Arcserve® N-Series Appliance User Guide

Version 1.0

arcserve

Legal Notices

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by Arcserve at any time. This Documentation is proprietary information of Arcserve and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Arcserve.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Arcserve copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Arcserve that all copies and partial copies of the Documentation have been returned to Arcserve or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, ARCSERVE PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL ARCSERVE BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF ARCSERVE IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is Arcserve.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Contact Arcserve Support

The Arcserve Support team offers a rich set of resources for resolving your technical issues and provides easy access to important product information.

Contact Support

With Arcserve Support:

- You can get in direct touch with the same library of information that is shared internally by our Arcserve Support experts. This site provides you with access to our knowledge-base (KB) documents. From here you easily search for and find the product-related KB articles which contain field-tested solutions for many top issues and common problems.
- You can use our Live Chat link to instantly launch a real-time conversation between you and the Arcserve Support team. With Live Chat, you can get immediate answers to your concerns and questions, while still maintaining access to the product.
- You can participate in the Arcserve Global User Community to ask and answer questions, share tips and tricks, discuss best practices and participate in conversations with your peers.
- You can open a support ticket. By opening a support ticket online, you can expect a callback from one of our experts in the product area you are inquiring about.
- You can access other helpful resources appropriate for your Arcserve product.

Contents

Chapter 1: About Arcserve N-Series Appliance Documentation

Arcserve N-Series Appliance User Guide helps you understand how to use Arcserve N-Series Appliance. To understand about Arcserve N-Series Appliance, see Introduction. Rest of the sections help you install and use Arcserve Appliance.

This section contains the following topics:

Language Support

A translated product (sometimes referred to as a localized product) includes local language support for the user interface of the product, online help and other documentation, as well as local language default settings for date, time, currency, and number formats.

This release is available only in English.

Product Documentation

For all Arcserve UDP related documentation, see Arcserve Documentation.

The Arcserve UDP Knowledge Center consists of the following documentation:

- **Arcserve UDP Solutions Guide**

  Provides detailed information on how to use the Arcserve UDP solution in a centrally-managed Console environment. This guide includes such information as how to install and configure the solution, how to protect and restore your data, how to get reports, and how to manage Arcserve High Availability. Procedures are centered around use of the Console and includes how to use the various protection Plans.

- **Arcserve UDP Release Notes**

  Provides high-level description of the major features, system requirements, known issues, documentation issues, and limitations of Arcserve Unified Data Protection.

- **Arcserve UDP Agent for Windows User Guide**

  Provides detailed information on how to use Arcserve UDP Agent in a Windows operating system. This guide includes such information as how to install and configure the agent and how to protect and restore your Windows nodes.

- **Arcserve UDP Agent for Linux User Guide**

  Provides detailed information on how to use Arcserve UDP Agent in a Linux operating system. This guide includes such information as how to install and configure the agent and how to protect and restore your Linux nodes.

Chapter 2: Introducing the Arcserve N-Series Appliance

This section contains the following topics:

Introduction

Arcserve N-Series Appliance is the first complete and most cost-effective data protection appliance, featuring Assured Recovery™. Each Arcserve N-Series Appliance is a self-contained, "set and forget" backup and recovery solution. Architected with cloud-native capabilities, its unmatched ease of deployment and usability combine with a broad set of features such as global source-based deduplication, multi-site replication, tape support, and automated data recovery capabilities. The Arcserve N-Series Appliance delivers unmatched operational agility and efficiency, and truly simplifies disaster recovery activities.

Arcserve N-Series Appliance is fully integrated with the industry-leading Arcserve Unified Data Protection software pre-installed in state-of-the art hardware. The appliance provides a complete and integrated data protection solution for all users to not only meet your current demands, but also the ever-changing backup, archive, and disaster recovery (DR) requirements of the future.

Arcserve N-series appliance, a hyper-converged data protection solution delivers a turnkey business continuity solution for modern enterprises, combining industry-leading hyper-converged infrastructure, cutting-edge cyber-security, and trusted backup and disaster recovery in a single cloud-scale DR solution. Arcserve N-series appliance also delivers a secure cloud-scale disaster recovery for enterprises, protecting their critical IT infrastructure from downtime, data loss, and ransomware.

N series-Single solution combines hyper-converged data center solution, integrated backup, and disaster recovery, integrated cyber-security and ransomware protection, assured recovery with SLA monitoring, for reliable recovery, cloud backup, and disaster recovery.

Customers who purchased Arcserve N-Series Appliance are entitled to receive the following software. For more information about how to install these software, see the Deployment section.

- Arcserve UDP
- Arcserve Unified Data Protection Agent for Linux
- Nutanix AOS
- Nutanix AHV
- Sophos Intercept X

For more information about Appliance warranty, see Appliance Warranty.

Arcserve Unified Data Protection

The Arcserve UDP software is a comprehensive solution to protect complex IT environments. The solution protects your data residing in various types of nodes such as Windows, Linux, and virtual machines on VMware ESX Servers or Microsoft Hyper-V Servers. You can back up data to either a local machine or a recovery point Server. A recovery point Server is a central Server where backups from multiple sources are stored.

For more information about supported operating systems, see Compatibility Matrix.

Arcserve UDP provides the following capabilities:

- Back up the data to deduplication/non-deduplication data stores on recovery point Servers
- Back up recovery points to tape, using integration with Arcserve Backup (which is also included within the appliance)
- Create virtual standby machines from backup data
- Replicate backup data to recovery point Servers and remote recovery point Servers
- Restore backup data and performs Bare Metal Recovery (BMR)
- Copy selected data backup files to a secondary backup location
- Configure and manage Arcserve Full System High Availability (HA) for critical Servers in your environment

Arcserve UDP replicates backup data that is saved as recovery points from one Server to another recovery point Server. You can also create virtual machines from the backup data that can act as standby machines when the source node fails. The standby virtual machine is created by converting recovery points to VMware ESX or Microsoft Hyper-V virtual machine format.

The Arcserve UDP solution provides integration with Arcserve High Availability. After you create scenarios in Arcserve High Availability, you can then manage and monitor your scenarios and perform operations like adding or deleting destination machines.

For more information, see Arcserve UDP Solution Guide.

Arcserve Unified Data Protection Agent for Linux

Arcserve Unified Data Protection Agent for Linux is a disk-based backup product that is designed for Linux operating systems. It provides a fast, simple, and reliable way to protect and recover critical business information. Arcserve Unified Data Protection Agent for Linux tracks changes on a node at the block level and then backs up only those changed blocks in an incremental process. As a result, it lets you perform frequent backups, reducing the size of each incremental backup (and the backup window) and providing a more up-to-date backup. Arcserve Unified Data Protection Agent for Linux also provides the capability to restore files or folders and perform a bare metal recovery (BMR) from a single backup. You can store the backup information either on a Network File System (NFS) share or in the Common Internet File System (CIFS) share, in the backup source node.

The latest version of Arcserve Unified Data Protection Agent for Linux is pre-installed in a virtual machine within the appliance. This virtual machine becomes the Linux Backup Server. Arcserve Unified Data Protection Agent for Linux is installed at the default installation path in the Arcserve N-Series Appliance.

When you open the Console, the Linux Backup Server is already added to the Console. The native host name of the Linux Backup Server is *Linux-BackupSvr*. However, on the Console, the Linux Backup Server adopts the host name of the Appliance with port 8018 configuration. The Linux Backup Server works behind NAT through port direction. The Linux Backup Server uses port 8018 to communicate and transfer data in the Arcserve N-Series Appliance.

Note: For more information about creating backup plans and restoring Linux machines, see Arcserve UDP Agent for Linux User Guide.

The Linux Backup Server uses the following default login information:

- Username – root
- Password – Arcserve

Note: We recommend to change the default password.

Safety Precautions

For your safety, read and follow all the instructions before attempting to unpack, connect, install, power on, or operate an Arcserve N-Series Appliance. Failure to adhere to the safety precautions can result in personal injury, equipment damage, or malfunction.

For more information about the safety precautions, see the Safety Precautions Appendix.

What is Not Included in the Box of Arcserve N-Series Appliance

The following items are not included in the box and may be needed for installation and configuration of the appliance:

- Monitor
- Keyboard
- External Storage Device (if needed)

Model N-Series

Arcserve N-Series Appliance Specifications				
Appliance Model	**N1100-4**	**N1200-4**	**N1400-4**	**N1600-4**
Data Protection Software	Arcserve UDP Premium Edition Included			
Hyperconvergence Platform	**Nutanix AOS for AHV Included**			
Cybersecurity Soft-ware	**Sophos Intercept X Advanced for Server Included**			
Rack size per node	2U - 4 nodes built-in	1U	2U	2U
Minimum number of nodes per cluster	4	4	4	4
HDD per node	9.6 TB	32 TB	96 TB	20 TB
SSD per node	15.36 TB			
RAM per node	512 GB	384 GB	384 GB	384 GB
Networking per node	Mellanox ConnectX-4 LX Dual Port 10/25GbE SFP28, rNDC 406-BBLG			
Processor per node	Intel Xeon Silver 4214R 2.4G, 12C/24T, 9.6GT/s, 16.5M Cache, Turbo, HT (100W) DDR4-2400 338-BVJX			
Cores per node	24			
Raw capacity per cluster	100 TB	189 TB	445 TB	540 TB
Usable capacity per cluster	40 TB	80 TB	160 TB	240 TB
Drives per cluster	24	16	48	48
Replication Fact-or/Failover Plan	RF2 (N+1)			

Scale-out Node (add-on)				
Appliance Model	**N1100***	**N1200**	**N1400**	**N1600**
Rack size per node	2U - 4 nodes built-in	1U	2U	2U
Number of nodes	4	1	1	1
HDD per node	9.6 TB	32 TB	96 TB	20 TB
SDD per node	15.36 TB	15.35 TB	15.36 TB	15.36 TB
RAM per node	512 GB	384 GB	384 GB	384 GB
Raw capacity per cluster	100 TB	47 TB	111 TB	135 TB
Usable capacity per cluster	40 TB	25 TB	50 TB	70 TB
Networking per node	Mellanox ConnectX-4 LX Dual Port 10/25GbE SFP28, rNDC 406-BBLG			
Processor per node	Intel Xeon Silver 4214R 2.4G, 12C/24T, 9.6GT/s, 16.5M Cache, Turbo, HT (100W) DDR4-2400 338-BVJX			

Ports Used by the Appliance

The following topics provide information about ports that are used by Arcserve UDP, Arcserve Backup, and the Appliance for Linux Support:

- Arcserve UDP
- Appliance for Linux Support

Arcserve UDP

This section contains the following topics:

Components Installed on Microsoft Windows

The following ports are required for backup and other jobs when you have a LAN environment:

Port #	Port Type	Initiated by	Listening Process	Description
1433	TCP	Remote Java	sqlsrvr.exe	Specifies the default communication port between the Arcserve UDP console and Microsoft SQL Server databases when they reside on different computers. **Note**: You can modify the default communication port when installing SQL Server.
4090	TCP	Arcserve UDP Agent	HATransServer.exe	Transfers data for Virtual Standby tasks in the proxy mode.
5000-5060	TCP	Arcserve UDP Server	GDDServer.exe	Reserved for Arcserve UDP RPS Global Deduplication Data Store Service (GDD). One Arcserve UDP GDD data store will use 3 free ports

				that start from 5000. It is needed when the data store with GDD is enabled for backup or the restore task is used.
6052	TCP	Arcserve Backup GDB	CA.ARCserve.CommunicationFoundation. WindowsService.exe	Com-munication that lets the Arcserve UDP Console and the Arcserve Backup Global Dashboard Primary Server syn-chronize data.
6054	TCP	Arcserve Backup	CA.ARCserve.Com-municationFoundation.WindowsService.exe	Com-munication that lets the Arcserve UDP Console and the Arcserve Backup Primary Server syn-chronize data.
8006				To shut down Tomcat that is used by the Arcserve UDP console.
8014	TCP	Arcserve UDP Console	Tomcat7.exe	Specifies the default HTTP/HTTPS com-munication port between remote man-agement con-soles and the

				Arcserve UDP Server. Specifies the default HTTP/HTTPS communication port between remote management consoles and the Arcserve UDP Agent. **Note**: You can modify the default communication port when you install the Arcserve UDP components.
8014	TCP	Arcserve UDP Server	httpd.exe	Specifies the default HTTP/HTTPS communication port between the Arcserve UDP Server and Arcserve UDP consoles. *Specifies the default shared port and the only port you must open when you use the Arcserve UDP Server as the replication destination. Do not open ports 5000-5060 which

				are used by data stores that have global deduplication enabled. **Note**: You can modify the default communication port when you install the Arcserve UDP components.
8015	TCP	Arcserve UDP Console	Tomcat7.exe	Specifies the default HTTP/HTTPS communication port between remote management consoles and the Arcserve UDP Server. Specifies the default HTTP/HTTPS communication port between remote management consoles and the Arcserve UDP Agent. **Note**: You can modify the default communication port when you install the Arcserve UDP components.

8016	TCP	Arcserve UDP Server	Tomcat7.exe	Reserved for Arcserve UDP Server Web Services to communicate with the Arcserve UDP RPS Port Sharing Service on the same Server. **Note**: The port cannot be customized and can be ignored for the firewall setting.
1800-5			CA.ARCserve.CommunicationFoundation.WindowsService.exe	To shutdown Tomcat that is used by the Arcserve UDP Server or Agent.

Components Installed on Linux

The following ports are required for backup and other jobs when you have a LAN environment:

Port #	Port Type	Initiated by	Listening Process	Description
22	TCP	SSH service		Arcserve UDP Linux third party dependency. Specifies the default for SSH service, however, you can change this port. This port is required for both incoming and outgoing communications.
67	UDP	Arcserve UDP Linux	bootpd	Used for the PXE boot Server. Only required if the user wants to use the PXE boot feature. This port is required for incoming communications. **Note**: The port number cannot be customized.
69	UDP	Arcserve UDP Linux	tffpd	Used for the PXE boot Server. Only required if the user wants to use the PXE boot feature. This port is required for incoming communications. **Note**: The port number cannot be customized.
8014	TCP	Arcserve UDP Linux	Java	Specifies the default HTTP/HTTPS communication ports between the remote consoles and the Arcserve UDP agent for Linux. This port is required for both incoming and outgoing communications.
18005	TCP	Arcserve UDP Linux	Java	Used by Tomcat, can be ignored for firewall settings.

Node Protected by UDP Linux Remotely

The following port is required for backup and other jobs when you have a LAN environment:

Port #	Port Type	Initiated by	Listening Process	Description
22		SSH service		Arcserve UDP Linux 3rd party dependency. Specifies the default for the SSH service, however, you can change this port. This port is required for both incoming and outgoing communications.

*Port sharing is supported for replication jobs. All data on different ports can be forwarded to port 8014 (default port for the Arcserve UDP Server, which can be modified during installation). When a replication job runs between two recovery point Servers across WAN, only port 8014 needs to be opened.

Similarly, for remote replications, the Remote administrator needs to open or forward port 8014 (for data replication) and port 8015 (default port for the Arcserve UDP console, which can be modified during installation) for local recovery point Servers to obtain the assigned replication plan.

Appliance for Linux Support

The following ports are required for backup and other jobs when you have a LAN environment:

Port #	Port Type	Initiated by	Listening Process	Description
8017	TCP			NAT port redirection, redirects 8017 on appliance to the Linux backup server in order to backup other Linux node to Amazon S3.
8018	TCP			NAT port redirection, redirects 8018 on appliance to the Linux Backup Server Agent port 8014.
8019	TCP			NAT port redirection, redirects 8019 on appliance to the Linux Backup Server SSH port 22.
8021	TCP			NAT port redirection, redirects 8021 on appliance to Linux backup server to backup other Linux node using 8021 port.
8036	TCP			NAT port redirection, redirects 8036 on appliance to the Linux Backup Server port 8036.
50000	TCP			NAT port redirection, redirects 50000 on appliance to Linux backup server in order to backup other Linux node to cloud using 50000 port.
50001	TCP			NAT port redirection, redirects 50001 on appliance to Linux backup server in order to backup other Linux node to cloud using 50001 port.
50002	TCP			NAT port redirection, redirects 50002 on appliance to Linux backup server in order to backup other Linux node to cloud using 50002 port.
50003	TCP			NAT port redirection, redirects 50003 on appliance to Linux backup server in order to backup other Linux node to cloud using 50003 port.
50004	TCP			NAT port redirection, redirects 50004 on appliance to Linux backup server in order to backup other Linux node to cloud using 50004 port.

Chapter 3: Installing the Arcserve N-Series Appliance

The appliance is intended for installation in restricted areas only. Only qualified personnel should perform initial setup and maintenance. For the complete installation process of Arcserve N-Series appliance, see the following:

- Appliance N Series Installation - Large Node
- Appliance N Series Installation - Medium Node
- Appliance N Series Installation - Small Node

Chapter 4: Deploying the Arcserve N-series Appliance

This section provides information about how to deploy the Arcserve N-series appliance.

Follow these steps:

1. Unpack the Nutanix nodes.
2. Mount the node in a rack.

   Notes:

   - For more information about how to unpack and mount the N-Series Appliance into a rack, see the following hardware installation guides:
     - Installation Guide for Large Node
     - Installation Guide for Medium Node
     - Installation Guide for Small Node
   - For more information about how to unpack and mount the block into a rack, see Dell support website.
3. Connect each node to the ethernet network through a network switch.

   For more information about how to connect each node to a network switch, see Connecting the Nodes.
4. Power-on the nodes. Once the power is switched on, each node will get an IP address automatically if the DHCP server is accessible to the nodes. If the DHCP server is not available, manually assign the static IP address to each node.
5. Install Nutanix foundation-5.1.1-Windows software on the VM in the same subnet where the Nutanix blocks or nodes are connected. To download the Nutanix foundation-5.1.1-Windows software, click here.
6. Form a Mine Cluster with AHV as the hypervisor.
7. Create a Nutanix Object Store.
8. Upload the bootstrap VM Disk image and Windows 2019 ISO image.
9. Create a bootstrap VM.
10. Deploy Nutanix Mine.

Review Prerequisites

Verify that you have completed the following prerequisite tasks:

- Assigned the DNS Server for UDP Console and UDP LBS hostname resolution.
- Assigned the DHCP server for dynamic IP address assignment for UDP Console and UDP LBS.

For Cluster Formation

- Nutanix foundation-5.1.1-Windows software is installed on the VM.
- Must have 18 Static or DHCP reserved IP addresses.
- Make sure to have Current Network Subnet IP and Gateway IP to discover the Nutanix nodes.
- Windows 2019 VM is installed in the same subnet as Nutanix Cluster connected.

For Object Store Deployment

- Object Network Switch is created.
- Must have 17 static or DHCP IP addresses.

How to Connect to Nodes

After installing the blocks in a rack, connect the nodes to a network through a network switch and then power-on the nodes. This section provides information about how to connect to nodes through a network switch.

Note: All the ports on the network must be in the same VLAN.

Follow these steps:

1. Connect the iDRAC port and data-only port, which are on the node to a network switch.
2. Connect the 1 GbE port on your device to the network switch data port.
3. Plug in the power cables, and then press the power button on the control panel for each node.
4. To verify whether each node is powered on, check the LED lights.

The nodes are connected to a network switch successfully.

How to Form a Nutanix Cluster

Start the cluster formation using the Nutanix foundation-5.1.1-Windows software deployed on the VM in the same subnet where the Nutanix blocks, or nodes are connected. This section provides information about how to form a Nutanix cluster.

Follow these steps:

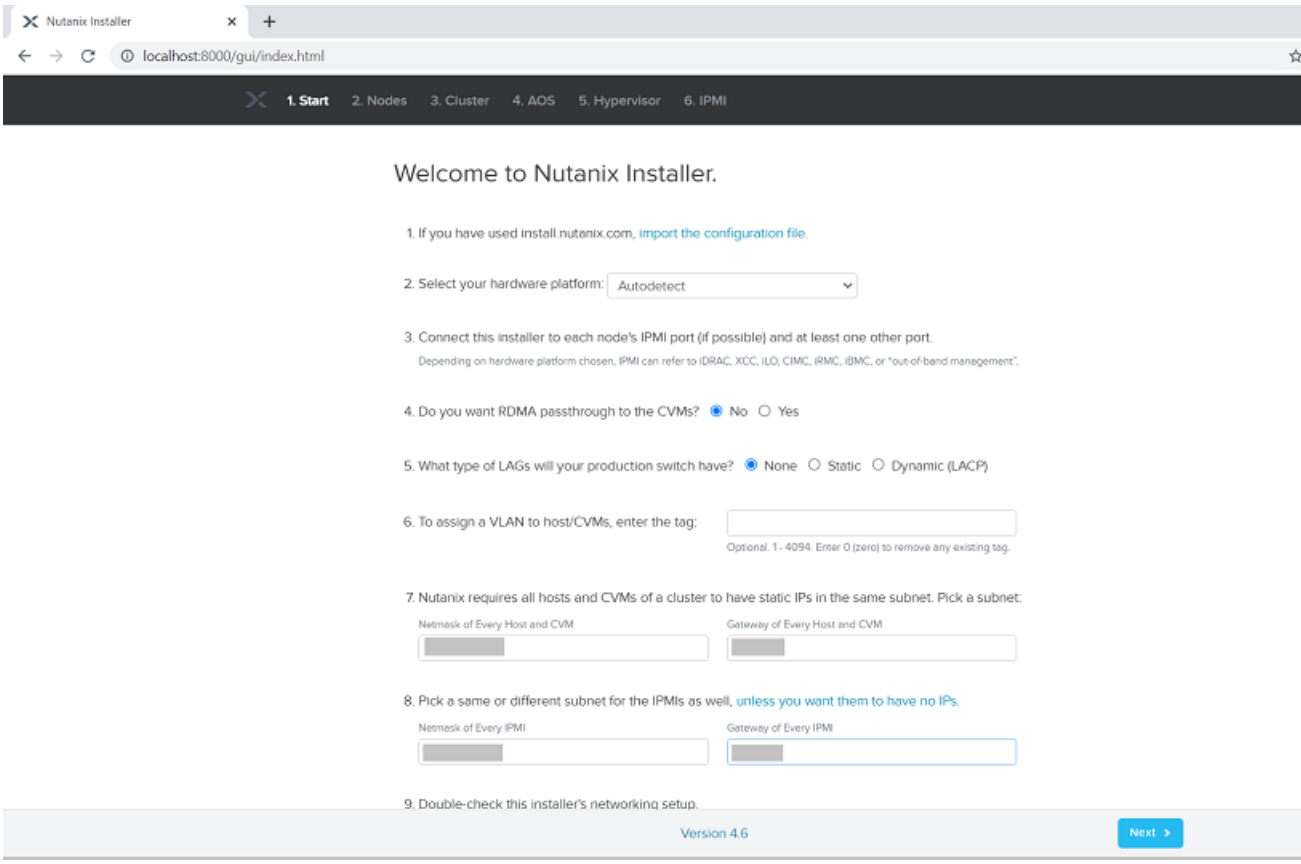
1. Open any browser, type the following URL in the address bar, and then press Enter to discover the Nutanix nodes.

   http://localhost:8000

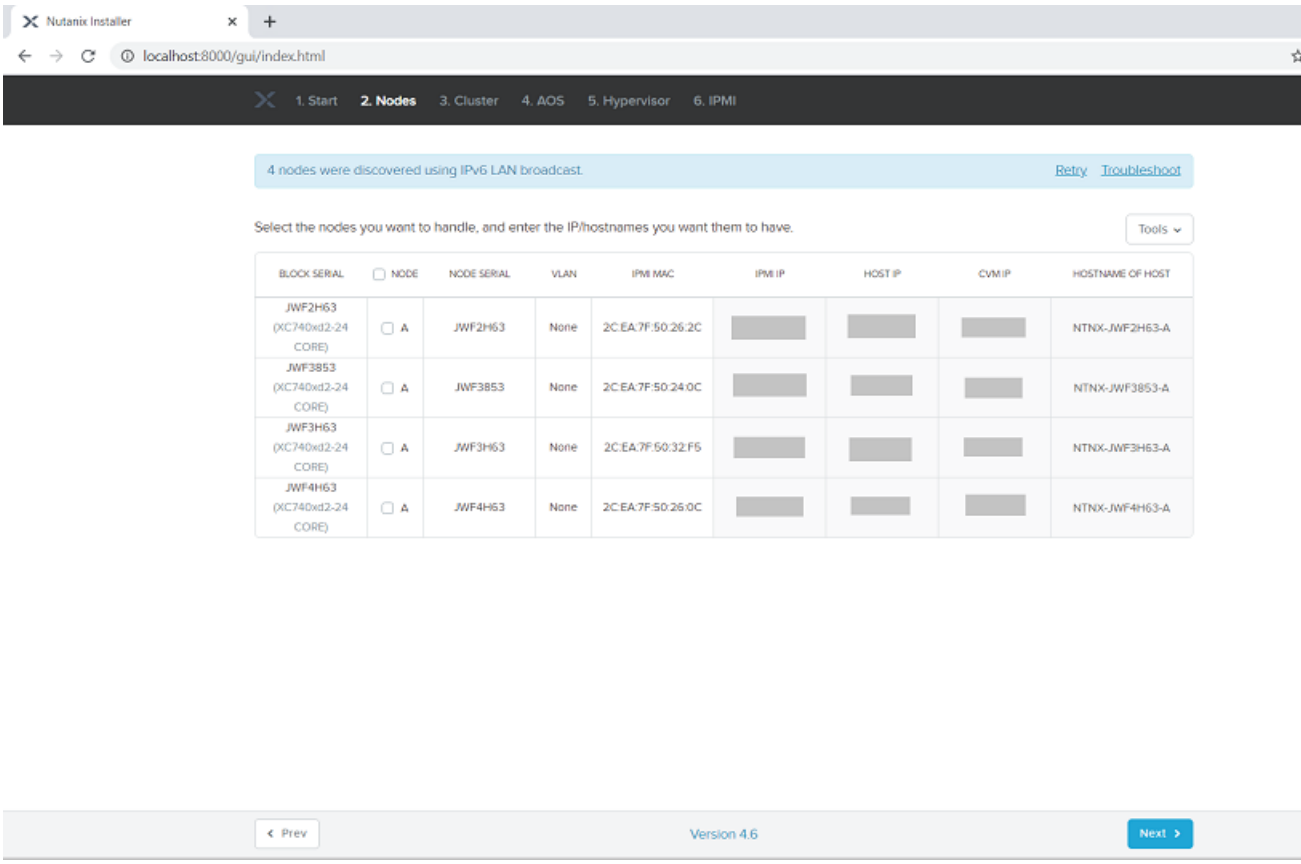
   The Nutanix Installer page appears with nodes in the specified subnet discovered and listed.

2. On the Start page, follow the instructions given in sequence. Select the appropriate input as needed, enter the following details, and then click **Next**:

   - **Netmask of Every Host and CVM:** Enter the netmask subnet of the Controller VM and hypervisor.
   - **Gateway of Every Host and CVM:** Enter the IP address of the gateway that a Controller VM and a hypervisor should use.
   - **Netmask of Every IPMI:** Enter the netmask of the IPMI subnet.
   - **Gateway of Every IPMI:** Enter the IP address of the gateway for the IPMI subnet.



3. On the Nodes page, select the nodes that you want to add to the Nutanix cluster, and then click **Next**.



Notes:

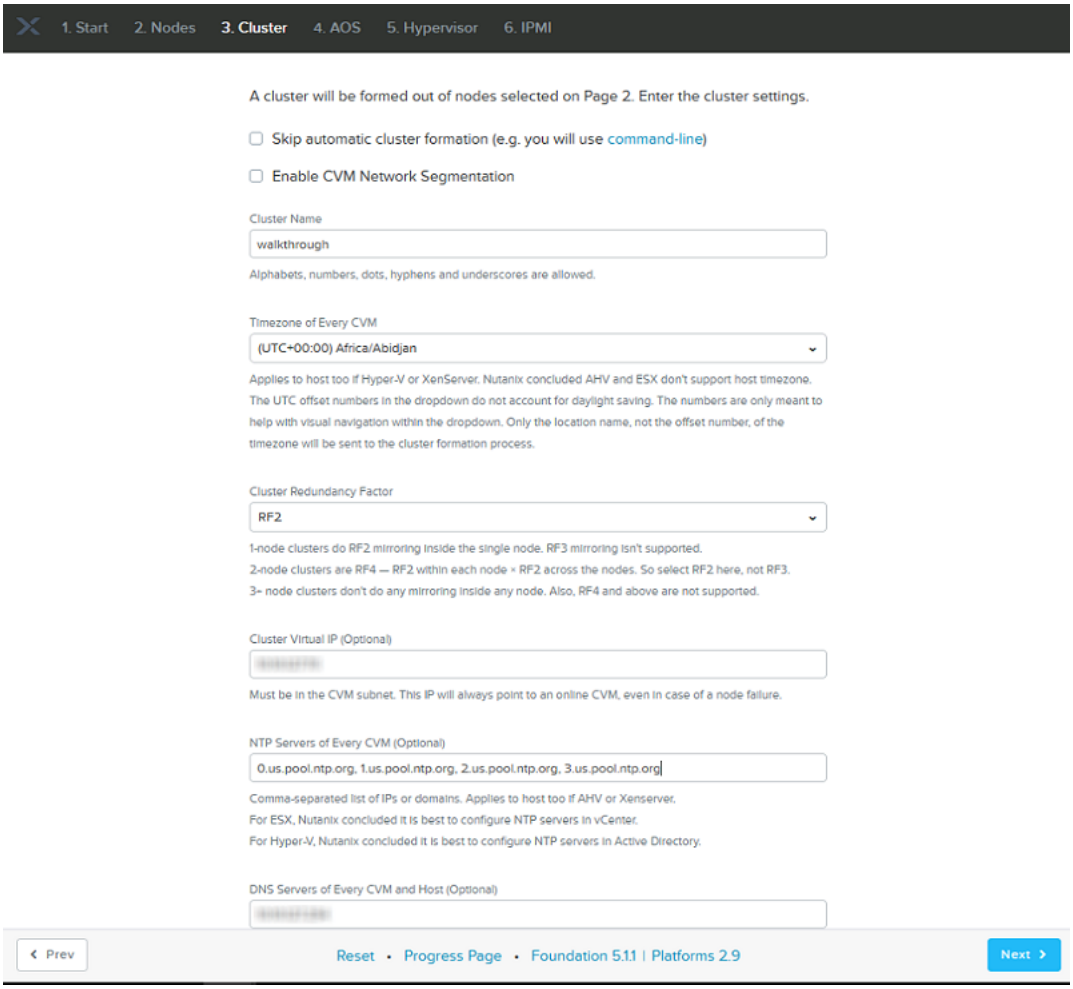
- Nodes that are part of other clusters also get listed but cannot be selected.
- All the 12 IP addresses (IPMI, host, and CVM) must be from the same subnet as the Nutanix cluster.
- To remove the unselected nodes, click the **Tools** drop-down list on the top-right corner, and then click **Remove Unselected Rows**.

4. On the Cluster page, do the following, and then click **Next**:
   - **Cluster Name:** Type a name for the cluster.
   - **Timezone of Every CVM:** From the drop-down list, select the appropriate time zone.
   - **Cluster Virtual IP (Optional):** Enter the virtual IP address of the cluster.
   - **NTP Servers of Every CVM:** Enter a list of NTP server IP addresses or domain names separated by commas. This is mandatory for Object Store creation.

Note: For more information about NTP server recommendations, see Nutanix documentation.

- **DNS Servers of Every CVM and Host (Optional):** Enter a list of DNS server IP addresses separated by commas. This field is required only if you have specified the NTP server as its domain name.
- **vRAM Allocation for Every CVM, in Gigabytes:** Enter the RAM in Gigabytes to be allocated to each CVM. Alternately, leave the *vRAM Allocation for Every CVM, in Gigabytes* field blank for the system to allocate the recommended defaults.

  Note: The cluster redundancy factor is selected by default based on the number of nodes selected.

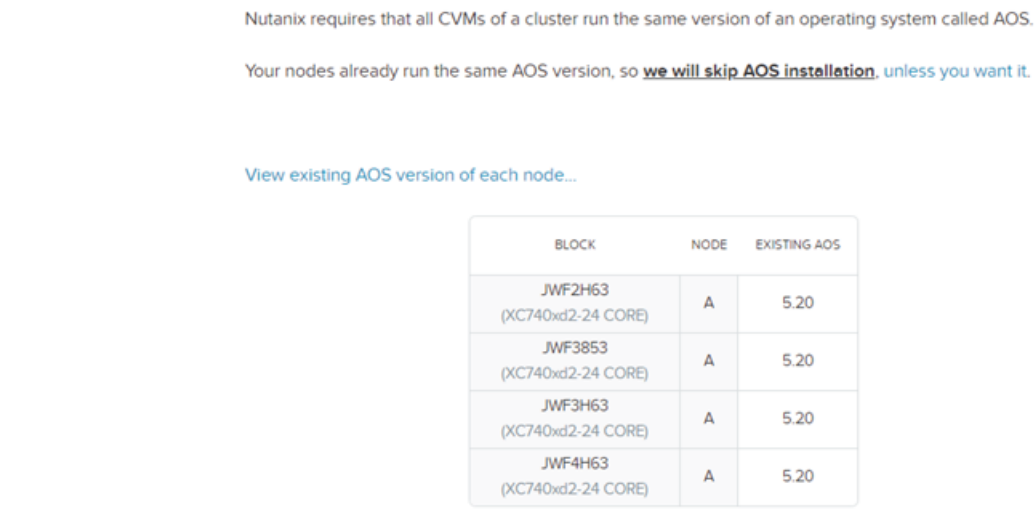


The AOS page appears and displays a table with a list of existing AOS versions for each node.

5. On the AOS page, to view the AOS version installed on each node, click the **View existing AOS version of each node..** link, and then click **Next**.

Notes:

- Nutanix recommends using the latest version of AOS that is suitable to your model.
- Make sure all the blocks in a node run on the same version of AOS. If the blocks are running on different versions, upgrade all nodes to the same version.
- If you want to install the different AOS versions, click the **unless you want it** link.



The Hypervisor page appears and displays a table with a list of AHV ISO images.

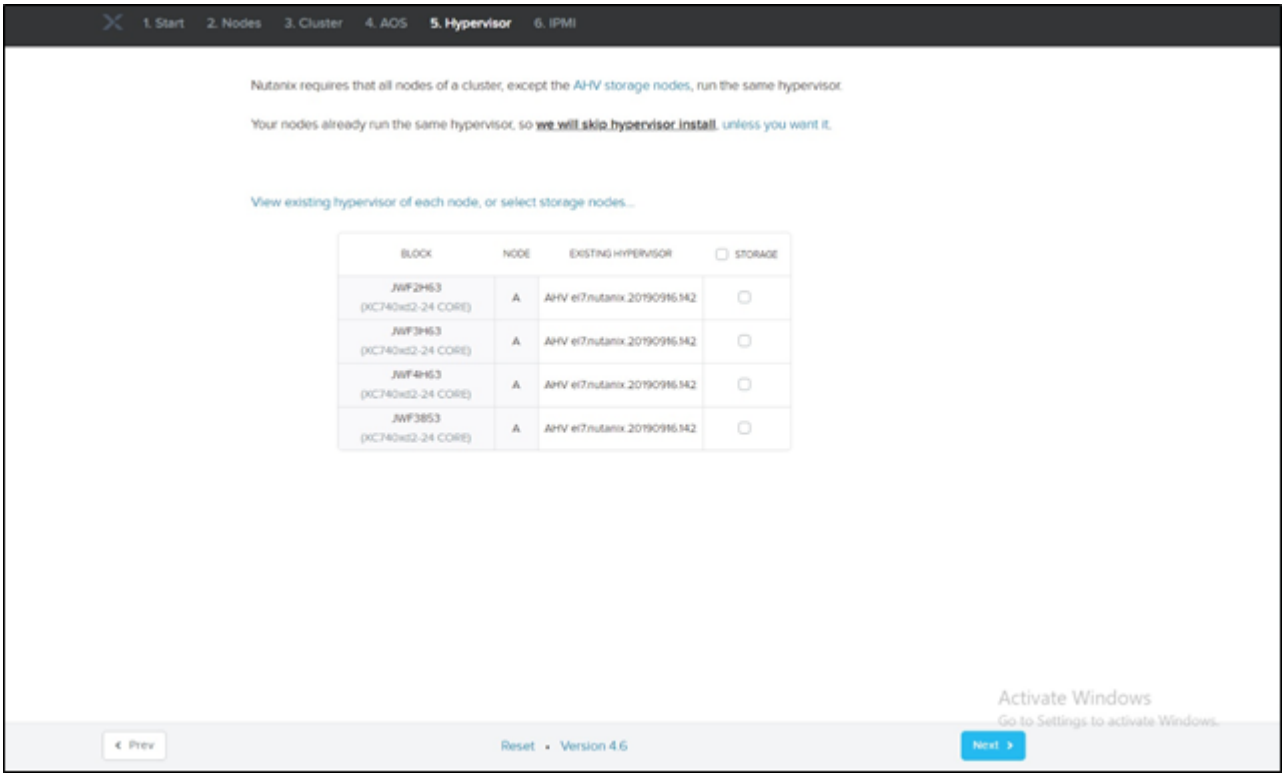
Important! By default, N-Series Appliance nodes are shipped with Arcserve supported Factory-imaged AOS and AHV version.

6. On the Hypervisor page, to view the hypervisor installed on each node or to select the nodes that you want to use for storage, click the **View existing**

hypervisor of each node, or select storage nodes.. link, and then click **Next**.

Notes:

- Make sure all the nodes in a cluster run on the same version of Hypervisor. If the nodes are running on different versions of Hypervisor, upgrade all nodes to the same version.
- If you want to install different hypervisor versions, click the **unless you want it** link.

