   A Prism Central task is started to create the case. If you selected to attach a log bundle and/or NCC summary output, a task is started for each selected item. The tasks run asynchronously, and you can check the progress (case creation, log collection, and health check tasks) through the tasks dashboard (see Tasks View on page 451). If a task encounters a problem, you can hover the cursor over the "Failed" status to see a brief explanation. Automatically generated comments (preceded by "Prism Central Automated Note:") are added to the case when the log/health checks collection starts and when the upload completes. When the tasks complete, the output (log bundle and NCC summary report) appear as attachments in the case summary (see Viewing Case Status on page 575).



Operation Message	Entity	Cluster	Percent	Status	Create Time	Duration
Log collector	Cluster	-	100%	Failed	05/22/19, 11:16:43 AM	29 seconds
Health check	Cluster	-	100%	Succeeded	05/22/19, 11:16:43 AM	44 seconds
Case #00562960 has been updated	Prism Central	-	100%	Succeeded	05/22/19, 11:16:42 AM	49 seconds
Log collector	Cluster	auto_cluster_prod...	100%	Failed	05/22/19, 11:16:42 AM	29 seconds
Health check	Cluster	auto_cluster_prod...	100%	Succeeded	05/22/19, 11:16:42 AM	1 minute 42 ...
Case #00562960 has been updated	Cluster	auto_cluster_prod...	100%	Succeeded	05/22/19, 11:16:41 AM	1 minute 49 ...
Create support case upload	Support case upload	-	100%	Succeeded	05/22/19, 11:16:35 AM	57 seconds

Figure 238: Tasks Dashboard for Prism Central (create case tasks)



19 Total Tasks — 1 - 19 of 19

Operation Message	Entity	Percent	Status	Create Time	Duration
Log collector	Cluster	100%	Failed	05/22/19, 11:16:42 AM	29 seconds
Health check	Cluster	100%	Succeeded	05/22/19, 11:16:42 AM	1 minute 42 secon...
Case #00562960 has been updated	Cluster	100%	Succeeded	05/22/19, 11:16:41 AM	1 minute 49 secon...
Create support case upload	Support case uplo...	100%	Succeeded	05/22/19, 11:16:35 AM	1 minute 56 secon...

Figure 239: Tasks Dashboard for Prism Element (create case tasks)

Viewing Case Status

You can view information about open support cases directly from Prism Central by clicking the Help icon in the main menu and selecting **Create Support Case** from the dropdown menu. This opens the **Create new support case** page, which displays summary information about open cases (if any). When you have one or more open cases, this page displays the following sections:

- **Open Cases** column (on the left). There is an entry (line) for each open case that includes the case name and number; click the desired case entry to displays summary information about that case in the main section of the page.
- Main section (in the middle). This section displays the creation date, description, attachments (if any), and other information related to the selected case. This is an abridged version of the full case details available from the Nutanix support portal (see below).
- **Key Insights** column (on the right). This section includes the following fields:
  - **Status**: Displays the current status of the case.
  - **Created By**: Displays the name of the user who created the case.
  - **Type**: Displays the type (category) of issue the user specified when creating the case.
  - **Case number**: Displays the number assigned to this case.
  - **Serial Number**: Displays the serial number of the asset (node) in question.
  - **Access Portal**: Includes a link to the Nutanix support portal. Clicking the **View Details in Portal** link opens the details page for that case in the support portal in a new tab or window. The details page in the support portal provides the full details and history of that case should you desire more information, and you can submit additional material to the case such as screen shots or other relevant information.

