Cloud Volumes ONTAP Dokumentation

Cloud Volumes ONTAP

NetApp
February 26, 2026

This PDF was generated from https://docs.netapp.com/de-de/storage-management-cloud-volumes-ontap/index.html on February 26, 2026. Always check docs.netapp.com for the latest.

Inhalt

Cloud Volumes ONTAP Dokumentation . . . 1
Versionshinweise . . . 2
Was ist neu in Cloud Volumes ONTAP . . . 2
26. Februar 2026 . . . 2
19. Februar 2026 . . . 4
17. Februar 2026 . . . 5
12. Februar 2026 . . . 5
10. Februar 2026 . . . 6
9. Februar 2026 . . . 6
12. Januar 2026 . . . 8
10. Dezember 2025 . . . 8
10. November 2025 . . . 9
17. Oktober 2025 . . . 9
06. Oktober 2025 . . . 9
04. September 2025 . . . 10
11. August 2025 . . . 10
14. Juli 2025 . . . 10
25. Juni 2025 . . . 11
29. Mai 2025 . . . 11
12. Mai 2025 . . . 11
16. April 2025 . . . 11
14. April 2025 . . . 12
03. April 2025 . . . 12
28. März 2025 . . . 12
12. März 2025 . . . 12
10. März 2025 . . . 13
06. März 2025 . . . 13
03. März 2025 . . . 13
18. Februar 2025 . . . 13
10. Februar 2025 . . . 13
09. Dezember 2024 . . . 14
11. November 2024 . . . 14
25. Oktober 2024 . . . 16
07. Oktober 2024 . . . 16
09. September 2024 . . . 16
23. August 2024 . . . 17
22. August 2024 . . . 17
08. August 2024 . . . 17
10. Juni 2024 . . . 18
17. Mai 2024 . . . 18
23. April 2024 . . . 18
08. März 2024 . . . 19
05. März 2024 . . . 19

02. Februar 2024 . . . 19
16. Januar 2024 . . . 19
08. Januar 2024 . . . 19
06. Dezember 2023 . . . 20
05. Dezember 2023 . . . 20
10. November 2023 . . . 21
08. November 2023 . . . 21
01. November 2023 . . . 21
23. Oktober 2023 . . . 21
06. Oktober 2023 . . . 22
10. September 2023 . . . 22
30. Juli 2023 . . . 22
26. Juli 2023 . . . 23
02. Juli 2023 . . . 23
26. Juni 2023 . . . 23
04. Juni 2023 . . . 23
07. Mai 2023 . . . 24
04. April 2023 . . . 25
3. April 2023 . . . 25
13. März 2023 . . . 27
05. März 2023 . . . 27
05. Februar 2023 . . . 28
1. Januar 2023 . . . 29
15. Dezember 2022 . . . 29
08. Dezember 2022 . . . 29
04. Dezember 2022 . . . 30
15. November 2022 . . . 30
06. November 2022 . . . 30
18. September 2022 . . . 31
31. Juli 2022 . . . 31
18. Juli 2022 . . . 32
3. Juli 2022 . . . 32
07. Juni 2022 . . . 33
02. Mai 2022 . . . 35
3. April 2022 . . . 36
27. Februar 2022 . . . 37
09. Februar 2022 . . . 37
06. Februar 2022 . . . 37
30. Januar 2022 . . . 38
02. Januar 2022 . . . 38
28. November 2021 . . . 40
04. Oktober 2021 . . . 41
02. September 2021 . . . 41
07. Juli 2021 . . . 41
30. Mai 2021 . . . 44

24. Mai 2021 . . . 45
11. April 2021 . . . 45
08. März 2021 . . . 45
04. Januar 2021 . . . 46
03. November 2020 . . . 48
Bekannte Einschränkungen . . . 48
Die Konsole unterstützt die Erstellung von FlexGroup -Volumes nicht . . . 48
Die Konsole unterstützt S3 mit Cloud Volumes ONTAP nicht . . . 48
Die Konsole unterstützt keine Notfallwiederherstellung für Speicher-VMs . . . 48
Versionshinweise zu Cloud Volumes ONTAP . . . 49
Erste Schritte . . . 50
Erfahren Sie mehr über Cloud Volumes ONTAP . . . 50
Unterstützte ONTAP -Versionen für Cloud Volumes ONTAP Bereitstellungen . . . 51
AWS . . . 51
Azurblau . . . 52
Google Cloud . . . 53
Erste Schritte mit Amazon Web Services . . . 54
Schnellstart für Cloud Volumes ONTAP in AWS . . . 54
Planen Sie Ihre Cloud Volumes ONTAP Konfiguration in AWS . . . 55
Richten Sie Ihr Netzwerk ein . . . 59
Richten Sie Cloud Volumes ONTAP für die Verwendung eines vom Kunden verwalteten Schlüssels in AWS ein . . . 84
Einrichten von AWS IAM-Rollen für Cloud Volumes ONTAP Knoten . . . 88
Einrichten der Lizenzierung für Cloud Volumes ONTAP in AWS . . . 97
Stellen Sie Cloud Volumes ONTAP in AWS mithilfe der Schnellbereitstellung bereit . . . 105
Starten Sie Cloud Volumes ONTAP in AWS . . . 109
Stellen Sie Cloud Volumes ONTAP in AWS Secret Cloud oder AWS Top Secret Cloud bereit . . . 123
Erste Schritte in Microsoft Azure . . . 140
Informieren Sie sich über die Bereitstellungsoptionen von Cloud Volumes ONTAP in Azure . . . 140
Erste Schritte in der NetApp Console . . . 142
Stellen Sie Cloud Volumes ONTAP vom Azure Marketplace bereit . . . 196
Erste Schritte in Google Cloud . . . 200
Schnellstart für Cloud Volumes ONTAP in Google Cloud . . . 200
Planen Sie Ihre Cloud Volumes ONTAP Konfiguration in Google Cloud . . . 201
Einrichten des Google Cloud-Netzwerks für Cloud Volumes ONTAP . . . 205
Richten Sie VPC Service Controls ein, um Cloud Volumes ONTAP in Google Cloud bereitzustellen . . . 218
Erstellen Sie ein Google Cloud-Dienstkonto für Cloud Volumes ONTAP . . . 220
Verwenden von kundenverwalteten Verschlüsselungsschlüsseln mit Cloud Volumes ONTAP . . . 223
Einrichten der Lizenzierung für Cloud Volumes ONTAP in Google Cloud . . . 224
Starten Sie Cloud Volumes ONTAP in Google Cloud . . . 229
Google Cloud Platform-Bildüberprüfung . . . 242
Verwenden Sie Cloud Volumes ONTAP . . . 254
Lizenzverwaltung . . . 254
Verwalten Sie die kapazitätsbasierte Lizenzierung für Cloud Volumes ONTAP . . . 254
Verwalten Sie Keystone -Abonnements für Cloud Volumes ONTAP über die NetApp Console . . . 259

Verwalten Sie die knotenbasierte Lizenzierung für Cloud Volumes ONTAP . . . 261
Volume- und LUN-Verwaltung . . . 267
Erstellen Sie ein FlexVol volume auf einem Cloud Volumes ONTAP -System . . . 267
Verwalten Sie Volumes auf Cloud Volumes ONTAP -Systemen . . . 273
Tieren Sie inaktive Cloud Volumes ONTAP Daten auf einen kostengünstigen Objektspeicher . . . 283
Stellen Sie von Ihrem Hostsystem aus eine Verbindung zu einem LUN auf Cloud Volumes ONTAP . . . 292
Beschleunigen Sie den Datenzugriff mit FlexCache -Volumes auf einem Cloud Volumes ONTAP System . . . 293
Aggregatverwaltung . . . 294
Erstellen Sie ein Aggregat für Cloud Volumes ONTAP Systeme . . . 294
Verwalten von Aggregaten für Cloud Volumes ONTAP -Cluster . . . 297
Verwalten Sie die Gesamtkapazität von Cloud Volumes ONTAP auf einem Konsolenagenten . . . 298
Verwalten der Festplattenleistung in Azure . . . 300
Storage-VM-Verwaltung . . . 303
Verwalten Sie Speicher-VMs für Cloud Volumes ONTAP . . . 303
Verwalten Sie datenbereitstellende Speicher-VMs für Cloud Volumes ONTAP in AWS . . . 305
Verwalten von datenbereitstellenden Speicher-VMs für Cloud Volumes ONTAP in Azure . . . 312
Verwalten Sie datenbereitstellende Speicher-VMs für Cloud Volumes ONTAP in Google Cloud . . . 315
Einrichten der Speicher-VM-Notfallwiederherstellung für Cloud Volumes ONTAP . . . 318
Sicherheit und Datenverschlüsselung . . . 318
Verschlüsseln Sie Volumes auf Cloud Volumes ONTAP mit NetApp -Verschlüsselungslösungen . . . 318
Verwalten Sie Cloud Volumes ONTAP Verschlüsselungsschlüssel mit dem AWS Key Management Service . . . 319
Verwalten Sie Cloud Volumes ONTAP Verschlüsselungsschlüssel mit Azure Key Vault . . . 320
Verwalten Sie Cloud Volumes ONTAP Verschlüsselungsschlüssel mit Google Cloud KMS . . . 327
Aktivieren Sie NetApp Ransomware-Schutzlösungen für Cloud Volumes ONTAP . . . 329
Erstellen Sie manipulationssichere Snapshot-Kopien von WORM-Dateien auf Cloud Volumes ONTAP 331
Systemadministration . . . 332
Upgrade von Cloud Volumes ONTAP . . . 332
Registrieren Sie Cloud Volumes ONTAP Pay-as-you-go-Systeme . . . 343
Konvertieren Sie eine knotenbasierte Cloud Volumes ONTAP -Lizenz in eine kapazitätsbasierte Lizenz . . . 345
Starten und Stoppen eines Cloud Volumes ONTAP -Systems . . . 347
Synchronisieren Sie die Cloud Volumes ONTAP -Systemzeit mithilfe des NTP-Servers . . . 350
Ändern Sie die Schreibgeschwindigkeit des Systems . . . 351
Ändern Sie das Administratorkennwort für den Cloud Volumes ONTAP -Cluster . . . 351
Systeme hinzufügen, entfernen oder löschen . . . 352
AWS -Verwaltung . . . 355
Azure-Verwaltung . . . 357
Google Cloud-Verwaltung . . . 369
Verwalten Sie Cloud Volumes ONTAP mit System Manager . . . 379
Verwalten von Cloud Volumes ONTAP über die CLI . . . 381
Systemzustand und Ereignisse . . . 382
Überprüfen Sie das AutoSupport -Setup für Cloud Volumes ONTAP . . . 382
EMS für Cloud Volumes ONTAP -Systeme konfigurieren . . . 386

Konzepte . . . 387
Lizenzierung . . . 387
Lizenzierung für Cloud Volumes ONTAP . . . 387
Erfahren Sie mehr über kapazitätsbasierte Lizenzen für Cloud Volumes ONTAP . . . 391
Storage . . . 396
Unterstützte Client-Protokolle für Cloud Volumes ONTAP . . . 396
Für Cloud Volumes ONTAP -Cluster verwendete Festplatten und Aggregate . . . 397
Erfahren Sie mehr über die Unterstützung für AWS Elastic Volumes mit Cloud Volumes ONTAP . . . 399
Erfahren Sie mehr über Data Tiering mit Cloud Volumes ONTAP in AWS, Azure oder Google Cloud . . . 405
Cloud Volumes ONTAP -Speicherverwaltung . . . 410
Schreibgeschwindigkeit . . . 413
Flash-Cache . . . 416
Erfahren Sie mehr über WORM-Speicher auf Cloud Volumes ONTAP . . . 416
Hochverfügbarkeitspaare . . . 419
Erfahren Sie mehr über Cloud Volumes ONTAP HA-Paare in AWS . . . 419
Erfahren Sie mehr über Cloud Volumes ONTAP HA-Paare in Azure . . . 426
Erfahren Sie mehr über Cloud Volumes ONTAP HA-Paare in Google Cloud . . . 431
Vorgänge sind nicht verfügbar, wenn ein Knoten im Cloud Volumes ONTAP HA-Paar offline ist . . . 436
Erfahren Sie mehr über die Datenverschlüsselung und den Ransomware-Schutz von Cloud Volumes ONTAP . . . 437
Verschlüsselung ruhender Daten . . . 437
ONTAP -Virenscan . . . 439
Ransomware-Schutz . . . 439
Erfahren Sie mehr über die Leistungsüberwachung für Cloud Volumes ONTAP -Workloads . . . 440
Leistungstechnische Berichte . . . 440
CPU-Leistung . . . 440
Lizenzverwaltung für knotenbasiertes BYOL . . . 441
BYOL-Systemlizenzen . . . 441
Lizenzmanagement für ein neues System . . . 441
Lizenzablauf . . . 441
Lizenzerneuerung . . . 442
Lizenzübertragung auf ein neues System . . . 442
Erfahren Sie, wie AutoSupport und Digital Advisor für Cloud Volumes ONTAP verwendet werden . . . 442
Unterstützte Standardkonfigurationen für Cloud Volumes ONTAP . . . 443
Standard-Setup . . . 443
Interne Festplatten für Systemdaten . . . 445
Wissen und Unterstützung . . . 449
Für Support registrieren . . . 449
Übersicht zur Support-Registrierung . . . 449
Registrieren Sie die NetApp Console für den NetApp Support . . . 449
NSS-Anmeldeinformationen für Cloud Volumes ONTAP Support zuordnen . . . 451
Hilfe erhalten . . . 453
Erhalten Sie Unterstützung für den Dateidienst eines Cloud-Anbieters . . . 453
Nutzen Sie Möglichkeiten zur Selbsthilfe . . . 453
Erstellen Sie einen Fall mit dem NetApp Support . . . 453

Verwalten Sie Ihre Supportfälle . . . 456
Rechtliche Hinweise . . . 458
Copyright . . . 458
Marken . . . 458
Patente . . . 458
Datenschutzrichtlinie . . . 458
Open Source . . . 458

Cloud Volumes ONTAP Dokumentation

Versionshinweise

Was ist neu in Cloud Volumes ONTAP

Informieren Sie sich über die Neuerungen beim Cloud Volumes ONTAP -Management in der NetApp Console.

Die auf dieser Seite beschriebenen Verbesserungen beziehen sich speziell auf die Verwaltung von Cloud Volumes ONTAP über die Konsole. Um zu erfahren, was es Neues bei der Cloud Volumes ONTAP -Software gibt, "Gehen Sie zu den Versionshinweisen zu Cloud Volumes ONTAP" .

26. Februar 2026

Unterstützung für Google Infrastructure Manager für private mode deployments

Cloud Volumes ONTAP 9.16.1 und höher unterstützen jetzt "Google Cloud Infrastructure Manager" (IM) anstelle von "Cloud Deployment Manager" (DM) für neue private Mode-Bereitstellungen in Google Cloud. Google wird Deployment Manager als Infrastrukturdienst in naher Zukunft zugunsten des fortschrittlicheren Infrastructure Manager einstellen.

Ab dem 25. Februar 2026 verwendet Cloud Volumes ONTAP den Infrastructure Manager für neue und bestehende Bereitstellungen im privaten Modus. Diese Tabelle erklärt die grundlegenden Arbeitsabläufe für Sie:

Szenario	Aktion	Neue APIs für den Agent	Neue Berechtigungen für den Agent	Neue Google Cloud APIs für Cloud Volumes ONTAP	Dokumentressourcen
Vorhandener Agent und bestehende Bereitstellung im privaten Modus	Aktualisieren Sie den NetApp Console-Agenten auf die neueste Version, indem Sie das Installationsprogramm von der NetApp Support Site herunterladen und den Agenten anschließend manuell auf Ihrem Host installieren, damit er die Infrastructure Manager APIs nutzen kann. Konvertieren Sie danach die bestehenden Cloud Volumes ONTAP Systeme zur Verwendung von Infrastructure Manager.	• Cloud Infrastructure Manager API • Cloud Quotas API • Cloud Build API	Alle für die Console-Version aufgeführten Berechtigungen: • "8. Dezember 2025" • "09. Februar 2026" • cloudbuild.workerpools.get • cloudbuild.workerpools.get	• https://cloudbuild.googleapis.com/v1 • https://www.googleapis.com/upload/storage/v1 • https://config.googleapis.com/v1	"Konfigurieren vorhandener Cloud Volumes ONTAP Deployments für Google Cloud Infrastructure Manager"

Szenario	Aktion	Neue APIs für den Agent	Neue Berechtigungen für den Agent	Neue Google Cloud APIs für Cloud Volumes ONTAP	Dokumentressourcen
Neuer Agent und neue Bereitstellung	Erstellen Sie einen neuen Agenten und stellen Sie ein neues Cloud Volumes ONTAP System im privaten Modus bereit.				• "Erstellen Sie einen Console-Agenten aus Google Cloud" • "Schnellstart für Bereitstellungen im privaten Modus"

Bei Bereitstellungen im privaten Modus sind einige Konfigurationsänderungen erforderlich, damit Cloud Volumes ONTAP den Infrastructure Manager verwenden kann. Siehe "Infrastructure Manager-Konfiguration für private Modus-Bereitstellungen".

Weiterführende Links

- "NetApp Console Agent 4.2.0 Versionshinweise"
- "Erforderliche Berechtigungen für Google Cloud Infrastructure Manager"

19. Februar 2026

Neue Regionen, die in Azure unterstützt werden

Sie können Cloud Volumes ONTAP 9.12.1 GA und höher jetzt in einzelnen und mehreren Verfügbarkeitszonen in Azure in den folgenden Regionen bereitstellen. Dies umfasst die Unterstützung sowohl für Einzelknoten- als auch für Hochverfügbarkeitsbereitstellungen (HA).

- Japan West (japanwest)
- Indonesien Central (indonesiacentral)

Eine Liste aller Regionen finden Sie im "Globale Regionenkarte unter Azure" .

17. Februar 2026

Cloud Volumes ONTAP Unterstützung für Google Cloud VMs der nächsten Generation

Mit 9.18.1 wechselt NetApp bei neuen Cloud Volumes ONTAP-Bereitstellungen von N2-VMs auf die nächste Generation der Google Cloud C3-Serien-VMs für ein schnelleres und skalierbareres Erlebnis. Sie können jetzt die Vorteile der C3-Serien-VMs nutzen, wenn Sie Cloud Volumes ONTAP 9.18.1 und höher in Google Cloud bereitstellen. Die C3-Serien-Maschinen bieten verbesserte Leistung und höhere Kapazitätsgrenzen durch die Verwendung von Google Virtual NIC (gVNIC) und Hyperdisk Balanced Disks, die dynamische Leistung für intensive Workloads gewährleisten.

Aktuell unterstützt Cloud Volumes ONTAP die C3-Serie nur in Einzelknoten-Bereitstellungen.

Wenn Ihr Cloud Volumes ONTAP-System Version 9.18.1 oder höher ausführt, verwenden die vorkonfigurierten Pakete, die Sie für einfache Einzelknotenbereitstellungen nutzen, automatisch C3-VMs, während Sie die IOPS- und Durchsatzparameter basierend auf Ihren Workload-Anforderungen anpassen können. Ebenso können Sie beim Erstellen von Aggregaten Hyperdisk Balanced-Festplatten hinzufügen, um in Google Cloud eine bessere Leistung und Skalierbarkeit zu erzielen. Zusätzlich können Sie die LSSD-Varianten der C3-Serie für die standardmäßige Flash Cache-Unterstützung auswählen.

Sie können den Datenträgertyp für C3-VMs beim Hinzufügen von Volumes zu Aggregaten nicht ändern, da C3 nur Hyperdisk Balanced-Datenträger unterstützt. Ebenso wird beim Replizieren eines Systems mit N2-VM-Typen auf eine C3-VM der Datenträgertyp standardmäßig auf Hyperdisk Balanced gesetzt.

"Unterstützte Konfigurationen für Cloud Volumes ONTAP in Google Cloud"

"Google documents: C3-Maschinenserie"

VNet-Sicherheit für Cloud Volumes ONTAP in Azure

Cloud Volumes ONTAP 9.18.1 und spätere Deployments in Azure Single- und Multi-Availability Zones unterstützen Azure Virtual Network (VNet)-Verschlüsselung als Teil ihrer mehrschichtigen Sicherheitsstrategie zum Schutz von Daten während der Übertragung. Cloud Volumes ONTAP nutzt Azures natives Datagram Transport Layer Security (DTLS)-Protokoll, um die Kommunikation zwischen ONTAP-Knoten, Managementschnittstellen und anderen Azure-Diensten zu sichern und so das Abfangen und den unbefugten Zugriff zu verhindern. Diese netzwerkbasierte Verschlüsselung ergänzt ONTAPs integrierte Speicher- und Data-at-Rest-Schutzmechanismen, um eine End-to-End-Sicherheit Ihrer Daten zu gewährleisten.

"Netzwerk für Azure VNet-Verschlüsselung"

12. Februar 2026

Unterstützung für Ebdsv5- und E104ids_v5-VMs in Azure

Ab Cloud Volumes ONTAP 9.18.1 können Sie Ebdsv5 und E104ids_v5 VMs für Einzelknoten- und Hochverfügbarkeitsbereitstellungen (HA) und Upgrades bereitstellen.

Ebdsv5 VMs innerhalb der Eb-Familie von Azure-VMs sind für eine höhere Remote-Speicherleistung optimiert. Sie können diese VMs für speicherintensive und E/A-lastige Unternehmens-Workloads wie relationale Datenbanken, In-Memory-Analysen und andere anspruchsvolle geschäftskritische Anwendungen verwenden.

E104ids_v5 ist eine isolierte VM-Instanz, die Ihnen hilft, geplante Wartungsfenster besser zu verwalten. Im Vergleich zu E80ids_v4 bietet sie einen deutlich höheren Festplattendurchsatz und IOPS sowie eine insgesamt bessere Netzwerkleistung.

"Unterstützte Konfigurationen für Cloud Volumes ONTAP in Azure"

"Azure documentation: Edsv5-Größenserie"

10. Februar 2026

Cloud Volumes ONTAP 9.18.1 GA

Sie können jetzt die NetApp Console verwenden, um die General Availability (GA) Version von Cloud Volumes ONTAP 9.18.1 in AWS, Azure und Google Cloud bereitzustellen und zu verwalten.

"Erfahren Sie mehr über diese Version von Cloud Volumes ONTAP" .

9. Februar 2026

Unterstützung für Google Cloud Infrastructure Manager

Cloud Volumes ONTAP 9.16.1 und höher unterstützen jetzt "Google Cloud Infrastructure Manager" (IM) anstelle von "Cloud Deployment Manager" (DM) für neue Bereitstellungen in Google Cloud. Google wird Deployment Manager als Infrastrukturdienst in naher Zukunft für den fortschrittlicheren Infrastructure Manager einstellen.

Ab dem 9. Februar 2026 verwendet Cloud Volumes ONTAP den Infrastructure Manager für neue und bestehende Bereitstellungen. Diese Tabelle erklärt einige Arbeitsabläufe für Sie:

Szenario	Aktion	Neue APIs für den Agent	Neue Berechtigungen für den Agent	Neue Google Cloud APIs für Cloud Volumes ONTAP	Dokumentressourcen
Vorhandener Agent und vorhandene Cloud Volumes ONTAP-Bereitstellung	Fügen Sie dem bestehenden Agenten neue APIs und Berechtigungen hinzu und konvertieren Sie das bestehende Cloud Volumes ONTAP System.	• Cloud Infrastructure Manager API • Cloud Quotas API	Alle für die Console-Version aufgeführten Berechtigungen: • "8. Dezember 2025" • "09. Februar 2026"	https://www.googleapis.com/upload/storage/v1 https://config.googleapis.com/v1	"Konfigurieren vorhandener Cloud Volumes ONTAP Deployments für Google Cloud Infrastructure Manager"

Szenario	Aktion	Neue APIs für den Agent	Neue Berechtigungen für den Agent	Neue Google Cloud APIs für Cloud Volumes ONTAP	Dokumentressourcen
Vorhandener Agent und neue Cloud Volumes ONTAP Bereitstellung	Fügen Sie dem bestehenden Agent neue APIs und Berechtigungen hinzu und stellen Sie ein neues Cloud Volumes ONTAP System bereit.	• Cloud Infrastructure Manager API • Cloud Quotas API	Alle für die Console-Version aufgeführten Berechtigungen: • "8. Dezember 2025" • "09. Februar 2026"	Alle Schritte für die neue Bereitstellung	"Erste Schritte mit Cloud Volumes ONTAP in Google Cloud"
Neuer Agent und neue Bereitstellung	Erstellen Sie einen neuen Agenten und stellen Sie ein neues Cloud Volumes ONTAP System bereit.				• "Erstellen Sie einen Console-Agenten aus Google Cloud" • "Erste Schritte mit Cloud Volumes ONTAP in Google Cloud"

Stellen Sie jetzt Cloud Volumes ONTAP bereit, damit es automatisch Infrastructure Manager verwendet, oder wechseln Sie Ihre bestehenden Bereitstellungen im Deployment Manager mithilfe eines Konvertierungstools zu Infrastructure Manager. Die Konvertierung ist ein einmaliger Vorgang, nach dem Ihre Systeme Infrastructure Manager verwenden. Siehe "Konfigurieren vorhandener Cloud Volumes ONTAP Deployments für Google Cloud Infrastructure Manager" für Anweisungen zur Ausführung des Konvertierungstools.

Cloud Volumes ONTAP-Systeme, die Infrastructure Manager verwenden, nutzen Google Cloud Storage-Buckets, um Daten und Datensätze in der Zone der ersten Bereitstellung zu speichern, um Bereitstellungsdatensätze zu speichern, die für nachfolgende Bereitstellungen wiederverwendet werden. Für diese Buckets können zusätzliche Kosten anfallen, aber bearbeiten oder löschen Sie die Buckets oder deren Inhalt nicht:

- `gs://netapp-cvo-infrastructure-manager-<project id>`: für ONTAP Versionen und SVM Terraform Templates, die für neue Cloud Volumes ONTAP Deployments verwendet werden. Innerhalb davon enthält der `dm-to-im-convert` bucket die Cloud Volumes ONTAP Terraform Dateien.
- `<gcp project number>-<region>-blueprint-config`: zum Speichern von Google Cloud Terraform-Artefakten.

Weiterführende Links

- "Erste Schritte mit Cloud Volumes ONTAP in Google Cloud"
- "NetApp Console Agent 4.2.0 Versionshinweise"
- "Erforderliche Berechtigungen für Google Cloud Infrastructure Manager"

12. Januar 2026

Bevorzugte Abrechnungsoption für Cloud Volumes ONTAP

Sie können nun eine bevorzugte Abrechnungsoption für die Berechnung Ihrer Cloud Volumes ONTAP Nutzung und etwaiger Mehrkosten auswählen. Da das Lizenzmodell Bring Your Own Licenses (BYOL) ab dem 25. Juni 2025 nur noch eingeschränkt verfügbar ist, hat NetApp im Abschnitt **Lizenzierung und Abonnements** der NetApp Console bevorzugte Abrechnungsmethoden hinzugefügt. Sie können entweder Ihr jährliches Marktplatz-Abonnement für die Abrechnung und die Beitreibung von Mehrkosten oder das bestehende BYOL-Modell als bevorzugte Option nutzen. Dies gibt Ihnen die Flexibilität, die Abrechnungsmethode zu wählen, die am besten zur Finanzstrategie und den Nutzungsmustern Ihres Unternehmens passt.

"Abrechnungseinstellungen und Überschreitungen"Die

10. Dezember 2025

Möglichkeit zur Leistungssteigerung von Premium SSD v2-Festplatten in Azure

Sie können die Leistung von Premium SSD v2 Managed Disks in Azure jetzt verbessern, indem Sie die IOPS- und Durchsatzparameter ändern. Mithilfe dieser Funktion können Sie die Speicherleistung Ihrer Systeme auf Basis Ihrer Arbeitslastanforderungen optimieren.

"Verwalten der Premium-SSD-v2-Festplattenleistung für Cloud Volumes ONTAP in Azure".

Vereinfachte Gebührenberechnung für Essentials-Lizenzen bei Überschreitung des Lizenzumfangs

Bei den jährlichen Verträgen/privaten Angeboten des Cloud Volumes ONTAP Marktplatzes sind die Berechnungen für die Überschreitung von Essentials-Lizenzen nun an die Bring Your Own License (BYOL)-Pakete angeglichen. Bisher wurden Mehrverbrauchsmengen zu den stundenweisen Marktpreisen für das jeweilige Essentials-Paket abgerechnet. Wenn Ihr jährlicher Marketplace-Vertrag mehrere Essentials-Pakete umfasst, berechnet die NetApp Console die Mehrkosten für ein Essentials-Paket auf Basis der verfügbaren Kapazität eines höherpreisigen Essentials-Pakets in Ihrem Abonnement. Dies vereinfacht die Berechnung von Mehrkosten für Essentials-Pakete und gewährleistet einen reibungslosen Übergang von der BYOL-Lizenzierung zu einem abonnementbasierten Modell.

"Wie Überschreitungen bei Essentials-Lizenzen abgerechnet werden"

Unterstützung für Azure Edsv6-Größenserien

Ab Cloud Volumes ONTAP 9.17.1 können Sie VMs der Azure Edsv6-Serie über die NetApp Console für neue Cloud Volumes ONTAP Instanzen bereitstellen. Cloud Volumes ONTAP 9.17.1 und spätere Versionen unterstützen bei neuen Bereitstellungen nur noch VMs der Generation 2. Diese Geräte der zweiten Generation sind mit den neuesten Technologien kompatibel, wie z. B. Unified Extensible Firmware Interface (UEFI), Azure Boost-Systemen und NVMe. Sie eignen sich ideal für speicherintensive Systeme und Anwendungen, die einen schnellen, lokalen Speicher benötigen, wie z. B. Datenbankserver und Analyse-Engines.

"Unterstützte Konfigurationen für Cloud Volumes ONTAP in Azure"

10. November 2025

Erweiterte NVMe-TCP-Unterstützung

Früher mussten bei der Bereitstellung von Cloud Volumes ONTAP Instanzen über NVMe-TCP die NVMe-Lizenzen vor der Bereitstellung manuell beschafft und angewendet werden. Mit diesem Update installiert Cloud Volumes ONTAP nun automatisch die erforderlichen NVMe-Lizenzen während der Bereitstellung, was den Einrichtungsprozess vereinfacht.

Bei bestehenden NVMe-TCP-Bereitstellungen ohne Lizenzen wendet Cloud Volumes ONTAP die Lizenzen automatisch an. Sie müssen das System neu starten, damit die Lizenzen wirksam werden.

Weitere Informationen finden Sie unter "Unterstützte Clientprotokolle für Cloud Volumes ONTAP: NVMe-TCP" Die

17. Oktober 2025

Cloud Volumes ONTAP in Azure jetzt auf die neuesten unterstützten Versionen beschränkt

Bereitstellungen und Upgrades von Cloud Volumes ONTAP in Azure über die NetApp Console sind jetzt auf die neuesten unterstützten Versionen beschränkt. Dies gewährleistet die Kompatibilität mit der neuesten von Microsoft unterstützten Hardwaregeneration und bietet die neuesten Funktionen und Sicherheitsverbesserungen. Die Konsole fordert Sie auf, auf die unterstützten Versionen zu aktualisieren.

Weitere Einzelheiten finden Sie unter:

- Einsatz: "Unterstützte ONTAP -Versionen für Cloud Volumes ONTAP Bereitstellungen"
- Aktualisierung: "Unterstützte Upgradepfade für Azure"

06. Oktober 2025

BlueXP heißt jetzt NetApp Console

Die NetApp Console basiert auf der verbesserten und neu strukturierten BlueXP -Grundlage und ermöglicht die zentrale Verwaltung von NetApp -Speicher und NetApp Data Services in On-Premises- und Cloud-Umgebungen auf Unternehmensniveau. Sie liefert Einblicke in Echtzeit, schnellere Arbeitsabläufe und eine vereinfachte Verwaltung mit hoher Sicherheit und Konformität.

Einzelheiten zu den Änderungen finden Sie im "Versionshinweise zur NetApp Console" .

Vereinfachte Cloud Volumes ONTAP Bereitstellung in AWS

Sie können Cloud Volumes ONTAP jetzt in AWS mithilfe einer schnellen Bereitstellungsmethode sowohl für Einzelknoten- als auch für Hochverfügbarkeitskonfigurationen (HA) bereitstellen. Dieser optimierte Prozess reduziert die Anzahl der Schritte im Vergleich zur erweiterten Methode, legt automatisch Standardwerte auf einer einzigen Seite fest und minimiert die Navigation, wodurch die Bereitstellung schneller und einfacher wird.

Weitere Informationen finden Sie unter "Stellen Sie Cloud Volumes ONTAP in AWS mithilfe der Schnellbereitstellung bereit" .

04. September 2025

Cloud Volumes ONTAP 9.17.1 RC

Sie können jetzt BlueXP verwenden, um den Release Candidate 1 von Cloud Volumes ONTAP 9.17.1 in Azure und Google Cloud bereitzustellen und zu verwalten. Diese Version ist jedoch nicht für die Bereitstellung und Aktualisierung in AWS verfügbar.

"Erfahren Sie mehr über diese Version von Cloud Volumes ONTAP".

11. August 2025

Ende der Verfügbarkeit optimierter Lizenzen

Ab dem 11. August 2025 wird die Lizenz „Cloud Volumes ONTAP Optimized“ veralten und kann in den Azure- und Google Cloud-Marktplätzen für Pay-as-you-go-Abonnements (PAYGO) nicht mehr erworben oder verlängert werden. Wenn Sie einen bestehenden Jahresvertrag mit einer optimierten Lizenz haben, können Sie die Lizenz bis zum Ende Ihres Vertrags weiter verwenden. Wenn Ihre optimierte Lizenz abläuft, können Sie sich für Cloud Volumes ONTAP Essentials- oder Professional-Lizenzen in BlueXP entscheiden.

Die Möglichkeit, optimierte Lizenzen hinzuzufügen oder zu erneuern, besteht jedoch über die APIs.

Informationen zu Lizenzpaketen finden Sie unter "Lizenzierung für Cloud Volumes ONTAP" .

Informationen zum Umschalten auf eine andere Lademethode finden Sie unter "Verwalten der kapazitätsbasierten Lizenzierung" .

14. Juli 2025

Unterstützung für transparenten Proxy

BlueXP unterstützt jetzt zusätzlich zu den vorhandenen expliziten Proxy-Verbindungen transparente Proxy-Server. Beim Erstellen oder Ändern des BlueXP Connector können Sie einen transparenten Proxyserver konfigurieren, um den Netzwerkverkehr zu und von Cloud Volumes ONTAP sicher zu verwalten.

Weitere Informationen zur Verwendung von Proxyservern in Cloud Volumes ONTAP finden Sie unter:

- "Netzwerkkonfigurationen zur Unterstützung des Connector-Proxys in AWS"
- "Netzwerkkonfigurationen zur Unterstützung des Connector-Proxys in Azure"
- "Netzwerkkonfigurationen zur Unterstützung des Connector-Proxys in Google Cloud"

Neuer VM-Typ wird für Cloud Volumes ONTAP in Azure unterstützt

Ab Cloud Volumes ONTAP 9.13.1 wird L8s_v3 als VM-Typ in Azure-Einzel- und Mehrfachverfügbarkeitszonen sowohl für neue als auch für bestehende Hochverfügbarkeitspaarbereitstellungen (HA) unterstützt.

Weitere Informationen finden Sie unter "Unterstützte Konfigurationen in Azure" .

25. Juni 2025

Eingeschränkte Verfügbarkeit der BYOL-Lizenzierung für Cloud Volumes ONTAP

Ab dem 25. Juni 2025 hat NetApp das BYOL-Lizenzmodell (Bring Your Own License) für Cloud Volumes ONTAP eingeschränkt. Die Einschränkung gilt für alle Kunden und Cloud Volumes ONTAP Bereitstellungen in AWS, Azure und Google Cloud. Ausgenommen sind lediglich Kunden des US-amerikanischen öffentlichen Sektors und Bereitstellungen in der Region China.

NetApp Support und Services laufen bis zum Ablauf Ihres BYOL-Vertrags weiter, Ihre abgelaufenen Lizenzen werden jedoch nicht erneuert oder verlängert. Nach Ablauf Ihrer BYOL-Lizenzen müssen Sie diese durch kapazitätsbasierte Lizenzen ersetzen, die Sie über Ihre Cloud-Marktplatz-Abonnements erworben haben. Ein kapazitätsbasiertes Lizenzmodell über Hyperscaler-Marktplätze vereinfacht die Lizenzierung und bietet größere Geschäftsvorteile. Kontaktieren Sie Ihr NetApp Accounts Team oder Ihre Kundenbetreuer, um Ihre Umstellungsmöglichkeiten zu besprechen.

Weitere Informationen finden Sie in dieser Kundenmitteilung: "CPC-00661: Änderungen an der BYOL-Richtlinie für Cloud Volumes ONTAP" .

29. Mai 2025

Bereitstellungen im privaten Modus für Cloud Volumes ONTAP 9.15.1 aktiviert

Sie können Cloud Volumes ONTAP 9.15.1 jetzt im privaten Modus in AWS, Azure und Google Cloud bereitstellen. Der private Modus ist sowohl für Einzelknoten- als auch für Hochverfügbarkeitsbereitstellungen (HA) von Cloud Volumes ONTAP 9.15.1 aktiviert.

Weitere Informationen zu Bereitstellungen im privaten Modus finden Sie unterhttps://docs.netapp.com/us-en/bluexp-setup-admin/concept-modes.html#restricted-mode["Erfahren Sie mehr über die Bereitstellungsmodi von BlueXP"^] .

12. Mai 2025

Erkennung von Bereitstellungen, die über den Azure-Marktplatz in BlueXP vorgenommen wurden

BlueXP verfügt jetzt über die Möglichkeit, die direkt über den Azure-Marktplatz bereitgestellten Cloud Volumes ONTAP -Systeme zu erkennen. Dies bedeutet, dass Sie diese Systeme jetzt wie jedes andere Cloud Volumes ONTAP System als Arbeitsumgebungen in BlueXP hinzufügen und verwalten können.

"Stellen Sie Cloud Volumes ONTAP vom Azure Marketplace bereit"

16. April 2025

Neue Regionen, die in Azure unterstützt werden

Sie können Cloud Volumes ONTAP 9.12.1 GA und höher jetzt in einzelnen und mehreren Verfügbarkeitszonen in Azure in den folgenden Regionen bereitstellen. Dies umfasst die Unterstützung sowohl für Einzelknoten- als

auch für Hochverfügbarkeitsbereitstellungen (HA).

- Spanien, Zentral
- Mexiko-Zentral

Eine Liste aller Regionen finden Sie im "Globale Regionenkarte unter Azure" .

14. April 2025

Automatisierte Erstellung von Storage-VMs durch die APIs in Google Cloud

Sie können jetzt die BlueXP -APIs verwenden, um die Erstellung von Speicher-VMs in Google Cloud zu automatisieren. Sie haben diese Funktion in Cloud Volumes ONTAP Hochverfügbarkeitskonfigurationen (HA) verwendet und können sie jetzt auch in Einzelknotenbereitstellungen verwenden. Mithilfe der BlueXP -APIs können Sie in Ihrer Google Cloud-Umgebung problemlos zusätzliche datenbereitstellende Speicher-VMs erstellen, umbenennen und löschen, ohne die erforderlichen Netzwerkschnittstellen, LIFs und Verwaltungs-LIFs manuell konfigurieren zu müssen. Diese Automatisierung vereinfacht den Prozess der Verwaltung von Speicher-VMs.

"Verwalten Sie datenbereitstellende Speicher-VMs für Cloud Volumes ONTAP in Google Cloud"

03. April 2025

Unterstützung für China-Regionen für Cloud Volumes ONTAP 9.13.1 in AWS

Sie können Cloud Volumes ONTAP 9.13.1 jetzt in AWS-Regionen in China bereitstellen. Dies umfasst die Unterstützung sowohl für Einzelknoten- als auch für Hochverfügbarkeitsbereitstellungen (HA). Es werden nur direkt von NetApp erworbene Lizenzen unterstützt.

Informationen zur regionalen Verfügbarkeit finden Sie im "Globale Regionenkarten für Cloud Volumes ONTAP" .

28. März 2025

Bereitstellungen im privaten Modus für Cloud Volumes ONTAP 9.14.1 aktiviert

Sie können Cloud Volumes ONTAP 9.14.1 jetzt im privaten Modus in AWS, Azure und Google Cloud bereitstellen. Der private Modus ist sowohl für Einzelknoten- als auch für Hochverfügbarkeitsbereitstellungen (HA) von Cloud Volumes ONTAP 9.14.1 aktiviert.

Weitere Informationen zu Bereitstellungen im privaten Modus finden Sie unterhttps://docs.netapp.com/us-en/bluexp-setup-admin/concept-modes.html#restricted-mode["Erfahren Sie mehr über die Bereitstellungsmodi von BlueXP"^] .

12. März 2025

Neue Regionen werden für die Bereitstellung mehrerer Verfügbarkeitszonen in Azure unterstützt.

Die folgenden Regionen unterstützen jetzt HA-Bereitstellungen in mehreren Verfügbarkeitszonen in Azure für Cloud Volumes ONTAP 9.12.1 GA und höher:

- Zentrale USA

- US Gov Virginia (US-Regierungsregion – Virginia)

Eine Liste aller Regionen finden Sie im "Globale Regionenkarte unter Azure" .

10. März 2025

Automatisierte Erstellung von Storage-VMs über die APIs in Azure

Sie können jetzt die BlueXP -APIs verwenden, um zusätzliche datenbereitstellende Speicher-VMs für Cloud Volumes ONTAP in Azure zu erstellen, umzubenennen und zu löschen. Durch die Verwendung der APIs wird der Prozess der Speicher-VM-Erstellung automatisiert, einschließlich der Konfiguration der erforderlichen Netzwerkschnittstellen, LIFs und eines Verwaltungs-LIF, wenn Sie eine Speicher-VM für Verwaltungszwecke verwenden müssen.

"Verwalten von datenbereitstellenden Speicher-VMs für Cloud Volumes ONTAP in Azure"

06. März 2025

Cloud Volumes ONTAP 9.16.1 GA

Sie können jetzt BlueXP verwenden, um die allgemein verfügbare Version von Cloud Volumes ONTAP 9.16.1 in Azure und Google Cloud bereitzustellen und zu verwalten. Diese Version ist jedoch nicht für die Bereitstellung und Aktualisierung in AWS verfügbar.

"Erfahren Sie mehr über die neuen Funktionen dieser Version von Cloud Volumes ONTAP" .

03. März 2025

Unterstützung für die Region „Neuseeland Nord“ in Azure

Die Region „Neuseeland Nord“ wird jetzt in Azure für Einzelknoten- und Hochverfügbarkeitskonfigurationen (HA) von Cloud Volumes ONTAP 9.12.1 GA und höher unterstützt. Beachten Sie, dass der Instanztyp Lsv3 in dieser Region nicht unterstützt wird.

Eine Liste aller unterstützten Regionen finden Sie im "Globale Regionenkarte unter Azure" .

18. Februar 2025

Einführung der direkten Bereitstellung im Azure Marketplace

Sie können jetzt die Vorteile der direkten Bereitstellung im Azure Marketplace nutzen, um Cloud Volumes ONTAP einfach und schnell direkt vom Azure Marketplace aus bereitzustellen. Mit dieser optimierten Methode können Sie die Kernfunktionen und -fähigkeiten von Cloud Volumes ONTAP in Ihrer Umgebung erkunden, ohne den BlueXP Connector einrichten oder andere Onboarding-Kriterien erfüllen zu müssen, die für die Bereitstellung von Cloud Volumes ONTAP über BlueXP erforderlich sind.

- "Informieren Sie sich über die Bereitstellungsoptionen von Cloud Volumes ONTAP in Azure"
- "Stellen Sie Cloud Volumes ONTAP vom Azure Marketplace bereit"

10. Februar 2025

Benutzerauthentifizierung für den Zugriff auf System Manager von BlueXP aktiviert

Als BlueXP -Administrator können Sie jetzt die Authentifizierung für ONTAP -Benutzer aktivieren, die von BlueXP aus auf ONTAP System Manager zugreifen. Sie können diese Option aktivieren, indem Sie die BlueXP Connector-Einstellungen bearbeiten. Diese Option ist für den Standard- und den privaten Modus verfügbar.

"Verwalten Sie Cloud Volumes ONTAP mit System Manager" .

BlueXP Advanced View wurde in System Manager umbenannt

Die Option zur erweiterten Verwaltung von Cloud Volumes ONTAP von BlueXP über ONTAP System Manager wurde von **Advanced View** in **System Manager** umbenannt.

"Verwalten Sie Cloud Volumes ONTAP mit System Manager" .

Einführung einer einfacheren Möglichkeit zur Lizenzverwaltung mit der BlueXP digital wallet

Jetzt können Sie die Verwaltung von Cloud Volumes ONTAP Lizenzen mithilfe verbesserter Navigationspunkte in der BlueXP digital wallet vereinfachen:

- Greifen Sie einfach über die Registerkarten **Verwaltung > Licenses and subscriptions > Übersicht/Direktlizenzen** auf Ihre Cloud Volumes ONTAP -Lizenzinformationen zu.
- Klicken Sie im Cloud Volume ONTAP Bereich auf der Registerkarte **Übersicht** auf **Anzeigen**, um einen umfassenden Überblick über Ihre kapazitätsbasierten Lizenzen zu erhalten. Diese erweiterte Ansicht bietet detaillierte Einblicke in Ihre Lizenzen und Abonnements.
- Wenn Sie die vorherige Benutzeroberfläche bevorzugen, können Sie auf die Schaltfläche **Zur alten Ansicht wechseln** klicken, um die Lizenzdetails nach Typ anzuzeigen und die Abrechnungsmethoden für Ihre Lizenzen zu ändern.

"Kapazitätsbasierte Lizenzen verwalten" .

09. Dezember 2024

Liste der unterstützten VMs für Azure aktualisiert, um sie an die Best Practices anzupassen

Die Maschinenfamilien DS_v2 und Es_v3 stehen bei der Bereitstellung neuer Instanzen von Cloud Volumes ONTAP in Azure auf BlueXP nicht mehr zur Auswahl. Diese Familien werden nur in älteren, bestehenden Systemen beibehalten und unterstützt. Neue Bereitstellungen von Cloud Volumes ONTAP werden in Azure erst ab der Version 9.12.1 unterstützt. Wir empfehlen Ihnen, entweder auf Es_v4 oder eine andere Serie umzusteigen, die mit Cloud Volumes ONTAP 9.12.1 und höher kompatibel ist. Die Maschinen der Serien DS_v2 und Es_v3 stehen jedoch für neue Bereitstellungen über die API zur Verfügung.

"Unterstützte Konfigurationen in Azure"

11. November 2024

Ende der Verfügbarkeit knotenbasierter Lizenzen

NetApp hat das Ende der Verfügbarkeit (EOA) und des Supports (EOS) der knotenbasierten Lizenzierung von Cloud Volumes ONTAP geplant. Ab dem 11. November 2024 wurde die begrenzte Verfügbarkeit von knotenbasierten Lizenzen beendet. Der Support für die knotenbasierte Lizenzierung endet am 31. Dezember 2024. Nach dem EOA Ihrer knotenbasierten Lizenzen sollten Sie mithilfe des BlueXP Lizenzkonvertierungstools auf eine kapazitätsbasierte Lizenzierung umsteigen.

Bei jährlichen oder längerfristigen Verpflichtungen empfiehlt NetApp , dass Sie sich vor dem EOA-Datum oder dem Ablaufdatum der Lizenz an Ihren NetApp -Vertreter wenden, um sicherzustellen, dass die Voraussetzungen für den Übergang erfüllt sind. Wenn Sie keinen langfristigen Vertrag für einen Cloud Volumes ONTAP Knoten haben und Ihr System mit einem On-Demand-Pay-as-you-go-Abonnement (PAYGO) betreiben, ist es wichtig, Ihre Konvertierung vor dem EOS-Datum zu planen. Sowohl bei Langzeitverträgen als auch bei PAYGO-Abonnements können Sie das Lizenzkonvertierungstool BlueXP für eine nahtlose Konvertierung verwenden.

"Ende der Verfügbarkeit von knotenbasierten Lizenzen" "Konvertieren Sie eine knotenbasierte Cloud Volumes ONTAP -Lizenz in eine kapazitätsbasierte Lizenz"

Entfernung knotenbasierter Bereitstellungen aus BlueXP

Die Option, Cloud Volumes ONTAP Systeme mithilfe knotenbasierter Lizenzen bereitzustellen, ist bei BlueXP veraltet. Mit Ausnahme einiger Sonderfälle können Sie für Cloud Volumes ONTAP Bereitstellungen bei keinem Cloud-Anbieter knotenbasierte Lizenzen verwenden.

NetApp erkennt die folgenden besonderen Lizenzierungsanforderungen in Übereinstimmung mit vertraglichen Verpflichtungen und betrieblichen Anforderungen an und wird in diesen Situationen weiterhin knotenbasierte Lizenzen unterstützen:

- Kunden aus dem öffentlichen Sektor der USA
- Bereitstellungen im privaten Modus
- Bereitstellungen von Cloud Volumes ONTAP in AWS in der Region China
- Wenn Sie über eine gültige, nicht abgelaufene By-Node-Lizenz verfügen, bringen Sie Ihre eigene Lizenz mit (BYOL-Lizenz)

"Ende der Verfügbarkeit von knotenbasierten Lizenzen"

Hinzufügen einer Cold Tier für Cloud Volumes ONTAP -Daten auf Azure Blob Storage

Mit BlueXP können Sie jetzt eine kalte Ebene auswählen, um die inaktiven Kapazitätsebenendaten im Azure Blob-Speicher zu speichern. Durch Hinzufügen der kalten Ebene zu den vorhandenen warmen und kalten Ebenen erhalten Sie eine günstigere Speicheroption und eine verbesserte Kosteneffizienz.

"Datentiering in Azure"

Option zum Einschränken des öffentlichen Zugriffs auf das Speicherkonto für Azure

Sie haben jetzt die Möglichkeit, den öffentlichen Zugriff auf Ihr Speicherkonto für Cloud Volumes ONTAP -Systeme in Azure einzuschränken. Durch die Deaktivierung des Zugriffs können Sie Ihre private IP-Adresse vor Offenlegung schützen, selbst innerhalb desselben VNet, falls die Sicherheitsrichtlinien Ihres Unternehmens eingehalten werden müssen. Diese Option deaktiviert auch die Datenschichtung für Ihre Cloud Volumes ONTAP Systeme und ist sowohl auf einzelne Knoten als auch auf Hochverfügbarkeitspaare anwendbar.

"Sicherheitsgruppenregeln" .

WORM-Aktivierung nach der Bereitstellung von Cloud Volumes ONTAP

Sie haben jetzt die Möglichkeit, mithilfe von BlueXP den WORM-Speicher (Write Once, Read Many) auf einem vorhandenen Cloud Volumes ONTAP System zu aktivieren. Diese Funktion bietet Ihnen die Flexibilität, WORM in einer Arbeitsumgebung zu aktivieren, auch wenn WORM bei der Erstellung nicht aktiviert war. Nach der Aktivierung können Sie WORM nicht mehr deaktivieren.

"Aktivieren von WORM in einer Cloud Volumes ONTAP Arbeitsumgebung"

25. Oktober 2024

Liste der unterstützten VMs für Google Cloud aktualisiert, um sie an die Best Practices anzupassen

Die Maschinen der n1-Serie stehen bei der Bereitstellung neuer Instanzen von Cloud Volumes ONTAP in Google Cloud auf BlueXP nicht mehr zur Auswahl. Die Maschinen der n1-Serie werden beibehalten und nur in älteren, bestehenden Systemen unterstützt. Neue Bereitstellungen von Cloud Volumes ONTAP werden in Google Cloud erst ab Version 9.8 unterstützt. Wir empfehlen Ihnen, auf die Maschinentypen der n2-Serie umzusteigen, die mit Cloud Volumes ONTAP 9.8 und höher kompatibel sind. Die Maschinen der n1-Serie werden jedoch für neue Bereitstellungen über die API verfügbar sein.

"Unterstützte Konfigurationen in Google Cloud" .

Unterstützung lokaler Zonen für Amazon Web Services im privaten Modus

BlueXP unterstützt jetzt AWS Local Zones für Cloud Volumes ONTAP Bereitstellungen mit hoher Verfügbarkeit (HA) im privaten Modus. Die Unterstützung, die zuvor nur auf den Standardmodus beschränkt war, wurde jetzt auf den privaten Modus erweitert.

> AWS Local Zones werden nicht unterstützt, wenn BlueXP im eingeschränkten Modus verwendet wird.

Weitere Informationen zu AWS Local Zones mit HA-Bereitstellungen finden Sie unter"Lokale AWS-Zonen" .

07. Oktober 2024

Verbesserte Benutzererfahrung bei der Versionsauswahl für das Upgrade

Wenn Sie ab dieser Version versuchen, Cloud Volumes ONTAP mithilfe der BlueXP -Benachrichtigung zu aktualisieren, erhalten Sie Hinweise zu den zu verwendenden Standard-, neuesten und kompatiblen Versionen. Außerdem können Sie jetzt den neuesten Patch oder die neueste Hauptversion auswählen, die mit Ihrer Cloud Volumes ONTAP -Instanz kompatibel ist, oder manuell eine Version für das Upgrade eingeben.

"Aktualisieren Sie die Cloud Volumes ONTAP -Software"

09. September 2024

WORM- und ARP-Funktionalitäten sind nicht mehr kostenpflichtig

Die integrierten Datenschutz- und Sicherheitsfunktionen WORM (Write Once Read Many) und ARP (Autonomous Ransomware Protection) werden mit Cloud Volumes ONTAP Lizenzen ohne zusätzliche Kosten angeboten. Das neue Preismodell gilt sowohl für neue als auch für bestehende BYOL- und PAYGO/Marketplace-Abonnements von AWS, Azure und Google Cloud. Sowohl kapazitätsbasierte als auch knotenbasierte Lizenzen enthalten ARP und WORM für alle Konfigurationen, einschließlich Einzelknoten und Hochverfügbarkeitspaaren (HA), ohne zusätzliche Kosten.

Die vereinfachte Preisgestaltung bringt Ihnen folgende Vorteile:

- Für Konten, die derzeit WORM und ARP umfassen, fallen für diese Funktionen keine Gebühren mehr an. In Zukunft werden Ihnen auf Ihrer Rechnung nur noch Gebühren für die Kapazitätsnutzung berechnet, wie es vor dieser Änderung der Fall war. WORM und ARP werden in Ihren zukünftigen Rechnungen nicht mehr

enthalten sein.

- Wenn Ihre aktuellen Konten diese Funktionen nicht enthalten, können Sie sich jetzt ohne zusätzliche Kosten für WORM und ARP entscheiden.
- Bei allen Cloud Volumes ONTAP Angeboten für neue Konten fallen keine Gebühren für WORM und ARP an.

Erfahren Sie mehr über diese Funktionen:

- "Aktivieren Sie NetApp Ransomware-Schutzlösungen für Cloud Volumes ONTAP"
- "WORM-Speicher"

23. August 2024

Region Kanada West wird jetzt in AWS unterstützt

Die Region Kanada West wird jetzt in AWS für Cloud Volumes ONTAP 9.12.1 GA und höher unterstützt.

Eine Liste aller Regionen finden Sie im "Globale Regionenkarte unter AWS" .

22. August 2024

Cloud Volumes ONTAP 9.15.1 GA

BlueXP kann jetzt die allgemein verfügbare Version von Cloud Volumes ONTAP 9.15.1 in AWS, Azure und Google Cloud bereitstellen und verwalten.

"Erfahren Sie mehr über die neuen Funktionen dieser Version von Cloud Volumes ONTAP" .

08. August 2024

Edge Cache-Lizenzpakete veraltet

Für zukünftige Bereitstellungen von Cloud Volumes ONTAP werden keine kapazitätsbasierten Lizenzpakete für Edge Cache mehr verfügbar sein. Sie können diese Funktionalität jedoch über die API nutzen.

Mindestversionsunterstützung für Flash Cache in Azure

Die für die Konfiguration von Flash Cache in Azure erforderliche Mindestversion von Cloud Volumes ONTAP ist 9.13.1 GA. Sie können für die Bereitstellung von Flash Cache auf Cloud Volumes ONTAP -Systemen in Azure nur ONTAP 9.13.1 GA und spätere Versionen verwenden.

Informationen zu unterstützten Konfigurationen finden Sie unter "Unterstützte Konfigurationen in Azure" .

Kostenlose Testversionen für Marktplatzabonnements veraltet

Die 30-tägige automatische kostenlose Test- oder Evaluierungslizenz für Pay-as-you-go-Abonnements im Marktplatz des Cloud-Anbieters ist in Cloud Volumes ONTAP nicht mehr verfügbar. Die Abrechnung für alle Arten von Marktplatz-Abonnements (PAYGO oder Jahresvertrag) wird ab der ersten Nutzung aktiviert, ohne kostenlose Testphase.

10. Juni 2024

Cloud Volumes ONTAP 9.15.0

BlueXP kann jetzt Cloud Volumes ONTAP 9.15.0 in AWS, Azure und Google Cloud bereitstellen und verwalten.

"Erfahren Sie mehr über die neuen Funktionen dieser Version von Cloud Volumes ONTAP" .

17. Mai 2024

Unterstützung für lokale Zonen von Amazon Web Services

Für Cloud Volumes ONTAP HA-Bereitstellungen ist jetzt Unterstützung für AWS Local Zones verfügbar. Bei AWS Local Zones handelt es sich um eine Infrastrukturbereitstellung, bei der Speicher, Rechenleistung, Datenbanken und andere ausgewählte AWS-Dienste in der Nähe von Großstädten und Industriegebieten angesiedelt sind.

AWS Local Zones werden unterstützt, wenn BlueXP im Standardmodus verwendet wird. Derzeit werden AWS Local Zones nicht unterstützt, wenn BlueXP im eingeschränkten oder privaten Modus verwendet wird.

Weitere Informationen zu AWS Local Zones mit HA-Bereitstellungen finden Sie unter "Lokale AWS-Zonen" .

23. April 2024

Neue Regionen werden für die Bereitstellung mehrerer Verfügbarkeitszonen in Azure unterstützt.

Die folgenden Regionen unterstützen jetzt HA-Bereitstellungen in mehreren Verfügbarkeitszonen in Azure für Cloud Volumes ONTAP 9.12.1 GA und höher:

- Deutschland West Mitte
- Polen, Mitte
- Westen USA 3
- Israel Central
- Italien Nord
- Kanada, Zentral

Eine Liste aller Regionen finden Sie im "Globale Regionenkarte unter Azure" .

Die Region Johannesburg wird jetzt in Google Cloud unterstützt

Die Region Johannesburg(`africa-south1` Region) wird jetzt in Google Cloud für Cloud Volumes ONTAP 9.12.1 GA und höher unterstützt.

Eine Liste aller Regionen finden Sie im "Globale Regionenkarte unter Google Cloud" .

Volume-Vorlagen und Tags werden nicht mehr unterstützt

Sie können kein Volume mehr aus einer Vorlage erstellen oder die Tags eines Volumes bearbeiten. Diese Aktionen standen im Zusammenhang mit dem BlueXP -Reparaturdienst, der nicht mehr verfügbar ist.

08. März 2024

Unterstützung für Amazon Instant Metadata Service v2

In AWS unterstützen Cloud Volumes ONTAP, der Mediator und der Connector jetzt Amazon Instant Metadata Service v2 (IMDSv2) für alle Funktionen. IMDSv2 bietet verbesserten Schutz vor Schwachstellen. Bisher wurde nur IMDSv1 unterstützt.

Falls Ihre Sicherheitsrichtlinien dies erfordern, können Sie Ihre EC2-Instanzen für die Verwendung von IMDSv2 konfigurieren. Anweisungen hierzu finden Sie unter "BlueXP -Setup- und Administrationsdokumentation zur Verwaltung vorhandener Connectors" .

05. März 2024

Cloud Volumes ONTAP 9.14.1 GA

BlueXP kann jetzt die allgemein verfügbare Version von Cloud Volumes ONTAP 9.14.1 in AWS, Azure und Google Cloud bereitstellen und verwalten.

"Erfahren Sie mehr über die neuen Funktionen dieser Version von Cloud Volumes ONTAP" .

02. Februar 2024

Unterstützung für VMs der Edv5-Serie in Azure

Cloud Volumes ONTAP unterstützt ab der Version 9.14.1 jetzt die folgenden VMs der Edv5-Serie.

- E4ds_v5
- E8ds_v5
- E20s_v5
- E32ds_v5
- E48ds_v5
- E64ds_v5

"Unterstützte Konfigurationen in Azure"

16. Januar 2024

Patch-Releases in BlueXP

Patch-Releases sind in BlueXP nur für die letzten drei Versionen von Cloud Volumes ONTAP verfügbar.

"Upgrade von Cloud Volumes ONTAP"

08. Januar 2024

Neue VMs für mehrere Azure-Verfügbarkeitszonen

Ab Cloud Volumes ONTAP 9.13.1 unterstützen die folgenden VM-Typen mehrere Azure-Verfügbarkeitszonen für neue und vorhandene Bereitstellungen von Hochverfügbarkeitspaaren:

- L16s_v3
- L32s_v3
- L48s_v3
- L64s_v3

"Unterstützte Konfigurationen in Azure"

06. Dezember 2023

Cloud Volumes ONTAP 9.14.1 RC1

BlueXP kann jetzt Cloud Volumes ONTAP 9.14.1 in AWS, Azure und Google Cloud bereitstellen und verwalten.

"Erfahren Sie mehr über die neuen Funktionen dieser Version von Cloud Volumes ONTAP" .

Maximales Limit für FlexVol volume von 300 TiB

Sie können jetzt mit System Manager und der ONTAP CLI ab Cloud Volumes ONTAP 9.12.1 P2 und 9.13.0 P2 und in BlueXP ab Cloud Volumes ONTAP 9.13.1 ein FlexVol volume mit einer maximalen Größe von 300 TiB erstellen.

- "Speicherlimits in AWS"
- "Speicherlimits in Azure"
- "Speicherlimits in Google Cloud"

05. Dezember 2023

Die folgenden Änderungen wurden eingeführt.

Neue Regionsunterstützung in Azure

Unterstützung einer einzelnen Verfügbarkeitszonenregion

Die folgenden Regionen unterstützen jetzt hochverfügbare Bereitstellungen in einzelnen Verfügbarkeitszonen in Azure für Cloud Volumes ONTAP 9.12.1 GA und höher:

- Tel Aviv
- Mailand

Unterstützung mehrerer Verfügbarkeitszonenregionen

Die folgenden Regionen unterstützen jetzt hochverfügbare Bereitstellungen in mehreren Verfügbarkeitszonen in Azure für Cloud Volumes ONTAP 9.12.1 GA und höher:

- Zentralindien
- Norwegen Ost
- Schweiz Nord
- Südafrika Nord
- Vereinigte Arabische Emirate Nord

Eine Liste aller Regionen finden Sie im "Globale Regionenkarte unter Azure" .

10. November 2023

Die folgende Änderung wurde mit der Version 3.9.35 des Connectors eingeführt.

Die Region Berlin wird jetzt in der Google Cloud unterstützt

Die Region Berlin wird jetzt in Google Cloud für Cloud Volumes ONTAP 9.12.1 GA und höher unterstützt.

Eine Liste aller Regionen finden Sie im "Globale Regionenkarte unter Google Cloud" .

08. November 2023

Die folgende Änderung wurde mit der Version 3.9.35 des Connectors eingeführt.

Die Region Tel Aviv wird jetzt in AWS unterstützt

Die Region Tel Aviv wird jetzt in AWS für Cloud Volumes ONTAP 9.12.1 GA und höher unterstützt.

Eine Liste aller Regionen finden Sie im "Globale Regionenkarte unter AWS" .

01. November 2023

Die folgende Änderung wurde mit der Version 3.9.34 des Connectors eingeführt.

Die Region Saudi-Arabien wird jetzt in Google Cloud unterstützt

Die Region Saudi-Arabien wird jetzt in Google Cloud für Cloud Volumes ONTAP und den Connector für Cloud Volumes ONTAP 9.12.1 GA und höher unterstützt.

Eine Liste aller Regionen finden Sie im "Globale Regionenkarte unter Google Cloud" .

23. Oktober 2023

Die folgende Änderung wurde mit der Version 3.9.34 des Connectors eingeführt.

Neue Regionen werden für HA-Bereitstellungen in mehreren Verfügbarkeitszonen in Azure unterstützt

Die folgenden Regionen in Azure unterstützen jetzt hochverfügbare Bereitstellungen in mehreren Verfügbarkeitszonen für Cloud Volumes ONTAP 9.12.1 GA und höher:

- Australien Ost
- Ostasien
- Frankreich, Mitte
- Nordeuropa
- Katar-Zentral
- Schweden, Mitte
- Westeuropa
- Westen USA 2

Eine Liste aller Regionen, die mehrere Verfügbarkeitszonen unterstützen, finden Sie im "Globale Regionenkarte unter Azure" .

06. Oktober 2023

Die folgende Änderung wurde mit der Version 3.9.34 des Connectors eingeführt.

Cloud Volumes ONTAP 9.14.0

BlueXP kann jetzt die allgemein verfügbare Version von Cloud Volumes ONTAP 9.14.0 in AWS, Azure und Google Cloud bereitstellen und verwalten.

"Erfahren Sie mehr über die neuen Funktionen dieser Version von Cloud Volumes ONTAP" .

10. September 2023

Die folgende Änderung wurde mit der Version 3.9.33 des Connectors eingeführt.

Unterstützung für VMs der Lsv3-Serie in Azure

Die Instanztypen L48s_v3 und L64s_v3 werden ab der Version 9.13.1 jetzt mit Cloud Volumes ONTAP in Azure für Einzelknoten- und Hochverfügbarkeitspaarbereitstellungen mit gemeinsam genutzten verwalteten Datenträgern in einzelnen und mehreren Verfügbarkeitszonen unterstützt. Diese Instanztypen unterstützen Flash Cache.

"Unterstützte Konfigurationen für Cloud Volumes ONTAP in Azure anzeigen" "Speicherlimits für Cloud Volumes ONTAP in Azure anzeigen"

30. Juli 2023

Die folgenden Änderungen wurden mit der Version 3.9.32 des Connectors eingeführt.

Flash-Cache und Unterstützung für hohe Schreibgeschwindigkeit in Google Cloud

Flash-Cache und hohe Schreibgeschwindigkeit können in Google Cloud für Cloud Volumes ONTAP 9.13.1 und höher separat aktiviert werden. Eine hohe Schreibgeschwindigkeit ist auf allen unterstützten Instanztypen verfügbar. Flash Cache wird auf den folgenden Instanztypen unterstützt:

- n2-Standard-16
- n2-Standard-32
- n2-Standard-48
- n2-Standard-64

Sie können diese Funktionen separat oder zusammen sowohl bei Einzelknoten- als auch bei Hochverfügbarkeitspaarbereitstellungen verwenden.

"Starten Sie Cloud Volumes ONTAP in Google Cloud"

Verbesserungen bei Nutzungsberichten

Es stehen nun verschiedene Verbesserungen der angezeigten Informationen in den Nutzungsberichten zur Verfügung. Im Folgenden sind die Verbesserungen der Nutzungsberichte aufgeführt:

- Die Einheit TiB ist jetzt im Namen der Spalten enthalten.
- Ein neues Feld „Knoten“ für Seriennummern ist jetzt enthalten.

- Im Nutzungsbericht der Storage-VMs ist jetzt eine neue Spalte „Workload-Typ“ enthalten.
- Die Namen der Arbeitsumgebungen sind jetzt in den Berichten zur Speicher-VM- und Volume-Nutzung enthalten.
- Der Datenträgertyp „Datei“ trägt jetzt die Bezeichnung „Primär (Lesen/Schreiben)“.
- Der Datenträgertyp „sekundär“ trägt jetzt die Bezeichnung „Sekundär (DP)“.

Weitere Informationen zu Nutzungsberichten finden Sie unter "Nutzungsberichte herunterladen" .

26. Juli 2023

Die folgenden Änderungen wurden mit der Version 3.9.31 des Connectors eingeführt.

Cloud Volumes ONTAP 9.13.1 GA

BlueXP kann jetzt die allgemein verfügbare Version von Cloud Volumes ONTAP 9.13.1 in AWS, Azure und Google Cloud bereitstellen und verwalten.

"Erfahren Sie mehr über die neuen Funktionen dieser Version von Cloud Volumes ONTAP" .

02. Juli 2023

Die folgenden Änderungen wurden mit der Version 3.9.31 des Connectors eingeführt.

Unterstützung für HA-Bereitstellungen in mehreren Verfügbarkeitszonen in Azure

Japan Ost und Korea Zentral in Azure unterstützen jetzt HA-Bereitstellungen in mehreren Verfügbarkeitszonen für Cloud Volumes ONTAP 9.12.1 GA und höher.

Eine Liste aller Regionen, die mehrere Verfügbarkeitszonen unterstützen, finden Sie im "Globale Regionenkarte unter Azure" .

Unterstützung für autonomen Ransomware-Schutz

Autonomous Ransomware Protection (ARP) wird jetzt auf Cloud Volumes ONTAP unterstützt. ARP-Unterstützung ist auf Cloud Volumes ONTAP Version 9.12.1 und höher verfügbar.

Weitere Informationen zu ARP mit Cloud Volumes ONTAP finden Sie unter "Autonomer Ransomware-Schutz" .

26. Juni 2023

Die folgende Änderung wurde mit der Version 3.9.30 des Connectors eingeführt.

Cloud Volumes ONTAP 9.13.1 RC1

BlueXP kann jetzt Cloud Volumes ONTAP 9.13.1 in AWS, Azure und Google Cloud bereitstellen und verwalten.

"Erfahren Sie mehr über die neuen Funktionen dieser Version von Cloud Volumes ONTAP" .

04. Juni 2023

Die folgende Änderung wurde mit der Version 3.9.30 des Connectors eingeführt.

Aktualisierung der Versionsauswahl für Cloud Volumes ONTAP

Über die Seite „Cloud Volumes ONTAP aktualisieren“ können Sie jetzt wählen, ob Sie auf die neueste verfügbare Version von Cloud Volumes ONTAP oder auf eine ältere Version aktualisieren möchten.

Weitere Informationen zum Upgrade von Cloud Volumes ONTAP über BlueXP finden Sie unter "Upgrade von Cloud Volumes ONTAP" .

07. Mai 2023

Die folgenden Änderungen wurden mit der Version 3.9.29 des Connectors eingeführt.

Die Region Katar wird jetzt in Google Cloud unterstützt

Die Region Katar wird jetzt in Google Cloud für Cloud Volumes ONTAP und den Connector für Cloud Volumes ONTAP 9.12.1 GA und höher unterstützt.

Die Region Schweden Mitte wird jetzt in Azure unterstützt

Die Region „Schweden, Mitte“ wird jetzt in Azure für Cloud Volumes ONTAP und den Connector für Cloud Volumes ONTAP 9.12.1 GA und höher unterstützt.

Unterstützung für HA-Bereitstellungen in mehreren Verfügbarkeitszonen in Azure Australien Ost

Die Region Australien-Ost in Azure unterstützt jetzt HA-Bereitstellungen in mehreren Verfügbarkeitszonen für Cloud Volumes ONTAP 9.12.1 GA und höher.

Aufschlüsselung der Ladenutzung

Jetzt können Sie herausfinden, was Ihnen in Rechnung gestellt wird, wenn Sie kapazitätsbasierte Lizenzen abonniert haben. Die folgenden Arten von Nutzungsberichten stehen zum Download aus der digitalen Geldbörse in BlueXP zur Verfügung. Die Nutzungsberichte liefern Kapazitätsdetails zu Ihren Abonnements und informieren Sie darüber, wie Ihnen die Ressourcen in Ihren Cloud Volumes ONTAP Abonnements in Rechnung gestellt werden. Die herunterladbaren Berichte können problemlos mit anderen geteilt werden.

- Cloud Volumes ONTAP Paketnutzung
- Nutzung auf hohem Niveau
- Nutzung von Speicher-VMs
- Volume-Nutzung

Weitere Informationen finden Sie unter "Kapazitätsbasierte Lizenzen verwalten" .

Beim Zugriff auf BlueXP ohne Marktplatz-Abonnement wird jetzt eine Benachrichtigung angezeigt

Wenn Sie jetzt ohne Marktplatzabonnement auf Cloud Volumes ONTAP in BlueXP zugreifen, wird eine Benachrichtigung angezeigt. In der Benachrichtigung heißt es: „Für diese Arbeitsumgebung ist ein Marktplatzabonnement erforderlich, um den Geschäftsbedingungen von Cloud Volumes ONTAP zu entsprechen.“

Neue Berechtigungen wurden der AWS IAM-Richtlinie für HA-Mediatoren hinzugefügt.

Diese neuen AWS-Berechtigungen wurden der IAM-Richtlinie für HA-Mediatoren in Cloud Volumes ONTAP Hochverfügbarkeitsumgebungen (HA) hinzugefügt:

- sts:Rolle übernehmen
- ec2:DescribeSubnets

04. April 2023

Unterstützung für China-Regionen für AWS

Ab Cloud Volumes ONTAP 9.12.1 GA werden China-Regionen in AWS jetzt wie folgt unterstützt.

- Einzelknotensysteme werden unterstützt.
- Es werden direkt von NetApp erworbene Lizenzen unterstützt.

Informationen zur regionalen Verfügbarkeit finden Sie im "Globale Regionenkarten für Cloud Volumes ONTAP" .

3. April 2023

Die folgenden Änderungen wurden mit der Version 3.9.28 des Connectors eingeführt.

Die Region Turin wird jetzt in Google Cloud unterstützt

Die Region Turin wird jetzt in Google Cloud für Cloud Volumes ONTAP und den Connector für Cloud Volumes ONTAP 9.12.1 GA und höher unterstützt.

BlueXP digital wallet -Erweiterung

Die BlueXP digital wallet zeigt jetzt die lizenzierte Kapazität an, die Sie mit privaten Angeboten auf dem Marktplatz erworben haben.

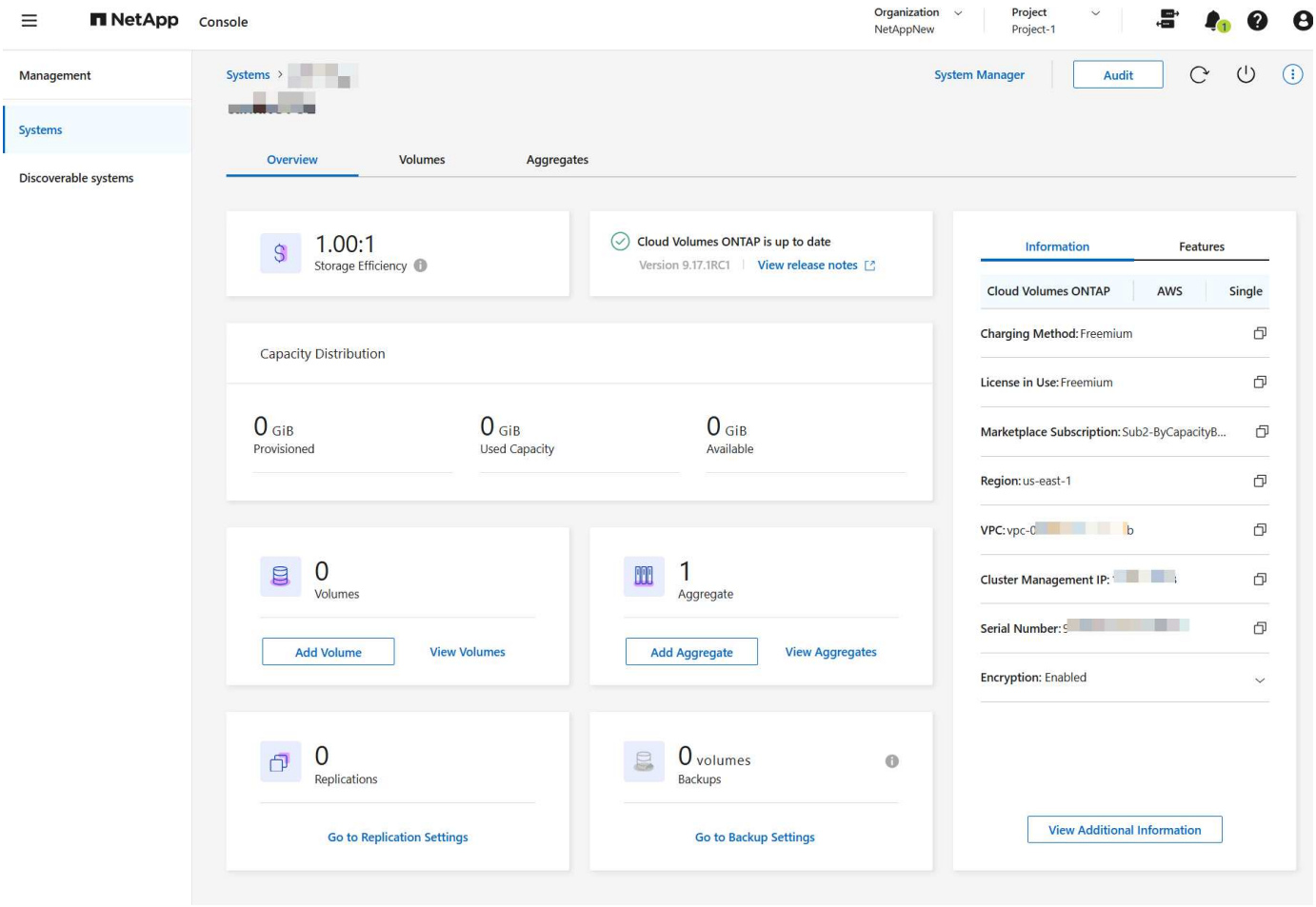
"Erfahren Sie, wie Sie die verbrauchte Kapazität in Ihrem Konto anzeigen können" .

Unterstützung für Kommentare während der Volume-Erstellung

Mit dieser Version können Sie beim Erstellen eines Cloud Volumes ONTAP FlexGroup Volumes oder FlexVol volume mithilfe der API Kommentare abgeben.

Neugestaltung der BlueXP -Benutzeroberfläche für die Seiten „Übersicht“, „Volumes“ und „Aggregates “ von Cloud Volumes ONTAP

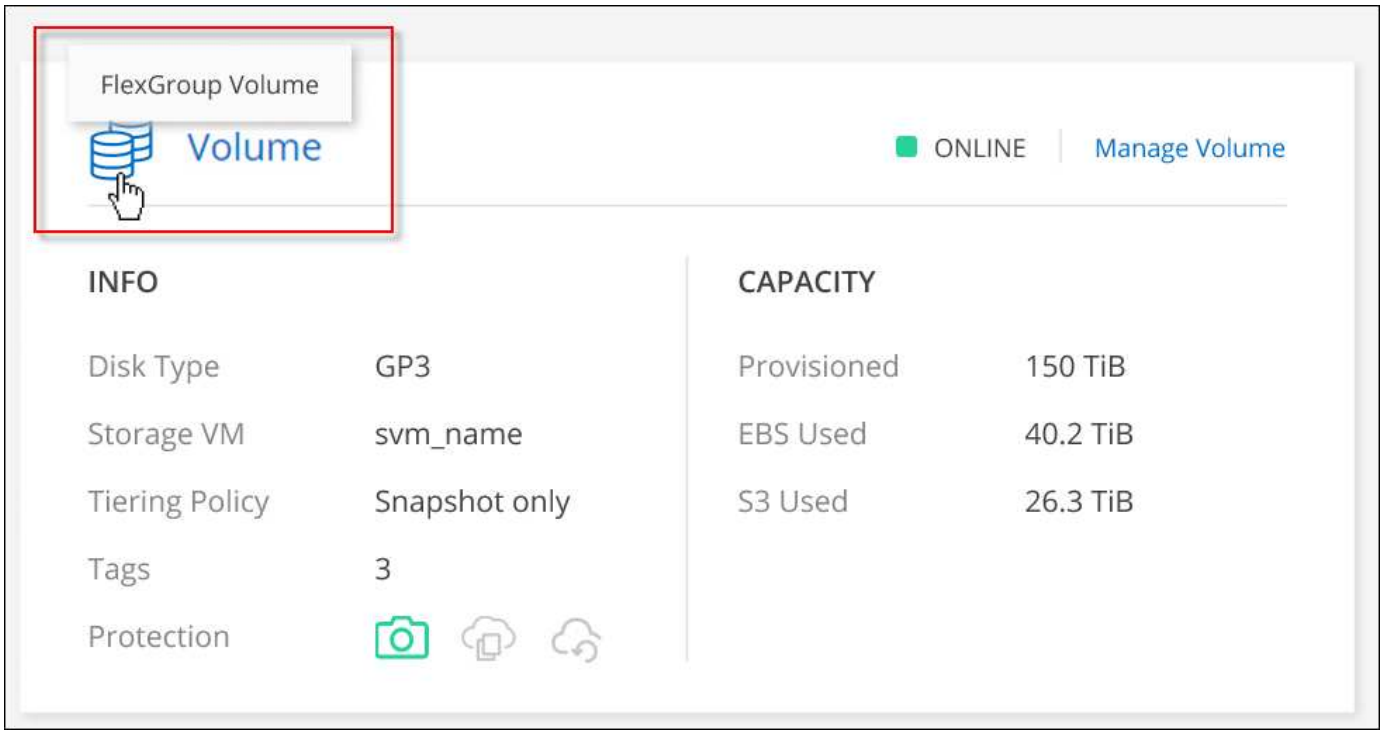
BlueXP verfügt jetzt über eine neu gestaltete Benutzeroberfläche für die Seiten „Übersicht“, „Volumes“ und „Aggregates “ von Cloud Volumes ONTAP . Das kachelbasierte Design präsentiert in jeder Kachel umfassendere Informationen und sorgt so für ein besseres Benutzererlebnis.



FlexGroup -Volumes über Cloud Volumes ONTAP sichtbar

FlexGroup -Volumes, die direkt über den ONTAP System Manager oder die ONTAP CLI erstellt wurden, können jetzt über die neu gestaltete Volume-Kachel in BlueXP angezeigt werden. Identisch mit den für FlexVol -Volumes bereitgestellten Informationen bietet BlueXP detaillierte Informationen für erstellte FlexGroup Volumes über eine spezielle Volume-Kachel.

Derzeit können Sie unter BlueXP nur vorhandene FlexGroup -Volumes anzeigen. Die Möglichkeit, FlexGroup -Volumes in BlueXP zu erstellen, ist nicht verfügbar, aber für eine zukünftige Version geplant.



"Erfahren Sie mehr über das Anzeigen erstellter FlexGroup -Volumes."

13. März 2023

Unterstützung für China-Regionen in Azure

Die Region China Nord 3 wird jetzt für Einzelknotenbereitstellungen von Cloud Volumes ONTAP 9.12.1 GA und 9.13.0 GA in Azure unterstützt. In diesen Regionen werden nur direkt von NetApp erworbene Lizenzen (BYOL-Lizenzen) unterstützt.

Neue Bereitstellungen von Cloud Volumes ONTAP in den Regionen China werden nur in 9.12.1 GA und 9.13.0 GA unterstützt. Sie können diese Versionen auf neuere Patches und Releases von Cloud Volumes ONTAP aktualisieren. Wenn Sie neuere Versionen von Cloud Volumes ONTAP in chinesischen Regionen bereitstellen möchten, wenden Sie sich an den NetApp Support.

Informationen zur regionalen Verfügbarkeit finden Sie im "Globale Regionenkarten für Cloud Volumes ONTAP" .

05. März 2023

Die folgenden Änderungen wurden mit der Version 3.9.27 des Connectors eingeführt.

Cloud Volumes ONTAP 9.13.0

BlueXP kann jetzt Cloud Volumes ONTAP 9.13.0 in AWS, Azure und Google Cloud bereitstellen und verwalten.

"Erfahren Sie mehr über die neuen Funktionen dieser Version von Cloud Volumes ONTAP" .

16 TiB- und 32 Tib-Unterstützung in Azure

Cloud Volumes ONTAP unterstützt jetzt Festplattengrößen von 16 TiB und 32 TiB für Hochverfügbarkeitsbereitstellungen, die auf verwalteten Festplatten in Azure ausgeführt werden.

Erfahren Sie mehr über "unterstützte Datenträgergrößen in Azure" .

MTEKM-Lizenz

Die Multi-Tenant Encryption Key Management (MTEKM)-Lizenz ist jetzt in neuen und vorhandenen Cloud Volumes ONTAP Systemen mit Version 9.12.1 GA oder höher enthalten.

Durch die mandantenfähige externe Schlüsselverwaltung können einzelne Storage-VMs (SVMs) bei Verwendung von NetApp Volume Encryption ihre eigenen Schlüssel über einen KMIP-Server verwalten.

"Erfahren Sie, wie Sie Volumes mit NetApp Verschlüsselungslösungen verschlüsseln" .

Unterstützung für Umgebungen ohne Internet

Cloud Volumes ONTAP wird jetzt in jeder Cloud-Umgebung unterstützt, die vollständig vom Internet isoliert ist. In diesen Umgebungen wird nur die knotenbasierte Lizenzierung (BYOL) unterstützt. Kapazitätsbasierte Lizenzierung wird nicht unterstützt. Installieren Sie zunächst die Connector-Software manuell, melden Sie sich bei der BlueXP Konsole an, die auf dem Connector ausgeführt wird, fügen Sie Ihre BYOL-Lizenz zur BlueXP digital wallet hinzu und stellen Sie dann Cloud Volumes ONTAP bereit.

- "Installieren Sie den Connector an einem Ort ohne Internetzugang"
- "Greifen Sie auf die BlueXP -Konsole auf dem Connector zu"
- "Hinzufügen einer nicht zugewiesenen Lizenz"

Flash Cache und hohe Schreibgeschwindigkeit in Google Cloud

Unterstützung für Flash Cache, hohe Schreibgeschwindigkeit und eine hohe maximale Übertragungseinheit (MTU) von 8.896 Byte ist jetzt für ausgewählte Instanzen mit der Version Cloud Volumes ONTAP 9.13.0 verfügbar.

Erfahren Sie mehr über "unterstützte Konfigurationen nach Lizenz für Google Cloud" .

05. Februar 2023

Die folgenden Änderungen wurden mit der Version 3.9.26 des Connectors eingeführt.

Erstellen einer Platzierungsgruppe in AWS

Für die Erstellung von Platzierungsgruppen mit AWS HA-Bereitstellungen in einer einzelnen Verfügbarkeitszone (AZ) ist jetzt eine neue Konfigurationseinstellung verfügbar. Jetzt können Sie fehlgeschlagene Platzierungsgruppenerstellungen umgehen und zulassen, dass einzelne AWS HA-AZ-Bereitstellungen erfolgreich abgeschlossen werden.

Ausführliche Informationen zum Konfigurieren der Einstellungen für die Platzierungsgruppenerstellung finden Sie unter "Konfigurieren der Platzierungsgruppenerstellung für AWS HA Single AZ" .

Aktualisierung der Konfiguration der privaten DNS-Zone

Jetzt ist eine neue Konfigurationseinstellung verfügbar, mit der Sie bei der Verwendung von Azure Private Links die Erstellung einer Verbindung zwischen einer privaten DNS-Zone und einem virtuellen Netzwerk vermeiden können. Die Erstellung ist standardmäßig aktiviert.

"Geben Sie BlueXP Details zu Ihrem Azure Private DNS"

WORM-Speicherung und Daten-Tiering

Sie können jetzt sowohl Data Tiering als auch WORM-Speicher zusammen aktivieren, wenn Sie ein Cloud Volumes ONTAP 9.8-System oder höher erstellen. Durch die Aktivierung der Datenschichtung mit WORM-Speicher können Sie die Daten in einem Objektspeicher in der Cloud schichten.

"Erfahren Sie mehr über WORM-Speicher."

1. Januar 2023

Die folgenden Änderungen wurden mit der Version 3.9.25 des Connectors eingeführt.

In Google Cloud verfügbare Lizenzpakete

Für Cloud Volumes ONTAP sind optimierte und Edge Cache-Kapazitäts-basierte Lizenzpakete im Google Cloud Marketplace als Pay-as-you-go-Angebot oder als Jahresvertrag verfügbar.

Siehe "Cloud Volumes ONTAP -Lizenzierung" .

Standardkonfiguration für Cloud Volumes ONTAP

Die Multi-Tenant Encryption Key Management (MTEKM)-Lizenz ist in neuen Cloud Volumes ONTAP Bereitstellungen nicht mehr enthalten.

Weitere Informationen zu den ONTAP -Funktionslizenzen, die automatisch mit Cloud Volumes ONTAP installiert werden, finden Sie unter "Standardkonfiguration für Cloud Volumes ONTAP" .

15. Dezember 2022

Cloud Volumes ONTAP 9.12.0

BlueXP kann jetzt Cloud Volumes ONTAP 9.12.0 in AWS und Google Cloud bereitstellen und verwalten.

"Erfahren Sie mehr über die neuen Funktionen dieser Version von Cloud Volumes ONTAP" .

08. Dezember 2022

Cloud Volumes ONTAP 9.12.1

BlueXP kann jetzt Cloud Volumes ONTAP 9.12.1 bereitstellen und verwalten, einschließlich Unterstützung für neue Funktionen und zusätzliche Regionen von Cloud-Anbietern.

"Erfahren Sie mehr über die neuen Funktionen dieser Version von Cloud Volumes ONTAP"

04. Dezember 2022

Die folgenden Änderungen wurden mit der Version 3.9.24 des Connectors eingeführt.

WORM + Cloud Backup jetzt während der Erstellung von Cloud Volumes ONTAP verfügbar

Während des Erstellungsprozesses von Cloud Volumes ONTAP können jetzt sowohl die Funktionen „Write Once, Read Many“ (WORM) als auch „Cloud Backup“ aktiviert werden.

Die Region Israel wird jetzt in Google Cloud unterstützt

Die Region Israel wird jetzt in Google Cloud für Cloud Volumes ONTAP und den Connector für Cloud Volumes ONTAP 9.11.1 P3 und höher unterstützt.

15. November 2022

Die folgenden Änderungen wurden mit der Version 3.9.23 des Connectors eingeführt.

ONTAP S3-Lizenz in Google Cloud

Eine ONTAP S3-Lizenz ist jetzt in neuen und vorhandenen Cloud Volumes ONTAP Systemen mit Version 9.12.1 oder höher in der Google Cloud Platform enthalten.

"ONTAP -Dokumentation: Erfahren Sie, wie Sie S3-Objektspeicherdienste konfigurieren und verwalten"

06. November 2022

Die folgenden Änderungen wurden mit der Version 3.9.23 des Connectors eingeführt.

Verschieben von Ressourcengruppen in Azure

Sie können jetzt eine Arbeitsumgebung innerhalb desselben Azure-Abonnements von einer Ressourcengruppe in eine andere Ressourcengruppe in Azure verschieben.

Weitere Informationen finden Sie unter "Verschieben von Ressourcengruppen" .

NDMP-Kopierzertifizierung

NDMP-Copy ist jetzt für die Verwendung mit Cloud Volume ONTAP zertifiziert.

Informationen zur Konfiguration und Verwendung von NDMP finden Sie im "ONTAP -Dokumentation: Übersicht über die NDMP-Konfiguration" .

Unterstützung für verwaltete Datenträgerverschlüsselung für Azure

Es wurde eine neue Azure-Berechtigung hinzugefügt, mit der Sie jetzt alle verwalteten Datenträger bei der Erstellung verschlüsseln können.

Weitere Informationen zu dieser neuen Funktionalität finden Sie unter "Richten Sie Cloud Volumes ONTAP für die Verwendung eines vom Kunden verwalteten Schlüssels in Azure ein" .

18. September 2022

Die folgenden Änderungen wurden mit der Version 3.9.22 des Connectors eingeführt.

Verbesserungen für Digital Wallet

- Das Digital Wallet zeigt jetzt eine Zusammenfassung des Optimized I/O-Lizenzpakets und der bereitgestellten WORM-Kapazität für Cloud Volumes ONTAP Systeme in Ihrem gesamten Konto an.

  Mithilfe dieser Angaben können Sie besser verstehen, welche Kosten Ihnen in Rechnung gestellt werden und ob Sie zusätzliche Kapazität erwerben müssen.

  "Erfahren Sie, wie Sie die verbrauchte Kapazität in Ihrem Konto anzeigen können" .

- Sie können jetzt von einer Lademethode zur optimierten Lademethode wechseln.

  "Erfahren Sie, wie Sie die Lademethode ändern" .

Optimieren Sie Kosten und Leistung

Sie können jetzt die Kosten und Leistung eines Cloud Volumes ONTAP Systems direkt vom Canvas aus optimieren.

Nachdem Sie eine Arbeitsumgebung ausgewählt haben, können Sie die Option **Kosten und Leistung optimieren** wählen, um den Instanztyp für Cloud Volumes ONTAP zu ändern. Durch die Auswahl einer kleineren Instanz können Sie Kosten senken, während der Wechsel zu einer größeren Instanz Ihnen dabei helfen kann, die Leistung zu optimieren.

[Ein Screenshot der Option „Kosten und Leistung optimieren“, die im Canvas verfügbar ist, nachdem Sie ein Cloud Volumes ONTAP -System ausgewählt haben.]

AutoSupport -Benachrichtigungen

BlueXP generiert jetzt eine Benachrichtigung, wenn ein Cloud Volumes ONTAP System keine AutoSupport Nachrichten senden kann. Die Benachrichtigung enthält einen Link zu Anweisungen, die Sie zur Behebung von Netzwerkproblemen verwenden können.

31. Juli 2022

Die folgenden Änderungen wurden mit der Version 3.9.21 des Connectors eingeführt.

MTEKM-Lizenz

Die Multi-Tenant Encryption Key Management (MTEKM)-Lizenz ist jetzt in neuen und vorhandenen Cloud Volumes ONTAP Systemen mit Version 9.11.1 oder höher enthalten.

Durch die mandantenfähige externe Schlüsselverwaltung können einzelne Storage-VMs (SVMs) bei Verwendung von NetApp Volume Encryption ihre eigenen Schlüssel über einen KMIP-Server verwalten.

"Erfahren Sie, wie Sie Volumes mit NetApp Verschlüsselungslösungen verschlüsseln" .

Proxyserver

BlueXP konfiguriert Ihre Cloud Volumes ONTAP -Systeme jetzt automatisch so, dass der Connector als

Proxyserver verwendet wird, wenn keine ausgehende Internetverbindung zum Senden von AutoSupport -Nachrichten verfügbar ist.

AutoSupport überwacht proaktiv den Zustand Ihres Systems und sendet Nachrichten an den technischen Support von NetApp .

Die einzige Voraussetzung besteht darin, sicherzustellen, dass die Sicherheitsgruppe des Connectors *eingehende* Verbindungen über Port 3128 zulässt. Sie müssen diesen Port öffnen, nachdem Sie den Connector bereitgestellt haben.

Lademethode ändern

Sie können jetzt die Abrechnungsmethode für ein Cloud Volumes ONTAP -System ändern, das eine kapazitätsbasierte Lizenzierung verwendet. Wenn Sie beispielsweise ein Cloud Volumes ONTAP -System mit dem Essentials-Paket bereitgestellt haben, können Sie es auf das Professional-Paket umstellen, wenn sich Ihre Geschäftsanforderungen ändern. Diese Funktion ist im Digital Wallet verfügbar.

"Erfahren Sie, wie Sie die Lademethode ändern" .

Verbesserung der Sicherheitsgruppe

Wenn Sie eine Cloud Volumes ONTAP Arbeitsumgebung erstellen, können Sie jetzt über die Benutzeroberfläche auswählen, ob die vordefinierte Sicherheitsgruppe nur Datenverkehr innerhalb des ausgewählten Netzwerks (empfohlen) oder aller Netzwerke zulassen soll.

[Ein Screenshot, der die Option „Datenverkehr zulassen innerhalb“ zeigt, die im Arbeitsumgebungsassistenten beim Auswählen einer Sicherheitsgruppe verfügbar ist.]

18. Juli 2022

Neue Lizenzpakete in Azure

Für Cloud Volumes ONTAP in Azure sind zwei neue kapazitätsbasierte Lizenzpakete verfügbar, wenn Sie über ein Azure Marketplace-Abonnement bezahlen:

- **Optimiert**: Bezahlen Sie für bereitgestellte Kapazität und E/A-Vorgänge separat
- **Edge Cache**: Lizenzierung für "Cloud Volumes Edge Cache"

"Erfahren Sie mehr über diese Lizenzpakete" .

3. Juli 2022

Die folgenden Änderungen wurden mit der Version 3.9.20 des Connectors eingeführt.

Digitale Geldbörse

Die digitale Geldbörse zeigt Ihnen jetzt die gesamte verbrauchte Kapazität in Ihrem Konto und die verbrauchte Kapazität pro Lizenzpaket an. Auf diese Weise können Sie besser nachvollziehen, welche Kosten Ihnen in Rechnung gestellt werden und ob Sie zusätzliche Kapazität erwerben müssen.

[Ein Screenshot, der die Digital Wallet-Seite für kapazitätsbasierte Lizenzen zeigt. Die Seite bietet einen Überblick über die verbrauchte Kapazität in Ihrem Konto und schlüsselt die verbrauchte Kapazität anschließend nach Lizenzpaket auf.]

Verbesserung von Elastic Volumes

BlueXP unterstützt jetzt die Funktion „Amazon EBS Elastic Volumes“ beim Erstellen einer Cloud Volumes ONTAP Arbeitsumgebung über die Benutzeroberfläche. Die Funktion „Elastic Volumes“ ist standardmäßig aktiviert, wenn gp3- oder io1-Datenträger verwendet werden. Sie können die anfängliche Kapazität basierend auf Ihrem Speicherbedarf auswählen und sie nach der Bereitstellung von Cloud Volumes ONTAP überarbeiten.

"Erfahren Sie mehr über die Unterstützung für Elastic Volumes in AWS" .

ONTAP S3-Lizenz in AWS

Eine ONTAP S3-Lizenz ist jetzt auf neuen und vorhandenen Cloud Volumes ONTAP Systemen mit Version 9.11.0 oder höher in AWS enthalten.

"ONTAP -Dokumentation: Erfahren Sie, wie Sie S3-Objektspeicherdienste konfigurieren und verwalten"

Neue Azure Cloud-Regionsunterstützung

Ab der Version 9.10.1 wird Cloud Volumes ONTAP jetzt in der Azure-Region „West US 3“ unterstützt.

"Vollständige Liste der unterstützten Regionen für Cloud Volumes ONTAP anzeigen"

ONTAP S3-Lizenz in Azure

Eine ONTAP S3-Lizenz ist jetzt auf neuen und vorhandenen Cloud Volumes ONTAP Systemen mit Version 9.9.1 oder höher in Azure enthalten.

"ONTAP -Dokumentation: Erfahren Sie, wie Sie S3-Objektspeicherdienste konfigurieren und verwalten"

07. Juni 2022

Die folgenden Änderungen wurden mit der Version 3.9.19 des Connectors eingeführt.

Cloud Volumes ONTAP 9.11.1

BlueXP kann jetzt Cloud Volumes ONTAP 9.11.1 bereitstellen und verwalten, einschließlich Unterstützung für neue Funktionen und zusätzliche Regionen von Cloud-Anbietern.

"Erfahren Sie mehr über die neuen Funktionen dieser Version von Cloud Volumes ONTAP"

Neue erweiterte Ansicht

Wenn Sie eine erweiterte Verwaltung von Cloud Volumes ONTAP durchführen müssen, können Sie dies mit dem ONTAP System Manager tun, einer Verwaltungsschnittstelle, die mit einem ONTAP -System bereitgestellt wird. Wir haben die System Manager-Schnittstelle direkt in BlueXP integriert, sodass Sie BlueXP für erweiterte Verwaltungsvorgänge nicht verlassen müssen.

Diese erweiterte Ansicht ist als Vorschau mit Cloud Volumes ONTAP 9.10.0 und höher verfügbar. Wir planen, dieses Erlebnis zu verfeinern und in kommenden Versionen Verbesserungen hinzuzufügen. Bitte senden Sie uns Feedback über den Chat im Produkt.

"Erfahren Sie mehr über die erweiterte Ansicht" .

Unterstützung für Amazon EBS Elastic Volumes

Die Unterstützung der Amazon EBS Elastic Volumes-Funktion mit einem Cloud Volumes ONTAP -Aggregat bietet eine bessere Leistung und zusätzliche Kapazität und ermöglicht BlueXP gleichzeitig, die zugrunde liegende Festplattenkapazität nach Bedarf automatisch zu erhöhen.

Unterstützung für Elastic Volumes ist ab den *neuen* Cloud Volumes ONTAP 9.11.0-Systemen und mit den EBS-Festplattentypen gp3 und io1 verfügbar.

"Erfahren Sie mehr über die Unterstützung für Elastic Volumes" .

Beachten Sie, dass die Unterstützung für Elastic Volumes neue AWS-Berechtigungen für den Connector erfordert:

```
"ec2:DescribeVolumesModifications",
"ec2:ModifyVolume",
```

Stellen Sie sicher, dass Sie diese Berechtigungen für jeden Satz von AWS-Anmeldeinformationen erteilen, den Sie zu BlueXP hinzugefügt haben. "Aktuelle Connector-Richtlinie für AWS anzeigen" .

Unterstützung für die Bereitstellung von HA-Paaren in gemeinsam genutzten AWS-Subnetzen

Cloud Volumes ONTAP 9.11.1 umfasst Unterstützung für AWS VPC-Sharing. Mit dieser Version des Connectors können Sie bei Verwendung der API ein HA-Paar in einem gemeinsam genutzten AWS-Subnetz bereitstellen.

"Erfahren Sie, wie Sie ein HA-Paar in einem gemeinsam genutzten Subnetz bereitstellen" .

Eingeschränkter Netzwerkzugriff bei Verwendung von Service-Endpunkten

BlueXP beschränkt jetzt den Netzwerkzugriff bei Verwendung eines VNet-Dienstendpunkts für Verbindungen zwischen Cloud Volumes ONTAP und Speicherkonten. BlueXP verwendet einen Dienstendpunkt, wenn Sie Azure Private Link-Verbindungen deaktivieren.

"Erfahren Sie mehr über Azure Private Link-Verbindungen mit Cloud Volumes ONTAP" .

Unterstützung für die Erstellung von Speicher-VMs in Google Cloud

Ab der Version 9.11.1 werden jetzt mehrere Speicher-VMs mit Cloud Volumes ONTAP in Google Cloud unterstützt. Ab dieser Version des Connectors können Sie mit BlueXP mithilfe der API Speicher-VMs auf Cloud Volumes ONTAP HA-Paaren in Google Cloud erstellen.

Für die Unterstützung beim Erstellen von Speicher-VMs sind neue Google Cloud-Berechtigungen für den Connector erforderlich:

```
- compute.instanceGroups.get
- compute.addresses.get
```

Beachten Sie, dass Sie die ONTAP CLI oder den System Manager verwenden müssen, um eine Storage-VM auf einem Einzelknotensystem zu erstellen.

- "Erfahren Sie mehr über Speicher-VM-Limits in Google Cloud"
- "Erfahren Sie, wie Sie datenbereitstellende Speicher-VMs für Cloud Volumes ONTAP in Google Cloud erstellen."

02. Mai 2022

Die folgenden Änderungen wurden mit der Version 3.9.18 des Connectors eingeführt.

Cloud Volumes ONTAP 9.11.0

BlueXP kann jetzt Cloud Volumes ONTAP 9.11.0 bereitstellen und verwalten.

"Erfahren Sie mehr über die neuen Funktionen dieser Version von Cloud Volumes ONTAP" .

Verbesserung der Mediator-Upgrades

Wenn BlueXP den Mediator für ein HA-Paar aktualisiert, überprüft es jetzt, ob ein neues Mediator-Image verfügbar ist, bevor es die Bootdiskette löscht. Diese Änderung stellt sicher, dass der Mediator auch dann erfolgreich weiterarbeiten kann, wenn der Upgrade-Prozess fehlschlägt.

Die Registerkarte „K8s“ wurde entfernt

Die Registerkarte „K8s“ war in einer früheren Version veraltet und wurde jetzt entfernt.

Jahresvertrag in Azure

Die Pakete Essentials und Professional sind jetzt in Azure über einen Jahresvertrag verfügbar. Sie können sich an Ihren NetApp Vertriebsmitarbeiter wenden, um einen Jahresvertrag abzuschließen. Der Vertrag ist als privates Angebot im Azure Marketplace verfügbar.

Nachdem NetApp Ihnen das private Angebot mitgeteilt hat, können Sie beim Abonnieren im Azure Marketplace während der Erstellung der Arbeitsumgebung den Jahresplan auswählen.

"Erfahren Sie mehr über die Lizenzierung" .

S3 Glacier Sofortabruf

Sie können jetzt gestaffelte Daten in der Amazon Simple Storage Service (Amazon S3) Glacier Instant Retrieval-Speicherklasse speichern.

"Erfahren Sie, wie Sie die Speicherklasse für mehrstufige Daten ändern" .

Für den Connector sind neue AWS-Berechtigungen erforderlich

Die folgenden Berechtigungen sind jetzt erforderlich, um eine AWS-Spread-Placement-Gruppe zu erstellen, wenn ein HA-Paar in einer einzelnen Availability Zone (AZ) bereitgestellt wird:

```
"ec2:DescribePlacementGroups",
"iam:GetRolePolicy",
```

Diese Berechtigungen sind jetzt erforderlich, um die Erstellung der Platzierungsgruppe durch BlueXP zu optimieren.

Stellen Sie sicher, dass Sie diese Berechtigungen für jeden Satz von AWS-Anmeldeinformationen erteilen, den Sie zu BlueXP hinzugefügt haben. "Aktuelle Connector-Richtlinie für AWS anzeigen" .

Neue Unterstützung für Google Cloud-Regionen

Cloud Volumes ONTAP wird ab Version 9.10.1 in den folgenden Google Cloud-Regionen unterstützt:

- Delhi (Asien-Süd2)
- Melbourne (Australien-Südost2)
- Mailand (Europa-West8) – nur einzelner Knoten
- Santiago (Südamerika-West1) – nur einzelner Knoten

"Vollständige Liste der unterstützten Regionen für Cloud Volumes ONTAP anzeigen"

Unterstützung für n2-standard-16 in Google Cloud

Der Maschinentyp n2-standard-16 wird jetzt mit Cloud Volumes ONTAP in Google Cloud unterstützt, beginnend mit der Version 9.10.1.

"Unterstützte Konfigurationen für Cloud Volumes ONTAP in Google Cloud anzeigen"

Verbesserungen der Google Cloud-Firewallrichtlinien

- Wenn Sie ein Cloud Volumes ONTAP HA-Paar in Google Cloud erstellen, zeigt BlueXP jetzt alle vorhandenen Firewall-Richtlinien in einer VPC an.

  Zuvor zeigte BlueXP keine Richtlinien in VPC-1, VPC-2 oder VPC-3 an, die kein Ziel-Tag hatten.

- Wenn Sie ein Cloud Volumes ONTAP Single-Node-System in Google Cloud erstellen, können Sie jetzt auswählen, ob die vordefinierte Firewall-Richtlinie den Datenverkehr nur innerhalb der ausgewählten VPC (empfohlen) oder in allen VPCs zulassen soll.

Verbesserung der Google Cloud-Dienstkonten

Wenn Sie das Google Cloud-Dienstkonto zur Verwendung mit Cloud Volumes ONTAP auswählen, zeigt BlueXP jetzt die E-Mail-Adresse an, die mit jedem Dienstkonto verknüpft ist. Durch die Anzeige der E-Mail-Adresse können Dienstkonten mit demselben Namen leichter unterschieden werden.

[Ein Screenshot des Dienstkontofelds]

3. April 2022

Der Systemmanager-Link wurde entfernt

Wir haben den System Manager-Link entfernt, der zuvor in einer Cloud Volumes ONTAP Arbeitsumgebung verfügbar war.

Sie können weiterhin eine Verbindung zum System Manager herstellen, indem Sie die IP-Adresse der Clusterverwaltung in einen Webbrowser eingeben, der über eine Verbindung zum Cloud Volumes ONTAP -System verfügt. "Erfahren Sie mehr über die Verbindung mit System Manager" .

Gebühren für WORM-Speicher

Da der Einführungssonderpreis nun abgelaufen ist, wird Ihnen die Nutzung des WORM-Speichers nun in Rechnung gestellt. Die Abrechnung erfolgt stündlich, entsprechend der insgesamt bereitgestellten Kapazität der WORM-Volumes. Dies gilt für neue und bestehende Cloud Volumes ONTAP Systeme.

