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.

© 2022 Arcserve, including its affiliates and subsidiaries. All rights reserved. Any third party trademarks or copyrights are the property of their respective owners.

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 .	1
Language Support	2
Product Documentation	3
Chapter 2: Introducing the Arcserve N-Series Appliance	5
Introduction	6
Arcserve Unified Data Protection	7
Arcserve Unified Data Protection Agent for Linux	8
Safety Precautions	9
What is Not Included in the Box of Arcserve N-Series Appliance	10
Model N-Series	10
Ports Used by the Appliance	12
Arcserve UDP	13
Components Installed on Microsoft Windows	14
Components Installed on Linux	19
Node Protected by UDP Linux Remotely	20
Appliance for Linux Support	21
Chapter 3: Installing the Arcserve N-Series Appliance	
Chapter 4: Deploying the Arcserve N-series Appliance	24
Chapter 4: Deploying the Arcserve N-series Appliance	24 26
Chapter 4: Deploying the Arcserve N-series Appliance Review Prerequisites How to Connect to Nodes	24 26 27
Chapter 4: Deploying the Arcserve N-series Appliance Review Prerequisites How to Connect to Nodes How to Form a Nutanix Cluster	24 26 27 28
Chapter 4: Deploying the Arcserve N-series Appliance Review Prerequisites How to Connect to Nodes How to Form a Nutanix Cluster How to Configure Cluster Details from Prism Element	24 26 27 28 37
Chapter 4: Deploying the Arcserve N-series Appliance Review Prerequisites How to Connect to Nodes How to Form a Nutanix Cluster How to Configure Cluster Details from Prism Element How to Create Network Switch for Cluster Formation	24 26 27 28 37 41
Chapter 4: Deploying the Arcserve N-series Appliance Review Prerequisites How to Connect to Nodes How to Form a Nutanix Cluster How to Configure Cluster Details from Prism Element How to Create Network Switch for Cluster Formation How to Create Network Switch for Object Store	24 26 27 28 37 41 44
Chapter 4: Deploying the Arcserve N-series Appliance Review Prerequisites How to Connect to Nodes How to Form a Nutanix Cluster How to Configure Cluster Details from Prism Element How to Create Network Switch for Cluster Formation How to Create Network Switch for Object Store How to Configure Nutanix Cluster Data Services IP Address	24 26 27 37 41 44 48
Chapter 4: Deploying the Arcserve N-series Appliance Review Prerequisites How to Connect to Nodes How to Form a Nutanix Cluster How to Configure Cluster Details from Prism Element How to Create Network Switch for Cluster Formation How to Create Network Switch for Object Store How to Configure Nutanix Cluster Data Services IP Address How to Deploy Prism Central VM for Cluster	24 26 27 37 41 41 48 50
Chapter 4: Deploying the Arcserve N-series Appliance Review Prerequisites How to Connect to Nodes How to Connect to Nodes How to Form a Nutanix Cluster How to Configure Cluster Details from Prism Element How to Create Network Switch for Cluster Formation How to Create Network Switch for Object Store How to Configure Nutanix Cluster Data Services IP Address How to Deploy Prism Central VM for Cluster How to Change the Default Password for Prism Central VM	24 26 27 28 37 41 44 48 50 55
Chapter 4: Deploying the Arcserve N-series Appliance Review Prerequisites How to Connect to Nodes How to Form a Nutanix Cluster How to Form a Nutanix Cluster How to Configure Cluster Details from Prism Element How to Create Network Switch for Cluster Formation How to Create Network Switch for Object Store How to Configure Nutanix Cluster Data Services IP Address How to Deploy Prism Central VM for Cluster How to Change the Default Password for Prism Central VM How to Register the Prism Central VM for Cluster	24 26 27 28 37 41 44 44 50 55 58
Chapter 4: Deploying the Arcserve N-series Appliance Review Prerequisites How to Connect to Nodes How to Form a Nutanix Cluster How to Form a Nutanix Cluster How to Configure Cluster Details from Prism Element How to Create Network Switch for Cluster Formation How to Create Network Switch for Object Store How to Configure Nutanix Cluster Data Services IP Address How to Deploy Prism Central VM for Cluster How to Change the Default Password for Prism Central VM How to Register the Prism Central VM for Cluster How to Update NTP Server in Prism Central	24 26 27 28 37 41 44 44 50 55 58 58 62
Chapter 4: Deploying the Arcserve N-series Appliance Review Prerequisites How to Connect to Nodes How to Connect to Nodes How to Form a Nutanix Cluster How to Configure Cluster Details from Prism Element How to Create Network Switch for Cluster Formation How to Create Network Switch for Object Store How to Configure Nutanix Cluster Data Services IP Address How to Configure Nutanix Cluster Data Services IP Address How to Change the Default Password for Prism Central VM How to Register the Prism Central VM for Cluster How to Update NTP Server in Prism Central How to Deploy Nutanix Object Store	24 26 27 28 37 41 44 44 50 55 58 62 63
Chapter 4: Deploying the Arcserve N-series Appliance Review Prerequisites How to Connect to Nodes How to Connect to Nodes How to Form a Nutanix Cluster How to Configure Cluster Details from Prism Element How to Create Network Switch for Cluster Formation How to Create Network Switch for Object Store How to Configure Nutanix Cluster Data Services IP Address How to Deploy Prism Central VM for Cluster How to Change the Default Password for Prism Central VM How to Register the Prism Central VM for Cluster How to Update NTP Server in Prism Central How to Deploy Nutanix Object Store Review the Prerequisites	24 26 27 28 37 41 44 44 50 55 58 58 62 63 64
Chapter 4: Deploying the Arcserve N-series Appliance Review Prerequisites How to Connect to Nodes How to Connect to Nodes How to Form a Nutanix Cluster How to Configure Cluster Details from Prism Element How to Create Network Switch for Cluster Formation How to Create Network Switch for Object Store How to Configure Nutanix Cluster Data Services IP Address How to Deploy Prism Central VM for Cluster How to Change the Default Password for Prism Central VM How to Register the Prism Central VM for Cluster How to Update NTP Server in Prism Central How to Deploy Nutanix Object Store Review the Prerequisites Deploying the Nutanix Object Store	24 26 27 28 37 41 44 48 50 55 58 58 62 63 64 65

How to Deploy Nutanix Mine	76
Review Prerequisites	77
Creating Bootstrap VM	78
Checking the DNS Server Reachability from Bootstrap VM	83
Deploying Arcserve UDP using Nutanix Mine Deployment Wizard	85
Accessing the Arcserve Home Dashboard and UDP Console	99
Maintenance Troubleshooting	101
Locating Mine Deployment Log Files	. 104
Chapter 5: Activating the N-Series Nutanix Cluster and Arcserve UDP License	.106
Chapter 6: Working with Arcserve N-Series Appliance	.108
Activate Arcserve Product on the Appliance	. 109
Create a Plan Using Arcserve N-Series Appliance Wizard	. 110
Create a Backup Plan for Linux Nodes	. 111
Create an On-Appliance Virtual Standby Plan	. 112
Create Plan to Backup the Linux Backup Server	. 113
Chapter 7: Performing Nutanix AOS Cluster Expansion	.117
Review Prerequisites	. 118
How to Perform Nutanix AOS Cluster Expansion	. 119
Chapter 8: Understanding Safety Precautions	125
General Safety Precautions	. 126
Electrical Safety Precautions	. 128
FCC Compliance	. 129
Electrostatic Discharge (ESD) Precautions	130
Chapter 9: Activating Sophos on the Arcserve N-Series Appli- ance	131
Manually Installing Sophos Intercept X Advanced for Server on Arcserve N-Series Appliance	. 132
Chapter 10: Troubleshooting	137
Unable to Check Prism Central Compatibility with AOS Version	. 138
Unable to View Arcserve Home Dashboard in the Prism Element	139
Nutanix Object Store Creation Fails Due to Time Out Error	140
Nutanix Mine Deployment Fails Due to Improper User Permissions or Lack of Enough Resources	. 141
Arcserve Home Dashboard does not Display when the Network Switch or Cluster i Rebooted	s . 142
Unable to Access the UDP Management Console UI from Outside the UDP Console VM	e 143
Nutanix Mine Deployment Fails Due to UDP VM Status Error	144

Nutanix Mine Deployment Fails Due To DNS Error	145
Chapter 11: Arcserve Appliance Return Policy	

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 <u>Intro-</u><u>duction</u>. Rest of the sections help you install and use Arcserve Appliance.

This section contains the following topics:

Language Support	2
Product Documentation	3

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 <u>Arcserve Documentation</u>.

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	6
Safety Precautions	
What is Not Included in the Box of Arcserve N-Series Appliance	
Model N-Series	
Ports Used by the Appliance	12

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 <u>Deployment</u> 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	. 7
Arcserve Unified Data Protection Agent for Linux	8

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 <u>Compatibility</u> <u>Matrix</u>.

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 <u>Arcserve UDP Solution Guide</u>.

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 preinstalled 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 <u>Safety Precautions</u> <u>Appendix</u>.