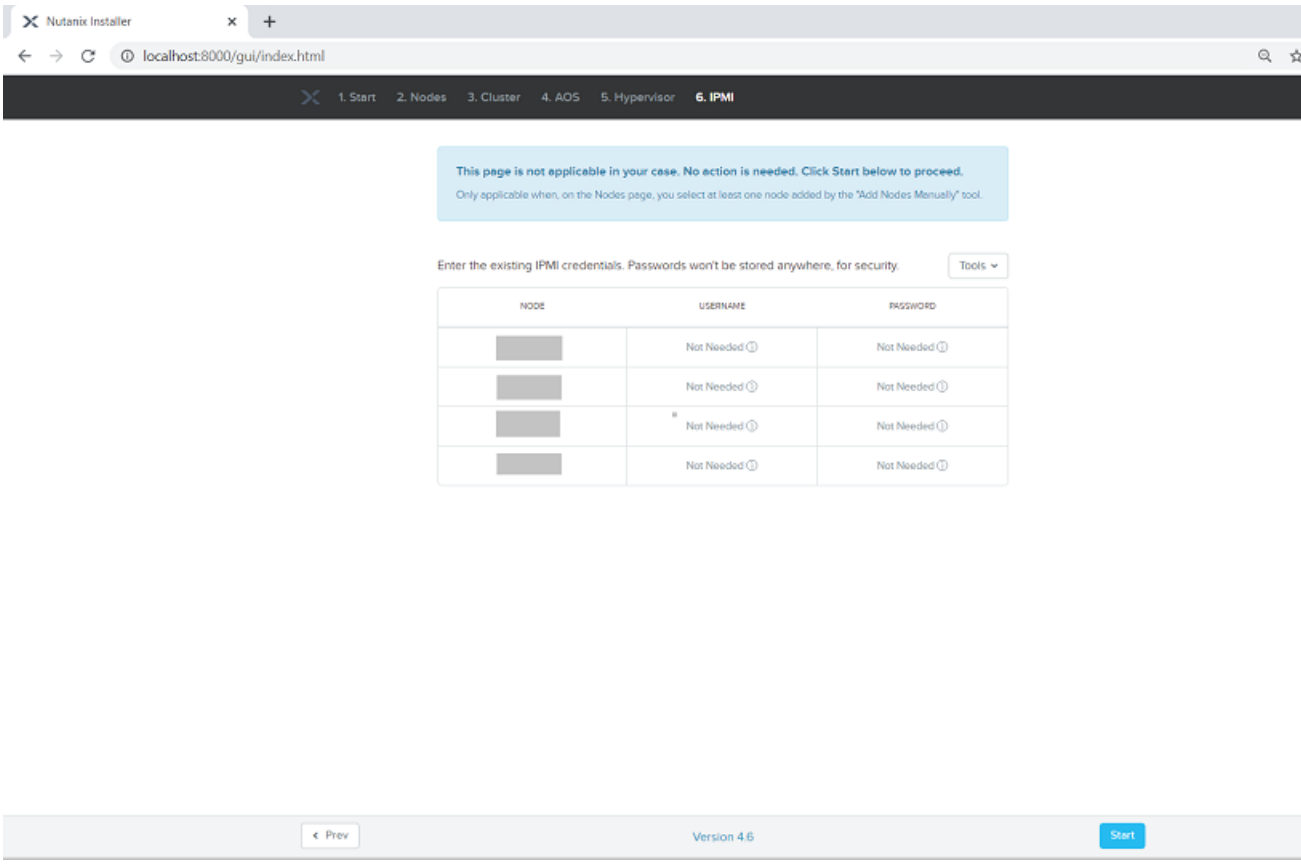


The IPMI page appears and displays a table with a list of selected nodes and prompts you to provide the credentials for each node.

7. On the IPMI page, to start the cluster creation, provide the IPMI credentials (for example, Username: root and Password: calvin), and then click **Start**.

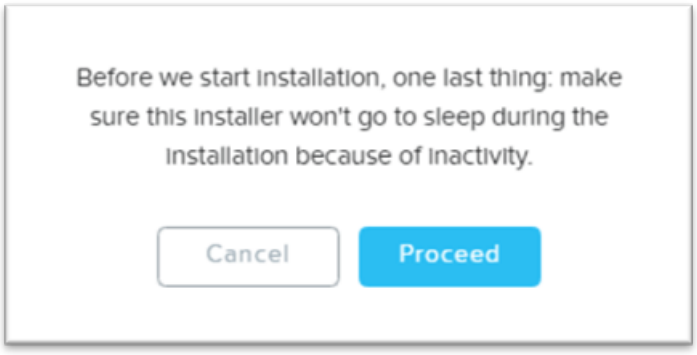
Notes:

- If no node is added manually or converted to manual node, the IPMI credentials are not required. Otherwise, you may need to verify your credentials again.
- The IPMI credentials are also not needed when the Foundation installer is running inside a CVM.

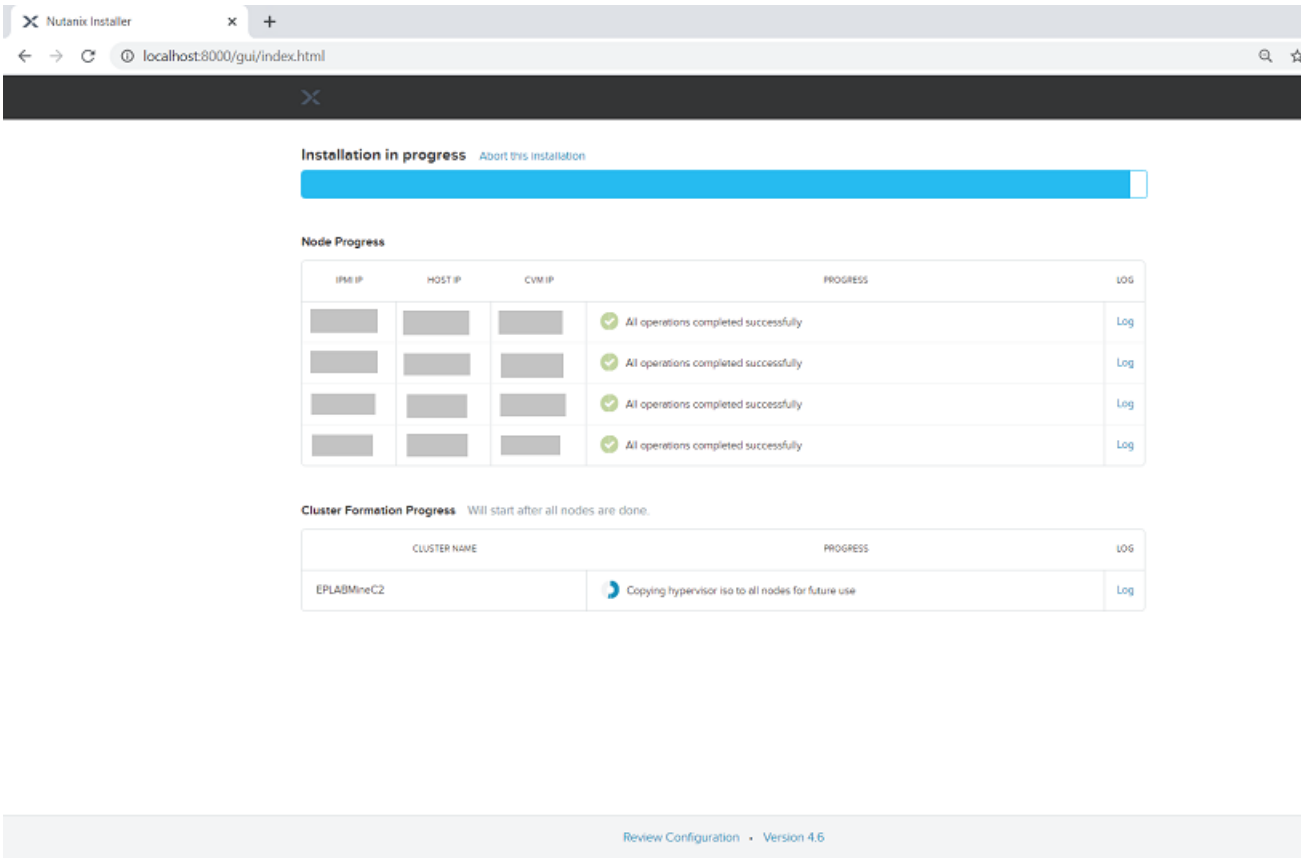


A pop-up dialog appears asking you to make sure your workstation device does not go into sleep during installation.

8. Click **Proceed** to confirm.

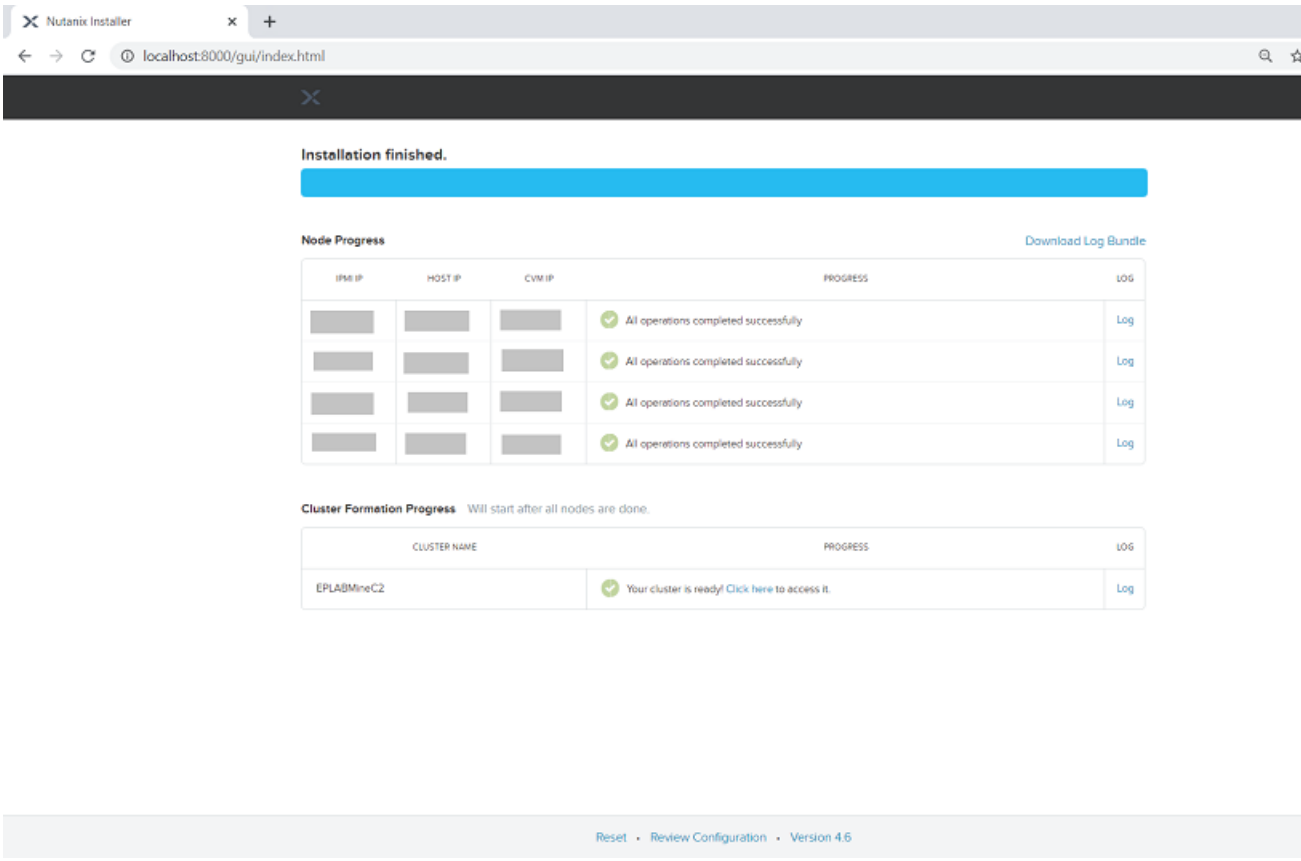


The cluster formation process starts, and the following screen is displayed:



9. After the installation process completes successfully, do the following:
   - To save all the log files, download the bundle file, which contains all the log files. To download the bundle file, click **Download Log Bundle**.
   - To open the Prism Element UI, click the **Click here** link on the Cluster Formation Progress section.

The Prism Element login screen appears.



Note: If the cluster formation fails, download the logs and contact Arcserve Support.

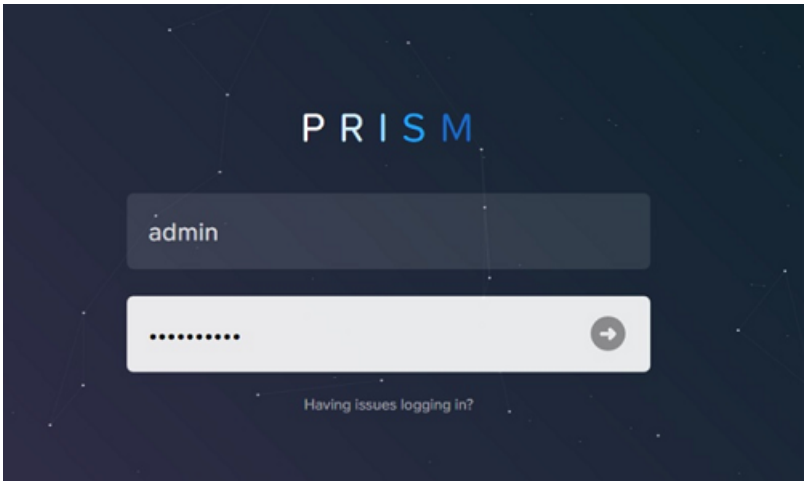
How to Configure Cluster Details from Prism Element

This section provides information about how to configure cluster details from Prism Element.

Note: To configure a cluster, a minimum of 2 IP addresses are required.

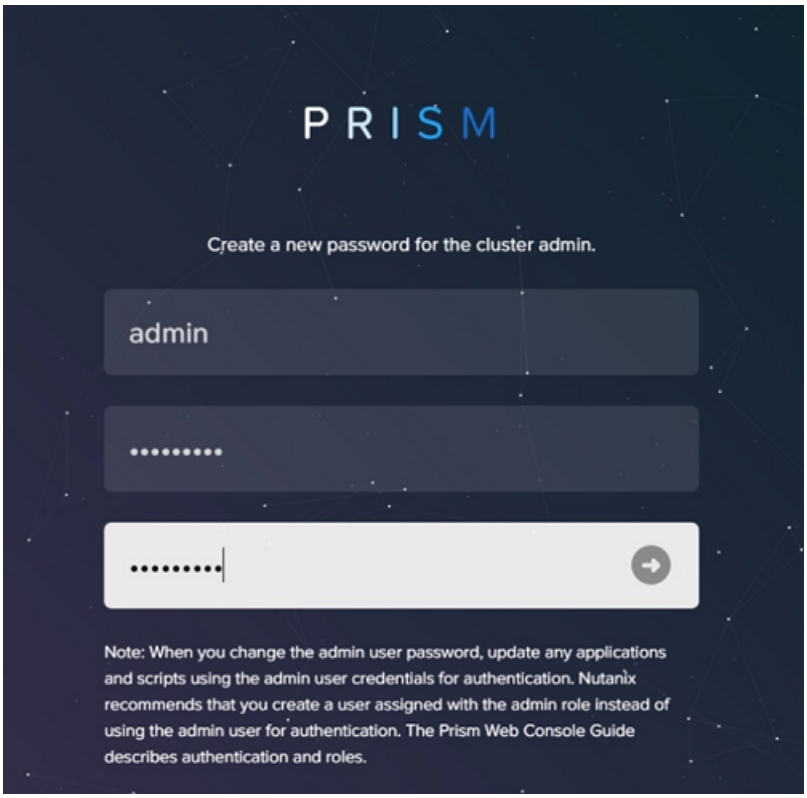
Follow these steps:

1. Log into the Prism Element web console as an admin user using the following credentials:
   - **Username:** admin
   - **Password:** Nutanix/4u



   As soon as you login for the first time, you are prompted to change your password.

2. Enter a new password, re-enter the password to confirm, and then press Enter or click the right arrow icon.



After the password is changed successfully, the new password gets synchronized across all the interfaces and Controller VMs.

3. Login again with the updated credentials.

   The Nutanix End User License Agreement (EULA) and Terms of Use screen appears.

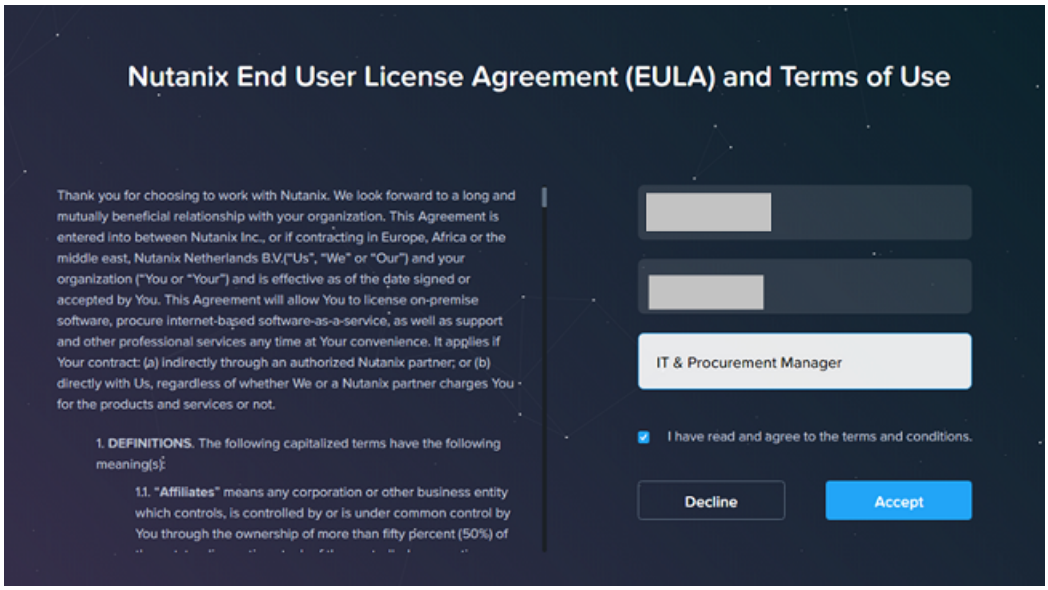
4. On the Nutanix End User License Agreement (EULA) and Terms of Use screen, do the following:

   a. Read the license agreement carefully.

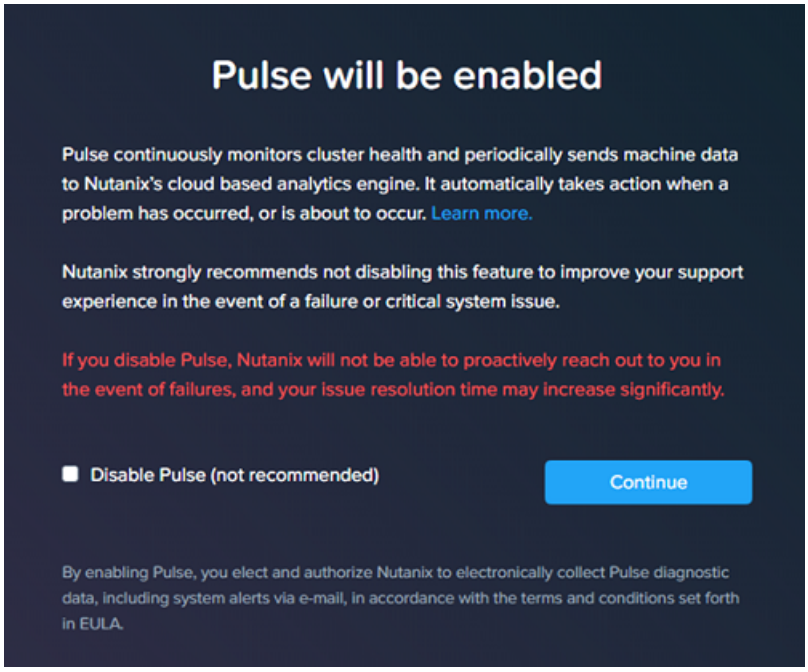
   b. Enter the appropriate information in the **Name**, **Company**, and **Job Title** fields as needed.

   c. Select the **I have read and agree to the terms and conditions** check box.

   d. Click **Accept**.



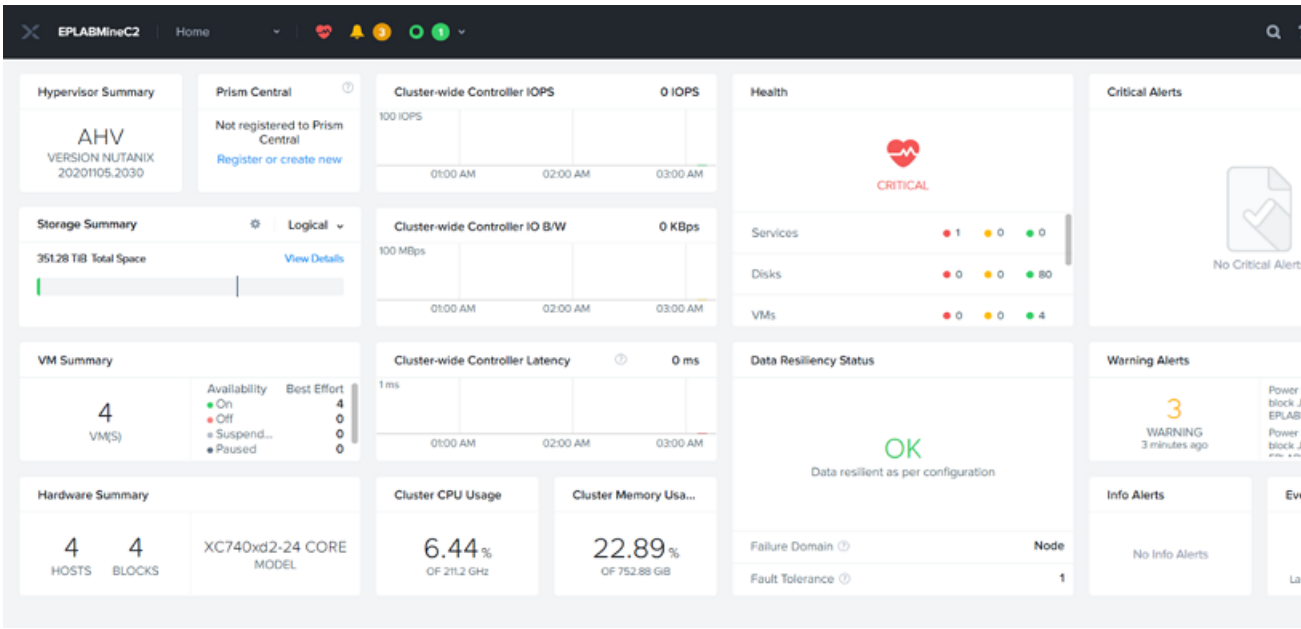
The *Pulse will be enabled* screen appears.



5. On the *Pulse will be enabled* screen, click **Continue**.

   Note: Nutanix does not recommend that you disable Pulse.

   The Prism Element dashboard opens.

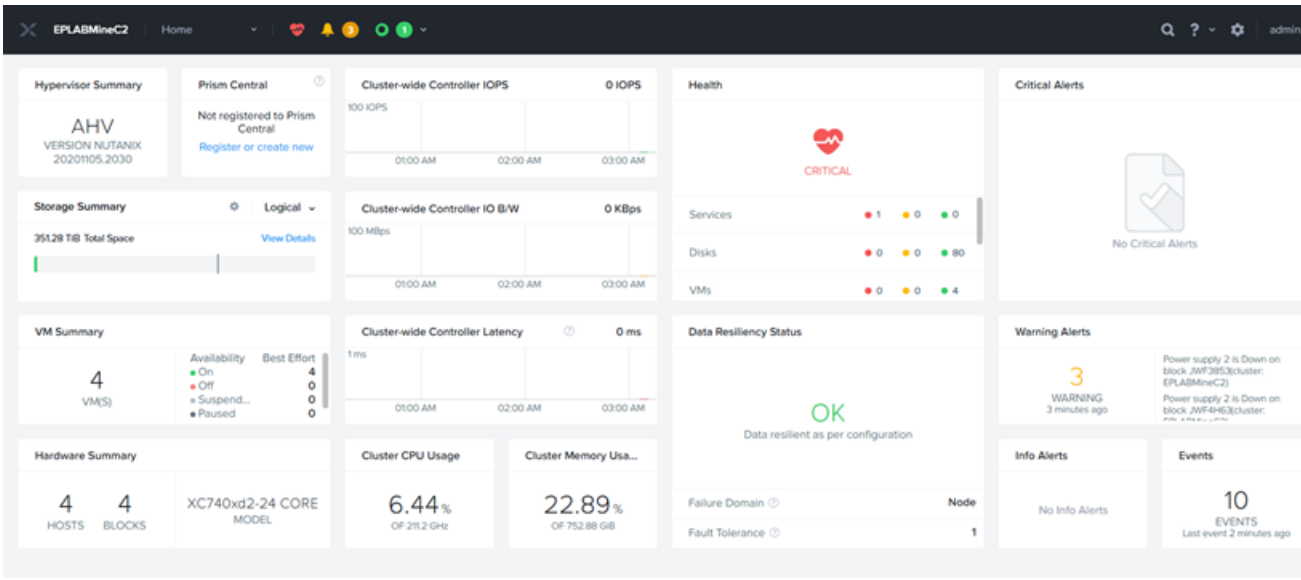

EPLABMineC2
Home
Hypervisor Summary
AHV
VERSION NUTANIX
20201105.2030
Prism Central
Not registered to Prism Central
Register or create new
Cluster-wide Controller IOPS
0 IOPS
100 IOPS
01:00 AM
02:00 AM
03:00 AM
Health
CRITICAL
Services
Disks
VMs
Critical Alerts
No Critical Alerts
Storage Summary
Logical
351.28 TiB Total Space
View Details
Cluster-wide Controller IO B/W
0 KBps
100 MBps
VM Summary
4
VM(S)
Availability
Best Effort
On
Off
Suspend...
Paused
Cluster-wide Controller Latency
0 ms
1 ms
Data Resiliency Status
OK
Data resilient as per configuration
Failure Domain
Node
Fault Tolerance
1
Warning Alerts
3
WARNING
3 minutes ago
Hardware Summary
4
HOSTS
4
BLOCKS
XC740xd2-24 CORE
MODEL
Cluster CPU Usage
6.44 %
OF 211.2 GHz
Cluster Memory Usa...
22.89 %
OF 752.88 GiB
Info Alerts
No Info Alerts

How to Create Network Switch for Cluster Formation

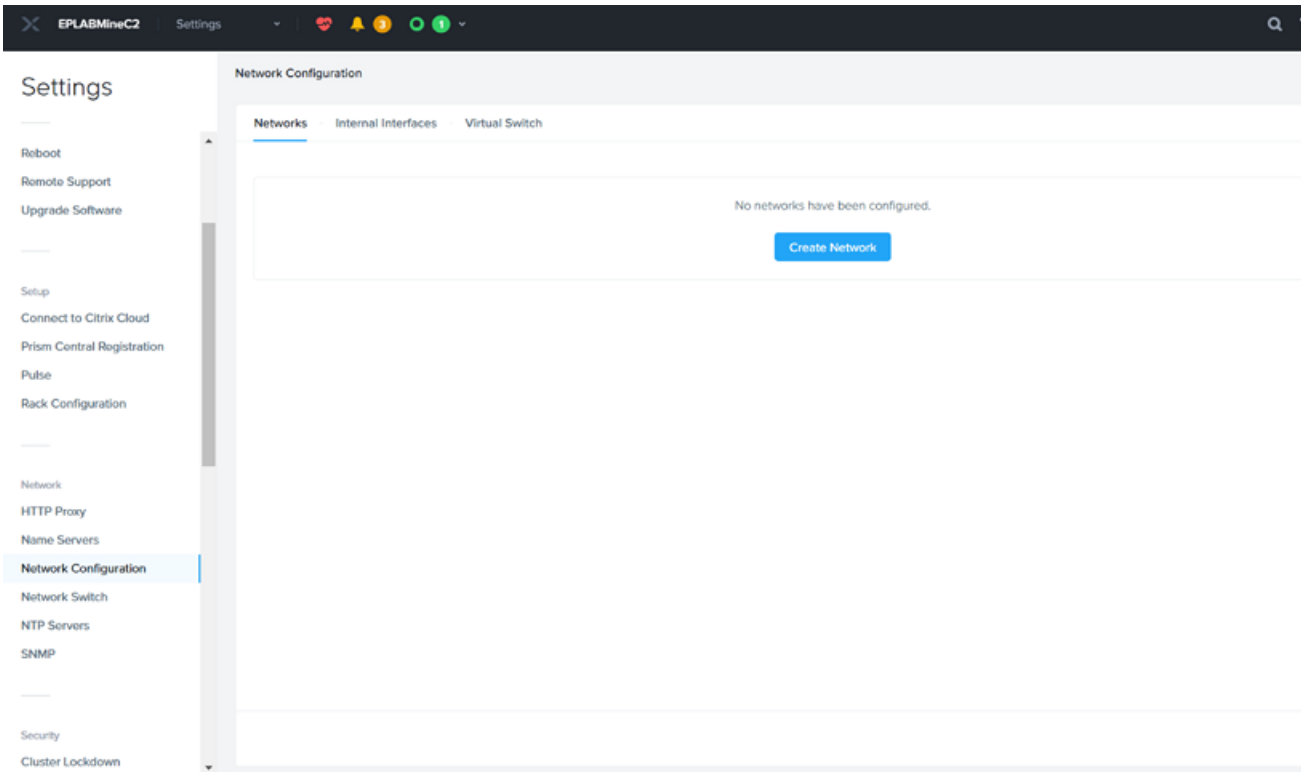
This section provides information about how to create a network switch for cluster formation.

Follow these steps:

1. Log into the Prism Central web console.
2. Click the settings icon on the top-right corner, and then select **Network Configuration**.



3. On the Network Configuration page, click **Create Network**.

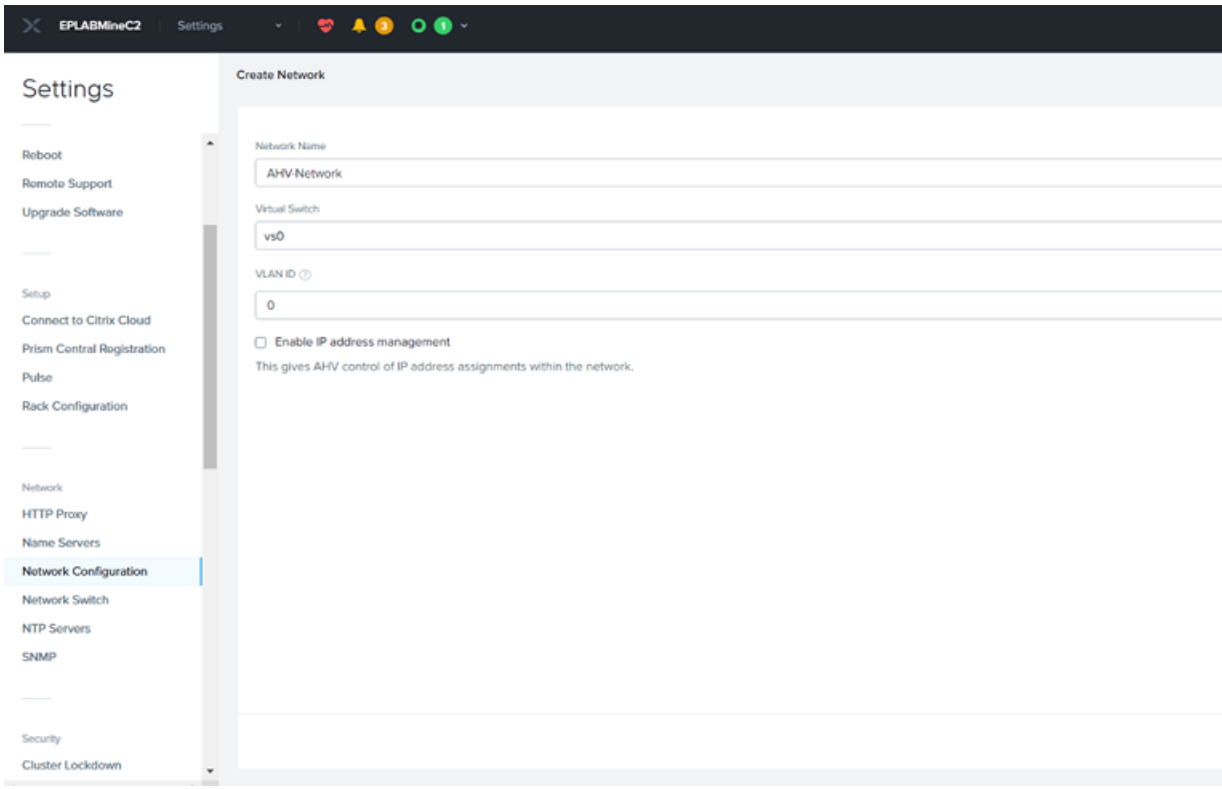


The Create Network page is displayed.

4. On the Create Network page, do the following:
   - **Network Name:** Type a name for the network.

     Note: The Virtual Switch is selected by default.
   - **VLAN ID**: Specify the VLAN number. Enter a number between 1 and 27

or 0 for the native VLAN.



5. Click **Save**.

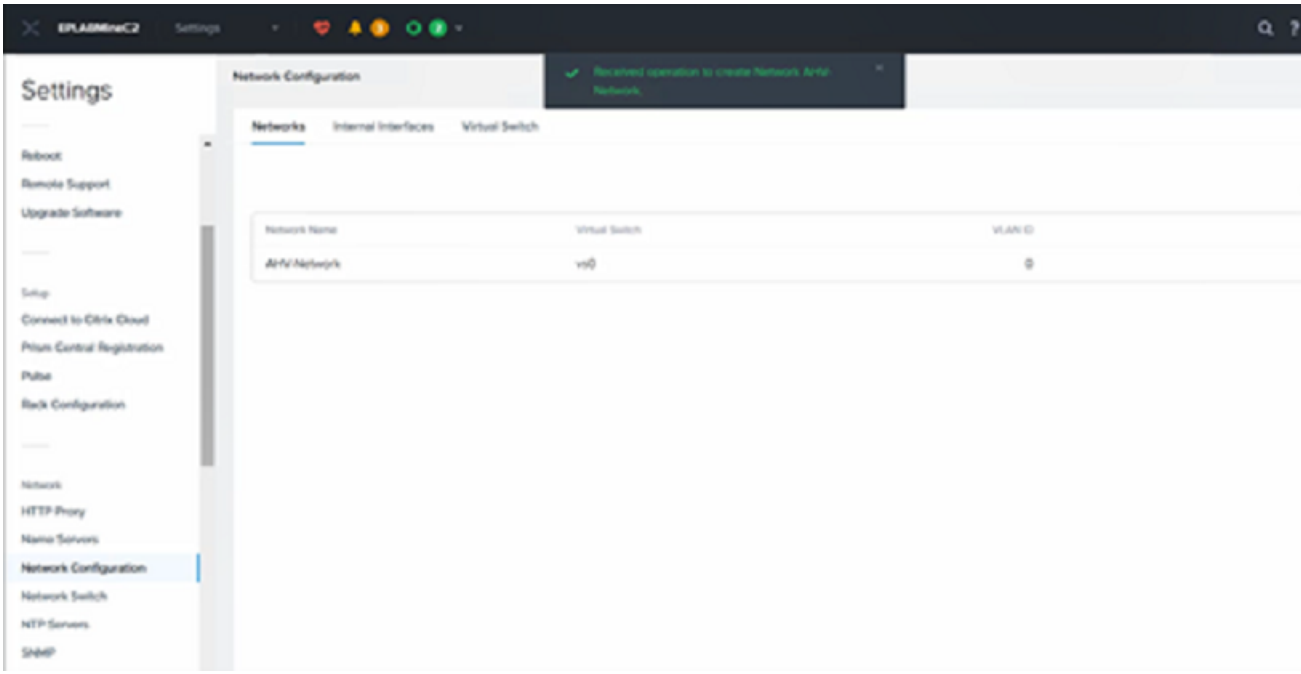
   The network switch is created, and the newly created switch is listed in the Networks tab of the Network Configuration page.

How to Create Network Switch for Object Store

This section provides information about how to create a network switch for the object store.

Follow these steps:

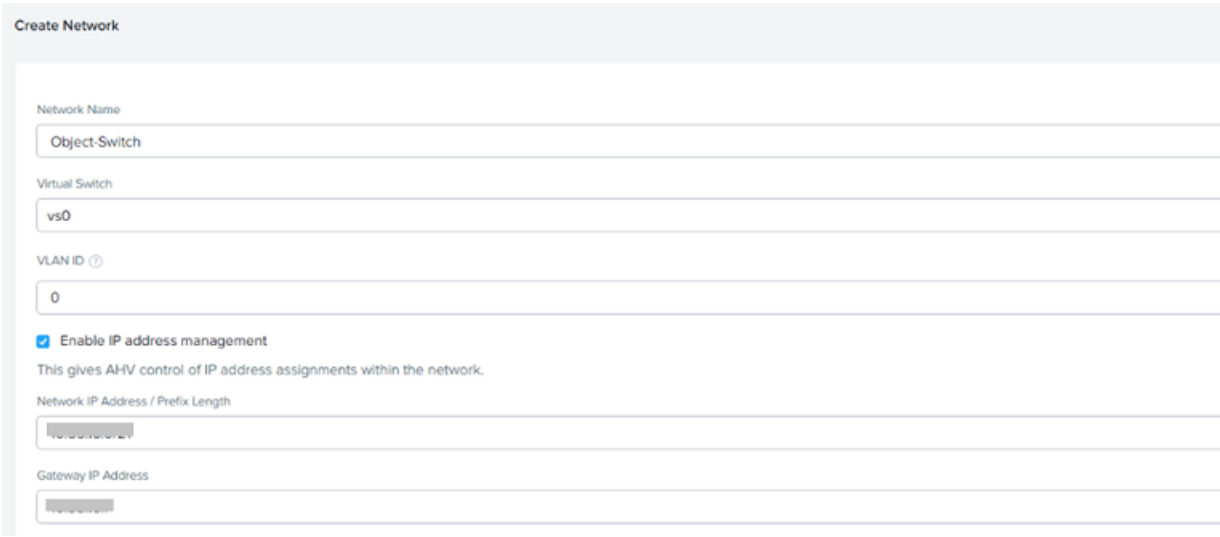
1. Log into the Prism Central web console.
2. Click the settings icon on the top-right corner, and then select **Network Configuration**.
3. On the Network Configuration page, click **+ Create Network**.



