Integration von OneXafe und UDP

Rechtliche Hinweise

Diese Dokumentation, die eingebettete Hilfesysteme und elektronisch verteilte Materialien enthält (im Folgenden als „Dokumentation“ bezeichnet), dient ausschließlich zu Ihrer Information und kann von Arcserve jederzeit geändert oder zurückgezogen werden. Diese Dokumentation umfasst urheberrechtlich geschützte Informationen von Arcserve und darf ohne vorherige schriftliche Zustimmung von Arcserve weder ganz noch teilweise kopiert, übertragen, reproduziert, offengelegt, verändert oder vervielfältigt werden.

Wenn Sie ein lizenzierter Benutzer der in der Dokumentation angesprochenen Softwareprodukte sind, dürfen Sie eine angemessene Anzahl von Kopien der Dokumentation für den internen Gebrauch durch Sie und Ihre Mitarbeiter in Verbindung mit dieser Software ausdrucken oder anderweitig zur Verfügung stellen, vorausgesetzt, dass alle Arcserve-Urheberrechtsvermerke und -Legenden auf jeder reproduzierten Kopie angebracht sind.

Das Recht, Kopien der Dokumentation auszudrucken oder anderweitig zur Verfügung zu stellen, ist auf den Zeitraum beschränkt, in dem die geltende Lizenz für diese Software in vollem Umfang in Kraft bleibt. Sollte die Lizenz aus irgendeinem Grund enden, liegt es in Ihrer Verantwortung, Arcserve schriftlich zu bestätigen, dass alle Kopien und Teilkopien der Dokumentation an Arcserve zurückgegeben oder zerstört wurden.

SOWEIT DIES NACH GELTENDEM RECHT ZULÄSSIG IST, STELLT ARCSERVE DIESE DOKUMENTATION „WIE BESEHEN“ OHNE JEGLICHE GEWÄHRLEISTUNG ZUR VERFÜGUNG, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF STILLSCHWEIGENDE GARANTIEN DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER DER NICHTVERLETZUNG VON RECHTEN. IN KEINEM FALL HAFTET ARCSERVE GEGENÜBER IHNEN ODER EINEM DRITTEN FÜR VERLUSTE ODER SCHÄDEN, WEDER DIREKT NOCH INDIREKT, DIE SICH AUS DER VERWENDUNG DIESER DOKUMENTATION ERGEBEN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF ENTGANGENEN GEWINN, VERLORENE INVESTITIONEN, BETRIEBSUNTERBRECHUNG, GOODWILL ODER DATENVERLUST, SELBST WENN ARCSERVE VOR DER MÖGLICHKEIT EINES SOLCHEN VERLUSTES ODER SCHADENS AUSDRÜCKLICH DARAUF HINGEWIESEN WIRD.

Die Verwendung von Softwareprodukten, auf die in der Dokumentation verwiesen wird, unterliegt de jeweiligen Lizenzvereinbarungen und diese Lizenzvereinbarungen werden durch die Bestimmungen dieses Hinweises in keiner Weise geändert.

Der Hersteller dieser Dokumentation ist Arcserve.

Bereitgestellt mit „eingeschränkten Rechten". Die Nutzung, Vervielfältigung oder Offenlegung durch die Regierung der Vereinigten Staaten unterliegt den Beschränkungen, die in den FAR-Abschnitten 12.212, 52.227-14 und 52.227-19(c)(1) - (2) und DFARS-Abschnitt 252.227-7014(b)(3), soweit anwendbar, oder deren Nachfolgern festgelegt sind.

Supportanfrage an Arcserve

Das Arcserve-Support-Team bietet eine Vielzahl von Ressourcen zur Lösung Ihrer technischen Probleme und ermöglicht einen einfachen Zugriff auf wichtige Produktinformationen.

Supportanfrage

Mit Arcserve Support:

- Sie können direkt auf die gleiche Informationsbibliothek zugreifen, die auch intern von unseren Arcserve-Support-Experten genutzt wird. Diese Seite bietet Ihnen Zugriff auf unsere Knowledge-Base (KB)-Dokumente. Von hier aus können Sie ganz einfach die produktbezogenen KB-Artikel suchen und finden, die die praxiserprobten Lösungen für viele Top-Themen und häufige Probleme enthalten.

- Sie können unseren Live-Chat-Link verwenden, um sofort eine Echtzeit-Konversation zwischen Ihnen und dem Arcserve-Support-Team zu starten. Mit dem Live-Chat erhalten Sie sofortige Antworten auf Ihre Anliegen und Fragen, während Sie weiterhin Zugriff auf das Produkt haben.

- Sie können an der Arcserve Global User Community teilnehmen, um Fragen zu stellen und zu beantworten, Tipps und Tricks auszutauschen, die besten Praktiken zu diskutieren und an Unterhaltungen mit Gleichgesinnten teilzunehmen.

- Sie können ein Support-Ticket eröffnen: Wenn Sie online ein Support-Ticket eröffnen, können Sie einen Rückruf von einem unserer Experten für den von Ihnen angefragten Produktbereich erwarten.

- Sie können auf weitere hilfreiche Ressourcen zugreifen, die für Ihr Arcserve-Produkt geeignet sind.

Inhalt

Kapitel 1: Übersicht

Arcserve UDP (UDP) ist eine umfassende Lösung zum Schutz komplexer IT-Umgebungen. Die Lösung schützt Ihre Daten, die sich in verschiedenen Arten von Knoten befinden, wie Windows, Linux und virtuelle Maschinen auf VMware ESX-Servern, Microsoft Hyper-V-Servern oder Nutanix AHV-Servern. Sie können die Daten entweder auf einem lokalen Rechner oder auf einem Wiederherstellungspunkt-Server sichern. Ein Wiederherstellungspunkt-Server ist ein zentraler Server, auf dem Backups aus mehreren Quellen gespeichert werden.

OneXafe verhindert mit seinem patentierten verteilten Objektspeicher jede Form des Überschreibens. Darüber hinaus führt OneXafe eine leistungsstarke integrierte Deduplizierung kontinuierlicher Snapshots durch, was den Bedarf an Speicherplatz reduziert. Die Scale-Out-Architektur von OneXafe erweitert den Speicherplatz nahtlos. Um diese Option zu aktivieren, fügen Sie jeweils ein Laufwerk oder mehrere Knoten innerhalb eines Clusters hinzu, ohne Konfigurationsänderungen an der Anwendung vorzunehmen.

Dieses Dokument enthält Informationen über die Integration von UDP und OneXafe, wodurch die Daten des UDP-Wiederherstellungspunkts für den Backup unveränderlich werden. Wenn beispielsweise ein Cyberkrimineller die Daten des UDP-Wiederherstellungspunkts durch einen Ransomware-Angriff löscht, kann die unveränderliche Snapshot-Funktion von OneXafe zur Rettung kommen und Optionen zur Wiederherstellung der verlorenen Daten bieten. Ein unveränderlicher Snapshot ist eine Kopie Ihrer Daten, die von Ransomware oder Benutzern nicht überschrieben oder gelöscht werden kann.

OneXafe Continuous Data Protection (CDP) führt in der ersten Stunde alle 90 Sekunden einen kontinuierlichen Snapshot durch. Anschließend führt es stündliche, tägliche und monatliche Snapshots durch. Snapshots helfen bei der Wiederherstellung von Daten in der zeitlich größtmöglichen Nähe eines Ransomware-Angriffs. Im Allgemeinen kann der Ransomware-Angriff die Primärdateien beschädigen, aber die Snapshots sind davon völlig unberührt. OneXafe bietet auch Optionen für eine einfache Wiederherstellung: Sie können einzelne Dateien, Ordner oder eine komplette Netzwerkfreigabe wiederherstellen.

Kapitel 2: OneXafe-Konfiguration

Dieser Abschnitt enthält Informationen zur Konfiguration des OneXafe-Clusters.

Um OneXafe-Cluster zu konfigurieren, gehen Sie wie folgt vor:

1. Richten Sie Ihre Netzwerkkonfiguration ein.
2. Erstellen Sie einen Cluster mit einem Knoten oder mehreren Knoten (bis zu 3 Knoten).
3. Registrieren Sie den Cluster im OneSystem-Konto (User Management und Storage Management) mit „Share Creation“.
4. Legen Sie eine virtuelle IP für den OneXafe-Cluster fest.

Dieses Dokument gilt für die folgenden oder neuere Versionen von UDP und OneXafe:

- UDP Version 8.0 oder neuer: Build 5628 für alle UDP-Komponenten, d. h. UDP-Konsole, Wiederherstellungspunkt-Server und UDP-Agenten.

- OneXafe-Cluster
  - Modelle: OneXafe 4412, 4417, 5410
  - Software-Version: 3.2.3 Cabernet Sauvignon oder neuer

Netzwerk konfigurieren

Dieser Abschnitt enthält Informationen über die Konfiguration des OneXafe-Netzwerks.

Um das Netzwerk zu konfigurieren, melden Sie sich bei der OneXafe-Webkonsole an und wechseln Sie zur Registerkarte **Configuration > Network**. Stellen Sie sicher, dass Sie verschiedene Netzwerkprofile haben, wie in der folgenden Abbildung gezeigt.

Hinweis: Wir empfehlen das Folgende:

- Für ein System mit vier Netzwerkanschlüssen legen Sie zwei Netzwerkprofile an: Verwaltung und Daten.
- Für ein System mit sechs Netzwerkanschlüssen legen Sie drei Netzwerkprofile an: Verwaltung, Daten und Cluster.
- 10GbE-Netzwerk

iDRAC for OneXafe-Cluster konfigurieren

Wenn ein Netzwerkkabel an den iDRAC-Port angeschlossen wird, erhält er standardmäßig eine DHCP-Adresse. Die standardmäßigen iDRAC-Anmeldedaten sind:

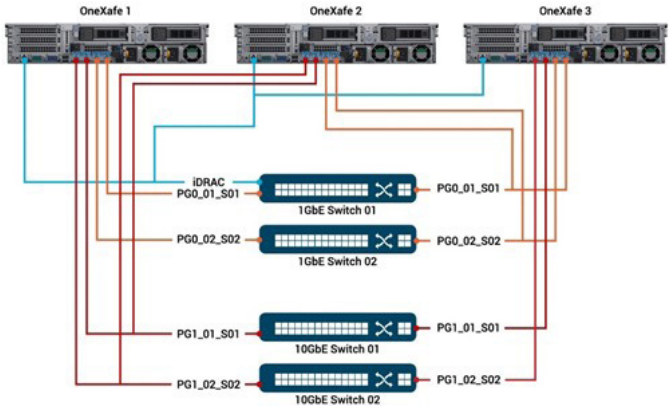
- Benutzername: admin
- Passwort: config

Für OneXafe, das in einem Netzwerk ohne DHCP-Server bereitgestellt wird, können Administratoren jetzt eine statische IP-Adresse für den iDRAC festlegen. Siehe auch Beispiel unten.

```
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
```

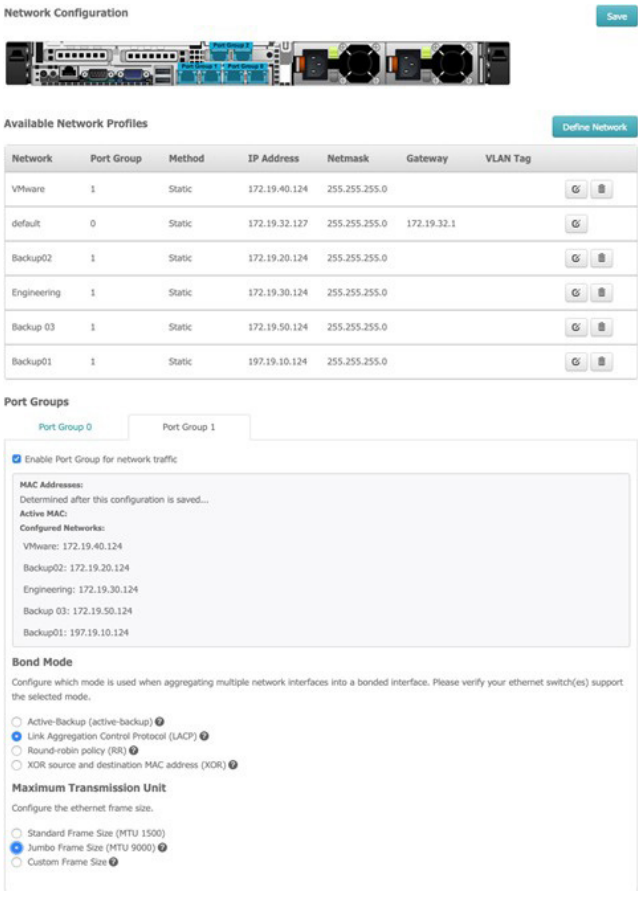
So konfigurieren Sie OneXafe-Netzwerke und Portgruppen ordnungsgemäß

Das folgende Netzwerkkonfigurationsdiagramm umfasst einen 3-Knoten-Cluster, zwei Portgruppen und iDRAC. Es enthält außerdem eine Netzwerkredundanz zu mehreren Switches. In diesem Beispiel sind die 10GbE-Switches stapelbar und die Ports sind in LAG konfiguriert.



Das folgende Beispiel enthält die Einstellungen für den gesamten OneXafe-Cluster, den iDRAC, die IP-Adresse für mehrere VLANs, Konfigurationsdetails und die Konfiguration von PG1 über die Webkonsole.