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				ed	
Hyperconvergence Platform	Nutanix AOS for AHV Included				
Cybersecurity Soft- ware	Sophos Intercept X Adv	anced fo	r Server I	ncluded	
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			6GT/s, 338-BVJX	
Cores per node		24			
Raw capacity per cluster	Raw capacity per 100 TB 189		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	Mellanox ConnectX-4 LX Dual Port 10/25GbE SFP28,			
node	rNDC 406-BBLG			
Processor per	Intel Xeon Silver 4214	R 2.4G, 12	C/24T, 9.	6GT/s,
node	16.5M Cache, Turbo, HT	(100W) DI	DR4-2400	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 #	Por- t Typ- e	lni- tiated by	Listening Process	Description
1433	ТСР	Remote Java	sqlsrvr.exe	Specifies the default com- munication port between the Arcserve UDP console and Microsoft SQL Server databases when they reside on dif- ferent com- puters. Note : You can modify the default com- munication port when installing SQL Server.
4090	тср	Arcserve UDP Agent	HATransServer.exe	Transfers data for Virtual Standby tasks in the proxy mode.
500- 0- 5060	ТСР	Arcserve UDP Server	GDDServer.exe	Reserved for Arcserve UDP RPS Global Deduplication Data Store Ser- vice (GDD). One Arcserve UDP GDD data store will use 3 free ports

I I I I I I I I I I I I I I I I I I I	5000. It
lis nee	ded
when	the data
store	with
GDD	s
enab	ed for
backu	ip or the
resto	re task is
used.	
Com-	
muni	cation
that I	ets the
Arcse	rve UDP
Arcserve Construction Foundation	ole and
6052 TCP Backup	rcserve
GDB Backu	ıp Global
Dash	board
Prima	ry
Serve	r syn-
chror	ize data.
Com-	
muni	cation
that I	ets the
Arcse	rve UDP
COLA TCD Arcserve CA.ARCserve.Com- Conse	ole and
Backup municationFoundation.WindowsService.exe the A	rcserve
Backu	ıp
Prima	ry
Serve	r syn-
chror	ize data.
To sh	ut down
Tomo	at that is
8006 used	by the
Arcse	rve UDP
conso	ole.
Speci	fies the
defau	lt
НТТР,	/HTTPS
Arcserve com-	
8014 TCP UDP Tomcat7.exe muni	cation
Console port l	between
remo	te man-
agem	ent con-
soles	and the

 Arcserve UDP Server. Specifies the defaut HTTP/HTTPS com- munication port between remote man- agement con- soles and the Arcserve UDP Agent. Note: You can modify the default com- munication port when you install the Arcserve UDP components. Specifies the default HTTP/HTTPS com- munication port when you install the Arcserve UDP consoles. Specifies the default HTTP/HTTPS com- munication port between the Arcserve UDP Server and Arcserve UDP Ser					
8014 TCP Arcserve 8014 TCP UDP 8014 TCP Arcserve 8014 TCP UDP 8014 TCP Server					Arcserve UDP
8014 TCP UDP Arcserve Base of the default of the					Server.
 8014 TCP 8014 TCP 4 Arcserve 8014 TCP 4 Arcserve 5 Arcserve 8014 TCP 801					Specifies the
 8014 TCP UDP Server Note: serve Note: Vou can modify the default com- munication port between Agent. Note: Vou can modify the default com- munication port when you install the Arcserve UDP components. Specifies the default HTTP/HTTPS Com- munication port between the Arcserve UDP Server and Arcserve UDP Server as the replication destination. Do not open ports 5000- 5060 which 					default
 k k k k k k k k k k k k k k k k k k k					HTTP/HTTPS
 8 1 A Former Part of the second second					com-
8014 TCP UDP Server httpd.exe Specifies the default shared port and the only or you use the Arcserve UDP components. 8014 TCP UDP httpd.exe Specifies the default shared port and the only or you use the Arcserve UDP components. 8014 TCP UDP httpd.exe Specifies the default shared port and the only or you use the Arcserve UDP components. 8014 TCP Server httpd.exe Specifies the default shared port and the only port and the only port you must open when you use the Arcserve UDP consoles. 8014 TCP Server httpd.exe Specifies the default shared port and the only port you must open when you use the Arcserve UDP consoles.					munication
8014 TCP UDP Arcserve Note: You can modify the default communication port when you install the Arcserve UDP components. 8014 TCP UDP httpd.exe Specifies the default HTTP/HTTPS communication port between the Arcserve UDP components. 8014 TCP UDP httpd.exe Specifies the default shared port and the only port you munication port and the arcserve UDP components. 8014 TCP Server httpd.exe Specifies the default shared port and the only port you must port you port you port you must port you port you must port you you port you must port you					port between
8014 TCP UDP Arcserve Note: N					remote man-
8014 TCP UDP Agent. 8014 TCP UDP httpd.exe 8014 TCP UDP httpd.exe 8014 TCP UDP httpd.exe 8014 TCP UDP httpd.exe 8014 TCP DDP td.exe 8014 TCP DDP td.exe					agement con-
 Arcserve UDP Agent. Note: You can modify the default com- munication port when you install the Arcserve UDP components. Specifies the default HTTP/HTTPS com- munication port between the Arcserve UDP Server and Arcserve UDP consoles. Specifies the default HTTP/HTTPS com- munication 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 and Arcserve UDP consoles. 					soles and the
Agent. Note: You can modify the default com- munication port when you install the Arcserve UDP components. Specifies the default HTTP/HTTPS com- munication port between the Arcserve UDP Server and Arcserve UDP Server and Arcserve UDP Server and Arcserve Arcserve UDP Server and Arcserve Arcserve Arcs					Arcserve UDP
 Note: You can modify the default communication port when you install the Arcserve UDP components. Specifies the default HTTP/HTTPS communication port between the Arcserve UDP Server and Arcserve UDP Server and Arcserve UDP components. 8014 TCP UDP httpd.exe Arcserve httpd.exe Arcserve UDP Server and Arcserve UDP Server between the Arcserve UDP Ser					Agent.
8014 TCP UDP Arcserve 8014 TCP UDP Server 8014 TCP UDP httpd.exe 8014 TCP UDP Server 8014 TCP UDP 8015 TCP 8014 TCP UDP 8015 TCP 8016 TCP 8016 TCP 8017 TCP					Note: You can
 8014 TCP 8014 TCP 9014 TCP<					modify the
8014 TCP Arcserve 8014 TCP Arcserve 8014 TCP Marcserve 900 Marcserve WDP Server 8014 TCP Marcserve 900 Marcserve WDP Server 900 Marcserve WDP Server 901 Marcserve WDP Server as 901 Marcserve WDP Server					default com-
8014 TCP Arcserve 8014 TCP UDP httpd.exe Specifies the default HTTP/HTTPS com- munication port between the Arcserve UDP Server and Arcserve Specifies the default munication 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 port and the only port you must open when you use the Arcserve UDP Server as the replication port s000- 5060 which					munication
 Normality of the second second					port when
Arcserve UDP components. Specifies the default HTTP/HTTPS com- munication 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 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					you install the
8014 TCP UDP httpd.exe Specifies the default HTTP/HTTPS com-munication port between the Arcserve UDP Server and Arcserve UDP consoles. 8014 TCP UDP httpd.exe *Specifies the only port you must open when you use the Arcserve UDP Server and the only port you must open when you use the Arcserve UDP Server as the replication. Do not open ports 5000-5060 which					Arcserve UDP
8014 TCP UDP httpd.exe 801					components.
 default HTTP/HTTPS com- munication 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 arcserve UDP Server 					Specifies the
8014 TCP <td></td> <td></td> <td></td> <td></td> <td>default</td>					default
8014 TCP LARCSERVE Arcserve 8014 TCP UDP httpd.exe 8014 TCP Httpd.exe Server 8014 TCP Httpd.exe Mutpd.exe 8014 TCP Httpd.exe Mutpd.exe 8014 TCP Httpd.exe Mutpd.exe 8014 TCP UDP Httpd.exe 8014 Httpd.exe UDP Mutpd.exe 8015 Httpd.exe UDP Mutpd.exe 8016					HTTP/HTTPS
 Munication 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 					com-
 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 					munication
8014TCPUDPHttpd.exeUDP consoles.8014TCPUDPhttpd.exe*Specifies the8014UDPhttpd.exedefault sharedServerport and theonly port youmust openwhen you usethe ArcserveUDP Server asthe ArcserveUDP Server asthe ont openports 5000-ports 5000-5060 which					port between
 8014 TCP UDP httpd.exe Server <l< td=""><td></td><td></td><td></td><td></td><td>the Arcserve</td></l<>					the Arcserve
8014TCPUDP Mttpd.exeArcserve UDP consoles.8014TCPUDP UDP Serverhttpd.exedefault 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					UDP Server
8014TCPUDP Mttpd.exeMttpd.exeSpecifies 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					and Arcserve
8014Arcserve*Specifies the default shared port and the only port you must open when you use the Arcserve UDP Server as the replication destination.8899989999899					UDP consoles.
8014TCPUDPhttpd.exedefault sharedServerServerport and the only port you must openonly port you must openV AAAAAV AAAAAV AAAAAV AAAAAV AAAAAV AAAAAV AAAAV AA <td< td=""><td></td><td></td><td>Arcserve</td><td></td><td>*Specifies the</td></td<>			Arcserve		*Specifies the
Server 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	8014	тср	UDP	httpd.exe	default shared
only port you must open when you use the Arcserve UDP Server as the replication destination. Do not open ports 5000- 5060 which			Server		port and the
must open when you use the Arcserve UDP Server as the replication destination. Do not open ports 5000- 5060 which					only port you
when you use the Arcserve UDP Server as the replication destination. Do not open ports 5000- 5060 which					must open
the Arcserve UDP Server as the replication destination. Do not open ports 5000- 5060 which					when you use
UDP Server as the replication destination. Do not open ports 5000- 5060 which					the Arcserve
the replication destination. Do not open ports 5000- 5060 which					UDP Server as
destination. Do not open ports 5000- 5060 which					the replication
Do not open ports 5000- 5060 which					destination.
ports 5000- 5060 which					Do not open
5060 which					ports 5000-
					5060 which

				are used by
				data stores
				that have
				global dedu-
				plication
				enabled.
				Note: You can
				modify the
				default com-
				munication
				port when
				you install the
				Arcserve UDP
				components.
				Specifies the
				default
				HTTP/HTTPS
				com-
				munication
				port between
				remote man-
				agement con-
				soles and the
				Arcserve UDP
				Server.
				Specifies the
				default
		Arcconico		HTTP/HTTPS
2015	тср		Tomcat7 ava	com-
0012	TCP	Concolo	Tomcat7.exe	munication
		CONSOLE		port between
				remote man-
				agement con-
				soles and the
				Arcserve UDP
				Agent.
				Note: You can
				modify the
				default com-
				munication
				port when
				you install the
				Arcserve UDP
				components.