"Informieren Sie sich über die Preise für WORM-Speicher" .

27. Februar 2022

Die folgenden Änderungen wurden mit der Version 3.9.16 des Connectors eingeführt.

Neu gestalteter Volume-Assistent

Der kürzlich eingeführte Assistent zum Erstellen neuer Volumes ist jetzt verfügbar, wenn Sie über die Option **Erweiterte Zuweisung** ein Volume auf einem bestimmten Aggregat erstellen.

"Erfahren Sie, wie Sie Volumes auf einem bestimmten Aggregat erstellen" .

09. Februar 2022

Marktplatz-Updates

- Das Essentials-Paket und das Professional-Paket sind jetzt auf allen Marktplätzen der Cloud-Anbieter verfügbar.

  Diese Abrechnungsmethoden nach Kapazität ermöglichen Ihnen die Zahlung pro Stunde oder den Abschluss eines Jahresvertrags direkt bei Ihrem Cloud-Anbieter. Sie haben weiterhin die Möglichkeit, eine Lizenz nach Kapazität direkt von NetApp zu erwerben.

  Wenn Sie über ein bestehendes Abonnement in einem Cloud-Marktplatz verfügen, sind Sie automatisch auch für diese neuen Angebote angemeldet. Sie können die Abrechnung nach Kapazität wählen, wenn Sie eine neue Cloud Volumes ONTAP Arbeitsumgebung bereitstellen.

  Wenn Sie ein neuer Kunde sind, werden Sie von BlueXP beim Erstellen einer neuen Arbeitsumgebung zum Abonnieren aufgefordert.

- Die Lizenzierung pro Knoten auf allen Marktplätzen der Cloud-Anbieter ist veraltet und für neue Abonnenten nicht mehr verfügbar. Dazu gehören Jahresverträge und Stundenabonnements (Explore, Standard und Premium).

  Für Bestandskunden mit aktivem Abonnement steht diese Abrechnungsmethode weiterhin zur Verfügung.

"Erfahren Sie mehr über die Lizenzierungsoptionen für Cloud Volumes ONTAP" .

06. Februar 2022

Austausch nicht zugewiesener Lizenzen

Wenn Sie über eine nicht zugewiesene knotenbasierte Lizenz für Cloud Volumes ONTAP verfügen, die Sie nicht verwendet haben, können Sie die Lizenz jetzt austauschen, indem Sie sie in eine Cloud Backup-Lizenz, Cloud Data Sense-Lizenz oder Cloud Tiering-Lizenz umwandeln.

Durch diese Aktion wird die Cloud Volumes ONTAP -Lizenz widerrufen und eine Lizenz für den Dienst im

Gegenwert von einem Dollar mit demselben Ablaufdatum erstellt.

"Erfahren Sie, wie Sie nicht zugewiesene knotenbasierte Lizenzen austauschen" .

30. Januar 2022

Die folgenden Änderungen wurden mit der Version 3.9.15 des Connectors eingeführt.

Neu gestaltete Lizenzauswahl

Wir haben den Lizenzauswahlbildschirm beim Erstellen einer neuen Cloud Volumes ONTAP Arbeitsumgebung neu gestaltet. Die Änderungen heben die im Juli 2021 eingeführten kapazitätsabhängigen Abrechnungsmethoden hervor und unterstützen kommende Angebote über die Marktplätze der Cloud-Anbieter.

Aktualisierung der digitalen Geldbörse

Wir haben das **Digital Wallet** aktualisiert, indem wir Cloud Volumes ONTAP -Lizenzen in einer einzigen Registerkarte konsolidiert haben.

02. Januar 2022

Die folgenden Änderungen wurden mit der Version 3.9.14 des Connectors eingeführt.

Unterstützung für zusätzliche Azure-VM-Typen

Cloud Volumes ONTAP wird ab Version 9.10.1 jetzt mit den folgenden VM-Typen in Microsoft Azure unterstützt:

- E4ds_v4
- E8ds_v4
- E32ds_v4
- E48ds_v4

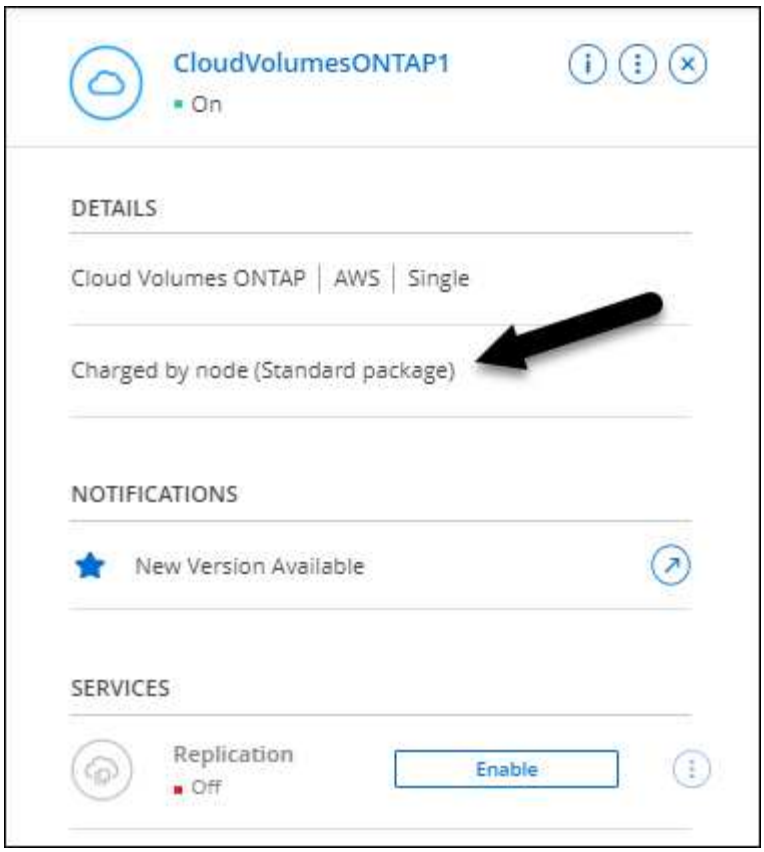
Gehen Sie zum "Versionshinweise zu Cloud Volumes ONTAP" für weitere Details zu unterstützten Konfigurationen.

FlexClone -Ladeupdate

Wenn Sie eine "kapazitätsbasierte Lizenz" Bei Cloud Volumes ONTAP wird Ihnen die von FlexClone -Volumes genutzte Kapazität nicht mehr in Rechnung gestellt.

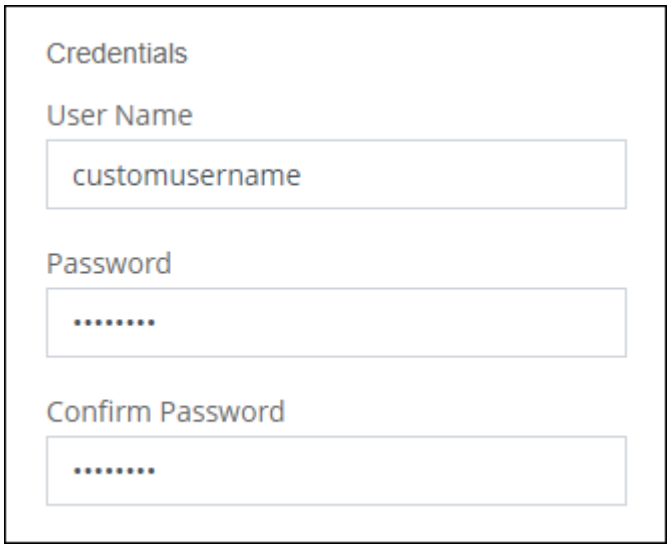
Lademethode wird jetzt angezeigt

BlueXP zeigt jetzt die Abrechnungsmethode für jede Cloud Volumes ONTAP Arbeitsumgebung im rechten Bereich des Canvas an.



Wählen Sie Ihren Benutzernamen

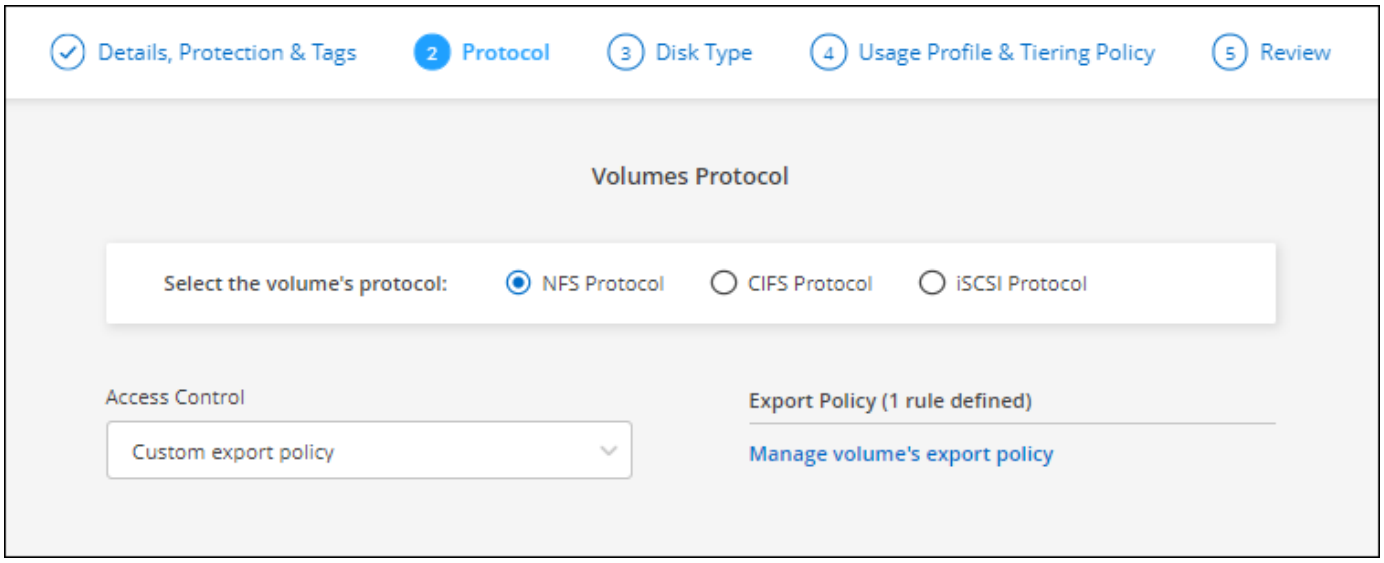
Wenn Sie eine Cloud Volumes ONTAP Arbeitsumgebung erstellen, haben Sie jetzt die Möglichkeit, Ihren bevorzugten Benutzernamen anstelle des standardmäßigen Administratorbenutzernamens einzugeben.



Verbesserungen bei der Volumeerstellung

Wir haben einige Verbesserungen an der Volumeerstellung vorgenommen:

- Wir haben den Assistenten zum Erstellen von Volumes für eine einfachere Verwendung neu gestaltet.
- Sie können jetzt eine benutzerdefinierte Exportrichtlinie für NFS auswählen.



28. November 2021

Die folgenden Änderungen wurden mit der Version 3.9.13 des Connectors eingeführt.

Cloud Volumes ONTAP 9.10.1

BlueXP kann jetzt Cloud Volumes ONTAP 9.10.1 bereitstellen und verwalten.

"Erfahren Sie mehr über die neuen Funktionen dieser Version von Cloud Volumes ONTAP" .

NetApp Keystone Abonnements

Sie können jetzt Keystone Abonnements verwenden, um für Cloud Volumes ONTAP HA-Paare zu bezahlen.

Ein Keystone Abonnement ist ein Abonnementdienst mit nutzungsabhängiger Bezahlung, der ein nahtloses Hybrid-Cloud-Erlebnis für diejenigen bietet, die OpEx-Verbrauchsmodelle gegenüber vorab getätigten Investitionskosten oder Leasing bevorzugen.

Ein Keystone -Abonnement wird mit allen neuen Versionen von Cloud Volumes ONTAP unterstützt, die Sie von BlueXP aus bereitstellen können.

- "Erfahren Sie mehr über NetApp Keystone -Abonnements" .
- "Erfahren Sie, wie Sie mit Keystone -Abonnements in BlueXP beginnen" .

Neue AWS-Regionsunterstützung

Cloud Volumes ONTAP wird jetzt in der AWS-Region Asien-Pazifik (Osaka) (ap-northeast-3) unterstützt.

Portreduzierung

Die Ports 8023 und 49000 sind auf Cloud Volumes ONTAP Systemen in Azure sowohl für Einzelknotensysteme als auch für HA-Paare nicht mehr geöffnet.

Diese Änderung gilt für *neue* Cloud Volumes ONTAP Systeme ab der Version 3.9.13 des Connectors.

04. Oktober 2021

Die folgenden Änderungen wurden mit der Version 3.9.11 des Connectors eingeführt.

Cloud Volumes ONTAP 9.10.0

BlueXP kann jetzt Cloud Volumes ONTAP 9.10.0 bereitstellen und verwalten.

"Erfahren Sie mehr über die neuen Funktionen dieser Version von Cloud Volumes ONTAP" .

Reduzierte Bereitstellungszeit

Wir haben die Zeit reduziert, die zum Bereitstellen einer Cloud Volumes ONTAP Arbeitsumgebung in Microsoft Azure oder in Google Cloud benötigt wird, wenn die normale Schreibgeschwindigkeit aktiviert ist. Die Bereitstellungszeit ist jetzt im Durchschnitt 3–4 Minuten kürzer.

02. September 2021

Die folgenden Änderungen wurden mit der Version 3.9.10 des Connectors eingeführt.

Vom Kunden verwalteter Verschlüsselungsschlüssel in Azure

Die Daten werden automatisch auf Cloud Volumes ONTAP in Azure verschlüsselt mit "Azure Storage Service-Verschlüsselung" mit einem von Microsoft verwalteten Schlüssel. Sie können jetzt stattdessen Ihren eigenen, vom Kunden verwalteten Verschlüsselungsschlüssel verwenden, indem Sie die folgenden Schritte ausführen:

1. Erstellen Sie in Azure einen Schlüsseltresor und generieren Sie dann einen Schlüssel in diesem Tresor.
2. Verwenden Sie von BlueXP aus die API, um eine Cloud Volumes ONTAP Arbeitsumgebung zu erstellen, die den Schlüssel verwendet.

"Erfahren Sie mehr über diese Schritte" .

07. Juli 2021

Die folgenden Änderungen wurden mit der Version 3.9.8 des Connectors eingeführt.

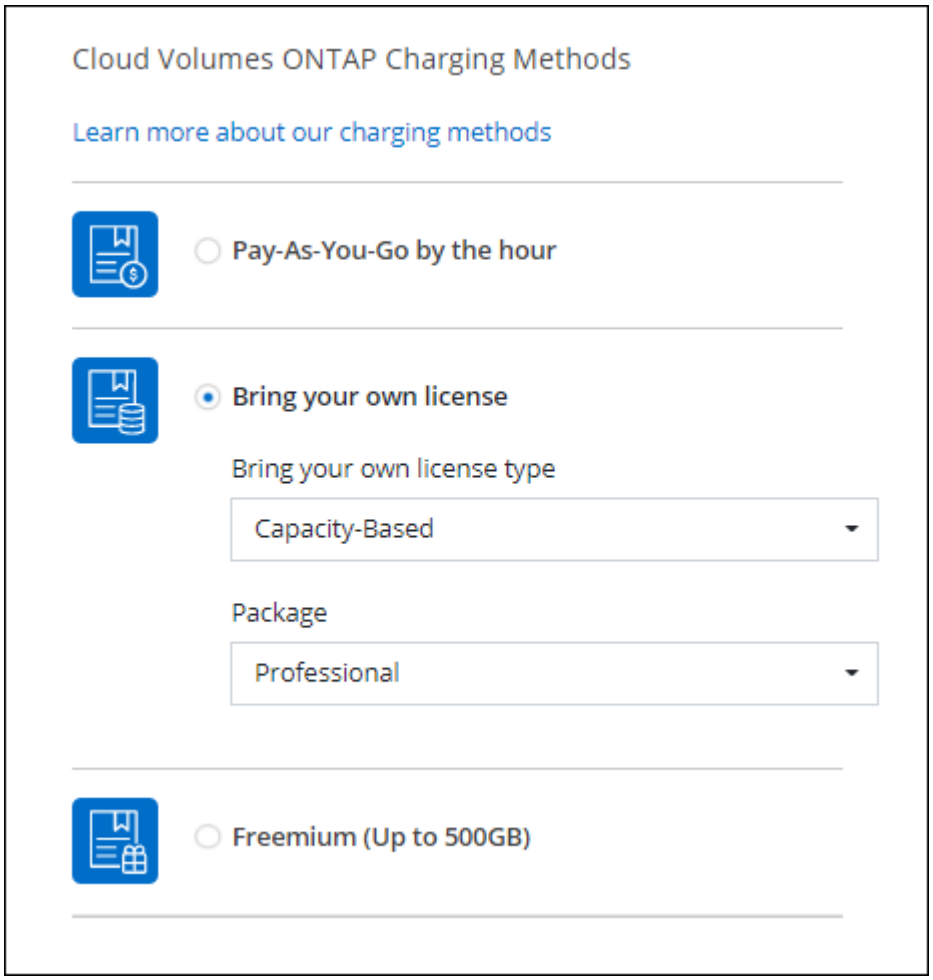
Neue Lademethoden

Für Cloud Volumes ONTAP sind neue Abrechnungsmethoden verfügbar.

- **Kapazitätsbasiertes BYOL**: Eine kapazitätsbasierte Lizenz ermöglicht es Ihnen, für Cloud Volumes ONTAP pro TiB Kapazität zu bezahlen. Die Lizenz ist mit Ihrem NetApp -Konto verknüpft und ermöglicht Ihnen die Erstellung mehrerer Cloud Volumes ONTAP Systeme, sofern über Ihre Lizenz genügend Kapazität verfügbar ist. Die kapazitätsbasierte Lizenzierung ist in Form eines Pakets verfügbar, entweder *Essentials* oder *Professional*.
- **Freemium-Angebot**: Mit Freemium können Sie alle Cloud Volumes ONTAP Funktionen von NetApp kostenlos nutzen (Gebühren des Cloud-Anbieters fallen weiterhin an). Sie sind auf 500 GiB bereitgestellte Kapazität pro System beschränkt und es gibt keinen Supportvertrag. Sie können bis zu 10 Freemium-Systeme haben.

  "Erfahren Sie mehr über diese Lizenzierungsoptionen" .

  Hier ein Beispiel für die Lademethoden, aus denen Sie wählen können:



WORM-Speicher zur allgemeinen Verwendung verfügbar

„Write Once, Read Many“-Speicher (WORM) befindet sich nicht mehr in der Vorschau und ist jetzt für die allgemeine Verwendung mit Cloud Volumes ONTAP verfügbar. "Erfahren Sie mehr über WORM-Speicher" .

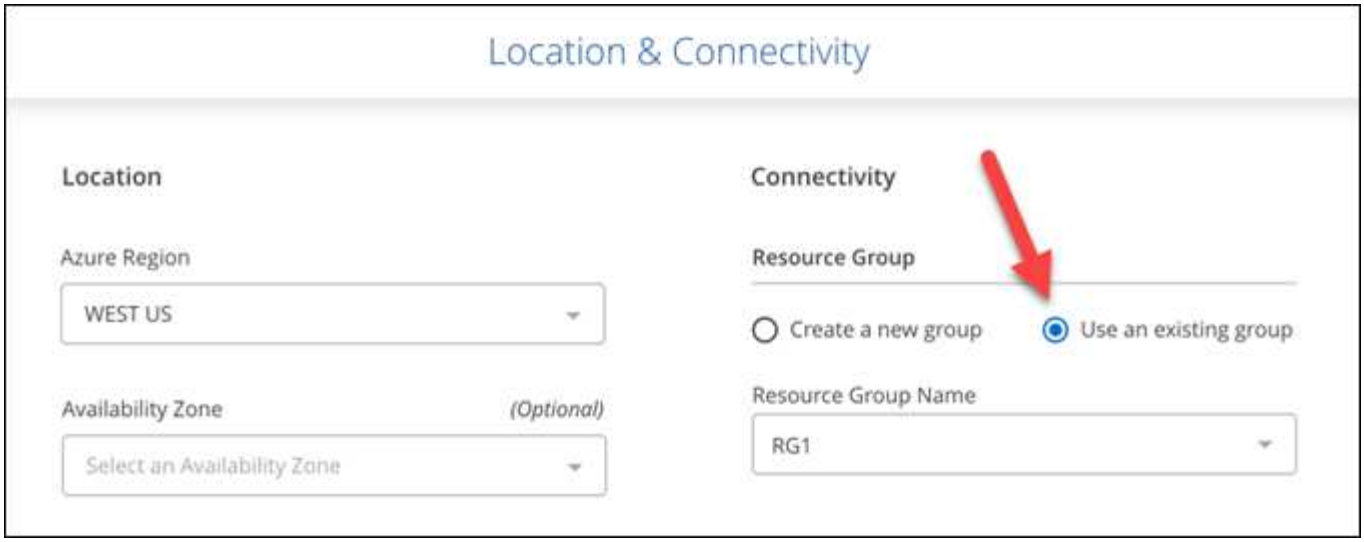
Unterstützung für m5dn.24xlarge in AWS

Ab der Version 9.9.1 unterstützt Cloud Volumes ONTAP jetzt den Instanztyp m5dn.24xlarge mit den folgenden Abrechnungsmethoden: PAYGO Premium, Bring Your Own License (BYOL) und Freemium.

"Unterstützte Konfigurationen für Cloud Volumes ONTAP in AWS anzeigen" .

Vorhandene Azure-Ressourcengruppen auswählen

Beim Erstellen eines Cloud Volumes ONTAP -Systems in Azure haben Sie jetzt die Möglichkeit, eine vorhandene Ressourcengruppe für die VM und die zugehörigen Ressourcen auszuwählen.



Die folgenden Berechtigungen ermöglichen BlueXP , Cloud Volumes ONTAP -Ressourcen aus einer Ressourcengruppe zu entfernen, falls die Bereitstellung fehlschlägt oder eine Löschung erfolgt:

```
"Microsoft.Network/privateEndpoints/delete",
"Microsoft.Compute/availabilitySets/delete",
```

Stellen Sie sicher, dass Sie diese Berechtigungen für jeden Satz von Azure-Anmeldeinformationen erteilen, den Sie zu BlueXP hinzugefügt haben. "Aktuelle Connector-Richtlinie für Azure anzeigen" .

Öffentlicher Blobzugriff jetzt in Azure deaktiviert

Als Sicherheitsverbesserung deaktiviert BlueXP jetzt den **öffentlichen Blob-Zugriff** beim Erstellen eines Speicherkontos für Cloud Volumes ONTAP.

Azure Private Link-Erweiterung

Standardmäßig aktiviert BlueXP jetzt eine Azure Private Link-Verbindung auf dem Boot-Diagnose-Speicherkonto für neue Cloud Volumes ONTAP Systeme.

Dies bedeutet, dass *alle* Speicherkonten für Cloud Volumes ONTAP jetzt eine private Verbindung verwenden.

"Erfahren Sie mehr über die Verwendung eines Azure Private Link mit Cloud Volumes ONTAP" .

Ausgeglichene persistente Datenträger in Google Cloud

Ab der Version 9.9.1 unterstützt Cloud Volumes ONTAP jetzt ausgeglichene persistente Festplatten (pd-balanced).

Diese SSDs gleichen Leistung und Kosten aus, indem sie weniger IOPS pro GiB bieten.

custom-4-16384 wird in Google Cloud nicht mehr unterstützt

Der Maschinentyp „custom-4-16384“ wird von neuen Cloud Volumes ONTAP Systemen nicht mehr unterstützt.

Wenn Sie bereits ein System auf diesem Maschinentyp laufen haben, können Sie es weiterhin verwenden, wir empfehlen jedoch, auf den Maschinentyp n2-standard-4 umzusteigen.

"Unterstützte Konfigurationen für Cloud Volumes ONTAP in Google Cloud anzeigen".

30. Mai 2021

Die folgenden Änderungen wurden mit der Version 3.9.7 des Connectors eingeführt.

Neues Professional-Paket in AWS

Mit einem neuen Professional-Paket können Sie Cloud Volumes ONTAP und Cloud Backup Service bündeln, indem Sie einen Jahresvertrag vom AWS Marketplace nutzen. Die Bezahlung erfolgt pro TiB. Mit diesem Abonnement können Sie keine lokalen Daten sichern.

Wenn Sie diese Zahlungsoption wählen, können Sie bis zu 2 PiB pro Cloud Volumes ONTAP System über EBS-Festplatten und Tiering auf S3-Objektspeicher (Einzelknoten oder HA) bereitstellen.

Gehen Sie zum "AWS Marketplace-Seite" um Preisdetails anzuzeigen und zu gehen "Versionshinweise zu Cloud Volumes ONTAP" um mehr über diese Lizenzierungsoption zu erfahren.

Tags auf EBS-Volumes in AWS

BlueXP fügt jetzt Tags zu EBS-Volumes hinzu, wenn es eine neue Cloud Volumes ONTAP Arbeitsumgebung erstellt. Die Tags wurden zuvor nach der Bereitstellung von Cloud Volumes ONTAP erstellt.

Diese Änderung kann hilfreich sein, wenn Ihre Organisation Service Control Policies (SCPs) zur Verwaltung von Berechtigungen verwendet.

Mindestabkühlungszeitraum für die Auto-Tiering-Richtlinie

Wenn Sie das Daten-Tiering auf einem Volume mithilfe der *auto*-Tiering-Richtlinie aktiviert haben, können Sie jetzt die Mindestkühlperiode mithilfe der API anpassen.

"Erfahren Sie, wie Sie die Mindestkühlzeit anpassen."

Verbesserung der benutzerdefinierten Exportrichtlinien

Wenn Sie ein neues NFS-Volume erstellen, zeigt BlueXP jetzt benutzerdefinierte Exportrichtlinien in aufsteigender Reihenfolge an, sodass Sie die benötigte Exportrichtlinie leichter finden können.

Löschen alter Cloud-Snapshots

BlueXP löscht jetzt ältere Cloud-Snapshots von Root- und Boot-Festplatten, die beim Bereitstellen eines Cloud Volumes ONTAP Systems und bei jedem Herunterfahren erstellt werden. Sowohl für das Root- als auch für das Boot-Volume werden nur die beiden aktuellsten Snapshots beibehalten.

Diese Verbesserung trägt dazu bei, die Kosten des Cloud-Anbieters zu senken, indem nicht mehr benötigte Snapshots entfernt werden.

Beachten Sie, dass ein Connector eine neue Berechtigung zum Löschen von Azure-Snapshots benötigt. "Aktuelle Connector-Richtlinie für Azure anzeigen" .

```
"Microsoft.Compute/snapshots/delete"
```

24. Mai 2021

Cloud Volumes ONTAP 9.9.1

BlueXP kann jetzt Cloud Volumes ONTAP 9.9.1 bereitstellen und verwalten.

"Erfahren Sie mehr über die neuen Funktionen dieser Version von Cloud Volumes ONTAP" .

11. April 2021

Die folgenden Änderungen wurden mit der Version 3.9.5 des Connectors eingeführt.

Logische Speicherplatzberichterstattung

BlueXP ermöglicht jetzt die logische Speicherplatzberichterstattung auf der anfänglichen Speicher-VM, die es für Cloud Volumes ONTAP erstellt.

Wenn der Speicherplatz logisch gemeldet wird, meldet ONTAP den Volume-Speicherplatz so, dass der gesamte durch die Speichereffizienzfunktionen eingesparte physische Speicherplatz auch als verwendet gemeldet wird.

Unterstützung für GP3-Festplatten in AWS

Cloud Volumes ONTAP unterstützt ab Version 9.7 jetzt General Purpose SSD (gp3)-Festplatten. gp3-Festplatten sind die kostengünstigsten SSDs, die Kosten und Leistung für ein breites Spektrum von Workloads ausbalancieren.

"Dimensionieren Sie Ihr System in AWS" .

Cold HDD-Festplatten werden in AWS nicht mehr unterstützt

Cloud Volumes ONTAP unterstützt keine Cold HDD-Festplatten (sc1) mehr.

TLS 1.2 für Azure-Speicherkonten

Wenn BlueXP Speicherkonten in Azure für Cloud Volumes ONTAP erstellt, ist die TLS-Version für das Speicherkonto jetzt Version 1.2.

08. März 2021

Die folgenden Änderungen wurden mit der Version 3.9.4 des Connectors eingeführt.

Cloud Volumes ONTAP 9.9.0

BlueXP kann jetzt Cloud Volumes ONTAP 9.9.0 bereitstellen und verwalten.

"Erfahren Sie mehr über die neuen Funktionen dieser Version von Cloud Volumes ONTAP" .

Unterstützung für die AWS C2S-Umgebung

Sie können Cloud Volumes ONTAP 9.8 jetzt in der AWS Commercial Cloud Services (C2S)-Umgebung bereitstellen.

"Stellen Sie Cloud Volumes ONTAP in AWS Secret Cloud oder AWS Top Secret Cloud bereit" .

AWS-Verschlüsselung mit kundenverwalteten CMKs

BlueXP ermöglichte Ihnen schon immer die Verschlüsselung von Cloud Volumes ONTAP -Daten mithilfe des AWS Key Management Service (KMS). Ab Cloud Volumes ONTAP 9.9.0 werden Daten auf EBS-Festplatten und auf S3 gestaffelte Daten verschlüsselt, wenn Sie einen vom Kunden verwalteten CMK auswählen. Bisher wurden nur EBS-Daten verschlüsselt.

Beachten Sie, dass Sie der Cloud Volumes ONTAP IAM-Rolle Zugriff gewähren müssen, um den CMK zu verwenden.

"Erfahren Sie mehr über die Einrichtung des AWS KMS mit Cloud Volumes ONTAP" .

Unterstützung für Azure DoD

Sie können Cloud Volumes ONTAP 9.8 jetzt im Azure Department of Defense (DoD) Impact Level 6 (IL6) bereitstellen.

Reduzierung der IP-Adresse in Google Cloud

Wir haben die Anzahl der IP-Adressen reduziert, die für Cloud Volumes ONTAP 9.8 und höher in Google Cloud erforderlich sind. Standardmäßig ist eine IP-Adresse weniger erforderlich (wir haben das Intercluster-LIF mit dem Node-Management-LIF vereinheitlicht). Sie haben auch die Möglichkeit, die Erstellung des SVM-Verwaltungs-LIF bei Verwendung der API zu überspringen, wodurch der Bedarf an einer zusätzlichen IP-Adresse reduziert würde.

"Weitere Informationen zu den IP-Adressanforderungen in Google Cloud" .

Shared VPC-Unterstützung in Google Cloud

Wenn Sie ein Cloud Volumes ONTAP HA-Paar in Google Cloud bereitstellen, können Sie jetzt gemeinsam genutzte VPCs für VPC-1, VPC-2 und VPC-3 auswählen. Bisher konnte nur VPC-0 ein gemeinsam genutztes VPC sein. Diese Änderung wird mit Cloud Volumes ONTAP 9.8 und höher unterstützt.

"Weitere Informationen zu den Netzwerkanforderungen von Google Cloud" .

04. Januar 2021

Die folgenden Änderungen wurden mit der Version 3.9.2 des Connectors eingeführt.

AWS-Außenposten

Vor einigen Monaten haben wir bekannt gegeben, dass Cloud Volumes ONTAP die Auszeichnung „Outposts Ready“ von Amazon Web Services (AWS) erhalten hat. Wir freuen uns, heute bekannt geben zu können, dass wir BlueXP und Cloud Volumes ONTAP mit AWS Outposts validiert haben.

Wenn Sie über einen AWS Outpost verfügen, können Sie Cloud Volumes ONTAP in diesem Outpost bereitstellen, indem Sie im Arbeitsumgebungsassistenten den Outpost VPC auswählen. Die Erfahrung ist die gleiche wie bei jedem anderen VPC, das sich in AWS befindet. Beachten Sie, dass Sie zuerst einen Connector in Ihrem AWS Outpost bereitstellen müssen.

Es gibt einige Einschränkungen, auf die hingewiesen werden muss:

- Derzeit werden nur Cloud Volumes ONTAP -Systeme mit einem Knoten unterstützt
- Die EC2-Instanzen, die Sie mit Cloud Volumes ONTAP verwenden können, sind auf das beschränkt, was

in Ihrem Outpost verfügbar ist

- Derzeit werden nur General Purpose SSDs (gp2) unterstützt

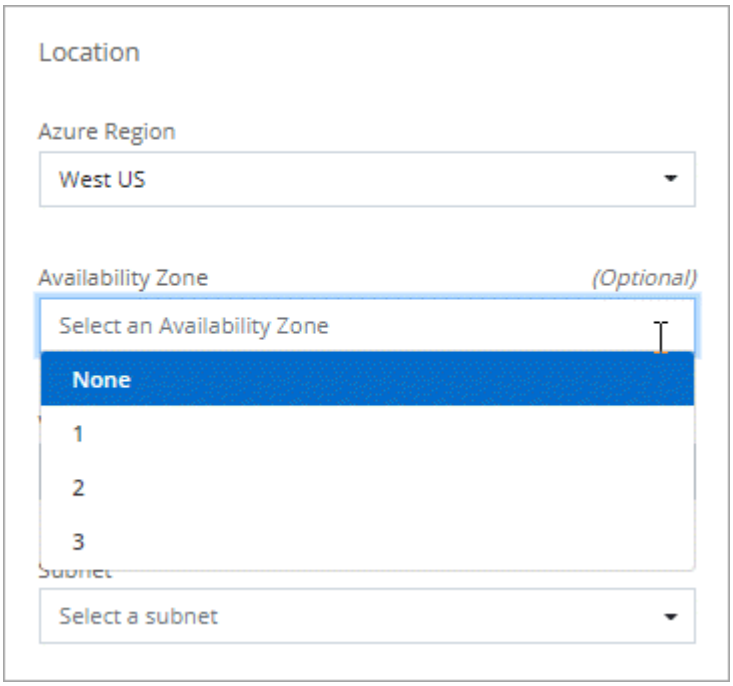
Ultra SSD VNVRAM in unterstützten Azure-Regionen

Cloud Volumes ONTAP kann jetzt eine Ultra SSD als VNVRAM verwenden, wenn Sie den VM-Typ E32s_v3 mit einem Einzelknotensystem verwenden "in jeder unterstützten Azure-Region".

VNVRAM bietet eine bessere Schreibleistung.

Auswählen einer Verfügbarkeitszone in Azure

Sie können jetzt die Availability Zone auswählen, in der Sie ein Cloud Volumes ONTAP -System mit einem einzelnen Knoten bereitstellen möchten. Wenn Sie keine AZ auswählen, wählt BlueXP eine für Sie aus.



Größere Festplatten in Google Cloud

Cloud Volumes ONTAP unterstützt jetzt 64 TB Festplatten in Google Cloud.

Die maximale Systemkapazität mit Festplatten allein bleibt aufgrund von Google Cloud-Beschränkungen bei 256 TB.

Neue Maschinentypen in Google Cloud

Cloud Volumes ONTAP unterstützt jetzt die folgenden Maschinentypen:

- n2-standard-4 mit der Explore-Lizenz und mit BYOL
- n2-standard-8 mit der Standardlizenz und mit BYOL
- n2-standard-32 mit der Premium-Lizenz und mit BYOL

03. November 2020

Die folgenden Änderungen wurden mit der Version 3.9.0 des Connectors eingeführt.

Azure Private Link für Cloud Volumes ONTAP

Standardmäßig aktiviert BlueXP jetzt eine Azure Private Link-Verbindung zwischen Cloud Volumes ONTAP und den zugehörigen Speicherkonten. Ein privater Link sichert Verbindungen zwischen Endpunkten in Azure.

- "Weitere Informationen zu Azure Private Links"
- "Erfahren Sie mehr über die Verwendung eines Azure Private Link mit Cloud Volumes ONTAP"

Bekannte Einschränkungen

Bekannte Einschränkungen kennzeichnen Plattformen, Geräte oder Funktionen, die von dieser Produktversion nicht unterstützt werden oder nicht ordnungsgemäß mit ihr zusammenarbeiten. Lesen Sie diese Einschränkungen sorgfältig durch.

Diese Einschränkungen gelten speziell für die Verwaltung von Cloud Volumes ONTAP in der NetApp Console. Um Einschränkungen der Cloud Volumes ONTAP -Software selbst anzuzeigen, "Gehen Sie zu den Versionshinweisen zu Cloud Volumes ONTAP" .

Die Konsole unterstützt die Erstellung von FlexGroup -Volumes nicht

Während Cloud Volumes ONTAP FlexGroup Volumes unterstützt, unterstützt die Konsole derzeit nicht die Erstellung von FlexGroup Volumes. Wenn Sie ein FlexGroup -Volume vom ONTAP System Manager oder der ONTAP CLI erstellen, sollten Sie den Kapazitätsverwaltungsmodus in der Konsole auf `Manual` . `Automatic` Der Modus funktioniert möglicherweise nicht richtig mit FlexGroup -Volumes.

Die Möglichkeit, FlexGroup -Volumes in der Konsole zu erstellen, ist für eine zukünftige Version geplant.

Die Konsole unterstützt S3 mit Cloud Volumes ONTAP nicht

Während Cloud Volumes ONTAP S3 als Option für skalierbaren Speicher unterstützt, bietet die Console keine Verwaltungsfunktionen für diese Funktion. Die Verwendung der Befehlszeile ist die empfohlene Vorgehensweise, um den S3-Clientzugriff von Cloud Volumes ONTAP zu konfigurieren. Weitere Informationen finden Sie in der "ONTAP S3 Konfigurationsleitfaden".

"Erfahren Sie mehr über die Unterstützung von ONTAP S3 und anderen Client-Protokollen durch Cloud Volumes ONTAP".

Die Konsole unterstützt keine Notfallwiederherstellung für Speicher-VMs

Die Konsole bietet keine Einrichtungs- oder Orchestrierungsunterstützung für die Notfallwiederherstellung von Storage VMs (SVM). Sie müssen ONTAP System Manager oder die ONTAP CLI verwenden.

"Erfahren Sie mehr über die Notfallwiederherstellung von SVM" .

Versionshinweise zu Cloud Volumes ONTAP

Die Versionshinweise für Cloud Volumes ONTAP enthalten veröffentlichungsspezifische Informationen. Was ist neu in der Version, unterstützte Konfigurationen, Speichergrenzen und alle bekannten Einschränkungen oder Probleme, die die Produktfunktionalität beeinträchtigen können.

"Gehen Sie zu den Versionshinweisen zu Cloud Volumes ONTAP"

Erste Schritte

Erfahren Sie mehr über Cloud Volumes ONTAP

Mit Cloud Volumes ONTAP können Sie Ihre Cloud-Speicherkosten und -Leistung optimieren und gleichzeitig Datenschutz, Sicherheit und Compliance verbessern.

Cloud Volumes ONTAP ist ein reines Software-Speichergerät, das die ONTAP Datenverwaltungssoftware in der Cloud ausführt. Es bietet Speicher der Enterprise-Klasse mit den folgenden Hauptfunktionen:

- Speichereffizienz

  Nutzen Sie die integrierte Datendeduplizierung, Datenkomprimierung, Thin Provisioning und Klonen, um die Speicherkosten zu minimieren.

- Hochverfügbarkeit

  Sorgen Sie für die Zuverlässigkeit Ihres Unternehmens und einen kontinuierlichen Betrieb bei Ausfällen in Ihrer Cloud-Umgebung.

- Datenschutz

  Cloud Volumes ONTAP nutzt SnapMirror, die branchenführende Replikationstechnologie von NetApp, um lokale Daten in die Cloud zu replizieren, sodass sekundäre Kopien für mehrere Anwendungsfälle problemlos verfügbar sind.

  Cloud Volumes ONTAP lässt sich außerdem in NetApp Backup and Recovery integrieren, um Sicherungs- und Wiederherstellungsfunktionen zum Schutz und zur Langzeitarchivierung Ihrer Cloud-Daten bereitzustellen.

  "Erfahren Sie mehr über Backup und Wiederherstellung"

- Daten-Tiering

  Wechseln Sie bei Bedarf zwischen Speicherpools mit hoher und niedriger Leistung, ohne Anwendungen offline zu nehmen.

- Anwendungskonsistenz

  Stellen Sie die Konsistenz von NetApp Snapshot-Kopien mithilfe von NetApp SnapCenter sicher.

  "Erfahren Sie mehr über SnapCenter"

- Datensicherheit

  Cloud Volumes ONTAP unterstützt die Datenverschlüsselung und bietet Schutz vor Viren und Ransomware.

- Kontrollen zur Einhaltung des Datenschutzes

  Durch die Integration mit NetApp Data Classification können Sie den Datenkontext verstehen und vertrauliche Daten identifizieren.

  "Erfahren Sie mehr über die Datenklassifizierung"

Lizenzen für ONTAP -Funktionen sind in Cloud Volumes ONTAP enthalten.

"Unterstützte Cloud Volumes ONTAP -Konfigurationen anzeigen"

"Erfahren Sie mehr über Cloud Volumes ONTAP"

Unterstützte ONTAP -Versionen für Cloud Volumes ONTAP Bereitstellungen

Die NetApp Console ermöglicht Ihnen die Auswahl aus mehreren verschiedenen ONTAP Versionen, wenn Sie ein Cloud Volumes ONTAP -System hinzufügen.

Cloud Volumes ONTAP-Versionen, die hier nicht aufgeführt sind, sind für neue Bereitstellungen nicht verfügbar. Die Patch- oder generische (General Availability) Version in einer hier aufgeführten Version stellt die Basisversion dar, die für die Bereitstellung verfügbar ist. Einzelheiten zu den verfügbaren Patches finden Sie in der "versionierte Versionshinweise" für jede Version.

Informationen zum Upgrade finden Sie unter "Unterstützte Upgradepfade".

AWS

Einzelner Knoten

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8
- 9.7 P5
- 9.5 P6

HA-Paar

- 9.18.1

- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8
- 9.7 P5
- 9.5 P6

Azurblau

Einzelner Knoten

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

HA-Paar

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

Google Cloud

Einzelner Knoten

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8
- 9.7 P5

HA-Paar

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8

Erste Schritte mit Amazon Web Services

Schnellstart für Cloud Volumes ONTAP in AWS

Beginnen Sie in wenigen Schritten mit Cloud Volumes ONTAP in AWS.

1 Erstellen eines Konsolenagenten

Wenn Sie kein "Konsolenagent" Sie müssen jedoch eines erstellen. "Erfahren Sie, wie Sie einen Konsolenagenten in AWS erstellen" .

Beachten Sie: Wenn Sie Cloud Volumes ONTAP in einem Subnetz bereitstellen möchten, in dem kein Internetzugang verfügbar ist, müssen Sie den Konsolenagenten manuell installieren und auf die NetApp Console zugreifen, die auf diesem Konsolenagenten ausgeführt wird. "Erfahren Sie, wie Sie den Konsolenagenten manuell an einem Ort ohne Internetzugang installieren." .

2 Planen Sie Ihre Konfiguration

Die Konsole bietet vorkonfigurierte Pakete, die Ihren Workload-Anforderungen entsprechen, oder Sie können Ihre eigene Konfiguration erstellen. Wenn Sie Ihre eigene Konfiguration auswählen, sollten Sie die Ihnen zur Verfügung stehenden Optionen verstehen. "Mehr erfahren" .

3 Richten Sie Ihr Netzwerk ein

1. Stellen Sie sicher, dass Ihr VPC und Ihre Subnetze die Konnektivität zwischen dem Konsolenagenten und Cloud Volumes ONTAP unterstützen.
2. Aktivieren Sie den ausgehenden Internetzugriff vom Ziel-VPC für NetApp AutoSupport.

   Dieser Schritt ist nicht erforderlich, wenn Sie Cloud Volumes ONTAP an einem Standort bereitstellen, an dem kein Internetzugang verfügbar ist.

3. Richten Sie einen VPC-Endpunkt für den Amazon Simple Storage Service (Amazon S3) Service ein.

   Ein VPC-Endpunkt ist erforderlich, wenn Sie kalte Daten von Cloud Volumes ONTAP auf kostengünstigen Objektspeicher verschieben möchten.

"Erfahren Sie mehr über die Netzwerkanforderungen" .

4 Einrichten des AWS KMS

Wenn Sie die Amazon-Verschlüsselung mit Cloud Volumes ONTAP verwenden möchten, müssen Sie sicherstellen, dass ein aktiver Customer Master Key (CMK) vorhanden ist. Sie müssen auch die Schlüsselrichtlinie für jeden CMK ändern, indem Sie die IAM-Rolle hinzufügen, die dem Konsolenagenten als *Schlüsselbenutzer* Berechtigungen erteilt. "Mehr erfahren" .

5 Starten Sie Cloud Volumes ONTAP über die Konsole

Klicken Sie auf **System hinzufügen**, wählen Sie den Systemtyp aus, den Sie bereitstellen möchten, und

führen Sie die Schritte im Assistenten aus. "Lesen Sie die Schritt-für-Schritt-Anleitung" .

Weiterführende Links

- "Erstellen Sie einen Konsolenagenten für AWS"
- "Erstellen Sie einen Konsolenagenten aus dem AWS Marketplace"
- "Installieren und Einrichten eines Konsolenagenten vor Ort"
- "AWS-Berechtigungen für den Konsolenagenten"

Planen Sie Ihre Cloud Volumes ONTAP Konfiguration in AWS

Wenn Sie Cloud Volumes ONTAP in AWS bereitstellen, können Sie ein vorkonfiguriertes System auswählen, das Ihren Workload-Anforderungen entspricht, oder Sie können Ihre eigene Konfiguration erstellen. Wenn Sie Ihre eigene Konfiguration auswählen, sollten Sie die Ihnen zur Verfügung stehenden Optionen verstehen.

Wählen Sie eine Cloud Volumes ONTAP -Lizenz

Für Cloud Volumes ONTAP sind mehrere Lizenzierungsoptionen verfügbar. Jede Option ermöglicht Ihnen die Auswahl eines Verbrauchsmodells, das Ihren Anforderungen entspricht.

- "Erfahren Sie mehr über die Lizenzierungsoptionen für Cloud Volumes ONTAP"
- "Erfahren Sie, wie Sie die Lizenzierung einrichten"

Wählen Sie eine unterstützte Region

Cloud Volumes ONTAP wird in den meisten AWS-Regionen unterstützt. "Vollständige Liste der unterstützten Regionen anzeigen" .

Neuere AWS-Regionen müssen aktiviert werden, bevor Sie Ressourcen in diesen Regionen erstellen und verwalten können. "AWS-Dokumentation: Erfahren Sie, wie Sie eine Region aktivieren" .

Wählen Sie eine unterstützte lokale Zone

Die Auswahl einer lokalen Zone ist optional. Cloud Volumes ONTAP wird in einigen AWS Local Zones, einschließlich Singapur, unterstützt. Cloud Volumes ONTAP in AWS unterstützt nur den Hochverfügbarkeitsmodus (HA) in einer einzelnen Verfügbarkeitszone. Bereitstellungen mit einem einzelnen Knoten werden nicht unterstützt.

> Cloud Volumes ONTAP bietet keine Unterstützung für Daten-Tiering und Cloud-Tiering in AWS Local Zones. Darüber hinaus werden lokale Zonen mit Instanzen, die nicht für Cloud Volumes ONTAP qualifiziert wurden, nicht unterstützt. Ein Beispiel hierfür ist Miami, das nicht als lokale Zone verfügbar ist, da es nur Gen6-Instanzen enthält, die nicht unterstützt und nicht qualifiziert sind.

"AWS-Dokumentation: Vollständige Liste der lokalen Zonen anzeigen" . Lokale Zonen müssen aktiviert werden, bevor Sie Ressourcen in diesen Zonen erstellen und verwalten können.

"AWS-Dokumentation: Erste Schritte mit AWS Local Zones" .

Wählen Sie eine unterstützte Instanz

Cloud Volumes ONTAP unterstützt je nach gewähltem Lizenztyp mehrere Instanztypen.

"Unterstützte Konfigurationen für Cloud Volumes ONTAP in AWS"

Speichergrenzen verstehen

Die Rohkapazitätsgrenze für ein Cloud Volumes ONTAP System ist an die Lizenz gebunden. Zusätzliche Beschränkungen wirken sich auf die Größe von Aggregaten und Volumina aus. Sie sollten sich dieser Beschränkungen bewusst sein, wenn Sie Ihre Konfiguration planen.

"Speicherlimits für Cloud Volumes ONTAP in AWS"

Dimensionieren Sie Ihr System in AWS

Durch die Dimensionierung Ihres Cloud Volumes ONTAP -Systems können Sie die Anforderungen an Leistung und Kapazität erfüllen. Bei der Auswahl eines Instanztyps, Datenträgertyps und einer Datenträgergröße sollten Sie einige wichtige Punkte beachten:

Instanztyp

- Passen Sie Ihre Workload-Anforderungen an den maximalen Durchsatz und die IOPS für jeden EC2-Instance-Typ an.
- Wenn mehrere Benutzer gleichzeitig in das System schreiben, wählen Sie einen Instanztyp, der über genügend CPUs verfügt, um die Anforderungen zu verwalten.
- Wenn Sie eine Anwendung haben, die hauptsächlich aus Lesevorgängen besteht, wählen Sie ein System mit ausreichend RAM.
  - "AWS-Dokumentation: Amazon EC2-Instanztypen"
  - "AWS-Dokumentation: Amazon EBS-optimierte Instances"

EBS-Festplattentyp

Im Großen und Ganzen sind die Unterschiede zwischen den EBS-Festplattentypen wie folgt. Weitere Informationen zu den Anwendungsfällen für EBS-Festplatten finden Sie unter "AWS-Dokumentation: EBS-Volume-Typen" .

- *General Purpose SSD (gp3)*-Festplatten sind die kostengünstigsten SSDs, die Kosten und Leistung für eine breite Palette von Arbeitslasten ausbalancieren. Die Leistung wird in Bezug auf IOPS und Durchsatz definiert. GP3-Festplatten werden mit Cloud Volumes ONTAP 9.7 und höher unterstützt.

  Wenn Sie eine GP3-Festplatte auswählen, trägt die NetApp Console Standard-IOPS- und Durchsatzwerte ein, die basierend auf der ausgewählten Festplattengröße eine Leistung bieten, die einer GP2-Festplatte entspricht. Sie können die Werte erhöhen, um zu einem höheren Preis eine bessere Leistung zu erzielen. Niedrigere Werte werden von uns jedoch nicht unterstützt, da dies zu einer schlechteren Leistung führen kann. Kurz gesagt: Bleiben Sie bei den Standardwerten oder erhöhen Sie sie. Senken Sie sie nicht. "AWS-Dokumentation: Erfahren Sie mehr über GP3-Festplatten und ihre Leistung" .

  Beachten Sie, dass Cloud Volumes ONTAP die Amazon EBS Elastic Volumes-Funktion mit GP3-Festplatten unterstützt. "Erfahren Sie mehr über die Unterstützung von Elastic Volumes" .

- *General Purpose SSD (gp2)*-Festplatten bieten ein ausgewogenes Verhältnis von Kosten und Leistung für eine breite Palette von Arbeitslasten. Die Leistung wird in IOPS definiert.

- *Provisioned IOPS SSD (io1)*-Festplatten sind für kritische Anwendungen gedacht, die höchste Leistung zu höheren Kosten erfordern.

  Beachten Sie, dass Cloud Volumes ONTAP die Amazon EBS Elastic Volumes-Funktion mit io1-Festplatten unterstützt. "Erfahren Sie mehr über die Unterstützung von Elastic Volumes" .

- *Durchsatzoptimierte HDD (st1)*-Festplatten sind für häufig aufgerufene Workloads gedacht, die einen schnellen und konsistenten Durchsatz zu einem niedrigeren Preis erfordern.

> Data Tiering zu Amazon Simple Storage Service (Amazon S3) wird nicht unterstützt, wenn sich Ihr Cloud Volumes ONTAP System in einer AWS Local Zone befindet, da der Zugriff auf die Amazon S3 Buckets außerhalb der Local Zone eine höhere Latenz verursacht und die Aktivitäten von Cloud Volumes ONTAP beeinträchtigt.

EBS-Festplattengröße

Wenn Sie eine Konfiguration wählen, die das"Amazon EBS Elastic Volumes-Funktion" , dann müssen Sie beim Starten eines Cloud Volumes ONTAP Systems eine anfängliche Festplattengröße auswählen. Danach können Sie"Überlassen Sie der Konsole die Verwaltung der Systemkapazität" , aber wenn Sie möchten"Aggregate selbst erstellen" , beachten Sie Folgendes:

- Alle Festplatten in einem Aggregat müssen die gleiche Größe haben.
- Die Leistung von EBS-Festplatten ist an die Festplattengröße gebunden. Die Größe bestimmt die Basis-IOPS und die maximale Burst-Dauer für SSD-Festplatten sowie den Basis- und Burst-Durchsatz für HDD-Festplatten.
- Letztendlich sollten Sie die Festplattengröße wählen, die Ihnen die benötigte *dauerhafte Leistung* bietet.
- Selbst wenn Sie größere Festplatten wählen (z. B. sechs 4-TiB-Festplatten), erhalten Sie möglicherweise nicht alle IOPS, da die EC2-Instanz ihr Bandbreitenlimit erreichen kann.

  Weitere Einzelheiten zur EBS-Festplattenleistung finden Sie unter "AWS-Dokumentation: EBS-Volume-Typen" .

  Wie oben erwähnt, wird die Auswahl einer Datenträgergröße bei Cloud Volumes ONTAP -Konfigurationen, die die Funktion „Amazon EBS Elastic Volumes“ unterstützen, nicht unterstützt. "Erfahren Sie mehr über die Unterstützung von Elastic Volumes" .

Standardsystemfestplatten anzeigen

Zusätzlich zum Speicher für Benutzerdaten erwirbt die Konsole auch Cloud-Speicher für Cloud Volumes ONTAP -Systemdaten (Boot-Daten, Root-Daten, Core-Daten und NVRAM). Zu Planungszwecken kann es hilfreich sein, diese Details zu überprüfen, bevor Sie Cloud Volumes ONTAP bereitstellen.

"Standardfestplatten für Cloud Volumes ONTAP Systemdaten in AWS anzeigen" .

> Der Konsolenagent benötigt außerdem eine Systemfestplatte. "Details zur Standardkonfiguration des Konsolenagenten anzeigen" .

Bereiten Sie die Bereitstellung von Cloud Volumes ONTAP in einem AWS Outpost vor

Wenn Sie über einen AWS Outpost verfügen, können Sie Cloud Volumes ONTAP in diesem Outpost bereitstellen, indem Sie während des Bereitstellungsprozesses die Outpost VPC auswählen. Die Erfahrung ist die gleiche wie bei jedem anderen VPC, das sich in AWS befindet. Beachten Sie, dass Sie zuerst einen

Konsolenagenten in Ihrem AWS Outpost bereitstellen müssen.

Es gibt einige Einschränkungen, auf die hingewiesen werden muss:

- Derzeit werden nur Cloud Volumes ONTAP -Systeme mit einem Knoten unterstützt
- Die EC2-Instanzen, die Sie mit Cloud Volumes ONTAP verwenden können, sind auf das beschränkt, was in Ihrem Outpost verfügbar ist
- Derzeit werden nur General Purpose SSDs (gp2) unterstützt

Sammeln von Netzwerkinformationen

Wenn Sie Cloud Volumes ONTAP in AWS starten, müssen Sie Details zu Ihrem VPC-Netzwerk angeben. Sie können ein Arbeitsblatt verwenden, um die Informationen von Ihrem Administrator zu sammeln.

Einzelner Knoten oder HA-Paar in einer einzelnen AZ

AWS-Informationen	Ihr Wert
Region	
VPC	
Subnetz	
Sicherheitsgruppe (falls Sie Ihre eigene verwenden)	

HA-Paar in mehreren AZs

AWS-Informationen	Ihr Wert
Region	
VPC	
Sicherheitsgruppe (falls Sie Ihre eigene verwenden)	
Verfügbarkeitszone Knoten 1	
Knoten 1-Subnetz	
Verfügbarkeitszone Knoten 2	
Knoten 2-Subnetz	
Mediator-Verfügbarkeitszone	
Mediator-Subnetz	
Schlüsselpaar für den Mediator	
Floating-IP-Adresse für den Cluster-Verwaltungsport	
Floating-IP-Adresse für Daten auf Knoten 1	
Floating-IP-Adresse für Daten auf Knoten 2	

AWS-Informationen	Ihr Wert
Routentabellen für Floating-IP-Adressen	

Wählen Sie eine Schreibgeschwindigkeit

Über die Konsole können Sie eine Schreibgeschwindigkeitseinstellung für Cloud Volumes ONTAP auswählen. Bevor Sie eine Schreibgeschwindigkeit auswählen, sollten Sie die Unterschiede zwischen den normalen und hohen Einstellungen sowie die Risiken und Empfehlungen bei der Verwendung einer hohen Schreibgeschwindigkeit verstehen. "Erfahren Sie mehr über die Schreibgeschwindigkeit" .

Auswählen eines Volume-Nutzungsprofils

ONTAP umfasst mehrere Speichereffizienzfunktionen, die die von Ihnen benötigte Gesamtspeichermenge reduzieren können. Wenn Sie in der Konsole ein Volume erstellen, können Sie ein Profil auswählen, das diese Funktionen aktiviert, oder ein Profil, das sie deaktiviert. Sie sollten mehr über diese Funktionen erfahren, um zu entscheiden, welches Profil Sie verwenden möchten.

Die Storage-Effizienzfunktionen von NetApp bieten folgende Vorteile:

Dünne Bereitstellung

Bietet Hosts oder Benutzern mehr logischen Speicher, als Sie tatsächlich in Ihrem physischen Speicherpool haben. Anstatt Speicherplatz vorab zuzuweisen, wird Speicherplatz jedem Volume dynamisch zugewiesen, während Daten geschrieben werden.

Deduplizierung

Verbessert die Effizienz, indem identische Datenblöcke lokalisiert und durch Verweise auf einen einzigen gemeinsamen Block ersetzt werden. Diese Technik reduziert den Speicherkapazitätsbedarf, indem redundante Datenblöcke, die sich auf demselben Datenträger befinden, eliminiert werden.

Komprimierung

Reduziert die zum Speichern von Daten erforderliche physische Kapazität durch Komprimieren von Daten innerhalb eines Volumes auf Primär-, Sekundär- und Archivspeicher.

Richten Sie Ihr Netzwerk ein

AWS-Netzwerk für Cloud Volumes ONTAP einrichten

Die NetApp Console übernimmt die Einrichtung von Netzwerkkomponenten für Cloud Volumes ONTAP, wie z. B. IP-Adressen, Netzmasken und Routen. Sie müssen sicherstellen, dass ausgehender Internetzugang verfügbar ist, dass genügend private IP-Adressen verfügbar sind, dass die richtigen Verbindungen vorhanden sind und mehr.

Allgemeine Anforderungen

Stellen Sie sicher, dass Sie die folgenden Anforderungen in AWS erfüllt haben.

Ausgehender Internetzugang für Cloud Volumes ONTAP -Knoten

Cloud Volumes ONTAP -Systeme erfordern ausgehenden Internetzugang für den Zugriff auf externe Endpunkte für verschiedene Funktionen. Cloud Volumes ONTAP kann nicht ordnungsgemäß funktionieren, wenn diese Endpunkte in Umgebungen mit strengen Sicherheitsanforderungen blockiert sind.

Der Konsolenagent kontaktiert für den täglichen Betrieb mehrere Endpunkte. Informationen zu den verwendeten Endpunkten finden Sie unter "Vom Konsolenagenten kontaktierte Endpunkte anzeigen" Und "Vorbereiten des Netzwerks für die Verwendung der Konsole" .

Cloud Volumes ONTAP Endpunkte

Cloud Volumes ONTAP verwendet diese Endpunkte zur Kommunikation mit verschiedenen Diensten.

Endpunkte	Gilt für	Zweck	Bereitstellungsmodi	Auswirkungen, wenn der Endpunkt nicht verfügbar ist
https://netapp-cloud-account.auth0.com	Authentifizierung	Wird zur Authentifizierung in der Konsole verwendet.	Standard- und eingeschränkte Modi.	Die Benutzerauthentifizierung schlägt fehl und die folgenden Dienste sind weiterhin nicht verfügbar: • Cloud Volumes ONTAP Dienste • ONTAP -Dienste • Protokolle und Proxy-Dienste
https://api.bluexp.netapp.com/tenancy	Mietverhältnis	Wird verwendet, um Cloud Volumes ONTAP -Ressourcen von der Konsole abzurufen, um Ressourcen und Benutzer zu autorisieren.	Standard- und eingeschränkte Modi.	Cloud Volumes ONTAP Ressourcen und die Benutzer sind nicht autorisiert.
https://mysupport.netapp.com/aods/asupmessage https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Wird verwendet, um AutoSupport Telemetriedaten an den NetApp Support zu senden.	Standard- und eingeschränkte Modi.	AutoSupport -Informationen bleiben unversehrt.

Endpunkte	Gilt für	Zweck	Bereitstellungsmodi	Auswirkungen, wenn der Endpunkt nicht verfügbar ist
Der genaue kommerzielle Endpunkt für den AWS-Dienst (mit dem Zusatz `amazonaws.com`) hängt von der von Ihnen verwendeten AWS-Region ab. Weitere Informationen finden Sie im "AWS-Dokumentation für Details" .	• CloudFormation • Elastische Compute Cloud (EC2) • Identitäts- und Zugriffsverwaltung (IAM) • Schlüsselverwaltungsdienst (KMS) • Sicherheitstokendienst (STS) • Amazon Simple Storage Service (S3)	Kommunikation mit AWS-Diensten.	Standard- und Privatmodus.	Cloud Volumes ONTAP kann nicht mit dem AWS-Dienst kommunizieren, um bestimmte Vorgänge in AWS auszuführen.
Der genaue Regierungsendpunkt für den AWS-Dienst hängt von der von Ihnen verwendeten AWS-Region ab. Die Endpunkte werden mit dem Suffix `amazonaws.com` Und `c2s.ic.gov` . Siehe "AWS SDK" Und "AWS-Dokumentation" für weitere Informationen.	• CloudFormation • Elastische Compute Cloud (EC2) • Identitäts- und Zugriffsverwaltung (IAM) • Schlüsselverwaltungsdienst (KMS) • Sicherheitstokendienst (STS) • Einfacher Speicherdienst (S3)	Kommunikation mit AWS-Diensten.	Eingeschränkter Modus.	Cloud Volumes ONTAP kann nicht mit dem AWS-Dienst kommunizieren, um bestimmte Vorgänge in AWS auszuführen.

Ausgehender Internetzugang für den HA-Mediator

Die HA-Mediatorinstanz muss über eine ausgehende Verbindung zum AWS EC2-Dienst verfügen, damit sie beim Speicherfailover helfen kann. Um die Verbindung bereitzustellen, können Sie eine öffentliche IP-Adresse hinzufügen, einen Proxyserver angeben oder eine manuelle Option verwenden.

Die manuelle Option kann ein NAT-Gateway oder ein Schnittstellen-VPC-Endpunkt vom Zielsubnetz zum AWS EC2-Dienst sein. Weitere Informationen zu VPC-Endpunkten finden Sie im "AWS-Dokumentation: Schnittstelle

für VPC-Endpunkte (AWS PrivateLink)" .

Netzwerkproxykonfiguration des NetApp Console Agenten

Sie können die Proxyserverkonfiguration des NetApp Console Agenten verwenden, um ausgehenden Internetzugriff von Cloud Volumes ONTAP zu aktivieren. Die Konsole unterstützt zwei Arten von Proxys:

- **Expliziter Proxy**: Der ausgehende Datenverkehr von Cloud Volumes ONTAP verwendet die HTTP-Adresse des Proxyservers, der während der Proxykonfiguration des Konsolenagenten angegeben wurde. Der Administrator hat möglicherweise auch Benutzeranmeldeinformationen und Stammzertifizierungsstellenzertifikate für eine zusätzliche Authentifizierung konfiguriert. Wenn ein Stamm-CA-Zertifikat für den expliziten Proxy verfügbar ist, stellen Sie sicher , dass Sie dasselbe Zertifikat erhalten und mithilfe des "ONTAP CLI: Sicherheitszertifikat installieren" Befehl.
- **Transparenter Proxy**: Das Netzwerk ist so konfiguriert, dass ausgehender Datenverkehr von Cloud Volumes ONTAP automatisch über den Proxy für den Konsolenagenten geleitet wird. Beim Einrichten eines transparenten Proxys muss der Administrator für die Konnektivität von Cloud Volumes ONTAP nur ein Stamm-CA-Zertifikat bereitstellen, nicht die HTTP-Adresse des Proxyservers. Stellen Sie sicher, dass Sie dasselbe Stamm-CA-Zertifikat erhalten und auf Ihr Cloud Volumes ONTAP System hochladen, indem Sie das "ONTAP CLI: Sicherheitszertifikat installieren" Befehl.

Informationen zum Konfigurieren von Proxy-Servern finden Sie im "Konfigurieren des Konsolenagenten zur Verwendung eines Proxyservers" .

Private IP-Adressen

Die Konsole weist Cloud Volumes ONTAP automatisch die erforderliche Anzahl privater IP-Adressen zu. Sie müssen sicherstellen, dass in Ihrem Netzwerk genügend private IP-Adressen verfügbar sind.

Die Anzahl der LIFs, die die Console für Cloud Volumes ONTAP bereitstellt, hängt davon ab, ob Sie ein Single-Node-System oder ein HA-Paar bereitstellen. Ein LIF ist eine IP-Adresse, die einem physischen Port zugeordnet ist.

IP-Adressen für ein Einzelknotensystem

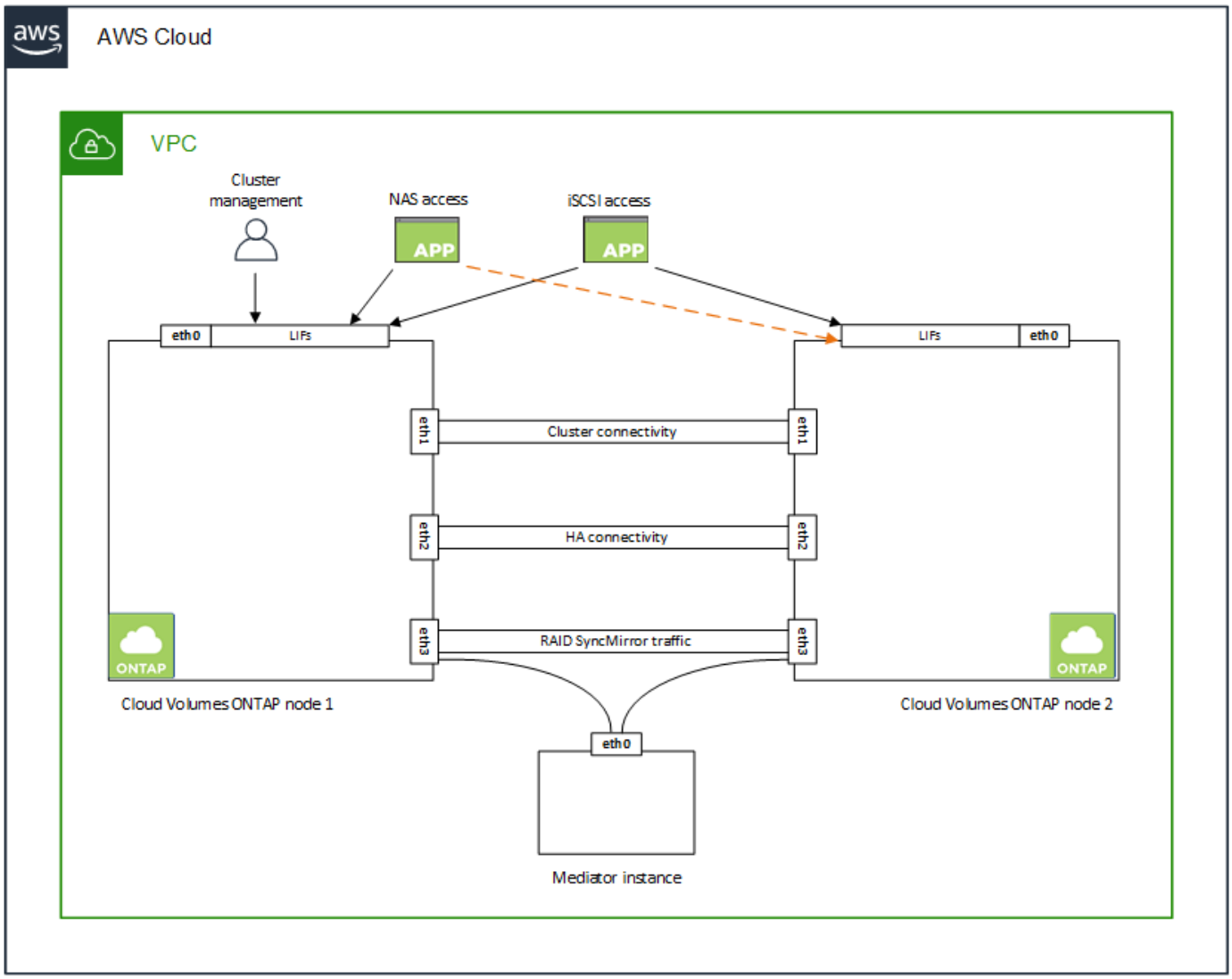
Die Konsole weist einem Einzelknotensystem 6 IP-Adressen zu.

Die folgende Tabelle enthält Details zu den LIFs, die jeder privaten IP-Adresse zugeordnet sind.

LIF	Zweck
Clusterverwaltung	Administrative Verwaltung des gesamten Clusters (HA-Paar).
Knotenverwaltung	Administrative Verwaltung eines Knotens.
Intercluster	Clusterübergreifende Kommunikation, Sicherung und Replikation.
NAS-Daten	Clientzugriff über NAS-Protokolle.
iSCSI-Daten	Clientzugriff über das iSCSI-Protokoll. Wird vom System auch für andere wichtige Netzwerk-Workflows verwendet. Dieses LIF ist erforderlich und sollte nicht gelöscht werden.
Speicher-VM-Verwaltung	Ein Storage-VM-Management-LIF wird mit Verwaltungstools wie SnapCenter verwendet.

IP-Adressen für HA-Paare

HA-Paare benötigen mehr IP-Adressen als ein Einzelknotensystem. Diese IP-Adressen sind auf verschiedene Ethernet-Schnittstellen verteilt, wie in der folgenden Abbildung dargestellt:



Die Anzahl der für ein HA-Paar erforderlichen privaten IP-Adressen hängt davon ab, welches Bereitstellungsmodell Sie wählen. Ein in einer *einzelnen* AWS Availability Zone (AZ) bereitgestelltes HA-Paar erfordert 15 private IP-Adressen, während ein in *mehreren* AZs bereitgestelltes HA-Paar 13 private IP-Adressen erfordert.

Die folgenden Tabellen enthalten Details zu den LIFs, die jeder privaten IP-Adresse zugeordnet sind.

LIF	Schnittstelle	Node	Zweck
Clusterverwaltung	eth0	Knoten 1	Administrative Verwaltung des gesamten Clusters (HA-Paar).
Knotenverwaltung	eth0	Knoten 1 und Knoten 2	Administrative Verwaltung eines Knotens.
Intercluster	eth0	Knoten 1 und Knoten 2	Clusterübergreifende Kommunikation, Sicherung und Replikation.

LIF	Schnittstelle	Node	Zweck
NAS-Daten	eth0	Knoten 1	Clientzugriff über NAS-Protokolle.
iSCSI-Daten	eth0	Knoten 1 und Knoten 2	Clientzugriff über das iSCSI-Protokoll. Wird vom System auch für andere wichtige Netzwerk-Workflows verwendet. Diese LIFs sind erforderlich und sollten nicht gelöscht werden.
Cluster-Konnektivität	eth1	Knoten 1 und Knoten 2	Ermöglicht den Knoten, miteinander zu kommunizieren und Daten innerhalb des Clusters zu verschieben.
HA-Konnektivität	eth2	Knoten 1 und Knoten 2	Kommunikation zwischen den beiden Knoten im Falle eines Failovers.
RSM-iSCSI-Datenverkehr	eth3	Knoten 1 und Knoten 2	RAID SyncMirror iSCSI-Verkehr sowie Kommunikation zwischen den beiden Cloud Volumes ONTAP Knoten und dem Mediator.
Vermittler	eth0	Vermittler	Ein Kommunikationskanal zwischen den Knoten und dem Mediator zur Unterstützung bei Speicherübernahme- und -rückgabeprozessen.

LIF	Schnittstelle	Node	Zweck
Knotenverwaltung	eth0	Knoten 1 und Knoten 2	Administrative Verwaltung eines Knotens.
Intercluster	eth0	Knoten 1 und Knoten 2	Clusterübergreifende Kommunikation, Sicherung und Replikation.
iSCSI-Daten	eth0	Knoten 1 und Knoten 2	Clientzugriff über das iSCSI-Protokoll. Diese LIFs verwalten auch die Migration von Floating-IP-Adressen zwischen Knoten. Diese LIFs sind erforderlich und sollten nicht gelöscht werden.
Cluster-Konnektivität	eth1	Knoten 1 und Knoten 2	Ermöglicht den Knoten, miteinander zu kommunizieren und Daten innerhalb des Clusters zu verschieben.
HA-Konnektivität	eth2	Knoten 1 und Knoten 2	Kommunikation zwischen den beiden Knoten im Falle eines Failovers.
RSM-iSCSI-Datenverkehr	eth3	Knoten 1 und Knoten 2	RAID SyncMirror iSCSI-Verkehr sowie Kommunikation zwischen den beiden Cloud Volumes ONTAP Knoten und dem Mediator.
Vermittler	eth0	Vermittler	Ein Kommunikationskanal zwischen den Knoten und dem Mediator zur Unterstützung bei Speicherübernahme- und -rückgabeprozessen.

Bei der Bereitstellung in mehreren Availability Zones sind mehrere LIFs verknüpft mit"Floating-IP-Adressen" , die nicht auf das private IP-Limit von AWS angerechnet werden.

Sicherheitsgruppen

Sie müssen keine Sicherheitsgruppen erstellen, da die Konsole dies für Sie erledigt. Wenn Sie Ihre eigene verwenden müssen, lesen Sie"Sicherheitsgruppenregeln" .

Suchen Sie nach Informationen zum Konsolenagenten? "Sicherheitsgruppenregeln für den Konsolenagenten anzeigen"

Verbindung für Daten-Tiering

Wenn Sie EBS als Performance-Tier und Amazon S3 als Capacity-Tier verwenden möchten, müssen Sie sicherstellen, dass Cloud Volumes ONTAP eine Verbindung zu S3 hat. Die beste Möglichkeit, diese Verbindung bereitzustellen, ist die Erstellung eines VPC-Endpunkts für den S3-Dienst. Anweisungen finden Sie unter "AWS-Dokumentation: Erstellen eines Gateway-Endpunkts".

Achten Sie beim Erstellen des VPC-Endpunkts darauf, die Region, VPC und Routentabelle auszuwählen, die der Cloud Volumes ONTAP -Instanz entspricht. Sie müssen auch die Sicherheitsgruppe ändern, um eine ausgehende HTTPS-Regel hinzuzufügen, die den Datenverkehr zum S3-Endpunkt ermöglicht. Andernfalls kann Cloud Volumes ONTAP keine Verbindung zum S3-Dienst herstellen.

Wenn Probleme auftreten, lesen Sie die "AWS Support Knowledge Center: Warum kann ich über einen Gateway-VPC-Endpunkt keine Verbindung zu einem S3-Bucket herstellen?"

Verbindungen zu ONTAP -Systemen

Um Daten zwischen einem Cloud Volumes ONTAP -System in AWS und ONTAP -Systemen in anderen Netzwerken zu replizieren, benötigen Sie eine VPN-Verbindung zwischen dem AWS VPC und dem anderen Netzwerk – beispielsweise Ihrem Unternehmensnetzwerk. Anweisungen hierzu finden Sie im "AWS-Dokumentation: Einrichten einer AWS-VPN-Verbindung" .

DNS und Active Directory für CIFS

Wenn Sie CIFS-Speicher bereitstellen möchten, müssen Sie DNS und Active Directory in AWS einrichten oder Ihr lokales Setup auf AWS erweitern.

Der DNS-Server muss Namensauflösungsdienste für die Active Directory-Umgebung bereitstellen. Sie können DHCP-Optionssätze so konfigurieren, dass der standardmäßige EC2-DNS-Server verwendet wird. Dabei darf es sich nicht um den von der Active Directory-Umgebung verwendeten DNS-Server handeln.

Anweisungen hierzu finden Sie im "AWS-Dokumentation: Active Directory-Domänendienste in der AWS Cloud: Schnellstart-Referenzbereitstellung" .

VPC-Freigabe

Ab der Version 9.11.1 werden Cloud Volumes ONTAP HA-Paare in AWS mit VPC-Sharing unterstützt. Durch die VPC-Freigabe kann Ihre Organisation Subnetze mit anderen AWS-Konten teilen. Um diese Konfiguration zu verwenden, müssen Sie Ihre AWS-Umgebung einrichten und dann das HA-Paar mithilfe der API bereitstellen.

"Erfahren Sie, wie Sie ein HA-Paar in einem gemeinsam genutzten Subnetz bereitstellen" .

Anforderungen für HA-Paare in mehreren AZs

Für Cloud Volumes ONTAP HA-Konfigurationen, die mehrere Availability Zones (AZs) verwenden, gelten zusätzliche AWS-Netzwerkanforderungen. Sie sollten diese Anforderungen überprüfen, bevor Sie ein HA-Paar starten, da Sie die Netzwerkdetails in der Konsole eingeben müssen, wenn Sie ein Cloud Volumes ONTAP -System hinzufügen.

Um zu verstehen, wie HA-Paare funktionieren, lesen Sie"Hochverfügbarkeitspaare" .

Verfügbarkeitszonen

Dieses HA-Bereitstellungsmodell verwendet mehrere AZs, um eine hohe Verfügbarkeit Ihrer Daten sicherzustellen. Sie sollten für jede Cloud Volumes ONTAP -Instanz und die Mediator-Instanz eine dedizierte AZ verwenden, die einen Kommunikationskanal zwischen dem HA-Paar bereitstellt.

In jeder Availability Zone sollte ein Subnetz verfügbar sein.

Floating-IP-Adressen für NAS-Daten und Cluster-/SVM-Verwaltung

HA-Konfigurationen in mehreren AZs verwenden Floating-IP-Adressen, die bei Fehlern zwischen Knoten migrieren. Sie sind von außerhalb der VPC nicht nativ zugänglich, es sei denn, Sie"Einrichten eines AWS Transit Gateways" .

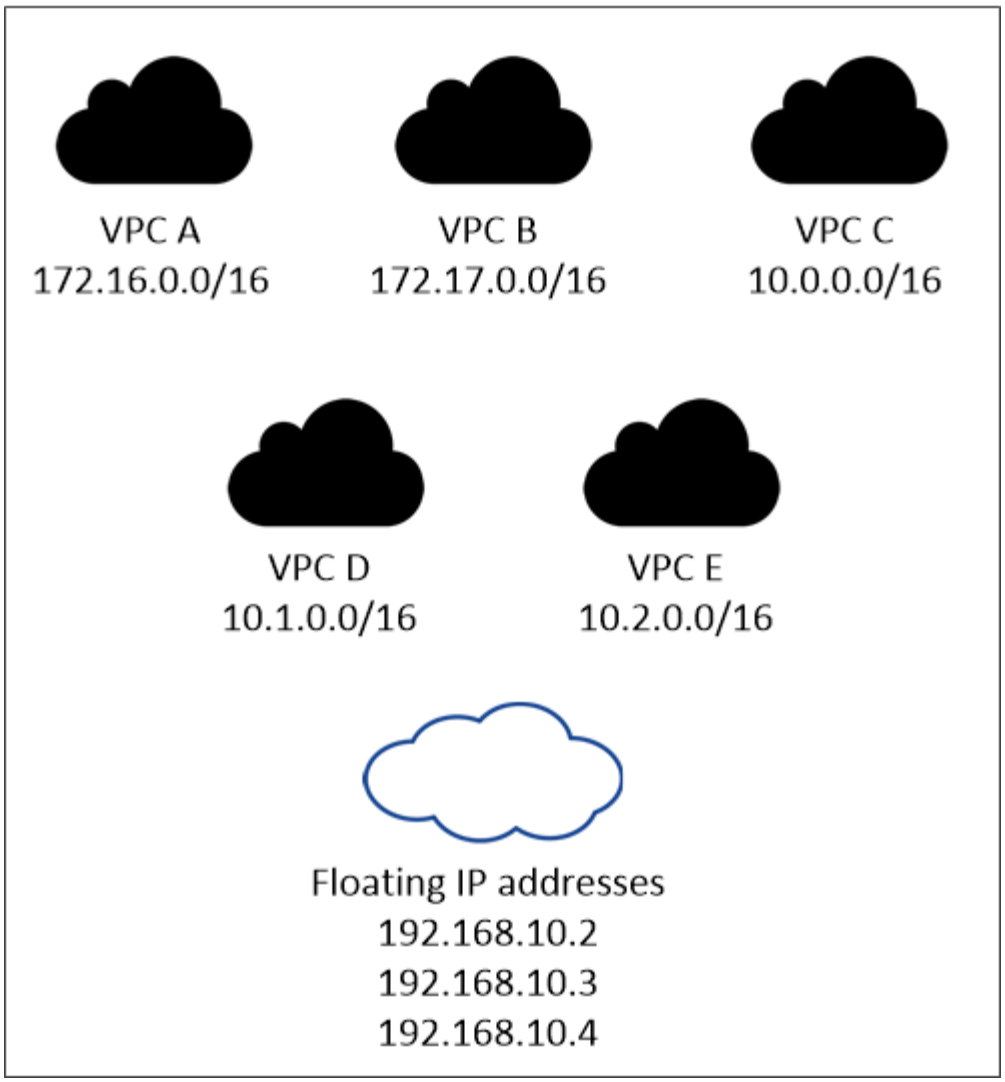
Eine Floating-IP-Adresse dient der Clusterverwaltung, eine für NFS/CIFS-Daten auf Knoten 1 und eine für NFS/CIFS-Daten auf Knoten 2. Eine vierte Floating-IP-Adresse für die SVM-Verwaltung ist optional.

> Wenn Sie SnapDrive für Windows oder SnapCenter mit dem HA-Paar verwenden, ist für das SVM-Verwaltungs-LIF eine Floating-IP-Adresse erforderlich.

Sie müssen die Floating-IP-Adressen eingeben, wenn Sie ein Cloud Volumes ONTAP HA-System hinzufügen. Die Konsole weist dem HA-Paar die IP-Adressen zu, wenn sie das System startet.

Die Floating-IP-Adressen müssen außerhalb der CIDR-Blöcke für alle VPCs in der AWS-Region liegen, in der Sie die HA-Konfiguration bereitstellen. Stellen Sie sich die Floating-IP-Adressen als logisches Subnetz vor, das sich außerhalb der VPCs in Ihrer Region befindet.

Das folgende Beispiel zeigt die Beziehung zwischen Floating-IP-Adressen und den VPCs in einer AWS-Region. Während sich die Floating-IP-Adressen für alle VPCs außerhalb der CIDR-Blöcke befinden, können sie über Routentabellen an Subnetze weitergeleitet werden.



Die Konsole erstellt automatisch statische IP-Adressen für den iSCSI-Zugriff und für den NAS-Zugriff von Clients außerhalb der VPC. Für diese Art von IP-Adressen müssen Sie keine Anforderungen erfüllen.

Transit-Gateway zur Ermöglichung des Floating-IP-Zugriffs von außerhalb der VPC

Falls erforderlich,"Einrichten eines AWS Transit Gateways" um den Zugriff auf die Floating-IP-Adressen eines HA-Paares von außerhalb der VPC zu ermöglichen, in der sich das HA-Paar befindet.

Routentabellen

Nachdem Sie die Floating-IP-Adressen angegeben haben, werden Sie aufgefordert, die Routentabellen auszuwählen, die Routen zu den Floating-IP-Adressen enthalten sollen. Dies ermöglicht dem Client den Zugriff auf das HA-Paar.

Wenn Sie nur eine Routentabelle für die Subnetze in Ihrer VPC haben (die Hauptroutentabelle), fügt die Konsole die Floating-IP-Adressen automatisch zu dieser Routentabelle hinzu. Wenn Sie mehr als eine Routentabelle haben, ist es sehr wichtig, beim Starten des HA-Paares die richtigen Routentabellen auszuwählen. Andernfalls haben einige Clients möglicherweise keinen Zugriff auf Cloud Volumes ONTAP.

Beispielsweise könnten Sie zwei Subnetze haben, die mit unterschiedlichen Routentabellen verknüpft sind.

Wenn Sie Routentabelle A, aber nicht Routentabelle B auswählen, können Clients im mit Routentabelle A verknüpften Subnetz auf das HA-Paar zugreifen, Clients im mit Routentabelle B verknüpften Subnetz jedoch nicht.

Weitere Informationen zu Routentabellen finden Sie im "AWS-Dokumentation: Routentabellen" .

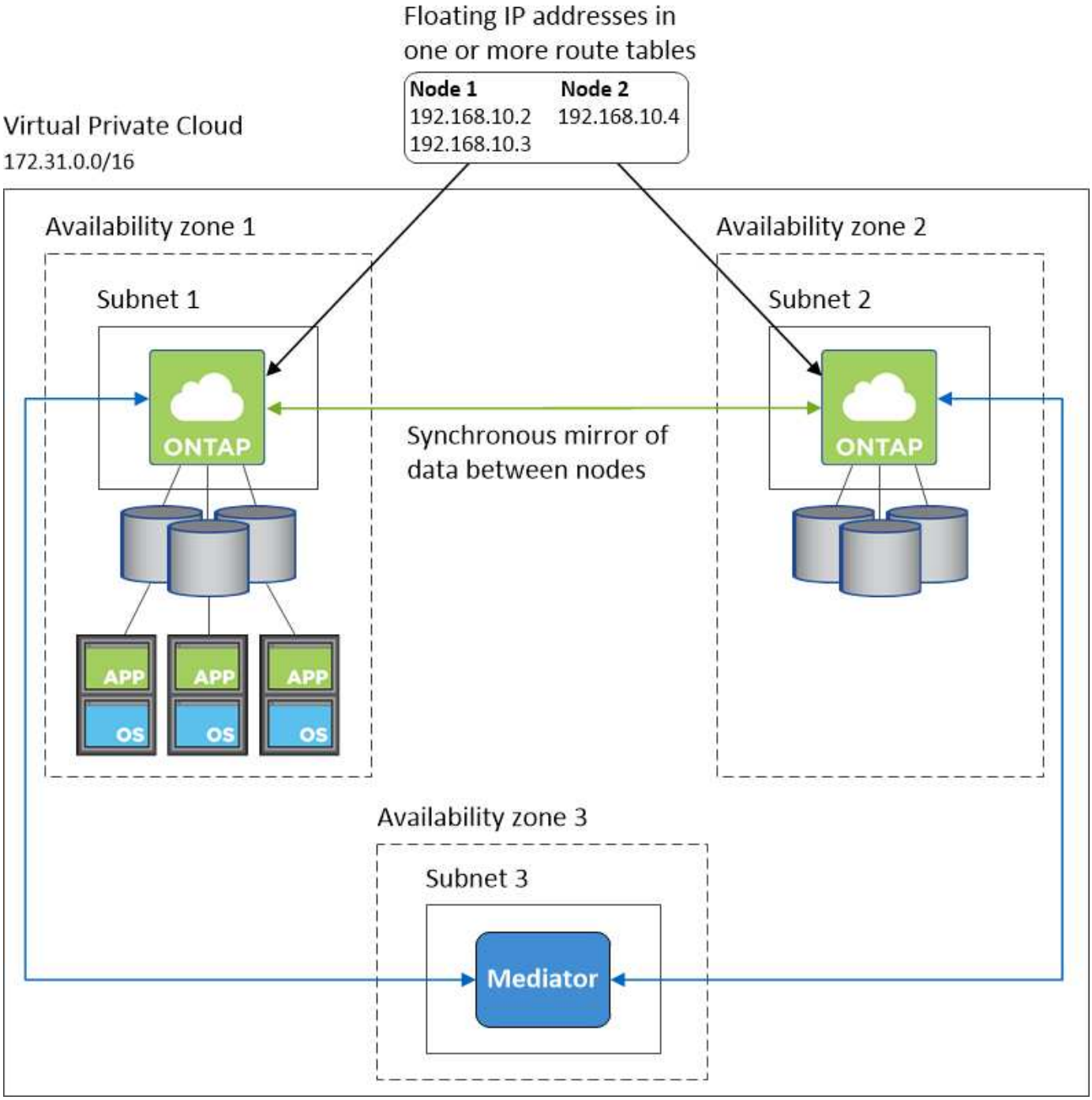
Anbindung an NetApp Management Tools

Um NetApp -Verwaltungstools mit HA-Konfigurationen zu verwenden, die sich in mehreren AZs befinden, haben Sie zwei Verbindungsoptionen:

1. Stellen Sie die NetApp -Verwaltungstools in einer anderen VPC bereit und"Einrichten eines AWS Transit Gateways" . Das Gateway ermöglicht den Zugriff auf die Floating-IP-Adresse für die Cluster-Management-Schnittstelle von außerhalb der VPC.
2. Stellen Sie die NetApp -Verwaltungstools im selben VPC mit einer ähnlichen Routing-Konfiguration wie NAS-Clients bereit.

Beispiel einer HA-Konfiguration

Das folgende Bild veranschaulicht die Netzwerkkomponenten, die für ein HA-Paar in mehreren AZs spezifisch sind: drei Availability Zones, drei Subnetze, Floating-IP-Adressen und eine Routentabelle.



Anforderungen für den Konsolenagenten

Wenn Sie noch keinen Konsolenagenten erstellt haben, sollten Sie die Netzwerkanforderungen überprüfen.

- "Netzwerkanforderungen für den Konsolenagenten anzeigen"
- "Sicherheitsgruppenregeln in AWS"

Verwandte Themen

- "Überprüfen Sie das AutoSupport -Setup für Cloud Volumes ONTAP"
- "Erfahren Sie mehr über die internen Ports von ONTAP" .

Einrichten eines AWS Transit Gateways für Cloud Volumes ONTAP HA-Paare

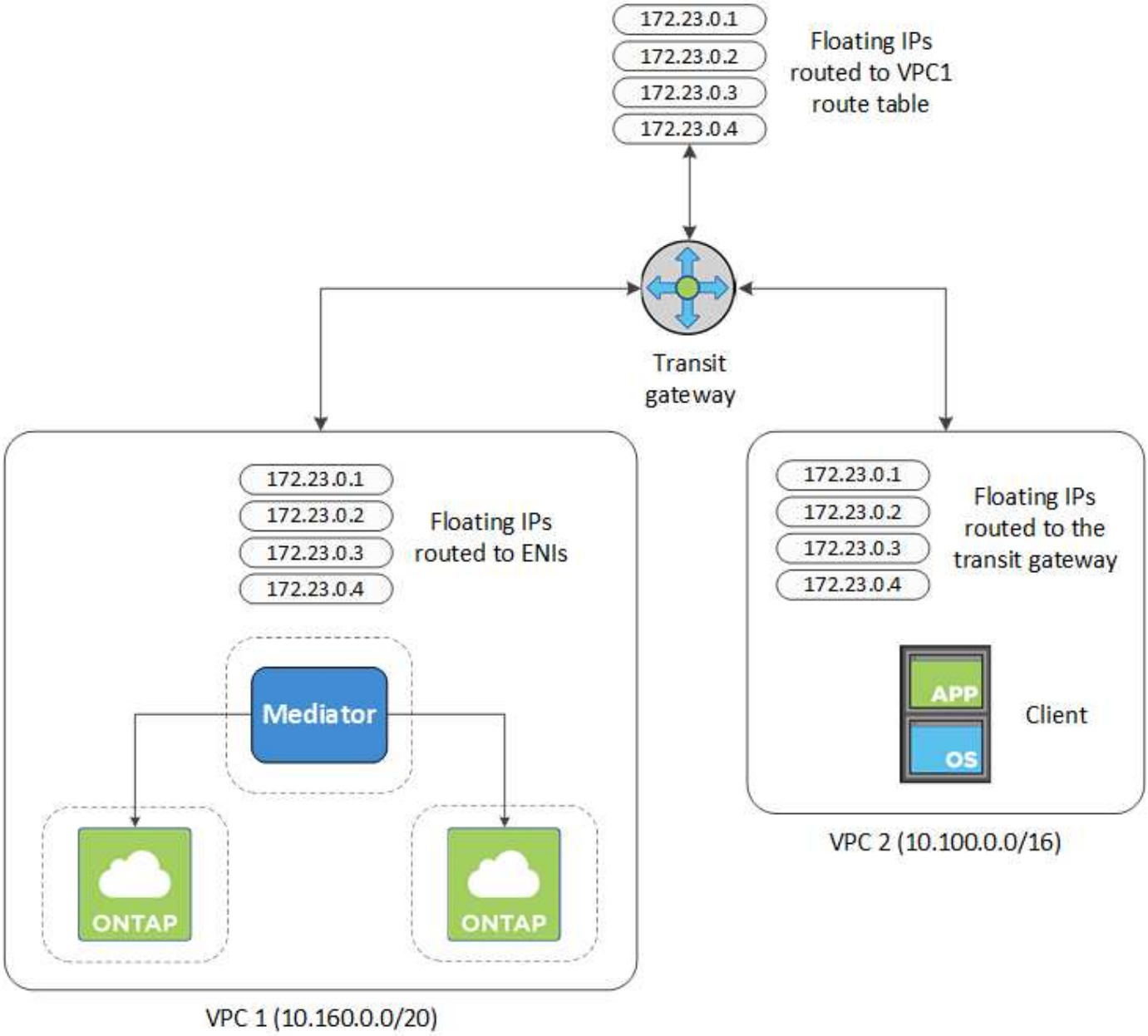
Richten Sie ein AWS Transit Gateway ein, um den Zugriff auf die HA-Paare zu ermöglichen."Floating-IP-Adressen" von außerhalb der VPC, in der sich das HA-Paar befindet.

Wenn eine Cloud Volumes ONTAP HA-Konfiguration über mehrere AWS Availability Zones verteilt ist, sind Floating-IP-Adressen für den NAS-Datenzugriff innerhalb der VPC erforderlich. Diese Floating-IP-Adressen können bei Fehlern zwischen Knoten migrieren, sind jedoch von außerhalb der VPC nicht nativ zugänglich. Separate private IP-Adressen ermöglichen den Datenzugriff von außerhalb der VPC, bieten jedoch kein automatisches Failover.

Floating-IP-Adressen werden auch für die Cluster-Management-Schnittstelle und das optionale SVM-Management-LIF benötigt.

Wenn Sie ein AWS-Transit-Gateway einrichten, ermöglichen Sie den Zugriff auf die Floating-IP-Adressen von außerhalb der VPC, in der sich das HA-Paar befindet. Das bedeutet, dass NAS-Clients und NetApp -Verwaltungstools außerhalb des VPC auf die Floating-IPs zugreifen können.

Hier ist ein Beispiel, das zwei VPCs zeigt, die durch ein Transit-Gateway verbunden sind. In einer VPC befindet sich ein HA-System, in der anderen ein Client. Sie könnten dann mithilfe der Floating-IP-Adresse ein NAS-Volume auf dem Client mounten.



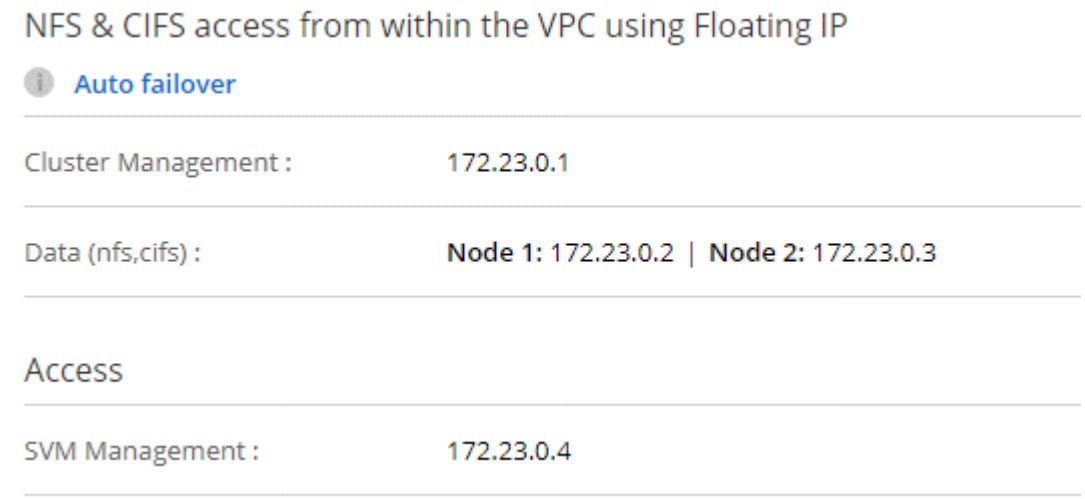
Die folgenden Schritte veranschaulichen, wie eine ähnliche Konfiguration eingerichtet wird.

Schritte

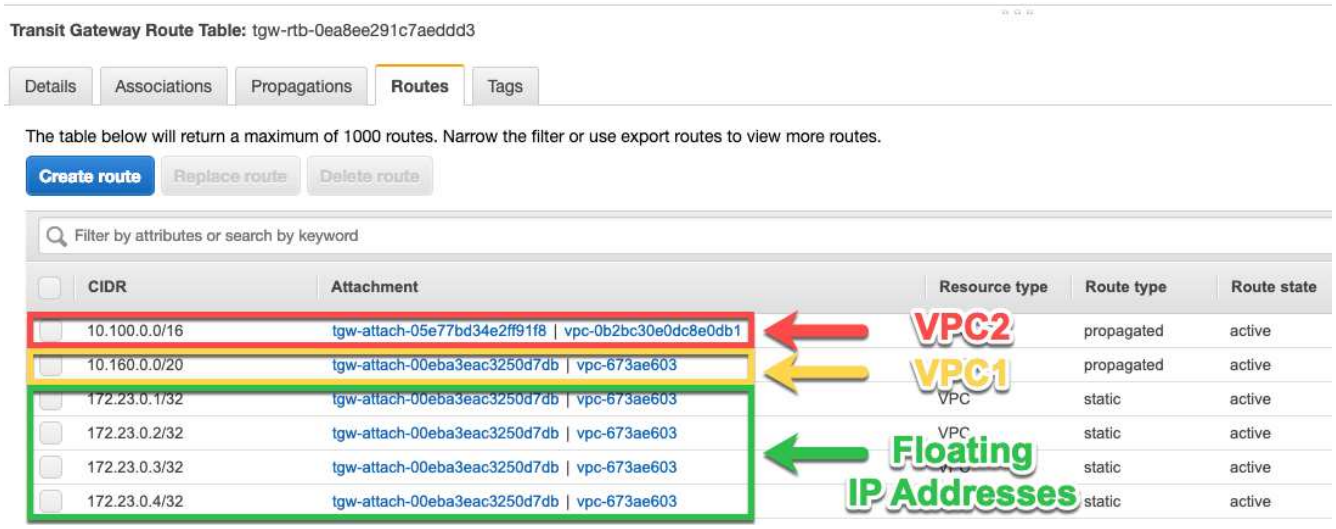
1. "Erstellen Sie ein Transit-Gateway und hängen Sie die VPCs an das Gateway an" .
2. Ordnen Sie die VPCs der Transit-Gateway-Routentabelle zu.
   a. Klicken Sie im **VPC**-Dienst auf **Transit Gateway Route Tables**.
   b. Wählen Sie die Routentabelle aus.
   c. Klicken Sie auf **Verknüpfungen** und wählen Sie dann **Verknüpfung erstellen**.
   d. Wählen Sie die zu verknüpfenden Anhänge (die VPCs) aus und klicken Sie dann auf **Verknüpfung erstellen**.
3. Erstellen Sie Routen in der Routentabelle des Transit-Gateways, indem Sie die Floating-IP-Adressen des HA-Paares angeben.

   Sie finden die Floating-IP-Adressen auf der Systeminformationsseite in der NetApp Console. Hier ist ein

Beispiel:



Das folgende Beispielbild zeigt die Routentabelle für das Transit Gateway. Es umfasst Routen zu den CIDR-Blöcken der beiden VPCs und vier Floating-IP-Adressen, die von Cloud Volumes ONTAP verwendet werden.

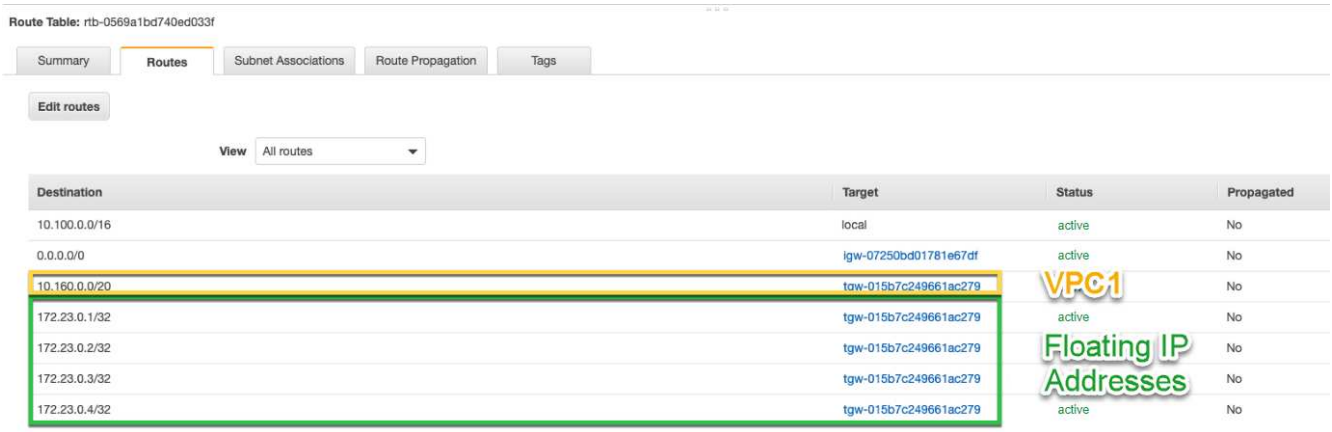


4. Ändern Sie die Routentabelle der VPCs, die auf die Floating-IP-Adressen zugreifen müssen.

   a. Fügen Sie den Floating-IP-Adressen Routeneinträge hinzu.

   b. Fügen Sie dem CIDR-Block der VPC, in der sich das HA-Paar befindet, einen Routeneintrag hinzu.

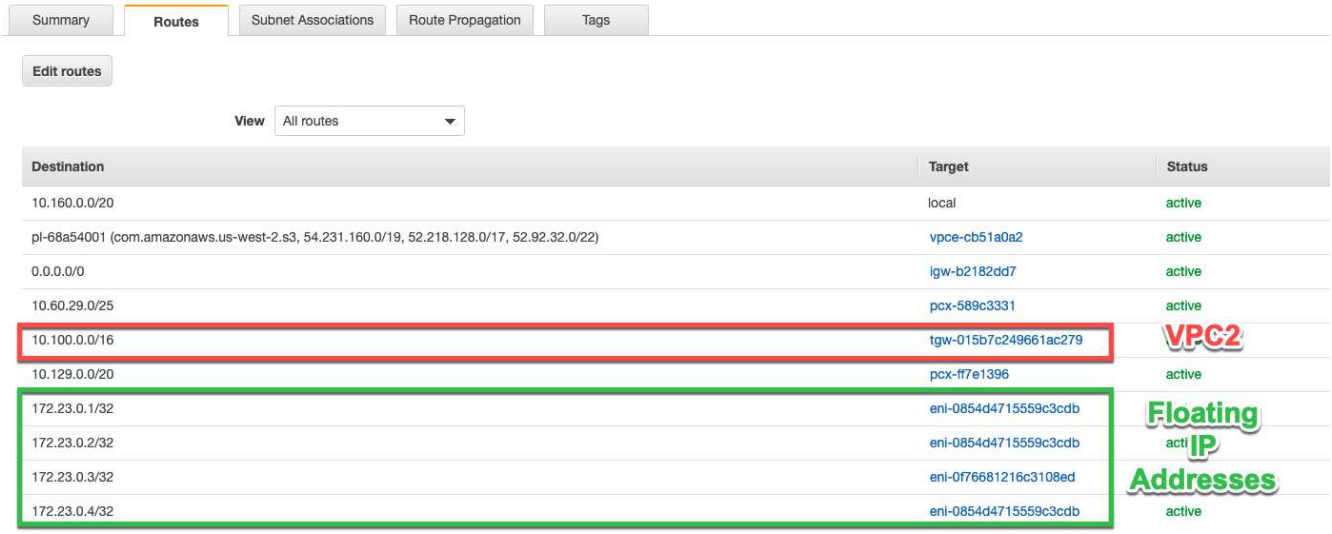
      Das folgende Beispielbild zeigt die Routentabelle für VPC 2, die Routen zu VPC 1 und die Floating-IP-Adressen enthält.



5. Ändern Sie die Routentabelle für die VPC des HA-Paares, indem Sie eine Route zur VPC hinzufügen, die Zugriff auf die Floating-IP-Adressen benötigt.

   Dieser Schritt ist wichtig, da er das Routing zwischen den VPCs abschließt.

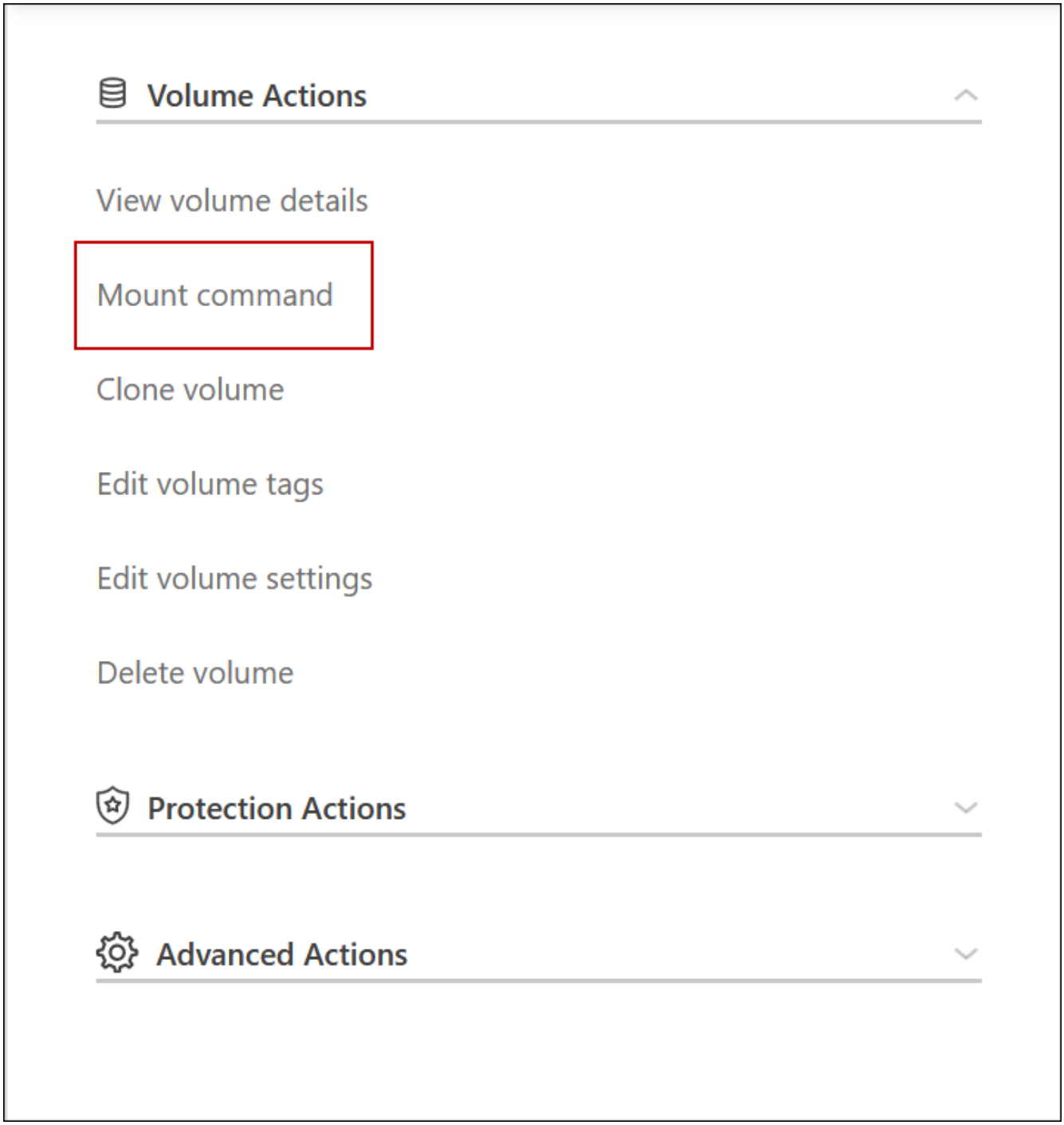
   Das folgende Beispielbild zeigt die Routentabelle für VPC 1. Es enthält eine Route zu den Floating-IP-Adressen und zu VPC 2, wo sich ein Client befindet. Die Konsole hat die Floating-IPs automatisch zur Routentabelle hinzugefügt, als sie das HA-Paar bereitgestellt hat.



