arcserve®

White Paper

Integrating OneXafe and UDP

Legal Notice

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

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

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

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

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

The manufacturer of this Documentation is Arcserve.

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

Contact Arcserve Support

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

Contact Support

With Arcserve Support:

- You can get in direct touch with the same library of information that is shared internally by our Arcserve Support experts. This site provides you with access to our knowledge-base (KB) documents. From here you easily search for and find the product-related KB articles that contains the 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 the 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: Overview

Arcserve UDP (UDP) 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, Microsoft Hyper-V servers or Nutanix AHV 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.

OneXafe, with its patented distributed object store, prevents any form of overwriting. Furthermore, OneXafe performs powerful inline deduplication on continuous snapshots, which reduces the data footprint. OneXafe's scale-out architecture expands storage seamlessly. To enable this option, add one drive at a time or multiple nodes within a cluster without any configuration changes to the application.

This document contains information about the integration of UDP and OneXafe, which makes the UDP backup recovery point data immutable. For instance, if a cyber-criminal deletes the UDP recovery point data by a ransomware attack, OneXafe's immutable snapshot feature can come to the rescue and provide options to recover the lost data. An immutable snapshot is a copy of your data that cannot be overwritten or deleted by ransomware or users.

OneXafe Continuous Data Protection (CDP) performs continuous snapshots every 90 seconds for the first hour. Subsequently, it performs hourly, daily, and monthly snapshots. Snapshots help to recover data as close to a ransomware attack. Generally, the ransomware attack can corrupt the primary files but the snapshots are completely unaffected. OneXafe also provide options for easy recovery – recover individual files, folder or complete network share.

Ransomware on the Rise But with OneXafe Never Pay the Ransom
Recover Your Data with OneXafe Continuous Immutable Snapshots

Chapter 2: OneXafe Configuration

This section provides information about how to configure OneXafe cluster.

To configure OneXafe Cluster, do the following:

1. Set up network configuration
2. Create a single node or multi-node (up to 3 nodes) cluster
3. Register the cluster in the OneSystem account (User Management and Storage Management) using Share Creation.
4. Set virtual IP for the OneXafe Cluster

This document applies to the following or newer versions of UDP and OneXafe:

- UDP version 8.0 or newer: Build 5628 for all the UDP components, which includes UDP Console, Recovery Point Server, and UDP agents.

- OneXafe Cluster
  - Models: OneXafe 4412, 4417, 5410
  - Software Version:3.2.3 Cabernet Sauvignon or newer

Configure Network

This section contains information on how to configure OneXafe Network.

To configure network, log into OneXafe Web Console and go to the **Configuration > Network** tab. Make sure you have different network profiles as shown in the below illustration.

Note: We recommend the following:

- For a system with four network ports, create two network profiles: Management and Data.
- For a system with six network ports, create three network profiles: Management, data, and Cluster.
- 10GbE networking

Configure iDRAC for OneXafe Cluster

By default, when a network cable is connected to the iDRAC port, it acquires a DHCP address. The default iDRAC login details are:

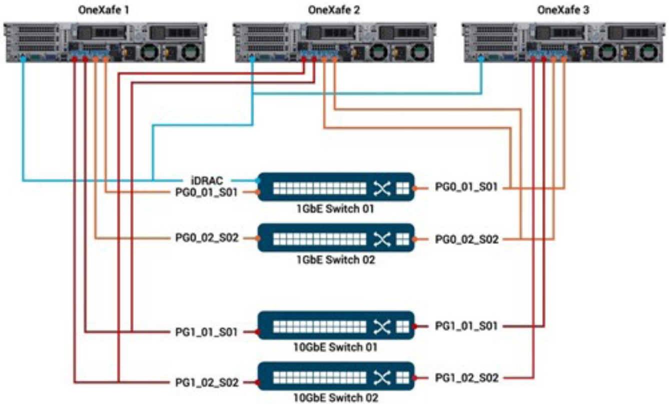
- User name: admin
- Password: config

For OneXafe deployed on a network without a DHCP server, admins can now set a static IP address for iDRAC. See the example below.

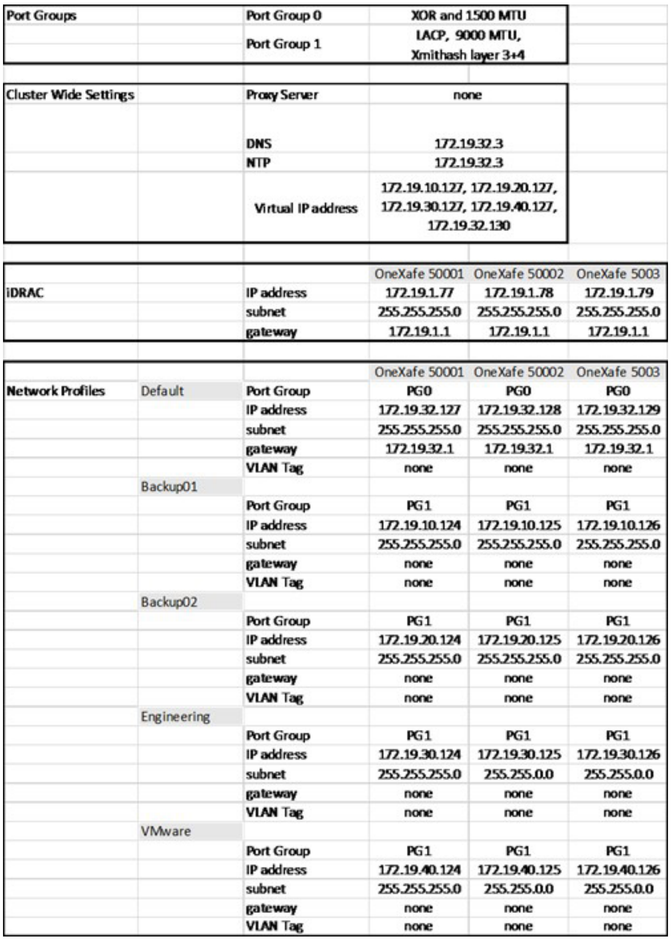
```
The last # show lan command is used to verify the setting.

oneblox50001(config) ipmi oneblox50001(config-ipmi) help
Documented commands (type help <topic>):
========================================
apply exit help lan logout reset show
Undocumented commands:
======================
end
oneblox50001(config-ipmi) help lan

Manage the IPMI lan interface and provide access to configuration parameters.

These setting will not be applied until the configuration is saved.
Usage:
lan
lan dhcp
lan static <addr> <netmask> [<gateway>] lan vlan <tag>

Examples:
- configure a static ip network and no gateway lan static inet 10.0.0.0 255.0.0.0

See Also:
apply

oneblox50001(config-ipmi) lan static 172.19.1.77 255.255.255.0
oneblox50001(config-ipmi) apply
oneblox50001(config-ipmi) show lan
```

How to Properly Configure OneXafe Networking and Port Groups

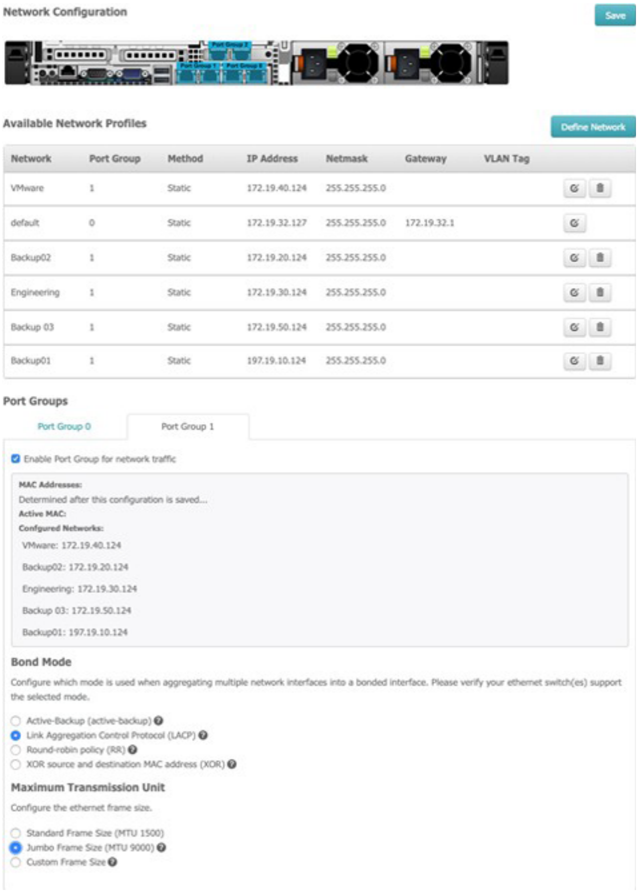
The following network configuration diagram includes a 3-node cluster, two port groups, and iDRAC. It also contains network redundancy to multiple switches. In this example, the 10GbE switches are stackable and the ports are configured in LAG.



The following example contains the OneXafe cluster-wide settings, iDRAC, multiple VLAN IP address, configuration details, and the configuration of PG1 through the web console.



Port Groups		Port Group 0	XOR and 1500 MTU		
		Port Group 1	LACP, 9000 MTU, Xmithash layer 3+4		
Cluster Wide Settings		Proxy Server	none		
		DNS	172.19.32.3		
		NTP	172.19.32.3		
		Virtual IP address	172.19.10.127, 172.19.20.127, 172.19.30.127, 172.19.40.127, 172.19.32.130		
			OneXafe 50001	OneXafe 50002	OneXafe 5003
iDRAC		IP address	172.19.1.77	172.19.1.78	172.19.1.79
		subnet	255.255.255.0	255.255.255.0	255.255.255.0
		gateway	172.19.1.1	172.19.1.1	172.19.1.1
			OneXafe 50001	OneXafe 50002	OneXafe 5003
Network Profiles	Default	Port Group	PG0	PG0	PG0
		IP address	172.19.32.127	172.19.32.128	172.19.32.129
		subnet	255.255.255.0	255.255.255.0	255.255.255.0
		gateway	172.19.32.1	172.19.32.1	172.19.32.1
		VLAN Tag	none	none	none
	Backup01				
		Port Group	PG1	PG1	PG1
		IP address	172.19.10.124	172.19.10.125	172.19.10.126
		subnet	255.255.255.0	255.255.255.0	255.255.255.0
		gateway	none	none	none
		VLAN Tag	none	none	none
	Backup02				
		Port Group	PG1	PG1	PG1
		IP address	172.19.20.124	172.19.20.125	172.19.20.126
		subnet	255.255.255.0	255.255.255.0	255.255.255.0
		gateway	none	none	none
		VLAN Tag	none	none	none
	Engineering				
		Port Group	PG1	PG1	PG1
		IP address	172.19.30.124	172.19.30.125	172.19.30.126
		subnet	255.255.255.0	255.255.0.0	255.255.0.0
		gateway	none	none	none
		VLAN Tag	none	none	none
	VMware				
		Port Group	PG1	PG1	PG1
		IP address	172.19.40.124	172.19.40.125	172.19.40.126
		subnet	255.255.255.0	255.255.0.0	255.255.0.0
		gateway	none	none	none
		VLAN Tag	none	none	none



Network Configuration

Available Network Profiles

Network	Port Group	Method	IP Address	Netmask	Gateway	VLAN Tag
VMware	1	Static	172.19.40.124	255.255.255.0		
default	0	Static	172.19.32.127	255.255.255.0	172.19.32.1	
Backup02	1	Static	172.19.20.124	255.255.255.0		
Engineering	1	Static	172.19.30.124	255.255.255.0		
Backup 03	1	Static	172.19.50.124	255.255.255.0		
Backup01	1	Static	197.19.10.124	255.255.255.0		

Port Groups

Port Group 0 | Port Group 1

☑ Enable Port Group for network traffic

MAC Addresses:
Determined after this configuration is saved...
Active MAC:
Confgured Networks:
VMware: 172.19.40.124
Backup02: 172.19.20.124
Engineering: 172.19.30.124
Backup 03: 172.19.50.124
Backup01: 197.19.10.124

Bond Mode

Configure which mode is used when aggregating multiple network interfaces into a bonded interface. Please verify your ethernet switch(es) support the selected mode.

○ Active-Backup (active-backup)
● Link Aggregation Control Protocol (LACP)
○ Round-robin policy (RR)
○ XOR source and destination MAC address (XOR)

Maximum Transmission Unit

Configure the ethernet frame size.

○ Standard Frame Size (MTU 1500)
● Jumbo Frame Size (MTU 9000)
○ Custom Frame Size

Example: OneXafe 3 node cluster Deployment Networking Configuration for 10GbE network

This example includes the following details:

- 10GbE network
- PG0 (XOR), PG1 (XOR)
- VLAN tagging

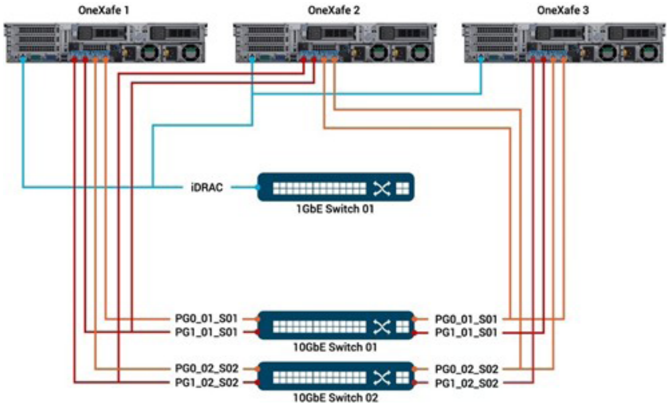
In this Backup/Recovery and VMware example, one VLAN is routable to a gateway for OneSystem access while other VLANs are not routable.

With the exconsole, the xmithash policy on PG1 can be set to layer3+4. By default, it is layer2+3 and will show as blank in the exconsole. All other port group settings can be done through the web console so the illustration is only for the xmithash policy setting.

```
oneblox50001(config-network)
oneblox50001(config-network) portgroup
Portgroup Enable Mtu Bondmode Xmithash
0 true 1500 active-backup
1 false 1500 active-backup
2 false 1500 active-backup
oneblox50001(config-network) portgroup xmithash 1 layer3+4
Portgroup Enable Mtu Bondmode Xmithash
0 true 1500 active-backup
1 false 1500 active-backup layer2+3 (current)
layer3+4 (pending)
2 false 1500 active-backup
oneblox50001(config-network) apply
oneblox50001(config-network) portgroup
Portgroup Enable Mtu Bondmode Xmithash
0 true 1500 active-backup
1 false 1500 active-backup layer3+4
2 false 1500 active-backup
oneblox50001(config-network)
```

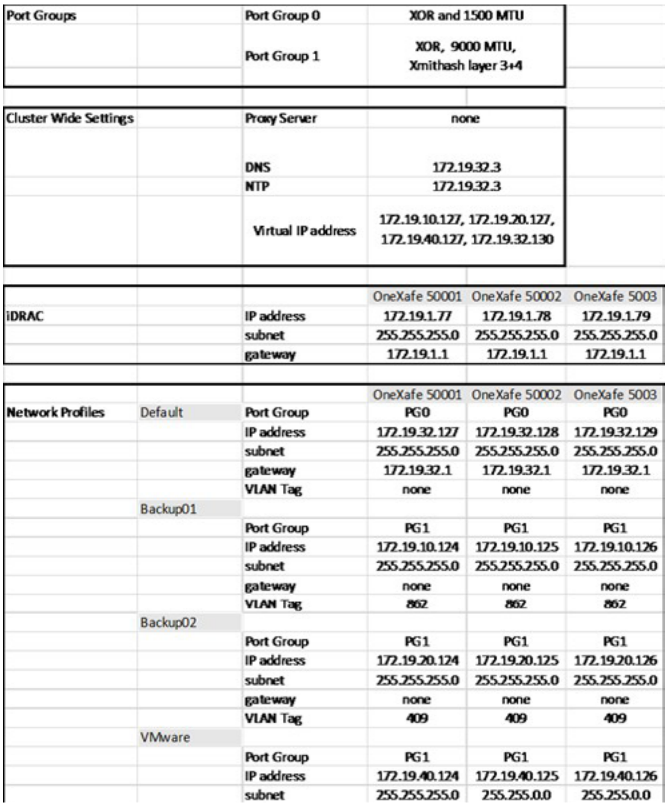
Note: The above example provides the required switch port configuration for the different hash algorithms.

