Erste Schritte

NetApp Backup and Recovery

NetApp
February 13, 2026

Inhalt

Erste Schritte

Erfahren Sie mehr über NetApp Backup and Recovery

NetApp Backup and Recovery ist ein Datenservice, der effizienten, sicheren und kostengünstigen Datenschutz für alle Ihre ONTAP Workloads bietet, einschließlich Volumes, Datenbanken, virtuellen Maschinen und Kubernetes-Workloads.

Die Unterstützung für Backup und Recovery ist bereits in alle ONTAP -Systeme integriert, sodass keine zusätzliche Hardware, Softwarelizenzen oder Medien-Gateways erforderlich sind. Dadurch werden Sicherungsvorgänge einfach und kostengünstig. Die NetApp Console vereinfacht die Implementierung jeder Backup-Strategie, einschließlich des gesamten Spektrums an 3-2-1-Backup-Varianten, ohne dass mehrere Ressourcenmanager oder spezialisiertes Personal erforderlich sind.

Dokumentation zum Schutz von VMware-, KVM-, Hyper-V- und Kubernetes-Workloads wird als Technologievorschau bereitgestellt. Bei diesem Vorschauangebot behält sich NetApp das Recht vor, Angebotsdetails, Inhalte und Zeitplan vor der allgemeinen Verfügbarkeit zu ändern.

Was Sie mit NetApp Backup and Recovery tun können

Verwenden Sie NetApp Backup and Recovery, um die folgenden Ziele zu erreichen:

- * ONTAP -Volumen-Workloads*:
  - Erstellen Sie lokale Snapshots, replizieren Sie auf sekundären Speicher und sichern Sie ONTAP -Volumes von lokalen ONTAP oder Cloud Volumes ONTAP Systemen auf Objektspeicher in Ihrem öffentlichen oder privaten Cloud-Konto.
  - Erstellen Sie inkrementelle Backups auf Blockebene, die dauerhaft auf einem anderen ONTAP Cluster und im Objektspeicher in der Cloud gespeichert werden.
  - Verwenden Sie NetApp Backup and Recovery zusammen mit SnapCenter.
  - Siehe"Schützen Sie ONTAP Volumes" .
- **Microsoft SQL Server-Arbeitslasten**:
  - Sichern Sie Microsoft SQL Server-Instanzen und -Datenbanken von On-Premises ONTAP, Cloud Volumes ONTAP oder Amazon FSx for NetApp ONTAP.
  - Stellen Sie Microsoft SQL Server-Datenbanken wieder her.
  - Klonen Sie Microsoft SQL Server-Datenbanken.
  - Verwenden Sie NetApp Backup and Recovery ohne SnapCenter.
  - Siehe"Schützen Sie Microsoft SQL Server-Workloads" .
- **VMware-Workloads (Vorschau mit neuer Benutzeroberfläche ohne SnapCenter Plug-in for VMware vSphere)**:
  - Schützen Sie Ihre VMware-VMs und Datenspeicher mit NetApp Backup and Recovery.
  - Sichern Sie VMware-Workloads auf Amazon Web Services S3 oder StorageGRID (für die Vorschau).
  - Stellen Sie VMware-Daten aus der Cloud wieder im lokalen vCenter wieder her.
  - Sie können die VM an genau demselben Speicherort wiederherstellen, von dem die Sicherung erstellt wurde, oder an einem anderen Speicherort.

- Verwenden Sie NetApp Backup and Recovery ohne SnapCenter Plug-in for VMware vSphere.
- Siehe"Schutz von VMware-Workloads" .

- **VMware-Workloads (mit SnapCenter Plug-in for VMware vSphere)**:
  - Sichern Sie VMs und Datenspeicher auf Amazon Web Services S3, Microsoft Azure Blob, Google Cloud Platform und StorageGRID und stellen Sie VMs auf dem lokalen SnapCenter Plug-in for VMware vSphere Host wieder her.
  - Stellen Sie mit NetApp Backup and Recovery VM-Daten aus der Cloud zurück in das lokale vCenter wieder her. Sie können die VM an genau demselben Speicherort wiederherstellen, von dem die Sicherung erstellt wurde, oder an einem anderen Speicherort.
  - Verwenden Sie NetApp Backup and Recovery zusammen mit dem SnapCenter Plug-in for VMware vSphere.
  - Siehe"Schutz von VMware-Workloads" .
- **KVM-Workloads (Vorschau)**:
  - Sichern und Wiederherstellen virtueller Maschinen
  - KVM-Speicherpools sichern
  - Verwenden Sie Schutzgruppen, um Sicherungsaufgaben zu verwalten
  - Siehe"Schützen Sie KVM -Workloads" .
- **Hyper-V-Workloads (Vorschau)**:
  - Sichern und Wiederherstellen virtueller Maschinen
  - Verwenden Sie Schutzgruppen, um Sicherungsaufgaben zu verwalten
  - Siehe"Schützen Sie Hyper-V-Workloads" .
- **Oracle Database workloads (Vorschau)**:
  - Sichern und Wiederherstellen von Datenbanken und Protokollen
  - Verwenden Sie Schutzgruppen, um Sicherungsaufgaben zu verwalten
  - Erstellen Sie Richtlinien zum Verwalten von Datenbank- und Protokollsicherungen
  - Schutz einer Datenbank mit einer 3-2-1-Backup-Architektur
  - Konfigurieren der Sicherungsaufbewahrung
  - Mounten und Unmounten von ARCHIVELOG-Backups
  - Siehe "Oracle Database-Workloads schützen".
- **Kubernetes-Workloads (Vorschau)**:
  - Verwalten und schützen Sie Ihre Kubernetes-Anwendungen und -Ressourcen an einem Ort.
  - Verwenden Sie Schutzrichtlinien, um Ihre inkrementellen Backups zu strukturieren.
  - Stellen Sie Anwendungen und Ressourcen in denselben oder in anderen Clustern und Namespaces wieder her.
  - Verwenden Sie NetApp Backup and Recovery ohne SnapCenter.
  - Siehe"Schützen Sie Kubernetes-Workloads" .

Vorteile der Verwendung von NetApp Backup and Recovery

NetApp Backup and Recovery bietet die folgenden Vorteile:

- **Effizient**: NetApp Backup and Recovery führt eine inkrementelle Replikation auf Blockebene durch, wodurch die Menge der replizierten und gespeicherten Daten erheblich reduziert wird. Dies trägt dazu bei, den Netzwerkverkehr und die Speicherkosten zu minimieren.
- **Sicher**: NetApp Backup and Recovery verschlüsselt Daten während der Übertragung und im Ruhezustand und verwendet sichere Kommunikationsprotokolle zum Schutz Ihrer Daten.
- **Kostengünstig**: NetApp Backup and Recovery verwendet die kostengünstigsten verfügbaren Speicherebenen in Ihrem Cloud-Konto und trägt so zur Kostensenkung bei.
- **Automatisiert**: NetApp Backup and Recovery erstellt automatisch Backups basierend auf einem vordefinierten Zeitplan, wodurch sichergestellt wird, dass Ihre Daten geschützt sind.
- **Flexibel**: NetApp Backup and Recovery ermöglicht Ihnen die Wiederherstellung von Daten auf demselben oder einem anderen System, was für Flexibilität bei der Datenwiederherstellung sorgt.

Kosten

NetApp berechnet Ihnen für die Nutzung der Testversion keine Gebühren. Sie sind jedoch für die Kosten verantwortlich, die mit den von Ihnen genutzten Cloud-Ressourcen verbunden sind, beispielsweise für Speicher- und Datenübertragungskosten.

Mit der Verwendung der Backup-to-Object-Funktion von NetApp Backup and Recovery mit ONTAP Systemen sind zwei Arten von Kosten verbunden:

- Ressourcengebühren
- Servicegebühren

Für die Erstellung von Snapshots oder replizierten Volumes fallen keine Gebühren an – außer dem Speicherplatz, der zum Speichern der Snapshots und replizierten Volumes benötigt wird.

Ressourcenkosten

Für die Objektspeicherkapazität und für das Schreiben und Lesen von Sicherungsdateien in der Cloud werden Ressourcengebühren an den Cloud-Anbieter gezahlt.

- Für die Sicherung auf Objektspeicher zahlen Sie Ihrem Cloud-Anbieter die Kosten für den Objektspeicher.

  Da NetApp Backup and Recovery die Speichereffizienz des Quellvolumes beibehält, zahlen Sie dem Cloud-Anbieter die Objektspeicherkosten für die Daten *nach* der ONTAP Effizienz (für die geringere Datenmenge nach Anwendung von Deduplizierung und Komprimierung).

- Für die Wiederherstellung von Daten mit Search & Restore werden bestimmte Ressourcen von Ihrem Cloud-Anbieter bereitgestellt. Außerdem fallen Kosten pro TiB an, die sich nach der Datenmenge richten, die von Ihren Suchanfragen gescannt wird. (Diese Ressourcen werden für Browse & Restore nicht benötigt.)
  - In AWS, "Amazon Athena" Und "AWS Glue" Ressourcen werden in einem neuen S3-Bucket bereitgestellt.
  - In Azure "Azure Synapse-Arbeitsbereich" Und "Azure Data Lake-Speicher" werden in Ihrem Speicherkonto bereitgestellt, um Ihre Daten zu speichern und zu analysieren.
  - Bei Google wird ein neuer Bucket bereitgestellt und der "Google Cloud BigQuery-Dienste" werden auf Konto-/Projektebene bereitgestellt.
- Wenn Sie Volumedaten aus einer Sicherungsdatei wiederherstellen möchten, die in einen Archivobjektspeicher verschoben wurde, fällt beim Cloud-Anbieter eine zusätzliche Abrufgebühr pro GiB und pro Anforderung an.

- Wenn Sie während der Wiederherstellung von Volumedaten eine Sicherungsdatei auf Ransomware scannen möchten (wenn Sie DataLock und Ransomware Resilience für Ihre Cloud-Sicherungen aktiviert haben), entstehen Ihnen auch bei Ihrem Cloud-Anbieter zusätzliche Kosten für den ausgehenden Datenverkehr.

Servicegebühren

Bei ONTAP Volume-Workloads werden Ihnen nur die Volumes in Rechnung gestellt, die durch Objektspeicher geschützt sind. Die Gebühren basieren auf der logischen Nutzkapazität der Quell ONTAP -Volumes vor Anwendung von Effizienzmaßnahmen, auch bekannt als Front-End-Terabytes (FETB).

Für Kubernetes-Workloads werden die Gebühren basierend auf der kombinierten Größe aller persistenten Volumes berechnet.

Für alle anderen Workloads werden Ihnen Ressourcen in Rechnung gestellt, die auf mindestens einem sekundären Speicherziel oder Objektspeicherziel geschützt sind. Die Gebühren werden anhand der logischen Größe der Quell-Workload berechnet. Bei Datenbanken bedeutet dies die Datenbankgröße; bei VMs die VM-Größe.

Es gibt drei Möglichkeiten, für Backup und Wiederherstellung zu bezahlen:

- Die erste Möglichkeit besteht darin, ein Abonnement bei Ihrem Cloud-Anbieter abzuschließen, bei dem Sie monatlich zahlen können.
- Die zweite Möglichkeit besteht im Kauf eines Jahresvertrags.
- Die dritte Möglichkeit besteht darin, Lizenzen direkt von NetApp zu erwerben. Siehe die Lizenzierung Im Abschnitt finden Sie weitere Details.

Lizenzierung

NetApp Backup and Recovery bietet eine kostenlose Testversion an, mit der Sie es für eine begrenzte Zeit ohne Lizenzschlüssel nutzen können.

Eine Backup-Lizenz ist nur für Sicherungs- und Wiederherstellungsvorgänge im Zusammenhang mit Objektspeichern erforderlich. Für das Erstellen von Snapshots und replizierten Volumes ist keine Lizenz erforderlich.