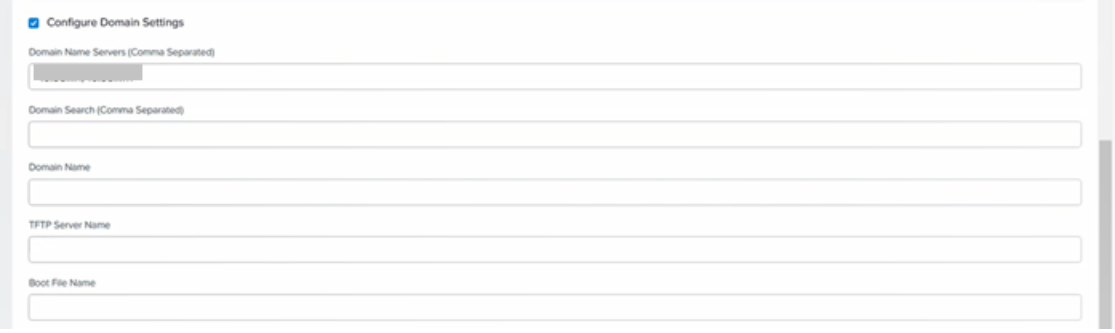
4. On the Create Network page, do the following:
   - **Network Name:** Type a name for the network.

     Note: The Virtual Switch is selected by default.
   - **VLAN ID:** Specify the same VLAN number that is used during the cluster formation.
   - **Enable IP address management:** To have the cluster control IP addressing in the network, select the **Enable IP address management** check box. When selected, the following fields are displayed:
     - **Network IP Address/Prefix Length:** Enter the gateway IP address for the network prefixed with the network prefix.
     - **Gateway IP Address:** Enter the default VLAN gateway IP address.

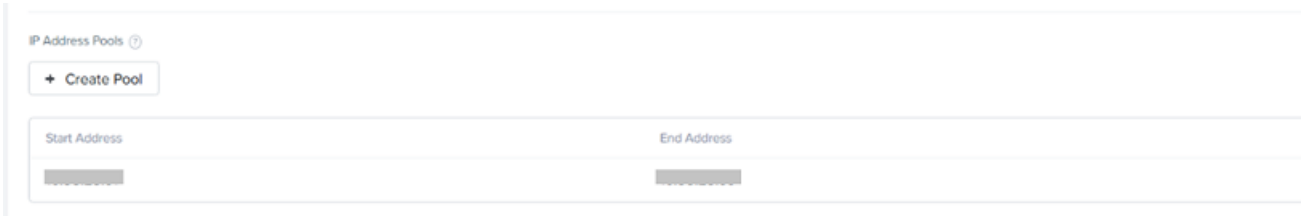
Note: If you did not select the **Enable IP address management** check box, you cannot enable or disable the IP address management (IPAM).



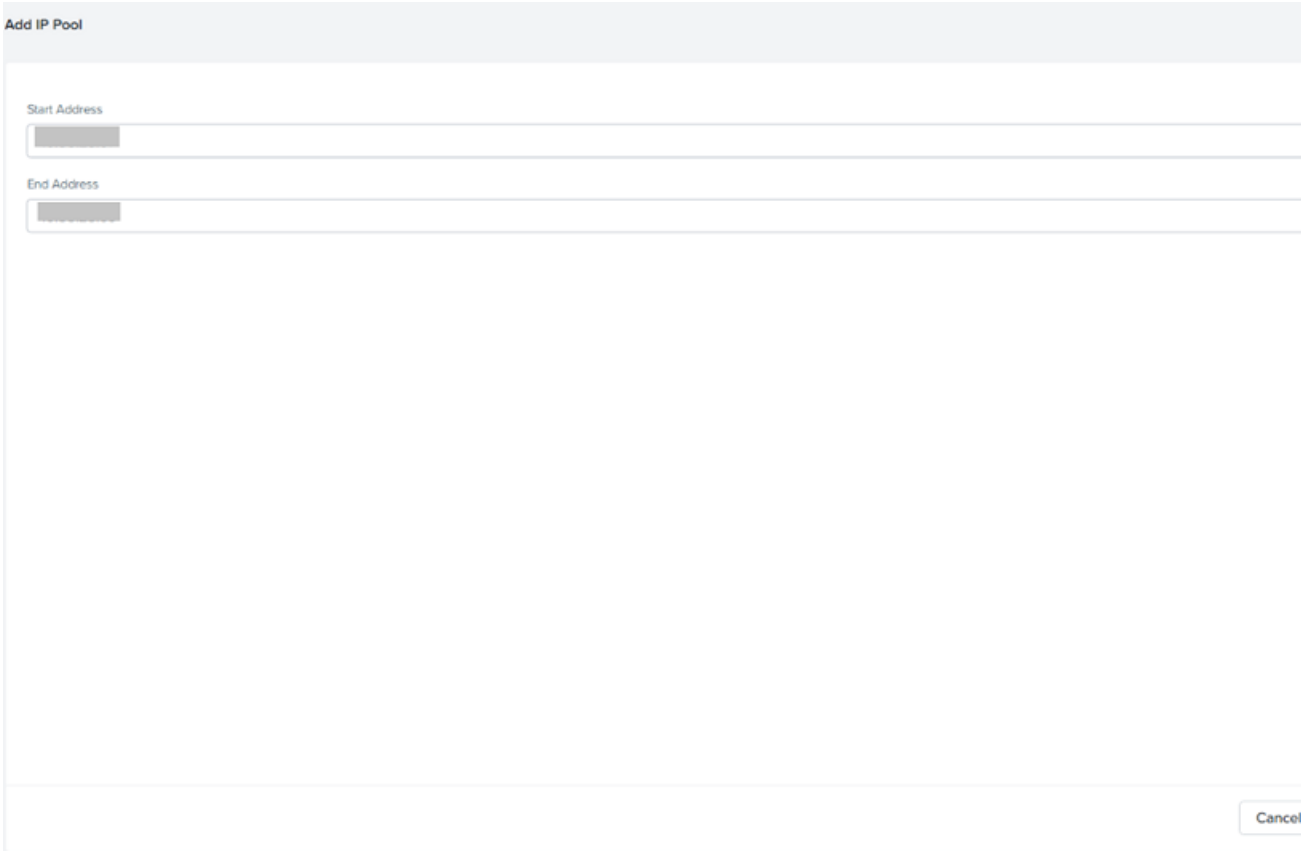
- **Configure Domain Settings:** To configure domain settings, select the **Configure Domain Settings** check box. When selected, the following fields are displayed:
  - **Domain Name Servers (Comma Separated):** Specify a list of DNS servers separated by commas.
  - **Domain Search (Comma Separated):** Specify a list of domains separated by commas.
  - **Domain Name:** Type a name for the VLAN domain.
  - **TFTP Server Name:** Specify the name of TFTP server from which the virtual machine downloads a boot file.
  - **Boot File Name:** Specify the name of the boot file downloaded from the TFTP server.



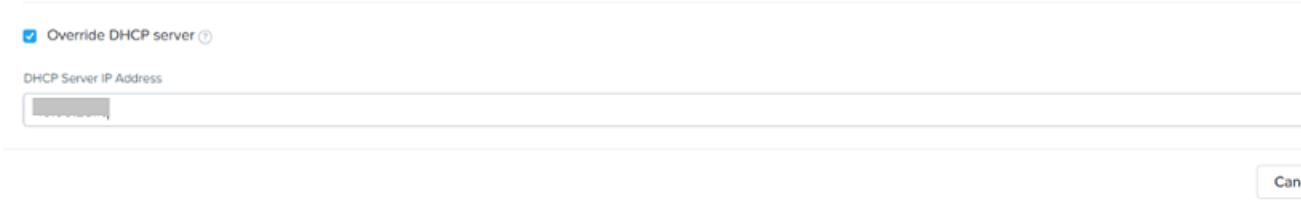
5. To specify the range of IP addresses that can be automatically assigned to the virtual NICs, under IP Address Pools, click **+ Create Pool**.



6. On the Add IP Pool page, do the following, and then click **Submit:**
   - **Start Address:** Enter the starting IP address of the range.
   - **End Address:** Enter the ending IP address of the range.



7. To configure a DHCP server, select the **Override DHCP server** check box, and then specify an IP address in the **DHCP Server IP Address** field. If the check box is not selected, the DHCP server IP address is automatically generated.



8. Click **Save**.

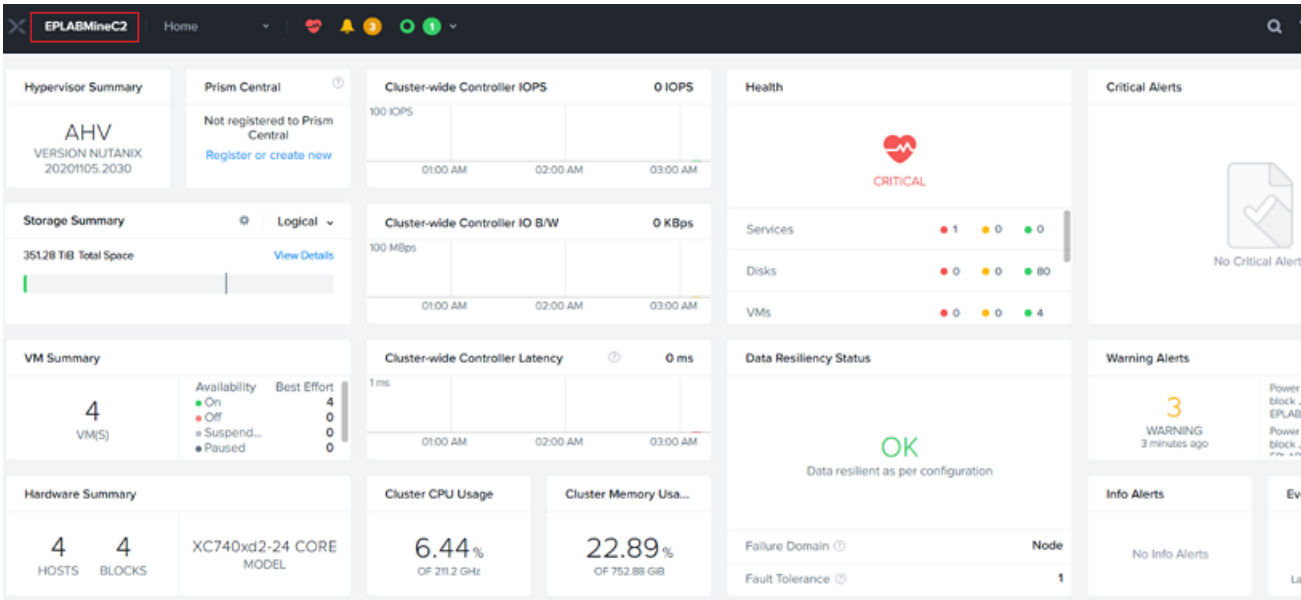
The Network switch is created successfully for Object Store.

How to Configure Nutanix Cluster Data Services IP Address

After the network switch is created for the Object Store, configure the data services IP address for Nutanix Cluster. Nutanix allows external access to cluster storage through the IP address of ISCSI data services. This section provides information about how to configure the data services IP address for Nutanix Cluster.

Follow these steps:

1. On the Prism Central home page, click the cluster name.

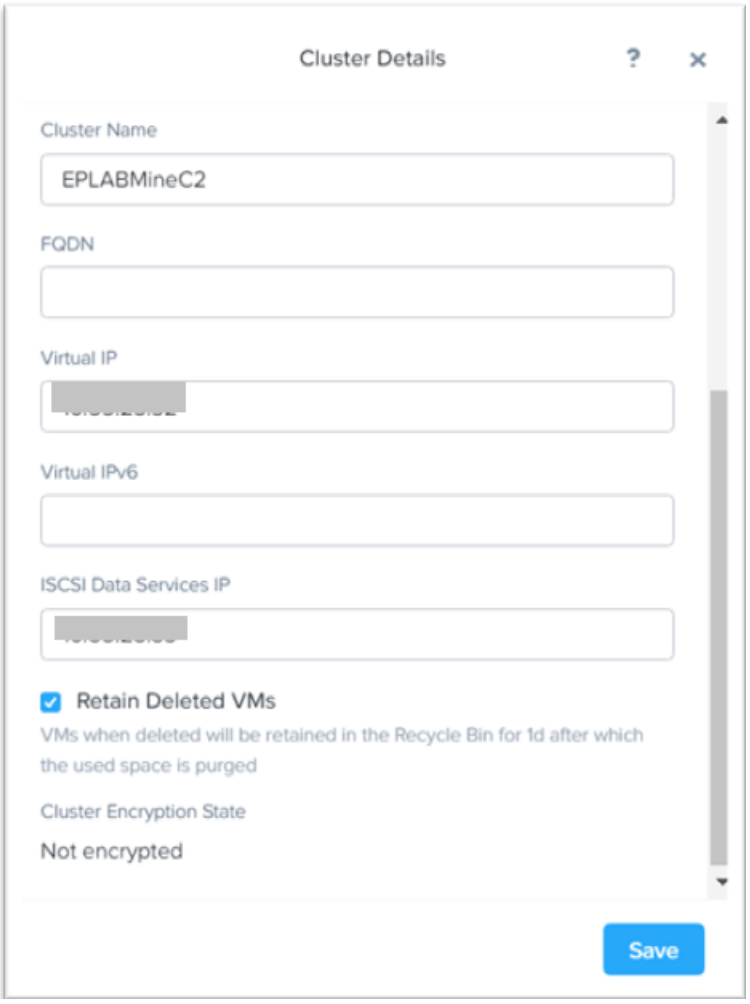


The Cluster Details dialog appears.

2. On the Cluster Details dialog, do the following:
   - **Cluster Name:** (Optional) Type a name for the cluster.
   - **ISCSI Data Services IP:** Enter the IP address of ISCSI Data Services.

     Important! Make sure the data services IP address is correct otherwise, all storage become unavailable for File Server and Nutanix

volumes.



3. Click **Save**.

   A confirmation message appears asking whether you want to proceed with updating the cluster and change the ISCSI Data Services IP.

4. Click **Yes** to confirm.

   The ISCSI Data Services IP address is configured successfully.

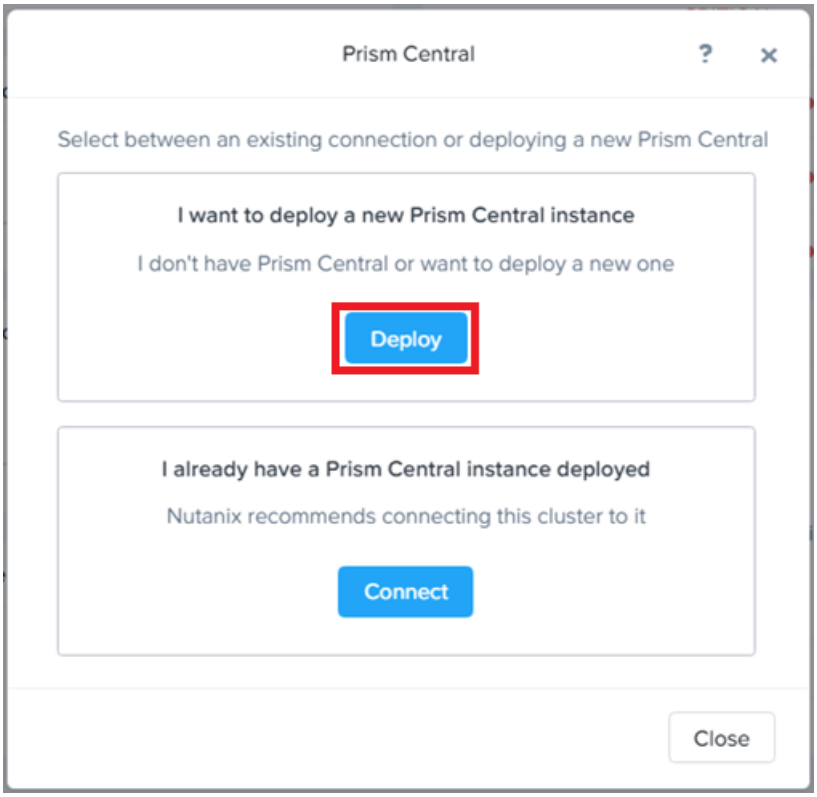
How to Deploy Prism Central VM for Cluster

This section provides information about how to deploy Prism Central VM for the cluster.

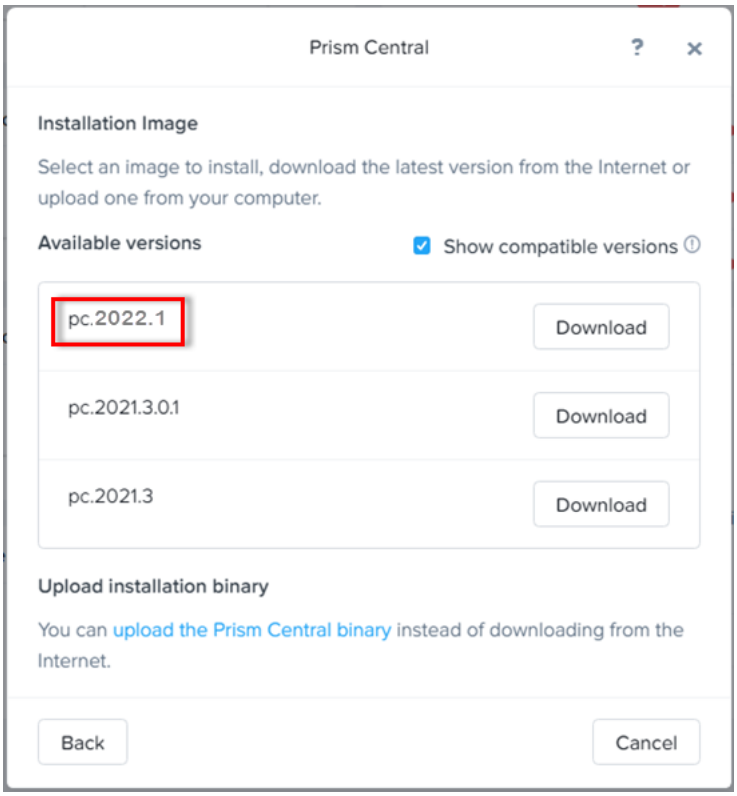
Important! To download the Prism Central image from the Nutanix support portal, make sure the cluster has an Internet connectivity. When the cluster does not have Internet connectivity, no entries appear on the *Installation Image* screen.

Follow these steps:

1. Log into the Prism Element web console.
2. On the Prism Element home page, under Prism Central widget, click **Register or create new**.
3. On the Prism Element dialog, to deploy a new Prism Central instance, click **Deploy**.

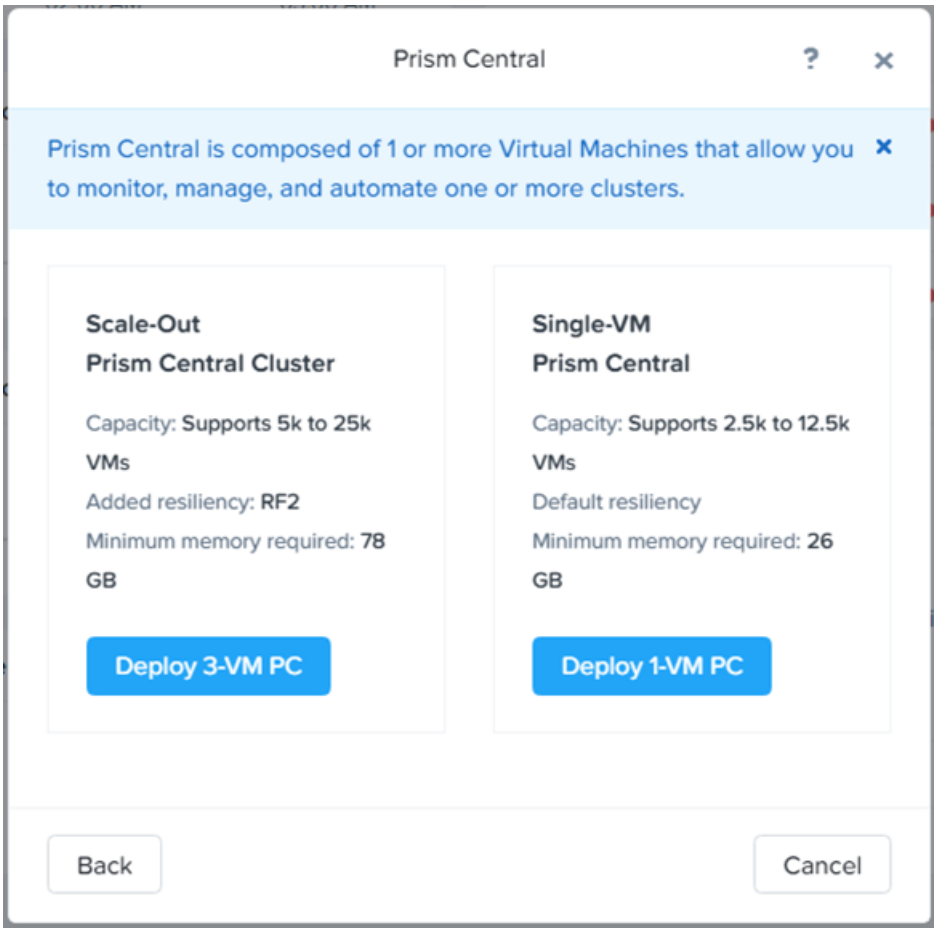


4. On the Installation Image screen, select the **pc.2022.1** version of image, and then click **Download**.



5. On the deploy screen, do one of the following:
   - To deploy a single-VM instance of Prism Central, click **Deploy 1-VM PC**.
   - To deploy a Scale-Out-VM instance of Prism Central, click **Deploy 3-VM PC**.

     Note: It is recommended to select 1-VM instance to avoid maintenance cost.



6. Do the following:
   a. Under General Configuration, do the following:
      - **VM Name:** Type a name for the Prism Central VM.
      - **Select a Container:** From the drop-down list, select a container for the Prism Central VM.

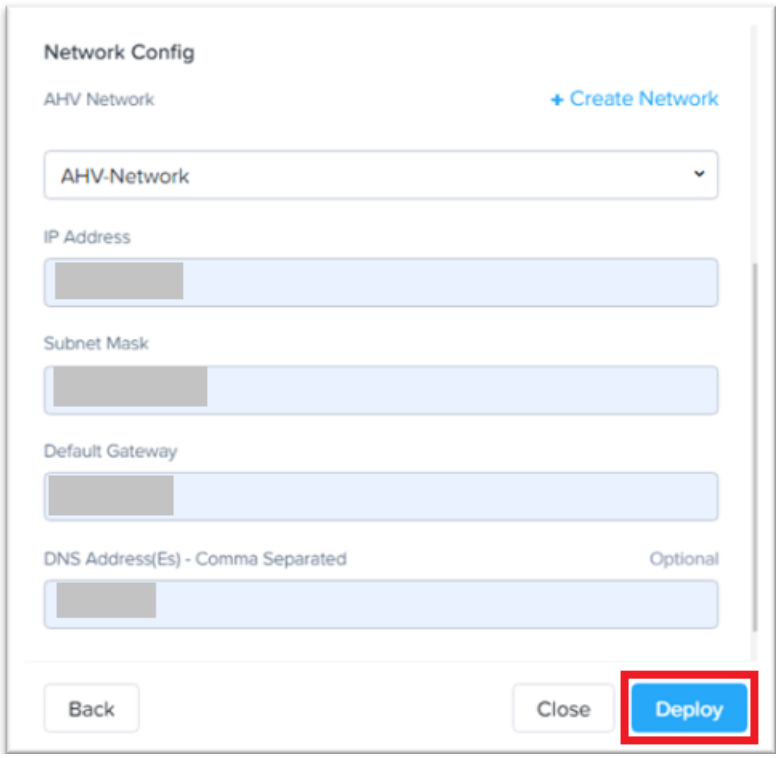
   b. Under VM Size, select the size of VM based on the number of guest VMs it must manage across all the registered clusters.

      Or

Click the **SMALL** option.

c. Under Network Config, do the following:

- **AHV Network:** The AHV network is selected by default.
- **IP Address:** Enter the static IP address for Prism Central VM.
- **Subnet Mask:** Enter the IP address of subnet mask.
- **Default Gateway:** Enter the IP address for gateway.
- **DNS Address(es):** Enter the IP address for one or more DNS servers separated by commas.



7. If all the entered details are correct, click **Deploy**.

The deployment process begins, and the Prism Central widget shows *Deploying* until the deployment process completes.

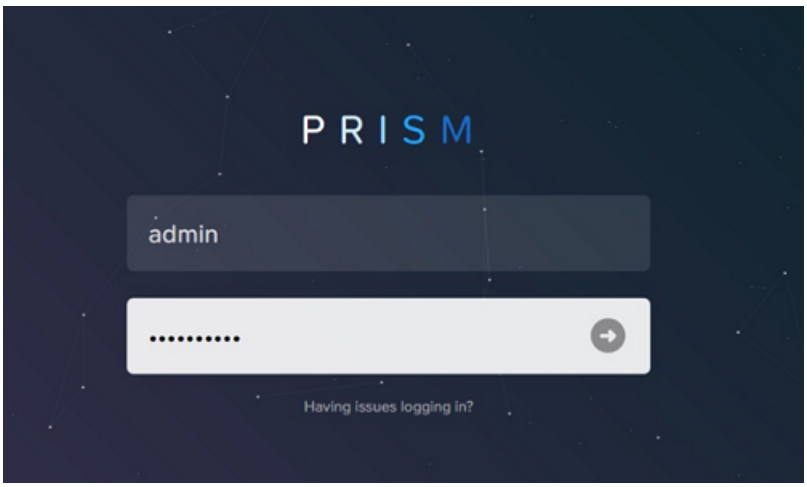
Note: After successfully deploying the Prism Central VM, log into the Prism Central VM using the IP provided previously during the deployment process, and then change the default password before registering the Prism Central VM in the Prism Element. For more information about how to change the default password, see How to Change the Default Password for the Prism Central VM.

How to Change the Default Password for Prism Central VM

This section provides information about how to change the default password for Prism Central VM.

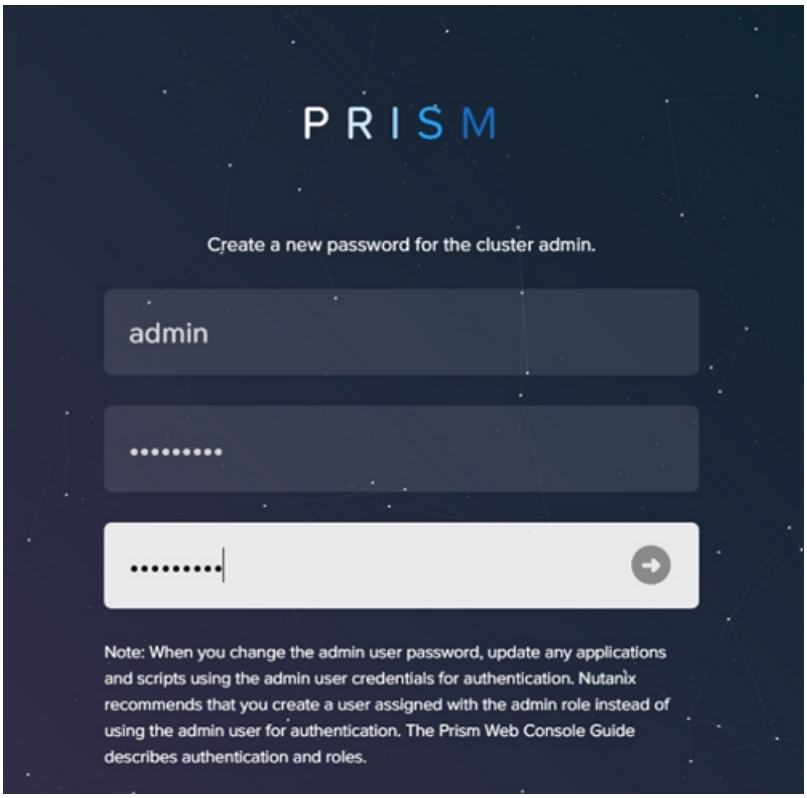
Follow these steps:

1. Log into the Prism Central VM as an admin user using the following credentials:
   - **Username:** admin
   - **Password:** Nutanix/4u



As soon as you login for the first time, you are prompted to change your password.

2. Enter a new password, re-enter the password to confirm, and then press Enter or click the right-arrow icon.



After the password is changed successfully, the new password gets synchronized across all the interfaces and Controller VMs.

3. Login again with the updated credentials.

   The Nutanix End User License Agreement (EULA) and Terms of Use screen appears.

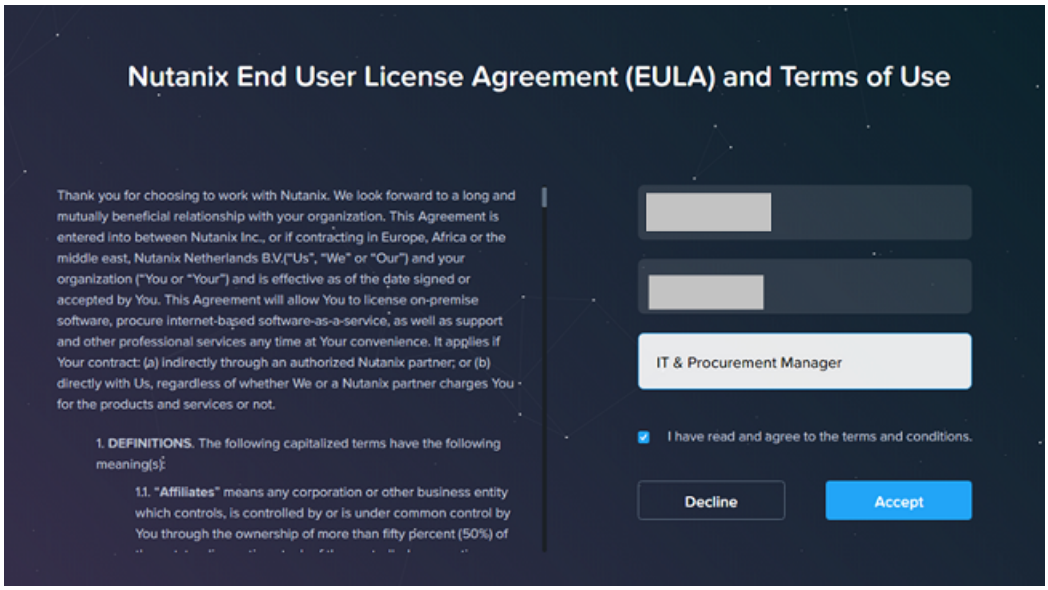
4. On the Nutanix End User License Agreement (EULA) and Terms of Use screen, do the following:

   a. Read the license agreement carefully.

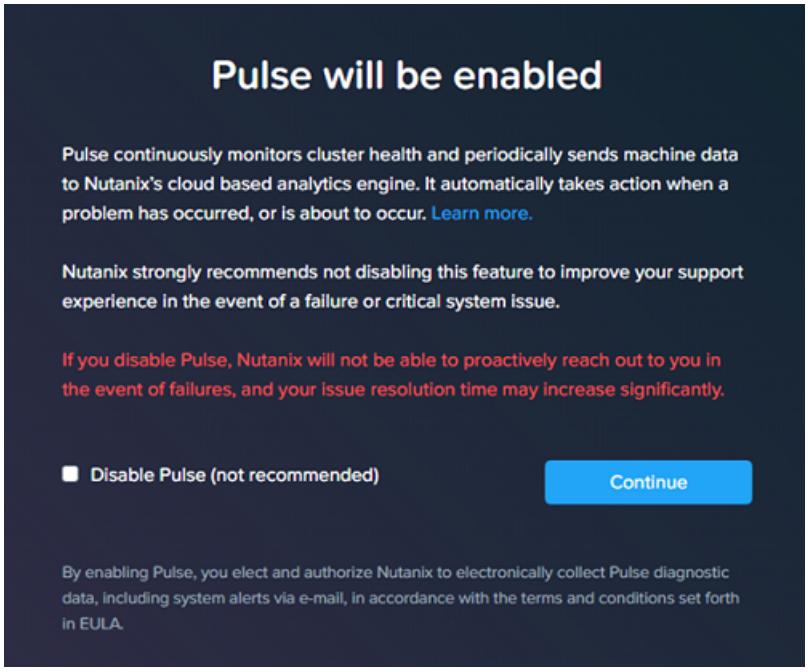
   b. Enter the appropriate information in the **Name**, **Company**, and **Job Title** fields as needed.

   c. Select the **I have read and agree to the terms and conditions** check box.

   d. Click **Accept**.



The *Pulse will be enabled* screen appears.



5. On the Pulse will be enabled screen, click **Continue**.

   Note: Nutanix does not recommend that you disable Pulse.

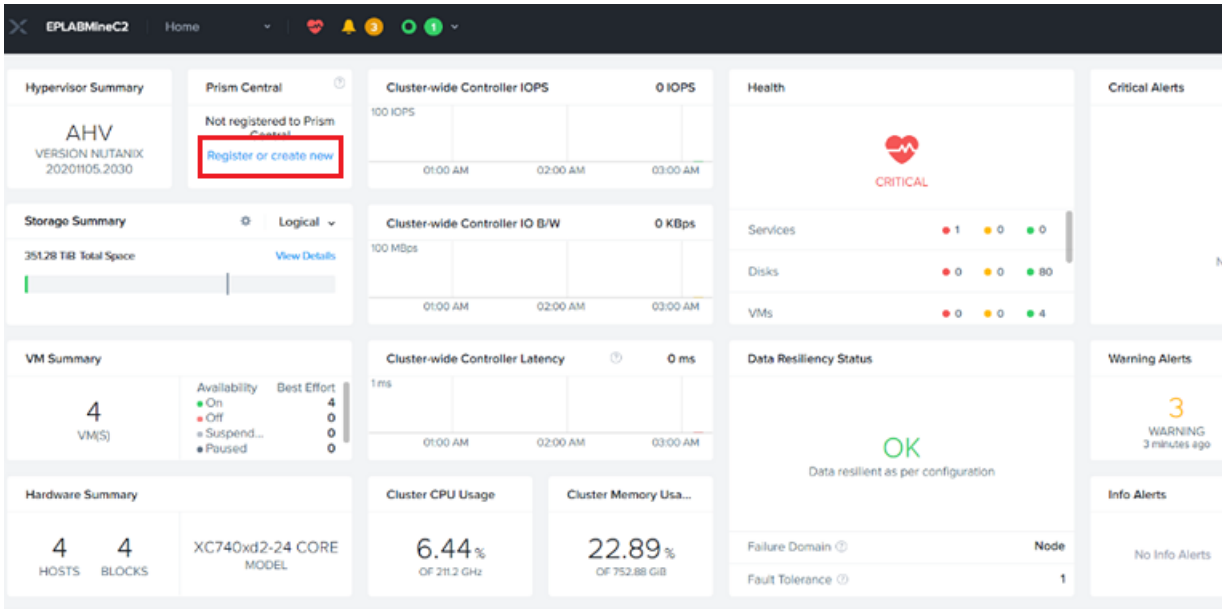
   The Prism Central dashboard opens.

How to Register the Prism Central VM for Cluster

This section provides information about how to register the Prism Central VM for cluster.

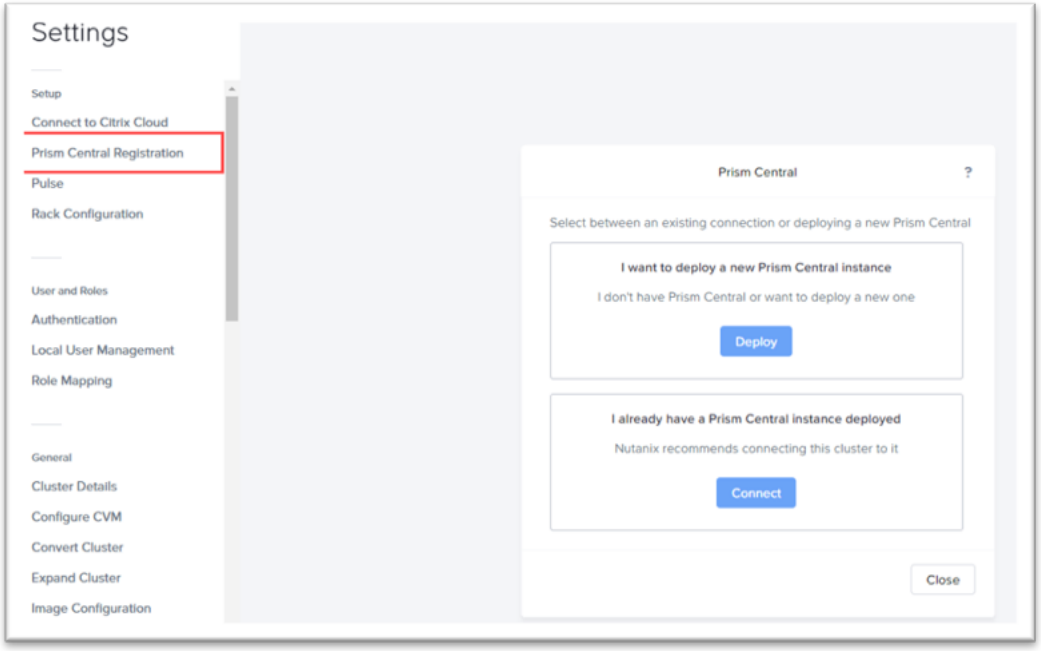
Follow these steps:

1. Log into the Prism Element web console.
2. To register the Prism Central VM, do one of the following:
   - On the Prism Central home page, under Prism Central widget, click **Register or create new**.