The following example is a network configuration diagram for a 3 node cluster, two-port groups, and iDRAC. There is network redundancy to multiple switches (except for iDRAC). In this example, the 10GbE switches are not stackable; hence the switches do not support LACP across multiple switches. In that case, select XOR as we recommend it as the next best option. However, LACP is the preferred bond mode.

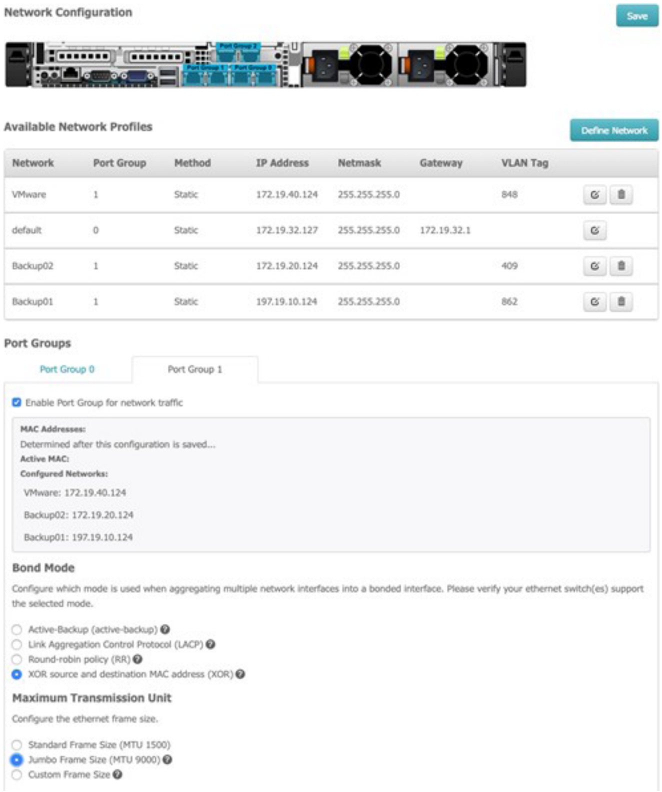


The following example includes OneXafe cluster-wide settings, iDRAC, multiple VLAN IP address, configuration details, and the configuration of PG1 through the web console.

Note: To move a network profile to a different port group, select the edit icon, and then select the desired port group. You don't have to



Port Groups		Port Group 0	XOR and 1500 MTU		
		Port Group 1	XOR, 9000 MTU, Xmithash layer 3+4		
Cluster Wide Settings		Proxy Server	none		
		DNS	172.19.32.3		
		NTP	172.19.32.3		
		Virtual IP address	172.19.10.127, 172.19.20.127, 172.19.40.127, 172.19.32.130		
			OneXafe 50001	OneXafe 50002	OneXafe 5003
iDRAC		IP address	172.19.1.77	172.19.1.78	172.19.1.79
		subnet	255.255.255.0	255.255.255.0	255.255.255.0
		gateway	172.19.1.1	172.19.1.1	172.19.1.1
			OneXafe 50001	OneXafe 50002	OneXafe 5003
Network Profiles	Default	Port Group	PG0	PG0	PG0
		IP address	172.19.32.127	172.19.32.128	172.19.32.129
		subnet	255.255.255.0	255.255.255.0	255.255.255.0
		gateway	172.19.32.1	172.19.32.1	172.19.32.1
		VLAN Tag	none	none	none
	Backup01				
		Port Group	PG1	PG1	PG1
		IP address	172.19.10.124	172.19.10.125	172.19.10.126
		subnet	255.255.255.0	255.255.255.0	255.255.255.0
		gateway	none	none	none
		VLAN Tag	862	862	862
	Backup02				
		Port Group	PG1	PG1	PG1
		IP address	172.19.20.124	172.19.20.125	172.19.20.126
		subnet	255.255.255.0	255.255.255.0	255.255.255.0
		gateway	none	none	none
		VLAN Tag	409	409	409
	VMware				
		Port Group	PG1	PG1	PG1
		IP address	172.19.40.124	172.19.40.125	172.19.40.126
		subnet	255.255.255.0	255.255.0.0	255.255.0.0



Network Configuration

Available Network Profiles

Network	Port Group	Method	IP Address	Netmask	Gateway	VLAN Tag
VMware	1	Static	172.19.40.124	255.255.255.0		848
default	0	Static	172.19.32.127	255.255.255.0	172.19.32.1	
Backup02	1	Static	172.19.20.124	255.255.255.0		409
Backup01	1	Static	197.19.10.124	255.255.255.0		862

Port Groups

Port Group 0 | Port Group 1

☑ Enable Port Group for network traffic

MAC Addresses:
Determined after this configuration is saved...
Active MAC:
Confgured Networks:
VMware: 172.19.40.124
Backup02: 172.19.20.124
Backup01: 197.19.10.124

Bond Mode

Configure which mode is used when aggregating multiple network interfaces into a bonded interface. Please verify your ethernet switch(es) support the selected mode.

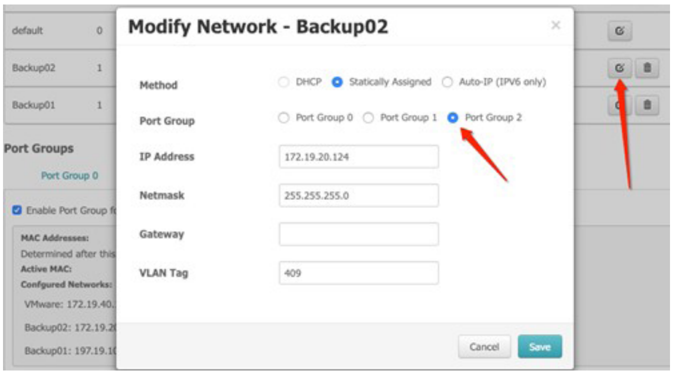
○ Active-Backup (active-backup)
○ Link Aggregation Control Protocol (LACP)
○ Round-robin policy (RR)
● XOR source and destination MAC address (XOR)

Maximum Transmission Unit

Configure the ethernet frame size.

○ Standard Frame Size (MTU 1500)
● Jumbo Frame Size (MTU 9000)
○ Custom Frame Size

delete and create a new network profile. The following image shows how Backup02 has been edited from Port Group 1 to Port Group 2.



Modify Network - Backup02

Method: ○ DHCP ● Statically Assigned ○ Auto-IP (IPV6 only)

Port Group: ○ Port Group 0 ○ Port Group 1 ● Port Group 2

IP Address: 172.19.20.124

Netmask: 255.255.255.0

Gateway:

VLAN Tag: 409

For more information, watch the video: Configuring Network Port Groups with OneBlox Exconsole.

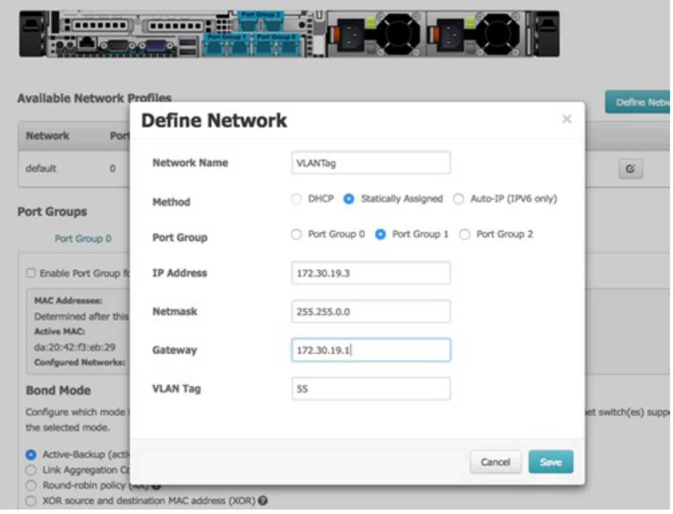
Configuring VLAN Tagging

With the OneXafe web console (and exconsole commands), admins may assign VLAN tags (tagging Ethernet packets with a value for routing purposes) to a network profile. VLAN tags are not required and many organizations opt to use portbased VLANs to route multiple subnets over the same switch ports.

When removing the VLAN tag from an existing network profile through exconsole or web console, set the VLAN tag value to ‘0’. Then click save (web console) or apply (exconsole).

Example:

- Miraki port based VLAN tagging
- Cisco Nexus 5000 Configuration Guide



Define Network

Network Name: VLANTag

Method: ○ DHCP ● Statically Assigned ○ Auto-IP (IPV6 only)

Port Group: ○ Port Group 0 ● Port Group 1 ○ Port Group 2

IP Address: 172.30.19.3

Netmask: 255.255.0.0

Gateway: 172.30.19.1

VLAN Tag: 55

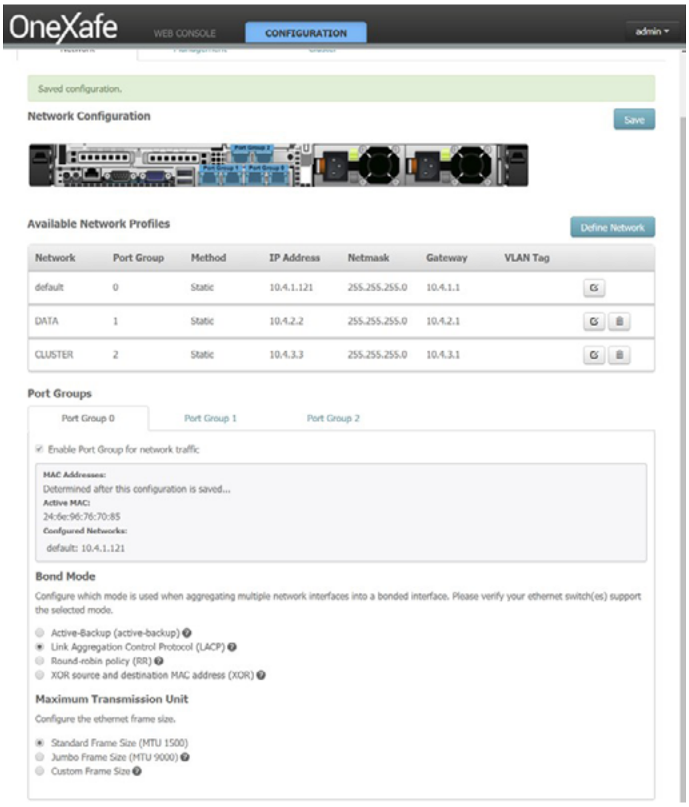
There are three networks that need to be configured and port groups that needs to be enabled in the recommended configuration:

1. Management (default) - Port Group 0
2. Data - Port Group 1
3. (Optional)Cluster - Port Group 2 – Advanced Networking

Management (default) - Port Group 0

Primary use - Used to communicate with OneSystem

- Does not require high-speed connections - 1GbE will suffice Static
- IP is highly recommended
- Path MTU discovery works on the connection up to OneSystem



Saved configuration.

Network Configuration

Available Network Profiles

Network	Port Group	Method	IP Address	Netmask	Gateway	VLAN Tag
default	0	Static	10.4.1.121	255.255.255.0	10.4.1.1	
DATA	1	Static	10.4.2.2	255.255.255.0	10.4.2.1	
CLUSTER	2	Static	10.4.3.3	255.255.255.0	10.4.3.1	

Port Groups

Port Group 0 | Port Group 1 | Port Group 2

☑ Enable Port Group for network traffic

MAC Addresses:
Determined after this configuration is saved...
Active MAC:
24:6e:96:76:70:85
Configured Networks:
default: 10.4.1.121

Bond Mode

Configure which mode is used when aggregating multiple network interfaces into a bonded interface. Please verify your ethernet switch(es) support the selected mode.

○ Active-Backup (active-backup)
● Link Aggregation Control Protocol (LACP)
○ Round-robin policy (RR)
○ XOR source and destination MAC address (XOR)

Maximum Transmission Unit

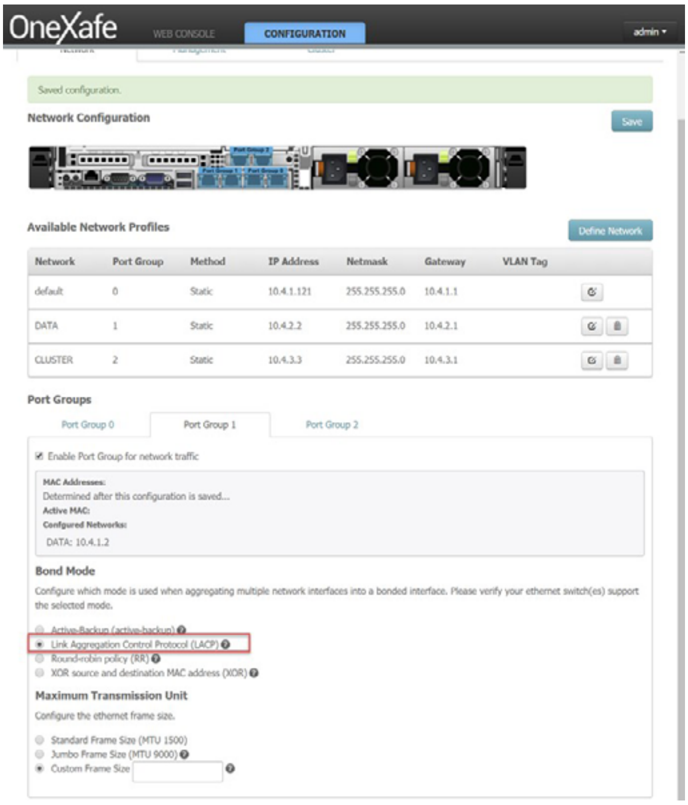
Configure the ethernet frame size.

● Standard Frame Size (MTU 1500)
○ Jumbo Frame Size (MTU 9000)
○ Custom Frame Size

Data - Port Group 1

Primary use - Used to communicate with the client network and ingestion (e.g. SMB shares, NFS exports)

- For optimal performance, ensure LACP is configured Static IP is highly recommended
- MTU should match your switch topology - typically 1500
- Communication to the cluster will happen via the VIP (Virtual IP) that is configured in this network - Communicating to the cluster through the VIP is done over SMB or NFS.
- Register the VIP to the domain as an FQDN
- Once data is ingested, the cluster operation goes through the cluster network. Ensure the Cluster Network has equal or greater bandwidth than the Data Network.
  - For example, if 20GB coming in the data side, ideally there would be 20GB to go out the cluster side, too.
  - In addition, there is a data placement protocol for puts/writing out the blocks into the distributed object storage.



Saved configuration.

Network Configuration

Available Network Profiles

Network	Port Group	Method	IP Address	Netmask	Gateway	VLAN Tag
default	0	Static	10.4.1.121	255.255.255.0	10.4.1.1	
DATA	1	Static	10.4.2.2	255.255.255.0	10.4.2.1	
CLUSTER	2	Static	10.4.3.3	255.255.255.0	10.4.3.1	

Port Groups

Port Group 0 | Port Group 1 | Port Group 2

☑ Enable Port Group for network traffic

MAC Addresses:
Determined after this configuration is saved...
Active MAC:
Confgured Networks:
DATA: 10.4.1.2

Bond Mode

Configure which mode is used when aggregating multiple network interfaces into a bonded interface. Please verify your ethernet switch(es) support the selected mode.

○ Active-Backup (active-backup)
● Link Aggregation Control Protocol (LACP)
○ Round-robin policy (RR)
○ XOR source and destination MAC address (XOR)

Maximum Transmission Unit

Configure the ethernet frame size.