Sie können zwischen drei Lizenzoptionen wählen:

- **Bring Your Own License (BYOL)**: Erwerben Sie eine laufzeitbasierte (1, 2 oder 3 Jahre) und kapazitätsbasierte (in 1-TiB-Schritten) Lizenz von NetApp. Geben Sie die angegebene Seriennummer in der NetApp Console ein, um das Gerät zu aktivieren. Die Lizenz deckt alle Quellsysteme in Ihrer Organisation ab. Eine Verlängerung ist erforderlich, wenn die Laufzeit oder die Kapazitätsgrenze erreicht ist.
- **Pay As You Go (PAYGO)**: Abonnieren Sie über den Marktplatz Ihres Cloud-Anbieters und zahlen Sie pro GiB an gesicherten Daten, die monatlich abgerechnet werden. Es ist keine Vorauszahlung erforderlich. Bei Ihrer ersten Anmeldung steht Ihnen eine 30-tägige kostenlose Testphase zur Verfügung. Weitere Informationen finden Sie unter "Nutzen Sie ein NetApp Backup and Recovery -PAYGO-Abonnement" .
- **Jahresvertrag**: Verfügbar über die AWS- und Azure-Marktplätze für 1, 2 oder 3 Jahre. Es stehen zwei Jahresverträge zur Verfügung:
  - **Cloud-Backup**: Sichert Cloud Volumes ONTAP und lokale ONTAP Daten.
  - **CVO Professional**: Bündelt Cloud Volumes ONTAP und NetApp Backup and Recovery mit unbegrenzten Backups für Cloud Volumes ONTAP -Volumes (die Backup-Kapazität wird nicht auf die

Lizenz angerechnet).

- Beim CVO Professional-Tarif gibt es zwei Arten von Gebühren:
  - **Ressourcenkosten**: Basierend auf der Speichernutzung. Weitere Informationen finden Sie unter "Lizenzierung für Cloud Volumes ONTAP" .
  - **Servicegebühren**: Gebühren für NetApp Backup and Recovery. Befindet sich das Quellvolume jedoch in einem Speichersystem, das den CVO Professional-Plan nutzt, wird NetApp Backup and Recovery kostenlos bereitgestellt.

Wenn Sie die Google Cloud Platform nutzen, fordern Sie ein individuelles Angebot von NetApp an und wählen Sie Ihren Tarif während der Aktivierung im Google Cloud Marketplace aus.

"Erfahren Sie, wie Sie Lizenzen einrichten".

Unterstützte Workloads, Systeme und Sicherungsziele

Unterstützte Arbeitslasten

NetApp Backup and Recovery schützt die folgenden Arten von Workloads:

- ONTAP -Volumes
- Microsoft SQL Server-Instanzen und -Datenbanken werden auf physischen Festplatten und VMware Virtual Machine Disks (VMDK) über VMFS oder NFS gespeichert.
- VMware-VMs und -Datenspeicher
- KVM-Workloads (Vorschau)
- Hyper-V-Workloads (Vorschau)
- Oracle Database-Workloads (Vorschau)
- Kubernetes-Workloads (Vorschau)

Unterstützte Systeme

- Lokales ONTAP SAN (iSCSI-Protokoll) und NAS (über NFS- und CIFS-Protokolle) mit ONTAP Version 9.8 oder höher
- Cloud Volumes ONTAP 9.8 oder höher für AWS (mit SAN und NAS)
- Cloud Volumes ONTAP 9.8 oder höher für Google Cloud Platform (unter Verwendung der NFS- und CIFS-Protokolle)
- Cloud Volumes ONTAP 9.8 oder höher für Microsoft Azure (mit SAN und NAS)
- Amazon FSx for NetApp ONTAP (nur Microsoft SQL Server-Workloads)

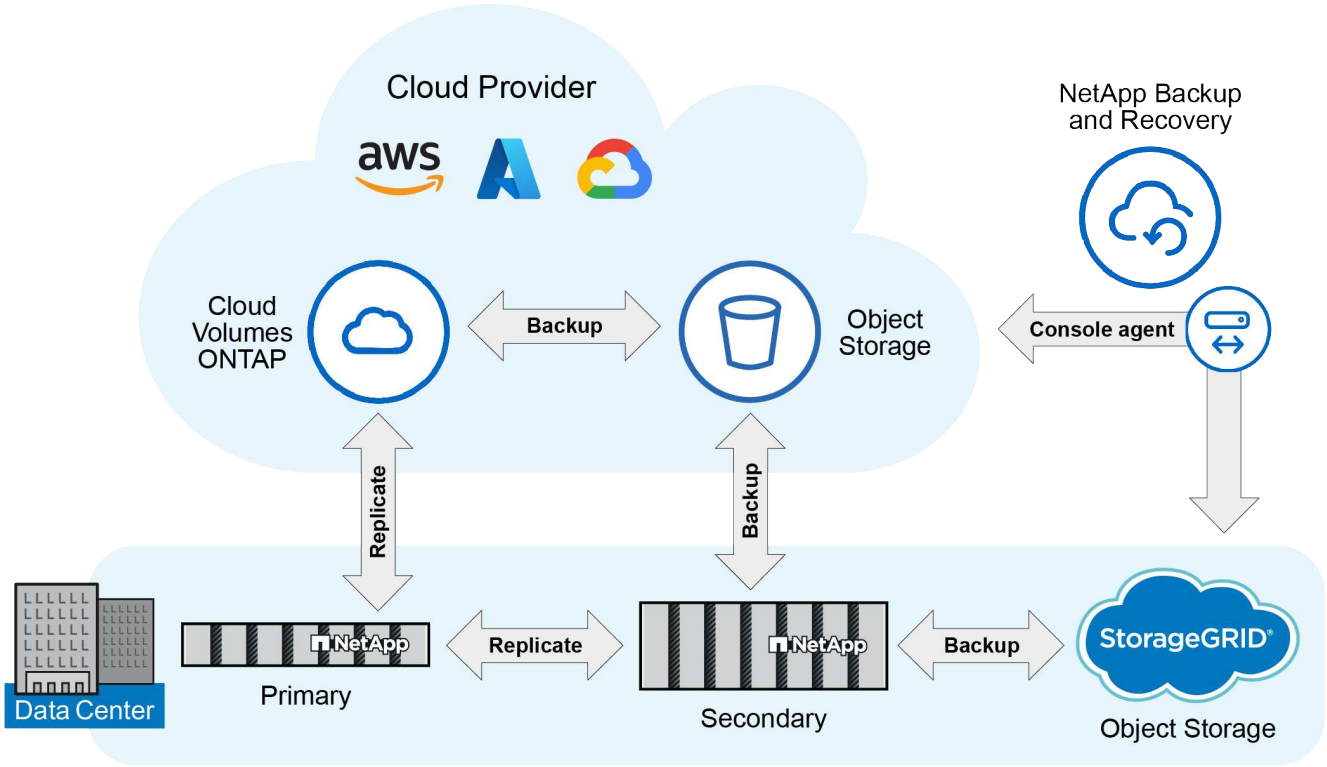
Unterstützte Sicherungsziele

- Amazon Web Services (AWS) S3
- Google Cloud-Speicher
- Microsoft Azure Blob (nicht verfügbar für VMware-Workloads in der Vorschau)
- StorageGRID
- ONTAP S3 (Nicht verfügbar für VMware-Workloads in der Vorschau)

So funktioniert NetApp Backup and Recovery

Wenn Sie NetApp Backup and Recovery aktivieren, führt der Dienst eine vollständige Sicherung Ihrer Daten durch. Nach der ersten Sicherung sind alle weiteren Sicherungen inkrementell. Dadurch wird der Netzwerkverkehr auf ein Minimum reduziert.

Das folgende Bild zeigt die Beziehung zwischen den Komponenten.



Auch die Übertragung vom Primär- zum Objektspeicher wird unterstützt, nicht nur die Übertragung vom Sekundärspeicher zum Objektspeicher.

Wo sich Backups in Objektspeicherorten befinden

Sicherungskopien werden in einem Objektspeicher gespeichert, den die NetApp Console in Ihrem Cloud-Konto erstellt. Es gibt einen Objektspeicher pro Cluster oder System und die Konsole benennt den Objektspeicher wie folgt: `netapp-backup-clusteruuid` . Denken Sie daran, diesen Objektspeicher nicht zu löschen.

- In AWS ermöglicht die NetApp Console die "Amazon S3-Funktion „Öffentlichen Zugriff blockieren“" auf dem S3-Bucket.
- In Azure verwendet die NetApp Console eine neue oder vorhandene Ressourcengruppe mit einem Speicherkonto für den Blob-Container. "blockiert den öffentlichen Zugriff auf Ihre Blob-Daten" standardmäßig.
- In StorageGRID verwendet die Konsole ein vorhandenes Speicherkonto für den Objektspeicher-Bucket.
- In ONTAP S3 verwendet die Konsole ein vorhandenes Benutzerkonto für den S3-Bucket.

Sicherungskopien sind mit Ihrer NetApp Console verknüpft

Sicherungskopien sind mit der NetApp Console verknüpft, in der sich der Konsolenagent befindet. "Erfahren Sie mehr über Identität und Zugriff auf die NetApp Console" .

Wenn Sie mehrere Konsolenagenten in derselben NetApp Console haben, zeigt jeder Konsolenagent dieselbe Liste mit Sicherungen an.

Begriffe, die Ihnen bei NetApp Backup and Recovery helfen könnten

Es kann für Sie von Vorteil sein, einige Begriffe im Zusammenhang mit dem Schutz zu verstehen.

- **Schutz**: Schutz in NetApp Backup and Recovery bedeutet, sicherzustellen, dass Snapshots und unveränderliche Backups regelmäßig mithilfe von Schutzrichtlinien in einer anderen Sicherheitsdomäne erfolgen.
- **Workload**: Ein Workload in NetApp Backup and Recovery kann ONTAP -Volumes, Microsoft SQL Server-Instanzen und -Datenbanken, VMware-VMs und -Datenspeicher oder Kubernetes-Cluster und -Anwendungen umfassen.

Voraussetzungen für NetApp Backup and Recovery

Beginnen Sie mit NetApp Backup and Recovery, indem Sie die Bereitschaft Ihrer Betriebsumgebung, NetApp Console Agenten und NetApp Console -Kontos überprüfen. Um NetApp Backup and Recovery verwenden zu können, benötigen Sie diese Voraussetzungen.

Voraussetzung für ONTAP 9.8 und höher

Auf der lokalen ONTAP Instanz muss eine ONTAP One-Lizenz aktiviert sein.

Voraussetzungen für Backups im Objektspeicher

Um Objektspeicher als Sicherungsziele zu verwenden, benötigen Sie ein Konto bei AWS S3, Microsoft Azure Blob, StorageGRID oder ONTAP und die entsprechenden Zugriffsberechtigungen.

- "Schützen Sie Ihre ONTAP Volume-Daten"

Anforderungen zum Schutz von Microsoft SQL Server-Workloads

Um NetApp Backup and Recovery für Microsoft SQL Server-Workloads zu verwenden, benötigen Sie die folgenden Voraussetzungen hinsichtlich Hostsystem, Speicherplatz und Größe.

Artikel	Anforderungen
Betriebssysteme	Microsoft Windows: Aktuelle Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .
Microsoft SQL Server-Versionen	Version 2012 und höher werden für VMware Virtual Machine File System (VMFS) und VMware Virtual Machine Disk (VMDK) NFS unterstützt.

Artikel	Anforderungen
SnapCenter Server-Version	Wenn Sie Ihre vorhandenen Daten aus SnapCenter in NetApp Backup and Recovery importieren möchten, ist SnapCenter Server Version 5.0 oder höher erforderlich. Wenn Sie bereits über SnapCenter verfügen, überprüfen Sie zunächst, ob Sie die Voraussetzungen erfüllt haben, bevor Sie aus SnapCenter importieren. Sehen"Voraussetzungen für den Import von Ressourcen aus SnapCenter" .
Mindest-RAM für das Plug-In auf dem SQL Server-Host	1 GB
Minimaler Installations- und Protokollspeicherplatz für das Plug-In auf dem SQL Server-Host	5 GB Weisen Sie ausreichend Speicherplatz zu und überwachen Sie den Speicherverbrauch des Protokollordners. Der erforderliche Protokollspeicherplatz variiert je nach Anzahl der durchgeführten Sicherungen und der Häufigkeit der Datenschutzvorgänge. Wenn nicht genügend Speicherplatz vorhanden ist, werden die Protokolle für die Vorgänge nicht erstellt.
Erforderliche Softwarepakete	• ASP.NET Core Runtime 8.0.12 Hosting Bundle (und alle nachfolgenden 8.0.x-Patches) • PowerShell 7.4.2 Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .

Anforderungen zum Schutz von VMware-Workloads

Sie benötigen bestimmte Anforderungen, um Ihre VMware-Workloads zu erkennen und zu schützen.