6. Aktualisieren Sie die Einstellungen der Sicherheitsgruppen auf „Gesamter Datenverkehr für die VPC“.
   a. Klicken Sie unter „Virtual Private Cloud“ auf **Subnetze**.
   b. Klicken Sie auf die Registerkarte **Routentabelle** und wählen Sie die gewünschte Umgebung für eine der Floating-IP-Adressen für ein HA-Paar aus.
   c. Klicken Sie auf **Sicherheitsgruppen**.
   d. Wählen Sie **Eingehende Regeln bearbeiten**.
   e. Klicken Sie auf **Regel hinzufügen**.
   f. Wählen Sie unter „Typ“ die Option „Gesamter Datenverkehr“ und dann die VPC-IP-Adresse aus.
   g. Klicken Sie auf **Regeln speichern**, um die Änderungen anzuwenden.
7. Hängen Sie Volumes mithilfe der Floating-IP-Adresse an Clients an.

   Sie finden die richtige IP-Adresse in der Konsole über die Option **Mount Command** im Bereich „Volumes

verwalten“ in der Konsole.



8. Wenn Sie ein NFS-Volume mounten, konfigurieren Sie die Exportrichtlinie so, dass sie mit dem Subnetz der Client-VPC übereinstimmt.

   "Erfahren Sie, wie Sie ein Volume bearbeiten" .

Weiterführende Links

- "Hochverfügbarkeitspaare in AWS"
- "Netzwerkanforderungen für Cloud Volumes ONTAP in AWS"

Stellen Sie Cloud Volumes ONTAP HA-Paare in einem gemeinsam genutzten AWS-Subnetz bereit

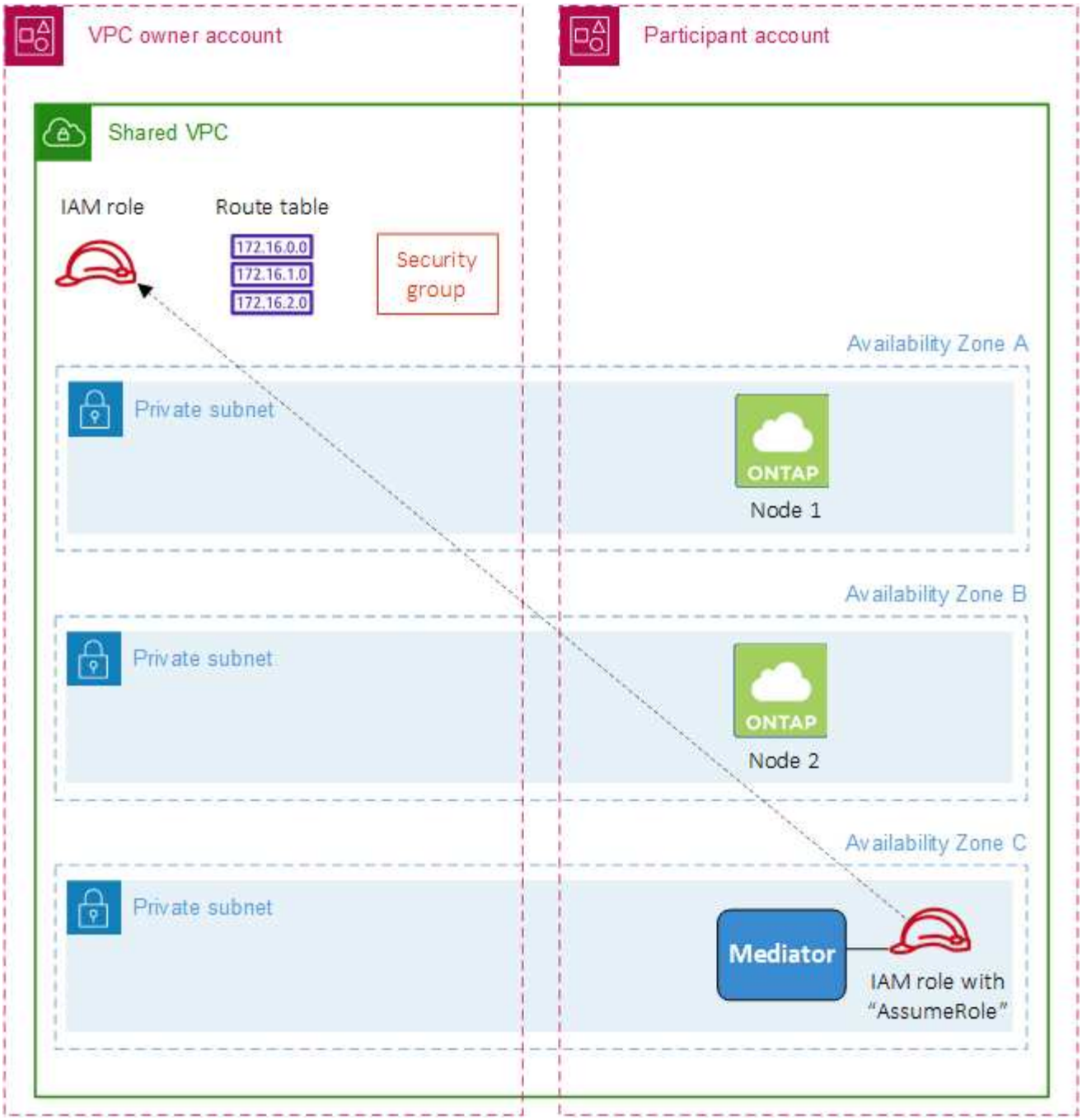
Ab der Version 9.11.1 werden Cloud Volumes ONTAP HA-Paare in AWS mit VPC-Sharing unterstützt. Durch die VPC-Freigabe kann Ihre Organisation Subnetze mit anderen AWS-Konten teilen. Um diese Konfiguration zu verwenden, müssen Sie Ihre AWS-Umgebung einrichten und dann das HA-Paar mithilfe der API bereitstellen.

Mit "VPC-Freigabe" , eine Cloud Volumes ONTAP HA-Konfiguration ist auf zwei Konten verteilt:

- Das VPC-Eigentümerkonto, dem das Netzwerk gehört (VPC, Subnetze, Routentabellen und Cloud Volumes ONTAP Sicherheitsgruppe)
- Das Teilnehmerkonto, in dem die EC2-Instanzen in gemeinsam genutzten Subnetzen bereitgestellt werden (dazu gehören die beiden HA-Knoten und der Mediator)

Im Fall einer Cloud Volumes ONTAP HA-Konfiguration, die über mehrere Availability Zones hinweg bereitgestellt wird, benötigt der HA-Mediator bestimmte Berechtigungen zum Schreiben in die Routentabellen im VPC-Eigentümerkonto. Sie müssen diese Berechtigungen bereitstellen, indem Sie eine IAM-Rolle einrichten, die der Mediator übernehmen kann.

Das folgende Bild zeigt die an dieser Bereitstellung beteiligten Komponenten:



Wie in den folgenden Schritten beschrieben, müssen Sie die Subnetze mit dem Teilnehmerkonto teilen und dann die IAM-Rolle und Sicherheitsgruppe im VPC-Eigentümerkonto erstellen.

Wenn Sie das Cloud Volumes ONTAP -System erstellen, erstellt die NetApp Console automatisch eine IAM-Rolle und fügt sie dem Mediator hinzu. Diese Rolle übernimmt die IAM-Rolle, die Sie im VPC-Eigentümerkonto erstellt haben, um Änderungen an den mit dem HA-Paar verknüpften Routentabellen vorzunehmen.

Schritte

1. Geben Sie die Subnetze im VPC-Eigentümerkonto für das Teilnehmerkonto frei.

   Dieser Schritt ist erforderlich, um das HA-Paar in gemeinsam genutzten Subnetzen bereitzustellen.

   "AWS-Dokumentation: Freigeben eines Subnetzes"

2. Erstellen Sie im VPC-Eigentümerkonto eine Sicherheitsgruppe für Cloud Volumes ONTAP.

   "Beachten Sie die Sicherheitsgruppenregeln für Cloud Volumes ONTAP" . Beachten Sie, dass Sie für den HA-Mediator keine Sicherheitsgruppe erstellen müssen. Die Konsole erledigt das für Sie.

3. Erstellen Sie im VPC-Eigentümerkonto eine IAM-Rolle, die die folgenden Berechtigungen umfasst:

```
Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
```

4. Verwenden Sie die API, um ein neues Cloud Volumes ONTAP System zu erstellen.

   Beachten Sie, dass Sie die folgenden Felder angeben müssen:

   - "Sicherheitsgruppen-ID"

     Das Feld „securityGroupId“ sollte die Sicherheitsgruppe angeben, die Sie im VPC-Eigentümerkonto erstellt haben (siehe Schritt 2 oben).

   - "assumeRoleArn" im "haParams"-Objekt

     Das Feld „assumeRoleArn“ sollte die ARN der IAM-Rolle enthalten, die Sie im VPC-Eigentümerkonto erstellt haben (siehe Schritt 3 oben).

     Beispiel:

```
"haParams": {
     "assumeRoleArn":
"arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}
```

   +
   "Erfahren Sie mehr über die Cloud Volumes ONTAP API"

Konfigurieren Sie die Erstellung von Platzierungsgruppen für Cloud Volumes ONTAP HA-Paare in einzelnen AWS-AZs

Bei Bereitstellungen mit hoher Verfügbarkeit (HA) von Cloud Volumes ONTAP in einer einzelnen AWS-Verfügbarkeitszone (AZ) kann es zu Fehlern und einem Rollback kommen, wenn die Erstellung der Platzierungsgruppe fehlschlägt. Die Erstellung der Platzierungsgruppe schlägt ebenfalls fehl und die Bereitstellung wird zurückgesetzt, wenn

der Cloud Volumes ONTAP Knoten und die Mediatorinstanz nicht verfügbar sind. Um dies zu vermeiden, können Sie die Konfiguration so ändern, dass die Bereitstellung auch dann abgeschlossen werden kann, wenn die Erstellung der Platzierungsgruppe fehlschlägt.

Wenn Sie den Rollback-Prozess umgehen, wird der Bereitstellungsprozess von Cloud Volumes ONTAP erfolgreich abgeschlossen und Sie werden benachrichtigt, dass die Erstellung der Platzierungsgruppe unvollständig ist.

Schritte

1. Verwenden Sie SSH, um eine Verbindung zum NetApp Console Agent-Host herzustellen und sich anzumelden.
2. Navigieren Sie zu `/opt/application/netapp/cloudmanager/docker_occm/data` .
3. Bearbeiten `app.conf` durch Ändern des Wertes der `rollback-on-placement-group-failure` Parameter auf `false` . Der Standardwert dieses Parameters ist `true` .

```
{
    "occm" : {
        "aws" : {
            "rollback-on-placement-group-failure" : false
        }
    }
}
```

4. Speichern Sie die Datei und melden Sie sich vom Konsolenagenten ab. Sie müssen den Konsolenagenten nicht neu starten.

AWS-Sicherheitsgruppen-Ein- und Ausgangsregeln für Cloud Volumes ONTAP

Die NetApp Console erstellt AWS-Sicherheitsgruppen, die die eingehenden und ausgehenden Regeln enthalten, die Cloud Volumes ONTAP für einen erfolgreichen Betrieb benötigt. Möglicherweise möchten Sie zu Testzwecken auf die Ports verweisen oder wenn Sie lieber Ihre eigenen Sicherheitsgruppen verwenden möchten.

Regeln für Cloud Volumes ONTAP

Die Sicherheitsgruppe für Cloud Volumes ONTAP erfordert sowohl eingehende als auch ausgehende Regeln.

Eingehende Regeln

Wenn Sie ein Cloud Volumes ONTAP -System hinzufügen und eine vordefinierte Sicherheitsgruppe auswählen, können Sie den Datenverkehr innerhalb einer der folgenden Gruppen zulassen:

- **Nur ausgewählte VPC**: Die Quelle für eingehenden Datenverkehr ist der Subnetzbereich der VPC für das Cloud Volumes ONTAP -System und der Subnetzbereich der VPC, in der sich der Konsolenagent befindet. Dies ist die empfohlene Option.
- **Alle VPCs**: Die Quelle für eingehenden Datenverkehr ist der IP-Bereich 0.0.0.0/0.

Protokoll	Hafen	Zweck
Alle ICMP	Alle	Pingen der Instanz
HTTP	80	HTTP-Zugriff auf die ONTAP System Manager-Webkonsole über die IP-Adresse des Cluster-Management-LIF
HTTPS	443	Konnektivität mit dem Konsolenagenten und HTTPS-Zugriff auf die ONTAP System Manager-Webkonsole unter Verwendung der IP-Adresse des Cluster-Management-LIF
SSH	22	SSH-Zugriff auf die IP-Adresse des Cluster-Management-LIF oder eines Node-Management-LIF
TCP	111	Remote Procedure Call für NFS
TCP	139	NetBIOS-Dienstsitzung für CIFS
TCP	161-162	Einfaches Netzwerkverwaltungsprotokoll
TCP	445	Microsoft SMB/CIFS über TCP mit NetBIOS-Framing
TCP	635	NFS-Mount
TCP	749	Kerberos
TCP	2049	NFS-Server-Daemon
TCP	3260	iSCSI-Zugriff über das iSCSI-Daten-LIF
TCP	4045	NFS-Sperrdaemon
TCP	4046	Netzwerkstatusmonitor für NFS
TCP	10000	Sicherung mit NDMP
TCP	11104	Verwaltung von Intercluster-Kommunikationssitzungen für SnapMirror
TCP	11105	SnapMirror Datenübertragung mithilfe von Intercluster-LIFs
UDP	111	Remote Procedure Call für NFS
UDP	161-162	Einfaches Netzwerkverwaltungsprotokoll
UDP	635	NFS-Mount
UDP	2049	NFS-Server-Daemon
UDP	4045	NFS-Sperrdaemon
UDP	4046	Netzwerkstatusmonitor für NFS
UDP	4049	NFS-Rquotad-Protokoll

Ausgangsregeln

Die vordefinierte Sicherheitsgruppe für Cloud Volumes ONTAP öffnet den gesamten ausgehenden Datenverkehr. Wenn das akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Nachrichten. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Ausgangsregeln.

Grundlegende Ausgangsregeln

Die vordefinierte Sicherheitsgruppe für Cloud Volumes ONTAP umfasst die folgenden ausgehenden Regeln.

Protokoll	Hafen	Zweck
Alle ICMP	Alle	Der gesamte ausgehende Verkehr
Alle TCP	Alle	Der gesamte ausgehende Verkehr
Alle UDP	Alle	Der gesamte ausgehende Verkehr

Erweiterte Ausgangsregeln

Wenn Sie strenge Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation von Cloud Volumes ONTAP erforderlich sind.

Die Quelle ist die Schnittstelle (IP-Adresse) auf dem Cloud Volumes ONTAP -System.

Service	Protokoll	Hafen	Quelle	Ziel	Zweck
Active Directory	TCP	88	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	UDP	137	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	UDP	138	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	NetBIOS-Datagrammdienst
	TCP	139	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	NetBIOS-Dienstsitzung
	TCP und UDP	389	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NetBIOS-Framing
	TCP	464	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern & festlegen (SET_CHANGE)
	UDP	464	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	TCP	749	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (RPCSEC_GSS)
	TCP	88	Daten-LIF (NFS, CIFS, iSCSI)	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	UDP	137	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	UDP	138	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	NetBIOS-Datagrammdienst
	TCP	139	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	NetBIOS-Dienstsitzung
	TCP und UDP	389	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NetBIOS-Framing
	TCP	464	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern & festlegen (SET_CHANGE)
	UDP	464	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	TCP	749	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern & festlegen (RPCSEC_GSS)

Service	Protokoll	Hafen	Quelle	Ziel	Zweck
AutoSupport	HTTPS	443	Knotenverwaltung LIF	mysupport.netapp.com	AutoSupport (HTTPS ist die Standardeinstellung)
	HTTP	80	Knotenverwaltung LIF	mysupport.netapp.com	AutoSupport (nur wenn das Transportprotokoll von HTTPS auf HTTP geändert wird)
	TCP	3128	Knotenverwaltung LIF	Konsolenagent	Senden von AutoSupport -Nachrichten über einen Proxyserver auf dem Konsolenagenten, wenn keine ausgehende Internetverbindung verfügbar ist
Sicherung auf S3	TCP	5010	Intercluster LIF	Sicherungsendpunkt oder Wiederherstellungsendpunkt	Sicherungs- und Wiederherstellungsvorgänge für die Funktion „Backup to S3“
Cluster	Der gesamte Verkehr	Der gesamte Verkehr	Alle LIFs auf einem Knoten	Alle LIFs auf dem anderen Knoten	Intercluster-Kommunikation (nur Cloud Volumes ONTAP HA)
	TCP	3000	Knotenverwaltung LIF	HA-Mediator	ZAPI-Aufrufe (nur Cloud Volumes ONTAP HA)
	ICMP	1	Knotenverwaltung LIF	HA-Mediator	Keep-Alive (nur Cloud Volumes ONTAP HA)
Konfigurationssicherungen	HTTP	80	Knotenverwaltung LIF	http://<IP-Adresse des Konsolenagenten>/occm/offboxconfig	Senden Sie Konfigurationssicherungen an den Konsolenagenten."ONTAP-Dokumentation"
DHCP	UDP	68	Knotenverwaltung LIF	DHCP	DHCP-Client für die Ersteinrichtung
DHCPS	UDP	67	Knotenverwaltung LIF	DHCP	DHCP-Server
DNS	UDP	53	Knotenverwaltungs-LIF und Daten-LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	Knotenverwaltung LIF	Zielserver	NDMP-Kopie
SMTP	TCP	25	Knotenverwaltung LIF	Mailserver	SMTP-Benachrichtigungen, können für AutoSupport verwendet werden

Service	Protokoll	Hafen	Quelle	Ziel	Zweck
SNMP	TCP	161	Knotenverwaltung LIF	Monitorserver	Überwachung durch SNMP-Traps
	UDP	161	Knotenverwaltung LIF	Monitorserver	Überwachung durch SNMP-Traps
	TCP	162	Knotenverwaltung LIF	Monitorserver	Überwachung durch SNMP-Traps
	UDP	162	Knotenverwaltung LIF	Monitorserver	Überwachung durch SNMP-Traps
SnapMirror	TCP	11104	Intercluster LIF	ONTAP Intercluster-LIFs	Verwaltung von Intercluster-Kommunikationssitzungen für SnapMirror
	TCP	11105	Intercluster LIF	ONTAP Intercluster-LIFs	SnapMirror -Datenübertragung
Syslog	UDP	514	Knotenverwaltung LIF	Syslog-Server	Syslog-Weiterleitungsnachrichten

Regeln für die externe Sicherheitsgruppe des HA-Mediators

Die vordefinierte externe Sicherheitsgruppe für den Cloud Volumes ONTAP HA-Mediator umfasst die folgenden eingehenden und ausgehenden Regeln.

Eingehende Regeln

Die vordefinierte Sicherheitsgruppe für den HA-Mediator enthält die folgende eingehende Regel.

Protokoll	Hafen	Quelle	Zweck
TCP	3000	CIDR des Konsolenagenten	RESTful-API-Zugriff vom Konsolenagenten

Ausgangsregeln

Die vordefinierte Sicherheitsgruppe für den HA-Mediator öffnet den gesamten ausgehenden Datenverkehr. Wenn das akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Nachrichten. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Ausgangsregeln.

Grundlegende Ausgangsregeln

Die vordefinierte Sicherheitsgruppe für den HA-Mediator umfasst die folgenden ausgehenden Regeln.

Protokoll	Hafen	Zweck
Alle TCP	Alle	Der gesamte ausgehende Verkehr
Alle UDP	Alle	Der gesamte ausgehende Verkehr

Erweiterte Ausgangsregeln

Wenn Sie strenge Regeln für den ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den HA-Mediator erforderlich sind.

Protokoll	Hafen	Ziel	Zweck
HTTP	80	IP-Adresse des Konsolenagenten auf der AWS EC2-Instanz	Upgrades für den Mediator herunterladen
HTTPS	443	ec2.amazonaws.com	Unterstützung beim Speicherfailover
UDP	53	ec2.amazonaws.com	Unterstützung beim Speicherfailover

Anstatt die Ports 443 und 53 zu öffnen, können Sie einen Schnittstellen-VPC-Endpunkt vom Zielsubnetz zum AWS EC2-Dienst erstellen.

Regeln für die interne Sicherheitsgruppe der HA-Konfiguration

Die vordefinierte interne Sicherheitsgruppe für eine Cloud Volumes ONTAP HA-Konfiguration umfasst die folgenden Regeln. Diese Sicherheitsgruppe ermöglicht die Kommunikation zwischen den HA-Knoten und zwischen dem Mediator und den Knoten.

Die Konsole erstellt immer diese Sicherheitsgruppe. Sie haben nicht die Möglichkeit, Ihre eigenen zu verwenden.

Eingehende Regeln

Die vordefinierte Sicherheitsgruppe umfasst die folgenden eingehenden Regeln.

Protokoll	Hafen	Zweck
Der gesamte Verkehr	Alle	Kommunikation zwischen dem HA-Mediator und den HA-Knoten

Ausgangsregeln

Die vordefinierte Sicherheitsgruppe umfasst die folgenden ausgehenden Regeln.

Protokoll	Hafen	Zweck
Der gesamte Verkehr	Alle	Kommunikation zwischen dem HA-Mediator und den HA-Knoten

Regeln für den Konsolenagenten

"Sicherheitsgruppenregeln für den Konsolenagenten anzeigen"

Richten Sie Cloud Volumes ONTAP für die Verwendung eines vom Kunden verwalteten Schlüssels in AWS ein

Wenn Sie die Amazon-Verschlüsselung mit Cloud Volumes ONTAP verwenden möchten, müssen Sie den AWS Key Management Service (KMS) einrichten.

Schritte

1. Stellen Sie sicher, dass ein aktiver Customer Master Key (CMK) vorhanden ist.

   Der CMK kann ein von AWS verwalteter CMK oder ein vom Kunden verwalteter CMK sein. Es kann sich im selben AWS-Konto wie die NetApp Console und Cloud Volumes ONTAP oder in einem anderen AWS-Konto befinden.

   "AWS-Dokumentation: Kundenmasterschlüssel (CMKs)"

2. Ändern Sie die Schlüsselrichtlinie für jeden CMK, indem Sie die IAM-Rolle hinzufügen, die der Konsole als *Schlüsselbenutzer* Berechtigungen erteilt.

   Durch Hinzufügen der Identity and Access Management (IAM)-Rolle als Hauptbenutzer erhält die Konsole die Berechtigung, den CMK mit Cloud Volumes ONTAP zu verwenden.

   "AWS-Dokumentation: Bearbeiten von Schlüsseln"

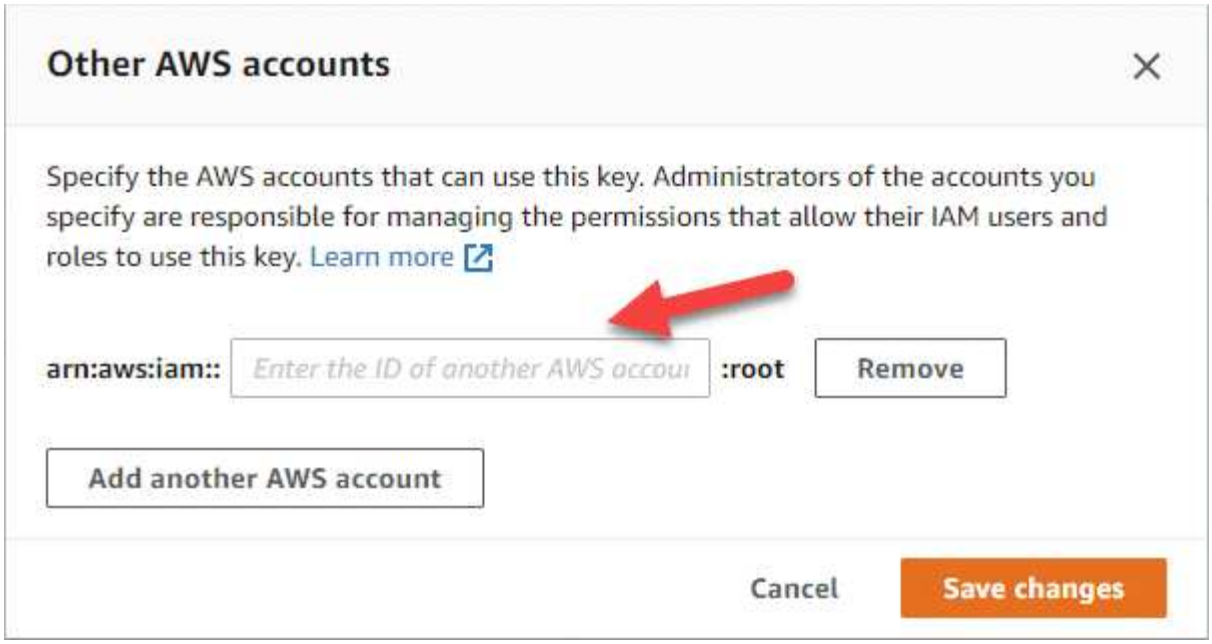
3. Wenn sich der CMK in einem anderen AWS-Konto befindet, führen Sie die folgenden Schritte aus:

   a. Gehen Sie von dem Konto, in dem sich der CMK befindet, zur KMS-Konsole.
   b. Wählen Sie den Schlüssel aus.
   c. Kopieren Sie im Bereich **Allgemeine Konfiguration** die ARN des Schlüssels.

      Sie müssen der Konsole die ARN bereitstellen, wenn Sie das Cloud Volumes ONTAP -System erstellen.

   d. Fügen Sie im Bereich **Andere AWS-Konten** das AWS-Konto hinzu, das der Konsole Berechtigungen erteilt.

      Normalerweise ist dies das Konto, unter dem die Konsole bereitgestellt wird. Wenn die Konsole nicht in AWS installiert ist, verwenden Sie das Konto, für das Sie AWS-Zugriffsschlüssel für die Konsole bereitgestellt haben.



e. Wechseln Sie nun zu dem AWS-Konto, das der Konsole Berechtigungen erteilt, und öffnen Sie die IAM-Konsole.

f. Erstellen Sie eine IAM-Richtlinie, die die unten aufgeführten Berechtigungen enthält.

g. Fügen Sie die Richtlinie der IAM-Rolle oder dem IAM-Benutzer hinzu, der Berechtigungen für die Konsole bereitstellt.

   Die folgende Richtlinie stellt die Berechtigungen bereit, die die Konsole benötigt, um den CMK vom externen AWS-Konto zu verwenden. Denken Sie daran, die Region und die Konto-ID in den Abschnitten „Ressource“ zu ändern.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
            ]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

+
Weitere Einzelheiten zu diesem Vorgang finden Sie im "AWS-Dokumentation: Benutzern anderer Konten die Verwendung eines KMS-Schlüssels gestatten" .

4. Wenn Sie einen vom Kunden verwalteten CMK verwenden, ändern Sie die Schlüsselrichtlinie für den CMK, indem Sie die Cloud Volumes ONTAP IAM-Rolle als *Schlüsselbenutzer* hinzufügen.

Dieser Schritt ist erforderlich, wenn Sie Data Tiering auf Cloud Volumes ONTAP aktiviert haben und die im Amazon Simple Storage Service (Amazon S3) Bucket gespeicherten Daten verschlüsseln möchten.

Sie müssen diesen Schritt *nach* der Bereitstellung von Cloud Volumes ONTAP ausführen, da die IAM-Rolle beim Erstellen eines Cloud Volumes ONTAP Systems erstellt wird. (Natürlich haben Sie die Möglichkeit, eine vorhandene Cloud Volumes ONTAP IAM-Rolle zu verwenden, sodass Sie diesen Schritt vorher ausführen können.)

"AWS-Dokumentation: Bearbeiten von Schlüsseln"

Einrichten von AWS IAM-Rollen für Cloud Volumes ONTAP Knoten

Jedem Cloud Volumes ONTAP -Knoten müssen AWS Identity and Access Management (IAM)-Rollen mit den erforderlichen Berechtigungen zugeordnet werden. Dasselbe gilt für den HA-Mediator. Am einfachsten ist es, die IAM-Rollen von der NetApp Console erstellen zu lassen, Sie können jedoch auch Ihre eigenen Rollen verwenden.

Diese Aufgabe ist optional. Wenn Sie ein Cloud Volumes ONTAP -System erstellen, besteht die Standardoption darin, die IAM-Rollen von der Konsole erstellen zu lassen. Wenn die Sicherheitsrichtlinien Ihres Unternehmens erfordern, dass Sie die IAM-Rollen selbst erstellen, führen Sie die folgenden Schritte aus.

In AWS Secret Cloud ist die Bereitstellung Ihrer eigenen IAM-Rolle erforderlich. "Erfahren Sie, wie Sie Cloud Volumes ONTAP in C2S bereitstellen" .

Schritte

1. Gehen Sie zur AWS IAM-Konsole.
2. Erstellen Sie IAM-Richtlinien, die die folgenden Berechtigungen enthalten:
    - Basisrichtlinie für Cloud Volumes ONTAP Knoten

Standardregionen

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud (USA)-Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-us-gov:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Streng geheime Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Geheime Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

- Sicherungsrichtlinie für Cloud Volumes ONTAP Knoten

  Wenn Sie NetApp Backup and Recovery mit Ihren Cloud Volumes ONTAP -Systemen verwenden möchten, muss die IAM-Rolle für die Knoten die zweite unten gezeigte Richtlinie enthalten.

Standardregionen

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "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"
        }
    ]
}
```

GovCloud (USA)-Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-us-gov: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-us-gov:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

Streng geheime Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso: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-iso:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

Geheime Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso-b: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-iso-b:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

- HA-Mediator

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses",
                "sts:AssumeRole",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

3. Erstellen Sie eine IAM-Rolle und fügen Sie der Rolle die von Ihnen erstellten Richtlinien hinzu.

Ergebnis

Sie verfügen jetzt über IAM-Rollen, die Sie beim Erstellen eines neuen Cloud Volumes ONTAP Systems auswählen können.

Weitere Informationen

- "AWS-Dokumentation: Erstellen von IAM-Richtlinien"
- "AWS-Dokumentation: Erstellen von IAM-Rollen"

Einrichten der Lizenzierung für Cloud Volumes ONTAP in AWS

Nachdem Sie entschieden haben, welche Lizenzierungsoption Sie mit Cloud Volumes ONTAP verwenden möchten, sind einige Schritte erforderlich, bevor Sie diese Lizenzierungsoption beim Erstellen eines neuen Systems auswählen können.

Freemium

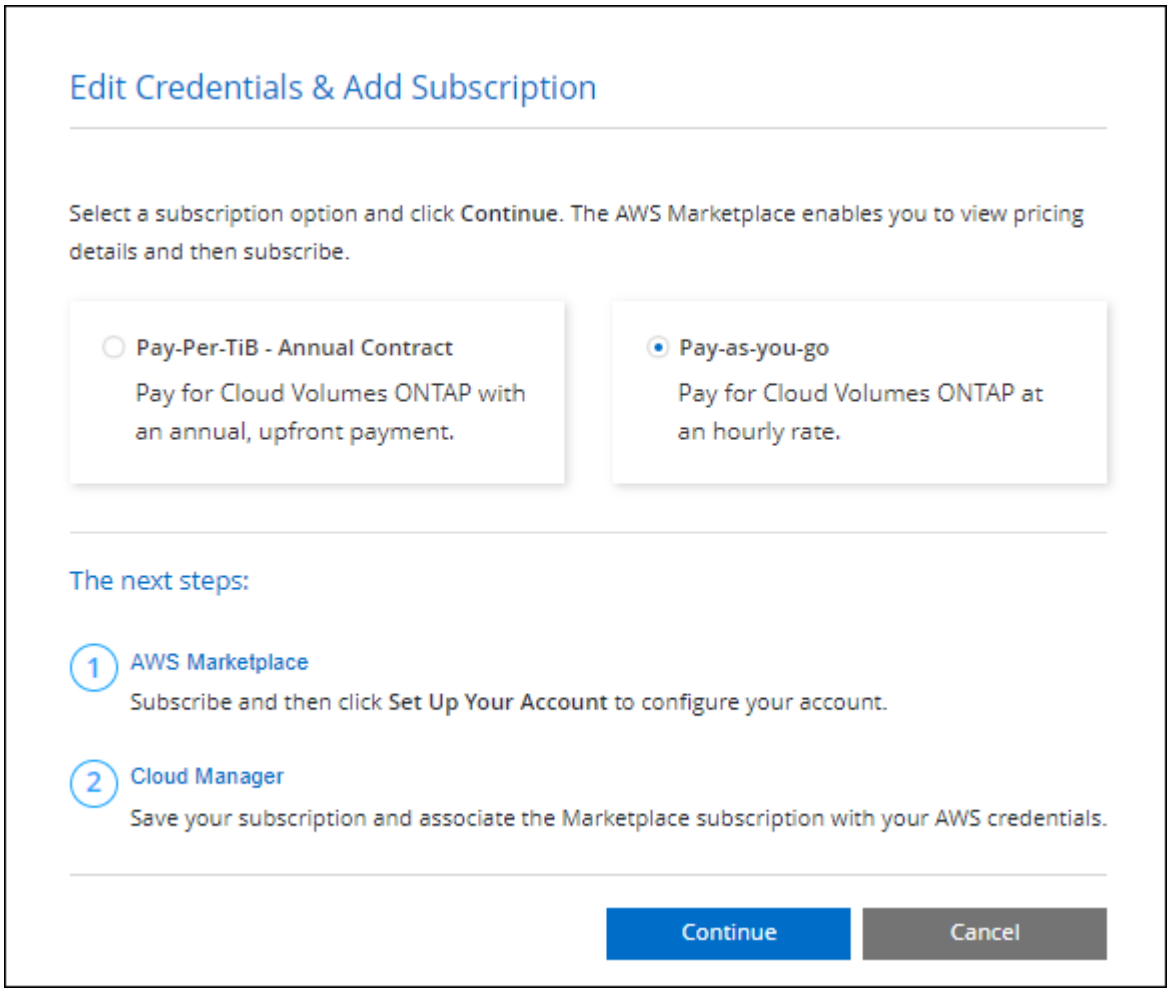
Wählen Sie das Freemium-Angebot, um Cloud Volumes ONTAP mit bis zu 500 GiB bereitgestellter Kapazität kostenlos zu nutzen. "Erfahren Sie mehr über das Freemium-Angebot" .

Schritte

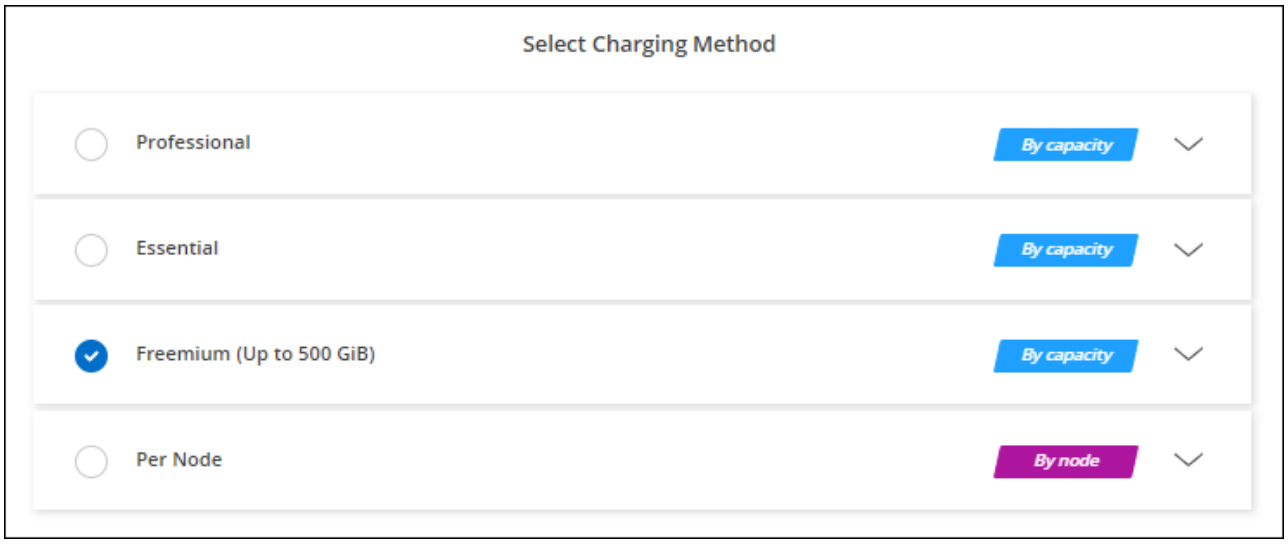
1. Wählen Sie im linken Navigationsmenü der NetApp Console*Speicher > Verwaltung* aus.
2. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten.

a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldeinformationen bearbeiten > Abonnement hinzufügen** und folgen Sie dann den Anweisungen, um das Pay-as-you-go-Angebot im AWS Marketplace zu abonnieren.

   Ihnen werden keine Kosten über das Marktplatz-Abonnement berechnet, es sei denn, Sie überschreiten 500 GiB bereitgestellte Kapazität. Zu diesem Zeitpunkt wird das System automatisch auf das"Essentials-Paket" .



a. Nachdem Sie zur Konsole zurückgekehrt sind, wählen Sie **Freemium** aus, wenn Sie die Seite mit den Abrechnungsmethoden erreichen.



"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in AWS an" .

Kapazitätsbasierte Lizenz

Mit der kapazitätsbasierten Lizenzierung können Sie für Cloud Volumes ONTAP pro TiB Kapazität bezahlen. Die kapazitätsbasierte Lizenzierung ist in Form eines *Pakets* verfügbar: das Essentials-Paket oder das Professional-Paket.

Die Pakete Essentials und Professional sind mit folgenden Verbrauchsmodellen bzw. Kaufoptionen erhältlich:

- Eine von NetApp erworbene Lizenz (Bring Your Own License (BYOL))
- Ein stündliches Pay-as-you-go-Abonnement (PAYGO) vom AWS Marketplace
- Ein Jahresvertrag vom AWS Marketplace

"Erfahren Sie mehr über kapazitätsbasierte Lizenzierung" .

In den folgenden Abschnitten wird beschrieben, wie Sie mit jedem dieser Verbrauchsmodelle beginnen.

BYOL

Zahlen Sie im Voraus, indem Sie eine Lizenz (BYOL) von NetApp erwerben, um Cloud Volumes ONTAP -Systeme bei jedem Cloud-Anbieter bereitzustellen.

NetApp hat den Erwerb, die Verlängerung und die Erneuerung von BYOL-Lizenzen eingeschränkt. Weitere Informationen finden Sie unter "Eingeschränkte Verfügbarkeit der BYOL-Lizenzierung für Cloud Volumes ONTAP" .

Schritte

1. "Kontaktieren Sie den NetApp -Vertrieb, um eine Lizenz zu erhalten"
2. "Fügen Sie Ihr NetApp Support Site-Konto zur Konsole hinzu"

   Die Konsole fragt automatisch den Lizenzierungsdienst von NetApp ab, um Details zu den Lizenzen abzurufen, die mit Ihrem NetApp Support Site-Konto verknüpft sind. Wenn keine Fehler auftreten, fügt die Konsole die Lizenzen automatisch zur Konsole hinzu.

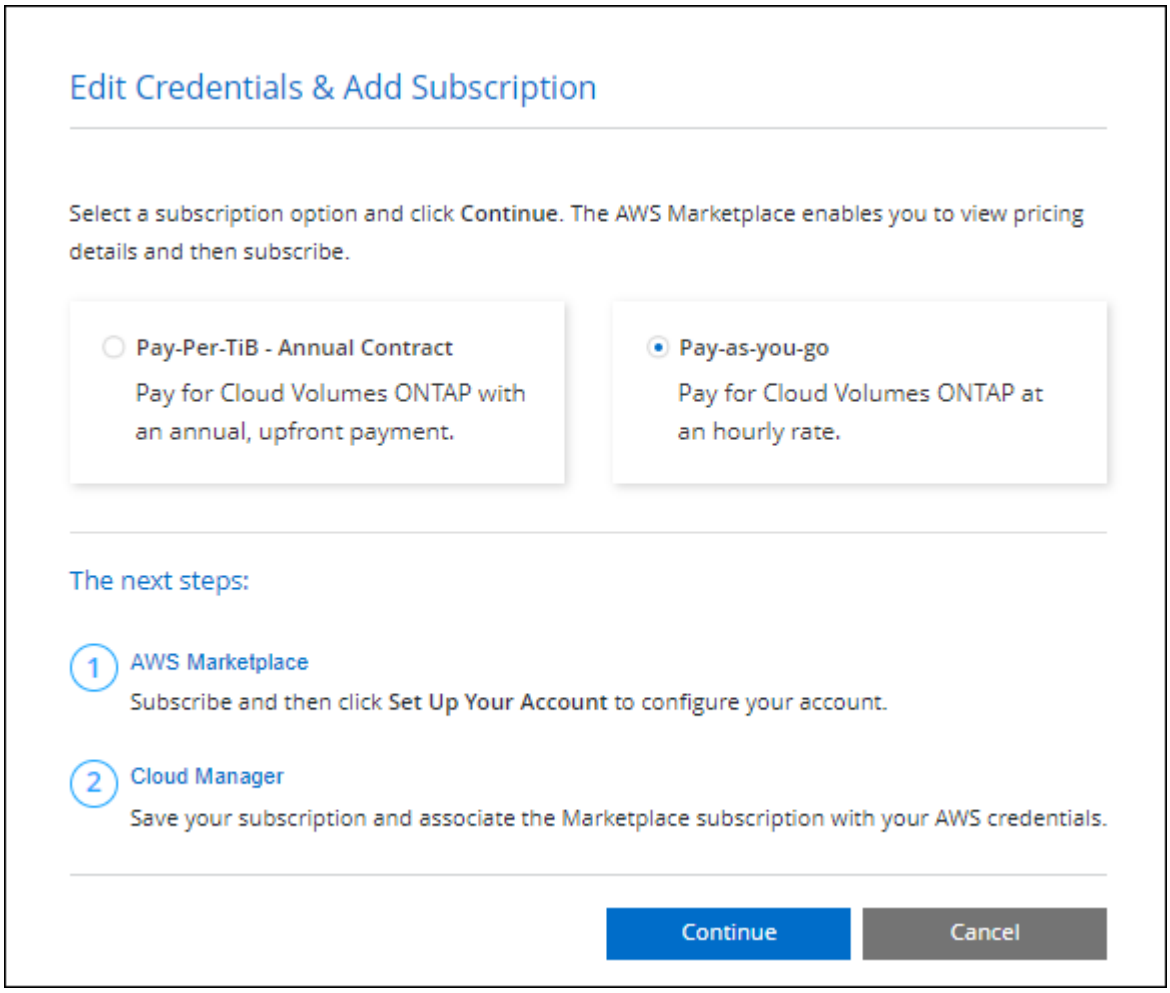
   Ihre Lizenz muss in der Konsole verfügbar sein, bevor Sie sie mit Cloud Volumes ONTAP verwenden

können. Bei Bedarf können Sie"Fügen Sie die Lizenz manuell zur Konsole hinzu" .

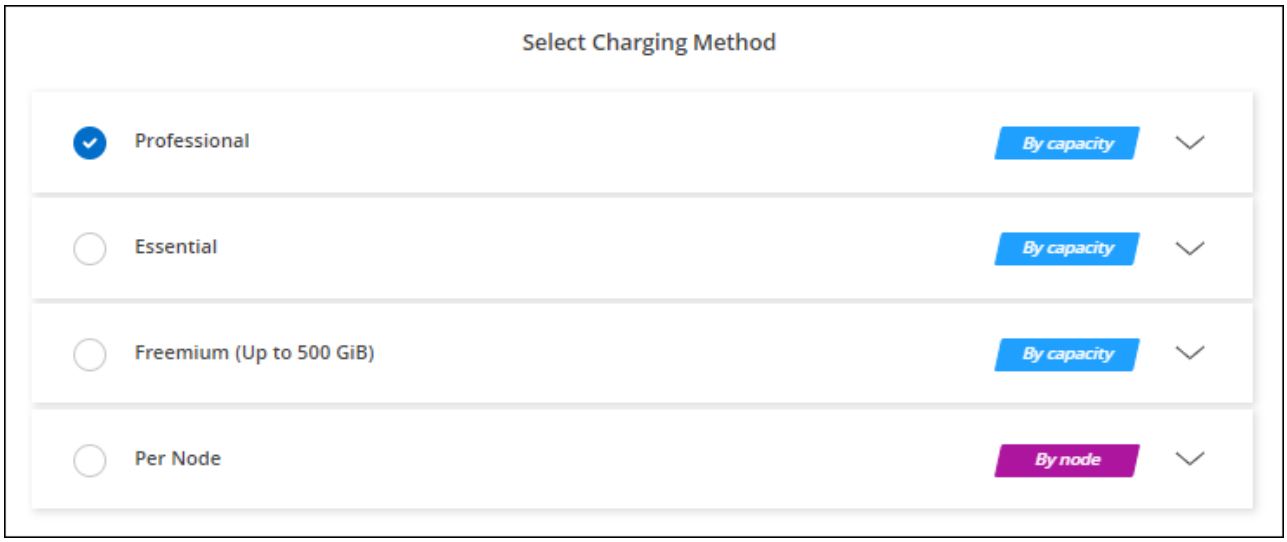
3. Klicken Sie auf der Seite **Systeme** der Konsole auf **System hinzufügen** und folgen Sie den Schritten.

   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldeinformationen bearbeiten > Abonnement hinzufügen** und folgen Sie dann den Anweisungen, um das Pay-as-you-go-Angebot im AWS Marketplace zu abonnieren.

      Die von Ihnen bei NetApp erworbene Lizenz wird immer zuerst in Rechnung gestellt. Wenn Sie jedoch Ihre lizenzierte Kapazität überschreiten oder die Laufzeit Ihrer Lizenz abläuft, wird Ihnen der Stundensatz auf dem Marktplatz in Rechnung gestellt.



   a. Nachdem Sie zur Konsole zurückgekehrt sind, wählen Sie auf der Seite mit den Abrechnungsmethoden ein kapazitätsbasiertes Paket aus.



"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in AWS an" .

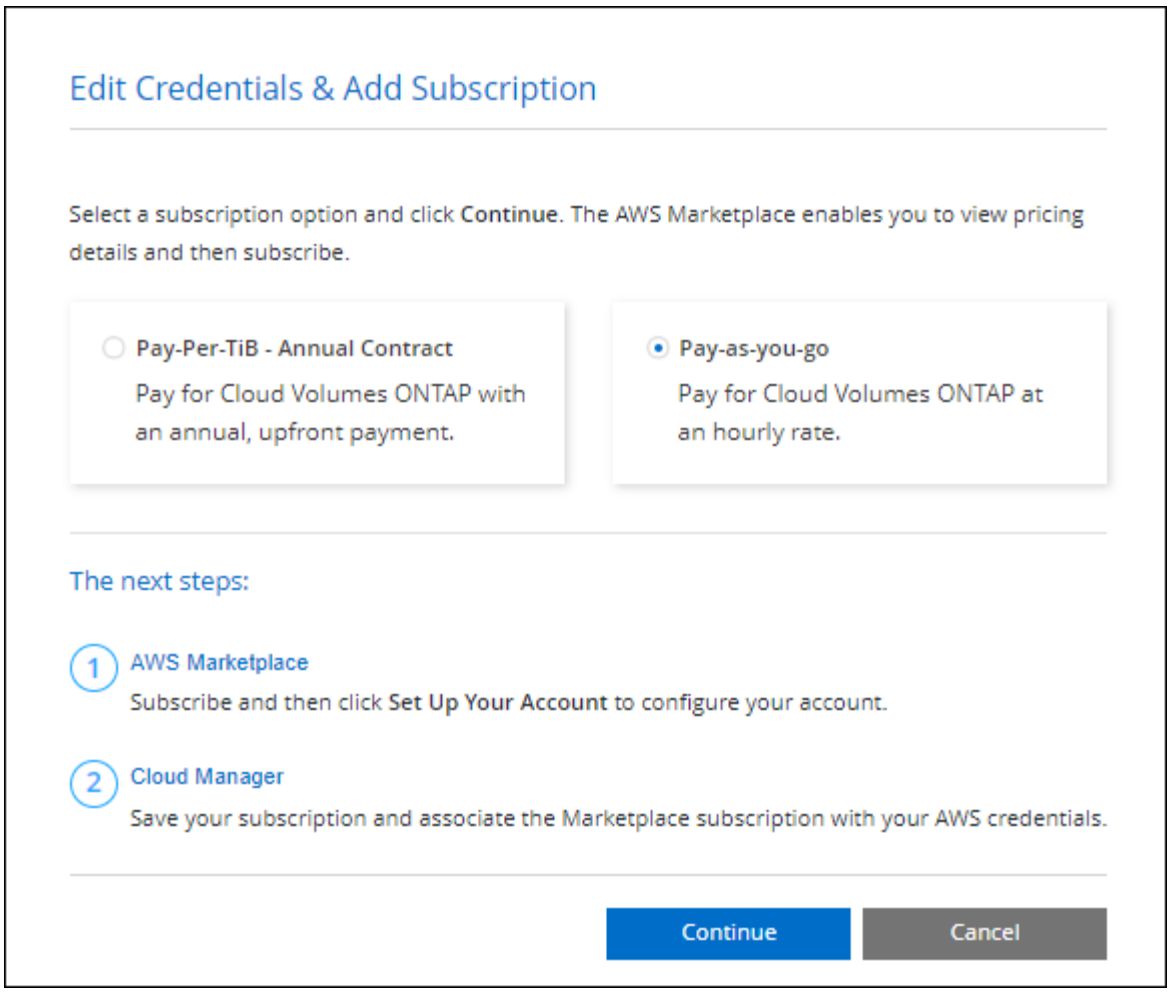
PAYGO-Abonnement

Zahlen Sie stundenweise, indem Sie das Angebot auf dem Marktplatz Ihres Cloud-Anbieters abonnieren.

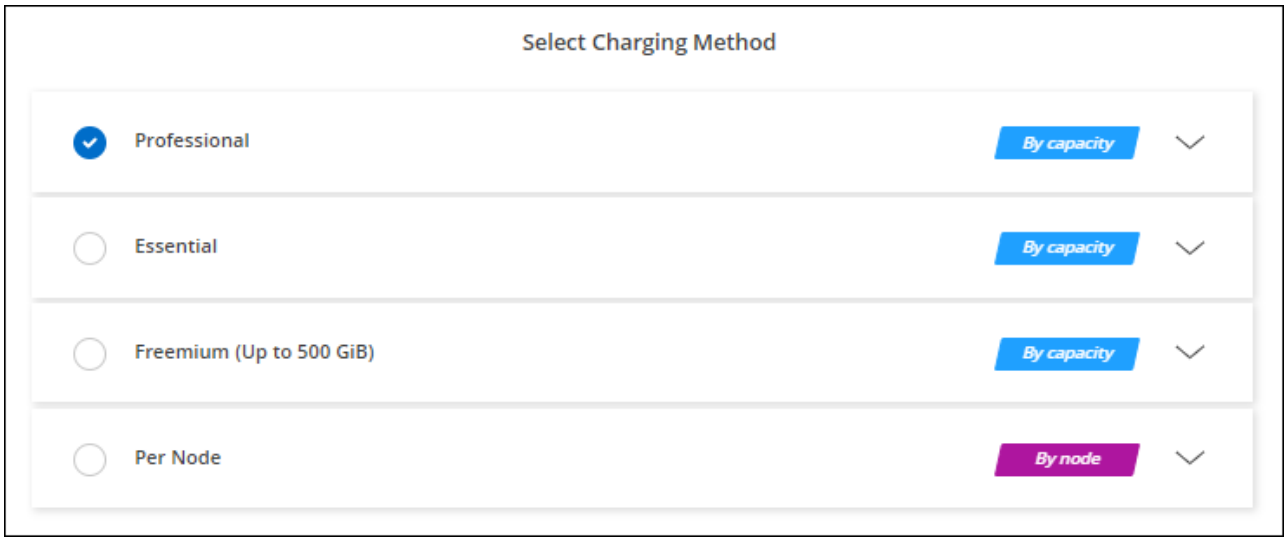
Wenn Sie ein Cloud Volumes ONTAP -System erstellen, werden Sie von der Konsole aufgefordert, die im AWS Marketplace verfügbare Vereinbarung zu abonnieren. Dieses Abonnement wird dann zum Aufladen mit dem System verknüpft. Sie können dasselbe Abonnement für zusätzliche Cloud Volumes ONTAP Systeme verwenden.

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten.
   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldeinformationen bearbeiten > Abonnement hinzufügen** und folgen Sie dann den Anweisungen, um das Pay-as-you-go-Angebot im AWS Marketplace zu abonnieren.



b. Nachdem Sie zur Konsole zurückgekehrt sind, wählen Sie auf der Seite mit den Abrechnungsmethoden ein kapazitätsbasiertes Paket aus.



"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in AWS an" .

Sie können die mit Ihren AWS-Konten verknüpften AWS Marketplace-Abonnements auf der Seite „Einstellungen > Anmeldeinformationen“ verwalten. "Erfahren Sie, wie Sie Ihre AWS-Konten und -Abonnements verwalten"

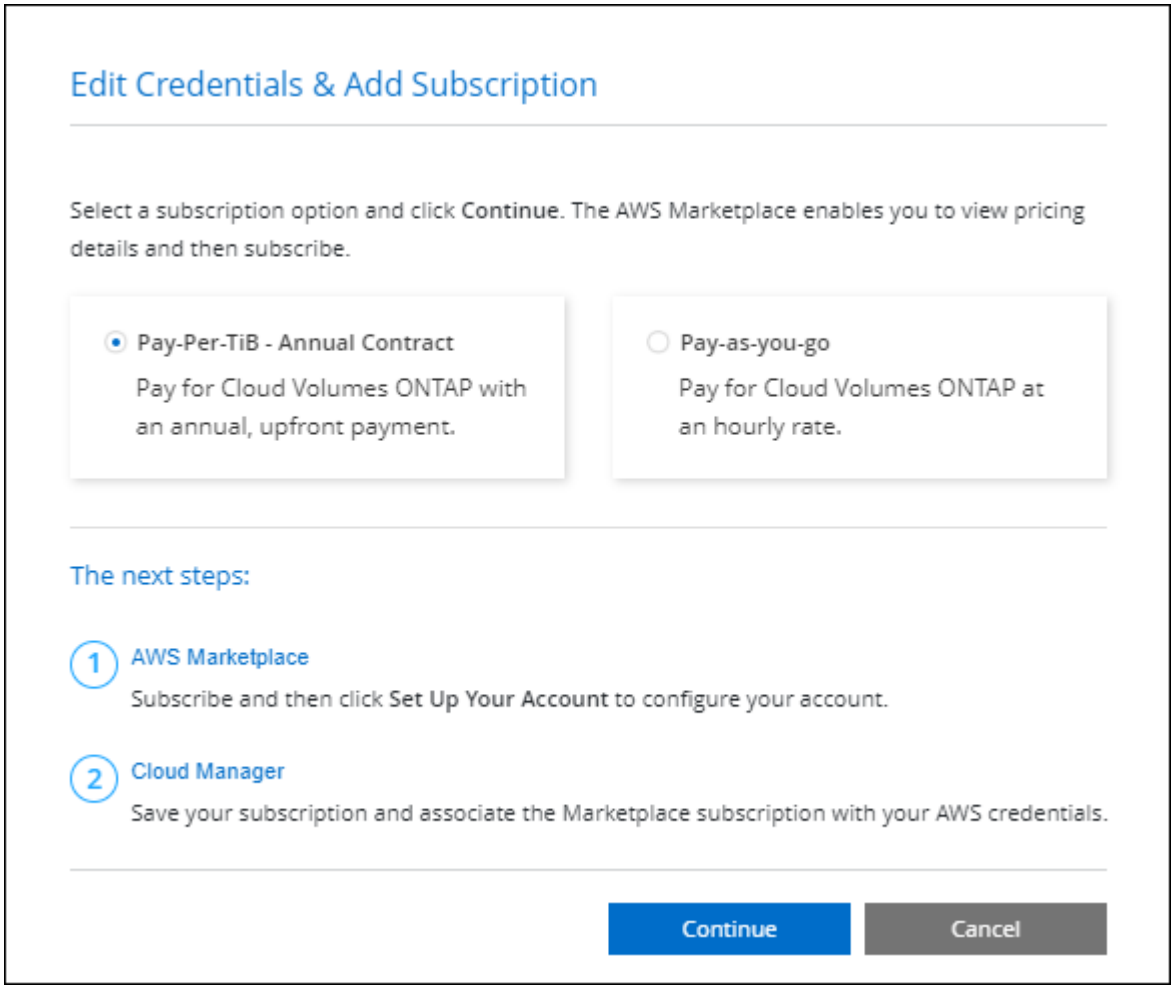
Jahresvertrag

Zahlen Sie jährlich, indem Sie einen Jahresvertrag auf dem Marktplatz Ihres Cloud-Anbieters erwerben.

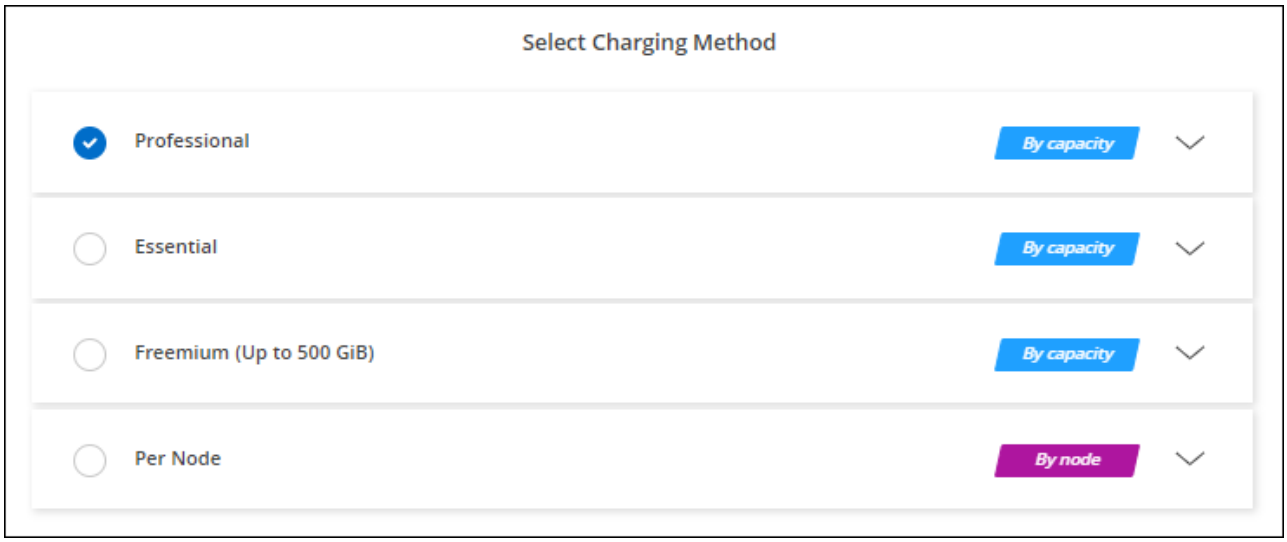
Ähnlich wie bei einem Stundenabonnement werden Sie von der Konsole aufgefordert, den Jahresvertrag zu abonnieren, der im AWS Marketplace verfügbar ist.

Schritte

1. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten.
   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldeinformationen bearbeiten > Abonnement hinzufügen** und folgen Sie dann den Anweisungen, um den Jahresvertrag im AWS Marketplace zu abonnieren.



   b. Nachdem Sie zur Konsole zurückgekehrt sind, wählen Sie auf der Seite mit den Abrechnungsmethoden ein kapazitätsbasiertes Paket aus.



"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in AWS an" .

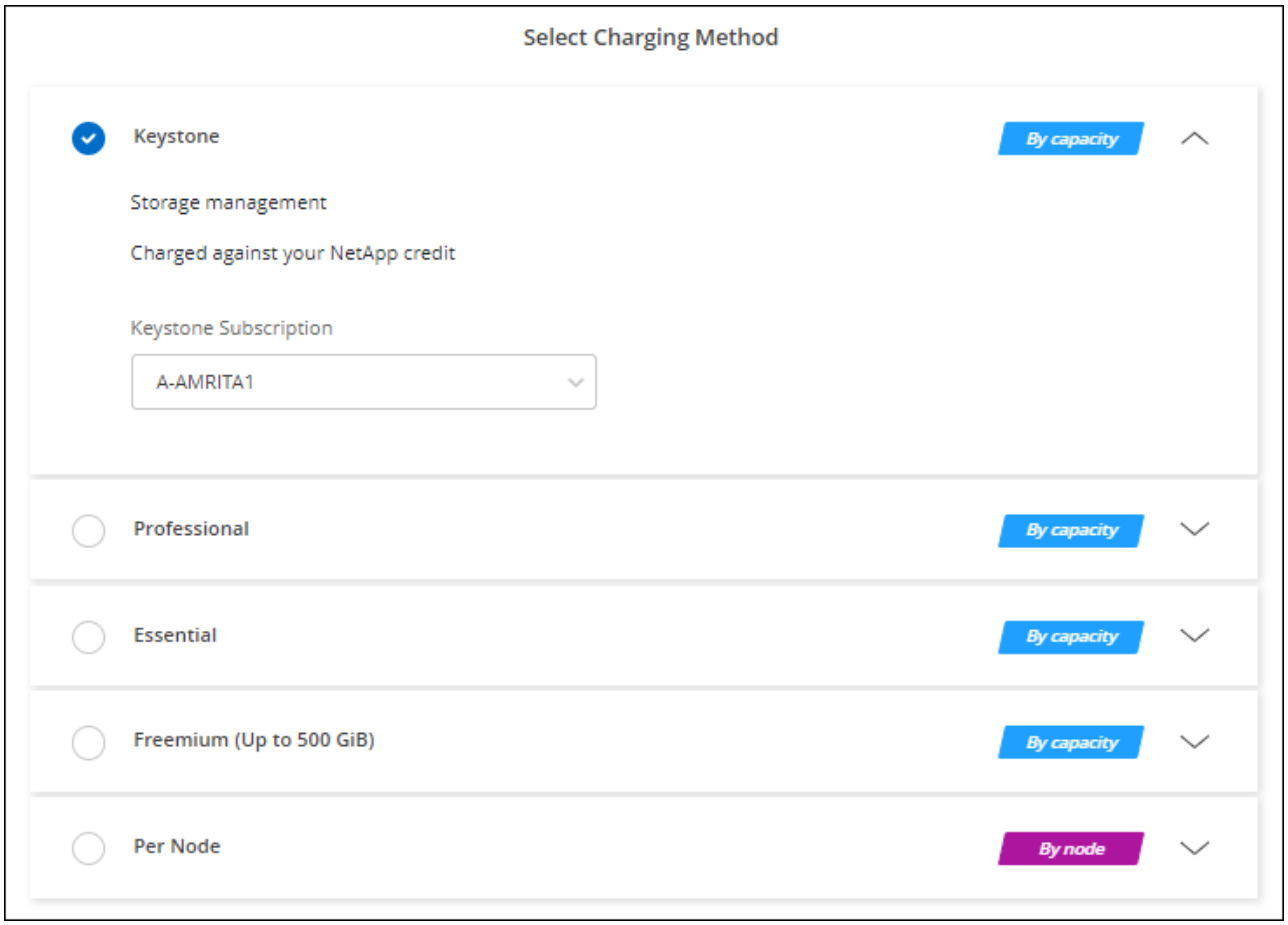
Keystone Abonnement

Bei einem Keystone -Abonnement handelt es sich um einen Abonnementdienst mit nutzungsabhängiger Bezahlung. "Erfahren Sie mehr über NetApp Keystone -Abonnements" .

Schritte

1. Wenn Sie noch kein Abonnement haben, "NetApp kontaktieren"
2. mailto:ng-keystone-success@netapp.com [Kontaktieren Sie NetApp], um Ihr Benutzerkonto mit einem oder mehreren Keystone Abonnements zu autorisieren.
3. Nachdem NetApp Ihr Konto autorisiert hat,"Verknüpfen Sie Ihre Abonnements zur Verwendung mit Cloud Volumes ONTAP" .
4. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten.

    a. Wählen Sie die Abrechnungsmethode „Keystone -Abonnement“ aus, wenn Sie zur Auswahl einer Abrechnungsmethode aufgefordert werden.



"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in AWS an" .

Knotenbasierte Lizenz

Eine knotenbasierte Lizenz ist die Lizenz der vorherigen Generation für Cloud Volumes ONTAP. Eine knotenbasierte Lizenz kann von NetApp (BYOL) erworben werden und ist nur in bestimmten Fällen für Lizenzverlängerungen verfügbar. Weitere Informationen finden Sie unter:

- "Ende der Verfügbarkeit knotenbasierter Lizenzen"
- "Ende der Verfügbarkeit von knotenbasierten Lizenzen"
- "Konvertieren Sie eine knotenbasierte Lizenz in eine kapazitätsbasierte Lizenz"

Stellen Sie Cloud Volumes ONTAP in AWS mithilfe der Schnellbereitstellung bereit

Sie können Cloud Volumes ONTAP in AWS mithilfe einer schnellen Bereitstellungsmethode sowohl für Einzelknoten- als auch für Hochverfügbarkeitskonfigurationen (HA) bereitstellen. Dieser vereinfachte Prozess reduziert die Bereitstellungsschritte im Vergleich zur erweiterten Methode. Darüber hinaus bietet es mehr Übersichtlichkeit im Arbeitsablauf, indem es automatisch Standardwerte auf einer einzigen Seite festlegt und die Navigation minimiert.

Bevor Sie beginnen

Sie benötigen Folgendes, um ein Cloud Volumes ONTAP -System in AWS von der NetApp Console aus hinzuzufügen.

- Ein Konsolenagent, der aktiv ist und läuft.
  - Sie sollten über eine "Konsolenagent, der mit Ihrem Projekt oder Arbeitsbereich verknüpft ist" .
  - "Sie sollten darauf vorbereitet sein, den Konsolenagenten immer laufen zu lassen" .
- Ein Verständnis der Konfiguration, die Sie verwenden möchten.

  Sie sollten sich vorbereitet haben, indem Sie eine Konfiguration ausgewählt und AWS-Netzwerkinformationen von Ihrem Administrator eingeholt haben. Weitere Einzelheiten finden Sie unter"Planen Ihrer Cloud Volumes ONTAP Konfiguration" .
- Ein Verständnis dafür, was zum Einrichten der Lizenzierung für Cloud Volumes ONTAP erforderlich ist.

  "Erfahren Sie, wie Sie die Lizenzierung einrichten" .
- DNS und Active Directory für CIFS-Konfigurationen.

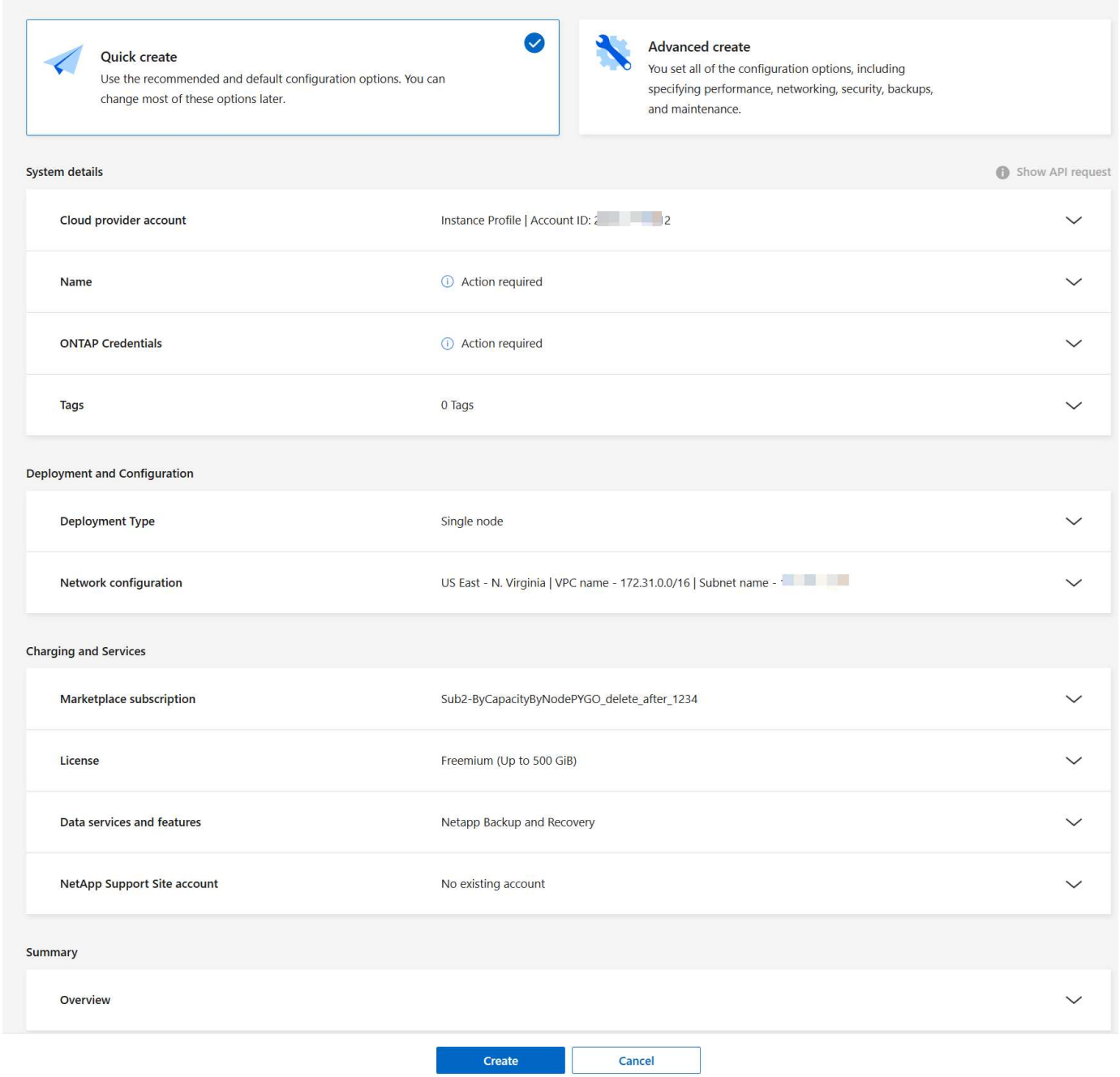
  Weitere Einzelheiten finden Sie unter"Netzwerkanforderungen für Cloud Volumes ONTAP in AWS" .

Informationen zu diesem Vorgang

Unmittelbar nachdem Sie das Cloud Volumes ONTAP -System erstellt haben, startet die NetApp Console eine Testinstanz im angegebenen VPC, um die Konnektivität zu überprüfen. Bei Erfolg beendet die Konsole die Instanz sofort und beginnt dann mit der Bereitstellung des Systems. Wenn die Konsole die Konnektivität nicht überprüfen kann, schlägt die Erstellung des Systems fehl. Die Testinstanz ist entweder eine `t2.nano` (für Standard-VPC-Miete) oder eine `m3.medium` (für dedizierte VPC-Miete).

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Klicken Sie auf der Canvas-Seite auf **System hinzufügen** und folgen Sie den Anweisungen.
3. Wählen Sie **Amazon Web Services** > * Cloud Volumes ONTAP* > **Neu hinzufügen**. Die Option **Schnell erstellen** ist standardmäßig ausgewählt.



Systemdetails

1. **Cloud-Anbieterkonto**: Die Kontodetails werden automatisch basierend auf Ihrem ausgewählten Konsolenagenten ausgefüllt. Wenn Sie mehrere Konten haben, wählen Sie das Konto aus, das Sie verwenden möchten. Wenn ein Konsolenagent nicht verfügbar ist, werden Sie aufgefordert, "Erstellen Sie einen Konsolenagenten" .
2. **Name**: Der Systemname. Die Konsole verwendet den Systemnamen (Clusternamen), um das Cloud Volumes ONTAP -System und die Amazon EC2-Instanz zu benennen. Wenn Sie diese Option auswählen, wird der Name auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet.
3. * ONTAP -Anmeldeinformationen* Dies sind die Anmeldeinformationen für das Cloud Volumes ONTAP Cluster-Administratorkonto. Sie können diese Anmeldeinformationen verwenden, um über ONTAP System Manager oder die ONTAP CLI eine Verbindung zu Cloud Volumes ONTAP herzustellen. Sie können den Standardbenutzernamen *admin* beibehalten oder in einen benutzerdefinierten Benutzernamen ändern.
4. **Tags** AWS-Tags sind Metadaten für Ihre AWS-Ressourcen. Die Konsole fügt die Tags der Cloud Volumes

ONTAP -Instanz und jeder mit der Instanz verknüpften AWS-Ressource hinzu. Sie können beim Erstellen eines Cloud Volumes ONTAP -Systems bis zu 15 Tags über die Benutzeroberfläche hinzufügen und nach der Erstellung weitere hinzufügen. Beachten Sie, dass die API Sie beim Erstellen eines Systems nicht auf vier Tags beschränkt. Informationen zu Tags finden Sie unter "AWS-Dokumentation: Markieren Ihrer Amazon EC2-Ressourcen" .

Bereitstellung und Konfiguration

1. **Bereitstellungstyp**: Wählen Sie den Bereitstellungstyp aus, den Sie verwenden möchten: Einzelknoten, Hochverfügbarkeit (HA) in einer einzelnen Verfügbarkeitszone (AZ) oder HA in einer Mehrfach-AZ.
2. **Netzwerkkonfiguration**: Geben Sie die Netzwerkinformationen ein, die Sie im "AWS-Arbeitsblatt" .
   a. **AWS-Region**: Standardmäßig ist die Region des zugehörigen Cloud-Kontos ausgewählt, das über VPC mit Subnetzressourcen verfügt.
   b. **VPC**: Geben Sie eine VPC für die AWS-Region mit einem Subnetz ein. Wenn keine Subnetze vorhanden sind, wird der Standardwert für die VPC ausgewählt.
   c. **Subnetz**: Sie können ein Subnetz für die VPC nur für eine Einzelknotenbereitstellung oder eine HA-Bereitstellung in einer einzelnen AZ auswählen.

Hohe Verfügbarkeit

Wenn Sie die HA-Konfiguration ausgewählt haben, geben Sie die folgenden Informationen ein:

HA in einzelner AZ

1. **Mediatorzugriff**: Geben Sie die Mediatorzugriffsinformationen an. Der Mediator ist eine separate Instanz, die den Zustand des HA-Paares überwacht und im Fehlerfall ein Quorum bereitstellt. Geben Sie den Namen des Schlüsselpaars an, damit die Mediatorinstanz eine Verbindung mit dem AWS EC2-Dienst herstellen kann, und wählen Sie die Verbindungsmethode aus.

HA in mehreren AZ

1. **Verfügbarkeitszonen und Mediator**: Wählen Sie die Verfügbarkeitszonen (AZs) für jeden Knoten und den Mediator sowie die entsprechenden Subnetze aus, in denen Sie das Cloud Volumes ONTAP HA-Paar bereitstellen möchten.
2. **Floating IPs**: Wenn Sie mehrere AZs auswählen, geben Sie die Floating-IP-Adressen für die NFS- und CIFS-Dienste sowie die Cluster- und SVM-Verwaltung an. Die IP-Adressen müssen für alle VPCs in der Region außerhalb des CIDR-Blocks liegen. Weitere Einzelheiten finden Sie unter"AWS-Netzwerkanforderungen für Cloud Volumes ONTAP HA in mehreren AZs" .
3. **Mediatorzugriff**: Geben Sie die Mediatorzugriffsinformationen an. Der Mediator ist eine separate Instanz, die den Zustand des HA-Paares überwacht und im Fehlerfall ein Quorum bereitstellt. Geben Sie den Namen des Schlüsselpaars an, damit die Mediatorinstanz eine Verbindung mit dem AWS EC2-Dienst herstellen kann, und wählen Sie die Verbindungsmethode aus.
4. **Routentabellen**: Wenn Sie mehrere AZs ausgewählt haben, wählen Sie die Routentabellen aus, die Routen zu den Floating-IP-Adressen enthalten. Wenn Sie mehr als eine Routentabelle haben, ist es wichtig, die richtigen Routentabellen auszuwählen. Andernfalls haben einige Clients möglicherweise keinen Zugriff auf das Cloud Volumes ONTAP HA-Paar. Weitere Informationen zu Routentabellen finden Sie im "AWS-Dokumentation: Routentabellen" .

Laden und Dienste

1. **Marketplace-Abonnement**: Wählen Sie das AWS-Marketplace-Abonnement aus, das Sie mit diesem Cloud Volumes ONTAP -System verwenden möchten.
2. **Lizenz**: Wählen Sie den Lizenztyp aus, den Sie mit diesem Cloud Volumes ONTAP -System verwenden

möchten. Sie können zwischen Professional-, Essential- und Premium-Lizenzen wählen. Informationen zu verschiedenen Lizenzen finden Sie unter"Erfahren Sie mehr über Cloud Volumes ONTAP -Lizenzen" .

3. **Datendienste und -funktionen**: Lassen Sie die Dienste aktiviert oder deaktivieren Sie die Dienste, die Sie nicht mit Cloud Volumes ONTAP verwenden möchten.
   - "Erfahren Sie mehr über die NetApp Klassifizierung"
   - "Erfahren Sie mehr über NetApp Backup and Recovery"
   - "Erfahren Sie mehr über WORM-Speicher auf Cloud Volumes ONTAP"

     Wenn Sie WORM und Daten-Tiering nutzen möchten, müssen Sie Backup und Recovery deaktivieren und ein Cloud Volumes ONTAP System mit Version 9.8 oder höher bereitstellen.

   - * NetApp Support Site-Konto*: Wenn Sie mehrere Konten haben, wählen Sie das Konto aus, das Sie verwenden möchten.

Zusammenfassung

Überprüfen oder bearbeiten Sie die eingegebenen Details und klicken Sie dann auf **Erstellen**.

Ändern Sie nach Abschluss des Bereitstellungsprozesses nicht die systemgenerierten Cloud Volumes ONTAP -Konfigurationen im AWS-Cloud-Portal, insbesondere nicht die System-Tags. Alle an diesen Konfigurationen vorgenommenen Änderungen können zu unerwartetem Verhalten oder Datenverlust führen.

Weiterführende Links

- "Planen Ihrer Cloud Volumes ONTAP Konfiguration"
- "Stellen Sie Cloud Volumes ONTAP in AWS mithilfe der erweiterten Bereitstellung bereit"

Starten Sie Cloud Volumes ONTAP in AWS

Sie können Cloud Volumes ONTAP in einer Einzelsystemkonfiguration oder als HA-Paar in AWS starten. Diese Methode bietet eine erweiterte Bereitstellungserfahrung, die mehr Konfigurationsoptionen und Flexibilität bietet als die Methode der schnellen Bereitstellung.

Bevor Sie beginnen

Bevor Sie beginnen, benötigen Sie Folgendes.

- Ein Konsolenagent, der aktiv ist und läuft.
  - Sie sollten über eine "Konsolenagent, der mit Ihrem System verknüpft ist" .
  - "Sie sollten darauf vorbereitet sein, den Konsolenagenten immer laufen zu lassen" .
- Ein Verständnis der Konfiguration, die Sie verwenden möchten.

  Sie sollten sich vorbereitet haben, indem Sie eine Konfiguration ausgewählt und AWS-Netzwerkinformationen von Ihrem Administrator eingeholt haben. Weitere Einzelheiten finden Sie unter"Planen Ihrer Cloud Volumes ONTAP Konfiguration" .

- Ein Verständnis dafür, was zum Einrichten der Lizenzierung für Cloud Volumes ONTAP erforderlich ist.

"Erfahren Sie, wie Sie die Lizenzierung einrichten" .

- DNS und Active Directory für CIFS-Konfigurationen.

  Weitere Einzelheiten finden Sie unter"Netzwerkanforderungen für Cloud Volumes ONTAP in AWS" .

Starten Sie ein Cloud Volumes ONTAP -System mit einem Knoten in AWS

Wenn Sie Cloud Volumes ONTAP in AWS starten möchten, müssen Sie in der NetApp Console ein neues System erstellen.

Informationen zu diesem Vorgang

Unmittelbar nach der Erstellung des Systems startet die Konsole eine Testinstanz in der angegebenen VPC, um die Konnektivität zu überprüfen. Bei Erfolg beendet die Konsole die Instanz sofort und beginnt dann mit der Bereitstellung des Cloud Volumes ONTAP Systems. Wenn die Konnektivität nicht überprüft werden kann, schlägt die Systemerstellung fehl. Die Testinstanz ist entweder eine `t2.nano` (für Standard-VPC-Miete) oder `m3.medium` (für dedizierte VPC-Miete).

Schritte

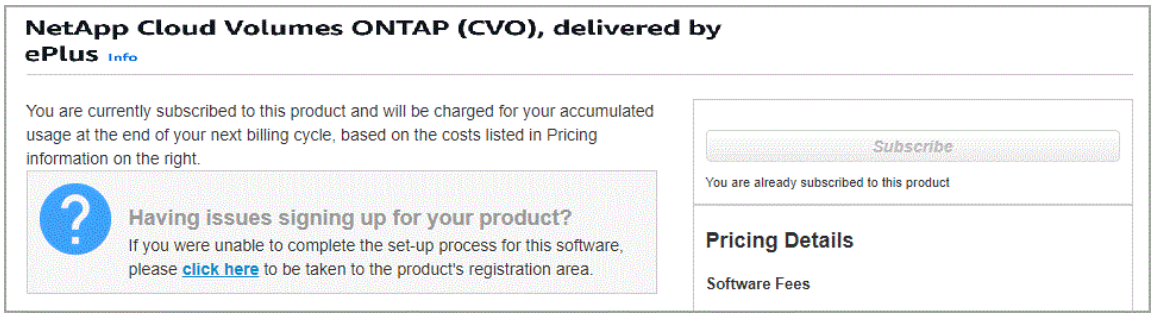
1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Anweisungen.
3. Wählen Sie **Amazon Web Services** und * Cloud Volumes ONTAP Single Node*.
4. Wählen Sie **Erweiterte Erstellung**. Da standardmäßig der Modus „Schnell erstellen“ ausgewählt ist, wird möglicherweise eine Meldung mit Standardwerten angezeigt. Klicken Sie auf **Weiter**.
5. Wenn Sie dazu aufgefordert werden, "Erstellen Sie einen Konsolenagenten" .
6. **Details und Anmeldeinformationen**: Ändern Sie optional die AWS-Anmeldeinformationen und das Abonnement, geben Sie einen Systemnamen ein, fügen Sie bei Bedarf Tags hinzu und geben Sie dann ein Kennwort ein.

   Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Tabelle werden die Felder beschrieben, für die Sie möglicherweise Anleitungen benötigen:

Feld	Beschreibung
Systemname	Die Konsole verwendet den Systemnamen, um sowohl das Cloud Volumes ONTAP -System als auch die Amazon EC2-Instanz zu benennen. Wenn Sie diese Option auswählen, wird der Name auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet.
Tags hinzufügen	AWS-Tags sind Metadaten für Ihre AWS-Ressourcen. Die Konsole fügt die Tags der Cloud Volumes ONTAP -Instanz und jeder mit der Instanz verknüpften AWS-Ressource hinzu. Sie können beim Erstellen eines Systems bis zu vier Tags über die Benutzeroberfläche hinzufügen und nach der Erstellung weitere hinzufügen. Beachten Sie, dass die API Sie beim Erstellen eines Systems nicht auf vier Tags beschränkt. Informationen zu Tags finden Sie unter "AWS-Dokumentation: Markieren Ihrer Amazon EC2-Ressourcen" .

Feld	Beschreibung
Benutzername und Passwort	Dies sind die Anmeldeinformationen für das Cloud Volumes ONTAP Clusteradministratorkonto. Sie können diese Anmeldeinformationen verwenden, um über ONTAP System Manager oder die ONTAP CLI eine Verbindung zu Cloud Volumes ONTAP herzustellen. Behalten Sie den Standardbenutzernamen *admin* bei oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.
Anmeldeinformationen bearbeiten	Wählen Sie die AWS-Anmeldeinformationen aus, die mit dem Konto verknüpft sind, in dem Sie dieses System bereitstellen möchten. Sie können das AWS-Marktplatz-Abonnement auch mit diesem Cloud Volumes ONTAP System verknüpfen. Klicken Sie auf **Abonnement hinzufügen**, um die ausgewählten Anmeldeinformationen einem neuen AWS Marketplace-Abonnement zuzuordnen. Das Abonnement kann ein Jahresvertrag sein oder die Nutzung von Cloud Volumes ONTAP nach Stundensatz. "Erfahren Sie, wie Sie der NetApp Console zusätzliche AWS-Anmeldeinformationen hinzufügen" .

Wenn mehrere IAM-Benutzer im selben AWS-Konto arbeiten, muss jeder Benutzer ein Abonnement abschließen. Nachdem der erste Benutzer sich angemeldet hat, informiert der AWS-Marktplatz nachfolgende Benutzer darüber, dass sie bereits angemeldet sind, wie im Bild unten gezeigt. Solange für das AWS-Konto ein Abonnement besteht, muss sich jeder IAM-Benutzer mit diesem Abonnement verknüpfen. Wenn die unten angezeigte Meldung angezeigt wird, klicken Sie auf den Link **hier klicken**, um zur Konsolen-Website zu gelangen und den Vorgang abzuschließen.



7. **Dienste**: Lassen Sie die Dienste aktiviert oder deaktivieren Sie die einzelnen Dienste, die Sie nicht mit Cloud Volumes ONTAP verwenden möchten.
   - "Erfahren Sie mehr über die NetApp Data Classification"
   - "Erfahren Sie mehr über NetApp Backup and Recovery"

   Wenn Sie WORM und Daten-Tiering nutzen möchten, müssen Sie Backup und Recovery deaktivieren und ein Cloud Volumes ONTAP System mit Version 9.8 oder höher bereitstellen.

8. **Standort und Konnektivität**: Geben Sie die Netzwerkinformationen ein, die Sie im "AWS-Arbeitsblatt" .

   In der folgenden Tabelle werden die Felder beschrieben, für die Sie möglicherweise Anleitungen benötigen:

Feld	Beschreibung
VPC	Wenn Sie über einen AWS Outpost verfügen, können Sie in diesem Outpost ein Cloud Volumes ONTAP -System mit einem einzelnen Knoten bereitstellen, indem Sie die Outpost VPC auswählen. Die Erfahrung ist die gleiche wie bei jedem anderen VPC, das sich in AWS befindet.
Generierte Sicherheitsgruppe	Wenn Sie die Sicherheitsgruppe von der Konsole erstellen lassen, müssen Sie auswählen, wie Sie den Datenverkehr zulassen: • Wenn Sie **Nur ausgewählte VPC** auswählen, ist die Quelle für eingehenden Datenverkehr der Subnetzbereich der ausgewählten VPC und der Subnetzbereich der VPC, in der sich der Konsolenagent befindet. Dies ist die empfohlene Option. • Wenn Sie **Alle VPCs** auswählen, ist die Quelle für eingehenden Datenverkehr der IP-Bereich 0.0.0.0/0.
Vorhandene Sicherheitsgruppe verwenden	Wenn Sie eine vorhandene Firewall-Richtlinie verwenden, stellen Sie sicher, dass diese die erforderlichen Regeln enthält. "Erfahren Sie mehr über Firewall-Regeln für Cloud Volumes ONTAP" .

9. **Datenverschlüsselung**: Wählen Sie keine Datenverschlüsselung oder von AWS verwaltete Verschlüsselung.

   Für die von AWS verwaltete Verschlüsselung können Sie einen anderen Customer Master Key (CMK) aus Ihrem Konto oder einem anderen AWS-Konto auswählen.

   Sie können die AWS-Datenverschlüsselungsmethode nicht mehr ändern, nachdem Sie ein Cloud Volumes ONTAP System erstellt haben.

   "Erfahren Sie, wie Sie AWS KMS für Cloud Volumes ONTAP einrichten" .

   "Erfahren Sie mehr über unterstützte Verschlüsselungstechnologien" .

10. **Abrechnungsmethoden und NSS-Konto**: Geben Sie an, welche Abrechnungsoption Sie mit diesem System verwenden möchten, und geben Sie dann ein NetApp Support Site-Konto an.
    - "Erfahren Sie mehr über die Lizenzierungsoptionen für Cloud Volumes ONTAP" .
    - "Erfahren Sie, wie Sie die Lizenzierung einrichten" .
11. * Cloud Volumes ONTAP -Konfiguration* (nur jährlicher AWS-Marktplatzvertrag): Überprüfen Sie die Standardkonfiguration und klicken Sie auf **Weiter** oder klicken Sie auf **Konfiguration ändern**, um Ihre eigene Konfiguration auszuwählen.

    Wenn Sie die Standardkonfiguration beibehalten, müssen Sie nur ein Volume angeben und dann die Konfiguration überprüfen und genehmigen.

12. **Vorkonfigurierte Pakete**: Wählen Sie eines der Pakete aus, um Cloud Volumes ONTAP schnell zu starten, oder klicken Sie auf **Konfiguration ändern**, um Ihre eigene Konfiguration auszuwählen.

    Wenn Sie sich für eines der Pakete entscheiden, müssen Sie lediglich ein Volumen angeben und anschließend die Konfiguration prüfen und freigeben.

13. **IAM-Rolle**: Behalten Sie am besten die Standardoption bei, damit die Konsole die Rolle für Sie erstellen kann.

Wenn Sie Ihre eigene Police verwenden möchten, muss diese"Richtlinienanforderungen für Cloud Volumes ONTAP Knoten" .

14. **Lizenzierung**: Ändern Sie die Cloud Volumes ONTAP -Version nach Bedarf und wählen Sie einen Instanztyp und die Instanzmietdauer aus.

> Wenn für die ausgewählte Version ein neuerer Release Candidate, eine allgemeine Verfügbarkeit oder ein Patch-Release verfügbar ist, aktualisiert die Konsole das System beim Erstellen des Systems auf diese Version. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.13.1 auswählen und 9.13.1 P4 verfügbar ist. Das Update erfolgt nicht von einer Version zur nächsten, beispielsweise von 9.13 auf 9.14.

15. **Zugrunde liegende Speicherressourcen**: Wählen Sie einen Datenträgertyp, konfigurieren Sie den zugrunde liegenden Speicher und entscheiden Sie, ob die Datenschichtung aktiviert bleiben soll.

    Beachten Sie Folgendes:

    - Der Datenträgertyp ist für das Anfangsvolume (und Aggregat). Sie können für nachfolgende Volumes (und Aggregate) einen anderen Datenträgertyp auswählen.
    - Wenn Sie eine gp3- oder io1-Festplatte auswählen, verwendet die Konsole die Elastic Volumes-Funktion in AWS, um die zugrunde liegende Speicherfestplattenkapazität bei Bedarf automatisch zu erhöhen. Sie können die anfängliche Kapazität basierend auf Ihrem Speicherbedarf auswählen und sie nach der Bereitstellung von Cloud Volumes ONTAP überarbeiten. "Erfahren Sie mehr über die Unterstützung für Elastic Volumes in AWS" .
    - Wenn Sie eine GP2- oder ST1-Festplatte auswählen, können Sie eine Festplattengröße für alle Festplatten im anfänglichen Aggregat und für alle zusätzlichen Aggregate auswählen, die die Konsole erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der erweiterten Zuordnungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.
    - Sie können beim Erstellen oder Bearbeiten eines Volumes eine bestimmte Volume-Tiering-Richtlinie auswählen.
    - Wenn Sie das Daten-Tiering deaktivieren, können Sie es für nachfolgende Aggregate aktivieren.

      "Erfahren Sie, wie Data Tiering funktioniert" .

16. **Schreibgeschwindigkeit & WORM**:

    a. Wählen Sie bei Bedarf die Schreibgeschwindigkeit **Normal** oder **Hoch**.

       "Erfahren Sie mehr über die Schreibgeschwindigkeit" .

    b. Aktivieren Sie bei Bedarf den WORM-Speicher (Write Once, Read Many).

       WORM kann nicht aktiviert werden, wenn die Datenschichtung für Cloud Volumes ONTAP Version 9.7 und darunter aktiviert wurde. Das Zurücksetzen oder Downgrade auf Cloud Volumes ONTAP 9.8 ist nach der Aktivierung von WORM und Tiering blockiert.

    "Erfahren Sie mehr über WORM-Speicher" .

    a. Wenn Sie den WORM-Speicher aktivieren, wählen Sie die Aufbewahrungsdauer aus.

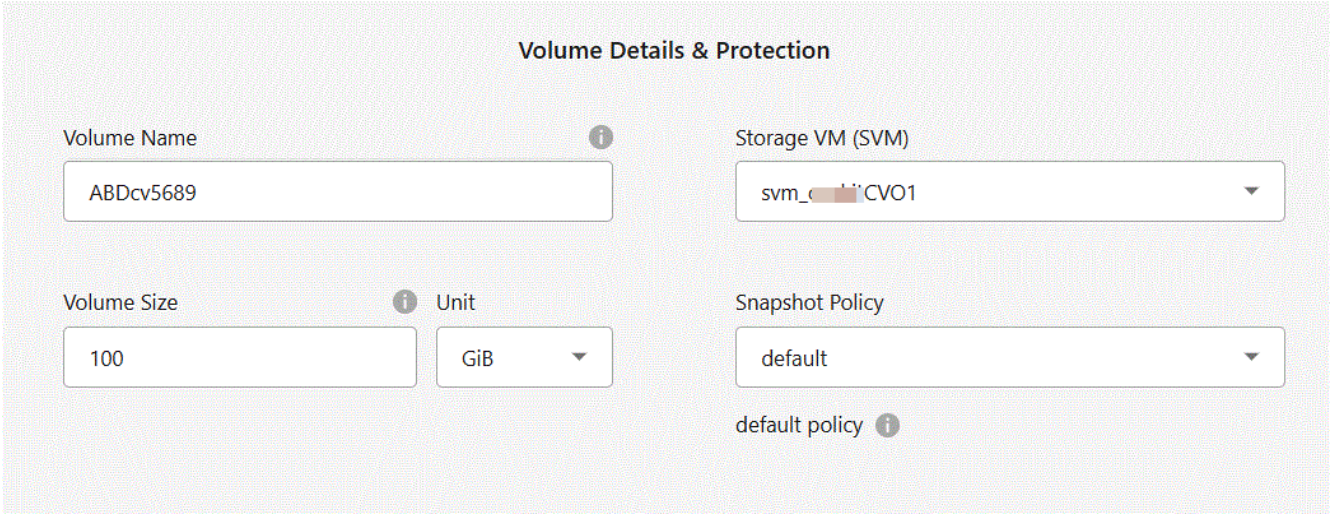
17. **Volume erstellen**: Geben Sie Details für das neue Volume ein oder klicken Sie auf **Überspringen**.

    "Erfahren Sie mehr über unterstützte Clientprotokolle und -versionen" .

Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Tabelle werden die Felder beschrieben, für die Sie möglicherweise Anleitungen benötigen:

Feld	Beschreibung
Größe	Die maximale Größe, die Sie eingeben können, hängt weitgehend davon ab, ob Sie Thin Provisioning aktivieren. Dadurch können Sie ein Volume erstellen, das größer ist als der ihm aktuell zur Verfügung stehende physische Speicher.
Zugriffskontrolle (nur für NFS)	Eine Exportrichtlinie definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt die Konsole einen Wert ein, der Zugriff auf alle Instanzen im Subnetz gewährt.
Berechtigungen und Benutzer/Gruppen (nur für CIFS)	Mit diesen Feldern können Sie die Zugriffsebene auf eine Freigabe für Benutzer und Gruppen steuern (auch als Zugriffskontrolllisten oder ACLs bezeichnet). Sie können lokale oder Domänen-Windows-Benutzer oder -Gruppen oder UNIX-Benutzer oder -Gruppen angeben. Wenn Sie einen Windows-Domänenbenutzernamen angeben, müssen Sie die Domäne des Benutzers im Format Domäne\Benutzername angeben.
Snapshot-Richtlinie	Eine Snapshot-Kopierrichtlinie gibt die Häufigkeit und Anzahl der automatisch erstellten NetApp Snapshot-Kopien an. Eine NetApp Snapshot-Kopie ist ein zeitpunktbezogenes Dateisystem-Image, das keine Auswirkungen auf die Leistung hat und nur minimalen Speicherplatz benötigt. Sie können die Standardrichtlinie oder keine auswählen. Für vorübergehende Daten können Sie „Keine“ auswählen, beispielsweise „tempdb“ für Microsoft SQL Server.
Erweiterte Optionen (nur für NFS)	Wählen Sie eine NFS-Version für das Volume aus: entweder NFSv3 oder NFSv4.
Initiatorgruppe und IQN (nur für iSCSI)	iSCSI-Speicherziele werden als LUNs (logische Einheiten) bezeichnet und Hosts als Standardblockgeräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Hostknotennamen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. iSCSI-Ziele stellen über Standard-Ethernet-Netzwerkadapter (NICs), TCP-Offload-Engine-Karten (TOE) mit Software-Initiatoren, konvergente Netzwerkadapter (CNAs) oder dedizierte Hostbusadapter (HBAs) eine Verbindung zum Netzwerk her und werden durch iSCSI-qualifizierte Namen (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt die Konsole automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volume erstellt haben, sodass keine Verwaltung erforderlich ist. Nachdem Sie das Volume erstellt haben,"Verwenden Sie den IQN, um von Ihren Hosts aus eine Verbindung zum LUN herzustellen" .

Das folgende Bild zeigt die erste Seite des Assistenten zur Volumeerstellung:



18. **CIFS-Setup**: Wenn Sie das CIFS-Protokoll gewählt haben, richten Sie einen CIFS-Server ein.

Feld	Beschreibung
DNS Primäre und sekundäre IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgelisteten DNS-Server müssen die Service Location Records (SRV) enthalten, die zum Auffinden der Active Directory-LDAP-Server und Domänencontroller für die Domäne erforderlich sind, der der CIFS-Server beitreten wird.
Beitretende Active Directory-Domäne	Der FQDN der Active Directory (AD)-Domäne, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zum Beitritt zur Domäne berechtigt sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
NetBIOS-Name des CIFS-Servers	Ein CIFS-Servername, der in der AD-Domäne eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domäne, die mit dem CIFS-Server verknüpft werden soll. Der Standardwert ist CN=Computers. Wenn Sie AWS Managed Microsoft AD als AD-Server für Cloud Volumes ONTAP konfigurieren, sollten Sie in dieses Feld **OU=Computers,OU=corp** eingeben.
DNS-Domäne	Die DNS-Domäne für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen ist die Domäne dieselbe wie die AD-Domäne.
NTP-Server	Wählen Sie **Active Directory-Domäne verwenden**, um einen NTP-Server mithilfe des Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Weitere Informationen finden Sie im "Dokumentation zur NetApp Console" für Details. Beachten Sie, dass Sie einen NTP-Server nur beim Erstellen eines CIFS-Servers konfigurieren können. Es ist nicht mehr konfigurierbar, nachdem Sie den CIFS-Server erstellt haben.

19. **Nutzungsprofil, Datenträgertyp und Tiering-Richtlinie**: Wählen Sie aus, ob Sie Speichereffizienzfunktionen aktivieren möchten, und bearbeiten Sie bei Bedarf die Volume-Tiering-Richtlinie.

    Weitere Informationen finden Sie unter"Grundlegendes zu Volume-Nutzungsprofilen" ,"Übersicht über Data

Tiering" , Und "KB: Welche Inline-Speichereffizienzfunktionen werden mit CVO unterstützt?"

20. **Überprüfen und genehmigen**: Überprüfen und bestätigen Sie Ihre Auswahl.
    a. Überprüfen Sie die Details zur Konfiguration.
    b. Klicken Sie auf **Weitere Informationen**, um Details zum Support und den AWS-Ressourcen anzuzeigen, die über die Konsole erworben werden.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie auf **Los**.

Ergebnis

Die Konsole startet die Cloud Volumes ONTAP Instanz. Sie können den Fortschritt auf der Seite **Audit** verfolgen.

Wenn beim Starten der Cloud Volumes ONTAP Instanz Probleme auftreten, überprüfen Sie die Fehlermeldung. Sie können auch das System auswählen und auf **Umgebung neu erstellen** klicken.

Weitere Hilfe finden Sie unter "NetApp Cloud Volumes ONTAP Unterstützung" .

Ändern Sie nach Abschluss des Bereitstellungsprozesses nicht die systemgenerierten Cloud Volumes ONTAP -Konfigurationen im AWS-Cloud-Portal, insbesondere nicht die System-Tags. Alle an diesen Konfigurationen vorgenommenen Änderungen können zu unerwartetem Verhalten oder Datenverlust führen.

Nach Abschluss

- Wenn Sie eine CIFS-Freigabe bereitgestellt haben, erteilen Sie Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner und stellen Sie sicher, dass diese Benutzer auf die Freigabe zugreifen und eine Datei erstellen können.
- Wenn Sie Kontingente auf Volumes anwenden möchten, verwenden Sie ONTAP System Manager oder die ONTAP CLI.

  Mithilfe von Kontingenten können Sie den Speicherplatz und die Anzahl der von einem Benutzer, einer Gruppe oder einem Qtree verwendeten Dateien beschränken oder verfolgen.

Starten Sie ein Cloud Volumes ONTAP HA-Paar in AWS

Wenn Sie ein Cloud Volumes ONTAP HA-Paar in AWS starten möchten, müssen Sie in der Konsole ein HA-System erstellen.

Einschränkung

Derzeit werden HA-Paare mit AWS Outposts nicht unterstützt.

Informationen zu diesem Vorgang

Unmittelbar nachdem Sie das Cloud Volumes ONTAP -System erstellt haben, startet die Konsole eine Testinstanz in der angegebenen VPC, um die Konnektivität zu überprüfen. Bei Erfolg beendet die Konsole die Instanz sofort und beginnt dann mit der Bereitstellung des Cloud Volumes ONTAP Systems. Wenn die Konnektivität nicht überprüft werden kann, schlägt die Systemerstellung fehl. Die Testinstanz ist entweder eine `t2.nano` (für Standard-VPC-Miete) oder `m3.medium` (für dedizierte VPC-Miete).

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.

2. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Anweisungen.
3. Wählen Sie **Amazon Web Services** und * Cloud Volumes ONTAP HA*.

   Einige lokale AWS-Zonen sind verfügbar.

   Bevor Sie AWS Local Zones verwenden können, müssen Sie Local Zones aktivieren und in Ihrem AWS-Konto ein Subnetz in der Local Zone erstellen. Folgen Sie den Schritten **Beitritt zu einer AWS Local Zone anmelden** und **Ihre Amazon VPC auf die Local Zone erweitern** im"AWS-Tutorial „Erste Schritte bei der Bereitstellung von Anwendungen mit geringer Latenz mit lokalen AWS-Zonen“" .

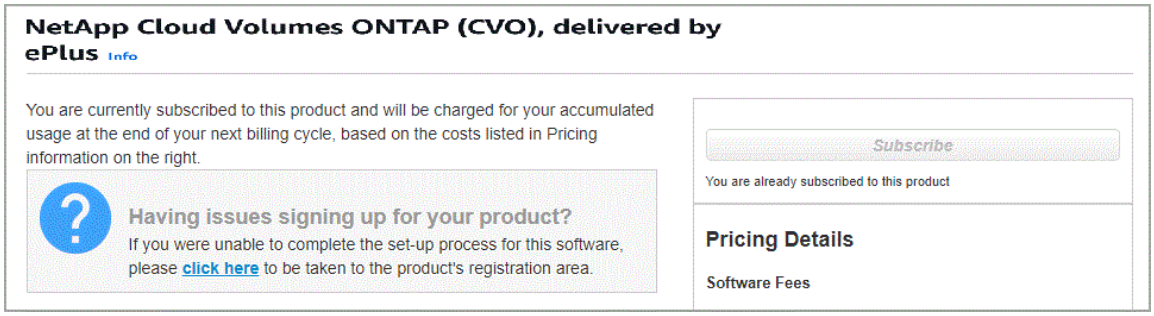
   Wenn Sie den Konsolenagenten 3.9.36 oder niedriger ausführen, müssen Sie die `DescribeAvailabilityZones` Berechtigung für die AWS-Rolle in der AWS EC2-Konsole.

4. **Details und Anmeldeinformationen**: Ändern Sie optional die AWS-Anmeldeinformationen und das Abonnement, geben Sie einen Systemnamen ein, fügen Sie bei Bedarf Tags hinzu und geben Sie dann ein Kennwort ein.

   Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Tabelle werden die Felder beschrieben, für die Sie möglicherweise Anleitungen benötigen:

Feld	Beschreibung
Systemname	Die Konsole verwendet den Systemnamen, um sowohl das Cloud Volumes ONTAP -System als auch die Amazon EC2-Instanz zu benennen. Wenn Sie diese Option auswählen, wird der Name auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet.
Tags hinzufügen	AWS-Tags sind Metadaten für Ihre AWS-Ressourcen. Die Konsole fügt die Tags der Cloud Volumes ONTAP -Instanz und jeder mit der Instanz verknüpften AWS-Ressource hinzu. Sie können beim Erstellen eines Systems bis zu vier Tags über die Benutzeroberfläche hinzufügen und nach der Erstellung weitere hinzufügen. Beachten Sie, dass die API Sie beim Erstellen eines Systems nicht auf vier Tags beschränkt. Informationen zu Tags finden Sie unter "AWS-Dokumentation: Markieren Ihrer Amazon EC2-Ressourcen" .
Benutzername und Passwort	Dies sind die Anmeldeinformationen für das Cloud Volumes ONTAP Clusteradministratorkonto. Sie können diese Anmeldeinformationen verwenden, um über ONTAP System Manager oder die ONTAP CLI eine Verbindung zu Cloud Volumes ONTAP herzustellen. Behalten Sie den Standardbenutzernamen *admin* bei oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.
Anmeldeinformationen bearbeiten	Wählen Sie die AWS-Anmeldeinformationen und das Marketplace-Abonnement für dieses Cloud Volumes ONTAP -System aus. Klicken Sie auf **Abonnement hinzufügen**, um die ausgewählten Anmeldeinformationen einem neuen AWS Marketplace-Abonnement zuzuordnen. Das Abonnement kann ein Jahresvertrag sein oder die Nutzung von Cloud Volumes ONTAP nach Stundensatz. Wenn Sie eine Lizenz direkt von NetApp erworben haben (Bring Your Own License (BYOL)), ist kein AWS-Abonnement erforderlich. NetApp hat den Erwerb, die Verlängerung und die Erneuerung von BYOL-Lizenzen eingeschränkt. Weitere Informationen finden Sie unter "Eingeschränkte Verfügbarkeit der BYOL-Lizenzierung für Cloud Volumes ONTAP" . "Erfahren Sie, wie Sie der Konsole zusätzliche AWS-Anmeldeinformationen hinzufügen" .

Wenn mehrere IAM-Benutzer im selben AWS-Konto arbeiten, muss jeder Benutzer ein Abonnement abschließen. Nachdem der erste Benutzer sich angemeldet hat, informiert der AWS-Marktplatz nachfolgende Benutzer darüber, dass sie bereits angemeldet sind, wie im Bild unten gezeigt. Solange für das AWS-Konto ein Abonnement besteht, muss sich jeder IAM-Benutzer mit diesem Abonnement verknüpfen. Wenn die unten angezeigte Meldung angezeigt wird, klicken Sie auf den Link **hier klicken**, um zur Konsolen-Website zu gelangen und den Vorgang abzuschließen.



5. **Dienste**: Lassen Sie die Dienste aktiviert oder deaktivieren Sie die einzelnen Dienste, die Sie mit diesem Cloud Volumes ONTAP System nicht verwenden möchten.
   - "Erfahren Sie mehr über die NetApp Data Classification"
   - "Erfahren Sie mehr über Backup und Wiederherstellung"

   Wenn Sie WORM und Daten-Tiering nutzen möchten, müssen Sie Backup und Recovery deaktivieren und ein Cloud Volumes ONTAP System mit Version 9.8 oder höher bereitstellen.

6. **HA-Bereitstellungsmodelle**: Wählen Sie eine HA-Konfiguration.

   Eine Übersicht über die Bereitstellungsmodelle finden Sie unter"Cloud Volumes ONTAP HA für AWS" .

7. **Standort und Konnektivität** (einzelne Verfügbarkeitszone (AZ)) oder **Region und VPC** (mehrere AZs): Geben Sie die Netzwerkinformationen ein, die Sie im AWS-Arbeitsblatt aufgezeichnet haben.

   In der folgenden Tabelle werden die Felder beschrieben, für die Sie möglicherweise Anleitungen benötigen:

Feld	Beschreibung
Generierte Sicherheitsgruppe	Wenn Sie die Sicherheitsgruppe von der Konsole erstellen lassen, müssen Sie auswählen, wie Sie den Datenverkehr zulassen: • Wenn Sie **Nur ausgewählte VPC** auswählen, ist die Quelle für eingehenden Datenverkehr der Subnetzbereich der ausgewählten VPC und der Subnetzbereich der VPC, in der sich der Konsolenagent befindet. Dies ist die empfohlene Option. • Wenn Sie **Alle VPCs** auswählen, ist die Quelle für eingehenden Datenverkehr der IP-Bereich 0.0.0.0/0.
Vorhandene Sicherheitsgruppe verwenden	Wenn Sie eine vorhandene Firewall-Richtlinie verwenden, stellen Sie sicher, dass diese die erforderlichen Regeln enthält. "Erfahren Sie mehr über Firewall-Regeln für Cloud Volumes ONTAP" .

8. **Konnektivität und SSH-Authentifizierung**: Wählen Sie Verbindungsmethoden für das HA-Paar und den Mediator.
9. **Floating IPs**: Wenn Sie mehrere AZs ausgewählt haben, geben Sie die Floating-IP-Adressen an.

   Die IP-Adressen müssen für alle VPCs in der Region außerhalb des CIDR-Blocks liegen. Weitere Einzelheiten finden Sie unter"AWS-Netzwerkanforderungen für Cloud Volumes ONTAP HA in mehreren AZs" .

10. **Routentabellen**: Wenn Sie mehrere AZs ausgewählt haben, wählen Sie die Routentabellen aus, die Routen zu den Floating-IP-Adressen enthalten sollen.

    Wenn Sie mehr als eine Routentabelle haben, ist es sehr wichtig, die richtigen Routentabellen auszuwählen. Andernfalls haben einige Clients möglicherweise keinen Zugriff auf das Cloud Volumes ONTAP HA-Paar. Weitere Informationen zu Routentabellen finden Sie im "AWS-Dokumentation: Routentabellen" .

11. **Datenverschlüsselung**: Wählen Sie keine Datenverschlüsselung oder von AWS verwaltete Verschlüsselung.

    Für die von AWS verwaltete Verschlüsselung können Sie einen anderen Customer Master Key (CMK) aus Ihrem Konto oder einem anderen AWS-Konto auswählen.

    Sie können die AWS-Datenverschlüsselungsmethode nicht mehr ändern, nachdem Sie ein Cloud Volumes ONTAP System erstellt haben.

    "Erfahren Sie, wie Sie AWS KMS für Cloud Volumes ONTAP einrichten" .

    "Erfahren Sie mehr über unterstützte Verschlüsselungstechnologien" .

12. **Abrechnungsmethoden und NSS-Konto**: Geben Sie an, welche Abrechnungsoption Sie mit diesem System verwenden möchten, und geben Sie dann ein NetApp Support Site-Konto an.
    - "Erfahren Sie mehr über die Lizenzierungsoptionen für Cloud Volumes ONTAP" .
    - "Erfahren Sie, wie Sie die Lizenzierung einrichten" .
13. * Cloud Volumes ONTAP -Konfiguration* (nur jährlicher AWS Marketplace-Vertrag): Überprüfen Sie die Standardkonfiguration und klicken Sie auf **Weiter** oder klicken Sie auf **Konfiguration ändern**, um Ihre eigene Konfiguration auszuwählen.

    Wenn Sie die Standardkonfiguration beibehalten, müssen Sie nur ein Volume angeben und dann die Konfiguration überprüfen und genehmigen.

14. **Vorkonfigurierte Pakete** (nur stündlich oder BYOL): Wählen Sie eines der Pakete aus, um Cloud Volumes ONTAP schnell zu starten, oder klicken Sie auf **Konfiguration ändern**, um Ihre eigene Konfiguration auszuwählen.

    Wenn Sie sich für eines der Pakete entscheiden, müssen Sie lediglich ein Volumen angeben und anschließend die Konfiguration prüfen und freigeben.

15. **IAM-Rolle**: Behalten Sie am besten die Standardoption bei, damit die Konsole die Rolle für Sie erstellen kann.

    Wenn Sie Ihre eigene Police verwenden möchten, muss diese"Richtlinienanforderungen für Cloud Volumes ONTAP Knoten und den HA-Mediator" .

16. **Lizenzierung**: Ändern Sie die Cloud Volumes ONTAP -Version nach Bedarf und wählen Sie einen Instanztyp und die Instanzmietdauer aus.

> Wenn für die ausgewählte Version ein neuerer Release Candidate, eine allgemeine Verfügbarkeit oder ein Patch-Release verfügbar ist, aktualisiert die Konsole das System beim Erstellen des Systems auf diese Version. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.13.1 auswählen und 9.13.1 P4 verfügbar ist. Das Update erfolgt nicht von einer Version zur nächsten, beispielsweise von 9.13 auf 9.14.

17. **Zugrunde liegende Speicherressourcen**: Wählen Sie einen Datenträgertyp, konfigurieren Sie den zugrunde liegenden Speicher und entscheiden Sie, ob die Datenschichtung aktiviert bleiben soll.

    Beachten Sie Folgendes:

    - Der Datenträgertyp ist für das Anfangsvolume (und Aggregat). Sie können für nachfolgende Volumes (und Aggregate) einen anderen Datenträgertyp auswählen.
    - Wenn Sie eine gp3- oder io1-Festplatte auswählen, verwendet die Konsole die Elastic Volumes-Funktion in AWS, um die zugrunde liegende Speicherfestplattenkapazität bei Bedarf automatisch zu erhöhen. Sie können die anfängliche Kapazität basierend auf Ihrem Speicherbedarf auswählen und sie nach der Bereitstellung von Cloud Volumes ONTAP überarbeiten. "Erfahren Sie mehr über die Unterstützung für Elastic Volumes in AWS" .
    - Wenn Sie eine GP2- oder ST1-Festplatte auswählen, können Sie eine Festplattengröße für alle Festplatten im anfänglichen Aggregat und für alle zusätzlichen Aggregate auswählen, die die Konsole erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der erweiterten Zuordnungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.
    - Sie können beim Erstellen oder Bearbeiten eines Volumes eine bestimmte Volume-Tiering-Richtlinie auswählen.
    - Wenn Sie das Daten-Tiering deaktivieren, können Sie es für nachfolgende Aggregate aktivieren.

      "Erfahren Sie, wie Data Tiering funktioniert" .

18. **Schreibgeschwindigkeit & WORM**:

    a. Wählen Sie bei Bedarf die Schreibgeschwindigkeit **Normal** oder **Hoch**.

       "Erfahren Sie mehr über die Schreibgeschwindigkeit" .

    b. Aktivieren Sie bei Bedarf den WORM-Speicher (Write Once, Read Many).

       WORM kann nicht aktiviert werden, wenn die Datenschichtung für Cloud Volumes ONTAP Version 9.7 und darunter aktiviert wurde. Das Zurücksetzen oder Downgrade auf Cloud Volumes ONTAP 9.8 ist nach der Aktivierung von WORM und Tiering blockiert.

    "Erfahren Sie mehr über WORM-Speicher" .

    a. Wenn Sie den WORM-Speicher aktivieren, wählen Sie die Aufbewahrungsdauer aus.

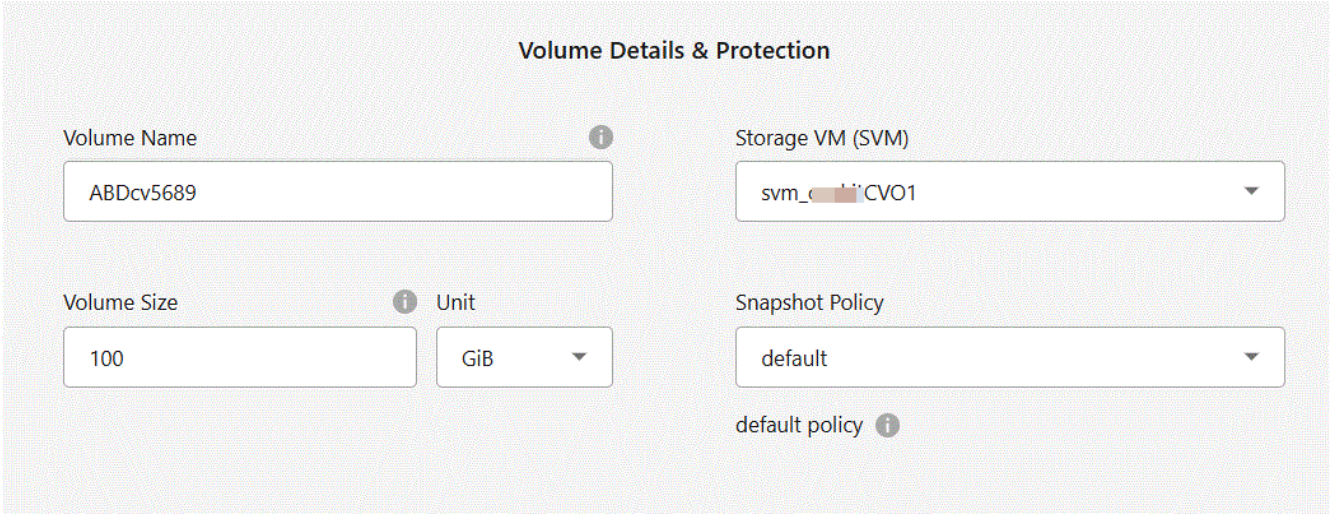
19. **Volume erstellen**: Geben Sie Details für das neue Volume ein oder klicken Sie auf **Überspringen**.

    "Erfahren Sie mehr über unterstützte Clientprotokolle und -versionen" .

    Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Tabelle werden die Felder beschrieben, für die Sie möglicherweise Anleitungen benötigen:

Feld	Beschreibung
Größe	Die maximale Größe, die Sie eingeben können, hängt weitgehend davon ab, ob Sie Thin Provisioning aktivieren. Dadurch können Sie ein Volume erstellen, das größer ist als der ihm aktuell zur Verfügung stehende physische Speicher.
Zugriffskontrolle (nur für NFS)	Eine Exportrichtlinie definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt die Konsole einen Wert ein, der Zugriff auf alle Instanzen im Subnetz gewährt.
Berechtigungen und Benutzer/Gruppen (nur für CIFS)	Mit diesen Feldern können Sie die Zugriffsebene auf eine Freigabe für Benutzer und Gruppen steuern (auch als Zugriffskontrolllisten oder ACLs bezeichnet). Sie können lokale oder Domänen-Windows-Benutzer oder -Gruppen oder UNIX-Benutzer oder -Gruppen angeben. Wenn Sie einen Windows-Domänenbenutzernamen angeben, müssen Sie die Domäne des Benutzers im Format Domäne\Benutzername angeben.
Snapshot-Richtlinie	Eine Snapshot-Kopierrichtlinie gibt die Häufigkeit und Anzahl der automatisch erstellten NetApp Snapshot-Kopien an. Eine NetApp Snapshot-Kopie ist ein zeitpunktbezogenes Dateisystem-Image, das keine Auswirkungen auf die Leistung hat und nur minimalen Speicherplatz benötigt. Sie können die Standardrichtlinie oder keine auswählen. Für vorübergehende Daten können Sie „Keine“ auswählen, beispielsweise „tempdb“ für Microsoft SQL Server.
Erweiterte Optionen (nur für NFS)	Wählen Sie eine NFS-Version für das Volume aus: entweder NFSv3 oder NFSv4.
Initiatorgruppe und IQN (nur für iSCSI)	iSCSI-Speicherziele werden als LUNs (logische Einheiten) bezeichnet und Hosts als Standardblockgeräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Hostknotennamen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. iSCSI-Ziele stellen über Standard-Ethernet-Netzwerkadapter (NICs), TCP-Offload-Engine-Karten (TOE) mit Software-Initiatoren, konvergente Netzwerkadapter (CNAs) oder dedizierte Hostbusadapter (HBAs) eine Verbindung zum Netzwerk her und werden durch iSCSI-qualifizierte Namen (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt die Konsole automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volume erstellt haben, sodass keine Verwaltung erforderlich ist. Nachdem Sie das Volume erstellt haben,"Verwenden Sie den IQN, um von Ihren Hosts aus eine Verbindung zum LUN herzustellen" .

Das folgende Bild zeigt die erste Seite des Assistenten zur Volumeerstellung:



20. **CIFS-Setup**: Wenn Sie das CIFS-Protokoll ausgewählt haben, richten Sie einen CIFS-Server ein.

Feld	Beschreibung
DNS Primäre und sekundäre IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgelisteten DNS-Server müssen die Service Location Records (SRV) enthalten, die zum Auffinden der Active Directory-LDAP-Server und Domänencontroller für die Domäne erforderlich sind, der der CIFS-Server beitreten wird.
Beitretende Active Directory-Domäne	Der FQDN der Active Directory (AD)-Domäne, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zum Beitritt zur Domäne berechtigt sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
NetBIOS-Name des CIFS-Servers	Ein CIFS-Servername, der in der AD-Domäne eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domäne, die mit dem CIFS-Server verknüpft werden soll. Der Standardwert ist CN=Computers. Wenn Sie AWS Managed Microsoft AD als AD-Server für Cloud Volumes ONTAP konfigurieren, sollten Sie in dieses Feld **OU=Computers,OU=corp** eingeben.
DNS-Domäne	Die DNS-Domäne für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen ist die Domäne dieselbe wie die AD-Domäne.
NTP-Server	Wählen Sie **Active Directory-Domäne verwenden**, um einen NTP-Server mithilfe des Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Weitere Informationen finden Sie im "Dokumentation zur NetApp Console" für Details. Beachten Sie, dass Sie einen NTP-Server nur beim Erstellen eines CIFS-Servers konfigurieren können. Es ist nicht mehr konfigurierbar, nachdem Sie den CIFS-Server erstellt haben.

21. **Nutzungsprofil, Datenträgertyp und Tiering-Richtlinie**: Wählen Sie aus, ob Sie Speichereffizienzfunktionen aktivieren möchten, und bearbeiten Sie bei Bedarf die Volume-Tiering-Richtlinie.

    Weitere Informationen finden Sie unter"Auswählen eines Volume-Nutzungsprofils" Und"Übersicht über

Data Tiering" .

22. **Überprüfen und genehmigen**: Überprüfen und bestätigen Sie Ihre Auswahl.
    a. Überprüfen Sie die Details zur Konfiguration.
    b. Klicken Sie auf **Weitere Informationen**, um Details zum Support und den AWS-Ressourcen anzuzeigen, die über die Konsole erworben werden.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie auf **Los**.

Ergebnis

Die Konsole startet das Cloud Volumes ONTAP HA-Paar. Sie können den Fortschritt auf der Seite **Audit** verfolgen.

Wenn beim Starten des HA-Paares Probleme auftreten, überprüfen Sie die Fehlermeldung. Sie können auch das System auswählen und auf „Umgebung neu erstellen“ klicken.

Weitere Hilfe finden Sie unter "NetApp Cloud Volumes ONTAP Unterstützung" .

Nach Abschluss

- Wenn Sie eine CIFS-Freigabe bereitgestellt haben, erteilen Sie Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner und stellen Sie sicher, dass diese Benutzer auf die Freigabe zugreifen und eine Datei erstellen können.
- Wenn Sie Kontingente auf Volumes anwenden möchten, verwenden Sie ONTAP System Manager oder die ONTAP CLI.

  Mithilfe von Kontingenten können Sie den Speicherplatz und die Anzahl der von einem Benutzer, einer Gruppe oder einem Qtree verwendeten Dateien beschränken oder verfolgen.

> Ändern Sie nach Abschluss des Bereitstellungsprozesses nicht die systemgenerierten Cloud Volumes ONTAP -Konfigurationen im AWS-Cloud-Portal, insbesondere nicht die System-Tags. Alle an diesen Konfigurationen vorgenommenen Änderungen können zu unerwartetem Verhalten oder Datenverlust führen.

Weiterführende Links

- "Planen Ihrer Cloud Volumes ONTAP Konfiguration"
- "Stellen Sie Cloud Volumes ONTAP in AWS mithilfe der Schnellbereitstellung bereit"

Stellen Sie Cloud Volumes ONTAP in AWS Secret Cloud oder AWS Top Secret Cloud bereit

Ähnlich wie bei einer Standard-AWS-Region können Sie die NetApp Console in"AWS Secret Cloud" und in"AWS Top Secret Cloud" zur Bereitstellung von Cloud Volumes ONTAP, das Funktionen der Enterprise-Klasse für Ihren Cloud-Speicher bietet. AWS Secret Cloud und Top Secret Cloud sind geschlossene Regionen, die speziell für die US-Geheimdienste bestimmt sind. Die Anweisungen auf dieser Seite gelten nur für Benutzer der AWS Secret Cloud- und Top Secret Cloud-Regionen.

Bevor Sie beginnen

Bevor Sie beginnen, überprüfen Sie die unterstützten Versionen in AWS Secret Cloud und Top Secret Cloud

und informieren Sie sich über den privaten Modus in der Konsole.

- Überprüfen Sie die folgenden unterstützten Versionen in AWS Secret Cloud und Top Secret Cloud:
  - Cloud Volumes ONTAP 9.12.1 P2
  - Version 3.9.32 des Konsolenagenten

    Der Konsolenagent ist zum Bereitstellen und Verwalten von Cloud Volumes ONTAP in AWS erforderlich. Sie melden sich bei der Konsole über die Software an, die auf der Instanz des Konsolenagenten installiert wird. Die SaaS-Website für die Konsole wird in AWS Secret Cloud und Top Secret Cloud nicht unterstützt.
- Erfahren Sie mehr über den privaten Modus

  In AWS Secret Cloud und Top Secret Cloud arbeitet die Konsole im *privaten Modus*. Im privaten Modus besteht von der Konsole aus keine Verbindung zur SaaS-Schicht. Sie können über eine lokale webbasierte Anwendung auf die Konsole zugreifen, die auf den Konsolenagenten zugreifen kann.

  Weitere Informationen zur Funktionsweise des privaten Modus finden Sie unter"den privaten Bereitstellungsmodus in der Konsole" .

Schritt 1: Richten Sie Ihr Netzwerk ein

Richten Sie Ihr AWS-Netzwerk so ein, dass Cloud Volumes ONTAP ordnungsgemäß funktioniert.

Schritte

1. Wählen Sie die VPC und Subnetze aus, in denen Sie die Instanz des Konsolenagenten und der Cloud Volumes ONTAP Instanzen starten möchten.
2. Stellen Sie sicher, dass Ihr VPC und Ihre Subnetze die Konnektivität zwischen dem Konsolenagenten und Cloud Volumes ONTAP unterstützen.
3. Richten Sie einen VPC-Endpunkt für den Amazon Simple Storage Service (Amazon S3) Service ein.

   Ein VPC-Endpunkt ist erforderlich, wenn Sie kalte Daten von Cloud Volumes ONTAP auf kostengünstigen Objektspeicher verschieben möchten.

Schritt 2: Berechtigungen einrichten

Richten Sie IAM-Richtlinien und -Rollen ein, die dem Konsolenagenten und Cloud Volumes ONTAP die Berechtigungen erteilen, die sie zum Ausführen von Aktionen in der AWS Secret Cloud oder Top Secret Cloud benötigen.

Sie benötigen für Folgendes jeweils eine IAM-Richtlinie und eine IAM-Rolle:

- Die Instanz des Konsolenagenten
- Cloud Volumes ONTAP Instanzen
- Für HA-Paare die Cloud Volumes ONTAP HA-Mediatorinstanz (wenn Sie HA-Paare bereitstellen möchten)

Schritte

1. Gehen Sie zur AWS IAM-Konsole und klicken Sie auf **Richtlinien**.
2. Erstellen Sie eine Richtlinie für die Instanz des Konsolenagenten.

Sie erstellen diese Richtlinien, um die S3-Buckets in Ihrer AWS-Umgebung zu unterstützen. Achten Sie beim späteren Erstellen der Buckets darauf, dass die Bucket-Namen mit dem Präfix `fabric-pool-` . Diese Anforderung gilt sowohl für die AWS Secret Cloud- als auch für die Top Secret Cloud-Regionen.

Geheime Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
```

```
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso-b:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
```

```
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Streng geheime Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
```

```
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
    ]
```

```
}
```