				Reserved for
				Arcserve UDP
				Server Web
				Services to
				communicate
				with the Arc-
				serve UDP RPS
		A		Port Sharing
0010	TOD	Arcserve	T	Service on the
8016	ICP	UDP Common	Tomcat7.exe	same Server.
		Server		Note: The
				port cannot
				be cus-
				tomized and
				can be
				ignored for
				the firewall
				setting.
				To shutdown
				Tomcat that is
1800-			CA.ARCserve.CommunicationFoundation.	used by the
5			WindowsService.exe	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	тср	SSH ser- vice		Arcserve UDP Linux third party dependency. Spe- cifies 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 incom- ing 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 incom- ing communications. Note : The port number cannot be customized.
8014	тср	Arcserve UDP Linux	Java	Specifies the default HTTP/HTTPS com- munication ports between the remote con- soles and the Arcserve UDP agent for Linux. This port is required for both incoming and outgoing communications.
18005	ТСР	Arcserve UDP Linux	Java	Used by Tomcat, can be ignored for firewall set- tings.

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
				Arcserve UDP Linux 3rd party dependency. Specifies
22		SSH ser-		the default for the SSH service, however, you can
22		vice		change this port. This port is required for both incom-
				ing 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	Initiated	Listening	Description
#	Туре	by	Process	Description
				NAT port redirection, redirects 8017 on appliance
8017	тср			to the Linux backup server in order to backup other
				Linux node to Amazon S3.
0010	тср			NAT port redirection, redirects 8018 on appliance
0010	TCP			to the Linux Backup Server Agent port 8014.
0010	тср			NAT port redirection, redirects 8019 on appliance
8019	TCP			to the Linux Backup Server SSH port 22.
				NAT port redirection, redirects 8021 on appliance
8021	тср			to Linux backup server to backup other Linux node
				using 8021 port.
8036	тср			NAT port redirection, redirects 8036 on appliance
8030	TCF			to the Linux Backup Server port 8036.
				NAT port redirection, redirects 50000 on appliance
50000	тср			to Linux backup server in order to backup other
				Linux node to cloud using 50000 port.
				NAT port redirection, redirects 50001 on appliance
50001	тср			to Linux backup server in order to backup other
				Linux node to cloud using 50001 port.
				NAT port redirection, redirects 50002 on appliance
50002	тср			to Linux backup server in order to backup other
				Linux node to cloud using 50002 port.
				NAT port redirection, redirects 50003 on appliance
50003	тср			to Linux backup server in order to backup other
				Linux node to cloud using 50003 port.
				NAT port redirection, redirects 50004 on appliance
50004	ТСР			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 <u>Dell support website</u>.
- 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 <u>Connecting the Nodes</u>.

- 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.
- 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 <u>here</u>.
- 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	26
How to Connect to Nodes	27
How to Form a Nutanix Cluster	28
How to Configure Cluster Details from Prism Element	37

How to Create Network Switch for Cluster Formation	41
How to Create Network Switch for Object Store	
How to Configure Nutanix Cluster Data Services IP Address	
How to Deploy Prism Central VM for Cluster	
How to Change the Default Password for Prism Central VM	
How to Register the Prism Central VM for Cluster	
How to Update NTP Server in Prism Central	
How to Deploy Nutanix Object Store	63
How to Generate and Download Access Keys	
How to Deploy Nutanix Mine	76

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.

- 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.

X Nutanix Installer x +
← → C O localhost:8000/gui/index.html
X 1. Start 2. Nodes 3. Cluster 4. AOS 5. Hypervisor 6. IPMI
Welcome to Nutanix Installer.
1. If you have used install.nutanix.com, import the configuration file.
2. Select your hardware platform: Autodetect
 Connect this installer to each node's IPMI port (if possible) and at least one other port. Depending on hardware platform chosen, IPMI can refer to IDRAC, XCC, ILO, CIMC, IBMC, or "out-of-band management".
4. Do you want RDMA passthrough to the CVMs? 🔹 No 🔿 Yes
5. What type of LAGs will your production switch have? 🖲 None 🔿 Static O Dynamic (LACP)
6. To assign a VLAN to host/CVMs, enter the tag: Optional. 1 - 4094. Enser 0 (zero) to remove any existing tag.
7. Nutanix requires all hosts and CVMs of a cluster to have static IPs in the same subnet. Pick a subnet: Netmask of Every Host and CVM Gateway of Every Host and CVM
8. Pick a same or different subnet for the IPMIs as well, unless you want them to have no IPs. Netnesk of Every IPMI Gatewary of Every IPMI
9. Double-check this installer's networking setup.
Version 4.6

ŵ

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

X Nutanix Installer	+								
\leftrightarrow \rightarrow C \odot localhost:8000/	gui/index.html								
		2. Nodes	3. Cluster 4	AOS	5. Hypervisor 6. I	PMI			
	4 nodes were o	discovered u	ising IPv6 LAN b	roadcast.					Retry Troubleshoot
	Select the nordes	you want to	bandle and ent	er the IP/h	ostnames vou want t	them to have			Tools
	Jelect the house	you maint to	nonale, and end	er ute it /it	osciumes you work	areni to nave.			10015 🗸
	BLOCK SERIAL	NODE	NODE SERIAL	VLAN	IPMI MAC	IPMLIP	HOSTIP	CVMIP	HOSTNAME OF HOST
	JWF2H63 (XC740xd2-24 CORE)	□ A	JWF2H63	None	2C:EA:7F:50:26:2C				NTNX-JWF2H63-A
	JWF3853 (XC740xd2-24 CORE)	□ A	JWF3853	None	2C:EA:7F:50:24:0C				NTNX-JWF3853-A
	JWF3H63 (XC740xd2-24 CORE)	□ A	JWF3H63	None	2C:EA:7F:50:32:F5				NTNX-JWF3H63-A
	JWF4H63 (XC740xd2-24 CORE)	□ A	JWF4H63	None	2C:EA:7F:50:26:0C		_		NTNX-JWF4H63-A

	< Prev	
--	--------	--

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 <u>Nutanix documentation</u>.

- 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.

X 1. Start 2. Nodes 3	3. Cluster 4. AOS 5. Hypervisor 6. IPMI
	A cluster will be formed out of nodes selected on Page 2. Enter the cluster settings.
	Skip automatic cluster formation (e.g. you will use command-line)
	Enable CVM Network Segmentation
	Cluster Name
	walkthrough
	Alphabets, numbers, dots, hyphens and underscores are allowed.
	Timezone of Every CVM
	(UTC+00:00) Africa/Abidjan 🗸
	Applies to host too if Hyper-V or XenServer. Nutanix concluded AHV and ESX don't support host timezone.
	The UTC offset numbers in the dropdown do not account for daylight saving. The numbers are only meant to
	help with visual navigation within the dropdown. Only the location name, not the offset number, of the
	timezone will be sent to the cluster formation process.
	Cluster Redundancy Factor
	RF2 v
	1-node clusters do RF2 mirroring inside the single node. RF3 mirroring isn't supported.
	2-node clusters are RF4 — RF2 within each node × RF2 across the nodes. So select RF2 here, not RF3.
	3~ node clusters don't do any mirroring inside any node. Also, H+4 and above are not supported.
	Cluster Virtual IP (Optional)
	1818 Birder Pate
	Must be in the CVM subnet. This IP will always point to an online CVM, even in case of a node failure.
	NTP Servers of Every CVM (Optional)
	0.us.pool.ntp.org, 1.us.pool.ntp.org, 2.us.pool.ntp.org, 3.us.pool.ntp.org
	Comma-separated list of IPs or domains. Applies to host too if AHV or Xenserver.
	For ESX, Nutanix concluded it is best to configure NTP servers in vCenter.
	For Hyper-V, Nutanix concluded it is best to configure NTP servers in Active Directory.
	DNS Servers of Every CVM and Host (Optional)
	10101121201
< Prev	Reset • Progress Page • Foundation 5.11 Platforms 2.9

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

 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.

Nutanix requires that all CVMs of a cluster run the same version of an operating system called AOS. Your nodes already run the same AOS version, so <u>we will skip AOS instellation</u>, unless you want it.

View existing AOS version of each node...

BLOCK	NODE	EXISTING AOS
JWF2H63 (XC740xd2-24 CORE)	А	5.20
JWF3853 (XC740xd2-24 CORE)	А	5.20
JWF3H63 (XC740xd2-24 CORE)	А	5.20
JWF4H63 (XC740xd2-24 CORE)	А	5.20

< Prev	Version 4.6	N

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.

1. Start 2. Nodes 3. Cluster	4. AOS 5. Hypervi	sor	6. IPMI				
Nutanix require Your nodes aire View existing hy	s that all nodes of a cluste ady run the same hypervi genvisor of each node, o	r, exce sor, so	pt the AHV storage nodes, n we will skip hypervisor inst storage nodes	in the same hy III. unless you v	pervisor. vant it.		
	BLOCK	NODE	EXISTING HYPERASOR	STORAGE			
	JWF2H63 (xc740xd2-24 CORE)	A	AHV el7nutanix.20190916.142				
	JWF3H63 (XC740x52-24 CORE)	۸	AHV el7nutanix.20190916.142				
	JWF4H63 (XC740H52-24 CORE)	A	AHV el7nutanix.20190916.342				
	JWF3853 (XC740xd2-24 CORE)	A	AHV el7nutanix.20190916.142				
						Activate Windows	
K Prev		Reset	Version 4.6			Next >	

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.