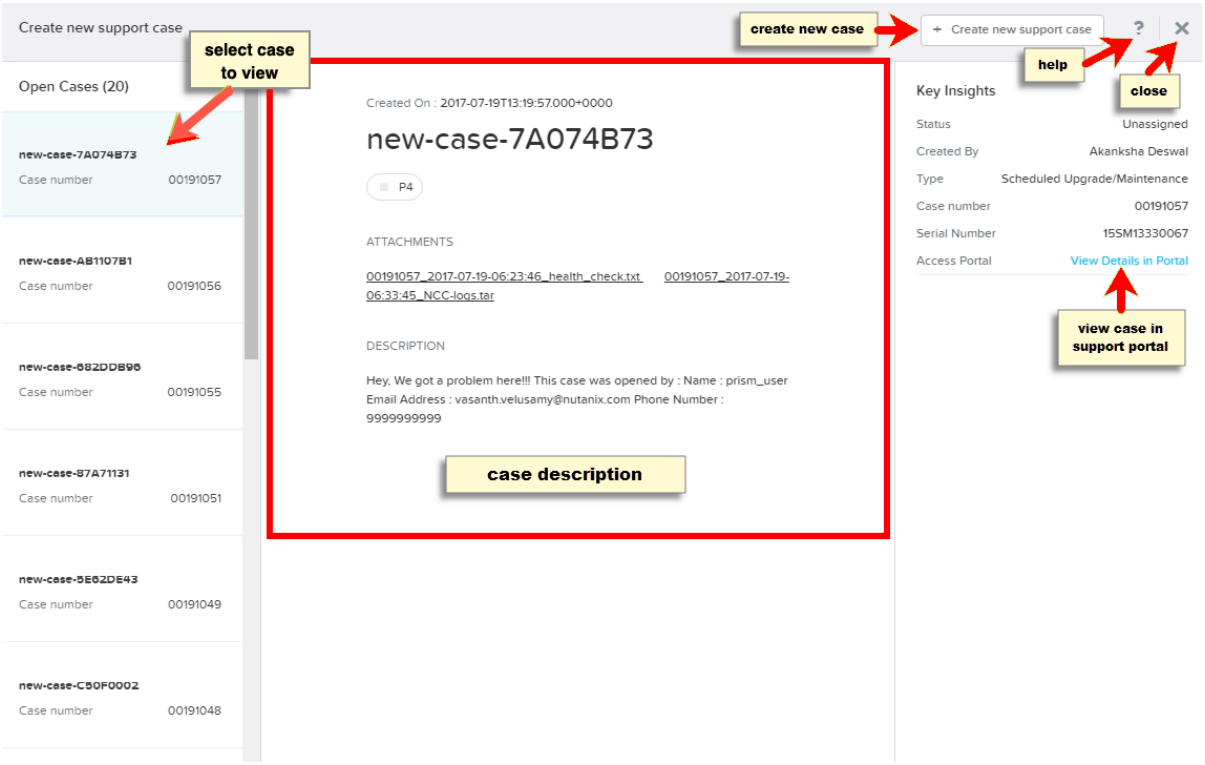


Figure 240: Create New Support Case Page (open cases)

Accessing the Nutanix Support Portal (Prism Central)

About this task

Nutanix provides a variety of support services and materials through its support portal.

Procedure

1. To access the Nutanix support portal from Prism Central, select **Support Portal** from the User icon dropdown menu of the main menu.

   The login screen for the Nutanix support portal appears in a new tab or window.

2. Enter your support account user name and password.
   The Nutanix support portal home page appears.

3. Select the desired service from the screen options.

   You can select an option from one of the main menu dropdown menus or search for a topic at the top of the screen, click one of the icons (Documentation, Open Case, View Cases, Downloads) in the middle, or view one of the selections at the bottom such as an announcement or KB article. The following table lists the menu options.

   > **Note:** Some options have restricted access and are not available to all users.

Table 154: Main Menu Options

Category	Option	Description
Documentation	Software Documentation	Displays a page from which you can view the Nutanix software manuals.
	Hardware Replacement Documentation	Displays a page from which you can view the Nutanix hardware replacement manuals.
	Knowledge Base	Displays a page from which you can view the knowledge base (KB) articles.
	Solutions Documentation	Displays a page from which you can view documents that describe how to implement the Nutanix platform to solve a variety of business applications.
	EOL Information	Displays a page from which you can view the end of life policy and bulletins.
	Field Advisories	Displays a page from which you can view field advisories.
	Training	Provides a link to the separate Nutanix training portal.
	Security Advisories	Displays a page from which you can view security advisories.
	AOS Upgrade Paths	Displays a page where you can see the supported AOS release upgrade paths.
	Compatibility Matrix	Displays a page from which you can view a compatibility matrix broken down (filtered) by hardware model, AOS version, hypervisor type and version, and feature version (NCC, Foundation, BMC/BIOS).
	Webinar Recordings	Displays a page with links to a selection of Nutanix training webinars.
Support	Open Case	Displays a form to create a support case.