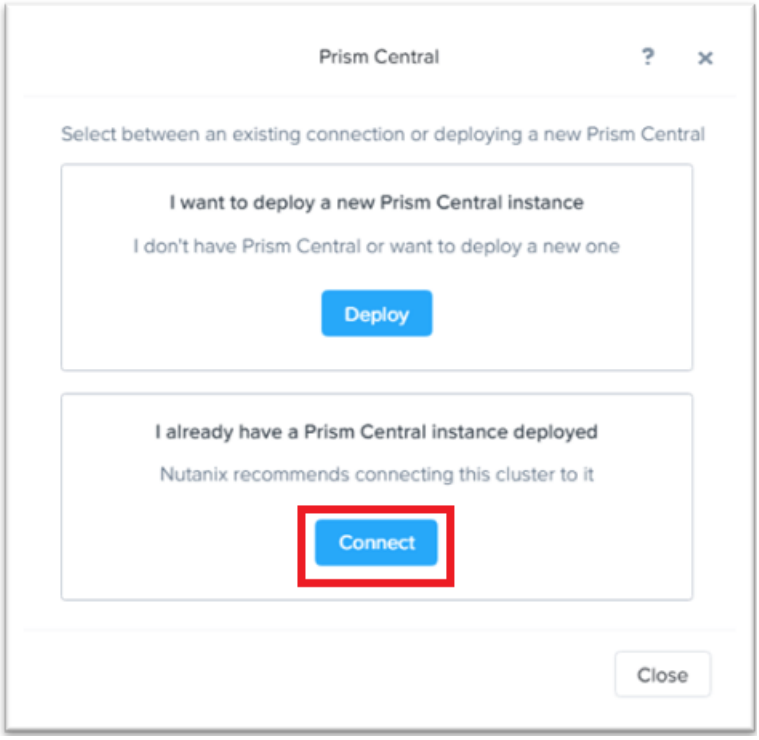


   - Click the settings icon on the top-right corner, and then select **Prism**

Central Registration.

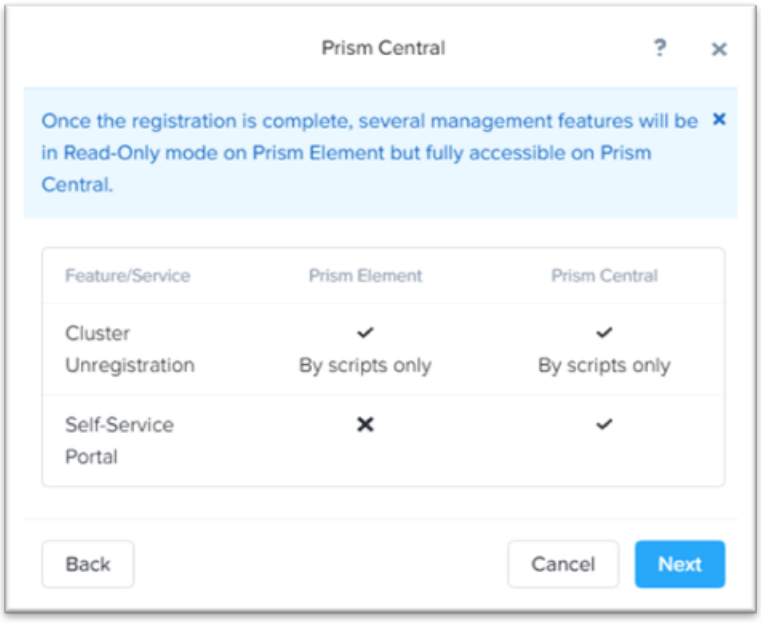


3. On the Prism Central dialog, click **Connect**.



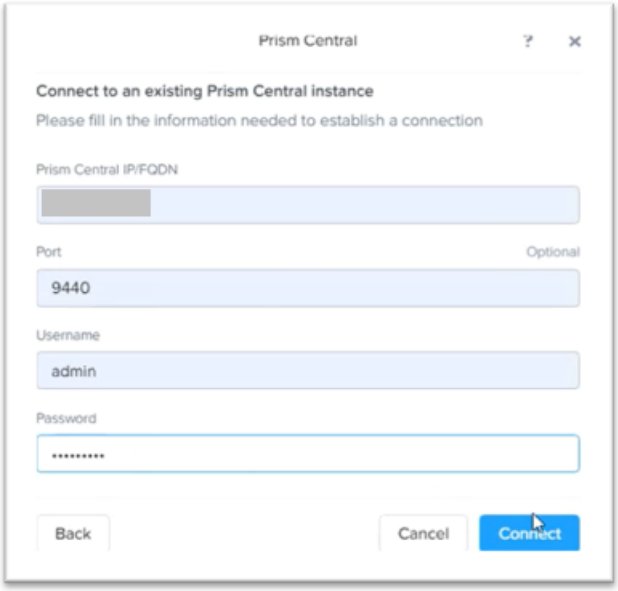
A screen appears displaying the services that are available on Prism Element and Prism Central.

4. Review the message, and then click **Next**.



5. On the connection screen, do the following:
   - **Prism Central IP/FQDN:** Enter the IP address of Prism Central VM.
   - **Port:** Enter the port number. The default port number is 9440.
   - **Username:** Type *admin* as Prism Central user name.
   - **Password:** Type a password for the Prism Central user name.

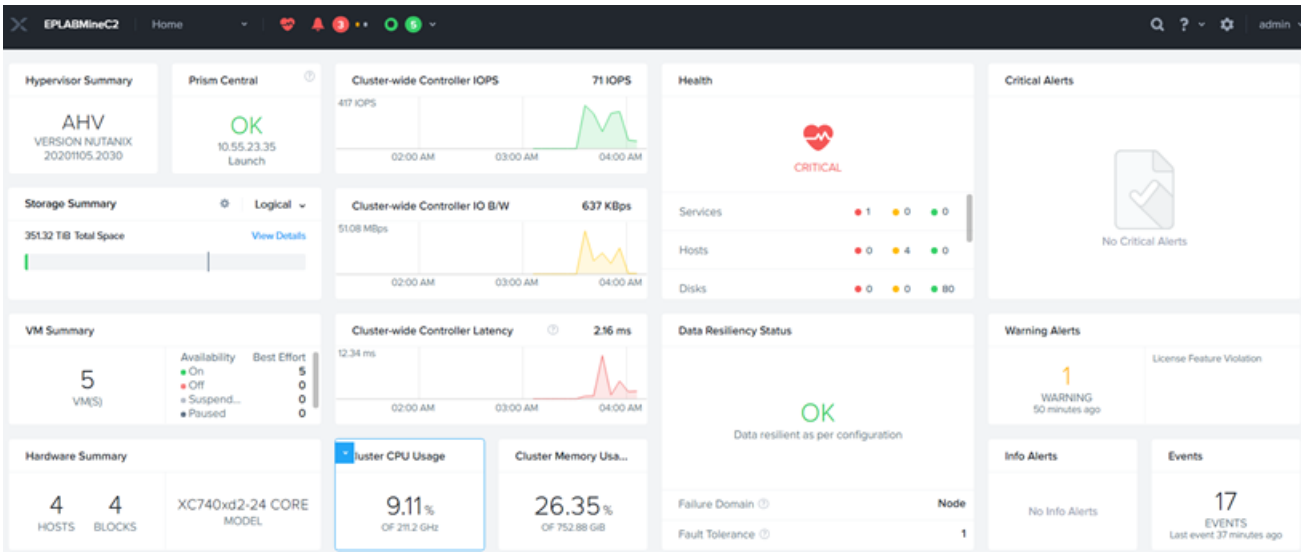
     Note: Change the Prism Central password before you register the Prism Central VM. The default Prism Central password is Nutanix/4u.



6. Click **Connect**.

The Nutanix cluster is registered successfully on the specified Prism Central VM and allows the flow of information between cluster and Prism Central.

7. To launch the Prism Central web console in your browser, on the Prism Central widget, click **OK**.



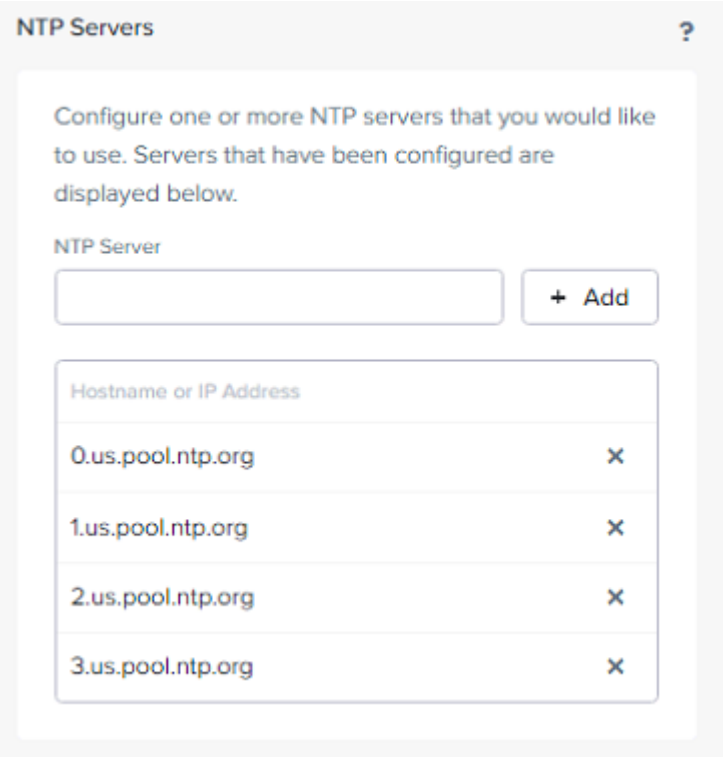
How to Update NTP Server in Prism Central

Before deploying Object Store services, the NTP Server details (host name or IP address) must be provided in Prism Central. This section provides information about how to update the NTP server details in Prism Central.

Follow these steps:

1. Log into the Prism Central web console.
2. Navigate to **Dashboard > Settings > NTP Servers**.

   The NTP Servers dialog opens.
3. On the NTP Servers dialog, enter the host name or IP address of the NTP server, and then click **+ Add**.



The NTP Server details are added to the Prism Central.

Note: To avoid the time out error due to single NTP server, add the following NTP servers as alternatives under Prism Element and Prism Central:

- 0.us.pool.ntp.org
- 1.us.pool.ntp.org
- 2.us.pool.ntp.org
- 3.us.pool.ntp.org

How to Deploy Nutanix Object Store

This section contains the following topics:

Review the Prerequisites

Before running Objects, verify that you have completed the following prerequisite tasks:

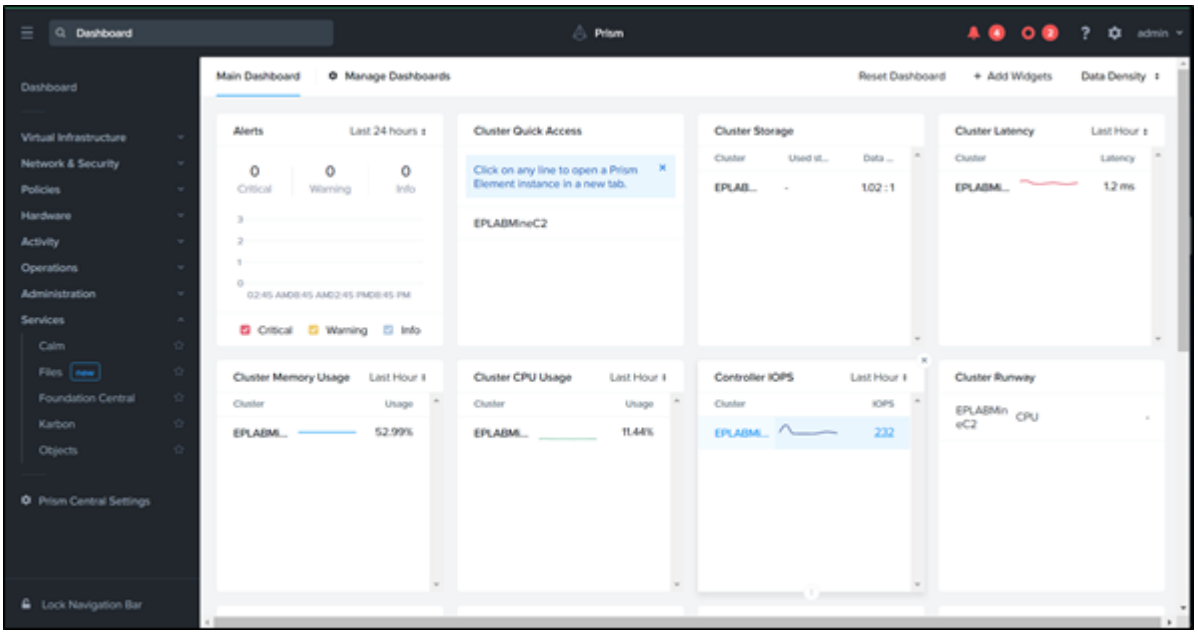
- For online deployment, make sure that you have an internet connectivity for both Prism Element and Prism Central.
- Domain Name Servers (DNS) are configured on Prism Element and Prism Central.
- Network Time Protocol (NTP) servers are configured on Prism Element and Prism Central.
- Virtual IP address and the data services IP address are set up on the Prism Element where you deploy the Objects.
- For AHV, make sure the VLANs required for Object Store Services and accessing the Object Store endpoints are configured on Prism Element correctly.

Deploying the Nutanix Object Store

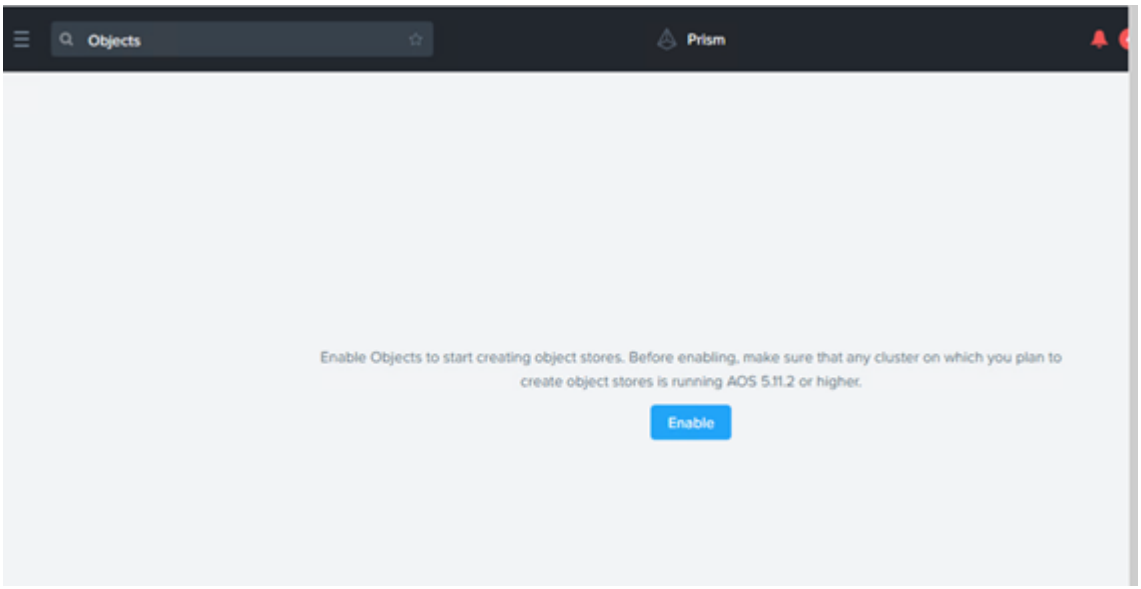
UDP requires Object Store to create a bucket and convert existing datastore into Object Store to store Backed-up data using RPS store functionality. This section provides information about how to deploy the Nutanix Object Store.

Follow these steps:

1. Log into the Prism Central web console.
2. Navigate to **Dashboard** > **Services** > **Objects**.

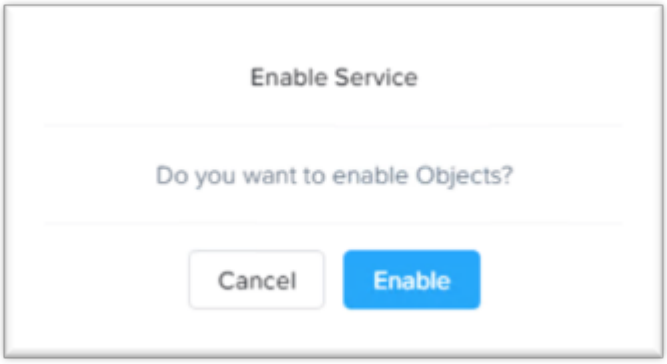


3. Click **Enable**.



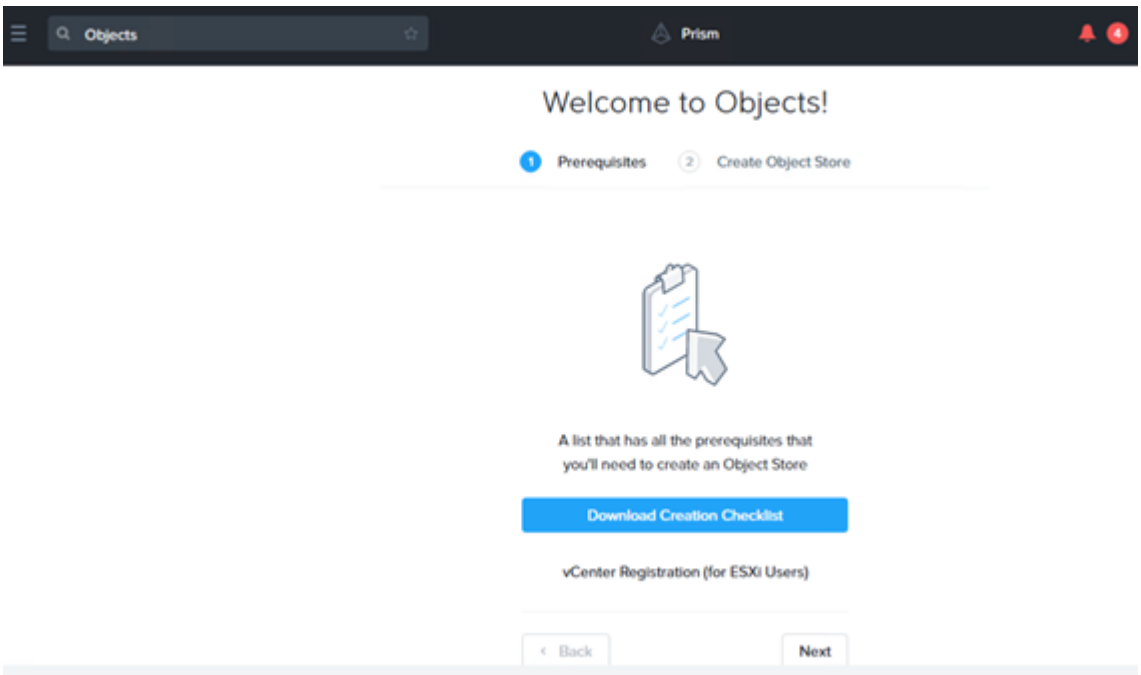
The Enable Service dialog appears.

4. On the Enable Service dialog, click **Enable**.

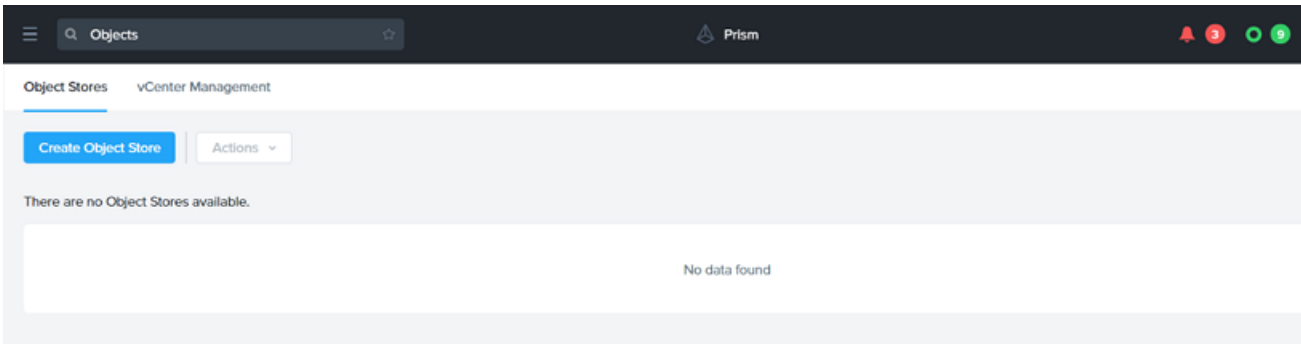


Note: Object Store Services are enabled only once.

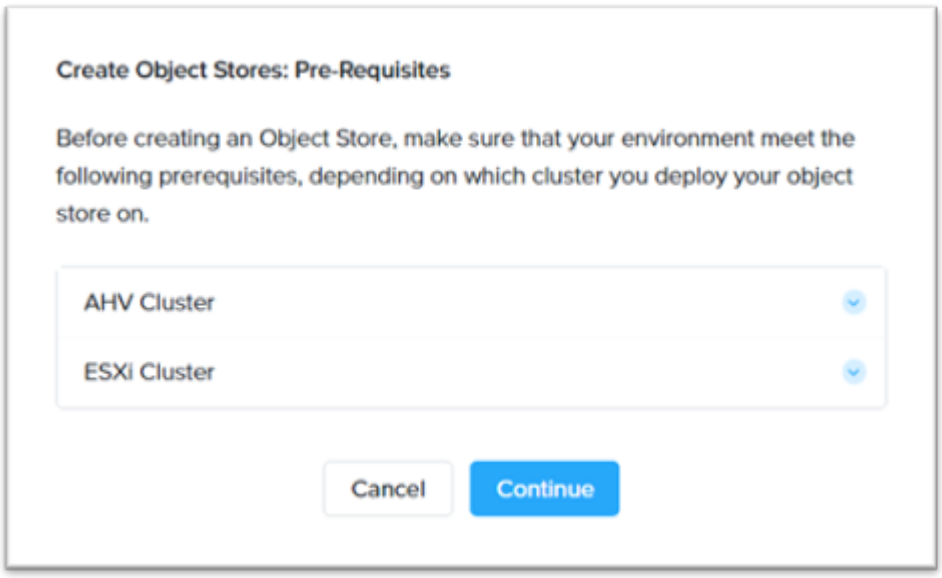
5. On the *Welcome to Objects!* screen, click **Next**.



6. On the Object Store page, click **Create Object Store**.



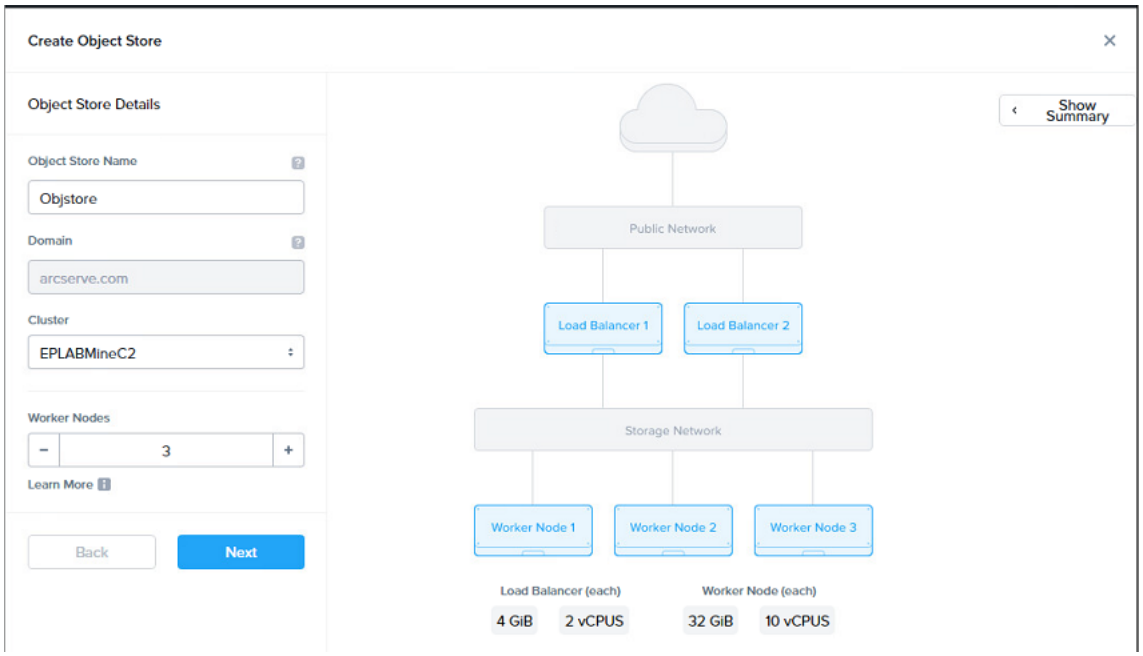
7. On the Create Object Stores: Pre-Requisites dialog, click **Continue** if you have met the given prerequisites.



8. On the Create Object Store screen, do the following:
   a. On the Object Store Details page, do the following, and then click **Next**:
      - **Object Store Name:** Type a name for the Object Store.

        Note: You cannot change the Object Store name once the object store is created.
      - **Domain:** Enter the domain for reference.
      - **Cluster:** From the drop-down list, select the cluster on which you want to deploy the object store.
      - **Worker Nodes:** Add the number of worker nodes.

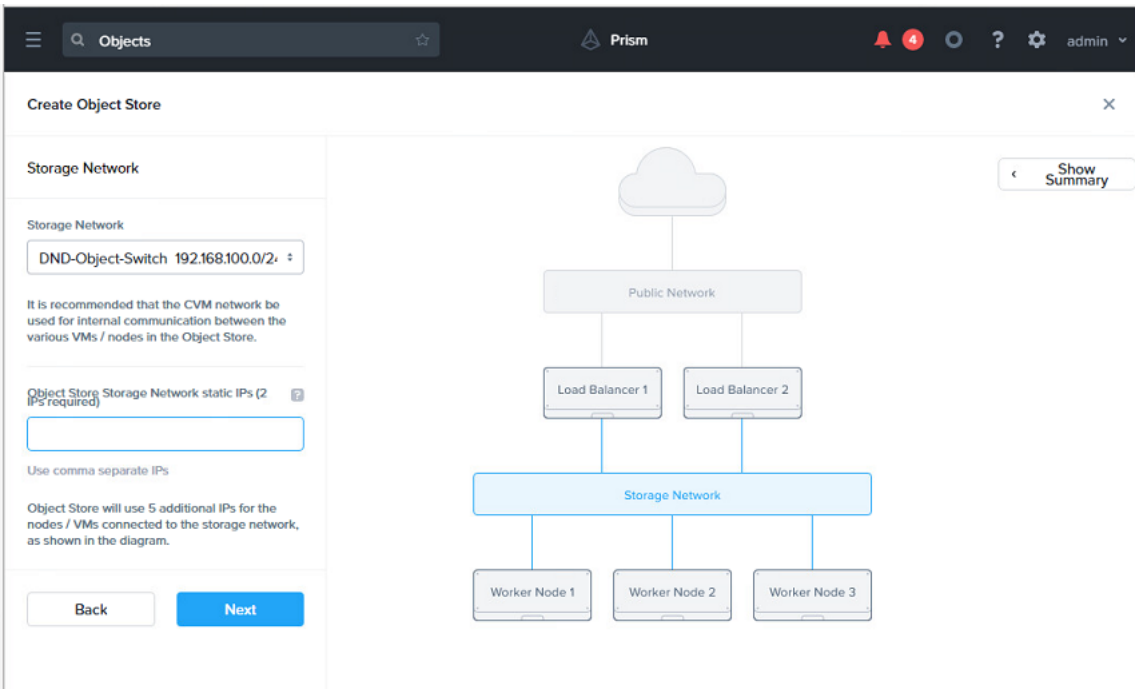
        Notes:
        - The configured worker nodes must not exceed the worker nodes of the cluster.
        - A minimum of 10 vCPUs and a memory of 32 GiB is required.
        - Every time you click plus **(+)**, 10 vCPUs and 32 GiB of memory gets added.
        - Each VM is allocated 10 vCPUs and a DHCP IP address.
        - vCPU and memory are linked. vCPU must be in multiple of 10 and memory in multiple of 32.



b. On the Storage Network page, do the following, and then click **Next**:

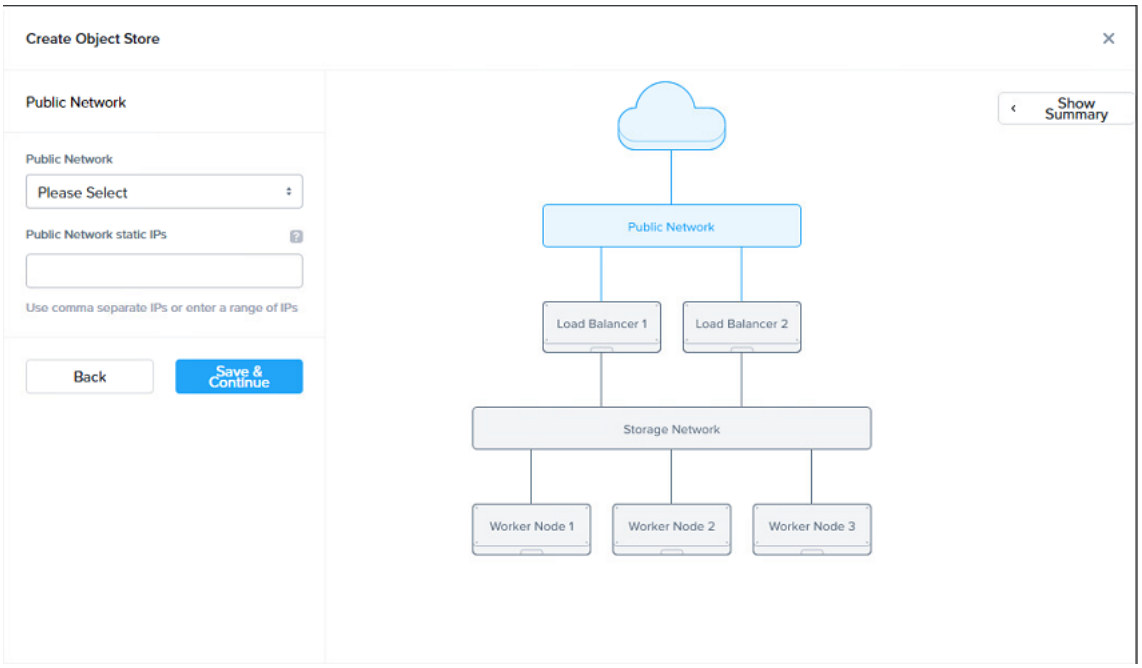
- **Storage Network:** From the drop-down list, select the storage network that is used for the internal communication between the components of an object store.
- **Object Store Storage Network Static IPs (2 IPs required):** Enter two storage network IP addresses separated by a comma. These two IP addresses are required only for AHV.

  Note: For ESXi, these two internal IP addresses are not required and selected automatically from the IPAM range configured for ESXi networks.

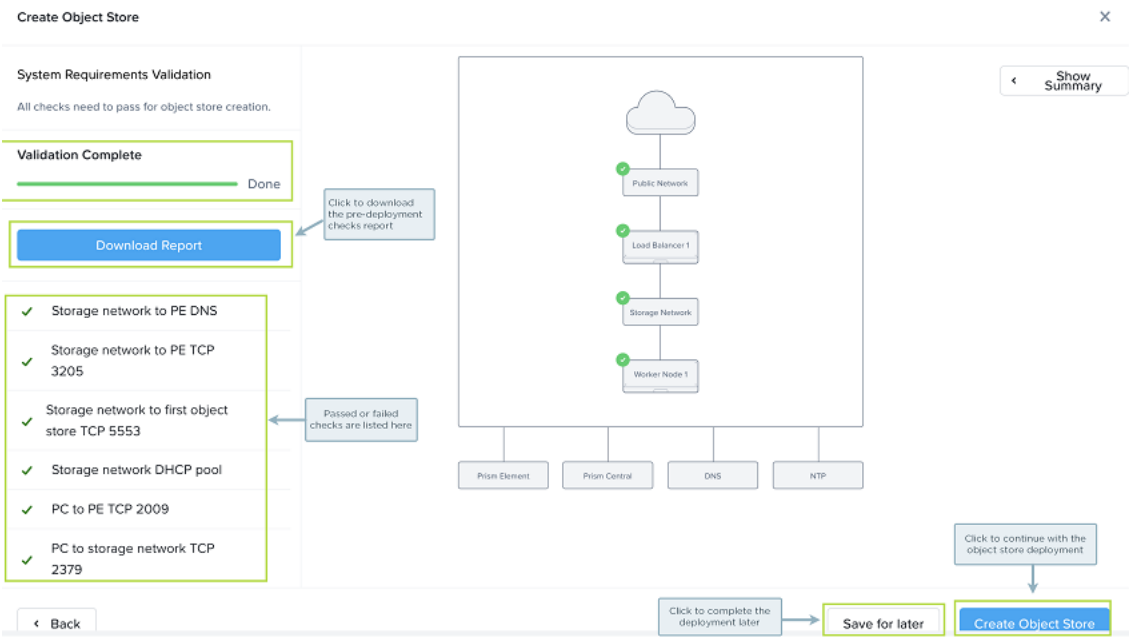


c. On the Public Network page, do the following, and then click **Save & Continue**:

- **Public Network:** From the drop-down list, select the external client access network. This network could be same as the internal access network and must have at least 4 IP addresses in the range of usable IP addresses.
- **Public Network static IPs:** Enter a minimum of 4 external client access IP addresses separated by a comma, or as a range of IP addresses. These IP addresses are within the client access network and are used to access the Object Store.



Before the deployment begins, the pre-check starts and a list of checks performed is displayed.



Notes:

- To start deployment, all the pre-checks must be validated.
- If NTP validation fails between Prism Central and Prism Element, provide a standard NTP server IP address.

d. Based on the pre-check result, do the following:

- If the pre-checks are validated, click **Download Report** to download the report, and then click **Create Object Store** to start with the object store deployment.
- If the pre-checks fail, an error message is displayed. Click **Download Report** to download the report. A Fail status is displayed next to the check name with a message. To complete the deployment process, fix the failed checks.

  You can view the status of the object store deployment after the pre-checks are validated.

The Object Store is now created successfully and gets listed under Object Stores tab.

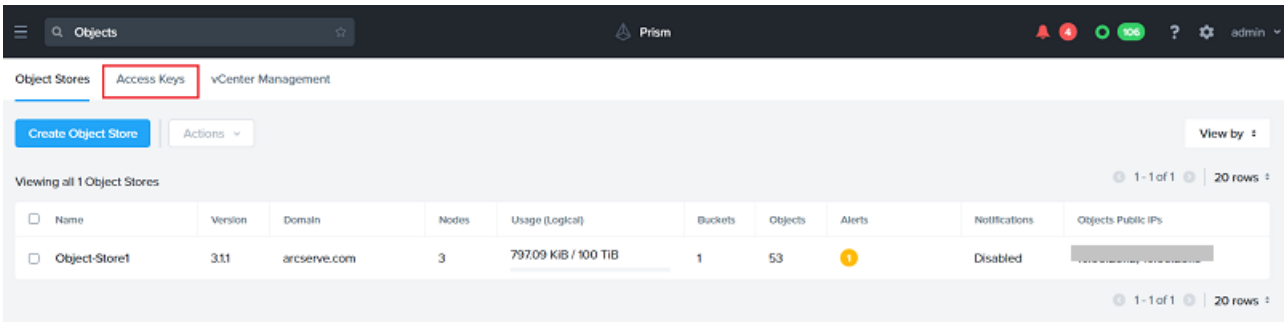
How to Generate and Download Access Keys

You can generate access key using the email address. This section provides information about how to generate and download access keys.

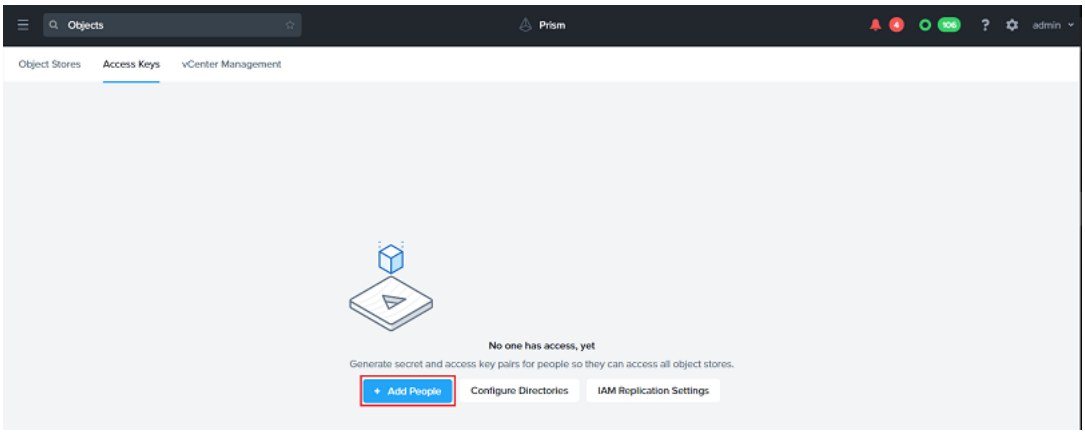
Note: You cannot share buckets without access keys.

Follow these steps:

1. Log into the Prism Central web console.
2. Navigate to **Dashboard** > **Services > Objects**.
3. Click the **Access Keys** tab.



