

Acronis

Acronis Cyber Infrastructure 3.5

Backup Gateway –
Schnellstartanleitung für VMware
vSphere

31. Juli 2020

Urheberrechtserklärung

Copyright ©Acronis International GmbH, 2003-2020. Alle Rechte vorbehalten.

'Acronis' and 'Acronis Secure Zone' sind eingetragene Markenzeichen von Acronis International GmbH.

'Acronis Compute with Confidence', 'Acronis Startup Recovery Manager', 'Acronis Instant Restore' und das Acronis Logo sind Markenzeichen von Acronis International GmbH.

Linux ist ein eingetragenes Markenzeichen von Linus Torvalds.

VMware und VMware Ready sind Warenzeichen bzw. eingetragene Markenzeichen von VMware, Inc, in den USA und anderen Jurisdiktionen.

Windows und MS-DOS sind eingetragene Markenzeichen der Microsoft Corporation.

Alle anderen erwähnten Markenzeichen und Urheberrechte sind Eigentum der jeweiligen Besitzer.

Eine Verteilung substantiell veränderter Versionen dieses Dokuments ohne explizite Erlaubnis des Urheberrechtinhabers ist untersagt.

Eine Weiterverbreitung dieses oder eines davon abgeleiteten Werks in gedruckter Form (als Buch oder Papier) für kommerzielle Nutzung ist verboten, sofern vom Urheberrechtsinhaber keine Erlaubnis eingeholt wurde.

DIE DOKUMENTATION WIRD „WIE VORLIEGEND“ ZUR VERFÜGUNG GESTELLT UND ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGEND MITINBEGRIFFENEN BEDINGUNGEN, ZUSAGEN UND GEWÄHRLEISTUNGEN, EINSCHLIESSLICH JEDLICHER STILLSCHWEIGEND MITINBEGRIFFENER GARANTIE ODER GEWÄHRLEISTUNG DER EIGNUNG FÜR DEN GEWÖHNLICHEN GEBRAUCH, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER GEWÄHRLEISTUNG FÜR RECHTSMÄNGEL SIND AUSGESCHLOSSEN, AUSSER WENN EIN DERARTIGER GEWÄHRLEISTUNGS AUSSCHLUSS RECHTLICH ALS UNGÜLTIG ANGESEHEN WIRD.

Die Software bzw. Dienstleistung kann Code von Drittherstellern enthalten. Die Lizenzvereinbarungen für solche Dritthersteller sind in der Datei 'license.txt' aufgeführt, die sich im Stammordner des Installationsverzeichnis befindet. Eine aktuelle Liste des verwendeten Dritthersteller-Codes sowie der dazugehörigen Lizenzvereinbarungen, die mit der Software bzw. Dienstleistung verwendet werden, finden Sie unter <http://kb.acronis.com/content/7696>.

Von Acronis patentierte Technologien

Die in diesem Produkt verwendeten Technologien werden durch einzelne oder mehrere U.S.-Patentnummern abgedeckt und geschützt: 7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234; sowie weitere, schwebende Patentanmeldungen.

Inhaltsverzeichnis

1. Über diese Anleitung	1
1.1 Anforderungen	1
2. Netzwerke konfigurieren	3
3. Virtuelle Maschinen erstellen	6
4. Acronis Cyber Infrastructure in virtuellen Maschinen bereitstellen	12
4.1 Den Management-Knoten bereitstellen	13
4.2 Sekundäre Knoten bereitstellen	15
5. Speicherplatz zu Acronis Cyber Infrastructure hinzufügen	17
6. Die Acronis Backup-Software über das Backup Gateway mit Storage-Backends verbinden	19
6.1 Über das Backup Gateway mit dem lokalen Storage-Cluster verbinden	20
6.2 Über das Backup Gateway mit externen NFS-Freigaben verbinden	23
6.3 Über das Backup Gateway mit Public Clouds verbinden	26
6.3.1 Wichtige Anforderungen und Einschränkungen	27
6.3.2 Das Backup Gateway einrichten	28

KAPITEL 1

Über diese Anleitung

In dieser Anleitung wird die Bereitstellung von Acronis Cyber Infrastructure sowie die Konfiguration des Backup Gateways auf VMware vSphere 6.5 (und höher) erläutert.

Kurz umrissen, müssen Sie Folgendes tun:

1. Konfigurieren Sie Netzwerke.
2. Erstellen Sie virtuelle Maschinen für Acronis Cyber Infrastructure.
3. Stellen Sie Acronis Cyber Infrastructure in den virtuellen Maschinen bereit.

All diese Schritte werden in den nachfolgenden Kapiteln ausführlicher beschrieben.

Nachdem Acronis Cyber Infrastructure bereitgestellt wurde, müssen Sie es für Ihr Szenario konfigurieren. Die Schritte zum Einrichten eines Backup Gateways werden im Abschnitt *„Die Acronis Backup-Software über das Backup Gateway mit Storage-Backends verbinden“* (Seite 19) erläutert. Weitere Anweisungen sind in der Anleitung für Administratoren aufgeführt.

1.1 Anforderungen

- Für das Backup Gateway-Szenario kann Acronis Cyber Infrastructure in einer einzelnen virtuellen Maschine bereitgestellt werden. Für allgemeine Bereitstellungen wird jedoch empfohlen, drei oder fünf virtuelle Maschinen zu erstellen, um Lastverteilung und Hochverfügbarkeit zu ermöglichen.
- Überprüfen Sie, dass der vSphere-Datenspeicher genügend freien Speicherplatz hat. Jede virtuelle Maschine belegt mindestens 425 GB (zwei 200-GB-Storage-Laufwerke und ein 25-GB-System-Laufwerk). Die Acronis Cyber Infrastructure-Vorlage nimmt ebenfalls ca. 35 GB ein.

- Stellen Sie sicher, dass der Host genügend Arbeitsspeicher hat. Das Minimum für ein Ein-Knoten-Setup beträgt 4 GB RAM. Ansonsten sind mindestens 8 GB RAM für den Management-Knoten erforderlich. Außerdem werden mindestens 4 GB RAM von jedem sekundären Knoten belegt.
- Verwenden Sie einen separaten Objekt-Container für jeden Backup Gateway-Cluster.

Bemerkung: Die vollständigen Hardware-Anforderungen für das Backup Gateway-Szenario sind hier beschrieben: [Hardware Requirements](#).

KAPITEL 2

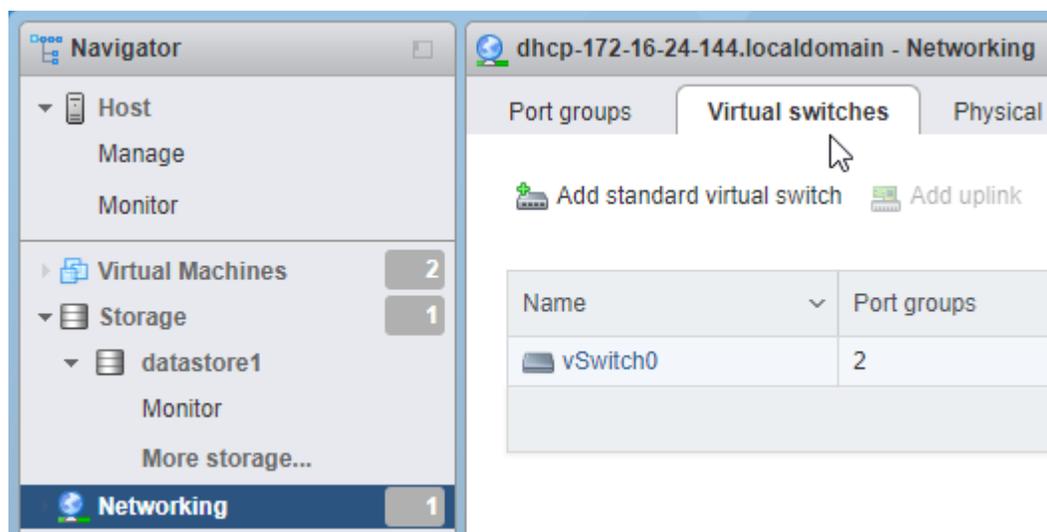
Netzwerke konfigurieren

Acronis Cyber Infrastructure benötigt typischerweise zwei Netzwerke: ‚öffentlich‘ für externe Konnektivität und ‚privat‘ für den Datenaustausch zwischen den virtuellen Maschinen. Während ein öffentliches Netzwerk bereits eingerichtet sein kann, empfehlen wir, auch dann ein dediziertes privates Netzwerk zu erstellen, wenn bereits eines vorhanden ist. Für die Erstellung eines privaten Netzwerks benötigen Sie einen virtuellen Switch mit benutzerdefinierten Sicherheitsparametern und eine Port-Gruppe.