Category	Option	Description
	View Cases	Displays a page from which you can view your current support cases.
	.NEXT Forums	Provides a link to the (separate) Nutanix Next Community forum.
	Terms & Conditions	Displays a page from which you can view various warranty and terms and conditions documents.
Downloads	AOS (NOS)	Displays a page from which you can download AOS releases.
	Acropolis File Services (AFS)	Displays a page from which you can download the Acropolis File Services.
	Acropolis Container Services (ACS)	Displays a page from which you can download the Acropolis Container Services.
	Hypervisor Details	Displays a page from which you can download Acropolis hypervisor versions. You can also download supporting files used when manually upgrading a hypervisor version (AHV, ESXi, or Hyper-V).
	Prism Central	Displays a page from which you can download the Prism Central installation bundle. There are separate bundles for installing on AHV, ESXi, or Hyper-V.
	Phoenix	Displays a page from which you can download Phoenix ISO files.
	Foundation	Displays a page from which you can download Foundation releases.
My Products	Installed Base	Displays a table of your installed Nutanix appliances, including the model type and serial number, location, and support coverage.

Category	Option	Description
	Licenses	Displays a table of your product licenses along with options to add or upgrade licenses for your clusters.

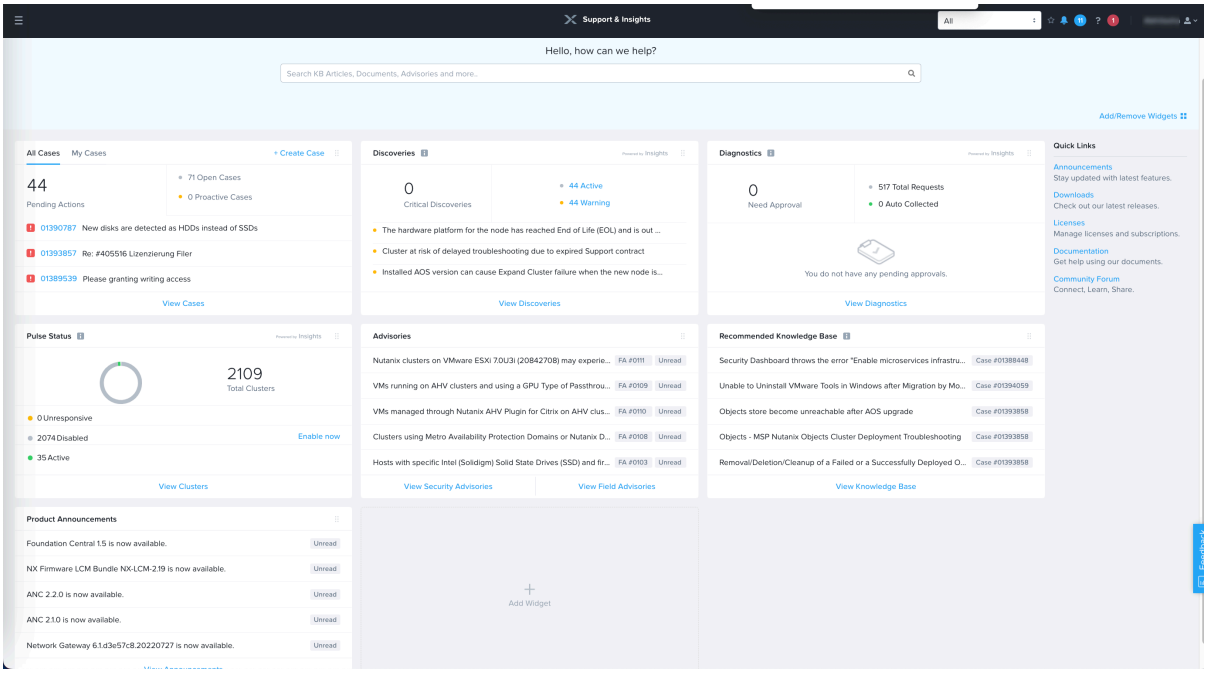


Figure 241: Nutanix Support Portal

Accessing the REST API Explorer

About this task

Nutanix provides a utility with the web console to help you get started with the REST API. The Explorer displays the parameters and format for the API calls that can be included in scripts. Sample API calls can be made to show the type of output you should expect to receive. Only an admin user can access the REST API Explorer.

The v3 API can be viewed in the REST API Explorer.

Procedure

1. Log on to Prism Central, click the User icon in the upper-right corner of the web console, and click **REST API Explorer**.

   The REST API Explorer displays a list of the objects that can be managed by the API.

2. Find the object you want to explore and click the name of the object to expand and show the detailed view of the operations that can be run on this object.