Softwareunterstützung

- NFS und VMFS-Datenspeicher werden unterstützt.
- Unterstützte NFS-Versionen: NFS 3 und NFS 4.1
- Unterstützte VMware ESXi Server-Versionen: 7.0U1 und höher
- Unterstützte VMware vCenter vSphere-Versionen: 7.0U1 und höher
- IP-Adressen: IPv4 und IPv6
- VMware TLS: 1.2, 1.3
- Unterstützter verbundener Speicher: ONTAP 9.13 oder höher

Verbindungs- und Portanforderungen zum Schutz von VMware-Workloads

Art des Anschlusses	Vorkonfigurierter Port
VMware ESXi-Server-Port	443 (HTTPS), bidirektional. Die Funktion „Gastdateiwiederherstellung“ verwendet diesen Port.
Speichercluster oder Speicher-VM-Port	443 (HTTPS), bidirektional. 80 (HTTP), bidirektional. Dieser Port wird für die Kommunikation zwischen der virtuellen Appliance und der Speicher-VM oder dem Cluster verwendet, der die Speicher-VM enthält.

Anforderungen an die rollenbasierte Zugriffskontrolle (RBAC) zum Schutz von VMware-Workloads

Das vCenter-Administratorkonto muss über die erforderlichen vCenter-Berechtigungen verfügen.

Eine Liste der erforderlichen vCenter-Berechtigungen finden Sie unter "SnapCenter Plug-in for VMware vSphere vCenter-Berechtigungen erforderlich" .

Anforderungen zum Schutz von KVM-Workloads

Sie benötigen bestimmte Anforderungen, um virtuelle KVM-Maschinen zu erkennen und zu schützen.

- Eine moderne Linux-Distribution mit Kernelversion 5.14.0-503.22.1.el9_5.x86_64 (longterm) oder höher
- Ihre KVM-Hosts und VMs müssen über eine Managementplattform verwaltet werden. NetApp Backup and Recovery unterstützt die folgenden Managementplattformen:
  - Apache CloudStack 4.22.0.0
- Stellen Sie sicher, dass eingehender Netzwerkverkehr von der Konsolenagentur zum KVM-Host an Port 22 zugelassen ist.
- QEMU-Gastagent Version 9.0.0 oder höher
- libvirt Version 10.5.0 oder höher

Um sicherzustellen, dass die Wiederherstellung von KVM-Workloads vollständig und erfolgreich verläuft, vergewissern Sie sich, dass die Einstellung **VM-konsistenten Snapshot aktivieren** in der Schutzrichtlinie, die Sie für KVM-Backups verwenden, aktiv ist.

Um den Schutz von KVM-VMs zu aktivieren, die von Benutzern ohne Root-Rechte verwaltet werden, führen Sie die folgenden Schritte aus:

1. Binden Sie das Volume als NFS3 ein, um die Verwendung von `nobody` Benutzer und Gruppe.
2. Verwenden Sie den folgenden Befehl, um einen Nicht-Root-Benutzer hinzuzufügen `qemu` Gruppen bilden und gleichzeitig ihre bestehenden Gruppen erhalten:

```
usermod -aG qemu <non-root-user>
```

3. Verwenden Sie den folgenden Befehl, um die Besitzrechte am Mount-Pfad zu übertragen. `qemu` Benutzer- und Gruppenberechtigungen für den Mount-Pfad ändern:

```
chown -R qemu:qemu <kvm_vm_mount_path> & chmod 771
<kvm_vm_mount_path>
```

4. Löschen Sie gegebenenfalls das vorhandene Verzeichnis NetApp_SnapCenter_Backups.

Anforderungen für den Schutz von Oracle Database Workloads

Stellen Sie sicher, dass Ihre Umgebung bestimmte Anforderungen zum Erkennen und Schützen von Oracle-Ressourcen erfüllt.

- Oracle-Datenbank:
  - Oracle 19C und 21C werden in einer eigenständigen Bereitstellung unterstützt.
  - Oracle Database muss im primären oder sekundären NetApp ONTAP Speicher bereitgestellt werden.
  - Host-OS-Unterstützung: Red Hat Enterprise Linux 8 und 9
- Objektspeicherunterstützung:
  - Azure-Objektspeicher
  - Amazon AWS
  - NetApp StorageGRID
  - ONTAP S3

Anforderungen zum Schutz von Kubernetes-Anwendungen

Sie benötigen spezifische Anforderungen, um Kubernetes-Ressourcen zu erkennen und Ihre Kubernetes-Anwendungen zu schützen.

Informationen zu den NetApp Console finden Sie unterIn der NetApp Console .

- Ein primäres ONTAP System (ONTAP 9.16.1 oder höher)
- Ein Kubernetes-Cluster – Zu den unterstützten Kubernetes-Distributionen und -Versionen gehören:
  - Anthos On-Prem (VMware) und Anthos auf Bare Metal 1.16
  - Kubernetes 1.27 – 1.33

    - OpenShift 4.10 – 4.18
    - Rancher Kubernetes Engine 2 (RKE2) v1.26.7+rke2r1, v1.28.5+rke2r1
    - Suse Rancher
- NetApp Trident 24.10 oder höher
- NetApp Trident Protect 25.07 oder später (installiert während der Kubernetes-Workload-Erkennung)
- NetApp Trident Protect Connector 25.07 or later (wird während der Kubernetes-Workload-Erkennung installiert)
    - Stellen Sie sicher, dass TCP-Port 443 in ausgehender Richtung zwischen dem Kubernetes-Cluster, dem Trident Protect Connector und dem Trident Protect Proxy ungefiltert ist.

Anforderungen zum Schutz von Hyper-V-Workloads

Stellen Sie sicher, dass Ihre Hyper-V-Instanz bestimmte Anforderungen zum Erkennen und Schützen virtueller Maschinen erfüllt.

- Softwareanforderungen für den Hyper-V Windows Server-Host:
    - Microsoft Hyper-V 2019, 2022 und 2025 Editionen
    - ASP.NET Core Runtime 8.0.12 Hosting Bundle (und alle nachfolgenden 8.0.x-Patches)
    - PowerShell 7.4.2 oder höher
    - Wenn Benutzer, die nicht Teil einer Administratordomäne sind, Hyper-V-VMs schützen sollen, stellen Sie sicher, dass der Benutzer über die folgenden Berechtigungen verfügt:
        - Stellen Sie sicher, dass der Benutzer Mitglied der lokalen Administratorgruppe ist.
        - Stellen Sie sicher, dass der Benutzer Teil der lokalen Sicherheitsrichtlinie „Anmelden als Dienst“ ist.
    - Stellen Sie sicher, dass in den Windows-Firewall-Einstellungen bidirektionaler HTTPS-Verkehr für die folgenden Ports zugelassen ist:
        - 8144 (NetApp -Plugin für Hyper-V)
        - 8145 (NetApp -Plugin für Windows)
- Hardwareanforderungen für den Hyper-V-Host:
    - Standalone- und FCI-Cluster-Hosts werden unterstützt
    - Mindestens 1 GB RAM für das NetApp Hyper-V-Plug-In auf dem Hyper-V-Host
    - Mindestens 5 GB Installations- und Protokollspeicherplatz für das Plug-In auf dem Hyper-V-Host

    > Stellen Sie sicher, dass Sie auf dem Hyper-V-Host genügend Speicherplatz für den Protokollordner zuweisen und dessen Nutzung regelmäßig überwachen. Der erforderliche Speicherplatz hängt davon ab, wie oft Backups und Datenschutzvorgänge durchgeführt werden. Wenn nicht genügend Speicherplatz vorhanden ist, werden keine Protokolle erstellt.

- NetApp ONTAP Konfigurationsanforderungen:
    - Ein primäres ONTAP System (ONTAP 9.14.1 oder höher)
    - Stellen Sie bei Hyper-V-Bereitstellungen, die CIFS-Freigaben zum Speichern von Daten virtueller Maschinen verwenden, sicher, dass die Eigenschaft „Continuous Availability Share“ auf dem ONTAP System aktiviert ist. Weitere Informationen finden Sie im "ONTAP-Dokumentation" Anweisungen hierzu finden Sie unter.

In der NetApp Console

Stellen Sie sicher, dass die NetApp Console die folgenden Anforderungen erfüllt.

- Ein Konsolenbenutzer sollte über die erforderliche Rolle und die erforderlichen Berechtigungen verfügen, um Vorgänge an Microsoft SQL Server- und Kubernetes-Workloads auszuführen. Um die Ressourcen zu erkennen, müssen Sie über die NetApp Backup and Recovery -Rolle des Superadministrators verfügen. Sehen"Rollenbasierter Zugriff auf Funktionen von NetApp Backup and Recovery" Weitere Informationen zu den Rollen und Berechtigungen, die zum Ausführen von Vorgängen in NetApp Backup and Recovery erforderlich sind.
- Eine Konsolenorganisation mit mindestens einem aktiven Konsolenagenten, der eine Verbindung zu lokalen ONTAP Clustern oder Cloud Volumes ONTAP.
- Mindestens ein Konsolensystem mit einem lokalen NetApp ONTAP oder Cloud Volumes ONTAP Cluster.
- Ein Konsolenagent

  Siehe "Erfahren Sie, wie Sie einen Konsolenagenten konfigurieren" Und "Standardanforderungen für die NetApp Console" .

  - Die Vorschauversion erfordert das Betriebssystem Ubuntu 22.04 LTS für den Konsolenagenten.

Einrichten der NetApp Console

Der nächste Schritt besteht darin, die Konsole und NetApp Backup and Recovery einzurichten.

Rezension "Standardanforderungen für die NetApp Console" .

Erstellen eines Konsolenagenten

Sie sollten sich an Ihr NetApp -Produktteam wenden, um Backup und Recovery auszuprobieren. Wenn Sie dann den Konsolenagenten verwenden, enthält dieser die entsprechenden Funktionen für den Dienst.

Informationen zum Erstellen eines Konsolenagenten in der NetApp Console vor der Verwendung des Dienstes finden Sie in der Konsolendokumentation. Dort wird beschrieben, "So erstellen Sie einen Konsolenagenten" .

Wo soll der Konsolenagent installiert werden?

Um einen Wiederherstellungsvorgang abzuschließen, kann der Konsolenagent an den folgenden Speicherorten installiert werden:

- Für Amazon S3 kann der Konsolenagent bei Ihnen vor Ort bereitgestellt werden.
- Für Azure Blob kann der Konsolen-Agent vor Ort bereitgestellt werden.
- Für StorageGRID muss der Konsolenagent in Ihren Räumlichkeiten bereitgestellt werden, mit oder ohne Internetzugang.
- Für ONTAP S3 kann der Konsolenagent in Ihren Räumlichkeiten (mit oder ohne Internetzugang) oder in einer Cloud-Provider-Umgebung bereitgestellt werden

Verweise auf „On-Premises ONTAP -Systeme“ umfassen FAS und AFF Systeme.

Einrichten der Lizenzierung für NetApp Backup and Recovery

Sie können NetApp Backup and Recovery lizenzieren, indem Sie bei Ihrem Cloud-Anbieter ein Pay-as-you-go-Abonnement (PAYGO) oder ein jährliches Marktplatz-Abonnement für * NetApp Intelligent Services* erwerben oder eine Bring-Your-Own-License (BYOL) von NetApp erwerben. Um NetApp Backup and Recovery auf einem System zu aktivieren, Backups Ihrer Produktionsdaten zu erstellen und Backup-Daten auf einem Produktionssystem wiederherzustellen, ist eine gültige Lizenz erforderlich.

Ein paar Anmerkungen, bevor Sie weiterlesen:

- Wenn Sie im Marktplatz Ihres Cloud-Anbieters bereits das Pay-as-you-go-Abonnement (PAYGO) für ein Cloud Volumes ONTAP System abonniert haben, sind Sie automatisch auch für NetApp Backup and Recovery angemeldet. Sie müssen sich nicht erneut anmelden.
- Die Bring-Your-Own-License (BYOL) von NetApp Backup and Recovery ist eine Floating-Lizenz, die Sie auf allen Systemen verwenden können, die mit Ihrer NetApp Console -Organisation oder Ihrem NetApp Console-Konto verknüpft sind. Wenn Ihnen also durch eine vorhandene BYOL-Lizenz ausreichend Sicherungskapazität zur Verfügung steht, müssen Sie keine weitere BYOL-Lizenz erwerben.
- Wenn Sie eine BYOL-Lizenz verwenden, wird empfohlen, dass Sie auch ein PAYGO-Abonnement abschließen. Wenn Sie mehr Daten sichern, als Ihre BYOL-Lizenz zulässt, oder wenn die Laufzeit Ihrer Lizenz abläuft, wird die Sicherung über Ihr Pay-as-you-go-Abonnement fortgesetzt – es kommt zu keiner Dienstunterbrechung.
- Wenn Sie lokale ONTAP Daten auf StorageGRID sichern, benötigen Sie eine BYOL-Lizenz, für den Speicherplatz des Cloud-Anbieters fallen jedoch keine Kosten an.