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



Beispiel: OneXafe 3-Knoten-Cluster-Bereitstellung, Netzwerkkonfiguration für 10GbE-Netzwerk

Dieses Beispiel enthält die folgenden Details:

- 10GbE-Netzwerk
- PG0 (XOR), PG1 (XOR)
- VLAN-Tagging

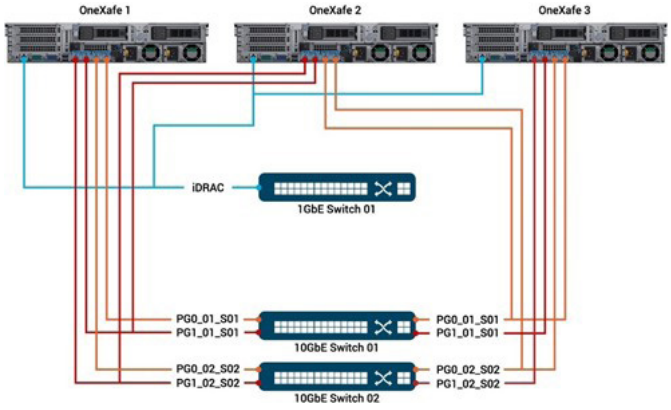
In diesem Beispiel für Backup/Wiederherstellung und VMware ist ein VLAN zu einem Gateway für den OneSystem-Zugriff routbar, während andere VLANs nicht routbar sind.

Mit der Exkonsole kann die xmithash-Richtlinie auf PG1 auf Schicht 3+4 gesetzt werden. Standardmäßig ist es Schicht 2+3 und wird in der Exkonsole als leer angezeigt. Alle anderen Portgruppen-Einstellungen können über die Web-Konsole vorgenommen werden. Daher bezieht sich die Abbildung nur auf die Einstellung der xmithash-Richtlinie.

```
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)
```

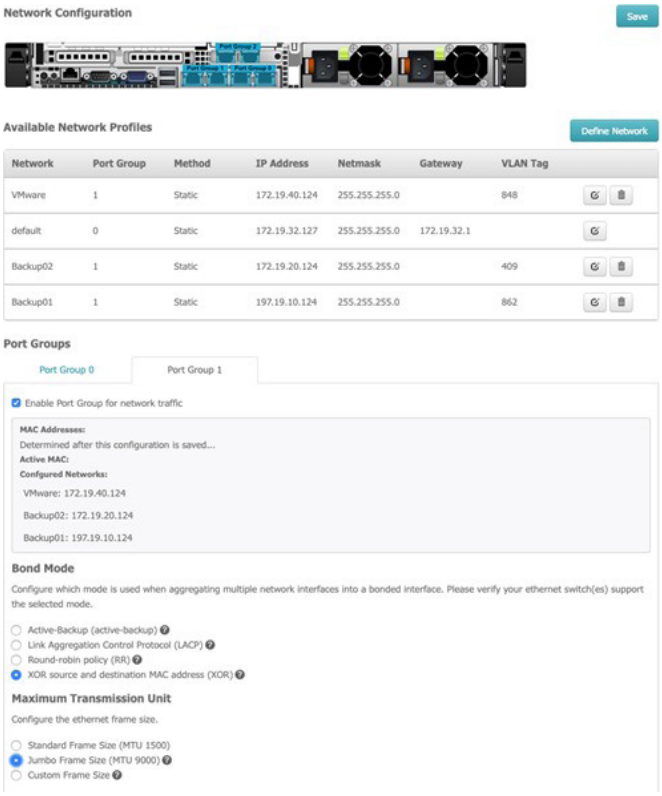
Hinweis: Das obige Beispiel liefert die erforderliche Switch-Port-Konfiguration für die verschiedenen Hash-Algorithmen.

Das folgende Beispiel ist ein Netzwerkkonfigurationsdiagramm für einen 3-Knoten-Cluster, Gruppen mit zwei Ports und iDRAC.
Es besteht außerdem eine Netzwerkredundanz zu mehreren Switches (außer iDRAC). In diesem Beispiel sind die 10GbE-Switches nicht stapelbar. Daher unterstützen die Switches kein LACP über mehrere Switches hinweg. Wählen Sie in diesem Fall XOR, da wir dies als die nächstbeste Option empfehlen. LACP ist jedoch der bevorzugte Bond-Modus.

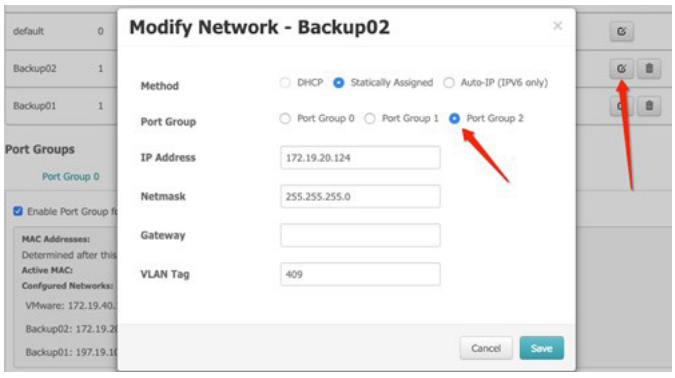


Das folgende Beispiel zeigt die Einstellungen für den gesamten OneXafe-Cluster, den iDRAC, die IP-Adresse für mehrere VLANs, Konfigurationsdetails und die Konfiguration von PG1 über die Webkonsole.

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



Hinweis: Um ein Netzwerkprofil in eine andere Portgruppe zu verschieben, wählen Sie das Bearbeitungssymbol und dann die gewünschte Portgruppe aus. Sie brauchen nicht zu löschen und ein neues Netzwerkprofil zu erstellen. Das folgende Bild zeigt, wie Backup02 von Portgruppe 1 zu Portgruppe 2 geändert wurde.



Weitere Informationen erhalten Sie in diesem Video: Konfiguration von Netzwerk-Portgruppen mit OneBlox Exconsole.

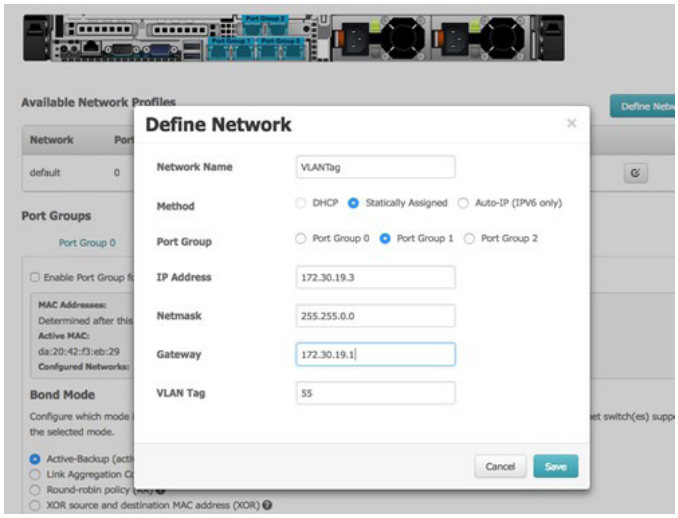
VLAN-Tagging konfigurieren

Mit der OneXafe-Webkonsole (und exconsole-Befehlen) können Administratoren einem Netzwerkprofil VLAN-Tags (Kennzeichnung von Ethernet-Paketen mit einem Wert für Routing-Zwecke) zuweisen. VLAN-Tags sind nicht erforderlich und viele Unternehmen entscheiden sich für portbasierte VLANs, um mehrere Subnetze über dieselben Switch-Ports zu leiten.

Wenn Sie das VLAN-Tag aus einem vorhandenen Netzwerkprofil über die Exkonsole oder die Webkonsole entfernen, setzen Sie den VLAN-Tag-Wert auf 0. Klicken Sie dann auf „Save“ (Webkonsole) oder „Apply“ (Exkonsole).

Beispiel:

- Portbasiertes VLAN-Tagging bei Miraki
- Konfigurationsleitfaden für Cisco Nexus 5000



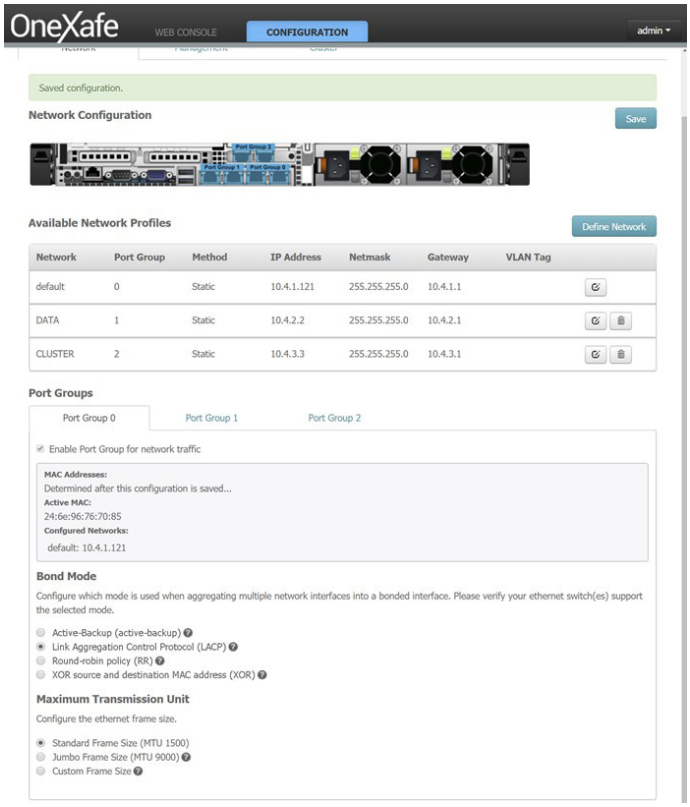
Es gibt drei Netzwerke, die konfiguriert werden müssen, und Portgruppen, die in der empfohlenen Konfiguration aktiviert werden müssen:

1. Verwaltung (Standard) - Portgruppe 0
2. Daten - Portgruppe 1
3. (Optional) Cluster - Portgruppe 2 – Erweitertes Netzwerk

Verwaltung (Standard) - Portgruppe 0

Primäre Verwendung - Zur Kommunikation mit OneSystem

- Benötigt keine Hochgeschwindigkeitsverbindungen - 1GbE reicht für statisch aus
- IP wird dringend empfohlen.
- Die Pfad-MTU-Ermittlung funktioniert auf der Verbindung bis zu OneSystem.

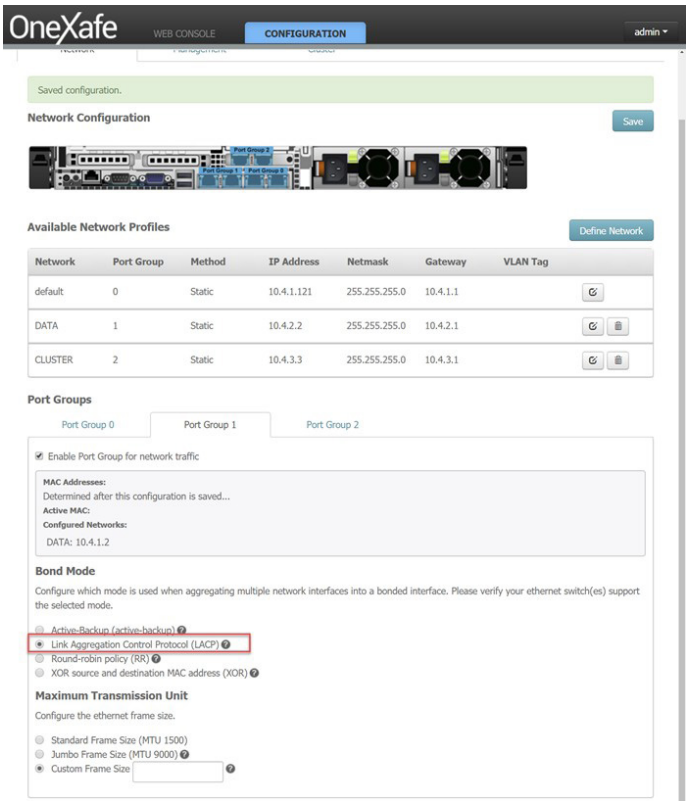


Daten - Portgruppe 1

Primäre Verwendung - Zur Kommunikation mit dem Client-Netzwerk und zum Einlesen (z. B. SMB-Freigaben, NFS-Exporte)

- Stellen Sie für eine optimale Leistung sicher, dass LACP konfiguriert ist. Statische IP wird dringend empfohlen.
- MTU sollte zu Ihrer Switch-Topologie passen - normalerweise 1500.
- Die Kommunikation zum Cluster erfolgt über die in diesem Netzwerk konfigurierte VIP (Virtual IP). Die Kommunikation zum Cluster über die VIP erfolgt über SMB oder NFS.
- Registrieren Sie das VIP als FQDN in der Domain.

- Sobald die Daten eingelesen sind, läuft der Cluster-Betrieb über das Cluster-Netzwerk. Sorgen Sie dafür, dass das Cluster-Netzwerk die gleiche oder eine größere Bandbreite als das Datennetzwerk hat.
  - Wenn zum Beispiel 20 GB auf der Datenseite eingehen, sollten idealerweise auch 20 GB auf der Clusterseite herausgehen.
  - Zusätzlich gibt es ein Datenplatzierungsprotokoll für das Setzen/Schreiben der Blöcke in den verteilten Objektspeicher.