4. On the Access Keys page, click **+ Add People**.

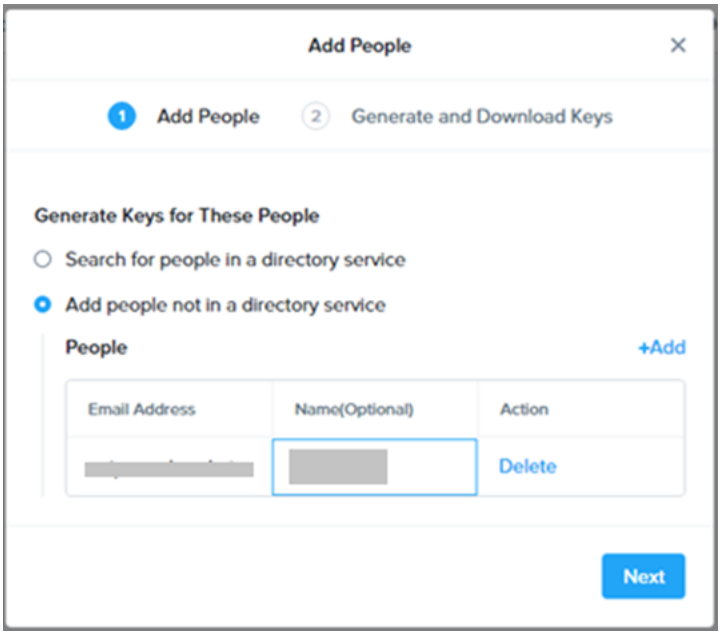


The Add People window appears.

5. On the Add People page, to add people not in a directory, select the **Add people not in a directory service** option, and then do the following:
   a. **Email Address:** Enter the email address of the people.
   b. **Name (Optional):** Type a display name for the user. The display name can contain up to 255 characters.

      Notes:

- To add multiple people (users), click **+ Add**.
- To delete the added user, click **Delete** under Action.

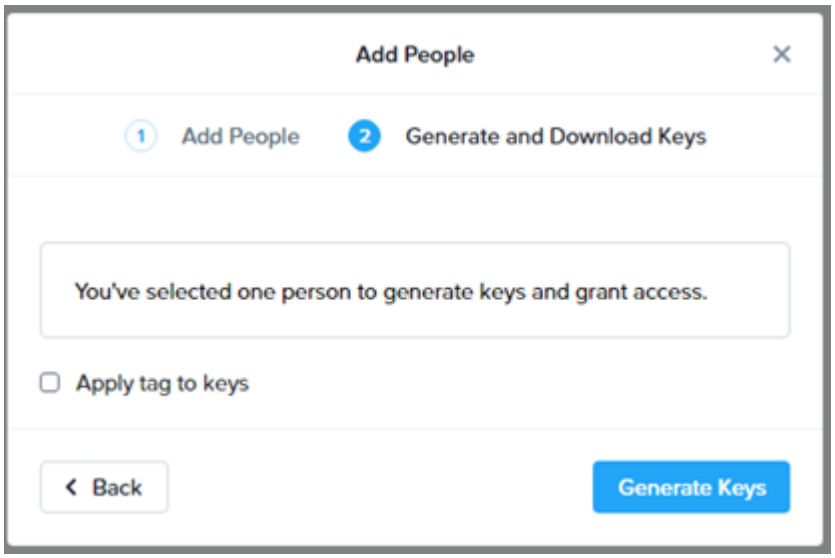


6. On the Generate and Download Keys page, do the following:
   a. (Optional) To apply tags to the access keys for key management, select the **Apply tags to keys** check box, and then type a name for the access keys.

      Notes:

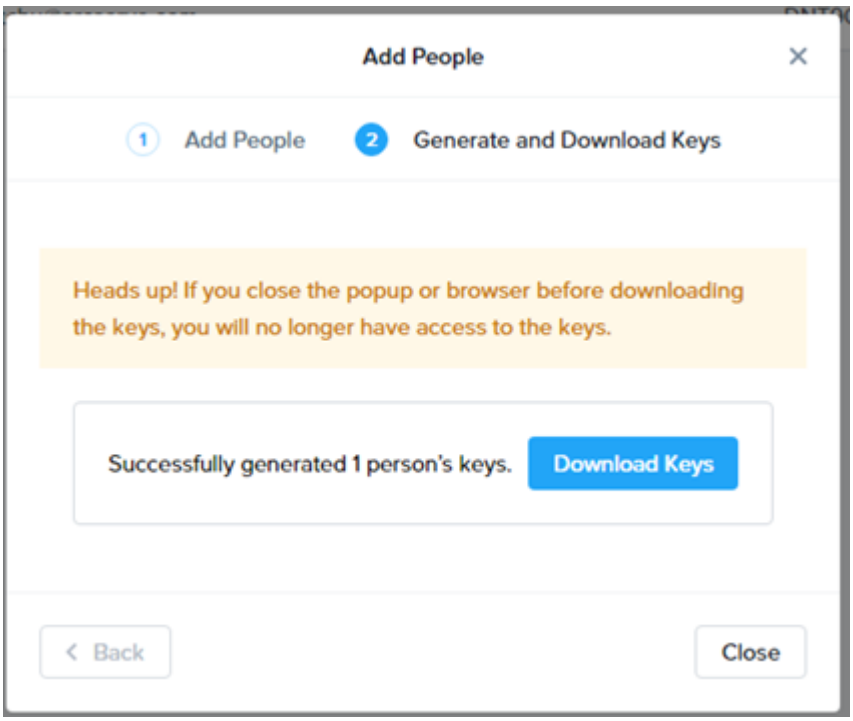
      - If multiple users are added, the same tag name applies to all the users.
      - You cannot change the tag once applied.

   b. Click **Generate Keys**.



The access keys are generated successfully.

7. To download the generated keys, click **Download Keys**.

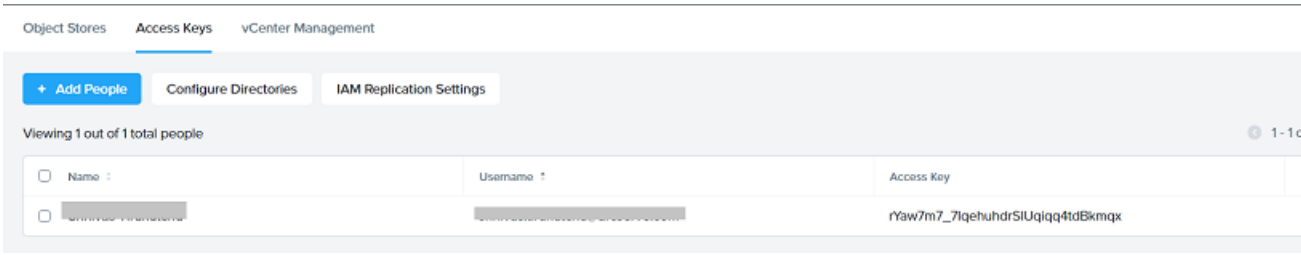


The keys are downloaded successfully.

Important! If you close the Add People dialog before downloading the keys, you cannot access the keys later.

8. Save the downloaded keys (Access Key and Secret Key) locally.
9. After downloading the access keys, to return to the Access Keys screen, click **Close**.

10. Click the **Object Stores** tab, and then save the public IPs displayed under the Objects Public IPs column.



The Public IP is required along with the Access Key and Secret Key in the Nutanix Mine deployment wizard in the Object Store input screen.

How to Deploy Nutanix Mine

Arcserve UDP allows to build a dedicated secondary storage solution designed to protect both Nutanix clusters and legacy IT environments. UDP's Nutanix Mine deployment wizard allows you to deploy the Arcserve UDP software products such as UDP Console, Recovery Point Server (RPS), and Linux Backup Server (LBS) in the Nutanix cluster environments.

This section contains the following topics:

Review Prerequisites

Verify that you have completed the following prerequisite tasks:

- Nutanix Prism Element with AOS 5.20 and above is installed successfully.
- Nutanix Objects has been setup and configured appropriately.
- Assigned the DNS Server for hostname resolution.
- Assigned the DHCP server for automatic IP address assignment.
- Bootstrap VM is created in the Nutanix Prism Element.

  Note: To download the Bootstrap VM image, click here.
- Windows Server 2019 standard edition ISO is downloaded and made available on Local VM.

  Note: To download the Windows Server 2019 standard edition ISO, see the *How to get the Windows Server 2019 IOT ISO File* topic in the Installation guide.

For more information about how to create Bootstrap VM in Nutanix Prism Element, see How to Create Bootstrap VM.

Creating Bootstrap VM

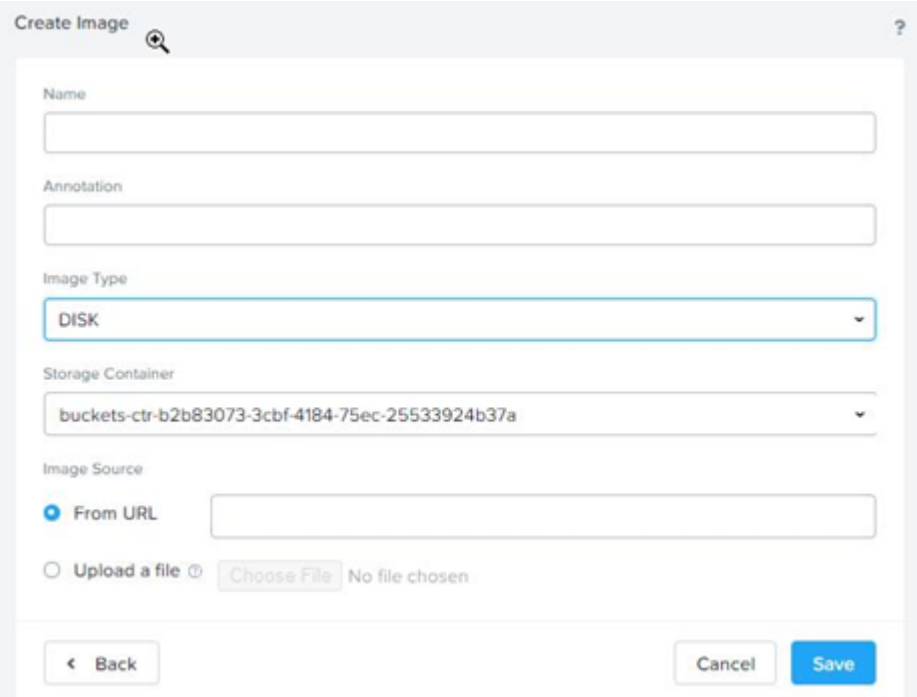
This section provides information about how to create Bootstrap VM in the Nutanix dashboard.

Follow these steps:

1. Log into the Nutanix cluster console using Admin credentials.
2. Click the settings icon on the top-right corner.
3. From the left pane, click **Image Configuration**.

   The Image Configuration dialog appears.
4. On the Image Configuration dialog, click **+ Upload Image** button.

   The Create Image dialog appears.
5. On the Create Image dialog, do the following, and then click **Save**:
   - **Name:** Type a name for the bootstrap image.
   - **Annotation:** Type a description if required. It is optional.
   - **Image Type:** From the drop-down list, select **DISK** as the image type.
   - **Storage Container:** From the drop-down list, select the default storage container.
   - **Image Source:** To upload the image, do the following:
     a. Select the **Upload a file** option, and then click **Choose File**.
     b. Navigate to the location where the Arcserve bootstrap VM Disk image is saved, select the image, and then click **Open**.



Wait until the image gets uploaded.

6. After the bootstrap VM Disk image is uploaded, go to **Settings**, select **VM**, and then click **Create VM**.
7. On the VM dashboard, click **+ Create VM**.

The Create VM dialog appears.

8. On the Create VM dialog, do the following:
    a. Under General Configuration, specify the following:
        - **Name:** Type a name for the VM.
        - **Description:** Type a description for the VM. It is optional.
        - **Timezone:** From the drop-down list, select the time zone that you want the VM to use.

    Note: Make sure the **Use this VM as an agent VM** check box is not selected as it is not required for bootstrap VM.

b. Under Compute Details, specify the following:

- **vCPU(s):** Enter the number of virtual CPUs to allocate to this VM. The default value is 2.
- **Number of Cores Per vCPU:** Enter the number of cores assigned to each vCPU. The default value is 2.
- **Memory:** Enter the amount of memory to allocate to the VM. The default value is 8 GiB (minimum).

c. Under Disks, do the following:

1. Click **+ Add New Disk**.

   The Add Disk dialog appears.

2. On the Add Disk dialog, do the following, and then click **Add**:

   - **Type:** From the drop-down list, select the type of storage disk. The default option is DISK.
   - **Operation:** To copy an image that you have uploaded using image service feature onto the disk, select the **Clone from Image Service** option from the drop-down list.
   - **Bus Type:** From the drop-down list, select **IDE** as the bus type.

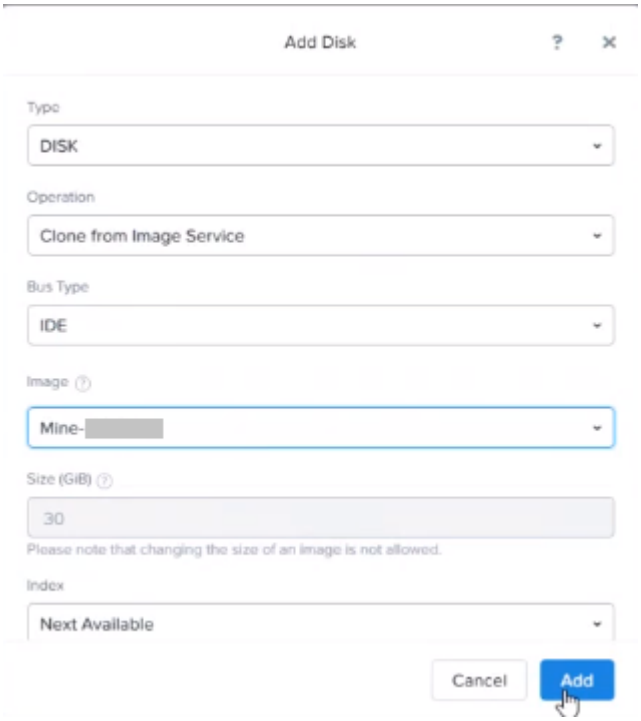
- **Image:** From the drop-down list, select the image that you have uploaded previously to Image Configuration.

  Notes:

  - The Image field gets populated automatically when you select the **Clone from Image Service** option.
  - After the image is selected, the Size (GiB) field displays the size of image automatically and gets disabled.

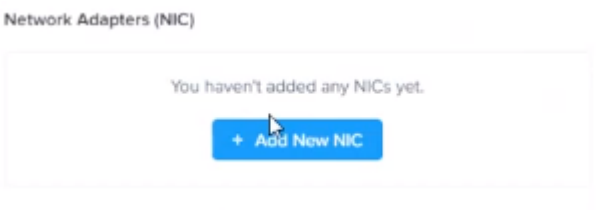
- **Index:** From the drop-down list, select the index.

  The disk gets added to the VM and appears in the table. You can edit and remove the disk as needed.



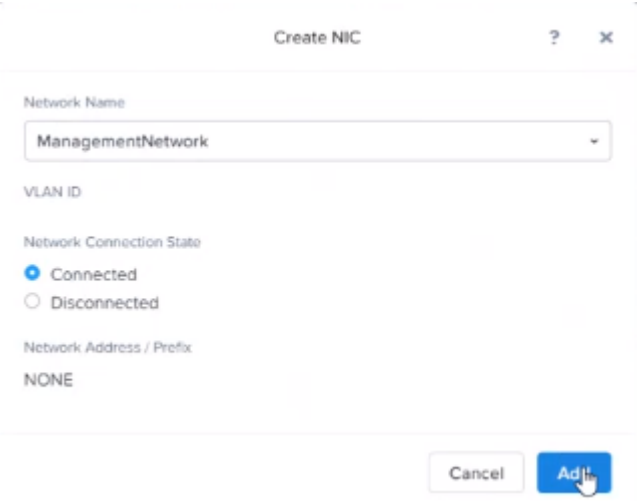
d. For Boot Configuration, retain defaults.

e. For Network Adapters (NIC), to create network interface for the VM, click **+ Add New NIC**.



The Create NIC dialog appears.

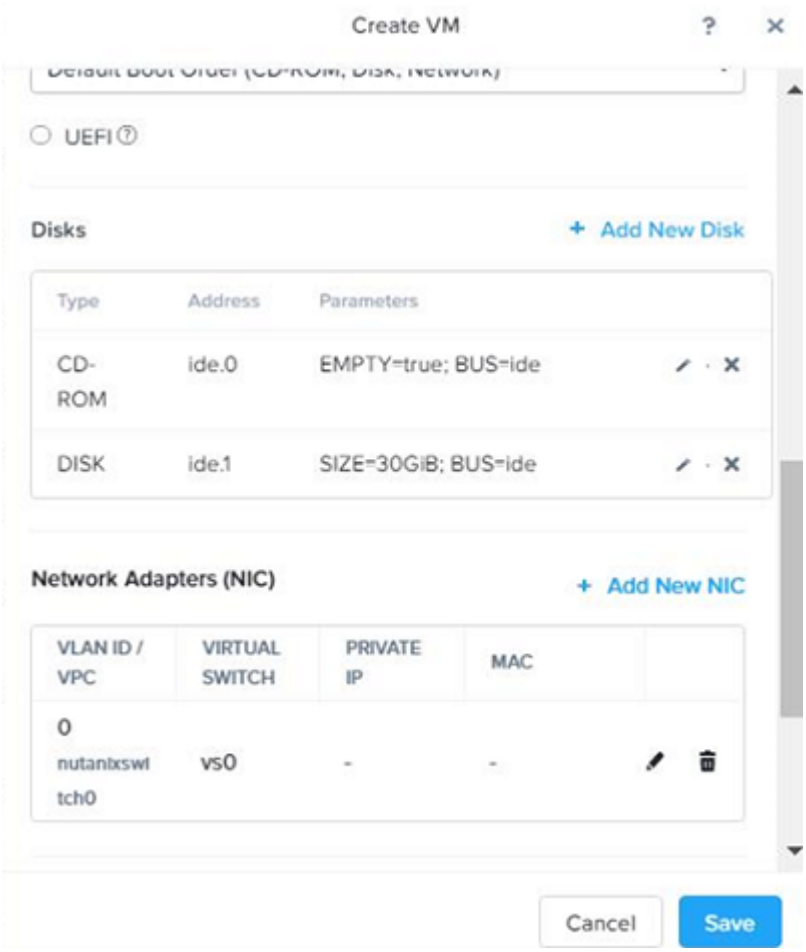
f. On the Create NIC dialog, retain defaults, and then click **Add**.



The network gets added in the table under Network Adapters (NIC). You can edit and remove the network as needed.

Note: The bootstrap VM must have at least one NIC added.

g. Verify the details, and then click **Save**.



The Bootstrap VM is created successfully and appears in the VM table.

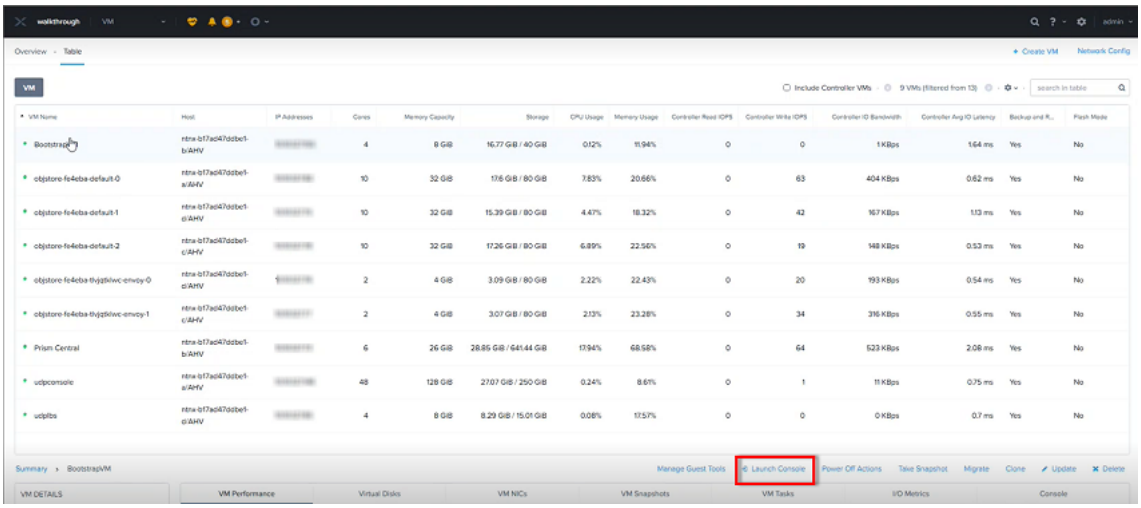
Note: Before proceeding with the Mine deployment process, check the DNS server reachability from Bootstrap VM. For more information, see Checking the DNS Server Reachability from Bootstrap VM.

Checking the DNS Server Reachability from Bootstrap VM

This section provides information about how to check the DNS server reachability from Bootstrap VM.

Follow these steps:

1. Power-on the Bootstrap VM that you have created and wait until the VM gets the IP address.
2. On the VM table, select the Bootstrap VM that you have created, and then click **Launch Console**.



3. Log into the Mine Bootstrap VM using ssh with the following credentials:
   - Username: root
   - Password: enOP@618
4. Install the following package before running the nslookup command from terminal:

   yum install bind-utils
5. After the *bind-utils* package is installed successfully, to check the DNS server connectivity from Bootstrap VM, follow these steps:
   a. To identify the DNS server IP address that is being returned, run the following command on bootstrap VM:

      nslookup <DNS IP address>

      Note: If nslookup fails to return the DNS information/IP address, verify with IT team for the right DNS information to provide during the Mine deployment rerun process.

   b. Check whether the DNS server is reachable using the *nslookup* and ping commands.

   c. Check whether the right DNS server IP address is returned.

   d. Check the DNS suffix with *nslookup* result.
6. After the *nslookup* command returns proper DNS IP/address information, to log out of the Bootstrap VM, run the following command, and then close the console window:

   exit
7. Start the Mine deployment process.

Deploying Arcserve UDP using Nutanix Mine Deployment Wizard

This section provides information about how to deploy Arcserve UDP using Nutanix Mine deployment wizard.

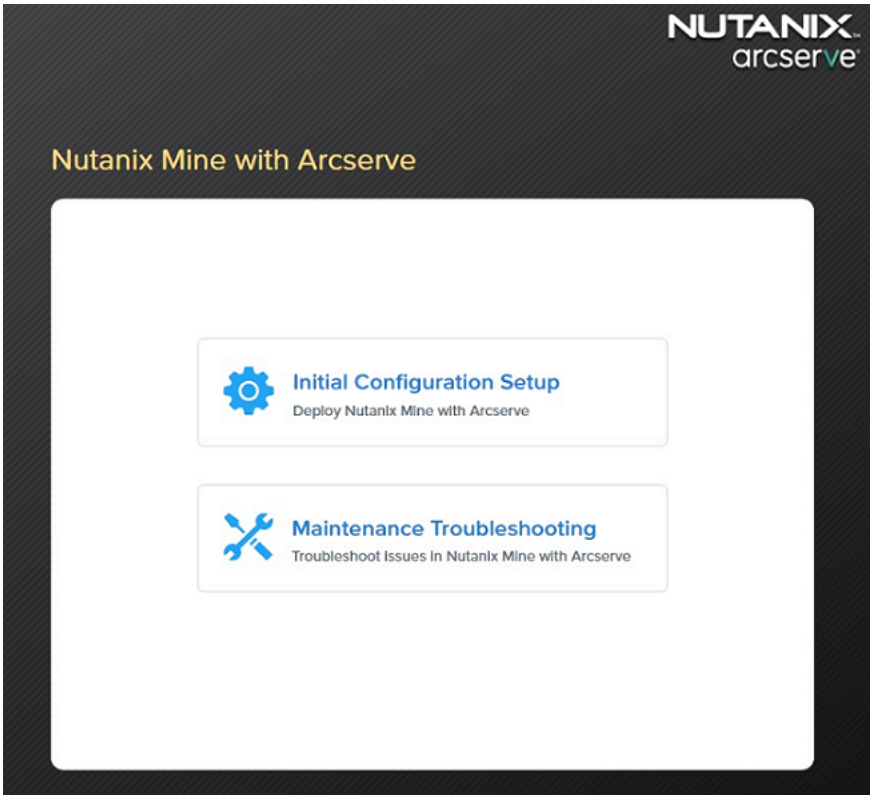
Follow these steps:

1. Open any browser, and then type the IP address of Bootstrap VM in the address bar/URL bar in the following format:

   https://<Bootstrap VM IP address>

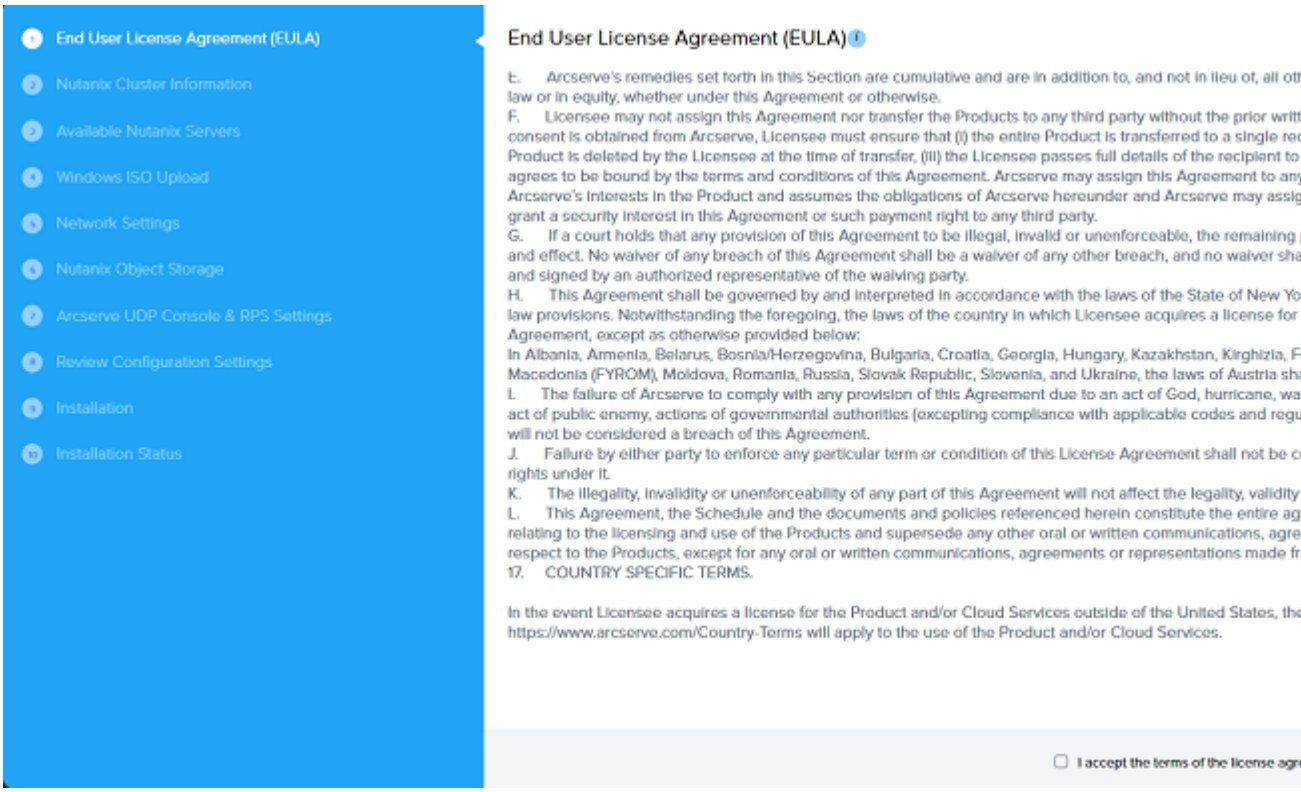
   The home screen of Bootstrap VM opens.

2. On the Nutanix Mine with Arcserve deployment wizard, click **Initial Configuration Setup**.



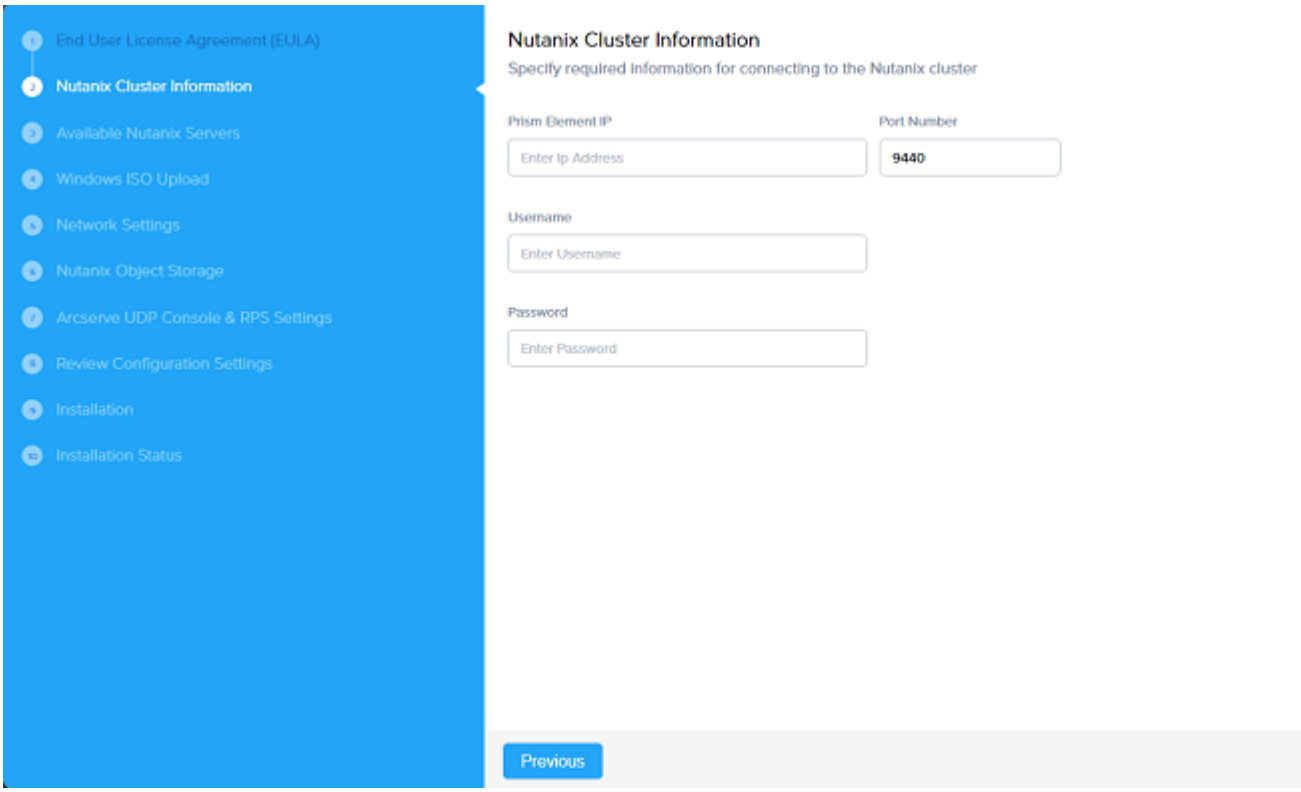
   The Nutanix Mine setup screen appears and displays the workflow.

3. On the End User License Agreement (EULA) page, read the license agreement carefully, select the **I accept the terms of the license agreement** check box, and then click **Next**.

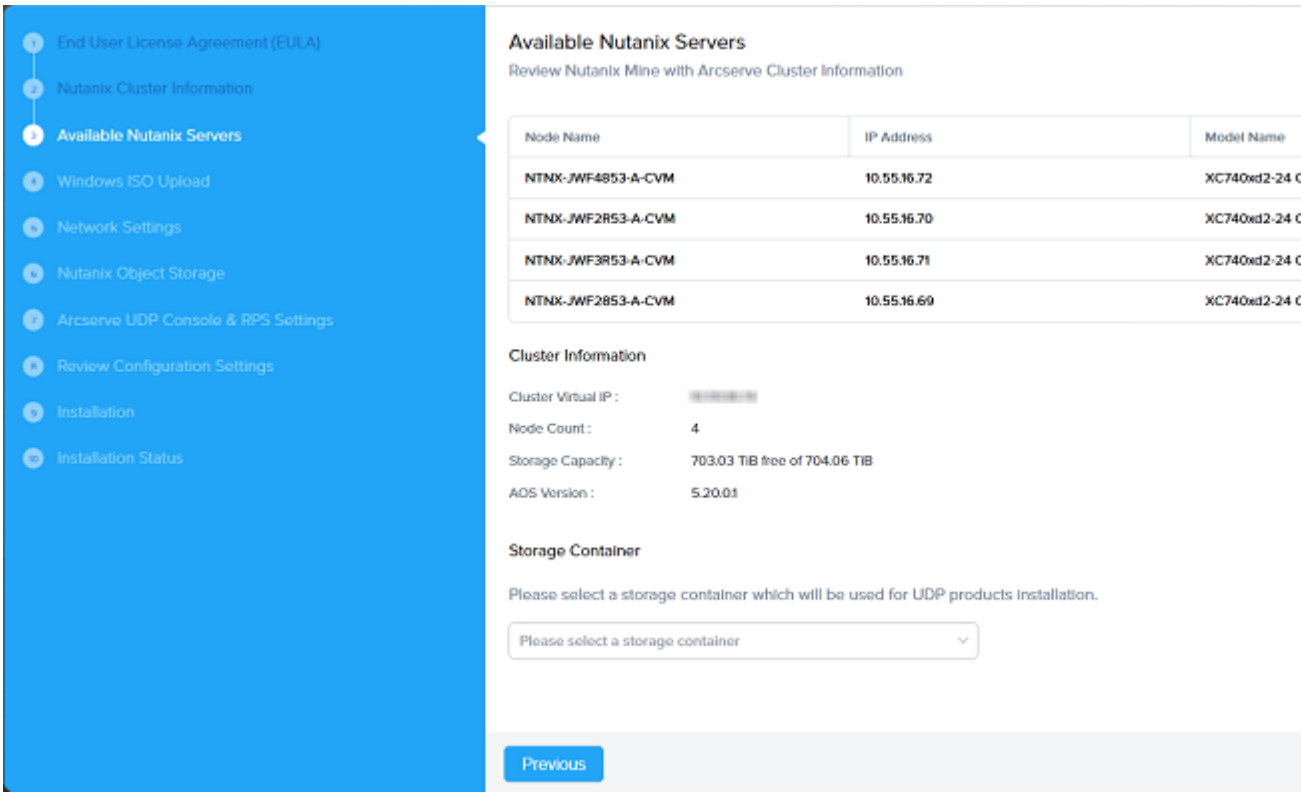


4. On the Nutanix Cluster Information page, to connect to a Nutanix cluster, specify the following details, and then click **Next**:
   - **Prism Element IP:** Enter the Virtual IP address of the Nutanix Prism Element.
   - **Port Number:** Enter the port number. The default port value is 9440.
   - **Username:** Type the user name of the cluster administrator.

     Note: We recommend creating a separate local account for the Nutanix Mine deployment wizard. Active directory is not recommended as it can prevent access to the wizard in case of any issue.
   - **Password:** Type the password of the cluster administrator.



5. On the Available Nutanix Servers page, review the Nutanix cluster information. Additionally, under Storage Container, select a default storage container from the drop-down list, and then click **Next**.

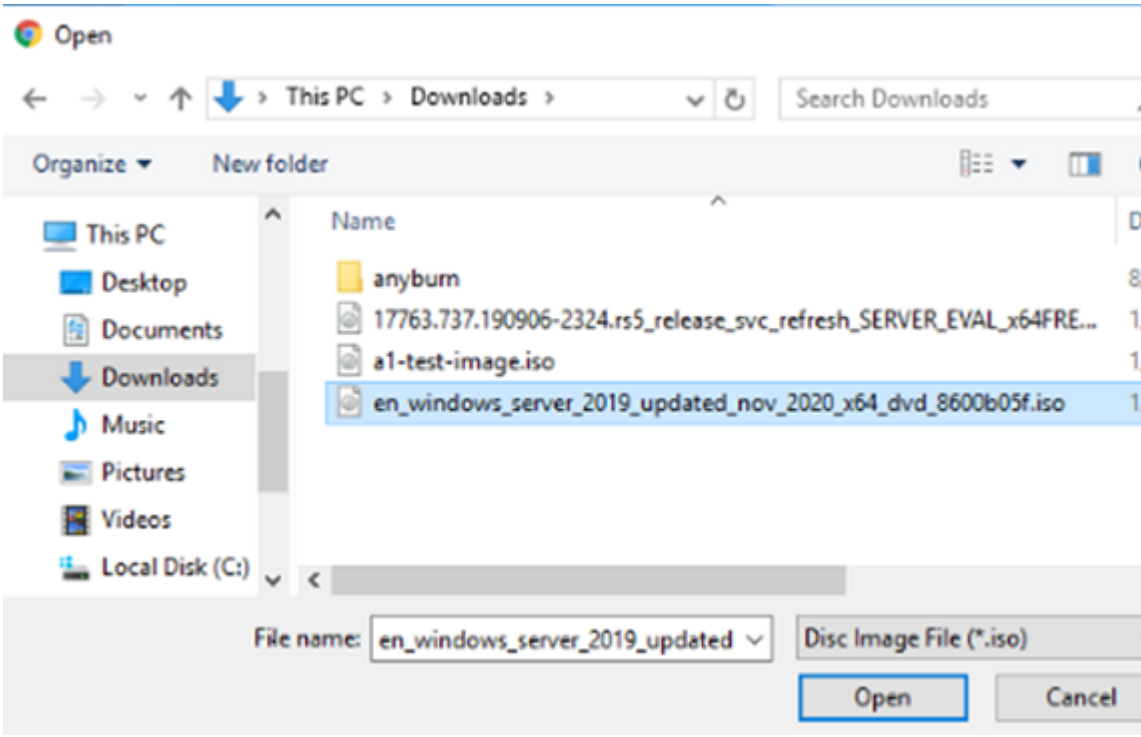


6. On the Windows ISO Upload page, to upload the Windows server ISO file, do one of the following, and then click **Next**:

   - If you want to upload the ISO file from your workstation, do the following:

     a. Select the **Upload Windows Server ISO File** and then click **Upload**.