"Erfahren Sie mehr über die Kosten im Zusammenhang mit der Verwendung von NetApp Backup and Recovery."

30 Tage kostenlos testen

Eine kostenlose 30-Tage-Testversion von NetApp Backup and Recovery ist verfügbar, wenn Sie sich im Marktplatz Ihres Cloud-Anbieters für ein Pay-as-you-go-Abonnement für * NetApp Intelligent Services* anmelden. Die kostenlose Testversion beginnt mit der Anmeldung zum Marktplatzeintrag. Beachten Sie: Wenn Sie beim Bereitstellen eines Cloud Volumes ONTAP -Systems für das Marktplatzabonnement bezahlen und dann 10 Tage später Ihre kostenlose Testversion von NetApp Backup and Recovery starten, haben Sie noch 20 Tage Zeit, die kostenlose Testversion zu nutzen.

Nach Ablauf der kostenlosen Testphase erfolgt die Umstellung automatisch und ohne Unterbrechung auf das PAYGO-Abo. Wenn Sie sich entscheiden, NetApp Backup and Recovery nicht weiter zu verwenden,"Aufheben der Registrierung von NetApp Backup and Recovery vom System" bevor die Testphase endet, und es entstehen Ihnen keine Kosten.

Kostenlose Testversion beenden

Wenn Sie NetApp Backup and Recovery nach Ablauf der kostenlosen Testversion weiterhin verwenden möchten, müssen Sie ein kostenpflichtiges Abonnement einrichten. Sie können dies über die NetApp Console tun, indem Sie zum Abschnitt „Abrechnung“ navigieren und einen Abonnementplan auswählen, der Ihren Anforderungen entspricht. Wenn Sie NetApp Backup and Recovery nicht weiter verwenden möchten, können Sie die kostenlose Testversion beenden.

Wenn Sie die kostenlose Testversion beenden, ohne einen kostenpflichtigen Plan zu abonnieren, werden Ihre Daten 60 Tage nach Ablauf der kostenlosen Testversion automatisch gelöscht. Optional können Sie Ihre Daten auch sofort vom System löschen lassen.

Schritte

1. Wählen Sie auf der Zielseite von NetApp Backup and Recovery **Kostenlose Testversion anzeigen** aus.
2. Wählen Sie **Kostenlose Testversion beenden**.
3. Wählen Sie **Daten sofort nach Beendigung meiner kostenlosen Testversion löschen**, um Ihre Daten sofort zu löschen.
4. Geben Sie **Testversion beenden** in das Feld ein.
5. Wählen Sie zur Bestätigung **Ende**.

Verwenden Sie ein NetApp Backup and Recovery PAYGO-Abonnement

Beim Pay-as-you-go-Modell zahlen Sie Ihrem Cloud-Anbieter die Kosten für die Objektspeicherung und die Lizenzkosten für das NetApp -Backup auf Stundenbasis in einem einzigen Abonnement. Sie sollten * NetApp Intelligent Services* im Marketplace abonnieren, auch wenn Sie über eine kostenlose Testversion verfügen oder Ihre eigene Lizenz mitbringen (BYOL):

- Durch das Abonnement wird sichergestellt, dass es nach Ablauf Ihrer kostenlosen Testversion zu keiner Dienstunterbrechung kommt. Nach Ablauf der Testphase werden Ihnen stündlich Gebühren entsprechend der Menge der von Ihnen gesicherten Daten berechnet.
- Wenn Sie mehr Daten sichern, als Ihre BYOL-Lizenz zulässt, werden die Datensicherungs- und Wiederherstellungsvorgänge über Ihr Pay-as-you-go-Abonnement fortgesetzt. Wenn Sie beispielsweise über eine BYOL-Lizenz mit 10 TiB verfügen, wird die gesamte Kapazität über 10 TiB hinaus über das PAYGO-Abonnement abgerechnet.

Während Ihrer kostenlosen Testphase oder wenn Sie Ihre BYOL-Lizenz nicht überschritten haben, werden Ihnen keine Kosten für Ihr Pay-as-you-go-Abonnement in Rechnung gestellt.

Es gibt einige PAYGO-Pläne für NetApp Backup and Recovery:

- Ein „Cloud Backup“-Paket, mit dem Sie Cloud Volumes ONTAP Daten und lokale ONTAP -Daten sichern können.
- Ein „CVO Professional“-Paket, mit dem Sie Cloud Volumes ONTAP und NetApp Backup and Recovery bündeln können. Dies beinhaltet unbegrenzte Backups für das Cloud Volumes ONTAP System unter Verwendung der Lizenz (die Backup-Kapazität wird nicht auf die lizenzierte Kapazität angerechnet). Mit dieser Option können Sie keine lokalen ONTAP -Daten sichern.

  Beachten Sie, dass für diese Option auch ein PAYGO-Abonnement für Backup und Wiederherstellung erforderlich ist, für berechtigte Cloud Volumes ONTAP Systeme jedoch keine Gebühren anfallen.

"Erfahren Sie mehr über diese kapazitätsbasierten Lizenzpakete".

Verwenden Sie diese Links, um NetApp Backup and Recovery über den Marktplatz Ihres Cloud-Anbieters zu abonnieren:

- AWS: "Preisdetails finden Sie im Marketplace-Angebot für NetApp Intelligent Services." Die
- Azurblau: "Preisdetails finden Sie im Marketplace-Angebot für NetApp Intelligent Services." Die
- Google Cloud: "Preisdetails finden Sie im Marketplace-Angebot für NetApp Intelligent Services." Die

Verwenden Sie einen Jahresvertrag

Bezahlen Sie jährlich für NetApp Backup and Recovery , indem Sie einen Jahresvertrag abschließen. Sie sind mit einer Laufzeit von 1, 2 oder 3 Jahren erhältlich.

Wenn Sie einen Jahresvertrag von einem Marktplatz haben, wird der gesamte Verbrauch von NetApp Backup and Recovery über diesen Vertrag abgerechnet. Sie können einen jährlichen Marktplatzvertrag nicht mit einem BYOL kombinieren.

Wenn Sie AWS verwenden, stehen Ihnen zwei Jahresverträge zur Verfügung: "AWS Marketplace-Seite" für Cloud Volumes ONTAP und lokale ONTAP Systeme:

- Ein „Cloud Backup“-Plan, mit dem Sie Cloud Volumes ONTAP -Daten und lokale ONTAP -Daten sichern können.

  Wenn Sie diese Option nutzen möchten, richten Sie Ihr Abonnement auf der Marketplace-Seite ein und dann "Verknüpfen Sie das Abonnement mit Ihren AWS-Anmeldeinformationen" . Beachten Sie, dass Sie mit diesem Jahresvertragsabonnement auch für Ihre Cloud Volumes ONTAP -Systeme bezahlen müssen, da Sie Ihren AWS-Anmeldeinformationen in der Konsole nur ein aktives Abonnement zuweisen können.

- Ein „CVO Professional“-Plan, der es Ihnen ermöglicht, Cloud Volumes ONTAP und NetApp Backup and Recovery zu bündeln. Dies beinhaltet unbegrenzte Backups für das Cloud Volumes ONTAP System unter Verwendung der Lizenz (die Backup-Kapazität wird nicht auf die lizenzierte Kapazität angerechnet). Mit dieser Option können Sie keine lokalen ONTAP -Daten sichern.

  Siehe die "Thema zur Lizenzierung von Cloud Volumes ONTAP" um mehr über diese Lizenzierungsoption zu erfahren.

  Wenn Sie diese Option nutzen möchten, können Sie den Jahresvertrag einrichten, wenn Sie ein Cloud Volumes ONTAP -System erstellen. Die Konsole fordert Sie dann auf, den AWS Marketplace zu abonnieren.

Wenn Sie Azure verwenden, stehen Ihnen zwei Jahresverträge zur Verfügung von "Azure Marketplace-Seite" für Cloud Volumes ONTAP und lokale ONTAP Systeme:

- Ein „Cloud Backup“-Plan, mit dem Sie Cloud Volumes ONTAP -Daten und lokale ONTAP -Daten sichern können.

  Wenn Sie diese Option nutzen möchten, richten Sie Ihr Abonnement auf der Marketplace-Seite ein und dann "Verknüpfen Sie das Abonnement mit Ihren Azure-Anmeldeinformationen" . Beachten Sie, dass Sie mit diesem Jahresvertragsabonnement auch für Ihre Cloud Volumes ONTAP -Systeme bezahlen müssen, da Sie Ihren Azure-Anmeldeinformationen in der Konsole nur ein aktives Abonnement zuweisen können.

- Ein „CVO Professional“-Plan, der es Ihnen ermöglicht, Cloud Volumes ONTAP und NetApp Backup and Recovery zu bündeln. Dies beinhaltet unbegrenzte Backups für das Cloud Volumes ONTAP System unter Verwendung der Lizenz (die Backup-Kapazität wird nicht auf die lizenzierte Kapazität angerechnet). Mit dieser Option können Sie keine lokalen ONTAP -Daten sichern.

  Siehe die "Thema zur Lizenzierung von Cloud Volumes ONTAP" um mehr über diese Lizenzierungsoption zu erfahren.

  Wenn Sie diese Option nutzen möchten, können Sie den Jahresvertrag einrichten, wenn Sie ein Cloud Volumes ONTAP -System erstellen und die Konsole Sie auffordert, den Azure Marketplace zu abonnieren.

Wenn Sie GCP verwenden, wenden Sie sich an Ihren NetApp Vertriebsmitarbeiter, um einen Jahresvertrag abzuschließen. Der Vertrag ist als privates Angebot im Google Cloud Marketplace verfügbar.

Nachdem NetApp Ihnen das private Angebot mitgeteilt hat, können Sie den Jahresplan auswählen, wenn Sie sich während der Aktivierung von NetApp Backup and Recovery über den Google Cloud Marketplace anmelden.

Verwenden Sie eine NetApp Backup and Recovery BYOL-Lizenz

Bring-Your-Own-Lizenzen von NetApp haben eine Laufzeit von 1, 2 oder 3 Jahren. Sie zahlen nur für die Daten, die Sie schützen, berechnet anhand der logisch genutzten Kapazität (*vor* jeglicher Effizienz) der Quell-ONTAP -Volumes, die gesichert werden. Diese Kapazität wird auch als Front-End-Terabyte (FETB) bezeichnet.

Bei der BYOL NetApp Backup and Recovery -Lizenz handelt es sich um eine Floating-Lizenz, bei der die Gesamtkapazität auf alle Systeme aufgeteilt wird, die mit Ihrer NetApp Console -Organisation oder Ihrem NetApp Console-Konto verknüpft sind. Für ONTAP -Systeme können Sie eine grobe Schätzung der benötigten Kapazität erhalten, indem Sie den CLI-Befehl ausführen `volume show -fields logical-used-by-afs` für die Volumes, die Sie sichern möchten.

Wenn Sie keine NetApp Backup and Recovery BYOL-Lizenz haben, klicken Sie auf das Chat-Symbol unten rechts in der Konsole, um eine zu erwerben.

Wenn Sie über eine nicht zugewiesene knotenbasierte Lizenz für Cloud Volumes ONTAP verfügen, die Sie nicht verwenden, können Sie diese optional in eine NetApp Backup and Recovery -Lizenz mit demselben Dollaräquivalent und demselben Ablaufdatum umwandeln. "Hier finden Sie weitere Einzelheiten" .

Sie verwenden die NetApp Console , um BYOL-Lizenzen zu verwalten. Sie können neue Lizenzen hinzufügen, vorhandene Lizenzen aktualisieren und den Lizenzstatus über die Konsole anzeigen.

"Informationen zum Hinzufügen von Lizenzen".