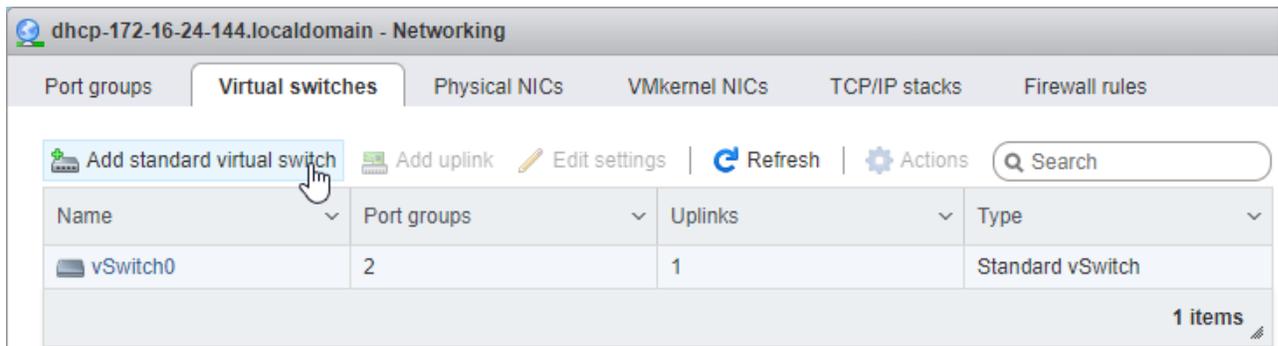
Bemerkung: Die vollständigen Netzwerkanforderungen sind hier aufgeführt: [Planning Network](#).

Befolgen Sie diese Schritte, um einen virtuellen Switch zu erstellen:

1. Klicken Sie im Host-Client im linken Menü auf **Networking**. Öffnen Sie die Registerkarte **Virtuelle Switche**.



2. Klicken Sie in der Symbolleiste auf **Virtueller Standard-Switch hinzufügen**.

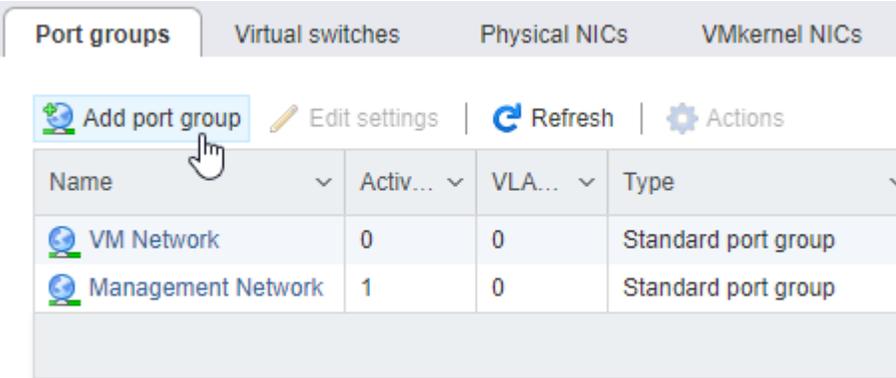


3. Geben Sie den Switch-Namen ein und erweitern Sie **Sicherheit**. Wählen Sie **Akzeptieren** beim **Promiscuous-Modus**, **MAC-Adressänderungen** und **Gefälschte Übertragungen**.

vSwitch Name	Private network switch
MTU	1500
▶ Link discovery	Click to expand
▼ Security	
Promiscuous mode	<input checked="" type="radio"/> Accept <input type="radio"/> Reject
MAC address changes	<input checked="" type="radio"/> Accept <input type="radio"/> Reject
Forged transmits	<input checked="" type="radio"/> Accept <input type="radio"/> Reject

Befolgen Sie diese Schritte, um eine Port-Gruppe zu erstellen:

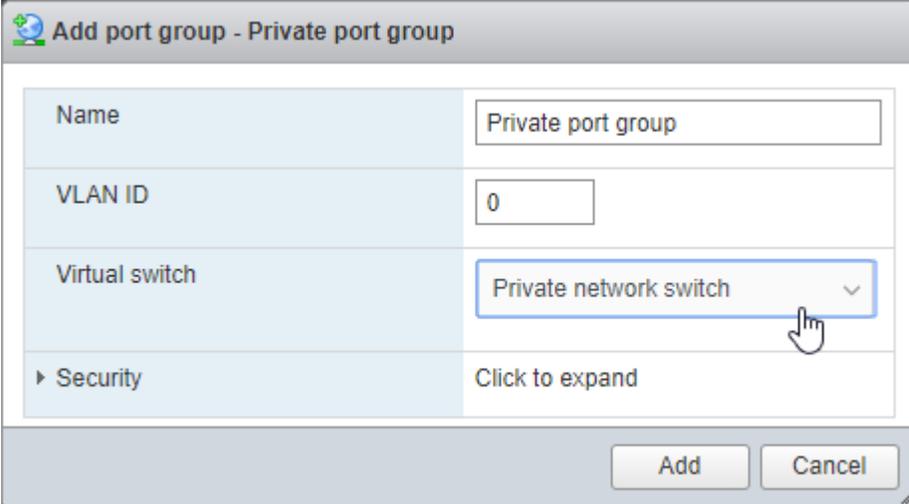
1. Öffnen Sie die Registerkarte **Port-Gruppen** und klicken Sie in der Symbolleiste auf **Port-Gruppe hinzufügen**.



The screenshot shows the 'Port groups' tab in the vSphere Network Configuration interface. The 'Add port group' button is highlighted with a mouse cursor. Below the button is a table listing existing port groups.

Name	Activ...	VLA...	Type
VM Network	0	0	Standard port group
Management Network	1	0	Standard port group

2. Geben Sie den Namen der Port-Gruppe ein. Wählen Sie den virtuellen Switch aus, den Sie zuvor erstellt haben.



The screenshot shows the 'Add port group - Private port group' dialog box. The 'Name' field is 'Private port group', 'VLAN ID' is '0', and 'Virtual switch' is 'Private network switch'. The 'Security' section is collapsed, showing 'Click to expand'. The 'Add' and 'Cancel' buttons are at the bottom right.

Name	Private port group
VLAN ID	0
Virtual switch	Private network switch
Security	Click to expand

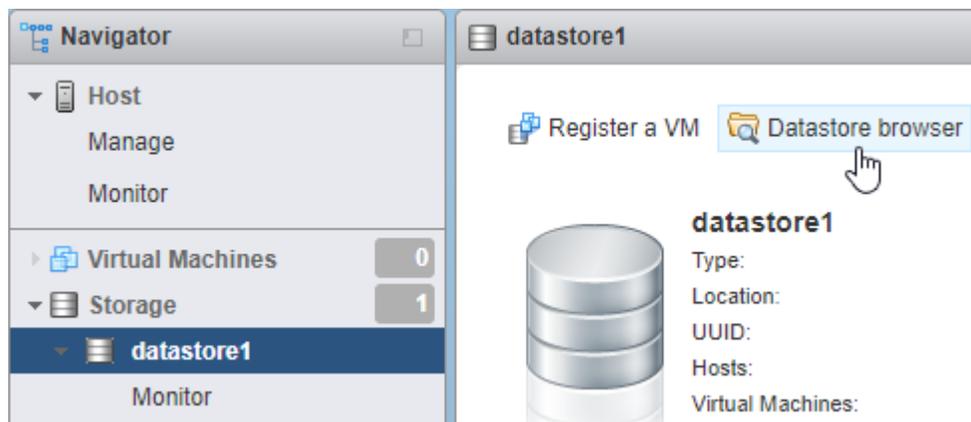
KAPITEL 3

Virtuelle Maschinen erstellen

Beschaffen Sie sich zuerst das Image von Acronis Cyber Infrastructure (zwei VMDK-Dateien). Besuchen Sie dafür die Produktseite und übermitteln Sie eine Anfrage.