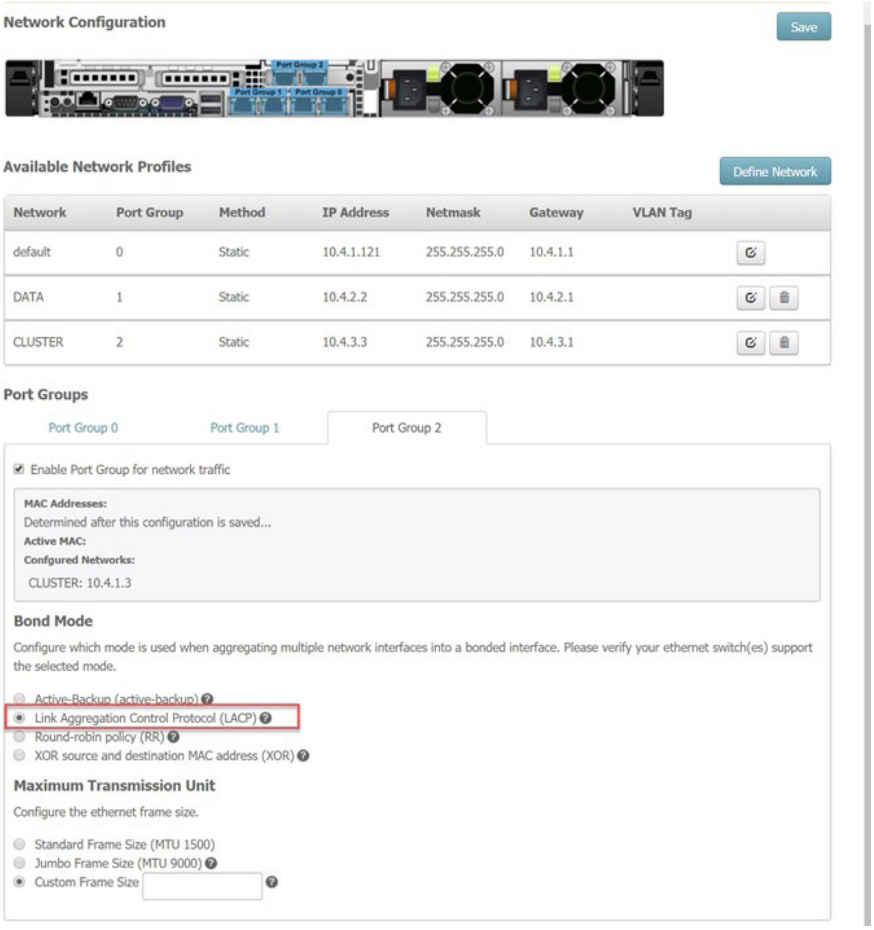


(Optional) Cluster - Portgruppe 2 – Erweitertes Netzwerk

Primäre Verwendung - wird für alle Kommunikationsfunktionen innerhalb des Clusters verwendet.

- Stellen Sie für eine optimale Leistung sicher, dass LACP konfiguriert ist.
- Das Cluster-Netzwerk wird während der Cluster-Konfiguration automatisch als IPv6 konfiguriert und es wird automatisch erkannt. Es wird angenommen, dass sich das Cluster-Netzwerk in denselben Switch-Domänen befindet und jeden Knoten sehen kann.
- Das LAN führt kein Protokoll aus, sondern nur die Endpunkte - in diesem Fall die OneXafe-Knoten. Das LAN kann sowohl IPv4- als auch IPv6-Datenverkehr übertragen. Die Knoten im Cluster verwenden IPv6 für die Autokonfiguration und die Kommunikation zwischen den Knoten.
- Die Clusterkonfiguration umfasst auch IPv6 - SLAC (Stateless Link Auto Config).
- Stellen Sie sicher, dass die Nachbarschaftserkennung auf allen Switches in der Umgebung aktiviert ist.
- Cluster-Kommunikation über Tunnel wird nicht unterstützt.
- Die erforderlichen Kommunikationsprotokolle sind:
  - Multicast (gleiche Switch-Fabric), der Cluster muss innerhalb der gleichen Multicast-Domäne liegen.
  - Die Cluster-Seite muss mit zwei verschiedenen Protokollen übersetzen. HA-Protokoll (Verwaltung, ein VIP in Betrieb halten usw.) und ein Multicast-Protokoll, VRRP (Virtual Route Redundancy Protocol).
- Neben dem Multicast-Protokoll wird auch der Punkt-zu-Punkt-Unicast-Verkehr über TCP über SSDP abgewickelt.
- Die häufigsten Fehlkonfigurationen sind Probleme im Zusammenhang mit Multicast und TCP-Flusskontrolle. Stellen Sie sicher, dass beide Protokolle auf allen mit einem OneXafe verbundenen Ports aktiviert sind.
  - Unsachgemäß konfigurierte TCP-Flusskontrolle kann einen Knoten aushungern. Stellen Sie die ordnungsgemäße Konfiguration der TCP-Flusskontrolle sicher, um das Risiko zu minimieren.

• Die ideale Konfiguration muss aus einem Cluster-Switch bestehen, der für den Cluster-Verkehr bestimmt ist.



Die empfohlenen Netzwerkkonfigurationen finden Sie an folgenden Stellen:

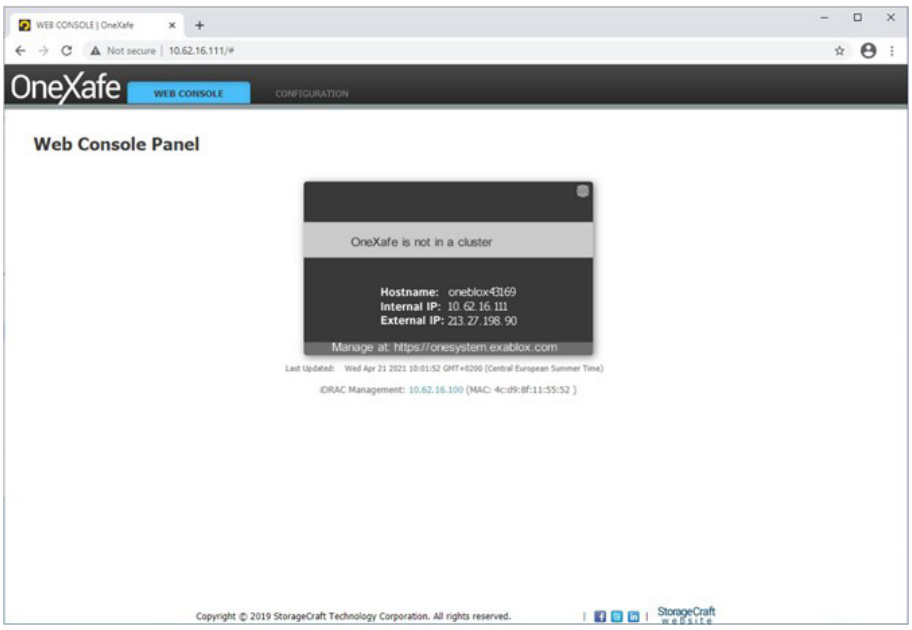
- Verfahrensweisen: So konfigurieren Sie OneXafe-Netzwerke und Portgruppen ordnungsgemäß
- Allgemeine Aufgaben - Netzwerk

Einzelknoten oder Mehrfachknoten-Cluster erstellen

Führen Sie diese Schritte durch:

1. Holen Sie sich von der OneXafe iDRAC-Konsole die IP für den Zugriff auf die OneXafe Web Console. Sie können die Cluster-Konfiguration und die Vernetzung über die OneXafe-Webkonsole durchführen.

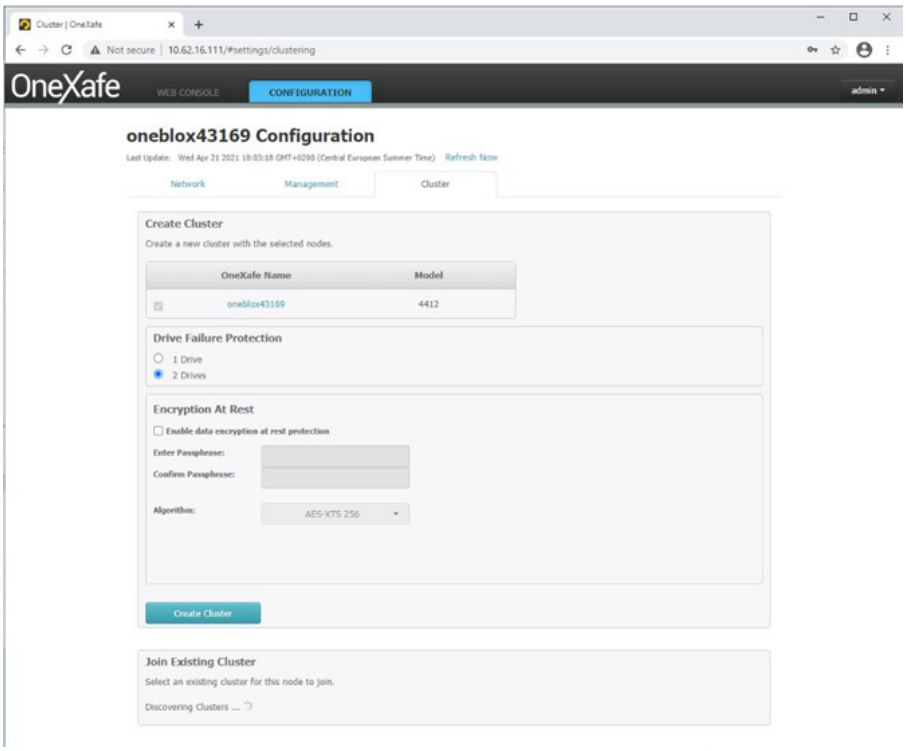
2. Gehen Sie zum Öffnen der OneXafe-Webkonsole zu http://<<device IP>>. The Startseite wird geöffnet.



3. Klicken Sie auf die Registerkarte „Configuration“ und geben Sie dann Ihre Anmeldedaten ein.
   - **Default Username:** admin
   - **Default Password:** config

Hinweis: Wenn Sie sich zum ersten Mal angemeldet haben, werden Sie aufgefordert, das Passwort zu ändern.

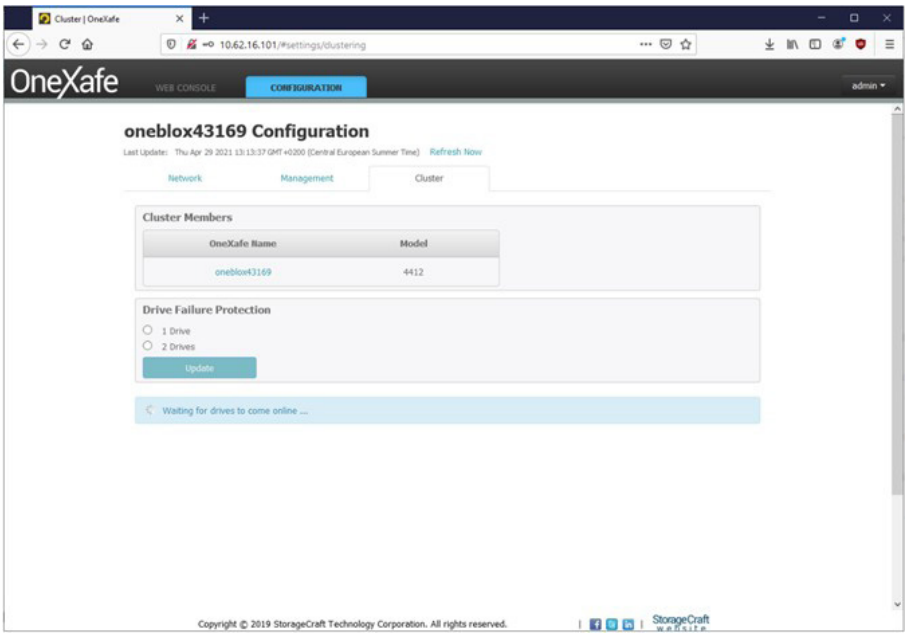
4. Um einen neuen Cluster mit den ausgewählten OneXafe-Knoten zu erstellen, gehen Sie zur Registerkarte **Configuration > Cluster** und gehen Sie dann wie folgt vor:
   a. Zeigen Sie die OneXafe-Knoten an und wählen Sie sie nach Bedarf aus.
   b. Wählen Sie für den Schutz vor Laufwerksausfällen die Laufwerke nach Bedarf aus.
   c. Um die Verschlüsselung gespeicherter Daten zu aktivieren, klicken Sie auf das Kontrollkästchen **Enable data encryption at rest protection**. Optional können Sie die Verschlüsselung gespeicherter Daten auch beim Erstellen von Clustern aktivieren.
   d. Klicken Sie auf die Schaltfläche **Create Cluster**.



In der folgenden Tabelle ist der Fehler-Domainschutz von Laufwerken und Knoten innerhalb eines Clusters dargestellt:

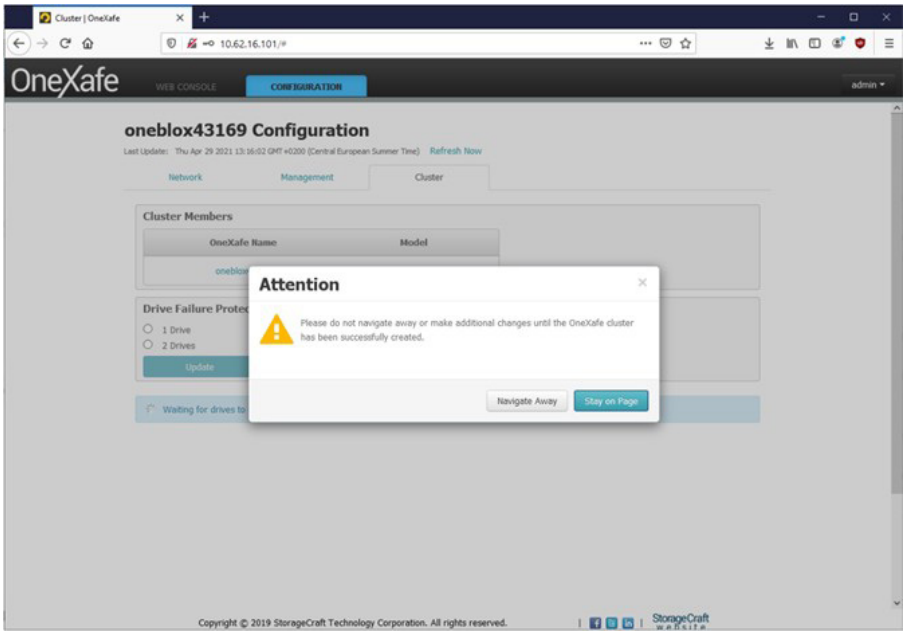
OneBlox 4312- und 4400-Cluster	1 Laufwerkfehler	1 Knotenfehler	2 Laufwerkfehler	2 Knotenfehler
1 Knoten-Cluster	Ja	Nein	Ja (Standardwert)	Nein
2-Knoten-Cluster	Ja	Ja (Lesen/Schreiben, je nachdem, welcher Knoten ausfällt)	Ja (Standardwert)	Nein
3-Knoten-Cluster	Ja	Ja	Ja (Standardwert)	Nein
4-Knoten-Cluster	Ja	Ja	Ja (Standardwert)	Ja (Lesen/Schreiben)
5-Knoten-Cluster und mehr	Ja	Ja	Ja (Standardwert)	Ja (Lesen/Schreiben)

Die Erstellung des Clusters wird initiiert.