3. Erstellen Sie eine Richtlinie für Cloud Volumes ONTAP.

Geheime Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Streng geheime Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Wenn Sie für HA-Paare die Bereitstellung eines Cloud Volumes ONTAP HA-Paares planen, erstellen Sie eine Richtlinie für den HA-Mediator.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

4. Erstellen Sie IAM-Rollen mit dem Rollentyp Amazon EC2 und fügen Sie die Richtlinien an, die Sie in den vorherigen Schritten erstellt haben.

   Erstellen Sie die Rolle:

   Ähnlich wie bei den Richtlinien sollten Sie eine IAM-Rolle für den Konsolenagenten und eine für die Cloud Volumes ONTAP Knoten haben. Für HA-Paare: Ähnlich wie bei den Richtlinien sollten Sie eine IAM-Rolle für den Konsolenagenten, eine für die Cloud Volumes ONTAP Knoten und eine für den HA-Mediator haben (wenn Sie HA-Paare bereitstellen möchten).

   Wählen Sie die Rolle aus:

   Sie müssen die IAM-Rolle des Konsolenagenten auswählen, wenn Sie die Instanz des Konsolenagenten starten. Sie können die IAM-Rollen für Cloud Volumes ONTAP auswählen, wenn Sie ein Cloud Volumes ONTAP -System über die Konsole erstellen. Für HA-Paare können Sie die IAM-Rollen für Cloud Volumes ONTAP und den HA-Mediator auswählen, wenn Sie ein Cloud Volumes ONTAP System erstellen.

Schritt 3: Einrichten des AWS KMS

Wenn Sie die Amazon-Verschlüsselung mit Cloud Volumes ONTAP verwenden möchten, stellen Sie sicher, dass die Anforderungen für den AWS Key Management Service (KMS) erfüllt sind.

Schritte

1. Stellen Sie sicher, dass in Ihrem Konto oder einem anderen AWS-Konto ein aktiver Customer Master Key (CMK) vorhanden ist.

   Der CMK kann ein von AWS verwalteter CMK oder ein vom Kunden verwalteter CMK sein.

2. Wenn sich der CMK in einem AWS-Konto befindet, das von dem Konto getrennt ist, in dem Sie Cloud Volumes ONTAP bereitstellen möchten, müssen Sie die ARN dieses Schlüssels abrufen.

   Sie müssen der Konsole die ARN bereitstellen, wenn Sie das Cloud Volumes ONTAP -System erstellen.

3. Fügen Sie die IAM-Rolle für die Instanz zur Liste der Schlüsselbenutzer für einen CMK hinzu.

   Dadurch erhält die Konsole die Berechtigung, den CMK mit Cloud Volumes ONTAP zu verwenden.

Schritt 4: Installieren Sie den Konsolenagenten und richten Sie die Konsole ein

Bevor Sie die Konsole zum Bereitstellen von Cloud Volumes ONTAP in AWS verwenden können, müssen Sie den Konsolenagenten installieren und einrichten. Es ermöglicht der Konsole, Ressourcen und Prozesse innerhalb Ihrer öffentlichen Cloud-Umgebung zu verwalten (dazu gehört Cloud Volumes ONTAP).

Schritte

1. Besorgen Sie sich ein von einer Zertifizierungsstelle (CA) signiertes Stammzertifikat im Base-64-codierten X.509-Format für Privacy Enhanced Mail (PEM). Informieren Sie sich über die Richtlinien und Verfahren Ihrer Organisation zum Erhalt des Zertifikats.

   > Für AWS Secret Cloud-Regionen sollten Sie die `NSS Root CA 2` Zertifikat und für Top Secret Cloud, das `Amazon Root CA 4` Zertifikat. Stellen Sie sicher, dass Sie nur diese Zertifikate und nicht die gesamte Kette hochladen. Die Datei für die Zertifikatskette ist groß und der Upload kann fehlschlagen. Sollten Sie über weitere Zertifikate verfügen, können Sie diese, wie im nächsten Schritt beschrieben, später hochladen.

   Sie müssen das Zertifikat während des Einrichtungsvorgangs hochladen. Die Konsole verwendet das vertrauenswürdige Zertifikat, wenn sie Anfragen über HTTPS an AWS sendet.

2. Starten Sie die Instanz des Konsolenagenten:
   a. Gehen Sie zur AWS Intelligence Community Marketplace-Seite für die Konsole.
   b. Wählen Sie auf der Registerkarte „Benutzerdefinierter Start“ die Option zum Starten der Instance von der EC2-Konsole aus.
   c. Folgen Sie den Anweisungen zum Konfigurieren der Instanz.

      Beachten Sie beim Konfigurieren der Instanz Folgendes:

      - Wir empfehlen t3.xlarge.
      - Sie müssen die IAM-Rolle auswählen, die Sie beim Einrichten der Berechtigungen erstellt haben.
      - Sie sollten die Standardspeicheroptionen beibehalten.
      - Die erforderlichen Verbindungsmethoden für den Konsolenagenten sind wie folgt: SSH, HTTP und HTTPS.
3. Richten Sie die Konsole von einem Host aus ein, der eine Verbindung zur Instanz hat:
   a. Öffnen Sie einen Webbrowser und geben Sie ein https://ipaddress Dabei ist ipaddress die IP-Adresse des Linux-Hosts, auf dem Sie den Konsolen-Agent installiert haben.
   b. Geben Sie einen Proxyserver für die Verbindung mit AWS-Diensten an.
   c. Laden Sie das Zertifikat hoch, das Sie in Schritt 1 erhalten haben.
   d. Folgen Sie den Anweisungen, um ein neues System einzurichten.
      - **Systemdetails**: Geben Sie einen Namen für den Konsolenagenten und Ihren Firmennamen ein.
      - **Administratorbenutzer erstellen**: Erstellen Sie den Administratorbenutzer für das System.

Dieses Benutzerkonto wird lokal auf dem System ausgeführt. Über die Konsole ist keine Verbindung zum Auth0-Dienst verfügbar.

- **Überprüfen**: Überprüfen Sie die Details, akzeptieren Sie die Lizenzvereinbarung und wählen Sie dann **Einrichten**.

e. Um die Installation des CA-signierten Zertifikats abzuschließen, starten Sie die Konsolen-Agent-Instanz von der EC2-Konsole aus neu.

4. Melden Sie sich nach dem Neustart des Konsolenagenten mit dem Administratorbenutzerkonto an, das Sie im Setup-Assistenten erstellt haben.

Schritt 5: (optional) Installieren Sie ein Zertifikat für den privaten Modus

Dieser Schritt ist für AWS Secret Cloud- und Top Secret Cloud-Regionen optional und nur erforderlich, wenn Sie neben den im vorherigen Schritt installierten Stammzertifikaten über weitere Zertifikate verfügen.

Schritte

1. Listet vorhandene installierte Zertifikate auf.
   a. Um die Docker-ID des OCCM-Containers (identifizierter Name „ds-occm-1“) zu erfassen, führen Sie den folgenden Befehl aus:

```
docker ps
```

   b. Um in den OCCM-Container zu gelangen, führen Sie den folgenden Befehl aus:

```
docker exec -it <docker-id> /bin/sh
```

   c. Um das Kennwort aus der Umgebungsvariable „TRUST_STORE_PASSWORD“ abzurufen, führen Sie den folgenden Befehl aus:

```
env
```

   d. Um alle installierten Zertifikate im Truststore aufzulisten, führen Sie den folgenden Befehl aus und verwenden Sie das im vorherigen Schritt erfasste Kennwort:

```
keytool -list -v -keystore occm.truststore
```

2. Fügen Sie ein Zertifikat hinzu.
   a. Um die Docker-ID des OCCM-Containers (identifizierter Name „ds-occm-1“) zu erfassen, führen Sie den folgenden Befehl aus:

```
docker ps
```

   b. Um in den OCCM-Container zu gelangen, führen Sie den folgenden Befehl aus:

```
docker exec -it <docker-id> /bin/sh
```

Speichern Sie die neue Zertifikatsdatei darin.

c. Um das Kennwort aus der Umgebungsvariable „TRUST_STORE_PASSWORD“ abzurufen, führen Sie den folgenden Befehl aus:

```
env
```

d. Um das Zertifikat zum Truststore hinzuzufügen, führen Sie den folgenden Befehl aus und verwenden Sie das Kennwort aus dem vorherigen Schritt:

```
keytool -import -alias <alias-name> -file <certificate-file-name>
-keystore occm.truststore
```

e. Um zu überprüfen, ob das Zertifikat installiert ist, führen Sie den folgenden Befehl aus:

```
keytool -list -v -keystore occm.truststore -alias <alias-name>
```

f. Um den OCCM-Container zu beenden, führen Sie den folgenden Befehl aus:

```
exit
```

g. Um den OCCM-Container zurückzusetzen, führen Sie den folgenden Befehl aus:

```
docker restart <docker-id>
```

Schritt 6: Fügen Sie der Konsole eine Lizenz hinzu

Wenn Sie eine Lizenz von NetApp erworben haben, müssen Sie sie der Konsole hinzufügen, damit Sie die Lizenz auswählen können, wenn Sie ein neues Cloud Volumes ONTAP -System erstellen. Diese Lizenzen bleiben nicht zugewiesen, bis Sie sie einem neuen Cloud Volumes ONTAP -System zuordnen.

Schritte

1. Wählen Sie im linken Navigationsmenü * Licenses and subscriptions* aus.
2. Wählen Sie im Bereich * Cloud Volumes ONTAP* die Option **Anzeigen** aus.
3. Wählen Sie auf der Registerkarte * Cloud Volumes ONTAP* die Option **Lizenzen > Knotenbasierte Lizenzen** aus.
4. Klicken Sie auf **Nicht zugewiesen**.
5. Klicken Sie auf **Nicht zugewiesene Lizenzen hinzufügen**.

6. Geben Sie die Seriennummer der Lizenz ein oder laden Sie die Lizenzdatei hoch.
7. Wenn Sie die Lizenzdatei noch nicht haben, müssen Sie die Lizenzdatei manuell von netapp.com hochladen.
   a. Gehen Sie zum"NetApp Lizenzdateigenerator" und melden Sie sich mit Ihren Anmeldeinformationen für die NetApp Support-Site an.
   b. Geben Sie Ihr Passwort ein, wählen Sie Ihr Produkt aus, geben Sie die Seriennummer ein, bestätigen Sie, dass Sie die Datenschutzrichtlinie gelesen und akzeptiert haben, und klicken Sie dann auf **Senden**.
   c. Wählen Sie, ob Sie die JSON-Datei „serialnumber.NLF“ per E-Mail oder durch direkten Download erhalten möchten.
8. Klicken Sie auf **Lizenz hinzufügen**.

Ergebnis

Die Konsole fügt die Lizenz als nicht zugewiesen hinzu, bis Sie sie einem neuen Cloud Volumes ONTAP -System zuordnen. Sie können die Lizenz im linken Navigationsmenü unter * Licenses and subscriptions > Cloud Volumes ONTAP > Anzeigen > Lizenzen* sehen.

Schritt 7: Starten Sie Cloud Volumes ONTAP von der Konsole aus

Sie können Cloud Volumes ONTAP Instanzen in AWS Secret Cloud und Top Secret Cloud starten, indem Sie in der Konsole neue Systeme erstellen.

Bevor Sie beginnen

Für HA-Paare ist ein Schlüsselpaar erforderlich, um die schlüsselbasierte SSH-Authentifizierung beim HA-Mediator zu aktivieren.

Schritte

1. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen**.
2. Wählen Sie unter **Erstellen** Cloud Volumes ONTAP aus.

   Für HA: Wählen Sie unter **Erstellen** Cloud Volumes ONTAP oder Cloud Volumes ONTAP HA aus.

3. Führen Sie die Schritte im Assistenten aus, um das Cloud Volumes ONTAP -System zu starten.

> Wählen Sie beim Auswählen im Assistenten unter **Dienste** nicht **Data Sense & Compliance** und **Backup in die Cloud** aus. Wählen Sie unter **Vorkonfigurierte Pakete** nur **Konfiguration ändern** aus und stellen Sie sicher, dass Sie keine andere Option ausgewählt haben. Vorkonfigurierte Pakete werden in den AWS Secret Cloud- und Top Secret Cloud-Regionen nicht unterstützt. Wenn Sie diese auswählen, schlägt Ihre Bereitstellung fehl.

Hinweise zur Bereitstellung von Cloud Volumes ONTAP HA in mehreren Availability Zones

Beachten Sie beim Abschließen des Assistenten für HA-Paare Folgendes.

- Sie sollten ein Transit-Gateway konfigurieren, wenn Sie Cloud Volumes ONTAP HA in mehreren Availability Zones (AZs) bereitstellen. Anweisungen hierzu finden Sie unter"Einrichten eines AWS Transit Gateways" .
- Stellen Sie die Konfiguration wie folgt bereit, da zum Zeitpunkt der Veröffentlichung nur zwei AZs in der AWS Top Secret Cloud verfügbar waren:
  - Knoten 1: Verfügbarkeitszone A

- Knoten 2: Verfügbarkeitszone B
- Vermittler: Verfügbarkeitszone A oder B

Hinweise zur Bereitstellung von Cloud Volumes ONTAP in Einzel- und HA-Knoten

Beachten Sie beim Abschließen des Assistenten Folgendes:

- Sie sollten die Standardoption zur Verwendung einer generierten Sicherheitsgruppe belassen.

  Die vordefinierte Sicherheitsgruppe enthält die Regeln, die Cloud Volumes ONTAP für einen erfolgreichen Betrieb benötigt. Wenn Sie Ihre eigene verwenden müssen, können Sie den Abschnitt Sicherheitsgruppe weiter unten lesen.

- Sie müssen die IAM-Rolle auswählen, die Sie beim Vorbereiten Ihrer AWS-Umgebung erstellt haben.
- Der zugrunde liegende AWS-Festplattentyp ist für das anfängliche Cloud Volumes ONTAP -Volume.

  Sie können für nachfolgende Volumes einen anderen Datenträgertyp auswählen.

- Die Leistung von AWS-Festplatten ist an die Festplattengröße gebunden.

  Sie sollten die Festplattengröße wählen, die Ihnen die benötigte Dauerleistung bietet. Weitere Einzelheiten zur EBS-Leistung finden Sie in der AWS-Dokumentation.

- Die Datenträgergröße ist die Standardgröße für alle Datenträger im System.

  Wenn Sie später eine andere Größe benötigen, können Sie mit der Option „Erweiterte Zuordnung“ ein Aggregat erstellen, das Festplatten einer bestimmten Größe verwendet.

Ergebnis

Die Cloud Volumes ONTAP Instanz wird gestartet. Sie können den Fortschritt auf der Seite **Audit** verfolgen.

Schritt 8: Installieren von Sicherheitszertifikaten für das Datentiering

Sie müssen Sicherheitszertifikate manuell installieren, um die Datenschichtung in den AWS Secret Cloud- und Top Secret Cloud-Regionen zu aktivieren.

Bevor Sie beginnen

1. Erstellen Sie S3-Buckets.

   Stellen Sie sicher, dass die Bucket-Namen mit dem Präfix `fabric-pool-.` Zum Beispiel `fabric-pool-testbucket` .

2. Behalten Sie die Stammzertifikate, die Sie installiert haben in `step 4` praktisch.

Schritte

1. Kopieren Sie den Text aus den Stammzertifikaten, die Sie installiert haben in `step 4` .
2. Stellen Sie mithilfe der CLI eine sichere Verbindung zum Cloud Volumes ONTAP -System her.
3. Installieren Sie die Stammzertifikate. Möglicherweise müssen Sie die Taste `ENTER` Taste mehrmals drücken:

```
security certificate install -type server-ca -cert-name <certificate-
name>
```

4. Wenn Sie dazu aufgefordert werden, geben Sie den gesamten kopierten Text ein, einschließlich und von `----- BEGIN CERTIFICATE -----` Zu `----- END CERTIFICATE -----` .
5. Bewahren Sie eine Kopie des von der Zertifizierungsstelle signierten digitalen Zertifikats zur späteren Verwendung auf.
6. Bewahren Sie den CA-Namen und die Seriennummer des Zertifikats auf.
7. Konfigurieren Sie den Objektspeicher für die AWS Secret Cloud- und Top Secret Cloud-Regionen: `set -privilege advanced -confirmations off`
8. Führen Sie diesen Befehl aus, um den Objektspeicher zu konfigurieren.

> ⓘ Alle Amazon Resource Names (ARNs) sollten mit dem Suffix `-iso-b` , wie zum Beispiel `arn:aws-iso-b` . Wenn beispielsweise eine Ressource eine ARN mit einer Region erfordert, verwenden Sie für Top Secret Cloud die Namenskonvention als `us-iso-b` für die `-server` Flagge. Verwenden Sie für AWS Secret Cloud `us-iso-b-1` .

```
storage aggregate object-store config create -object-store-name
<S3Bucket> -provider-type AWS_S3 -auth-type EC2-IAM -server <s3.us-iso-
b-1.server_name> -container-name <fabric-pool-testbucket> -is-ssl
-enabled true -port 443
```

9. Überprüfen Sie, ob der Objektspeicher erfolgreich erstellt wurde: `storage aggregate object-store show -instance`
10. Hängen Sie den Objektspeicher an das Aggregat an. Dies sollte für jedes neue Aggregat wiederholt werden: `storage aggregate object-store attach -aggregate <aggr1> -object-store -name <S3Bucket>`

Erste Schritte in Microsoft Azure

Informieren Sie sich über die Bereitstellungsoptionen von Cloud Volumes ONTAP in Azure

NetApp bietet zwei Optionen für die Bereitstellung von Cloud Volumes ONTAP auf Azure. Cloud Volumes ONTAP verlässt sich traditionell auf die NetApp Console für Bereitstellung und Orchestrierung. Ab Cloud Volumes ONTAP 9.16.1 können Sie die Vorteile der direkten Bereitstellung im Azure Marketplace nutzen, einem optimierten Prozess, der Zugriff auf eine begrenzte, aber dennoch leistungsstarke Reihe von Funktionen und Optionen von Cloud Volumes ONTAP bietet.

Wenn Sie Cloud Volumes ONTAP direkt vom Azure Marketplace bereitstellen, müssen Sie weder den Konsolen-Agenten einrichten noch andere Sicherheits- und Onboarding-Kriterien erfüllen, die für die Bereitstellung von Cloud Volumes ONTAP über die Konsole erforderlich sind. Über den Azure Marketplace können Sie Cloud Volumes ONTAP mit wenigen Klicks schnell bereitstellen und die wichtigsten Funktionen

und Möglichkeiten in Ihrer Umgebung erkunden.

Nach Abschluss der Bereitstellung im Azure Marketplace können Sie diese Systeme in der Konsole entdecken. Nach der Erkennung können Sie sie als Cloud Volumes ONTAP -Systeme verwalten und alle Konsolenfunktionen nutzen. Weitere Informationen finden Sie unter "Entdecken Sie die bereitgestellten Systeme in der Konsole" .

Hier ist der Funktionsvergleich zwischen den beiden Optionen. Beachten Sie, dass sich die Funktionen einer über den Azure Marketplace bereitgestellten eigenständigen Instanz ändern, wenn sie in der Konsole erkannt wird.

	Azure-Marktplatz	**NetApp Console**
Einarbeitung	Kürzere und einfachere, minimale Vorbereitung für den direkten Einsatz erforderlich	Längerer Onboarding-Prozess, einschließlich der Installation des Konsolen-Agenten
Unterstützte Typen virtueller Maschinen (VM)	Eds_v5- und Ls_v3-Instance-Typen	Vollständige Palette an VM-Typen.https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-azure.html["Unterstützte Konfigurationen in Azure"^]
Lizenz	Kostenlose Lizenz	Jede kapazitätsbasierte Lizenz."Cloud Volumes ONTAP -Lizenzierung"
* NetApp Unterstützung*	Nicht enthalten	Verfügbar, je nach Lizenztyp
Kapazität	Bis zu 500 GiB	Erweiterbar durch Konfiguration
Bereitstellungsmodell	Bereitstellung im Hochverfügbarkeitsmodus (HA) in einer einzelnen Verfügbarkeitszone (AZ)	Alle unterstützten Konfigurationen, einschließlich Einzelknoten- und HA-Modi, Einzel- und Mehrfach-AZ-Bereitstellungen
Unterstützter Datenträgertyp	Verwaltete Premium-SSD-v2-Datenträger	Breitere Unterstützung."Standardkonfiguration für Cloud Volumes ONTAP"
Schreibgeschwindigkeit (schneller Schreibmodus)	Nicht unterstützt	Wird basierend auf Ihrer Konfiguration unterstützt. "Erfahren Sie mehr über die Schreibgeschwindigkeiten in Cloud Volumes ONTAP" .
Orchestrierungsfunktionen	Nicht verfügbar	Verfügbar über die NetApp Console, basierend auf dem Lizenztyp
Anzahl der unterstützten Speicher-VMs	Eine pro Bereitstellung	Mehrere Speicher-VMs, basierend auf Ihrer Konfiguration."Unterstützte Anzahl von Speicher-VMs"
Ändern des Instanztyps	Nicht unterstützt	Unterstützt
* FabricPool Stufeneinteilung*	Nicht unterstützt	Unterstützt

Weiterführende Links

- Direkte Bereitstellung im Azure Marketplace:"Stellen Sie Cloud Volumes ONTAP vom Azure Marketplace bereit"
- Bereitstellung über die Konsole:"Schnellstart für Cloud Volumes ONTAP in Azure"
- "Dokumentation zur NetApp Console"

Erste Schritte in der NetApp Console

Schnellstart für Cloud Volumes ONTAP in Azure

Beginnen Sie in wenigen Schritten mit Cloud Volumes ONTAP für Azure.

Erstellen eines Konsolenagenten

Wenn Sie kein "Konsolenagent" Sie müssen jedoch eines erstellen. "Erfahren Sie, wie Sie einen Konsolen-Agent in Azure erstellen"

Beachten Sie: Wenn Sie Cloud Volumes ONTAP in einem Subnetz bereitstellen möchten, in dem kein Internetzugang verfügbar ist, müssen Sie den Konsolenagenten manuell installieren und auf die NetApp Console zugreifen, die auf diesem Konsolenagenten ausgeführt wird. "Erfahren Sie, wie Sie den Konsolenagenten manuell an einem Ort ohne Internetzugang installieren."

Planen Sie Ihre Konfiguration

Die Konsole bietet vorkonfigurierte Pakete, die Ihren Workload-Anforderungen entsprechen, oder Sie können Ihre eigene Konfiguration erstellen. Wenn Sie Ihre eigene Konfiguration auswählen, sollten Sie die Ihnen zur Verfügung stehenden Optionen verstehen. Weitere Informationen finden Sie unter"Planen Sie Ihre Cloud Volumes ONTAP -Konfiguration in Azure" .

Richten Sie Ihr Netzwerk ein

1. Stellen Sie sicher, dass Ihr VNet und Ihre Subnetze die Konnektivität zwischen dem Konsolenagenten und Cloud Volumes ONTAP unterstützen.
2. Aktivieren Sie den ausgehenden Internetzugriff vom Ziel-VPC für NetApp AutoSupport.

   Dieser Schritt ist nicht erforderlich, wenn Sie Cloud Volumes ONTAP an einem Standort bereitstellen, an dem kein Internetzugang verfügbar ist.

"Erfahren Sie mehr über die Netzwerkanforderungen" .

Starten Sie Cloud Volumes ONTAP

Klicken Sie auf **System hinzufügen**, wählen Sie den Systemtyp aus, den Sie bereitstellen möchten, und führen Sie die Schritte im Assistenten aus. "Lesen Sie die Schritt-für-Schritt-Anleitung" .

Weiterführende Links

- "Erstellen eines Konsolenagenten über die Konsole"

- "Erstellen eines Konsolen-Agenten aus dem Azure Marketplace"
- "Installieren der Konsolenagentensoftware auf einem Linux-Host"
- "Was die Konsole mit Berechtigungen macht"

Planen Sie Ihre Cloud Volumes ONTAP -Konfiguration in Azure

Wenn Sie Cloud Volumes ONTAP in Azure bereitstellen, können Sie ein vorkonfiguriertes System auswählen, das Ihren Workload-Anforderungen entspricht, oder Sie können Ihre eigene Konfiguration erstellen. Wenn Sie Ihre eigene Konfiguration auswählen, sollten Sie die Ihnen zur Verfügung stehenden Optionen verstehen.

Wählen Sie eine Cloud Volumes ONTAP -Lizenz

Für Cloud Volumes ONTAP sind mehrere Lizenzierungsoptionen verfügbar. Jede Option ermöglicht Ihnen die Auswahl eines Verbrauchsmodells, das Ihren Anforderungen entspricht.

- "Erfahren Sie mehr über die Lizenzierungsoptionen für Cloud Volumes ONTAP"
- "Erfahren Sie, wie Sie die Lizenzierung einrichten"

Wählen Sie eine unterstützte Region

Cloud Volumes ONTAP wird in den meisten Microsoft Azure-Regionen unterstützt. "Vollständige Liste der unterstützten Regionen anzeigen" .

Wählen Sie einen unterstützten VM-Typ

Cloud Volumes ONTAP unterstützt je nach gewähltem Lizenztyp mehrere VM-Typen.

"Unterstützte Konfigurationen für Cloud Volumes ONTAP in Azure"

Speichergrenzen verstehen

Die Rohkapazitätsgrenze für ein Cloud Volumes ONTAP System ist an die Lizenz gebunden. Zusätzliche Beschränkungen wirken sich auf die Größe von Aggregaten und Volumina aus. Sie sollten sich dieser Beschränkungen bewusst sein, wenn Sie Ihre Konfiguration planen.

"Speicherlimits für Cloud Volumes ONTAP in Azure"

Dimensionieren Sie Ihr System in Azure

Durch die Dimensionierung Ihres Cloud Volumes ONTAP -Systems können Sie die Anforderungen an Leistung und Kapazität erfüllen. Bei der Auswahl eines VM-Typs, Datenträgertyps und einer Datenträgergröße sollten Sie einige wichtige Punkte beachten:

Typ der virtuellen Maschine

Sehen Sie sich die unterstützten virtuellen Maschinentypen im "Versionshinweise zu Cloud Volumes ONTAP" und überprüfen Sie dann Details zu jedem unterstützten VM-Typ. Beachten Sie, dass jeder VM-Typ eine bestimmte Anzahl von Datenträgern unterstützt.

- "Azure-Dokumentation: Allgemeine Größen virtueller Computer"
- "Azure-Dokumentation: Arbeitsspeicheroptimierte Größen virtueller Computer"

Azure-Datenträgertyp mit Einzelknotensystemen

Wenn Sie Volumes für Cloud Volumes ONTAP erstellen, müssen Sie den zugrunde liegenden Cloud-Speicher auswählen, den Cloud Volumes ONTAP als Festplatte verwendet.

Einzelknotensysteme können diese Arten von Azure Managed Disks verwenden:

- *Premium SSD Managed Disks* bieten hohe Leistung für I/O-intensive Workloads zu höheren Kosten.
- *Premium SSD v2 Managed Disks* bieten im Vergleich zu Premium SSD Managed Disks eine höhere Leistung mit geringerer Latenz zu geringeren Kosten.
- *Standard-SSD-Managed Disks* bieten konsistente Leistung für Workloads, die niedrige IOPS erfordern.
- *Standard HDD Managed Disks* sind eine gute Wahl, wenn Sie keine hohen IOPS benötigen und Ihre Kosten senken möchten.

Weitere Einzelheiten zu den Anwendungsfällen dieser Festplatten finden Sie unter "Microsoft Azure-Dokumentation: Welche Datenträgertypen sind in Azure verfügbar?" .

Azure-Datenträgertyp mit HA-Paaren

HA-Systeme verwenden Premium SSD Shared Managed Disks, die beide eine hohe Leistung für E/A-intensive Workloads zu höheren Kosten bieten. HA-Bereitstellungen, die vor der Version 9.12.1 erstellt wurden, verwenden Premium-Seitenblobs.

Azure-Datenträgergröße

Wenn Sie Cloud Volumes ONTAP -Instanzen starten, müssen Sie die Standarddatenträgergröße für Aggregate auswählen. Die NetApp Console verwendet diese Datenträgergröße für das anfängliche Aggregat und für alle zusätzlichen Aggregate, die sie erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Sie können Aggregate erstellen, die eine andere Festplattengröße als die Standardgröße verwenden, indem Sie"Verwenden der erweiterten Zuordnungsoption" .

Alle Festplatten in einem Aggregat müssen die gleiche Größe haben.

Bei der Auswahl einer Festplattengröße sollten Sie mehrere Faktoren berücksichtigen. Die Festplattengröße hat Einfluss darauf, wie viel Sie für den Speicher bezahlen, auf die Größe der Volumes, die Sie in einem Aggregat erstellen können, auf die für Cloud Volumes ONTAP verfügbare Gesamtkapazität und auf die Speicherleistung.

Die Leistung von Azure Premium Storage ist an die Datenträgergröße gebunden. Größere Festplatten bieten höhere IOPS und einen höheren Durchsatz. Beispielsweise kann die Wahl von 1-TiB-Festplatten eine bessere Leistung bieten als 500-GiB-Festplatten, allerdings zu höheren Kosten.

Es gibt keine Leistungsunterschiede zwischen den Festplattengrößen für Standardspeicher. Sie sollten die Festplattengröße basierend auf der benötigten Kapazität auswählen.

Informationen zu IOPS und Durchsatz nach Datenträgergröße finden Sie in Azure:

- "Microsoft Azure: Managed Disks – Preise"
- "Microsoft Azure: Page Blobs-Preise"

Standardsystemfestplatten anzeigen

Zusätzlich zum Speicher für Benutzerdaten erwirbt die Konsole auch Cloud-Speicher für Cloud Volumes ONTAP -Systemdaten (Boot-Daten, Root-Daten, Core-Daten und NVRAM). Zu Planungszwecken kann es hilfreich sein, diese Details zu überprüfen, bevor Sie Cloud Volumes ONTAP bereitstellen.

"Anzeigen der Standarddatenträger für Cloud Volumes ONTAP -Systemdaten in Azure" .

Der Konsolenagent benötigt außerdem eine Systemfestplatte. "Details zur Standardkonfiguration des Konsolenagenten anzeigen" .

Sammeln von Netzwerkinformationen

Wenn Sie Cloud Volumes ONTAP in Azure bereitstellen, müssen Sie Details zu Ihrem virtuellen Netzwerk angeben. Sie können ein Arbeitsblatt verwenden, um die Informationen von Ihrem Administrator zu sammeln.

Azure-Informationen	Ihr Wert
Region	
Virtuelles Netzwerk (VNet)	
Subnetz	
Netzwerksicherheitsgruppe (falls Sie Ihre eigene verwenden)	

Wählen Sie eine Schreibgeschwindigkeit

Über die Konsole können Sie eine Schreibgeschwindigkeitseinstellung für Cloud Volumes ONTAP auswählen. Bevor Sie eine Schreibgeschwindigkeit auswählen, sollten Sie die Unterschiede zwischen den normalen und hohen Einstellungen sowie die Risiken und Empfehlungen bei der Verwendung einer hohen Schreibgeschwindigkeit verstehen. "Erfahren Sie mehr über die Schreibgeschwindigkeit" .

Auswählen eines Volume-Nutzungsprofils

ONTAP umfasst mehrere Speichereffizienzfunktionen, die die von Ihnen benötigte Gesamtspeichermenge reduzieren können. Wenn Sie in der Konsole ein Volume erstellen, können Sie ein Profil auswählen, das diese Funktionen aktiviert, oder ein Profil, das sie deaktiviert. Sie sollten mehr über diese Funktionen erfahren, um zu entscheiden, welches Profil Sie verwenden möchten.

Die Storage-Effizienzfunktionen von NetApp bieten folgende Vorteile:

Dünne Bereitstellung

Bietet Hosts oder Benutzern mehr logischen Speicher, als Sie tatsächlich in Ihrem physischen Speicherpool haben. Anstatt Speicherplatz vorab zuzuweisen, wird Speicherplatz jedem Volume dynamisch zugewiesen, während Daten geschrieben werden.

Deduplizierung

Verbessert die Effizienz, indem identische Datenblöcke lokalisiert und durch Verweise auf einen einzigen gemeinsamen Block ersetzt werden. Diese Technik reduziert den Speicherkapazitätsbedarf, indem redundante Datenblöcke, die sich auf demselben Datenträger befinden, eliminiert werden.

Komprimierung

Reduziert die zum Speichern von Daten erforderliche physische Kapazität durch Komprimieren von Daten innerhalb eines Volumes auf Primär-, Sekundär- und Archivspeicher.

Einrichten des Azure-Netzwerks für Cloud Volumes ONTAP

Die NetApp Console übernimmt die Einrichtung von Netzwerkkomponenten für Cloud Volumes ONTAP, wie z. B. IP-Adressen, Netzmasken und Routen. Sie müssen sicherstellen, dass ausgehender Internetzugang verfügbar ist, dass genügend private IP-Adressen verfügbar sind, dass die richtigen Verbindungen vorhanden sind und mehr.

Anforderungen für Cloud Volumes ONTAP

Die folgenden Netzwerkanforderungen müssen in Azure erfüllt sein.

Ausgehender Internetzugang

Cloud Volumes ONTAP -Systeme erfordern ausgehenden Internetzugang für den Zugriff auf externe Endpunkte für verschiedene Funktionen. Cloud Volumes ONTAP kann nicht ordnungsgemäß funktionieren, wenn diese Endpunkte in Umgebungen mit strengen Sicherheitsanforderungen blockiert sind.

Der Konsolenagent kontaktiert außerdem mehrere Endpunkte für den täglichen Betrieb. Informationen zu Endpunkten finden Sie unter "Vom Konsolenagenten kontaktierte Endpunkte anzeigen" Und "Vorbereiten des Netzwerks für die Verwendung der Konsole" .

Cloud Volumes ONTAP Endpunkte

Cloud Volumes ONTAP verwendet diese Endpunkte zur Kommunikation mit verschiedenen Diensten.

Endpunkte	Gilt für	Zweck	Bereitstellungsmodi	Auswirkungen bei Nichtverfügbarkeit
https://netapp-cloud-account.auth0.com	Authentifizierung	Wird zur Authentifizierung in der Konsole verwendet.	Standard- und eingeschränkte Modi.	Die Benutzerauthentifizierung schlägt fehl und die folgenden Dienste sind weiterhin nicht verfügbar: • Cloud Volumes ONTAP Dienste • ONTAP -Dienste • Protokolle und Proxy-Dienste
https://vault.azure.net	Schlüsseltresor	Wird verwendet, um geheime Clientschlüssel aus dem Azure Key Vault abzurufen, wenn kundenverwaltete Schlüssel (CMK) verwendet werden.	Standard-, eingeschränkter und privater Modus.	Cloud Volumes ONTAP Dienste sind nicht verfügbar.

Endpunkte	Gilt für	Zweck	Bereitstellungsmodi	Auswirkungen bei Nichtverfügbarkeit
https://api.bluexp.netapp.com/tenancy	Mietverhältnis	Wird verwendet, um die Cloud Volumes ONTAP -Ressourcen von der Konsole abzurufen, um Ressourcen und Benutzer zu autorisieren.	Standard- und eingeschränkte Modi.	Cloud Volumes ONTAP Ressourcen und die Benutzer sind nicht autorisiert.
https://mysupport.netapp.com/aods/asupmessage https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Wird verwendet, um AutoSupport Telemetriedaten an den NetApp Support zu senden.	Standard- und eingeschränkte Modi.	AutoSupport -Informationen bleiben unversehrt.
https://management.azure.com https://login.microsoftonline.com https://bluexpinfraprod.eastus2.data.azurecr.io https://core.windows.net	Öffentliche Regionen	Kommunikation mit Azure-Diensten.	Standard-, eingeschränkter und privater Modus.	Cloud Volumes ONTAP kann nicht mit dem Azure-Dienst kommunizieren, um bestimmte Vorgänge für die Konsole in Azure auszuführen.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Region China	Kommunikation mit Azure-Diensten.	Standard-, eingeschränkter und privater Modus.	Cloud Volumes ONTAP kann nicht mit dem Azure-Dienst kommunizieren, um bestimmte Vorgänge für die Konsole in Azure auszuführen.
https://management.microsoftazure.de https://login.microsoftonline.de https://blob.core.cloudapi.de https://core.cloudapi.de	Deutschland Region	Kommunikation mit Azure-Diensten.	Standard-, eingeschränkter und privater Modus.	Cloud Volumes ONTAP kann nicht mit dem Azure-Dienst kommunizieren, um bestimmte Vorgänge für die Konsole in Azure auszuführen.
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	Regierungsregionen	Kommunikation mit Azure-Diensten.	Standard-, eingeschränkter und privater Modus.	Cloud Volumes ONTAP kann nicht mit dem Azure-Dienst kommunizieren, um bestimmte Vorgänge für die Konsole in Azure auszuführen.

Endpunkte	Gilt für	Zweck	Bereitstellungsmodi	Auswirkungen bei Nichtverfügbarkeit
https://management.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud	Regierungsregionen des Verteidigungsministeriums	Kommunikation mit Azure-Diensten.	Standard-, eingeschränkter und privater Modus.	Cloud Volumes ONTAP kann nicht mit dem Azure-Dienst kommunizieren, um bestimmte Vorgänge für die Konsole in Azure auszuführen.

Netzwerkproxykonfiguration des NetApp Console Agenten

Sie können die Proxyserverkonfiguration des NetApp Console Agenten verwenden, um ausgehenden Internetzugriff von Cloud Volumes ONTAP zu aktivieren. Die Konsole unterstützt zwei Arten von Proxys:

- **Expliziter Proxy**: Der ausgehende Datenverkehr von Cloud Volumes ONTAP verwendet die HTTP-Adresse des Proxyservers, der während der Proxykonfiguration des Konsolenagenten angegeben wurde. Der Administrator hat möglicherweise auch Benutzeranmeldeinformationen und Stammzertifizierungsstellenzertifikate für eine zusätzliche Authentifizierung konfiguriert. Wenn ein Stamm-CA-Zertifikat für den expliziten Proxy verfügbar ist, stellen Sie sicher , dass Sie dasselbe Zertifikat erhalten und mithilfe des "ONTAP CLI: Sicherheitszertifikat installieren" Befehl.
- **Transparenter Proxy**: Das Netzwerk ist so konfiguriert, dass ausgehender Datenverkehr von Cloud Volumes ONTAP automatisch über den Proxy für den Konsolenagenten geleitet wird. Beim Einrichten eines transparenten Proxys muss der Administrator für die Konnektivität von Cloud Volumes ONTAP nur ein Stamm-CA-Zertifikat bereitstellen, nicht die HTTP-Adresse des Proxyservers. Stellen Sie sicher, dass Sie dasselbe Stamm-CA-Zertifikat erhalten und auf Ihr Cloud Volumes ONTAP System hochladen, indem Sie das "ONTAP CLI: Sicherheitszertifikat installieren" Befehl.

Informationen zum Konfigurieren von Proxy-Servern finden Sie im "Konfigurieren des Konsolenagenten zur Verwendung eines Proxyservers" .

IP-Adressen

Die Konsole weist Cloud Volumes ONTAP in Azure automatisch die erforderliche Anzahl privater IP-Adressen zu. Sie müssen sicherstellen, dass in Ihrem Netzwerk genügend private IP-Adressen verfügbar sind.

Die Anzahl der für Cloud Volumes ONTAP zugewiesenen LIFs hängt davon ab, ob Sie ein Einzelknotensystem oder ein HA-Paar bereitstellen. Ein LIF ist eine IP-Adresse, die einem physischen Port zugeordnet ist. Ein SVM-Management-LIF ist für Management-Tools wie SnapCenter erforderlich.

Ein iSCSI-LIF bietet Clientzugriff über das iSCSI-Protokoll und wird vom System für andere wichtige Netzwerk-Workflows verwendet. Diese LIFs sind erforderlich und sollten nicht gelöscht werden.

IP-Adressen für ein Einzelknotensystem

Die Console weist einem Einzelknotensystem 5 oder 6 IP-Adressen zu:

- Cluster-Verwaltungs-IP

- Knotenverwaltungs-IP
- Intercluster-IP für SnapMirror
- NFS/CIFS-IP
- iSCSI-IP

> Die iSCSI-IP bietet Clientzugriff über das iSCSI-Protokoll. Es wird vom System auch für andere wichtige Netzwerk-Workflows verwendet. Dieses LIF ist erforderlich und sollte nicht gelöscht werden.

- SVM-Verwaltung (optional – nicht standardmäßig konfiguriert)

IP-Adressen für HA-Paare

Die Konsole weist während der Bereitstellung 4 NICs (pro Knoten) IP-Adressen zu.

Beachten Sie, dass die Console auf HA-Paaren eine SVM-Management-LIF erstellt, aber nicht auf Einzelknotensystemen in Azure.

NIC0

- Knotenverwaltungs-IP
- Intercluster-IP
- iSCSI-IP

> Die iSCSI-IP bietet Clientzugriff über das iSCSI-Protokoll. Es wird vom System auch für andere wichtige Netzwerk-Workflows verwendet. Dieses LIF ist erforderlich und sollte nicht gelöscht werden.

NIC1

- Cluster-Netzwerk-IP

NIC2

- Cluster-Interconnect-IP (HA IC)

NIC3

- Pageblob NIC-IP (Festplattenzugriff)

> NIC3 ist nur auf HA-Bereitstellungen anwendbar, die Page-Blob-Speicher verwenden.

Die oben genannten IP-Adressen werden bei Failover-Ereignissen nicht migriert.

Darüber hinaus sind 4 Frontend-IPs (FIPs) für die Migration bei Failover-Ereignissen konfiguriert. Diese Frontend-IPs befinden sich im Load Balancer.

- Cluster-Verwaltungs-IP
- NodeA-Daten-IP (NFS/CIFS)
- NodeB-Daten-IP (NFS/CIFS)

- SVM-Verwaltungs-IP

Sichere Verbindungen zu Azure-Diensten

Standardmäßig aktiviert die Konsole einen Azure Private Link für Verbindungen zwischen Cloud Volumes ONTAP und Azure Page Blob Storage-Konten.

In den meisten Fällen müssen Sie nichts tun – die Konsole verwaltet den Azure Private Link für Sie. Wenn Sie jedoch Azure Private DNS verwenden, müssen Sie eine Konfigurationsdatei bearbeiten. Sie sollten sich auch über eine Anforderung hinsichtlich des Speicherorts des Konsolen-Agenten in Azure im Klaren sein.

Sie können die Private Link-Verbindung auch deaktivieren, wenn dies für Ihre Geschäftsanforderungen erforderlich ist. Wenn Sie die Verknüpfung deaktivieren, konfiguriert die Konsole Cloud Volumes ONTAP so, dass stattdessen ein Service-Endpunkt verwendet wird.

"Erfahren Sie mehr über die Verwendung von Azure Private Links oder Service-Endpunkten mit Cloud Volumes ONTAP" .

Netzwerk für Azure VNet-Verschlüsselung

Cloud Volumes ONTAP unterstützt "Azure Virtual Network (VNet)-Verschlüsselung" die Verschlüsselung des VM-zu-VM-Datenverkehrs innerhalb eines VNet oder zwischen verbundenen VNets. Diese Funktion wird auf der Azure VNet-Ebene konfiguriert und ist unabhängig von der Cloud Volumes ONTAP-Topologie (Single Node oder HA).

Sie müssen lediglich sicherstellen, dass Accelerated Networking auf den Netzwerkkarten der VM aktiviert ist und die Anforderungen und Einschränkungen der Azure VNet-Verschlüsselung überprüfen, bevor Sie die Funktion aktivieren. Sie sollten NetApp verwaltete Load-Balancer-Objekte nicht ändern.

"Azure documentation: VNet-Verschlüsselung und Accelerated Networking".

Verbindungen zu anderen ONTAP -Systemen

Um Daten zwischen einem Cloud Volumes ONTAP -System in Azure und ONTAP -Systemen in anderen Netzwerken zu replizieren, benötigen Sie eine VPN-Verbindung zwischen dem Azure VNet und dem anderen Netzwerk, beispielsweise Ihrem Unternehmensnetzwerk.

Anweisungen hierzu finden Sie im "Microsoft Azure-Dokumentation: Erstellen einer Site-to-Site-Verbindung im Azure-Portal" .

Port für die HA-Verbindung

Ein Cloud Volumes ONTAP HA-Paar umfasst eine HA-Verbindung, die es jedem Knoten ermöglicht, kontinuierlich zu prüfen, ob sein Partner funktioniert, und Protokolldaten für den nichtflüchtigen Speicher des anderen zu spiegeln. Die HA-Verbindung verwendet den TCP-Port 10006 für die Kommunikation.

Standardmäßig ist die Kommunikation zwischen den HA-Interconnect-LIFs offen und es gibt keine Sicherheitsgruppenregeln für diesen Port. Wenn Sie jedoch eine Firewall zwischen den HA-Interconnect-LIFs erstellen, müssen Sie sicherstellen, dass der TCP-Verkehr für Port 10006 geöffnet ist, damit das HA-Paar ordnungsgemäß funktionieren kann.

Nur ein HA-Paar in einer Azure-Ressourcengruppe

Sie müssen für jedes Cloud Volumes ONTAP HA-Paar, das Sie in Azure bereitstellen, eine *dedizierte* Ressourcengruppe verwenden. In einer Ressourcengruppe wird nur ein HA-Paar unterstützt.

Bei der Konsole treten Verbindungsprobleme auf, wenn Sie versuchen, ein zweites Cloud Volumes ONTAP HA-Paar in einer Azure-Ressourcengruppe bereitzustellen.

Sicherheitsgruppenregeln

Die Konsole erstellt Azure-Sicherheitsgruppen, die die eingehenden und ausgehenden Regeln für den erfolgreichen Betrieb von Cloud Volumes ONTAP enthalten. "Sicherheitsgruppenregeln für den Konsolenagenten anzeigen" .

Die Azure-Sicherheitsgruppen für Cloud Volumes ONTAP erfordern, dass die entsprechenden Ports für die interne Kommunikation zwischen den Knoten geöffnet sind. "Erfahren Sie mehr über die internen Ports von ONTAP" .

Wir empfehlen nicht, die vordefinierten Sicherheitsgruppen zu ändern oder benutzerdefinierte Sicherheitsgruppen zu verwenden. Wenn Sie dies jedoch tun müssen, beachten Sie, dass für den Bereitstellungsprozess das Cloud Volumes ONTAP -System vollständigen Zugriff innerhalb seines eigenen Subnetzes benötigt. Wenn Sie nach Abschluss der Bereitstellung die Netzwerksicherheitsgruppe ändern möchten, achten Sie darauf, dass die Cluster-Ports und HA-Netzwerk-Ports geöffnet bleiben. Dies gewährleistet eine nahtlose Kommunikation innerhalb des Cloud Volumes ONTAP Clusters (Any-to-Any-Kommunikation zwischen den Knoten).

Eingangsregeln für Einzelknotensysteme

Wenn Sie ein Cloud Volumes ONTAP -System hinzufügen und eine vordefinierte Sicherheitsgruppe auswählen, können Sie den Datenverkehr innerhalb einer der folgenden Gruppen zulassen:

- **Nur ausgewähltes VNet**: Die Quelle für eingehenden Datenverkehr ist der Subnetzbereich des VNet für das Cloud Volumes ONTAP -System und der Subnetzbereich des VNet, in dem sich der Konsolenagent befindet. Dies ist die empfohlene Option.
- **Alle VNets**: Die Quelle für eingehenden Datenverkehr ist der IP-Bereich 0.0.0.0/0.
- **Deaktiviert**: Diese Option schränkt den öffentlichen Netzwerkzugriff auf Ihr Speicherkonto ein und deaktiviert die Datenschichtung für Cloud Volumes ONTAP -Systeme. Dies ist eine empfohlene Option, wenn Ihre privaten IP-Adressen aufgrund von Sicherheitsbestimmungen und -richtlinien nicht einmal innerhalb desselben VNet offengelegt werden sollen.

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
1000 eingehendes SSH	22 TCP	Beliebig zu Beliebig	SSH-Zugriff auf die IP-Adresse des Cluster-Management-LIF oder eines Node-Management-LIF
1001 eingehendes_http	80 TCP	Beliebig zu Beliebig	HTTP-Zugriff auf die ONTAP System Manager-Webkonsole über die IP-Adresse des Cluster-Management-LIF
1002 inbound_111_tcp	111 TCP	Beliebig zu Beliebig	Remote Procedure Call für NFS
1003 inbound_111_udp	111 UDP	Beliebig zu Beliebig	Remote Procedure Call für NFS

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
1004 inbound_139	139 TCP	Beliebig zu Beliebig	NetBIOS-Dienstsitzung für CIFS
1005 inbound_161-162 _tcp	161-162 TCP	Beliebig zu Beliebig	Einfaches Netzwerkverwaltungsprotokoll
1006 inbound_161-162 _udp	161-162 UDP	Beliebig zu Beliebig	Einfaches Netzwerkverwaltungsprotokoll
1007 inbound_443	443 TCP	Beliebig zu Beliebig	Konnektivität mit dem Konsolenagenten und HTTPS-Zugriff auf die ONTAP System Manager-Webkonsole unter Verwendung der IP-Adresse des Cluster-Management-LIF
1008 inbound_445	445 TCP	Beliebig zu Beliebig	Microsoft SMB/CIFS über TCP mit NetBIOS-Framing
1009 inbound_635_tcp	635 TCP	Beliebig zu Beliebig	NFS-Mount
1010 inbound_635_udp	635 UDP	Beliebig zu Beliebig	NFS-Mount
1011 inbound_749	749 TCP	Beliebig zu Beliebig	Kerberos
1012 inbound_2049_tcp	2049 TCP	Beliebig zu Beliebig	NFS-Server-Daemon
1013 inbound_2049_udp	2049 UDP	Beliebig zu Beliebig	NFS-Server-Daemon
1014 inbound_3260	3260 TCP	Beliebig zu Beliebig	iSCSI-Zugriff über das iSCSI-Daten-LIF
1015 inbound_4045-4046_tcp	4045-4046 TCP	Beliebig zu Beliebig	NFS-Sperrdaemon und Netzwerkstatusmonitor
1016 inbound_4045-4046_udp	4045-4046 UDP	Beliebig zu Beliebig	NFS-Sperrdaemon und Netzwerkstatusmonitor
1017 eingehend_10000	10000 TCP	Beliebig zu Beliebig	Sicherung mit NDMP
1018 eingehend_11104-11105	11104-11105 TCP	Beliebig zu Beliebig	SnapMirror -Datenübertragung
3000 inbound_deny _all_tcp	Beliebiger TCP-Port	Beliebig zu Beliebig	Blockieren Sie den gesamten anderen eingehenden TCP-Verkehr
3001 inbound_deny _all_udp	Beliebiger Port UDP	Beliebig zu Beliebig	Blockieren Sie den gesamten anderen eingehenden UDP-Verkehr

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
65000 AllowVnetInBound	Beliebiger Port, jedes Protokoll	VirtualNetwork zu VirtualNetwork	Eingehender Datenverkehr aus dem VNet
65001 AllowAzureLoad BalancerInBound	Beliebiger Port, jedes Protokoll	AzureLoadBalancer zu Any	Datenverkehr vom Azure Standard Load Balancer
65500 DenyAllInBound	Beliebiger Port, jedes Protokoll	Beliebig zu Beliebig	Blockieren Sie den gesamten anderen eingehenden Datenverkehr

Eingehende Regeln für HA-Systeme

Wenn Sie ein Cloud Volumes ONTAP -System hinzufügen und eine vordefinierte Sicherheitsgruppe auswählen, können Sie den Datenverkehr innerhalb einer der folgenden Gruppen zulassen:

- **Nur ausgewähltes VNet**: Die Quelle für eingehenden Datenverkehr ist der Subnetzbereich des VNet für das Cloud Volumes ONTAP -System und der Subnetzbereich des VNet, in dem sich der Konsolenagent befindet. Dies ist die empfohlene Option.
- **Alle VNets**: Die Quelle für eingehenden Datenverkehr ist der IP-Bereich 0.0.0.0/0.

HA-Systeme haben weniger eingehende Regeln als Einzelknotensysteme, da der eingehende Datenverkehr über den Azure Standard Load Balancer geleitet wird. Aus diesem Grund sollte der Datenverkehr vom Load Balancer geöffnet sein, wie in der "AllowAzureLoadBalancerInBound"-Regel dargestellt.

- **Deaktiviert**: Diese Option schränkt den öffentlichen Netzwerkzugriff auf Ihr Speicherkonto ein und deaktiviert die Datenschichtung für Cloud Volumes ONTAP -Systeme. Dies ist eine empfohlene Option, wenn Ihre privaten IP-Adressen aufgrund von Sicherheitsbestimmungen und -richtlinien nicht einmal innerhalb desselben VNet offengelegt werden sollen.

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
100 inbound_443	443 Jedes Protokoll	Beliebig zu Beliebig	Konnektivität mit dem Konsolenagenten und HTTPS-Zugriff auf die ONTAP System Manager-Webkonsole unter Verwendung der IP-Adresse des Cluster-Management-LIF
101 eingehend_111_tcp	111 Jedes Protokoll	Beliebig zu Beliebig	Remote Procedure Call für NFS
102 inbound_2049_tcp	2049 Jedes Protokoll	Beliebig zu Beliebig	NFS-Server-Daemon
111 eingehendes_ssh	22 Jedes Protokoll	Beliebig zu Beliebig	SSH-Zugriff auf die IP-Adresse des Cluster-Management-LIF oder eines Node-Management-LIF

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
121 inbound_53	53 Jedes Protokoll	Beliebig zu Beliebig	DNS und CIFS
65000 AllowVnetInBound	Beliebiger Port, jedes Protokoll	VirtualNetwork zu VirtualNetwork	Eingehender Datenverkehr aus dem VNet
65001 AllowAzureLoad BalancerInBound	Beliebiger Port, jedes Protokoll	AzureLoadBalancer zu Any	Datenverkehr vom Azure Standard Load Balancer
65500 DenyAllInBound	Beliebiger Port, jedes Protokoll	Beliebig zu Beliebig	Blockieren Sie den gesamten anderen eingehenden Datenverkehr

Ausgangsregeln

Die vordefinierte Sicherheitsgruppe für Cloud Volumes ONTAP öffnet den gesamten ausgehenden Datenverkehr. Wenn das akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Nachrichten. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Ausgangsregeln.

Grundlegende Ausgangsregeln

Die vordefinierte Sicherheitsgruppe für Cloud Volumes ONTAP umfasst die folgenden ausgehenden Regeln.

Hafen	Protokoll	Zweck
Alle	Alle TCP	Der gesamte ausgehende Verkehr
Alle	Alle UDP	Der gesamte ausgehende Verkehr

Erweiterte Ausgangsregeln

Wenn Sie strenge Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation von Cloud Volumes ONTAP erforderlich sind.

Die Quelle ist die Schnittstelle (IP-Adresse) auf dem Cloud Volumes ONTAP -System.

Service	Hafen	Protokoll	Quelle	Ziel	Zweck
Active Directory	88	TCP	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	137	UDP	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	138	UDP	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	NetBIOS-Datagrammdienst
	139	TCP	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	NetBIOS-Dienstsitzung
	389	TCP und UDP	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	LDAP
	445	TCP	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NetBIOS-Framing
	464	TCP	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern & festlegen (SET_CHANGE)
	464	UDP	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	749	TCP	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (RPCSEC_GSS)
	88	TCP	Daten-LIF (NFS, CIFS, iSCSI)	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	137	UDP	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	138	UDP	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	NetBIOS-Datagrammdienst
	139	TCP	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	NetBIOS-Dienstsitzung
	389	TCP und UDP	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	LDAP
	445	TCP	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NetBIOS-Framing
	464	TCP	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern & festlegen (SET_CHANGE)
	464	UDP	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	749	TCP	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern & festlegen (RPCSEC_GSS)

Service	Hafen	Protokoll	Quelle	Ziel	Zweck
AutoSupport	HTTPS	443	Knotenverwaltung LIF	mysupport.netapp.com	AutoSupport (HTTPS ist die Standardeinstellung)
	HTTP	80	Knotenverwaltung LIF	mysupport.netapp.com	AutoSupport (nur wenn das Transportprotokoll von HTTPS auf HTTP geändert wird)
	TCP	3128	Knotenverwaltung LIF	Konsolenagent	Senden von AutoSupport -Nachrichten über einen Proxyserver auf dem Konsolenagenten, wenn keine ausgehende Internetverbindung verfügbar ist
Konfigurationssicherungen	HTTP	80	Knotenverwaltung LIF	http://<IP-Adresse des Konsolenagenten>/occm/offboxconfig	Senden Sie Konfigurationssicherungen an den Konsolenagenten. "ONTAP-Dokumentation" .
DHCP	68	UDP	Knotenverwaltung LIF	DHCP	DHCP-Client für die Ersteinrichtung
DHCPS	67	UDP	Knotenverwaltung LIF	DHCP	DHCP-Server
DNS	53	UDP	Knotenverwaltungs-LIF und Daten-LIF (NFS, CIFS)	DNS	DNS
NDMP	18600–18699	TCP	Knotenverwaltung LIF	Zielserver	NDMP-Kopie
SMTP	25	TCP	Knotenverwaltung LIF	Mailserver	SMTP-Benachrichtigungen, können für AutoSupport verwendet werden
SNMP	161	TCP	Knotenverwaltung LIF	Monitorserver	Überwachung durch SNMP-Traps
	161	UDP	Knotenverwaltung LIF	Monitorserver	Überwachung durch SNMP-Traps
	162	TCP	Knotenverwaltung LIF	Monitorserver	Überwachung durch SNMP-Traps
	162	UDP	Knotenverwaltung LIF	Monitorserver	Überwachung durch SNMP-Traps
SnapMirror	11104	TCP	Intercluster LIF	ONTAP Intercluster-LIFs	Verwaltung von Intercluster-Kommunikationssitzungen für SnapMirror
	11105	TCP	Intercluster LIF	ONTAP Intercluster-LIFs	SnapMirror -Datenübertragung
Syslog	514	UDP	Knotenverwaltung LIF	Syslog-Server	Syslog-Weiterleitungsnachrichten

Anforderungen für den Konsolenagenten

Wenn Sie noch keinen Konsolenagenten erstellt haben, sollten Sie auch die Netzwerkanforderungen für den Konsolenagenten überprüfen.

- "Netzwerkanforderungen für den Konsolenagenten anzeigen"
- "Sicherheitsgruppenregeln in Azure"

Verwandte Themen

- "Überprüfen Sie das AutoSupport -Setup für Cloud Volumes ONTAP"
- "Erfahren Sie mehr über die internen Ports von ONTAP" .

Richten Sie Cloud Volumes ONTAP für die Verwendung eines vom Kunden verwalteten Schlüssels in Azure ein

Daten werden auf Cloud Volumes ONTAP in Azure mithilfe der Azure Storage Service Encryption mit einem von Microsoft verwalteten Schlüssel automatisch verschlüsselt. Sie können stattdessen jedoch Ihren eigenen Verschlüsselungsschlüssel verwenden, indem Sie die Schritte auf dieser Seite befolgen.

Übersicht über die Datenverschlüsselung

Cloud Volumes ONTAP -Daten werden in Azure automatisch verschlüsselt mit "Azure Storage Service-Verschlüsselung" . Die Standardimplementierung verwendet einen von Microsoft verwalteten Schlüssel. Es ist keine Einrichtung erforderlich.

Wenn Sie einen vom Kunden verwalteten Schlüssel mit Cloud Volumes ONTAP verwenden möchten, müssen Sie die folgenden Schritte ausführen:

1. Erstellen Sie in Azure einen Schlüsseltresor und generieren Sie dann einen Schlüssel in diesem Tresor.
2. Verwenden Sie in der NetApp Console die API, um ein Cloud Volumes ONTAP -System zu erstellen, das den Schlüssel verwendet.

So werden Daten verschlüsselt

Die Konsole verwendet einen Datenträgerverschlüsselungssatz, der die Verwaltung von Verschlüsselungsschlüsseln mit verwalteten Datenträgern und nicht mit Seitenblobs ermöglicht. Alle neuen Datenträger verwenden ebenfalls denselben Datenträgerverschlüsselungssatz. Niedrigere Versionen verwenden den von Microsoft verwalteten Schlüssel anstelle des vom Kunden verwalteten Schlüssels.

Nachdem Sie ein Cloud Volumes ONTAP -System erstellt haben, das für die Verwendung eines vom Kunden verwalteten Schlüssels konfiguriert ist, werden Cloud Volumes ONTAP Daten wie folgt verschlüsselt.

Cloud Volumes ONTAP Konfiguration	Für die Schlüsselverschlüsselung verwendete Systemfestplatten	Für die Schlüsselverschlüsselung verwendete Datenträger
Einzelner Knoten	• Stiefel • Kern • NVRAM	• Wurzel • Daten

Cloud Volumes ONTAP Konfiguration	Für die Schlüsselverschlüsselung verwendete Systemfestplatten	Für die Schlüsselverschlüsselung verwendete Datenträger
Azure HA – einzelne Verfügbarkeitszone mit Seitenblobs	• Stiefel • Kern • NVRAM	Keine
Azure HA – einzelne Verfügbarkeitszone mit gemeinsam genutzten verwalteten Datenträgern	• Stiefel • Kern • NVRAM	• Wurzel • Daten
Azure HA mehrere Verfügbarkeitszonen mit gemeinsam genutzten verwalteten Datenträgern	• Stiefel • Kern • NVRAM	• Wurzel • Daten

Alle Azure-Speicherkonten für Cloud Volumes ONTAP werden mit einem vom Kunden verwalteten Schlüssel verschlüsselt. Wenn Sie Ihre Speicherkonten während der Erstellung verschlüsseln möchten, müssen Sie die ID der Ressource in der Cloud Volumes ONTAP Erstellungsanforderung erstellen und angeben. Dies gilt für alle Arten von Bereitstellungen. Wenn Sie ihn nicht angeben, werden die Speicherkonten trotzdem verschlüsselt, aber die Konsole erstellt zuerst die Speicherkonten mit einer von Microsoft verwalteten Schlüsselverschlüsselung und aktualisiert dann die Speicherkonten, um den vom Kunden verwalteten Schlüssel zu verwenden.

Schlüsselrotation in Cloud Volumes ONTAP

Wenn Sie Ihre Verschlüsselungsschlüssel konfigurieren, müssen Sie das Azure-Portal verwenden, um die automatische Schlüsselrotation einzurichten und zu aktivieren. Durch das Erstellen und Aktivieren einer neuen Version von Verschlüsselungsschlüsseln wird sichergestellt, dass Cloud Volumes ONTAP die neueste Schlüsselversion automatisch erkennen und für die Verschlüsselung verwenden kann. So wird sichergestellt, dass Ihre Daten ohne manuelles Eingreifen sicher bleiben.

Informationen zum Konfigurieren Ihrer Schlüssel und zum Einrichten der Schlüsselrotation finden Sie in den folgenden Microsoft Azure-Dokumentationsthemen:

- "Konfigurieren der automatischen Rotation kryptografischer Schlüssel in Azure Key Vault"
- "Azure PowerShell – Aktivieren von kundenseitig verwalteten Schlüsseln"

> Stellen Sie nach der Konfiguration der Schlüssel sicher, dass Sie "*Automatische Drehung aktivieren*" , damit Cloud Volumes ONTAP die neuen Schlüssel verwenden kann, wenn die vorherigen Schlüssel ablaufen. Wenn Sie diese Option im Azure-Portal nicht aktivieren, kann Cloud Volumes ONTAP die neuen Schlüssel nicht automatisch erkennen, was zu Problemen bei der Speicherbereitstellung führen kann.

Erstellen einer benutzerseitig zugewiesenen verwalteten Identität

Sie haben die Möglichkeit, eine Ressource namens „benutzerseitig zugewiesene verwaltete Identität“ zu erstellen. Auf diese Weise können Sie Ihre Speicherkonten verschlüsseln, wenn Sie ein Cloud Volumes ONTAP -System erstellen. Wir empfehlen, diese Ressource zu erstellen, bevor Sie einen Schlüsseltresor

erstellen und einen Schlüssel generieren.

Die Ressource hat die folgende ID: `userassignedidentity` .

Schritte

1. Gehen Sie in Azure zu Azure-Diensten und wählen Sie **Verwaltete Identitäten** aus.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie die folgenden Details an:
   - **Abonnement**: Wählen Sie ein Abonnement. Wir empfehlen, dasselbe Abonnement wie das Abonnement des Konsolenagenten zu wählen.
   - **Ressourcengruppe**: Verwenden Sie eine vorhandene Ressourcengruppe oder erstellen Sie eine neue.
   - **Region**: Wählen Sie optional dieselbe Region wie der Konsolenagent aus.
   - **Name**: Geben Sie einen Namen für die Ressource ein.
4. Fügen Sie optional Tags hinzu.
5. Klicken Sie auf **Erstellen**.

Erstellen eines Schlüsseltresors und Generieren eines Schlüssels

Der Schlüsseltresor muss sich im selben Azure-Abonnement und in derselben Region befinden, in der Sie das Cloud Volumes ONTAP -System erstellen möchten.

Wenn dueine benutzerseitig zugewiesene verwaltete Identität erstellt , während Sie den Schlüsseltresor erstellen, sollten Sie auch eine Zugriffsrichtlinie für den Schlüsseltresor erstellen.

Schritte

1. "Erstellen eines Schlüsseltresors in Ihrem Azure-Abonnement" .

   Beachten Sie die folgenden Anforderungen für den Schlüsseltresor:

   - Der Schlüsseltresor muss sich in derselben Region wie das Cloud Volumes ONTAP -System befinden.
   - Die folgenden Optionen sollten aktiviert sein:
     - **Soft-Delete** (diese Option ist standardmäßig aktiviert, darf aber *nicht* deaktiviert werden)
     - **Spülschutz**
     - **Azure Disk Encryption für die Volume-Verschlüsselung** (für Einzelknotensysteme, HA-Paare in mehreren Zonen und HA-Einzel-AZ-Bereitstellungen)

       Die Verwendung von vom Azure-Kunden verwalteten Verschlüsselungsschlüsseln hängt davon ab, ob die Azure-Datenträgerverschlüsselung für den Schlüsseltresor aktiviert ist.

   - Die folgende Option sollte aktiviert sein, wenn Sie eine benutzerseitig zugewiesene verwaltete Identität erstellt haben:
     - **Richtlinie zum Tresorzugriff**
2. Wenn Sie „Tresorzugriffsrichtlinie“ ausgewählt haben, klicken Sie auf „Erstellen“, um eine Zugriffsrichtlinie für den Schlüsseltresor zu erstellen. Wenn nicht, fahren Sie mit Schritt 3 fort.
   a. Wählen Sie die folgenden Berechtigungen aus:

- erhalten
- Liste
- entschlüsseln
- verschlüsseln
- Schlüssel auspacken
- Wrap-Schlüssel
- verifizieren
- Zeichen

b. Wählen Sie die vom Benutzer zugewiesene verwaltete Identität (Ressource) als Prinzipal aus.

c. Überprüfen und erstellen Sie die Zugriffsrichtlinie.

3. "Generieren eines Schlüssels im Schlüsseltresor" .

   Beachten Sie folgende Anforderungen an den Schlüssel:

   - Der Schlüsseltyp muss **RSA** sein.
   - Die empfohlene RSA-Schlüsselgröße ist **2048**, es werden jedoch auch andere Größen unterstützt.

Erstellen Sie ein System, das den Verschlüsselungsschlüssel verwendet

Nachdem Sie den Schlüsseltresor erstellt und einen Verschlüsselungsschlüssel generiert haben, können Sie ein neues Cloud Volumes ONTAP System erstellen, das für die Verwendung des Schlüssels konfiguriert ist. Diese Schritte werden durch die Verwendung der API unterstützt.

Erforderliche Berechtigungen

Wenn Sie einen vom Kunden verwalteten Schlüssel mit einem Cloud Volumes ONTAP System mit einem einzelnen Knoten verwenden möchten, stellen Sie sicher, dass der Konsolenagent über die folgenden Berechtigungen verfügt:

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.Compute/diskEncryptionSets/delete"
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

"Aktuelle Liste der Berechtigungen anzeigen"

Schritte

1. Rufen Sie die Liste der Schlüsseltresore in Ihrem Azure-Abonnement mithilfe des folgenden API-Aufrufs ab.

   Für ein HA-Paar: `GET /azure/ha/metadata/vaults`

   Für einen einzelnen Knoten: `GET /azure/vsa/metadata/vaults`

Notieren Sie sich den **Namen** und die **Ressourcengruppe**. Sie müssen diese Werte im nächsten Schritt angeben.

"Erfahren Sie mehr über diesen API-Aufruf" .

2. Rufen Sie die Liste der Schlüssel im Tresor mithilfe des folgenden API-Aufrufs ab.

   Für ein HA-Paar: `GET /azure/ha/metadata/keys-vault`

   Für einen einzelnen Knoten: `GET /azure/vsa/metadata/keys-vault`

   Notieren Sie sich den **Schlüsselnamen**. Sie müssen diesen Wert (zusammen mit dem Tresornamen) im nächsten Schritt angeben.

   "Erfahren Sie mehr über diesen API-Aufruf" .

3. Erstellen Sie mithilfe des folgenden API-Aufrufs ein Cloud Volumes ONTAP -System.

   a. Für ein HA-Paar:

      `POST /azure/ha/working-environments`

      Der Anforderungstext muss die folgenden Felder enthalten:

      ```
      "azureEncryptionParameters": {
                    "key": "keyName",
                    "vaultName": "vaultName"
      }
      ```

      Fügen Sie die `"userAssignedIdentity": " userAssignedIdentityId"` Feld, wenn Sie diese Ressource zur Verwendung für die Speicherkontoverschlüsselung erstellt haben.

      "Erfahren Sie mehr über diesen API-Aufruf" .

   b. Für ein Single-Node-System:

      `POST /azure/vsa/working-environments`

      Der Anforderungstext muss die folgenden Felder enthalten:

      ```
      "azureEncryptionParameters": {
                    "key": "keyName",
                    "vaultName": "vaultName"
      }
      ```

      Fügen Sie die `"userAssignedIdentity": " userAssignedIdentityId"` Feld, wenn Sie diese Ressource zur Verwendung für die Speicherkontoverschlüsselung erstellt haben.

"Erfahren Sie mehr über diesen API-Aufruf" .

Ergebnis

Sie verfügen über ein neues Cloud Volumes ONTAP -System, das für die Verwendung Ihres vom Kunden verwalteten Schlüssels zur Datenverschlüsselung konfiguriert ist.

Einrichten der Lizenzierung für Cloud Volumes ONTAP in Azure

Nachdem Sie entschieden haben, welche Lizenzierungsoption Sie mit Cloud Volumes ONTAP verwenden möchten, sind einige Schritte erforderlich, bevor Sie diese Lizenzierungsoption beim Erstellen eines neuen Systems auswählen können.

Freemium

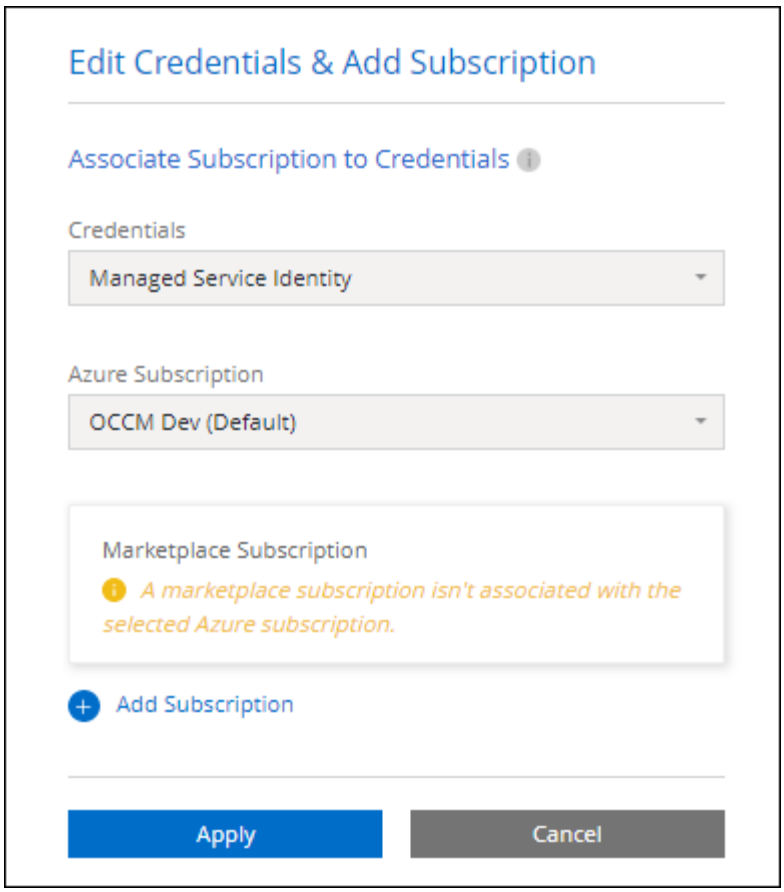
Wählen Sie das Freemium-Angebot, um Cloud Volumes ONTAP mit bis zu 500 GiB bereitgestellter Kapazität kostenlos zu nutzen. "Erfahren Sie mehr über das Freemium-Angebot" .

Schritte

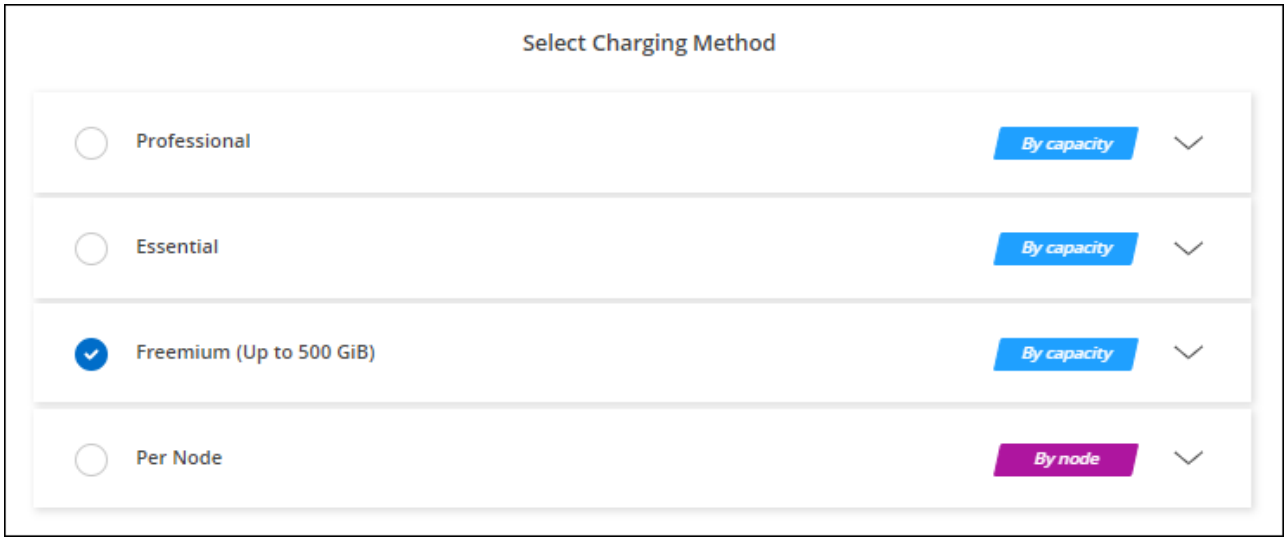
1. Wählen Sie im linken Navigationsmenü der NetApp Console*Speicher > Verwaltung* aus.
2. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten.

    a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldeinformationen bearbeiten > Abonnement hinzufügen** und folgen Sie dann den Anweisungen, um das Pay-as-you-go-Angebot im Azure Marketplace zu abonnieren.

    Ihnen werden keine Kosten über das Marktplatz-Abonnement berechnet, es sei denn, Sie überschreiten 500 GiB bereitgestellte Kapazität. Zu diesem Zeitpunkt wird das System automatisch auf das"Essentials-Paket" .



a. Nachdem Sie zur Konsole zurückgekehrt sind, wählen Sie **Freemium** aus, wenn Sie die Seite mit den Abrechnungsmethoden erreichen.



"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in Azure an" .

Kapazitätsbasierte Lizenz

Mit der kapazitätsbasierten Lizenzierung können Sie für Cloud Volumes ONTAP pro TiB Kapazität bezahlen. Die kapazitätsbasierte Lizenzierung ist in Form eines *Pakets* verfügbar: das Essentials-Paket oder das Professional-Paket.

Die Pakete Essentials und Professional sind mit folgenden Verbrauchsmodellen bzw. Kaufoptionen erhältlich:

- Eine von NetApp erworbene Lizenz (Bring Your Own License (BYOL))
- Ein stündliches Pay-as-you-go-Abonnement (PAYGO) aus dem Azure Marketplace
- Ein Jahresvertrag

"Erfahren Sie mehr über kapazitätsbasierte Lizenzierung" .

In den folgenden Abschnitten wird beschrieben, wie Sie mit jedem dieser Verbrauchsmodelle beginnen.

BYOL

Zahlen Sie im Voraus, indem Sie eine Lizenz (BYOL) von NetApp erwerben, um Cloud Volumes ONTAP -Systeme bei jedem Cloud-Anbieter bereitzustellen.

NetApp hat den Erwerb, die Verlängerung und die Erneuerung von BYOL-Lizenzen eingeschränkt. Weitere Informationen finden Sie unter "Eingeschränkte Verfügbarkeit der BYOL-Lizenzierung für Cloud Volumes ONTAP" .

Schritte

1. "Kontaktieren Sie den NetApp -Vertrieb, um eine Lizenz zu erhalten"
2. "Fügen Sie Ihr NetApp Support Site-Konto zur Konsole hinzu"

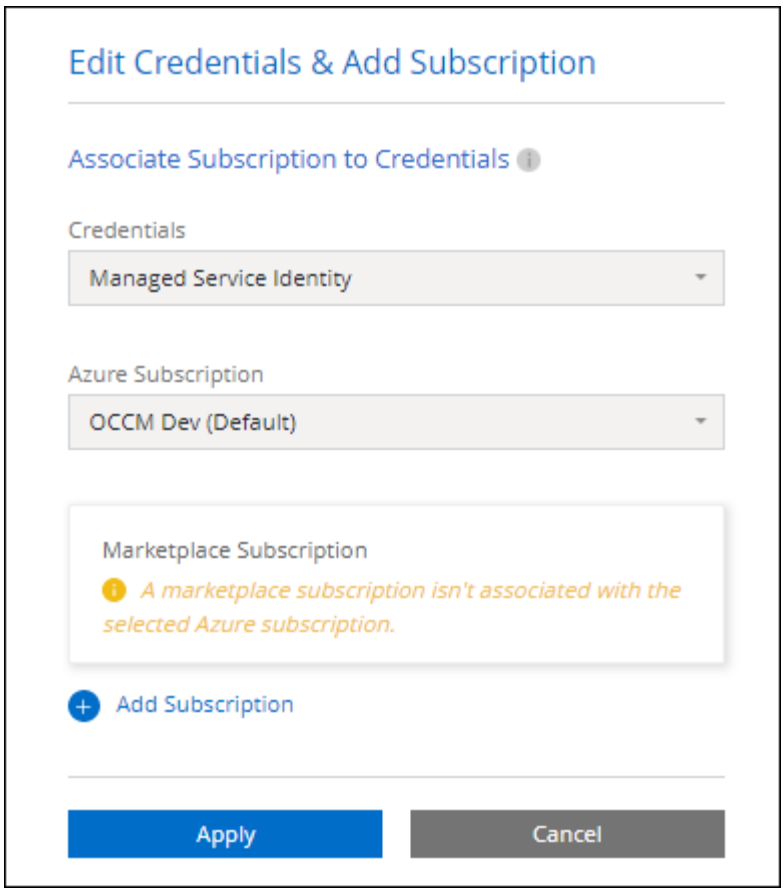
   Die Konsole fragt automatisch den Lizenzierungsdienst von NetApp ab, um Details zu den Lizenzen abzurufen, die mit Ihrem NetApp Support Site-Konto verknüpft sind. Wenn keine Fehler auftreten, fügt die Konsole die Lizenzen automatisch zur Konsole hinzu.

   Ihre Lizenz muss in der Konsole verfügbar sein, bevor Sie sie mit Cloud Volumes ONTAP verwenden können. Bei Bedarf können Sie"Fügen Sie die Lizenz manuell zur Konsole hinzu" .

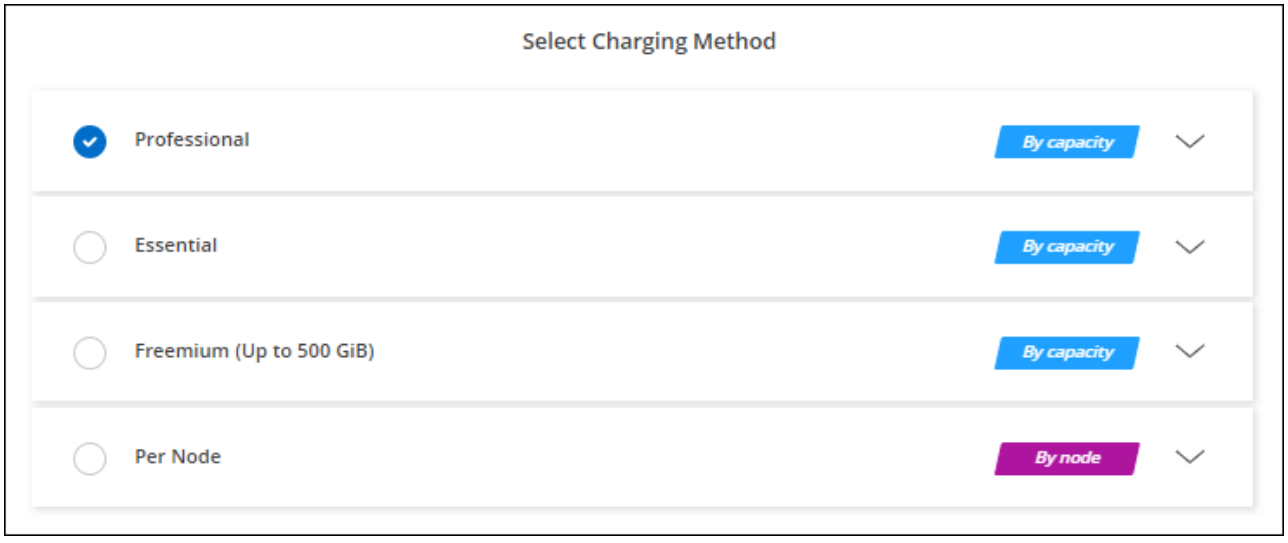
3. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten.

   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldeinformationen bearbeiten > Abonnement hinzufügen** und folgen Sie dann den Anweisungen, um das Pay-as-you-go-Angebot im Azure Marketplace zu abonnieren.

      Die von Ihnen bei NetApp erworbene Lizenz wird immer zuerst in Rechnung gestellt. Wenn Sie jedoch Ihre lizenzierte Kapazität überschreiten oder die Laufzeit Ihrer Lizenz abläuft, wird Ihnen der Stundensatz auf dem Marktplatz in Rechnung gestellt.



a. Nachdem Sie zur Konsole zurückgekehrt sind, wählen Sie auf der Seite mit den Abrechnungsmethoden ein kapazitätsbasiertes Paket aus.



"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in Azure an" .

PAYGO-Abonnement

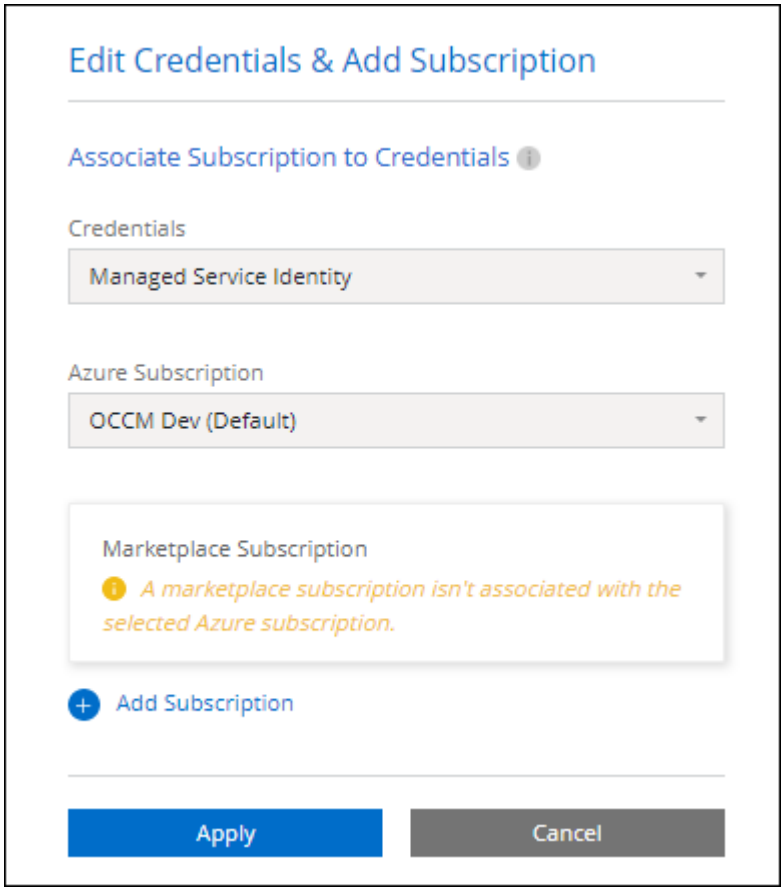
Zahlen Sie stundenweise, indem Sie das Angebot auf dem Marktplatz Ihres Cloud-Anbieters abonnieren.

Wenn Sie ein Cloud Volumes ONTAP -System erstellen, werden Sie von der Konsole aufgefordert, die im Azure Marketplace verfügbare Vereinbarung zu abonnieren. Dieses Abonnement wird dann zum Aufladen mit

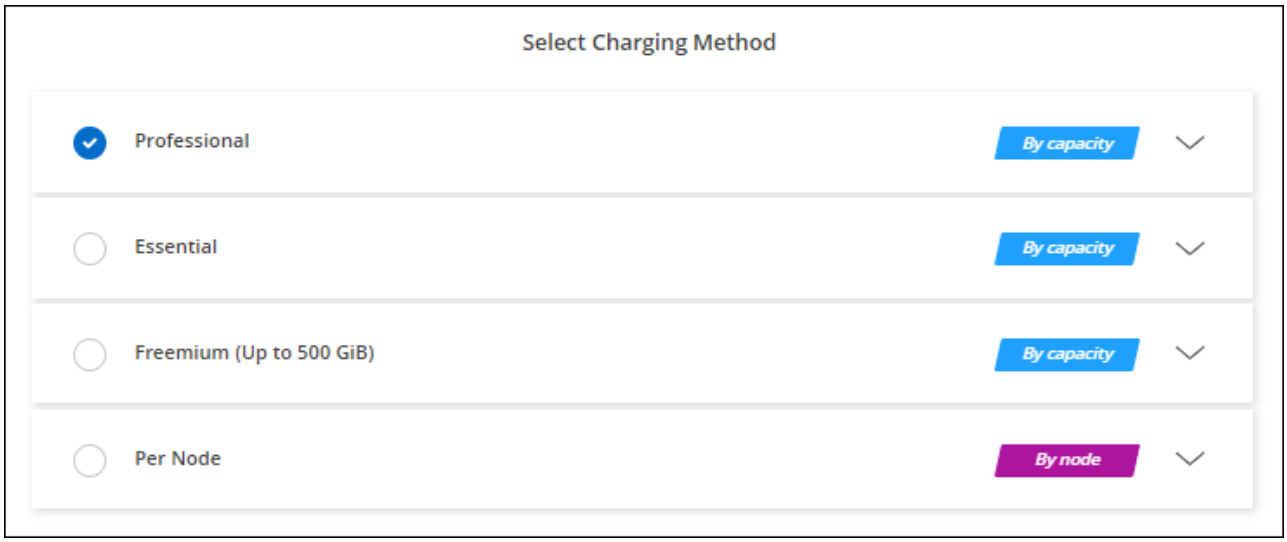
dem System verknüpft. Sie können dasselbe Abonnement für zusätzliche Systeme verwenden.