   For example, click **alerts**. All the API calls for **alerts** are displayed.

   a. Click **GET** to show the details for this API call.

   b. Click **Try it out!** to test the API call when used with your cluster.

   c. Similarly, you can explore other API calls.

HELP RESOURCES

There are several information sources that you can access at any time when you need help:

- Prism Central help documentation (see Accessing Online Help (Prism Central) on page 580).
- Nutanix customer support portal (see Accessing the Nutanix Support Portal (Prism Central) on page 576).
- Nutanix community forum (see Accessing the Nutanix Next Community on page 582).
- Glossary of terms (see Nutanix Glossary).

Accessing Online Help (Prism Central)

About this task

Prism Central includes online help documentation that you can access at any time.

Procedure

1. To open the online help, choose one of the following from the Help icon dropdown menu of the main menu:

   » Select **Help with this page** to display help documentation that describes the current screen.

   > **Note:** In a task window click the Help icon in the upper right to display the help documentation for that window.

   » Select **Online Documentation** to display the **Help Organization** page.

   A context-sensitive help page or the **Help Organization** page appears in a new tab or window. (These pages are located on the Nutanix support portal.) The **Help Organization** page provides descriptions of the major help topics with links to the entry page for each major topic. The display includes a breadcrumb at the top to navigate through the help pages.

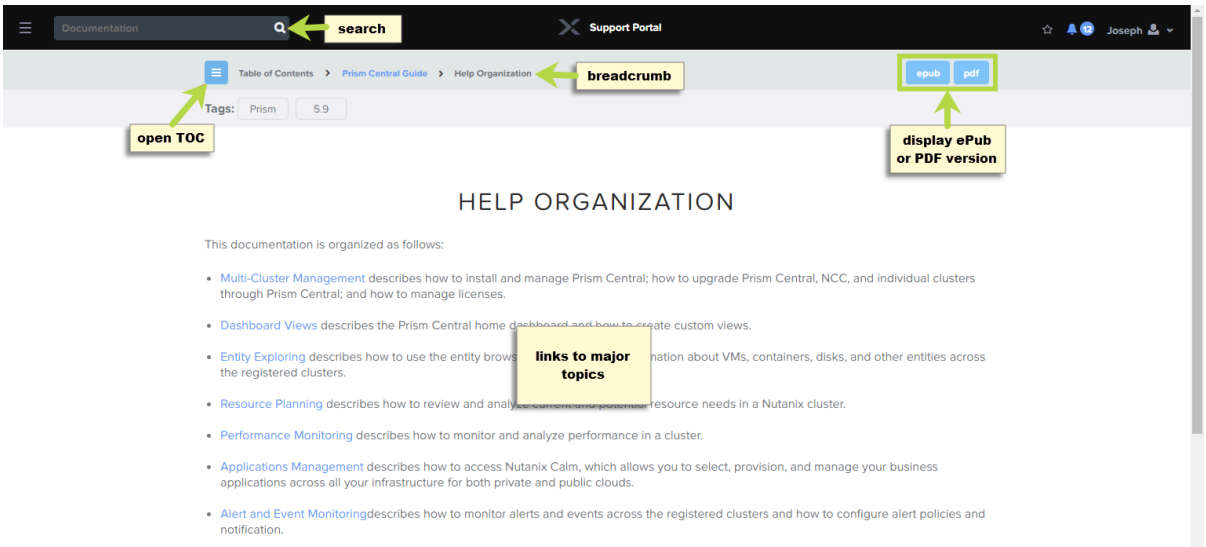


Figure 242: Help Organization Page

2. To select a topic from the table of contents, click the Navigation icon.

   A table of contents pane appears on the left. Click a topic in the table of contents to display that topic.