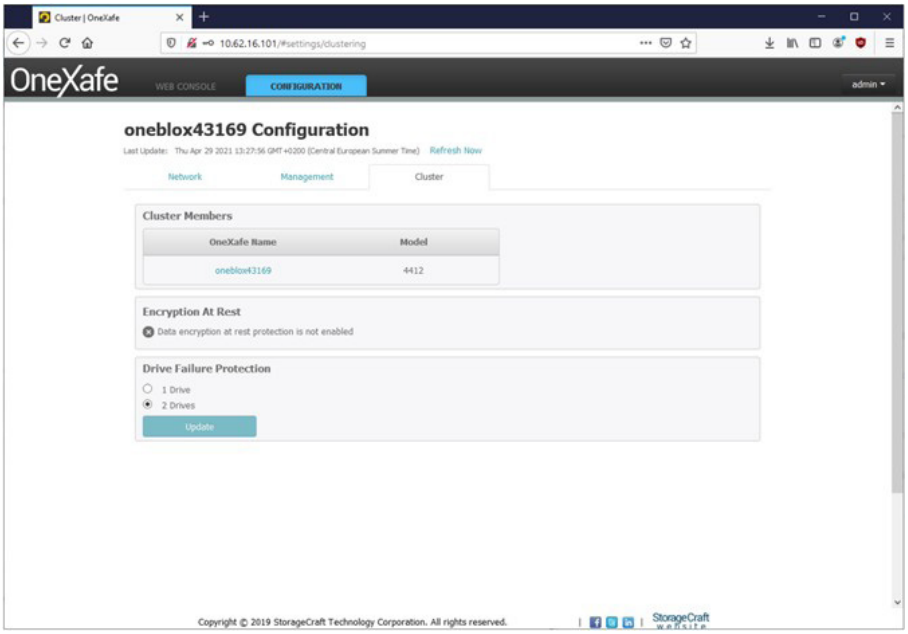


Hinweis: Wir empfehlen, dass Sie auf der Seite bleiben, bis der Cluster erstellt wird. Wenn Sie versuchen, vom Bildschirm weg zu navigieren oder weitere Änderungen vorzunehmen, wird die folgende Meldung angezeigt.

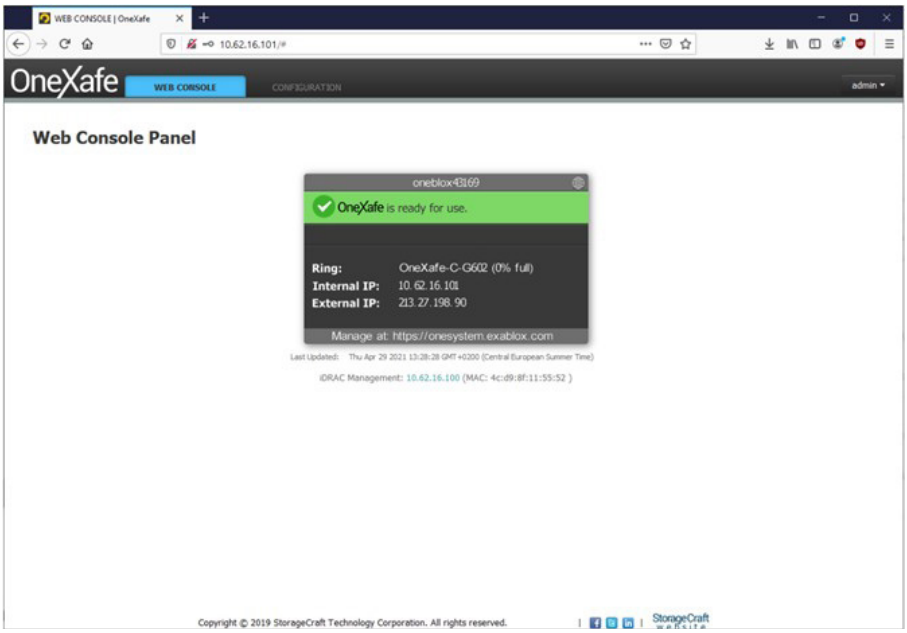
Einzelknoten oder Mehrfachknoten-Cluster erstellen



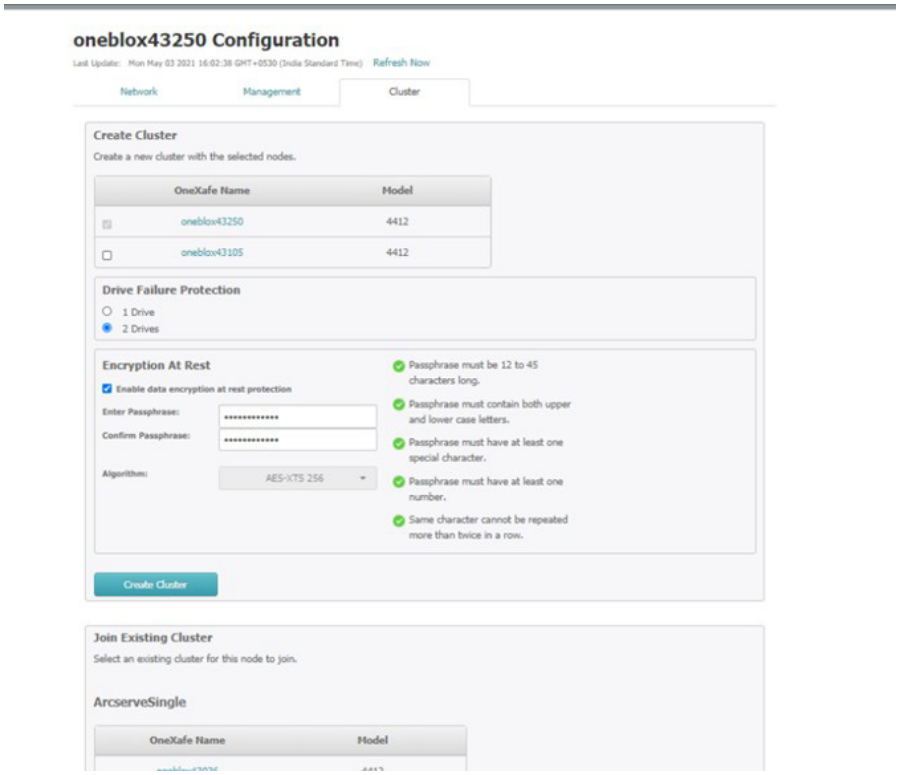
Der Cluster ist erstellt und einsatzbereit.



Der Status wird auf der Registerkarte „Web Console“ aktualisiert.



5. Um einen zweiten Knoten zum Cluster hinzuzufügen, melden Sie sich an der Webkonsole des zweiten Knotens an, indem Sie die Schritte 1 und 2 ausführen, und navigieren Sie dann zu „Configuration > Cluster“.
6. Klicken Sie unter dem Abschnitt „Join Existing Cluster“ auf die Schaltfläche „Join“, um dem Cluster einen weiteren Knoten hinzuzufügen.

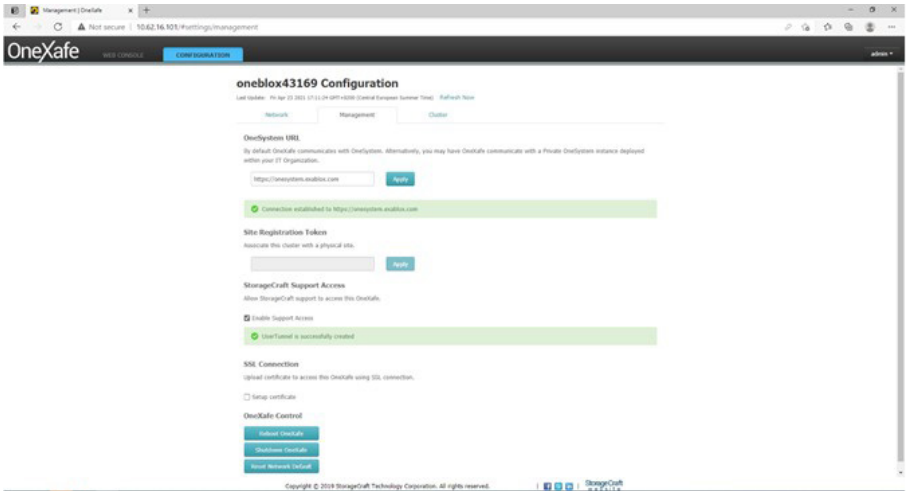


7. Um dem Cluster einen dritten Knoten hinzuzufügen, führen Sie die Schritte 5 und 6 aus.

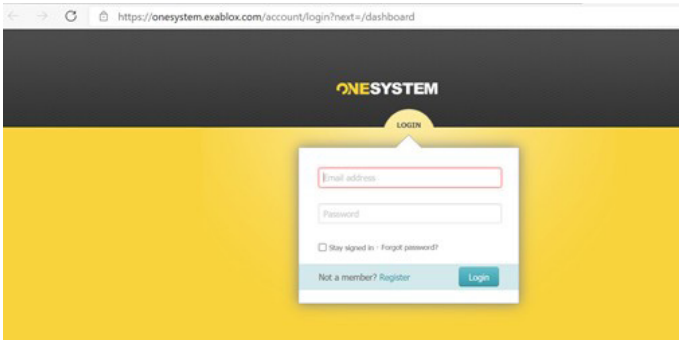
OneXafe im OneSystem-Konto registrieren

Führen Sie diese Schritte durch:

1. Melden Sie sich bei der OneXafe-Webkonsole an und gehen Sie dann zur Registerkarte „Configuration > Management“.

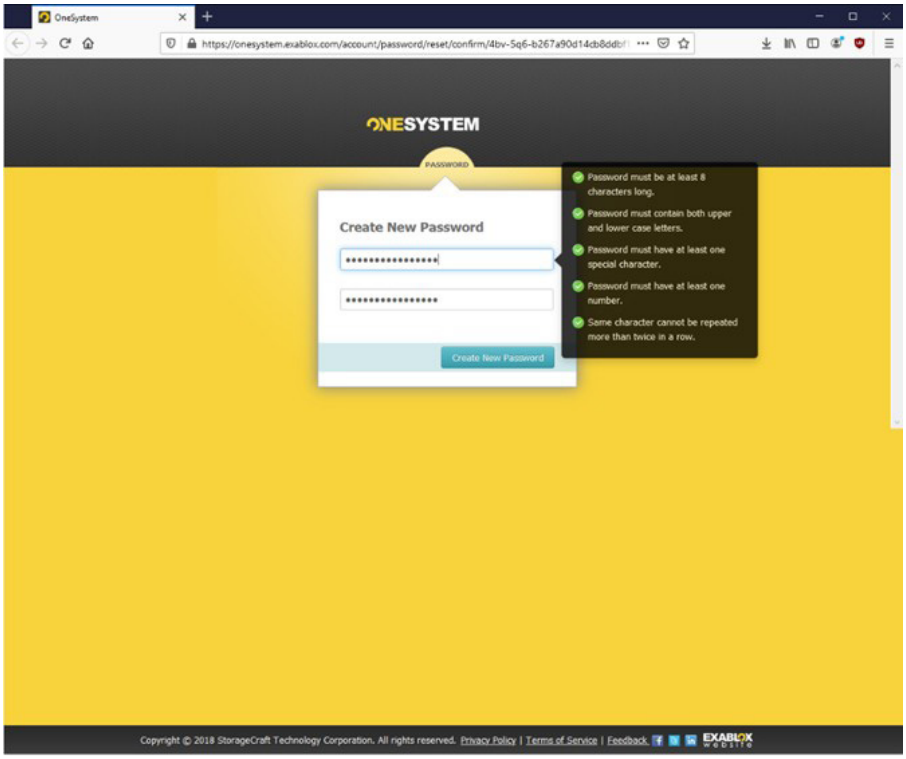


2. Kopieren Sie die OneSystem-URL (https://onesystem.exablox.com) und fügen Sie sie in das neue Fenster eines Browsers ein.