Überschreitung der Lizenzkapazität

Wenn Sie Ihr lizenziertes Speicherkontingent überschreiten, fallen PAYGO-Gebühren an; ohne ein PAYGO-Abonnement können Sie keine neuen Backups erstellen, bestehende Backups bleiben jedoch ohne Servicegarantie wiederherstellbar. Erneuern Sie Ihre Lizenz unbedingt, bevor sie abläuft; eine abgelaufene Lizenz verhindert neue Backups und unterbricht den Service.

Einrichten von Sicherheitszertifikaten für StorageGRID und ONTAP in NetApp Backup and Recovery

Erstellen Sie ein Sicherheitszertifikat, um die Kommunikation zwischen NetApp Backup and Recovery und StorageGRID oder ONTAP zu ermöglichen.

Erstellen Sie ein Sicherheitszertifikat für StorageGRID

Wenn die Kommunikation zwischen NetApp Backup and Recovery Containern und StorageGRID das StorageGRID -Zertifikat überprüfen soll, führen Sie die folgenden Schritte aus.

Das generierte Zertifikat sollte CN und Subject Alternative Name als den Namen enthalten, der in NetApp Backup and Recovery angegeben wurde, als Sie die Sicherung aktiviert haben.

Schritte

1. Befolgen Sie die Schritte in der StorageGRID -Dokumentation, um das StorageGRID -Zertifikat zu erstellen.

   "StorageGRID Informationen zum Konfigurieren von Zertifikaten"

2. Aktualisieren Sie StorageGRID mit dem Zertifikat, falls Sie dies noch nicht getan haben.
3. Melden Sie sich als Root-Benutzer beim Konsolenagenten an. Laufen:

   ```
   sudo su
   ```

4. Holen Sie sich das Docker-Volume von NetApp Backup and Recovery (Cloud Backup Service). Laufen:

   ```
   docker volume ls | grep cbs
   ```

   Ausgabebeispiel:

   ```
   local service-manager-2_cloudmanager_cbs_volume"
   ```

   Der Volumename ist in den Bereitstellungsmodi „Standard“, „Privat“ und „Eingeschränkt“ unterschiedlich. In diesem Beispiel wird der Standardmodus verwendet. Siehe "Bereitstellungsmodi der NetApp Console" .

5. Suchen Sie den Einhängepunkt des NetApp Backup and Recovery -Volumes. Laufen:

   ```
   docker volume inspect service-manager-2_cloudmanager_cbs_volume | grep
   Mountpoint
   ```

   Ausgabebeispiel:

   ```
   "Mountpoint": "/var/lib/docker/volumes/service-manager-
   2_cloudmanager_cbs_volume/_data"
   ```

   Der Einhängepunkt ist in den Bereitstellungsmodi „Standard“, „Privat“ und „Eingeschränkt“ unterschiedlich. Dieses Beispiel zeigt eine Standard-Cloud-Bereitstellung. Siehe "Bereitstellungsmodi der NetApp Console" .

6. Wechseln Sie in das MountPoint-Verzeichnis. Laufen:

   ```
   cd /var/lib/docker/volumes/service-manager-
   2_cloudmanager_cbs_volume/_data
   ```

7. Wenn das Zertifikat von StorageGRID von der Stammzertifizierungsstelle und einer

Zwischenzertifizierungsstelle signiert ist, fügen Sie die `pem` Dateien von beiden in eine Datei mit dem Namen `sgws.crt` am aktuellen Standort. Fügen Sie das Blattzertifikat nicht zu dieser Datei hinzu.

Schritte für den Cloudmanager_CBS-Container

Sie müssen die StorageGRID -Server-Zertifikatsüberprüfung in NetApp Backup and Recovery (Cloud Backup Service) aktivieren.

1. Wechseln Sie zum Verzeichnis des Docker-Volumes, das Sie in den vorherigen Schritten erhalten haben.

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Wechseln Sie in das Konfigurationsverzeichnis.

```
cd cbs_config
```

3. Erstellen und speichern Sie eine Konfigurationsdatei wie unten gezeigt mit einem der folgenden Namen, basierend auf Ihrer Bereitstellungsumgebung:

   - `production-customer.json`Wird für Bereitstellungen im Standardmodus und eingeschränkten Modus verwendet.
   - `darksite-customer.json`Wird für Bereitstellungen im privaten Modus verwendet.

   Siehe "Bereitstellungsmodi der NetApp Console" .

   Konfigurationsdatei

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  }
}
```

4. Verlassen Sie den Container. Laufen:

```
exit
```

5. Neustart `cloudmanager_cbs` . Laufen:

```
docker restart cloudmanager_cbs
```

Schritte für den Container „cloudmanager_cbs_catalog“

Als Nächstes müssen Sie die StorageGRID -Server-Zertifikatsüberprüfung für den Katalogisierungsdienst aktivieren.

1. Wechseln Sie zum Docker-Volume:

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Konfigurieren Sie den Katalog. Laufen:

```
cd cbs_catalog_config
```

3. Erstellen Sie eine Konfigurationsdatei wie unten gezeigt mit einem der folgenden Namen, basierend auf Ihrer Bereitstellungsumgebung:

   - `production-customer.json`Wird für Bereitstellungen im Standardmodus und eingeschränkten Modus verwendet.
   - `darksite-customer.json`Wird für Bereitstellungen im privaten Modus verwendet.

   Siehe "Bereitstellungsmodi der NetApp Console" .

   Katalogkonfigurationsdatei

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  }
}
```

4. Starten Sie den Katalog neu. Laufen:

```
docker restart cloudmanager_cbs_catalog
```

Aktualisieren Sie das Konsolen-Agent-Zertifikat mit dem StorageGRID -Zertifikat basierend auf dem Agent-Betriebssystem

Ubuntu

1. Kopieren Sie das SGWS-Zertifikat nach `/usr/local/share/ca-certificates` . Hier ist ein Beispiel:

   ```
   cp /config/sgws.crt /usr/local/share/ca-certificates/
   ```

   Wo `sgws.crt` ist das Stamm-CA-Zertifikat.

2. Aktualisieren Sie die Hostzertifikate mit dem StorageGRID -Zertifikat. Laufen

   ```
   sudo update-ca-certificates
   ```

Red Hat Enterprise Linux

1. Kopieren Sie das SGWS-Zertifikat nach `/etc/pki/ca-trust/source/anchors/` .

   ```
   cp /config/sgws.crt /etc/pki/ca-trust/source/anchors/
   ```

   Wo `sgws.crt` ist das Stamm-CA-Zertifikat.

2. Aktualisieren Sie die Hostzertifikate mit dem StorageGRID -Zertifikat.

   ```
   update-ca-trust extract
   ```

3. Aktualisieren Sie die `ca-bundle.crt`

   ```
   cd /etc/pki/tls/certs/
   openssl x509 -in ca-bundle.crt -text -noout
   ```

4. Um zu überprüfen, ob die Zertifikate vorhanden sind, führen Sie den folgenden Befehl aus:

   ```
   openssl crl2pkcs7 -nocrl -certfile /etc/pki/tls/certs/ca-bundle.crt |
   openssl pkcs7 -print_certs | grep subject | head
   ```

Erstellen Sie ein Sicherheitszertifikat für ONTAP

Wenn die Kommunikation zwischen den NetApp Backup and Recovery -Containern und ONTAP das ONTAP -Zertifikat validieren soll, führen Sie die folgenden Schritte aus.

NetApp Backup and Recovery verwendet die Cluster Management IP, um eine Verbindung mit ONTAP herzustellen. Geben Sie die IP-Adresse des Clusters in die alternativen Betreffnamen des Zertifikats ein. Geben Sie diesen Schritt an, wenn Sie die CSR mithilfe der System Manager-Benutzeroberfläche generieren.

Verwenden Sie die System Manager-Dokumentation, um ein neues CA-Zertifikat für ONTAP zu erstellen.

- "Zertifikate mit System Manager verwalten"
- "So verwalten Sie ONTAP SSL-Zertifikate mit System Manager"

Schritte

1. Melden Sie sich als Root beim Konsolenagenten an. Laufen:

```
sudo su
```

2. Holen Sie sich das Docker-Volume für NetApp Backup and Recovery . Laufen:

```
docker volume ls | grep cbs
```

Ausgabebeispiel:

```
local service-manager-2_cloudmanager_cbs_volume
```

Der Volumename ist in den Bereitstellungsmodi „Standard“, „Privat“ und „Eingeschränkt“ unterschiedlich. Dieses Beispiel zeigt eine Standard-Cloud-Bereitstellung. Siehe "Bereitstellungsmodi der NetApp Console" .

3. Besorgen Sie sich die Halterung für das Volume. Laufen:

```
docker volume inspect service-manager-2_cloudmanager_cbs_volume | grep
Mountpoint
```

Ausgabebeispiel:

```
"Mountpoint": "/var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

Der Einhängepunkt ist in den Bereitstellungsmodi „Standard“, „Privat“ und „Eingeschränkt“ unterschiedlich. Dieses Beispiel zeigt eine Standard-Cloud-Bereitstellung. Siehe "Bereitstellungsmodi der NetApp Console" .

4. Wechseln Sie in das Mountpoint-Verzeichnis. Laufen:

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

5. Führen Sie einen der folgenden Schritte aus:
   - Wenn das ONTAP -Zertifikat von der Stammzertifizierungsstelle und einer Zwischenzertifizierungsstelle signiert ist, fügen Sie die `pem` Dateien von beiden in eine Datei mit dem Namen `ontap.crt` am aktuellen Standort.
   - Wenn das ONTAP -Zertifikat von einer einzigen Zertifizierungsstelle signiert ist, benennen Sie das `pem` Datei als `ontap.crt` und kopieren Sie es an den aktuellen Speicherort. Fügen Sie das Blattzertifikat nicht zu dieser Datei hinzu.

Schritte für den Cloudmanager_CBS-Container

Aktivieren Sie als Nächstes die ONTAP -Server-Zertifikatsüberprüfung in NetApp Backup and Recovery (Cloud Backup Service).

1. Wechseln Sie zum Verzeichnis des Docker-Volumes, das Sie in den vorherigen Schritten erhalten haben.

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Wechseln Sie in das Konfigurationsverzeichnis. Laufen:

```
cd cbs_config
```

3. Erstellen Sie eine Konfigurationsdatei wie unten gezeigt mit einem der folgenden Namen, basierend auf Ihrer Bereitstellungsumgebung:
   - `production-customer.json`Wird für Bereitstellungen im Standardmodus und eingeschränkten Modus verwendet.
   - `darksite-customer.json`Wird für Bereitstellungen im privaten Modus verwendet.

     Siehe "Bereitstellungsmodi der NetApp Console" .

     Konfigurationsdatei

```
{
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

4. Verlassen Sie den Container. Laufen:

```
exit
```

5. Starten Sie NetApp Backup and Recovery neu. Laufen:

```
docker restart cloudmanager_cbs
```

Schritte für den Container „cloudmanager_cbs_catalog“

Aktivieren Sie die ONTAP -Server-Zertifikatsüberprüfung für den Katalogisierungsdienst.

1. Wechseln Sie zum Docker-Volume. Laufen:

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Laufen:

```
cd cbs_catalog_config
```

3. Erstellen Sie eine Konfigurationsdatei wie unten gezeigt mit einem der folgenden Namen, basierend auf Ihrer Bereitstellungsumgebung:

   - `production-customer.json`Wird für Bereitstellungen im Standardmodus und eingeschränkten Modus verwendet.
   - `darksite-customer.json`Wird für Bereitstellungen im privaten Modus verwendet.

   Siehe "Bereitstellungsmodi der NetApp Console" .