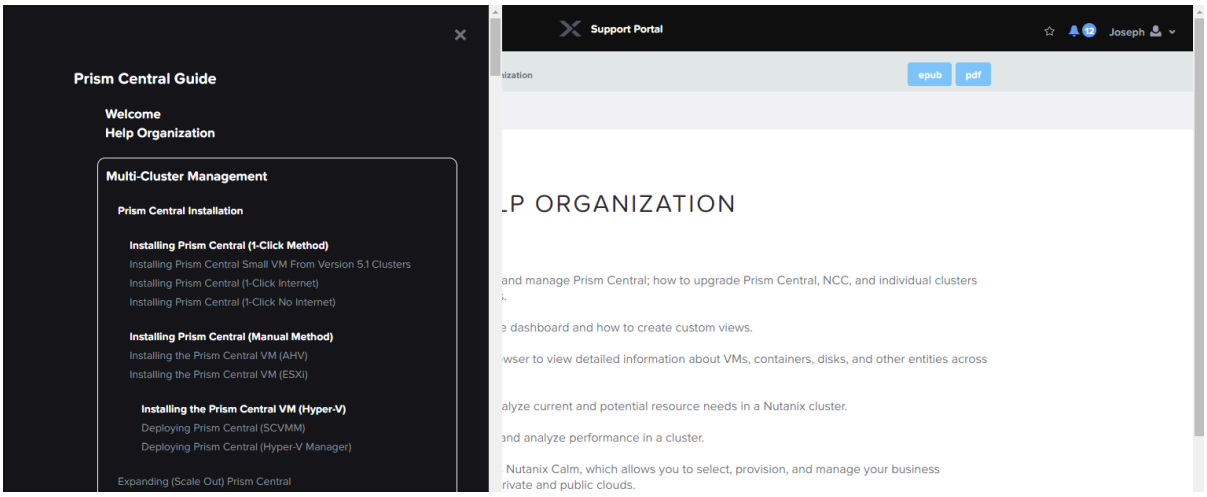


Figure 243: Table of Contents Pane

3. To display all the help contents as a single document, click **epub** or **pdf** in the upper right.

   You can view the *Prism Central Infrastructure Guide* in either ePUB or PDF format by selecting the appropriate option. If your browser does not support the selected format, you can download the PDF or ePUB file.

4. To search for a topic, click the magnifying glass icon in the main menu bar and enter a search string in the field.

   This searches not only the help contents, but also all the documentation, knowledge base articles, and solution briefs. Matching results appear below the search field. Click a topic from the search results to display that topic.

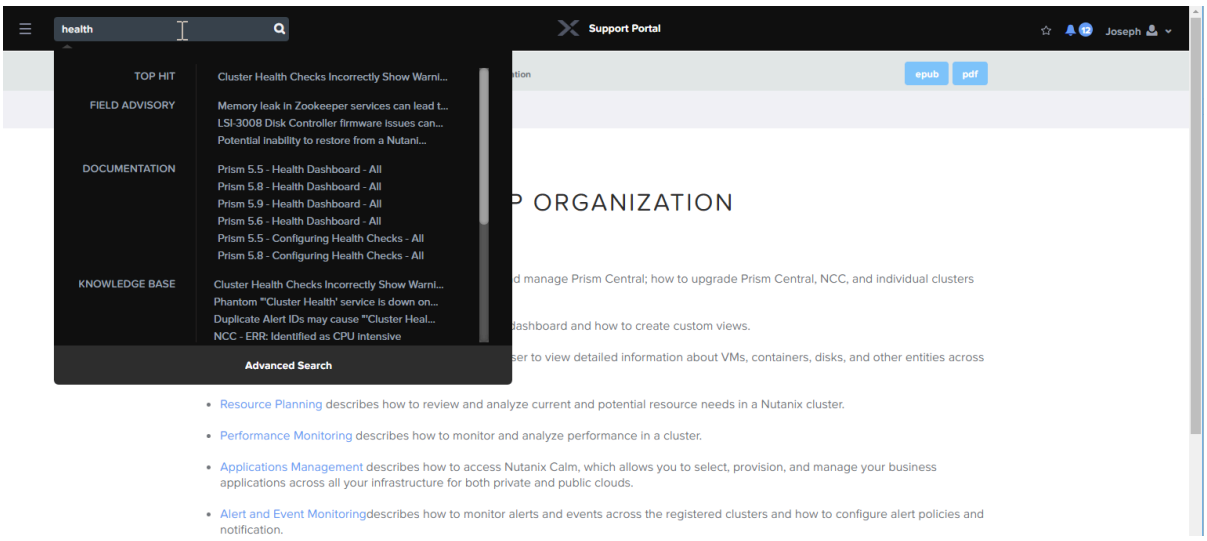


Figure 244: Search Results Example

Accessing the Nutanix Next Community

Nutanix maintains a community forum for customers and partners to facilitate a peer-to-peer exchange of ideas, tips, and information about Nutanix technologies and the rapidly changing landscape of data center IT.

Procedure

- To access the Nutanix next community forum from Prism Central, select **Nutanix Next Community** from the Help icon dropdown menu of the main menu (see Prism Central Landing Page on page 14).