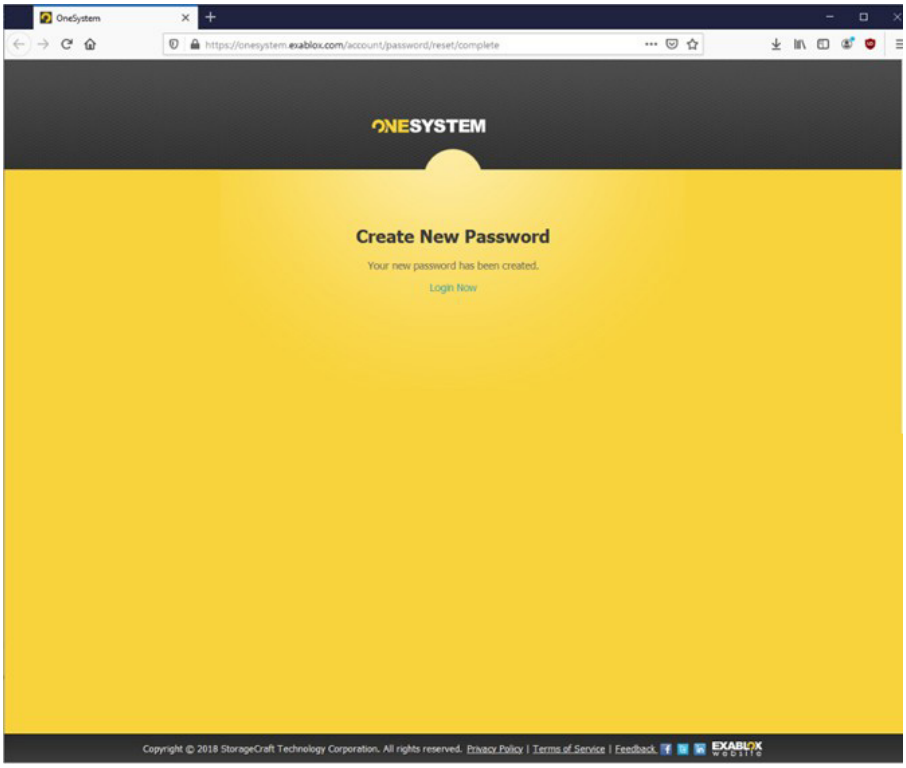


3. Klicken Sie auf die Schaltfläche „Register“, geben Sie die Details ein und klicken Sie dann auf „Register“.

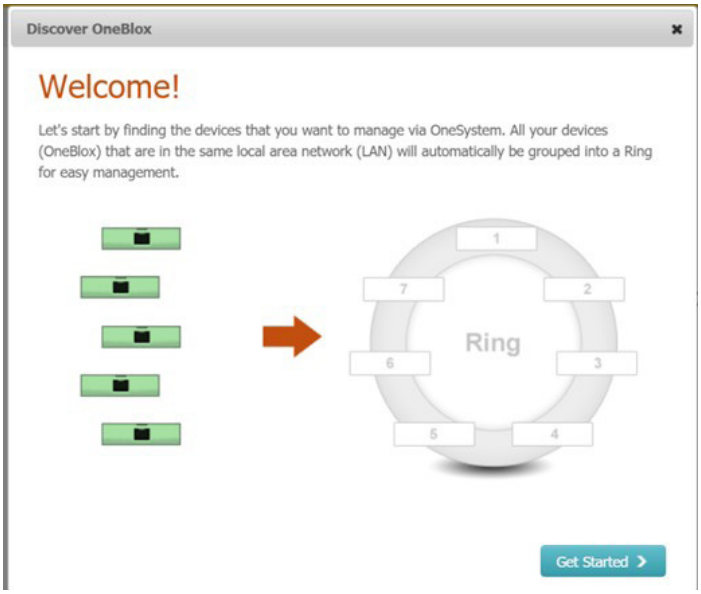
Nachdem Sie sich registriert haben, erhalten Sie eine E-Mail-Benachrichtigung. Um Ihr Konto zu bestätigen und Ihr Passwort zurückzusetzen, klicken Sie auf den in der E-Mail angegebenen Link.



Ihr neues Passwort wird erstellt.

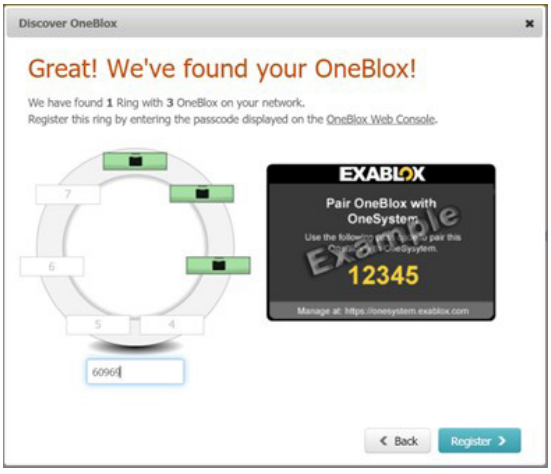


4. Melden Sie sich mit dem neuen Passwort bei OneSystem an.
5. Klicken Sie auf der Seite „Overview“ auf „Actions > Register New Rings“. Der Bildschirm „Discover OneBlox“ wird geöffnet.

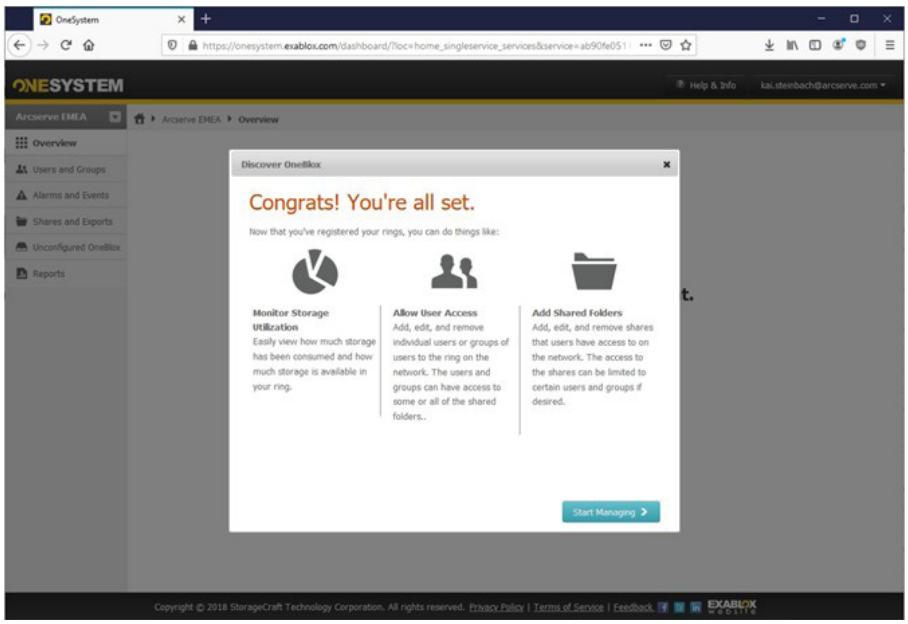


6. Um OneBlox finden, klicken Sie auf die Schaltfläche „Get started“.
7. Um OneBlox zu finden, wählen Sie eine der folgenden Optionen:
   - **Discover OneBlox:** Findet OneBlox automatisch.
   - I need to find my OneBlox by IP address: Ermöglicht das Finden von OneBlox anhand einer IP-Adresse. Geben Sie im Feld „External IP Address“ die IP-Adresse ein und klicken Sie auf „Next“.

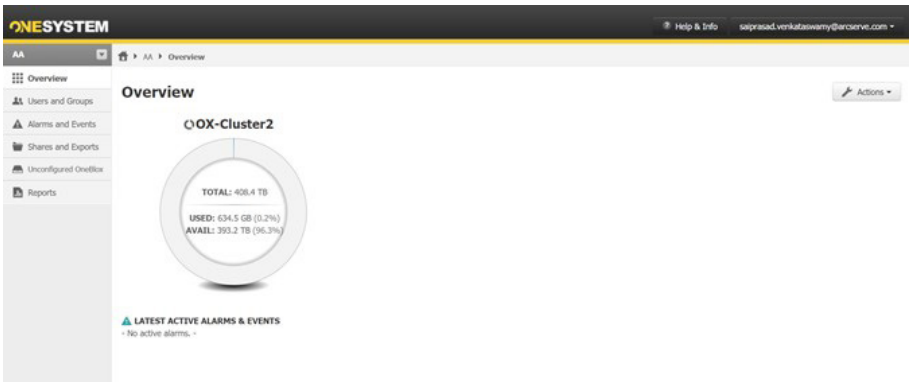
8. Um OneBlox mit OneSystem zu koppeln, rufen Sie den Passcode ab und geben ihn in das Textfeld ein. Um den Passcode abzurufen, klicken Sie auf das Bild **Exablox**.



9. Klicken Sie nach der Eingabe des Passcodes auf die Schaltfläche „Registrieren“.



OneBlox ist nun mit OneSystem gekoppelt.

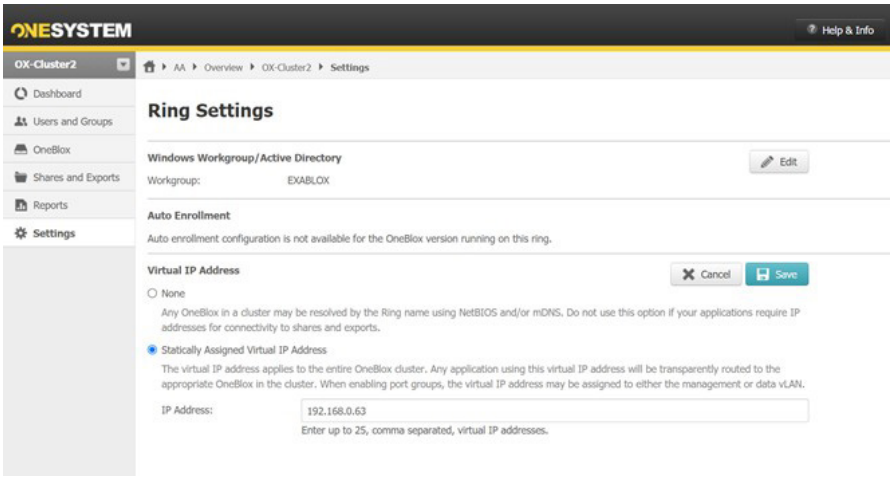


Hinweis: Weitere Informationen über OneXafe finden Sie im Benutzerhandbuch zu StorageCraft OneXafe.

Virtuelle IP von OneXafe-Cluster konfigurieren

Führen Sie diese Schritte durch:

1. Melden Sie sich im OneSystem an.
2. Klicken Sie auf der Übersichtsseite auf den entsprechenden OneXafe-Cluster-Ring.
3. Um zu den Ring-Einstellungen zu navigieren, klicken Sie auf den Bereich „Settings“.
4. Klicken Sie auf die Schaltfläche „Edit“, die sich neben den Einstellungen für die virtuelle IP befindet, weisen Sie eine statische IP zu und klicken Sie dann auf die Schaltfläche „Save“.



Hinweis: Weitere Informationen über OneXafe finden Sie im Benutzerhandbuch zu StorageCraft OneXafe.

Kapitel 3: UDP und OneXafe zum Erreichen einer unveränderlichen Speicherung für Backups konfigurieren

In diesem Abschnitt finden Sie Informationen zur Konfiguration von UDP und OneXafe, um die Daten des UDP-Wiederherstellungspunkts unveränderbar zu machen, sowie zu den Schritten, die für die Datenwiederherstellung im Falle von Ransomware-Angriffen zu befolgen sind.

Das OneXafe-Dateisystem basiert auf einem unveränderlichen Objektspeicher, bei dem Objekte nur einmal geschrieben und nie verändert werden. Daher werden die Objekte im Gegensatz zu vielen Dateisystemen nie „an Ort und Stelle“ überschrieben.

Alle Client-Änderungen an Dateisystemdaten führen immer zu neuen Objekten, auch wenn es sich um bestehende Objekte handelt, die geändert werden. Jedes Objekt ist außerdem verschlüsselt, durch kryptographische Hashes geschützt und bildet einen Merkle-Baum (wie eine Blockchain). Die Daten des Objekts werden beim Zurücklesen immer validiert, um die Unveränderlichkeit zu gewährleisten. Bei Snapshots wird einfach der Root-Hash des Baums notiert und kann sofort erstellt werden. Snapshots sind also die Ansicht des Dateisystems zu dem Zeitpunkt, an dem der Snapshot gemacht wird. Dies friert das Dateisystem ein und da die zugrunde liegenden Objekte, auf die Snapshots zeigen, unveränderlich sind und nicht geändert werden können, erbt der Snapshot diese Unveränderlichkeit. Er kann nicht von einer externen Quelle geändert oder modifiziert werden.

Snapshots machen die Objekte und dadurch auch das Dateisystem verfügbar, womit es möglich wird, zu bestimmten Zeitpunkten zurückzugehen und auf einfache Art die Unveränderlichkeit von Objekten und damit auch der zugrundeliegenden Daten zu garantieren.