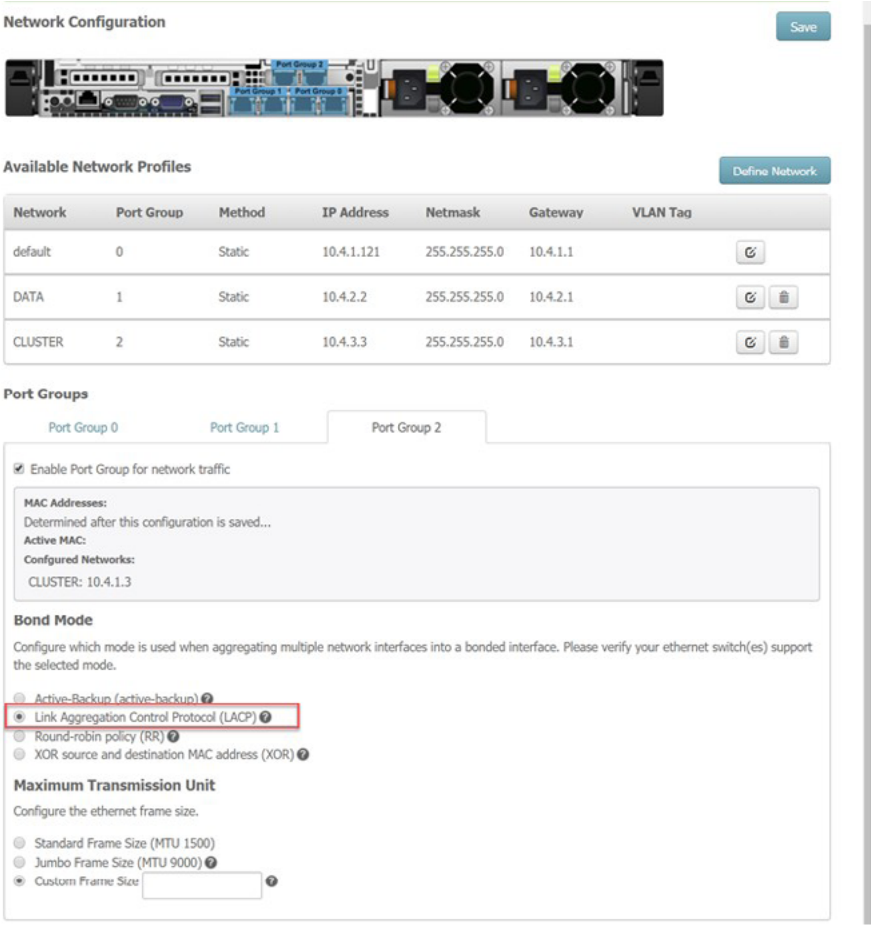
○ Standard Frame Size (MTU 1500)
○ Jumbo Frame Size (MTU 9000)
● Custom Frame Size

(Optional) Cluster - Port Group 2 – Advanced Networking

Primary use - Used for all intra-cluster communication functions.

- For optimal performance, ensure LACP is configured.
- The cluster network is auto-configured during the cluster configuration as IPv6 and is auto-discovered. Assuming that the cluster network is in the same switch domains and can see each node.
- The LAN doesn't run a protocol, only the endpoints – in this case the OneXafe nodes. The LAN can carry both IPv4 and IPv6 traffic. The nodes in the cluster use IPv6 to auto-config and communicate between the nodes.
- The cluster configuration also includes IPv6 - SLAC (Stateless Link Auto Config).
- Ensure that neighborhood discovery is enabled on all switches in the environment.
- Cluster communication across tunnels is not supported.
- Required communication protocols are:
  - Multicast (same switch fabric), our cluster must exist within the same multicast domain.
  - The cluster side needs to translate using two different protocols. HA protocol (management, keep a VIP alive, etc.) and a multicast protocol, VRRP (Virtual Route Redundancy Protocol).
- In addition to the multicast protocol, point-to-point unicast traffic over TCP is done over SSDP.

- The most common misconfigurations are issues related to multicast and TCP flow control - ensure both protocols are enabled on all ports connected to a OneXafe.
  - Improperly configured TCP flow control can starve a node - ensure proper configuration of TCP flow control to mitigate risk.
- Ideal configuration must consist of a cluster switch that is dedicated to the cluster traffic.



Network Configuration

Available Network Profiles

Network	Port Group	Method	IP Address	Netmask	Gateway	VLAN Tag
default	0	Static	10.4.1.121	255.255.255.0	10.4.1.1	
DATA	1	Static	10.4.2.2	255.255.255.0	10.4.2.1	
CLUSTER	2	Static	10.4.3.3	255.255.255.0	10.4.3.1	

Port Groups

☑ Enable Port Group for network traffic

MAC Addresses:
Determined after this configuration is saved...
Active MAC:
Confgured Networks:
CLUSTER: 10.4.1.3

Bond Mode

Configure which mode is used when aggregating multiple network interfaces into a bonded interface. Please verify your ethernet switch(es) support the selected mode.

○ Active-Backup (active-backup)
● Link Aggregation Control Protocol (LACP)
○ Round-robin policy (RR)
○ XOR source and destination MAC address (XOR)

Maximum Transmission Unit

Configure the ethernet frame size.

○ Standard Frame Size (MTU 1500)
○ Jumbo Frame Size (MTU 9000)
● Custom Frame Size

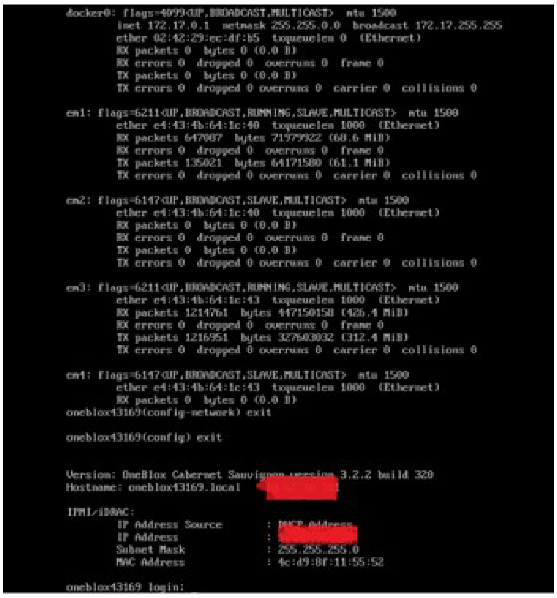
For recommended network configurations, see the following:

- How To: Properly Configure OneXafe Networking and Port Groups
- Common Tasks - Networking

Create Single Node or Multi Node Cluster

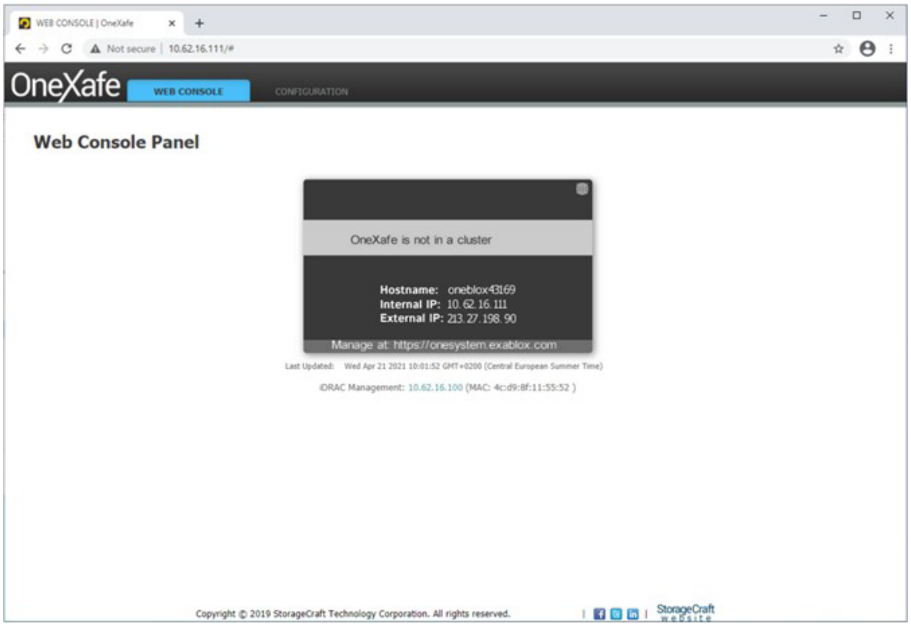
Follow these steps:

1. From the OneXafe iDRAC Console, get the IP to access OneXafe Web Console. You can perform cluster configuration and networking from the OneXafe Web Console.



```
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:29:ec:df:b5  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

em1: flags=6211<UP,BROADCAST,RUNNING,SLAVE,MULTICAST>  mtu 1500
        ether e4:43:4b:64:1c:40  txqueuelen 1000  (Ethernet)
        RX packets 647007  bytes 71979922 (68.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 135021  bytes 64171580 (61.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

em2: flags=6147<UP,BROADCAST,SLAVE,MULTICAST>  mtu 1500
        ether e4:43:4b:64:1c:40  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

em3: flags=6211<UP,BROADCAST,RUNNING,SLAVE,MULTICAST>  mtu 1500
        ether e4:43:4b:64:1c:43  txqueuelen 1000  (Ethernet)
        RX packets 1214761  bytes 447150158 (426.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1216951  bytes 327603032 (312.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

em4: flags=6147<UP,BROADCAST,SLAVE,MULTICAST>  mtu 1500
        ether e4:43:4b:64:1c:43  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
oneblox43169(config-network) exit

oneblox43169(config) exit


Version: OneBlox Cabernet Sauvi[redacted] 3.2.2 build 320
Hostname: oneblox43169.local

IPMI/iDRAC:
        IP Address Source       : [redacted]
        IP Address              :
        Subnet Mask             : 255.255.255.0
        MAC Address             : 4c:d9:8f:11:55:52

oneblox43169 login:
```

2. To open OneXafe WebConsole, go to http://<<device IP>>. The Home page opens.



Web Console Panel

OneXafe is not in a cluster

Hostname: oneblox43169
Internal IP: 10. 62. 16. 111
External IP: 213. 27. 198. 90

Manage at: https://onesystem.exablox.com

Last Updated: Wed Apr 21 2021 10:01:52 GMT+0200 (Central European Summer Time)

iDRAC Management: 10.62.16.100 (MAC: 4c:d9:8f:11:55:52)

Copyright © 2019 StorageCraft Technology Corporation. All rights reserved.

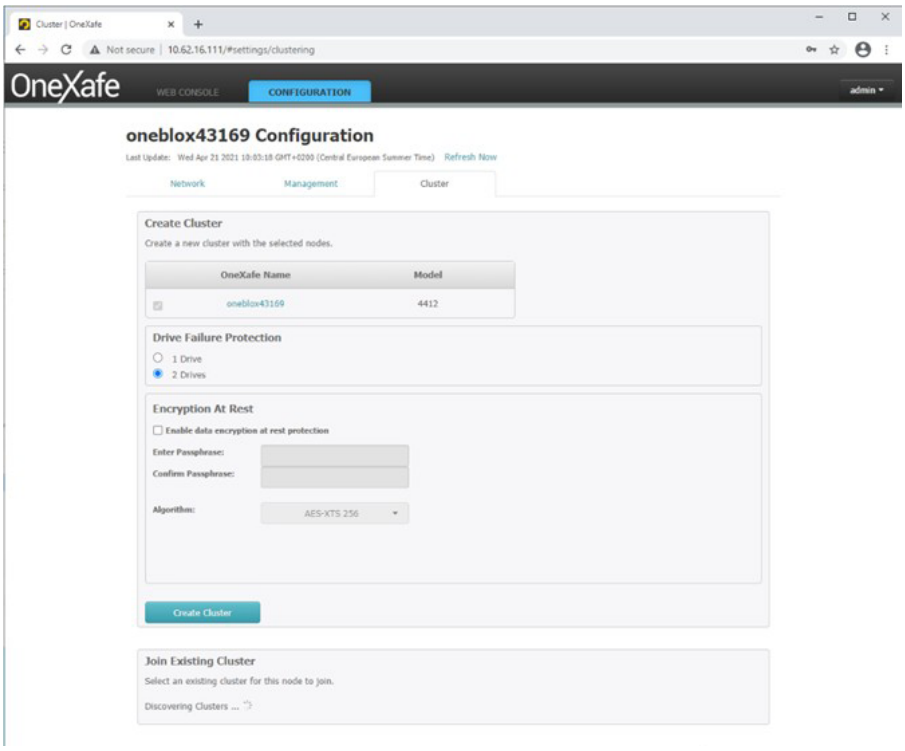
3. Click the Configuration tab, and then enter your login details.

- **Default Username:** admin
- **Default Password:** config

Note: If you have logged in for the first time, you are prompted to modify the password.

4. To create a new cluster with the selected OneXafe nodes, go to the **Configuration > Cluster** tab, and then do the following:

   a. View and select the OneXafe nodes as needed.
   b. For Drive Failure Protection, select the drives as needed.
   c. To enable Encryption At Rest, click the **Enable data encryption at rest protection** check box. Optionally, you can enable Encryption at Rest even when creating cluster.
   d. Click the **Create Cluster** button.



oneblox43169 Configuration

Last Update: Wed Apr 21 2021 10:03:18 GMT+0200 (Central European Summer Time) Refresh Now

Create Cluster

Create a new cluster with the selected nodes.

	OneXafe Name	Model
☑	oneblox43169	4412

Drive Failure Protection

○ 1 Drive
● 2 Drives

Encryption At Rest

□ Enable data encryption at rest protection

Enter Passphrase:

Confirm Passphrase:

Algorithm: AES-XTS 256

Join Existing Cluster

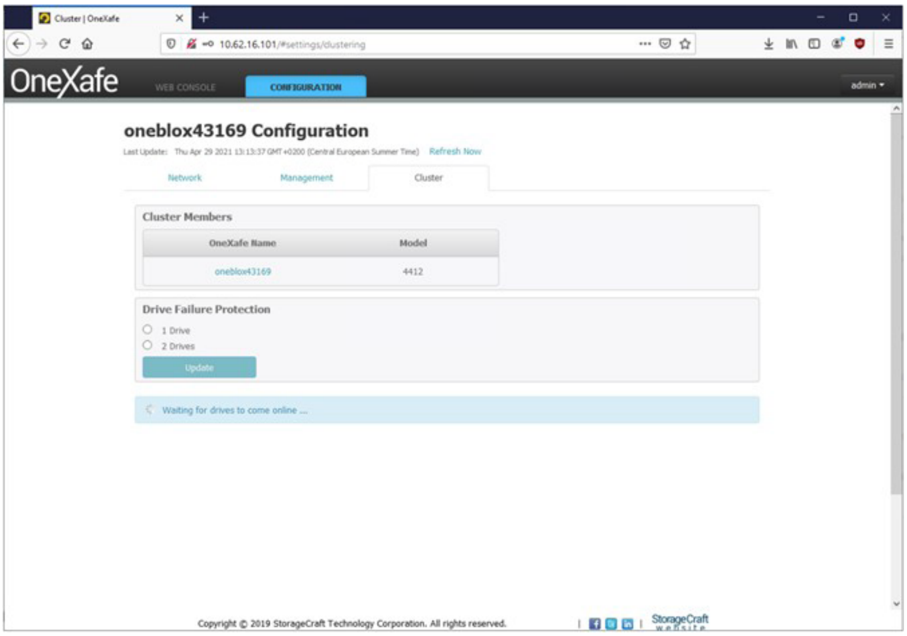
Select an existing cluster for this node to join.

Discovering Clusters ...