   Konfigurationsdatei

```
{
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

4. Starten Sie NetApp Backup and Recovery neu. Laufen:

```
docker restart cloudmanager_cbs_catalog
```

Erstellen Sie ein Zertifikat für ONTAP und StorageGRID

Wenn Sie das Zertifikat sowohl für ONTAP als auch für StorageGRID aktivieren müssen, sieht die Konfigurationsdatei folgendermaßen aus:

Konfigurationsdatei für ONTAP und StorageGRID

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  },
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

Richten Sie Sicherungsziele ein, bevor Sie NetApp Backup and Recovery verwenden

Bevor Sie NetApp Backup and Recovery verwenden, führen Sie einige Schritte zum Einrichten von Sicherungszielen aus.

Bevor Sie beginnen, überprüfen Sie"Voraussetzungen" um sicherzustellen, dass Ihre Umgebung bereit ist.

Vorbereiten des Sicherungsziels

Bereiten Sie eines oder mehrere der folgenden Sicherungsziele vor:

- NetApp StorageGRID.

  Siehe "Entdecken Sie StorageGRID" .

  Siehe "StorageGRID -Dokumentation" für Details zu StorageGRID.

- Amazon Web Services. Siehe "Amazon S3-Dokumentation" .

Gehen Sie wie folgt vor, um AWS als Sicherungsziel vorzubereiten:

  - Richten Sie ein Konto in AWS ein.
  - Konfigurieren Sie die S3-Berechtigungen in AWS, die im nächsten Abschnitt aufgeführt sind.
  - Weitere Informationen zur Verwaltung Ihres AWS-Speichers in der Konsole finden Sie unter "Verwalten Sie Ihre Amazon S3-Buckets" .

- Microsoft Azure.
  - Siehe "Azure NetApp Files Dokumentation" .
  - Richten Sie ein Konto in Azure ein.
  - Konfigurieren "Azure-Berechtigungen" in Azure.
  - Weitere Informationen zur Verwaltung Ihres Azure-Speichers in der Konsole finden Sie unter "Verwalten Ihrer Azure-Speicherkonten" .

Nachdem Sie Optionen im Sicherungsziel selbst konfiguriert haben, konfigurieren Sie es später als Sicherungsziel in NetApp Backup and Recovery. Einzelheiten zum Konfigurieren des Sicherungsziels in NetApp Backup and Recovery finden Sie unter"Ermitteln von Sicherungszielen" .

S3-Berechtigungen einrichten

Sie müssen zwei Sätze von AWS S3-Berechtigungen konfigurieren:

- Berechtigungen für den Konsolenagenten zum Erstellen und Verwalten des S3-Buckets.
- Berechtigungen für den lokalen ONTAP Cluster, damit dieser Daten aus dem S3-Bucket lesen und schreiben kann.

Schritte

1. Stellen Sie sicher, dass der Konsolenagent über die erforderlichen Berechtigungen verfügt. Weitere Einzelheiten finden Sie unter "Richtlinienberechtigungen für die NetApp Console" .

   Wenn Sie Backups in AWS China-Regionen erstellen, müssen Sie den AWS-Ressourcennamen „arn“ unter allen *Resource*-Abschnitten in den IAM-Richtlinien von „aws“ in „aws-cn“ ändern. Beispiel: `arn:aws-cn:s3:::netapp-backup-*` .

2. Wenn Sie den Dienst aktivieren, werden Sie vom Backup-Assistenten aufgefordert, einen Zugriffsschlüssel und einen geheimen Schlüssel einzugeben. Diese Anmeldeinformationen werden an den ONTAP Cluster weitergegeben, damit ONTAP Daten im S3-Bucket sichern und wiederherstellen kann. Dazu müssen Sie einen IAM-Benutzer mit den folgenden Berechtigungen erstellen.

   Weitere Informationen finden Sie im "AWS-Dokumentation: Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer" .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource": "arn:aws:s3:::netapp-backup-*",
      "Effect": "Allow",
      "Sid": "backupPolicy"
    },
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*/*",
      "Effect": "Allow"
    }
  ]
}
```

Melden Sie sich bei NetApp Backup and Recovery an

Sie verwenden die NetApp Console , um sich bei NetApp Backup and Recovery anzumelden.

NetApp Backup and Recovery verwendet Identitäts- und Zugriffsverwaltung, um zu steuern, was jeder Benutzer tun kann.

Einzelheiten zu den Aktionen, die jede Rolle ausführen kann, finden Sie unter"NetApp Backup and Recovery -Benutzerrollen" .

Um sich bei der NetApp Console anzumelden, können Sie Ihre Anmeldeinformationen für die NetApp -Support -Site verwenden oder sich mit Ihrer E-Mail-Adresse und einem Kennwort für die Anmeldung bei der NetApp Console registrieren. "Erfahren Sie mehr über die Anmeldung" .

*Erforderliche NetApp Console * Superadministrator für Backup und Wiederherstellung oder Administratorrolle für Backup und Wiederherstellung zur Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Um einen Konsolenagenten hinzuzufügen, müssen Sie über die Superadministratorrolle „Backup und Wiederherstellung“ verfügen.

Schritte

1. Öffnen Sie einen Webbrowser und gehen Sie zu "NetApp Console" .

   Die Anmeldeseite der NetApp Console wird angezeigt.

2. Melden Sie sich bei der Konsole an.
3. Wählen Sie in der linken Navigation der Konsole **Schutz** > **Sicherung und Wiederherstellung**.
   - Wenn Sie sich zum ersten Mal bei Backup and Recovery anmelden und noch kein System zur Seite **Systeme** hinzugefügt haben, zeigt Backup and Recovery die Startseite "Willkommen bei der neuen NetApp Backup and Recovery" mit der Option zum Hinzufügen eines Systems an. Einzelheiten zum Hinzufügen eines Systems zur Seite **Systeme** finden Sie unter "Erste Schritte mit dem Standardmodus der NetApp Console"Die
   - Wenn Sie sich zum ersten Mal bei Backup and Recovery anmelden und zwar ein System in der Konsole haben, aber keine Ressourcen erkannt wurden, wird die Seite *Willkommen bei der neuen NetApp Backup and Recovery* mit einer Option zum **Erkennen von Ressourcen** angezeigt.
4. Falls noch nicht geschehen, wählen Sie die Option **Erkennen und verwalten**.
   - Informationen zu Microsoft SQL Server-Workloads finden Sie unter"Entdecken Sie Microsoft SQL Server-Workloads" .
   - Informationen zu VMware-Workloads finden Sie unter"Entdecken Sie VMware-Workloads" .
   - Informationen zu KVM-Workloads finden Sie unter"Entdecken Sie KVM-Workloads" .
   - Für Oracle Database-Workloads siehe "Oracle Database-Workloads entdecken".
   - Informationen zu Hyper-V-Workloads finden Sie unter"Entdecken Sie Hyper-V-Workloads" .
   - Informationen zu Kubernetes-Workloads finden Sie unter"Entdecken Sie Kubernetes-Workloads" .

Ermitteln Sie externe Sicherungsziele in NetApp Backup and Recovery

Führen Sie einige Schritte aus, um externe Sicherungsziele in NetApp Backup and Recovery zu ermitteln oder manuell hinzuzufügen.

Ermitteln eines Sicherungsziels

Konfigurieren Sie Ihre Sicherungsziele (Amazon Web Services (AWS) S3, Microsoft Azure Blob Storage, Google Cloud Storage oder StorageGRID), bevor Sie NetApp Backup and Recovery verwenden.

Sie können diese Ziele automatisch ermitteln oder manuell hinzufügen.

Geben Sie Anmeldeinformationen für den Zugriff auf das Speicherkonto ein. NetApp Backup and Recovery verwendet diese Anmeldeinformationen, um die Workloads zu ermitteln, die Sie sichern möchten.

Bevor Sie beginnen

Sie müssen mindestens eine Arbeitslast ermitteln, bevor Sie ein externes Sicherungsziel hinzufügen können.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie die Registerkarte **Offsite-Sicherungsziele**.
3. Wählen Sie **Sicherungsziel ermitteln**.
4. Wählen Sie einen der Sicherungszieltypen: **Amazon Web Services (AWS) S3**, **Microsoft Azure Blob Storage**, * StorageGRID* oder * ONTAP S3*.
5. Wählen Sie im Abschnitt **Speicherort der Anmeldeinformationen auswählen** den Speicherort aus, an dem sich die Anmeldeinformationen befinden, und wählen Sie dann aus, wie die Anmeldeinformationen verknüpft werden sollen.
6. Wählen Sie **Weiter**.
7. Geben Sie die Anmeldeinformationen ein. Die Informationen variieren je nach Art des ausgewählten Sicherungsziels und dem von Ihnen gewählten Speicherort der Anmeldeinformationen.
   - Für AWS:
     - **Anmeldeinformationsname**: Geben Sie den AWS-Anmeldeinformationsnamen ein.
     - **Zugriffsschlüssel**: Geben Sie das AWS-Geheimnis ein.
     - **Geheimschlüssel**: Geben Sie den geheimen AWS-Schlüssel ein.
   - Für Azure:
     - **Anmeldeinformationsname**: Geben Sie den Anmeldeinformationsnamen für Azure Blob Storage ein.
     - **Clientgeheimnis**: Geben Sie das Clientgeheimnis von Azure Blob Storage ein.
     - **Anwendungs-ID (Client-ID)**: Wählen Sie die Azure Blob Storage-Anwendungs-ID aus.
     - **Verzeichnis-Mandanten-ID**: Geben Sie die Azure Blob Storage-Mandanten-ID ein.
   - Für StorageGRID:
     - **Anmeldeinformationsname**: Geben Sie den Anmeldeinformationsnamen von StorageGRID ein.
     - **Gateway-Knoten-FQDN**: Geben Sie einen FQDN-Namen für StorageGRID ein.

- **Port**: Geben Sie die Portnummer für StorageGRID ein.
- **Zugriffsschlüssel**: Geben Sie den StorageGRID S3-Zugriffsschlüssel ein.
- **Geheimschlüssel**: Geben Sie den geheimen Schlüssel von StorageGRID S3 ein.

◦ Für ONTAP S3:

- **Anmeldeinformationsname**: Geben Sie den Anmeldeinformationsnamen für ONTAP S3 ein.
- **Gateway-Knoten-FQDN**: Geben Sie einen FQDN-Namen für ONTAP S3 ein.
- **Port**: Geben Sie die Portnummer für ONTAP S3 ein.
- **Zugriffsschlüssel**: Geben Sie den ONTAP S3-Zugriffsschlüssel ein.
- **Geheimschlüssel**: Geben Sie den geheimen Schlüssel von ONTAP S3 ein.

8. Wählen Sie **Entdecken**.

Einen Bucket für ein Sicherungsziel hinzufügen

Anstatt Buckets automatisch von NetApp Backup and Recovery erkennen zu lassen, können Sie einem externen Sicherungsziel manuell einen Bucket hinzufügen.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie **Offsite-Sicherungsziele**.
3. Wählen Sie das Ziel aus und wählen Sie rechts die **Aktionen*** **Symbol und wählen Sie *Bucket hinzufügen**.
4. Geben Sie die Bucket-Informationen ein. Die Informationen unterscheiden sich je nach Art des ausgewählten Sicherungsziels.

◦ Für AWS:

- **Bucketname**: Geben Sie den Namen des S3-Buckets ein. Das Präfix „netapp-backup“ ist ein erforderliches Präfix und wird automatisch zu dem von Ihnen angegebenen Namen hinzugefügt.
- **AWS-Konto**: Geben Sie den AWS-Kontonamen ein.
- **Bucket-Region**: Geben Sie die AWS-Region für den Bucket ein.
- **S3-Objektsperre aktivieren**: Wählen Sie diese Option, um die S3-Objektsperre für den Bucket zu aktivieren. S3 Object Lock verhindert, dass Objekte für einen bestimmten Aufbewahrungszeitraum gelöscht oder überschrieben werden, und bietet so eine zusätzliche Ebene des Datenschutzes. Sie können dies nur aktivieren, wenn Sie einen Bucket erstellen, und Sie können es später nicht mehr deaktivieren.
  - **Governance-Modus**: Wählen Sie diese Option, um den Governance-Modus für den S3 Object Lock-Bucket zu aktivieren. Im Governance-Modus können Sie Objekte vor dem Löschen oder Überschreiben durch die meisten Benutzer schützen, bestimmten Benutzern ist jedoch das Ändern der Aufbewahrungseinstellungen gestattet.
  - **Compliance-Modus**: Wählen Sie diese Option, um den Compliance-Modus für den S3 Object Lock-Bucket zu aktivieren. Der Compliance-Modus verhindert, dass Benutzer, einschließlich des Root-Benutzers, die Aufbewahrungseinstellungen ändern oder Objekte löschen, bis die Aufbewahrungsfrist abgelaufen ist.
- **Versionierung**: Wählen Sie diese Option, um die Versionierung für den S3-Bucket zu aktivieren. Durch die Versionierung können Sie mehrere Versionen von Objekten im Bucket behalten, was für Sicherungs- und Wiederherstellungszwecke nützlich sein kann.