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten.
   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldeinformationen bearbeiten > Abonnement hinzufügen** und folgen Sie dann den Anweisungen, um das Pay-as-you-go-Angebot im Azure Marketplace zu abonnieren.



   b. Nachdem Sie zur Konsole zurückgekehrt sind, wählen Sie auf der Seite mit den Abrechnungsmethoden ein kapazitätsbasiertes Paket aus.



"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in Azure an" .

Sie können die mit Ihren Azure-Konten verknüpften Azure Marketplace-Abonnements auf der Seite „Einstellungen > Anmeldeinformationen“ verwalten. "Erfahren Sie, wie Sie Ihre Azure-Konten und -Abonnements verwalten"

Jahresvertrag

Bezahlen Sie Cloud Volumes ONTAP jährlich, indem Sie einen Jahresvertrag abschließen.

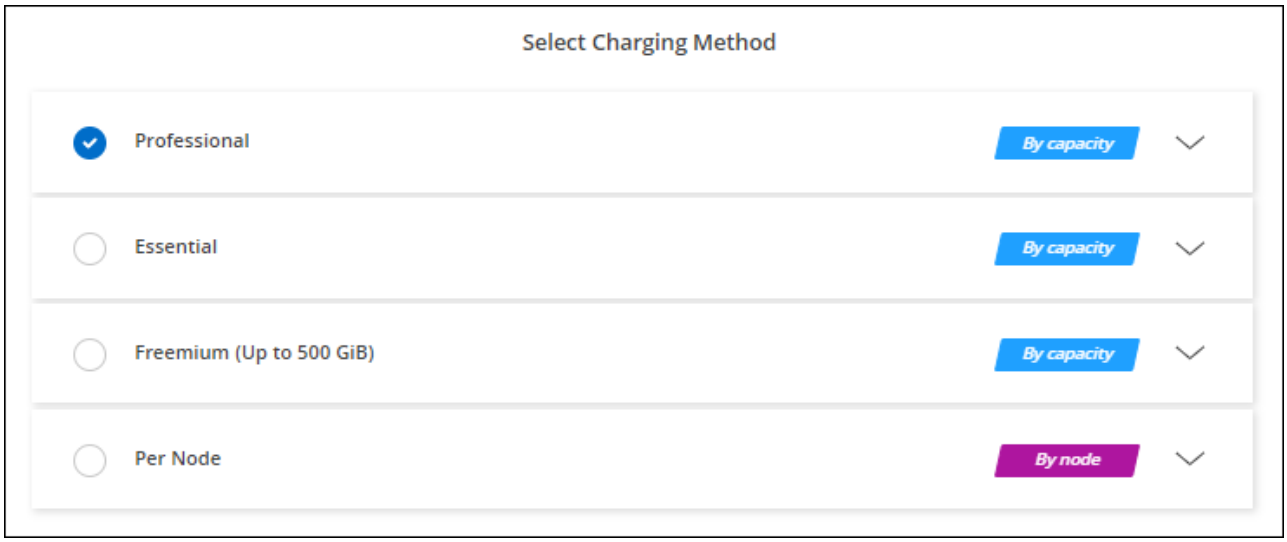
Schritte

1. Wenden Sie sich an Ihren NetApp Vertriebsmitarbeiter, um einen Jahresvertrag abzuschließen.

   Der Vertrag ist als *privates* Angebot im Azure Marketplace verfügbar.

   Nachdem NetApp Ihnen das private Angebot mitgeteilt hat, können Sie bei der Systemerstellung den Jahresplan auswählen, wenn Sie sich im Azure Marketplace anmelden.

2. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten.
   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldeinformationen bearbeiten > Abonnement hinzufügen > Fortfahren**.
   b. Wählen Sie im Azure-Portal den Jahresplan aus, der mit Ihrem Azure-Konto geteilt wurde, und klicken Sie dann auf **Abonnieren**.
   c. Nachdem Sie zur Konsole zurückgekehrt sind, wählen Sie auf der Seite mit den Abrechnungsmethoden ein kapazitätsbasiertes Paket aus.



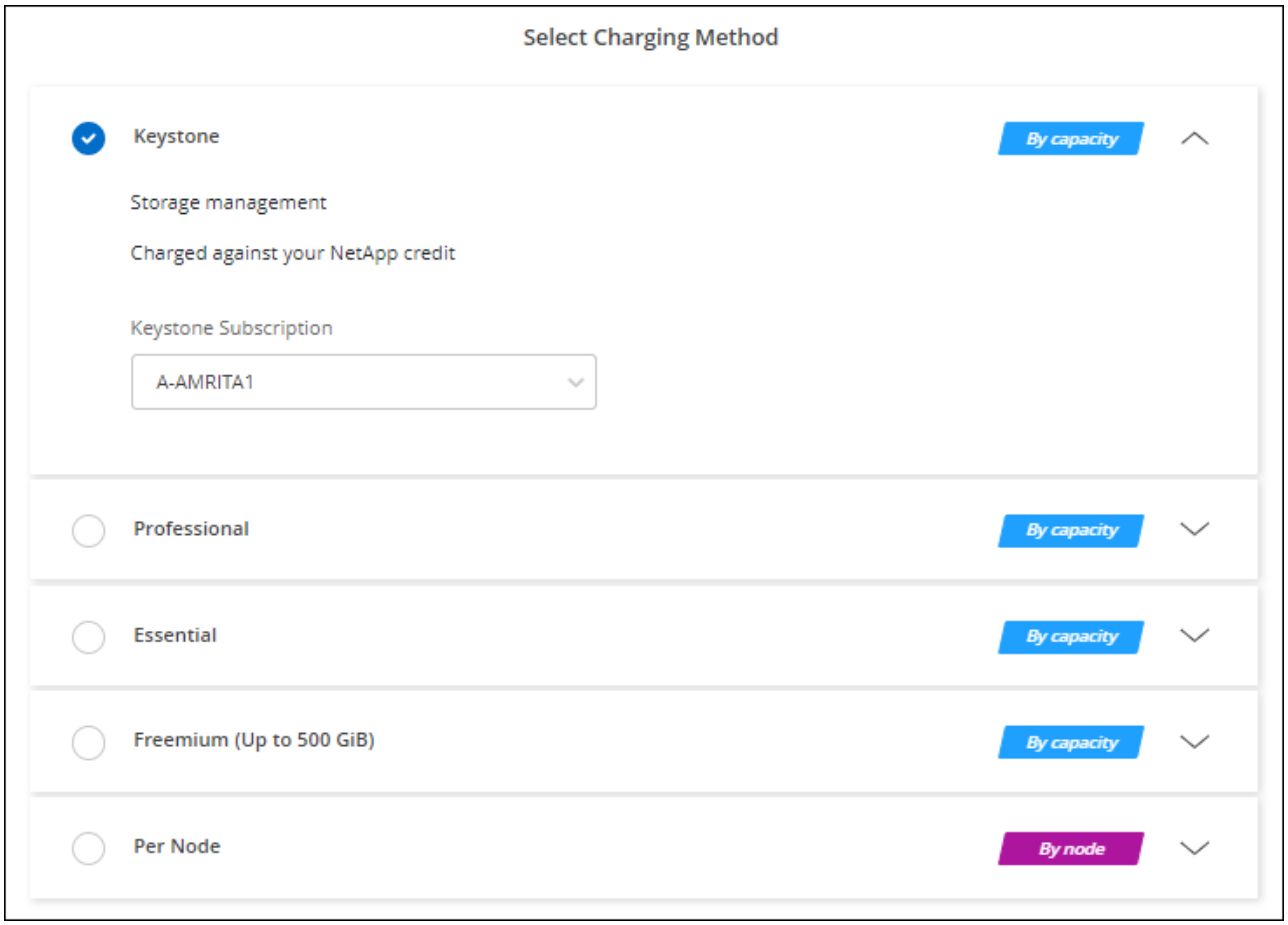
"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in Azure an" .

Keystone Abonnement

Bei einem Keystone -Abonnement handelt es sich um einen Abonnementdienst mit nutzungsabhängiger Bezahlung. "Erfahren Sie mehr über NetApp Keystone -Abonnements" .

Schritte

1. Wenn Sie noch kein Abonnement haben, "NetApp kontaktieren"
2. mailto:ng-keystone-success@netapp.com [Kontaktieren Sie NetApp], um Ihr Benutzerkonto in der Konsole mit einem oder mehreren Keystone Abonnements zu autorisieren.
3. Nachdem NetApp Ihr Konto autorisiert hat,"Verknüpfen Sie Ihre Abonnements zur Verwendung mit Cloud Volumes ONTAP" .
4. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten.
   a. Wählen Sie die Abrechnungsmethode „Keystone -Abonnement“ aus, wenn Sie zur Auswahl einer Abrechnungsmethode aufgefordert werden.



"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in Azure an" .

Knotenbasierte Lizenz

Eine knotenbasierte Lizenz ist die Lizenz der vorherigen Generation für Cloud Volumes ONTAP. Eine knotenbasierte Lizenz kann von NetApp (BYOL) erworben werden und ist nur in bestimmten Fällen für Lizenzverlängerungen verfügbar. Weitere Informationen finden Sie unter:

- "Ende der Verfügbarkeit knotenbasierter Lizenzen"
- "Ende der Verfügbarkeit von knotenbasierten Lizenzen"
- "Konvertieren Sie eine knotenbasierte Lizenz in eine kapazitätsbasierte Lizenz"

Aktivieren Sie den Hochverfügbarkeitsmodus für Cloud Volumes ONTAP in Azure

Sie sollten den Hochverfügbarkeitsmodus (HA) von Microsoft Azure aktivieren, um ungeplante Failover-Zeiten zu reduzieren und die NFSv4-Unterstützung für Cloud Volumes ONTAP zu ermöglichen. Wenn Sie diesen Modus aktivieren, können Ihre Cloud Volumes ONTAP HA-Knoten bei ungeplanten Failovern auf CIFS- und NFSv4-Clients ein niedriges Recovery Time Objective (RTO) von 60 Sekunden erreichen.

Ab Cloud Volumes ONTAP 9.10.1 haben wir die ungeplante Failover-Zeit für Cloud Volumes ONTAP HA-Paare, die in Microsoft Azure ausgeführt werden, reduziert und Unterstützung für NFSv4 hinzugefügt. Um diese Verbesserungen für Cloud Volumes ONTAP verfügbar zu machen, müssen Sie die Hochverfügbarkeitsfunktion in Ihrem Azure-Abonnement aktivieren.

Informationen zu diesem Vorgang

NetApp Console fordert Sie mit diesen Details auf, wenn die Funktion in einem Azure-Abonnement aktiviert werden muss. Beachten Sie Folgendes:

- Es gibt keine Probleme mit der Hochverfügbarkeit Ihres Cloud Volumes ONTAP HA-Paares. Diese Azure-Funktion arbeitet mit ONTAP zusammen, um die vom Client beobachtete Anwendungsausfallzeit für NFS-Protokolle zu reduzieren, die aus ungeplanten Failover-Ereignissen resultiert.
- Das Aktivieren dieser Funktion hat keine Unterbrechungen für Cloud Volumes ONTAP HA-Paare.
- Das Aktivieren dieser Funktion für Ihr Azure-Abonnement verursacht keine Probleme mit anderen VMs.
- Cloud Volumes ONTAP verwendet einen internen Azure Load Balancer während Failovers von Cluster- und SVM-Management-LIFs auf CIFS- und NFS-Clients.
- Wenn der HA-Modus aktiviert ist, scannt die Konsole das System alle 12 Stunden, um die internen Azure Load Balancer-Regeln zu aktualisieren.

Schritte

Ein Azure-Benutzer mit *Owner*-Berechtigungen kann die Funktion über die Azure CLI aktivieren.

1. "Greifen Sie über das Azure-Portal auf die Azure Cloud Shell zu"
2. Registrieren Sie die Funktion für den Hochverfügbarkeitsmodus:

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

3. Überprüfen Sie optional, ob die Funktion jetzt registriert ist:

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

Die Azure CLI sollte ein Ergebnis ähnlich dem folgenden zurückgeben:

```
{
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

Weiterführende Links

1. "Microsoft Azure documentation: Übersicht über Hochverfügbarkeitsports"
2. "Microsoft Azure documentation: Erste Schritte mit der Azure CLI"

Aktivieren Sie VMOrchestratorZonalMultiFD für Cloud Volumes ONTAP in Azure

Für die Bereitstellung von VM-Instanzen in lokal redundanten Speicher-Einzelverfügbarkeitszonen (Local-Redundant Storage, LRS) sollten Sie die Microsoft `Microsoft.Compute/VMOrchestratorZonalMultiFD` Funktion für Ihre Abonnements. Im Hochverfügbarkeitsmodus (HA) erleichtert diese Funktion die Bereitstellung von Knoten in separaten Fehlerdomänen in derselben Verfügbarkeitszone.

Wenn Sie diese Funktion nicht aktivieren, erfolgt keine zonale Bereitstellung und die vorherige nicht zonale LRS-Bereitstellung wird wirksam.

Informationen zur VM-Bereitstellung in einer einzelnen Verfügbarkeitszone finden Sie unter"Hochverfügbarkeitspaare in Azure" .

Führen Sie diese Schritte als Benutzer mit „Eigentümer“-Berechtigungen aus:

Schritte

1. Greifen Sie über das Azure-Portal auf Azure Cloud Shell zu. Weitere Informationen finden Sie im "Microsoft Azure-Dokumentation: Erste Schritte mit Azure Cloud Shell" .
2. Registrieren Sie sich für die `Microsoft.Compute/VMOrchestratorZonalMultiFD` Funktion, indem Sie diesen Befehl ausführen:

   ```
   az account set -s <Azure_subscription_name_or_ID> az feature register --name VMOrchestratorZonalMultiFD --namespace Microsoft.Compute
   ```

3. Überprüfen Sie den Registrierungsstatus und das Ausgabebeispiel:

   ```
   az feature show -n VMOrchestratorZonalMultiFD --namespace Microsoft.Compute { "id": "/subscriptions/<ID>/providers/Microsoft.Features/providers/Microsoft.Compute/features/VMOrchestratorZonalMultiFD", "name": "Microsoft.Compute/VMOrchestratorZonalMultiFD", "properties": { "state": "Registered" }, "type": "Microsoft.Features/providers/features" }
   ```

Starten Sie Cloud Volumes ONTAP in Azure

Sie können ein Einzelknotensystem oder ein HA-Paar in Azure starten, indem Sie ein Cloud Volumes ONTAP-System in der NetApp Console erstellen.

Bevor Sie beginnen

Bevor Sie beginnen, benötigen Sie Folgendes.

- Ein Konsolenagent, der aktiv ist und läuft.
  - Sie sollten über eine "Konsolenagent, der mit Ihrem System verknüpft ist" .
  - "Sie sollten darauf vorbereitet sein, den Konsolenagenten immer laufen zu lassen" .

- Ein Verständnis der Konfiguration, die Sie verwenden möchten.

  Sie sollten eine Konfiguration geplant haben und die erforderlichen Azure-Netzwerkdetails von Ihrem Administrator erhalten haben. Weitere Informationen finden Sie unter "Planen Ihrer Cloud Volumes ONTAP Konfiguration" .

- Ein Verständnis dafür, was zum Einrichten der Lizenzierung für Cloud Volumes ONTAP erforderlich ist.

  "Erfahren Sie, wie Sie die Lizenzierung einrichten" .

Informationen zu diesem Vorgang

Wenn die Konsole ein Cloud Volumes ONTAP -System in Azure erstellt, erstellt sie mehrere Azure-Objekte, z. B. eine Ressourcengruppe, Netzwerkschnittstellen und Speicherkonten. Am Ende des Assistenten können Sie eine Zusammenfassung der Ressourcen überprüfen.

Möglicher Datenverlust

Die bewährte Methode besteht darin, für jedes Cloud Volumes ONTAP -System eine neue, dedizierte Ressourcengruppe zu verwenden.

Aufgrund des Risikos eines Datenverlusts wird die Bereitstellung von Cloud Volumes ONTAP in einer vorhandenen, gemeinsam genutzten Ressourcengruppe nicht empfohlen. Während die Konsole Cloud Volumes ONTAP -Ressourcen im Falle eines Bereitstellungsfehlers oder einer Löschung aus einer freigegebenen Ressourcengruppe entfernen kann, kann es vorkommen, dass ein Azure-Benutzer versehentlich Cloud Volumes ONTAP -Ressourcen aus einer freigegebenen Ressourcengruppe löscht.

Starten Sie ein Cloud Volumes ONTAP -System mit einem Knoten in Azure

Wenn Sie ein Single-Node-Cloud Volumes ONTAP-System in Azure starten möchten, müssen Sie in der Console ein Single-Node-System erstellen.

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Anweisungen.
3. **Wählen Sie einen Standort**: Wählen Sie **Microsoft Azure** und * Cloud Volumes ONTAP Single Node*.
4. Wenn Sie dazu aufgefordert werden, "Erstellen Sie einen Konsolenagenten" .
5. **Details und Anmeldeinformationen**: Ändern Sie optional die Azure-Anmeldeinformationen und das Abonnement, geben Sie einen Clusternamen an, fügen Sie bei Bedarf Tags hinzu und geben Sie dann die Anmeldeinformationen an.

   In der folgenden Tabelle werden die Felder beschrieben, für die Sie möglicherweise Anleitungen benötigen:

Feld	Beschreibung
Systemname	Die Konsole verwendet den Systemnamen, um sowohl das Cloud Volumes ONTAP -System als auch die virtuelle Azure-Maschine zu benennen. Wenn Sie diese Option auswählen, wird der Name auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet.

Feld	Beschreibung
Ressourcengruppen-Tags	Tags sind Metadaten für Ihre Azure-Ressourcen. Wenn Sie in dieses Feld Tags eingeben, fügt die Konsole sie der Ressourcengruppe hinzu, die mit dem Cloud Volumes ONTAP -System verknüpft ist. Sie können beim Erstellen eines Systems bis zu vier Tags über die Benutzeroberfläche hinzufügen und nach der Erstellung weitere hinzufügen. Beachten Sie, dass die API Sie beim Erstellen eines Systems nicht auf vier Tags beschränkt. Informationen zu Tags finden Sie unter "Microsoft Azure-Dokumentation: Verwenden von Tags zum Organisieren Ihrer Azure-Ressourcen" Die
Benutzername und Passwort	Dies sind die Anmeldeinformationen für das Cloud Volumes ONTAP Clusteradministratorkonto. Sie können diese Anmeldeinformationen verwenden, um über ONTAP System Manager oder die ONTAP CLI eine Verbindung zu Cloud Volumes ONTAP herzustellen. Behalten Sie den Standardbenutzernamen *admin* bei oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.
Anmeldeinformationen bearbeiten	Sie können für die Verwendung mit diesem Cloud Volumes ONTAP -System andere Azure-Anmeldeinformationen und ein anderes Azure-Abonnement auswählen. Sie müssen dem ausgewählten Azure-Abonnement ein Azure Marketplace-Abonnement zuordnen, um ein Cloud Volumes ONTAP System mit nutzungsbasierter Bezahlung bereitzustellen. "Erfahren Sie, wie Sie Anmeldeinformationen hinzufügen" .

6. **Dienste**: Aktivieren oder deaktivieren Sie die einzelnen Dienste, die Sie mit Cloud Volumes ONTAP verwenden möchten oder nicht.
   - "Erfahren Sie mehr über die NetApp Data Classification"
   - "Erfahren Sie mehr über NetApp Backup and Recovery"

   Wenn Sie WORM und Daten-Tiering nutzen möchten, müssen Sie Backup und Recovery deaktivieren und ein Cloud Volumes ONTAP System mit Version 9.8 oder höher bereitstellen.

7. **Standort**: Wählen Sie eine Region, eine Verfügbarkeitszone, ein VNet und ein Subnetz aus und aktivieren Sie dann das Kontrollkästchen, um die Netzwerkkonnektivität zwischen dem Konsolenagenten und dem Zielstandort zu bestätigen.

   Für Regionen in China werden Einzelknotenbereitstellungen nur in Cloud Volumes ONTAP 9.12.1 GA und 9.13.0 GA unterstützt. Sie können diese Versionen auf neuere Patches und Releases von Cloud Volumes ONTAP aktualisieren, wie"in Azure unterstützt" . Wenn Sie neuere Versionen von Cloud Volumes ONTAP in chinesischen Regionen bereitstellen möchten, wenden Sie sich an den NetApp Support. In den Regionen Chinas werden nur direkt von NetApp erworbene Lizenzen unterstützt, Marktplatz-Abonnements sind nicht verfügbar.

8. **Konnektivität**: Wählen Sie eine neue oder vorhandene Ressourcengruppe und entscheiden Sie dann, ob Sie die vordefinierte Sicherheitsgruppe oder Ihre eigene verwenden möchten.

   In der folgenden Tabelle werden die Felder beschrieben, für die Sie möglicherweise Anleitungen benötigen:

Feld	Beschreibung
Ressourcengruppe	Erstellen Sie eine neue Ressourcengruppe für Cloud Volumes ONTAP oder verwenden Sie eine vorhandene Ressourcengruppe. Die bewährte Methode besteht darin, eine neue, dedizierte Ressourcengruppe für Cloud Volumes ONTAP zu verwenden. Obwohl es möglich ist , Cloud Volumes ONTAP in einer vorhandenen, gemeinsam genutzten Ressourcengruppe bereitzustellen, wird dies aufgrund des Risikos eines Datenverlusts nicht empfohlen. Weitere Einzelheiten finden Sie in der obigen Warnung. Wenn das von Ihnen verwendete Azure-Konto über die "erforderliche Berechtigungen" , entfernt die Konsole Cloud Volumes ONTAP -Ressourcen aus einer Ressourcengruppe, falls die Bereitstellung fehlschlägt oder gelöscht wird.
Generierte Sicherheitsgruppe	Wenn Sie die Sicherheitsgruppe von der Konsole erstellen lassen, müssen Sie auswählen, wie Sie den Datenverkehr zulassen: • Wenn Sie **Nur ausgewähltes VNet** auswählen, ist die Quelle für eingehenden Datenverkehr der Subnetzbereich des ausgewählten VNet und der Subnetzbereich des VNet, in dem sich der Konsolenagent befindet. Dies ist die empfohlene Option. • Wenn Sie **Alle VNets** auswählen, ist die Quelle für eingehenden Datenverkehr der IP-Bereich 0.0.0.0/0.
Vorhandene verwenden	Wenn Sie eine vorhandene Sicherheitsgruppe auswählen, muss diese die Anforderungen von Cloud Volumes ONTAP erfüllen. "Anzeigen der Standardsicherheitsgruppe" .

9. **Abrechnungsmethoden und NSS-Konto**: Geben Sie an, welche Abrechnungsoption Sie mit diesem System verwenden möchten, und geben Sie dann ein NetApp Support Site-Konto an.
   - "Erfahren Sie mehr über die Lizenzierungsoptionen für Cloud Volumes ONTAP" .
   - "Erfahren Sie, wie Sie die Lizenzierung einrichten" .
10. **Vorkonfigurierte Pakete**: Wählen Sie eines der Pakete aus, um schnell ein Cloud Volumes ONTAP System bereitzustellen, oder klicken Sie auf **Meine eigene Konfiguration erstellen**.

    Wenn Sie sich für eines der Pakete entscheiden, müssen Sie lediglich ein Volumen angeben und anschließend die Konfiguration prüfen und freigeben.
11. **Lizenzierung**: Ändern Sie bei Bedarf die Cloud Volumes ONTAP -Version und wählen Sie einen virtuellen Maschinentyp aus.

    Wenn für die ausgewählte Version ein neuerer Release Candidate, eine allgemeine Verfügbarkeit oder ein Patch-Release verfügbar ist, aktualisiert BlueXP das System beim Erstellen der Arbeitsumgebung auf diese Version. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.16.1 P3 auswählen und 9.16.1 P4 verfügbar ist. Das Update erfolgt nicht von einer Version zur nächsten, beispielsweise von 9.15 auf 9.16.
12. **Abonnieren Sie über den Azure Marketplace**: Diese Seite wird Ihnen angezeigt, wenn die Konsole keine programmgesteuerten Bereitstellungen von Cloud Volumes ONTAP aktivieren konnte. Befolgen Sie die auf dem Bildschirm aufgeführten Schritte. Siehe "Programmatische Bereitstellung von Marketplace-Produkten"

für weitere Informationen.

13. **Zugrunde liegende Speicherressourcen**: Wählen Sie Einstellungen für das anfängliche Aggregat: einen Datenträgertyp, eine Größe für jeden Datenträger und ob die Datenaufteilung auf Blob-Speicher aktiviert werden soll.

    Beachten Sie Folgendes:

    - Wenn der öffentliche Zugriff auf Ihr Speicherkonto innerhalb des VNet deaktiviert ist, können Sie das Daten-Tiering in Ihrem Cloud Volumes ONTAP System nicht aktivieren. Weitere Informationen finden Sie unter"Sicherheitsgruppenregeln" .
    - Der Datenträgertyp ist für das ursprüngliche Volume. Sie können für nachfolgende Volumes einen anderen Datenträgertyp auswählen.
    - Die Datenträgergröße gilt für alle Datenträger im anfänglichen Aggregat und für alle zusätzlichen Aggregate, die die Konsole erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der erweiterten Zuordnungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.

      Hilfe zur Auswahl von Datenträgertyp und -größe finden Sie unter"Dimensionierung Ihres Systems in Azure" .
    - Sie können beim Erstellen oder Bearbeiten eines Volumes eine bestimmte Volume-Tiering-Richtlinie auswählen.
    - Wenn Sie das Daten-Tiering deaktivieren, können Sie es für nachfolgende Aggregate aktivieren.

      "Weitere Informationen zum Daten-Tiering" .

14. **Schreibgeschwindigkeit & WORM**:

    a. Wählen Sie bei Bedarf die Schreibgeschwindigkeit **Normal** oder **Hoch**.

       "Erfahren Sie mehr über die Schreibgeschwindigkeit" .

    b. Aktivieren Sie bei Bedarf den WORM-Speicher (Write Once, Read Many).

       Diese Option ist nur für bestimmte VM-Typen verfügbar. Informationen zu den unterstützten VM-Typen finden Sie unter"Unterstützte Konfigurationen nach Lizenz für HA-Paare" .

       WORM kann nicht aktiviert werden, wenn die Datenschichtung für Cloud Volumes ONTAP Version 9.7 und darunter aktiviert wurde. Das Zurücksetzen oder Downgrade auf Cloud Volumes ONTAP 9.8 ist nach der Aktivierung von WORM und Tiering blockiert.

    "Erfahren Sie mehr über WORM-Speicher" .

    a. Wenn Sie den WORM-Speicher aktivieren, wählen Sie die Aufbewahrungsdauer aus.

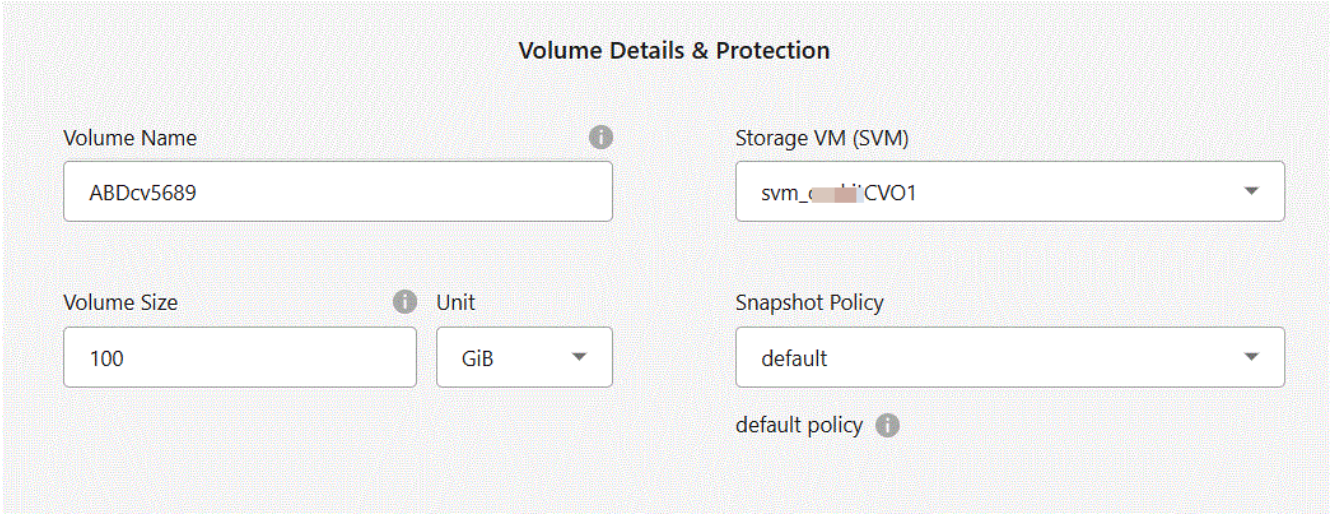
15. **Volume erstellen**: Geben Sie Details für das neue Volume ein oder klicken Sie auf **Überspringen**.

    "Erfahren Sie mehr über unterstützte Clientprotokolle und -versionen" .

    Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Tabelle werden die Felder beschrieben, für die Sie möglicherweise Anleitungen benötigen:

Feld	Beschreibung
Größe	Die maximale Größe, die Sie eingeben können, hängt weitgehend davon ab, ob Sie Thin Provisioning aktivieren. Dadurch können Sie ein Volume erstellen, das größer ist als der ihm aktuell zur Verfügung stehende physische Speicher.
Zugriffskontrolle (nur für NFS)	Eine Exportrichtlinie definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt die Konsole einen Wert ein, der Zugriff auf alle Instanzen im Subnetz gewährt.
Berechtigungen und Benutzer/Gruppen (nur für CIFS)	Mit diesen Feldern können Sie die Zugriffsebene auf eine Freigabe für Benutzer und Gruppen steuern (auch als Zugriffskontrolllisten oder ACLs bezeichnet). Sie können lokale oder Domänen-Windows-Benutzer oder -Gruppen oder UNIX-Benutzer oder -Gruppen angeben. Wenn Sie einen Windows-Domänenbenutzernamen angeben, müssen Sie die Domäne des Benutzers im Format Domäne\Benutzername angeben.
Snapshot-Richtlinie	Eine Snapshot-Kopierrichtlinie gibt die Häufigkeit und Anzahl der automatisch erstellten NetApp Snapshot-Kopien an. Eine NetApp Snapshot-Kopie ist ein zeitpunktbezogenes Dateisystem-Image, das keine Auswirkungen auf die Leistung hat und nur minimalen Speicherplatz benötigt. Sie können die Standardrichtlinie oder keine auswählen. Für vorübergehende Daten können Sie „Keine“ auswählen, beispielsweise „tempdb“ für Microsoft SQL Server.
Erweiterte Optionen (nur für NFS)	Wählen Sie eine NFS-Version für das Volume aus: entweder NFSv3 oder NFSv4.
Initiatorgruppe und IQN (nur für iSCSI)	iSCSI-Speicherziele werden als LUNs (logische Einheiten) bezeichnet und Hosts als Standardblockgeräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Hostknotennamen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. iSCSI-Ziele stellen über Standard-Ethernet-Netzwerkadapter (NICs), TCP-Offload-Engine-Karten (TOE) mit Software-Initiatoren, konvergente Netzwerkadapter (CNAs) oder dedizierte Hostbusadapter (HBAs) eine Verbindung zum Netzwerk her und werden durch iSCSI-qualifizierte Namen (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt die Konsole automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volume erstellt haben, sodass keine Verwaltung erforderlich ist. Nachdem Sie das Volume erstellt haben,"Verwenden Sie den IQN, um von Ihren Hosts aus eine Verbindung zum LUN herzustellen" .

Das folgende Bild zeigt die erste Seite des Assistenten zur Volumeerstellung:



16. **CIFS-Setup**: Wenn Sie das CIFS-Protokoll gewählt haben, richten Sie einen CIFS-Server ein.

Feld	Beschreibung
DNS Primäre und sekundäre IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgelisteten DNS-Server müssen die Service Location Records (SRV) enthalten, die zum Auffinden der Active Directory-LDAP-Server und Domänencontroller für die Domäne erforderlich sind, der der CIFS-Server beitreten wird.
Beitretende Active Directory-Domäne	Der FQDN der Active Directory (AD)-Domäne, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zum Beitritt zur Domäne berechtigt sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
NetBIOS-Name des CIFS-Servers	Ein CIFS-Servername, der in der AD-Domäne eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domäne, die mit dem CIFS-Server verknüpft werden soll. Der Standardwert ist CN=Computers. Um Azure AD Domain Services als AD-Server für Cloud Volumes ONTAP zu konfigurieren, sollten Sie in dieses Feld **OU=AADDC Computers** oder **OU=AADDC Users** eingeben.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure-Dokumentation: Erstellen einer Organisationseinheit (OU) in einer von Azure AD Domain Services verwalteten Domäne"^]
DNS-Domäne	Die DNS-Domäne für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen ist die Domäne dieselbe wie die AD-Domäne.
NTP-Server	Wählen Sie **Active Directory-Domäne verwenden**, um einen NTP-Server mithilfe des Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Weitere Informationen finden Sie im "Dokumentation zur NetApp Console" für Details. Beachten Sie, dass Sie einen NTP-Server nur beim Erstellen eines CIFS-Servers konfigurieren können. Es ist nicht mehr konfigurierbar, nachdem Sie den CIFS-Server erstellt haben.

17. **Nutzungsprofil, Datenträgertyp und Tiering-Richtlinie**: Wählen Sie aus, ob Sie Speichereffizienzfunktionen aktivieren möchten, und ändern Sie bei Bedarf die Volume-Tiering-Richtlinie.

Weitere Informationen finden Sie unter"Grundlegendes zu Volume-Nutzungsprofilen" Und"Übersicht über Data Tiering" .

18. **Überprüfen und genehmigen**: Überprüfen und bestätigen Sie Ihre Auswahl.
    a. Überprüfen Sie die Details zur Konfiguration.
    b. Klicken Sie auf **Weitere Informationen**, um Details zum Support und den Azure-Ressourcen anzuzeigen, die die Konsole erwerben wird.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie auf **Los**.

Ergebnis

Die Konsole stellt das Cloud Volumes ONTAP -System bereit. Sie können den Fortschritt auf der Audit-Seite verfolgen.

Wenn bei der Bereitstellung des Cloud Volumes ONTAP Systems Probleme auftreten, überprüfen Sie die Fehlermeldung. Sie können auch das System auswählen und auf **Umgebung neu erstellen** klicken.

Weitere Hilfe finden Sie unter "NetApp Cloud Volumes ONTAP Unterstützung" .

Ändern Sie nach Abschluss des Bereitstellungsprozesses nicht die systemgenerierten Cloud Volumes ONTAP Konfigurationen im Azure-Portal, insbesondere nicht die System-Tags. Alle an diesen Konfigurationen vorgenommenen Änderungen können zu unerwartetem Verhalten oder Datenverlust führen.

Nach Abschluss

- Wenn Sie eine CIFS-Freigabe bereitgestellt haben, erteilen Sie Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner und stellen Sie sicher, dass diese Benutzer auf die Freigabe zugreifen und eine Datei erstellen können.
- Wenn Sie Kontingente auf Volumes anwenden möchten, verwenden Sie ONTAP System Manager oder die ONTAP CLI.

  Mithilfe von Kontingenten können Sie den Speicherplatz und die Anzahl der von einem Benutzer, einer Gruppe oder einem Qtree verwendeten Dateien beschränken oder verfolgen.

Starten Sie ein Cloud Volumes ONTAP HA-Paar in Azure

Wenn Sie ein Cloud Volumes ONTAP HA-Paar in Azure starten möchten, müssen Sie in der Konsole ein HA-System erstellen.

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Anweisungen.
3. Wenn Sie dazu aufgefordert werden, "Erstellen Sie einen Konsolenagenten" .
4. **Details und Anmeldeinformationen**: Ändern Sie optional die Azure-Anmeldeinformationen und das Abonnement, geben Sie einen Clusternamen an, fügen Sie bei Bedarf Tags hinzu und geben Sie dann die Anmeldeinformationen an.

   In der folgenden Tabelle werden die Felder beschrieben, für die Sie möglicherweise Anleitungen benötigen:

Feld	Beschreibung
Systemname	Die Konsole verwendet den Systemnamen, um sowohl das Cloud Volumes ONTAP -System als auch die virtuelle Azure-Maschine zu benennen. Wenn Sie diese Option auswählen, wird der Name auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet.
Ressourcengruppen-Tags	Tags sind Metadaten für Ihre Azure-Ressourcen. Wenn Sie in dieses Feld Tags eingeben, fügt die Konsole sie der Ressourcengruppe hinzu, die mit dem Cloud Volumes ONTAP -System verknüpft ist. Sie können beim Erstellen eines Systems bis zu vier Tags über die Benutzeroberfläche hinzufügen und nach der Erstellung weitere hinzufügen. Beachten Sie, dass die API Sie beim Erstellen eines Systems nicht auf vier Tags beschränkt. Informationen zu Tags finden Sie unter "Microsoft Azure-Dokumentation: Verwenden von Tags zum Organisieren Ihrer Azure-Ressourcen" Die
Benutzername und Passwort	Dies sind die Anmeldeinformationen für das Cloud Volumes ONTAP Clusteradministratorkonto. Sie können diese Anmeldeinformationen verwenden, um über ONTAP System Manager oder die ONTAP CLI eine Verbindung zu Cloud Volumes ONTAP herzustellen. Behalten Sie den Standardbenutzernamen *admin* bei oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.
Anmeldeinformationen bearbeiten	Sie können für die Verwendung mit diesem Cloud Volumes ONTAP -System andere Azure-Anmeldeinformationen und ein anderes Azure-Abonnement auswählen. Sie müssen dem ausgewählten Azure-Abonnement ein Azure Marketplace-Abonnement zuordnen, um ein Cloud Volumes ONTAP System mit nutzungsbasierter Bezahlung bereitzustellen. "Erfahren Sie, wie Sie Anmeldeinformationen hinzufügen" .

5. **Dienste**: Aktivieren oder deaktivieren Sie die einzelnen Dienste, je nachdem, ob Sie sie mit Cloud Volumes ONTAP verwenden möchten.
   - "Erfahren Sie mehr über die NetApp Data Classification"
   - "Erfahren Sie mehr über NetApp Backup and Recovery"

   Wenn Sie WORM und Daten-Tiering nutzen möchten, müssen Sie Backup und Recovery deaktivieren und ein Cloud Volumes ONTAP System mit Version 9.8 oder höher bereitstellen.

6. **HA-Bereitstellungsmodelle**:
   a. Wählen Sie **Einzelne Verfügbarkeitszone** oder **Mehrere Verfügbarkeitszonen**.
      - Wählen Sie für einzelne Verfügbarkeitszonen eine Azure-Region, eine Verfügbarkeitszone, ein VNet und ein Subnetz aus.

        Ab Cloud Volumes ONTAP 9.15.1 können Sie VM-Instanzen (Virtual Machine) im HA-Modus in einzelnen Verfügbarkeitszonen (AZs) in Azure bereitstellen. Sie müssen eine Zone und eine Region auswählen, die diese Bereitstellung unterstützen. Wenn die Zone oder Region die zonale Bereitstellung nicht unterstützt, wird der vorherige nicht zonale Bereitstellungsmodus für LRS verwendet. Informationen zu den unterstützten Konfigurationen für gemeinsam genutzte verwaltete Datenträger finden Sie unter"HA-Konfiguration einer einzelnen Verfügbarkeitszone mit gemeinsam genutzten verwalteten Datenträgern" .

      - Wählen Sie für mehrere Verfügbarkeitszonen eine Region, ein VNet, ein Subnetz, eine Zone für

Knoten 1 und eine Zone für Knoten 2 aus.

b. Aktivieren Sie das Kontrollkästchen **Ich habe die Netzwerkkonnektivität überprüft…**.

7. **Konnektivität**: Wählen Sie eine neue oder vorhandene Ressourcengruppe und entscheiden Sie dann, ob Sie die vordefinierte Sicherheitsgruppe oder Ihre eigene verwenden möchten.

   In der folgenden Tabelle werden die Felder beschrieben, für die Sie möglicherweise Anleitungen benötigen:

Feld	Beschreibung
Ressourcengruppe	Erstellen Sie eine neue Ressourcengruppe für Cloud Volumes ONTAP oder verwenden Sie eine vorhandene Ressourcengruppe. Die bewährte Methode besteht darin, eine neue, dedizierte Ressourcengruppe für Cloud Volumes ONTAP zu verwenden. Obwohl es möglich ist , Cloud Volumes ONTAP in einer vorhandenen, gemeinsam genutzten Ressourcengruppe bereitzustellen, wird dies aufgrund des Risikos eines Datenverlusts nicht empfohlen. Weitere Einzelheiten finden Sie in der obigen Warnung. Sie müssen für jedes Cloud Volumes ONTAP HA-Paar, das Sie in Azure bereitstellen, eine dedizierte Ressourcengruppe verwenden. In einer Ressourcengruppe wird nur ein HA-Paar unterstützt. Bei der Konsole treten Verbindungsprobleme auf, wenn Sie versuchen, ein zweites Cloud Volumes ONTAP HA-Paar in einer Azure-Ressourcengruppe bereitzustellen. Wenn das von Ihnen verwendete Azure-Konto über die "erforderliche Berechtigungen" , entfernt die Konsole Cloud Volumes ONTAP -Ressourcen aus einer Ressourcengruppe, falls die Bereitstellung fehlschlägt oder gelöscht wird.
Generierte Sicherheitsgruppe	Wenn Sie die Sicherheitsgruppe von der Konsole erstellen lassen, müssen Sie auswählen, wie Sie den Datenverkehr zulassen: • Wenn Sie **Nur ausgewähltes VNet** auswählen, ist die Quelle für eingehenden Datenverkehr der Subnetzbereich des ausgewählten VNet und der Subnetzbereich des VNet, in dem sich der Konsolenagent befindet. Dies ist die empfohlene Option. • Wenn Sie **Alle VNets** auswählen, ist die Quelle für eingehenden Datenverkehr der IP-Bereich 0.0.0.0/0.
Vorhandene verwenden	Wenn Sie eine vorhandene Sicherheitsgruppe auswählen, muss diese die Anforderungen von Cloud Volumes ONTAP erfüllen. "Anzeigen der Standardsicherheitsgruppe" .

8. **Abrechnungsmethoden und NSS-Konto**: Geben Sie an, welche Abrechnungsoption Sie mit diesem System verwenden möchten, und geben Sie dann ein NetApp Support Site-Konto an.
   - "Erfahren Sie mehr über die Lizenzierungsoptionen für Cloud Volumes ONTAP" .
   - "Erfahren Sie, wie Sie die Lizenzierung einrichten" .
9. **Vorkonfigurierte Pakete**: Wählen Sie eines der Pakete aus, um schnell ein Cloud Volumes ONTAP System bereitzustellen, oder klicken Sie auf **Konfiguration ändern**.

   Wenn Sie sich für eines der Pakete entscheiden, müssen Sie lediglich ein Volumen angeben und

anschließend die Konfiguration prüfen und freigeben.

10. **Lizenzierung**: Ändern Sie die Cloud Volumes ONTAP -Version nach Bedarf und wählen Sie einen virtuellen Maschinentyp aus.

    Wenn für die ausgewählte Version ein neuerer Release Candidate, eine allgemeine Verfügbarkeit oder ein Patch-Release verfügbar ist, aktualisiert die Konsole das System beim Erstellen auf diese Version. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.13.1 auswählen und 9.13.1 P4 verfügbar ist. Das Update erfolgt nicht von einer Version zur nächsten, beispielsweise von 9.13 auf 9.14.

11. **Abonnieren Sie über den Azure Marketplace**: Befolgen Sie die Schritte, wenn die Konsole keine programmgesteuerten Bereitstellungen von Cloud Volumes ONTAP aktivieren konnte.
12. **Zugrunde liegende Speicherressourcen**: Wählen Sie Einstellungen für das anfängliche Aggregat: einen Datenträgertyp, eine Größe für jeden Datenträger und ob die Datenaufteilung auf Blob-Speicher aktiviert werden soll.

    Beachten Sie Folgendes:

    - Die Datenträgergröße gilt für alle Datenträger im anfänglichen Aggregat und für alle zusätzlichen Aggregate, die die Konsole erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der erweiterten Zuordnungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.

      Hilfe zur Auswahl einer Festplattengröße finden Sie unter"Dimensionieren Sie Ihr System in Azure" .

    - Wenn der öffentliche Zugriff auf Ihr Speicherkonto innerhalb des VNet deaktiviert ist, können Sie das Daten-Tiering in Ihrem Cloud Volumes ONTAP System nicht aktivieren. Weitere Informationen finden Sie unter"Sicherheitsgruppenregeln" .
    - Sie können beim Erstellen oder Bearbeiten eines Volumes eine bestimmte Volume-Tiering-Richtlinie auswählen.
    - Wenn Sie das Daten-Tiering deaktivieren, können Sie es für nachfolgende Aggregate aktivieren.

      "Weitere Informationen zum Daten-Tiering" .

    - Ab Cloud Volumes ONTAP 9.15.0P1 werden Azure-Seitenblobs für neue Bereitstellungen mit Hochverfügbarkeitspaaren nicht mehr unterstützt. Wenn Sie derzeit Azure-Seitenblobs in vorhandenen Bereitstellungen mit Hochverfügbarkeitspaaren verwenden, können Sie in den VMs der Edsv4- und Edsv5-Serie zu neueren VM-Instanztypen migrieren.

      "Erfahren Sie mehr über unterstützte Konfigurationen in Azure" .

13. **Schreibgeschwindigkeit & WORM**:

    a. Wählen Sie bei Bedarf die Schreibgeschwindigkeit **Normal** oder **Hoch**.

       "Erfahren Sie mehr über die Schreibgeschwindigkeit" .

    b. Aktivieren Sie bei Bedarf den WORM-Speicher (Write Once, Read Many).

       Diese Option ist nur für bestimmte VM-Typen verfügbar. Informationen zu den unterstützten VM-Typen finden Sie unter"Unterstützte Konfigurationen nach Lizenz für HA-Paare" .

       WORM kann nicht aktiviert werden, wenn die Datenschichtung für Cloud Volumes ONTAP Version 9.7

und darunter aktiviert wurde. Das Zurücksetzen oder Downgrade auf Cloud Volumes ONTAP 9.8 ist nach der Aktivierung von WORM und Tiering blockiert.

"Erfahren Sie mehr über WORM-Speicher" .

a. Wenn Sie den WORM-Speicher aktivieren, wählen Sie die Aufbewahrungsdauer aus.

14. **Sichere Kommunikation mit Speicher und WORM**: Wählen Sie, ob eine HTTPS-Verbindung zu Azure-Speicherkonten aktiviert werden soll, und aktivieren Sie bei Bedarf den WORM-Speicher (Write Once, Read Many).

    Die HTTPS-Verbindung besteht von einem Cloud Volumes ONTAP 9.7 HA-Paar zu Azure Page Blob Storage-Konten. Beachten Sie, dass das Aktivieren dieser Option die Schreibleistung beeinträchtigen kann. Sie können die Einstellung nicht mehr ändern, nachdem Sie das System erstellt haben.

    "Erfahren Sie mehr über WORM-Speicher" .

    WORM kann nicht aktiviert werden, wenn die Datenschichtung aktiviert wurde.

    "Erfahren Sie mehr über WORM-Speicher" .

15. **Volume erstellen**: Geben Sie Details für das neue Volume ein oder klicken Sie auf **Überspringen**.

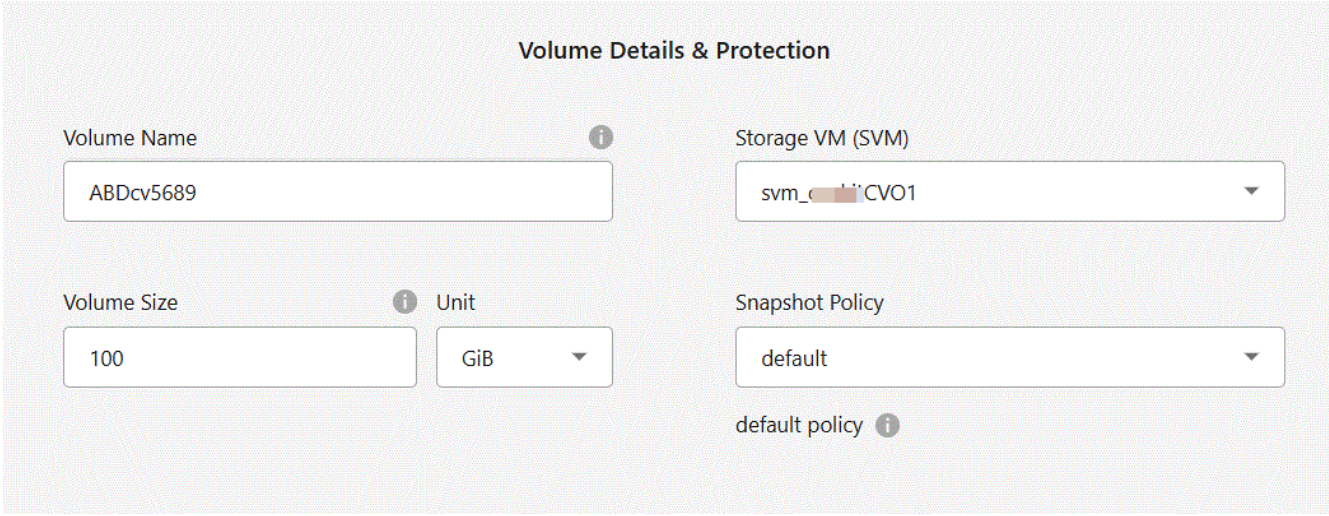
    "Erfahren Sie mehr über unterstützte Clientprotokolle und -versionen" .

    Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Tabelle werden die Felder beschrieben, für die Sie möglicherweise Anleitungen benötigen:

Feld	Beschreibung
Größe	Die maximale Größe, die Sie eingeben können, hängt weitgehend davon ab, ob Sie Thin Provisioning aktivieren. Dadurch können Sie ein Volume erstellen, das größer ist als der ihm aktuell zur Verfügung stehende physische Speicher.
Zugriffskontrolle (nur für NFS)	Eine Exportrichtlinie definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt die Konsole einen Wert ein, der Zugriff auf alle Instanzen im Subnetz gewährt.
Berechtigungen und Benutzer/Gruppen (nur für CIFS)	Mit diesen Feldern können Sie die Zugriffsebene auf eine Freigabe für Benutzer und Gruppen steuern (auch als Zugriffskontrolllisten oder ACLs bezeichnet). Sie können lokale oder Domänen-Windows-Benutzer oder -Gruppen oder UNIX-Benutzer oder -Gruppen angeben. Wenn Sie einen Windows-Domänenbenutzernamen angeben, müssen Sie die Domäne des Benutzers im Format Domäne\Benutzername angeben.
Snapshot-Richtlinie	Eine Snapshot-Kopierrichtlinie gibt die Häufigkeit und Anzahl der automatisch erstellten NetApp Snapshot-Kopien an. Eine NetApp Snapshot-Kopie ist ein zeitpunktbezogenes Dateisystem-Image, das keine Auswirkungen auf die Leistung hat und nur minimalen Speicherplatz benötigt. Sie können die Standardrichtlinie oder keine auswählen. Für vorübergehende Daten können Sie „Keine“ auswählen, beispielsweise „tempdb“ für Microsoft SQL Server.
Erweiterte Optionen (nur für NFS)	Wählen Sie eine NFS-Version für das Volume aus: entweder NFSv3 oder NFSv4.

Feld	Beschreibung
Initiatorgruppe und IQN (nur für iSCSI)	iSCSI-Speicherziele werden als LUNs (logische Einheiten) bezeichnet und Hosts als Standardblockgeräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Hostknotennamen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. iSCSI-Ziele stellen über Standard-Ethernet-Netzwerkadapter (NICs), TCP-Offload-Engine-Karten (TOE) mit Software-Initiatoren, konvergente Netzwerkadapter (CNAs) oder dedizierte Hostbusadapter (HBAs) eine Verbindung zum Netzwerk her und werden durch iSCSI-qualifizierte Namen (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt die Konsole automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volume erstellt haben, sodass keine Verwaltung erforderlich ist. Nachdem Sie das Volume erstellt haben,"Verwenden Sie den IQN, um von Ihren Hosts aus eine Verbindung zum LUN herzustellen" .

Das folgende Bild zeigt die erste Seite des Assistenten zur Volumeerstellung:



16. **CIFS-Setup**: Wenn Sie das CIFS-Protokoll gewählt haben, richten Sie einen CIFS-Server ein.

Feld	Beschreibung
DNS Primäre und sekundäre IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgelisteten DNS-Server müssen die Service Location Records (SRV) enthalten, die zum Auffinden der Active Directory-LDAP-Server und Domänencontroller für die Domäne erforderlich sind, der der CIFS-Server beitreten wird.
Beitretende Active Directory-Domäne	Der FQDN der Active Directory (AD)-Domäne, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zum Beitritt zur Domäne berechtigt sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
NetBIOS-Name des CIFS-Servers	Ein CIFS-Servername, der in der AD-Domäne eindeutig ist.

Feld	Beschreibung
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domäne, die mit dem CIFS-Server verknüpft werden soll. Der Standardwert ist CN=Computers. Um Azure AD Domain Services als AD-Server für Cloud Volumes ONTAP zu konfigurieren, sollten Sie in dieses Feld **OU=AADDC Computers** oder **OU=AADDC Users** eingeben.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure-Dokumentation: Erstellen einer Organisationseinheit (OU) in einer von Azure AD Domain Services verwalteten Domäne"^]
DNS-Domäne	Die DNS-Domäne für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen ist die Domäne dieselbe wie die AD-Domäne.
NTP-Server	Wählen Sie **Active Directory-Domäne verwenden**, um einen NTP-Server mithilfe des Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Weitere Informationen finden Sie im "Dokumentation zur NetApp Console" für Details. Beachten Sie, dass Sie einen NTP-Server nur beim Erstellen eines CIFS-Servers konfigurieren können. Es ist nicht mehr konfigurierbar, nachdem Sie den CIFS-Server erstellt haben.

17. **Nutzungsprofil, Datenträgertyp und Tiering-Richtlinie**: Wählen Sie aus, ob Sie Speichereffizienzfunktionen aktivieren möchten, und ändern Sie bei Bedarf die Volume-Tiering-Richtlinie.

    Weitere Informationen finden Sie unter"Auswählen eines Volume-Nutzungsprofils" ,"Übersicht über Data Tiering" , Und "KB: Welche Inline-Speichereffizienzfunktionen werden mit CVO unterstützt?"

18. **Überprüfen und genehmigen**: Überprüfen und bestätigen Sie Ihre Auswahl.
    a. Überprüfen Sie die Details zur Konfiguration.
    b. Klicken Sie auf **Weitere Informationen**, um Details zum Support und den Azure-Ressourcen anzuzeigen, die die Konsole erwerben wird.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie auf **Los**.

Ergebnis

Die Konsole stellt das Cloud Volumes ONTAP -System bereit. Sie können den Fortschritt auf der Audit-Seite verfolgen.

Wenn bei der Bereitstellung des Cloud Volumes ONTAP Systems Probleme auftreten, überprüfen Sie die Fehlermeldung. Sie können auch das System auswählen und auf **Umgebung neu erstellen** klicken.

Weitere Hilfe finden Sie unter "NetApp Cloud Volumes ONTAP Unterstützung" .

Nach Abschluss

- Wenn Sie eine CIFS-Freigabe bereitgestellt haben, erteilen Sie Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner und stellen Sie sicher, dass diese Benutzer auf die Freigabe zugreifen und eine Datei erstellen können.
- Wenn Sie Kontingente auf Volumes anwenden möchten, verwenden Sie ONTAP System Manager oder die ONTAP CLI.

  Mithilfe von Kontingenten können Sie den Speicherplatz und die Anzahl der von einem Benutzer, einer Gruppe oder einem Qtree verwendeten Dateien beschränken oder verfolgen.

Ändern Sie nach Abschluss des Bereitstellungsprozesses nicht die systemgenerierten Cloud Volumes ONTAP Konfigurationen im Azure-Portal, insbesondere nicht die System-Tags. Alle an diesen Konfigurationen vorgenommenen Änderungen können zu unerwartetem Verhalten oder Datenverlust führen.

Weiterführende Links

*"Planen Ihrer Cloud Volumes ONTAP -Konfiguration in Azure" *"Stellen Sie Cloud Volumes ONTAP in Azure über den Azure Marketplace bereit"

Überprüfen des Azure-Plattformimages

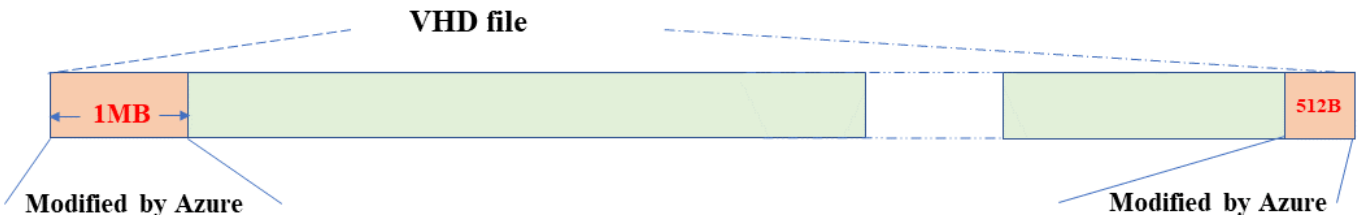
Azure Marketplace-Imageüberprüfung für Cloud Volumes ONTAP

Die Azure-Image-Verifizierung entspricht den erweiterten Sicherheitsanforderungen von NetApp . Das Überprüfen einer Bilddatei ist ein unkomplizierter Vorgang. Allerdings erfordert die Überprüfung der Azure-Image-Signatur besondere Überlegungen für die Azure-VHD-Image-Datei, da diese im Azure Marketplace geändert wird.

Die Azure-Image-Verifizierung wird auf Cloud Volumes ONTAP 9.15.0 und höher unterstützt.

Azures Änderung veröffentlichter VHD-Dateien

Die 1 MB (1048576 Bytes) am Anfang und 512 Bytes am Ende der VHD-Datei werden von Azure geändert. NetApp signiert die verbleibende VHD-Datei.



Im Beispiel ist die VHD-Datei 10 GB groß. Der von NetApp signierte Teil ist grün markiert (10 GB – 1 MB – 512 Byte).

Weiterführende Links

- "Seitenfehler-Blog: So signieren und verifizieren Sie mit OpenSSL"
- "Verwenden Sie das Azure Marketplace-Image, um ein VM-Image für Ihre Azure Stack Edge Pro-GPU zu erstellen | Microsoft Learn"
- "Exportieren/Kopieren eines verwalteten Datenträgers in ein Speicherkonto mithilfe der Azure CLI | Microsoft Learn"
- "Schnellstart für Azure Cloud Shell – Bash | Microsoft Learn"
- "So installieren Sie die Azure CLI | Microsoft Learn"
- "az storage blob copy | Microsoft Learn"
- "Mit Azure CLI Sign in – Anmeldung und Authentifizierung | Microsoft Learn"

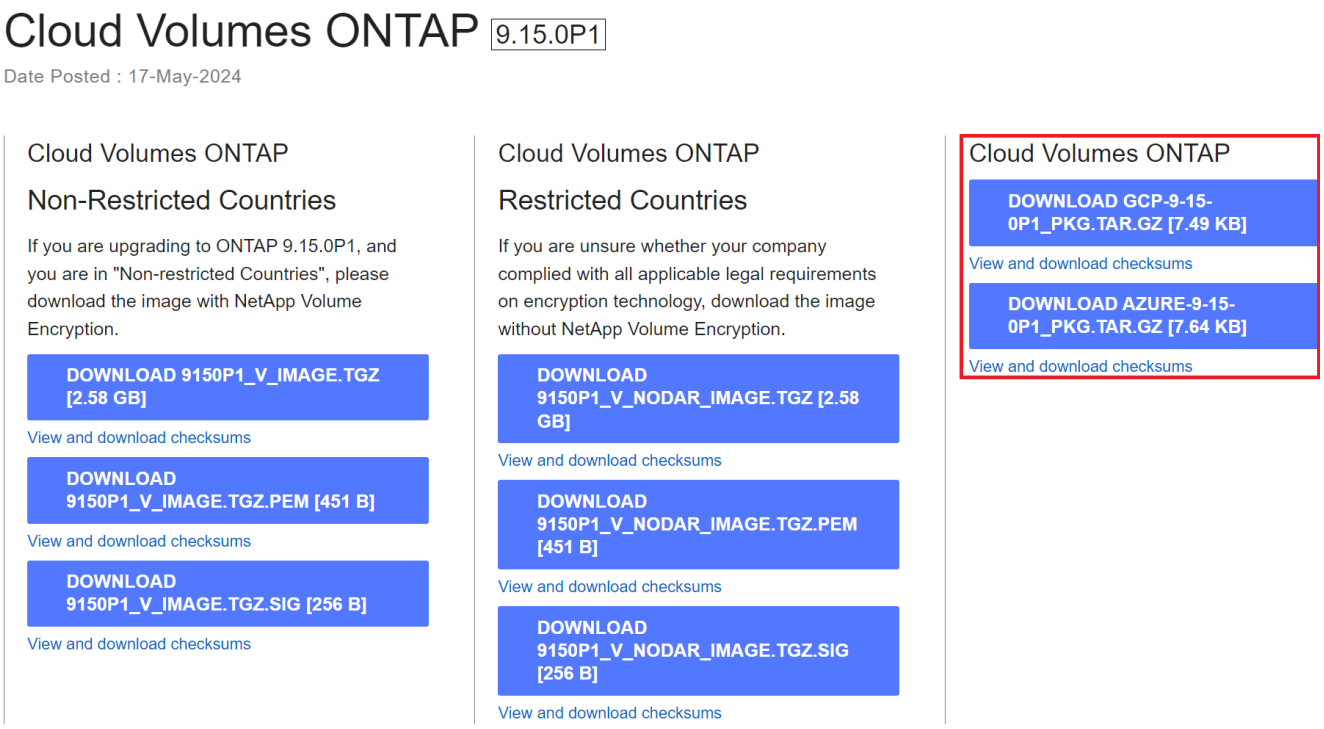
Laden Sie die Azure-Image-Datei für Cloud Volumes ONTAP herunter

Sie können die Azure-Imagedatei von der "NetApp Support Site" .

Die Datei *tar.gz* enthält die für die Bildsignaturüberprüfung erforderlichen Dateien. Zusammen mit der *tar.gz* -Datei sollten Sie auch die *Prüfsummen*-Datei für das Image herunterladen. Die Prüfsummendatei enthält die `md5` Und `sha256` Prüfsummen der *tar.gz*-Datei.

Schritte

1. Gehen Sie zum "Cloud Volumes ONTAP Produktseite auf der NetApp Support-Site" und laden Sie die erforderliche Softwareversion aus dem Bereich **Downloads** herunter.
2. Klicken Sie auf der Downloadseite von Cloud Volumes ONTAP auf die herunterladbare Datei für das Azure-Image und laden Sie die Datei *tar.gz* herunter.



3. Führen Sie unter Linux Folgendes aus: `md5sum AZURE-<version>_PKG.TAR.GZ` .

   Führen Sie unter macOS Folgendes aus: `sha256sum AZURE-<version>_PKG.TAR.GZ` .

4. Überprüfen Sie, ob die `md5sum` Und `sha256sum` Die Werte stimmen mit denen im heruntergeladenen Azure-Image überein.
5. Extrahieren Sie unter Linux und macOS die Datei *tar.gz* mit dem `tar -xzf` Befehl.

   Die extrahierte *tar.gz*-Datei enthält die Digest-Datei (*.sig*), die Datei mit dem öffentlichen Schlüsselzertifikat (*.pem*) und die Datei mit dem Kettenzertifikat (*.pem*).

   Beispielausgabe nach dem Extrahieren der tar.gz-Datei:

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp  384 May  13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May  13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 version_readme
```

Exportieren Sie VHD-Images für Cloud Volumes ONTAP aus dem Azure Marketplace

Sobald das VHD-Image in der Azure-Cloud veröffentlicht ist, wird es nicht mehr von NetApp verwaltet. Stattdessen wird das veröffentlichte Image auf dem Azure-Marktplatz platziert. Wenn das Image bereitgestellt und im Azure Marketplace veröffentlicht wird, ändert Azure 1 MB am Anfang und 512 Byte am Ende der VHD. Um die Signatur der VHD-Datei zu überprüfen, müssen Sie das von Azure geänderte VHD-Image aus dem Azure Marketplace exportieren.

Bevor Sie beginnen

Stellen Sie sicher, dass die Azure CLI auf Ihrem System installiert ist oder die Azure Cloud Shell über das Azure-Portal verfügbar ist. Weitere Informationen zur Installation der Azure CLI finden Sie im "Microsoft-Dokumentation: So installieren Sie die Azure CLI" .

Schritte

1. Ordnen Sie die Cloud Volumes ONTAP -Version auf Ihrem System der Image-Version des Azure Marketplace zu, indem Sie den Inhalt der Datei *version_readme* verwenden. Die Cloud Volumes ONTAP -Version wird repräsentiert durch `buildname` und die Azure Marketplace-Imageversion wird dargestellt durch `version` in den Versionszuordnungen.

   Im folgenden Beispiel wird die Cloud Volumes ONTAP -Version `9.15.0P1` ist der Azure Marketplace-Imageversion zugeordnet `9150.01000024.05090105` . Diese Azure Marketplace-Imageversion wird später zum Festlegen der Image-URN verwendet.

   ```
   [
    "buildname": "9.15.0P1",
       "publisher": "netapp",
        "version": "9150.01000024.05090105"

   ]
   ```

2. Identifizieren Sie die Region, in der Sie die VMs erstellen möchten. Der Regionsname wird als Wert für die `locName` Variable beim Festlegen der URN des Marktplatzbilds. Führen Sie diesen Befehl aus, um die verfügbaren Regionen aufzulisten:

   ```
   az account list-locations -o table
   ```

In dieser Tabelle erscheint der Regionsname in der `Name` Feld.

```
$ az account list-locations -o table
DisplayName               Name                 RegionalDisplayName
------------------------  -------------------
-------------------------------------
East US                   eastus               (US) East US
East US 2                 eastus2              (US) East US 2
South Central US          southcentralus       (US) South Central US
...
```

3. Überprüfen Sie die SKU-Namen für die entsprechenden Cloud Volumes ONTAP Versionen und VM-Bereitstellungstypen in der folgenden Tabelle. Der SKU-Name wird als Wert für die `skuName` Variable beim Festlegen der URN des Marktplatzbilds.

   Beispielsweise sollten alle Einzelknotenbereitstellungen mit Cloud Volumes ONTAP 9.15.0 `ontap_cloud_byol` als SKU-Name.

* Cloud Volumes ONTAP Version*	**VM-Bereitstellung durch**	**SKU-Name**
9.17.1 und höher	Der Azure Marketplace	ontap_cloud_direct_gen2
9.17.1 und höher	Die NetApp Console	ontap_cloud_gen2
9.16.1	Der Azure Marketplace	ontap_cloud_direct
9.16.1	Die Konsole	ontap_cloud
9.15.1	Die Konsole	ontap_cloud
9.15.0	Die Konsole, Einzelknotenbereitstellungen	ontap_cloud_byol
9.15.0	Die Konsole, Hochverfügbarkeitsbereitstellungen (HA)	ontap_cloud_byol_ha

4. Nachdem Sie die ONTAP -Version und das Azure Marketplace-Image zugeordnet haben, exportieren Sie die VHD-Datei mithilfe der Azure Cloud Shell oder der Azure CLI aus dem Azure Marketplace.

Exportieren einer VHD-Datei mit Azure Cloud Shell unter Linux

Exportieren Sie aus Azure Cloud Shell das Marketplace-Image in die VHD-Datei (z. B. *9150.01000024.05090105.vhd*) und laden Sie es auf Ihr lokales Linux-System herunter. Führen Sie diese Schritte aus, um das VHD-Image vom Azure Marketplace abzurufen.

Schritte

1. Legen Sie die URN und andere Parameter des Marktplatzbilds fest. Das URN-Format ist `<publisher>:<offer>:<sku>:<version>` . Optional können Sie NetApp Marketplace-Images auflisten, um die richtige Image-Version zu bestätigen.

```
PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName $pubName
-Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...
```

2. Erstellen Sie einen neuen verwalteten Datenträger aus dem Marketplace-Image mit der passenden Imageversion:

```
PS /home/user1> $diskName = "9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = "fnf1"
PS /home/user1> az disk create -g $diskRG -n $diskName --image-reference
$urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds 3600
--access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-Json)[0].accessSas
```

3. Exportieren Sie die VHD-Datei vom verwalteten Datenträger in Azure Storage. Erstellen Sie einen Container mit der entsprechenden Zugriffsebene. In diesem Beispiel haben wir einen Container namens `vm-images` mit `Container` Zugriffsebene. Rufen Sie den Zugriffsschlüssel für das Speicherkonto aus dem Azure-Portal ab: **Speicherkonten > *Beispielname* > Zugriffsschlüssel > *Schlüssel1* > *Schlüssel* > Anzeigen > <*Kopie*>**

```
PS /home/user1> $storageAccountName = “examplesaname”
PS /home/user1> $containerName = “vm-images”
PS /home/user1> $storageAccountKey = "<replace with the above access
key>"
PS /home/user1> $destBlobName = “9150.01000024.05090105.vhd”
PS /home/user1> $destContext = New-AzureStorageContext
-StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri $diskAccessSAS
-DestContainer $containerName -DestContext $destContext -DestBlob
$destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState –Container $containerName
–Context $destContext -Blob $destBlobName
```

4. Laden Sie das generierte Image auf Ihr Linux-System herunter. Verwenden Sie die `wget` Befehl zum Herunterladen der VHD-Datei:

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

Die URL folgt einem Standardformat. Zur Automatisierung können Sie die URL-Zeichenfolge wie unten gezeigt ableiten. Alternativ können Sie die Azure CLI verwenden `az` Befehl, um die URL abzurufen. Beispiel-URL:https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

5. Bereinigen des verwalteten Datenträgers

```
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName
$diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

Exportieren einer VHD-Datei mit der Azure CLI unter Linux

Exportieren Sie das Marktplatz-Image mithilfe der Azure CLI von einem lokalen Linux-System in eine VHD-Datei.

Schritte

1. Melden Sie sich bei der Azure CLI an und listen Sie Marketplace-Images auf:

```
% az login --use-device-code
```

2. Um sich anzumelden, öffnen Sie die Seite in einem Webbrowser https://microsoft.com/devicelogin und geben Sie den Authentifizierungscode ein.

```
% az vm image list --all --publisher netapp --offer netapp-ontap-cloud
--sku ontap_cloud_byol
...
{
"architecture": "x64",
"offer": "netapp-ontap-cloud",
"publisher": "netapp",
"sku": "ontap_cloud_byol",
"urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
"version": "9150.01000024.05090105"
},
...
```

3. Erstellen Sie einen neuen verwalteten Datenträger aus dem Marketplace-Image mit der passenden Image-Version.

```
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level Read
--name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
```

Um den Prozess zu automatisieren, muss das SAS aus der Standardausgabe extrahiert werden. Anleitungen finden Sie in den entsprechenden Dokumenten.

4. Exportieren Sie die VHD-Datei vom verwalteten Datenträger.

   a. Erstellen Sie einen Container mit der entsprechenden Zugriffsebene. In diesem Beispiel wird ein Container mit dem Namen `vm-images` mit `Container` Zugriffsebene verwendet wird.

   b. Rufen Sie den Zugriffsschlüssel für das Speicherkonto aus dem Azure-Portal ab: **Speicherkonten > *Beispielname* > Zugriffsschlüssel > *Schlüssel1* > *Schlüssel* > Anzeigen > <*Kopie*>**

      Sie können auch die `az` Befehl für diesen Schritt.

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS --destination
-container $containerName --account-name $storageAccountName --account
-key $storageAccountKey --destination-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

5. Überprüfen Sie den Status der Blobkopie.

```
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
    "copy": {
      "completionTime": null,
      "destinationSnapshot": null,
      "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxx",
      "incrementalCopy": null,
      "progress": "10737418752/10737418752",
      "source": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
    },
....
```

6. Laden Sie das generierte Image auf Ihren Linux-Server herunter.

```
wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>
```

Die URL folgt einem Standardformat. Zur Automatisierung können Sie die URL-Zeichenfolge wie unten gezeigt ableiten. Alternativ können Sie die Azure CLI verwenden `az` Befehl, um die URL abzurufen. Beispiel-URL:https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

7. Bereinigen des verwalteten Datenträgers

```
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

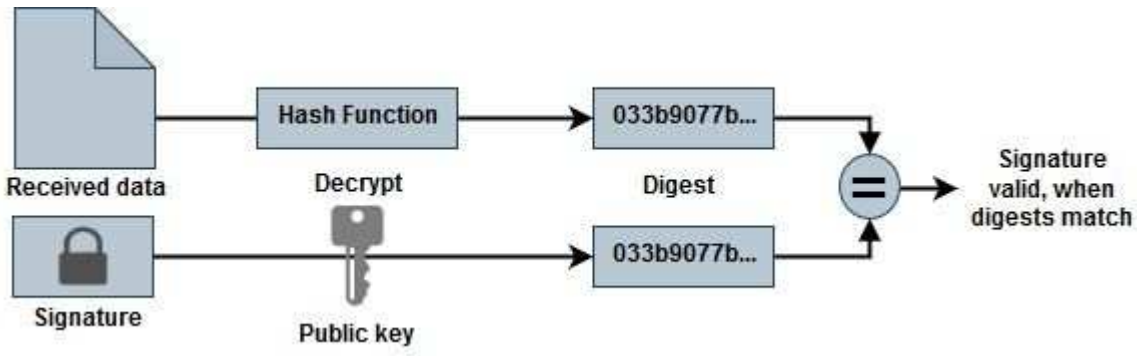
Dateisignatur überprüfen

Azure Marketplace-Imagesignaturüberprüfung für Cloud Volumes ONTAP

Der Azure-Imageüberprüfungsprozess generiert eine Digest-Datei aus der VHD-Datei, indem er am Anfang 1 MB und am Ende 512 Byte entfernt und dann eine Hash-Funktion anwendet. Um dem Signaturverfahren zu entsprechen, wird *sha256* zum Hashing verwendet.

Zusammenfassung des Workflows zur Dateisignaturüberprüfung

Nachfolgend finden Sie eine Übersicht über den Workflow-Prozess zur Dateisignaturüberprüfung.



- Herunterladen des Azure-Images von der "NetApp Support Site" und Extrahieren der Digest-Datei (.sig), der Public-Key-Zertifikatdatei (.pem) und der Kettenzertifikatdatei (.pem). Weitere Informationen finden Sie unter "Herunterladen der Azure-Image-Digest-Datei" für weitere Informationen.
- Überprüfung der Vertrauenskette.
- Extrahieren des öffentlichen Schlüssels (.pub) aus dem öffentlichen Schlüsselzertifikat (.pem).
- Entschlüsseln der Digest-Datei mithilfe des extrahierten öffentlichen Schlüssels.
- Vergleichen Sie das Ergebnis mit einem neu generierten Digest einer temporären Datei, die aus der Bilddatei erstellt wurde, nachdem 1 MB am Anfang und 512 Byte am Ende entfernt wurden. Dieser Schritt wird mithilfe des OpenSSL-Befehlszeilentools ausgeführt. Das OpenSSL-CLI-Tool zeigt eine entsprechende Meldung an, wenn die Zuordnung der Dateien erfolgreich war oder fehlgeschlagen ist.

```
openssl dgst -verify <public_key> -keyform <form> <hash_function>
-signature <digest_file> -binary <temporary_file>
```

Überprüfen der Azure Marketplace-Imagesignatur für Cloud Volumes ONTAP unter Linux

Die Überprüfung der Signatur einer exportierten VHD-Datei unter Linux umfasst die Validierung der Vertrauenskette, die Bearbeitung der Datei und die Überprüfung der Signatur.

Schritte

1. Laden Sie die Azure-Imagedatei von der "NetApp Support Site" und extrahieren Sie die Digest-Datei (.sig), die Public-Key-Zertifikatdatei (.pem) und die Kettenzertifikatdatei (.pem).

   Siehe "Herunterladen der Azure-Image-Digest-Datei" für weitere Informationen.

2. Überprüfen Sie die Vertrauenskette.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Entfernen Sie 1 MB (1.048.576 Bytes) am Anfang und 512 Bytes am Ende der VHD-Datei. Bei der Verwendung `tail` , Die `-c +K` Option generiert Bytes aus dem K-ten Byte der Datei. Daher geht es 1048577 an `tail -c` .

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. Verwenden Sie OpenSSL, um den öffentlichen Schlüssel aus dem Zertifikat zu extrahieren und die extrahierte Datei (sign.tmp) mit der Signaturdatei und dem öffentlichen Schlüssel zu überprüfen.

   Die Eingabeaufforderung zeigt Meldungen an, die den Erfolg oder Misserfolg der Überprüfung basierend auf deren Erfolg anzeigen.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Räumen Sie den Arbeitsbereich auf.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Überprüfen der Azure Marketplace-Imagesignatur für Cloud Volumes ONTAP unter macOS

Die Überprüfung der Signatur einer exportierten VHD-Datei unter Linux umfasst die Validierung der Vertrauenskette, die Bearbeitung der Datei und die Überprüfung der Signatur.

Schritte

1. Laden Sie die Azure-Imagedatei von der "NetApp Support Site" und extrahieren Sie die Digest-Datei (.sig), die Public-Key-Zertifikatdatei (.pem) und die Kettenzertifikatdatei (.pem).

   Siehe "Herunterladen der Azure-Image-Digest-Datei" für weitere Informationen.

2. Überprüfen Sie die Vertrauenskette.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Entfernen Sie 1 MB (1.048.576 Bytes) am Anfang und 512 Bytes am Ende der VHD-Datei. Bei der Verwendung `tail` , Die `-c +K` Option generiert Bytes aus dem K-ten Byte der Datei. Daher geht es 1048577 an `tail -c` . Beachten Sie, dass die Ausführung des Tail-Befehls unter macOS etwa zehn Minuten dauern kann.

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. Verwenden Sie OpenSSL, um den öffentlichen Schlüssel aus dem Zertifikat zu extrahieren und die extrahierte Datei (sign.tmp) mit der Signaturdatei und dem öffentlichen Schlüssel zu überprüfen. Die Eingabeaufforderung zeigt Meldungen an, die den Erfolg oder Misserfolg der Überprüfung basierend auf deren Erfolg anzeigen.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Räumen Sie den Arbeitsbereich auf.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Stellen Sie Cloud Volumes ONTAP vom Azure Marketplace bereit

Sie können die direkte Bereitstellung über den Azure Marketplace verwenden, um Cloud Volumes ONTAP schnell und einfach bereitzustellen. Über den Azure Marketplace können Sie Cloud Volumes ONTAP mit wenigen Klicks schnell bereitstellen und die wichtigsten Funktionen und Möglichkeiten in Ihrer Umgebung erkunden.

Weitere Informationen zu diesem Angebot finden Sie unter"Informieren Sie sich über die Angebote von Cloud Volumes ONTAP in der NetApp Console und im Marketplace." .

Informationen zu diesem Vorgang

Das Cloud Volumes ONTAP -System, das mithilfe der direkten Bereitstellung im Azure Marketplace bereitgestellt wird, verfügt über diese Eigenschaften. Beachten Sie, dass sich die Funktionen einer über den Azure Marketplace bereitgestellten eigenständigen Instanz ändern, wenn sie in der NetApp Console erkannt wird.

- Die neueste Cloud Volumes ONTAP -Version (9.16.1 oder höher).
- Eine kostenlose Lizenz für Cloud Volumes ONTAP , die auf 500 GiB bereitgestellte Kapazität begrenzt ist. Diese Lizenz beinhaltet keinen NetApp Support und hat kein Ablaufdatum.
- Zwei Knoten, die im Hochverfügbarkeitsmodus (HA) in einer einzigen Verfügbarkeitszone (AZ) konfiguriert und mit Standardseriennummern bereitgestellt sind. Die Storage-VMs (Storage-VMs) werden in einem"flexibler Orchestrierungsmodus" .
- Ein Aggregat für die standardmäßig erstellte Instanz.
- Eine verwaltete Premium-SSD-v2-Festplatte mit 500 GiB bereitgestellter Kapazität sowie eine Root- und eine Datenfestplatte.

- Eine bereitgestellte Datenspeicher-VM mit NFS-, CIFS-, iSCSI- und NVMe/TCP-Datendiensten. Sie können keine zusätzlichen Datenspeicher-VMs hinzufügen.
- Installierte Lizenzen für NFS, CIFS (SMB), iSCSI, Autonomous Ransomware Protection (ARP), SnapLock und SnapMirror.
- "ONTAP temperaturempfindliche Speichereffizienz (TSSE)", Volume-Verschlüsselung und externe Schlüsselverwaltung standardmäßig aktiviert.
- Diese Funktionen werden nicht unterstützt:
  - FabricPool -Stufen
  - Ändern des Speicher-VM-Typs
  - Schnellschreibmodus

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie über ein gültiges Azure Marketplace-Abonnement verfügen.
- Stellen Sie sicher, dass Sie die Netzwerkanforderungen für ein"HA-Bereitstellung in einer einzigen AZ" in Azure. Weitere Informationen finden Sie unter "Einrichten des Azure-Netzwerks für Cloud Volumes ONTAP" .
- Um Cloud Volumes ONTAP bereitzustellen, muss Ihnen eine dieser Azure-Rollen zugewiesen werden:
  - Der `contributor` Rolle mit den Standardberechtigungen. Weitere Informationen finden Sie im "Microsoft Azure-Dokumentation: Integrierte Azure-Rollen" .
  - Eine benutzerdefinierte RBAC-Rolle mit den folgenden Berechtigungen. Weitere Informationen finden Sie im "Azure-Dokumentation: Benutzerdefinierte Azure-Rollen" .

```
"Berechtigungen": [ { "Aktionen": [ "Microsoft.AAD/register/action",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Network/loadBalancers/write", "Microsoft.ClassicCompute/virtualMachines/write",
"Microsoft.Compute/capacityReservationGroups/deploy/action",
"Microsoft.ClassicCompute/virtualMachines/networkInterfaces/associatedNetworkSecurityGroups/
write", "Microsoft.Network/networkInterfaces/write", "Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Network/virtualNetworks/write", "Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/read", "Microsoft.Compute/disks/write",
"Microsoft.Compute/virtualMachineScaleSets/write", "Microsoft.Resources/deployments/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/subnets/write" ], "notActions": [], "dataActions": [],
"notDataActions": [] } ]
```

Wenn Sie den Ressourcenanbieter "Microsoft.storage" für Ihr Abonnement registriert haben, benötigen Sie nicht die `Microsoft.AAD/register/action` Erlaubnis. Weitere Informationen finden Sie im "Azure-Dokumentation: Azure-Berechtigungen für Speicher" .

Schritte

1. Suchen Sie auf der Azure Marketplace-Site nach NetApp -Produkten.

2. Wählen Sie * NetApp Cloud Volumes ONTAP direct*.
3. Klicken Sie auf **Erstellen**, um den Bereitstellungsassistenten zu starten.
4. Wählen Sie einen Plan aus. In der **Plan**-Liste werden normalerweise die neuesten Versionen von Cloud Volumes ONTAP angezeigt.
5. Geben Sie auf der Registerkarte **Grundlagen** die folgenden Details an:
    - **Abonnement**: Wählen Sie ein Abonnement aus. Die Bereitstellung wird an die Abonnementnummer gekoppelt.
    - **Ressourcengruppe**: Verwenden Sie eine vorhandene Ressourcengruppe oder erstellen Sie eine neue. Ressourcengruppen helfen bei der Zuweisung aller Ressourcen, wie z. B. Festplatten und Speicher-VMs, innerhalb einer einzigen Gruppe für ein Cloud Volumes ONTAP System.
    - **Region**: Wählen Sie eine Region aus, die die Azure HA-Bereitstellung in einer einzelnen AZ unterstützt. Sie sehen in der Liste nur die verfügbaren Regionen.
    - **Größe**: Wählen Sie eine Speicher-VM-Größe für die unterstützte verwaltete Premium-SSD-v2-Festplatte aus.
    - **Zone**: Wählen Sie eine Zone für die von Ihnen ausgewählte Region aus.
    - **Admin-Passwort**: Legen Sie ein Passwort fest. Mit diesem Admin-Passwort melden Sie sich nach der Bereitstellung am System an.
    - **Passwort bestätigen**: Geben Sie zur Bestätigung dasselbe Passwort erneut ein.
        - Fügen Sie auf der Registerkarte **Netzwerk** ein virtuelles Netzwerk und ein Subnetz hinzu oder wählen Sie sie aus den Listen aus.

          Um die Einschränkungen von Microsoft Azure einzuhalten, sollten Sie beim Einrichten eines neuen virtuellen Netzwerks ein neues Subnetz erstellen. Wenn Sie ein vorhandenes Netzwerk auswählen, sollten Sie ebenfalls ein vorhandenes Subnetz auswählen.

        - Um eine vordefinierte Netzwerksicherheitsgruppe auszuwählen, wählen Sie **Ja**. Wählen Sie **Nein** aus, um eine vordefinierte Azure-Netzwerksicherheitsgruppe mit den erforderlichen Verkehrsregeln zuzuweisen. Weitere Informationen finden Sie unter "Sicherheitsgruppenregeln für Azure" .
        - Bestätigen Sie auf der Registerkarte **Erweitert**, ob die beiden für diese Bereitstellung erforderlichen Azure-Funktionen festgelegt wurden. Siehe"Aktivieren Sie eine Azure-Funktion für Cloud Volumes ONTAP Single AZ-Bereitstellungen" Und"Aktivieren Sie den Hochverfügbarkeitsmodus für Cloud Volumes ONTAP in Azure" .
        - Sie können Name-Wert-Paare für die Ressourcen oder Ressourcengruppen auf der Registerkarte **Tags** definieren.
        - Überprüfen Sie auf der Registerkarte **Überprüfen + Erstellen** die Details und starten Sie die Bereitstellung.

Nach Abschluss

Wählen Sie das Benachrichtigungssymbol aus, um den Fortschritt Ihrer Bereitstellung anzuzeigen. Nachdem Cloud Volumes ONTAP bereitgestellt wurde, können Sie die für Vorgänge aufgelistete Speicher-VM anzeigen.

Sobald Sie darauf zugreifen können, verwenden Sie ONTAP System Manager oder die ONTAP CLI, um sich mit den von Ihnen festgelegten Administratoranmeldeinformationen bei der Speicher-VM anzumelden. Anschließend können Sie Volumes, LUNs oder Freigaben erstellen und die Speicherfunktionen von Cloud Volumes ONTAP nutzen.

Beheben von Bereitstellungsproblemen

Cloud Volumes ONTAP -Systeme, die direkt über den Azure-Marktplatz bereitgestellt werden, umfassen keinen Support von NetApp. Wenn während der Bereitstellung Probleme auftreten, können Sie diese selbstständig beheben.

Schritte

1. Gehen Sie auf der Azure Marketplace-Site zu **Bootdiagnose > Serielles Protokoll**.
2. Laden Sie die Serienprotokolle herunter und untersuchen Sie sie.
3. Informationen zur Fehlerbehebung finden Sie in der Produktdokumentation und in den Knowledge Base-Artikeln (KB).
   - "Azure Marketplace-Dokumentation"
   - "NetApp Dokumentation"
   - "NetApp KB-Artikel"

Entdecken Sie die bereitgestellten Systeme in der Konsole

Sie können die Cloud Volumes ONTAP -Systeme, die Sie mithilfe der direkten Bereitstellung im Azure Marketplace bereitgestellt haben, ermitteln und auf der Seite **Systeme** in der Konsole verwalten. Der Konsolenagent erkennt die Systeme, fügt sie hinzu, wendet die erforderlichen Lizenzen an und schaltet die vollständigen Funktionen der Konsole für diese Systeme frei. Die ursprüngliche HA-Konfiguration in einer einzelnen AZ mit PSSD v2 Managed Disks bleibt erhalten und das System wird beim selben Azure-Abonnement und derselben Ressourcengruppe registriert wie die ursprüngliche Bereitstellung.

Informationen zu diesem Vorgang

Beim Erkennen der Cloud Volumes ONTAP -Systeme, die mithilfe der direkten Bereitstellung im Azure Marketplace bereitgestellt wurden, führt der Konsolenagent die folgenden Aufgaben aus:

- Ersetzt die freien Lizenzen der ermittelten Systeme als reguläre kapazitätsbasierte"Freemium-Lizenzen" .
- Behält die vorhandenen Funktionen der bereitgestellten Systeme bei und fügt die zusätzlichen Funktionen der Konsole hinzu, z. B. Datenschutz, Datenverwaltung und Sicherheitsfunktionen.
- Ersetzt die installierten Lizenzen auf den Knoten durch neue ONTAP -Lizenzen für NFS, CIFS (SMB), iSCSI, ARP, SnapLock und SnapMirror.
- Konvertiert die generischen Knotenseriennummern in eindeutige Seriennummern.
- Weist den Ressourcen nach Bedarf neue System-Tags zu.
- Wandelt die dynamischen IP-Adressen der Instanz in statische IP-Adressen um.
- Ermöglicht die Funktionalitäten von"FabricPool -Stufen" ,"AutoSupport" , Und"Einmal schreiben, oft lesen" (WORM)-Speicher auf den bereitgestellten Systemen. Sie können diese Funktionen bei Bedarf über die Konsole aktivieren.
- Registriert die Instanzen bei den NSS-Konten, die zu ihrer Erkennung verwendet werden.
- Aktiviert Kapazitätsmanagementfunktionen in"automatischer und manueller Modus" für die entdeckten Systeme.

Bevor Sie beginnen

Stellen Sie sicher, dass die Bereitstellung auf dem Azure-Marktplatz abgeschlossen ist. Der Konsolenagent kann die Systeme nur erkennen, wenn die Bereitstellung abgeschlossen ist und sie zur Erkennung bereitstehen.

Schritte

In der Konsole folgen Sie dem Standardverfahren zum Erkennen vorhandener Systeme. Weitere Informationen finden Sie unter "Fügen Sie der Konsole ein vorhandenes Cloud Volumes ONTAP -System hinzu" .

> Während der Erkennung werden möglicherweise Fehlermeldungen angezeigt, die Sie jedoch ignorieren können, bis der Erkennungsprozess abgeschlossen ist. Ändern Sie während der Erkennung nicht die systemgenerierten Cloud Volumes ONTAP -Konfigurationen im Azure Marketplace-Portal, insbesondere nicht die System-Tags. Alle an diesen Konfigurationen vorgenommenen Änderungen können zu unerwartetem Systemverhalten führen.

Nach Abschluss

Nachdem die Erkennung abgeschlossen ist, können Sie die auf der Seite **Systeme** in der Konsole aufgelisteten Systeme anzeigen. Sie können verschiedene Verwaltungsaufgaben ausführen, wie zum Beispiel"Erweiterung des Aggregats" ,"Hinzufügen von Volumes" ,"Bereitstellung zusätzlicher Speicher-VMs" , Und"Ändern der Instanztypen" .

Weiterführende Links

Weitere Informationen zum Erstellen von Speicher finden Sie in der ONTAP -Dokumentation:

- "Erstellen von Volumes für NFS"
- "Erstellen von LUNs für iSCSI"
- "Freigaben für CIFS erstellen"

Erste Schritte in Google Cloud

Schnellstart für Cloud Volumes ONTAP in Google Cloud

Beginnen Sie in wenigen Schritten mit Cloud Volumes ONTAP in Google Cloud.

Erstellen eines Konsolenagenten

Wenn Sie keinen haben "Konsolenagent" Dennoch müssen Sie einen erstellen. "Erfahren Sie, wie Sie einen Konsolenagenten in Google Cloud erstellen"

Beachten Sie: Wenn Sie Cloud Volumes ONTAP in einem Subnetz bereitstellen möchten, in dem kein Internetzugang verfügbar ist, müssen Sie den Konsolenagenten manuell installieren und auf die NetApp Console zugreifen, die auf diesem Konsolenagenten ausgeführt wird. "Erfahren Sie, wie Sie den Konsolenagenten manuell an einem Ort ohne Internetzugang installieren."

Planen Sie Ihre Konfiguration

Die Konsole bietet vorkonfigurierte Pakete, die Ihren Workload-Anforderungen entsprechen, oder Sie können Ihre eigene Konfiguration erstellen. Wenn Sie Ihre eigene Konfiguration auswählen, sollten Sie die Ihnen zur Verfügung stehenden Optionen verstehen.

"Erfahren Sie mehr über die Planung Ihrer Konfiguration" .

Richten Sie Ihr Netzwerk ein

1. Stellen Sie sicher, dass Ihr VPC und Ihre Subnetze die Konnektivität zwischen dem Konsolenagenten und Cloud Volumes ONTAP unterstützen.
2. Wenn Sie Data Tiering aktivieren möchten, "Konfigurieren Sie das Cloud Volumes ONTAP Subnetz für den privaten Google-Zugriff" .
3. Wenn Sie ein HA-Paar bereitstellen, stellen Sie sicher, dass Sie über vier VPCs verfügen, jede mit ihrem eigenen Subnetz.
4. Wenn Sie eine gemeinsam genutzte VPC verwenden, weisen Sie dem Dienstkonto des Konsolenagenten die Rolle „Compute Network User“ zu.
5. Aktivieren Sie den ausgehenden Internetzugriff vom Ziel-VPC für NetApp AutoSupport.

   Dieser Schritt ist nicht erforderlich, wenn Sie Cloud Volumes ONTAP an einem Standort bereitstellen, an dem kein Internetzugang verfügbar ist.

"Erfahren Sie mehr über die Netzwerkanforderungen" .

Einrichten eines Dienstkontos

Cloud Volumes ONTAP erfordert aus zwei Gründen ein Google Cloud-Dienstkonto. Die erste ist, wenn Sie aktivieren"Daten-Tiering" um kalte Daten in kostengünstigen Objektspeicher in Google Cloud zu verschieben. Die zweite Möglichkeit besteht darin, dass Sie die "NetApp Backup and Recovery" um Volumes auf kostengünstigem Objektspeicher zu sichern.

Sie können ein Servicekonto einrichten und es für beide Zwecke verwenden. Das Dienstkonto muss über die Rolle **Storage Admin** verfügen.

"Lesen Sie die Schritt-für-Schritt-Anleitung" .

Google Cloud-APIs aktivieren

"Aktivieren Sie Google Cloud APIs in Ihrem Projekt". "Diese APIs", die Sie möglicherweise bereits im Rahmen der Erstellung des Console-Agenten aktiviert haben, sind für die Bereitstellung von Cloud Volumes ONTAP in Google Cloud erforderlich.

Starten Sie Cloud Volumes ONTAP über die Konsole

Klicken Sie auf **System hinzufügen**, wählen Sie den Systemtyp aus, den Sie bereitstellen möchten, und führen Sie die Schritte im Assistenten aus. "Lesen Sie die Schritt-für-Schritt-Anleitung" .

Weiterführende Links

- "Erstellen eines Konsolenagenten"
- "Installieren der Konsolenagentensoftware auf einem Linux-Host"
- "Google Cloud-Berechtigungen für den Konsolenagenten"

Planen Sie Ihre Cloud Volumes ONTAP Konfiguration in Google Cloud

Wenn Sie Cloud Volumes ONTAP in Google Cloud bereitstellen, können Sie ein vorkonfiguriertes System auswählen, das Ihren Workload-Anforderungen entspricht, oder Sie können Ihre eigene Konfiguration erstellen. Wenn Sie Ihre eigene Konfiguration

auswählen, sollten Sie die Ihnen zur Verfügung stehenden Optionen verstehen.

Wählen Sie eine Cloud Volumes ONTAP -Lizenz

Für Cloud Volumes ONTAP sind mehrere Lizenzierungsoptionen verfügbar. Jede Option ermöglicht Ihnen die Auswahl eines Verbrauchsmodells, das Ihren Anforderungen entspricht.

- "Erfahren Sie mehr über die Lizenzierungsoptionen für Cloud Volumes ONTAP"
- "Erfahren Sie, wie Sie die Lizenzierung einrichten"

Wählen Sie eine unterstützte Region

Cloud Volumes ONTAP wird in den meisten Google Cloud-Regionen unterstützt. "Vollständige Liste der unterstützten Regionen anzeigen" .

Wählen Sie einen unterstützten Maschinentyp

Cloud Volumes ONTAP unterstützt je nach gewähltem Lizenztyp mehrere Maschinentypen.

"Unterstützte Konfigurationen für Cloud Volumes ONTAP in Google Cloud"

Speichergrenzen verstehen

Die Rohkapazitätsgrenze für ein Cloud Volumes ONTAP System ist an die Lizenz gebunden. Zusätzliche Beschränkungen wirken sich auf die Größe von Aggregaten und Volumina aus. Sie sollten sich dieser Beschränkungen bewusst sein, wenn Sie Ihre Konfiguration planen.

"Speichergrenzen für Cloud Volumes ONTAP in Google Cloud"

Dimensionieren Sie Ihr System in Google Cloud

Durch die Dimensionierung Ihres Cloud Volumes ONTAP -Systems können Sie die Anforderungen an Leistung und Kapazität erfüllen. Bei der Auswahl eines Maschinentyps, Datenträgertyps und einer Datenträgergröße sollten Sie einige wichtige Punkte beachten:

Maschinentyp

Schauen Sie sich die unterstützten Maschinentypen in der "Versionshinweise zu Cloud Volumes ONTAP" Anschließend können Sie bei Google die Details zu jedem unterstützten Maschinentyp einsehen. Passen Sie Ihre Workload-Anforderungen an die Anzahl der vCPUs und den Arbeitsspeicher für den Maschinentyp an. Beachten Sie, dass jeder CPU-Kern die Netzwerkleistung erhöht.

Weitere Einzelheiten finden Sie im Folgenden:

- "Google Cloud-Dokumentation: N1-Standardmaschinentypen"
- "Google Cloud-Dokumentation: Leistung"

Datenträgertypen

Wenn Sie Volumes für Cloud Volumes ONTAP erstellen, müssen Sie den zugrunde liegenden Cloud-Speicher auswählen, den Cloud Volumes ONTAP für eine Festplatte verwendet. Der Datenträgertyp kann einer der folgenden sein:

- *Zonale persistente SSD-Festplatten*: Persistente SSD-Festplatten eignen sich am besten für Workloads, die hohe zufällige IOPS-Raten erfordern.

- *Zonal Balanced Persistent Disks*: Diese SSDs gleichen Leistung und Kosten aus, indem sie niedrigere IOPS pro GB bereitstellen.
- *Zonale persistente Standarddatenträger*: Persistente Standarddatenträger sind wirtschaftlich und können sequenzielle Lese-/Schreibvorgänge verarbeiten.

  Weitere Einzelheiten finden Sie im "Google Cloud-Dokumentation: Zonale persistente Datenträger (Standard und SSD)" .

Festplattengröße

Sie müssen eine anfängliche Festplattengröße auswählen, wenn Sie ein Cloud Volumes ONTAP -System bereitstellen. Anschließend können Sie die Kapazität eines Systems von der NetApp Console verwalten lassen. Wenn Sie jedoch selbst Aggregate erstellen möchten, beachten Sie Folgendes:

- Alle Festplatten in einem Aggregat müssen die gleiche Größe haben.
- Bestimmen Sie den Platzbedarf unter Berücksichtigung der Leistung.
- Die Leistung persistenter Datenträger skaliert automatisch mit der Datenträgergröße und der Anzahl der dem System zur Verfügung stehenden vCPUs.

  Weitere Einzelheiten finden Sie im Folgenden:

  - "Google Cloud-Dokumentation: Zonale persistente Datenträger (Standard und SSD)"
  - "Google Cloud-Dokumentation: Optimieren der Leistung von persistenten Festplatten und lokalen SSDs"

Standardsystemfestplatten anzeigen

Zusätzlich zum Speicher für Benutzerdaten erwirbt die Konsole auch Cloud-Speicher für Cloud Volumes ONTAP -Systemdaten (Boot-Daten, Root-Daten, Core-Daten und NVRAM). Zu Planungszwecken kann es hilfreich sein, diese Details zu überprüfen, bevor Sie Cloud Volumes ONTAP bereitstellen.

- "Standardfestplatten für Cloud Volumes ONTAP -Systemdaten in Google Cloud anzeigen" .
- "Google Cloud-Dokumentation: Übersicht über Cloud-Kontingente"

  Google Cloud Compute Engine erzwingt Kontingente für die Ressourcennutzung. Stellen Sie daher sicher, dass Sie Ihr Limit nicht erreicht haben, bevor Sie Cloud Volumes ONTAP bereitstellen.

Der Konsolenagent benötigt außerdem eine Systemfestplatte. "Details zur Standardkonfiguration des Konsolenagenten anzeigen" .

Sammeln von Netzwerkinformationen

Wenn Sie Cloud Volumes ONTAP in Google Cloud bereitstellen, müssen Sie Details zu Ihrem virtuellen Netzwerk angeben. Sie können ein Arbeitsblatt verwenden, um die Informationen von Ihrem Administrator zu erfassen.

Netzwerkinformationen für ein Einzelknotensystem

Google Cloud-Informationen	Ihr Wert
Region	

Google Cloud-Informationen	Ihr Wert
Zone	
VPC-Netzwerk	
Subnetz	
Firewall-Richtlinie (falls Sie Ihre eigene verwenden)	

Netzwerkinformationen für ein HA-Paar in mehreren Zonen

Google Cloud-Informationen	Ihr Wert
Region	
Zone für Knoten 1	
Zone für Knoten 2	
Zone für den Mediator	
VPC-0 und Subnetz	
VPC-1 und Subnetz	
VPC-2 und Subnetz	
VPC-3 und Subnetz	
Firewall-Richtlinie (falls Sie Ihre eigene verwenden)	

Netzwerkinformationen für ein HA-Paar in einer einzelnen Zone

Google Cloud-Informationen	Ihr Wert
Region	
Zone	
VPC-0 und Subnetz	
VPC-1 und Subnetz	
VPC-2 und Subnetz	
VPC-3 und Subnetz	
Firewall-Richtlinie (falls Sie Ihre eigene verwenden)	

Wählen Sie eine Schreibgeschwindigkeit

Mit der Konsole können Sie eine Schreibgeschwindigkeitseinstellung für Cloud Volumes ONTAP auswählen, mit Ausnahme von Hochverfügbarkeitspaaren (HA) in Google Cloud. Bevor Sie eine Schreibgeschwindigkeit auswählen, sollten Sie die Unterschiede zwischen den normalen und hohen Einstellungen sowie die Risiken und Empfehlungen bei der Verwendung einer hohen Schreibgeschwindigkeit verstehen. "Erfahren Sie mehr über die Schreibgeschwindigkeit" .

Auswählen eines Volume-Nutzungsprofils

ONTAP umfasst mehrere Speichereffizienzfunktionen, die die von Ihnen benötigte Gesamtspeichermenge reduzieren können. Wenn Sie in der Konsole ein Volume erstellen, können Sie ein Profil auswählen, das diese Funktionen aktiviert, oder ein Profil, das sie deaktiviert. Sie sollten mehr über diese Funktionen erfahren, um zu entscheiden, welches Profil Sie verwenden möchten.

Die Storage-Effizienzfunktionen von NetApp bieten folgende Vorteile:

Dünne Bereitstellung

Bietet Hosts oder Benutzern mehr logischen Speicher, als Sie tatsächlich in Ihrem physischen Speicherpool haben. Anstatt Speicherplatz vorab zuzuweisen, wird Speicherplatz jedem Volume dynamisch zugewiesen, während Daten geschrieben werden.

Deduplizierung

Verbessert die Effizienz, indem identische Datenblöcke lokalisiert und durch Verweise auf einen einzigen gemeinsamen Block ersetzt werden. Diese Technik reduziert den Speicherkapazitätsbedarf, indem redundante Datenblöcke, die sich auf demselben Datenträger befinden, eliminiert werden.

Komprimierung

Reduziert die zum Speichern von Daten erforderliche physische Kapazität durch Komprimieren von Daten innerhalb eines Volumes auf Primär-, Sekundär- und Archivspeicher.

Einrichten des Google Cloud-Netzwerks für Cloud Volumes ONTAP

Die NetApp Console übernimmt die Einrichtung von Netzwerkkomponenten für Cloud Volumes ONTAP, wie z. B. IP-Adressen, Netzmasken und Routen. Sie müssen sicherstellen, dass ausgehender Internetzugang verfügbar ist, dass genügend private IP-Adressen verfügbar sind, dass die richtigen Verbindungen vorhanden sind und mehr.

Wenn Sie ein HA-Paar einsetzen möchten, sollten Sie"Erfahren Sie, wie HA-Paare in Google Cloud funktionieren." .

Anforderungen für Cloud Volumes ONTAP

Die folgenden Anforderungen müssen in Google Cloud erfüllt sein.

Anforderungen, die speziell für Einzelknotensysteme gelten

Wenn Sie ein Einzelknotensystem bereitstellen möchten, stellen Sie sicher, dass Ihr Netzwerk die folgenden Anforderungen erfüllt.

Eine VPC

Für ein Einzelknotensystem ist eine Virtual Private Cloud (VPC) erforderlich.

Private IP-Adressen

Für ein Einzelknotensystem in Google Cloud weist die Console den folgenden Komponenten private IP-Adressen zu:

- Node

- Cluster
- Speicher-VM
- Daten-NAS-LIF
- Daten-iSCSI-LIF

Sie können die Erstellung des Storage VM (SVM)-Verwaltungs-LIF überspringen, wenn Sie Cloud Volumes ONTAP mithilfe der API bereitstellen und das folgende Flag angeben:

```
skipSvmManagementLif: true
```

Ein LIF ist eine IP-Adresse, die einem physischen Port zugeordnet ist. Für Verwaltungstools wie SnapCenter ist ein Storage VM (SVM)-Verwaltungs-LIF erforderlich.

Spezifische Anforderungen für HA-Paare

Wenn Sie ein HA-Paar bereitstellen möchten, stellen Sie sicher, dass Ihr Netzwerk die folgenden Anforderungen erfüllt.

Eine oder mehrere Zonen

Sie können die hohe Verfügbarkeit Ihrer Daten sicherstellen, indem Sie eine HA-Konfiguration über mehrere oder in einer einzigen Zone bereitstellen. Die Konsole fordert Sie beim Erstellen des HA-Paares auf, mehrere Zonen oder eine einzelne Zone auszuwählen.

- Mehrere Zonen (empfohlen)

  Durch die Bereitstellung einer HA-Konfiguration über drei Zonen hinweg wird eine kontinuierliche Datenverfügbarkeit gewährleistet, wenn innerhalb einer Zone ein Fehler auftritt. Beachten Sie, dass die Schreibleistung im Vergleich zur Verwendung einer einzelnen Zone etwas geringer ist, aber minimal.

- Einzelzone

  Bei der Bereitstellung in einer einzelnen Zone verwendet eine Cloud Volumes ONTAP HA-Konfiguration eine Richtlinie für verteilte Platzierung. Diese Richtlinie stellt sicher, dass eine HA-Konfiguration vor einem einzelnen Fehlerpunkt innerhalb der Zone geschützt ist, ohne dass separate Zonen zur Fehlerisolierung verwendet werden müssen.