🔀 1. Start 2. Nod	les 3. Cluster 4. AOS 5. H	lypervisor 6. IPMI		
	This page is not applicable in Only applicable when, on the Node	your case. No action is needed. Cli s page, you select at least one node adde	ick Start below to proceed, d by the "Add Nodes Manually" tool.	
	Enter the existing IPMI credentials	. Passwords won't be stored anywhe	ere, for security. Tools 🛩	
	NODE	USERNAME	PASSWORD	
		Not Needed ①	Not Needed ①	
		Not Needed ①	Not Needed ①	
		" Not Needed ①	Not Needed ①	
		Not Needed ①	Not Needed ①	

Prev Version 4.6 Start

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:

Installation i	n progress 🖉	Abort this installation	1	
Node Progress				
IPM IP	HOSTIP	CVMIP	PROGRESS	LOG
			All operations completed successfully	Log
			All operations completed successfully	Log
			All operations completed successfully	Log
			All operations completed successfully	Log
Cluster Formati	on Progress Wi	l start after all node	es are done.	
	CLUSTER NAME		PROGRESS	LOG
EPLABMineC2			Copying hypervisor iso to all nodes for future use	Log

Review Configuration + Version 4.6

Qź

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.

× Nutanix Installer ×	+				
← → C (① localhost:8000/gui/	index.html				Q
	Installation finished.				
	Node Progress			Download Log Bundle	
	IPM IP HOST IP	CVMIP	PROGRESS	105	
			All operations completed successfully	Log	
			All operations completed successfully	Log	
			All operations completed successfully	Log	
			All operations completed successfully	Log	
	Cluster Formation Progress	Will start after all nod	es are done.		
	CLUSTER NAM	IE	PROGRESS	LOG	
	EPLA8MineC2		Your cluster is ready! Click here to access it.	Log	

Reset • Review Configuration • Version 4.6

Note: If the cluster formation fails, download the logs and contact <u>Arcserve</u> <u>Support</u>.

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

	PRISM		
admin			
		0	
	Having issues logging in?		

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.

	PRISM
	Create a new password for the cluster admin.
	admin
1	
	••••••
	······
	Note: When you change the admin user password, update any applications and scripts using the admin user credentials for authentication. Nutanix recommends that you create a user assigned with the admin role instead of using the admin user for authentication. The Prism Web Console Guide describes authentication and roles.

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.



On the Pulse will be enabled screen, click Continue.
 Note: Nutanix does not recommend that you disable Pulse.
 The Prism Element dashboard opens.



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**.

EPLABMineC2 H	iome 👻 😻 🐥	00~						Q.? ∽ \$‡ admi
Hypervisor Summary	Prism Central	Cluster-wide Controller IOP	5 0 IOPS	Health			Critical Alerts	
AHV VERSION NUTANIX 20201105.2030	Not registered to Prism Central Register or create new	00.00 AM	02:00 AM 03:00 AM	CRITICAL				
Storage Summary	Contraction Logical -	Cluster-wide Controller IO I	B/W 0 KBps	Services	•1 •0	••		
35128 TiB Total Space	View Details	100 MBps		Disks	• 0 • 0	• 80	No Cri	tical Alerts
		01:00 AM	02:00 AM 03:00 AM	VMs	• 0 • 0	• 4		
VM Summary		Cluster-wide Controller Late	ency 💿 0 ms	Data Resiliency Status			Warning Alerts	
4 vM(S)	Availability Best Effort On 4 Off 0 suspend 0 Paused 0	1 ms 01:00 AM	02:00 AM 03:00 AM	ОК			3 WARNING 3 minutes ago	Power supply 2 is Down on block JWF3853(cluster: EPLA8MineC2) Power supply 2 is Down on block JWF4H50(cluster: Tot LEAK_c02)
Hardware Summary		Cluster CPU Usage	Cluster Memory Usa	Data resilient as per o	onfiguration		Info Alerts	Events
,		Control of a storige						
4 4	XC740xd2-24 CORE	6.44%	22.89%	Failure Domain ①		Node	No Info Alerts	10
HOSTS BLOCKS	maddala	OF 211.2 GHz	OF 752.88 GiB	Fault Tolerance ③		1		EVENTS Last event 2 minutes ago

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

EPLABMineC2 Sett	tings 👻 🤓 🐥 💽 🔿 🕢 🗸	٩
Settings	Network Configuration	
	Networks Internal Interfaces Virtual Switch	
Reboot	·	
Remote Support		
Upgrade Software	No networks have been configured.	
	Create Network	
Section .		
Connect to Citrix Cloud		
Prism Central Registration		
Pulse		
Rack Configuration		
Network		
HTTP Proxy		
Name Servers		
Network Configuration		
Network Switch		
NTP Servers		
PINWIN		
Security		
Cluster Lockdown		

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.

EPLABMineC2 Sett	tings 🗸 💝 🙏 🗿 🔿 🕦 🗸
Settings	Create Network
Reboot	Nituoit Name
Remote Support	AHVNetwork
Upgrade Software	Virtual Switch
	vs0
Setup	
Connect to Citrix Cloud	0
Prism Central Registration	Enable IP address management
Pulse	This gives AHV control of IP address assignments within the network.
Rack Configuration	
Network	
HTTP Proxy	
Name Servers	
Network Configuration	
Network Switch	
NTP Servers	
SNMP	
Security	
Cluster Lockdown	•

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.

× BLABMING2 Set	nes 🔄 🗢 🔶 🔍 🕈			9 1
Settings	Network Configuration	 Received operation to create Network Artic Network 	\	
	Networks Internal Interfaces Vir	tual Switch		
Rebot				
Remote Support				
Upgrate Software	BE Return Name	What laden	VLAND	
	Art/ Network	- Dev	0	
Selar				
Connect to Olirix Doud				
Prism Central Registration				
Pube				
Reck Configuration				
Network				
HTTP Prory				
Name Servers				
Network Configuration				
Network Switch				
NTP Servers				
52MP				

- 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).

Create Network	
Network Name	
Object-Switch	
Virtual Switch	
vs0	
O di najv	
0	
Enable IP address management	
This gives AHV control of IP address assignments within the network.	
Network IP Address / Prefix Length	
Gateway IP Address	

- 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.

Configure Domain Settings
Domain Name Servers (Comma Separated)
Donain Search (Comma Separated)
Domain Name
TFTP Server Name
Boot File Name

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

Address Pools (?)	
+ Create Pool	
Start Address	End Address

- 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.

Ad	Id IP Pool	
	Start Address	
	End Address	
		Cance
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 how is not selected, the DHCP server IP address is automatically gon	
	erated.	

☑ Override DHCP server ⊙	
DHCP Server IP Address	

Can

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.

EPLABMineC2	ome 🗸 🤝 🐥	O 🛈 ×					٩
Hypervisor Summary	Prism Central	Cluster-wide Controller IOI	PS 0 IOPS	Health		Critical Alerts	
AHV VERSION NUTANIX 20201105.2030	Not registered to Prism Central Register or create new	00 IOPS 01:00 AM	02:00 AM 03:00 AM	CRITICAL			
Storage Summary	Contraction Logical -	Cluster-wide Controller IO	B/W 0 KBps	Services • 1	• 0 • 0		\sim
351.28 TiB Total Space	View Details	100 MBps		Disks • 0	• 0 • 80	No Cr	itical Alert
		01:00 AM	02:00 AM 03:00 AM	VMs • 0	• 0 • 4		
VM Summary		Cluster-wide Controller Lat	tency 🔿 0 ms	Data Resiliency Status		Warning Alerts	
4 VM(S)	Availability Best Effort On 4 Off 0 e Suspend 0 Paused 0	1ms 01:00 AM	02:00 AM 03:00 AM	ОК		3 WARNING 3 minutes ago	Power block . EPLAB Power block .
Hardware Summary		Cluster CPU Usage	Cluster Memory Usa	Data resilient as per configur	ation	Info Alerts	Ev
4 4	XC740xd2-24 CORE	6.44%	22.89%	Failure Domain ①	Node	No Info Alerts	
HOSTS BLOCKS	er ren al la la	OF 211.2 GHz	OF 752.88 GiB	Fault Tolerance ③	1		L

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.

	Cluster Details ?	×
Cluster Name		
EPLABMineC2		
FQDN		
Virtual IP		
		ן ך
Virtual IPv6		
		ר
ISCSI Data Services IP		
		ן ך
Retain Deleted VM	Иs	
VMs when deleted will be	e retained in the Recycle Bin for 1d after which	
the used space is purged	1	
Cluster Encryption State		
Not encrypted		

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**.

Prism Central	?	:
Select between an existing connection or deploying a new Pris	m Cer	ntra
I want to deploy a new Prism Central instance		
I don't have Prism Central or want to deploy a new one		
Deploy		
I already have a Prism Central instance deployed		
Nutanix recommends connecting this cluster to it		
Connect		
	Clos	se

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

Prism Central	? x
Installation Image Select an image to install, download the latest version upload one from your computer.	n from the Internet or
Available versions Show of pc.2022.1	Download
pc.2021.3.0.1	Download
pc.2021.3	Download
Upload installation binary You can upload the Prism Central binary instead of do Internet.	ownloading from the
Back	Cancel

- 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.

Scale Out	Single VM
Prism Central Cluster	Prism Central
Capacity: Supports 5k to 25k	Capacity: Supports 2.5k to 12.5k
VMs	VMs
Added resiliency: RF2	Default resiliency
Minimum memory required: 78	Minimum memory required: 26
GB	GB

- 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.

M Name
Prism Central

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.

elect the size of your Prism Cer	ntral VM.		
-			
Size	vCPUs	Memory (GB)	Storage (GiB)
SMALL - (UP TO 2,500 VMs)	6	26	500
 LARGE - (UP TO 12,500 VMs) 	10	44	2500

- 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.

Network Config	
AHV Network	+ Create Network
AHV-Network	~
IP Address	
Subnet Mask	
Default Gateway	
DNS Address(Es) - Comma Separated	Optional
Back	Close Deploy

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

	PRISM		
admin			
		Θ	
	Having issues logging in?		

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.