The following table outlines the fault domain protection of drives and nodes within a cluster:

OneBlox 4312 and 4400 Clusters	1 Drive Failure	1 Node Failure	2 Drives Failure	2 Node Failure
1 node cluster	Yes	No	Yes (Default)	No
2 node cluster	Yes	Yes (read/write depending on which node fails)	Yes (Default)	No
3 node cluster	Yes	Yes	Yes (Default)	No
4 node cluster	Yes	Yes	Yes (Default)	Yes (read/write)
5 and greater node cluster	Yes	Yes	Yes (Default)	Yes (read/write)

The cluster creation is initiated.



oneblox43169 Configuration

Last Update: Thu Apr 29 2021 13:13:37 GMT +0200 (Central European Summer Time) Refresh Now

Cluster Members

OneXafe Name	Model
oneblox43169	4412

Drive Failure Protection

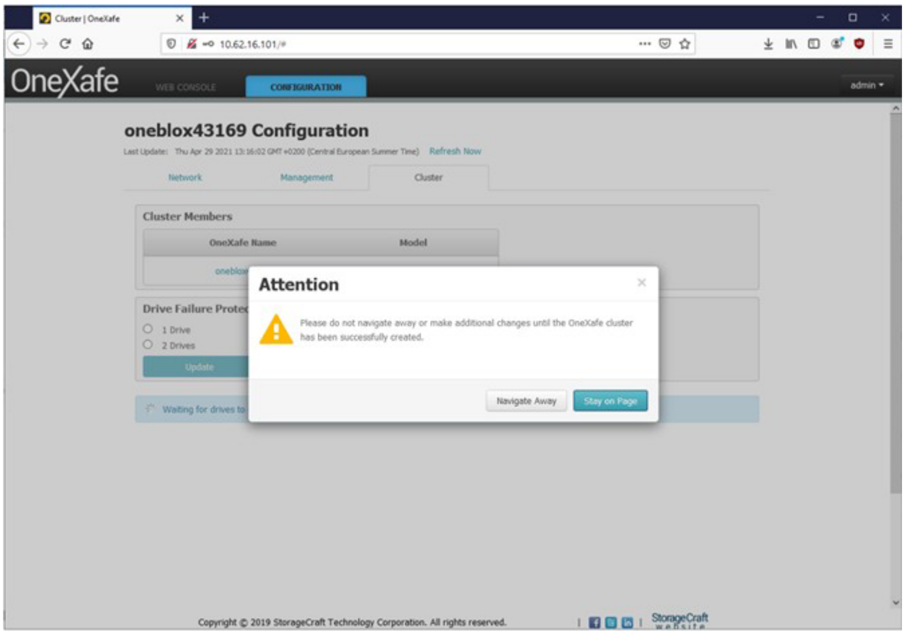
○ 1 Drive
○ 2 Drives

Waiting for drives to come online ...

Copyright © 2019 StorageCraft Technology Corporation. All rights reserved.

Note: We recommend that you stay in the page till the cluster gets created. If you try to navigate away from the screen or make additional changes, the following message gets displayed.

Create Single Node or Multi Node Cluster



oneblox43169 Configuration

Last Update: Thu Apr 29 2021 13:16:02 GMT +0200 (Central European Summer Time) Refresh Now

Cluster Members

OneXafe Name	Model
oneblox	

Drive Failure Protec

○ 1 Drive

○ 2 Drives

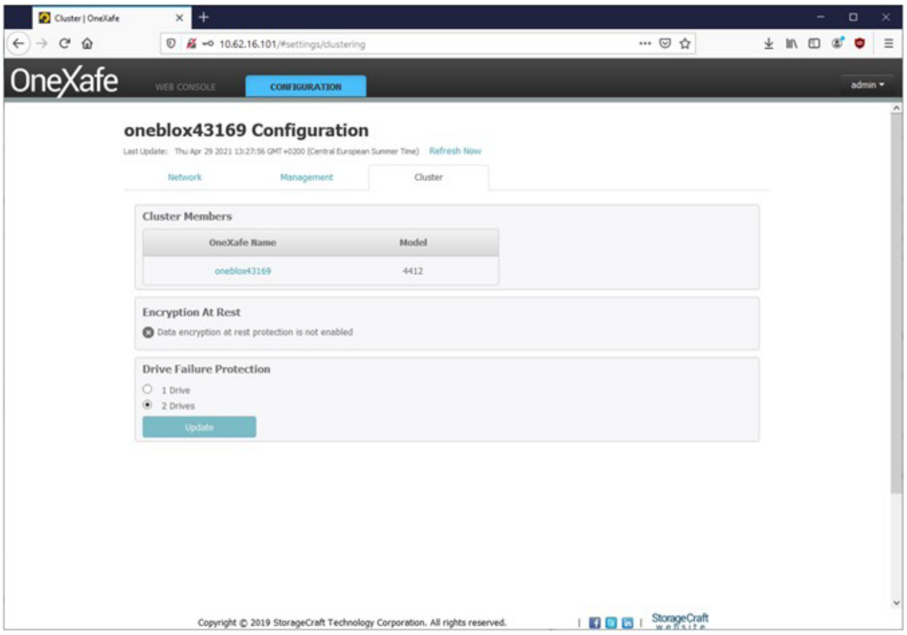
Waiting for drives to

Attention

Please do not navigate away or make additional changes until the OneXafe cluster has been successfully created.

Copyright © 2019 StorageCraft Technology Corporation. All rights reserved.

The cluster is created and ready for use.



oneblox43169 Configuration

Last Update: Thu Apr 29 2021 13:27:56 GMT +0200 (Central European Summer Time) Refresh Now

Cluster Members

OneXafe Name	Model
oneblox43169	4412

Encryption At Rest

Data encryption at rest protection is not enabled

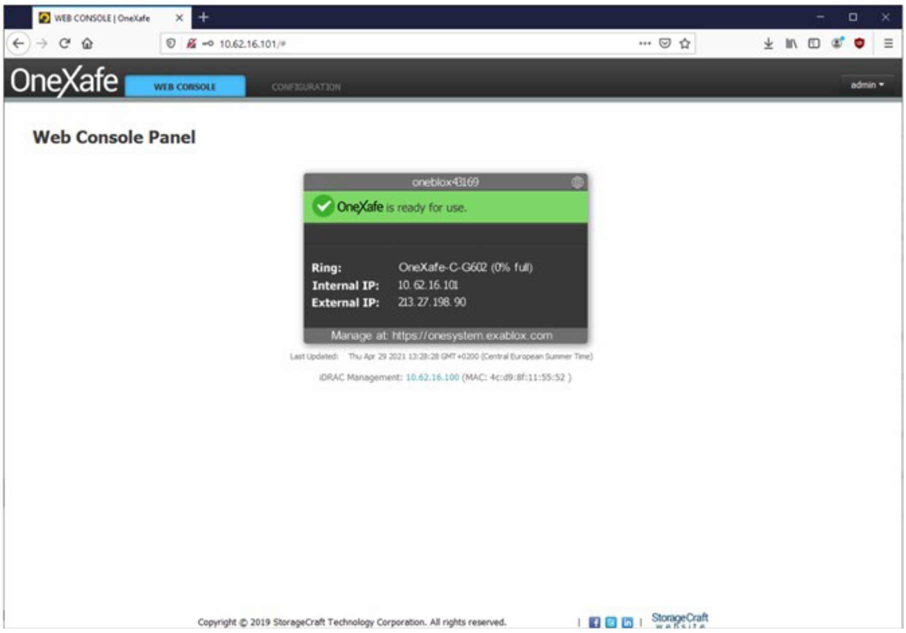
Drive Failure Protection

○ 1 Drive

● 2 Drives

Copyright © 2019 StorageCraft Technology Corporation. All rights reserved.

The status is updated in the Web Console tab.



Web Console Panel

oneblox43169

OneXafe is ready for use.

Ring: OneXafe-C-G602 (0% full)
Internal IP: 10.62.16.101
External IP: 213.27.198.90

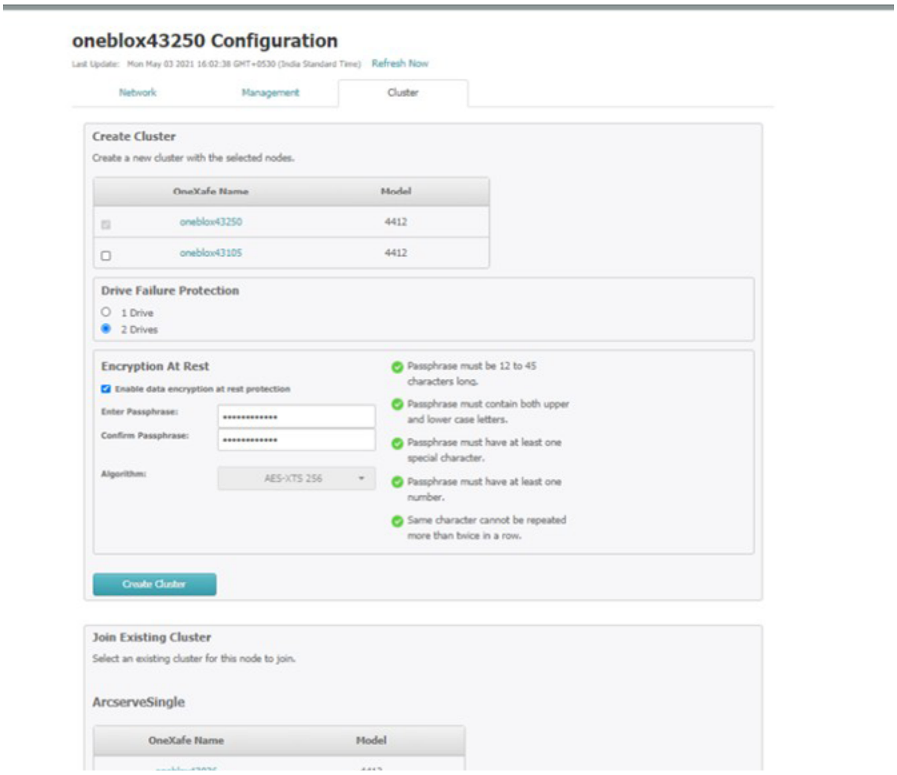
Manage at: https://onesystem.exablox.com

Last Updated: Thu Apr 29 2021 13:28:28 GMT+0200 (Central European Summer Time)

iDRAC Management: 10.62.16.100 (MAC: 4c:d9:8f:11:55:52)

Copyright © 2019 StorageCraft Technology Corporation. All rights reserved.

5. To join a second node to the Cluster, log into the second node Web Console following the steps 1 and 2, and then navigate to Configuration > Cluster.
6. Under the Join Existing Cluster section, click the Join button to add another node to the cluster.



oneblox43250 Configuration

Last Update: Mon May 03 2021 16:02:38 GMT+0530 (India Standard Time)

Create Cluster

Create a new cluster with the selected nodes.

	OneXafe Name	Model
☑	oneblox43250	4412
□	oneblox43105	4412

Drive Failure Protection

○ 1 Drive
● 2 Drives

Encryption At Rest

☑ Enable data encryption at rest protection

Enter Passphrase: *************

Confirm Passphrase: *************

Algorithm: AES-XTS 256

✓ Passphrase must be 12 to 45 characters long.
✓ Passphrase must contain both upper and lower case letters.
✓ Passphrase must have at least one special character.
✓ Passphrase must have at least one number.
✓ Same character cannot be repeated more than twice in a row.

Join Existing Cluster

Select an existing cluster for this node to join.

ArcserveSingle

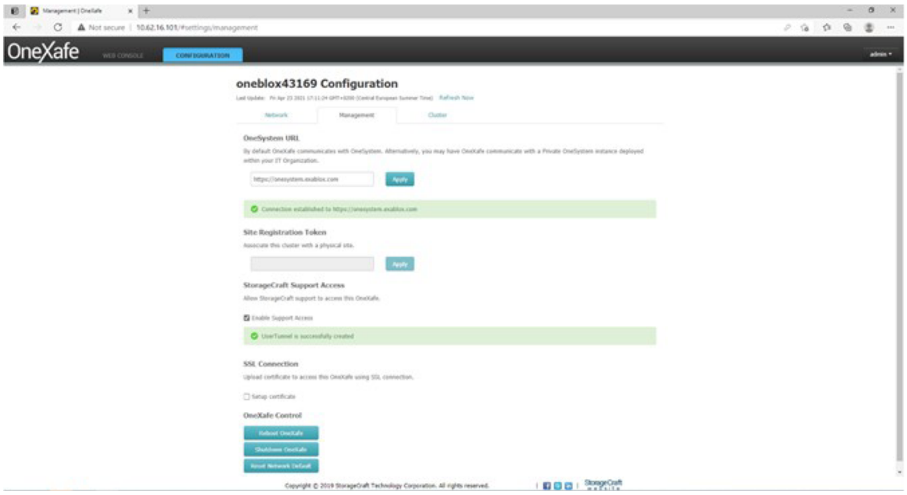
OneXafe Name	Model

7. To add a third node to the Cluster, follow steps 5 and 6.

Register OneXafe to OneSystem account

Follow these steps:

1. Log into OneXafe Web Console, and then go to the Configuration > Management tab.



oneblox43169 Configuration

Last Update: Fri Apr 23 2021 17:11:24 GMT+0200 (Central European Summer Time) Refresh Now

OneSystem URL

By default OneXafe communicates with OneSystem. Alternatively, you may have OneXafe communicate with a Private OneSystem instance deployed within your IT Organization.

https://onesystem.exablox.com

Connection established to https://onesystem.exablox.com

Site Registration Token

Associate this cluster with a physical site.

StorageCraft Support Access

Allow StorageCraft support to access this OneXafe.

☑ Enable Support Access

UserTunnel is successfully created

SSL Connection

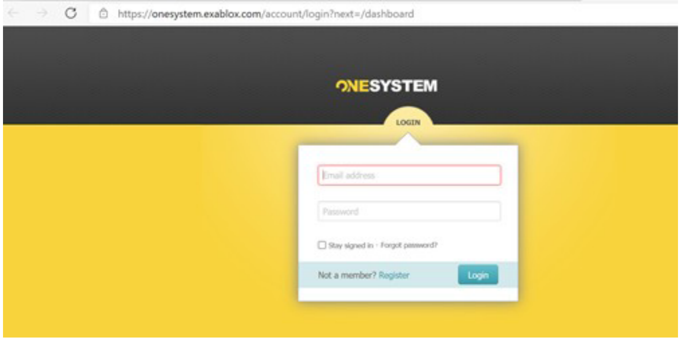
Upload certificate to access this OneXafe using SSL connection.

☐ Setup certificate

OneXafe Control

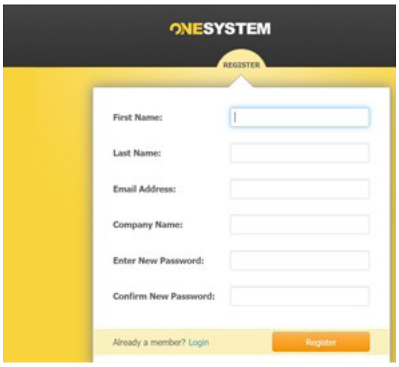
Copyright © 2019 StorageCraft Technology Corporation. All rights reserved.