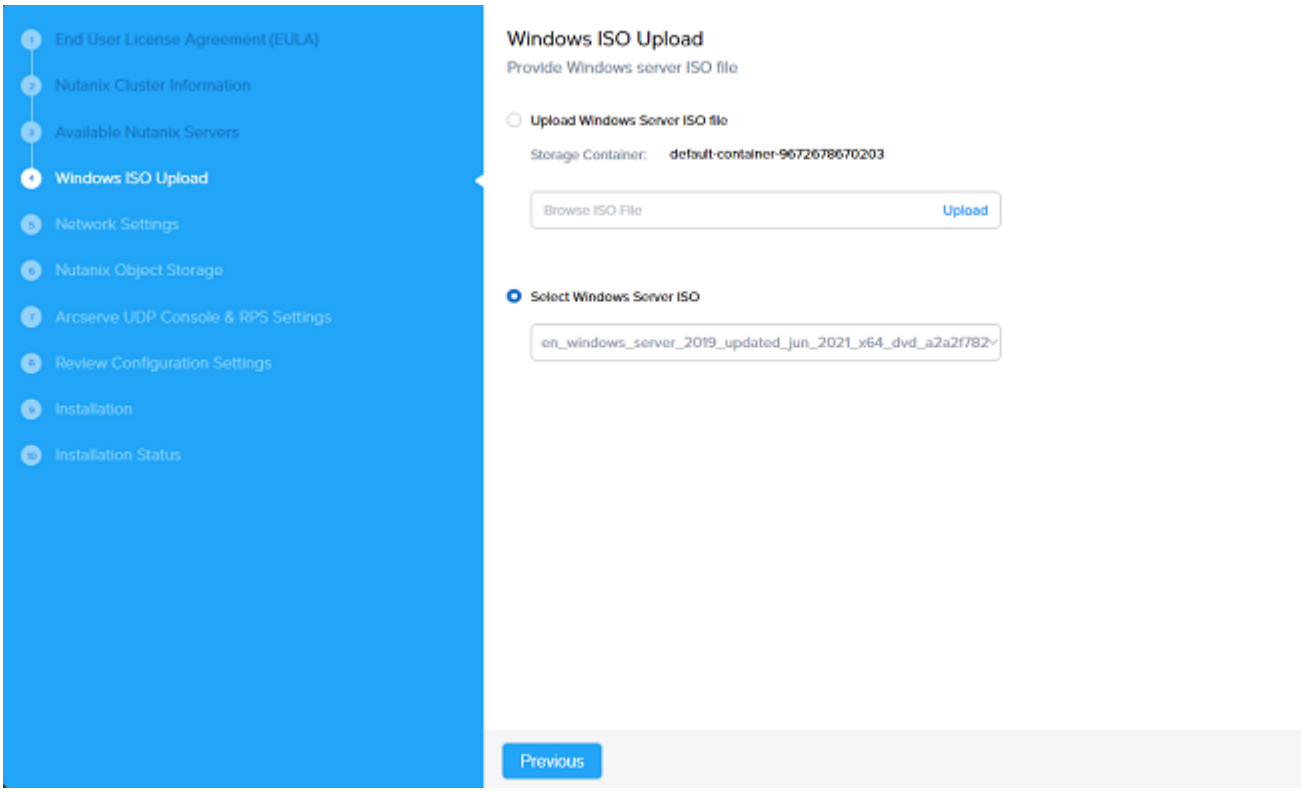
     b. Specify the location of Windows 2019 standard ISO image downloaded from the Arcserve download link, and then click **Open**.



     Wait until the upload progress reaches to 100%.

   - If you have already downloaded the ISO file and copied it into the Image Configuration, click **Select Windows Server ISO**, and then select the Window server ISO file from the drop-down list.

     Note: For deployment on Nutanix clusters, Arcserve UDP supports only Windows Server 2019 operating system.



7. On the Network Settings page, specify the following, and then click **Next**:
   - **Network Name:** From the drop-down list, select the network name or type a new name for the network as needed.

     Note: To add a new network, go to Nutanix dashboard.
   - **VLAN ID:** Enter the VLAN ID for the network.

     Note: If you specify the VLAN value other than 0, make sure to configure the network switches accordingly.
   - **DNS 1:** Enter the IP address of the DNS server.
   - **DNS 2 (Optional):** Enter the IP address of the second DNS server if needed.
   - **Specify the Domain Credentials (Optional):** Specifies the credentials for a domain. If you want to add UDP Console + RPS, and additional RPS systems into the domain, specify the following domain credentials:
     - **Domain Name:** Enter the domain name.
     - **Username:** Specifies the user name that has access rights to log into the domain.

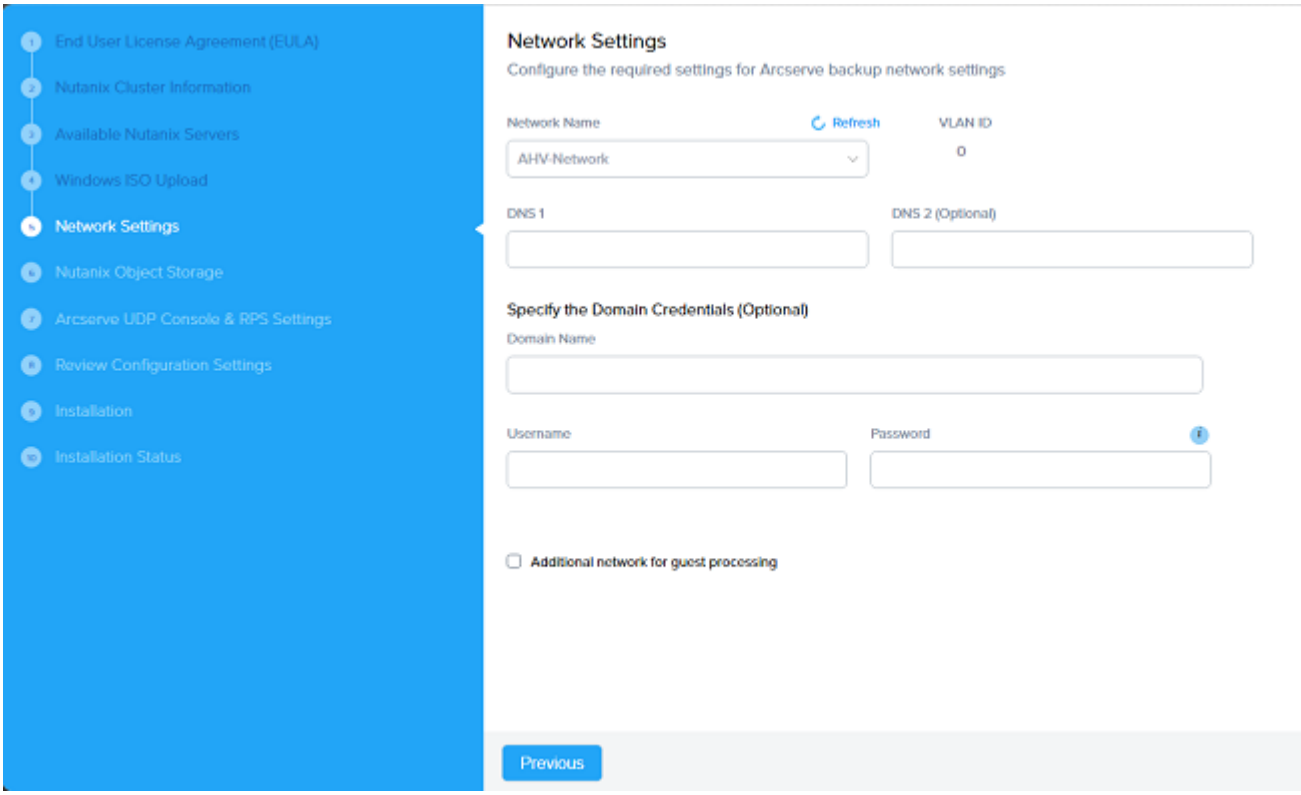
       Type the user name in the following format:

domain\name

- **Password:** Type the corresponding password for the Username.

- **Additional network for guest processing:** To create an additional network for guest processing, select the **Additional network for guest processing** check box.

  Note: If you want the VMs to be backed up on a different network other than the Arcserve infrastructure, select the **Additional network for guest processing** check box. Creating an additional network is optional.



Note: To reset the network settings, click **Refresh**.

8. On the Nutanix Object Storage page, do the following, and then click **Next**:

   - **Access Key ID:** Enter the Access Key ID.
   - **Secret Key:** Enter the Secret Key.

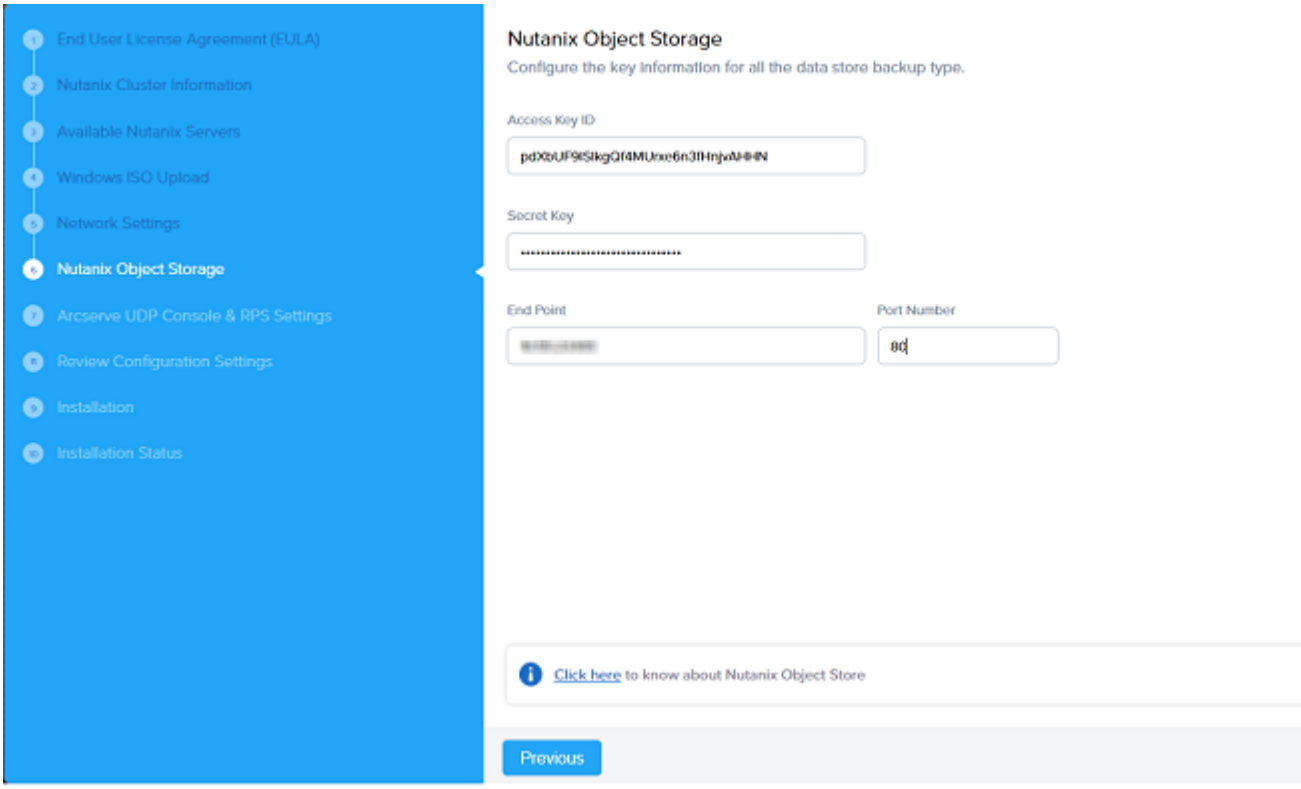
     Note: Use the Access Key and Secret Key that is downloaded during the Object Store deployment.

   - **End Point:** Enter the End Point IP address.

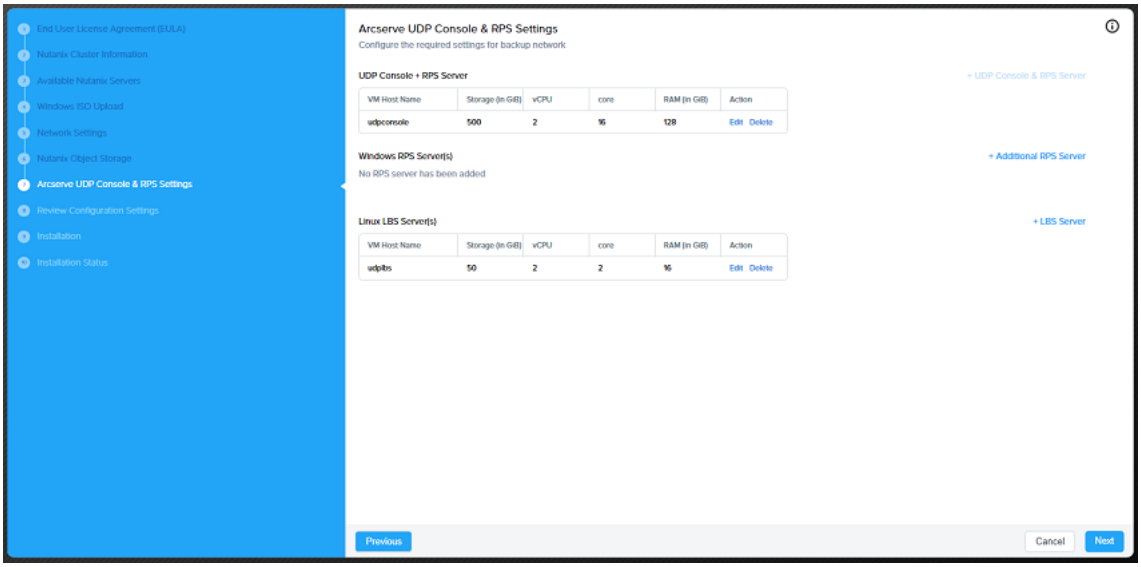
     Note: Use the public IP address provided during the Object Store

deployment.

- **Port Number:** Enter the port number. The default port value is 80.



9. On the Arcserve UDP Console & RPS Settings page, do the following, and then click **Next**:



Modify UDP Console + RPS Server

To modify UDP Console and RPS Server, follow these steps:

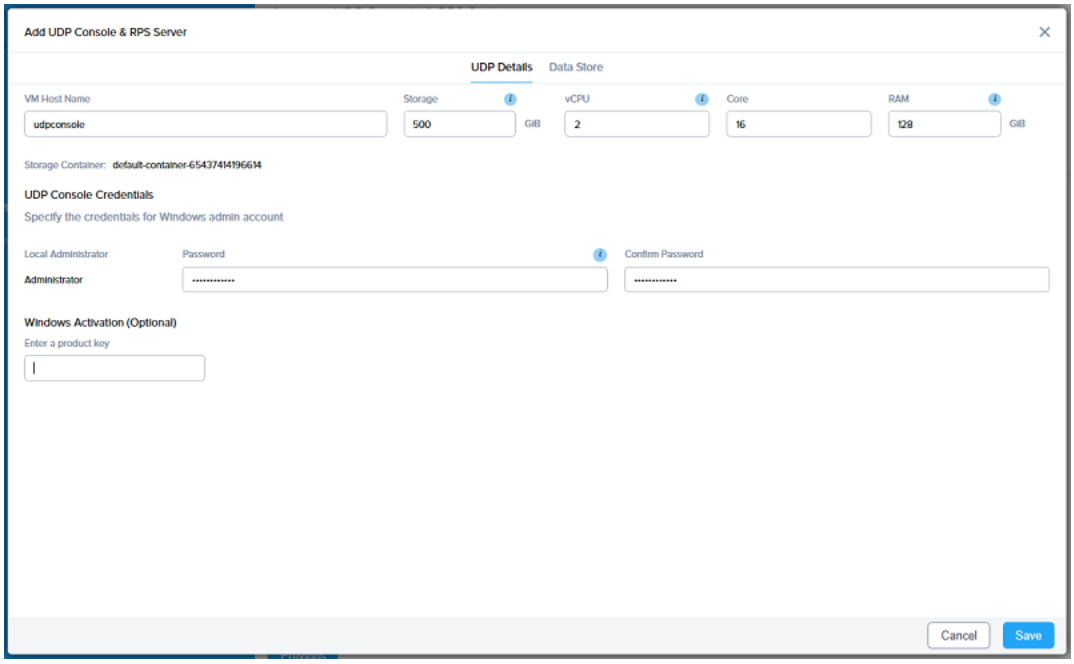
a. Click **Edit**.

The Add UDP Console & RPS Server screen appears.

b. Under UDP Details tab, change the following settings as needed:

- **VM Host Name:** Enter a valid host name of the VM that can be resolved by DHCP.
- **Storage:** Enter the virtual disk capacity for the VM.
- **vCPU:** Enter the number of virtual CPUs to allocate to the UDP Console.
- **Core:** Enter the number of cores assigned to each virtual CPU.
- **RAM:** Enter the amount of RAM to allocate to the UDP Console VM.
- **UDP Console Credentials:** Specifies the UDP Console credentials for the Windows admin account. Enter the local administrator password and then retype the password to confirm.
- **Windows Activation (Optional):** To activate Windows, provide the Windows activation key.

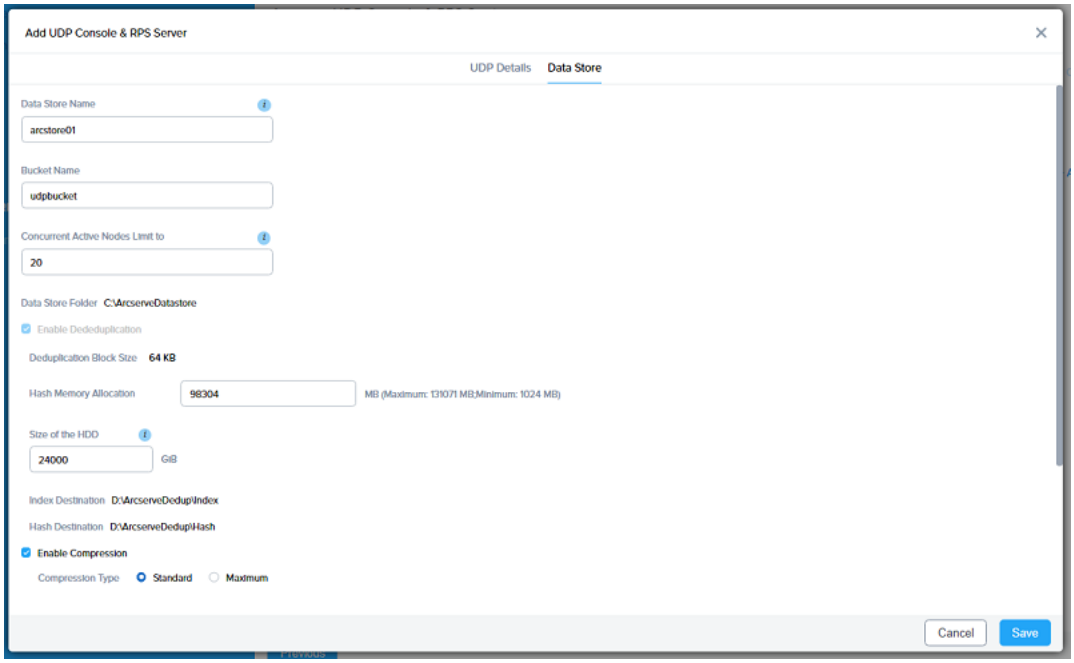
  Note: If the activation key is not provided, you can activate Windows in a timely manner from the UDP Console Windows OS.



c. Under Data Store tab, change the following settings as needed:

- **Data Store Name:** Enter the data store name.
- **Bucket Name:** Enter the bucket name.
- **Concurrent Active Nodes Limit to:** Enter the number of concurrent active nodes that you want to limit. The default value is 4.

  Note: By default, the Enable Deduplication option is enabled.
- **Deduplication Block Size:** Enter the deduplication block size. The default value is 64 KB.
- **Hash Memory Allocation:** Specifies the amount of physical memory that you allocate to keep hashes. Enter the memory size in the range of 1024 MB to 8191 MB.
- **Size of the HDD:** Enter the size of HDD in GiB.
- **Enable Compression:** To enable the data compression settings, select the **Enable Compression** check box, and then select the compression type.
- **Enable Encryption:** To enable the data encryption settings, select the **Enable Encryption** check box, type the encryption password, and then retype the encryption password to confirm.



d. Click **Save**.

Add Windows RPS Server(s)

To add Windows RPS server, follow these steps:

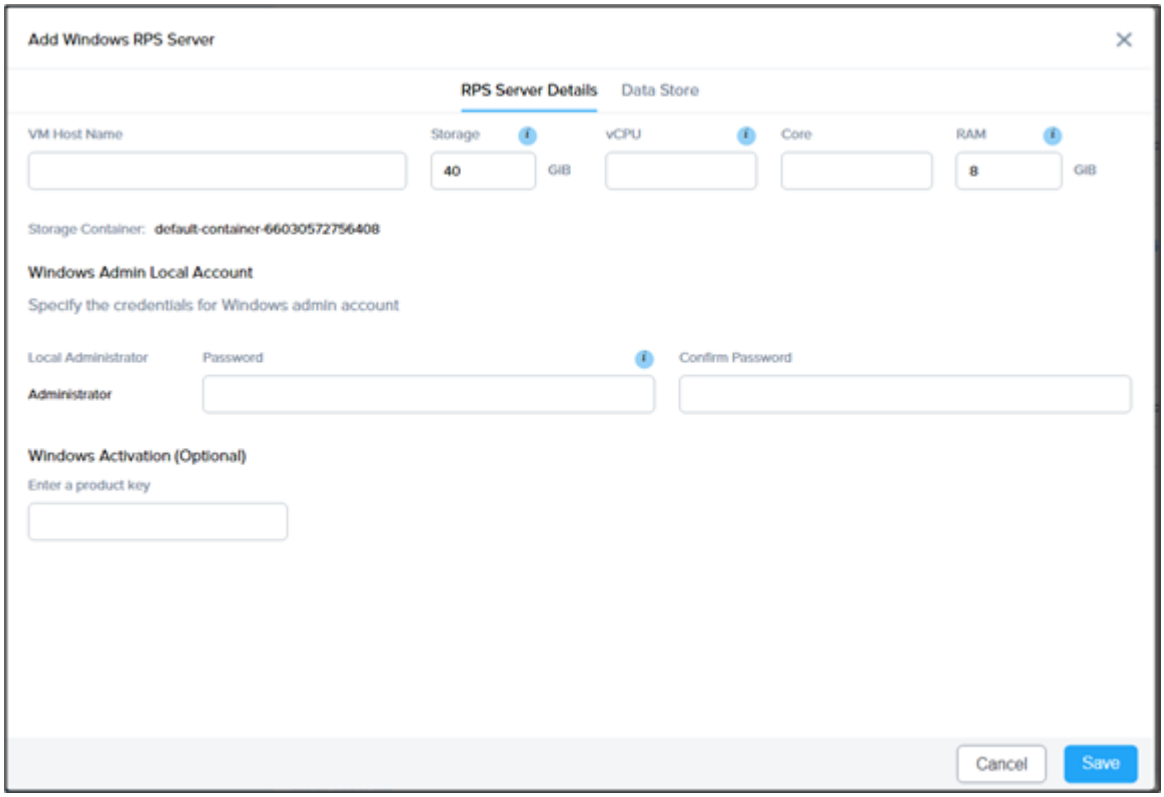
a. Click **+ Additional RPS Server**.

   The Add Windows RPS Server screen appears.

b. Under RPS Server Details tab, specify the following:

   - **VM Host Name:** Enter a valid host name of the VM that can be resolved by DHCP.
   - **Storage:** Enter the virtual disk capacity for the VM.
   - **vCPU:** Enter the number of virtual CPUs to allocate to the Windows RPS server.
   - **Core:** Enter the number of cores assigned to each virtual CPU.
   - **RAM:** Enter the amount of RAM to allocate to the Windows RPS server.
   - **Windows Admin Local Account:** Specifies the credentials for Windows admin local account. Enter the local administrator password, and then retype the password to confirm.
   - **Windows Activation (Optional):** To activate Windows, provide the Windows activation key.

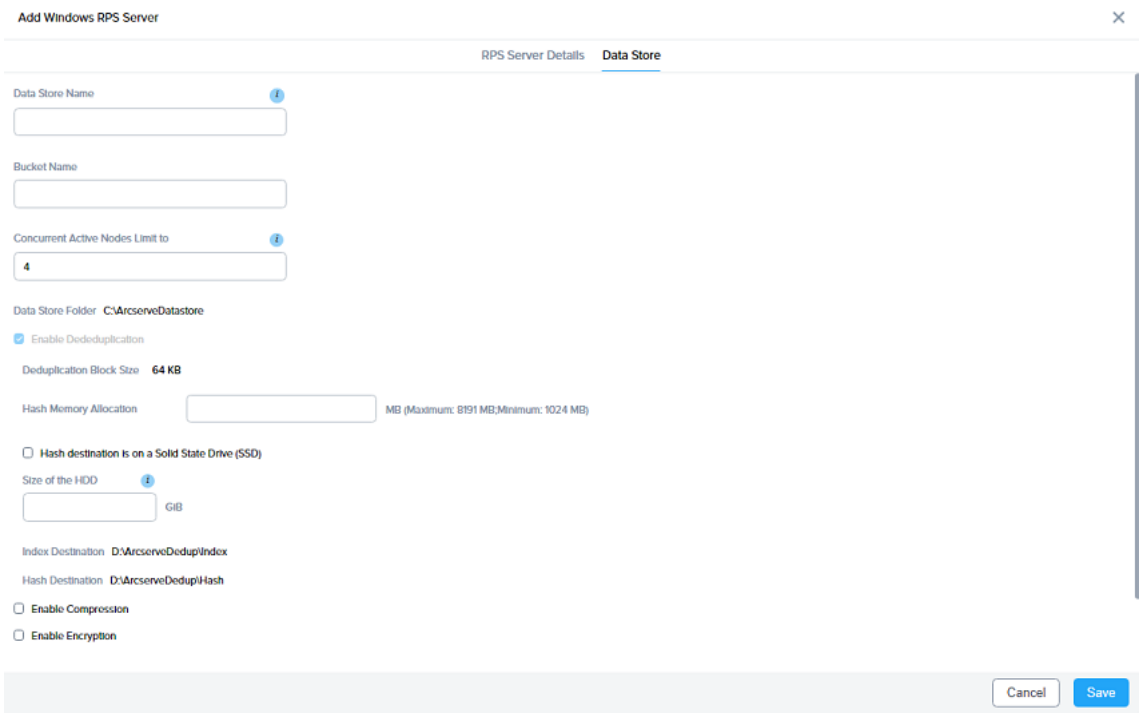
     Note: If the activation key is not provided, you can activate Windows in a timely manner from UDP RPS Windows OS.



c. Under Data Store tab, specify the following:

- **Data Store Name:** Enter the data store name.
- **Bucket Name:** Enter the bucket name.
- **Concurrent Active Nodes Limit to:** Enter the number of concurrent active nodes that you want to limit. The default value is 4.

  Note: By default, the Enable Deduplication option is enabled.
- **Deduplication Block Size:** Enter the deduplication block size. The default value is 64 KB.
- **Hash Memory Allocation:** Specifies the amount of physical memory that you allocate to keep hashes. Enter the memory size in the range of 1024 MB to 8191 MB.
- **Hash destination is on Solid State Drive (SSD):** To create the deduplication datastores such as Data Destination, Index Destination, and Hash Destination on the SSD storage drive, select the **Hash destination is on Solid State Drive (SSD)** check box. The Size of the SSD field gets populated. Enter the size of SSD in GiB.
- **Enable Compression:** Select the **Enable Compression** check box to enable the data compression settings.
- **Enable Encryption:** Select the **Enable Encryption** check box to enable the data encryption settings.



d. Click **Save**.

Add Linux LBS Server(s)

To add LBS server, follow these steps:

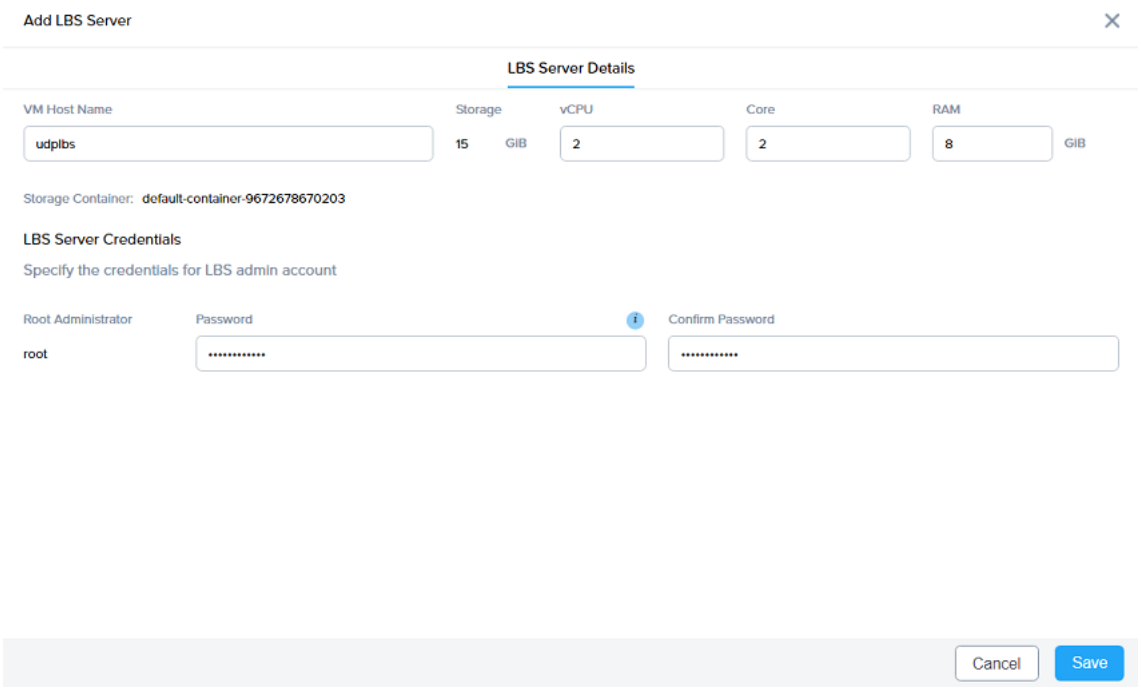
a. Click **+ LBS Server**.

The Add LBS Server screen appears.

b. On the Add LBS Server screen, specify the following:

- **VM Host Name:** Enter a valid host name of the VM that can be resolved by DHCP.
- **Storage:** Specifies the storage capacity for the LBS server. The default storage capacity is 15 GiB.

  Note: For UDP LBS, 15 GiB is allocated by default.
- **vCPU:** Enter the number of virtual CPUs for the LBS server.
- **Core:** Enter the number of cores assigned to each virtual CPU.
- **RAM:** Enter the amount of RAM to allocate to the LBS server.
- **LBS Server Credentials:** Specifies the credentials for LBS admin account. Enter the root administrator password and then retype the password to confirm.

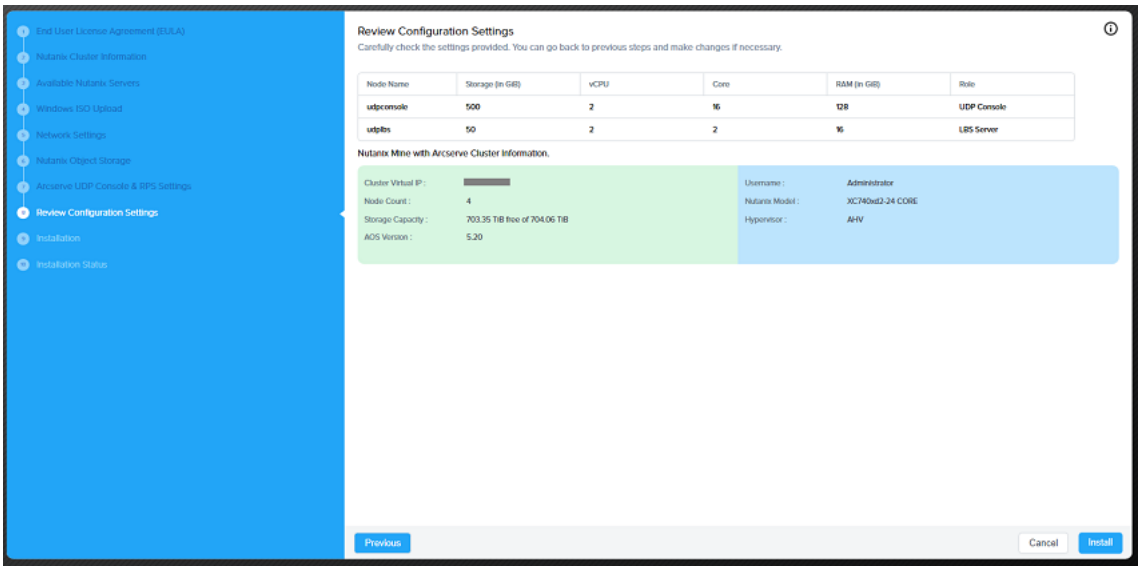


c. Click **Save**.

Notes:

- By default, the UDP Console is added and the + UDP Console & RPS Server option is disabled.
- You cannot add multiple UDP Consoles, but you can add multiple RPS and LBS servers as needed.
- You can edit and delete UDP Console, RPS, and LBS servers if required. If you click the **Delete** option, you are asked whether you are sure to remove the corresponding server. Click **Delete** to confirm.

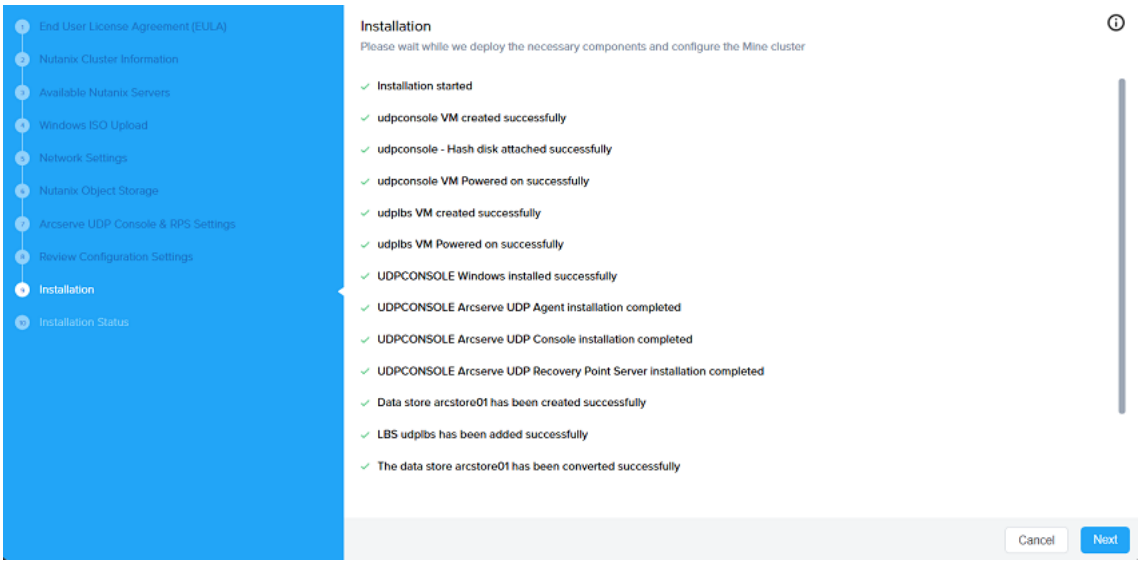
10. On the Review Configuration Settings page, review the information, and do one of the following:
    - If the information is correct, click **Install**.
    - If the information is incorrect, to make changes to the settings of the previous pages as needed, click **Previous**. Return to the Review Configuration Settings page again, and then click **Install**.



The installation begins. A status bar appears and displays the status messages as the installation progresses.

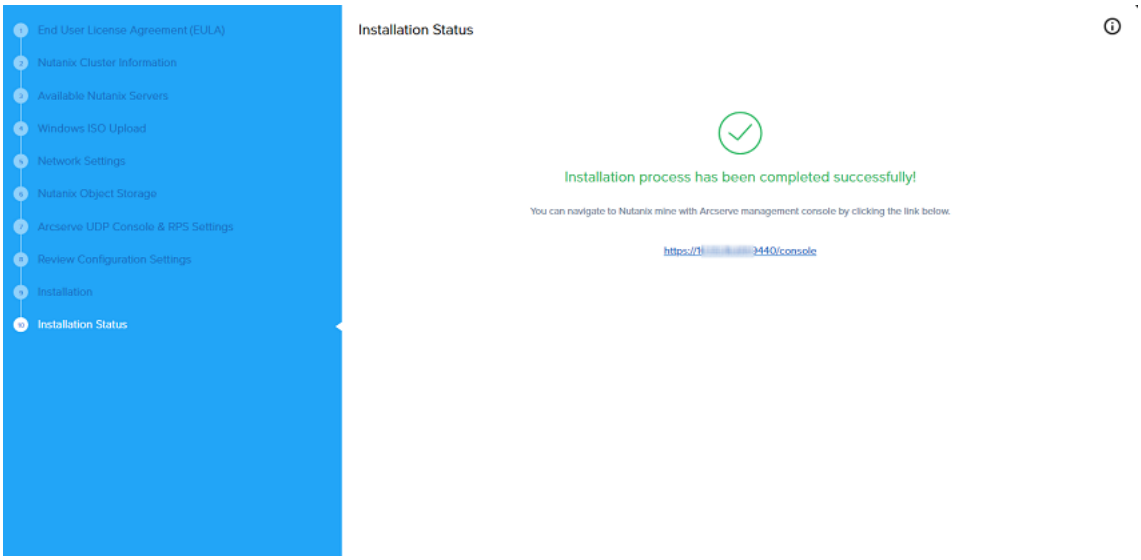
Note: The installation process typically takes approximately 1 hour 30 minutes to complete. After the installation completes, the *Next* button is enabled.