  The Nutanix Next Community main page appears in a new tab or window. From this page you can search existing posts, ask questions, and provide comments.

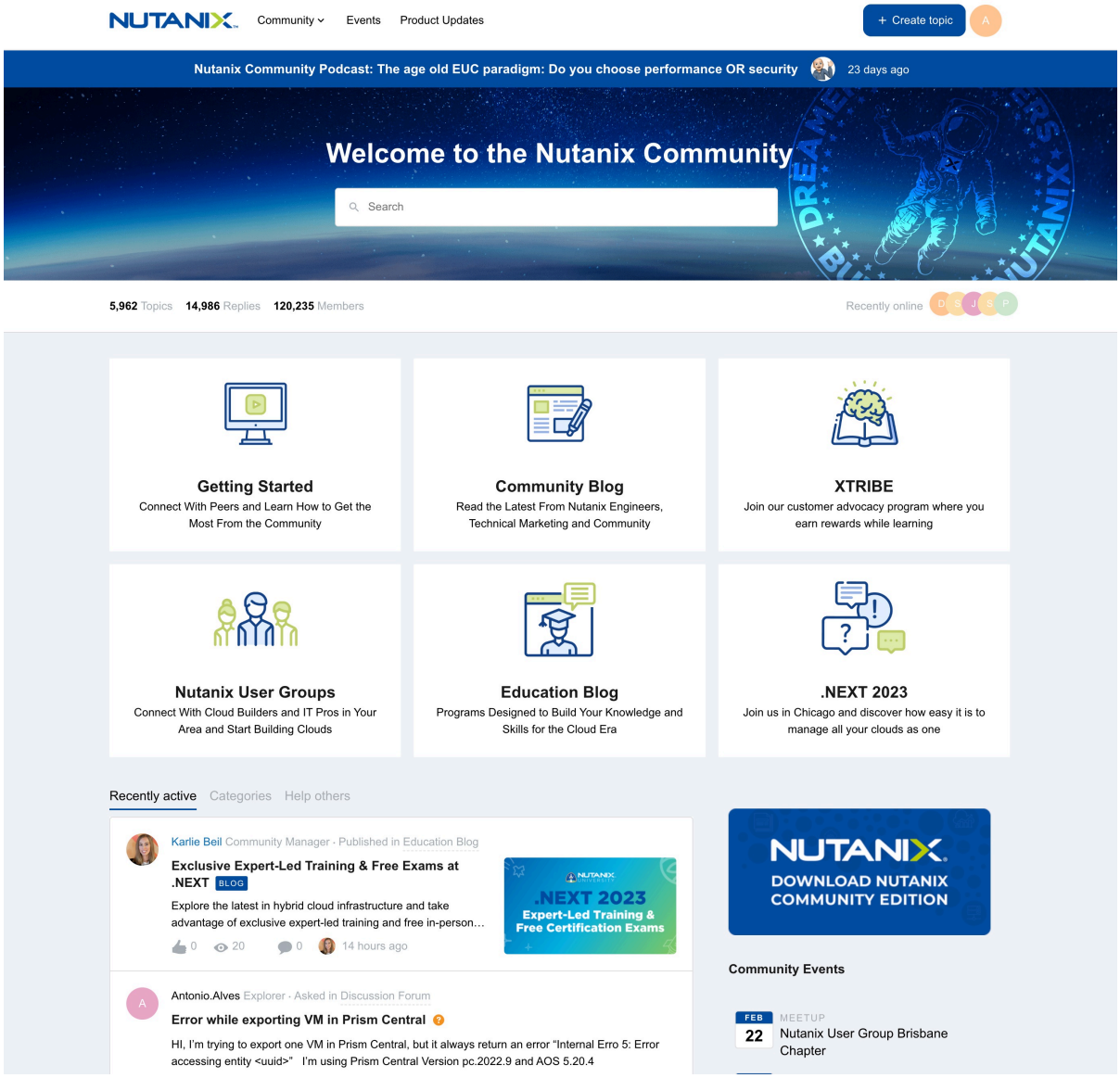


Figure 245: Next Community Screen

Glossary

For terms used in this guide, see Nutanix Glossary.

COPYRIGHT

Copyright 2024 Nutanix, Inc.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Nutanix and the Nutanix logo are registered trademarks of Nutanix, Inc. in the United States and/or other jurisdictions. All other brand and product names mentioned herein are for identification purposes only and may be trademarks of their respective holders.