2. Copy and paste the OneSystem URL (https://onesystem.exablox.com) in the new window of a browser.

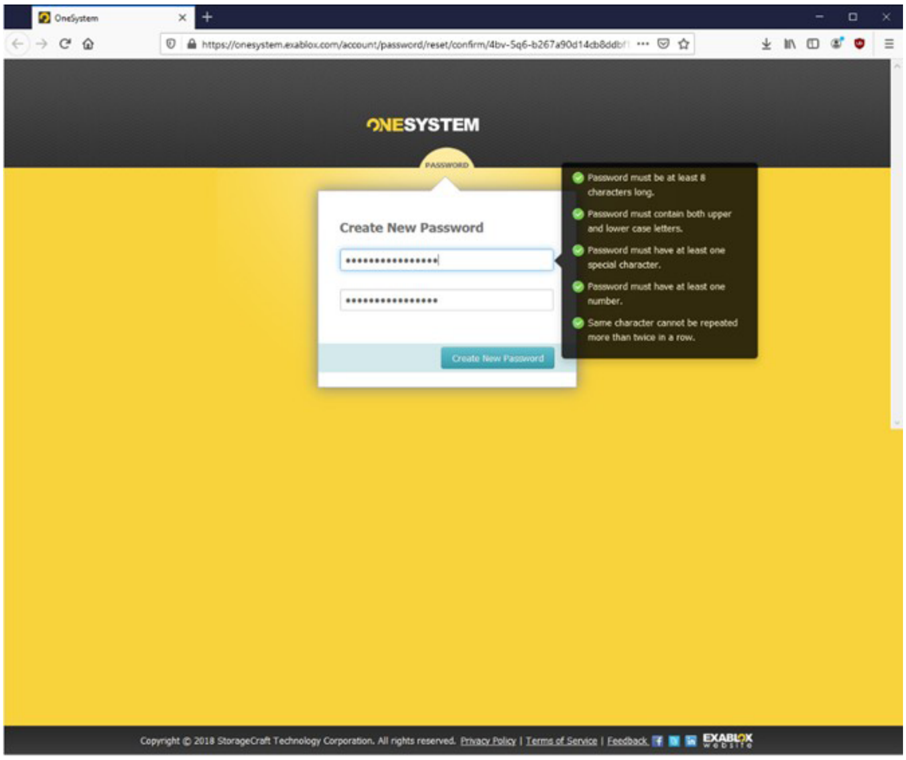


https://onesystem.exablox.com/account/login?next=/dashboard
ONESYSTEM
LOGIN
Email address
Password
☐ Stay signed in · Forgot password?
Not a member? Register
Login

3. Click the Register button, provide the details, and then click Register.



After you register, you will receive an email notification. To confirm your account and reset your password, click the link given in the email.



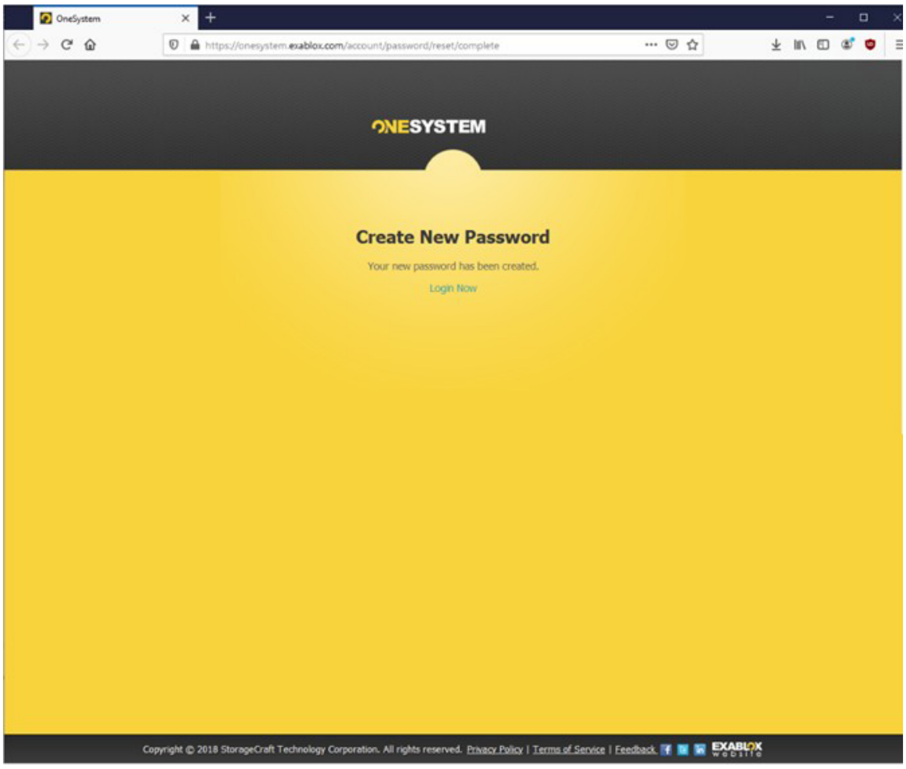
https://onesystem.exablox.com/account/password/reset/confirm/4bv-5q6-b267a90d14db8ddbf

Create New Password

- Password must be at least 8 characters long.
- Password must contain both upper and lower case letters.
- Password must have at least one special character.
- Password must have at least one number.
- Same character cannot be repeated more than twice in a row.

Copyright © 2018 StorageCraft Technology Corporation. All rights reserved. Privacy Policy | Terms of Service | Feedback

Your new password is created.



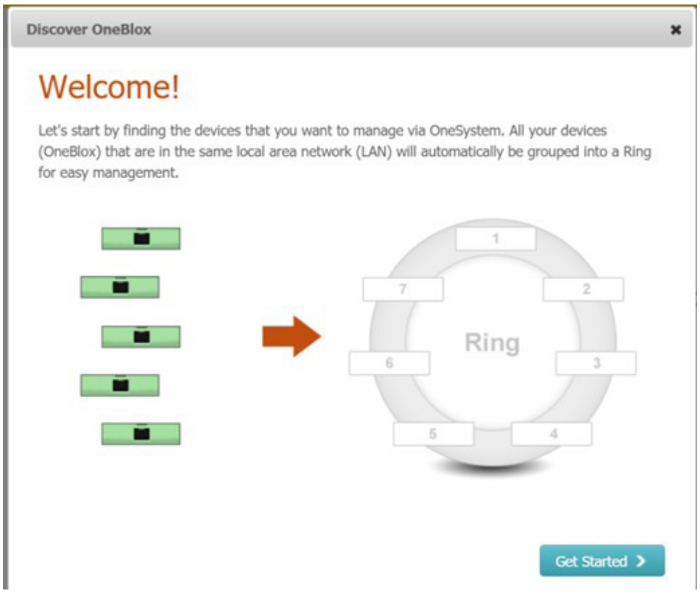
https://onesystem.exablox.com/account/password/reset/complete

Create New Password

Your new password has been created.

Copyright © 2018 StorageCraft Technology Corporation. All rights reserved. Privacy Policy | Terms of Service | Feedback

4. Using the new password, log into OneSystem.
5. On the Overview page, click Actions > Register New Rings. The Discover OneBlox screen opens.



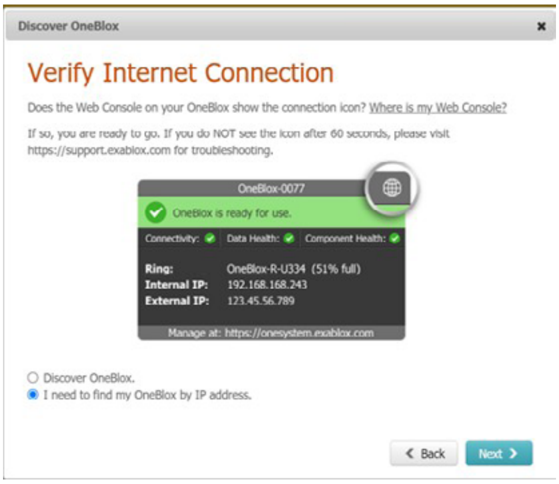
Discover OneBlox

Welcome!

Let's start by finding the devices that you want to manage via OneSystem. All your devices (OneBlox) that are in the same local area network (LAN) will automatically be grouped into a Ring for easy management.

6. To discover OneBlox, click the Get Started button.
7. To get the OneBlox discovered, select one of the following options:

- **Discover OneBlox:** Discovers OneBlox automatically.



Discover OneBlox

Verify Internet Connection

Does the Web Console on your OneBlox show the connection icon? Where is my Web Console?

If so, you are ready to go. If you do NOT see the icon after 60 seconds, please visit https://support.exablox.com for troubleshooting.

OneBlox-0077

OneBlox is ready for use.

Connectivity: ✓ Data Health: ✓ Component Health: ✓

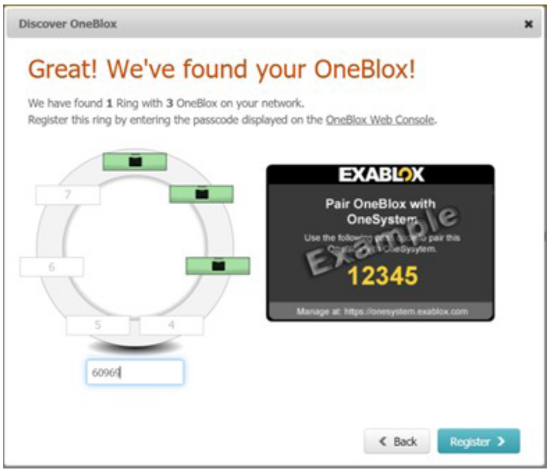
Ring: OneBlox-R-U334 (51% full)
Internal IP: 192.168.168.243
External IP: 123.45.56.789

Manage at: https://onesystem.exablox.com

○ Discover OneBlox.
● I need to find my OneBlox by IP address.

- I need to find my OneBlox by IP address: Allows you to discover OneBlox using an IP address. In the External IP Address box, type the IP address and click Next.

8. To pair OneBlox with OneSystem, retrieve the passcode and enter it in the text box. To retrieve the passcode, click the **Exablox** image.



Discover OneBlox

Great! We've found your OneBlox!

We have found **1** Ring with **3** OneBlox on your network.
Register this ring by entering the passcode displayed on the OneBlox Web Console.

EXABLOX

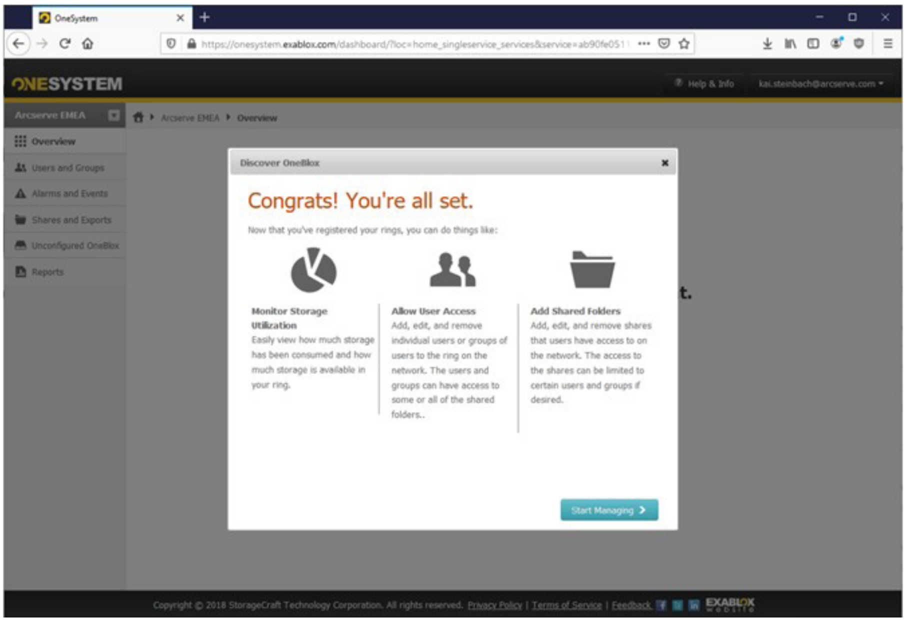
Pair OneBlox with OneSystem

12345

Manage at: https://onesystem.exablox.com

60969

9. After you type the passcode, click the Register button.



OneSystem
https://onesystem.exablox.com/dashboard/?loc=home_singleservice_services&service=ab90fe051
ONESYSTEM
Help & Info
kai.steinbach@arcserve.com
Arcserve EMEA
Overview
Users and Groups
Alarms and Events
Shares and Exports
Unconfigured OneBlox
Reports
Arcserve EMEA ▸ Overview
Start Managing ›
Copyright © 2018 StorageCraft Technology Corporation. All rights reserved. Privacy Policy | Terms of Service | Feedback
EXABLOX

Discover OneBlox

Congrats! You're all set.

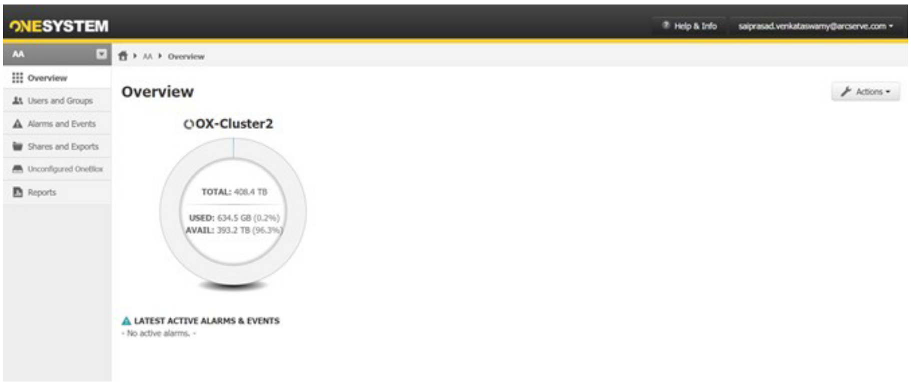
Now that you've registered your rings, you can do things like:

Monitor Storage Utilization
Easily view how much storage has been consumed and how much storage is available in your ring.

Allow User Access
Add, edit, and remove individual users or groups of users to the ring on the network. The users and groups can have access to some or all of the shared folders..

Add Shared Folders
Add, edit, and remove shares that users have access to on the network. The access to the shares can be limited to certain users and groups if desired.

OneBlox is now paired with Onesystem.



Overview

OX-Cluster2

TOTAL: 408.4 TB

USED: 634.5 GB (0.2%)
AVAIL: 393.2 TB (96.3%)

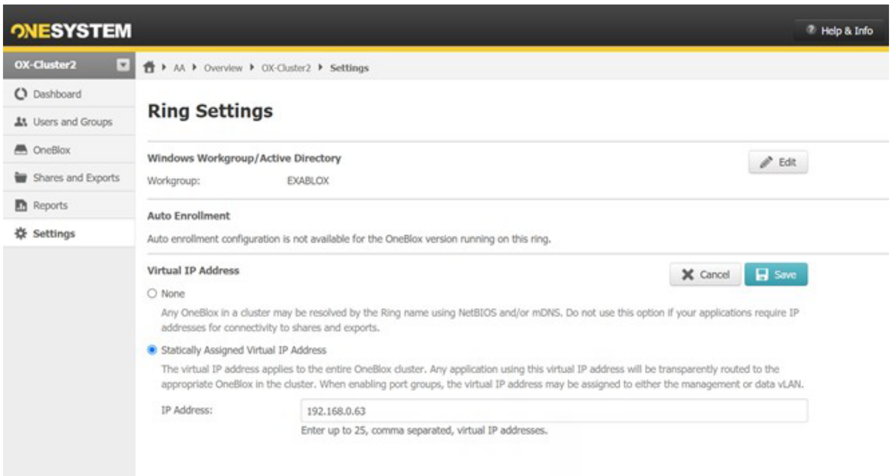
LATEST ACTIVE ALARMS & EVENTS
- No active alarms. -

Note: For more information about OneXafe, see StorageCraft OneXafe User Guide.

Configure Virtual IP of OneXafe Cluster

Follow these steps:

1. Log into the OneSystem account.
2. From the overview page, click on the corresponding OneXafe Cluster Ring.
3. To navigate to the Ring settings, click on the Settings pane.
4. Click the Edit button that is next to Virtual IP settings, assign a static IP, and then click the Save button.



Ring Settings

Windows Workgroup/Active Directory
Workgroup: EXABLOX

Auto Enrollment
Auto enrollment configuration is not available for the OneBlox version running on this ring.

Virtual IP Address

○ None
Any OneBlox in a cluster may be resolved by the Ring name using NetBIOS and/or mDNS. Do not use this option if your applications require IP addresses for connectivity to shares and exports.

● Statically Assigned Virtual IP Address
The virtual IP address applies to the entire OneBlox cluster. Any application using this virtual IP address will be transparently routed to the appropriate OneBlox in the cluster. When enabling port groups, the virtual IP address may be assigned to either the management or data vLAN.