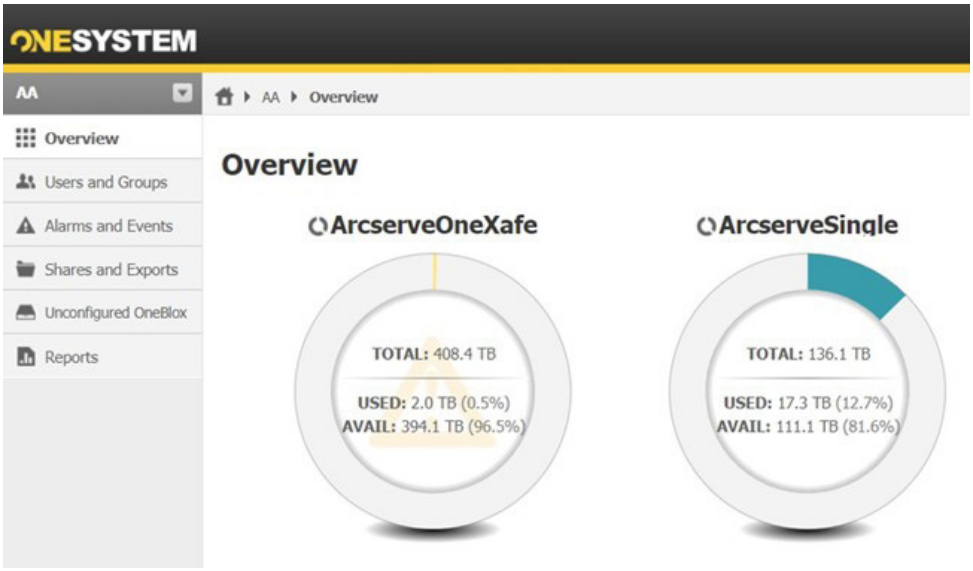
- SMB-Freigaben im OneXafe-Speichersystem erstellen
- Wiederherstellung nach einem Ransomware-Angriff
- Erforderliche Zugangsdaten während der Wiederherstellung
- OneXafe-Snapshot zu einer neuen Freigabe hochstufen
- Deduplizierungs-Datenspeicher in UDP importieren
- Bekannte Einschränkungen

SMB-Freigaben im OneXafe-Speichersystem erstellen

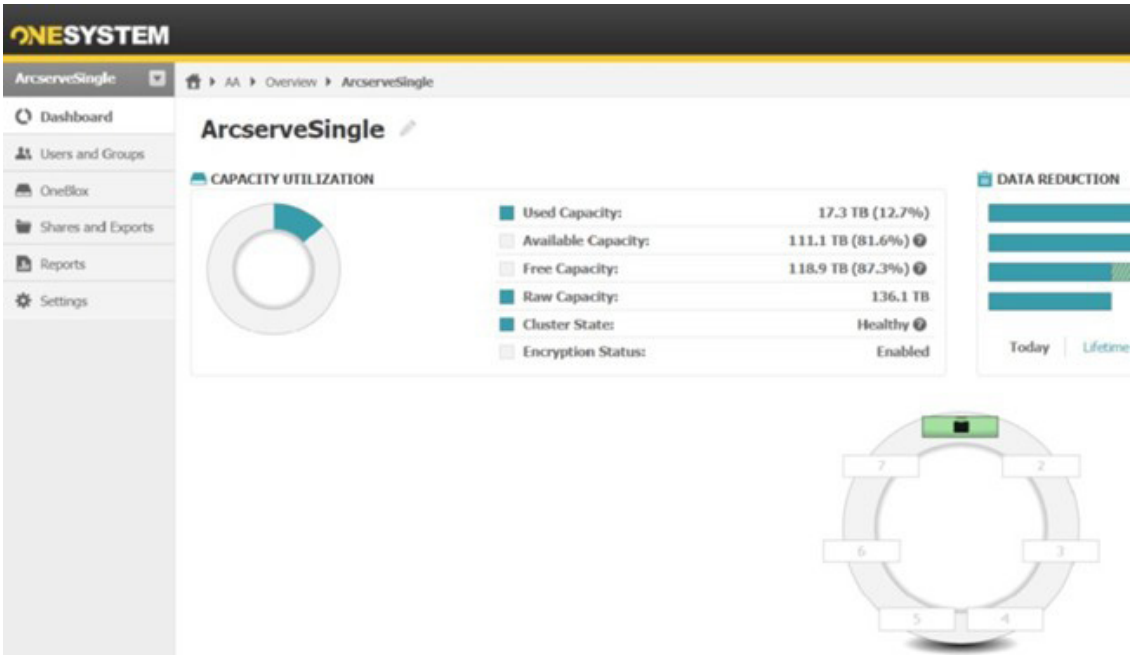
Dieser Abschnitt enthält Informationen zum Erstellen von SMB-Freigaben im OneXafe-Speichersystem.

Führen Sie diese Schritte durch:

1. Melden Sie sich bei dem OneSystem-Konto an, das das OneXafe-System verwaltet.
2. Klicken Sie auf der Übersichtsseite auf den entsprechenden Ring.



Die Dashboard-Seite für den ausgewählten Ring wird geöffnet.



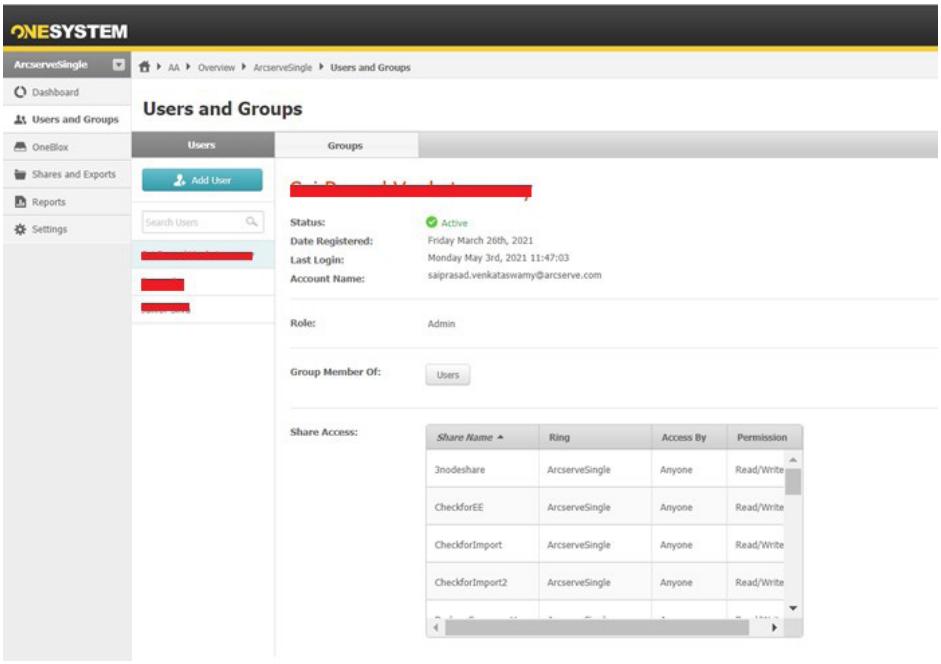
3. Um Benutzer mit verschiedenen Berechtigungsstufen zu erstellen, die spezifisch für OneSystem sind, klicken Sie auf **User and Groups**. Sie können dieselben Benutzer für die Zugriffsberechtigungen von OneXafe Share verwenden.

Hinweis: Standardmäßig haben alle Benutzer im Active Directory (AD) Zugriff auf die OneXafe-Freigaben. Wir empfehlen daher die Bewährten Methoden für die Sicherung von Active Directory von Microsoft.

Bei Benutzern, die auf AD beschränkt sind, wird die Zugriffsrichtlinie auf alle SMB-Freigaben innerhalb des OneXafe-Clusters angewendet. Dadurch wird eine Freigabe erstellt, auf die alle registrierten AD-Benutzer in Ihrer Organisation lesend und schreibend zugreifen können. Nun kann jeder Domänen-Administrator oder delegierte AD-Administrator die Berechtigungen oder ACLs innerhalb der Freigabe nach Belieben ändern (siehe Active Directory-Benutzer und -Computer).

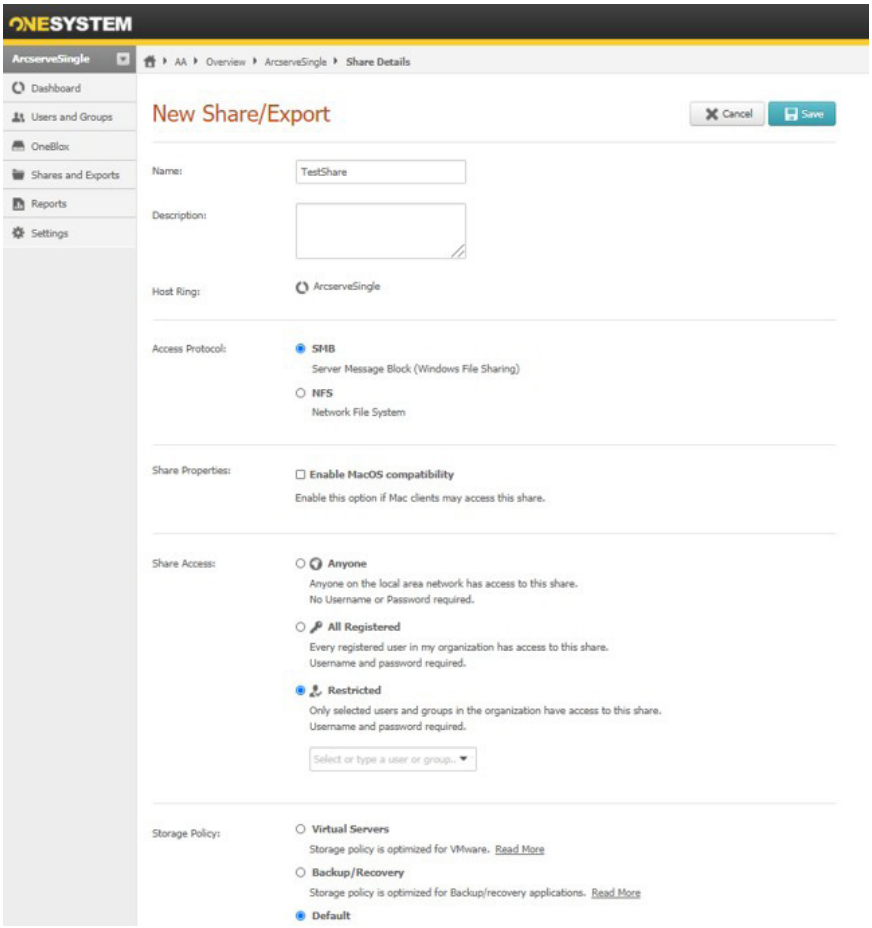
Wenn OneXafe nur als Sicherungsziel und nicht für allgemeine Dateifreigabezwecke verwendet wird, empfehlen wir, das OneXafe-System nicht mit Active Directory (AD) zu verbinden. Wenden Sie diese Maßnahme an, um Ihre Datensicherungsinfrastruktur besser zu trennen, falls Active Directory kompromittiert wird.

Delegierte Admininstatoren, Benutzer und/oder Gruppen können auf Wunsch zur Freigabe hinzugefügt werden. Dadurch erhalten die aufgeführten Mitglieder explizite AD ACL-Kontrolle.



4. Klicken Sie auf **Shares and Exports** und dann auf die Schaltfläche **Add**.

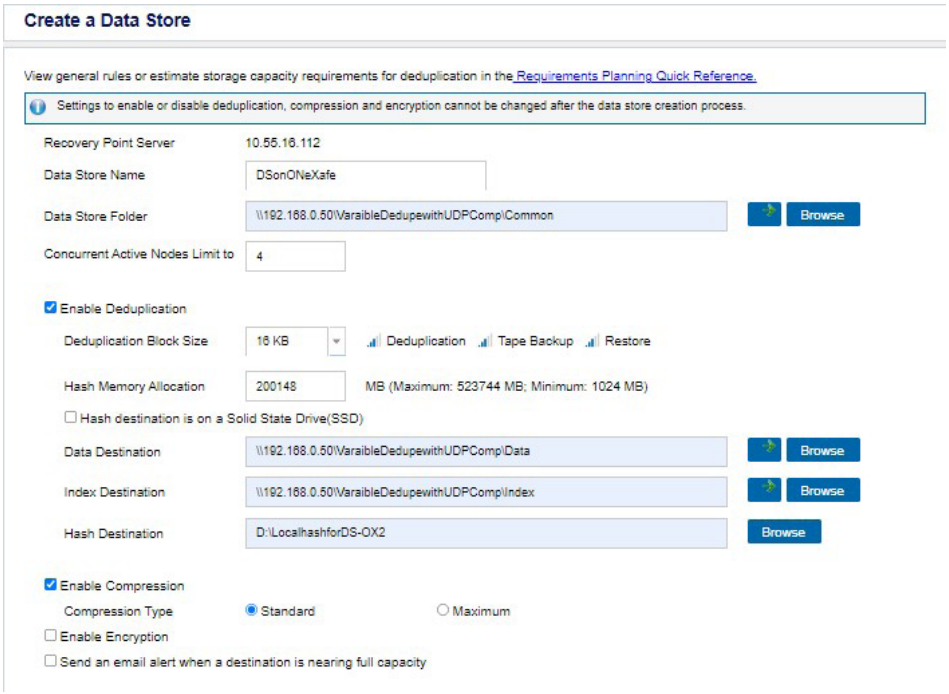
5. Wählen Sie im Bildschirm „New Share/Export“ für „Access Protocol“ die Option **SMB**.
6. Um den Lese- und Schreibzugriff für einen bestimmten Benutzer freizugeben, wählen Sie für „Share Access“ die Option **Restricted** aus und wählen Sie dann einen Benutzer oder eine Gruppe aus oder geben Sie diese ein, falls erforderlich.



UDP-Deduplizierungs-Datenspeicher erstellen

Bevor Sie die in diesem Abschnitt angegebenen Schritte ausführen, melden Sie sich bei der UDP-Konsole an und tun Folgendes.

- Wählen Sie für die Deduplizierungsblockgröße die Option 64 KB und geben Sie dann einen lokalen Ordnerpfad für Hash-Pfad an.
- Stellen Sie sicher, dass alle verbleibenden Pfade für den Deduplizierungs-Datenspeicher wie Dataspeicher-Ordner, Datenziel und Indexziel auf OneXafe Cluster liegen.
- Stellen Sie sicher, dass Sie den Freigabepfad mit OneXafe Cluster Virtual IP angeben. Die virtuelle IP von OneXafe Cluster ist unabhängig von jeder Knoten-IP des Clusters und macht die Freigabe hoch verfügbar.



Datenspeicher hinzufügen

Um ein Ziel zu erstellen, benötigt der Wiederherstellungspunkt-Server Datenspeicher. Der Datenspeicher gibt an, wo die Backup-Daten gespeichert werden. Sie können mehrere Datenspeicher zu einem RPS hinzufügen.

Führen Sie diese Schritte durch:

1. Klicken Sie auf die Registerkarte „Resources“.
2. Navigieren Sie im linken Fensterbereich zu „Destinations“ und klicken Sie auf „Recovery Point Servers“. Die Ziele: Die Seite „Recovery Point Servers“ wird angezeigt.
3. Führen Sie eine der folgenden Aktionen aus.
   - Klicken Sie mit rechts auf einen Wiederherstellungspunkt-Server.
   - Wählen Sie einen Wiederherstellungspunkt-Server aus und klicken Sie im mittleren Bereich auf die Dropdown-Liste „Actions“.