Laden Sie anschließend die zwei VMDK-Dateien in den VMware vSphere-Datenspeicher hoch:

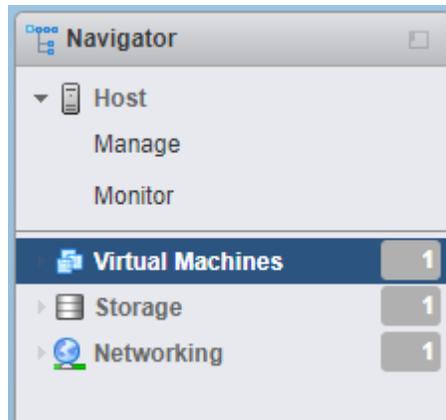
1. Klicken Sie im Fensterbereich **Navigator** auf den gewünschten Datenspeicher. Klicken Sie in dessen Symbolleiste auf **Datenspeicher-Browser**.
2. Erstellen Sie im **Datenspeicher-Browser** ein Verzeichnis, das nach Ihrer virtuellen Maschine benannt ist.



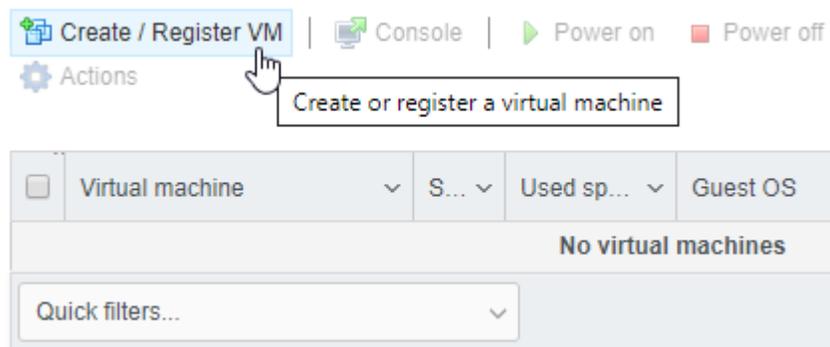
3. Laden Sie das Image von Acronis Cyber Infrastructure (die zwei VMDK-Dateien) in dieses Verzeichnis hoch.

Führen Sie die folgenden Schritte aus, um eine virtuelle Maschine für Acronis Cyber Infrastructure zu erstellen:

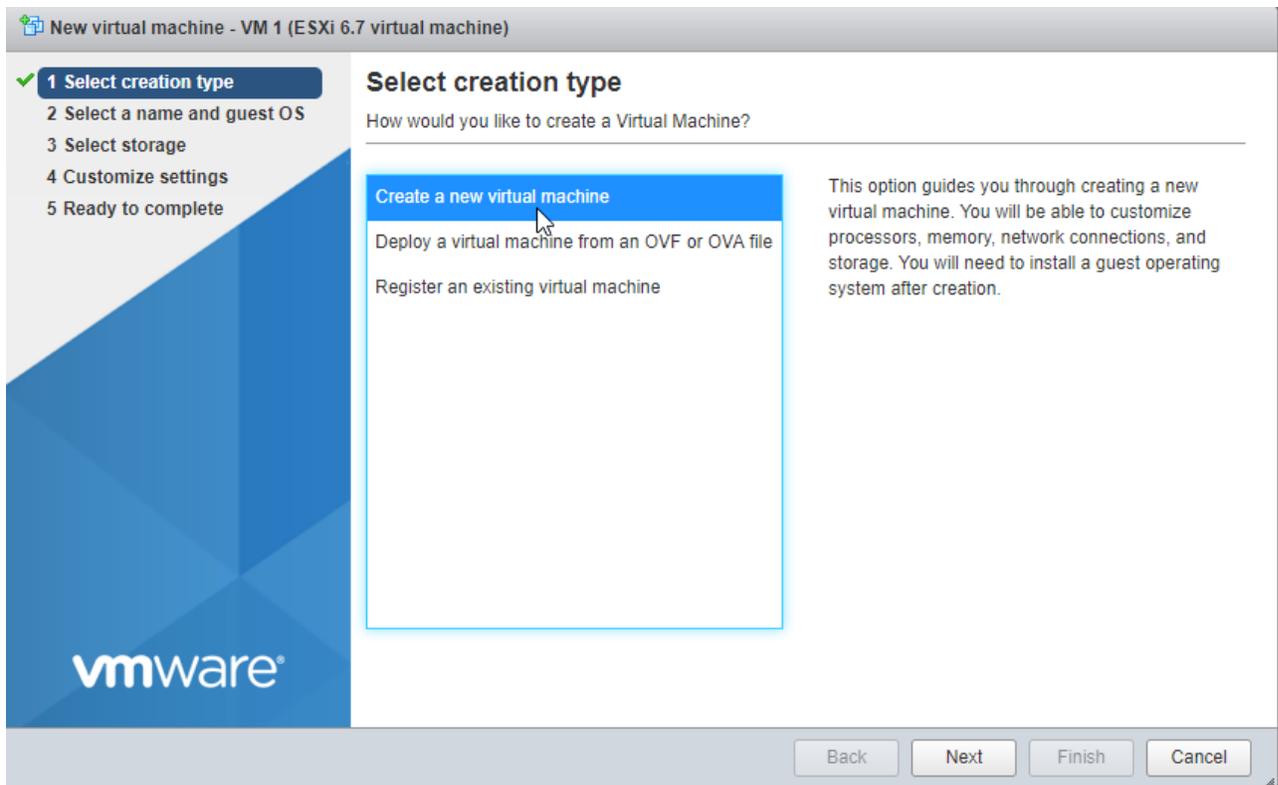
1. Klicken Sie im Host-Client im linken Menü auf **Virtuelle Maschinen**.



2. Klicken Sie in der Symbolleiste auf **Erstellen / VM registrieren**.



3. Wählen Sie in Schritt 1 des Assistenten **Neue virtuelle Maschine** den Befehl **Eine neue virtuelle Maschine erstellen**. Klicken Sie auf **Weiter**.



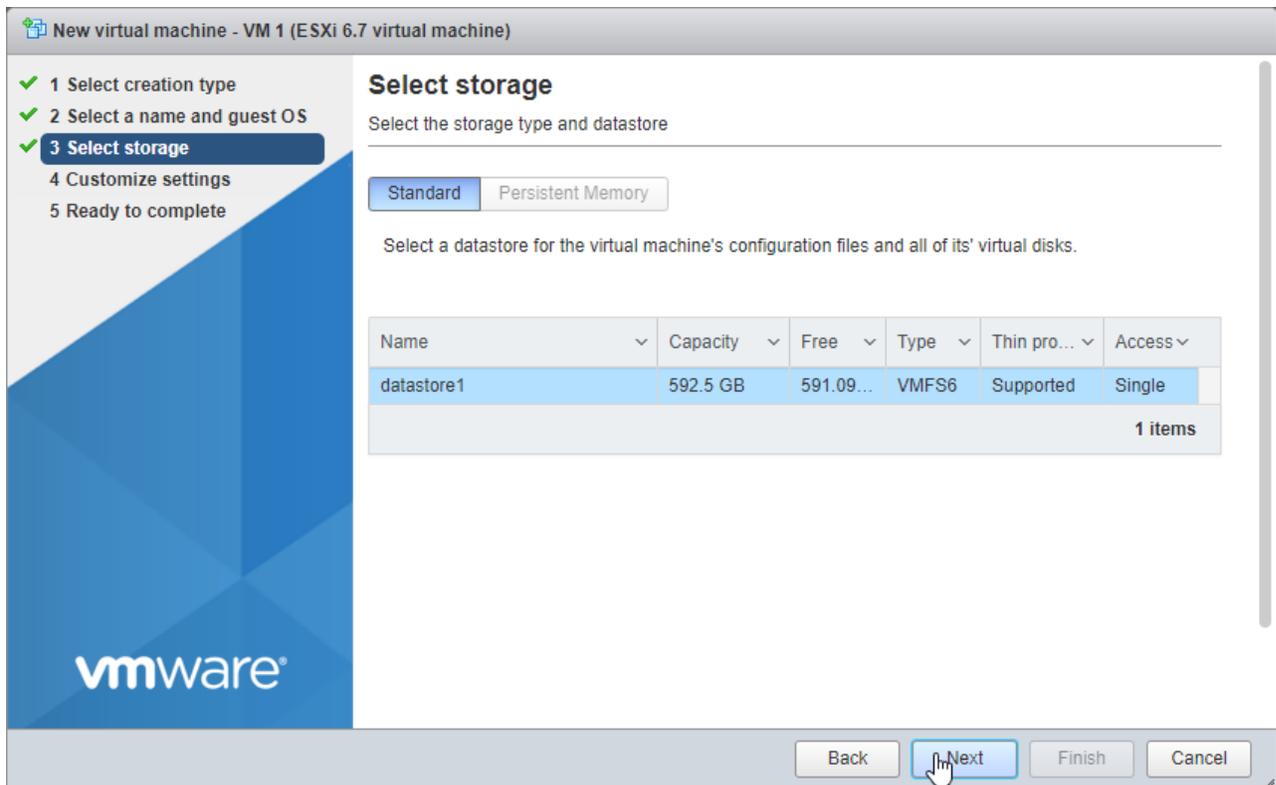
4. Geben Sie in Schritt 2 einen Namen für die virtuelle Maschine ein und wählen Sie dann das Gastbetriebssystem aus. Klicken Sie auf **Weiter**.