IP Address: 192.168.0.63
Enter up to 25, comma separated, virtual IP addresses.

Note: For more information about OneXafe, see StorageCraft OneXafe User Guide.

Chapter 3: Configuring UDP and OneXafe to Achieve Immutable Storage for Backups

This section provides information about how to configure UDP and OneXafe to make UDP recovery point data immutable and the steps to be followed for data recovery in case of ransomware attacks.

OneXafe File System is based on an Immutable Object Store where objects are written only once and never modified. Hence, the objects are never over-written “in place” unlike many file systems.

Any client modification to file system data always results in new objects, even if they are existing objects that are being modified. Each object is also encrypted and protected by cryptographic hashes and form a Merkle tree (like a block-chain). The data of the object is always validated when read back to ensure immutability. Snapshots involve simply noting down the root hash of the tree and can be taken instantaneously. So snapshots are the view of the file system at the instant when that snapshot is taken. It freezes the file system and as the underlying objects pointed by snapshots are “immutable” and cannot be changed, the snapshot inherits this “immutability.” It cannot be changed or modified by an external source.

Snapshots make the objects, thus making the File System available, which allows it to go back to specific points in time, easily guaranteeing the immutability of objects and, therefore, the underlying data.

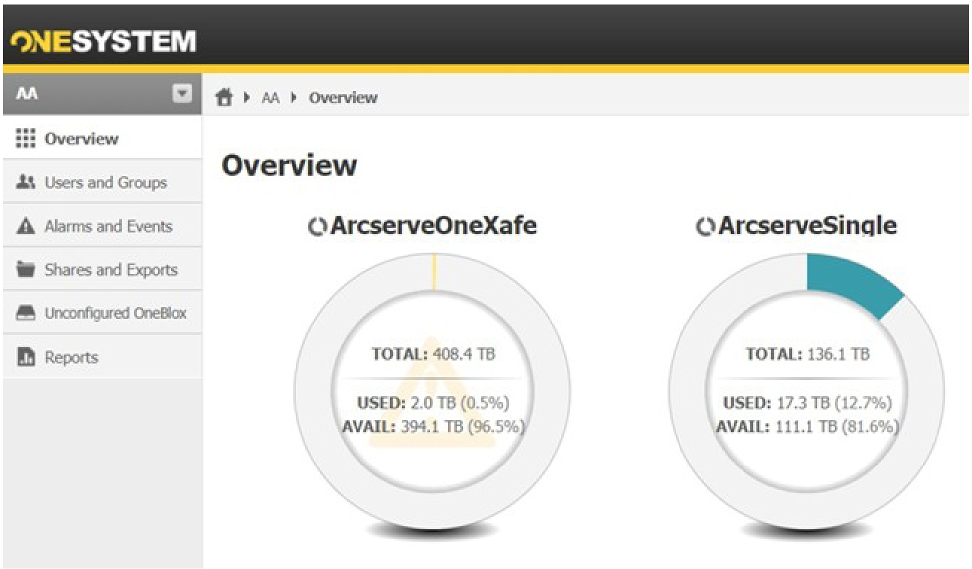
- Create SMB Shares on OneXafe Storage System
- Recover from a Ransomware Attack
- Required Credentials during Recovery
- Promote a OneXafe Snapshot to a New Share
- Import Dedupe Datastore to UDP
- Known Limitations

Create SMB Shares on OneXafe Storage System

This section provides information about how to create SMB shares on OneXafe Storage System.

Follow these steps:

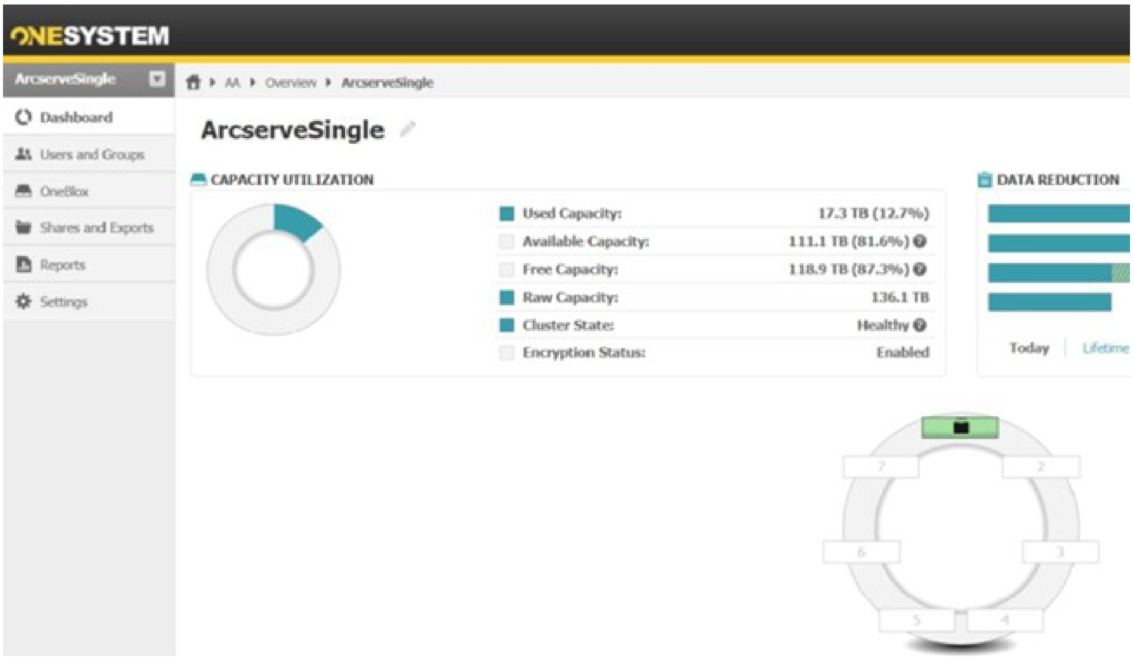
1. Log into the OneSystem account that manages the OneXafe system.
2. On the Overview page, click on the corresponding ring.



ArcserveOneXafe
TOTAL: 408.4 TB
USED: 2.0 TB (0.5%)
AVAIL: 394.1 TB (96.5%)

ArcserveSingle
TOTAL: 136.1 TB
USED: 17.3 TB (12.7%)
AVAIL: 111.1 TB (81.6%)

The Dashboard page for the selected ring opens.



ArcserveSingle

CAPACITY UTILIZATION

Used Capacity:	17.3 TB (12.7%)
Available Capacity:	111.1 TB (81.6%)
Free Capacity:	118.9 TB (87.3%)
Raw Capacity:	136.1 TB
Cluster State:	Healthy
Encryption Status:	Enabled

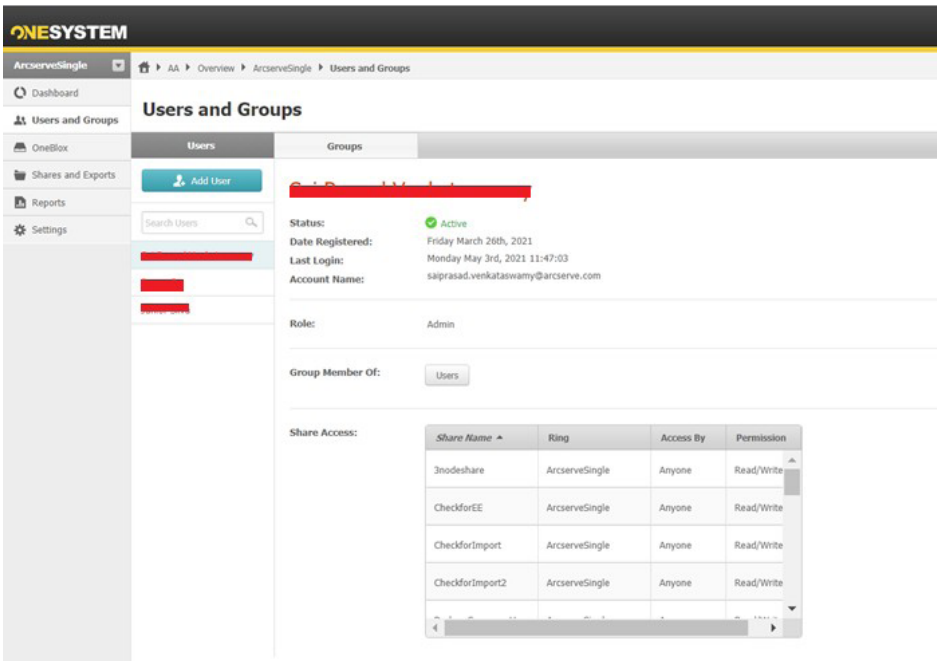
3. To create users with different permission levels that are specific to OneSystem, click **User and Groups**. You can use the same users for the OneXafe Share access permissions.

Note: By default, all the users in the Active Directory (AD) have access to the OneXafe shares. Hence, we recommend to follow Microsoft Best Practices for Securing Active Directory.

Restricted to AD, users will have the access policy applied to all SMB shares within the OneXafe cluster. This will create a share that is read/write accessible to all registered AD Users in your organization. Now any Domain Admin or Delegated AD Admin may change the permissions or ACLs within the share as desired (see “Active Directory Users and Computers”).

If OneXafe is only used as a backup target and not for general file sharing purposes, we recommend that you do not join the OneXafe system with Active Directory (AD). Apply this measure to add more separation for your data protection infrastructure in case the Active Directory is compromised.

Delegate admins, users, and/or groups may be added to the share if desired. This will give explicit AD ACL control to the members listed.



Users and Groups

[redacted]

[redacted]

[redacted]

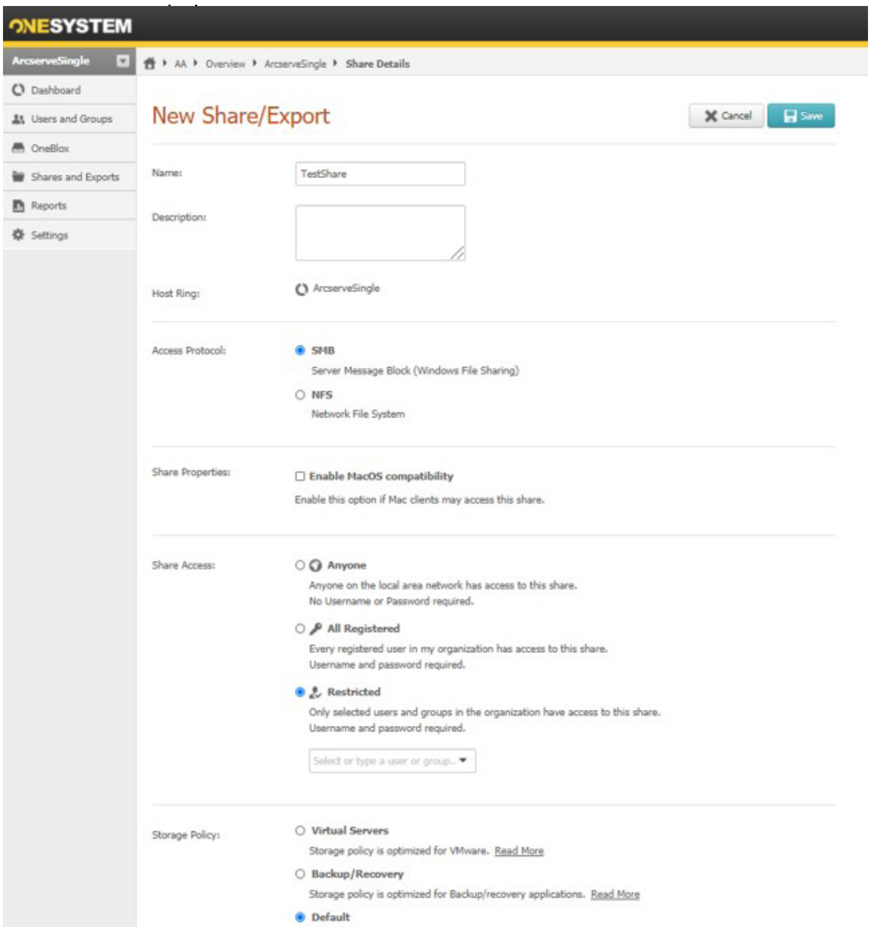
[redacted]

Status:	✓ Active
Date Registered:	Friday March 26th, 2021
Last Login:	Monday May 3rd, 2021 11:47:03
Account Name:	saiprasad.venkataswamy@arcserve.com
Role:	Admin
Group Member Of:	Users

Share Access:

Share Name	Ring	Access By	Permission
3nodeshare	ArcserveSingle	Anyone	Read/Write
CheckforEE	ArcserveSingle	Anyone	Read/Write
CheckforImport	ArcserveSingle	Anyone	Read/Write
CheckforImport2	ArcserveSingle	Anyone	Read/Write

4. Click **Shares and Exports**, and the click the **Add** button.
5. On the New Share/Export screen, for Access Protocol, select **SMB**.
6. To provide the read-write access to a specific user, for Share Access, select **Restricted**, and then select or type a user or



New Share/Export

Name: TestShare

Description:

Host Ring: ArcserveSingle

Access Protocol:
● SMB
Server Message Block (Windows File Sharing)
○ NFS
Network File System

Share Properties:
☐ Enable MacOS compatibility
Enable this option if Mac clients may access this share.

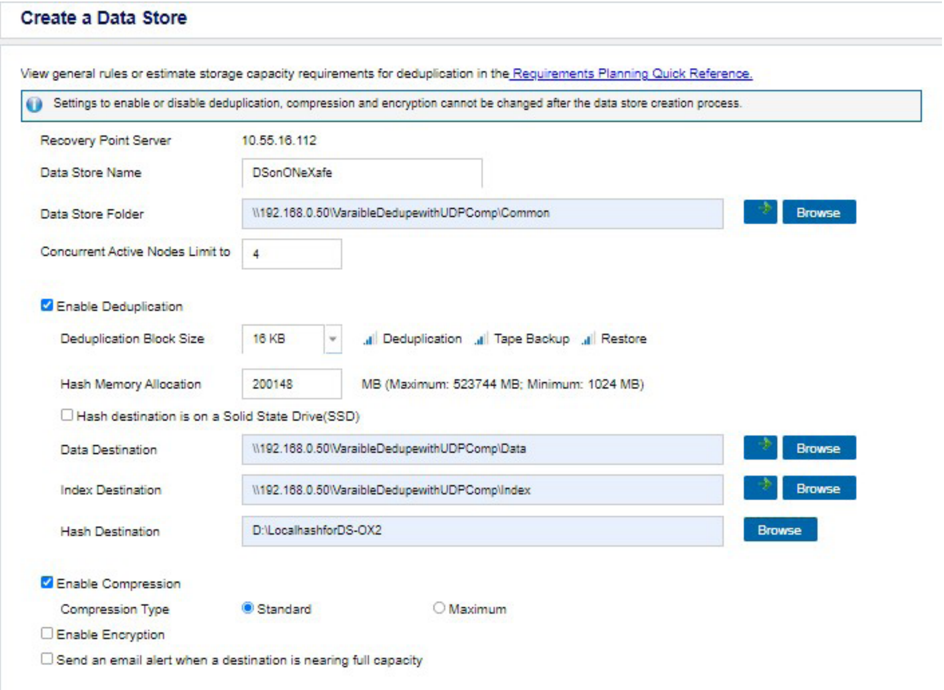
Share Access:
○ Anyone
Anyone on the local area network has access to this share.
No Username or Password required.
○ All Registered
Every registered user in my organization has access to this share.
Username and password required.
● Restricted
Only selected users and groups in the organization have access to this share.
Username and password required.
Select or type a user or group... ▾

Storage Policy:
○ Virtual Servers
Storage policy is optimized for VMware. Read More
○ Backup/Recovery
Storage policy is optimized for Backup/recovery applications. Read More
● Default

Create UDP Dedupe Datastore

Before you perform the steps given in this section, log into the UDP Console, and then make sure to do the following.