	PRISM
	Create a new password for the cluster admin.
	admin
1	
. AN	••••••
X	
	Note: When you change the admin user password, update any applications and scripts using the admin user credentials for authentication. Nutanix recommends that you create a user assigned with the admin role instead of using the admin user for authentication. The Prism Web Console Guide describes authentication and roles.

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.

Pulse will be er	nabled
Pulse continuously monitors cluster health and pe	riodically sends machine data
to Nutanix's cloud based analytics engine. It auton	natically takes action when a
problem has occurred, or is about to occur. Learn	more.
Nutanix strongly recommends not disabling this fe	ature to improve your support
experience in the event of a failure or critical syste	m issue.
If you disable Pulse, Nutanix will not be able to pro	pactively reach out to you in
the event of failures, and your issue resolution tim	e may increase significantly.
Disable Pulse (not recommended)	Continue
By enabling Pulse, you elect and authorize Nutanix to elec data, including system alerts via e-mail, in accordance with in EULA.	tronically collect Pulse diagnostic the terms and conditions set forth

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.

EPLABMineC2	ome 🔹 🧇 🐥	o 💿 🗸				
Hypervisor Summary	Prism Central	Cluster-wide Controller IOP	PS 0 IOPS	Health		Critical Alerts
AHV VERSION NUTANIX 20201105.2030	Not registered to Prism Central Register or create new	01:00 AM	02:00 AM 03:00 AM	CRITICAL		
Storage Summary	O Logical v	Cluster-wide Controller IO	B/W OKBps	Services	•1 •0 •0	1
351.28 TiB Total Space	View Details	100 MBps		Disks	• 0 • 0 • 80	, i
		01:00 AM	02:00 AM 03:00 AM	VMs	• 0 • 0 • 4	
VM Summary		Cluster-wide Controller Lat	ency 💿 0 ms	Data Resiliency Status		Warning Alerts
4 vm(s)	Availability Best Effort On 4 Off 0 = Suspend 0 • Paused 0	1ms 0t.00 AM	02:00 AM 03:00 AM	ОК		3 WARNING 3 minutes ago
Hardware Summary		Cluster CPU Usage	Cluster Memory Usa	Data resilient as per cor	nfiguration	Info Alerts
4 4	XC740xd2-24 CORE	6.44%	22.89%	Failure Domain ①	Nod	e No Info Alerts
HOSTS BLOCKS	MODEL	OF 211.2 GHz	OF 752.88 GiB	Fault Tolerance ②		1

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

ettings	
up	
nnect to Citrix Cloud	
sm Central Registration	
se	Prism Central ?
k Configuration	Select between an existing connection or deploying a new Prism Central
-	I want to deploy a new Prism Central instance
r and Roles	I don't have Prism Central or want to deploy a new one
hentication	
al User Management	Deploy
e Mapping	
	I already have a Prism Central instance deployed
ieral	Nutanix recommends connecting this cluster to it
ster Details	Connect
figure CVM	
nvert Cluster	
and Cluster	Close
as Configuration	

Central Registration.

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

Prism Central	?	×
Select between an existing connection or deploying a new Prism	n Cen	tral
I want to deploy a new Prism Central instance I don't have Prism Central or want to deploy a new one		
Deploy		
I already have a Prism Central instance deployed		
Nutanix recommends connecting this cluster to it		
Connect		
	Clos	e

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

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

	Prism Central	? >
Once the registration n Read-Only mode or Central.	is complete, several mana n Prism Element but fully a	gement features will be 3 ccessible on Prism
Feature/Service	Prism Element	Prism Central
Cluster	~	~
Unregistration	By scripts only	By scripts only
Self-Service	×	~
Portal		

- 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.

Connect to an exist	ng Prism Central instance	
Please fill in the info	rmation needed to establish a connecti	on
Prism Central IP/FQDN		
Port		Option
9440		
Username		
admin		
Password		

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**.

EPLABMineC2 Home	• 🗢 🔺 🖸 💀 🗿 •					Q ? ~ Ø admin
Hypervisor Summary Prism Cen	tral Cluster-wide Contr	oller IOPS 71 IOPS	Health		Critical Alerts	
AHV CONTAINS 20201105-2030	417 JOPS 5.23.35 02:00 AM	03:00 AM 04:00 AM	CRITICAL			
Storage Summary O	Logical ~ Cluster-wide Contr	oller IO B/W 637 KBps	Services • 1 • 0	• •		
351.32 TIB Total Space	View Details 51.08 M8ps		Hosts • 0 • 4	• •	No Critic	al Alerts
	02:00 AM	03:00 AM 04:00 AM	Disks • 0 • 0	• 80		
VM Summary	Cluster-wide Contr	oller Latency O 2.16 ms	Data Resiliency Status		Warning Alerts	
5 VM(S) Availability On • Off • Suspend • Paused	Best Effort 5 0 0 0 02:00 AM	01:00 AM 04:00 AM	OK		1 WARNING 50 minutes ago	License Feature Violation
Hardware Summary	Iuster CPU Usage	Cluster Memory Usa	Data resilient as per configuration		Info Alerts	Events
4 4 XC740xd2 HOSTS BLOCKS MO	2-24 CORE 9.11% OFEL OFE 0F271.2 GHz	26.35% OF 752.88 GB	Failure Domain ① Fault Tolerance ①	Node 1	No Info Alerts	17 EVENTS Last event 37 minutes ago

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.

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	64
Deploying the Nutanix Object Store	. 65

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.

E Q Deshboard		👌 Prism		🔺 🖸 O 😰 📍 🗘 admin ~
Dashboard	Main Dashboard Ø Manage Dashboards		Reset Dashboard	1 + Add Widgets Data Density :
Virtual Infrastructure	Alerts Last 24 hours a	Cluster Quick Access	Cluster Storage	Cluster Latency Last Hour :
Network & Security -		Click on any line to open a Prism X Element instance in a new tab.	Cluster Used st., Data *	Cluster Latency *
Hardware -	3	EPLA8MneC2		
Activity · · · · · · · · · · · · · · · · · · ·	1			
Administration -	0 0245 AMDERS AMD245 PMDERS PM			
Celm 2	🖸 Critical 🖸 Warning 🖺 Info			
Files 🛶 🗠	Cluster Memory Usage Last Hour I	Cluster CPU Usage Last Hour I	Controller IOPS Last Hour #	Cluster Runway
Foundation Central	Cluster Usage *	Cluster Usage *	Custor KOPS *	EPLABMin CPU -
Objects 🗠				
Prism Central Settings				
Lock Nevigation Bar				

3. Click Enable.

≡	Objects		A Prism	
		Enable Objects to start creating obj creat	ect stores. Before enabling, make sure that any cluster on which you p e object stores is running AOS 5.11.2 or higher.	alan to
			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.

⊇ Q. Objects	☆ 💍 Prism	A ()
	Welcome to Objects!	
	Prerequisites 2 Create Object Store	
	A list that has all the prerequisites that you'll need to create an Object Store	
	Download Creation Checklist	
	vCenter Registration (for ESXi Users)	
	< Back Next	

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

≅ Q Objects		A Prism	A 3 0 9
Object Stores vCent	er Management		
Create Object Store	Actions ~		
There are no Object Stor	es available.		
		No data found	
7. On the Create Object Stores: Pre-Requisites dialog, click **Continue** if you have met the given prerequisites.

perore creating an	Object Store, make sure that ye	our environment meet the
ollowing prerequisi store on.	ites, depending on which clust	er you deploy your object
AHV Cluster		•
ESXi Cluster		۲

- 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.

Create Object Store	
Object Store Details	< Show
Object Store Name	
Objstore	
Domain 🛛	Public Network
arcserve.com	
Cluster EPLABMineC2 ÷	Load Balancer 1
Worker Nodes	Storano Notwork
- 3 +	Storage network
Learn More	
	Worker Node 1 Worker Node 2 Worker Node 3
Back Next	
	Load Balancer (each) Worker Node (each)
	4 GiB 2 vCPUS 32 GiB 10 vCPUS

- 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.

⊟ Q Objects	🔄 👌 Prism	4 0	0	?	🌣 ad	min Y
Create Object Store						×
Storage Network					Sho Summ	w ary
Storage Network DND-Object-Switch 192.168.100.0/2 +						
It is recommended that the CVM network be used for internal communication between the various VMs / nodes in the Object Store.	Public Network					
Object Store Storage Network static IPs (2 👔	Load Balancer 1					
Use comma separate IPs Object Store will use 5 additional IPs for the nodes / VMs connected to the storage network, as shown in the diagram.	Storage Network					
Back Next	Worker Node 1 Worker Node 2 Worker Node 3					

- 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.

Create Object Store		×
Public Network		< Show Summary
Public Network		
Public Network static IPs	Public Network	
Use comma separate IPs or enter a range of IPs	Load Balancer 1 Load Balancer 2	
Back Save & Continue		
	Storage Network	
	Worker Node 1 Worker Node 2 Worker Node 3	

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

Create Object Store	×
System Requirements Validation All checks need to pass for object store creation.	Show Summary
Validation Complete Done Click to download the pre-deployment checks report Load Balancer 1	
Storage network to PE DNS Storage network to PE TCP 3205	
Storage network to first object store TCP 5553	
Storage network DHCP pool Pisn Bernet Prisn Bernet Prisn Bernet DNS NTP	Click to continue with the
PC to storage network TCP 2379 Clock to complete the	object store department
Save for late	Create Object Store

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 **Down-load 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.

E Q. Objec	5			👌 Prism					0 🚥	? 🌣	admin Ƴ
Object Stores	Access Keys VCenter	Management									
Create Object	Store Actions ~									View	by :
Viewing all 1 Obje	ct Stores								3 1-10	of1 💿 20	rows *
□ Name	Version	Domain	Nodes	Usage (Logical)	Buckets	Objects	Alerts	Notifications	Objects Public IP	5	
Object-St	ore1 3.1.1	arcserve.com	3	797.09 KiB / 100 TiB	1	53	0	Disabled			
									3 1-1	of 1 💿 20	rows *

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

⊟ Q Obje	cts		🖉 Prism	A 🖸	0 🚥	?\$	
Object Stores	Access Keys	vCenter Management					
			No one has access, yet				
			Generate secret and access key pairs for people so they can access all object	stores.			
			+ Add People Configure Directories IAM Replication Setting	s			

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.