The screenshot shows the 'New virtual machine - VM 1 (ESXi 6.7 virtual machine)' wizard. On the left, a progress bar indicates five steps: 1. Select creation type (checked), 2. Select a name and guest OS (highlighted), 3. Select storage, 4. Customize settings, and 5. Ready to complete. The VMware logo is visible at the bottom left of this sidebar.

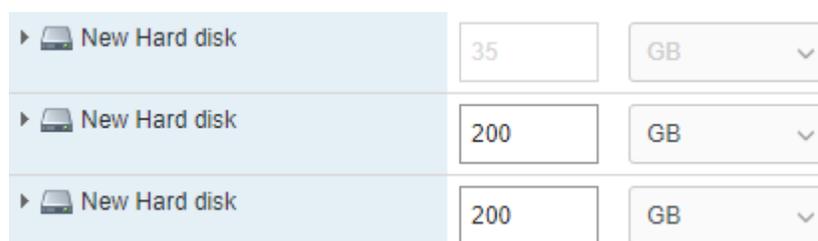
The main area is titled 'Select a name and guest OS' and includes the instruction 'Specify a unique name and OS'. A text input field for 'Name' contains 'VM 1'. Below this, a note states: 'Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance. Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.'

Three dropdown menus are present: 'Compatibility' is set to 'ESXi 6.7 virtual machine', 'Guest OS family' is set to 'Linux', and 'Guest OS version' is set to 'Red Hat Enterprise Linux 7 (64-bit)'. At the bottom right, there are four buttons: 'Back', 'Next' (with a mouse cursor over it), 'Finish', and 'Cancel'.

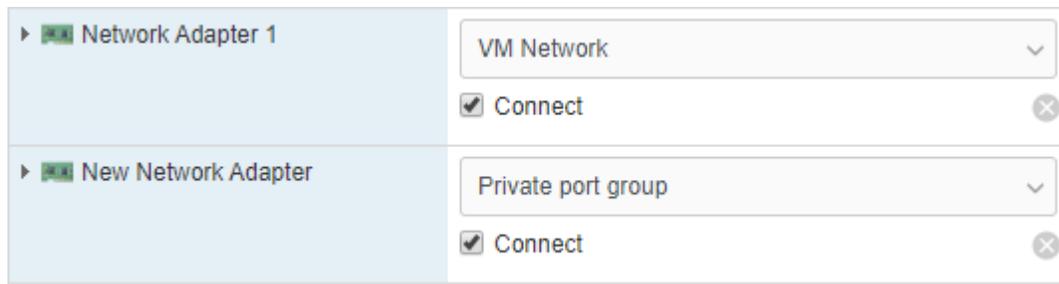
5. Wählen Sie in Schritt 3 den Storage-Typ und den Datenspeicher aus. Überprüfen Sie, dass der Datenspeicher genügend freien Speicherplatz hat.



6. Entfernen Sie in Schritt 4 das vorhandene Laufwerk und klicken Sie in der Symbolleiste auf **Festplatte hinzufügen**. Wählen Sie **Existierende Festplatte** und suchen Sie nach dem Image, das Sie zuvor in den Datenspeicher hochgeladen haben. Klicken Sie auf **Auswählen**.
7. Klicken Sie in der Symbolleiste erneut auf **Festplatte hinzufügen**. Wählen Sie **Neue Standard-Festplatte**. Legen Sie deren Größe auf 200 GB fest. Wiederholen Sie diesen Schritt, um ein weiteres Laufwerk mit 200 GB hinzuzufügen. Alles in allem sollten Sie letztendlich drei Laufwerke haben: 35 GB, 200 GB und 200 GB.



8. Klicken Sie im Fenster **Einstellungen anpassen** in der Symbolleiste auf **Netzwerkadapter hinzufügen**. Stellen Sie sicher, dass ein Adapter mit dem öffentlichen Netzwerk verbunden ist, während der andere mit der von Ihnen erstellten privaten Port-Gruppe verbunden ist.



9. Überprüfen Sie in Schritt 5 die Konfiguration und klicken Sie dann auf **Beenden**.

10. Wählen Sie die virtuelle Maschine im **Navigator**-Menü aus und starten Sie diese.

Wiederholen Sie diese Schritte, um so viele virtuelle Maschinen zu erstellen, wie Sie auf der Grundlage des gewünschten Szenarios benötigen (siehe Abschnitt *Anforderungen* (Seite 1)).

KAPITEL 4

Acronis Cyber Infrastructure in virtuellen Maschinen bereitstellen

Gehen Sie folgendermaßen vor, wenn die virtuelle Maschine gestartet wurde:

1. Melden Sie sich als Storage-User mit dem vorgegebenen Kennwort (welches password lautet) an. Sie werden direkt anschließend aufgefordert, das Kennwort zu ändern. Beispiel:

```
You are required to change your password immediately (root enforced)
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user storage-user.
Changing password for storage-user.
(current) UNIX password:
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Bei (current) UNIX password geben Sie password ein; bei New password und Retype new password geben Sie dann ein neues Kennwort ein. Das Kennwort wird sowohl für den Storage-User als auch den Benutzer ,root' geändert.

2. Melden Sie sich erneut als Storage-User sowie unter Verwendung des neuen Kennworts ein und wechseln Sie dann zum Benutzer ,root'.

```
$ sudo su
```

3. Konfigurieren und aktivieren Sie die Netzwerkschnittstelle eth1:

```
# cat > /etc/sysconfig/network-scripts/ifcfg-eth1 << EOF
ARPCHECK="no"
BOOTPROTO="static"
IPADDR=192.168.1.<node>
NETMASK=255.255.255.0
DEVICE="eth1"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
NAME="eth1"
ONBOOT="yes"
EOF
# ifup eth1
```

Wobei <node> für die Knoten-Nummer steht: 2 für den Management-Knoten, 3 für den ersten sekundären Knoten – und so weiter.

- Überprüfen Sie, dass die IP-Adresse zugewiesen wurde – und die Schnittstelle verfügbar ist, z.B. mit `ip -4 a show eth1`.

Die weitere Konfiguration variiert in Abhängigkeit von der Knoten-Rolle. Sie müssen einen einzelnen Management-Knoten bereitstellen und können bei Bedarf auch zwei oder vier sekundäre Knoten bereitstellen.

4.1 Den Management-Knoten bereitstellen

- Führen Sie folgenden Befehl als Benutzer `root` aus, um den Management-Knoten zu registrieren und dessen Admin-Panel zu initialisieren:

```
# echo '<passwd>' | /usr/libexec/vstorage-ui-backend/bin/configure-backend.sh \
-i <int_net> -x <ext_net>
# systemctl start vstorage-ui-backend
# systemctl start vstorage-ui-agent
# /usr/libexec/vstorage-ui-agent/bin/register-storage-node.sh -m <mn_IP>
```

Dabei ist <passwd> das gewünschte Administrator-Kennwort; <int_net> ist die interne (private) Netzwerkschnittstelle; <ext_net> ist die externe (öffentliche) Netzwerkschnittstelle und <mn_IP> ist die IP-Adresse des Management-Knotens.

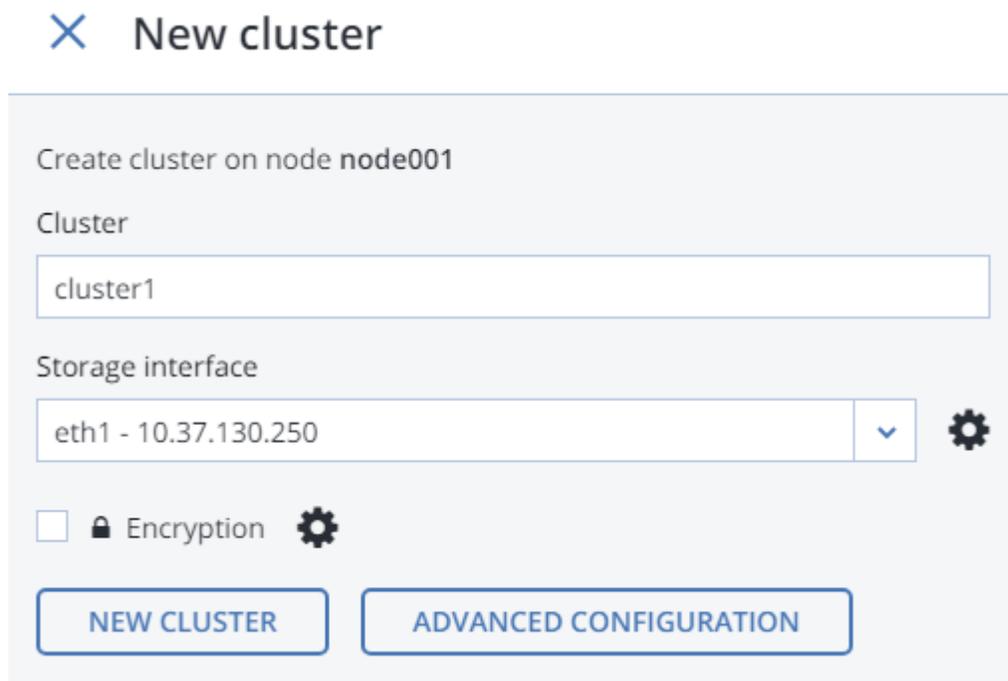
- Starten Sie die virtuelle Maschine neu. Die IP-Adresse des Admin-Panels wird im Willkommensfenster des Terminals angezeigt. Jetzt können Sie sich im Admin-Panel über den Port 8888 anmelden. Verwenden Sie den Benutzernamen `admin` und das `root`-Kennwort des Management-Knotens, welches Sie im vorherigen Schritt bereitgestellt haben.

Im Admin-Panel sehen Sie den Knoten, den Sie in der Liste **NICHT ZUGEWIESEN** auf der Anzeige **INFRASTRUKTUR** -> **Knoten** bereitgestellt haben.

3. Klicken Sie in der Anzeige **INFRASTRUKTUR** -> **Netzwerke** auf **Bearbeiten**. Machen Sie den Traffic-Typ **Compute-API** für das öffentliche Netzwerk verfügbar und klicken Sie auf **Speichern**.

Jetzt müssen Sie den Storage-Cluster erstellen. Gehen Sie folgendermaßen vor:

1. Öffnen Sie die Anzeige **INFRASTRUKTUR** -> **Knoten** und klicken Sie in der Liste **NICHT ZUGEWIESEN** auf einen Knoten.
2. Klicken Sie in der Knoten-Übersichtsanzeige auf **Cluster erstellen**.
3. Geben Sie im Feld **Cluster** eine Bezeichnung für den Cluster ein. Der Name darf nur lateinische Buchstaben (a-z, A-Z), Zahlen (0-9), Unterstriche (,) und normale Bindestriche (-,) enthalten.



× New cluster

Create cluster on node **node001**

Cluster

cluster1

Storage interface

eth1 - 10.37.130.250

Encryption

NEW CLUSTER **ADVANCED CONFIGURATION**

4. Klicken Sie auf **NEUER CLUSTER**.

Der Storage-Cluster ist bereit. Sie können nun mit der Bereitstellung von sekundären Knoten fortfahren, sofern Ihr Szenario dies erfordert. Wenn Sie nur einen einzelnen Knoten für das Backup Gateway benötigen, fahren Sie mit Abschnitt *„Die Acronis Backup-Software über das Backup Gateway mit Storage-Backends verbinden* (Seite 19) fort.

4.2 Sekundäre Knoten bereitstellen

Gehen Sie folgendermaßen vor, um einen sekundären Knoten in einer virtuellen Maschine bereitzustellen:

1. Ermitteln Sie die IP-Adresse und das Token des Management-Knotens über das Admin-Panel. Öffnen Sie die Anzeige **INFRASTRUKTUR** -> **Knoten**. Klicken Sie auf **KNOTEN HINZUFÜGEN**, um eine Anzeige mit der IP-Adresse des Management-Knotens und dem Token aufzurufen.
2. Öffnen Sie das Terminal der virtuellen Maschine und registrieren Sie folgendermaßen den sekundären Knoten im Admin-Panel:

```
# /usr/libexec/vstorage-ui-agent/bin/register-storage-node.sh -m <mn_addr> -t <token>
```

Dabei steht <mn_addr> für die IP-Adresse des Management-Knotens und <token> für das Token, das im Admin-Panel abgerufen wurde.

Der neu registrierte sekundäre Knoten wird im Admin-Panel auf der Anzeige **INFRASTRUKTUR** -> **Knoten** in der Liste **NICHT ZUGEWIESEN** angezeigt.

3. Fügen Sie den sekundären Knoten dem Storage-Cluster hinzu:
 - 3.1. Klicken Sie in der Anzeige **INFRASTRUKTUR** -> **Knoten** auf einen nicht zugewiesenen Knoten.
 - 3.2. Klicken Sie in der Knoten-Übersichtsanzeige auf **Zu Cluster hinzufügen**.
 - 3.3. Stellen Sie sicher, dass im Listenfeld **Storage-Schnittstelle** diejenige Netzwerkschnittstelle ausgewählt ist, die mit einem Netzwerk mit dem Traffic-Typ **Storage** verbunden ist.

Wenn keine Knoten-Netzwerk-Schnittstellen konfiguriert sind, klicken Sie auf das Zahnradsymbol und weisen Sie der Netzwerkschnittstelle eines Knotens ein Netzwerk mit dem Traffic-Typ **Storage** zu.

✕ Join cluster

Node to join: node002

Storage interface

eth1 - 10.37.130.28
▼
⚙️

JOIN CLUSTER

ADVANCED CONFIGURATION

- 3.4. Klicken Sie auf **Zu Cluster hinzufügen**, damit Acronis Cyber Infrastructure die Rollen den Laufwerken automatisch zuweist und dem aktuellen Cluster den Knoten hinzufügt. Alternativ können Sie auch auf **Erweiterte Konfiguration** klicken, wenn Sie die Rollen jedem Laufwerk manuell zuordnen wollen.

Wiederholen Sie diese Schritte für jeden sekundären Knoten. Nachdem sich alle im Storage-Cluster befinden, können Sie in der Anzeige **EINSTELLUNGEN** -> **Management-Knoten** ->

MANAGEMENT-HOCHVERFÜGBARKEIT die Hochverfügbarkeit für den Managementknoten aktivieren.

Jetzt können Sie mit der Einrichtung von Acronis Cyber Infrastructure für das gewünschte Szenario fortfahren. Anweisungen über die Durchführung verschiedener Konfigurationstaks sind in der Anleitung für Administratoren aufgeführt.

KAPITEL 5

Speicherplatz zu Acronis Cyber Infrastructure hinzufügen

Bevor Sie neue Laufwerke erstellen, sollten Sie die folgenden Empfehlungen für deren Dimensionierung beachten:

1. Wenn Sie einen Cluster oder mehrere Knoten haben, sollten die Knoten aus Redundanzgründen gleich groß sein. Dann werden die Daten gleichmäßiger auf diese verteilt. Weitere Informationen dazu finden Sie hier: [Understanding Allocatable Disk Space](#).
2. Laufwerke mit gleicher Größe sind hilfreich, um die Lasten gleichmäßiger zu verteilen. Innerhalb eines Clusters ist die Nutzung/Belastung eines Laufwerks proportional zu dessen Größe. Wenn Sie z.B. ein Laufwerk mit 10 TB und eines mit 2 TB haben, werden bei einer 50%-igen Cluster-Last 5 TB bzw. 1 TB verwendet.

Wenn Sie den physischen Speicherplatz auf Ihrem Storage-Cluster vergrößern wollen, können Sie neue virtuelle Laufwerke zu Ihren Knoten hinzufügen. Verwenden Sie auf Ihrer virtuellen Acronis Cyber Infrastructure-Maschine nicht die Option **extend disk** („Festplatte erweitern“) von VMware vSphere, weil die Größe des Dateisystems nicht entsprechend angepasst wird. Erstellen Sie stattdessen ein neues virtuelles Laufwerk und fügen Sie dieses (wie unten beschrieben) Ihrer virtuellen Maschine hinzu.

Fügen Sie Ihrer virtuellen Maschine ein neues virtuelles Laufwerk hinzu – wie im Abschnitt [„Einer virtuellen Maschine ein neues Laufwerk hinzufügen“](#) beschrieben. Dieses wird anschließend im Admin-Panel von Acronis Cyber Infrastructure in der Liste der Laufwerke des Knotens aufgeführt.

Befolgen Sie dann im Admin-Panel diese Schritte, um das neue Laufwerk zu konfigurieren:

1. Klicken Sie in der Anzeige **INFRASTRUKTUR** -> **Knoten** auf den Knoten mit dem erstellten Laufwerk: Klicken Sie in den Bereich **LAUFWERKE**>, um alle Laufwerke des Knotens einzusehen.

2. Das Laufwerk mit der Rolle **Nicht zugewiesen**, das Sie zuvor erstellt haben. Wählen Sie dieses aus und klicken Sie rechts auf den Befehl **Zuweisen**.
3. Wählen Sie in der Anzeige **Rolle wählen** die Rolle **Storage** aus, dann eine Storage-Ebene und aktivieren Sie schließlich (bei Bedarf) die Prüfsummenbildung. Weitere Informationen finden Sie hier: [Assigning Disk Roles Manually](#).

✕ Choose role

<input checked="" type="radio"/> Storage	Caching and checksumming
<input type="radio"/> Metadata	<input type="text" value="Enable checksumming"/> ▾
<input type="radio"/> Cache	Tier
<input type="radio"/> Metadata+Cache	<input type="text" value="Tier 0"/> ▾
<input type="radio"/> Unassigned	

KAPITEL 6

Die Acronis Backup-Software über das Backup Gateway mit Storage-Backends verbinden

Der Backup Gateway-Storage-Zugriffspunkt (auch einfach nur ‚Gateway‘ genannt) ist für Service-Provider gedacht, die Acronis Backup Cloud und/oder Acronis Backup Advanced einsetzen und einen lokalen Storage für die Backup-Daten ihrer Kunden organisieren wollen.

Mit dem Backup Gateway können Service-Provider leicht einen Storage für das von Acronis verwendete proprietäre, deduplizierungsfreundliche Datenformat konfigurieren.

Das Backup Gateway unterstützt folgende Storage-Backends:

- Storage-Cluster mit Software-Redundanz mithilfe von Lösch-Codierung
- NFS-Freigaben
- Public Clouds, darunter eine Reihe von S3-Lösungen sowie Microsoft Azure, OpenStack Swift und Google Cloud Platform

Ihre Wahl sollte zwar von Ihrem Einsatzzweck und Ihren Anforderungen abhängen, aber wir empfehlen, die Acronis Backup-Daten in einem lokalen Storage-Cluster zu speichern. Denn dann können Sie durch WAN-Optimierungen und Datenlokalität die beste Performance erzielen. Wenn Sie Backups in einer NFS-Freigabe oder einer Public Cloud speichern, wird dies zu unvermeidlichen Datenübertragungen und anderen Overheads führen, die die Gesamtperformance senken.

Beachten Sie bitte Folgendes:

- Wenn Sie das Backup Gateway konfigurieren, müssen Sie die Anmeldedaten Ihres Administratorkontos aus der Acronis Backup-Software bereitstellen.
- Wenn kein lokaler, sondern ein externer Storage (z.B. NFS) mit dem Backup Gateway verwendet wird, muss die Redundanz durch den entsprechenden externen Storage bereitgestellt werden. Das Backup Gateway selbst ermöglicht keine Datenredundanz und führt auch keine Dateneduplizierungen durch.
- Um das Backup Gateway in Acronis Backup Cloud registrieren zu können, sollte die Zwei-Faktor-Authentifizierung (2FA) für Ihr Partner-Konto deaktiviert sein.

6.1 Über das Backup Gateway mit dem lokalen Storage-Cluster verbinden

Bevor Sie fortfahren, sollten Sie sicherstellen, dass der als Ziel verwendete Storage über ausreichend Speicherplatz für vorhandene und neue Backups verfügt.

Gehen Sie folgendermaßen vor, um das Backup Gateway einzurichten:

1. Überprüfen Sie im Fenster **INFRASTRUKTUR** -> **Netzwerke**, dass die Traffic-Typen **ABGW privat** und **ABGW öffentlich** den Netzwerken hinzugefügt wurden, die Sie verwenden wollen.
2. Klicken Sie im linken Menü auf **STORAGE-SERVICES** -> **Backup Storage**.
3. Wählen Sie den/die Knoten aus, auf denen die Gateway-Services laufen sollen, und klicken Sie dann im rechten Menü auf **Gateway erstellen**.
4. Wählen Sie **Dieser Acronis Cyber Infrastructure-Cluster** als Storage-Typ.
5. Stellen Sie sicher, dass die richtige Netzwerkschnittstelle im Listenfeld ausgewählt ist. Klicken Sie auf **WEITER**.

Klicken Sie bei Bedarf auf das Zahnradsymbol und konfigurieren Sie dann in der Anzeige **Netzwerkkonfiguration** die Netzwerkschnittstellen des Knotens.



6. Wählen Sie auf der Registerkarte **Volume-Parameter** die gewünschte Storage-Ebene, Fehlerdomäne und den Datenredundanzmodus aus. Weitere Informationen finden Sie in den Abschnitten ‚Understanding Storage Tiers‘, ‚Understanding Failure Domains‘ und ‚Understanding Data Redundancy‘.

← **Volume parameters**

Tier:

Tier 0 ▼

Data redundancy: Failure domain:

Erasure coding Host ▼

Encoding 1+0	0% overhead
Encoding 1+1	100% overhead
Encoding 1+2	200% overhead

BACK NEXT

Redundanz durch Replikation wird für das Backup Gateway nicht unterstützt. Für die Lösch-Codierung ist eine Änderung des Redundanzschemas deaktiviert, weil dies die Cluster-Performance herabsetzen könnte. Der Grund dafür ist, dass die Neucodierung eine erhebliche Menge an Cluster-Ressourcen über einen langen Zeitraum erfordern würde. Wenn Sie das Redundanzschema dennoch ändern wollen, können Sie sich an den technischen Support wenden.

Klicken Sie auf **WEITER**.

7. Spezifizieren Sie auf der Registerkarte **DNS-Konfiguration** den externen DNS-Namen für dieses Gateway, beispielsweise `backupgateway.beispiel.com`. Stellen Sie sicher, dass jeder Knoten, auf dem der Gateway Service läuft, einen offenen Port für ausgehende Internetverbindungen und eingehende Verbindungen von Ihrer Acronis Backup-Software hat. Die Backup Agenten werden diese(n) Adresse/Port verwenden, um Ihre Backup-Daten hochzuladen.

Wichtig: Konfigurieren Sie Ihren DNS-Server nach dem im Admin-Panel vorgeschlagenen Beispiel.

Wichtig: Passen Sie jedes Mal, wenn Sie Knoten im Backup Gateway-Cluster ändern, die DNS-Einstellungen entsprechend an.

< DNS configuration

DNS name

backup.example.com

This may require changing the DNS server configuration, which may look as follows:

```
$TTL 1h
@ IN SOA ns1.myhoster.com. root.backup.example.com. (
2018120313 ;serial
1h ;refresh
30m ;retry
7d ;expiration
1h ) ;minimum
```

BACK NEXT

Klicken Sie auf **Weiter**.

- Spezifizieren Sie im Bereich **In Backup-Software registrieren** die folgenden Informationen für Ihr Acronis Produkt:

Wichtig: Stellen Sie sicher, dass die Zwei-Faktor-Authentifizierung (2FA) für Ihr Partner-Konto deaktiviert ist. Sie können diese auch für einen bestimmten Benutzer innerhalb eines 2FA-fähigen Mandanten deaktivieren, wie es in der [Acronis Cyber Cloud-Dokumentation](#) beschrieben ist, und die Benutzeranmeldedaten spezifizieren.

- Spezifizieren Sie bei **Adresse** die Adresse des Acronis Backup Cloud-Management-Portals (z.B. <https://cloud.acronis.com/>) oder den Host-Namen bzw. alternativ die IP-Adresse sowie den Port des Management Servers von Acronis Backup Advanced (z.B. <http://192.168.1.2:9877>).
- Spezifizieren Sie bei **Konto** die Anmeldedaten eines Partner-Kontos in der Cloud oder eines Organisationsadministrators auf dem lokalen Management Server.

9. Klicken Sie abschließend auf **FERTIG**.

6.2 Über das Backup Gateway mit externen NFS-Freigaben verbinden

Beachten Sie diese Einschränkungen:

- Acronis Cyber Infrastructure stellt keine Datenredundanz für NFS-Volumes bereit. Abhängig von der Implementierung können NFS-Freigaben ihre eigene Hard- oder Software-Redundanz verwenden.
- In der aktuellen Version von Acronis Cyber Infrastructure kann nur ein (1) Cluster-Knoten Backups auf einem NFS-Volume speichern.

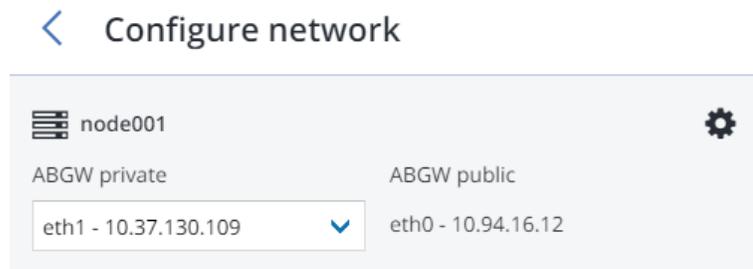
Stellen Sie Folgendes sicher, bevor Sie fortfahren:

1. Die NFS-Freigabe verfügt über genügend Speicherplatz für die Backups.
2. Jeder NFS-Export wird nur von einem (1) Gateway verwendet. Konfigurieren Sie insbesondere nicht zwei Acronis Cyber Infrastructure-Installationen so, dass diese denselben NFS-Export als Backup Storage verwenden.

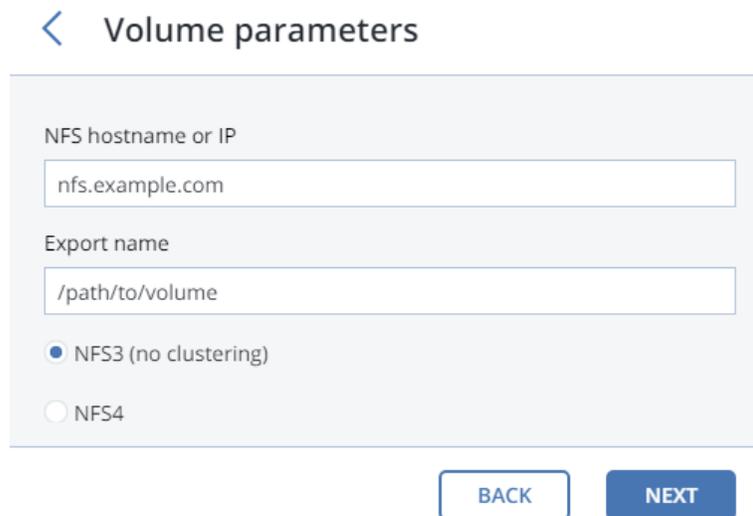
Gehen Sie folgendermaßen vor, um das Backup Gateway einzurichten:

1. Überprüfen Sie im Fenster **INFRASTRUKTUR** -> **Netzwerke**, dass die Traffic-Typen **ABGW privat** und **ABGW öffentlich** den Netzwerken hinzugefügt wurden, die Sie verwenden wollen.
2. Klicken Sie im linken Menü auf **STORAGE-SERVICES** -> **Backup Storage**.
3. Wählen Sie den/die Knoten aus, auf denen die Gateway-Services laufen sollen, und klicken Sie dann im rechten Menü auf **Gateway erstellen**.
4. Wählen Sie **Network File System** als Storage-Typ.
5. Stellen Sie sicher, dass die richtige Netzwerkschnittstelle im Listenfeld ausgewählt ist. Klicken Sie auf **WEITER**.

Klicken Sie bei Bedarf auf das Zahnradsymbol und konfigurieren Sie dann in der Anzeige **Netzwerkkonfiguration** die Netzwerkschnittstellen des Knotens.



- Spezifizieren Sie auf der Registerkarte **Volume-Parameter** den Host-Namen oder die IP-Adresse der NFS-Freigabe sowie den Exportnamen. Klicken Sie auf **WEITER**.



- Spezifizieren Sie auf der Registerkarte **DNS-Konfiguration** den externen DNS-Namen für dieses Gateway, beispielsweise `backupgateway.beispiel.com`. Stellen Sie sicher, dass jeder Knoten, auf dem der Gateway Service läuft, einen offenen Port für ausgehende Internetverbindungen und eingehende Verbindungen von Ihrer Acronis Backup-Software hat. Die Backup Agenten werden diese(n) Adresse/Port verwenden, um Ihre Backup-Daten hochzuladen.

Wichtig: Konfigurieren Sie Ihren DNS-Server nach dem im Admin-Panel vorgeschlagenen Beispiel.

Wichtig: Passen Sie jedes Mal, wenn Sie Knoten im Backup Gateway-Cluster ändern, die DNS-Einstellungen entsprechend an.

< DNS configuration

DNS name

backup.example.com

This may require changing the DNS server configuration, which may look as follows:

```
$TTL 1h
@ IN SOA ns1.myhoster.com. root.backup.example.com. (
  2018120313 ; serial
  1h ; refresh
  30m ; retry
  7d ; expiration
  1h ) ; minimum
```

BACK NEXT

Klicken Sie auf **Weiter**.

- Spezifizieren Sie im Bereich **In Backup-Software registrieren** die folgenden Informationen für Ihr Acronis Produkt:

Wichtig: Stellen Sie sicher, dass die Zwei-Faktor-Authentifizierung (2FA) für Ihr Partner-Konto deaktiviert ist. Sie können diese auch für einen bestimmten Benutzer innerhalb eines 2FA-fähigen Mandanten deaktivieren, wie es in der [Acronis Cyber Cloud-Dokumentation](#) beschrieben ist, und die Benutzeranmeldedaten spezifizieren.

- Spezifizieren Sie bei **Adresse** die Adresse des Acronis Backup Cloud-Management-Portals (z.B. <https://cloud.acronis.com/>) oder den Host-Namen bzw. alternativ die IP-Adresse sowie den Port des Management Servers von Acronis Backup Advanced (z.B. <http://192.168.1.2:9877>).
- Spezifizieren Sie bei **Konto** die Anmeldedaten eines Partner-Kontos in der Cloud oder eines Organisationsadministrators auf dem lokalen Management Server.

9. Klicken Sie abschließend auf **FERTIG**.

6.3 Über das Backup Gateway mit Public Clouds verbinden

Das Backup Gateway ermöglicht Ihnen, eine Reihe von Public Clouds und On-Premise-Objekt-Storage-Lösungen als Backup Storage für Acronis Backup Cloud oder Acronis Backup Advanced zu verwenden:

- Amazon S3
- IBM Cloud
- Alibaba Cloud
- IJ
- Cleversafe
- Cloudian
- Microsoft Azure
- Swift Object Storage
- Softlayer (Swift)
- Google Cloud Platform
- Wasabi
- Andere Lösungen, die S3 verwenden

Verglichen mit einem lokalen Storage-Cluster bewirkt die Verwendung einer Public Cloud als Backup Storage jedoch eine erhöhte Latenz bei I/O-Anfragen und damit eine verringerte Performance für alle entsprechenden Backup-Aktionen. Aus diesem Grund empfehlen wir, möglichst einen lokalen Storage-Cluster als Storage-Backend zu verwenden.

Bei Backups handelt es sich um sogenannte „Cold Data“ (selten verwendete Daten) mit einem spezifischen Zugriffsmuster: auf diese Daten wird nicht häufig zugegriffen, aber sie sollen bei Zugriff möglichst umgehend verfügbar sein. Für diesen Fall ist es daher kosteneffizienter, Storage-Klassen zu wählen, die für eine

Langzeitspeicherung und eher seltenen Datenzugriffen ausgelegt sind. Zu den empfohlenen Storage-Klassen gehören:

- **Infrequent Access** für Amazon S3
- **Cool Blob Storage** für Microsoft Azure
- **Nearline** und **Coldline** Storage für Google Cloud Platform

Storage-Klassen zur Datenarchivierung (wie Amazon S3 Glacier, Azure Archive Blob oder Google Archive) können nicht für Backups verwendet werden, weil sie keinen sofortigen Zugriff auf die Daten bereitstellen. Mit hohen Zugriffslatenzen (von mehreren Stunden) ist es technisch unmöglich, Archive zu durchsuchen, Daten schnell wiederherzustellen oder inkrementelle Backups zu erstellen. Auch wenn ein Archiv-Storage in der Regel sehr kosteneffizient ist, sollten Sie bedenken, dass es einige unterschiedliche Kostenfaktoren gibt. So setzen sich etwa die Gesamtkosten für einen Public Cloud Storage aus Ausgaben für die Speicherung der Daten, den allgemeinen Betrieb, den Datenverkehr, Datenabrufe, frühzeitige Löschungen usw. zusammen. Beispielsweise kann ein Storage Service zur Datenarchivierung eine Zahlung für sechs Monate Storage-Nutzung verlangen, obwohl nur einmal Daten abgerufen wurden. Wenn es erwartet wird, dass auf die Storage-Daten häufiger zugegriffen wird, können solche zusätzlichen Kosten die Gesamtkosten für die Datenspeicherung erheblich nach oben treiben. Um niedrige Datenabrufzeiten und hohe Kosten zu vermeiden, empfehlen wir, Acronis Cyber Cloud für die Speicherung von Backup-Daten zu verwenden.

6.3.1 Wichtige Anforderungen und Einschränkungen

1. Beim Arbeiten mit Public Clouds verwendet das Backup Gateway den lokalen Storage als Staging-Bereich und zur Speicherung von Service-Informationen. Daten, die in eine Public Cloud hochgeladen werden sollen, werden also zuerst lokal gespeichert und erst anschließend zu ihrem Ziel gesendet. Daher ist es wichtig, dass der lokale Storage persistent und redundant ist, damit die Daten nicht verloren gehen können. Es gibt mehrere Möglichkeiten, die Persistenz und Redundanz des lokalen Storage sicherzustellen. Sie können das Backup Gateway auf mehreren Cluster-Knoten bereitstellen und einen guten Redundanzmodus wählen. Wenn Acronis Cyber Infrastructure zusammen mit dem Gateway auf einem einzelnen physischen Knoten bereitgestellt wird, können Sie die Redundanz des lokalen Storage dadurch erreichen, dass Sie ihn über mehrere lokale Laufwerke hinweg replizieren. Wenn Acronis Cyber Infrastructure zusammen mit dem Gateway auf einer virtuellen Maschine bereitgestellt wird, stellen Sie sicher, dass die Redundanz durch die Virtualisierungslösung umgesetzt wird, auf der die VM läuft.

2. Stellen Sie sicher, dass der lokale Storage-Cluster über genügend logischen Speicherplatz für das Staging (Zwischenspeicherung von Daten) verfügt. Wenn Sie Backups beispielsweise täglich durchführen, sollte der bereitgestellte Speicherplatz für die Backups von mindestens 1,5 Tagen reichen. Wenn sich die tägliche Backup-Datenmenge auf 2 TB summiert, sollten Sie also mindestens 3 TB logischen Speicherplatz zur Verfügung stellen. Der erforderliche Raw-Speicherplatz hängt vom verwendeten Codierungsmodus ab: beispielsweise 9 TB (3 TB per Knoten) im 1+2-Modus, 5 TB (1 TB pro Knoten) im 3+2-Modus usw.
3. Wenn Sie Backups in einer Amazon S3 Cloud speichern wollen, beachten Sie, dass das Backup Gateway aus Gründen der Konsistenz von Amazon S3 gelegentlich den Zugriff auf solche Backups blockieren kann. Das bedeutet, dass Amazon S3 gelegentlich veraltete Daten zurücksenden kann, da Zeit benötigt wird, um die neueste Version der Daten zu verarbeiten und zugänglich zu machen. Das Backup Gateway erkennt solche Verzögerungen aber und schützt die Backup-Integrität, indem es den Zugriff auf die Daten solange blockiert, bis die Cloud aktualisiert wurde.
4. Verwenden Sie einen separaten Objekt-Container für jeden Backup Gateway-Cluster.

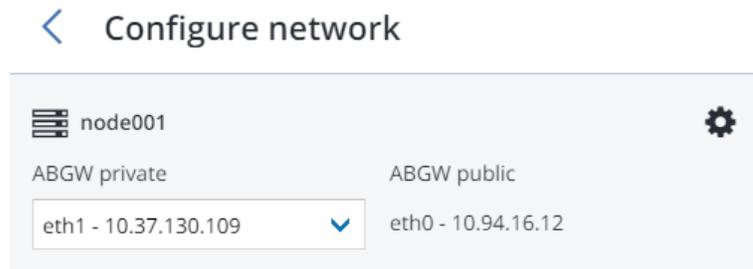
6.3.2 Das Backup Gateway einrichten

Bevor Sie fortfahren, sollten Sie sicherstellen, dass der Ziel-Storage über ausreichend Speicherplatz für die Backups verfügt.

Gehen Sie folgendermaßen vor, um das Backup Gateway einzurichten:

1. Überprüfen Sie im Fenster **INFRASTRUKTUR** -> **Netzwerke**, dass die Traffic-Typen **ABGW privat** und **ABGW öffentlich** den Netzwerken hinzugefügt wurden, die Sie verwenden wollen.
2. Klicken Sie im linken Menü auf **STORAGE-SERVICES** -> **Backup Storage**.
3. Wählen Sie den/die Knoten aus, auf denen die Gateway-Services laufen sollen, und klicken Sie dann im rechten Menü auf **Gateway erstellen**.
4. Wählen Sie **Public Cloud** als Storage-Typ.
5. Stellen Sie sicher, dass die richtige Netzwerkschnittstelle im Listenfeld ausgewählt ist. Klicken Sie auf **WEITER**.

Klicken Sie bei Bedarf auf das Zahnradsymbol und konfigurieren Sie dann in der Anzeige **Netzwerkkonfiguration** die Netzwerkschnittstellen des Knotens.



6. Tun Sie im Bereich **Public Cloud-Parameter** Folgendes:

- 6.1. Wählen Sie einen Public Cloud-Provider. Wenn Ihr Provider nicht in der Liste steht, aber S3-kompatibel ist, versuchen Sie **AuthV2-kompatibel (S3)** oder **AuthV4-kompatibel (S3)**.
- 6.2. Spezifizieren Sie in Abhängigkeit vom gewählten Provider die **Region**, die **Authentifizierungs-(Keystone)-URL** oder die **Endpunkt-URL**.
- 6.3. Spezifizieren Sie bei einem Swift Object Storage die Version des Authentifizierungsprotokolls und die benötigten Attribute.
- 6.4. Spezifizieren Sie die benötigten Anmeldedaten. Wählen Sie bei Google Cloud eine JSON-Datei mit Schlüsseln zum Hochladen aus.
- 6.5. Spezifizieren Sie den Ordner (Bucket, Container), in dem die Backups gespeichert werden sollen. Für den Ordner muss Schreibzugriff bestehen.

Verwenden Sie einen separaten Objekt-Container für jeden Backup Gateway-Cluster.

Klicken Sie auf **WEITER**.

7. Spezifizieren Sie im Bereich **In Backup-Software registrieren** die folgenden Informationen für Ihr Acronis Produkt:

Wichtig: Stellen Sie sicher, dass die Zwei-Faktor-Authentifizierung (2FA) für Ihr Partner-Konto deaktiviert ist. Sie können diese auch für einen bestimmten Benutzer innerhalb eines 2FA-fähigen Mandanten deaktivieren, wie es in der [Acronis Cyber Cloud-Dokumentation](#) beschrieben ist, und die Benutzeranmeldedaten spezifizieren.

- Spezifizieren Sie bei **Adresse** die Adresse des Acronis Backup Cloud-Management-Portals (z.B. <https://cloud.acronis.com/>) oder den Host-Namen bzw. alternativ die IP-Adresse sowie den Port des Management Servers von Acronis Backup Advanced (z.B. <http://192.168.1.2:9877>).

- Spezifizieren Sie bei **Konto** die Anmeldedaten eines Partner-Kontos in der Cloud oder eines Organisationsadministrators auf dem lokalen Management Server.
8. Klicken Sie abschließend auf **FERTIG**.