11. To view the installation status, click **Next**.



12. On the Installation Status page, the following message appears:

Installation process has been completed successfully!



After the installation is complete, to view the Arcserve Home dashboard, which now shows Arcserve information, click the link given on the Installation Status page.

Arcserve UDP is deployed successfully onto the Nutanix cluster.

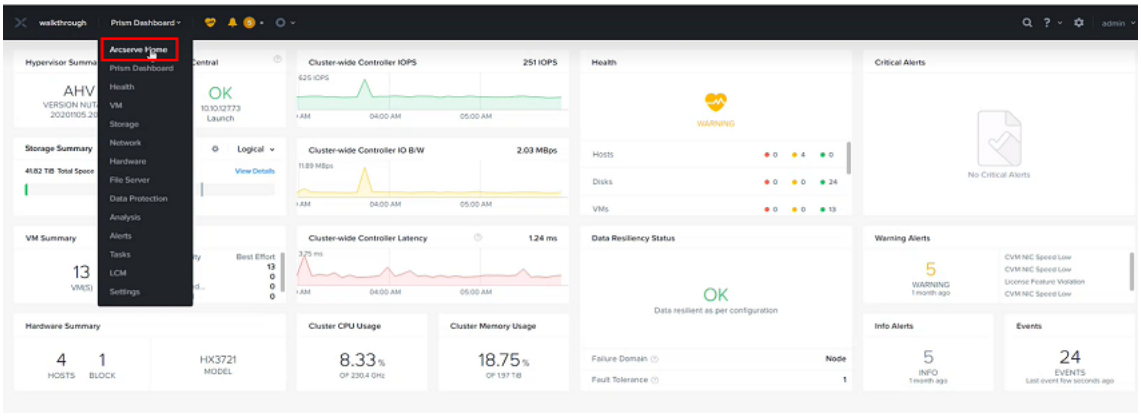
Note: To re-register the reverse proxy, see Maintenance and Troubleshooting.

Accessing the Arcserve Home Dashboard and UDP Console

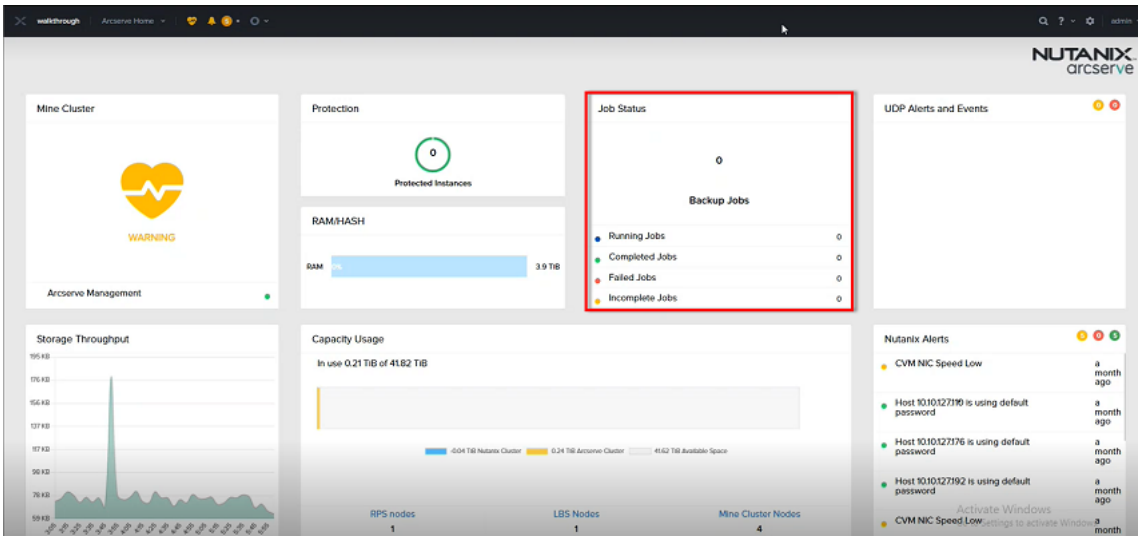
This section provides information about how to access the Arcserve Home dashboard and UDP Console.

Follow these steps:

1. To view the Arcserve Home dashboard, do one of the following:
   - Click the URL that appears on the *Installation Status* page. For information, see Step 12 of Mine Deployment process.
   - Log into the Prism Element web console using admin credentials.
2. On the Prism Element Home page, navigate to Prism Dashboard drop-down list, and then select **Arcserve Home**.

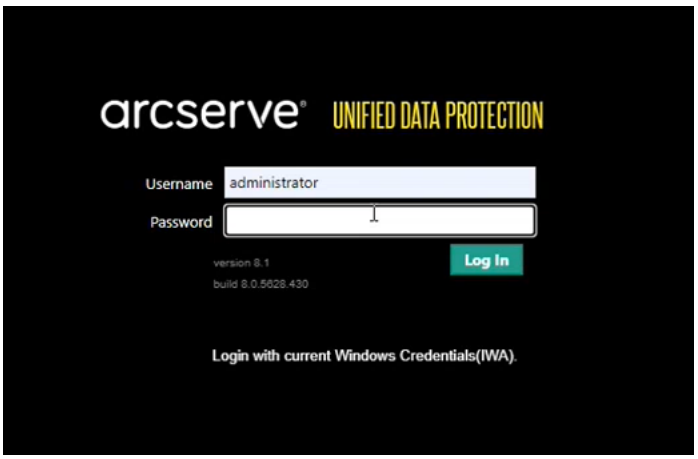


3. To access UDP Console, on the Arcserve Home dashboard, navigate to **Job Status** wizard, and then click any one of the following options:
   - Running Jobs
   - Completed Jobs
   - Failed Jobs
   - Incomplete Jobs



A new window opens with the UDP Console login page.

4. Log into the UDP Console as an administrator.



Note: Type the same username and password that you have provided during the Mine deployment process.

Maintenance Troubleshooting

This section provides information about how to re-register the reverse proxy. You can repair the existing UDP installation such as modify/re-install the Arcserve Home dashboard.

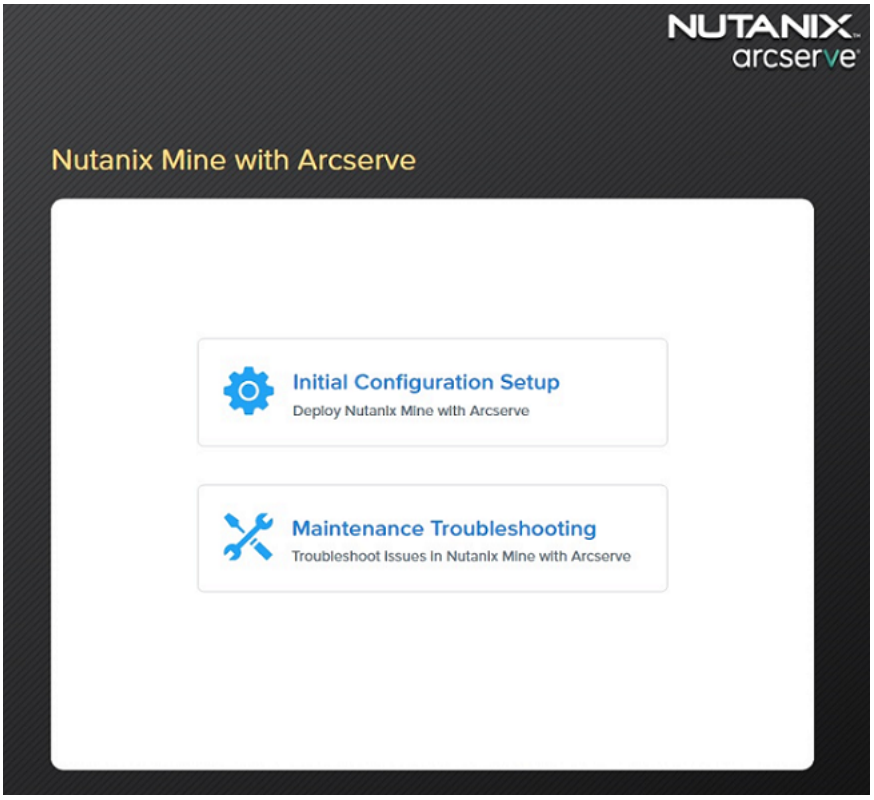
Follow these steps:

1. Open any browser, and then type the IP address of Bootstrap VM in the address bar/URL bar in the following format:

   https://<Bootstrap VM IP address>

   The home screen of Bootstrap VM opens.

2. On the Nutanix Mine with Arcserve deployment wizard, click **Maintenance and Troubleshooting**.

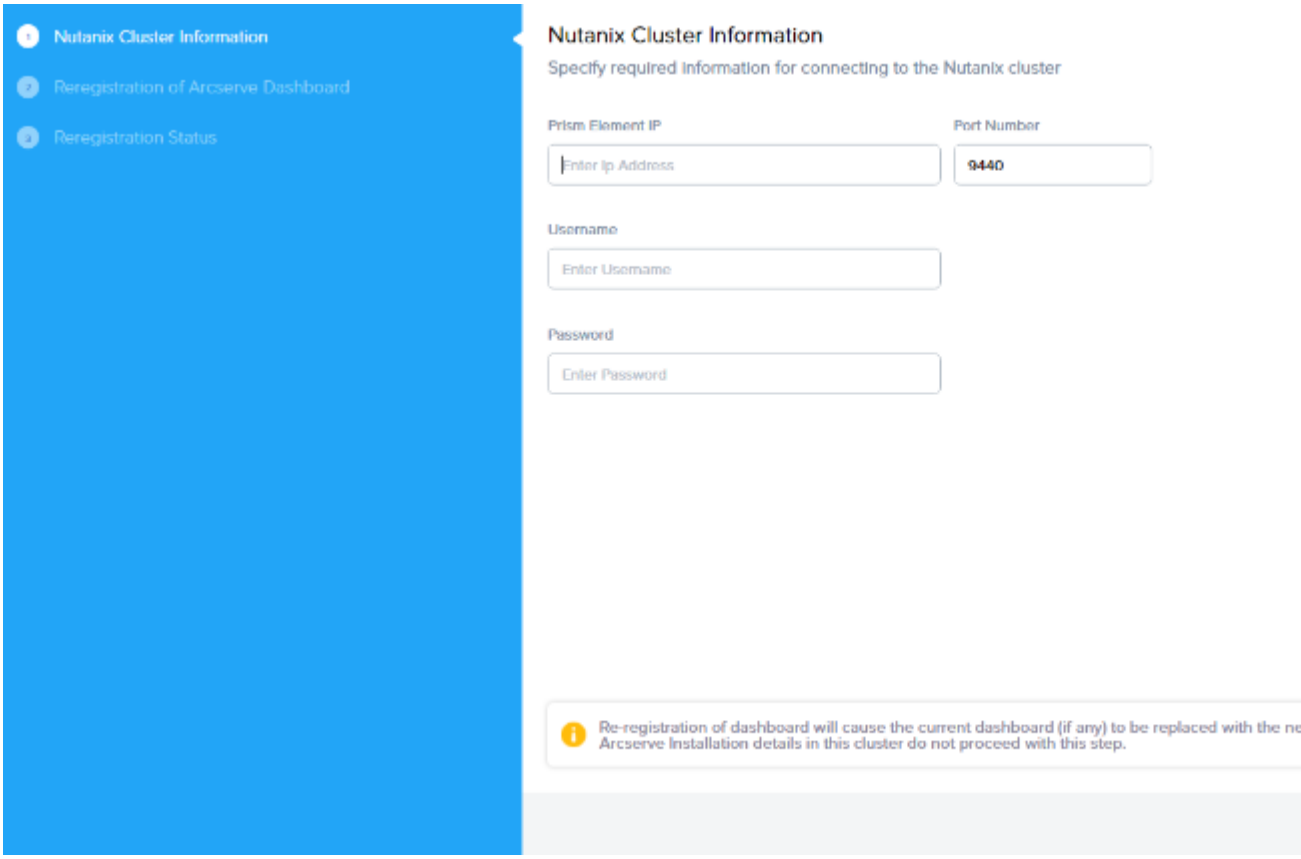


   The Nutanix Mine deployment wizard troubleshooting screen appears and displays the workflow.

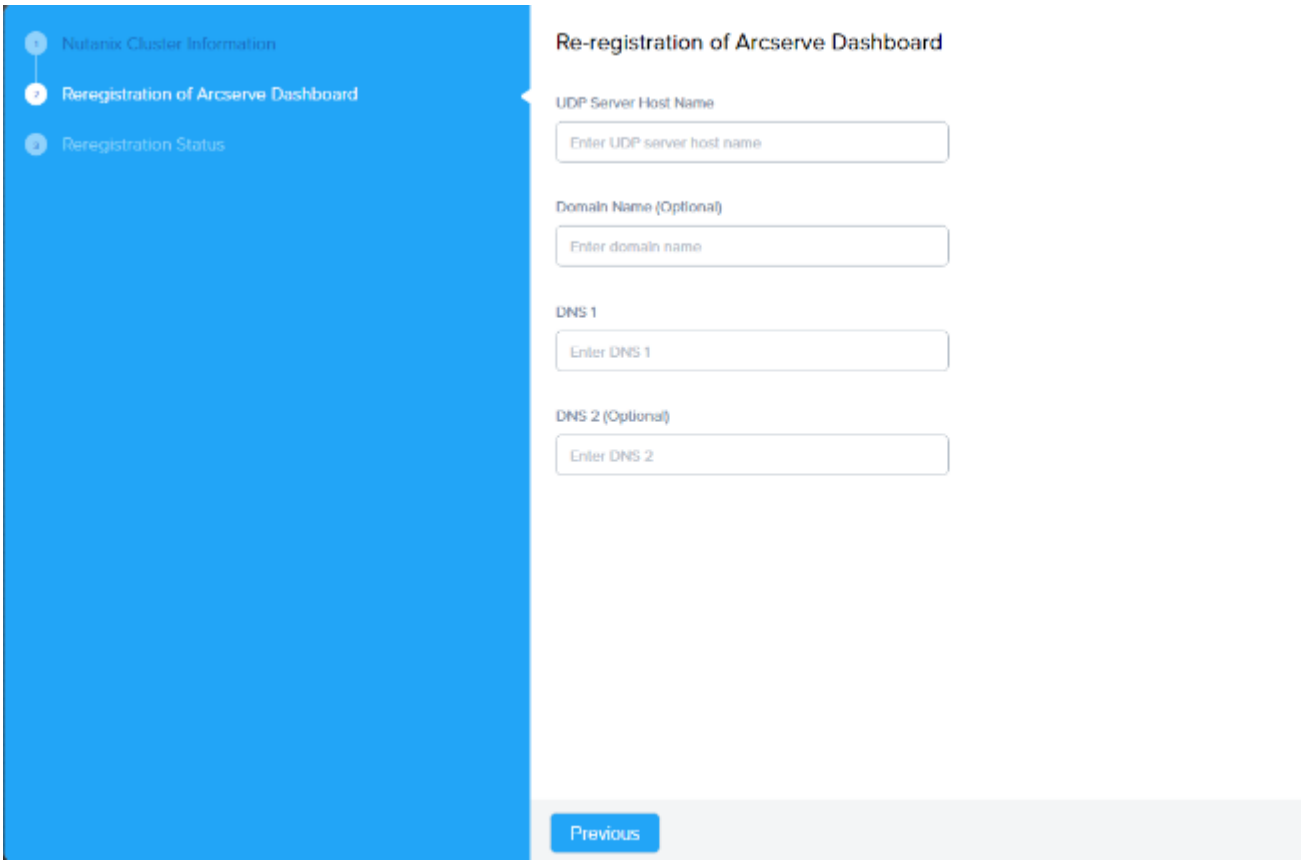
3. On the Nutanix Cluster Information page, to connect to the Nutanix cluster, specify the following details, and then click **Next**:

   Note: Provide the details of the Nutanix cluster where you have Arcserve UDP installed.

- **Prism Element IP:** Enter the IP address of Nutanix Prism Element.
- **Port Number:** Enter the port number. The default port value is 9440.
- **Username:** Type the user name of the cluster administrator.
- **Password:** Type the password of the cluster administrator.

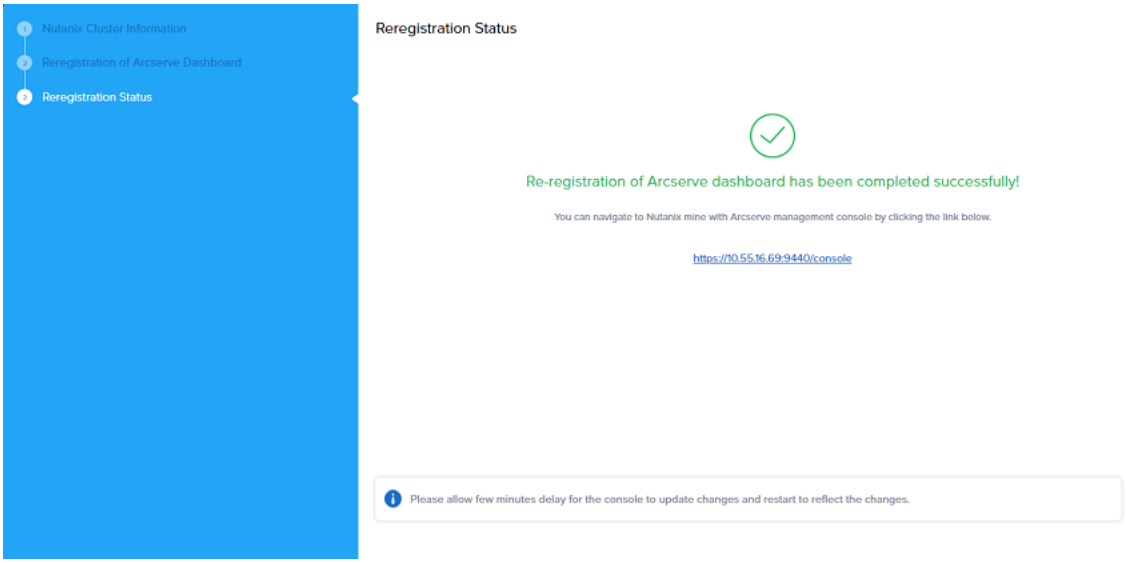


4. On the Re-registration of Arcserve Dashboard page, do the following, and then click **Reinstall**:
   - **UDP Server Host Name:** Enter the UDP server host name.
   - **Domain Name (Optional):** Enter the domain name if required.
   - **DNS 1:** Enter the IP address of the DNS server.
   - **DNS 2 (Optional):** Enter the IP address of the second DNS server if needed.



5. On the Re-registration Status page, the following message appears:

Re-registration of Arcserve dashboard has been completed successfully!



After the Re-registration process is completed successfully, to navigate to the Nutanix cluster with Arcserve Management Console, click the link given on the Re-registration Status page.

Locating Mine Deployment Log Files

You can find the Mine deployment log files under bootstrap VM in the following locations:

- */home/ArcServeUDP/deploy_scripts/arcserve.log*

  Logs about VM's Windows OS installation and UDP installation.

- */home/ArcServeUDP/deploy_scripts/status.log*

  Logs about image uploads and VM's creation status.

- */home/ArcServeUDP/deploy_scripts/log_timestamp.log*

  Logs about image uploads such as VM's creation status, dashboard setup in-detail with errors, and information recorded related to deployment.

- */root/.pm2/logs/www-error.log*

  Logs about the failure requests made with errors from deployment wizard.

- */root/.pm2/logs/www-out.log*

  Logs about all the requests made from deployment wizard.

Note: To log into the bootstrap VM, use the following credentials:

- Username: root
- Password: enOP@618

Chapter 5: Activating the N-Series Nutanix Cluster and Arcserve UDP License

To get the licenses required for N-Series Nutanix Cluster and Arcserve UDP product, contact Arcserve support.

Chapter 6: Working with Arcserve N-Series Appliance

Using Arcserve N-Series Appliance, you can create backup plans for Windows, Linux, and virtual machines. You can also write data to a tape device and create a virtual standby machine.

This section contains the following topics:

Activate Arcserve Product on the Appliance

For activating Arcserve product on the Appliance, see Arcserve Product Licensing Online Help.

Create a Plan Using Arcserve N-Series Appliance Wizard

A plan is a collection of steps that defines which nodes to back up and when to back up. The Arcserve N-Series Appliance lets you create basic plans. Creating a plan using the Arcserve wizard is a three-step process:

1. Add the nodes you want to protect.

   You can select Windows nodes or virtual machines from vCenter/ESX or Hyper-V Servers.

2. Define the backup schedule.
3. Review and confirm the plan.

In addition to a basic plan, Arcserve UDP lets you create complex plans and control many parameters from the UDP Console. To create complex plans from the UDP Console, see the *Arcserve UDP Solutions Guide*.

Create a Backup Plan for Linux Nodes

You can back up Linux nodes from the Arcserve N-Series Appliance UDP Console. The Linux Backup Server is already added to the UDP Console.

Follow these steps:

1. Open the Arcserve N-Series Appliance UDP Console.
2. Click **resources**, **Plans**, **All Plans**.
3. Create a Linux Backup plan.
4. Specify the Source, Destination, Schedule, and Advanced configurations.

   Note: For more information about each of the configurations, see How to Create a Linux Backup Plan in the Solutions Guide.
5. Run the backup plan.

Create an On-Appliance Virtual Standby Plan

Arcserve N-Series Appliance has the capability to serve as a virtual standby machine.

Follow these steps:

1. Verify and ensure that you have a successful backup plan.
2. Open the Arcserve N-Series Appliance Console.
3. Navigate to the plans and modify the backup plan.
4. Add a Virtual Standby task.
5. Update the Source, Destination, Virtual Machine configurations.

   Note: For more information about the configurations, see How to Create a Virtual Standby Plan topic in the Arcserve UDP Solutions Guide.

6. Save and run the plan.

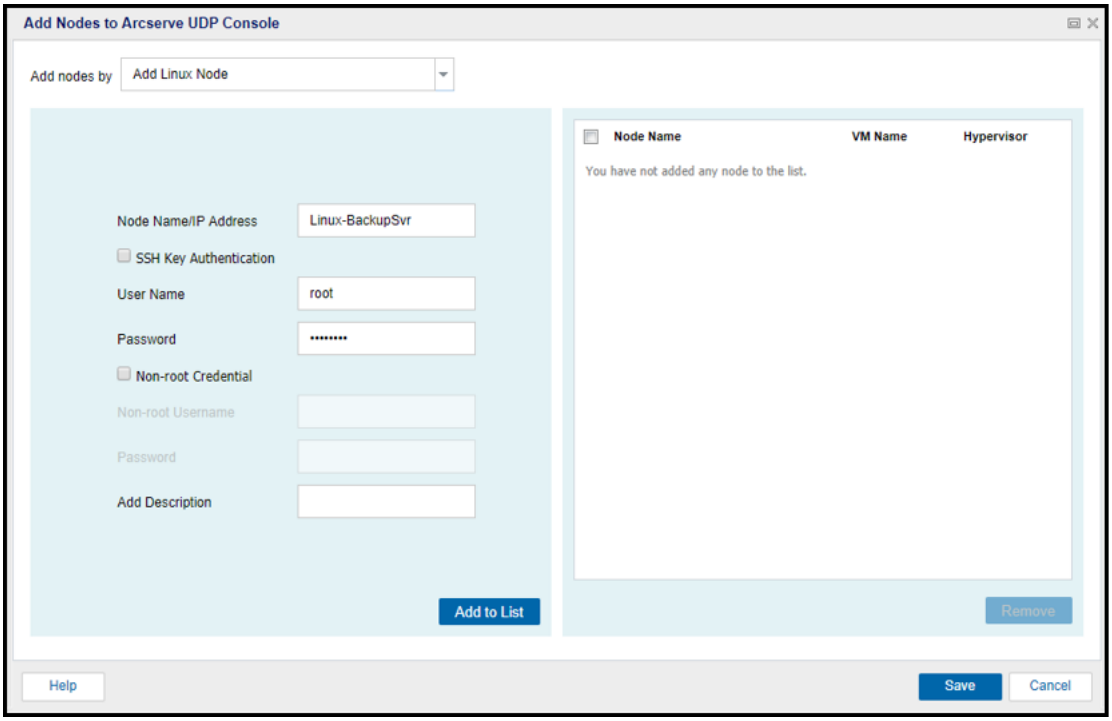
Create Plan to Backup the Linux Backup Server

In the Arcserve N-Series Appliance, you can configure the Linux Backup Server to backup.

Follow these steps:

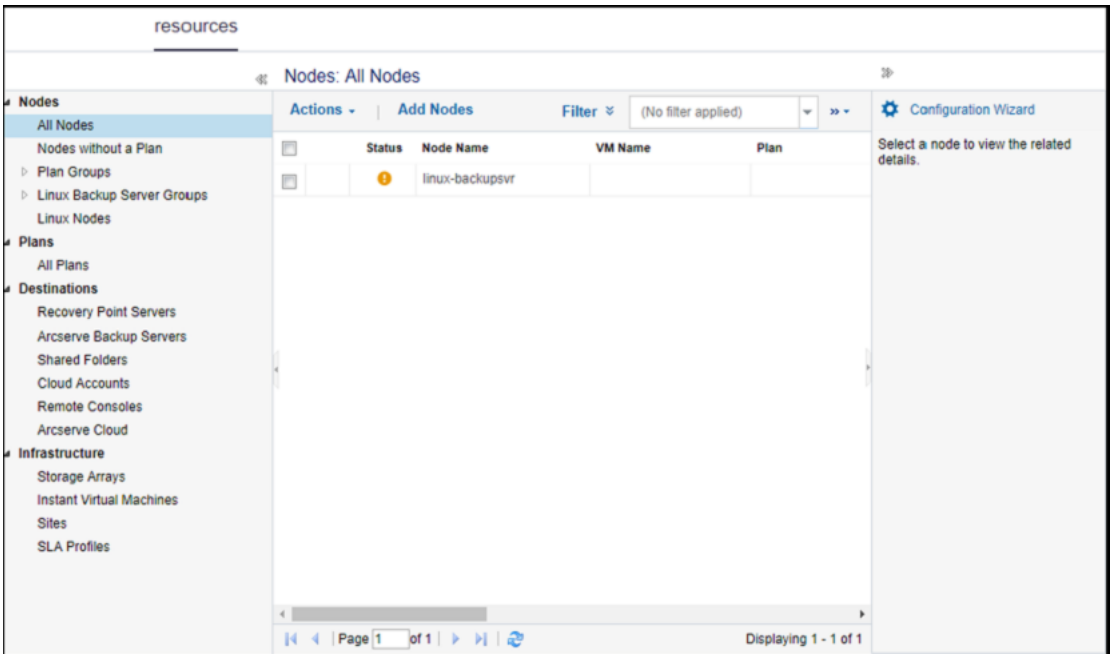
1. From Arcserve UDP Console, click the **resources** tab.
2. Click **All Nodes** in the right pane.
3. From the center pane, click **Add Nodes**.

   The **Add Nodes to Arcserve UDP Console** dialog opens.
4. From the **Add Nodes by** drop-down list, select *Add Linux Node*.
5. Provide the node credentials and click **Add to List**.



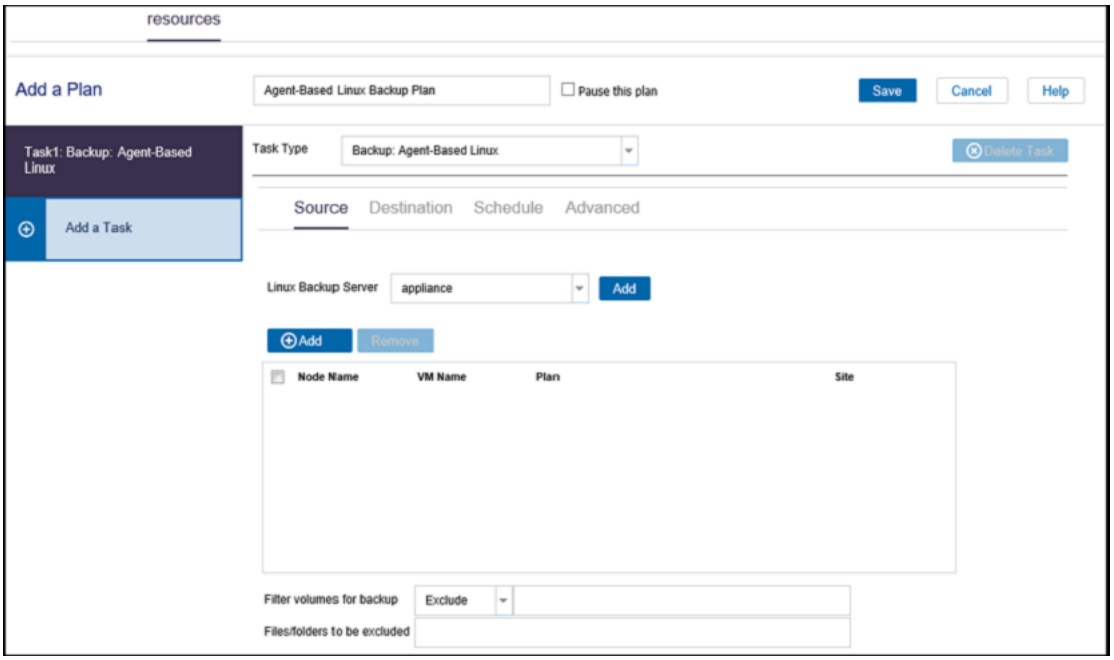
6. Click **Save**.

   The added Linux node is displayed in the **All Nodes** list.

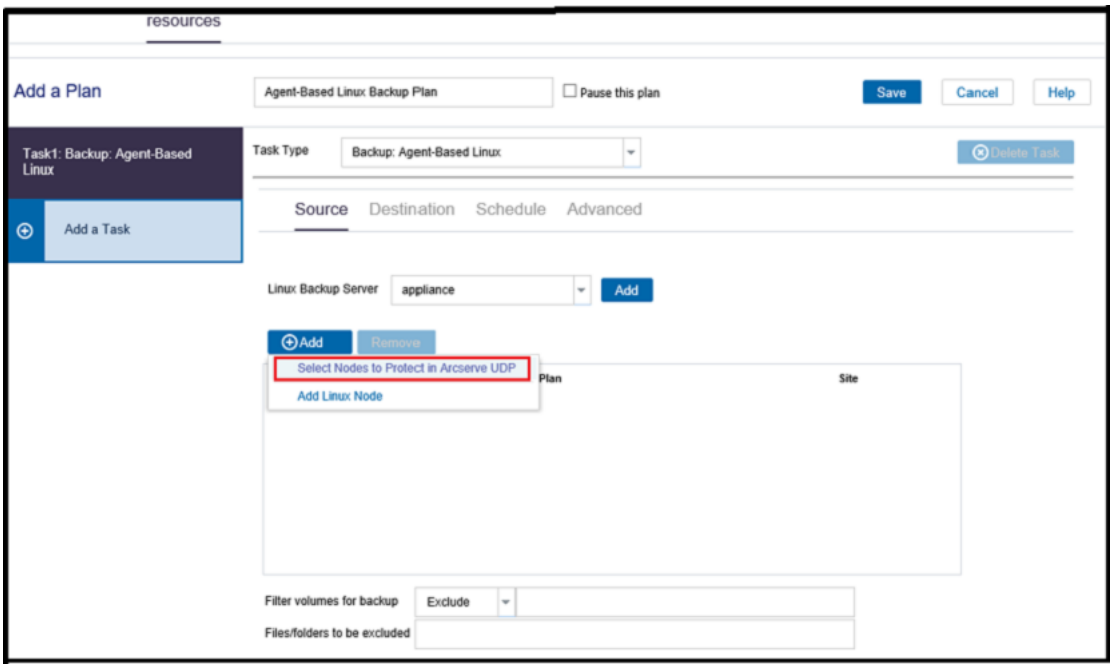


7. Navigate to **All Plans** and create an Agent-based Linux plan.

   The **Source** tab appears.

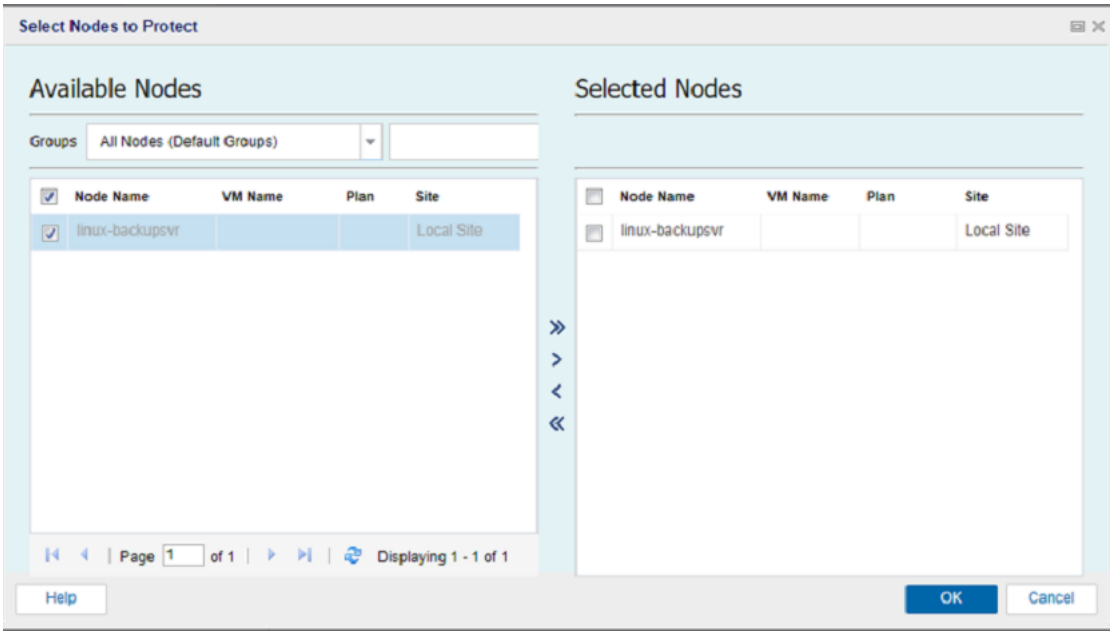


8. From the **Add** drop-down list, select *Select Nodes to Protect in Arcserve UDP*.



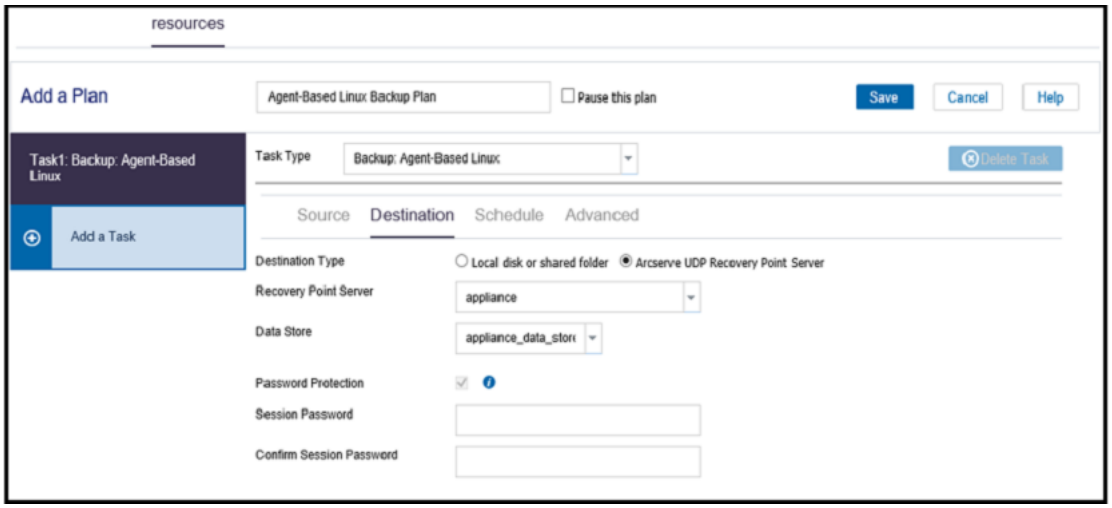
The **Select Nodes to Protect** dialog opens.

9. Protect the added Linux node and click **OK**.

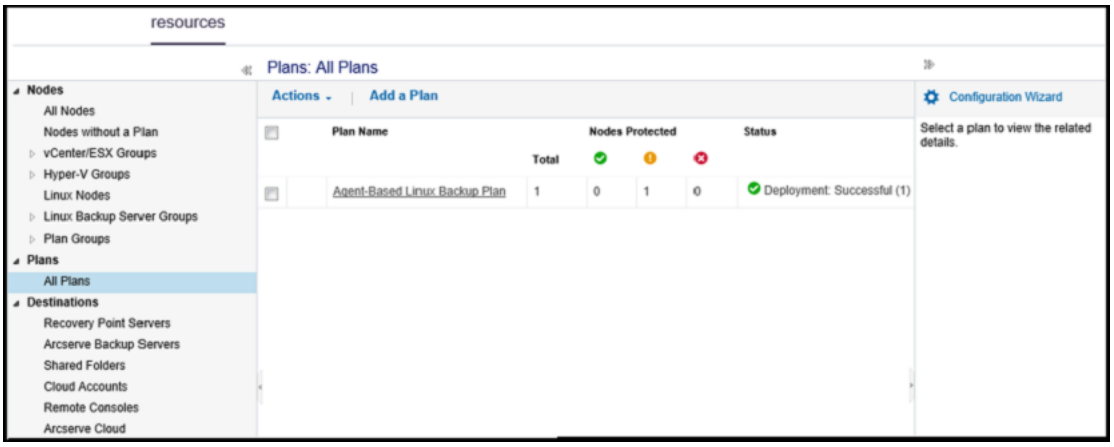


The **Destination** tab appears.