- For Deduplication Block Size, select 64 KB, and then provide a local folder path for Hash path.
- Make sure all the remaining paths for the Dedupe datastore such as Datastore Folder, Data Destination and Index Destination reside on OneXafe Cluster.
- Make sure to provide the share path using OneXafe Cluster Virtual IP. The virtual IP of OneXafe Cluster is independent of a ny node ip of the cluster and make the share high available.



Create a Data Store

View general rules or estimate storage capacity requirements for deduplication in the Requirements Planning Quick Reference.

Settings to enable or disable deduplication, compression and encryption cannot be changed after the data store creation process.

Recovery Point Server: 10.55.16.112

Data Store Name: DSonONeXafe

Data Store Folder: \\192.168.0.50\VaraibleDedupewithUDPComp\Common

Concurrent Active Nodes Limit to: 4

☑ Enable Deduplication

Deduplication Block Size: 16 KB

Hash Memory Allocation: 200148 MB (Maximum: 523744 MB; Minimum: 1024 MB)

□ Hash destination is on a Solid State Drive(SSD)

Data Destination: \\192.168.0.50\VaraibleDedupewithUDPComp\Data

Index Destination: \\192.168.0.50\VaraibleDedupewithUDPComp\Index

Hash Destination: D:\LocalhashforDS-OX2

☑ Enable Compression

Compression Type: ● Standard ○ Maximum

□ Enable Encryption

□ Send an email alert when a destination is nearing full capacity

Add a Data Store

To create a destination, the recovery point server needs data stores. The data store specifies where the backup data is stored. You can add multiple data stores to an RPS.

Follow these steps:

1. Click the resources tab.
2. From the left pane, navigate to Destinations and click Recovery Point Servers. The Destinations: Recovery Point Servers page is displayed.
3. Perform one of the following actions:
   - Right-click a recovery point server.
   - Select a recovery point server, and from the center pane, click the Actions drop-down list.

A list of options is displayed.

4. Click Add a Data Store.

The Create a Data Store page is displayed with the name of the specified recovery point server.

5. Specify the following fields and click Save.

Recovery Point Server

Defines the recovery point server where the data store is created. The recovery point server is already added by default.

Data Store Name

Defines the name of the data store.

Data Store Folder

Defines the location of the folder where the data store is created. Click Browse to select the destination folder.

Concurrent Active Nodes Limit to

Specifies the maximum concurrent jobs on the data store.

Default Value: 4

Refers to a value from 1 to 9999. The value indicates the number of jobs that can concurrently run. If the running jobs meet the number, another job is placed in to the queue and job can only start when one of the running job completes. The completed job could mean a finished, canceled, or a failed job.

The number applies to the Job Types but not to the Server nodes. For example, number 5 indicates that five backup jobs are running. Any job scheduled after five backup jobs waits in the queue, but you can submit another job such as File System Catalog.

If the value is more than 16 or 32, messages are displayed to warn about the increased demand on hardware.

Note: Limit to number only impacts the replication outbound job, not the replication inbound job. Limit to number does not impact the Restore or BMR jobs. Such jobs are not placed in a queue.

Enable Deduplication

Specifies that deduplication is enabled for this data store. Arcserve UDP supports both types of deduplication: Source-side deduplication and Global deduplication. Source-side deduplication prevents duplicate data blocks to move across network from a particular agent. Global deduplication eliminates duplicate data across all client machines based on the volume cluster level.

Deduplication Block Size

Defines the deduplication block size. The options are 4 KB, 8 KB, 16 KB, 32 KB, and 64 KB. The deduplication block size also impacts the Deduplication capacity estimation. For example, if you change the default 16 KB to 32 KB, the Deduplication capacity estimations double. Increasing the deduplication block size can decrease the deduplication percentage.

Hash Memory Allocation

Specifies the amount of physical memory that you allocate to keep hashes. This field is pre-filled with a default value. The default value is based on the following calculation:

If the physical memory of the RPS is smaller than 4 GB (or is identical to 4 GB), the default value of **Hash Memory Allocation** is identical to the physical memory of the RPS.

If the physical memory of the RPS is greater than 4 GB, Arcserve UDP calculates the available free memory at this time. Assume that the available free memory is X GB at present. Arcserve UDP further checks the following conditions:

- If (X * 80%) > = 4 GB, the default value of **Hash Memory Allocation** is (X * 80%).
- If (X * 80%) < 4 GB, the default value of **Hash Memory Allocation** is 4 GB.

Example: Consider the RPS has 32 GB of physical memory. Assume that operating system and other applications use 4 GB memory while creating the data store. So, the available free memory at this time is 28 GB. Then, the default value of **Hash Memory Allocation** is 22.4 GB (22.4 GB = 28 GB * 80%).

Hash Destination is on a Solid State Drive (SSD)

Specifies if the hash folder is on a solid state drive.

Note: Configure the hash destination on local SSD, if the Hash destination is on a Solid State Drive(SSD) option is enabled.

Data Destination

Defines the data destination folder to save the actual unique data blocks. Use the largest disk to store data as that contains the original data blocks of source.

Note: The Data Destination path should be a blank folder.

Index Destination

Defines the index destination folder to store the index files. Choose a different disk to improve the deduplication processing.

Note: The Index Destination path should be a blank folder.

Hash Destination

Defines the path to store the hash database. Arcserve UDP uses the SHA1 algorithm to generate the hash for source data. The hash values are managed by the hash database. Selecting a high speed Solid State Drive (SSD) increases the deduplication capacity and requires a lower memory allocation. For better hash performance, we recommend to format the SSD volume as NTFS file system with 4KB volume cluster size.

Note: The Hash Destination path should be an empty folder.

Note: You cannot specify the same path for the following four folders: Data Store folder, Data Destination, Index Destination, and Hash Destination.

Enable Compression

Specifies that the data compression settings are enabled.

Compression Type

Specifies whether to use the standard or maximum compression type.

Compression is often selected to decrease the usage of the disk space, but also has an inverse impact on your backup speed due to the increased CPU usage. Based on your requirement, you can select one of the three available options.

Note: For more information, see Compression Type.

Enable Encryption

Specifies that encryption settings are enabled. When you select this option, you must specify and confirm the encryption password.

Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. The Arcserve UDP solution uses secure, AES (Advanced Encryption Standard) encryption algorithms to achieve maximum security and privacy of your data. For data stores, encryption or No encryption is supported. For Encryption, only AES-256 is available.

A password is not required when you are attempting to restore to the computer from which the backup was performed. However, when you attempt to restore to a different computer, a password is required. By default, only for the first login password is required. To enter password even after the first login, the administrator needs to manually stop Arcserve UDP Agent Explorer Extension Service.

Send an email alert when a destination is nearing full capacity

Selecting this option configures the data store to send email alert. RPS sends out email alerts to recipients when data store destination folder is nearing full capacity.

Configure Email

This button appears only when you enable the option of Send an email alert when a destination is nearing full capacity. The button helps you provide as email ID to receive alerts. Click the Configure Email button to load global email alert settings from Console>Settings>Email and Alert configuration. If global Email settings is not available, clicking the Configure Email button opens Email settings dialog to set email details.

The data store is created and gets displayed on the center pane. Click the data store to view the details in the right pane.

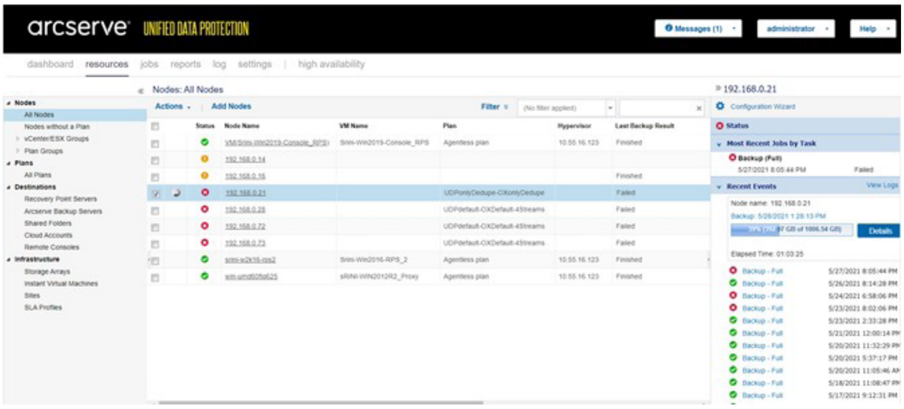
Recover from a Ransomware Attack

In case of a ransomware attack or any breach on the Arcserve UDP Recovery Point Server, there may be a backup recovery point data loss. Hence, we recommend you to perform the following:

- A fresh installation of Windows.
- Create a new password
- A fresh installation of UDP.
- Identify the valid snapshot, and then promote the snapshot as a new share.

To identify valid snapshots, do the following:

1. Identify the right time from Arcserve UDP activity log
    a. Log into the UDP console, and then click All nodes.
    b. Select the node that has backups scheduled to destinations residing on OneXafe SMB share.
    c. On the right panel, click the specific backup job.



Nodes: All Nodes

Status	Node Name	VM Name	Plan	Hypervisor	Last Backup Result
✓	VM(Srini-Win2019-Console_RPS)	Srini-Win2019-Console_RPS	Agentless plan	10.55.16.123	Finished
!	192.168.0.14				
!	192.168.0.16				Finished
⊘	192.168.0.21		UDPonlyDedupe-OXonlyDedupe		Failed
⊘	192.168.0.28		UDPdefault-OXDefault-4Streams		Failed
⊘	192.168.0.72		UDPdefault-OXDefault-4Streams		Failed
⊘	192.168.0.73		UDPdefault-OXDefault-4Streams		Failed
✓	srini-w2k16-rps2	Srini-Win2016-RPS_2	Agentless plan	10.55.16.123	Finished
✓	sin-umd60fq625	sRINI-WIN2012R2_Proxy	Agentless plan	10.55.16.123	Finished

192.168.0.21

Status

Most Recent Jobs by Task

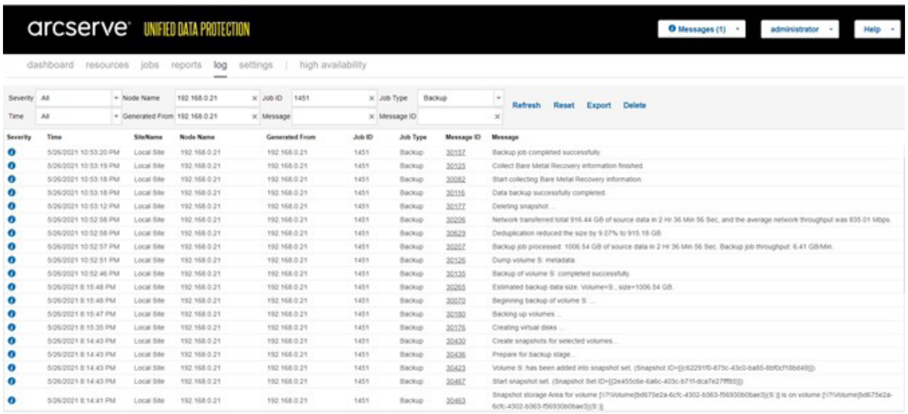
Backup (Full) 5/27/2021 8:05:44 PM Failed

Recent Events

Node name: 192.168.0.21
Backup: 5/28/2021 1:28:13 PM
39% (392.97 GB of 1006.54 GB)
Elapsed Time: 01:03:25

⊘	Backup - Full	5/27/2021 8:05:44 PM
✓	Backup - Full	5/26/2021 8:14:28 PM
⊘	Backup - Full	5/24/2021 6:58:06 PM
⊘	Backup - Full	5/23/2021 8:02:06 PM
✓	Backup - Full	5/23/2021 2:33:28 PM
✓	Backup - Full	5/21/2021 12:00:14 PM
✓	Backup - Full	5/20/2021 11:32:29 PM
✓	Backup - Full	5/20/2021 5:37:17 PM
✓	Backup - Full	5/20/2021 11:05:46 AM
✓	Backup - Full	5/18/2021 11:08:47 PM
✓	Backup - Full	5/17/2021 9:12:31 PM

Make a note of the job completion time for any successful UDP backup job.



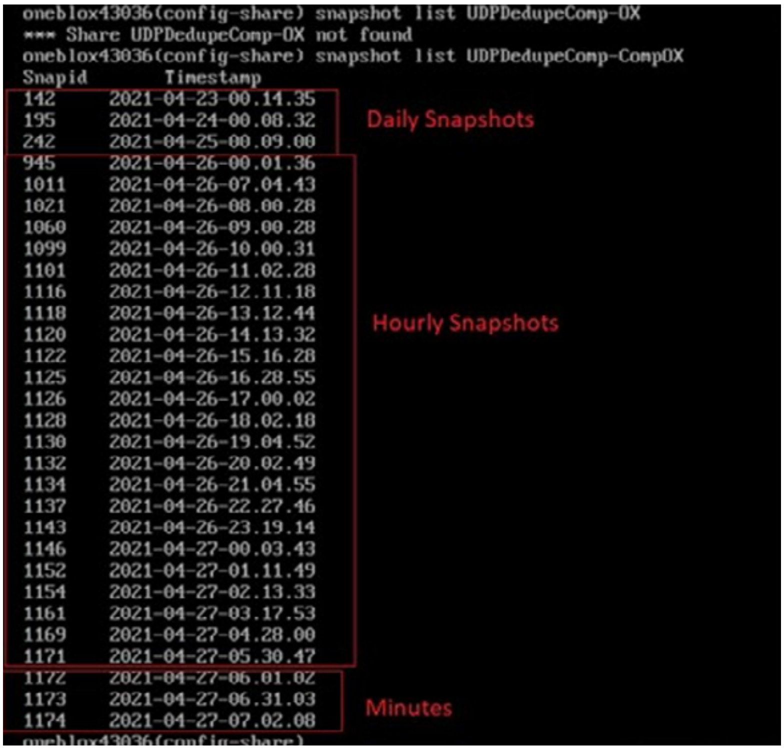
Severity: All; Node Name: 192.168.0.21; Job ID: 1451; Job Type: Backup
Time: All; Generated From: 192.168.0.21; Message: ; Message ID:

Severity	Time	SiteName	Node Name	Generated From	Job ID	Job Type	Message ID	Message
i	5/26/2021 10:53:20 PM	Local Site	192.168.0.21	192.168.0.21	1451	Backup	30157	Backup job completed successfully.
i	5/26/2021 10:53:19 PM	Local Site	192.168.0.21	192.168.0.21	1451	Backup	30125	Collect Bare Metal Recovery information finished.
i	5/26/2021 10:53:18 PM	Local Site	192.168.0.21	192.168.0.21	1451	Backup	30082	Start collecting Bare Metal Recovery information.
i	5/26/2021 10:53:18 PM	Local Site	192.168.0.21	192.168.0.21	1451	Backup	30116	Data backup successfully completed.
i	5/26/2021 10:53:12 PM	Local Site	192.168.0.21	192.168.0.21	1451	Backup	30177	Deleting snapshot ...
i	5/26/2021 10:52:58 PM	Local Site	192.168.0.21	192.168.0.21	1451	Backup	30206	Network transferred total 916.44 GB of source data in 2 Hr 36 Min 56 Sec, and the average network throughput was 835.01 Mbps.
i	5/26/2021 10:52:58 PM	Local Site	192.168.0.21	192.168.0.21	1451	Backup	30629	Deduplication reduced the size by 9.07% to 915.18 GB.
i	5/26/2021 10:52:57 PM	Local Site	192.168.0.21	192.168.0.21	1451	Backup	30207	Backup job processed: 1006.54 GB of source data in 2 Hr 36 Min 56 Sec. Backup job throughput: 6.41 GB/Min.
i	5/26/2021 10:52:51 PM	Local Site	192.168.0.21	192.168.0.21	1451	Backup	30126	Dump volume S: metadata.
i	5/26/2021 10:52:46 PM	Local Site	192.168.0.21	192.168.0.21	1451	Backup	30135	Backup of volume S: completed successfully.
i	5/26/2021 8:15:48 PM	Local Site	192.168.0.21	192.168.0.21	1451	Backup	30265	Estimated backup data size: Volume=S:, size=1006.54 GB.
i	5/26/2021 8:15:48 PM	Local Site	192.168.0.21	192.168.0.21	1451	Backup	30070	Beginning backup of volume S: ...
i	5/26/2021 8:15:47 PM	Local Site	192.168.0.21	192.168.0.21	1451	Backup	30180	Backing up volumes ...
i	5/26/2021 8:15:35 PM	Local Site	192.168.0.21	192.168.0.21	1451	Backup	30176	Creating virtual disks ...
i	5/26/2021 8:14:43 PM	Local Site	192.168.0.21	192.168.0.21	1451	Backup	30430	Create snapshots for selected volumes...
i	5/26/2021 8:14:43 PM	Local Site	192.168.0.21	192.168.0.21	1451	Backup	30436	Prepare for backup stage...
i	5/26/2021 8:14:43 PM	Local Site	192.168.0.21	192.168.0.21	1451	Backup	30423	Volume S: has been added into snapshot set. (Snapshot ID={{c62291f0-875c-43c0-ba85-8bf0cf18b649}})
i	5/26/2021 8:14:43 PM	Local Site	192.168.0.21	192.168.0.21	1451	Backup	30467	Start snapshot set. (Snapshot Set ID={{2e455c6e-6a6c-403c-b71f-dca7e27fff85}})
i	5/26/2021 8:14:41 PM	Local Site	192.168.0.21	192.168.0.21	1451	Backup	30453	Snapshot storage Area for volume [\\?\Volume{bd675e2a-6cfc-4302-b363-f56930b0bae3}(S:)] is on volume [\\?\Volume{bd675e2a-6cfc-4302-b363-f56930b0bae3}(S:)]