   Eine Liste mit Aktionen wird angezeigt.
4. Klicken Sie auf „Add a Data Store“.

   Die Seite „Create a Data Store“ wird mit dem Namen des angegebenen Wiederherstellungspunkt-Servers angezeigt.
5. Füllen Sie die folgenden Felder aus und klicken Sie auf „Save“.

Recovery Point Server

Definiert den Wiederherstellungspunkt-Server, auf dem der Datenspeicher erstellt wird. Der Wiederherstellungspunkt-Server wurde bereits standardmäßig hinzugefügt.

Data Store Name

Gibt den Namen des Datenspeichers an.

Data Store Folder

Legt den Speicherort des Ordners fest, in dem der Datenspeicher erstellt wird. Klicken Sie auf „Browse“, um den Zielordner auszuwählen.

Concurrent Active Nodes Limit to

Gibt die maximale Anzahl gleichzeitiger Jobs auf dem Datenspeicher an.

Default Value: 4

Ein Wert von 1 bis 9999. Der Wert gibt die Anzahl der Jobs an, die gleichzeitig ausgeführt werden können. Wenn die laufenden Jobs der Anzahl entsprechen, wird ein weiterer Job in die Warteschlange gestellt und der Job kann erst starten, wenn einer der laufenden Jobs abgeschlossen ist. Der abgeschlossene Job kann ein beendeter, abgebrochener oder fehlgeschlagener Job sein.

Der Wert gilt für die Jobtypen, aber nicht für die Serverknoten. Die Zahl 5 zeigt zum Beispiel an, dass fünf Backup-Jobs laufen. Jeder Job, der nach fünf Backup-Jobs geplant wurde, wartet in der Warteschlange, aber Sie können einen anderen Job wie z. B. den Dateisystemkatalog einreichen.

Wenn der Wert mehr als 16 oder 32 beträgt, werden Meldungen angezeigt, um vor der erhöhten Anforderung an die Hardware zu warnen.

Hinweis: Die Beschränkung der Anzahl wirkt sich nur auf den Replikations-Ausgangs-Job aus, nicht auf den Replikations-Eingangs-Job. Die Beschränkung der Anzahl wirkt sich nicht auf Wiederherstellungs- oder BMR-Jobs aus. Solche Jobs werden nicht in eine Warteschlange aufgenommen.

Enable Deduplication

Gibt an, dass die Deduplizierung für diesen Datenspeicher aktiviert ist. Arcserve UDP unterstützt beide Arten der Deduplizierung: Quellenseitige Deduplizierung und globale Deduplizierung. Die quellenseitige Deduplizierung verhindert, dass doppelte Datenblöcke von einem bestimmten Agenten über das Netzwerk verschoben werden. Die globale Deduplizierung eliminiert doppelte Daten auf allen Client-Rechnern auf der Ebene des Volume-Clusters.

Deduplication Block Size

Definiert die Größe der Deduplizierungsblöcke. Die Optionen sind 4 KB, 8 KB, 16 KB, 32 KB und 64 KB. Die Größe der Deduplizierungsblöcke wirkt sich auch auf die Schätzung der Deduplizierungskapazität aus. Wenn Sie z. B. den Standardwert von 16 KB auf 32 KB ändern, verdoppeln sich die Schätzungen der Deduplizierungskapazität. Eine Erhöhung der Deduplizierungsblockgröße kann den Deduplizierungsprozentsatz verringern.

Hash Memory Allocation

Gibt den Umfang des physischen Speichers an, den Sie für die Speicherung von Hashes zuweisen. In diesem Feld wird der Standardwert vorgegeben. Der Standardwert basiert auf der folgenden Kalkulation:

Wenn der physische Speicher des RPS kleiner als 4 GB ist (oder mit 4 GB identisch ist), ist der Standardwert von **Hash Memory Allocation** identisch mit dem physischen Speicher des RPS.

Wenn der physische Speicher des RPS größer als 4 GB ist, berechnet Arcserve UDP den zu diesem Zeitpunkt verfügbaren freien Speicher. Nehmen Sie an, dass der verfügbare freie Speicher derzeit X GB beträgt. Arcserve UDP überprüft außerdem die folgenden Bedingungen:

- Wenn (X * 80 %) > = 4 GB, ist der Standardwert von **Hash Memory Allocation** (X * 80 %).
- Wenn (X * 80 %) < 4 GB, ist der Standardwert von **Hash Memory Allocation** 4 GB.

Beispiel: Nehmen wir den Fall, dass RPS 32 GB physikalischem Speicher hat. Angenommen, das Betriebssystem und andere Anwendungen verwenden beim Erstellen des Datenspeichers 4 GB Speicher. Der verfügbare freie Arbeitsspeicher beträgt zu diesem Zeitpunkt 28 GB. Dann ist der Standardwert von **Hash Memory Allocation** 22,4 GB (22,4 GB = 28 GB * 80 %).

Hash Destination is on a Solid State Drive (SSD)

Gibt an, ob sich der Hash-Ordner auf einem Solid-State-Laufwerk befindet.

Hinweis: Konfigurieren Sie die Hash Destination auf der lokalen SSD, wenn die Option „Hash destination is on a Solid State Drive(SSD)“ aktiviert ist.

Data Destination

Definiert den Datenzielordner zum Speichern der tatsächlichen eindeutigen Datenblöcke. Verwenden Sie die größte Festplatte zum Speichern von Daten, da diese die Originaldatenblöcke der Quelle enthält.

Hinweis: Der Pfad für „Data Destination“ sollte ein leerer Ordner sein.

Index Destination

Definiert den Index-Zielordner zum Speichern der Indexdateien. Wählen Sie einen anderen Datenträger, um die Deduplizierungsverarbeitung zu verbessern.

Hinweis: Der Pfad für „Index Destination“ sollte ein leerer Ordner sein.

Hash Destination

Definiert den Pfad zum Speichern der Hash-Datenbank. Arcserve UDP verwendet den SHA1-Algorithmus, um den Hash für Quelldaten zu erzeugen. Die Hash-Werte werden von der Hash-Datenbank verwaltet. Die Auswahl eines schnellen Solid-State-Laufwerks (SSD) erhöht die Deduplizierungskapazität und erfordert eine geringere Speicherzuweisung. Für eine bessere Hash-Performance empfehlen wir, das SSD-Volume als NTFS-Dateisystem mit 4 KB Volume-Clustergröße zu formatieren.

Hinweis: Der Pfad für „Hash Destination“ sollte ein leerer Ordner sein.

Hinweis: Sie können für die folgenden vier Ordner nicht denselben Pfad angeben: Data Store, Data Destination, Index Destination und Hash Destination.

Enable Compression

Gibt an, dass die Datenkomprimierungseinstellungen aktiviert sind.

Compression Type

Gibt an, ob der Standard- oder der maximale Kompressionstyp verwendet werden soll.

Die Komprimierung wird oft gewählt, um den Speicherplatzbedarf zu verringern, wirkt sich aber aufgrund der erhöhten CPU-Auslastung auch negativ auf die Backup-Geschwindigkeit aus. Basierend auf Ihren Anforderungen können Sie eine der drei verfügbaren Optionen auswählen.

Hinweis: Weitere Informationen finden Sie unter Komprimierungstyp.

Enable Encryption

Gibt an, dass die Verschlüsselungseinstellungen aktiviert sind. Wenn Sie diese Option wählen, müssen Sie das Verschlüsselungspasswort angeben und bestätigen.

Datenverschlüsselung ist die Übersetzung von Daten in eine Form, die ohne einen Entschlüsselungsmechanismus unverständlich ist. Die Arcserve UDP-Lösung verwendet sichere AES-Verschlüsselungsalgorithmen (Advanced Encryption Standard), um ein Maximum an Sicherheit und Schutz für Ihre Daten zu erreichen. Für Datenspeicher wird Verschlüsselung oder keine Verschlüsselung unterstützt. Für die Verschlüsselung steht nur AES-256 zur Verfügung.

Ein Passwort ist nicht erforderlich, wenn Sie versuchen, auf dem Computer wiederherzustellen, von dem der Backup durchgeführt wurde. Wenn Sie jedoch versuchen, auf einem anderen Computer wiederherzustellen, ist ein Passwort erforderlich. Standardmäßig ist nur beim ersten Anmelden ein Passwort erforderlich. Um das Passwort auch nach der ersten Anmeldung einzugeben, muss der Administrator den Arcserve UDP Agent Explorer Extension Service manuell stoppen.

Send an email alert when a destination is nearing full capacity

Wenn Sie diese Option auswählen, wird der Datenspeicher so konfiguriert, dass er eine E-Mail-Warnung sendet. RPS sendet E-Mail-Warnungen an Empfänger, wenn der Zielordner des Datenspeichers fast voll ist.

Configure Email

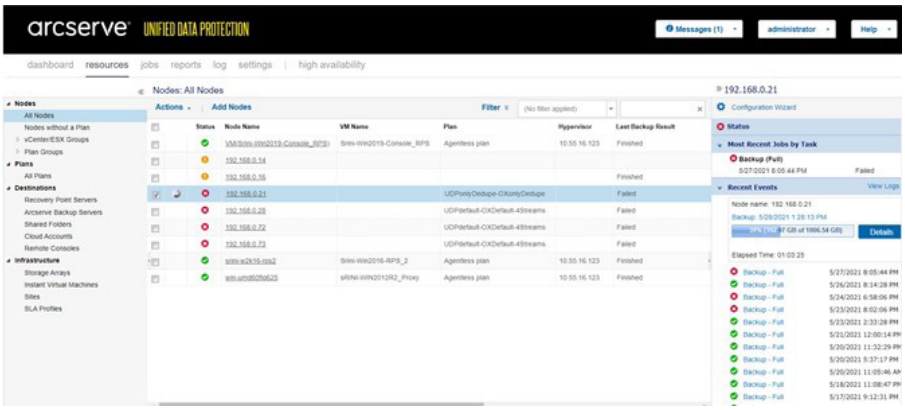
Diese Schaltfläche wird nur angezeigt, wenn Sie die Option „Send an email alert when a destination is nearing full capacity“ aktivieren. Mit dieser Schaltfläche können Sie eine E-Mail-ID angeben, um Warnungen zu erhalten. Klicken Sie auf die Schaltfläche „Configure Email“, um die globalen E-Mail-Alarmeinstellungen aus „Console>Settings>Email and Alert configuration“ zu laden. Wenn die globalen E-Mail-Einstellungen nicht verfügbar sind, wird durch Klicken auf die Schaltfläche „Configure Email“ das Dialogfeld „Email settings“ geöffnet, um E-Mail-Details festzulegen.

Der Datenspeicher wird erstellt und im mittleren Bereich angezeigt. Klicken Sie auf den Datenspeicher, um die Details im rechten Bereich anzuzeigen.

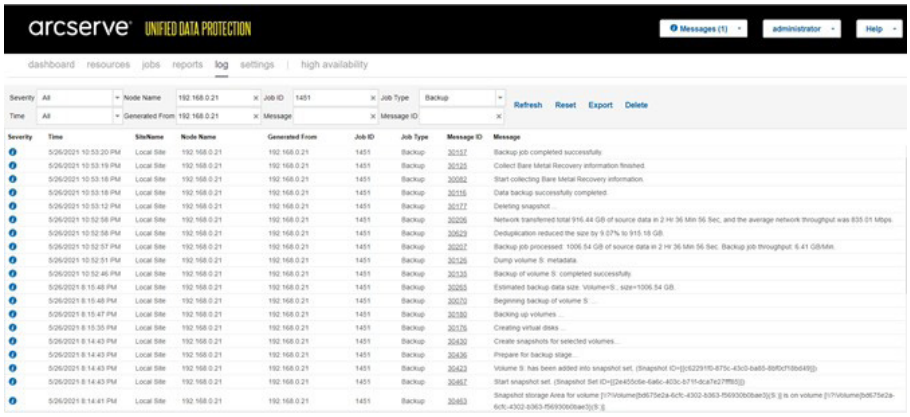
Wiederherstellung nach einem Ransomware-Angriff

Bei einem Ransomware-Angriff oder einem Angriff auf den Arcserve UDP Recovery Point Server kann es zu einem Datenverlust des Backup-Wiederherstellungspunkts kommen. Daher empfehlen wir Ihnen, Folgendes durchzuführen:

- Windows neu installieren
- Neues Passwort festlegen
- UDP neu installieren
- Identifizieren Sie den gültigen Snapshot und legen Sie den Snapshot dann als neue Freigabe fest. Um gültige Snapshots zu identifizieren, gehen Sie wie folgt vor:
  1. Suchen Sie den richtigen Zeitpunkt imm Arcserve UDP-Aktivitätsprotokoll.
     a. Melden Sie sich bei der UDP-Konsole an und klicken Sie auf „All nodes“.
     b. Wählen Sie den Knoten aus, für den Backups auf Ziele geplant sind, die sich auf einer OneXafe-SMB-Freigabe befinden.
     c. Klicken Sie im rechten Bereich auf den entsprechenden Backup-Job.