	1 Add People	e 2 Generate an	nd Download Keys	
Ger	nerate Keys for These	People		
0	Search for people in a	a directory service		
0	Add people not in a d	lirectory service		
	People			+Add
	Email Address	Name(Optional)	Action	
			Delete	

- 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.

Add People	×
1 Add People 2 Generate and Download Keys	
You've selected one person to generate keys and grant access.	
K Back Generate Ke	eys

The access keys are generated successfully.

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

	Add People	>
1 Add People	Generate and Download Keys	
ts up! If you close the set of th	he popup or browser before downloadinger have access to the keys.	ng
uccessfully generat	ted 1 person's keys. Download Keys	
	1 Add People ds up! If you close t eys, you will no lor uccessfully genera	Add People Generate and Download Keys sup! If you close the popup or browser before downloadi eys, you will no longer have access to the keys. uccessfully generated 1 person's 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.

Object Stores Access Keys vCenter Management			
Add People Configure Directories IAM Replication Setting	ngs		
Viewing 1 out of 1 total people			3 1-10
Name :	Usemane 1	Access Key	
		rYaw7m7_7lqehuhdrSlUqiqq4tdBkmqx	

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	77
Creating Bootstrap VM	78
Checking the DNS Server Reachability from Bootstrap VM	83
Deploying Arcserve UDP using Nutanix Mine Deployment Wizard	85
Accessing the Arcserve Home Dashboard and UDP Console	
Maintenance Troubleshooting	
Locating Mine Deployment Log Files	

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 <u>here</u>.

 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 <u>Installation</u> guide.

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

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**.

Name Annotation Image Type DISK V Storage Container buckets-ctr-b2b83073-3cbf-4184-75ec-25533924b37a V Image Source From URL Upload a file Choose File No file chosen	ate Image		
Annotation mage Type DISK	Name		
Annotation mage Type DISK			
mage Type DISK ~ Storage Container buckets-ctr-b2b83073-3cbf-4184-75ec-25533924b37a ~ mage Source From URL Upload a file ① Choose File No file chosen	Annotation		
mage Type DISK DISK			
DISK	mage Type		
Storage Container buckets-ctr-b2b83073-3cbf-4184-75ec-25533924b37a mage Source From URL Upload a file Choose File No file chosen	DISK		*
buckets-ctr-b2b83073-3cbf-4184-75ec-25533924b37a • mage Source • From URL • O Upload a file (*) • Choose File No file chosen	itorage Container		
From URL O Upload a file Choose File No file chosen	buckets-ctr-b2b83073-3cbf-4184-75ec-255339	924b37a	*
From URL Upload a file ① Choose File No file chosen	mage Source		
D Upload a file @ Choose File No file chosen	From URL		
	Upload a file Thoose File No file chose	en	
Cancel Save	4 Pack	Cancel	Sauce

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.

Name	
BootstrapVM	
Description	
Optional	
Timezone	
(UTC) UTC	

- 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).

Compute Details	
vCPU(s)	
2	
Number Of Cores Per vCPU	
2	
Memory (1)	
8	GIB

- 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.

Add Disk		?	×
Туре			
DISK			*
Operation			
Clone from Image Service			*
Bus Type			
IDE			•
Image 🕐			
Mine-			-
Size (GiB) ⑦			
30			
Please note that changing the size of an image is not al	lowed.		
Index			
Next Available			*
	Cancel	Ad chy	Id

d. For Boot Configuration, retain defaults.

oot Configuration	
Legacy BIOS	
Set Boot Priority	
Default Boot Order (CD-ROM, Disk, Network)	-

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

ethorn Aus	press (rec)
	You haven't added any NICs yet.
	+ 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.

					UEFI (1)
k	Add New Disk	+ /			isks
			Parameters	Address	Туре
×	/ · x	BUS=ide	EMPTY=true;	ide.0	CD- ROM
×	2 · X	8US=ide	SIZE=30GiB;	ide.1	DISK
С	Add New NIC	+		oters (NIC)	etwork Ada
		MAC	PRIVATE	VIRTUAL	VLAN ID / VPC
	/ 8	1	ā.	vs0	0 nutantxswl tch0

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 <u>Checking the DNS</u> <u>Server Reachability from Bootstrap VM</u>.

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.

🗙 walkthrough VM	♥ ▲ ◎ ・ 0	-										Q ?	- ¢ ∣ admin -
Overview - Table												+ Create VI	Network Config
VM									O Inclus	se Controller VMa - 🔘 9 Vi	Vis (filtered from 13)	Ø v - Searc	h in table 🔍 🔍
* VM None	Host	I ^a Addresses	Cares	Memory Capacity	Storage	CPU Usage	Memory Usage	Controller Rood IOPS	Controller Write IDPS	Controller10 Bandwidth	Controller Avg IO Latency	Beckup and R.,	Flash Made
* Bootstrage ^{by}	ntra-b17ad47ddbc1- b/AHV	101012-000	4	8 GIB	16.77 GIB / 40 GIB	012%	11,94%	۰	0	1KBps	1,64 ms	Yes	No
objstore fe4eba-default-0	ntra-b17ad47ddbe1- a/AHV		10	32.648	17.6 GIB / 80 GIB	7.83%	20.66%	0	63	404 KBps	0.62 ms	Yes	No
objstore-fe4eba-default-1	ntrix-b17ad47ddbc1- d/AHV	101012770	10	32 GIB	15.39 GIB / 80 GIB	4.47%	18.32%	٥	42	%7KBps	113 ms	Yes	No
cbjstore-fe4eba-default-2	ntna-b17ad47ddbo1- c/AHV	101012-00	10	32 G48	17.26 GB / B0 GB	6.09%	22.56%	٥	19	H8 KBps	0.53 ms	Yes	No
* objstore fe4eba tvjqtkiwc envoy-0	ntra-b17ad47ddbe1- d/AHV		2	4 G/8	3.09 GiB / 80 GiB	2.22%	22.43%	0	20	193 KBps	0.54 ms	Yes	No
objstore-fe4eba-tivjq5kiwc-envoy-1	ntrix-b17ad47ddbe1- c/AHV	10101277	2	4 G/B	3.07 GIB / 80 GIB	2/3%	23.26%	0	34	316 KBps	0.55 ms	Yes	No
Prism Central	ntra-b17ad47ddbo1- b/AHV	101010-011	6	26 Gi8	28.85 Gi8 / 641,44 Gi8	17,94%	68.58%	٥	64	523 KBps	2.08 ms	Yes	No
* udpconsole	ntra-b17ad47ddbe5- a/AHV	1010101108	48	128 G/B	27.07 GIB / 250 GIB	0.24%	8.67%	0	,	11 KBps	075 ms	Yes	No
* udplbs	ntra-b17ad47ddbe1- d/AHV	101012-000	4	808	8.29 GIB / 15.01 GIB	0.06%	17.57%	٥	0	0 KBps	0.7 ms	Yes	No
-													
Summary > BootstrapVM							M	anage Guest Tools	Launch Console	Power Off Actions Take	Snapshot Migrate	Clone / L	Ipdate × Delete
VM DETAILS	VM Performa	ance	Virtual Disks		VM NICs		VM Snapsho	6	VM Tasks	I/O Mi	review	Core	iole

- 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.
- 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.

End User License Agreement (EULA)	Nutanix Cluster Informatio	n
 Nutanix Cluster Information 	Specify required information for c	onnecting to the Nutanix cluster
Available Nutanix Servers	Prism Element IP	Port Number
Windows ISO Upload	Enter Ip Address	9440
Network Settings	Usemame	
Nutanix Object Storage	Enter Username	
Arcserve UDP Console & RPS Settings	Password	
Review Configuration Settings	Enter Password	
Installation		
Installation Status		
	Previous	

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**.

9	End User License Agreement (EULA)	Available Nutanix Review Nutanix Mine w	Servers ith Arcserve Cluster Info	rmation	
	Available Nutanix Servers	Node Name		IP Address	Model Name
0	Windows ISO Upload	NTNX-JWF4853-A-CVM		10.55.16.72	XC740xd2-24 0
0	Network Settings	NTNX-JWF2R53-A-CVM	l.	10.55.16.70	XC740xd2-24 0
0	Nutanix Object Storage	NTNX-JWF3R53-A-CVM		10.55.16.71	XC740xd2-24 0
	Arcserve UDP Console & RPS Settings	NTNX-JWF2853-A-CVM		10.55.16.69	XC740xd2-24 0
	Review Configuration Settings	Cluster Information			
	Installation	Cluster Virtual IP :	101003-001		
	Installation Status	Node Count:	4		
	instaliation status	Storage Capacity : AOS Version :	703.03 TIB free of 704.06	118	
		Storage Container			
		Please select a storage	container which will be	used for UDP products Installation.	
		Please select a storage	container	~	
		Previous			

- 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**.

💿 Open					
← → ~ ↑ 🕹	 This PC 	C > Downloads >	√ Ö	Search Downloads	,
Organize 🔻 Ne	w folder			III • 🔲	
This PC	^ Na	ime	^		۵
E. Desktop		anyburn			8
Documents	0	17763.737.190906-2324.rs5	release_svc_	refresh_SERVER_EVAL_x64FRE	1
Downloads		a1-test-image.iso			1
h Music	-	en_windows_server_2019_u	pdated_nov	_2020_x64_dvd_8600b05f.iso	1
Pictures					
Videos					
🏪 Local Disk (C:) ~ <				
	File name	en_windows_server_2019_u	updated \vee	Disc Image File (*.iso)	
				Open Cancel	

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.