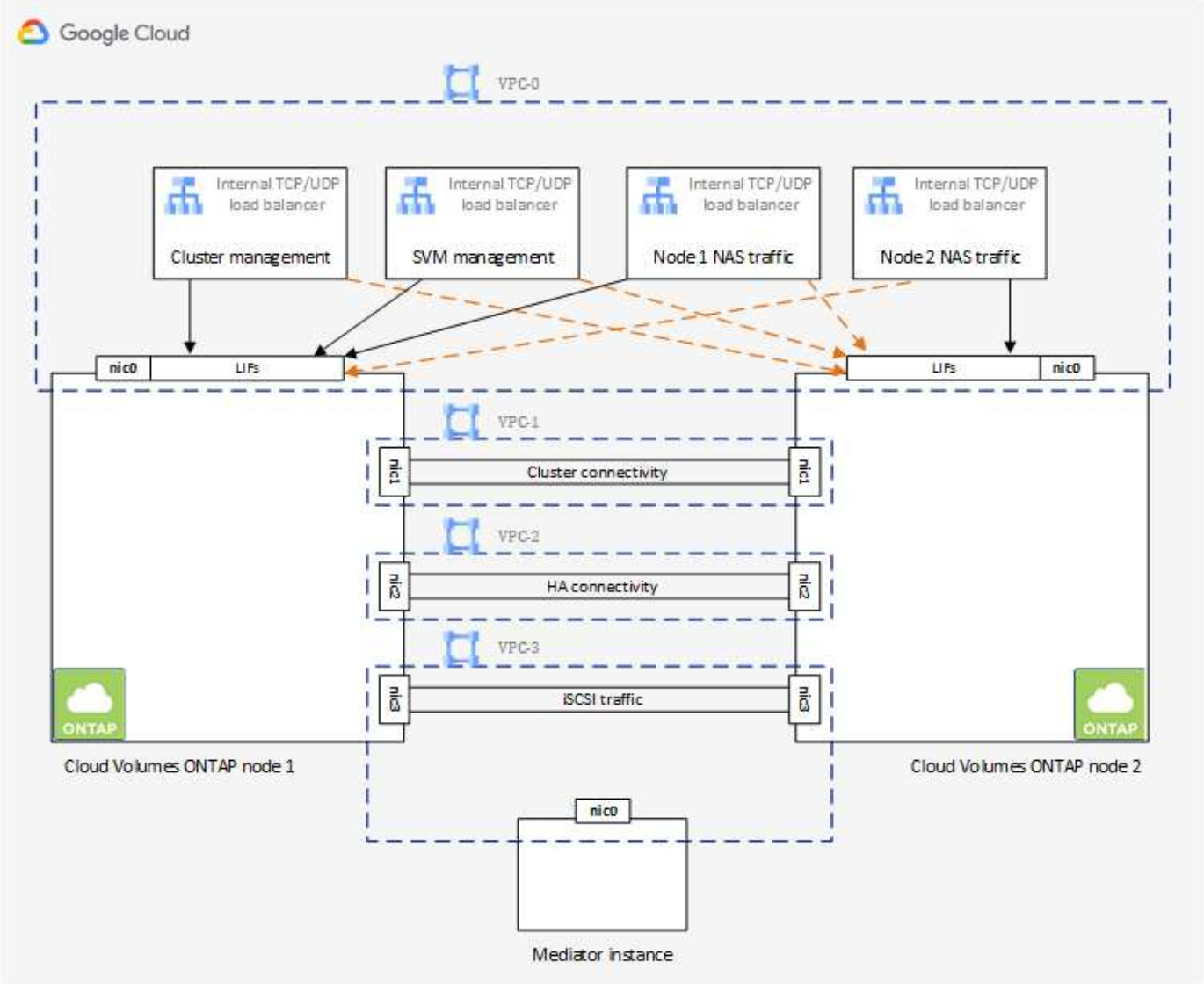
  Dieses Bereitstellungsmodell senkt Ihre Kosten, da zwischen den Zonen keine Gebühren für den Datenausgang anfallen.

Vier virtuelle private Clouds

Für eine HA-Konfiguration werden vier Virtual Private Clouds (VPCs) benötigt. Es sind vier VPCs erforderlich, da Google Cloud erfordert, dass sich jede Netzwerkschnittstelle in einem separaten VPC-Netzwerk befindet.

Die Konsole fordert Sie beim Erstellen des HA-Paares auf, vier VPCs auszuwählen:

- VPC-0 für eingehende Verbindungen zu den Daten und Knoten
- VPC-1, VPC-2 und VPC-3 für die interne Kommunikation zwischen den Knoten und dem HA-Mediator



Subnetze

Für jede VPC ist ein privates Subnetz erforderlich.

Wenn Sie den Konsolenagenten in VPC-0 platzieren, müssen Sie den privaten Google-Zugriff im Subnetz aktivieren, um auf die APIs zuzugreifen und die Datenschichtung zu aktivieren.

Die Subnetze in diesen VPCs müssen unterschiedliche CIDR-Bereiche haben. Sie dürfen keine überlappenden CIDR-Bereiche haben.

Private IP-Adressen

Die Konsole weist Cloud Volumes ONTAP in Google Cloud automatisch die erforderliche Anzahl privater IP-Adressen zu. Sie müssen sicherstellen, dass in Ihrem Netzwerk genügend private Adressen verfügbar sind.

Die Anzahl der für Cloud Volumes ONTAP zugewiesenen LIFs hängt davon ab, ob Sie ein Einzelknotensystem oder ein HA-Paar bereitstellen. Ein LIF ist eine IP-Adresse, die einem physischen Port zugeordnet ist. Ein SVM-Management-LIF ist für Management-Tools wie SnapCenter erforderlich.

- **Einzelknoten** Die NetApp Console weist einem Einzelknotensystem 4 IP-Adressen zu:

- Knotenverwaltung LIF
- Clustermanagement LIF
- iSCSI-Daten-LIF

  Ein iSCSI-LIF bietet Clientzugriff über das iSCSI-Protokoll und wird vom System für andere wichtige Netzwerk-Workflows verwendet. Diese LIFs sind erforderlich und sollten nicht gelöscht werden.

- NAS LIF

  Sie können die Erstellung des Storage VM (SVM)-Verwaltungs-LIF überspringen, wenn Sie Cloud Volumes ONTAP mithilfe der API bereitstellen und das folgende Flag angeben:

```
skipSvmManagementLif: true
```

- **HA-Paar** Die Konsole weist einem HA-Paar 12-13 IP-Adressen zu:
  - 2 Knotenverwaltungs-LIFs (e0a)
  - 1 Clustermanagement LIF (e0a)
  - 2 iSCSI-LIFs (e0a)

    Ein iSCSI-LIF bietet Clientzugriff über das iSCSI-Protokoll und wird vom System für andere wichtige Netzwerk-Workflows verwendet. Diese LIFs sind erforderlich und sollten nicht gelöscht werden.

  - 1 oder 2 NAS-LIFs (e0a)
  - 2 Cluster-LIFs (e0b)
  - 2 HA Interconnect-IP-Adressen (e0c)
  - 2 RSM iSCSI-IP-Adressen (e0d)

    Sie können die Erstellung des Storage VM (SVM)-Verwaltungs-LIF überspringen, wenn Sie Cloud Volumes ONTAP mithilfe der API bereitstellen und das folgende Flag angeben:

```
skipSvmManagementLif: true
```

Interne Lastenausgleichsmodule

Die Konsole erstellt vier interne Google Cloud-Load Balancer (TCP/UDP), die den eingehenden Datenverkehr zum Cloud Volumes ONTAP HA-Paar verwalten. Von Ihrer Seite ist keine Einrichtung erforderlich. Wir haben dies als Anforderung aufgeführt, um Sie lediglich über den Netzwerkverkehr zu informieren und etwaige Sicherheitsbedenken auszuräumen.

Ein Load Balancer dient der Clusterverwaltung, einer der Verwaltung von Storage-VMs (SVM), einer dem NAS-Verkehr zu Knoten 1 und der letzte dem NAS-Verkehr zu Knoten 2.

Die Einrichtung für jeden Load Balancer ist wie folgt:

- Eine gemeinsam genutzte private IP-Adresse
- Ein globaler Gesundheitscheck

Standardmäßig sind die vom Integritätscheck verwendeten Ports 63001, 63002 und 63003.

- Ein regionaler TCP-Backend-Dienst
- Ein regionaler UDP-Backend-Dienst
- Eine TCP-Weiterleitungsregel
- Eine UDP-Weiterleitungsregel
- Der globale Zugriff ist deaktiviert

  Obwohl der globale Zugriff standardmäßig deaktiviert ist, wird die Aktivierung nach der Bereitstellung unterstützt. Wir haben es deaktiviert, da der regionsübergreifende Datenverkehr deutlich höhere Latenzen aufweist. Wir wollten sicherstellen, dass Sie aufgrund versehentlicher regionsübergreifender Mounts keine negativen Erfahrungen machen. Die Aktivierung dieser Option richtet sich nach Ihren Geschäftsanforderungen.

Gemeinsam genutzte VPCs

Cloud Volumes ONTAP und der Konsolenagent werden in einem gemeinsam genutzten Google Cloud VPC und auch in eigenständigen VPCs unterstützt.

Für ein Single-Node-System kann die VPC entweder eine Shared VPC oder eine Standalone VPC sein.

Für ein HA-Paar werden vier VPCs benötigt. Jede dieser VPCs kann entweder gemeinsam genutzt oder eigenständig sein. Beispielsweise könnte VPC-0 eine gemeinsam genutzte VPC sein, während VPC-1, VPC-2 und VPC-3 eigenständige VPCs sein könnten.

Mit einer gemeinsam genutzten VPC können Sie virtuelle Netzwerke über mehrere Projekte hinweg konfigurieren und zentral verwalten. Sie können gemeinsam genutzte VPC-Netzwerke im *Hostprojekt* einrichten und den Konsolenagenten und die virtuellen Maschineninstanzen von Cloud Volumes ONTAP in einem *Serviceprojekt* bereitstellen.

"Google Cloud-Dokumentation: Übersicht über Shared VPC" .

"Überprüfen Sie die erforderlichen freigegebenen VPC-Berechtigungen, die in der Bereitstellung des Konsolenagenten behandelt werden."

Paketspiegelung in VPCs

"Paketspiegelung"muss im Google Cloud-Subnetz deaktiviert werden, in dem Sie Cloud Volumes ONTAP bereitstellen.

Ausgehender Internetzugang

Cloud Volumes ONTAP -Systeme erfordern ausgehenden Internetzugang für den Zugriff auf externe Endpunkte für verschiedene Funktionen. Cloud Volumes ONTAP kann nicht ordnungsgemäß funktionieren, wenn diese Endpunkte in Umgebungen mit strengen Sicherheitsanforderungen blockiert sind.

Der Konsolenagent kontaktiert außerdem mehrere Endpunkte für den täglichen Betrieb. Informationen zu den Endpunkten finden Sie unter "Vom Konsolenagenten kontaktierte Endpunkte anzeigen" Und "Vorbereiten des Netzwerks für die Verwendung der Konsole" .

Cloud Volumes ONTAP Endpunkte

Cloud Volumes ONTAP verwendet diese Endpunkte zur Kommunikation mit verschiedenen Diensten.

Endpunkte	Gilt für	Zweck	Bereitstellungsmodus	Auswirkungen, wenn der Endpunkt nicht verfügbar ist
https://netapp-cloud-account.auth0.com	Authentifizierung	Wird zur Authentifizierung in der Konsole verwendet.	Standard- und eingeschränkte Modi.	Die Benutzerauthentifizierung schlägt fehl und die folgenden Dienste sind weiterhin nicht verfügbar: • Cloud Volumes ONTAP Dienste • ONTAP -Dienste • Protokolle und Proxy-Dienste
https://api.bluexp.netapp.com/tenancy	Mietverhältnis	Wird verwendet, um Cloud Volumes ONTAP -Ressourcen von der Konsole abzurufen, um Ressourcen und Benutzer zu autorisieren.	Standard- und eingeschränkte Modi.	Cloud Volumes ONTAP Ressourcen und die Benutzer sind nicht autorisiert.
https://mysupport.netapp.com/aods/asupmessage https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Wird verwendet, um AutoSupport Telemetriedaten an den NetApp Support zu senden.	Standard- und eingeschränkte Modi.	AutoSupport -Informationen bleiben unversehrt.

Endpunkte	Gilt für	Zweck	Bereitstellungsmodus	Auswirkungen, wenn der Endpunkt nicht verfügbar ist
https://cloudbuild.googleapis.com/v1 (nur für private Bereitstellungen) https://cloudkms.googleapis.com/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://compute.googleapis.com/compute/v1 https://www.googleapis.com/compute/beta https://www.googleapis.com/compute/v1/projects/ https://www.googleapis.com/deploymentmanager/v2/projects https://www.googleapis.com/storage/v1 https://www.googleapis.com/upload/storage/v1 https://config.googleapis.com/v1 https://iam.googleapis.com/v1 https://storage.googleapis.com/storage/v1	Google Cloud (kommerzielle Nutzung).	Kommunikation mit Google Cloud-Diensten.	Standard-, eingeschränkter und privater Modus.	Cloud Volumes ONTAP kann nicht mit dem Google Cloud-Dienst kommunizieren, um bestimmte Vorgänge für die Konsole in Google Cloud auszuführen.

Verbindungen zu ONTAP -Systemen in anderen Netzwerken

Um Daten zwischen einem Cloud Volumes ONTAP -System in Google Cloud und ONTAP -Systemen in anderen Netzwerken zu replizieren, benötigen Sie eine VPN-Verbindung zwischen der VPC und dem anderen Netzwerk, beispielsweise Ihrem Unternehmensnetzwerk.

"Google Cloud-Dokumentation: Cloud VPN-Übersicht" .

Firewall-Regeln

Die Konsole erstellt Google Cloud-Firewallregeln, die die eingehenden und ausgehenden Regeln enthalten, die Cloud Volumes ONTAP für einen erfolgreichen Betrieb benötigt. Möglicherweise möchten Sie zu Testzwecken auf die Ports verweisen oder wenn Sie lieber Ihre eigenen Firewall-Regeln verwenden möchten.

Die Firewall-Regeln für Cloud Volumes ONTAP erfordern sowohl eingehende als auch ausgehende Regeln. Wenn Sie eine HA-Konfiguration bereitstellen, sind dies die Firewall-Regeln für Cloud Volumes ONTAP in

VPC-0.

Beachten Sie, dass für eine HA-Konfiguration zwei Sätze von Firewall-Regeln erforderlich sind:

- Ein Regelsatz für HA-Komponenten in VPC-0. Diese Regeln ermöglichen den Datenzugriff auf Cloud Volumes ONTAP.
- Ein weiterer Regelsatz für HA-Komponenten in VPC-1, VPC-2 und VPC-3. Diese Regeln sind für die eingehende und ausgehende Kommunikation zwischen den HA-Komponenten offen. Mehr erfahren .

Suchen Sie nach Informationen zum Konsolenagenten? "Firewallregeln für den Konsolenagenten anzeigen"

Eingehende Regeln

Wenn Sie ein Cloud Volumes ONTAP -System hinzufügen, können Sie während der Bereitstellung den Quellfilter für die vordefinierte Firewall-Richtlinie auswählen:

- **Nur ausgewählte VPC**: Der Quellfilter für eingehenden Datenverkehr ist der Subnetzbereich der VPC für das Cloud Volumes ONTAP -System und der Subnetzbereich der VPC, in der sich der Konsolenagent befindet. Dies ist die empfohlene Option.
- **Alle VPCs**: Der Quellfilter für eingehenden Datenverkehr ist der IP-Bereich 0.0.0.0/0.

Wenn Sie Ihre eigene Firewall-Richtlinie verwenden, stellen Sie sicher, dass Sie alle Netzwerke hinzufügen, die mit Cloud Volumes ONTAP kommunizieren müssen. Achten Sie jedoch auch darauf, beide Adressbereiche hinzuzufügen, damit der interne Google Load Balancer ordnungsgemäß funktioniert. Diese Adressen sind 130.211.0.0/22 und 35.191.0.0/16. Weitere Informationen finden Sie im "Google Cloud-Dokumentation: Load Balancer-Firewallregeln" .

Protokoll	Hafen	Zweck
Alle ICMP	Alle	Pingen der Instanz
HTTP	80	HTTP-Zugriff auf die ONTAP System Manager-Webkonsole über die IP-Adresse des Cluster-Management-LIF
HTTPS	443	Konnektivität mit dem Konsolenagenten und HTTPS-Zugriff auf die ONTAP System Manager-Webkonsole unter Verwendung der IP-Adresse des Cluster-Management-LIF
SSH	22	SSH-Zugriff auf die IP-Adresse des Cluster-Management-LIF oder eines Node-Management-LIF
TCP	111	Remote Procedure Call für NFS
TCP	139	NetBIOS-Dienstsitzung für CIFS
TCP	161-162	Einfaches Netzwerkverwaltungsprotokoll
TCP	445	Microsoft SMB/CIFS über TCP mit NetBIOS-Framing
TCP	635	NFS-Mount
TCP	749	Kerberos
TCP	2049	NFS-Server-Daemon
TCP	3260	iSCSI-Zugriff über das iSCSI-Daten-LIF

Protokoll	Hafen	Zweck
TCP	4045	NFS-Sperrdaemon
TCP	4046	Netzwerkstatusmonitor für NFS
TCP	10000	Sicherung mit NDMP
TCP	11104	Verwaltung von Intercluster-Kommunikationssitzungen für SnapMirror
TCP	11105	SnapMirror Datenübertragung mithilfe von Intercluster-LIFs
TCP	63001-63050	Lastenausgleichs-Testports, um festzustellen, welcher Knoten fehlerfrei ist (nur für HA-Paare erforderlich)
UDP	111	Remote Procedure Call für NFS
UDP	161-162	Einfaches Netzwerkverwaltungsprotokoll
UDP	635	NFS-Mount
UDP	2049	NFS-Server-Daemon
UDP	4045	NFS-Sperrdaemon
UDP	4046	Netzwerkstatusmonitor für NFS
UDP	4049	NFS-Rquotad-Protokoll

Ausgangsregeln

Die vordefinierte Sicherheitsgruppe für Cloud Volumes ONTAP öffnet den gesamten ausgehenden Datenverkehr. Wenn das akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Nachrichten. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Ausgangsregeln.

Grundlegende Ausgangsregeln

Die vordefinierte Sicherheitsgruppe für Cloud Volumes ONTAP umfasst die folgenden ausgehenden Regeln.

Protokoll	Hafen	Zweck
Alle ICMP	Alle	Der gesamte ausgehende Verkehr
Alle TCP	Alle	Der gesamte ausgehende Verkehr
Alle UDP	Alle	Der gesamte ausgehende Verkehr

Erweiterte Ausgangsregeln

Wenn Sie strenge Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation von Cloud Volumes ONTAP erforderlich sind. Die Cloud Volumes ONTAP -Cluster verwenden die folgenden Ports zur Regulierung des Knotenverkehrs.

Die Quelle ist die Schnittstelle (IP-Adresse) des Cloud Volumes ONTAP Systems.

Service	Protokoll	Hafen	Quelle	Ziel	Zweck
Active Directory	TCP	88	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	UDP	137	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	UDP	138	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	NetBIOS-Datagrammdienst
	TCP	139	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	NetBIOS-Dienstsitzung
	TCP und UDP	389	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NetBIOS-Framing
	TCP	464	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern & festlegen (SET_CHANGE)
	UDP	464	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	TCP	749	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (RPCSEC_GSS)
	TCP	88	Daten-LIF (NFS, CIFS, iSCSI)	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	UDP	137	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	UDP	138	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	NetBIOS-Datagrammdienst
	TCP	139	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	NetBIOS-Dienstsitzung
	TCP und UDP	389	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NetBIOS-Framing
	TCP	464	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern & festlegen (SET_CHANGE)
	UDP	464	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	TCP	749	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern & festlegen (RPCSEC_GSS)

Service	Protokoll	Hafen	Quelle	Ziel	Zweck
AutoSupport	HTTPS	443	Knotenverwaltung LIF	mysupport.netapp.com	AutoSupport (HTTPS ist die Standardeinstellung)
	HTTP	80	Knotenverwaltung LIF	mysupport.netapp.com	AutoSupport (nur wenn das Transportprotokoll von HTTPS auf HTTP geändert wird)
	TCP	3128	Knotenverwaltung LIF	Konsolenagent	Senden von AutoSupport -Nachrichten über einen Proxyserver auf dem Konsolenagenten, wenn keine ausgehende Internetverbindung verfügbar ist
Konfigurationssicherungen	HTTP	80	Knotenverwaltung LIF	http://<IP-Adresse des Konsolenagenten>/occm/offboxconfig	Senden Sie Konfigurationssicherungen an den Konsolenagenten."ONTAP-Dokumentation"
DHCP	UDP	68	Knotenverwaltung LIF	DHCP	DHCP-Client für die Ersteinrichtung
DHCPS	UDP	67	Knotenverwaltung LIF	DHCP	DHCP-Server
DNS	UDP	53	Knotenverwaltungs-LIF und Daten-LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	Knotenverwaltung LIF	Zielserver	NDMP-Kopie
SMTP	TCP	25	Knotenverwaltung LIF	Mailserver	SMTP-Benachrichtigungen, können für AutoSupport verwendet werden
SNMP	TCP	161	Knotenverwaltung LIF	Monitorserver	Überwachung durch SNMP-Traps
	UDP	161	Knotenverwaltung LIF	Monitorserver	Überwachung durch SNMP-Traps
	TCP	162	Knotenverwaltung LIF	Monitorserver	Überwachung durch SNMP-Traps
	UDP	162	Knotenverwaltung LIF	Monitorserver	Überwachung durch SNMP-Traps
SnapMirror	TCP	11104	Intercluster LIF	ONTAP Intercluster-LIFs	Verwaltung von Intercluster-Kommunikationssitzungen für SnapMirror
	TCP	11105	Intercluster LIF	ONTAP Intercluster-LIFs	SnapMirror -Datenübertragung
Syslog	UDP	514	Knotenverwaltung LIF	Syslog-Server	Syslog-Weiterleitungsnachrichten

Regeln für VPC-1, VPC-2 und VPC-3

In Google Cloud wird eine HA-Konfiguration über vier VPCs bereitgestellt. Die für die HA-Konfiguration in VPC-0 erforderlichen Firewall-Regeln sindoben für Cloud Volumes ONTAP aufgeführt .

In der Zwischenzeit ermöglichen die vordefinierten Firewall-Regeln, die für die Instanzen in VPC-1, VPC-2 und VPC-3 erstellt wurden, die eingehende Kommunikation über *alle* Protokolle und Ports. Diese Regeln ermöglichen die Kommunikation zwischen HA-Knoten.

Die Kommunikation von den HA-Knoten zum HA-Mediator erfolgt über Port 3260 (iSCSI).

> Um eine hohe Schreibgeschwindigkeit für neue Google Cloud HA-Paarbereitstellungen zu ermöglichen, ist für VPC-1, VPC-2 und VPC-3 eine maximale Übertragungseinheit (MTU) von mindestens 8.896 Bytes erforderlich. Wenn Sie vorhandene VPC-1, VPC-2 und VPC-3 auf eine MTU von 8.896 Bytes aktualisieren möchten, müssen Sie während des Konfigurationsvorgangs alle vorhandenen HA-Systeme herunterfahren, die diese VPCs verwenden.

Infrastructure Manager-Konfiguration für private Modus-Bereitstellungen

Wenn Sie Cloud Volumes ONTAP 9.16.1 oder höher im privaten Modus bereitstellen möchten, müssen Sie einige Konfigurationsänderungen vornehmen, damit Cloud Volumes ONTAP den Google Cloud Infrastructure Manager als Bereitstellungsdienst anstelle von Deployment Manager verwenden kann, den Google schließlich außer Betrieb nehmen wird.

Bevor Sie beginnen

- Stellen Sie sicher, dass Ihr Cloud Volumes ONTAP-System Version 9.16.1 oder höher ist. Falls dies nicht der Fall ist, führen Sie ein Upgrade Ihres Systems durch. Siehe "Upgrade von Cloud Volumes ONTAP" für Anweisungen.
- Stellen Sie sicher, dass die Google Cloud APIs aktiviert sind. Siehe "Google Cloud APIs aktivieren".
- Stellen Sie sicher, dass die Cloud Build API aktiviert ist. Siehe "Aktivieren Sie die Cloud Build API hier".
- Überprüfen Sie, ob das Dienstkonto des Console-Agenten über alle Standardberechtigungen verfügt. Stellen Sie außerdem sicher, dass das Dienstkonto die `cloudbuild.workerpools.get` und `cloudbuild.workerpools.list` Berechtigungen hat. Siehe "Google Cloud-Berechtigungen für den Konsolenagenten".

Schritte

1. Erstellen Sie einen privaten Workerpool mit dieser Konfiguration in derselben Region wie die Cloud Volumes ONTAP Bereitstellungen. Informationen zum Erstellen eines privaten Workerpools finden Sie unter "Google Cloud documentation: Private Pools erstellen und verwalten" und "Google Cloud Build-Preise".

   Der Worker-Pool muss die folgende Konfiguration aufweisen:

   - Maschinentyp: e2-medium
   - Festplattengröße: 100 GB
   - Externe IP zuweisen: False
   - Netzwerk: Standard oder privat.
   - Das Subnetz ist für den Zugriff konfiguriert "Google APIs". Führen Sie die folgenden Schritte aus, um sicherzustellen, dass das Subnetz auf die Google APIs zugreifen kann:
     i. Stellen Sie sicher, dass „Private Google Access“ für das Subnetz aktiviert ist.

ii. Gehen Sie zu **VPC Network level > Private Service Access Tab > Allocated IP ranges for services**.

iii. Wählen Sie **Allocate IP range** und weisen Sie den internen IP-Bereich für die private Verbindung zum Google Compute Service zu.

iv. Wählen Sie unter **Private connection to services** die Option **Create Connection**.

v. Wählen Sie **Connected service producer = Google Cloud Platform**.

vi. Weisen Sie die Zuweisung für den privaten Verbindung-IP-Bereich zu, den Sie im vorherigen Schritt erstellt haben.

2. Stellen Sie diesen Worker-Pool bereit und lassen Sie ihn für das Management von Cloud Volumes ONTAP laufen. Google Cloud verwendet diesen Worker-Pool, um alle Terraform-Operationen in einer isolierten Umgebung auszuführen.
3. Bei der Bereitstellung von Cloud Volumes ONTAP im privaten Modus wählen Sie den Namen dieses Worker-Pools im Feld **GCP Worker Pool** aus. Siehe "Starten Sie Cloud Volumes ONTAP in Google Cloud" für Anweisungen.

Anforderungen für den Konsolenagenten

Wenn Sie noch keinen Konsolenagenten erstellt haben, sollten Sie die Netzwerkanforderungen überprüfen.

- "Netzwerkanforderungen für den Konsolenagenten anzeigen"
- "Firewall-Regeln in Google Cloud"

Netzwerkkonfigurationen zur Unterstützung des Konsolenagent-Proxys

Sie können die für den Konsolenagenten konfigurierten Proxyserver verwenden, um ausgehenden Internetzugriff von Cloud Volumes ONTAP zu ermöglichen. Die Konsole unterstützt zwei Arten von Proxys:

- **Expliziter Proxy**: Der ausgehende Datenverkehr von Cloud Volumes ONTAP verwendet die HTTP-Adresse des Proxyservers, der während der Proxy-Konfiguration des Konsolenagenten angegeben wurde. Der Konsolenagent-Administrator hat möglicherweise auch Benutzeranmeldeinformationen und Stamm-CA-Zertifikate für eine zusätzliche Authentifizierung konfiguriert. Wenn ein Stamm-CA-Zertifikat für den expliziten Proxy verfügbar ist, stellen Sie sicher , dass Sie dasselbe Zertifikat erhalten und mithilfe des "ONTAP CLI: Sicherheitszertifikat installieren" Befehl.
- **Transparenter Proxy**: Das Netzwerk ist so konfiguriert, dass ausgehender Datenverkehr von Cloud Volumes ONTAP automatisch über den Proxy des Konsolenagenten geleitet wird. Beim Einrichten eines transparenten Proxys muss der Konsolen-Agent-Administrator nur ein Stamm-CA-Zertifikat für die Konnektivität von Cloud Volumes ONTAP bereitstellen, nicht die HTTP-Adresse des Proxy-Servers. Stellen Sie sicher, dass Sie dasselbe Stamm-CA-Zertifikat erhalten und auf Ihr Cloud Volumes ONTAP System hochladen, indem Sie das "ONTAP CLI: Sicherheitszertifikat installieren" Befehl.

Informationen zum Konfigurieren von Proxy-Servern für den Konsolen-Agenten finden Sie im "Konfigurieren eines Konsolenagenten zur Verwendung eines Proxyservers" .

Konfigurieren Sie Netzwerk-Tags für Cloud Volumes ONTAP in Google Cloud

Während der transparenten Proxy-Konfiguration des Konsolen-Agenten fügt der Administrator ein Netzwerk-Tag für Google Cloud hinzu. Sie müssen dasselbe Netzwerk-Tag für Ihre Cloud Volumes ONTAP Konfiguration abrufen und manuell hinzufügen. Dieses Tag ist für die ordnungsgemäße Funktion des Proxyservers erforderlich.

1. Suchen Sie in der Google Cloud Console Ihr Cloud Volumes ONTAP System.

2. Gehen Sie zu **Details > Netzwerk > Netzwerk-Tags**.
3. Fügen Sie das für den Konsolenagenten verwendete Tag hinzu und speichern Sie die Konfiguration.

Verwandte Themen

- "Überprüfen Sie das AutoSupport -Setup für Cloud Volumes ONTAP"
- "Erfahren Sie mehr über die internen Ports von ONTAP" .

Richten Sie VPC Service Controls ein, um Cloud Volumes ONTAP in Google Cloud bereitzustellen

Wenn Sie Ihre Google Cloud-Umgebung mit VPC Service Controls sperren möchten, sollten Sie verstehen, wie NetApp Console und Cloud Volumes ONTAP mit den Google Cloud-APIs interagieren und wie Sie Ihren Service-Perimeter für die Bereitstellung von Console und Cloud Volumes ONTAP konfigurieren.

Mit VPC Service Controls können Sie den Zugriff auf von Google verwaltete Dienste außerhalb eines vertrauenswürdigen Perimeters steuern, den Datenzugriff von nicht vertrauenswürdigen Standorten blockieren und die Risiken einer nicht autorisierten Datenübertragung mindern. "Erfahren Sie mehr über Google Cloud VPC Service Controls" .

So kommunizieren NetApp -Dienste mit VPC Service Controls

Die Konsole kommuniziert direkt mit den Google Cloud-APIs. Dies wird entweder von einer externen IP-Adresse außerhalb von Google Cloud (z. B. von api.services.cloud.netapp.com) oder innerhalb von Google Cloud von einer internen Adresse ausgelöst, die dem Konsolenagenten zugewiesen ist.

Abhängig vom Bereitstellungsstil des Konsolenagenten müssen möglicherweise bestimmte Ausnahmen für Ihren Service-Perimeter gemacht werden.

Bilder

Sowohl Cloud Volumes ONTAP als auch die Console verwenden Images aus einem Projekt innerhalb von Google Cloud, das von NetApp verwaltet wird. Dies kann die Bereitstellung des Console-Agenten und von Cloud Volumes ONTAP beeinträchtigen, wenn Ihre Organisation eine Richtlinie hat, die die Verwendung von Images blockiert, die nicht innerhalb der Organisation gehostet werden.

Sie können einen Konsolenagenten manuell mithilfe der manuellen Installationsmethode bereitstellen, Cloud Volumes ONTAP muss jedoch auch Bilder aus dem NetApp -Projekt abrufen. Sie müssen eine Zulassungsliste angeben, um einen Konsolenagenten und Cloud Volumes ONTAP bereitzustellen.

Bereitstellen eines Konsolenagenten

Der Benutzer, der einen Konsolenagenten bereitstellt, muss auf ein Image verweisen können, das in der Projekt-ID *netapp-cloudmanager* und der Projektnummer *14190056516* gehostet wird.

Bereitstellen von Cloud Volumes ONTAP

- Das Konsolendienstkonto muss auf ein Image verweisen, das in der Projekt-ID *netapp-cloudmanager* und der Projektnummer *14190056516* aus dem Dienstprojekt gehostet wird.
- Das Dienstkonto für den standardmäßigen Google APIs-Dienstagenten muss auf ein in der Projekt-ID *netapp-cloudmanager* gehostetes Bild und die Projektnummer *14190056516* aus dem Dienstprojekt verweisen.

Beispiele für die Regeln, die zum Abrufen dieser Bilder mit VPC Service Controls erforderlich sind, sind unten definiert.

VPC Service Controls-Perimeterrichtlinien

Richtlinien ermöglichen Ausnahmen von den VPC-Dienststeuerungsregeln. Weitere Informationen zu Richtlinien finden Sie unter "Google Cloud VPC Service Controls Policy Dokumentation".

Um die von der Konsole benötigten Richtlinien festzulegen, navigieren Sie zu Ihrem VPC Service Controls Perimeter innerhalb Ihrer Organisation und fügen Sie die folgenden Richtlinien hinzu. Die Felder sollten mit den Optionen auf der Richtlinienseite „VPC Service Controls“ übereinstimmen. Beachten Sie auch, dass **alle** Regeln erforderlich sind und die **ODER**-Parameter im Regelsatz verwendet werden sollten.

Ingress-Regeln

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Service Project]
    Services =
        Service name: iam.googleapis.com
          Service methods: All actions
        Service name: compute.googleapis.com
          Service methods:All actions
```

ODER

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Host Project]
    Services =
        Service name: compute.googleapis.com
          Service methods: All actions
```

ODER

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
    Source > All sources allowed
To:
    Projects =
        [Service Project]
        [Host Project]
    Services =
        Service name: compute.googleapis.com
        Service methods: All actions
```

Ausgangsregeln

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
To:
    Projects =
        14190056516
    Service =
        Service name: compute.googleapis.com
        Service methods: All actions
```

Die oben angegebene Projektnummer ist das Projekt *netapp-cloudmanager*, das von NetApp zum Speichern von Images für den Konsolenagenten und für Cloud Volumes ONTAP verwendet wird.

Erstellen Sie ein Google Cloud-Dienstkonto für Cloud Volumes ONTAP

Cloud Volumes ONTAP erfordert aus zwei Gründen ein Google Cloud-Dienstkonto. Die erste ist, wenn Sie aktivieren"Daten-Tiering" um kalte Daten in kostengünstigen Objektspeicher in Google Cloud zu verschieben. Die zweite Möglichkeit besteht darin, dass Sie die "NetApp Backup and Recovery" um Volumes auf kostengünstigem Objektspeicher zu sichern.

Cloud Volumes ONTAP verwendet das Servicekonto, um auf einen Bucket für mehrstufige Daten und einen anderen Bucket für Backups zuzugreifen und diese zu verwalten.

Sie können ein Servicekonto einrichten und es für beide Zwecke verwenden. Das Dienstkonto muss über die Rolle **Storage Admin** verfügen.

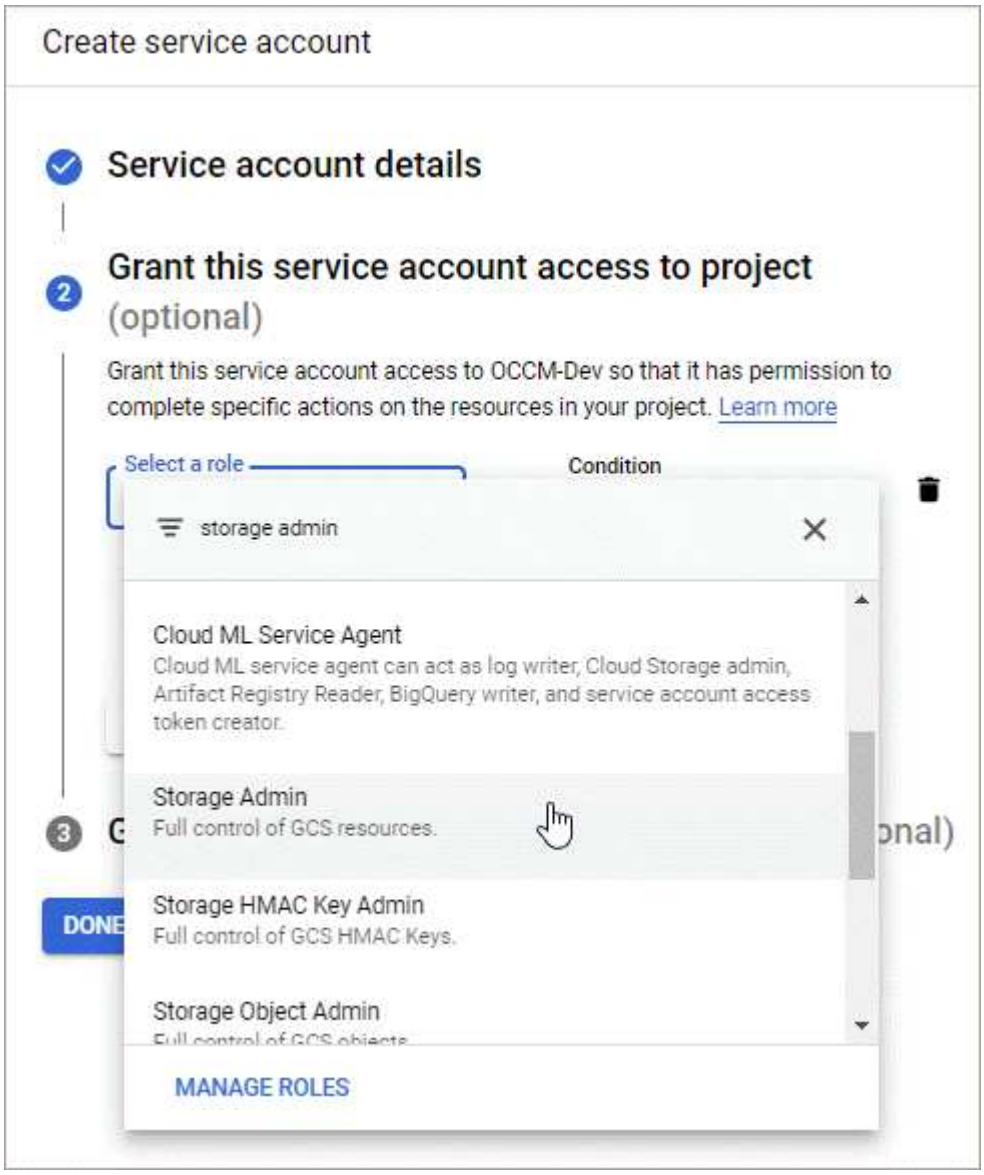
Schritte

1. In der Google Cloud Console "Gehen Sie zur Seite „Dienstkonten“".
2. Wählen Sie Ihr Projekt aus.

3. Klicken Sie auf **Dienstkonto erstellen** und geben Sie die erforderlichen Informationen ein.

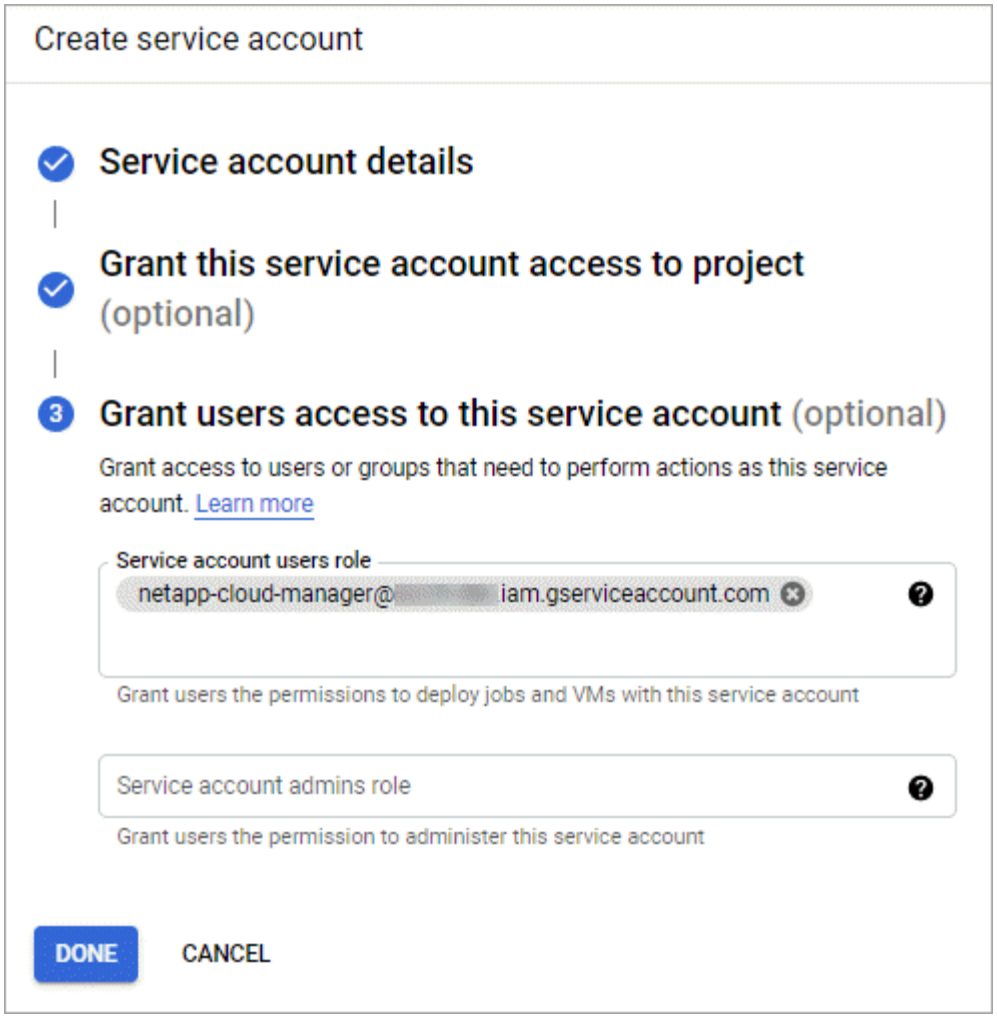
   a. **Servicekontodetails**: Geben Sie einen Namen und eine Beschreibung ein.

   b. **Diesem Dienstkonto Zugriff auf das Projekt gewähren**: Wählen Sie die Rolle **Speicheradministrator** aus.



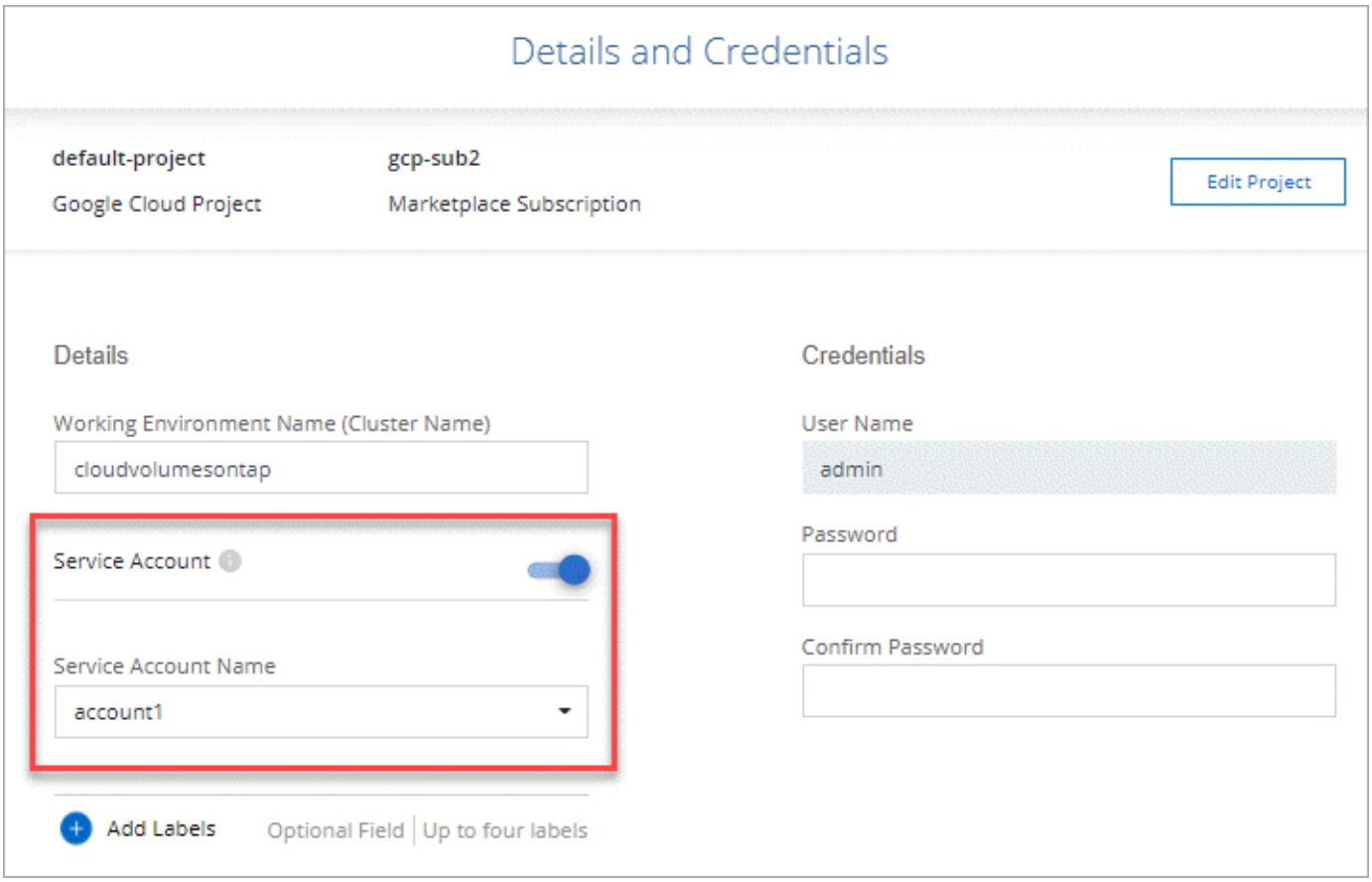
   c. **Benutzern Zugriff auf dieses Dienstkonto gewähren**: Fügen Sie das Dienstkonto des Konsolen-Agenten als *Dienstkontobenutzer* zu diesem neuen Dienstkonto hinzu.

      Dieser Schritt ist nur für die Datenschichtung erforderlich. Für die Sicherung und Wiederherstellung ist es nicht erforderlich.



Wie geht es weiter?

Sie müssen das Dienstkonto später auswählen, wenn Sie ein Cloud Volumes ONTAP -System erstellen.



Verwenden von kundenverwalteten Verschlüsselungsschlüsseln mit Cloud Volumes ONTAP

Während Google Cloud Storage Ihre Daten immer verschlüsselt, bevor sie auf die Festplatte geschrieben werden, können Sie mithilfe der APIs ein Cloud Volumes ONTAP -System erstellen, das *vom Kunden verwaltete Verschlüsselungsschlüssel* verwendet. Dies sind Schlüssel, die Sie mithilfe des Cloud Key Management Service in GCP generieren und verwalten.

Schritte

1. Stellen Sie sicher, dass das Dienstkonto des Konsolen-Agenten über die richtigen Berechtigungen auf Projektebene verfügt, und zwar in dem Projekt, in dem der Schlüssel gespeichert ist.

   Die Berechtigungen werden in der "die Dienstkontoberechtigungen standardmäßig" Dies gilt jedoch möglicherweise nicht, wenn Sie ein alternatives Projekt für den Cloud Key Management Service verwenden.

   Die Berechtigungen lauten wie folgt:

   ```
   - cloudkms.cryptoKeyVersions.useToEncrypt
   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.list
   ```

2. Stellen Sie sicher, dass das Dienstkonto für die "Google Compute Engine-Dienstagent" verfügt über Cloud KMS-Verschlüsselungs-/Entschlüsselungsberechtigungen für den Schlüssel.

   Der Name des Dienstkontos verwendet das folgende Format: „service-[service_project_number]@compute-system.iam.gserviceaccount.com“.

   "Google Cloud-Dokumentation: Verwenden von IAM mit Cloud KMS – Zuweisen von Rollen für eine Ressource"

3. Rufen Sie die ID des Schlüssels ab, indem Sie den Befehl „get“ für den `/gcp/vsa/metadata/gcp-encryption-keys` API-Aufruf oder durch Auswahl von „Ressourcennamen kopieren“ auf dem Schlüssel in der GCP-Konsole.
4. Wenn Sie vom Kunden verwaltete Verschlüsselungsschlüssel verwenden und Daten in den Objektspeicher verschieben, versucht die NetApp Console, dieselben Schlüssel zu verwenden, die zum Verschlüsseln der persistenten Datenträger verwendet werden. Sie müssen jedoch zunächst Google Cloud Storage-Buckets aktivieren, um die Schlüssel verwenden zu können:

   a. Suchen Sie den Google Cloud Storage-Dienstagenten, indem Sie den "Google Cloud-Dokumentation: Abrufen des Cloud Storage-Dienstagenten" .
   b. Navigieren Sie zum Verschlüsselungsschlüssel und weisen Sie dem Google Cloud Storage-Dienstagenten die Berechtigungen zum Verschlüsseln/Entschlüsseln von Cloud KMS zu.

   Weitere Informationen finden Sie unter "Google Cloud-Dokumentation: Verwenden von vom Kunden verwalteten Verschlüsselungsschlüsseln"

5. Verwenden Sie den Parameter „gcpEncryption“ bei Ihrer API-Anfrage, wenn Sie ein System erstellen.

   Beispiel

```
"gcpEncryptionParameters": {
    "key": "projects/project-1/locations/us-east4/keyRings/keyring-1/cryptoKeys/generatedkey1"
  }
```

Weitere Informationen finden Sie im "Dokumentation zur NetApp Console" Weitere Informationen zur Verwendung des Parameters „GcpEncryption“.

Einrichten der Lizenzierung für Cloud Volumes ONTAP in Google Cloud

Nachdem Sie entschieden haben, welche Lizenzierungsoption Sie mit Cloud Volumes ONTAP verwenden möchten, sind einige Schritte erforderlich, bevor Sie diese Lizenzierungsoption beim Erstellen eines neuen Systems auswählen können.

Freemium

Wählen Sie das Freemium-Angebot, um Cloud Volumes ONTAP mit bis zu 500 GiB bereitgestellter Kapazität kostenlos zu nutzen. "Erfahren Sie mehr über das Freemium-Angebot" .

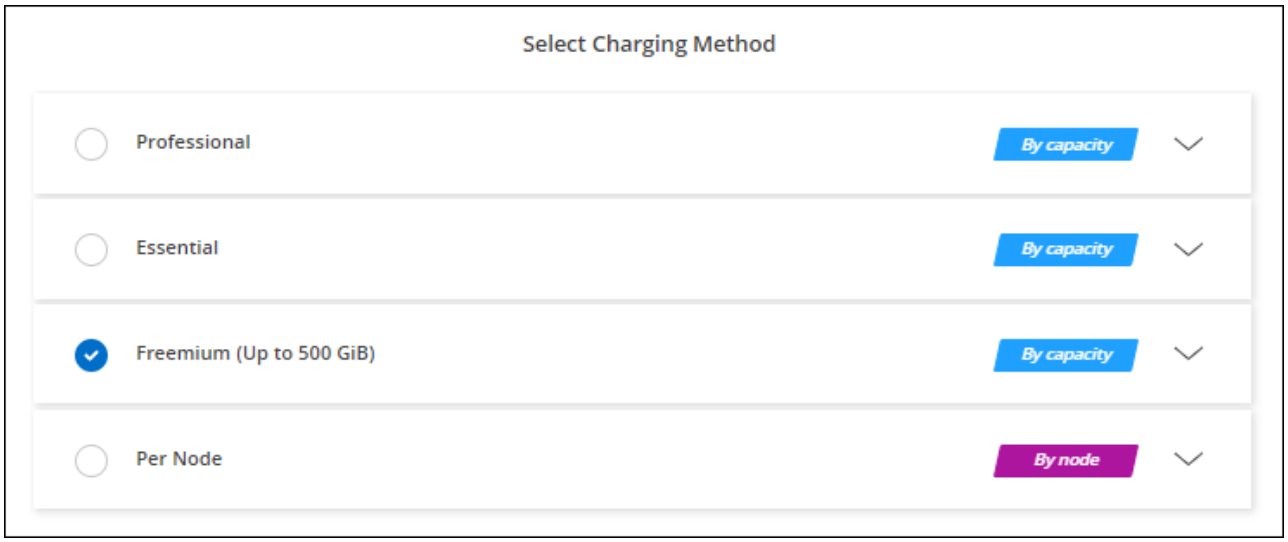
Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.

2. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten in der NetApp Console.
   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldeinformationen bearbeiten > Abonnement hinzufügen** und folgen Sie dann den Anweisungen, um das Pay-as-you-go-Angebot im Google Cloud Marketplace zu abonnieren.

      Ihnen werden keine Kosten über das Marktplatz-Abonnement berechnet, es sei denn, Sie überschreiten 500 GiB bereitgestellte Kapazität. Zu diesem Zeitpunkt wird das System automatisch auf das"Essentials-Paket" .

   b. Nachdem Sie zur Konsole zurückgekehrt sind, wählen Sie **Freemium** aus, wenn Sie die Seite mit den Abrechnungsmethoden erreichen.



"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in Google Cloud an" .

Kapazitätsbasierte Lizenz

Mit der kapazitätsbasierten Lizenzierung können Sie für Cloud Volumes ONTAP pro TiB Kapazität bezahlen. Die kapazitätsbasierte Lizenzierung ist in Form eines *Pakets* verfügbar: dem Essentials- oder Professional-Paket.

Die Pakete Essentials und Professional sind mit folgenden Verbrauchsmodellen bzw. Kaufoptionen erhältlich:

- Eine von NetApp erworbene Lizenz (Bring Your Own License (BYOL))
- Ein stündliches Pay-as-you-go-Abonnement (PAYGO) vom Google Cloud Marketplace
- Ein Jahresvertrag

"Erfahren Sie mehr über kapazitätsbasierte Lizenzierung" .

In den folgenden Abschnitten wird beschrieben, wie Sie mit jedem dieser Verbrauchsmodelle beginnen.

BYOL

Zahlen Sie im Voraus, indem Sie eine Lizenz (BYOL) von NetApp erwerben, um Cloud Volumes ONTAP -Systeme bei jedem Cloud-Anbieter bereitzustellen.

NetApp hat den Erwerb, die Verlängerung und die Erneuerung von BYOL-Lizenzen eingeschränkt. Weitere Informationen finden Sie unter "Eingeschränkte Verfügbarkeit der BYOL-Lizenzierung für Cloud Volumes ONTAP" .

Schritte

1. "Kontaktieren Sie den NetApp -Vertrieb, um eine Lizenz zu erhalten"
2. "Fügen Sie Ihr NetApp Support Site-Konto zur NetApp Console hinzu"

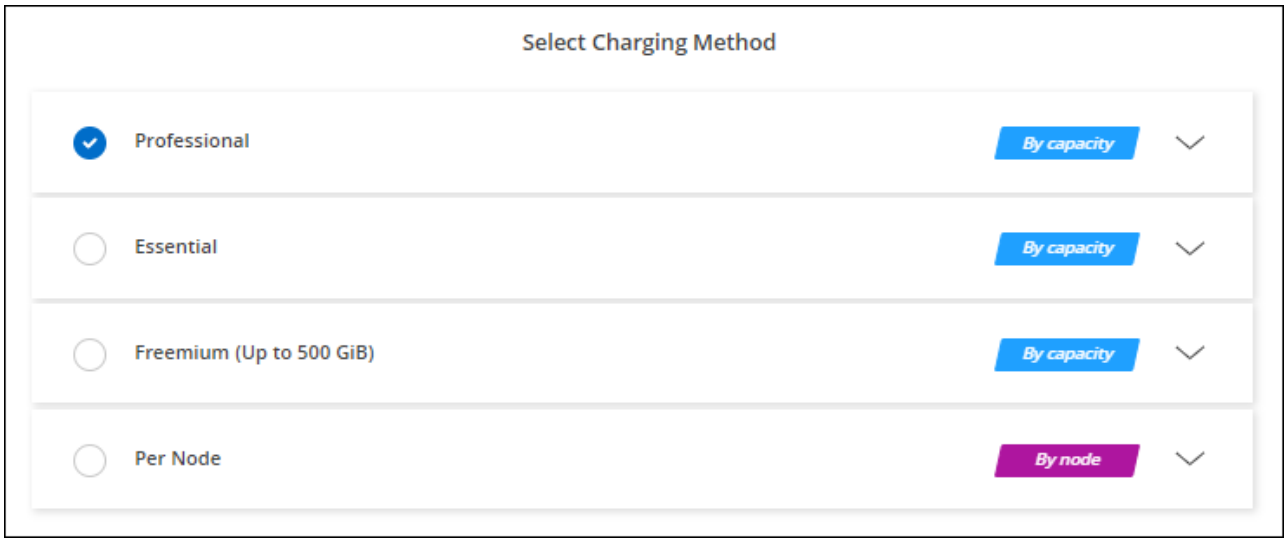
   Die Konsole fragt automatisch den Lizenzierungsdienst von NetApp ab, um Details zu den Lizenzen abzurufen, die mit Ihrem NetApp Support Site-Konto verknüpft sind. Wenn keine Fehler auftreten, fügt die Konsole die Lizenzen hinzu.

   Ihre Lizenz muss in der Konsole verfügbar sein, bevor Sie sie mit Cloud Volumes ONTAP verwenden können. Bei Bedarf können Sie"Fügen Sie die Lizenz manuell zur Konsole hinzu" .

3. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten.
   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldeinformationen bearbeiten > Abonnement hinzufügen** und folgen Sie dann den Anweisungen, um das Pay-as-you-go-Angebot im Google Cloud Marketplace zu abonnieren.

      Die von Ihnen bei NetApp erworbene Lizenz wird immer zuerst in Rechnung gestellt. Wenn Sie jedoch Ihre lizenzierte Kapazität überschreiten oder die Laufzeit Ihrer Lizenz abläuft, wird Ihnen der Stundensatz auf dem Marktplatz in Rechnung gestellt.

   b. Nachdem Sie zur Konsole zurückgekehrt sind, wählen Sie auf der Seite mit den Abrechnungsmethoden ein kapazitätsbasiertes Paket aus.



"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in Google Cloud an" .

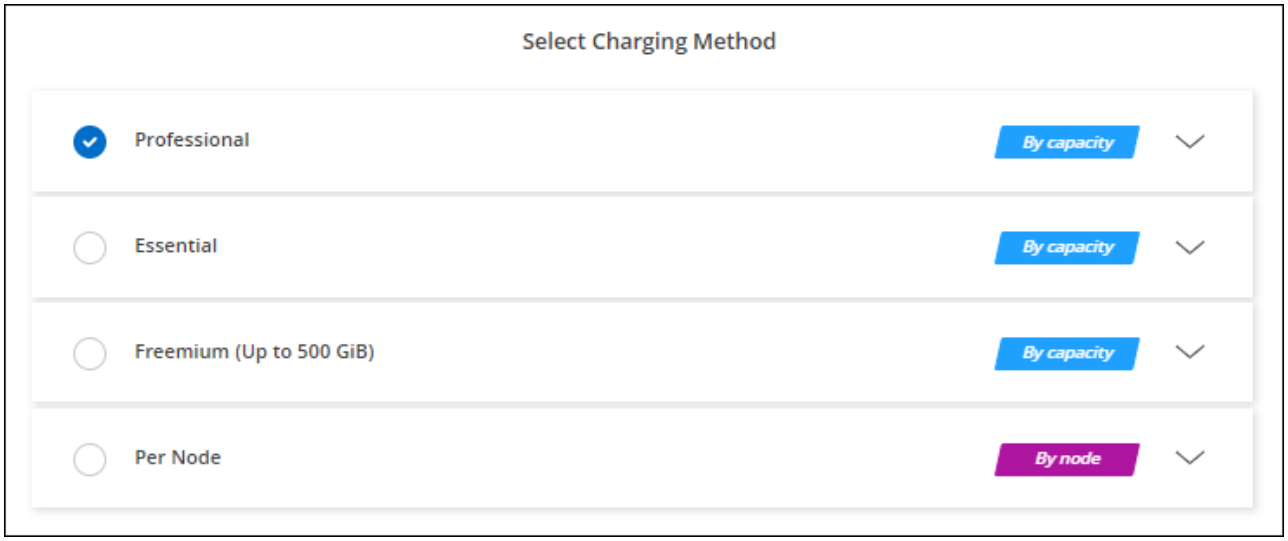
PAYGO-Abonnement

Zahlen Sie stundenweise, indem Sie das Angebot auf dem Marktplatz Ihres Cloud-Anbieters abonnieren.

Wenn Sie ein Cloud Volumes ONTAP -System erstellen, werden Sie von der Konsole aufgefordert, die im Google Cloud Marketplace verfügbare Vereinbarung zu abonnieren. Dieses Abonnement wird dann zum Aufladen mit dem System verknüpft. Sie können dasselbe Abonnement für zusätzliche Systeme verwenden.

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten.
   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldeinformationen bearbeiten > Abonnement hinzufügen** und folgen Sie dann den Anweisungen, um das Pay-as-you-go-Angebot im Google Cloud Marketplace zu abonnieren.
   b. Nachdem Sie zur Konsole zurückgekehrt sind, wählen Sie auf der Seite mit den Abrechnungsmethoden ein kapazitätsbasiertes Paket aus.



"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in Google Cloud an" .

Sie können die mit Ihren Konten verknüpften Google Cloud Marketplace-Abonnements auf der Seite „Einstellungen > Anmeldeinformationen“ verwalten. "Erfahren Sie, wie Sie Ihre Google Cloud-Anmeldeinformationen und -Abonnements verwalten"

Jahresvertrag

Bezahlen Sie Cloud Volumes ONTAP jährlich, indem Sie einen Jahresvertrag abschließen.

Schritte

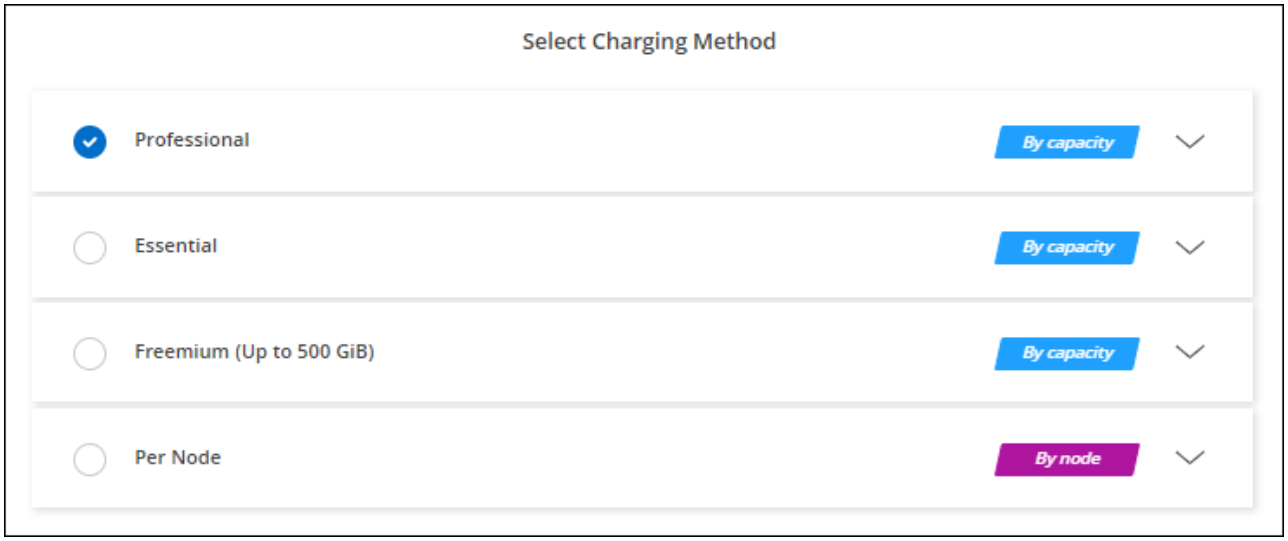
1. Wenden Sie sich an Ihren NetApp Vertriebsmitarbeiter, um einen Jahresvertrag abzuschließen.

   Der Vertrag ist als *privates* Angebot im Google Cloud Marketplace verfügbar.

   Nachdem NetApp Ihnen das private Angebot mitgeteilt hat, können Sie bei der Anmeldung im Google Cloud Marketplace während der Systemerstellung den Jahresplan auswählen.

2. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten.
   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldeinformationen bearbeiten > Abonnement hinzufügen** und folgen Sie dann den Anweisungen, um den Jahresplan im Google Cloud Marketplace zu abonnieren.
   b. Wählen Sie in Google Cloud den Jahresplan aus, der mit Ihrem Konto geteilt wurde, und klicken Sie dann auf **Abonnieren**.
   c. Nachdem Sie zur Konsole zurückgekehrt sind, wählen Sie auf der Seite mit den

Abrechnungsmethoden ein kapazitätsbasiertes Paket aus.



"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in Google Cloud an" .

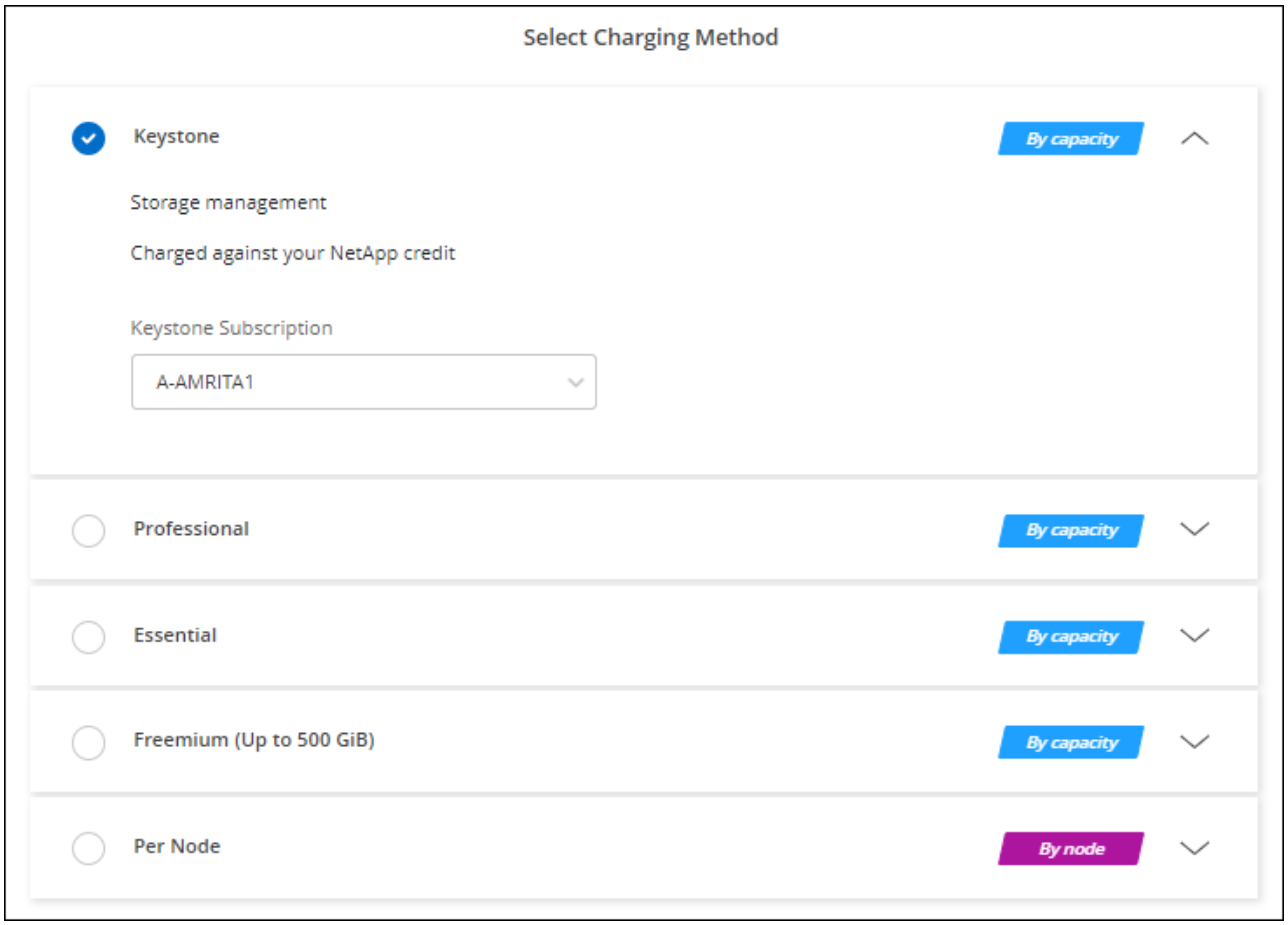
Keystone Abonnement

Bei einem Keystone -Abonnement handelt es sich um einen Abonnementdienst mit nutzungsabhängiger Bezahlung. "Erfahren Sie mehr über NetApp Keystone -Abonnements" .

Schritte

1. Wenn Sie noch kein Abonnement haben, "NetApp kontaktieren"
2. mailto:ng-keystone-success@netapp.com [Kontaktieren Sie NetApp], um Ihr Konsolenbenutzerkonto mit einem oder mehreren Keystone Abonnements zu autorisieren.
3. Nachdem NetApp Ihr Konto autorisiert hat,"Verknüpfen Sie Ihre Abonnements zur Verwendung mit Cloud Volumes ONTAP" .
4. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten.

    a. Wählen Sie die Abrechnungsmethode „Keystone -Abonnement“ aus, wenn Sie zur Auswahl einer Abrechnungsmethode aufgefordert werden.



"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in Google Cloud an" .

Knotenbasierte Lizenz

Eine knotenbasierte Lizenz ist die Lizenz der vorherigen Generation für Cloud Volumes ONTAP. Eine knotenbasierte Lizenz kann von NetApp (BYOL) erworben werden und ist nur in bestimmten Fällen für Lizenzverlängerungen verfügbar. Weitere Informationen finden Sie unter:

- "Ende der Verfügbarkeit knotenbasierter Lizenzen"
- "Ende der Verfügbarkeit von knotenbasierten Lizenzen"
- "Konvertieren Sie eine knotenbasierte Lizenz in eine kapazitätsbasierte Lizenz"

Starten Sie Cloud Volumes ONTAP in Google Cloud

Sie können Cloud Volumes ONTAP in einer Einzelknotenkonfiguration oder als HA-Paar in Google Cloud starten.

Bevor Sie beginnen

Bevor Sie beginnen, benötigen Sie Folgendes.

- Ein NetApp Console-Agent, der betriebsbereit ist.
  - Sie sollten über eine "Konsolenagent, der mit Ihrem System verknüpft ist" .

- "Sie sollten darauf vorbereitet sein, den Konsolenagenten immer laufen zu lassen" .
- Das mit dem Console-Agenten verknüpfte Dienstkonto "sollte über die erforderlichen Berechtigungen verfügen"

- Ein Verständnis der Konfiguration, die Sie verwenden möchten.

  Sie sollten sich vorbereitet haben, indem Sie eine Konfiguration ausgewählt und von Ihrem Administrator Informationen zum Google Cloud-Netzwerk eingeholt haben. Weitere Einzelheiten finden Sie unter"Planen Ihrer Cloud Volumes ONTAP Konfiguration" .

- Ein Verständnis dafür, was zum Einrichten der Lizenzierung für Cloud Volumes ONTAP erforderlich ist.

  "Erfahren Sie, wie Sie die Lizenzierung einrichten" .

- Google Cloud APIs sollten "in Ihrem Projekt aktiviert" :
  - Cloud Deployment Manager V2 API
  - Cloud Logging API
  - Cloud Resource Manager-API
  - Compute Engine-API
  - API für Identitäts- und Zugriffsverwaltung (IAM)

Starten Sie ein Einzelknotensystem in Google Cloud

Erstellen Sie in der NetApp Console ein System, um Cloud Volumes ONTAP in Google Cloud zu starten.

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Anweisungen.
3. **Wählen Sie einen Standort**: Wählen Sie **Google Cloud** und * Cloud Volumes ONTAP*.
4. Wenn Sie dazu aufgefordert werden, "Erstellen Sie einen Konsolenagenten" .
5. **Details und Anmeldeinformationen**: Wählen Sie ein Projekt aus, geben Sie einen Clusternamen an, wählen Sie optional ein Dienstkonto aus, fügen Sie optional Bezeichnungen hinzu und geben Sie dann die Anmeldeinformationen an.

   In der folgenden Tabelle werden die Felder beschrieben, für die Sie möglicherweise Anleitungen benötigen:

Feld	Beschreibung
Systemname	Die Konsole verwendet den Systemnamen, um sowohl das Cloud Volumes ONTAP -System als auch die Google Cloud VM-Instanz zu benennen. Wenn Sie diese Option auswählen, wird der Name auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet.
Dienstkontoname	Wenn Sie planen,"Daten-Tiering" oder "NetApp Backup and Recovery" mit Cloud Volumes ONTAP, dann müssen Sie **Servicekonto** aktivieren und ein Servicekonto auswählen, das über die vordefinierte Rolle „Storage Admin“ verfügt. "Erfahren Sie, wie Sie ein Dienstkonto erstellen" .

Feld	Beschreibung
Beschriftungen hinzufügen	Labels sind Metadaten für Ihre Google Cloud-Ressourcen. Die Konsole fügt die Labels dem Cloud Volumes ONTAP -System und den mit dem System verknüpften Google Cloud-Ressourcen hinzu. Sie können beim Erstellen eines Systems bis zu vier Beschriftungen über die Benutzeroberfläche hinzufügen und nach der Erstellung weitere hinzufügen. Beachten Sie, dass die API Sie beim Erstellen eines Systems nicht auf vier Labels beschränkt. Informationen zu Etiketten finden Sie im "Google Cloud-Dokumentation: Kennzeichnungsressourcen" .
Benutzername und Passwort	Dies sind die Anmeldeinformationen für das Cloud Volumes ONTAP Clusteradministratorkonto. Sie können diese Anmeldeinformationen verwenden, um über ONTAP System Manager oder die ONTAP CLI eine Verbindung zu Cloud Volumes ONTAP herzustellen. Behalten Sie den Standardbenutzernamen *admin* bei oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.
Projekt bearbeiten	Wählen Sie das Projekt aus, in dem Cloud Volumes ONTAP gespeichert werden soll. Das Standardprojekt ist das Projekt der Konsole. Wenn in der Dropdown-Liste keine weiteren Projekte angezeigt werden, haben Sie das Dienstkonto noch nicht mit anderen Projekten verknüpft. Gehen Sie zur Google Cloud Console, öffnen Sie den IAM-Dienst und wählen Sie das Projekt aus. Fügen Sie das Dienstkonto mit der Rolle, die Sie für die Console verwenden, zu diesem Projekt hinzu. Sie müssen diesen Schritt für jedes Projekt wiederholen. Dies ist das Dienstkonto, das Sie für die Konsole eingerichtet haben."wie auf dieser Seite beschrieben" . Klicken Sie auf **Abonnement hinzufügen**, um die ausgewählten Anmeldeinformationen einem Abonnement zuzuordnen. Um ein Cloud Volumes ONTAP -System mit nutzungsbasierter Bezahlung zu erstellen, müssen Sie ein Google Cloud-Projekt auswählen, das mit einem Abonnement für Cloud Volumes ONTAP aus dem Google Cloud-Marktplatz verknüpft ist. Siehe "Verknüpfen eines Marktplatz-Abonnements mit Google Cloud-Anmeldeinformationen" .

6. **Dienste**: Wählen Sie die Dienste aus, die Sie auf diesem System verwenden möchten. Um Backup und Recovery auszuwählen oder NetApp Cloud Tiering zu verwenden, müssen Sie in Schritt 3 das Servicekonto angegeben haben.

   Wenn Sie WORM und Daten-Tiering nutzen möchten, müssen Sie Backup und Recovery deaktivieren und ein Cloud Volumes ONTAP System mit Version 9.8 oder höher bereitstellen.

7. **Standort & Konnektivität**: Wählen Sie die Google Cloud-Region und -Zone für Ihr System, wählen Sie eine Firewall-Richtlinie und bestätigen Sie die Netzwerkverbindung zu Google Cloud storage für die Daten-Tiering.

   In der folgenden Tabelle werden die Felder beschrieben, für die Sie möglicherweise Anleitungen benötigen:

Feld	Beschreibung
Konnektivitätsüberprüfung	Um kalte Daten in einen Google Cloud Storage-Bucket zu verschieben, muss das Subnetz, in dem sich Cloud Volumes ONTAP befindet, für den privaten Google-Zugriff konfiguriert werden. Anweisungen hierzu finden Sie unter "Google Cloud-Dokumentation: Konfigurieren des privaten Google-Zugriffs" .
Generierte Firewall-Richtlinie	Wenn Sie die Firewall-Richtlinie von der Konsole erstellen lassen, müssen Sie auswählen, wie Sie den Datenverkehr zulassen: • Wenn Sie **Nur ausgewählte VPC** auswählen, ist der Quellfilter für eingehenden Datenverkehr der Subnetzbereich der ausgewählten VPC und der Subnetzbereich der VPC, in der sich der Konsolenagent befindet. Dies ist die empfohlene Option. • Wenn Sie **Alle VPCs** auswählen, ist der Quellfilter für eingehenden Datenverkehr der IP-Bereich 0.0.0.0/0.
Vorhandene Firewall-Richtlinie verwenden	Wenn Sie eine vorhandene Firewall-Richtlinie verwenden, stellen Sie sicher, dass diese die erforderlichen Regeln enthält:"Erfahren Sie mehr über Firewall-Regeln für Cloud Volumes ONTAP"

8. **Abrechnungsmethoden und NSS-Konto**: Geben Sie an, welche Abrechnungsoption Sie mit diesem System verwenden möchten, und geben Sie dann ein NetApp Support Site-Konto an:
   - "Erfahren Sie mehr über die Lizenzierungsoptionen für Cloud Volumes ONTAP"
   - "Erfahren Sie, wie Sie die Lizenzierung einrichten"
9. **Vorkonfigurierte Pakete**: Wählen Sie eines der Pakete aus, um schnell ein Cloud Volumes ONTAP-System bereitzustellen, oder klicken Sie auf **Eigene Konfiguration erstellen**. Die vorkonfigurierten Pakete variieren je nach gewählter Cloud Volumes ONTAP Version. Zum Beispiel zeigt die Console für Cloud Volumes ONTAP 9.18.1 und höher Pakete mit C3-VMs, einschließlich Hyperdisk Balanced-Festplatten, an. Sie können die Konfigurationen, wie IOPS- und Durchsatzparameter, basierend auf Ihren Workload-Anforderungen anpassen.

   Wenn Sie sich für eines der Pakete entscheiden, müssen Sie lediglich ein Volumen angeben und anschließend die Konfiguration prüfen und freigeben.
10. **Lizenzierung**: Ändern Sie die Cloud Volumes ONTAP -Version nach Bedarf und wählen Sie einen Maschinentyp aus.

    Wenn für eine ausgewählte Version ein neuerer Release Candidate, eine allgemeine Verfügbarkeit oder ein Patch-Release verfügbar ist, aktualisiert die Konsole das System beim Erstellen auf diese Version. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.13.1 auswählen und 9.13.1 P4 verfügbar ist. Das Update erfolgt nicht von einer Version zur nächsten, beispielsweise von 9.13 auf 9.14.
11. **Zugrunde liegende Speicherressourcen**: Wählen Sie Einstellungen für das anfängliche Aggregat: einen Datenträgertyp und die Größe für jeden Datenträger.

    Der Datenträgertyp ist für das ursprüngliche Volume. Sie können für nachfolgende Volumes einen anderen Datenträgertyp auswählen.

    Die Datenträgergröße gilt für alle Datenträger im anfänglichen Aggregat und für alle zusätzlichen Aggregate, die die Konsole erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der

erweiterten Zuordnungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.

Hilfe zur Auswahl von Datenträgertyp und -größe finden Sie unter"Dimensionieren Sie Ihr System in Google Cloud" .

12. **Flash-Cache, Schreibgeschwindigkeit und WORM**:

    a. Aktivieren Sie **Flash Cache** oder wählen Sie **Normal** oder **High** Schreibgeschwindigkeit, wenn Sie es benötigen.

       Erfahren Sie mehr über "Flash-Cache" und "Schreibgeschwindigkeit".

       Eine hohe Schreibgeschwindigkeit und eine höhere maximale Übertragungseinheit (MTU) von 8.896 Bytes sind über die Schreibgeschwindigkeitsoption **Hohe** verfügbar. Darüber hinaus erfordert die höhere MTU von 8.896 die Auswahl von VPC-1, VPC-2 und VPC-3 für die Bereitstellung. Weitere Informationen zu VPC-1, VPC-2 und VPC-3 finden Sie unter "Regeln für VPC-1, VPC-2 und VPC-3" .

    b. Aktivieren Sie bei Bedarf den WORM-Speicher (Write Once, Read Many).

       WORM kann nicht aktiviert werden, wenn die Datenschichtung für Cloud Volumes ONTAP Version 9.7 und darunter aktiviert wurde. Das Zurücksetzen oder Downgrade auf Cloud Volumes ONTAP 9.8 ist nach der Aktivierung von WORM und Tiering blockiert.

    "Erfahren Sie mehr über WORM-Speicher" .

    a. Wenn Sie den WORM-Speicher aktivieren, wählen Sie die Aufbewahrungsdauer aus.

13. **Daten-Tiering in Google Cloud Platform**: Wählen Sie, ob das Daten-Tiering für das anfängliche Aggregat aktiviert werden soll, wählen Sie eine Speicherklasse für die gestuften Daten und wählen Sie dann entweder ein Dienstkonto mit der vordefinierten Rolle „Speicheradministrator“ (erforderlich für Cloud Volumes ONTAP 9.7 oder höher) oder ein Google Cloud-Konto (erforderlich für Cloud Volumes ONTAP 9.6).

    Beachten Sie Folgendes:

    - Die Konsole richtet das Dienstkonto auf der Cloud Volumes ONTAP Instanz ein. Dieses Dienstkonto bietet Berechtigungen für die Datenschichtung in einem Google Cloud Storage-Bucket. Stellen Sie sicher, dass Sie das Dienstkonto des Konsolenagenten als Benutzer des Tiering-Dienstkontos hinzufügen, da Sie es sonst nicht aus der Konsole auswählen können.
    - Hilfe zum Hinzufügen eines Google Cloud-Kontos finden Sie unter "Einrichten und Hinzufügen von Google Cloud-Konten für Daten-Tiering mit 9.6" .
    - Sie können beim Erstellen oder Bearbeiten eines Volumes eine bestimmte Volume-Tiering-Richtlinie auswählen.
    - Wenn Sie die Datenschichtung deaktivieren, können Sie sie bei nachfolgenden Aggregaten wieder aktivieren, aber Sie müssen das System ausschalten und ein Dienstkonto aus der Google Cloud Console hinzufügen.

      "Weitere Informationen zum Daten-Tiering" .

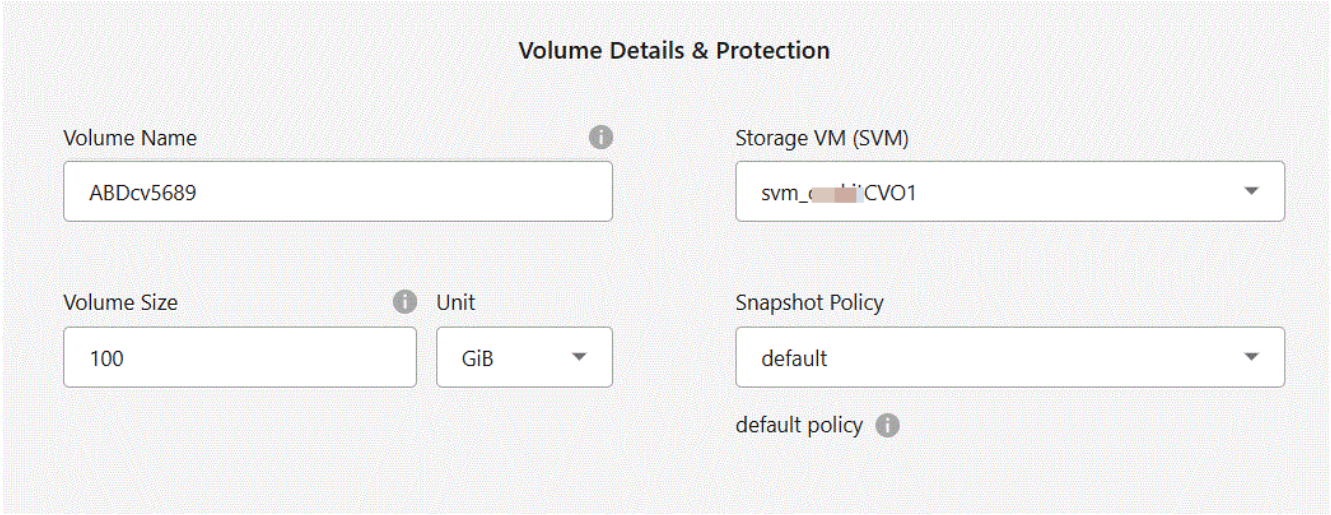
14. **Volume erstellen**: Geben Sie Details für das neue Volume ein oder klicken Sie auf **Überspringen**.

    "Erfahren Sie mehr über unterstützte Clientprotokolle und -versionen" .

Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Tabelle werden die Felder beschrieben, für die Sie möglicherweise Anleitungen benötigen:

Feld	Beschreibung
Größe	Die maximale Größe, die Sie eingeben können, hängt weitgehend davon ab, ob Sie Thin Provisioning aktivieren. Dadurch können Sie ein Volume erstellen, das größer ist als der ihm aktuell zur Verfügung stehende physische Speicher.
Zugriffskontrolle (nur für NFS)	Eine Exportrichtlinie definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt die Konsole einen Wert ein, der Zugriff auf alle Instanzen im Subnetz gewährt.
Berechtigungen und Benutzer/Gruppen (nur für CIFS)	Mit diesen Feldern können Sie die Zugriffsebene auf eine Freigabe für Benutzer und Gruppen steuern (auch als Zugriffskontrolllisten oder ACLs bezeichnet). Sie können lokale oder Domänen-Windows-Benutzer oder -Gruppen oder UNIX-Benutzer oder -Gruppen angeben. Wenn Sie einen Windows-Domänenbenutzernamen angeben, müssen Sie die Domäne des Benutzers im Format Domäne\Benutzername angeben.
Snapshot-Richtlinie	Eine Snapshot-Kopierrichtlinie gibt die Häufigkeit und Anzahl der automatisch erstellten NetApp Snapshot-Kopien an. Eine NetApp Snapshot-Kopie ist ein zeitpunktbezogenes Dateisystem-Image, das keine Auswirkungen auf die Leistung hat und nur minimalen Speicherplatz benötigt. Sie können die Standardrichtlinie oder keine auswählen. Für vorübergehende Daten können Sie „Keine“ auswählen, beispielsweise „tempdb“ für Microsoft SQL Server.
Erweiterte Optionen (nur für NFS)	Wählen Sie eine NFS-Version für das Volume aus: entweder NFSv3 oder NFSv4.
Initiatorgruppe und IQN (nur für iSCSI)	iSCSI-Speicherziele werden als LUNs (logische Einheiten) bezeichnet und Hosts als Standardblockgeräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Hostknotennamen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. iSCSI-Ziele stellen über Standard-Ethernet-Netzwerkadapter (NICs), TCP-Offload-Engine-Karten (TOE) mit Software-Initiatoren, konvergente Netzwerkadapter (CNAs) oder dedizierte Hostbusadapter (HBAs) eine Verbindung zum Netzwerk her und werden durch iSCSI-qualifizierte Namen (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt die Konsole automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volume erstellt haben, sodass keine Verwaltung erforderlich ist. Nachdem Sie das Volume erstellt haben,"Verwenden Sie den IQN, um von Ihren Hosts aus eine Verbindung zum LUN herzustellen" .

Das folgende Bild zeigt die erste Seite des Assistenten zur Volumeerstellung:



15. **CIFS-Setup**: Wenn Sie das CIFS-Protokoll gewählt haben, richten Sie einen CIFS-Server ein.

Feld	Beschreibung
DNS Primäre und sekundäre IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgelisteten DNS-Server müssen die Service Location Records (SRV) enthalten, die zum Auffinden der Active Directory-LDAP-Server und Domänencontroller für die Domäne erforderlich sind, der der CIFS-Server beitreten wird. Wenn Sie Google Managed Active Directory konfigurieren, kann auf AD standardmäßig mit der IP-Adresse 169.254.169.254 zugegriffen werden.
Beitretende Active Directory-Domäne	Der FQDN der Active Directory (AD)-Domäne, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zum Beitritt zur Domäne berechtigt sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
NetBIOS-Name des CIFS-Servers	Ein CIFS-Servername, der in der AD-Domäne eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domäne, die mit dem CIFS-Server verknüpft werden soll. Der Standardwert ist CN=Computers. Um Google Managed Microsoft AD als AD-Server für Cloud Volumes ONTAP zu konfigurieren, geben Sie in dieses Feld **OU=Computers,OU=Cloud** ein.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud-Dokumentation: Organisationseinheiten in Google Managed Microsoft AD"^]
DNS-Domäne	Die DNS-Domäne für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen ist die Domäne dieselbe wie die AD-Domäne.
NTP-Server	Wählen Sie **Active Directory-Domäne verwenden**, um einen NTP-Server mithilfe des Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Weitere Informationen finden Sie im "Dokumentation zur NetApp Console" für Details. Beachten Sie, dass Sie einen NTP-Server nur beim Erstellen eines CIFS-Servers konfigurieren können. Es ist nicht mehr konfigurierbar, nachdem Sie den CIFS-Server erstellt haben.

16. **Nutzungsprofil, Datenträgertyp und Tiering-Richtlinie**: Wählen Sie aus, ob Sie Speichereffizienzfunktionen aktivieren möchten, und ändern Sie bei Bedarf die Volume-Tiering-Richtlinie.

    Weitere Informationen finden Sie unter"Auswählen eines Volume-Nutzungsprofils" ,"Übersicht über Data Tiering" , Und "KB: Welche Inline-Speichereffizienzfunktionen werden mit CVO unterstützt?"

17. **Überprüfen und genehmigen**: Überprüfen und bestätigen Sie Ihre Auswahl.
    a. Überprüfen Sie die Details zur Konfiguration.
    b. Klicken Sie auf **Weitere Informationen**, um Details zum Support und den Google Cloud-Ressourcen anzuzeigen, die über die Konsole erworben werden.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie auf **Los**.

Ergebnis

Die Konsole stellt das Cloud Volumes ONTAP -System bereit. Sie können den Fortschritt auf der Seite **Audit** verfolgen.

Wenn bei der Bereitstellung des Cloud Volumes ONTAP Systems Probleme auftreten, überprüfen Sie die Fehlermeldung. Sie können auch das System auswählen und auf **Umgebung neu erstellen** klicken.

Weitere Hilfe finden Sie unter "NetApp Cloud Volumes ONTAP Unterstützung" .

Nach Abschluss

- Wenn Sie eine CIFS-Freigabe bereitgestellt haben, erteilen Sie Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner und stellen Sie sicher, dass diese Benutzer auf die Freigabe zugreifen und eine Datei erstellen können.
- Wenn Sie Kontingente auf Volumes anwenden möchten, verwenden Sie ONTAP System Manager oder die ONTAP CLI.

  Mithilfe von Kontingenten können Sie den Speicherplatz und die Anzahl der von einem Benutzer, einer Gruppe oder einem Qtree verwendeten Dateien beschränken oder verfolgen.

> Nach Abschluss des Bereitstellungsprozesses dürfen die systemgenerierten Cloud Volumes ONTAP Konfigurationen im Google Cloud-Portal, wie zum Beispiel die System-Tags und die in den Google Cloud-Ressourcen festgelegten Labels, nicht verändert werden. Jegliche Änderungen an diesen Konfigurationen können zu unerwartetem Verhalten oder Datenverlust führen.

Starten Sie ein HA-Paar in Google Cloud

Erstellen Sie in der Konsole ein System, um Cloud Volumes ONTAP in Google Cloud zu starten.

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Klicken Sie auf der Seite **Systeme** auf **Speicher > System** und folgen Sie den Anweisungen.
3. **Wählen Sie einen Standort**: Wählen Sie **Google Cloud** und * Cloud Volumes ONTAP HA*.
4. **Details und Anmeldeinformationen**: Wählen Sie ein Projekt aus, geben Sie einen Clusternamen an, wählen Sie optional ein Dienstkonto aus, fügen Sie optional Bezeichnungen hinzu und geben Sie dann die Anmeldeinformationen an.

In der folgenden Tabelle werden die Felder beschrieben, für die Sie möglicherweise Anleitungen benötigen:

Feld	Beschreibung
Systemname	Die Konsole verwendet den Systemnamen, um sowohl das Cloud Volumes ONTAP -System als auch die Google Cloud VM-Instanz zu benennen. Wenn Sie diese Option auswählen, wird der Name auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet.
Dienstkontoname	Wenn Sie die"NetApp Cloud Tiering" oder "Sicherung und Wiederherstellung" Dienste müssen Sie den Schalter **Dienstkonto** aktivieren und dann das Dienstkonto auswählen, das über die vordefinierte Rolle „Speicheradministrator“ verfügt.
Beschriftungen hinzufügen	Labels sind Metadaten für Ihre Google Cloud-Ressourcen. Die Konsole fügt die Labels dem Cloud Volumes ONTAP -System und den mit dem System verknüpften Google Cloud-Ressourcen hinzu. Sie können beim Erstellen eines Systems bis zu vier Beschriftungen über die Benutzeroberfläche hinzufügen und nach der Erstellung weitere hinzufügen. Beachten Sie, dass die API Sie beim Erstellen eines Systems nicht auf vier Labels beschränkt. Informationen zu Etiketten finden Sie unter "Google Cloud-Dokumentation: Kennzeichnungsressourcen" .
Benutzername und Passwort	Dies sind die Anmeldeinformationen für das Cloud Volumes ONTAP Clusteradministratorkonto. Sie können diese Anmeldeinformationen verwenden, um über ONTAP System Manager oder die ONTAP CLI eine Verbindung zu Cloud Volumes ONTAP herzustellen. Behalten Sie den Standardbenutzernamen *admin* bei oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.
Projekt bearbeiten	Wählen Sie das Projekt aus, in dem Cloud Volumes ONTAP residieren soll. Wenn in der Dropdown-Liste keine weiteren Projekte angezeigt werden, haben Sie das Dienstkonto noch nicht mit anderen Projekten verknüpft. Gehen Sie zur Google Cloud Console, öffnen Sie den IAM-Dienst und wählen Sie das Projekt aus. Fügen Sie das Dienstkonto mit der Rolle, die Sie für die Console verwenden, zu diesem Projekt hinzu. Sie müssen diesen Schritt für jedes Projekt wiederholen. Dies ist das Dienstkonto, das Sie für die Konsole eingerichtet haben."wie auf dieser Seite beschrieben" . Klicken Sie auf **Abonnement hinzufügen**, um die ausgewählten Anmeldeinformationen einem Abonnement zuzuordnen. Um ein Cloud Volumes ONTAP -System mit nutzungsbasierter Bezahlung zu erstellen, müssen Sie ein Google Cloud-Projekt auswählen, das mit einem Abonnement für Cloud Volumes ONTAP aus dem Google Cloud Marketplace verknüpft ist. Siehe "Verknüpfen eines Marktplatz-Abonnements mit Google Cloud-Anmeldeinformationen" .

5. **Dienste**: Wählen Sie die Dienste aus, die Sie auf diesem System verwenden möchten. Um „Backup und Wiederherstellung“ auszuwählen oder NetApp Cloud Tiering zu verwenden, müssen Sie in Schritt 3 das Dienstkonto angegeben haben.

Wenn Sie WORM und Daten-Tiering nutzen möchten, müssen Sie Backup und Recovery deaktivieren und ein Cloud Volumes ONTAP System mit Version 9.8 oder höher bereitstellen.

6. **HA-Bereitstellungsmodelle**: Wählen Sie mehrere Zonen (empfohlen) oder eine einzelne Zone für die HA-Konfiguration. Wählen Sie dann eine Region und eine Zone aus.

   "Erfahren Sie mehr über HA-Bereitstellungsmodelle" .

7. **Konnektivität**: Wählen Sie vier verschiedene VPCs für die HA-Konfiguration, ein Subnetz in jedem VPC und dann eine Firewall-Richtlinie aus.

   "Erfahren Sie mehr über die Netzwerkanforderungen" .

   In der folgenden Tabelle werden die Felder beschrieben, für die Sie möglicherweise Anleitungen benötigen:

Feld	Beschreibung
Generierte Richtlinie	Wenn Sie die Firewall-Richtlinie von der Konsole erstellen lassen, müssen Sie auswählen, wie Sie den Datenverkehr zulassen: • Wenn Sie **Nur ausgewählte VPC** auswählen, ist der Quellfilter für eingehenden Datenverkehr der Subnetzbereich der ausgewählten VPC und der Subnetzbereich der VPC, in der sich der Konsolenagent befindet. Dies ist die empfohlene Option. • Wenn Sie **Alle VPCs** auswählen, ist der Quellfilter für eingehenden Datenverkehr der IP-Bereich 0.0.0.0/0.
Vorhandene verwenden	Wenn Sie eine vorhandene Firewall-Richtlinie verwenden, stellen Sie sicher, dass diese die erforderlichen Regeln enthält. "Erfahren Sie mehr über Firewall-Regeln für Cloud Volumes ONTAP" .

8. **Abrechnungsmethoden und NSS-Konto**: Geben Sie an, welche Abrechnungsoption Sie mit diesem System verwenden möchten, und geben Sie dann ein NetApp Support Site-Konto an.
   - "Erfahren Sie mehr über die Lizenzierungsoptionen für Cloud Volumes ONTAP" .
   - "Erfahren Sie, wie Sie die Lizenzierung einrichten" .
9. **Vorkonfigurierte Pakete**: Wählen Sie eines der Pakete aus, um schnell ein Cloud Volumes ONTAP System bereitzustellen, oder klicken Sie auf **Meine eigene Konfiguration erstellen**.

   Wenn Sie sich für eines der Pakete entscheiden, müssen Sie lediglich ein Volumen angeben und anschließend die Konfiguration prüfen und freigeben.

10. **Lizenzierung**: Ändern Sie die Cloud Volumes ONTAP -Version nach Bedarf und wählen Sie einen Maschinentyp aus.

    Wenn für die ausgewählte Version ein neuerer Release Candidate, eine allgemeine Verfügbarkeit oder ein Patch-Release verfügbar ist, aktualisiert die Konsole das System beim Erstellen auf diese Version. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.13.1 auswählen und 9.13.1 P4 verfügbar ist. Das Update erfolgt nicht von einer Version zur nächsten, beispielsweise von 9.13 auf 9.14.

11. **Zugrunde liegende Speicherressourcen**: Wählen Sie Einstellungen für das anfängliche Aggregat: einen Datenträgertyp und die Größe für jeden Datenträger.

    Der Datenträgertyp ist für das ursprüngliche Volume. Sie können für nachfolgende Volumes einen anderen Datenträgertyp auswählen.

    Die Datenträgergröße gilt für alle Datenträger im anfänglichen Aggregat und für alle zusätzlichen Aggregate, die die Konsole erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der erweiterten Zuordnungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.

    Hilfe zur Auswahl von Datenträgertyp und -größe finden Sie unter"Dimensionieren Sie Ihr System in Google Cloud" .

12. **Flash-Cache, Schreibgeschwindigkeit und WORM**:

    a. Aktivieren Sie **Flash Cache** oder wählen Sie **Normal** oder **High** Schreibgeschwindigkeit, wenn Sie es benötigen.

       Erfahren Sie mehr über "Flash-Cache" und "Schreibgeschwindigkeit".

       > ⓘ Eine hohe Schreibgeschwindigkeit und eine höhere maximale Übertragungseinheit (MTU) von 8.896 Bytes sind über die Schreibgeschwindigkeitsoption **Hohe** mit den Instance-Typen n2-standard-16, n2-standard-32, n2-standard-48 und n2-standard-64 verfügbar. Darüber hinaus erfordert die höhere MTU von 8.896 die Auswahl von VPC-1, VPC-2 und VPC-3 für die Bereitstellung. Eine hohe Schreibgeschwindigkeit und eine MTU von 8.896 sind funktionsabhängig und können innerhalb einer konfigurierten Instanz nicht einzeln deaktiviert werden. Weitere Informationen zu VPC-1, VPC-2 und VPC-3 finden Sie unter "Regeln für VPC-1, VPC-2 und VPC-3" .

    b. Aktivieren Sie bei Bedarf den WORM-Speicher (Write Once, Read Many).

       WORM kann nicht aktiviert werden, wenn die Datenschichtung für Cloud Volumes ONTAP Version 9.7 und darunter aktiviert wurde. Das Zurücksetzen oder Downgrade auf Cloud Volumes ONTAP 9.8 ist nach der Aktivierung von WORM und Tiering blockiert.

    "Erfahren Sie mehr über WORM-Speicher" .

    a. Wenn Sie den WORM-Speicher aktivieren, wählen Sie die Aufbewahrungsdauer aus.

13. **Daten-Tiering in Google Cloud**: Wählen Sie, ob Sie das Daten-Tiering für das anfängliche Aggregat aktivieren möchten, wählen Sie eine Speicherklasse für die gestuften Daten und wählen Sie dann ein Dienstkonto mit der vordefinierten Rolle „Speicheradministrator“.

    Beachten Sie Folgendes:

    - Die Konsole richtet das Dienstkonto auf der Cloud Volumes ONTAP Instanz ein. Dieses Dienstkonto bietet Berechtigungen für die Datenschichtung in einem Google Cloud Storage-Bucket. Stellen Sie sicher, dass Sie das Dienstkonto des Konsolenagenten als Benutzer des Tiering-Dienstkontos hinzufügen, da Sie es sonst nicht aus der Konsole auswählen können.
    - Sie können beim Erstellen oder Bearbeiten eines Volumes eine bestimmte Volume-Tiering-Richtlinie auswählen.
    - Wenn Sie die Datenschichtung deaktivieren, können Sie sie bei nachfolgenden Aggregaten wieder aktivieren, aber Sie müssen das System ausschalten und ein Dienstkonto aus der Google Cloud

Console hinzufügen.

"Weitere Informationen zum Daten-Tiering" .

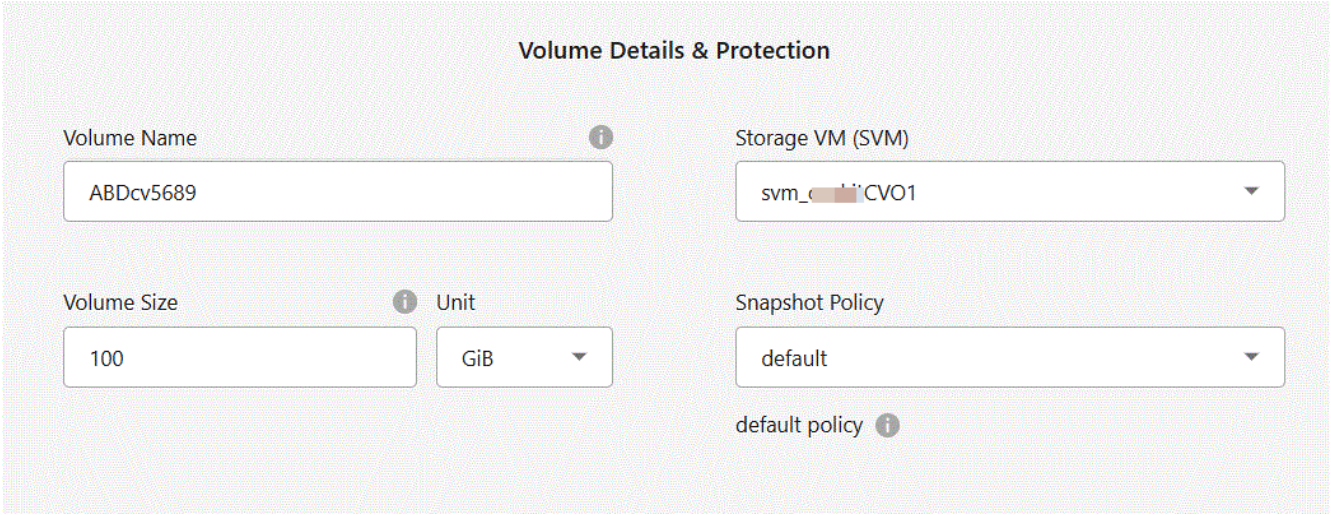
14. **Volume erstellen**: Geben Sie Details für das neue Volume ein oder klicken Sie auf **Überspringen**.

"Erfahren Sie mehr über unterstützte Clientprotokolle und -versionen" .

Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Tabelle werden die Felder beschrieben, für die Sie möglicherweise Anleitungen benötigen:

Feld	Beschreibung
Größe	Die maximale Größe, die Sie eingeben können, hängt weitgehend davon ab, ob Sie Thin Provisioning aktivieren. Dadurch können Sie ein Volume erstellen, das größer ist als der ihm aktuell zur Verfügung stehende physische Speicher.
Zugriffskontrolle (nur für NFS)	Eine Exportrichtlinie definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt die Konsole einen Wert ein, der Zugriff auf alle Instanzen im Subnetz gewährt.
Berechtigungen und Benutzer/Gruppen (nur für CIFS)	Mit diesen Feldern können Sie die Zugriffsebene auf eine Freigabe für Benutzer und Gruppen steuern (auch als Zugriffskontrolllisten oder ACLs bezeichnet). Sie können lokale oder Domänen-Windows-Benutzer oder -Gruppen oder UNIX-Benutzer oder -Gruppen angeben. Wenn Sie einen Windows-Domänenbenutzernamen angeben, müssen Sie die Domäne des Benutzers im Format Domäne\Benutzername angeben.
Snapshot-Richtlinie	Eine Snapshot-Kopierrichtlinie gibt die Häufigkeit und Anzahl der automatisch erstellten NetApp Snapshot-Kopien an. Eine NetApp Snapshot-Kopie ist ein zeitpunktbezogenes Dateisystem-Image, das keine Auswirkungen auf die Leistung hat und nur minimalen Speicherplatz benötigt. Sie können die Standardrichtlinie oder keine auswählen. Für vorübergehende Daten können Sie „Keine“ auswählen, beispielsweise „tempdb“ für Microsoft SQL Server.
Erweiterte Optionen (nur für NFS)	Wählen Sie eine NFS-Version für das Volume aus: entweder NFSv3 oder NFSv4.
Initiatorgruppe und IQN (nur für iSCSI)	iSCSI-Speicherziele werden als LUNs (logische Einheiten) bezeichnet und Hosts als Standardblockgeräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Hostknotennamen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. iSCSI-Ziele stellen über Standard-Ethernet-Netzwerkadapter (NICs), TCP-Offload-Engine-Karten (TOE) mit Software-Initiatoren, konvergente Netzwerkadapter (CNAs) oder dedizierte Hostbusadapter (HBAs) eine Verbindung zum Netzwerk her und werden durch iSCSI-qualifizierte Namen (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt die Konsole automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volume erstellt haben, sodass keine Verwaltung erforderlich ist. Nachdem Sie das Volume erstellt haben,"Verwenden Sie den IQN, um von Ihren Hosts aus eine Verbindung zum LUN herzustellen" .

Das folgende Bild zeigt die erste Seite des Assistenten zur Volumeerstellung:



15. **CIFS-Setup**: Wenn Sie das CIFS-Protokoll gewählt haben, richten Sie einen CIFS-Server ein.