2. Identify the right snapshot in the OneXafe UI based on the UDP job completion time.

To retrieve a list of the snapshot, do the following:

1. Log into the OneXafe console, and then run the following commands:.
   Share
   Snapshot list <<sharename>>



```
oneblox43036(config-share) snapshot list UDPDedupeComp-OX
*** Share UDPDedupeComp-OX not found
oneblox43036(config-share) snapshot list UDPDedupeComp-CompOX
Snapid        Timestamp
142       2021-04-23-00.14.35
195       2021-04-24-00.08.32
242       2021-04-25-00.09.00
945       2021-04-26-00.01.36
1011      2021-04-26-07.04.43
1021      2021-04-26-08.00.28
1060      2021-04-26-09.00.28
1099      2021-04-26-10.00.31
1101      2021-04-26-11.02.28
1116      2021-04-26-12.11.18
1118      2021-04-26-13.12.44
1120      2021-04-26-14.13.32
1122      2021-04-26-15.16.28
1125      2021-04-26-16.28.55
1126      2021-04-26-17.00.02
1128      2021-04-26-18.02.18
1130      2021-04-26-19.04.52
1132      2021-04-26-20.02.49
1134      2021-04-26-21.04.55
1137      2021-04-26-22.27.46
1143      2021-04-26-23.19.14
1146      2021-04-27-00.03.43
1152      2021-04-27-01.11.49
1154      2021-04-27-02.13.33
1161      2021-04-27-03.17.53
1169      2021-04-27-04.28.00
1171      2021-04-27-05.30.47
1172      2021-04-27-06.01.02
1173      2021-04-27-06.31.03
1174      2021-04-27-07.02.08
oneblox43036(config-share)
```

2. Pick the OneXafe snapshot that was created after the last successful backup on UDP side.

Required Credentials during Recovery

Make sure to keep credentials for the following ready in case of recovery:

- OneXafe iDRAC
- OneXafe Local admin account (command line)
- OneSystem admin account (for management)
- Onesystem user account (for RPS datastore access)
- UDP system- Windows admin and IPMI
- UDP RPS datastore encryption password (if used)
- UDP Plan passwords (if used)

Promote a OneXafe Snapshot to a New Share

To promote a OneXafe snapshot to a new share, use the following commands:

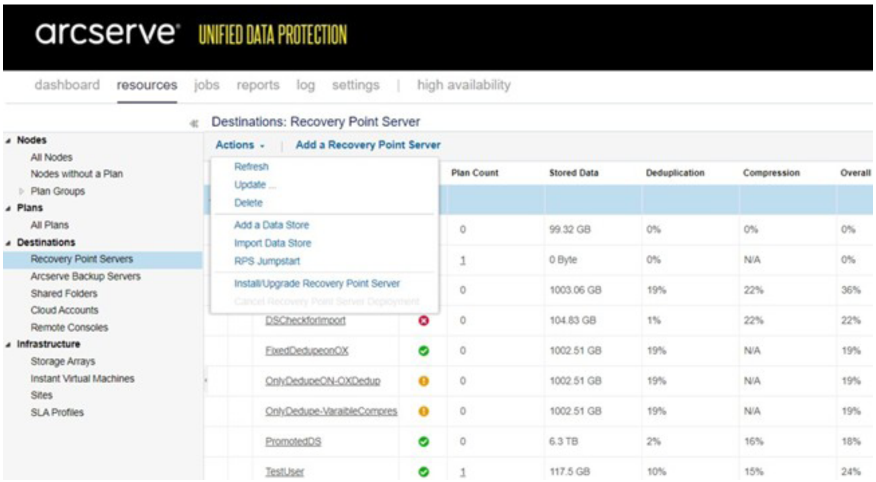
```
oneblox43005(config-share) enable
oneblox43005(config-share) snapshot list <<share name>>
oneblox43005(config-share) snapshot promote <<old sharename>> <<snapshotid>>
<<new sharename>>
oneblox43005(config-share) update <<new sharename>> -writeable
oneblox43005(config-share) disable
```

Import Dedupe Datastore to UDP

This section provides information about how to import a dedupe datastore to UDP.

Follow these steps:

1. Log into the UDP console.
2. From the resources tab, under Destinations, click **Recovery Point Servers**.
3. From the Actions drop-down list, select **Import Data Store**.

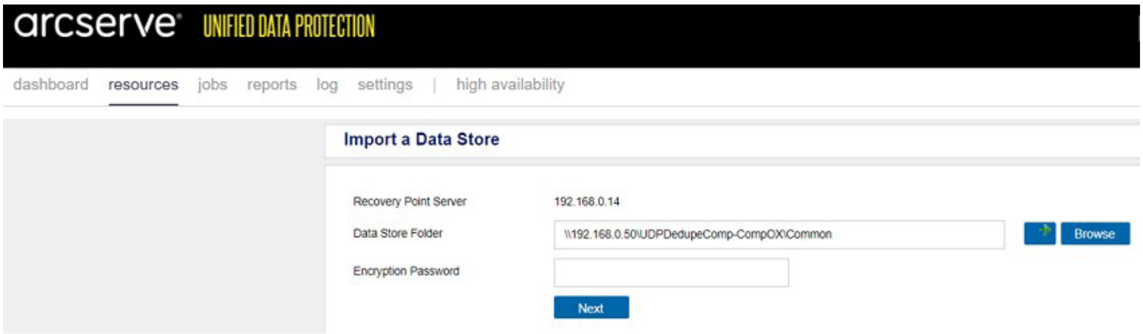


Destinations: Recovery Point Server

		Plan Count	Stored Data	Deduplication	Compression	Overall
		0	99.32 GB	0%	0%	0%
		1	0 Byte	0%	N/A	0%
		0	1003.06 GB	19%	22%	36%
DSCheckforImport	⊗	0	104.83 GB	1%	22%	22%
FixedDedupeonOX	✓	0	1002.51 GB	19%	N/A	19%
OnlyDedupeON-OXDedup	!	0	1002.51 GB	19%	N/A	19%
OnlyDedupe-VaraibleCompres	!	0	1002.51 GB	19%	N/A	19%
PromotedDS	✓	0	6.3 TB	2%	16%	18%
TestUser	✓	1	117.5 GB	10%	15%	24%

The Import a Data Store page opens.

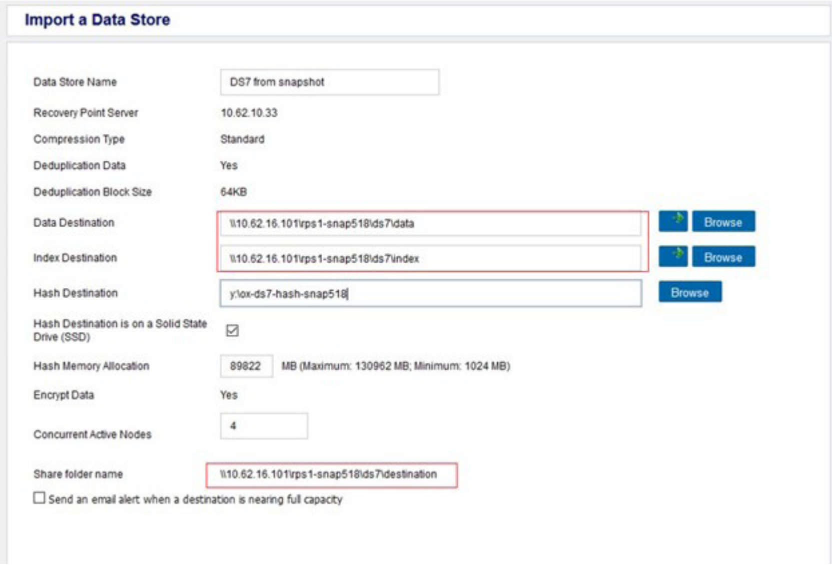
4. To select the Data Store Folder path, click the **Browse** button and select the path, and then click **Next**.



Import a Data Store

Recovery Point Server	192.168.0.14
Data Store Folder	\\192.168.0.50\UDPDedupeComp-CompOX\Common
Encryption Password	

5. In the Import a Data Store screen, based on the Share folder name path, map the relevant **Data Destination** and **Index Destination** paths.

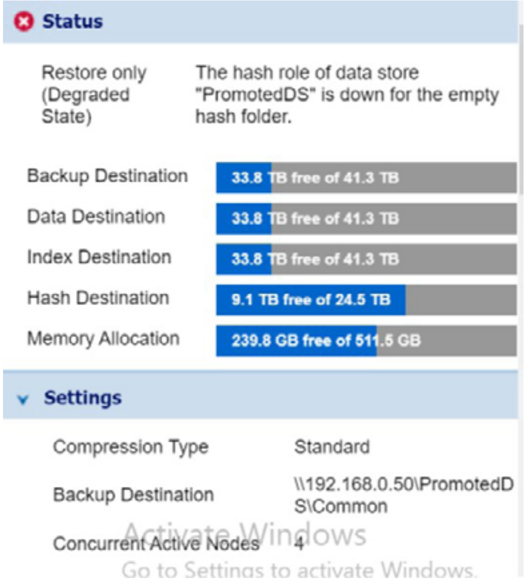


Import a Data Store

Data Store Name	DS7 from snapshot
Recovery Point Server	10.62.10.33
Compression Type	Standard
Deduplication Data	Yes
Deduplication Block Size	64KB
Data Destination	\\10.62.16.101\rps1-snap518\ds7\data
Index Destination	\\10.62.16.101\rps1-snap518\ds7\index
Hash Destination	y:\ox-ds7-hash-snap518
Hash Destination is on a Solid State Drive (SSD)	☑
Hash Memory Allocation	89822 MB (Maximum: 130962 MB; Minimum: 1024 MB)
Encrypt Data	Yes
Concurrent Active Nodes	4
Share folder name	\\10.62.16.101\rps1-snap518\ds7\destination

☐ Send an email alert when a destination is nearing full capacity

6. For Hash, provide an empty folder path, and then click **Save**. The data store gets imported in the **Restore Only** mode.



Status

Restore only (Degraded State) — The hash role of data store "PromotedDS" is down for the empty hash folder.

Backup Destination	33.8 TB free of 41.3 TB
Data Destination	33.8 TB free of 41.3 TB
Index Destination	33.8 TB free of 41.3 TB
Hash Destination	9.1 TB free of 24.5 TB
Memory Allocation	239.8 GB free of 511.5 GB

Settings

Compression Type	Standard
Backup Destination	\\192.168.0.50\PromotedDS\Common
Concurrent Active Nodes	4

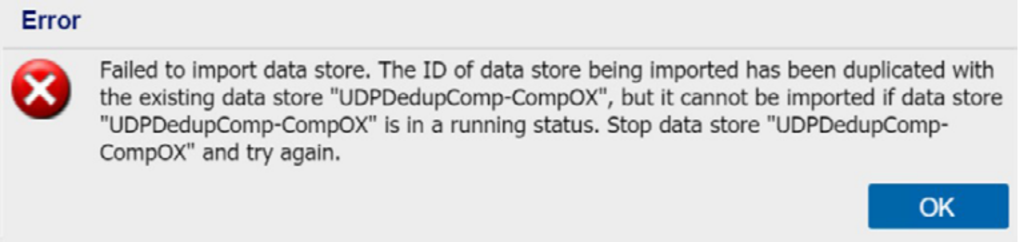
Note: You can perform restores of any required files and folders in the Restore only mode.

7. To regenerate the Dedupe Datastore Hash data, from the command line, navigate to C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN on the UDP Recovery Point Server and run **as_gddmgr.exe**, and then use the following command:

```
as_gddmgr.exe -Scan RebuildHash <<Datastore Name>> -NewHashPath
<<NewHashPath>>
```

8. After the Hash generation is complete, you can start the data store and modify the existing plan to point to the new data store. You can use this new data store to continue to write for future backups.

If you import the new share to the same UDP server where the old data store resides, the following error message is displayed.



Error

Failed to import data store. The ID of data store being imported has been duplicated with the existing data store "UDPDedupComp-CompOX", but it cannot be imported if data store "UDPDedupComp-CompOX" is in a running status. Stop data store "UDPDedupComp-CompOX" and try again.

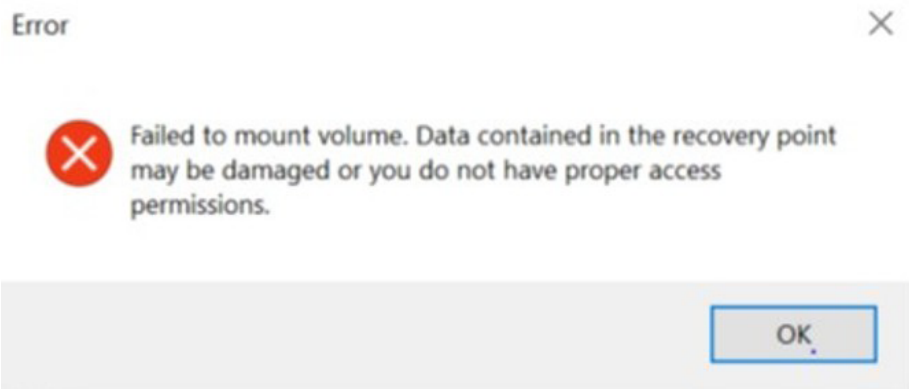
We recommend that you import the data store on a new server or fully delete the old data store from UDP as the authentication is already compromised.

Known Limitations

- For OneXafe, the snapshots are promoted as new shares with the same user permissions as the original share. During the promotion of the snapshot, you cannot provide different authentication.

  After the share is created using the OneSystem login, you can modify the permissions for the new share.

- Navigating the OneXafe Share from the Windows explorer and changing it to the UDP Recovery Point Server view fails when the destination resides on the OneXafe share.



Error

Failed to mount volume. Data contained in the recovery point may be damaged or you do not have proper access permissions.

- During maintenance activity or for some other reason, if any of the nodes in the OneXafe Cluster is shutdown the active UDP backup job might fail with the following error:

  An error has occurred from deduplication Data role on server 192.168.0.14. Error message = [The operations for this file (create, close, read, write) failed.]. You might experience the same behavior when the OneXafe node is Powered ON back.

  The next scheduled backup job will not have any impact because of this operation.