10. The default destination displayed is the data store created using Appliance wizard. Select Local disk or shared folder to backup the node if required.



11. After providing the settings related to plan, click **Save**.



You can perform backup for the added Linux Backup Server successfully.

Chapter 7: Performing Nutanix AOS Cluster Expansion

This section contains the following topics:

Review Prerequisites

Verify that you have completed the following prerequisite tasks before performing the cluster expansion:

- The version of cluster node installed must be same as the version of AOS and AHV.
- Check the Health dashboard and make sure the cluster is healthy before adding any nodes. Fix the issue if any health checks fail.
- Make sure the current add node operations are completed, if any.
- Check the Hardware dashboard to make sure all the nodes are in the correct metadata state. When the Metadata store is disabled on the node or a node is removed from the metadata store, click **Enable Metadata Store**.

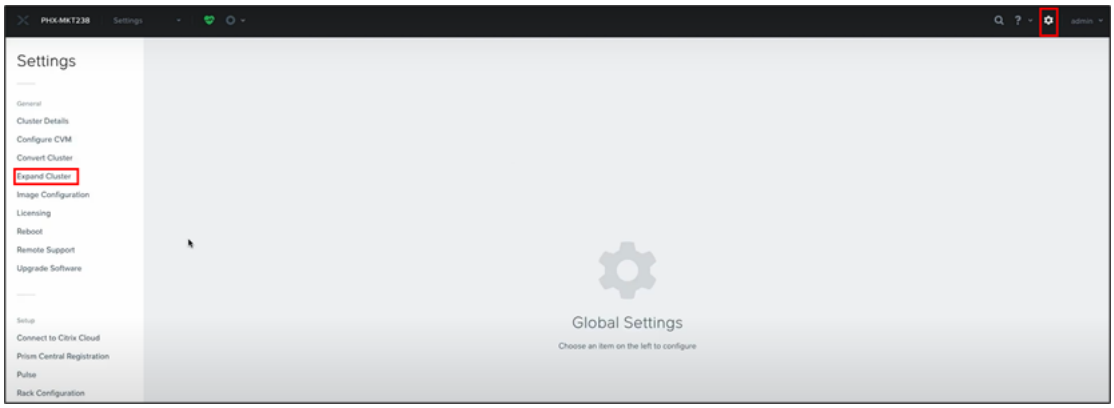
How to Perform Nutanix AOS Cluster Expansion

You can add new nodes to a cluster at any time after the nodes are installed and connected to the network on the same subnet as the cluster. The cluster expansion process verifies whether the version of AOS installed on existing and new nodes is same. If the AOS version does not match, the necessary upgrades are performed for all the nodes to have the same AOS version.

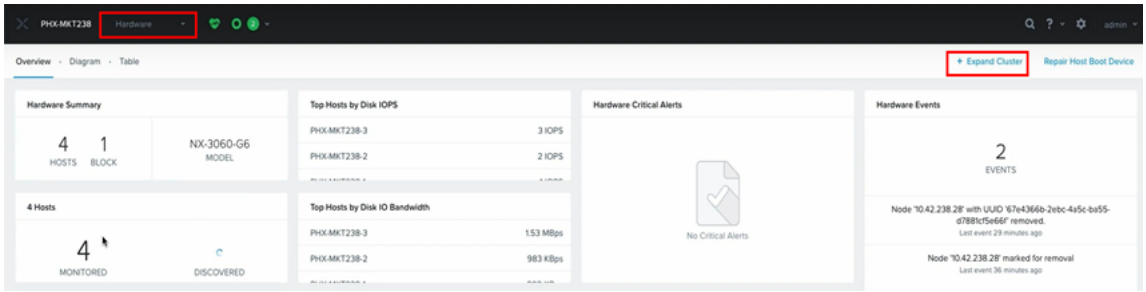
This section provides information about how to perform Nutanix AOS cluster expansion on Prism Element.

To add one or more nodes to an existing cluster, follow these steps:

1. Log into the Prism Element web console using admin credentials.
2. Do one of the following:
   - Click the settings icon on the top-right corner, and then select **Expand Cluster**.



   - Navigate to the drop-down list on the top-left corner, select **Hardware**, and then click the **+ Expand Cluster** button on the Hardware dashboard.

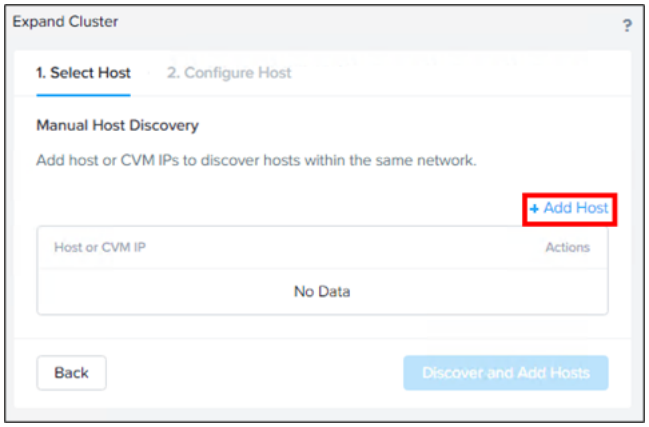


The Expand Cluster dialog appears and displays the list of nodes discovered on the *Select Host* page.

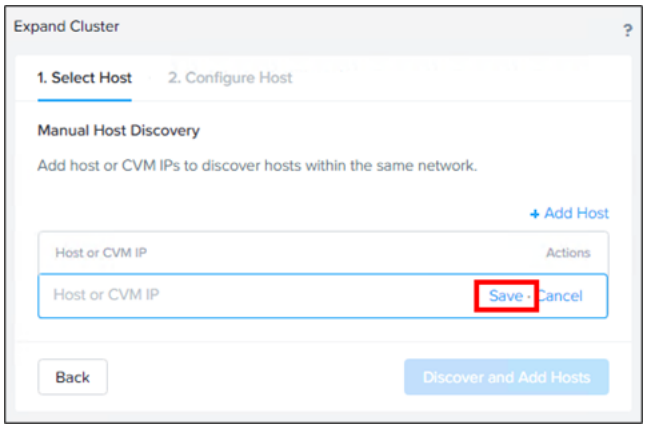
Note: To discover hosts manually within the same network, do the following:

a. On the Expand Cluster dialog, click **+ Discover Hosts Manually**.

b. On the Manual Host Discovery page, click **+ Add Host**.



c. Specify the host or Controller VM (CVM) IP address, and then click **Save.**



d. Click **Discover and Add Hosts**.

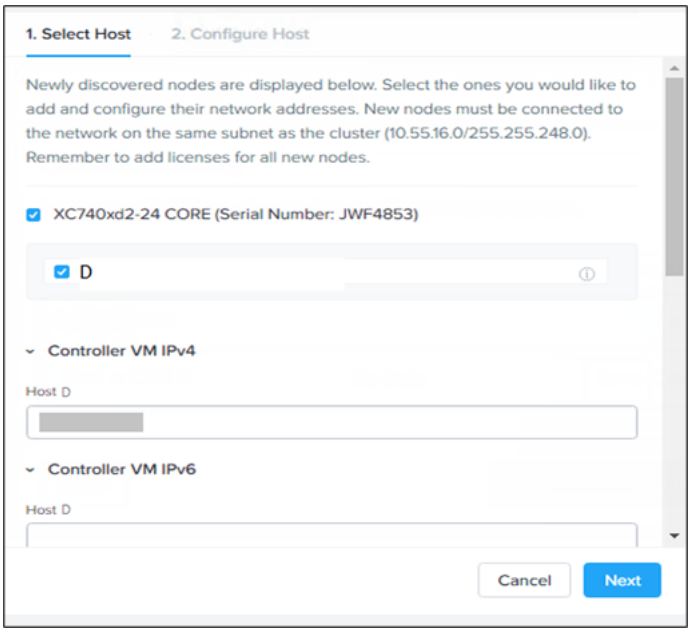
The node is discovered and added successfully.

3. On the Select Host screen, do the following:

a. Select the checkbox for each node (host) that you want to add to the cluster. If you do not want to add any node to the cluster, unselect the checkbox of the corresponding node.

b. For Controller VM IPv4, Hypervisor IPv4, and IPMI IPv4, verify whether the IP addresses assigned to all the hosts to be added are correct. If not, change the incorrect IP address as needed.

c. Click **Next**.



The Configure Host screen appears.

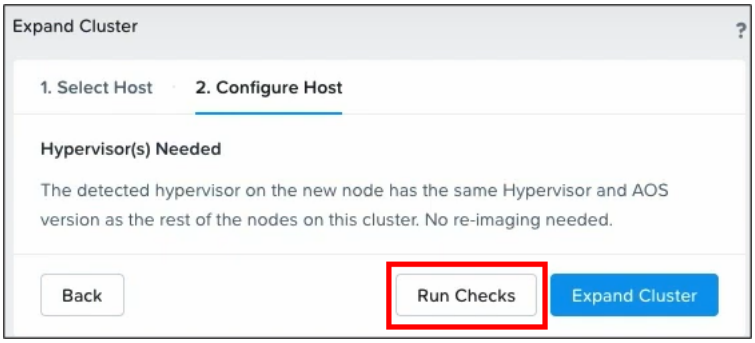
The software detects the hypervisor that is installed on the newly discovered node and checks whether the hypervisor version matches with the cluster.

Notes:

- If the hypervisor detected on a newly discovered node has the same hypervisor and AOS version as the remaining nodes on the cluster, no re-imaging is required.
- If the hypervisor does not match, you are prompted to browse for the hypervisor file on your local computer.

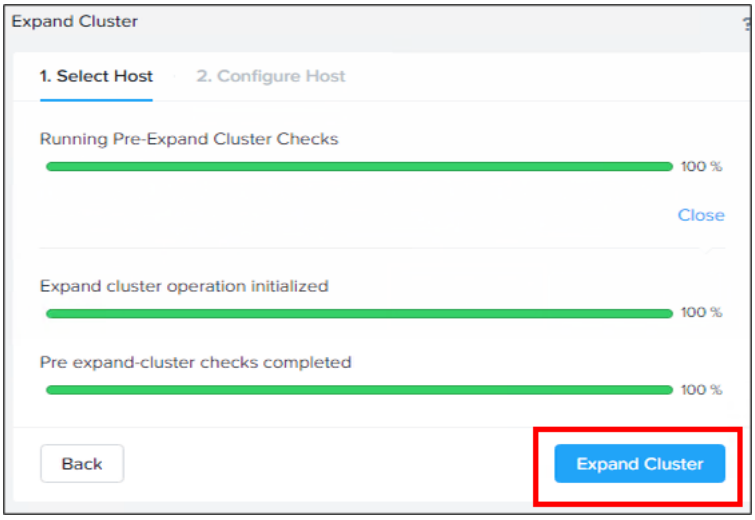
  After the file is uploaded, the node is imaged with the hypervisor required.

4. After providing the CVM, Hypervisor, and IPMI IPs, to check the compatibility of newly added node with the existing cluster, click **Run Checks**.



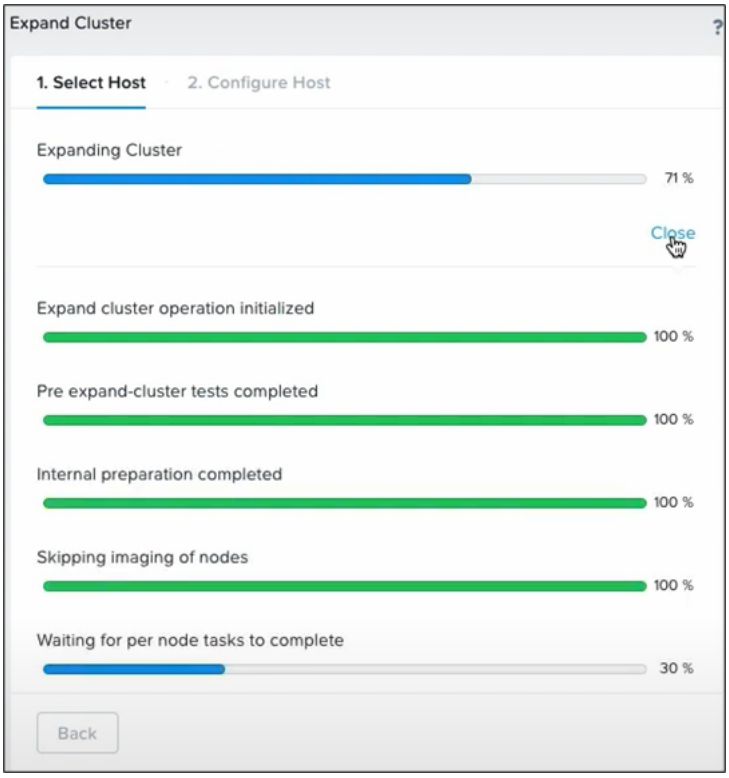
The pre-expand cluster checks begin, and displays the status of pre-expansion.

5. After the pre-expand cluster checks completed successfully, click **Expand Cluster**.



The Expand Cluster dialog closes and the add node process begins.

After the cluster expansion starts, a progress bar appears and displays the status of the expansion.



Notes:

- For more information about the progress of cluster expansion, click **open**.

- Red bar indicates an issue. For more information about the issue, hover the cursor over the red bar text.

6. To see the newly added node, navigate to drop-down list on the top-left corner, and then select **Hardware**.

The Hardware dashboard now displays the existing and newly added hosts on the cluster.

For more information about the hosts, click the **Table** tab.

Chapter 8: Understanding Safety Precautions

This section contains the following topics:

General Safety Precautions

You must adhere to the following general safety precautions to protect yourself and to protect the appliance from damage or malfunction:

- For EMI Class A Equipment (Business equipment), this equipment is registered for Electromagnetic Conformity Registration as business equipment (A) and not home equipment. Sellers or users are required to take caution in this regard.

  A급기기(업무용방송통신기자재)

  이기기는업무용(A급)으로전자파적합기기로서판매자또는사용자는이점을주의하시기바라며,가정외의지역에서사용하는것을목적으로합니다

  Note: This safety precaution only applies to South Korea. For more details, contact Arcserve Support at https://www.arcserve.com/support or call 0079885215375 (South Korea).

- Inspect the box in which the appliance was shipped and ensure that there are no visible signs of damage. If there is evidence of damage, please retain all packaging materials and contact Arcserve Support immediately at: https://www.arcserve.com/support.
- Decide on a suitable location for the rack unit that will hold the appliance. It should be situated in a clean, dust-free area that is well ventilated and free of clutter. Avoid areas where heat, electrical noise, and electromagnetic fields are generated.
- You will also need it placed near at least one grounded power outlet. Depending on the model, the appliance includes either one power supply or a redundant power supply and will then require two grounded outlets.
- The appliance is only for use in a restricted location.
  - Access can only be gained by service persons or by users who have been instructed about the reasons for the restrictions applied to the location and about any precautions that shall be taken; and
  - Access is through the use of a tool or lock and key, or other means of security, and is controlled by the authority responsible for the location.
- Place the appliance top cover and any components that are removed from the appliance on a table so that you do not accidentally step on the components.

- While working on the appliance, do not wear loose clothing such as neckties and unbuttoned shirt sleeves, which can come into contact with electrical circuits or be pulled into a cooling fan.
- Remove any jewelry or metal objects from your body, which are excellent metal conductors that can create short circuits and harm you if they come into contact with printed circuit boards (PCBs) or areas where power is present.
- After accessing the inside of the appliance, close the appliance and secure it to the rack unit with the retention screws after ensuring that all connections have been made.

Electrical Safety Precautions

You must adhere to the following electrical safety precautions to protect yourself and to protect the appliance from damage or malfunction:

- Be aware of the locations of the power on/off switch on the appliance as well as the room's emergency power-off switch, disconnection switch, or electrical outlet. If an electrical accident occurs, you can then quickly remove power from the appliance.
- Do not work alone when working with high-voltage components.
- Power should always be disconnected from the appliance when removing or installing main system components, such as the Serverboard, memory modules and the DVD-ROM and floppy drives (not necessary for hot swappable drives). When disconnecting power, you should first power down the appliance with the operating system and then unplug the power cords from all the power supply modules in the appliance.
- When working around exposed electrical circuits, another person who is familiar with the power-off controls should be nearby to switch off the power, if necessary.
- Use only one hand when working with powered-on electrical equipment. This is to avoid making a complete circuit, which will cause electrical shock. Use extreme caution when using metal tools, which can easily damage any electrical components or circuit boards they come into contact with.
- Do not use mats designed to decrease electrostatic discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.
- The power supply power cord must include a grounding plug and must be plugged into grounded electrical outlets.
- Serverboard Battery: **CAUTION** - There is a danger of explosion if the onboard battery is installed upside down, which will reverse its polarities This battery must be replaced only with the same or an equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer’s instructions.
- DVD-ROM laser: **CAUTION** - this Server may have come equipped with a DVD-ROM drive. To prevent direct exposure to the laser beam and hazardous radiation exposure, do not open the enclosure or use the unit in any unconventional way.

FCC Compliance

This appliance complies with part 15 of the FCC Rules. Operation is subject to the following conditions:

- This appliance may not cause harmful interference, and
- This appliance must accept any interference received, including interference that may cause undesired operation

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user is required to correct the interference at his own expense.

Electrostatic Discharge (ESD) Precautions

Electrostatic Discharge (ESD) is generated by two objects with different electrical charges coming into contact with each other. An electrical discharge is created to neutralize this difference, which can damage electronic components and printed circuit boards. Devices that are sensitive to ESD, such as Serverboards, motherboards, PCIe cards, drives, processors, and memory cards require special handling. Use the following precautions to help neutralize the difference of electrical charges coming into contact with each other, before contact is made, to protect your equipment from ESD:

- Use a rubber mat that has been specifically designed as an electrical insulator. Do not use a mat designed to decrease electrostatic discharge as protection from electrical shock.
- Use a grounded wrist strap designed to prevent static discharge.
- Use antistatic or electrostatic discharge (ESD) preventive clothing or gloves.
- Keep all components and printed circuit boards (PCBs) in their antistatic bags until ready for use.
- Touch a grounded metal object before removing the board from the antistatic bag.
- Do not let components or PCBs come into contact with your clothing, which may retain a charge even if you are wearing a wrist strap.
- Handle a board by its edges only. Do not touch its components, peripheral chips, memory modules, or contacts.
- When handling chips or modules, avoid touching their pins.
- Put the Serverboard and peripherals back into their antistatic bags when not in use.
- For grounding purposes, verify your appliance provides excellent conductivity between the power supply, the case, the mounting fasteners, and the Serverboard.

Chapter 9: Activating Sophos on the Arcserve N-Series Appliance

This section provides information about how to activate Sophos on the Arcserve N-Series Appliance manually.

Manually Installing Sophos Intercept X Advanced for Server on Arcserve N-Series Appliance

The integration of Sophos Intercept X Advanced for Server on Arcserve N-Series Appliance enables the following:

- Protect data and system backups from ransomware and other attacks
- Endpoint protection that combines signature-based and signatureless malware detection.
- Deep learning neural network
- Anti-exploit technology
- CyptoGuard anti-ransomware and WipeGuard technologies, and more to stop the widest range of endpoint threats

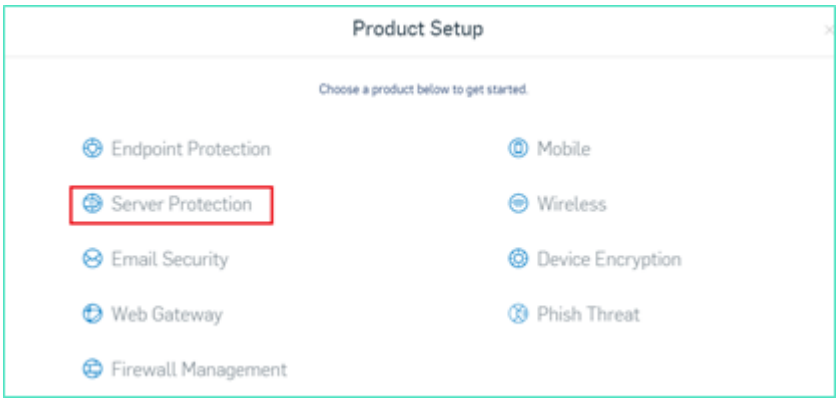
Note: If Arcserve Appliances were shipped to you on or after October 15, 2019, Sophos Intercept X is pre-installed. An email is sent to you as part of the delivery process and it contains the activation instructions. Otherwise, follow the instructions given below to manually install Sophos Intercept X.

Follow these steps:

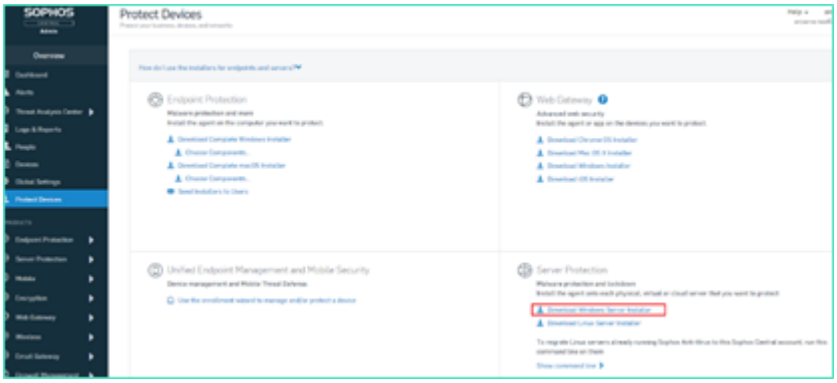
1. On the Arcserve Support Website, create an account.
2. To request for a free copy of Sophos Intercept X Advanced, provide all relevant details in the Sophos Request form and submit it to Arcserve Support. It is mandatory to share the details of Email ID and Order ID. You will receive an auto-generated email confirmation.

   After you confirm your email ID, Arcserve processes your request and creates an account on the Sophos Central and sends an email with instructions on how to create a password.
3. To create a password for your new account on Sophos Central, follow the instructions in the email.
4. Log into the Arcserve Appliances as an administrator or as a user with local administrative privileges.

   Note: For security reasons, do not join the appliances using the Active Directory Domain.
5. From your appliance, log into Sophos Central, and then follow step 3 and 4.
6. Open the Product Setup dialog, then select **Server Protection**.



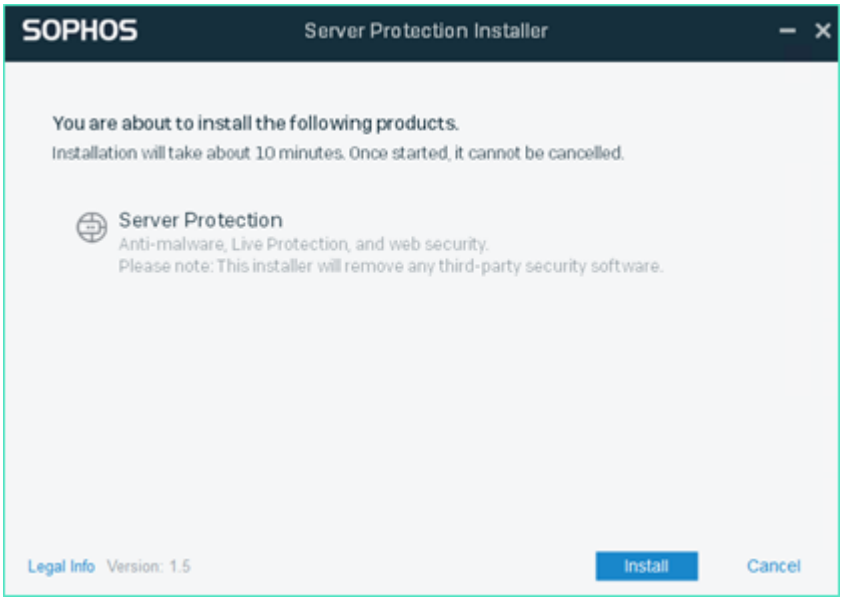
7. From the Server Protection section, click **Download Windows Server Installer**, and then save **SophosSetup.exe** installer to a folder on UDP.



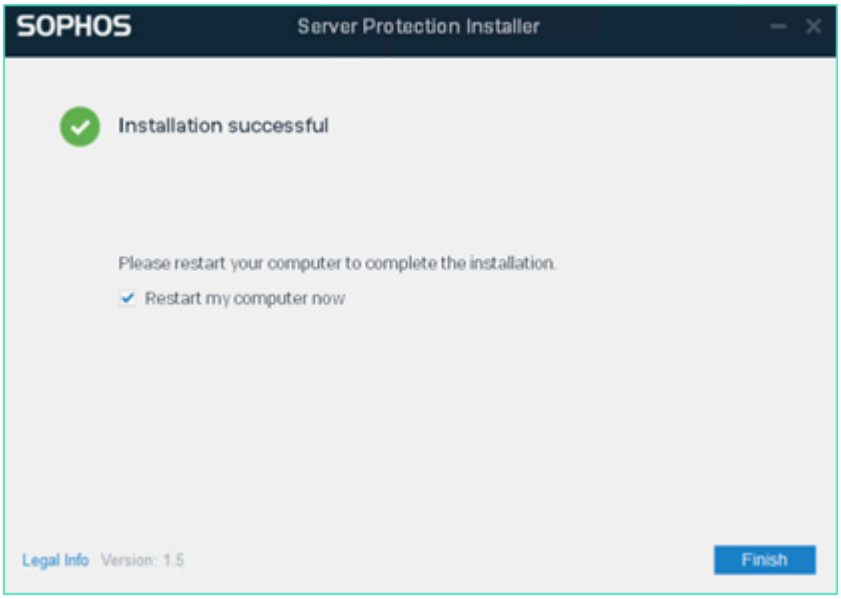
8. To start the installer, open the folder, and then double-click **SophosSetup.exe**.

Note: If there are any antivirus products on your appliance, it is recommended to uninstall before starting the installer.

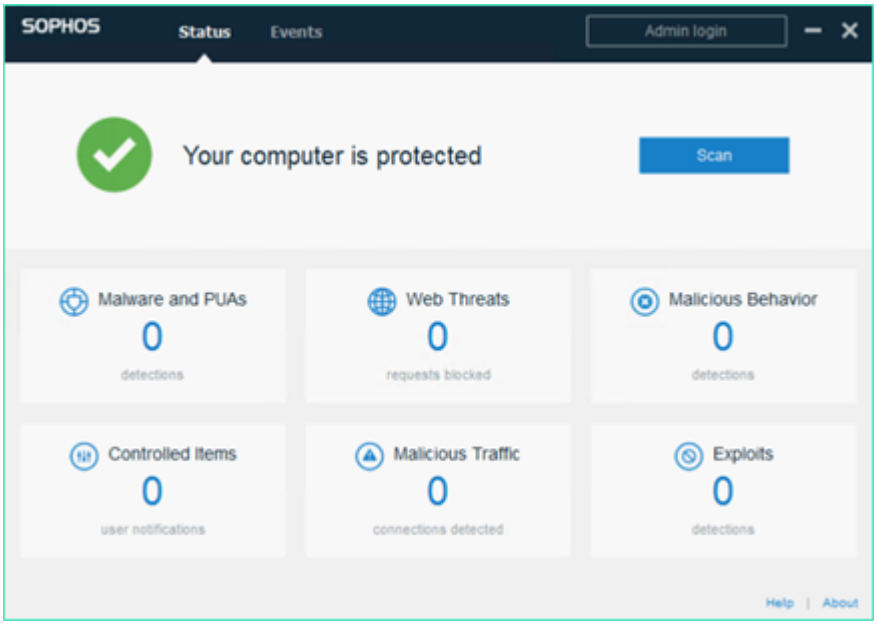
9. Click **Install**.



10. To restart your system immediately, click **Finish**. To restart later, uncheck the **Restart my computer now** option.



11. To view the protection status, open the **Sophos Intercept X** interface.



The status indicates that the Arcserve Appliance is secured from ransomware attacks, malware, web threats, and zero-day exploits.

12. To access Sophos Central, click **Admin Login**. It allows you to manage Sophos Intercept X Advanced Server, set alerts and policies, and so on.

Notes:

- It is mandatory to have Internet access in the appliance to install 'Sophos Intercept X Advanced' and any related updates. Sophos Intercept X Advanced is cloud based and there are no offline installers available.
- If you have already purchased another appliance previously and have a Sophos account through Arcserve, use the same account for all your Arcserve Appliances.
- If you already have a Sophos account through any other purchase, such as directly from Sophos, provide a different email address for a separate account on Sophos Central.
- If the Sophos installation fails for any reason, follow the on-screen or email instructions that are provided along with the error message.
- To receive the Sophos Intercept X Advanced for Server updates such as malware definition updates and version upgrades, you must have a valid and active maintenance for your Appliance.

For further assistance, please contact Arcserve Technical Support on phone (+1.844.765.7043) or online, or contact your local Arcserve support office.

Chapter 10: Troubleshooting

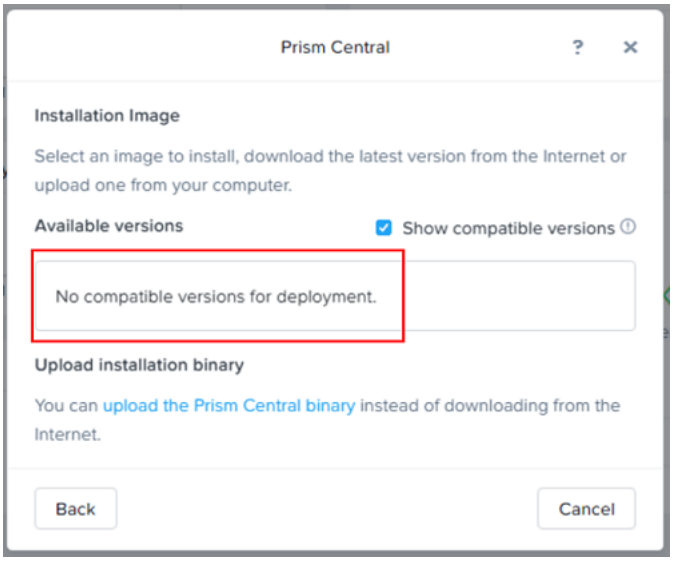
This section contains the following topics:

Unable to Check Prism Central Compatibility with AOS Version

Symptom

On the Prism Element home page, when you click **Register or create new** under Prism Central wizard, the Prism Central dialog appears and displays the following message under *Available versions* field:

No compatible versions for deployment.



Solution

As a workaround, do the following:

1. Check the Prism Central compatibility with AOS version using the following link:

   https://portal.nutanix.com/page/documents/compatibility-interoperability-matrix/interoperability

2. Download the compatible Prism Central binaries from the *portal.nutanix.-com* site.
3. Navigate to **Prism Central** wizard, click **Register or create new**, and then upload the downloaded .json and .tar files manually.

Unable to View Arcserve Home Dashboard in the Prism Element

Symptom

In the Prism Element, Arcserve Home dashboard displays login window and prompts you to enter the username and password.

Solution

The login window appears due to the connection timeout between the UDP Console VM and the Prism Element.

As a workaround, to view the Arcserve Home dashboard, enter the login credentials of UDP Console running in the Prism Element.

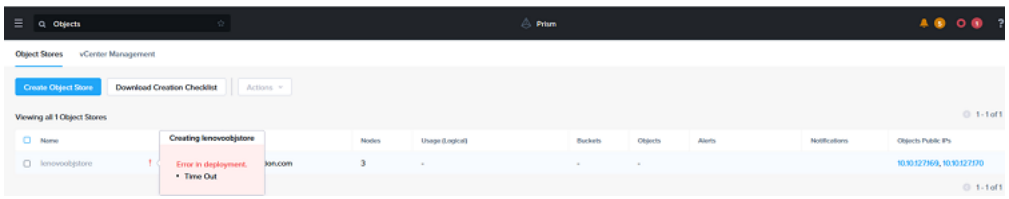
Nutanix Object Store Creation Fails Due to Time Out Error

Symptom

Nutanix object store creation fails, and the following error occurs:

Error in deployment.

Time Out



Solution

This error occurs due to the communication or network time-out between the Prism Element, Prism Central, and NTP servers.

As a workaround, do the following:

1. Log into the Prism Central web console.
2. Navigate to **Dashboard** > **Services** > **Objects**.
3. To delete any failed Object Store, select the check box as needed, go to the **Actions** drop-down list, and then click **Delete**.

   A confirmation message appears.
4. Click **Confirm** to delete.
5. After successfully deleting the failed Object Store, re-initiate the Object store creation. To create the Object Store, see Deploying the Nutanix Object Store.

The Object store is created successfully.

Nutanix Mine Deployment Fails Due to Improper User Permissions or Lack of Enough Resources

Nutanix Mine deployment fails and displays the following error:

Prism V2 post API call failed for: vms

Symptom

During the Nutanix Mine deployment process, the deployment fails and displays the following error:

Prism V2 post API call failed for: vms

Solution

This error occurs due to improper user permissions or lack of enough resources in the cluster to continue the deployment.

As a workaround, do the following:

1. Check whether the provided user has Cluster Admin role assigned in the Nutanix Prism Element.
2. Re-run the Mine deployment process with updated user credentials.
3. Check whether the Nutanix Prism Element cluster has enough resources to create the UDP Console, RPS and LBS VMs without any issues.

The Nutanix Mine is deployed successfully.

Arcserve Home Dashboard does not Display when the Network Switch or Cluster is Rebooted

Symptom:

When the network switch or cluster is rebooted, Arcserve Home dashboard does not display in the Prism Element.

Solution:

As a workaround, re-install the Arcserve Home dashboard in the Prism Element.

For more information about how to re-install Arcserve Home dashboard, see Maintenance Troubleshooting.

Unable to Access the UDP Management Console UI from Outside the UDP Console VM

Symptom

When you click the **Yes** option on the Network dialog populated for the first time after the deployment of UDP Console VM, the Windows automatically block previously opened UDP ports. As a result, the Windows firewall ports get blocked.

Solution

As a workaround, to access the UDP Management Console UI from outside the UDP Console VM, open the following UDP ports in firewall, which are required to perform backup and other jobs when you have a LAN environment:

- 8014
- 8015

For more information, see Communication Ports Used by Arcserve UDP.

Nutanix Mine Deployment Fails Due to UDP VM Status Error

Nutanix Mine deployment fails sometimes and displays the following error:

Unable to get UDP VM status.

Symptom

During the Nutanix Mine deployment process, the deployment fails sometimes and displays the following error:

Unable to get UDP VM status.

Solution

This error occurs due to an issue with the UDP Console windows installation, or IP address issue with DNS server.

As a workaround, do the following:

1. Check the UDP Console VM status in the cluster and see whether the deployment fails due to wrong product key or network communication issue. If an incorrect Windows product key was entered, provide the right product key during the subsequent Mine deployment process.
2. After checking the UDP console VM status, clean-up existing UDP Console and UDP LBS VMs in the Nutanix Cluster.
3. Re-run the Mine deployment process.

The Nutanix Mine is deployed successfully.

Nutanix Mine Deployment Fails Due To DNS Error

Nutanix Mine deployment fails sometimes and displays the following error:

Failed to proceed with the Installation, failed to resolve the DNS.

Symptom

During the Nutanix Mine deployment process, the deployment fails sometimes and displays the following error:

Failed to proceed with the Installation, failed to resolve the DNS.

Solution

This error occurs due to an improper communication with the local DNS server while connecting with UDP Console VM for executing remaining tasks.

As a workaround, do the following:

1. Log into the Mine Bootstrap VM using ssh with the following credentials:
   - Username: root
   - Password: enOP@618
2. Install the following package before running the nslookup command from terminal:

   yum install bind-utils
3. After the *bind-utils* package is installed successfully, to check the DNS server connectivity from Bootstrap VM, follow these steps:
   a. To identify the DNS server IP address that is being returned, run the following command on bootstrap VM:

      nslookup <DNS IP address>

      Note: If nslookup fails to return the DNS information / IP address, verify with IT team for the right DNS information to provide during the Mine deployment rerun process.
   b. Check whether the DNS server is reachable using the *nslookup* and ping commands.
   c. Check whether the right DNS server IP address is returned.
   d. Check the DNS suffix with *nslookup* result.
   e. Ping the UDP Console VM from bootstrap VM and check whether the UDP Console VM responds to ping request.

f. To check the network connectivity of UDP Console from bootstrap VM, run the following command:

ping udpconsole

Note: If ping request fails to resolve the udpconsole IP address, verify with IT team for right DNS server information to provide during the Mine deployment rerun process.

4. Based on the results of nslookup and tracert udpconsole commands, clean-up existing UDP Console and UDP LBS VMs in the Nutanix Cluster.
5. Re-run the Mine deployment process.

The Nutanix Mine is deployed successfully.

Chapter 11: Arcserve Appliance Return Policy

A valid RMA (Return Material Authorization) number is required to return a product to Arcserve. Contact the Arcserve Technical Support department to obtain an RMA number. Refer to arcserve.com/support to contact customer care. Support team can inform where to send the RMA data.

Returns are subject to a re-stocking fee of 10%. Exceptions are:

1. If an order was fulfilled incorrectly, Arcserve will accept RMA and provide full credit.
2. If a defective item is returned within 30 days, Arcserve will accept RMA and provide full credit.
3. If there are hardware technical issues that are unresolved by support after a reasonable period of time to resolve, Arcserve will accept RMA and provide a hardware swap for a unit of equivalent value.

Information needed for the RMA request:

- Product serial number (located on the back of the appliance)
- Arcserve Order Number
- Partner contact name
- Partner phone number
- Partner Email address
- Customer contact name (if available)
- Phone number (if available)
- Email address (if available)
- Description of problem and any troubleshooting already performed.
- Shipping service requested and shipping address.

The RMA number must be clearly marked on the outside of the packaging. All RMAs must be shipped using adequate packaging. All RMAs should be shipped using a reputable carrier that offers package tracking and insurance. Any shipping damage or lost RMAs is the responsibility of customer.