Feld	Beschreibung
DNS Primäre und sekundäre IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgelisteten DNS-Server müssen die Service Location Records (SRV) enthalten, die zum Auffinden der Active Directory-LDAP-Server und Domänencontroller für die Domäne erforderlich sind, der der CIFS-Server beitreten wird. Wenn Sie Google Managed Active Directory konfigurieren, kann auf AD standardmäßig mit der IP-Adresse 169.254.169.254 zugegriffen werden.
Beitretende Active Directory-Domäne	Der FQDN der Active Directory (AD)-Domäne, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zum Beitritt zur Domäne berechtigt sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
NetBIOS-Name des CIFS-Servers	Ein CIFS-Servername, der in der AD-Domäne eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domäne, die mit dem CIFS-Server verknüpft werden soll. Der Standardwert ist CN=Computers. Um Google Managed Microsoft AD als AD-Server für Cloud Volumes ONTAP zu konfigurieren, geben Sie in dieses Feld **OU=Computers,OU=Cloud** ein.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud-Dokumentation: Organisationseinheiten in Google Managed Microsoft AD"^]
DNS-Domäne	Die DNS-Domäne für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen ist die Domäne dieselbe wie die AD-Domäne.
NTP-Server	Wählen Sie **Active Directory-Domäne verwenden**, um einen NTP-Server mithilfe des Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Weitere Informationen finden Sie im "Dokumentation zur NetApp Console" für Details. Beachten Sie, dass Sie einen NTP-Server nur beim Erstellen eines CIFS-Servers konfigurieren können. Es ist nicht mehr konfigurierbar, nachdem Sie den CIFS-Server erstellt haben.

16. **Nutzungsprofil, Datenträgertyp und Tiering-Richtlinie**: Wählen Sie aus, ob Sie Speichereffizienzfunktionen aktivieren möchten, und ändern Sie bei Bedarf die Volume-Tiering-Richtlinie.

    Weitere Informationen finden Sie unter"Auswählen eines Volume-Nutzungsprofils" ,"Übersicht über Data Tiering" , Und "KB: Welche Inline-Speichereffizienzfunktionen werden mit CVO unterstützt?"

17. **Überprüfen und genehmigen**: Überprüfen und bestätigen Sie Ihre Auswahl.
    a. Überprüfen Sie die Details zur Konfiguration.
    b. Klicken Sie auf **Weitere Informationen**, um Details zum Support und den Google Cloud-Ressourcen anzuzeigen, die über die Konsole erworben werden.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie auf **Los**.

Ergebnis

Die Konsole stellt das Cloud Volumes ONTAP -System bereit. Sie können den Fortschritt auf der Seite **Audit** verfolgen.

Wenn bei der Bereitstellung des Cloud Volumes ONTAP Systems Probleme auftreten, überprüfen Sie die Fehlermeldung. Sie können auch das System auswählen und auf **Umgebung neu erstellen** klicken.

Weitere Hilfe finden Sie unter "NetApp Cloud Volumes ONTAP Unterstützung" .

Nach Abschluss

- Wenn Sie eine CIFS-Freigabe bereitgestellt haben, erteilen Sie Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner und stellen Sie sicher, dass diese Benutzer auf die Freigabe zugreifen und eine Datei erstellen können.
- Wenn Sie Kontingente auf Volumes anwenden möchten, verwenden Sie ONTAP System Manager oder die ONTAP CLI.

  Mithilfe von Kontingenten können Sie den Speicherplatz und die Anzahl der von einem Benutzer, einer Gruppe oder einem Qtree verwendeten Dateien beschränken oder verfolgen.

> Nach Abschluss des Bereitstellungsprozesses dürfen die systemgenerierten Cloud Volumes ONTAP Konfigurationen im Google Cloud-Portal, wie zum Beispiel die System-Tags und die in den Google Cloud-Ressourcen festgelegten Labels, nicht verändert werden. Jegliche Änderungen an diesen Konfigurationen können zu unerwartetem Verhalten oder Datenverlust führen.

Weiterführende Links

- "Planen Ihrer Cloud Volumes ONTAP Konfiguration in Google Cloud"

Google Cloud Platform-Bildüberprüfung

Erfahren Sie, wie das Google Cloud-Image in Cloud Volumes ONTAP verifiziert wird

Die Google Cloud-Image-Verifizierung entspricht den erweiterten Sicherheitsanforderungen von NetApp . Am Skript zur Bildgenerierung wurden Änderungen vorgenommen, um das Bild unterwegs mit speziell für diese Aufgabe generierten privaten Schlüsseln zu signieren. Sie können die Integrität des Google Cloud-

Images überprüfen, indem Sie den signierten Digest und das öffentliche Zertifikat für Google Cloud verwenden, die über heruntergeladen werden können "NSS" für eine bestimmte Version.

Die Google Cloud-Image-Verifizierung wird auf der Cloud Volumes ONTAP -Softwareversion 9.13.0 oder höher unterstützt.

Konvertieren Sie das Google Cloud-Image in das Rohformat für Cloud Volumes ONTAP

Das Image, das zum Bereitstellen neuer Instanzen, Upgrades oder in vorhandenen Images verwendet wird, wird mit den Clients geteilt durch "die NetApp Support Site (NSS)" . Der signierte Digest und die Zertifikate können über das NSS-Portal heruntergeladen werden. Stellen Sie sicher, dass Sie den Digest und die Zertifikate für die richtige Version herunterladen, die dem vom NetApp Support freigegebenen Image entspricht. Beispielsweise verfügen 9.13.0-Images über einen signierten 9.13.0-Digest und Zertifikate, die auf NSS verfügbar sind.

Warum ist dieser Schritt notwendig?

Die Bilder aus der Google Cloud können nicht direkt heruntergeladen werden. Um das Bild anhand des signierten Digests und der Zertifikate zu überprüfen, benötigen Sie einen Mechanismus zum Vergleichen der beiden Dateien und zum Herunterladen des Bildes. Dazu müssen Sie das Image in ein disk.raw-Format exportieren/konvertieren und die Ergebnisse in einem Speicher-Bucket in Google Cloud speichern. Die Datei disk.raw wird dabei getarnt und gzippt.

Das Benutzer-/Dienstkonto benötigt Berechtigungen, um Folgendes auszuführen:

- Zugriff auf den Google-Speicherplatz
- In den Google Storage-Bucket schreiben
- Cloud-Build-Jobs erstellen (wird während des Exportvorgangs verwendet)
- Zugriff auf das gewünschte Bild
- Erstellen von Aufgaben zum Exportieren von Bildern

Um das Image zu überprüfen, muss es in ein disk.raw-Format konvertiert und dann heruntergeladen werden.

Verwenden Sie die Google Cloud-Befehlszeile, um das Google Cloud-Image zu exportieren

Die bevorzugte Methode zum Exportieren eines Bildes in den Cloud-Speicher ist die Verwendung des "Befehl „gcloud compute images export“" . Dieser Befehl nimmt das bereitgestellte Bild und konvertiert es in eine disk.raw-Datei, die getarnt und gzippt wird. Die generierte Datei wird unter der Ziel-URL gespeichert und kann anschließend zur Überprüfung heruntergeladen werden.

Der Benutzer/das Konto muss über Berechtigungen zum Zugriff auf und Schreiben in den gewünschten Bucket, zum Exportieren des Bilds und für Cloud-Builds (die von Google zum Exportieren des Bilds verwendet werden) verfügen, um diesen Vorgang auszuführen.

Exportieren Sie das Google Cloud-Image mit gcloud

Klicken Sie hier, um anzuzeigen

```
$ gcloud compute images export \
    --destination-uri DESTINATION_URI \
    --image IMAGE_NAME

# For our example:
$ gcloud compute images export \
    --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-
gcp-demo \
    --image example-user-20230120115139


## DEMO ##
# Step 1 - Optional: Checking access and listing objects in the
destination bucket
$ gsutil ls gs://example-user-export-image-bucket/

# Step 2 - Exporting the desired image to the bucket
$ gcloud compute images export --image example-user-export-image-demo
--destination-uri gs://example-user-export-image-bucket/export-
demo.tar.gz
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-
project/locations/us-central1/builds/xxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-
build/builds;region=us-central1/xxxxxxxxxxxx?project=xxxxxxxxxxxx].
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-
export-image-demo" from project "example-demo-project".
[image-export]: 2023-01-25T18:13:49Z Validating workflow
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-
export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "setup-disks"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "run-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "wait-for-inst-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "copy-image-object"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "delete-inst"
[image-export]: 2023-01-25T18:13:51Z Validation Complete
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-
project
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```
[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
```

```
StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'
value:'10'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Running export tool."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size
will most likely be much smaller."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Beginning export process..."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-
r88px/outs/image-export-export-disk.tar.gz."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),
total written size: 992 MiB (198 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),
total written size: 1.5 GiB (17 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished creating gzipped image of
\"/dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of
6."
```

```
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished export in  48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: <serial-output key:'target-size-gb'
value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-
25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-
export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step
"delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk"
(IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-
size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-
size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning
up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished
cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz


# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION
```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to
file://CVO_GCP_Signed_Digest.tar.gz
  Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s

Average throughput: 213.3MiB/s
$ ls -l
total 1565036
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44
CVO_GCP_Signed_Digest.tar.gz
```

ZIP-Dateien extrahieren

```
# Extracting files from the digest
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```

Weitere Informationen zum Exportieren eines Bildes über Google Cloud finden Sie im "Google Cloud-Dokument zum Exportieren eines Bildes" .

Bildsignaturprüfung

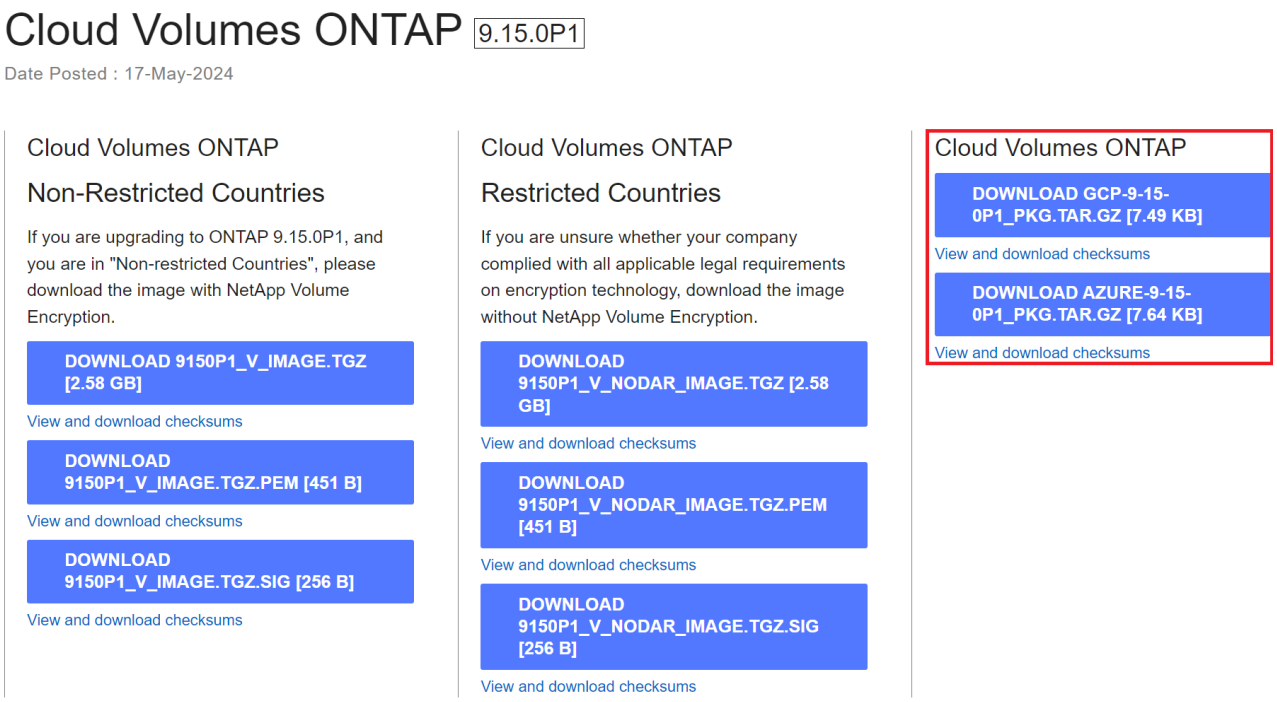
Google Cloud-Image-Signaturprüfung für Cloud Volumes ONTAP

Um das exportierte, von Google Cloud signierte Image zu überprüfen, müssen Sie die Image-Digest-Datei vom NSS herunterladen, um die Datei disk.raw und den Inhalt der Digest-Datei zu validieren.

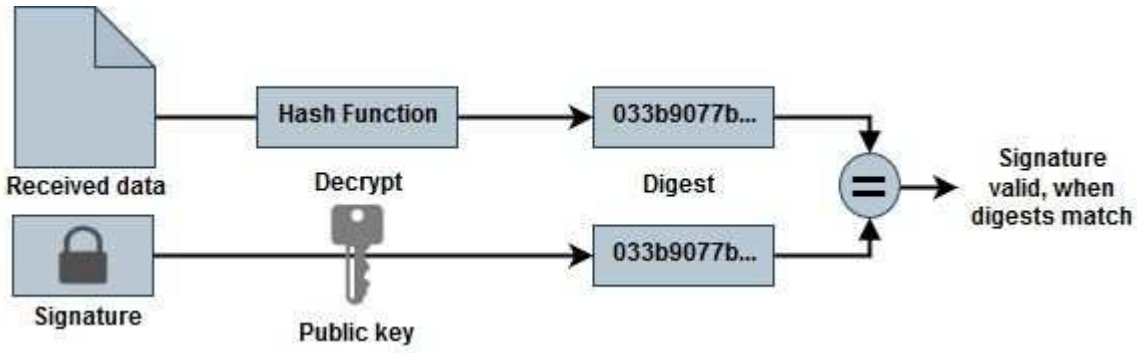
Zusammenfassung des Workflows zur signierten Bildüberprüfung

Nachfolgend finden Sie eine Übersicht über den Workflow-Prozess zur Überprüfung signierter Bilder in Google Cloud.

- Aus dem "NSS" , laden Sie das Google Cloud-Archiv mit den folgenden Dateien herunter:
  - Signierter Digest (.sig)
  - Zertifikat mit dem öffentlichen Schlüssel (.pem)
  - Zertifikatskette (.pem)



- Laden Sie die konvertierte disk.raw-Datei herunter
- Validieren Sie das Zertifikat mithilfe der Zertifikatskette
- Validieren Sie den signierten Digest mithilfe des Zertifikats, das den öffentlichen Schlüssel enthält
  - Entschlüsseln Sie den signierten Digest mit dem öffentlichen Schlüssel, um den Digest der Bilddatei zu extrahieren
  - Erstellen Sie einen Digest der heruntergeladenen disk.raw-Datei
  - Vergleichen Sie die beiden Digest-Dateien zur Validierung



Überprüfen Sie die Google Cloud-Image-Datei disk.raw für Cloud Volumes ONTAP mit OpenSSL

Sie können die von Google Cloud heruntergeladene Datei disk.raw mit dem Inhalt der Digest-Datei vergleichen, der über die "NSS" mit OpenSSL.

Die OpenSSL-Befehle zur Validierung des Images sind mit Linux-, macOS- und Windows-Computern kompatibel.

Schritte

1. Überprüfen Sie das Zertifikat mit OpenSSL.

Klicken Sie hier, um anzuzeigen

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OCSP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OCSP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem  -url ${ocsp_url} -resp_text
-respout resp.der
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
    Produced At: Jan 19 15:14:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5
    Cert Status: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
         f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
         af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
         1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
         d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
         cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
         1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
         15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
         8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
         e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
         5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
         b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
         9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
         24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
         5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
         2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
         17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
         d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
         15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
         44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
         cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
         e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
         6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
         77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:
```

```
         e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
         22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
         38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
         fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
         bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK
```

2. Legen Sie die heruntergeladene Datei disk.raw, die Signatur und die Zertifikate in einem Verzeichnis ab.
3. Extrahieren Sie den öffentlichen Schlüssel mithilfe von OpenSSL aus dem Zertifikat.
4. Entschlüsseln Sie die Signatur mit dem extrahierten öffentlichen Schlüssel und überprüfen Sie den Inhalt der heruntergeladenen Datei disk.raw.

Klicken Sie hier, um anzuzeigen

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```

Verwenden Sie Cloud Volumes ONTAP

Lizenzverwaltung

Verwalten Sie die kapazitätsbasierte Lizenzierung für Cloud Volumes ONTAP

Verwalten Sie Ihre kapazitätsbasierten Lizenzen über die NetApp Console, um sicherzustellen, dass Ihr NetApp Konto über genügend Kapazität für Ihre Cloud Volumes ONTAP Systeme verfügt.

Kapazitätsbasierte Lizenzen ermöglichen Ihnen die Zahlung für Cloud Volumes ONTAP pro TiB Kapazität.

Sie können kapazitätsbasierte Cloud Volumes ONTAP Lizenzen über die NetApp Console verwalten.

> Während die tatsächliche Nutzung und Messung der in der Konsole verwalteten Produkte und Dienste immer in GiB und TiB berechnet wird, werden die Begriffe GB/GiB und TB/TiB synonym verwendet. Dies spiegelt sich in den Cloud Marketplace-Angeboten, Preisangeboten, Angebotsbeschreibungen und anderen unterstützenden Dokumenten wider

"Erfahren Sie mehr über Cloud Volumes ONTAP -Lizenzen" .

So werden Lizenzen zur NetApp Console hinzugefügt

Nachdem Sie eine Lizenz von Ihrem NetApp Vertriebsmitarbeiter erworben haben, sendet Ihnen NetApp eine E-Mail mit der Seriennummer und weiteren Lizenzdetails.

In der Zwischenzeit fragt die Konsole automatisch den Lizenzierungsdienst von NetApp ab, um Details zu den Lizenzen zu erhalten, die mit Ihrem NetApp Support Site-Konto verknüpft sind. Wenn keine Fehler vorliegen, werden die Lizenzen hinzugefügt.

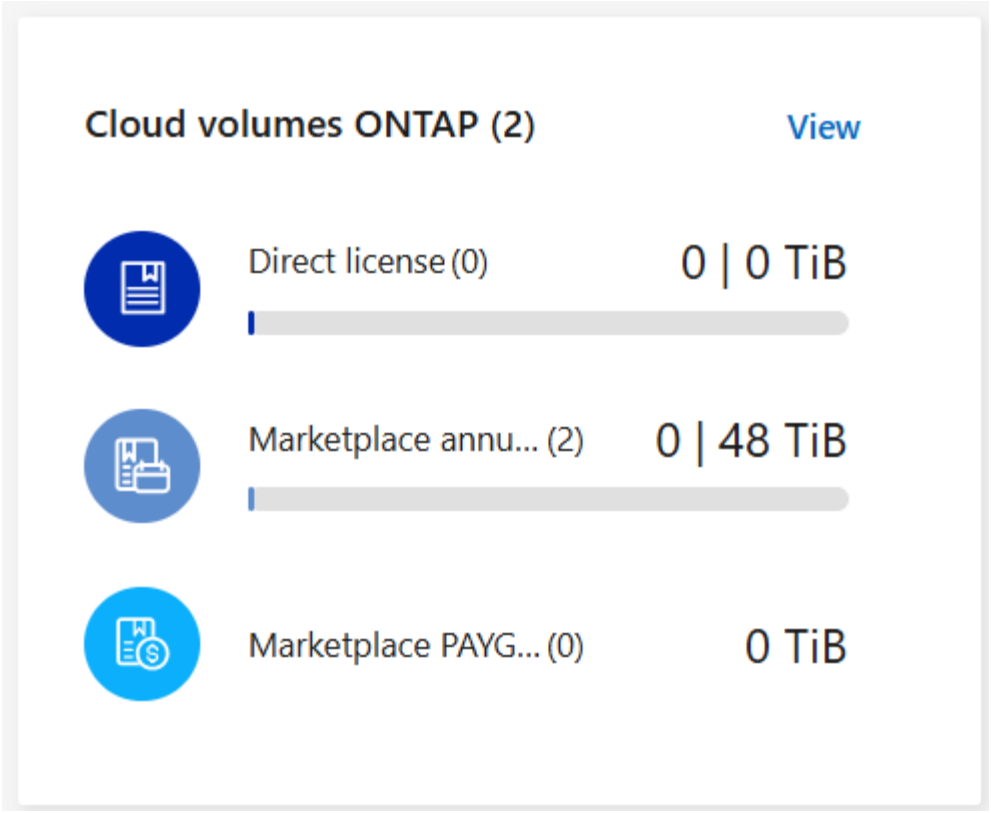
Wenn die Konsole die Lizenz nicht hinzufügen kann, müssen Sie sie manuell hinzufügen. Wenn der Konsolenagent beispielsweise an einem Ort ohne Internetzugang installiert ist, müssen Sie die Lizenzen selbst hinzufügen. "Erfahren Sie, wie Sie Ihrem Konto erworbene Lizenzen hinzufügen" .

Zeigen Sie die verbrauchte Kapazität in Ihrem Konto an

Die Konsole zeigt Ihnen die insgesamt verbrauchte Kapazität in Ihrem Konto und die verbrauchte Kapazität nach Lizenzpaket an. Auf diese Weise können Sie besser nachvollziehen, welche Kosten Ihnen in Rechnung gestellt werden und ob Sie zusätzliche Kapazität erwerben müssen.

Schritte

1. Wählen Sie im linken Navigationsbereich **Verwaltung > Licenses and subscriptions** aus.
2. Auf der Registerkarte **Übersicht** wird auf der Kachel „Cloud Volumes ONTAP“ die aktuell für Ihr Konto bereitgestellte Kapazität angezeigt.



- *Direktlizenz* ist die gesamte bereitgestellte Kapazität aller Cloud Volumes ONTAP Systeme in Ihrem NetApp Konto. Die Abrechnung erfolgt auf Grundlage der bereitgestellten Größe jedes Volumes, unabhängig vom lokalen, genutzten, gespeicherten oder effektiven Speicherplatz innerhalb des Volumes.
- *Jahresvertrag* ist die gesamte lizenzierte Kapazität (Bring Your Own License (BYOL) oder Marketplace-Vertrag), die Sie von NetApp erworben haben.
- *PAYGO* ist die gesamte bereitgestellte Kapazität mithilfe von Cloud-Marktplatz-Abonnements. Die Abrechnung über PAYGO erfolgt nur, wenn die verbrauchte Kapazität höher ist als die lizenzierte Kapazität oder wenn in der Konsole keine BYOL-Lizenz verfügbar ist.

3. Wählen Sie **Anzeigen**, um die verbrauchte Kapazität für jedes Ihrer Lizenzpakete anzuzeigen.
4. Wählen Sie die Registerkarte **Lizenzen** aus, um Details zu jeder von Ihnen erworbenen Paketlizenz anzuzeigen.

   Um die angezeigten Kapazitäten für das Essentials-Paket besser zu verstehen, sollten Sie mit der Funktionsweise des Ladevorgangs vertraut sein. "Informieren Sie sich über die Gebühren für das Essentials-Paket" .

5. Wählen Sie die Registerkarte **Abonnements** aus, um die verbrauchte Kapazität nach Lizenzverbrauchsmodell anzuzeigen. Diese Registerkarte umfasst sowohl PAYGO- als auch Jahresvertragslizenzen.

   Sie sehen nur die Abonnements, die mit der Organisation verknüpft sind, die Sie gerade anzeigen.

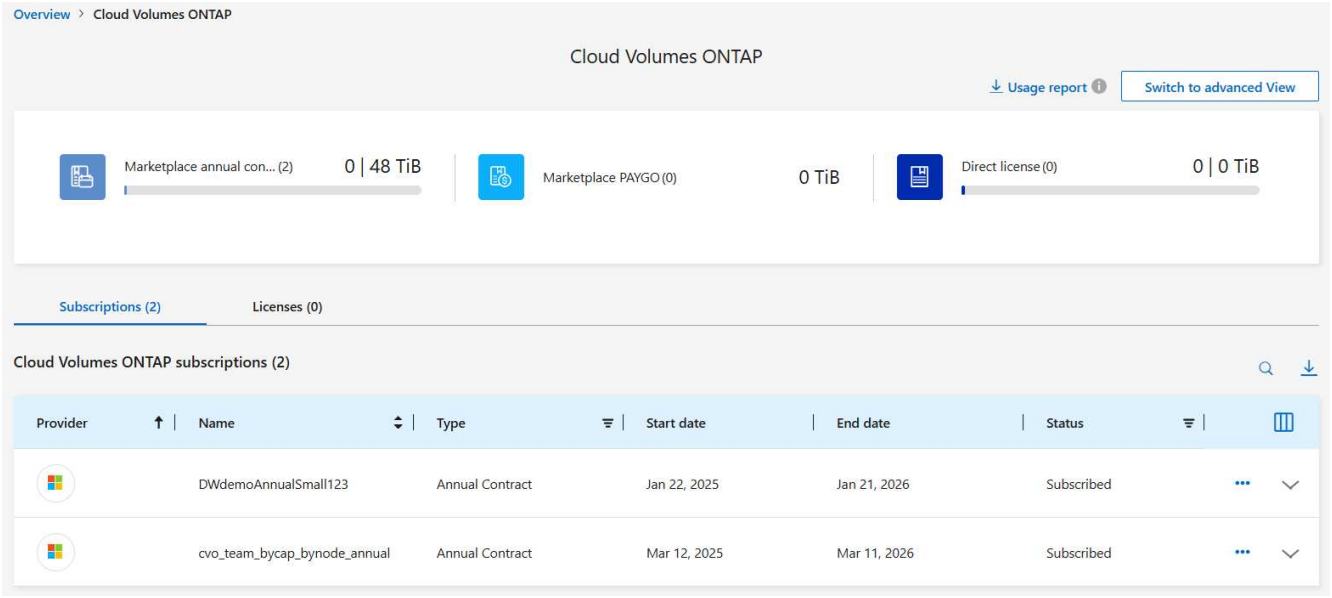
6. Während Sie die Informationen zu Ihren Abonnements anzeigen, können Sie mit den Details in der Tabelle interagieren. Erweitern Sie eine Zeile, um weitere Details anzuzeigen.
   - Wählen um auszuwählen, welche Spalten in der Tabelle angezeigt werden. Beachten Sie, dass die Spalten „Laufzeit“ und „Automatische Verlängerung“ nicht standardmäßig angezeigt werden. In der Spalte „Automatische Verlängerung“ werden nur Verlängerungsinformationen für Azure-Verträge

angezeigt.

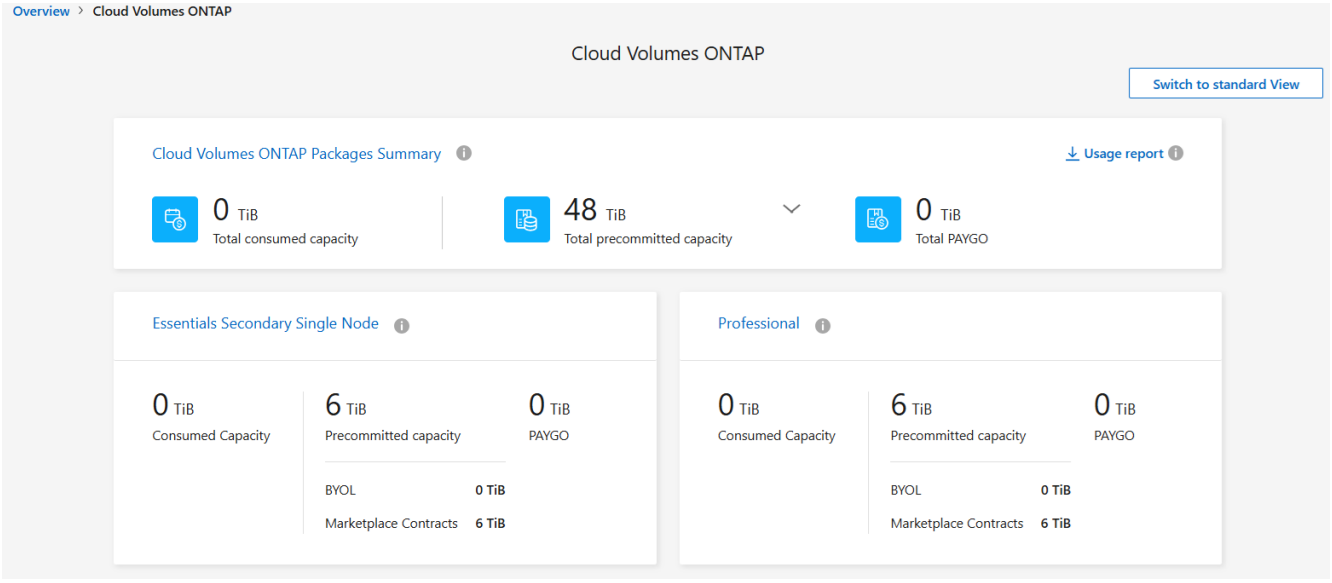
Paketdetails anzeigen

Sie können Details zur pro Paket genutzten Kapazität anzeigen, indem Sie auf der Cloud Volumes ONTAP -Seite in den Legacy-Modus wechseln.

1. Wählen Sie im linken Navigationsbereich **Verwaltung > Licenses and subscriptions** aus.
2. Auf der Registerkarte **Übersicht** wird auf der Kachel „Cloud Volumes ONTAP“ die aktuell für Ihr Konto bereitgestellte Kapazität angezeigt.
3. Wählen Sie **Anzeigen**, um die bereitgestellte Kapazität für jedes Ihrer Lizenzpakete anzuzeigen.
4. Wählen Sie **Zur erweiterten Ansicht wechseln**.



5. Zeigen Sie die Details des Pakets an, das Sie sehen möchten.



Lademethoden ändern

Die kapazitätsbasierte Lizenzierung ist in Form eines *Pakets* verfügbar. Wenn Sie ein Cloud Volumes ONTAP -System erstellen, können Sie je nach Ihren Geschäftsanforderungen aus mehreren Lizenzpaketen wählen. Sollten sich Ihre Anforderungen nach der Erstellung des Systems ändern, können Sie das Paket jederzeit ändern. Beispielsweise könnten Sie vom Essentials-Paket zum Professional-Paket wechseln.

"Erfahren Sie mehr über kapazitätsbasierte Lizenzpakete" .

Informationen zu diesem Vorgang

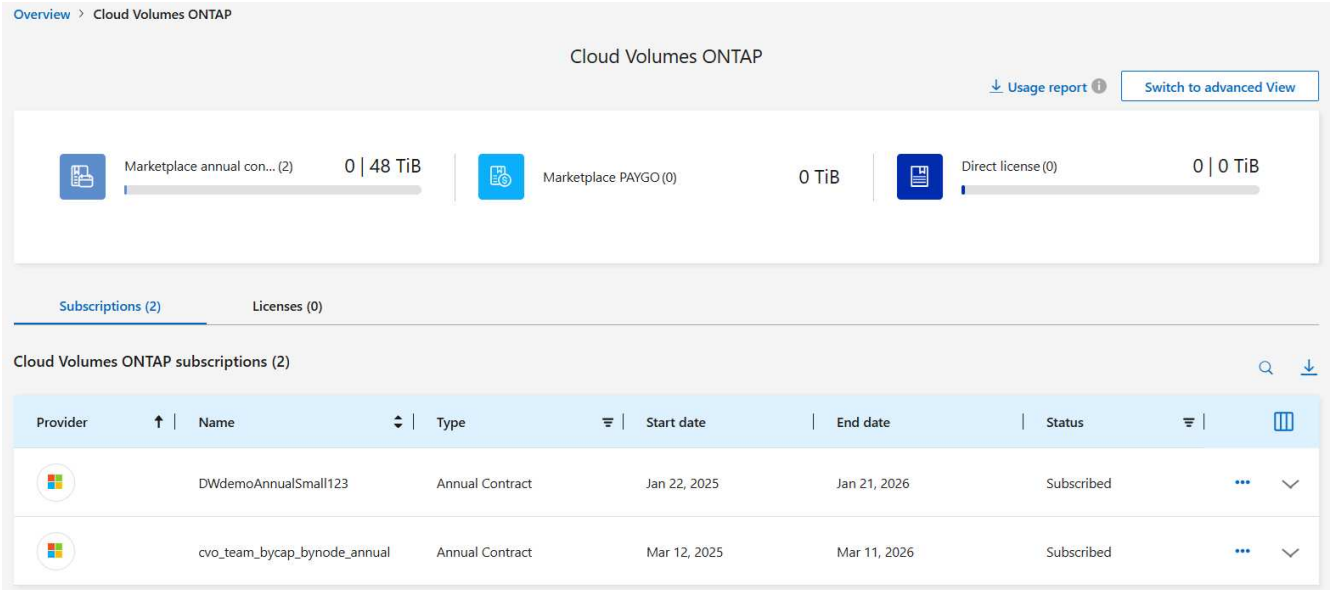
- Das Ändern der Abrechnungsmethode hat keinen Einfluss darauf, ob Ihnen die Kosten über eine von NetApp erworbene Lizenz (BYOL) oder über das Pay-as-you-go-Abonnement (PAYGO) Ihres Cloud-Anbieters berechnet werden.

  Die Konsole versucht immer zuerst, eine Lizenz abzurechnen. Wenn keine Lizenz verfügbar ist, wird dies über ein Marktplatz-Abonnement abgerechnet. Sie müssen ein BYOL-Abonnement nicht in ein Marktplatz-Abonnement umwandeln oder umgekehrt.

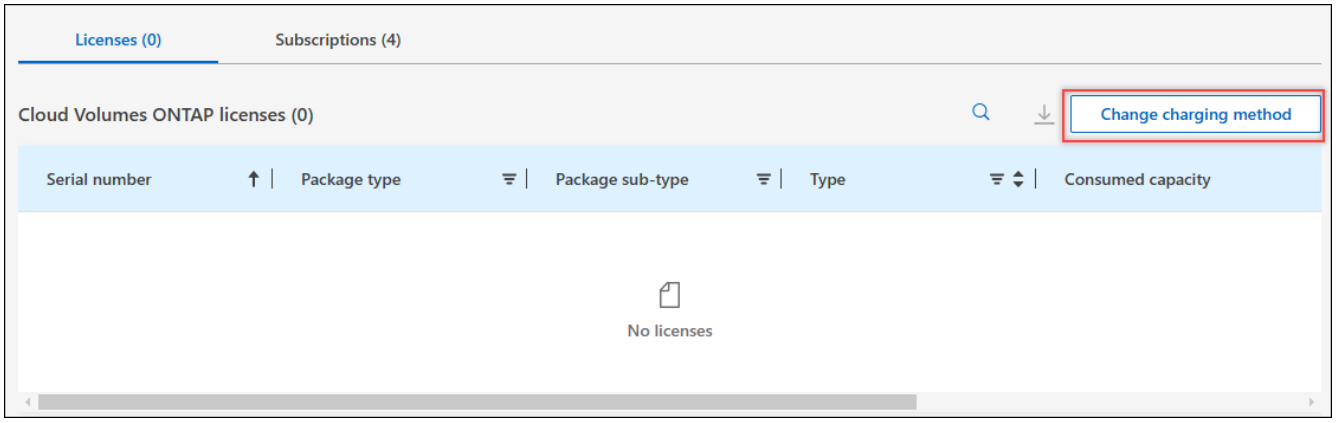
- Wenn Sie über ein privates Angebot oder einen Vertrag vom Marktplatz Ihres Cloud-Anbieters verfügen, führt der Wechsel zu einer Abrechnungsmethode, die nicht in Ihrem Vertrag enthalten ist, dazu, dass Ihnen BYOL (wenn Sie eine Lizenz von NetApp erworben haben) oder PAYGO in Rechnung gestellt wird.

Schritte

1. Wählen Sie im linken Navigationsbereich **Verwaltung > Licenses and subscriptions** aus.
2. Wählen Sie die Registerkarte **Übersicht**.
3. Wählen Sie auf der Kachel „Cloud Volumes ONTAP“ **Anzeigen** aus.
4. Wählen Sie **Zur erweiterten Ansicht wechseln**.



5. Scrollen Sie nach unten zur Tabelle **Kapazitätsbasierte Lizenz** und wählen Sie **Abrechnungsmethode ändern**.



6. Wählen Sie im Popup-Fenster **Abrechnungsmethode ändern** ein Cloud Volumes ONTAP System aus, wählen Sie die neue Abrechnungsmethode und bestätigen Sie dann, dass Sie verstanden haben, dass sich die Änderung des Pakettyps auf die Servicegebühren auswirkt.
7. Wählen Sie **Lademethode ändern**.

Nutzungsberichte herunterladen

Sie können vier Nutzungsberichte von der Konsole herunterladen. Diese Nutzungsberichte liefern Kapazitätsdetails zu Ihren Abonnements und informieren Sie darüber, wie Ihnen die Ressourcen in Ihren Cloud Volumes ONTAP Abonnements in Rechnung gestellt werden. Die herunterladbaren Berichte erfassen Daten zu einem bestimmten Zeitpunkt und können problemlos mit anderen geteilt werden.

Die folgenden Berichte stehen zum Download bereit. Die angezeigten Kapazitätswerte sind in TiB angegeben.

- **Nutzung auf hoher Ebene**: Dieser Bericht enthält die folgenden Informationen:
  - Gesamte verbrauchte Kapazität
  - Gesamte vorab festgelegte Kapazität
  - Gesamte BYOL-Kapazität
  - Gesamtkapazität der Marketplace-Verträge
  - Gesamte PAYGO-Kapazität
- * Cloud Volumes ONTAP -Paketnutzung*: Dieser Bericht enthält die folgenden Informationen für jedes Paket:
  - Gesamte verbrauchte Kapazität
  - Gesamte vorab festgelegte Kapazität
  - Gesamte BYOL-Kapazität
  - Gesamtkapazität der Marketplace-Verträge
  - Gesamte PAYGO-Kapazität
- **Nutzung von Storage-VMs**: Dieser Bericht zeigt, wie die berechnete Kapazität auf Cloud Volumes ONTAP

Systeme und Storage Virtual Machines (SVMs) aufgeteilt ist. Diese Informationen sind nur im Bericht verfügbar. Es enthält die folgenden Informationen:

  - System-ID und Name (wird als UUID angezeigt)
  - Wolke
  - NetApp Konto-ID
  - Systemkonfiguration
  - SVM-Name
  - Bereitgestellte Kapazität
  - Übersicht der geladenen Kapazität
  - Abrechnungszeitraum für den Marktplatz
  - Cloud Volumes ONTAP Paket oder -Funktion
  - Name des SaaS Marketplace-Abonnements wird aufgeladen
  - Abrechnung der SaaS Marketplace-Abonnement-ID
  - Arbeitslasttyp
- **Volume-Nutzung**: Dieser Bericht zeigt, wie die berechnete Kapazität nach Volumes in einem Cloud Volumes ONTAP System aufgeschlüsselt ist. Diese Informationen sind auf keinem Bildschirm der Konsole verfügbar. Es enthält die folgenden Informationen:
  - System-ID und Name (wird als UUID angezeigt)
  - SVN-Name
  - Datenträger-ID
  - Datenträgertyp
  - Vom Volumen bereitgestellte Kapazität

> FlexClone -Volumes sind in diesem Bericht nicht enthalten, da für diese Volume-Typen keine Gebühren anfallen.

Schritte

1. Wählen Sie im linken Navigationsbereich **Verwaltung > Licenses and subscriptions** aus.
2. Wählen Sie auf der Registerkarte **Übersicht** in der Kachel „Cloud Volumes ONTAP“ die Option **Anzeigen** aus.
3. Wählen Sie **Nutzungsbericht**.

   Der Nutzungsbericht wird heruntergeladen.
4. Öffnen Sie die heruntergeladene Datei, um auf die Berichte zuzugreifen.

Verwalten Sie Keystone -Abonnements für Cloud Volumes ONTAP über die NetApp Console

Verwalten Sie Ihre Keystone -Abonnements in der NetApp Console , indem Sie Abonnements für die Verwendung mit Cloud Volumes ONTAP aktivieren und Änderungen an der zugesagten Kapazität für die Service-Levels Ihres Abonnements anfordern. Durch die Anforderung zusätzlicher Kapazität für ein Servicelevel wird mehr Speicherplatz für

Cloud Volumes ONTAP Systeme bereitgestellt.

NetApp Keystone ist ein flexibler, abonnementbasierter Pay-as-you-grow-Service, der Kunden, die OpEx gegenüber CapEx oder Leasing bevorzugen, ein Hybrid-Cloud-Erlebnis bietet.

"Erfahren Sie mehr über Keystone"

Autorisieren Sie Ihr Konto

Bevor Sie Keystone -Abonnements in der Konsole verwenden und verwalten können, müssen Sie sich an NetApp wenden, um Ihr Konsolenkonto mit Ihren Keystone -Abonnements zu autorisieren.

Schritte

1. Wählen Sie im Menü der NetApp Console **Administration > Licenses and subscriptions**.
2. Wählen Sie * Keystone -Abonnements* aus.
3. Wenn Sie die Seite **Willkommen bei NetApp Keystone** sehen, senden Sie eine E-Mail an die auf der Seite angegebene Adresse.

   Ein NetApp -Mitarbeiter wird Ihre Anfrage bearbeiten, indem er Ihr Konto für den Zugriff auf die Abonnements autorisiert.
4. Kehren Sie zur Registerkarte * Keystone -Abonnements* zurück, um Ihre Abonnements anzuzeigen.

Verknüpfen eines Abonnements

Nachdem NetApp Ihr Konto autorisiert hat, können Sie Keystone Abonnements zur Verwendung mit Cloud Volumes ONTAP verknüpfen. Mit dieser Aktion können Benutzer das Abonnement als Abrechnungsmethode für neue Cloud Volumes ONTAP Systeme auswählen.

Schritte

1. Wählen Sie im Menü der NetApp Console **Administration > Licenses and subscriptions**.
2. Wählen Sie * Keystone -Abonnements* aus.
3. Klicken Sie für das Abonnement, das Sie verknüpfen möchten, auf ••• und wählen Sie **Link**.

Ergebnis

Das Abonnement ist jetzt mit Ihrer Konsolenorganisation oder Ihrem Konsolenkonto verknüpft und kann beim Erstellen einer Cloud Volumes ONTAP Arbeitsumgebung ausgewählt werden.

Fordern Sie mehr oder weniger zugesicherte Kapazität an

Wenn Sie die zugesagte Kapazität für die Service-Levels Ihres Abonnements ändern möchten, können Sie direkt von der Konsole aus eine Anfrage an NetApp senden. Durch die Anforderung zusätzlicher Kapazität für ein Servicelevel wird mehr Speicherplatz für Cloud Volumes ONTAP Systeme bereitgestellt.

Schritte

1. Wählen Sie im Menü der NetApp Console **Administration > Licenses and subscriptions**.
2. Wählen Sie * Keystone -Abonnements* aus.
3. Klicken Sie für das Abonnement, dessen Kapazität Sie anpassen möchten, auf ••• und wählen Sie **Details anzeigen und bearbeiten**.
4. Geben Sie die angeforderte zugesagte Kapazität für ein oder mehrere Abonnements ein.

5. Scrollen Sie nach unten, geben Sie zusätzliche Details für die Anfrage ein und klicken Sie dann auf **Senden**.

Ergebnis

Ihre Anfrage erstellt zur Bearbeitung ein Ticket im NetApp-System.

Überwachen der Nutzung

Mit dem Digital Advisor -Dashboard können Sie die Nutzung des Keystone Abonnements überwachen und Berichte erstellen.

"Erfahren Sie mehr über die Überwachung der Abonnementnutzung"

Aufheben der Verknüpfung eines Abonnements

Wenn Sie ein Keystone -Abonnement nicht mehr mit der Konsole verwenden möchten, können Sie die Verknüpfung des Abonnements aufheben. Beachten Sie, dass Sie die Verknüpfung eines Abonnements nur aufheben können, wenn es nicht mit einem vorhandenen Cloud Volumes ONTAP Abonnement verknüpft ist.

Schritte

1. Wählen Sie im Menü der NetApp Console **Administration > Licenses and subscriptions**.
2. Wählen Sie * Keystone*.
3. Klicken Sie für das Abonnement, dessen Verknüpfung Sie aufheben möchten, auf ••• und wählen Sie **Verknüpfung aufheben**.

Ergebnis

Die Verknüpfung des Abonnements mit Ihrer Konsolenorganisation oder Ihrem Konto wird aufgehoben und steht beim Erstellen einer Cloud Volumes ONTAP Arbeitsumgebung nicht mehr zur Auswahl.

Verwalten Sie die knotenbasierte Lizenzierung für Cloud Volumes ONTAP

Verwalten Sie knotenbasierte Lizenzen in der NetApp Console, um sicherzustellen, dass jedes Cloud Volumes ONTAP -System über eine gültige Lizenz mit der erforderlichen Kapazität verfügt.

Knotenbasierte Lizenzen sind das Lizenzmodell der vorherigen Generation (und für Neukunden nicht verfügbar):

- Bring Your Own License (BYOL)-Lizenzen, die bei NetApp erworben wurden
- Stündliche Pay-as-you-go-Abonnements (PAYGO) vom Marktplatz Ihres Cloud-Anbieters

Sie können knotenbasierte Cloud Volumes ONTAP -Lizenzen über die NetApp Console verwalten.

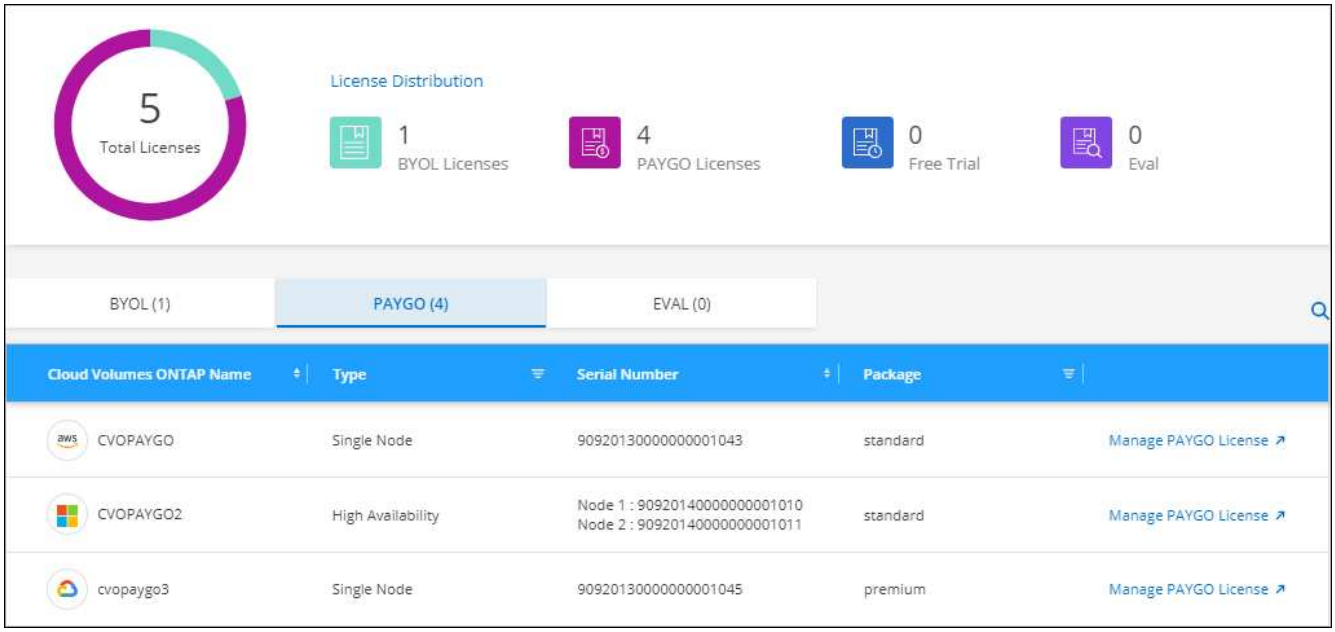
"Erfahren Sie mehr über Cloud Volumes ONTAP -Lizenzen" .

Verwalten von PAYGO-Lizenzen

Über das Menü „Licenses and subscriptions“ können Sie Details zu jedem Ihrer PAYGO Cloud Volumes ONTAP Systeme anzeigen, einschließlich der Seriennummer und des PAYGO-Lizenztyps.

Schritte

1. Wählen Sie im linken Navigationsbereich **Verwaltung > Licenses and subscriptions** aus.
2. Wählen Sie die Registerkarte **Übersicht**.
3. Wählen Sie auf der Kachel „Cloud Volumes ONTAP“ **Anzeigen** aus.
4. Wählen Sie **Knotenbasierte Lizenzen** aus der Dropdown-Liste aus.
5. Klicken Sie auf **PAYGO**.
6. Sehen Sie sich in der Tabelle Details zu jeder Ihrer PAYGO-Lizenzen an.



7. Klicken Sie bei Bedarf auf **PAYGO-Lizenz verwalten**, um die PAYGO-Lizenz zu ändern oder den Instanztyp zu ändern.

BYOL-Lizenzen verwalten

Verwalten Sie Lizenzen, die Sie direkt von NetApp erworben haben, indem Sie Systemlizenzen und Lizenzen für zusätzliche Kapazität hinzufügen und entfernen.

NetApp hat den Erwerb, die Verlängerung und die Erneuerung von BYOL-Lizenzen eingeschränkt. Weitere Informationen finden Sie unter "Eingeschränkte Verfügbarkeit der BYOL-Lizenzierung für Cloud Volumes ONTAP" .

Nicht zugewiesene Lizenzen hinzufügen

Fügen Sie der Konsole eine knotenbasierte Lizenz hinzu, damit Sie die Lizenz auswählen können, wenn Sie ein neues Cloud Volumes ONTAP -System erstellen. Die Konsole identifiziert diese Lizenzen als *nicht zugewiesen*.

Schritte

1. Wählen Sie im linken Navigationsbereich **Verwaltung > Licenses and subscriptions** aus.
2. Wählen Sie die Registerkarte **Übersicht**.
3. Wählen Sie auf der Kachel „Cloud Volumes ONTAP“ **Anzeigen** aus.
4. Wählen Sie **Knotenbasierte Lizenzen** aus der Dropdown-Liste aus.

5. Klicken Sie auf **Nicht zugewiesen**.
6. Klicken Sie auf **Nicht zugewiesene Lizenzen hinzufügen**.
7. Geben Sie die Seriennummer der Lizenz ein oder laden Sie die Lizenzdatei hoch.

   Wenn Sie die Lizenzdatei noch nicht haben, lesen Sie den folgenden Abschnitt.

8. Klicken Sie auf **Lizenz hinzufügen**.

Ergebnis

Die Konsole fügt die Lizenz hinzu. Die Lizenz wird als nicht zugewiesen gekennzeichnet, bis Sie sie einem neuen Cloud Volumes ONTAP -System zuordnen. Danach wird die Lizenz auf die Registerkarte **BYOL** unter * Licenses and subscriptions* verschoben.

Austausch nicht zugewiesener knotenbasierter Lizenzen

Wenn Sie über eine nicht zugewiesene knotenbasierte Lizenz für Cloud Volumes ONTAP verfügen, die Sie nicht verwendet haben, können Sie die Lizenz austauschen, indem Sie sie in eine NetApp Backup and Recovery -Lizenz, eine NetApp Data Classification -Lizenz oder eine NetApp Cloud Tiering -Lizenz umwandeln.

Durch den Austausch der Lizenz wird die Cloud Volumes ONTAP -Lizenz widerrufen und eine Lizenz im Gegenwert von einem Dollar für den Dienst erstellt:

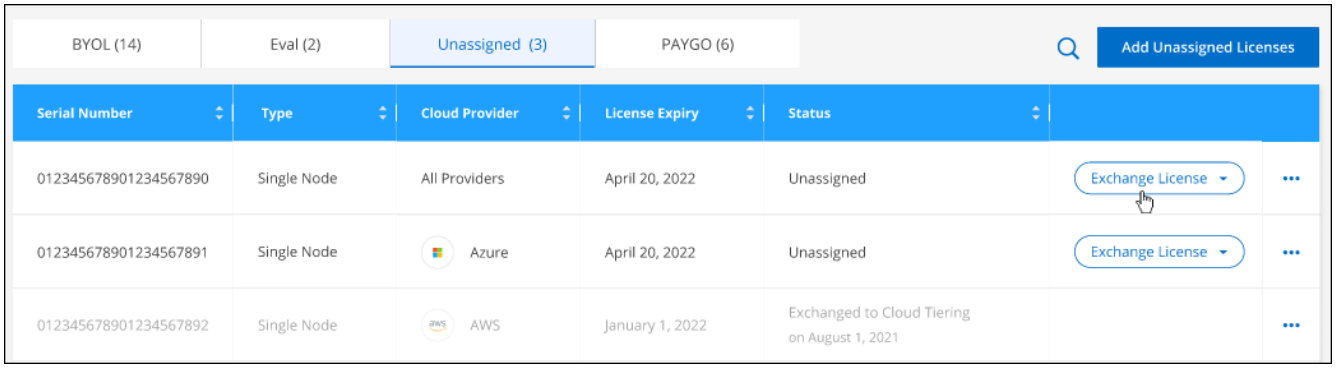
- Die Lizenzierung für ein Cloud Volumes ONTAP HA-Paar wird in eine 51 TiB Direktlizenz umgewandelt
- Die Lizenzierung für einen Cloud Volumes ONTAP Einzelknoten wird in eine 32 TiB-Direktlizenz umgewandelt

Die konvertierte Lizenz hat dasselbe Ablaufdatum wie die Cloud Volumes ONTAP -Lizenz.

"Sehen Sie sich die Anleitung zum Austausch knotenbasierter Lizenzen an."

Schritte

1. Wählen Sie im linken Navigationsbereich **Verwaltung > Licenses and subscriptions** aus.
2. Wählen Sie die Registerkarte **Übersicht**.
3. Wählen Sie auf der Kachel „Cloud Volumes ONTAP“ **Anzeigen** aus.
4. Wählen Sie **Knotenbasierte Lizenzen** aus der Dropdown-Liste aus.
5. Klicken Sie auf **Nicht zugewiesen**.
6. Klicken Sie auf **Lizenz austauschen**.



7. Wählen Sie den Dienst aus, bei dem Sie die Lizenz eintauschen möchten.
8. Wählen Sie bei entsprechender Aufforderung eine zusätzliche Lizenz für das HA-Paar aus.
9. Lesen Sie die rechtlichen Einwilligungserklärungen und klicken Sie auf **Zustimmen**.

Ergebnis

Die Konsole konvertiert die nicht zugewiesene Lizenz in den von Ihnen ausgewählten Dienst. Sie können die neue Lizenz auf der Registerkarte **Data Services-Lizenzen** anzeigen.

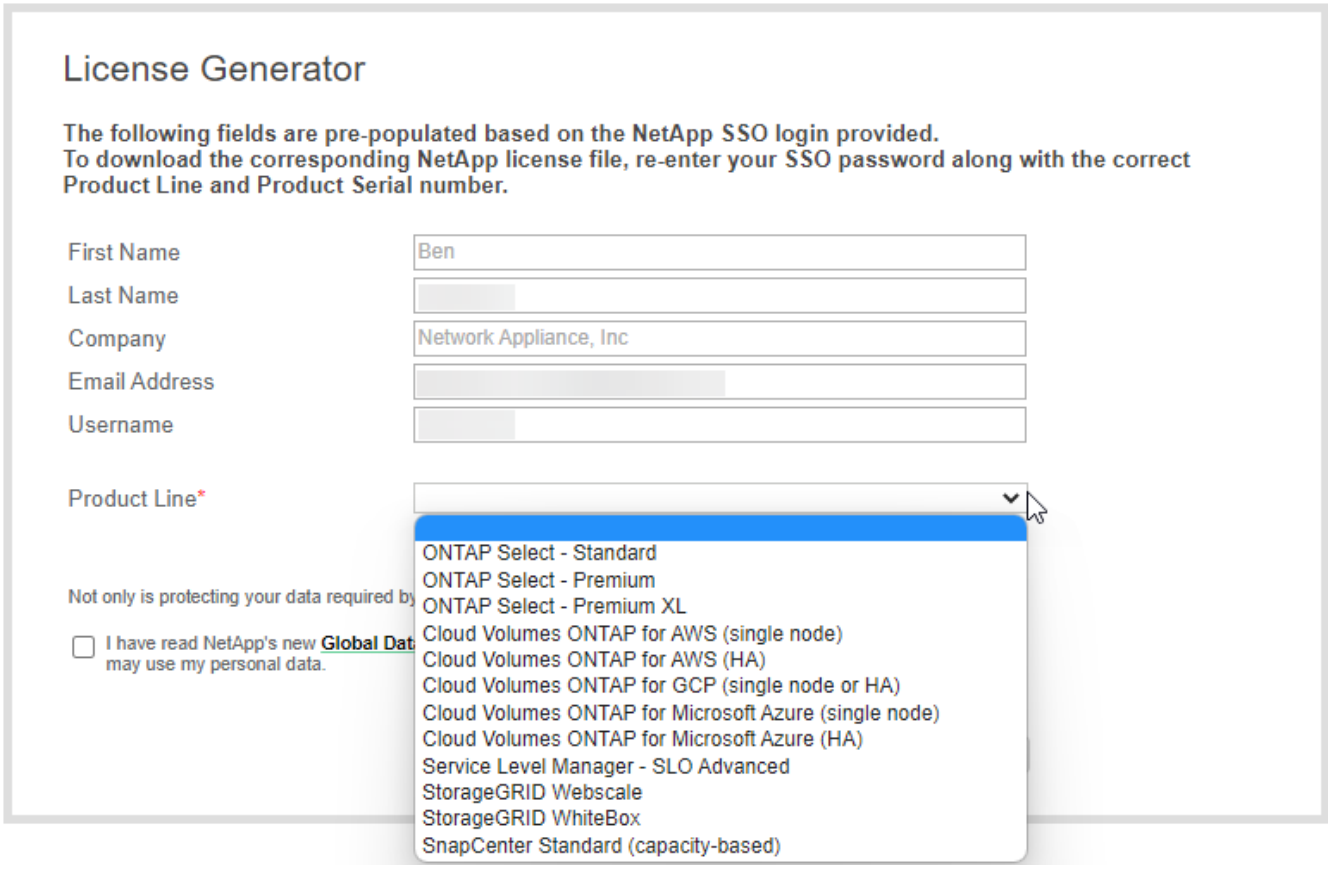
Erhalten Sie eine Systemlizenzdatei

In den meisten Fällen kann die Konsole Ihre Lizenzdatei automatisch über Ihr NetApp Support Site-Konto abrufen. Wenn dies jedoch nicht möglich ist, müssen Sie die Lizenzdatei manuell hochladen. Wenn Sie die Lizenzdatei nicht haben, können Sie sie von netapp.com beziehen.

Schritte

1. Gehen Sie zum "NetApp Lizenzdateigenerator" und melden Sie sich mit Ihren Anmeldeinformationen für die NetApp Support-Site an.
2. Geben Sie Ihr Passwort ein, wählen Sie Ihr Produkt aus, geben Sie die Seriennummer ein, bestätigen Sie, dass Sie die Datenschutzrichtlinie gelesen und akzeptiert haben, und klicken Sie dann auf **Senden**.

   Beispiel



3. Wählen Sie, ob Sie die JSON-Datei „serialnumber.NLF“ per E-Mail oder durch direkten Download erhalten möchten.

Aktualisieren einer Systemlizenz

Wenn Sie ein BYOL-Abonnement verlängern, indem Sie sich an einen NetApp -Vertreter wenden, erhält die Konsole automatisch die neue Lizenz von NetApp und installiert sie auf dem Cloud Volumes ONTAP System. Wenn die Konsole über die sichere Internetverbindung nicht auf die Lizenzdatei zugreifen kann, können Sie die Datei selbst abrufen und dann manuell hochladen.

Schritte

1. Wählen Sie im linken Navigationsbereich **Verwaltung > Licenses and subscriptions** aus.
2. Wählen Sie die Registerkarte **Übersicht**.
3. Wählen Sie auf der Kachel „Cloud Volumes ONTAP“ **Anzeigen** aus.
4. Wählen Sie **Knotenbasierte Lizenzen** aus der Dropdown-Liste aus.
5. Erweitern Sie auf der Registerkarte **BYOL** die Details für ein Cloud Volumes ONTAP System.
6. Klicken Sie auf das Aktionsmenü neben der Systemlizenz und wählen Sie **Lizenz aktualisieren**.
7. Laden Sie die Lizenzdatei (oder Dateien, wenn Sie ein HA-Paar haben) hoch.
8. Klicken Sie auf **Lizenz aktualisieren**.

Ergebnis

Die Konsole aktualisiert die Lizenz auf dem Cloud Volumes ONTAP -System.

Verwalten von Lizenzen für zusätzliche Kapazität

Sie können zusätzliche Kapazitätslizenzen für ein Cloud Volumes ONTAP BYOL-System erwerben, um mehr als die 368 TiB Kapazität zuzuweisen, die mit einer BYOL-Systemlizenz bereitgestellt werden. Sie können beispielsweise eine zusätzliche Lizenzkapazität erwerben, um Cloud Volumes ONTAP bis zu 736 TiB Kapazität zuzuweisen. Oder Sie erwerben drei zusätzliche Kapazitätslizenzen, um bis zu 1,4 PiB zu erhalten.

Die Anzahl der Lizenzen, die Sie für ein Einzelknotensystem oder ein HA-Paar erwerben können, ist unbegrenzt.

Kapazitätslizenzen hinzufügen

Erwerben Sie eine Lizenz für zusätzliche Kapazität, indem Sie uns über das Chat-Symbol unten rechts in der Konsole kontaktieren. Nachdem Sie die Lizenz erworben haben, können Sie sie auf ein Cloud Volumes ONTAP System anwenden.

Schritte

1. Wählen Sie im linken Navigationsbereich **Verwaltung > Licenses and subscriptions** aus.
2. Wählen Sie die Registerkarte **Übersicht**.
3. Wählen Sie auf der Kachel „Cloud Volumes ONTAP“ **Anzeigen** aus.
4. Wählen Sie **Knotenbasierte Lizenzen** aus der Dropdown-Liste aus.
5. Erweitern Sie auf der Registerkarte **BYOL** die Details für ein Cloud Volumes ONTAP System.
6. Klicken Sie auf **Kapazitätslizenz hinzufügen**.
7. Geben Sie die Seriennummer ein oder laden Sie die Lizenzdatei (oder Dateien, wenn Sie ein HA-Paar haben) hoch.
8. Klicken Sie auf **Kapazitätslizenz hinzufügen**.

Aktualisieren von Kapazitätslizenzen

Wenn Sie die Laufzeit einer Lizenz für zusätzliche Kapazität verlängert haben, müssen Sie die Lizenz in der Konsole aktualisieren.

Schritte

1. Wählen Sie im linken Navigationsbereich **Verwaltung > Licenses and subscriptions** aus.
2. Wählen Sie die Registerkarte **Übersicht**.
3. Wählen Sie auf der Kachel „Cloud Volumes ONTAP“ **Anzeigen** aus.
4. Wählen Sie **Knotenbasierte Lizenzen** aus der Dropdown-Liste aus.
5. Erweitern Sie auf der Registerkarte **BYOL** die Details für ein Cloud Volumes ONTAP System.
6. Klicken Sie auf das Aktionsmenü neben der Kapazitätslizenz und wählen Sie **Lizenz aktualisieren**.
7. Laden Sie die Lizenzdatei (oder Dateien, wenn Sie ein HA-Paar haben) hoch.
8. Klicken Sie auf **Lizenz aktualisieren**.

Kapazitätslizenzen entfernen

Wenn eine Lizenz für zusätzliche Kapazität abgelaufen ist und nicht mehr verwendet wird, können Sie sie jederzeit entfernen.

Schritte

1. Wählen Sie im linken Navigationsbereich **Verwaltung > Licenses and subscriptions** aus.
2. Wählen Sie die Registerkarte **Übersicht**.
3. Wählen Sie auf der Kachel „Cloud Volumes ONTAP“ **Anzeigen** aus.
4. Wählen Sie **Knotenbasierte Lizenzen** aus der Dropdown-Liste aus.
5. Erweitern Sie auf der Registerkarte **BYOL** die Details für ein Cloud Volumes ONTAP System.
6. Klicken Sie auf das Aktionsmenü neben der Kapazitätslizenz und wählen Sie **Lizenz entfernen**.
7. Klicken Sie auf **Entfernen**.

Wechsel zwischen PAYGO und BYOL

Die Konvertierung eines Systems von der PAYGO-By-Node-Lizenzierung zur BYOL-By-Node-Lizenzierung (und umgekehrt) wird nicht unterstützt. Wenn Sie zwischen einem Pay-as-you-go-Abonnement und einem BYOL-Abonnement wechseln möchten, müssen Sie ein neues System bereitstellen und Daten vom vorhandenen System auf das neue System replizieren.

Schritte

1. Erstellen Sie ein neues Cloud Volumes ONTAP System.
2. Richten Sie für jedes Volume, das Sie replizieren müssen, eine einmalige Datenreplikation zwischen den Systemen ein.

   "Erfahren Sie, wie Sie Daten zwischen Systemen replizieren"

3. Beenden Sie das Cloud Volumes ONTAP -System, das Sie nicht mehr benötigen, indem Sie das ursprüngliche System löschen.

   "Erfahren Sie, wie Sie ein Cloud Volumes ONTAP -System löschen" .

Weiterführende Links

Link:"Ende der Verfügbarkeit von knotenbasierten Lizenzen" "Konvertieren Sie knotenbasierte Lizenzen in kapazitätsbasierte"

Volume- und LUN-Verwaltung

Erstellen Sie ein FlexVol volume auf einem Cloud Volumes ONTAP -System

Wenn Sie nach dem Start Ihres ersten Cloud Volumes ONTAP -Systems mehr Speicher benötigen, können Sie über die NetApp Console neue FlexVol Volumes für NFS, CIFS oder iSCSI erstellen.

Sie haben mehrere Möglichkeiten, ein neues Volume zu erstellen:

- Geben Sie Details für ein neues Volume an und überlassen Sie der Konsole die Verwaltung der zugrunde liegenden Datenaggregate.Mehr erfahren
- Erstellen Sie ein Volume auf einem Datenaggregat Ihrer Wahl.Mehr erfahren
- Erstellen Sie ein Volume auf dem zweiten Knoten in einer HA-Konfiguration.Mehr erfahren

Bevor Sie beginnen

Einige Hinweise zur Volume-Bereitstellung:

- Wenn Sie ein iSCSI-Volume erstellen, erstellt die Konsole automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volume erstellt haben, sodass keine Verwaltung erforderlich ist. Nachdem Sie das Volume erstellt haben,"Verwenden Sie den IQN, um von Ihren Hosts aus eine Verbindung zum LUN herzustellen" .
- Sie können zusätzliche LUNs vom ONTAP System Manager oder der ONTAP CLI erstellen.
- Wenn Sie CIFS in AWS verwenden möchten, müssen Sie DNS und Active Directory eingerichtet haben. Weitere Einzelheiten finden Sie unter"Netzwerkanforderungen für Cloud Volumes ONTAP für AWS" .
- Wenn Ihre Cloud Volumes ONTAP Konfiguration die Funktion Amazon EBS Elastic Volumes unterstützt, möchten Sie möglicherweise"Erfahren Sie mehr darüber, was passiert, wenn Sie ein Volume erstellen" .

Erstellen eines Volumes

Die gängigste Methode zum Erstellen eines Volumes besteht darin, den benötigten Volumetyp anzugeben und dann die Konsole die Datenträgerzuweisung für Sie übernehmen zu lassen. Sie haben aber auch die Möglichkeit, das spezifische Aggregat auszuwählen, auf dem Sie das Volume erstellen möchten.

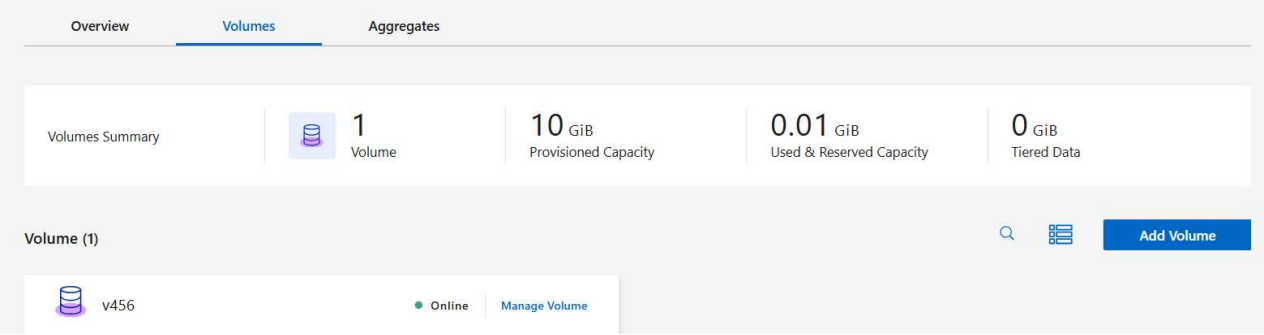
Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Doppelklicken Sie auf der Seite **Systeme** auf den Namen des Cloud Volumes ONTAP -Systems, auf dem Sie ein FlexVol volume bereitstellen möchten.

   Sie können ein Volume erstellen, indem Sie die Datenträgerzuweisung von der Konsole übernehmen lassen, oder Sie können ein bestimmtes Aggregat für das Volume auswählen. Die Auswahl eines bestimmten Aggregats wird nur empfohlen, wenn Sie die Datenaggregate auf Ihrem Cloud Volumes ONTAP System gut kennen.

Jedes Aggregat

Wählen Sie die Registerkarte „Volumes“ und klicken Sie auf „Volume hinzufügen“.

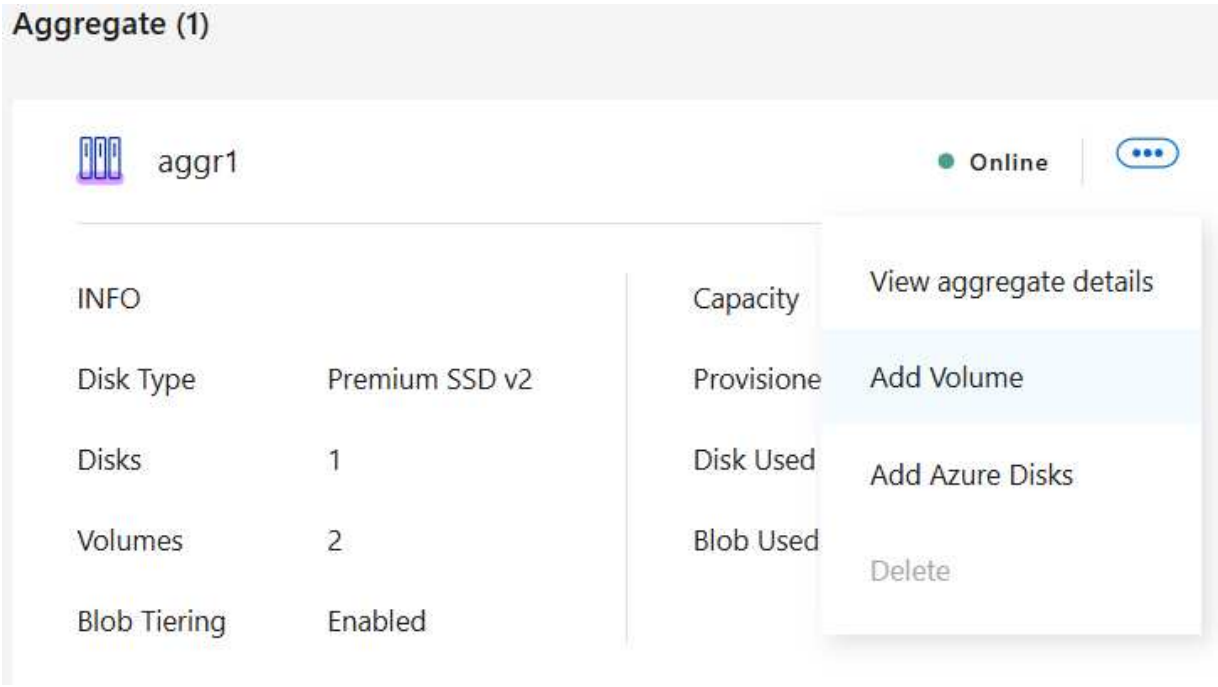


Spezifisches Aggregat

a. Gehen Sie auf der Registerkarte **Aggregate** zum gewünschten Aggregat und klicken Sie auf das ••• Symbol.

b. Wählen Sie **Volume hinzufügen**

.



3. Befolgen Sie die Schritte im Assistenten, um das Volume zu erstellen.

   a. **Details, Schutz und Tags**: Geben Sie grundlegende Details zum Volume ein und wählen Sie eine Snapshot-Richtlinie aus.

      Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Liste werden die Felder beschrieben, für die Sie möglicherweise Anleitungen benötigen:

Feld	Beschreibung
Datenträgername	Der identifizierbare Name, den Sie für das neue Volume eingeben können.

Feld	Beschreibung
Volumengröße	Die maximale Größe, die Sie eingeben können, hängt weitgehend davon ab, ob Sie Thin Provisioning aktivieren. Dadurch können Sie ein Volume erstellen, das größer ist als der ihm aktuell zur Verfügung stehende physische Speicher.
Speicher-VM (SVM)	Eine Storage-VM ist eine virtuelle Maschine, die innerhalb von ONTAP ausgeführt wird und Ihren Clients Speicher- und Datendienste bereitstellt. Sie kennen dies möglicherweise als SVM oder VServer. Cloud Volumes ONTAP ist standardmäßig mit einer Speicher-VM konfiguriert, einige Konfigurationen unterstützen jedoch zusätzliche Speicher-VMs. Sie können die Speicher-VM für das neue Volume angeben.
Snapshot-Richtlinie	Eine Snapshot-Kopierrichtlinie gibt die Häufigkeit und Anzahl der automatisch erstellten NetApp Snapshot-Kopien an. Eine NetApp Snapshot-Kopie ist ein zeitpunktbezogenes Dateisystem-Image, das keine Auswirkungen auf die Leistung hat und nur minimalen Speicherplatz benötigt. Sie können die Standardrichtlinie oder keine auswählen. Für vorübergehende Daten können Sie „Keine“ auswählen, beispielsweise „tempdb“ für Microsoft SQL Server.

b. **Protokoll**: Wählen Sie ein Protokoll für das Volume (NFS, CIFS oder iSCSI) und geben Sie dann die erforderlichen Informationen ein.

   Wenn Sie CIFS auswählen und kein Server eingerichtet ist, werden Sie von der Konsole aufgefordert, die CIFS-Konnektivität einzurichten, nachdem Sie auf **Weiter** geklickt haben.

   "Erfahren Sie mehr über unterstützte Clientprotokolle und -versionen" .

   In den folgenden Abschnitten werden Felder beschrieben, für die Sie möglicherweise Anleitungen benötigen. Die Beschreibungen sind nach Protokoll geordnet.

NFS

Zugriffskontrolle

Wählen Sie eine benutzerdefinierte Exportrichtlinie, um das Volume für Clients verfügbar zu machen.

Exportpolitik

Definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt die Konsole einen Wert ein, der Zugriff auf alle Instanzen im Subnetz gewährt.

CIFS

Berechtigungen und Benutzer/Gruppen

Ermöglicht Ihnen, die Zugriffsebene auf eine SMB-Freigabe für Benutzer und Gruppen zu steuern (auch als Zugriffskontrolllisten oder ACLs bezeichnet). Sie können lokale oder Domänen-Windows-Benutzer oder -Gruppen oder UNIX-Benutzer oder -Gruppen angeben. Wenn Sie einen Windows-Domänenbenutzernamen angeben, müssen Sie die Domäne des Benutzers im Format Domäne\Benutzername angeben.

DNS Primäre und sekundäre IP-Adresse

Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgelisteten DNS-Server müssen die Service Location Records (SRV) enthalten, die zum Auffinden der Active Directory-LDAP-Server und Domänencontroller für die Domäne erforderlich sind, der der CIFS-Server beitreten wird.

Wenn Sie Google Managed Active Directory konfigurieren, kann auf AD standardmäßig mit der IP-Adresse 169.254.169.254 zugegriffen werden.

Beitretende Active Directory-Domäne

Der FQDN der Active Directory (AD)-Domäne, der der CIFS-Server beitreten soll.

Anmeldeinformationen, die zum Beitritt zur Domäne berechtigt sind

Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.

NetBIOS-Name des CIFS-Servers

Ein CIFS-Servername, der in der AD-Domäne eindeutig ist.

Organisationseinheit

Die Organisationseinheit innerhalb der AD-Domäne, die mit dem CIFS-Server verknüpft werden soll. Der Standardwert ist CN=Computers.

- Um AWS Managed Microsoft AD als AD-Server für Cloud Volumes ONTAP zu konfigurieren, geben Sie in dieses Feld **OU=Computers,OU=corp** ein.
- Um Azure AD Domain Services als AD-Server für Cloud Volumes ONTAP zu konfigurieren, geben Sie in dieses Feld **OU=AADDC Computers** oder **OU=AADDC Users** ein.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure-Dokumentation: Erstellen einer Organisationseinheit (OU) in einer von Azure AD Domain Services verwalteten Domäne"^]
- Um Google Managed Microsoft AD als AD-Server für Cloud Volumes ONTAP zu konfigurieren, geben Sie in dieses Feld **OU=Computers,OU=Cloud** ein.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud-

Dokumentation: Organisationseinheiten in Google Managed Microsoft AD"^]

DNS-Domäne

Die DNS-Domäne für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen ist die Domäne dieselbe wie die AD-Domäne.

NTP-Server

Wählen Sie **Active Directory-Domäne verwenden**, um einen NTP-Server mithilfe des Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Weitere Informationen finden Sie im "Dokumentation zur NetApp Console" .

Beachten Sie, dass Sie einen NTP-Server nur beim Erstellen eines CIFS-Servers konfigurieren können. Es ist nicht mehr konfigurierbar, nachdem Sie den CIFS-Server erstellt haben.

iSCSI

LUN

iSCSI-Speicherziele werden als LUNs (logische Einheiten) bezeichnet und Hosts als Standardblockgeräte präsentiert. Wenn Sie ein iSCSI-Volume erstellen, erstellt die Konsole automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volume erstellt haben, sodass keine Verwaltung erforderlich ist. Nachdem Sie das Volume erstellt haben,"Verwenden Sie den IQN, um von Ihren Hosts aus eine Verbindung zum LUN herzustellen" .

Initiatorgruppe

Initiatorgruppen (igroups) geben an, welche Hosts auf bestimmte LUNs im Speichersystem zugreifen können

Host-Initiator (IQN)

iSCSI-Ziele stellen über Standard-Ethernet-Netzwerkadapter (NICs), TCP-Offload-Engine-Karten (TOE) mit Software-Initiatoren, konvergente Netzwerkadapter (CNAs) oder dedizierte Hostbusadapter (HBAs) eine Verbindung zum Netzwerk her und werden durch iSCSI-qualifizierte Namen (IQNs) identifiziert.

a. **Datenträgertyp**: Wählen Sie basierend auf Ihren Leistungsanforderungen und Kostenanforderungen einen zugrunde liegenden Datenträgertyp für das Volume aus.
   - "Dimensionierung Ihres Systems in AWS"
     - "Dimensionierung Ihres Systems in Azure"
     - "Dimensionierung Ihres Systems in Google Cloud"

4. **Nutzungsprofil & Tiering-Richtlinie**: Wählen Sie, ob Sie Speichereffizienzfunktionen auf dem Volume aktivieren oder deaktivieren möchten, und wählen Sie dann eine"Volume-Tiering-Richtlinie" .

   ONTAP umfasst mehrere Speichereffizienzfunktionen, die die von Ihnen benötigte Gesamtspeichermenge reduzieren können. Die Storage-Effizienzfunktionen von NetApp bieten folgende Vorteile:

   Dünne Bereitstellung

   Bietet Hosts oder Benutzern mehr logischen Speicher, als Sie tatsächlich in Ihrem physischen Speicherpool haben. Anstatt Speicherplatz vorab zuzuweisen, wird Speicherplatz jedem Volume dynamisch zugewiesen, während Daten geschrieben werden.

Deduplizierung

Verbessert die Effizienz, indem identische Datenblöcke lokalisiert und durch Verweise auf einen einzigen gemeinsamen Block ersetzt werden. Diese Technik reduziert den Speicherkapazitätsbedarf, indem redundante Datenblöcke, die sich auf demselben Datenträger befinden, eliminiert werden.

Komprimierung

Reduziert die zum Speichern von Daten erforderliche physische Kapazität durch Komprimieren von Daten innerhalb eines Volumes auf Primär-, Sekundär- und Archivspeicher.

5. **Überprüfen**: Überprüfen Sie die Details zum Datenträger und klicken Sie dann auf **Hinzufügen**.

Ergebnis

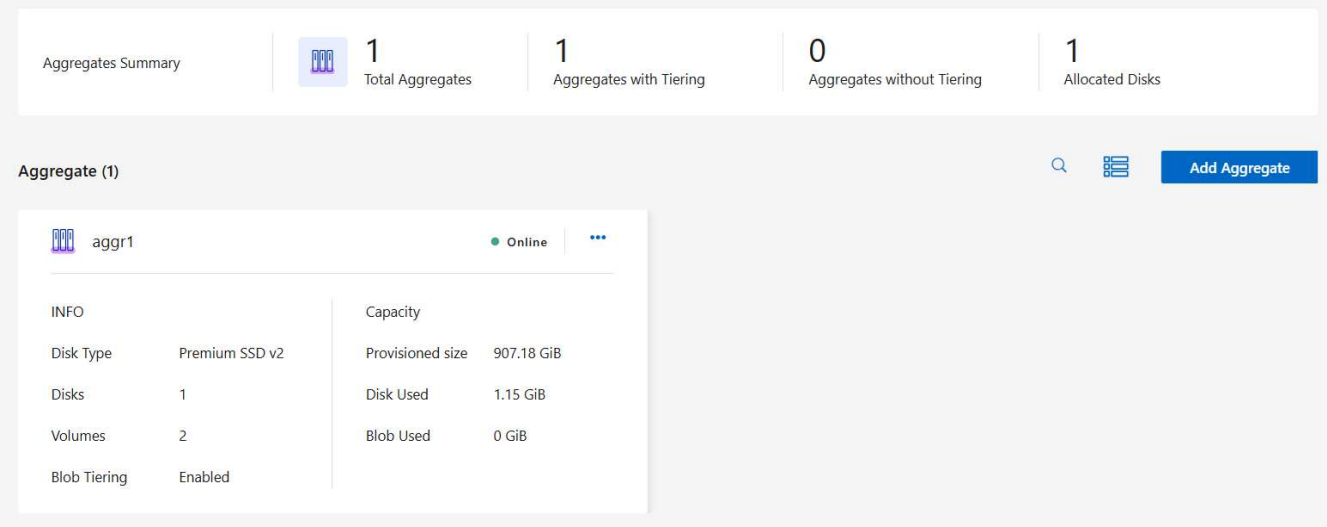
Die Konsole erstellt das Volume auf dem Cloud Volumes ONTAP -System.

Erstellen Sie ein Volume auf dem zweiten Knoten in einer HA-Konfiguration

Standardmäßig erstellt die Konsole Volumes auf dem ersten Knoten in einer HA-Konfiguration. Wenn Sie eine Aktiv-Aktiv-Konfiguration benötigen, in der beide Knoten Daten an Clients bereitstellen, müssen Sie Aggregate und Volumes auf dem zweiten Knoten erstellen.

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Doppelklicken Sie auf der Seite **Systeme** auf den Namen des Cloud Volumes ONTAP -Systems, auf dem Sie Aggregate verwalten möchten.
3. Klicken Sie auf der Registerkarte „Aggregate“ auf **Aggregat hinzufügen** und erstellen Sie das Aggregat.



4. Wählen Sie für Home Node den zweiten Knoten im HA-Paar.
5. Nachdem die Konsole das Aggregat erstellt hat, wählen Sie es aus und klicken Sie dann auf **Volume erstellen**.
6. Geben Sie Details für das neue Volume ein und klicken Sie dann auf **Erstellen**.

Ergebnis

Die Konsole erstellt das Volume auf dem zweiten Knoten im HA-Paar.

Für HA-Paare, die in mehreren AWS-Verfügbarkeitszonen bereitgestellt werden, müssen Sie das Volume mithilfe der Floating-IP-Adresse des Knotens, auf dem sich das Volume befindet, auf Clients mounten.

Nachdem Sie ein Volume erstellt haben

Wenn Sie eine CIFS-Freigabe bereitgestellt haben, erteilen Sie Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner und stellen Sie sicher, dass diese Benutzer auf die Freigabe zugreifen und eine Datei erstellen können.

Wenn Sie Kontingente auf Volumes anwenden möchten, müssen Sie ONTAP System Manager oder die ONTAP CLI verwenden. Mithilfe von Kontingenten können Sie den Speicherplatz und die Anzahl der von einem Benutzer, einer Gruppe oder einem Qtree verwendeten Dateien beschränken oder verfolgen.

Verwalten Sie Volumes auf Cloud Volumes ONTAP -Systemen

Sie können Volumes und CIFS-Server in der NetApp Console verwalten. Sie können Volumes auch verschieben, um Kapazitätsprobleme zu vermeiden.

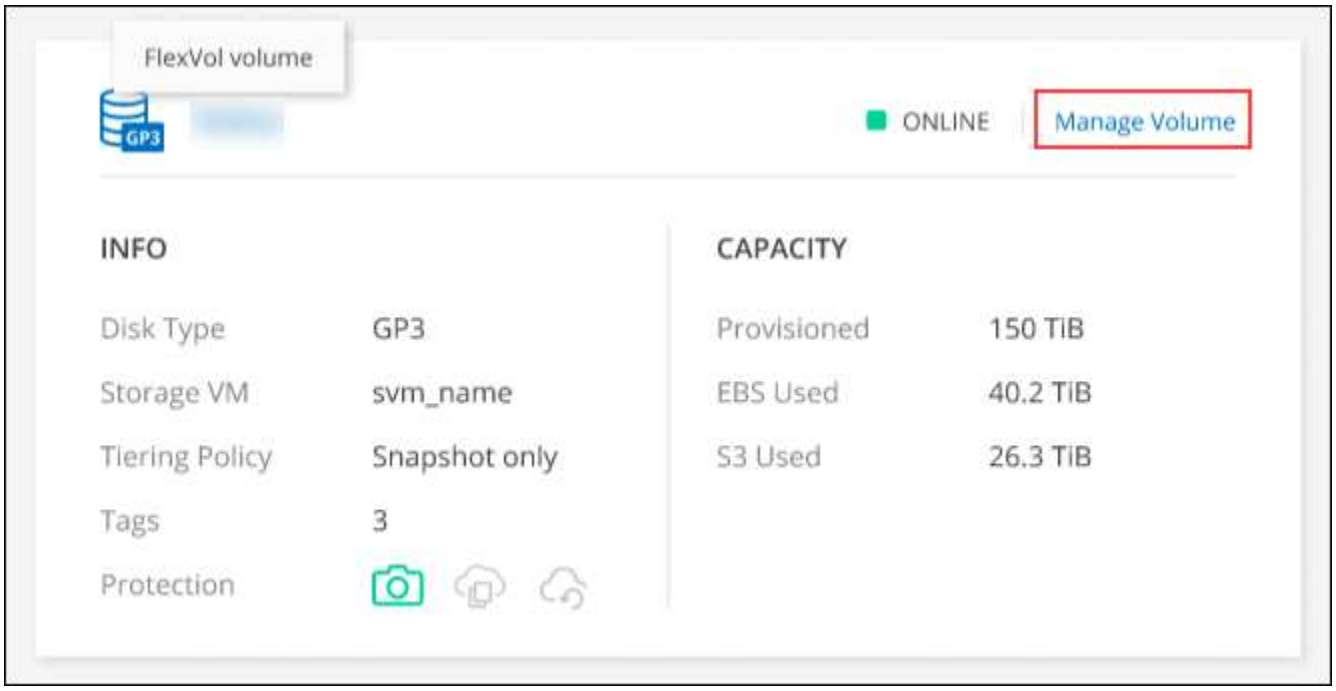
Sie können Volumes in der Standardansicht der NetApp Console oder über den ONTAP System Manager verwalten, der in der Konsole für erweitertes Volume-Management enthalten ist. Die Standardansicht bietet eine begrenzte Anzahl an Optionen zum Ändern Ihrer Volumes. System Manager bietet erweiterte Verwaltungsfunktionen wie Klonen, Größenänderung, Ändern der Einstellungen für Anti-Ransomware, Analyse, Schutz und Aktivitätsverfolgung sowie Verschieben von Volumes zwischen Ebenen. Weitere Informationen finden Sie unter"Verwalten Sie Cloud Volumes ONTAP mit System Manager" .

Verwalten von Volumes

Mithilfe der Standardansicht der Konsole können Sie Volumes entsprechend Ihrem Speicherbedarf verwalten. Sie können Volumes anzeigen, bearbeiten, klonen, wiederherstellen und löschen.

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Doppelklicken Sie auf der Seite **Systeme** auf das Cloud Volumes ONTAP -System, auf dem Sie Volumes verwalten möchten.
3. Wählen Sie die Registerkarte **Volumes**.



4. Klicken Sie auf der Kachel des gewünschten Volumes auf **Volume verwalten**.

Aufgabe	Aktion
Informationen zu einem Volume anzeigen	Klicken Sie unter „Volume-Aktionen“ im Bereich „Volumes verwalten“ auf „Volume-Details anzeigen“.
Holen Sie sich den NFS-Mount-Befehl	a. Klicken Sie unter „Volume-Aktionen“ im Bereich „Volumes verwalten“ auf **Mount-Befehl**. b. Klicken Sie auf **Kopieren**.
Klonen eines Volumes	a. Klicken Sie im Bereich „Volumes verwalten“ unter „Volume-Aktionen“ auf „Volume klonen“. b. Ändern Sie den Klonnamen nach Bedarf und klicken Sie dann auf **Klonen**. Dieser Vorgang erstellt ein FlexClone -Volume. Ein FlexClone -Volume ist eine beschreibbare, zeitpunktbezogene Kopie, die platzsparend ist, da sie nur wenig Speicherplatz für Metadaten verwendet und dann nur zusätzlichen Speicherplatz verbraucht, wenn Daten geändert oder hinzugefügt werden. Weitere Informationen zu FlexClone -Volumes finden Sie im "ONTAP 9 Handbuch zur logischen Speicherverwaltung" .

Aufgabe	Aktion
Bearbeiten eines Volumes (nur Volumes mit Lese-/Schreibzugriff)	a. Klicken Sie unter „Volume-Aktionen“ im Bereich „Volumes verwalten“ auf „Volume-Einstellungen bearbeiten“ b. Ändern Sie die Snapshot-Richtlinie, die NFS-Protokollversion, die NFS-Zugriffskontrollliste (Exportrichtlinie) oder die Freigabeberechtigungen des Volumes und klicken Sie dann auf **Übernehmen**. Wenn Sie benutzerdefinierte Snapshot-Richtlinien benötigen, können Sie diese mit ONTAP System Manager erstellen.
Löschen eines Volumes	a. Klicken Sie im Bereich „Volumes verwalten“ unter „Volume-Aktionen“ auf „Volume löschen“. b. Geben Sie im Fenster „Volume löschen“ den Namen des Volumes ein, das Sie löschen möchten. c. Klicken Sie zur Bestätigung erneut auf **Löschen**.
Erstellen Sie bei Bedarf eine Snapshot-Kopie	a. Klicken Sie unter „Schutzaktionen“ im Bereich „Volumes verwalten“ auf „Snapshot-Kopie erstellen“*. b. Ändern Sie bei Bedarf den Namen und klicken Sie dann auf **Erstellen**.
Wiederherstellen von Daten aus einer Snapshot-Kopie auf einem neuen Volume	a. Klicken Sie unter „Schutzaktionen“ im Bereich „Volumes verwalten“ auf „Aus Snapshot-Kopie wiederherstellen“*. b. Wählen Sie eine Snapshot-Kopie aus, geben Sie einen Namen für das neue Volume ein und klicken Sie dann auf **Wiederherstellen**.
Ändern des zugrunde liegenden Datenträgertyps	a. Klicken Sie unter „Erweiterte Aktionen“ im Bereich „Volumes verwalten“ auf „Datenträgertyp ändern“. b. Wählen Sie den Datenträgertyp aus und klicken Sie dann auf **Ändern**. Die Konsole verschiebt das Volume in ein vorhandenes Aggregat, das den ausgewählten Datenträgertyp verwendet, oder erstellt ein neues Aggregat für das Volume.

Aufgabe	Aktion
Ändern der Tiering-Richtlinie	a. Klicken Sie unter „Erweiterte Aktionen“ im Bereich „Volumes verwalten“ auf **Tiering-Richtlinie ändern**. b. Wählen Sie eine andere Richtlinie aus und klicken Sie auf **Ändern**. Die Konsole verschiebt das Volume in ein vorhandenes Aggregat, das den ausgewählten Datenträgertyp mit Tiering verwendet, oder erstellt ein neues Aggregat für das Volume.
Löschen eines Volumes	a. Wählen Sie ein Volume aus und klicken Sie dann auf **Löschen**. b. Geben Sie den Namen des Volumes in das Dialogfeld ein. c. Klicken Sie zur Bestätigung erneut auf **Löschen**.

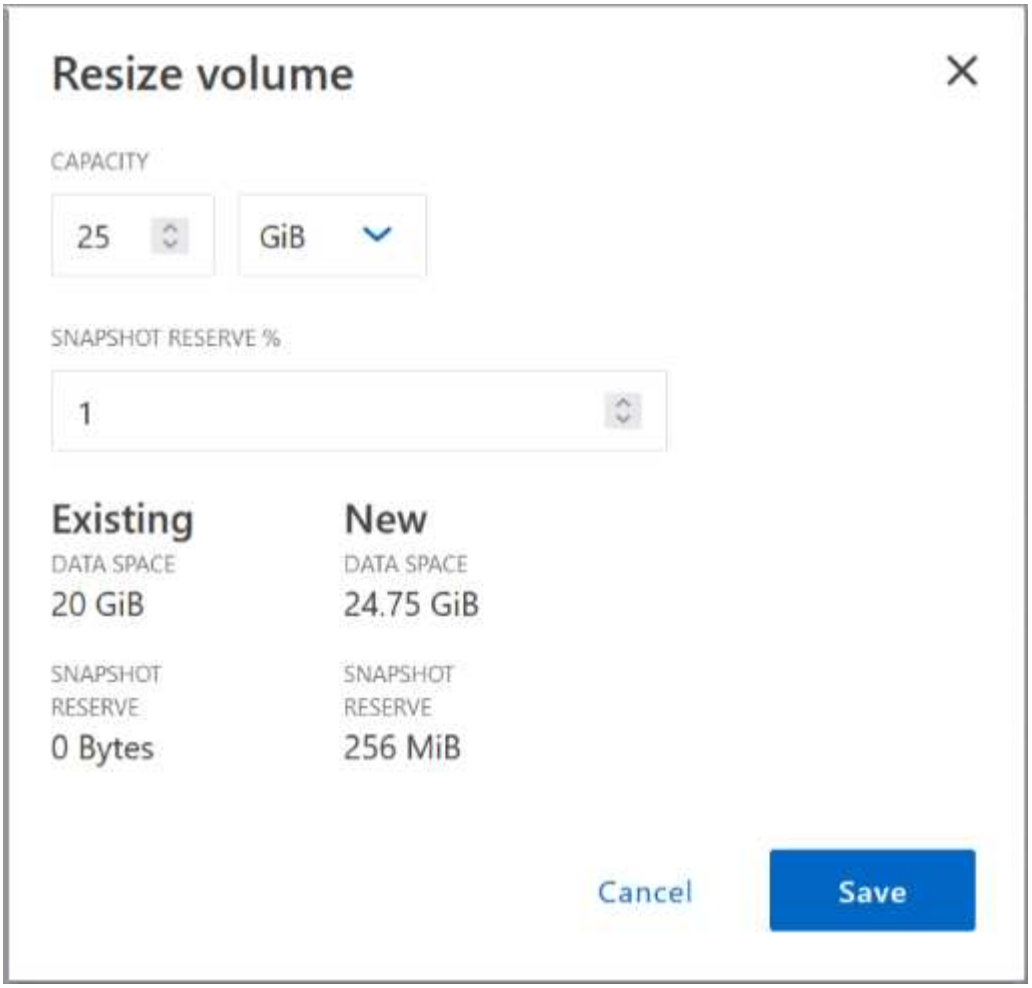
Ändern der Größe eines Volumes

Standardmäßig wächst ein Volume automatisch auf eine maximale Größe an, wenn der Speicherplatz erschöpft ist. Der Standardwert ist 1.000, was bedeutet, dass das Volume auf das 11-fache seiner Größe anwachsen kann. Dieser Wert kann in den Einstellungen des Konsolenagenten konfiguriert werden.

Wenn Sie die Größe Ihres Volumes ändern müssen, können Sie dies über den ONTAP System Manager in der Konsole tun.

Schritte

1. Klicken Sie auf die System Manager-Ansicht, um die Größe eines Volumes über den ONTAP System Manager zu ändern. Weitere Informationen finden Sie unter "Erste Schritte" .
2. Wählen Sie im linken Navigationsmenü **Speicher > Volumes** aus.
3. Identifizieren Sie in der Liste der Volumes das Volume, dessen Größe Sie ändern möchten.
4. Klicken Sie auf das Optionssymbol .
5. Wählen Sie **Größe ändern**.
6. Bearbeiten Sie auf dem Bildschirm **Volumegröße ändern** die Kapazität und den Prozentsatz der Snapshot-Reserve nach Bedarf. Sie können den vorhandenen, verfügbaren Platz mit der geänderten Kapazität vergleichen.
7. Klicken Sie auf **Speichern**.



Berücksichtigen Sie beim Ändern der Volumegröße unbedingt die Kapazitätsgrenzen Ihres Systems. Gehen Sie zum "Versionshinweise zu Cloud Volumes ONTAP" für weitere Informationen.

Ändern Sie den CIFS-Server

Wenn Sie Ihre DNS-Server oder Active Directory-Domäne ändern, müssen Sie den CIFS-Server in Cloud Volumes ONTAP ändern, damit er den Clients weiterhin Speicher bereitstellen kann.

Schritte

1. Klicken Sie auf der Registerkarte **Übersicht** des Cloud Volumes ONTAP Systems im rechten Bereich auf die Registerkarte **Funktion**.
2. Klicken Sie unter dem Feld „CIFS-Setup“ auf das **Bleistiftsymbol**, um das Fenster „CIFS-Setup“ anzuzeigen.
3. Geben Sie die Einstellungen für den CIFS-Server an:

Aufgabe	Aktion
Wählen Sie Storage VM (SVM)	Wenn Sie die Cloud Volume ONTAP Storage Virtual Machine (SVM) auswählen, werden die konfigurierten CIFS-Informationen angezeigt.
Beitretende Active Directory-Domäne	Der FQDN der Active Directory (AD)-Domäne, der der CIFS-Server beitreten soll.

Aufgabe	Aktion
Anmeldeinformationen, die zum Beitritt zur Domäne berechtigt sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
DNS Primäre und sekundäre IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgelisteten DNS-Server müssen die Service Location Records (SRV) enthalten, die zum Auffinden der Active Directory-LDAP-Server und Domänencontroller für die Domäne erforderlich sind, der der CIFS-Server beitritt. ifdef::gcp[] Wenn Sie Google Managed Active Directory konfigurieren, kann auf AD standardmäßig mit der IP-Adresse 169.254.169.254 zugegriffen werden. endif::gcp[]
DNS-Domäne	Die DNS-Domäne für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen ist die Domäne dieselbe wie die AD-Domäne.
NetBIOS-Name des CIFS-Servers	Ein CIFS-Servername, der in der AD-Domäne eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domäne, die mit dem CIFS-Server verknüpft werden soll. Der Standardwert ist CN=Computers. • Um AWS Managed Microsoft AD als AD-Server für Cloud Volumes ONTAP zu konfigurieren, geben Sie in dieses Feld **OU=Computers,OU=corp** ein. • Um Azure AD Domain Services als AD-Server für Cloud Volumes ONTAP zu konfigurieren, geben Sie in dieses Feld **OU=AADDC Computers** oder **OU=AADDC Users** ein."Azure-Dokumentation: Erstellen einer Organisationseinheit (OU) in einer von Azure AD Domain Services verwalteten Domäne" • Um Google Managed Microsoft AD als AD-Server für Cloud Volumes ONTAP zu konfigurieren, geben Sie in dieses Feld **OU=Computers,OU=Cloud** ein."Google Cloud-Dokumentation: Organisationseinheiten in Google Managed Microsoft AD"

4. Klicken Sie auf **Festlegen**.

Ergebnis

Cloud Volumes ONTAP aktualisiert den CIFS-Server mit den Änderungen.

Verschieben eines Volumes

Verschieben Sie Volumes zur Kapazitätsauslastung, Leistungsverbesserung und zur Erfüllung von Service-Level-Agreements.

Sie können ein Volume im ONTAP System Manager verschieben, indem Sie ein Volume und das Zielaggregat auswählen, den Volume-Verschiebungsvorgang starten und optional den Volume-Verschiebungsjob überwachen. Bei Verwendung des System Managers wird ein Volume-Verschiebungsvorgang automatisch abgeschlossen.

Schritte

1. Verwenden Sie ONTAP System Manager oder die ONTAP CLI, um die Volumes in das Aggregat zu verschieben.

   In den meisten Situationen können Sie den System Manager zum Verschieben von Volumes verwenden.

   Anweisungen hierzu finden Sie im"ONTAP 9 Volume Move Express-Handbuch" .

Verschieben Sie ein Volume, wenn die Konsole die Meldung „Aktion erforderlich“ anzeigt.

Die Konsole zeigt möglicherweise die Meldung „Aktion erforderlich“ an, die besagt, dass das Verschieben eines Volumes erforderlich ist, um Kapazitätsprobleme zu vermeiden, dass Sie das Problem jedoch selbst beheben müssen. In diesem Fall müssen Sie ermitteln, wie das Problem behoben werden kann, und dann ein oder mehrere Volumes verschieben.

> Die Konsole zeigt diese Meldungen „Aktion erforderlich“ an, wenn ein Aggregat 90 % seiner Kapazität erreicht hat. Wenn die Datenschichtung aktiviert ist, werden die Meldungen angezeigt, wenn ein Aggregat 80 % der genutzten Kapazität erreicht hat. Standardmäßig sind 10 % freier Speicherplatz für die Datenschichtung reserviert. "Erfahren Sie mehr über das Freispeicherverhältnis für Data Tiering" .

Schritte

1. wie Kapazitätsprobleme behoben werden können .
2. Verschieben Sie basierend auf Ihrer Analyse Volumes, um Kapazitätsprobleme zu vermeiden:
   - um Kapazitätsprobleme zu vermeiden .
   - um Kapazitätsprobleme zu vermeiden .

Ermitteln Sie, wie Kapazitätsprobleme behoben werden können

Wenn die Konsole keine Empfehlungen zum Verschieben eines Volumes zur Vermeidung von Kapazitätsproblemen bereitstellen kann, müssen Sie die Volumes identifizieren, die Sie verschieben müssen, und feststellen, ob Sie sie in ein anderes Aggregat auf demselben System oder in ein anderes System verschieben sollten.

Schritte

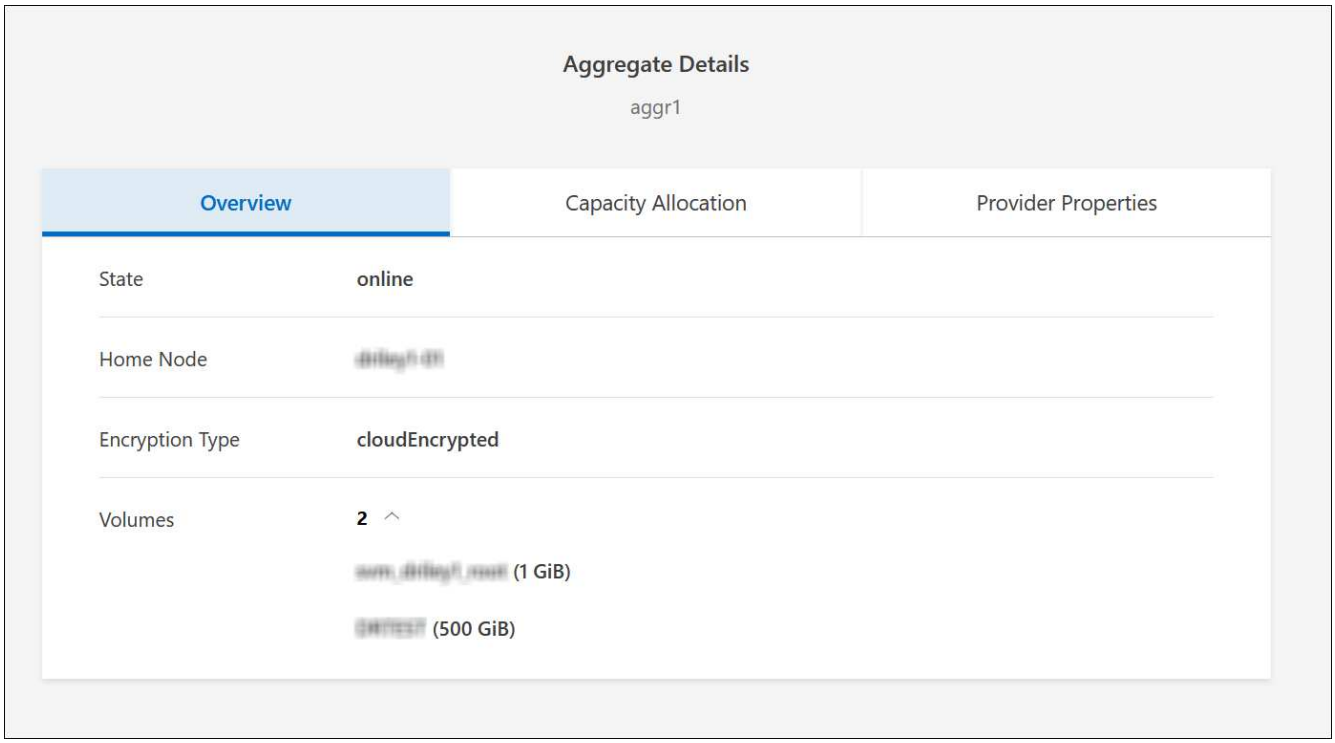
1. Sehen Sie sich die erweiterten Informationen in der Meldung „Aktion erforderlich“ an, um das Aggregat zu identifizieren, das seine Kapazitätsgrenze erreicht hat.

   Die erweiterten Informationen sollten beispielsweise in etwa wie folgt lauten: „Aggregat aggr1 hat seine Kapazitätsgrenze erreicht.“

2. Identifizieren Sie ein oder mehrere Volumes, die aus dem Aggregat verschoben werden sollen:

   a. Klicken Sie im Cloud Volumes ONTAP -System auf die Registerkarte **Aggregate**.
   b. Klicken Sie auf der Aggregatkachel auf das ••• Symbol und klicken Sie dann auf **Gesamtdetails anzeigen**.
   c. Überprüfen Sie auf der Registerkarte **Übersicht** des Bildschirms **Aggregatdetails** die Größe jedes Volumes und wählen Sie ein oder mehrere Volumes aus, die aus dem Aggregat verschoben werden sollen.

      Sie sollten Volumes auswählen, die groß genug sind, um Speicherplatz im Aggregat freizugeben, damit Sie in Zukunft zusätzliche Kapazitätsprobleme vermeiden.



3. Wenn das System das Festplattenlimit nicht erreicht hat, sollten Sie die Volumes auf ein vorhandenes Aggregat oder ein neues Aggregat auf demselben System verschieben.

   Weitere Informationen finden Sie unterVerschieben Sie Volumes auf ein anderes Aggregat, um Kapazitätsprobleme zu vermeiden .

4. Wenn das System das Festplattenlimit erreicht hat, führen Sie einen der folgenden Schritte aus:
   a. Löschen Sie alle nicht verwendeten Volumes.
   b. Ordnen Sie Volumes neu an, um Speicherplatz auf einem Aggregat freizugeben.

      Weitere Informationen finden Sie unterVerschieben Sie Volumes auf ein anderes Aggregat, um Kapazitätsprobleme zu vermeiden .

   c. Verschieben Sie zwei oder mehr Volumes auf ein anderes System mit freiem Speicherplatz.

      Weitere Informationen finden Sie unterVerschieben Sie Volumes auf ein anderes Aggregat, um Kapazitätsprobleme zu vermeiden .

Verschieben Sie Volumes auf ein anderes System, um Kapazitätsprobleme zu vermeiden

Sie können ein oder mehrere Volumes auf ein anderes Cloud Volumes ONTAP System verschieben, um Kapazitätsprobleme zu vermeiden. Dies ist möglicherweise erforderlich, wenn das System sein Festplattenlimit erreicht hat.

Informationen zu diesem Vorgang

Sie können die Schritte in dieser Aufgabe befolgen, um die folgende Meldung „Aktion erforderlich“ zu korrigieren:

Das Verschieben eines Volumes ist notwendig, um Kapazitätsprobleme zu vermeiden. Die Konsole kann diese Aktion jedoch nicht für Sie ausführen, da das System das Festplattenlimit erreicht hat.

Schritte

1. Identifizieren Sie ein Cloud Volumes ONTAP -System mit verfügbarer Kapazität oder stellen Sie ein neues System bereit.
2. Ziehen Sie das Quellsystem per Drag & Drop auf das Zielsystem, um eine einmalige Datenreplikation des Volumes durchzuführen.

   Weitere Informationen finden Sie unter"Daten zwischen Systemen replizieren" .
3. Gehen Sie zur Seite „Replikationsstatus“ und brechen Sie dann die SnapMirror -Beziehung ab, um das replizierte Volume von einem Datenschutzvolume in ein Lese-/Schreibvolume umzuwandeln.

   Weitere Informationen finden Sie unter"Verwalten von Datenreplikationszeitplänen und -beziehungen" .
4. Konfigurieren Sie das Volume für den Datenzugriff.

   Informationen zum Konfigurieren eines Zielvolumes für den Datenzugriff finden Sie im"ONTAP 9 Volume Disaster Recovery Express-Handbuch" .
5. Löschen Sie das ursprüngliche Volume.

   Weitere Informationen finden Sie unter"Verwalten von Volumes" .

Verschieben Sie Volumes auf ein anderes Aggregat, um Kapazitätsprobleme zu vermeiden

Sie können ein oder mehrere Volumes in ein anderes Aggregat verschieben, um Kapazitätsprobleme zu vermeiden.

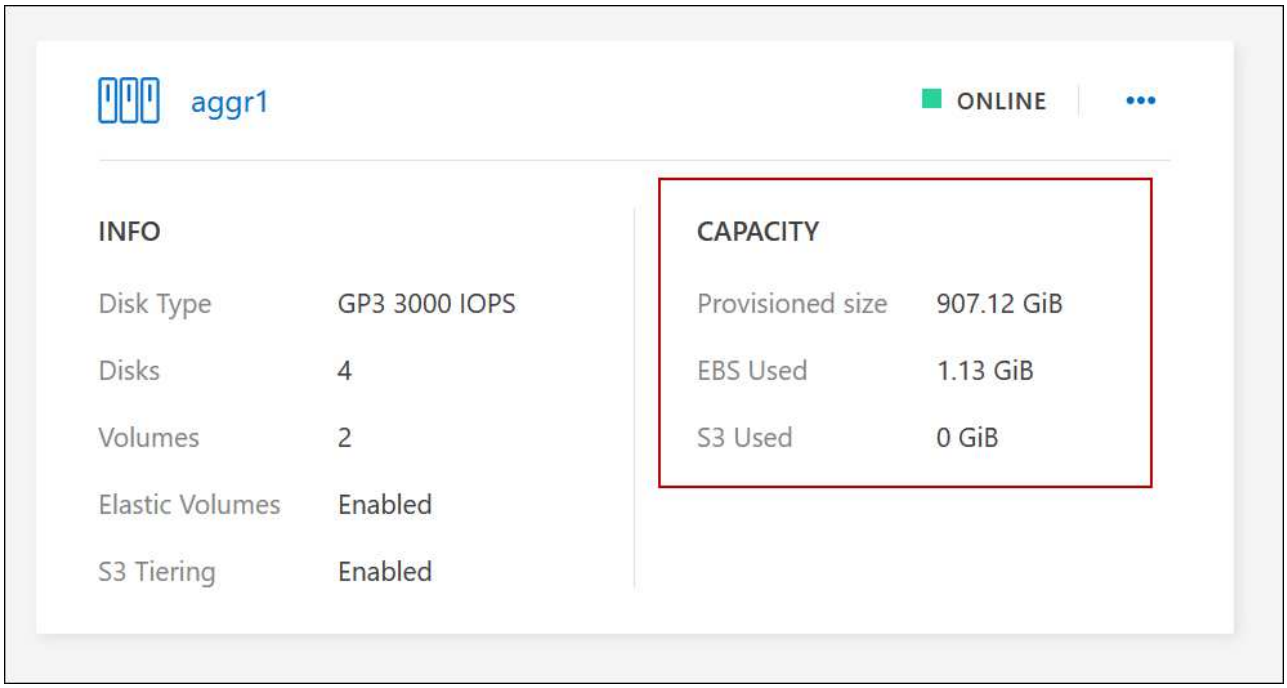
Informationen zu diesem Vorgang

Sie können die Schritte in dieser Aufgabe befolgen, um die folgende Meldung „Aktion erforderlich“ zu korrigieren:

Um Kapazitätsprobleme zu vermeiden, ist das Verschieben von zwei oder mehr Volumes erforderlich. Die Konsole kann diese Aktion jedoch nicht für Sie ausführen.

Schritte

1. Überprüfen Sie, ob ein vorhandenes Aggregat über freie Kapazität für die Volumes verfügt, die Sie verschieben müssen:
   a. Klicken Sie im Cloud Volumes ONTAP -System auf die Registerkarte **Aggregate**.
   b. Klicken Sie auf der gewünschten Aggregatkachel auf das ••• Symbol und dann **Aggregierte Details anzeigen**, um die verfügbare Kapazität anzuzeigen (bereitgestellte Größe abzüglich verwendeter aggregierter Kapazität).



2. Fügen Sie bei Bedarf Datenträger zu einem vorhandenen Aggregat hinzu:
   a. Wählen Sie das Aggregat aus und klicken Sie dann auf das ••• Symbol > **Datenträger hinzufügen**.
   b. Wählen Sie die Anzahl der hinzuzufügenden Datenträger aus und klicken Sie dann auf **Hinzufügen**.
3. Wenn keine Aggregate über verfügbare Kapazität verfügen, erstellen Sie ein neues Aggregat.

   Weitere Informationen finden Sie unter"Erstellen von Aggregaten" .
4. Verwenden Sie ONTAP System Manager oder die ONTAP CLI, um die Volumes in das Aggregat zu verschieben.
5. In den meisten Situationen können Sie den System Manager zum Verschieben von Volumes verwenden.

   Anweisungen hierzu finden Sie im"ONTAP 9 Volume Move Express-Handbuch" .

Gründe, warum eine Volumenbewegung langsam verlaufen kann

Das Verschieben eines Volumes kann länger dauern als erwartet, wenn eine der folgenden Bedingungen für Cloud Volumes ONTAP zutrifft:

- Das Volume ist ein Klon.
- Das Volume ist ein übergeordnetes Volume eines Klons.
- Das Quell- oder Zielaggregat verfügt über eine einzelne durchsatzoptimierte HDD-Festplatte (st1).
- Eines der Aggregate verwendet ein älteres Benennungsschema für Objekte. Beide Aggregate müssen dasselbe Namensformat verwenden.

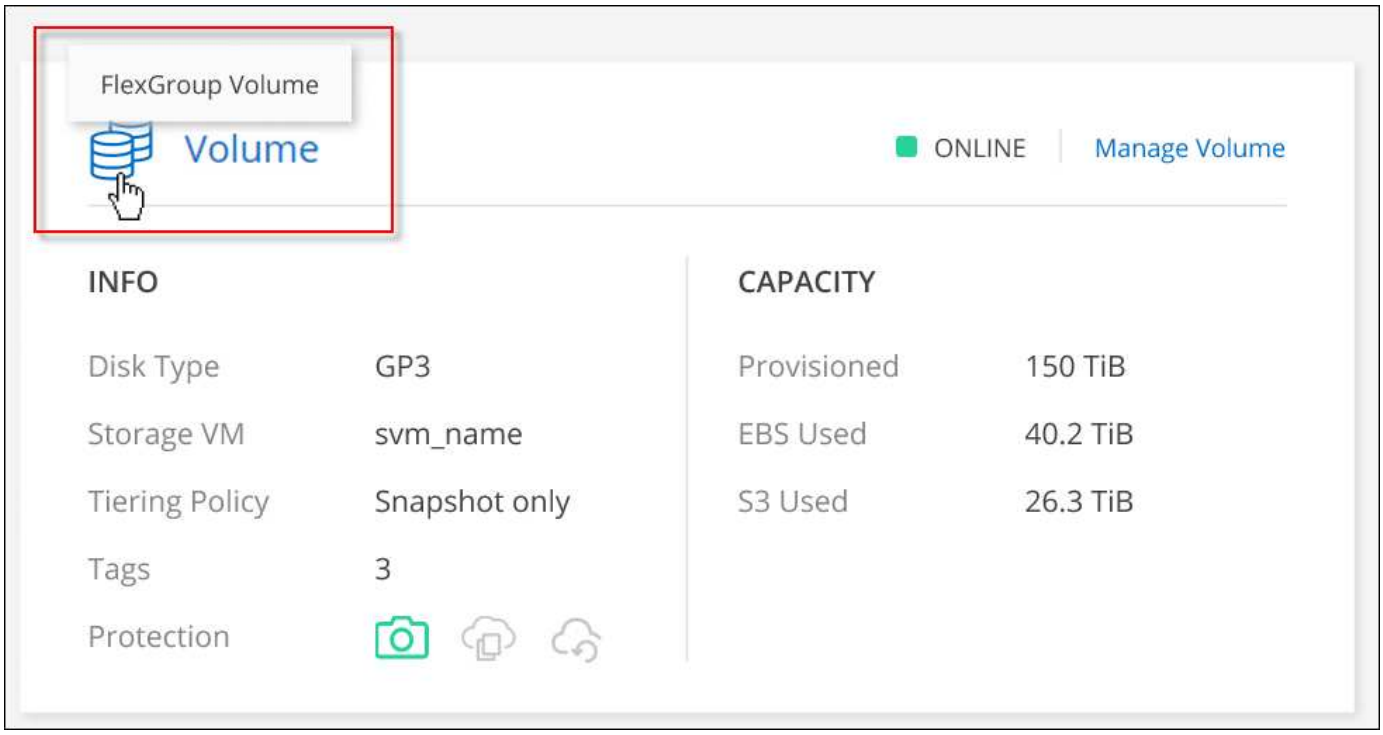
  Ein älteres Benennungsschema wird verwendet, wenn die Datenschichtung für ein Aggregat in der Version 9.4 oder früher aktiviert wurde.
- Die Verschlüsselungseinstellungen der Quell- und Zielaggregate stimmen nicht überein oder es wird eine Neuverschlüsselung durchgeführt.
- Beim Verschieben des Volumes wurde die Option *-tiering-policy* angegeben, um die Tiering-Richtlinie zu

ändern.

- Beim Verschieben des Volumes wurde die Option *-generate-destination-key* angegeben.

FlexGroup -Volumes anzeigen

Sie können FlexGroup Volumes, die über ONTAP System Manager oder die ONTAP CLI erstellt wurden, direkt über die Registerkarte „Volumes“ in der Konsole anzeigen. Sie können detaillierte Informationen zu den FleGroup-Volumes über eine spezielle Kachel **Volumes** anzeigen, in der Sie jede FlexGroup Volume-Gruppe über den Hover-Text des Symbols identifizieren können. Darüber hinaus können Sie FlexGroup Volumes in der Volume-Listenansicht über die Spalte „Volume-Stil“ identifizieren und sortieren.



Derzeit können Sie unter der Konsole nur vorhandene FlexGroup -Volumes anzeigen. Sie können in der Konsole keine FlexGroup Volumes erstellen.

Tieren Sie inaktive Cloud Volumes ONTAP Daten auf einen kostengünstigen Objektspeicher

Sie können die Speicherkosten für Cloud Volumes ONTAP senken, indem Sie eine SSD- oder HDD-Leistungsstufe für Hot Data mit einer Objektspeicherkapazitätsstufe für inaktive Daten kombinieren. Die Datenschichtung wird durch die FabricPool -Technologie ermöglicht. Eine allgemeine Übersicht finden Sie unter"Übersicht über Data Tiering" .

Um Data Tiering einzurichten, müssen Sie Folgendes tun:

1 **Wählen Sie eine unterstützte Konfiguration**

Die meisten Konfigurationen werden unterstützt. Wenn Sie über ein Cloud Volumes ONTAP -System mit der aktuellsten Version verfügen, können Sie loslegen. "Mehr erfahren" .

2 Stellen Sie die Konnektivität zwischen Cloud Volumes ONTAP und Objektspeicher sicher

- Für AWS benötigen Sie einen VPC-Endpunkt für Amazon Simple Storage Service (Amazon S3). Mehr erfahren.
- Für Azure müssen Sie nichts tun, solange die NetApp Console über die erforderlichen Berechtigungen verfügt. Mehr erfahren .
- Für Google Cloud müssen Sie das Subnetz für den privaten Google-Zugriff konfigurieren und ein Dienstkonto einrichten. Mehr erfahren .

3 Stellen Sie sicher, dass Sie über ein Aggregat mit aktiviertem Tiering verfügen

Um die Datenschichtung auf einem Datenträger zu aktivieren, muss sie auf einem Aggregat aktiviert werden. Sie sollten sich über die Anforderungen für neue und vorhandene Volumes im Klaren sein. dass Tiering für Aggregate aktiviert ist.,Mehr erfahren .

4 Wählen Sie eine Tiering-Richtlinie beim Erstellen, Ändern oder Replizieren eines Volumes

Die NetApp Console fordert Sie auf, eine Tiering-Richtlinie auszuwählen, wenn Sie ein Volume erstellen, ändern oder replizieren.

- "Tier-Daten von Lese-/Schreib-Volumes"
- "Tier-Daten aus Datenschutzvolumes"

Was ist für die Datenschichtung nicht erforderlich?

- Sie müssen keine Funktionslizenz installieren, um die Datenschichtung zu aktivieren.
- Sie müssen keinen Objektspeicher für die Kapazitätsebene erstellen. Die Konsole erledigt das für Sie.
- Sie müssen die Datenschichtung nicht auf Systemebene aktivieren.

  Die Konsole erstellt beim Erstellen des Systems einen Objektspeicher für kalte Daten.nachdem Sie die Anforderungen implementiert haben,solange es keine Verbindungs- oder Berechtigungsprobleme gibt . Danach müssen Sie nur noch das Daten-Tiering auf Volumes aktivieren (und in einigen Fällendass Tiering für Aggregate aktiviert ist.,auf Zuschlagstoffen).

Konfigurationen, die Daten-Tiering unterstützen

Sie können die Datenschichtung aktivieren, wenn Sie bestimmte Konfigurationen und Funktionen verwenden.

Unterstützung in AWS

- Daten-Tiering wird in AWS ab Cloud Volumes ONTAP 9.2 unterstützt.
- Die Leistungsstufe kann aus General Purpose SSDs (gp3 oder gp2) oder Provisioned IOPS SSDs (io1) bestehen.

Wir empfehlen, bei Verwendung von durchsatzoptimierten HDDs (st1) keine Datenschichtung in Objektspeicher vorzunehmen.

- Die inaktiven Daten werden in Amazon S3-Buckets verteilt. Eine Staffelung auf andere Anbieter wird nicht unterstützt.

Unterstützung in Azure

- Datentiering wird in Azure wie folgt unterstützt:
  - Version 9.4 in mit Einzelknotensystemen
  - Version 9.6 mit HA-Paaren
- Die Leistungsstufe kann aus verwalteten Premium-SSD-Datenträgern, verwalteten Standard-SSD-Datenträgern oder verwalteten Standard-HDD-Datenträgern bestehen.
- Die inaktiven Daten werden in Microsoft Azure Blob verschoben. Eine Staffelung auf andere Anbieter wird nicht unterstützt.

Unterstützung in Google Cloud

- Daten-Tiering wird in Google Cloud ab Cloud Volumes ONTAP 9.6 unterstützt.
- Die Leistungsstufe kann entweder aus persistenten SSD-Festplatten, ausgeglichenen persistenten Festplatten oder persistenten Standardfestplatten bestehen.
- Die inaktiven Daten werden in Google Cloud Storage gespeichert. Eine Staffelung auf andere Anbieter wird nicht unterstützt.

Interoperabilität von Funktionen

- Die Datenschichtung wird durch Verschlüsselungstechnologien unterstützt.
- Auf Volumes muss Thin Provisioning aktiviert sein.

Anforderungen

Abhängig von Ihrem Cloud-Anbieter müssen bestimmte Verbindungen und Berechtigungen eingerichtet werden, damit Cloud Volumes ONTAP kalte Daten in den Objektspeicher verschieben kann.

Anforderungen für das Tiering von Kaltdaten zu Amazon S3

Stellen Sie sicher, dass Cloud Volumes ONTAP eine Verbindung zu Amazon S3 hat. Der beste Weg, diese Verbindung bereitzustellen, ist das Erstellen eines VPC-Endpunkts für den S3-Dienst. Anweisungen finden Sie unter "AWS-Dokumentation: Erstellen eines Gateway-Endpunkts".

Achten Sie beim Erstellen des VPC-Endpunkts darauf, die Region, VPC und Routentabelle auszuwählen, die der Cloud Volumes ONTAP -Instanz entspricht. Sie müssen auch die Sicherheitsgruppe ändern, um eine ausgehende HTTPS-Regel hinzuzufügen, die den Datenverkehr zum S3-Endpunkt ermöglicht. Andernfalls kann Cloud Volumes ONTAP keine Verbindung zum S3-Dienst herstellen.

Wenn Probleme auftreten, lesen Sie "AWS Support Knowledge Center: Warum kann ich über einen Gateway-VPC-Endpunkt keine Verbindung zu einem S3-Bucket herstellen?" .

Anforderungen zum Tiering kalter Daten in Azure Blob Storage

Sie müssen keine Verbindung zwischen der Leistungsebene und der Kapazitätsebene einrichten, solange die Konsole über die erforderlichen Berechtigungen verfügt. Die Konsole aktiviert einen VNet-Dienstendpunkt für Sie, wenn die benutzerdefinierte Rolle für den Konsolenagenten über die folgenden Berechtigungen verfügt:

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

Die benutzerdefinierte Rolle umfasst standardmäßig die Berechtigungen. "Azure-Berechtigung für den Konsolen-Agent anzeigen"

Anforderungen zum Tiering kalter Daten in einen Google Cloud Storage-Bucket

- Das Subnetz, in dem sich Cloud Volumes ONTAP befindet, muss für privaten Google-Zugriff konfiguriert werden. Anweisungen hierzu finden Sie unter "Google Cloud-Dokumentation: Konfigurieren des privaten Google-Zugriffs" .
- An Cloud Volumes ONTAP muss ein Dienstkonto angehängt werden.

  "Erfahren Sie, wie Sie dieses Dienstkonto einrichten" .

  Sie werden aufgefordert, dieses Dienstkonto auszuwählen, wenn Sie ein Cloud Volumes ONTAP -System erstellen.

  Wenn Sie während der Bereitstellung kein Dienstkonto auswählen, müssen Sie Cloud Volumes ONTAP herunterfahren, die Google Cloud Console aufrufen und dann das Dienstkonto mit den Cloud Volumes ONTAP-Instanzen verknüpfen. Anschließend können Sie die Datenschichtung wie im nächsten Abschnitt beschrieben aktivieren.

- Um den Bucket mit vom Kunden verwalteten Verschlüsselungsschlüsseln zu verschlüsseln, aktivieren Sie die Verwendung des Schlüssels im Google Cloud Storage-Bucket.

  "Erfahren Sie, wie Sie vom Kunden verwaltete Verschlüsselungsschlüssel mit Cloud Volumes ONTAP verwenden" .

Aktivieren Sie Data Tiering, nachdem Sie die Anforderungen implementiert haben

Die Konsole erstellt beim Erstellen des Systems einen Objektspeicher für kalte Daten, sofern keine Verbindungs- oder Berechtigungsprobleme vorliegen. Wenn Sie die oben aufgeführten Anforderungen erst nach der Erstellung des Systems implementiert haben, müssen Sie das Tiering manuell über die API oder den ONTAP System Manager aktivieren, der den Objektspeicher erstellt.

Die Möglichkeit, Tiering über die Konsole zu aktivieren, wird in einer zukünftigen Version von Cloud Volumes ONTAP verfügbar sein.

Stellen Sie sicher, dass Tiering für Aggregate aktiviert ist.

Um Data Tiering auf einem Volume zu aktivieren, muss Data Tiering auf einem Aggregat aktiviert sein. Sie sollten sich über die Anforderungen für neue und vorhandene Volumes im Klaren sein.

- **Neue Bände**

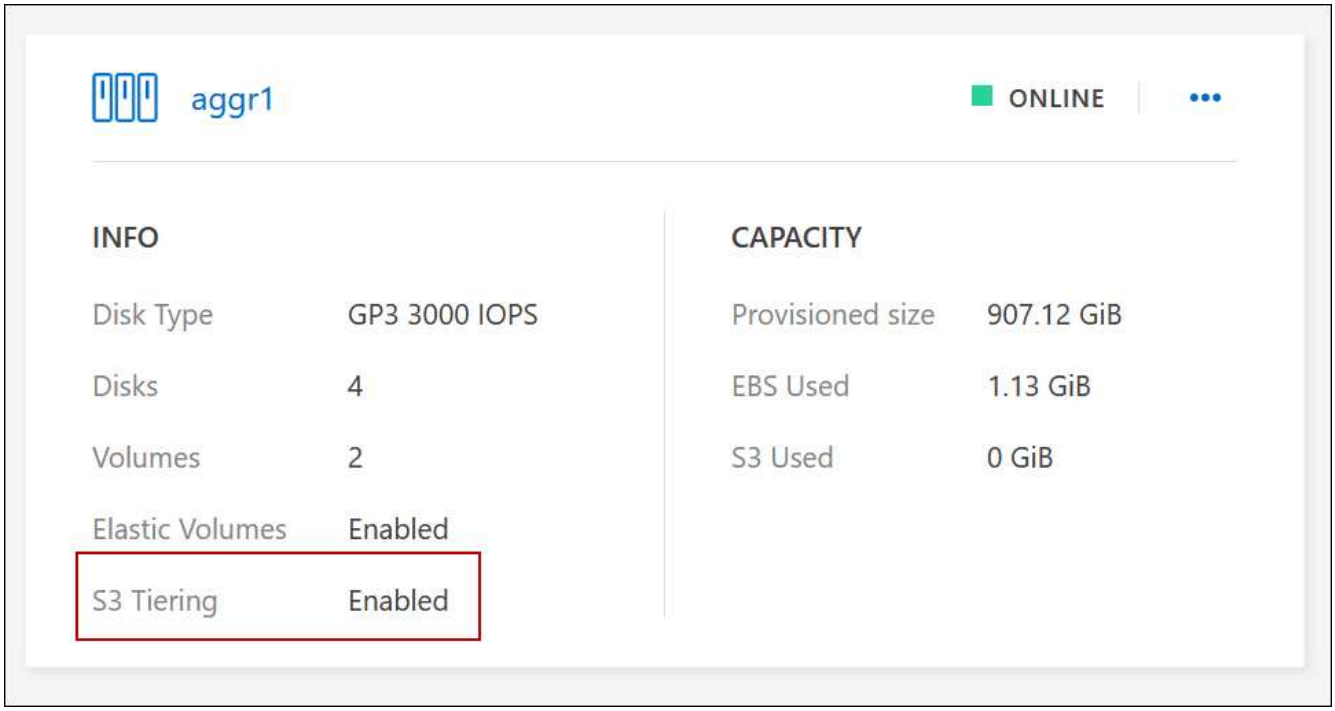
  Wenn Sie Data Tiering auf einem neuen Volume aktivieren, müssen Sie sich nicht um die Aktivierung von Data Tiering auf einem Aggregat kümmern. Die Konsole erstellt das Volume auf einem vorhandenen Aggregat mit aktiviertem Tiering oder erstellt ein neues Aggregat für das Volume, wenn noch kein Aggregat mit aktiviertem Data-Tiering vorhanden ist.

- **Vorhandene Bände**

  Um die Datenschichtung auf einem vorhandenen Volume zu aktivieren, stellen Sie sicher, dass sie auf dem zugrunde liegenden Aggregat aktiviert ist. Wenn die Datenaufteilung auf dem vorhandenen Aggregat nicht aktiviert ist, müssen Sie ONTAP System Manager verwenden, um ein vorhandenes Aggregat an den Objektspeicher anzuhängen.

Schritte zum Bestätigen, ob Tiering für ein Aggregat aktiviert ist

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Öffnen Sie das Cloud Volumes ONTAP System.
3. Wählen Sie die Registerkarte **Aggregate** aus und prüfen Sie, ob die Tiering-Funktion für das Aggregat aktiviert oder deaktiviert ist.



Schritte zum Aktivieren der Tiering-Funktion für ein Aggregat

1. Klicken Sie im ONTAP System Manager auf **Speicher > Tiers**.
2. Klicken Sie auf das Aktionsmenü für das Aggregat und wählen Sie **Cloud-Ebenen anhängen**.
3. Wählen Sie die anzuhängende Cloud-Ebene aus und klicken Sie auf **Speichern**.

Wie geht es weiter?

Sie können jetzt das Daten-Tiering auf neuen und vorhandenen Volumes aktivieren, wie im nächsten Abschnitt erläutert.

Tier-Daten von Lese-/Schreib-Volumes

Cloud Volumes ONTAP kann inaktive Daten auf Lese-/Schreib-Volumes in kostengünstigen Objektspeicher verschieben und so die Leistungsebene für Hot Data freigeben.

Schritte

1. Erstellen Sie auf der Registerkarte **Volumes** unter dem System ein neues Volume oder ändern Sie die

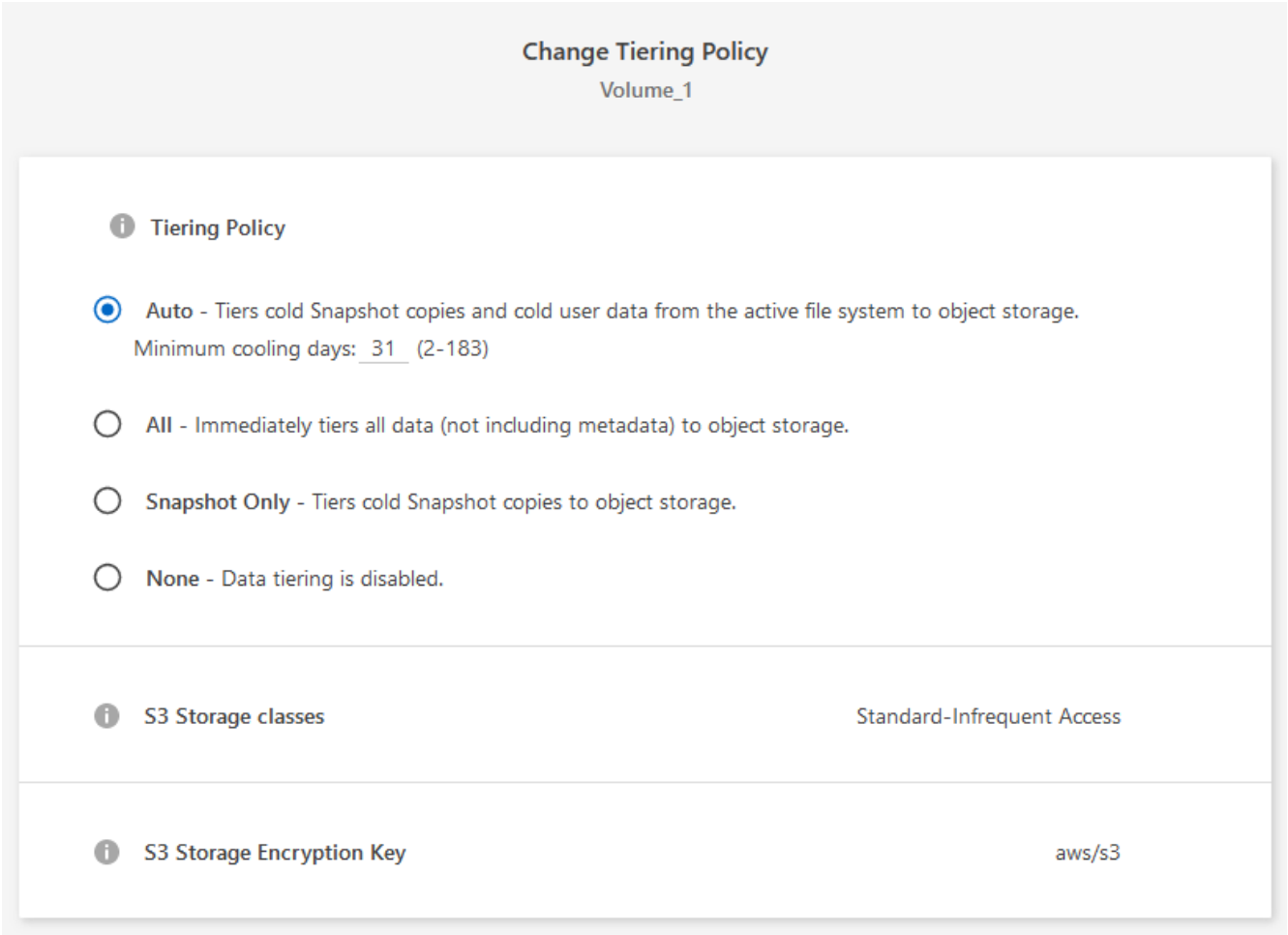
Ebene eines vorhandenen Volumes:

Aufgabe	Aktion
Erstellen eines neuen Volumes	Klicken Sie auf **Neues Volume hinzufügen**.
Ändern eines vorhandenen Volumes	Wählen Sie die gewünschte Volume-Kachel aus, klicken Sie auf **Volume verwalten**, um auf das rechte Fenster „Volumes verwalten“ zuzugreifen, und klicken Sie dann im rechten Fenster auf **Erweiterte Aktionen** und **Tiering-Richtlinie ändern**.

2. Wählen Sie eine Tiering-Richtlinie aus.

   Eine Beschreibung dieser Richtlinien finden Sie unter"Übersicht über Data Tiering" .

   Beispiel



   Die Konsole erstellt ein neues Aggregat für das Volume, wenn noch kein Aggregat mit aktivierter Datenschichtung vorhanden ist.

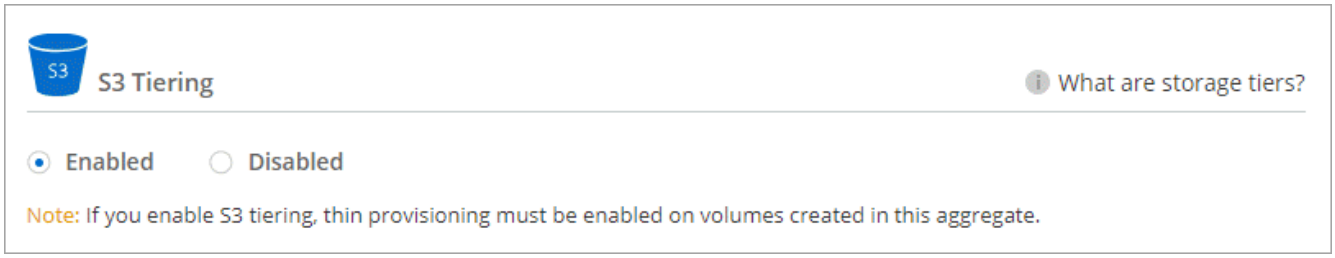
Tier-Daten aus Datenschutzvolumes

Cloud Volumes ONTAP kann Daten von einem Datenschutz-Volume auf eine Kapazitätsebene verschieben. Wenn Sie das Zielvolume aktivieren, werden die Daten beim Lesen schrittweise in die Leistungsstufe verschoben.

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Wählen Sie auf der Seite **Systeme** das Cloud Volumes ONTAP System aus, das das Quellvolume enthält, und ziehen Sie es dann auf das System, auf das Sie das Volume replizieren möchten.
3. Folgen Sie den Anweisungen, bis Sie die Tiering-Seite erreichen, und aktivieren Sie das Data Tiering für den Objektspeicher.

   Beispiel

   Hilfe zum Replizieren von Daten finden Sie unter "Daten in und aus der Cloud replizieren" .

Ändern der Speicherklasse für mehrstufige Daten

Nachdem Sie Cloud Volumes ONTAP bereitgestellt haben, können Sie Ihre Speicherkosten senken, indem Sie die Speicherklasse für inaktive Daten ändern, auf die 30 Tage lang nicht zugegriffen wurde. Wenn Sie auf die Daten zugreifen, sind die Zugriffskosten höher. Dies müssen Sie berücksichtigen, bevor Sie die Speicherklasse ändern.

Die Speicherklasse für mehrstufige Daten gilt systemweit – nicht pro Volume.

Informationen zu unterstützten Speicherklassen finden Sie unter"Übersicht über Data Tiering" .

Schritte

1. Klicken Sie im Cloud Volumes ONTAP System auf das Menüsymbol und dann auf **Speicherklassen** oder **Blob Storage Tiering**.
2. Wählen Sie eine Speicherklasse und klicken Sie dann auf **Speichern**.

Ändern des freien Speicherplatzverhältnisses für das Daten-Tiering

Das Verhältnis des freien Speicherplatzes für die Datenschichtung definiert, wie viel freier Speicherplatz auf Cloud Volumes ONTAP SSDs/HDDs erforderlich ist, wenn Daten in den Objektspeicher eingeschichtet werden. Die Standardeinstellung ist 10 % freier Speicherplatz, Sie können die Einstellung jedoch Ihren Anforderungen entsprechend anpassen.

Sie können beispielsweise weniger als 10 % freien Speicherplatz wählen, um sicherzustellen, dass Sie die gekaufte Kapazität nutzen. Die Konsole kann dann zusätzliche Festplatten für Sie kaufen, wenn zusätzliche Kapazität benötigt wird (bis Sie das Festplattenlimit für das Aggregat erreichen).

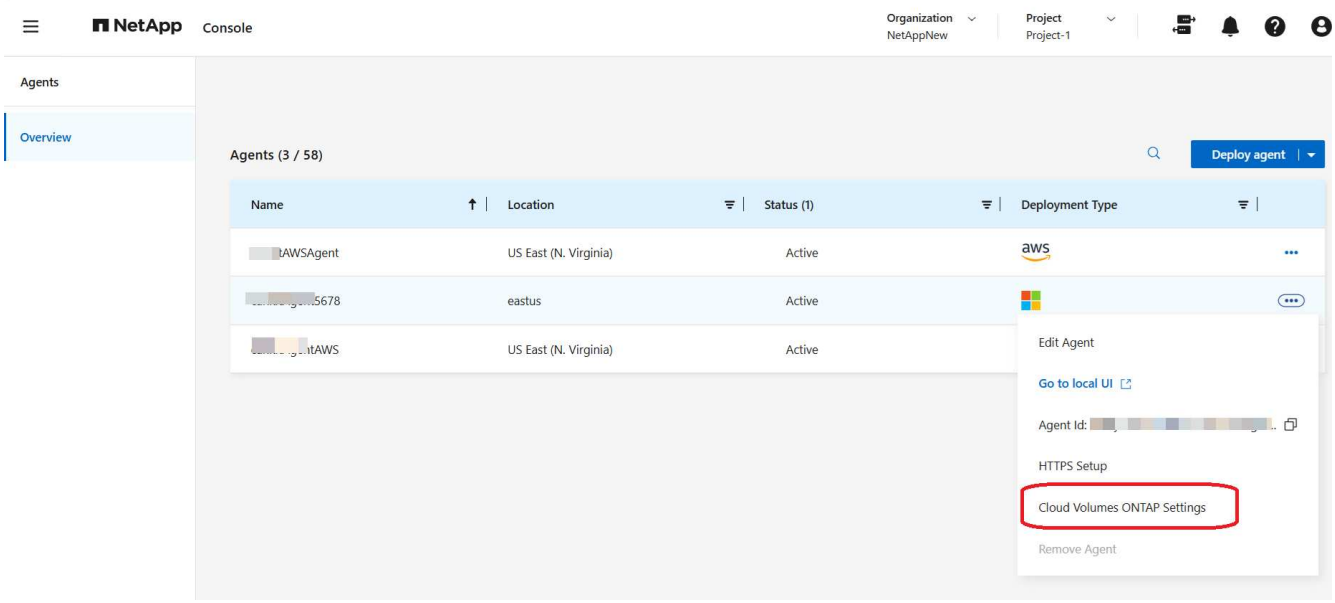
> Wenn nicht genügend Speicherplatz vorhanden ist, kann Cloud Volumes ONTAP die Daten nicht verschieben und es kann zu Leistungseinbußen kommen. Jede Änderung sollte mit Vorsicht vorgenommen werden. Wenn Sie unsicher sind, wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

Das Verhältnis ist für Notfallwiederherstellungsszenarien wichtig, da Cloud Volumes ONTAP beim Lesen der

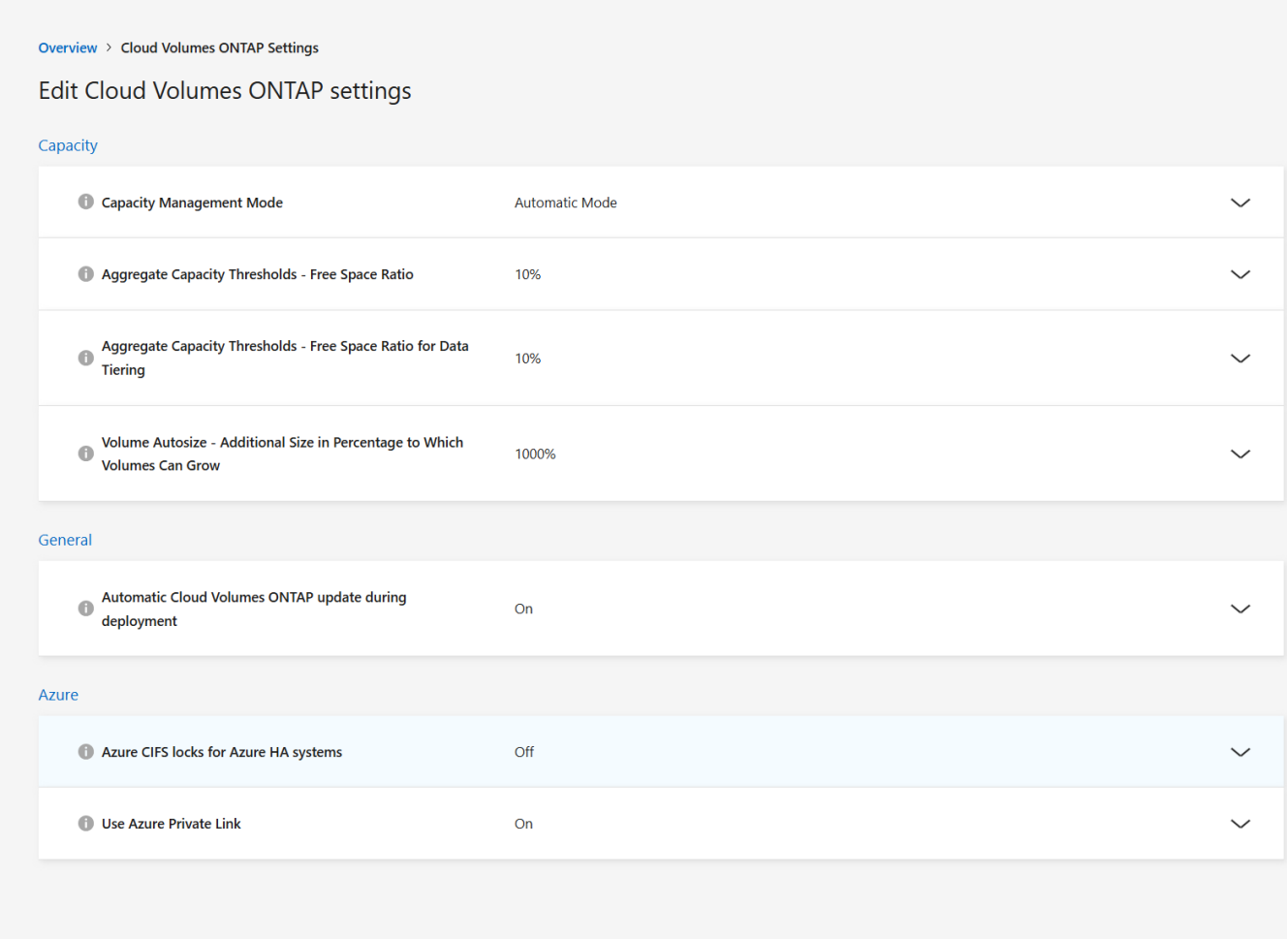
Daten aus dem Objektspeicher die Daten auf SSDs/HDDs verschiebt, um eine bessere Leistung zu erzielen. Wenn nicht genügend Speicherplatz vorhanden ist, kann Cloud Volumes ONTAP die Daten nicht verschieben. Berücksichtigen Sie dies bei der Änderung des Verhältnisses, damit Sie Ihren Geschäftsanforderungen gerecht werden können.

Schritte

1. Gehen Sie im linken Navigationsbereich zu **Administration > Agenten**.
2. Klicken Sie auf das ••• Symbol für den Konsolenagenten, der Ihr Cloud Volumes ONTAP -System verwaltet.
3. Wählen Sie * Cloud Volumes ONTAP -Einstellungen*.



4. Klicken Sie unter **Kapazität** auf **Schwellenwerte für aggregierte Kapazität – Verhältnis des freien Speicherplatzes für Daten-Tiering**.



5. Ändern Sie das Verhältnis des freien Speicherplatzes entsprechend Ihren Anforderungen und klicken Sie auf **Speichern**.

Ändern der Abkühlphase für die Auto-Tiering-Richtlinie

Wenn Sie das Daten-Tiering auf einem Cloud Volumes ONTAP Volume mithilfe der *auto*-Tiering-Richtlinie aktiviert haben, können Sie die Standard-Kühlperiode basierend auf Ihren Geschäftsanforderungen anpassen. Diese Aktion wird nur mit ONTAP CLI und API unterstützt.

Die Kühlperiode ist die Anzahl der Tage, die Benutzerdaten in einem Volume inaktiv bleiben müssen, bevor sie als „kalt“ betrachtet und in den Objektspeicher verschoben werden.

Die Standard-Abkühlungsperiode für die Auto-Tiering-Richtlinie beträgt 31 Tage. Sie können die Kühlperiode wie folgt ändern:

- 9.8 oder höher: 2 Tage bis 183 Tage
- 9.7 oder früher: 2 Tage bis 63 Tage

Schritt

1. Verwenden Sie den Parameter *minimumCoolingDays* mit Ihrer API-Anfrage, wenn Sie ein Volume erstellen oder ein vorhandenes Volume ändern.

Entfernen eines S3-Buckets bei der Außerbetriebnahme eines Systems

Sie können einen S3-Bucket mit den aus einem Cloud Volumes ONTAP System abgestuften Daten löschen, wenn Sie die Umgebung außer Betrieb nehmen.

Sie können den S3-Bucket nur löschen, wenn:

- Das Cloud Volume ONTAP -System wird aus der Konsole gelöscht.
- Alle Objekte werden aus dem Bucket gelöscht und der S3-Bucket ist leer.

Wenn Sie ein Cloud Volumes ONTAP -System außer Betrieb nehmen, wird der für die Umgebung erstellte S3-Bucket nicht automatisch gelöscht. Stattdessen verbleibt es in einem verwaisten Zustand, um einen versehentlichen Datenverlust zu verhindern. Sie können die Objekte im Bucket löschen und dann den S3-Bucket selbst entfernen oder ihn für die spätere Verwendung aufbewahren. Siehe "ONTAP CLI: vServer Object-Store-Server Bucket löschen" .

Stellen Sie von Ihrem Hostsystem aus eine Verbindung zu einem LUN auf Cloud Volumes ONTAP

Wenn Sie ein iSCSI-Volume erstellen, erstellt die NetApp Console automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volume erstellt haben, sodass keine Verwaltung erforderlich ist. Nachdem Sie das Volume erstellt haben, verwenden Sie den IQN, um von Ihren Hosts aus eine Verbindung mit der LUN herzustellen.

Beachten Sie Folgendes:

- Die automatische Kapazitätsverwaltung der Konsole gilt nicht für LUNs. Beim Erstellen einer LUN wird die Autogrow-Funktion deaktiviert.
- Sie können zusätzliche LUNs vom ONTAP System Manager oder der ONTAP CLI erstellen.

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Doppelklicken Sie auf der Seite **Systeme** auf das Cloud Volumes ONTAP -System, auf dem Sie Volumes verwalten möchten.
3. Wählen Sie im System die Registerkarte **Volumes**.
4. Gehen Sie zur Kachel des gewünschten Volumes und wählen Sie dann **Volume verwalten** aus, um auf das Bedienfeld „Volumes verwalten“ auf der rechten Seite zuzugreifen.
5. Klicken Sie auf **Ziel-iQN**.
6. Klicken Sie auf **Kopieren**, um den iQN-Namen zu kopieren.
7. Richten Sie eine iSCSI-Verbindung vom Host zur LUN ein.
    - "ONTAP 9 iSCSI Express-Konfiguration für Red Hat Enterprise Linux: Starten der iSCSI-Sitzungen mit dem Ziel"
    - "ONTAP 9 iSCSI Express-Konfiguration für Windows: Starten von iSCSI-Sitzungen mit dem Ziel"
    - "ONTAP SAN-Hostkonfiguration"

Beschleunigen Sie den Datenzugriff mit FlexCache -Volumes auf einem Cloud Volumes ONTAP System

Ein FlexCache -Volume ist ein Speichervolume, das SMB- und NFS-Lesedaten von einem Ursprungs- (oder Quell-)Volume zwischenspeichert. Nachfolgende Lesevorgänge der zwischengespeicherten Daten führen zu einem schnelleren Zugriff auf diese Daten.

Sie können FlexCache -Volumes verwenden, um den Datenzugriff zu beschleunigen oder den Datenverkehr von stark beanspruchten Volumes zu entlasten. FlexCache -Volumes tragen zur Leistungsverbesserung bei, insbesondere wenn Clients wiederholt auf dieselben Daten zugreifen müssen, da die Daten direkt bereitgestellt werden können, ohne dass auf das Ursprungsvolume zugegriffen werden muss. FlexCache -Volumes eignen sich gut für leseintensive System-Workloads.

NetApp Console ermöglicht die Verwaltung von FlexCache -Volumes mit der"NetApp Volume Caching" .

Sie können auch die ONTAP CLI oder den ONTAP System Manager verwenden, um FlexCache -Volumes zu erstellen und zu verwalten:

- "FlexCache -Volumes für schnelleren Datenzugriff – Power Guide"
- "Erstellen von FlexCache -Volumes im System Manager"

Arbeiten Sie mit FlexCache , wenn der Ursprung verschlüsselt ist

Beim Konfigurieren von FlexCache auf einem Cloud Volumes ONTAP System, bei dem das Ursprungsvolume verschlüsselt ist, sind zusätzliche Schritte erforderlich, um sicherzustellen, dass das FlexCache Volume ordnungsgemäß auf die verschlüsselten Daten zugreifen und diese zwischenspeichern kann.

Bevor Sie beginnen

1. **Verschlüsselungseinrichtung**: Stellen Sie sicher, dass das Quellvolume vollständig verschlüsselt und betriebsbereit ist. Bei Cloud Volumes ONTAP -Systemen umfasst dies die Integration mit Cloud-

spezifischen Schlüsselverwaltungsdiensten.

Bei AWS bedeutet dies normalerweise die Verwendung des AWS Key Management Service (KMS). Weitere Informationen finden Sie unter"Schlüssel mit AWS Key Management Service verwalten" .

Für Azure müssen Sie Azure Key Vault für NetApp Volume Encryption (NVE) einrichten. Weitere Informationen finden Sie unter"Verwalten von Schlüsseln mit Azure Key Vault" .

Bei Google Cloud ist es der Google Cloud Key Management Service. Weitere Informationen finden Sie unter"Schlüssel mit dem Cloud Key Management Service von Google verwalten" .

1. **Schlüsselverwaltungsdienste**: Überprüfen Sie vor dem Erstellen eines FlexCache -Volumes, ob die Schlüsselverwaltungsdienste auf dem Cloud Volumes ONTAP System richtig konfiguriert sind. Diese Konfiguration ist für das FlexCache -Volume unerlässlich, um die Daten vom Ursprungsvolume zu entschlüsseln.
2. **Lizenzierung**: Bestätigen Sie, dass eine gültige FlexCache -Lizenz verfügbar und auf dem Cloud Volumes ONTAP System aktiviert ist.
3. * ONTAP Version*: Stellen Sie sicher, dass die ONTAP Version Ihres Cloud Volumes ONTAP Systems FlexCache mit verschlüsselten Volumes unterstützt. Siehe die neuesten "ONTAP -Versionshinweise" oder Kompatibilitätsmatrix für weitere Informationen.
4. **Netzwerkkonfiguration**: Stellen Sie sicher, dass die Netzwerkkonfiguration eine nahtlose Kommunikation zwischen dem Ursprungsvolume und dem FlexCache -Volume ermöglicht. Dazu gehören das richtige Routing und die DNS-Auflösung in einer Cloud-Umgebung.

Schritte

Erstellen Sie ein FlexCache -Volume auf Ihrem Cloud Volumes ONTAP System mit einem verschlüsselten Quellvolume. Ausführliche Schritte und weitere Überlegungen finden Sie in den folgenden Abschnitten:

- "FlexCache -Volumes für schnelleren Datenzugriff – Power Guide"
- "Erstellen von FlexCache -Volumes im System Manager"

Aggregatverwaltung

Erstellen Sie ein Aggregat für Cloud Volumes ONTAP Systeme

Sie können Aggregate selbst erstellen oder dies bei der Volume-Erstellung von der NetApp Console für Sie erledigen lassen. Der Vorteil der eigenen Erstellung von Aggregaten besteht darin, dass Sie die zugrunde liegende Festplattengröße auswählen können. Dadurch können Sie Ihr Aggregat an die Kapazität oder Leistung anpassen, die Sie benötigen.

Alle Datenträger und Aggregate müssen direkt von der Konsole aus erstellt und gelöscht werden. Sie sollten diese Aktionen nicht von einem anderen Verwaltungstool aus durchführen. Dies kann die Systemstabilität beeinträchtigen, die Möglichkeit, in Zukunft Festplatten hinzuzufügen, einschränken und möglicherweise zu überflüssigen Gebühren des Cloud-Anbieters führen.

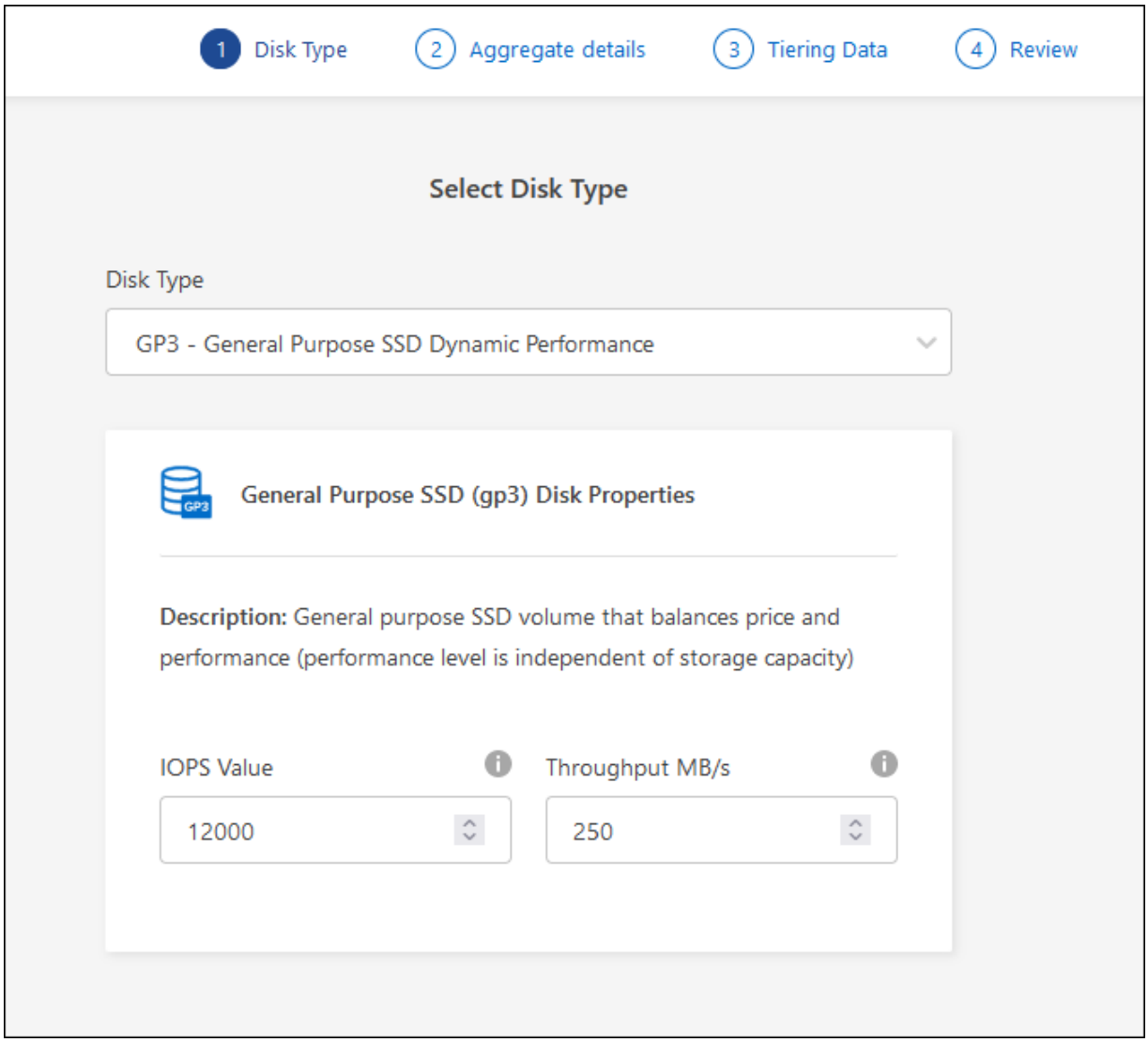
Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.

2. Doppelklicken Sie auf der Seite **Systeme** auf den Namen des Cloud Volumes ONTAP -Systems, auf dem Sie Aggregate verwalten möchten.
3. Klicken Sie auf der Registerkarte „Aggregate“ auf **Aggregat hinzufügen** und geben Sie dann Details für das Aggregat an.

AWS

- Wenn Sie aufgefordert werden, einen Datenträgertyp und eine Datenträgergröße auszuwählen, lesen Sie"Planen Sie Ihre Cloud Volumes ONTAP Konfiguration in AWS" .
- Wenn Sie aufgefordert werden, die Kapazitätsgröße des Aggregats einzugeben, erstellen Sie ein Aggregat auf einer Konfiguration, die die Funktion „Amazon EBS Elastic Volumes“ unterstützt. Der folgende Screenshot zeigt ein Beispiel eines neuen Aggregats, das aus GP3-Festplatten besteht.



"Erfahren Sie mehr über die Unterstützung für Elastic Volumes" .

Azurblau

Hilfe zu Datenträgertyp und Datenträgergröße finden Sie unter"Planen Sie Ihre Cloud Volumes ONTAP -Konfiguration in Azure" .

Google Cloud

Hilfe zu Datenträgertyp und Datenträgergröße finden Sie unter"Planen Sie Ihre Cloud Volumes ONTAP Konfiguration in Google Cloud" .

4. Klicken Sie auf **Hinzufügen** und dann auf **Genehmigen und kaufen**.

Verwalten von Aggregaten für Cloud Volumes ONTAP -Cluster

Verwalten Sie Aggregate selbst, indem Sie Datenträger hinzufügen, Informationen zu den Aggregaten anzeigen und sie löschen.

Alle Festplatten und Aggregate müssen direkt von der NetApp Console aus erstellt und gelöscht werden. Sie sollten diese Aktionen nicht von einem anderen Verwaltungstool aus durchführen. Dies kann die Systemstabilität beeinträchtigen, die Möglichkeit, in Zukunft Festplatten hinzuzufügen, einschränken und möglicherweise zu überflüssigen Gebühren des Cloud-Anbieters führen.

Bevor Sie beginnen

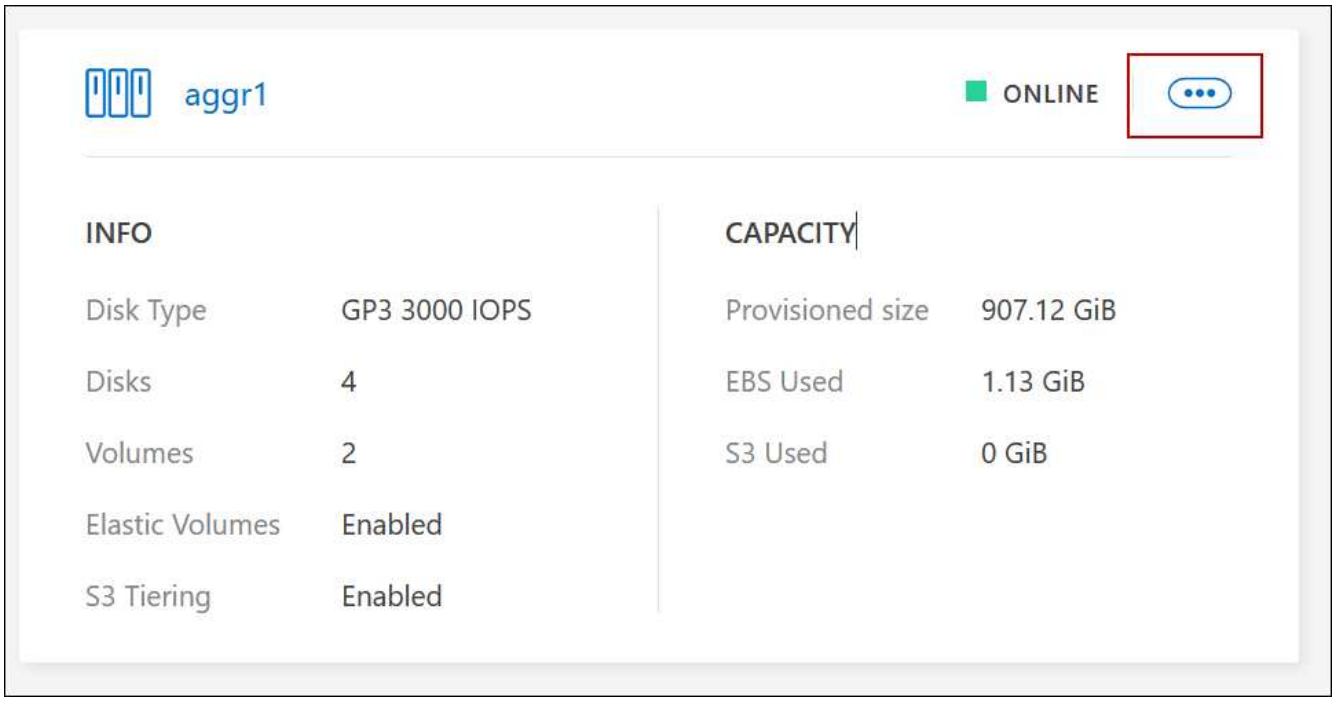
Wenn Sie ein Aggregat löschen möchten, müssen Sie zuerst die Volumes im Aggregat gelöscht haben.

Informationen zu diesem Vorgang

Wenn in einem Aggregat der Speicherplatz ausgeht, können Sie Volumes mithilfe des ONTAP System Manager auf ein anderes Aggregat verschieben.

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Doppelklicken Sie auf der Seite **Systeme** auf das Cloud Volumes ONTAP -System, auf dem Sie Aggregate verwalten möchten.
3. Klicken Sie in den Systemdetails auf die Registerkarte **Aggregate**.
4. Klicken Sie für das gewünschte Aggregat auf das ••• Symbol für die Verwaltungsaktionen.



5. Verwalten Sie Ihre Aggregate über die verfügbaren Optionen im ••• Speisekarte.

Um einem Aggregat Festplatten hinzuzufügen, müssen alle Festplatten im Aggregat dieselbe Größe haben.

Für AWS können Sie die Kapazität eines Aggregats erhöhen, das Amazon EBS Elastic Volumes unterstützt.

1. Unter dem ••• Klicken Sie im Menü auf **Kapazität erhöhen**.
2. Geben Sie die zusätzliche Kapazität ein, die Sie hinzufügen möchten, und klicken Sie dann auf **Erhöhen**.

Beachten Sie, dass Sie die Kapazität des Aggregats um mindestens 256 GiB oder 10 % der Aggregatgröße erhöhen müssen. Wenn Sie beispielsweise ein Aggregat von 1,77 TiB haben, sind 10 % 181 GiB. Das ist weniger als 256 GiB, daher muss die Größe des Aggregats um das Minimum von 256 GiB erhöht werden.

Verwalten Sie die Gesamtkapazität von Cloud Volumes ONTAP auf einem Konsolenagenten

Jeder Konsolenagent verfügt über Einstellungen, die bestimmen, wie er die Gesamtkapazität für Cloud Volumes ONTAP verwaltet.

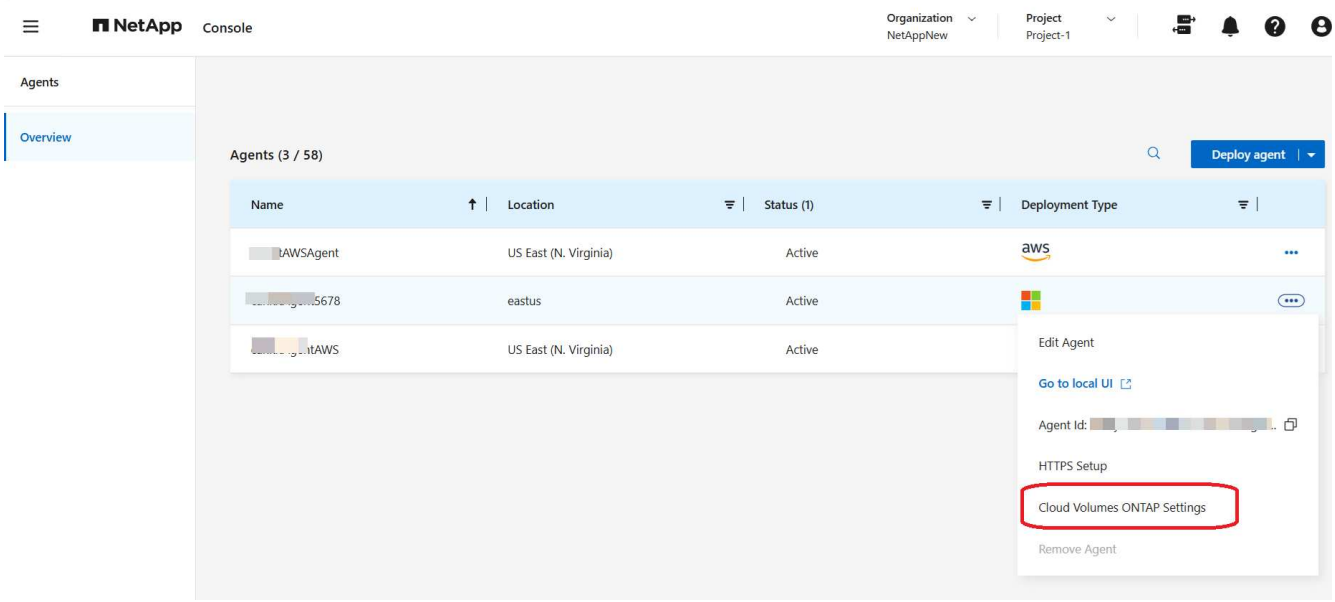
Diese Einstellungen wirken sich auf alle Cloud Volumes ONTAP Systeme aus, die von einem Konsolenagenten verwaltet werden. Wenn Sie einen anderen Konsolenagenten haben, kann dieser anders konfiguriert werden.

Erforderliche Berechtigungen

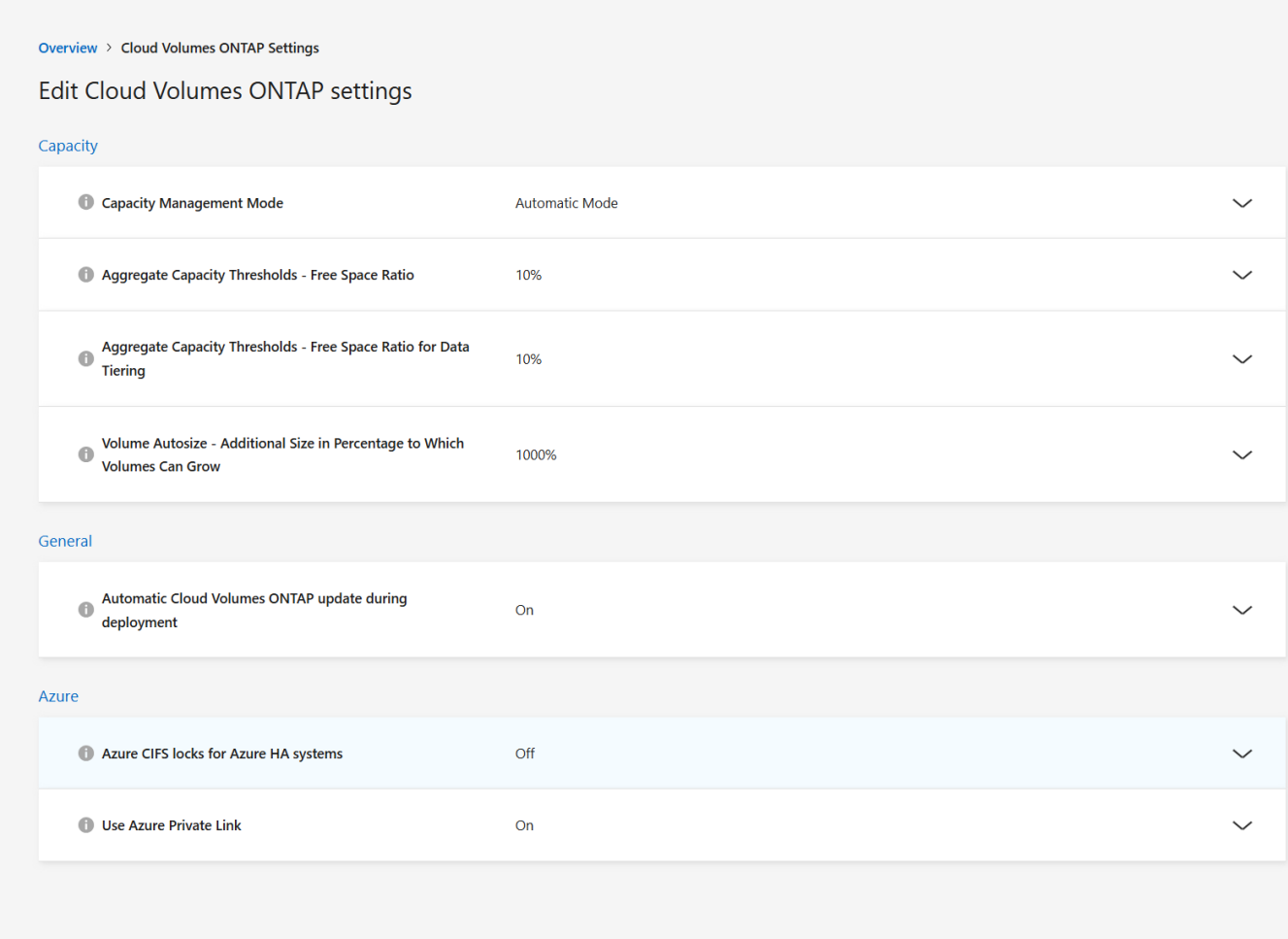
Sie benötigen die Organisations- oder Kontoadministratorrechte der NetApp Console, um die Cloud Volumes ONTAP -Einstellungen zu ändern.

Schritte

1. Gehen Sie im linken Navigationsbereich zu **Administration > Agenten**.
2. Klicken Sie auf das ••• Symbol für den Konsolenagenten, der Ihr Cloud Volumes ONTAP -System verwaltet.
3. Wählen Sie * Cloud Volumes ONTAP -Einstellungen*.



4. Ändern Sie unter **Kapazität** die folgenden Einstellungen:



Kapazitätsverwaltungsmodus

Wählen Sie, ob die Konsole Sie über Entscheidungen zur Speicherkapazität benachrichtigen oder ob sie die Kapazitätsanforderungen automatisch für Sie verwalten soll.

"Erfahren Sie, wie der Kapazitätsverwaltungsmodus funktioniert" .

Verhältnis zwischen aggregierter Kapazitätsschwelle und freiem Speicherplatz

Dieses Verhältnis ist ein Schlüsselparameter bei Entscheidungen zum Kapazitätsmanagement und es ist wichtig, seine Auswirkungen zu verstehen, unabhängig davon, ob Sie sich im automatischen oder manuellen Modus des Kapazitätsmanagements befinden. Es wird empfohlen, diesen Schwellenwert unter Berücksichtigung Ihres spezifischen Speicherbedarfs und des erwarteten Wachstums festzulegen, um ein Gleichgewicht zwischen Ressourcennutzung und Kosten zu wahren.

Wenn im manuellen Modus das Verhältnis des freien Speicherplatzes auf einem Aggregat unter den angegebenen Schwellenwert fällt, wird eine Benachrichtigung ausgelöst, die Sie darauf hinweist, dass Sie Maßnahmen ergreifen sollten, um das niedrige Verhältnis des freien Speicherplatzes zu beheben. Es ist wichtig, diese Benachrichtigungen zu überwachen und die Gesamtkapazität manuell zu verwalten, um Dienstunterbrechungen zu vermeiden und eine optimale Leistung sicherzustellen.

Das Verhältnis des freien Speicherplatzes wird wie folgt berechnet: (aggregierte Kapazität – insgesamt genutzte Kapazität auf dem Aggregat) / aggregierte Kapazität

Siehe"Automatisches Kapazitätsmanagement" Erfahren Sie jetzt, wie die Kapazität in Cloud Volumes ONTAP automatisch verwaltet wird.

Schwellenwerte für aggregierte Kapazität – Verhältnis des freien Speicherplatzes für Data Tiering

Definiert, wie viel freier Speicherplatz auf der Leistungsebene (Festplatten) erforderlich ist, wenn Daten auf eine Kapazitätsebene (Objektspeicher) verschoben werden.

Das Verhältnis ist für Notfallwiederherstellungsszenarien wichtig. Wenn Daten aus der Kapazitätsebene gelesen werden, verschiebt Cloud Volumes ONTAP die Daten in die Leistungsebene, um eine bessere Leistung zu erzielen. Wenn nicht genügend Speicherplatz vorhanden ist, kann Cloud Volumes ONTAP die Daten nicht verschieben.

5. Klicken Sie auf **Speichern**.

Verwalten der Festplattenleistung in Azure

Verwalten der Premium-SSD-v2-Festplattenleistung für Cloud Volumes ONTAP in Azure

Sie können die Leistung von Cloud Volumes ONTAP in Azure optimieren, indem Sie die IOPS- und Durchsatzparameter für Premium SSD v2-Datenträger konfigurieren. Diese Funktionalität ist nur verfügbar, wenn Cloud Volumes ONTAP bereits mit dem Festplattentyp Azure Premium SSD v2 bereitgestellt wurde, nicht jedoch während der Erstbereitstellung. Durch die Leistungssteigerung können Sie die volle Flexibilität und die Hochleistungsfähigkeit von Azure Premium SSD v2-Datenträgern nutzen.

Premium SSD v2-Festplatten unterstützen Workloads, die eine schnelle, zuverlässige Leistung mit niedriger Latenz, hoher IOPS und hohem Durchsatz erfordern. Durch Anpassen der IOPS- und Durchsatzeinstellungen können Sie die Leistung der Aggregate in Ihrer Bereitstellung individuell anpassen. Weitere Informationen zu Premium SSD v2-Festplatten finden Sie unter "Setzen Sie eine Premium SSD v2-Festplatte ein." Die

Nutzen Sie die APIs, um den Prozess zum Ändern der Einstellungen der Premium SSD v2-Festplatte zu automatisieren. Informationen zum Ausführen von Cloud Volumes ONTAP -API-Aufrufen finden Sie unter "Ihr erster API-Aufruf" Die

Informationen zu diesem Vorgang

- Diese Funktion gilt für Cloud Volumes ONTAP Bereitstellungen in Azure-Einzelverfügbarkeitszonen.
- Durch eine einheitliche Änderung der Festplatteneinstellungen wird die Leistung der RAID-Gruppe bzw. des RAID-Aggregats verändert. Die Leistung aller Festplatten im Aggregat wird auf das gleiche Niveau angepasst, um eine konsistente Leistung im gesamten Aggregat zu gewährleisten.
- Die Änderungen betreffen ein einzelnes Aggregat und nicht andere Aggregate innerhalb einer Gruppe.
- Premium SSD v2-Festplatten, die während der Cloud Volumes ONTAP Bereitstellung oder Kapazitätsoptimierung in der NetApp Console automatisch bereitgestellt oder über die APIs hinzugefügt werden, können alle modifiziert werden.
- Eine Größenänderung der Festplatte (Änderung der Festplattenkapazität) wird nicht unterstützt.

Bevor Sie beginnen

Beachten Sie folgende Punkte, bevor Sie die IOPS- und Durchsatzparameter für Premium SSD v2-Festplatten konfigurieren:

- Stellen Sie sicher, dass Sie ausschließlich Premium SSD v2-Datenträger ausgewählt haben. Premium SSD v1-Festplatten oder Root- und Boot-Festplatten sind von dieser Änderung ausgeschlossen.
- Verwenden Sie die von Cloud Volumes ONTAP während der Bereitstellung festgelegten vorkonfigurierten Basiseinstellungen als minimale IOPS- und Durchsatzwerte für die jeweilige Festplattengröße. Diese

Grundeinstellungen entsprechen den Leistungseigenschaften der Premium SSD v1.

- Stellen Sie die IOPS- und Durchsatzwerte auf oder über dem Mindestwert für Ihre Festplattengröße ein. Beispielsweise sollte bei einer Festplattengröße von 1 TB der minimale IOPS-Wert auf 5.000 und der minimale Durchsatzwert auf 200 MB/s eingestellt werden. Sie können Werte konfigurieren, die höher als diese Mindestwerte sind, aber nicht niedriger.
- Konfigurieren Sie die Werte innerhalb der unterstützten Premium SSD v2-Bereiche: IOPS zwischen 3000 und 80000 und Durchsatz zwischen 125 und 1200 MB/s.
- Stellen Sie sicher, dass die Größe Ihrer Premium SSD v2-Festplatte im unterstützten Bereich von 500 GB bis 32 TB für Cloud Volumes ONTAP in Azure liegt. Beachten Sie, dass diese Größenbeschränkungen von den von Azure für Premium SSD v2-Festplatten angebotenen Minimal- und Maximalwerten abweichen.

Schritte

- Verwenden Sie den folgenden API-Aufruf, um die Attributwerte für IOPS und Durchsatz zu ändern:

  Sie können diese API maximal viermal innerhalb eines 24-Stunden-Zeitraums aufrufen.