- **Tags**: Wählen Sie Tags für den S3-Bucket aus. Tags sind Schlüssel-Wert-Paare, die zum Organisieren und Verwalten Ihrer S3-Ressourcen verwendet werden können.
- **Verschlüsselung**: Wählen Sie die Art der Verschlüsselung für den S3-Bucket aus. Zur Auswahl stehen entweder von AWS S3 verwaltete Schlüssel oder AWS Key Management Service-Schlüssel. Wenn Sie AWS Key Management Service-Schlüssel auswählen, müssen Sie die Schlüssel-ID angeben.

◦ Für Azure:

- **Abonnement**: Wählen Sie den Namen des Azure Blob Storage-Containers aus.
- **Ressourcengruppe**: Wählen Sie den Namen der Azure-Ressourcengruppe aus.
- **Instanzdetails**:
  - **Speicherkontoname**: Geben Sie den Namen des Azure Blob Storage-Containers ein.
  - **Azure-Region**: Geben Sie die Azure-Region für den Container ein.
  - **Leistungstyp**: Wählen Sie den Leistungstyp „Standard“ oder „Premium“ für den Azure Blob Storage-Container aus, der das erforderliche Leistungsniveau angibt.
  - **Verschlüsselung**: Wählen Sie den Verschlüsselungstyp für den Azure Blob Storage-Container aus. Zur Auswahl stehen entweder von Microsoft verwaltete Schlüssel oder vom Kunden verwaltete Schlüssel. Wenn Sie vom Kunden verwaltete Schlüssel auswählen, müssen Sie den Namen des Schlüsseltresors und den Schlüsselnamen angeben.

◦ Für StorageGRID:

- **Name des Sicherungsziels**: Wählen Sie den Namen des StorageGRID Buckets aus.
- **Bucket-Name**: Geben Sie den Namen des StorageGRID Buckets ein.
- **Region**: Geben Sie die StorageGRID -Region für den Bucket ein.
- **Versionierung aktivieren**: Wählen Sie diese Option, um die Versionierung für den StorageGRID Bucket zu aktivieren. Durch die Versionierung können Sie mehrere Versionen von Objekten im Bucket behalten, was für Sicherungs- und Wiederherstellungszwecke nützlich sein kann.
- **Objektsperre**: Wählen Sie diese Option, um die Objektsperre für den StorageGRID Bucket zu aktivieren. Durch die Objektsperre wird verhindert, dass Objekte für einen bestimmten Aufbewahrungszeitraum gelöscht oder überschrieben werden, und so eine zusätzliche Ebene des Datenschutzes geschaffen. Sie können dies nur aktivieren, wenn Sie einen Bucket erstellen, und Sie können es später nicht mehr deaktivieren.
- **Kapazität**: Geben Sie die Kapazität für den StorageGRID Bucket ein. Dies ist die maximale Datenmenge, die im Bucket gespeichert werden kann.

◦ Für ONTAP S3:

- **Name des Sicherungsziels**: Wählen Sie den Namen des ONTAP S3-Buckets aus.
- **Bucket-Zielname**: Geben Sie den Namen des ONTAP S3-Buckets ein.
- **Kapazität**: Geben Sie die Kapazität für den ONTAP S3-Bucket ein. Dies ist die maximale Datenmenge, die im Bucket gespeichert werden kann.
- **Versionierung aktivieren**: Wählen Sie diese Option, um die Versionierung für den ONTAP S3-Bucket zu aktivieren. Durch die Versionierung können Sie mehrere Versionen von Objekten im Bucket behalten, was für Sicherungs- und Wiederherstellungszwecke nützlich sein kann.
- **Objektsperre**: Wählen Sie diese Option, um die Objektsperre für den ONTAP S3-Bucket zu aktivieren. Durch die Objektsperre wird verhindert, dass Objekte für einen bestimmten Aufbewahrungszeitraum gelöscht oder überschrieben werden, und so eine zusätzliche Ebene des Datenschutzes geschaffen. Sie können dies nur aktivieren, wenn Sie einen Bucket erstellen, und

Sie können es später nicht mehr deaktivieren.

5. Wählen Sie **Hinzufügen**.

Anmeldeinformationen für ein Sicherungsziel ändern

Geben Sie die für den Zugriff auf das Sicherungsziel erforderlichen Anmeldeinformationen ein.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie **Offsite-Sicherungsziele**.
3. Wählen Sie das Ziel aus und wählen Sie rechts die **Aktionen*** **Symbol und wählen Sie *Anmeldeinformationen ändern**.
4. Geben Sie die neuen Anmeldeinformationen für das Sicherungsziel ein. Die Informationen unterscheiden sich je nach Art des ausgewählten Sicherungsziels.
5. Wählen Sie **Fertig**.

Wechseln Sie zu anderen NetApp Backup and Recovery -Workloads

Sie können zwischen den verschiedenen NetApp Backup and Recovery -Workloads wechseln.

Wechseln Sie zu einer anderen Arbeitslast

Sie können in der NetApp Backup and Recovery -Benutzeroberfläche zu einer anderen Arbeitslast wechseln.

Schritte

1. Wählen Sie in der linken Navigation der Konsole **Schutz** > **Sicherung und Wiederherstellung**.
2. Wählen Sie in der oberen rechten Ecke der Seite die Dropdown-Liste **Workload wechseln** aus.
3. Wählen Sie die Arbeitslast aus, zu der Sie wechseln möchten.

   Die Seite wird aktualisiert und zeigt die ausgewählte Arbeitslast an.

Konfigurieren der NetApp Backup and Recovery -Einstellungen

Nachdem Sie die NetApp Console eingerichtet haben, konfigurieren Sie die Sicherungs- und Wiederherstellungseinstellungen. Fügen Sie Anmeldeinformationen für Hostressourcen hinzu, importieren Sie SnapCenter -Ressourcen, konfigurieren Sie Protokollverzeichnisse und legen Sie VMware vCenter-Einstellungen fest. Führen Sie diese Schritte aus, bevor Sie Daten sichern oder wiederherstellen.

- Anmeldeinformationen für Hostressourcen hinzufügen für alle Windows-, Microsoft SQL Server-, Oracle Database- oder Linux-Hosts, bei denen NetApp Backup and Recovery eine Authentifizierung durchführen muss. Dies umfasst die Anmeldeinformationen des Windows-Gastbetriebssystems, die beim Wiederherstellen von Gastdateien oder -ordnern verwendet werden.

- Verwalten der VMware vCenter-Einstellungen.
- Importieren und Verwalten von SnapCenter -Hostressourcen. (Nur Microsoft SQL Server-Workloads)
- Fügen Sie eine KVM-Managementplattform hinzu.Die (Nur KVM-Workloads)
- Konfigurieren von Protokollverzeichnissen in Snapshots für Windows-Hosts.
- Erstellen einer Ausführungs-Hook-Vorlage zum Ausführen von Skripten vor und nach Backup-Jobs. (Nur Kubernetes-Workloads)

*Erforderliche NetApp Console * Superadministrator für Backup und Wiederherstellung, Backup-Administrator für Backup und Wiederherstellung, Wiederherstellungsadministrator für Backup und Wiederherstellung. Erfahren Sie mehr über"Rollen und Berechtigungen für Backup und Wiederherstellung" . "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Anmeldeinformationen für Hostressourcen hinzufügen

Fügen Sie Anmeldeinformationen für Hostressourcen hinzu. NetApp Backup and Recovery verwendet diese Anmeldeinformationen, um Workloads zu erkennen und Backup-Richtlinien anzuwenden.

Wenn Sie keine Anmeldeinformationen haben, erstellen Sie diese mit Berechtigungen für den Zugriff auf und die Verwaltung von Host-Workloads.

Sie müssen die folgenden Arten von Anmeldeinformationen konfigurieren:

- Microsoft SQL Server-Anmeldeinformationen
- SnapCenter Windows-Host-Anmeldeinformationen
- Anmeldeinformationen des Windows-Gastbetriebssystems, die beim Wiederherstellen von Gastdateien oder -ordnern verwendet werden
- Oracle-Datenbank-Zugangsdaten
- Anmeldeinformationen für den Linux-Host

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Einstellungen** aus.
2. Wählen Sie den Abwärtspfeil für **Anmeldeinformationen**.
3. Wählen Sie **Neue Anmeldeinformationen hinzufügen**.
4. Geben Sie die Zugangsdaten ein. Je nach gewähltem Authentifizierungsmodus werden unterschiedliche Felder angezeigt. Bewegen Sie den Mauszeiger über das Informationssymbol **i**, um weitere Informationen zu den Feldern zu erhalten.
    - **Name der Anmeldeinformationen**: Geben Sie einen Namen für die Anmeldeinformationen ein.
    - **Authentifizierungsmodus**: Wählen Sie **Windows**, **Microsoft SQL**, **Oracle Database** oder **Linux**.

Für Microsoft SQL Server-Workloads müssen Sie Anmeldeinformationen sowohl für Windows als auch für Microsoft SQL Server eingeben, daher müssen Sie zwei Sätze von Anmeldeinformationen hinzufügen.

Windows

i. Wenn Sie **Windows** ausgewählt haben:

- **Agenten**: Wählen Sie einen Konsolenagenten aus der Liste aus.
- **Domänen- und Benutzername**: Geben Sie den NetBIOS- oder Domänen-FQDN und den Benutzernamen für die Anmeldeinformationen ein.
- **Passwort**: Geben Sie das Passwort für die Anmeldeinformationen ein.

Microsoft SQL Server

i. Wenn Sie **Microsoft SQL Server** ausgewählt haben:

- **Domänen- und Benutzername**: Geben Sie den NetBIOS- oder Domänen-FQDN und den Benutzernamen für die Anmeldeinformationen ein.
- **Passwort**: Geben Sie das Passwort für die Anmeldeinformationen ein.
- **Hosts**: Wählen Sie eine ermittelte SQL Server-Hostadresse aus.
- **SQL Server-Instanz**: Wählen Sie eine erkannte SQL Server-Instanz aus.

Oracle-Datenbank

i. Wenn Sie **Oracle Database** ausgewählt haben:

- **Agenten**: Wählen Sie einen Konsolenagenten aus der Liste aus.
- **Benutzername**: Geben Sie den Benutzernamen für die Anmeldeinformationen ein.
- **Passwort**: Geben Sie das Passwort für die Anmeldeinformationen ein.

Linux

i. Wenn Sie **Linux** ausgewählt haben:

- **Agenten**: Wählen Sie einen Konsolenagenten aus der Liste aus.
- **Benutzername**: Geben Sie den Benutzernamen für die Anmeldeinformationen ein.
- **Passwort**: Geben Sie das Passwort für die Anmeldeinformationen ein.

5. Wählen Sie **Hinzufügen**.

Anmeldeinformationen für Hostressourcen bearbeiten

Sie können das Passwort für alle von Ihnen erstellten Zugangsdaten später bearbeiten.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Einstellungen** aus.
2. Wählen Sie den Abwärtspfeil aus, um den Abschnitt **Anmeldeinformationen** zu erweitern.
3. Wählen Sie das Symbol Aktionen ••• > **Anmeldeinformationen bearbeiten**.
   - **Passwort**: Geben Sie das Passwort für die Anmeldeinformationen ein.
4. Wählen Sie **Speichern**.

Verwalten der VMware vCenter-Einstellungen

Geben Sie VMware vCenter-Anmeldeinformationen ein, um Workloads für die Sicherung zu ermitteln. Wenn

Sie keine Anmeldeinformationen haben, erstellen Sie diese mit Berechtigungen für den Zugriff auf und die Verwaltung der VMware vCenter Server-Workloads.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Einstellungen** aus.
2. Wählen Sie den Abwärtspfeil aus, um den Abschnitt **VMware vCenter** zu erweitern.
3. Wählen Sie **vCenter hinzufügen**.
4. Geben Sie die VMware vCenter Server-Informationen ein.
   - **vCenter FQDN oder IP-Adresse**: Geben Sie einen FQDN-Namen oder die IP-Adresse für den VMware vCenter Server ein.
   - **Benutzername** und **Passwort**: Geben Sie den Benutzernamen und das Passwort für den VMware vCenter Server ein.
   - **Port**: Geben Sie die Portnummer für den VMware vCenter Server ein.
   - **Protokoll**: Wählen Sie **HTTP** oder **HTTPS**.
5. Wählen Sie **Hinzufügen**.