End User License Agreement (EULA)	Network Settings	
Nutanix Cluster Information	Configure the required settings for Ar	rcserve backup network settings
Available Nutanix Servers	Network Name	C Refresh VLAN ID
Windows ISO Upload	AHV-Network	~
Network Settings	DNS 1	DNS 2 (Optional)
Nutanix Object Storage		
Arcserve UDP Console & RPS Settings	Specify the Domain Credentials (Opti	onal)
Review Configuration Settings	Domain Name	
Installation		
Installation Status	Username	Password
	Additional network for guest processing	3
	_	
	Previous	

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.

End User License Agreement (EULA)	Nutanix Object Storage	
Nutanix Cluster Information	Configure the key information for all the data store	backup type.
Available Nutanix Servers	Access Key ID	
Windows ISO Upload	pdXbUF9ISIkgQI4MUore6n3IHnjvAl+HN	
Network Settings	Secret Key	
 Nutanix Object Storage 		
Arcserve UDP Console & RPS Settings	End Point	Port Number
Review Configuration Settings	B-00-0100	80
Installation		
Installation Status		
	Click here to know about Nutanix Object Store	
	Previous	

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

End User License Agreement (EULA) Nutaela Cluster Information	Arcserve UDP Console & RPS Settings Conjugate the required settings for backup network						0	
Available Nutanix Servers	UDP Console + RPS Sen	ver					+ UDP Console & RPS Server	
Windows ISO Upload	VM Host Name	Storage (in GiB)	VCPU	core	RAM (in GiB)	Action		
Network Settings	udpconsole	500	2	96	128	Edit Delete		
Nutanix Object Storage	Windows RPS Server(s)						+ Additional RPS Server	
Arcserve UDP Console & RPS Settings	No RPS server has been	added						
Review Configuration Settings								
Installation	Linux LBS Server(s)	firme in Citi	-001		BAM IN COD	Action	+ LBS Server	
Installation Status	udpibs	50	2	2	15 K	Edit Delete		
	Previous						Cancel	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.

Add UDP Console & RPS	Server						×
		U	DP Details D	ata Store			
VM Host Name		Storage	(1)	VCPU	Core	RAM	۲
udpconsole		500	GIB	2	16	128	GIB
Storage Container: default-o	ontainer-65437414196614						
UDP Console Credentials	5						
Specify the credentials for	or Windows admin account						
Local Administrator	Password			Cor	nfirm Password		
Administrator				-			
Enter a product key							
						Can	cel Save

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.

Add UDP Console & RPS Server		×
	UDP Details Data Store	
Data Store Name (1		
arcstore01		
Bucket Name		
udpbucket		
Concurrent Active Nodes Limit to		
20		
Data Store Folder C:\ArcserveDatastore		
Enable Dededuplication		
Deduplication Block Size 64 KB		
Hash Memory Allocation 98304	MB (Maximum: 131071 MB;Minimum: 1024 MB)	
Size of the HDD		
24000 GiB		
Index Destination D:VArcserveDedupVIndex		
Hash Destination D:\ArcserveDedup\Hash		
Enable Compression		
Compression Type • Standard · Maximum		
	Car	ncel Save

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.

Add Windows RPS Ser	rver					×
		RPS S	Server Detail	s Data Sto	re	
VM Host Name		Storage 40	GIB	VCPU	Core	RAM () 8 GIB
Storage Container: defau Windows Admin Local Specify the credentials	It-container-66030572756408 Account s for Windows admin account					
Local Administrator Administrator Windows Activation (O	Password ptional)				ionfirm Password	
Enter a product key						
						Cancel

- 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.

Add Windows RP3 Server				~
		RPS Server Details	Data Store	
Data Store Name				
Bucket Name				
Concurrent Active Nodes Limit to	٢			
4				
Data Store Folder C:\ArcserveDatas	tore			
Enable Dededuplication				
Deduplication Block Size 64 KB				
Hash Memory Allocatton		MB (Maximum: 8191 MB;Minimum: 1024 MB)		
Hash destination is on a Solid !	State Drive (SSD)			
Size of the HDD				
GIB				
Index Destination D:ArcserveDee	dup\Index			
Hash Destination D:\ArcserveDed	lup\Hash			
Enable Compression				
Enable Encryption				
				Cancel

Add Windows DDS Sonio

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.

Add LBS Server							×
		L	BS Server Deta	ls			
VM Host Name		Storage	VCPU		Core	RAM	
udpibs		15 G	iB 2		2	8	GIB
Storage Container: default	Storage Container: default-container-9672678670203 LBS Server Credentials						
Specify the credentials	for LBS admin account						
Root Administrator	Password			i Confirm Pa	assword		
root					•		

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**.

•	End User License Agreement (EULA) Nutanik Cluster Information	Review Configuration	on Settings ngs provided. You can go back	to previous steps and make ch	anges if	f necessary.			Ū
•	Available Nutanix Servers	Node Name	Storage (in GiB)	VCPU	Core		RAM (in GIB)	Role	
•	Windows ISO Upload	udpconsole	500	2	16		128	UDP Console	
	Network Settings	udpibs	50	2	2		16	LBS Server	
	Nutanik Object Storage	Nutantx Mine with Arcser	ve Cluster Information.						
	Arcserve UDP Console & RPS Settings	Cluster Virtual IP :				Usemane :	Administrator		
	Review Configuration Settings	Node Count :	4			Nutantx Model :	XC740xd2-24 CORE		
0	Installation	ADS Version :	5.20			Hypervisor :	AHV		
	Installation Status								
		Previous						Cancel	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.

End User License Agreement (EULA)	Installation Please wait while we deploy the necessary components and configure the Mine cluster	0
Nutanic Cluster Information Available Nutanic Servers Windows ISO Upload	v udpconsole - Hash disk attached successfully	
Nutanix Object Storage Nutanix Object Storage Arcserve UDP Console & RPS Settings Review Configuration Settings Installation Installation	udpconsole VM Powered on successfully udplbs VM created successfully udplbs VM Powered on successfully UDPCONSOLE Windows installed successfully UDPCONSOLE Arcserve UDP Agent installation completed	
	UDPCONSOLE Arcserve UDP Console installation completed UDPCONSOLE Arcserve UDP Recovery Point Server installation completed Data store arcstore01 has been created successfully LBS udpits has been added successfully The data store arcstore01 has been converted successfully	Cancel 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 <u>Maintenance and Troubleshoot</u>ing.

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 <u>Step 12</u> 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

🗧 walkthrough Accenve Home 👻 💝 🐥 🎯 • 🔿 •				b	٥	2.? × ⊅ admin
					N	arcserve
Mine Cluster	Protection		Job Status		UDP Alerts and Events	0 0
~	0 Protected Instances		0 Backup Jobs			
WARNING	RAM/HASH		Running Jobs	0		
	Dam 23.	3.9 TB	Completed Jobs	0		
Arresta Management			 Failed Jobs 	0		
Arcsa te management			 Incomplete Jobs 	0		
Storage Throughput	Capacity Usage				Nutanix Alerts	000
195 KB 176 KB	In use 0.21 TiB of 41.82 TiB				CVM NIC Speed Low	a month ago
156 KB					 Host 10.10.127/190 is using default password 	a month
137 KD	- 604 TB Natarox C	uster 0.24 Til	Arconve Cluster 41.52 TB Available Space		 Host 10.10.127376 is using default password 	a month
50 KD					 Host 10.10.127.192 is using default password 	a month
5910	RPS nodes	LBS	Nodes Mine Cluster N	lodes	Activate Window	ago /s ate Window a

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.

Nutanix Cluster Information	Nutanix Cluster Information	
	Specify required information for connecting to t	the Nutanix cluster
Reregistration Status	Prism Element IP	Port Number
	Enter Ip Address	9440
	Username	_
	Enter Username	
	Descoursed	
	Password	
	Enter Password	
	Re-registration of dashboard will cause the Arcserve Installation details in this cluster d	current dashboard (if any) to be replaced with the n to not proceed with this step.

- 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.
| Nutanix Cluster Information | Re-registration of Arcserve Dashboard |
|--------------------------------------|---------------------------------------|
| Reregistration of Arcserve Dashboard | UDP Server Host Name |
| Reregistration Status | Enter UDP server host name |
| | Domain Name (Optional) |
| | Enter domain name |
| | DNS 1 |
| | Enter DNS 1 |
| | DNS 2 (Optional) |
| | Enter DNS 2 |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | Previous |

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 indetail 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 <u>Arcserve support</u>.

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	
Create a Plan Using Arcserve N-Series Appliance Wizard	110
Create a Backup Plan for Linux Nodes	111
Create an On-Appliance Virtual Standby Plan	
Create Plan to Backup the Linux Backup Server	113

Activate Arcserve Product on the Appliance

For activating Arcserve product on the Appliance, see <u>Arcserve Product Licensing</u> 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 <u>Arcserve UDP Solutions Guide</u>.

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 <u>How to</u> <u>Create a Linux Backup Plan</u> 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 <u>How to Create a</u> <u>Virtual Standby Plan</u> 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.