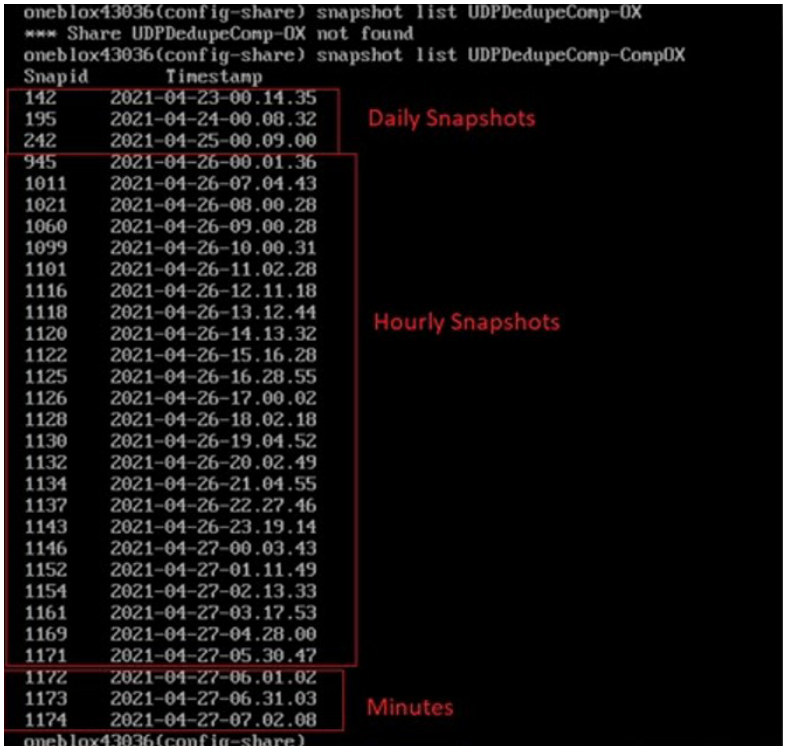
Notieren Sie sich die Fertigstellungszeit für jeden erfolgreichen UDP-Backup-Job.



2. Identifizieren Sie den richtigen Snapshot in der OneXafe-Benutzeroberfläche anhand der UDP-Job-Abschlusszeit.

Um eine Liste des Snapshots abzurufen, gehen Sie wie folgt vor:

1. Melden Sie sich bei der OneXafe-Konsole an und führen Sie dann die folgenden Befehle aus:
   Share
   Snapshot list <<Freigabename>>



2. Wählen Sie den OneXafe-Snapshot, der nach dem letzten erfolgreichen Snapshot auf der UDP-Seite erstellt wurde.

Erforderliche Zugangsdaten während der Wiederherstellung

Halten Sie für den Fall einer Wiederherstellung die Anmeldedaten für Folgendes bereit:

- OneXafe iDRAC
- Lokales OneXafe-Administratorkonto (Befehlszeile)
- OneSystem-Administratorkonto (für Verwaltung)
- OneSystem-Benutzerkonto (für RPS-Ddatenspeicherzugriff)
- UDP-System - Windows-Administrator und IPMI
- UDP RPS-Datenspeicher-Verschlüsselungspasswort (falls verwendet)
- UDP Plan-Passwörter (falls verwendet)

OneXafe-Snapshot zu einer neuen Freigabe hochstufen

Um einen OneXafe-Snapshot zu einer neuen Freigabe hochzustufen, verwenden Sie die folgenden Befehle:

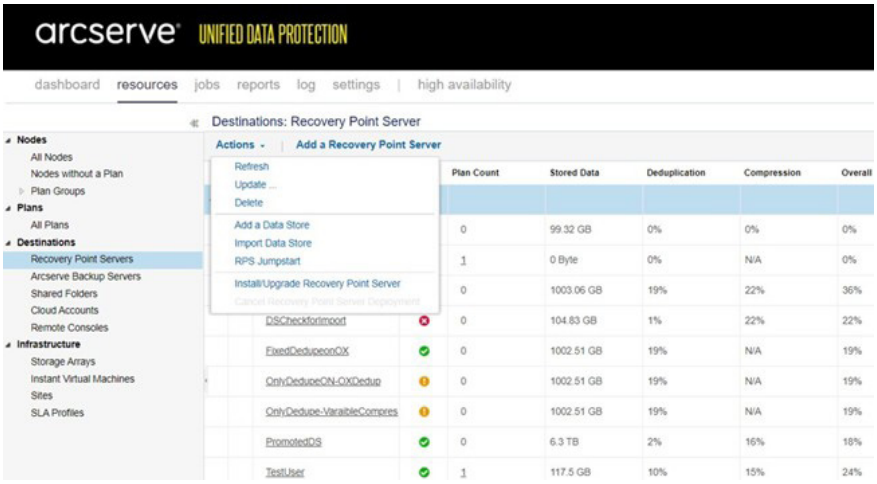
```
oneblox43005(config-share) enable
oneblox43005(config-share) snapshot list <<share name>>
oneblox43005(config-share) snapshot promote <<old sharename>> <<snapshotid>>
<<new sharename>>
oneblox43005(config-share) update <<new sharename>> -writeable
oneblox43005(config-share) disable
```

Deduplizierungs-Datenspeicher in UDP importieren

Dieser Abschnitt enthält Informationen zum Importieren eines Deduplizierungs-Datenspeichers in UDP.

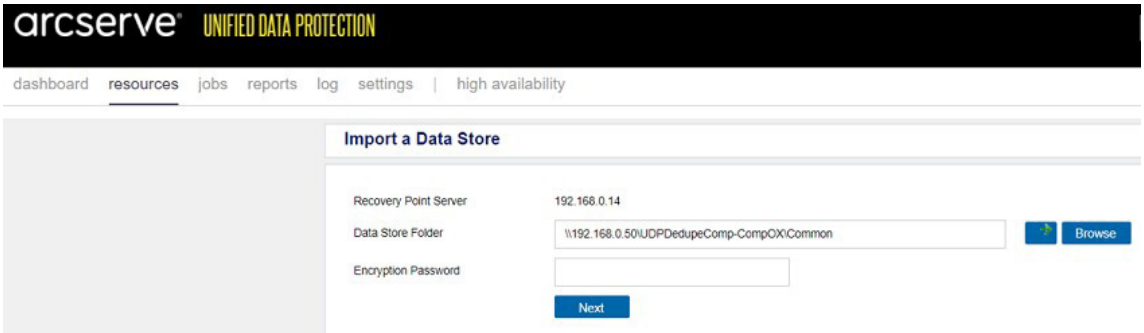
Führen Sie diese Schritte durch:

1. Melden Sie sich bei der UDP-Konsole an.
2. Klicken Sie auf der Registerkarte „Resources“ unter „Ziele“ auf **Recovery Point Servers**.
3. Wählen Sie in der Dropdown-Liste „Actions“ die Option **Import Data Store**.

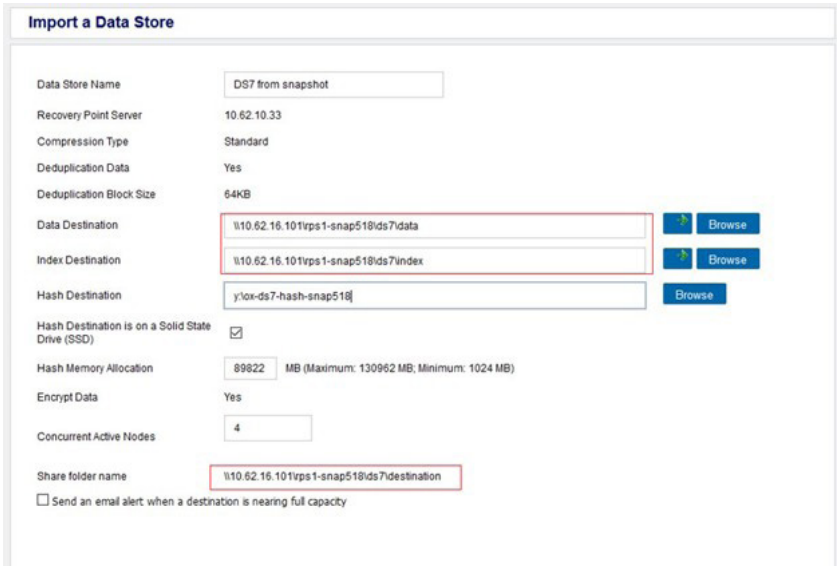


Die Seite „mport a Data Store“ wird geöffnet.

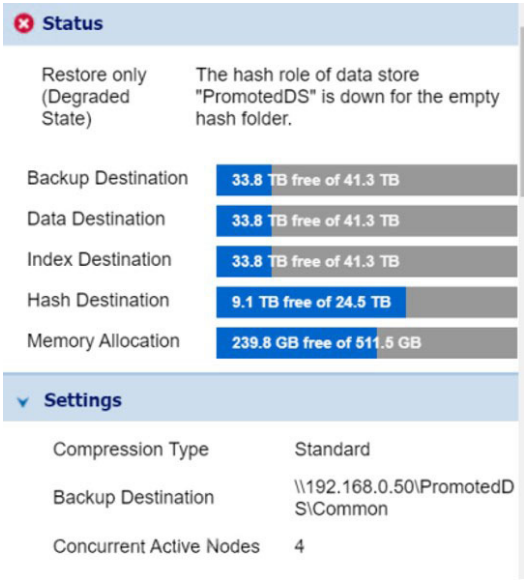
4. Um den Pfad zum Datenspeicher-Ordner auszuwählen, klicken Sie auf die Schaltfläche **Browse**, wählen Sie den Pfad aus und klicken Sie dann auf **Next**.



5. Ordnen Sie im Bildschirm „Import a Data Store“ basierend auf dem Pfad des Freigabeordners die entsprechenden Pfade für **Data Destination** und **Index Destination** zu.



6. Geben Sie für Hash einen leeren Ordnerpfad an und klicken Sie dann auf **Save**. Der Datenspeicher wird im Modus **Restore Only** importiert.



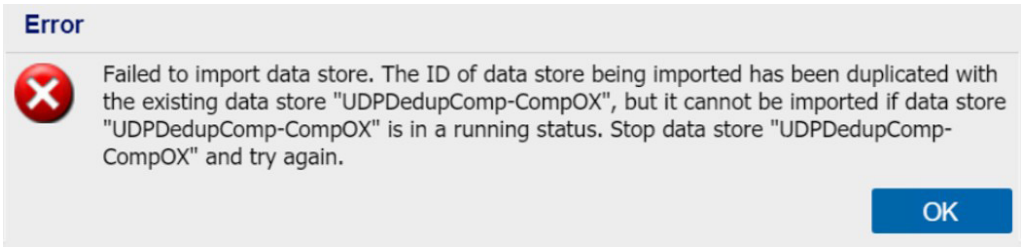
Hinweis: Im Modus Restore only können Sie beliebige Dateien und Ordner wiederherstellen.

7. Um die Hash-Daten des Deduplizierungs-Datenspeichers neu zu generieren, navigieren Sie von der Befehlszeile aus zu C:\Programme\Arcserve\Unified Data Protection\Engine\BIN auf dem UDP-Wiederherstellungspunkt-Server, führen Sie **as_gddmgr.exe** aus, und verwenden Sie dann den folgenden Befehl:

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

8. Nachdem die Hash-Generierung abgeschlossen ist, können Sie den Datenspeicher starten und den vorhandenen Plan so ändern, dass er auf den neuen Datenspeicher verweist. Sie können diesen neuen Datenspeicher verwenden, um für zukünftige Backups weiter zu schreiben.

Wenn Sie die neue Freigabe auf denselben UDP-Server importieren, auf dem sich der alte Datenspeicher befindet, wird die folgende Fehlermeldung angezeigt.



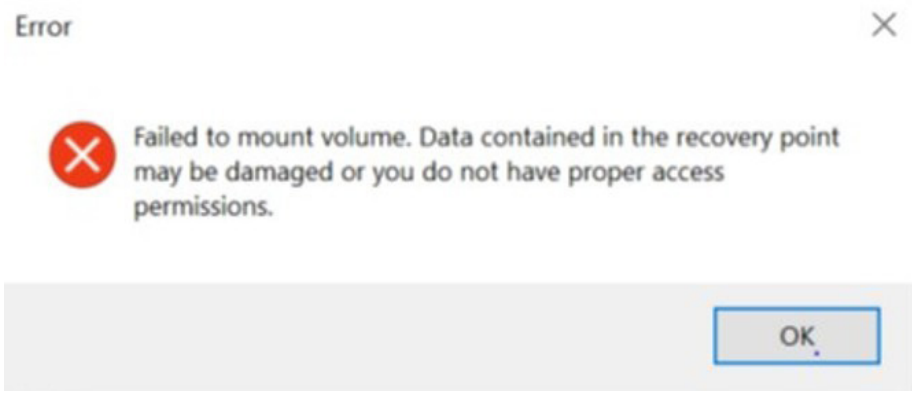
Wir empfehlen, den Datenspeicher auf einen neuen Server zu importieren oder den alten Datenspeicher vollständig aus UDP zu löschen, da die Authentifizierung bereits beeinträchtigt ist.

Bekannte Einschränkungen

- Bei OneXafe werden die Snapshots als neue Freigaben mit denselben Benutzerberechtigungen wie die ursprüngliche Freigabe hochgestuft. Während des Hochstufens des Snapshots können Sie keine andere Authentifizierung anbieten.

  Nachdem die Freigabe mit der OneSystem-Anmeldung erstellt wurde, können Sie die Berechtigungen für die neue Freigabe ändern.

- Das Navigieren zur OneXafe-Freigabe aus dem Windows-Explorer und der Wechsel in die UDP-Wiederherstellungspunkt-Server-Ansicht schlägt fehl, wenn sich das Ziel auf der OneXafe-Freigabe befindet.



- Wenn während Wartungsarbeiten oder aus anderen Gründen einer der Knoten im OneXafe-Cluster heruntergefahren wird, kann der aktive UDP-Backup-Job mit dem folgenden Fehler fehlschlagen:

  An error has occurred from deduplication Data role on server 192.168.0.14. Fehlermeldung = [The operations for this file (create, close, read, write) failed.]. Möglicherweise tritt das gleiche Verhalten auf, wenn der OneXafe-Knoten wieder eingeschaltet wird.

  Der nächste geplante Backup-Job wird durch diesen Vorgang keine Auswirkungen haben.