Importieren und Verwalten von SnapCenter -Hostressourcen

Wenn Sie zuvor SnapCenter zum Sichern Ihrer Ressourcen verwendet haben, können Sie diese Ressourcen in NetApp Backup and Recovery importieren und verwalten. Mit dieser Option können Sie SnapCenter -Serverinformationen importieren, um mehrere SnapCenter -Server zu registrieren und Datenbank-Workloads zu ermitteln.

Dies ist ein zweiteiliger Prozess:

- Importieren Sie SnapCenter Server-Anwendungs- und Hostressourcen
- Verwalten ausgewählter SnapCenter -Hostressourcen

Importieren Sie SnapCenter Server-Anwendungs- und Hostressourcen

Dieser erste Schritt importiert Hostressourcen aus SnapCenter und zeigt diese Ressourcen auf der Inventarseite von NetApp Backup and Recovery an. Zu diesem Zeitpunkt werden die Ressourcen noch nicht von NetApp Backup and Recovery verwaltet.

Nachdem Sie SnapCenter -Hostressourcen importiert haben, übernimmt NetApp Backup and Recovery nicht die Schutzverwaltung. Dazu müssen Sie die Verwaltung dieser Ressourcen in NetApp Backup and Recovery ausdrücklich auswählen.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Einstellungen** aus.
2. Wählen Sie den Abwärtspfeil aus, um den Abschnitt **Aus SnapCenter importieren** zu erweitern.
3. Wählen Sie **Aus SnapCenter importieren**, um die SnapCenter -Ressourcen zu importieren.
4. Geben Sie * Anmeldeinformationen für die SnapCenter -Anwendung* ein:
   a. * SnapCenter FQDN oder IP-Adresse*: Geben Sie den FQDN oder die IP-Adresse der SnapCenter -Anwendung selbst ein.
   b. **Port**: Geben Sie die Portnummer für den SnapCenter -Server ein.

c. **Benutzername** und **Passwort**: Geben Sie den Benutzernamen und das Passwort für den SnapCenter -Server ein.

d. **Konsolenagent**: Wählen Sie den Konsolenagenten für SnapCenter aus.

5. Geben Sie * SnapCenter -Server-Host-Anmeldeinformationen* ein:

   a. **Vorhandene Anmeldeinformationen**: Wenn Sie diese Option auswählen, können Sie die vorhandenen Anmeldeinformationen verwenden, die Sie bereits hinzugefügt haben. Geben Sie den Anmeldenamen ein.

   b. **Neue Anmeldeinformationen hinzufügen**: Wenn Sie keine vorhandenen SnapCenter -Host -Anmeldeinformationen haben, können Sie neue Anmeldeinformationen hinzufügen. Geben Sie den Anmeldenamen, den Authentifizierungsmodus, den Benutzernamen und das Kennwort ein.

6. Wählen Sie **Importieren**, um Ihre Eingaben zu bestätigen und den SnapCenter -Server zu registrieren.

   Wenn der SnapCenter -Server bereits registriert ist, können Sie die vorhandenen Registrierungsdetails aktualisieren.

Ergebnis

Auf der Inventarseite werden die importierten SnapCenter -Ressourcen angezeigt.

Verwalten von SnapCenter -Hostressourcen

Nachdem Sie die SnapCenter -Ressourcen importiert haben, verwalten Sie diese Hostressourcen in NetApp Backup and Recovery. Nachdem Sie die Verwaltung dieser importierten Ressourcen ausgewählt haben, kann NetApp Backup and Recovery die Ressourcen, die Sie aus SnapCenter importieren, sichern und wiederherstellen. Sie müssen diese Ressourcen nicht mehr im SnapCenter Server verwalten.

Schritte

1. Nachdem Sie die SnapCenter -Ressourcen importiert haben, wählen Sie auf der angezeigten Inventarseite die importierten SnapCenter -Ressourcen aus, die von nun an von NetApp Backup and Recovery verwaltet werden sollen.
2. Wählen Sie das Symbol Aktionen ••• > **Verwalten**, um die Ressourcen zu verwalten.
3. Wählen Sie **In NetApp Console verwalten**.

   Auf der Inventarseite wird unter dem Hostnamen **Verwaltet** angezeigt, um anzuzeigen, dass die ausgewählten Hostressourcen jetzt von NetApp Backup and Recovery verwaltet werden.

Importierte SnapCenter -Ressourcen bearbeiten

Sie können SnapCenter -Ressourcen später erneut importieren oder die importierten SnapCenter -Ressourcen bearbeiten, um die Registrierungsdetails zu aktualisieren.

Sie können nur die Port- und Kennwortdetails für den SnapCenter -Server ändern.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Einstellungen** aus.
2. Wählen Sie den Abwärtspfeil für **Aus SnapCenter importieren**.

   Auf der Seite „Aus SnapCenter importieren“ werden alle vorherigen Importe angezeigt.

3. Wählen Sie das Symbol Aktionen ••• > **Bearbeiten**, um die Ressourcen zu aktualisieren.

4. Aktualisieren Sie bei Bedarf das SnapCenter -Passwort und die Portdetails.
5. Wählen Sie **Importieren**.

Fügen Sie eine KVM-Managementplattform hinzu.

Wenn Sie die Apache CloudStack-Managementplattform zur Verwaltung von KVM-Ressourcen verwenden, müssen Sie diese mit NetApp Backup and Recovery integrieren, damit Backup and Recovery die verwalteten KVM-Hosts und VMs erkennen und schützen kann.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Einstellungen** aus.
2. Klicken Sie auf den Abwärtspfeil, um den Abschnitt **Managementplattform** zu erweitern.
3. Wählen Sie **Verwaltungsplattform-Anmeldeinformationen hinzufügen**.
4. Geben Sie die folgenden Informationen ein:
   - **IP-Adresse oder FQDN der Managementplattform**: Geben Sie die IP-Adresse oder den vollqualifizierten Domänennamen der Managementplattform ein.
   - **API-Schlüssel**: Geben Sie den API-Schlüssel ein, der zur Authentifizierung von API-Anfragen verwendet werden soll.
   - **Geheimer Schlüssel**: Geben Sie den geheimen Schlüssel ein, der zur Authentifizierung von API-Anfragen verwendet werden soll.
   - **Port**: Geben Sie den Port ein, der für die Kommunikation zwischen Backup und Recovery und der Managementplattform verwendet werden soll.
   - **Agenten**: Wählen Sie einen Konsolenagenten aus, der die Kommunikation zwischen Backup und Recovery und der Managementplattform erleichtern soll.
5. Wenn Sie fertig sind, wählen Sie **Hinzufügen**.

Konfigurieren von Protokollverzeichnissen in Snapshots für Windows-Hosts

Bevor Sie Richtlinien für Windows-Hosts erstellen, sollten Sie Protokollverzeichnisse in Snapshots für Windows-Hosts konfigurieren. Protokollverzeichnisse werden zum Speichern der Protokolle verwendet, die während des Sicherungsvorgangs generiert werden.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie auf der Inventarseite eine Arbeitslast aus und wählen Sie dann das Symbol Aktionen ••• > **Details anzeigen**, um die Arbeitslastdetails anzuzeigen.
3. Wählen Sie auf der Seite mit den Inventardetails, auf der Microsoft SQL Server angezeigt wird, die Registerkarte „Hosts“ aus.
4. Wählen Sie auf der Seite „Inventardetails“ einen Host aus und wählen Sie das Symbol „Aktionen“ ••• > **Protokollverzeichnis konfigurieren**.
5. Durchsuchen Sie das Protokollverzeichnis oder geben Sie den Pfad ein.
6. Wählen Sie **Speichern**.

Erstellen einer Ausführungs-Hook-Vorlage

Sie können eine benutzerdefinierte Ausführungs-Hook-Vorlage erstellen, mit der Sie Aktionen vor oder nach

einem Datenschutzvorgang für eine Anwendung ausführen können.

Vorlagen, die Sie hier erstellen, sind nur beim Schutz von Kubernetes-Workloads verwendbar.

Schritte

1. Gehen Sie in der Konsole zu **Schutz** > **Sicherung und Wiederherstellung**.
2. Wählen Sie die Registerkarte **Einstellungen**.
3. Erweitern Sie den Abschnitt **Ausführungs-Hook-Vorlage**.
4. Wählen Sie **Ausführungs-Hook-Vorlage erstellen**.
5. Geben Sie einen Namen für den Ausführungs-Hook ein.
6. Wählen Sie optional einen Hook-Typ aus. Beispielsweise wird ein Post-Restore-Hook ausgeführt, nachdem der Wiederherstellungsvorgang abgeschlossen ist.
7. Geben Sie im Textfeld **Skript** das ausführbare Shell-Skript ein, das Sie als Teil der Ausführungs-Hook-Vorlage ausführen möchten. Optional können Sie **Skript hochladen** auswählen, um stattdessen eine Skriptdatei hochzuladen.
8. Wählen Sie **Erstellen**.

   Nachdem Sie die Vorlage erstellt haben, wird sie in der Vorlagenliste im Abschnitt **Ausführungs-Hook-Vorlage** angezeigt.

Richten Sie rollenbasierte Zugriffssteuerung in NetApp Backup and Recovery ein

Um die Sicherheit zu erhöhen und den Ressourcenzugriff zu kontrollieren, konfigurieren Sie rollenbasierte Zugriffssteuerung für NetApp Backup and Recovery. Die NetApp Console unterstützt rollenbasierte Zugriffssteuerung (RBAC) für einige Backup and Recovery Workloads. Sie können diesen Workloads spezifische Administrator- oder Betrachterrollen zuweisen. Andere Workloads, die noch keine rollenbasierte Zugriffssteuerung unterstützen, bleiben für alle Benutzer mit Backup and Recovery Rollen zugänglich, bis die Zuordnung auf Projektebene unterstützt wird.

Führen Sie diese Schritte aus, um den Zugriff auf Ressourcen in Ihrer Organisation zu steuern. Nehmen Sie Änderungen auf der Seite **Administration > Identität und Zugriff** im NetApp Console-Menü vor.

Diese Schritte setzen voraus, dass Ihnen in der Console die Rolle „Organization Admin“ zugewiesen ist.

Schritte

1. Erstellen Sie die Identitäts- und Zugriffsprojektstruktur.

   Als Organisationsadministrator richten Sie den Ordner für Identität und Zugriff sowie die Projektstruktur ein, in der die Workloads gespeichert werden.

2. Benutzerrollen zuweisen.
   a. Primäre Option:

Fügen Sie jedem für Arbeitslasten vorgesehenen Projekt Benutzer hinzu und weisen Sie ihnen die entsprechende Rolle zu. Beispiel:

- **Organisationsadministrator** und **Backup and Recovery Superadministrator**: Ein Benutzer mit diesen Rollen kann alle Ressourcen in allen Organisationen sehen, und Backup and Recovery Workloads erkennen und diese Projekten zuordnen (zum Beispiel US East oder US West).
- **Ordner- oder Projektadministrator** und **Backup and Recovery Superadmin**: Ein Benutzer mit diesen Rollen kann nur die Ressourcen in dem Ordner oder Projekt sehen, für das er Berechtigungen hat, kann aber Backup and Recovery Workloads erkennen und sie diesem Projekt zuweisen.

b. Alternative Option:

Anstatt einem Benutzer vollen Backup and Recovery-Administratorzugriff zu gewähren, können Sie sich selbst die Backup and Recovery-Superadmin-Rolle zuweisen und die Workloads direkt entdecken.

3. Workloads in NetApp Backup and Recovery ermitteln.

Organisation-Admins oder Ordner- oder Projekt-Admins entdecken die verfügbaren Workloads und wählen das entsprechende Projekt aus (wie US East oder US West). Jeder Workload wird automatisch dem ausgewählten Projekt zugeordnet.

4. Fügen Sie Benutzer zu Projekten hinzu.

Organisation-Admins oder Ordner-/Projekt-Admins fügen Console-Benutzer zu Projekten mit Workloads hinzu. Weisen Sie Benutzern die Rolle Organization viewer und eine Backup and Recovery-Rolle entsprechend ihren Zugriffsanforderungen zu. Benutzer mit der richtigen Backup and Recovery-Rolle erhalten automatisch Zugriff auf neue Workloads in diesen Projekten.

Verwandte Informationen

- "Erfahren Sie mehr über das NetApp Console-Identitäts- und Zugriffsmanagement".
- "NetApp Backup and Recovery -Rollen in der NetApp Console".