Add Nodes to	Arcserve UDP Console							
Add nodes by	Add Linux Node	v						
				E Y	Node Name	VM Name	Hypervisor	
٩	Node Name/IP Address	Linux-BackupSvr						
0	SSH Key Authentication							
U	User Name	root						
F	Password							
í.	Non-root Credential							
P								
F	Password							
4	Add Description							
		Add	d to List				Remove	
						_		_
Help						S	Cano Cano	el

6. Click Save.

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

resources								
42	Nodes: A	II Node	s					3>
Nodes	Actions -	A	id Nodes	Filter ×	(No filter applied)	~		Configuration Wizard
All Nodes					(10 110 0)			
Nodes without a Plan		Status	Node Name	VM N	ame	Plan		Select a node to view the related details
Plan Groups	E7	0	linux-backupsvr					octano.
Linux Backup Server Groups								
Linux Nodes								
Plans								
All Plans								
Destinations								
Recovery Point Servers								
Arcserve Backup Servers								
Shared Folders	1							
Cloud Accounts								
Remote Consoles								
Arcserve Cloud								
 Infrastructure 								
Storage Arrays								
Instant Virtual Machines								
Sites								
SLA Profiles								
	4						•	
	🚺 🖣 🏼 Pa	ige 1	of 1 🕨 🕅			Displaying 1	- 1 of 1	

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

The **Source** tab appears.

resources					
Add a Plan	Agent-Based Linux Bac	kup Plan	Pause this plan	Save	Cancel Help
Task1: Backup: Agent-Based Linux	Task Type Backup	o: Agent-Based Linux	Y		Opelete Task
Add a Task	Source De	stination Schedule	Advanced		
	Linux Backup Server	appliance	✓ Add		
		move			
	Node Name	VM Name P	tarı	Site	
	Filter volumes for back	IP Exclude -			

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

resources					
Add a Plan	Agent-Based Linux Backup	Plan	Pause this plan	Save	Cancel Help
Task1: Backup: Agent-Based Linux	Task Type Backup: A	gent-Based Linux	Ŧ		Delete Task
O Add a Task	Source Dest	ination Schedule	Advanced		
	Linux Backup Server	appliance	✓ Add		
	Add Remo Select Nodes to Pro Add Linux Node	ve lect in Arcserve UDP	lan	Site	
	Eilter volumes for backup	Evaluate -			
	Files/folders to be exclude	d			

The Select Nodes to Protect dialog opens.

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

elect	Nodes to Protect										E
Ava	ilable Nodes	5			S	Sele	ected Nodes				
iroup	All Nodes (Def	ault Groups)	•								
1	Node Name	VM Name	Plan	Site			Node Name	VM Name	Plan	Site	
1	linux-backupsvr			Local Site			linux-backupsvr			Local Site	
					»						
					>						
					<						
					«						
н	I Page 1	of 1 🕨 🕨	🛛 🥏 Dis	playing 1 - 1 of 1							
										01	nce

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.

resources							
Add a Plan	Agent-Based	Linux Backup Plan		Pause this plan		Save	Cancel Help
Task1: Backup: Agent-Based Linux	Task Type	Backup: Agent-Base	d Linux	Ŧ			Oelete Task
Add a Task	Source Destination Typ	e Destination	Schedule	Advanced	ve UDP Recovery Point Server		
	Recovery Point	Server	appliance		¥		
	Data Store		appliance_data_s	store 👻			
	Password Prote	ction	0				
	Session Passwo	brd					
	Confirm Session	n Password					

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

resources								
4	Plans: A	II Plans						30
Nodes All Nodes	Actions	- Add a Plan						Configuration Wizard
Nodes without a Plan		Plan Name		Nodes P	rotected		Status	Select a plan to view the related details
vCenter/ESX Groups			Total	0	0	0		dound.
Hyper-V Groups Linux Nodes		Agent-Based Linux Backup Plan	1	0	1	0	Deployment: Successful (1)	
Linux Backup Server Groups	_							
Plan Groups								
⊿ Plans								
All Plans								
⊿ Destinations								
Recovery Point Servers								
Arcserve Backup Servers								
Shared Folders								
Cloud Accounts	4							
Remote Consoles								
Arcserve Cloud								

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	. 118
How to Perform Nutanix AOS Cluster Expansion	119

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.

PHOCMIKT238 Settings	- 😻 O + Q. ? - 🔯 adm -
Settings	
General	
Cluster Details	
Configure CVM	
Convert Cluster	
Expand Cluster	
Image Configuration	
Licensing	
Reboot	
Remote Support	
Upgrade Software	
Setup	Global Settings
Connect to Citrix Cloud	Clobal Settings
Prism Central Registration	Unosse an sem on the Mit Io Congure
Pulse	
Rack Configuration	

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

X PHX-MKT238 Hardware	· · © 0 @ ·				Q ? × ¢ admin ×
Overview - Diagram - Table					+ Expand Cluster Repair Host Boot Device
Hardware Summary		Top Hosts by Disk IOPS		Hardware Critical Alerts	Hardware Events
4 1	NX-3060-G6	PHX:MKT238-3	3 IOPS		
HOSTS BLOCK	MODEL	PHX:MKT238-2	2 IOP5		2 EVENTS
		No. of Concession,	1.00.00		
4 Hosts		Top Hosts by Disk IO Bandwidth			Node 10.42.238.28' with UUID '67e4366b-2ebc-4a5c-ba55- d7881cf5e66' removed.
4		PHX-MKT238-3	1.53 MBps	No Critical Alerts	Last event 29 minutes ago
4 MONITORED	C	PHX:MKT238-2	983 KBps		Node '10.42.238.26' marked for removal Last event 36 minutes ago
	COCOTENED	AL 117 1 117 1 117 1 117 1 117	AAA 11A		

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.

Expand Cluster	?
1. Select Host 2. Configure Host	
Manual Host Discovery	
Add host or CVM IPs to discover hosts within the same	e network.
	+ Add Host
Host or CVM IP	Actions
No Data	

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

1. Select Host 2. Configure Host	
Manual Host Discovery	
Add host or CVM IPs to discover hosts wit	thin the same network.
	+ Add Ho
Host or CVM IP	+ Add Ho: Actions
Host or CVM IP Host or CVM IP	+ Add Ho: Actions Save - Cancel

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.

Newly discovered nodes are displayed below. Select the ones you would like to add and configure their network addresses. New nodes must be connected to the network on the same subnet as the cluster (10.55.16.0/255.255.248.0). Remember to add licenses for all new nodes.	
2 XC740xd2-24 CORE (Serial Number: JWF4853)	
🖬 D	
 Controller VM IPv4 Host D Controller VM IPv6 	
lost D	

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**.

1. Select Host	2. Configure Host	
Hypervisor(s) N	eeded	
The detected hy	pervisor on the new node has the same Hyperviso	or and AOS

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.

Expand Cluster	?
1. Select Host 2. Configure Host	
Expanding Cluster	
	/1%
	Close
Expand cluster operation initialized	100 %
Pre expand-cluster tests completed	100 %
	100 %
Internal preparation completed	100 %
Stripping imposing of pages	
Skipping maging of nodes	100 %
Waiting for per node tasks to complete	
	30 %
Back	

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	
Electrical Safety Precautions	
FCC Compliance	
Electrostatic Discharge (ESD) Precautions	

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)

이 기 기 는 업 무 용 (A급)으로 전 자 파 적 합 기 기 로 서 판 매 자 또 는 사 용 자 는 이 점 을 주 의 하 시 기 바 라 며,가 정 외 의 지 역 에 서 사 용 하 는 것 을 목 적 으 로 합 니 다

Note: This safety precaution only applies to South Korea. For more details, contact Arcserve Support at <u>https://www.arcserve.com/support</u> 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: <u>https://www.arcserve.com/support</u>.
- 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.
- To request for a free copy of Sophos Intercept X Advanced, provide all relevant details in the <u>Sophos Request form</u> 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**.

	Product Setup	×
Choose a product below to get started.		
S Endpoint Protection	() Mobile	
Server Protection	Wireless	
😣 Email Security	O Device Encryption	
🕑 Web Gateway	(3) Phish Threat	
😂 Firewall Management		

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

SOPHOS	Protect Devices	Malga a antara tak
Overand Contrast Anno Const Anapon Cantor Const Anapon Const	Not do to a devind for for indigation and array in No. Second Second S	Both Ontoneys Annual of an annual Manual of an annual Manual of an annual Manual of an annual Manual Ma
	 Unified Enclosiet Management and Mulder Security Bene mergenetic at Management and Mulder Security in the mediated start is merge order protects a times 	Source: Photo: Source Photo: Photo: Source Photo: Ph

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.

SOPHOS Status	vents	Admin login – 🗙
Your com	nputer is protected	Scan
Malware and PUAs O detections	Web Threats O requests blocked	Malicious Behavior O detections
(iii) Controlled Items O user notifications	Malicious Traffic O connections detected	S Exploits O detections
		Help About

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 <u>online</u>, 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	. 138
Unable to View Arcserve Home Dashboard in the Prism Element	. 139
Nutanix Object Store Creation Fails Due to Time Out Error	140
Nutanix Mine Deployment Fails Due to Improper User Permissions or Lack of Enoug Resources	<u>h</u> 141
Arcserve Home Dashboard does not Display when the Network Switch or Cluster is Rebooted	142
Unable to Access the UDP Management Console UI from Outside the UDP Console VM	143
Nutanix Mine Deployment Fails Due to UDP VM Status Error	144
Nutanix Mine Deployment Fails Due To DNS Error	. 145

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.

Prism Central	?	×
Installation Image		
Select an image to install, download the latest version from the la upload one from your computer.	nternet	or
Available versions	version	s 🕛
No compatible versions for deployment.		
Upload installation binary		
You can upload the Prism Central binary instead of downloading Internet.	from th	ne
Back	Cance	el

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-interoperabilitymatrix/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

= 0, Objects	¢				👌 Prism					4 0	0 🚯 🔅
Object Stores VCenter Management											
Create Object Stoor Deadline Deadline Actions >											
Vewing all Object Stores 0 1-1											0 1-1of1
Nome	Creating lenovoobjstore		Nodes	Usage (Logical)		Buckets	Objects	Alerts	Notifications	Objects Public IPs	
Ienovoobjstore	Error in deployment. Time Out	lan.com	3							10.10.127369, 10.10	127170
											@ 1-1of1

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.
- After successfully deleting the failed Object Store, re-initiate the Object store creation. To create the Object Store, see <u>Deploying the Nutanix</u> <u>Object Store</u>.

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 <u>Main-tenance Troubleshooting</u>.

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**
- **8**015

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:

- 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, cleanup 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 <u>arcserve.com/support</u> 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.