  ```
  PUT /azure/vsa/aggregates/{workingEnvironmentId}/{aggregateName}
  ```

  Fügen Sie die folgenden Parameter in den Anforderungstext ein:

  ```
  {
    "aggregateName": "aggr_name",
    "iops": "modified_iops_value",
    "throughput": "modified_throughput_value",
    "workingEnvironmentId": "we_id"
  }
  ```

Nach Abschluss

Nachdem die API eine Antwort zurückgegeben hat, die anzeigt, dass der Vorgang erfolgreich war, überprüfen Sie die geänderten Parameter, indem Sie die Datenträgerdetails im Azure-Portal für Ihr Cloud Volumes ONTAP System überprüfen.

Ähnliche Informationen

- "Vorbereiten der Verwendung der API"
- "Cloud Volumes ONTAP -Workflows"
- "Abrufen der erforderlichen Kennungen"
- "REST-APIs für Cloud Volumes ONTAP verwenden"
- "Premium SSD v2 mit VMs in Verfügbarkeitsgruppen verwenden"

Ändern der Leistungsstufe von Premium-SSD-Festplatten in Cloud Volumes ONTAP in Azure

Sie können die Leistungsstufe von Premium SSD-verwalteten Datenträgern in Cloud Volumes ONTAP in Azure über das Azure-Portal erhöhen. Dies ist ein manueller Prozess, bei dem die Festplattenebene jeder Premium-SSD-Festplatte auf eine leistungsstärkere Ebene geändert wird. Durch die Änderung der Leistungsstufe Ihrer NVRAM Festplatte können Leistungsengpässe behoben und die Effizienz Ihres Cloud Volumes ONTAP

Systems verbessert werden, indem höhere IOPS- und Durchsatzkapazitäten bereitgestellt werden.

Stellen Sie sicher, dass Sie mit dem NetApp -Support zusammenarbeiten, um festzustellen, ob der Engpass in Ihrer Umgebung auf die NVRAM Festplatte zurückzuführen ist und ob ein Upgrade der Speicherebene das Problem behebt.

Informationen zu diesem Vorgang

- Standardmäßig verwendet Cloud Volumes ONTAP in Azure Premium-SSD-Festplatten für NVRAM in der P20-Tierstufe. Die P20-Leistungsstufe bietet eine ausgewogene Performance, die für die meisten Arbeitslasten geeignet ist. Wenn Ihre Arbeitslast jedoch eine höhere Leistung erfordert, können Sie die NVRAM Festplatte auf eine höhere Stufe wie z. B. P30 aufrüsten.

  Derzeit ist ein Upgrade einer NVRAM Festplatte von der P20- auf die P30-Stufe nur über das Azure-Portal möglich.

- Sie ändern die Größe der Festplatte nicht. Die Größe beträgt weiterhin 512 GB. Dieses Verfahren ändert lediglich die Leistungsstufe der Festplatte.

Bevor Sie beginnen

- Prüfen Sie sorgfältig, ob diese Änderung notwendig ist, da ein Upgrade der NVRAM Festplatte auf eine höhere Leistungsstufe zusätzliche Kosten verursacht.
- Ihre Cloud Volumes ONTAP Version muss 9.11.1 oder höher sein. Bei älteren Versionen können Sie auf Version 9.11.1 oder höher aktualisieren oder einen Feature Policy Variation Request (FPVR) beim NetApp -Support einreichen.

Schritte

Dieses Szenario geht von zwei Knoten aus. `node01` Und `node02` in der Cloud Volumes ONTAP Hochverfügbarkeits- (HA) Bereitstellung. Verwenden Sie das Azure-Portal, um die Tarifstufe zu aktualisieren.

1. Führen Sie diesen Befehl aus, um Folgendes zu erstellen `node1` der aktive Knoten. Manuelles Failover `node02`Die

   ```
   storage failover takeover -ofnode <Node02>
   ```

2. Sign in .
3. Sobald die Übernahme abgeschlossen ist, wechseln Sie zur VM-Instanz für `node02`Klicken Sie auf die Schaltfläche **Stopp**, um es auszuschalten.
4. Navigieren Sie zur Ressourcengruppe für `node02` Wählen Sie in der Liste der Datenträger den NVRAM Datenträger aus, dessen Ebene Sie ändern möchten.
5. Wählen Sie **Größe + Leistung**.
6. Wählen Sie im Dropdown-Menü **Leistungsstufe** die Option aus `P30 - 5000 IOPS, 200MB/s`Die
7. Wählen Sie **Größe ändern**.
8. Schalten Sie den/die/das `node02` Beispiel.
9. Überprüfen Sie die Azure-Seriellkonsole, bis die Meldung angezeigt wird: `waiting for giveback`Die
10. Führen Sie diesen Befehl aus, um zurückzugeben `node02`:

    ```
    storage failover giveback -ofnode <Node02>
    ```

11. Wiederholen Sie diese Schritte am `node01` um zu machen `node02` übernehmen `node01`damit Sie die NVRAM Disk-Ebene für `node01`Die

Nach Abschluss

Wenn Sie beide Knoten eingeschaltet haben, überprüfen Sie die geänderten Parameter, indem Sie die Datenträgerdetails im Azure-Portal für Ihr Cloud Volumes ONTAP System überprüfen.

Ähnliche Informationen

- Azure-Dokumentation: "Ändern Sie Ihre Leistungsstufe ohne Ausfallzeiten."
- Wissensdatenbank für das Support-Team: "So erhöhen Sie die Leistungsstufe eines NVRAM Datenträgers in Azure CVO"
- "Aktualisieren Sie die Cloud Volumes ONTAP Softwareversionen"

Storage-VM-Verwaltung

Verwalten Sie Speicher-VMs für Cloud Volumes ONTAP

Eine Storage-VM ist eine virtuelle Maschine, die innerhalb von ONTAP ausgeführt wird und Ihren Clients Speicher- und Datendienste bereitstellt. Sie kennen dies möglicherweise als *SVM* oder *vServer*. Cloud Volumes ONTAP ist standardmäßig mit einer Speicher-VM konfiguriert, einige Konfigurationen unterstützen jedoch zusätzliche Speicher-VMs.

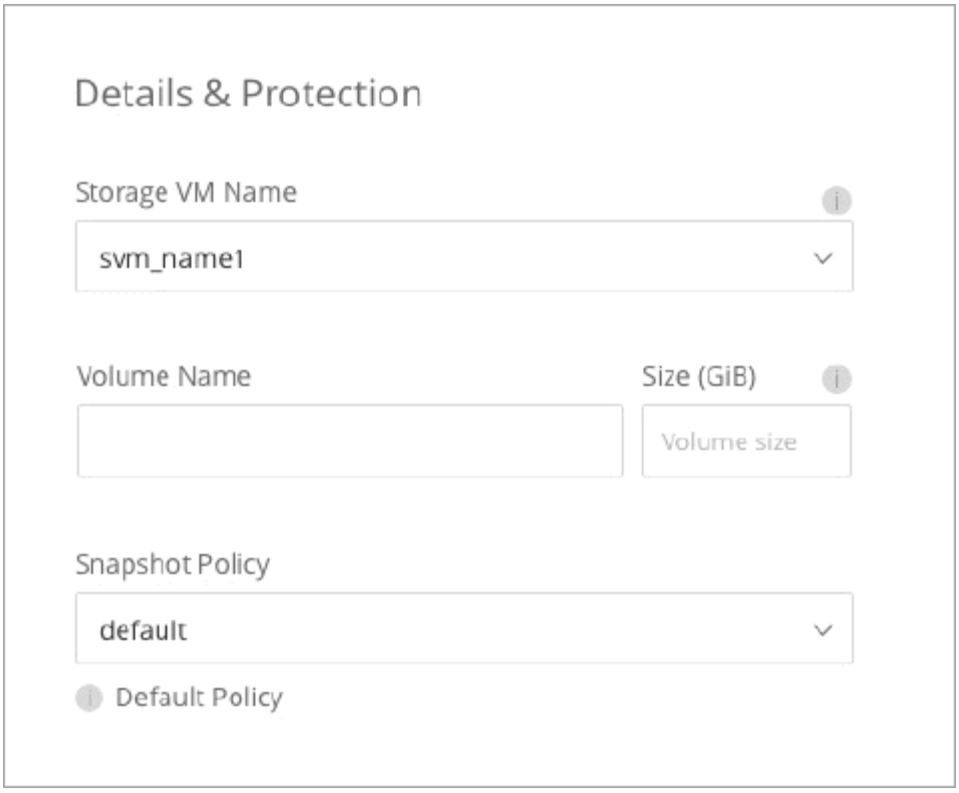
Unterstützte Anzahl von Speicher-VMs

Bei bestimmten Konfigurationen werden mehrere Speicher-VMs unterstützt. Gehen Sie zum "Versionshinweise zu Cloud Volumes ONTAP" um die unterstützte Anzahl von Speicher-VMs für Ihre Version von Cloud Volumes ONTAP zu überprüfen.

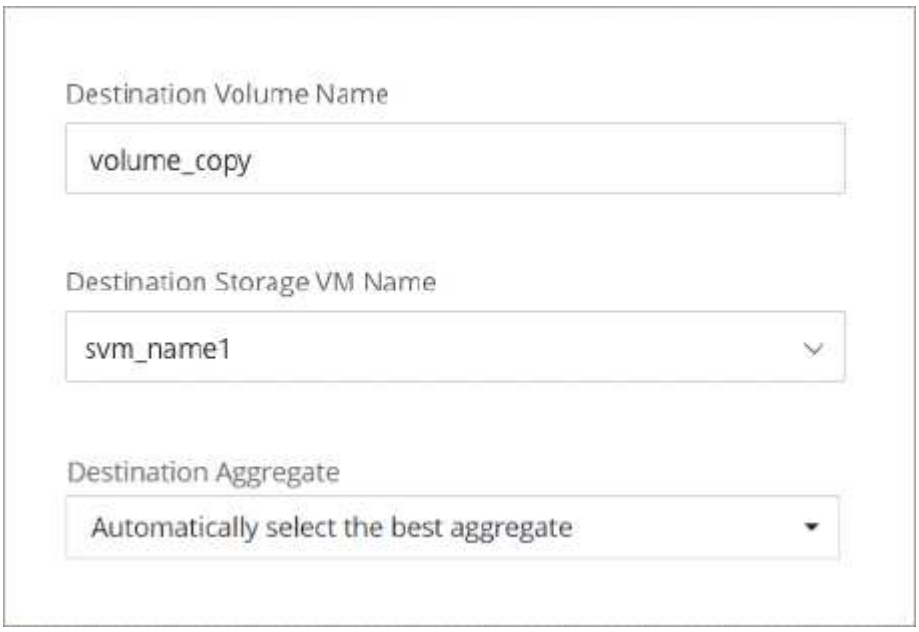
Arbeiten mit mehreren Speicher-VMs

Die NetApp Console unterstützt alle zusätzlichen Speicher-VMs, die Sie vom ONTAP System Manager oder der ONTAP CLI erstellen.

Das folgende Bild zeigt beispielsweise, wie Sie beim Erstellen eines Volumes eine Speicher-VM auswählen können.



Und das folgende Bild zeigt, wie Sie eine Speicher-VM auswählen können, wenn Sie ein Volume auf ein anderes System replizieren.



Ändern Sie den Namen der Standard-Speicher-VM

Die Konsole benennt automatisch die einzelne Speicher-VM, die sie für Cloud Volumes ONTAP erstellt. Über den ONTAP System Manager, die ONTAP CLI oder die API können Sie den Namen der Speicher-VM ändern, wenn Sie strenge Benennungsstandards haben. Beispielsweise möchten Sie möglicherweise, dass der Name mit der Benennung der Speicher-VMs für Ihre ONTAP Cluster übereinstimmt.

Verwalten Sie datenbereitstellende Speicher-VMs für Cloud Volumes ONTAP in AWS

Eine Storage-VM ist eine virtuelle Maschine, die innerhalb von ONTAP ausgeführt wird und Ihren Clients Speicher- und Datendienste bereitstellt. Sie kennen dies möglicherweise als *SVM* oder *vServer*. Cloud Volumes ONTAP ist standardmäßig mit einer Speicher-VM konfiguriert, einige Konfigurationen unterstützen jedoch zusätzliche Speicher-VMs.

Um zusätzliche datenbereitstellende Speicher-VMs zu erstellen, müssen Sie IP-Adressen in AWS zuweisen und dann ONTAP -Befehle basierend auf Ihrer Cloud Volumes ONTAP Konfiguration ausführen.

Unterstützte Anzahl von Speicher-VMs

Ab der Version 9.7 werden mehrere Speicher-VMs mit bestimmten Cloud Volumes ONTAP -Konfigurationen unterstützt. Gehen Sie zum "Versionshinweise zu Cloud Volumes ONTAP" um die unterstützte Anzahl von Speicher-VMs für Ihre Version von Cloud Volumes ONTAP zu überprüfen.

Alle anderen Cloud Volumes ONTAP -Konfigurationen unterstützen eine Datenspeicher-VM und eine Zielspeicher-VM, die für die Notfallwiederherstellung verwendet wird. Sie können die Zielspeicher-VM für den Datenzugriff aktivieren, wenn es auf der Quellspeicher-VM zu einem Ausfall kommt.

Überprüfen der Grenzwerte für Ihre Konfiguration

Jede EC2-Instance unterstützt eine maximale Anzahl privater IPv4-Adressen pro Netzwerkschnittstelle. Sie müssen das Limit überprüfen, bevor Sie in AWS IP-Adressen für die neue Speicher-VM zuweisen.

Schritte

1. Gehen Sie zum "Abschnitt „Speicherlimits“ in den Versionshinweisen zu Cloud Volumes ONTAP" .
2. Ermitteln Sie die maximale Anzahl von IP-Adressen pro Schnittstelle für Ihren Instanztyp.
3. Notieren Sie sich diese Nummer, da Sie sie im nächsten Abschnitt benötigen, wenn Sie IP-Adressen in AWS zuweisen.

IP-Adressen in AWS zuweisen

Bevor Sie LIFs für die neue Speicher-VM erstellen, müssen dem Port e0a in AWS private IPv4-Adressen zugewiesen werden.

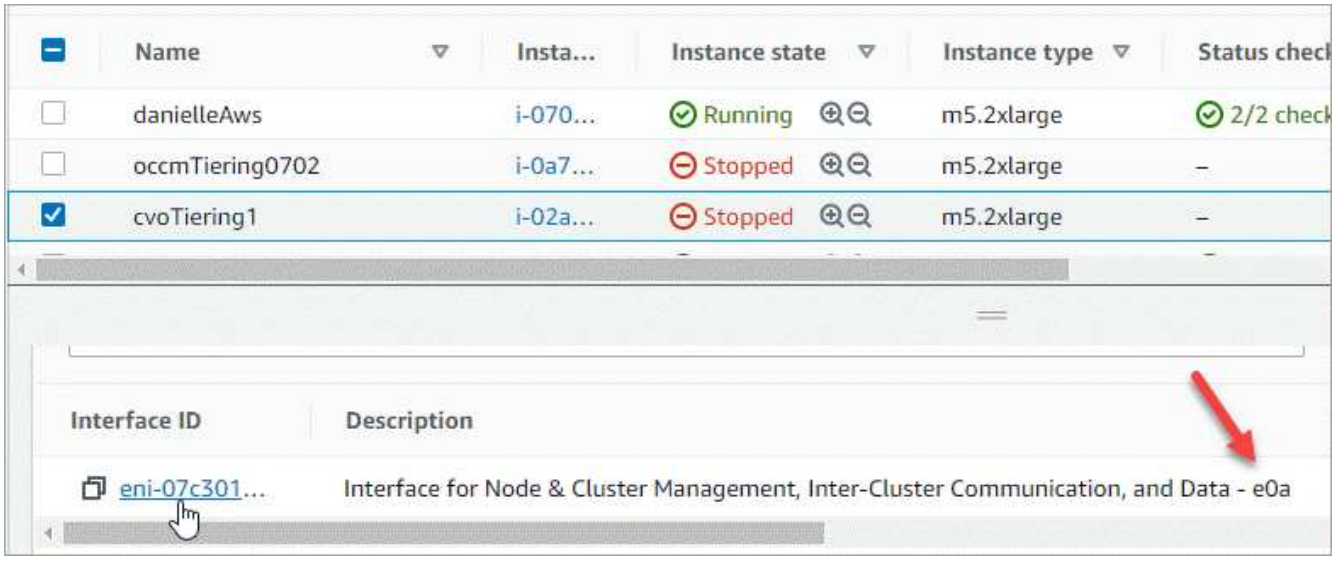
Beachten Sie, dass ein optionales Management-LIF für eine Storage-VM eine private IP-Adresse auf einem Einzelknotensystem und auf einem HA-Paar in einer einzelnen AZ benötigt. Dieses Management-LIF stellt eine Verbindung zu Management-Tools wie SnapCenter bereit.

Schritte

1. Melden Sie sich bei AWS an und öffnen Sie den EC2-Dienst.
2. Wählen Sie die Cloud Volumes ONTAP -Instanz aus und klicken Sie auf **Netzwerk**.

   Wenn Sie eine Speicher-VM auf einem HA-Paar erstellen, wählen Sie Knoten 1 aus.

3. Scrollen Sie nach unten zu **Netzwerkschnittstellen** und klicken Sie auf die **Schnittstellen-ID** für Port e0a.



4. Wählen Sie die Netzwerkschnittstelle aus und klicken Sie auf **Aktionen > IP-Adressen verwalten**.
5. Erweitern Sie die Liste der IP-Adressen für e0a.
6. Überprüfen Sie die IP-Adressen:
   a. Zählen Sie die Anzahl der zugewiesenen IP-Adressen, um zu bestätigen, dass der Port Platz für zusätzliche IPs hat.

      Sie sollten die maximale Anzahl unterstützter IP-Adressen pro Schnittstelle im vorherigen Abschnitt dieser Seite ermittelt haben.

   b. Optional: Gehen Sie zur ONTAP CLI für Cloud Volumes ONTAP und führen Sie **network interface show** aus, um zu bestätigen, dass jede dieser IP-Adressen verwendet wird.

      Wenn eine IP-Adresse nicht verwendet wird, können Sie sie mit der neuen Speicher-VM verwenden.
7. Klicken Sie in der AWS-Konsole auf **Neue IP-Adresse zuweisen**, um zusätzliche IP-Adressen basierend auf der Anzahl zuzuweisen, die Sie für die neue Speicher-VM benötigen.
   - Einzelknotensystem: Eine ungenutzte sekundäre private IP ist erforderlich.

     Eine optionale sekundäre private IP ist erforderlich, wenn Sie ein Verwaltungs-LIF auf der Speicher-VM erstellen möchten.

   - HA-Paar in einer einzelnen AZ: Auf Knoten 1 ist eine ungenutzte sekundäre private IP erforderlich.

     Eine optionale sekundäre private IP ist erforderlich, wenn Sie ein Verwaltungs-LIF auf der Speicher-VM erstellen möchten.

   - HA-Paar in mehreren AZs: Auf jedem Knoten ist eine ungenutzte sekundäre private IP erforderlich.
8. Wenn Sie die IP-Adresse auf einem HA-Paar in einer einzelnen AZ zuweisen, aktivieren Sie **Neuzuweisung sekundärer privater IPv4-Adressen zulassen**.
9. Klicken Sie auf **Speichern**.
10. Wenn Sie ein HA-Paar in mehreren AZs haben, müssen Sie diese Schritte für Knoten 2 wiederholen.

Erstellen Sie eine Storage-VM auf einem Einzelknotensystem

Diese Schritte erstellen eine neue Storage-VM auf einem Einzelknotensystem. Eine private IP-Adresse ist erforderlich, um eine NAS-LIF zu erstellen, und eine weitere optionale private IP-Adresse wird benötigt, wenn Sie eine Management-LIF erstellen möchten.

Schritte

1. Erstellen Sie die Speicher-VM und eine Route zur Speicher-VM.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. Erstellen Sie ein NAS-LIF.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node
```

   Wobei *private_ip_x* eine ungenutzte sekundäre private IP auf e0a ist.

3. Optional: Erstellen Sie ein LIF zur Speicher-VM-Verwaltung.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node
```

   Wobei *private_ip_y* eine weitere ungenutzte sekundäre private IP auf e0a ist.

4. Weisen Sie der Speicher-VM ein oder mehrere Aggregate zu.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

   Dieser Schritt ist erforderlich, da die neue Speicher-VM Zugriff auf mindestens ein Aggregat benötigt, bevor Sie Volumes auf der Speicher-VM erstellen können.

Erstellen Sie eine Speicher-VM auf einem HA-Paar in einer einzelnen AZ

Mit diesen Schritten wird eine neue Speicher-VM auf einem HA-Paar in einer einzelnen AZ erstellt. Zum Erstellen eines NAS-LIF ist eine private IP-Adresse erforderlich, und wenn Sie ein Verwaltungs-LIF erstellen möchten, ist eine weitere optionale private IP-Adresse erforderlich.

Beide LIFs werden auf Knoten 1 zugewiesen. Die privaten IP-Adressen können bei Fehlern zwischen Knoten verschoben werden.

Schritte

1. Erstellen Sie die Speicher-VM und eine Route zur Speicher-VM.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. Erstellen Sie ein NAS-LIF auf Knoten 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node1
```

   Wobei *private_ip_x* eine ungenutzte sekundäre private IP auf e0a von cvo-node1 ist. Diese IP-Adresse kann im Falle einer Übernahme auf e0a von cvo-node2 verschoben werden, da die Servicerichtlinie „default-data-files“ angibt, dass IPs auf den Partnerknoten migriert werden können.

3. Optional: Erstellen Sie ein LIF zur Speicher-VM-Verwaltung auf Knoten 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

   Wobei *private_ip_y* eine weitere ungenutzte sekundäre private IP auf e0a ist.

4. Weisen Sie der Speicher-VM ein oder mehrere Aggregate zu.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

   Dieser Schritt ist erforderlich, da die neue Speicher-VM Zugriff auf mindestens ein Aggregat benötigt, bevor Sie Volumes auf der Speicher-VM erstellen können.

5. Wenn Sie Cloud Volumes ONTAP 9.11.1 oder höher ausführen, ändern Sie die Netzwerkdienstrichtlinien für die Speicher-VM.

   Das Ändern der Dienste ist erforderlich, da dadurch sichergestellt wird, dass Cloud Volumes ONTAP das iSCSI-LIF für ausgehende Verwaltungsverbindungen verwenden kann.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client
```

Erstellen Sie eine Speicher-VM auf einem HA-Paar in mehreren AZs

Mit diesen Schritten wird eine neue Speicher-VM auf einem HA-Paar in mehreren AZs erstellt.

Für ein NAS-LIF ist eine *Floating*-IP-Adresse erforderlich und für ein Management-LIF optional. Für diese Floating-IP-Adressen müssen Sie in AWS keine privaten IPs zuweisen. Stattdessen werden die Floating-IPs in der AWS-Routentabelle automatisch so konfiguriert, dass sie auf die ENI eines bestimmten Knotens im selben VPC verweisen.

Damit Floating IPs mit ONTAP funktionieren, muss auf jeder Speicher-VM auf jedem Knoten eine private IP-Adresse konfiguriert werden. Dies spiegelt sich in den folgenden Schritten wider, in denen auf Knoten 1 und Knoten 2 ein iSCSI-LIF erstellt wird.

Schritte

1. Erstellen Sie die Speicher-VM und eine Route zur Speicher-VM.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. Erstellen Sie ein NAS-LIF auf Knoten 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_nas_floating_2 -home-node cvo-node1
```

   - Die Floating-IP-Adresse muss außerhalb der CIDR-Blöcke für alle VPCs in der AWS-Region liegen, in der Sie die HA-Konfiguration bereitstellen. 192.168.209.27 ist ein Beispiel für eine Floating-IP-Adresse. "Erfahren Sie mehr über die Auswahl einer Floating-IP-Adresse" .
   - `-service-policy default-data-files`zeigt an, dass IPs zum Partnerknoten migriert werden können.

3. Optional: Erstellen Sie ein LIF zur Speicher-VM-Verwaltung auf Knoten 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

4. Erstellen Sie ein iSCSI-LIF auf Knoten 1.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmask nodei1Mask -lif
ip_node1_iscsi_2 -home-node cvo-node1
```

   - Dieses iSCSI-LIF ist erforderlich, um die LIF-Migration der Floating-IPs in der Speicher-VM zu unterstützen. Es muss kein iSCSI-LIF sein, aber es kann nicht für die Migration zwischen Knoten konfiguriert werden.
   - `-service-policy default-data-block`gibt an, dass eine IP-Adresse nicht zwischen Knoten migriert.
   - *private_ip* ist eine ungenutzte sekundäre private IP-Adresse auf eth0 (e0a) von cvo_node1.

5. Erstellen Sie ein iSCSI-LIF auf Knoten 2.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmaskNode2Mask -lif
ip_node2_iscsi_2 -home-node cvo-node2
```

- Dieses iSCSI-LIF ist erforderlich, um die LIF-Migration der Floating-IPs in der Speicher-VM zu unterstützen. Es muss kein iSCSI-LIF sein, aber es kann nicht für die Migration zwischen Knoten konfiguriert werden.
- `-service-policy default-data-block`gibt an, dass eine IP-Adresse nicht zwischen Knoten migriert.
- *private_ip* ist eine ungenutzte sekundäre private IP-Adresse auf eth0 (e0a) von cvo_node2.

6. Weisen Sie der Speicher-VM ein oder mehrere Aggregate zu.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

Dieser Schritt ist erforderlich, da die neue Speicher-VM Zugriff auf mindestens ein Aggregat benötigt, bevor Sie Volumes auf der Speicher-VM erstellen können.

7. Wenn Sie Cloud Volumes ONTAP 9.11.1 oder höher ausführen, ändern Sie die Netzwerkdienstrichtlinien für die Speicher-VM.

Das Ändern der Dienste ist erforderlich, da dadurch sichergestellt wird, dass Cloud Volumes ONTAP das iSCSI-LIF für ausgehende Verwaltungsverbindungen verwenden kann.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client
```

Verwalten von datenbereitstellenden Speicher-VMs für Cloud Volumes ONTAP in Azure

Eine Storage-VM ist eine virtuelle Maschine, die innerhalb von ONTAP ausgeführt wird und Ihren Clients Speicher- und Datendienste bereitstellt. Sie kennen dies möglicherweise als *SVM* oder *vServer*. Cloud Volumes ONTAP ist standardmäßig mit einer Speicher-VM konfiguriert, Sie können jedoch zusätzliche Speicher-VMs erstellen, wenn Sie Cloud Volumes ONTAP in Azure ausführen.

Um zusätzliche datenbereitstellende Speicher-VMs in Azure zu erstellen und zu verwalten, sollten Sie die APIs verwenden. Dies liegt daran, dass die APIs den Prozess der Erstellung der Speicher-VMs und der Konfiguration der erforderlichen Netzwerkschnittstellen automatisieren. Beim Erstellen der Speicher-VMs konfiguriert die NetApp Console die erforderlichen LIF-Dienste sowie ein iSCSI-LIF, das für die ausgehende SMB/CIFS-Kommunikation von der Speicher-VM erforderlich ist.

Informationen zum Ausführen von Cloud Volumes ONTAP API-Aufrufen finden Sie unter "Ihr erster API-Aufruf" .

Unterstützte Anzahl von Speicher-VMs

Ab Cloud Volumes ONTAP 9.9.0 werden, basierend auf Ihrer Lizenz, mehrere Speicher-VMs mit bestimmten Konfigurationen unterstützt. Weitere Informationen finden Sie im "Versionshinweise zu Cloud Volumes ONTAP" um die unterstützte Anzahl von Speicher-VMs für Ihre Version von Cloud Volumes ONTAP zu überprüfen.

Alle Versionen von Cloud Volumes ONTAP vor 9.9.0 unterstützen eine Daten-Storage-VM und eine Ziel-Storage-VM, die für die Notfallwiederherstellung verwendet wird. Sie können die Zielspeicher-VM für den Datenzugriff aktivieren, wenn es auf der Quellspeicher-VM zu einem Ausfall kommt.

Erstellen einer Speicher-VM

Basierend auf Ihrer Konfiguration und dem Lizenztyp können Sie mithilfe der APIs für die NetApp Console mehrere Storage-VMs auf einem Einzelknotensystem oder in einer Hochverfügbarkeitskonfiguration (HA) erstellen.

Informationen zu diesem Vorgang

Wenn Sie Storage-VMs mithilfe der APIs erstellen, ändert die Konsole neben der Konfiguration der erforderlichen Netzwerkschnittstellen auch die `default-data-files` Richtlinien auf den Datenspeicher-VMs, indem Sie die folgenden Dienste aus dem NAS-Daten-LIF entfernen und sie dem iSCSI-Daten-LIF hinzufügen, das für ausgehende Verwaltungsverbindungen verwendet wird:

- `data-fpolicy-client`
- `management-ad-client`
- `management-dns-client`
- `management-ldap-client`
- `management-nis-client`

Bevor Sie beginnen

Der Konsolenagent benötigt bestimmte Berechtigungen zum Erstellen von Speicher-VMs für Cloud Volumes ONTAP. Die erforderlichen Berechtigungen sind enthalten in "die von NetApp bereitgestellten Richtlinien" .

Einzelknotensystem

Verwenden Sie den folgenden API-Aufruf, um eine Storage-VM auf einem Single-Node-System zu erstellen.

`POST /azure/vsa/working-environments/{workingEnvironmentId}/svm`

Fügen Sie die folgenden Parameter in den Anforderungstext ein:

```
{ "svmName": "myNewSvm1"
   "svmPassword": "optional, the API takes the cluster password if not
provided"
   "mgmtLif": "optional, to create an additional management LIF, if you
want to use the storage VM for management purposes"}
```

HA-Paar

Verwenden Sie den folgenden API-Aufruf, um eine Speicher-VM auf einem HA-Paar zu erstellen:

```
POST /azure/ha/working-environments/{workingEnvironmentId}/svm
```

Fügen Sie die folgenden Parameter in den Anforderungstext ein:

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
   "mgmtLif": "optional value, to create an additional management LIF, if
you want to use the storage VM for management purposes"}
```

Verwalten Sie Storage-VMs auf Einzelknotensystemen und HA-Paaren

Mithilfe der APIs können Sie Speicher-VMs sowohl in Einzelknoten- als auch in HA-Konfigurationen umbenennen und löschen.

Bevor Sie beginnen

Der Konsolenagent benötigt bestimmte Berechtigungen zum Verwalten von Speicher-VMs für Cloud Volumes ONTAP. Die erforderlichen Berechtigungen sind enthalten in "die von NetApp bereitgestellten Richtlinien" .

Umbenennen einer Speicher-VM

Um eine Speicher-VM umzubenennen, sollten Sie die Namen der vorhandenen Speicher-VM und der neuen Speicher-VM als Parameter angeben.

Schritte

- Verwenden Sie den folgenden API-Aufruf, um eine Storage-VM auf einem Einzelknotensystem umzubenennen:

  ```
  PUT /azure/vsa/working-environments/{workingEnvironmentId}/svm
  ```

  Fügen Sie die folgenden Parameter in den Anforderungstext ein:

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

- Verwenden Sie den folgenden API-Aufruf, um eine Speicher-VM auf einem HA-Paar umzubenennen:

  ```
  PUT /azure/ha/working-environments/{workingEnvironmentId}/svm
  ```

  Fügen Sie die folgenden Parameter in den Anforderungstext ein:

```
{
  "svmNewName": "NewSvmName",
  "svmName": "OldSvmName"
}
```

Löschen einer Speicher-VM

In einer Einzelknoten- oder HA-Konfiguration können Sie eine Speicher-VM entfernen, wenn sie keine aktiven Volumes hat.

Schritte

- Verwenden Sie den folgenden API-Aufruf, um eine Storage-VM auf einem Einzelknotensystem zu löschen:

  ```
  DELETE /azure/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}
  ```

- Verwenden Sie den folgenden API-Aufruf, um eine Speicher-VM auf einem HA-Paar zu löschen:

  ```
  DELETE /azure/ha/working-environments/{workingEnvironmentId}/svm/{svmName}
  ```

Ähnliche Informationen

- "Vorbereiten der Verwendung der API"
- "Cloud Volumes ONTAP -Workflows"
- "Abrufen der erforderlichen Kennungen"
- "Verwenden Sie die REST-APIs für die NetApp Console"

Verwalten Sie datenbereitstellende Speicher-VMs für Cloud Volumes ONTAP in Google Cloud

Eine Storage-VM ist eine virtuelle Maschine, die innerhalb von ONTAP ausgeführt wird und Ihren Clients Speicher- und Datendienste bereitstellt. Sie kennen dies möglicherweise als *SVM* oder *vServer*. Cloud Volumes ONTAP ist standardmäßig mit einer Speicher-VM konfiguriert, einige Konfigurationen unterstützen jedoch zusätzliche Speicher-VMs.

Um zusätzliche datenbereitstellende Speicher-VMs in Google Cloud zu erstellen und zu verwalten, sollten Sie die APIs verwenden. Dies liegt daran, dass die APIs den Prozess der Erstellung der Speicher-VMs und der Konfiguration der erforderlichen Netzwerkschnittstellen automatisieren. Beim Erstellen der Speicher-VMs konfiguriert die NetApp Console die erforderlichen LIF-Dienste sowie ein iSCSI-LIF, das für die ausgehende SMB/CIFS-Kommunikation von der Speicher-VM erforderlich ist.

Informationen zum Ausführen von Cloud Volumes ONTAP API-Aufrufen finden Sie unter "Ihr erster API-Aufruf" .

Unterstützte Anzahl von Speicher-VMs

Ab Cloud Volumes ONTAP 9.11.1 werden, basierend auf Ihrer Lizenz, mehrere Speicher-VMs mit bestimmten Konfigurationen unterstützt. Weitere Informationen finden Sie im "Versionshinweise zu Cloud Volumes ONTAP" um die unterstützte Anzahl von Speicher-VMs für Ihre Version von Cloud Volumes ONTAP zu überprüfen.

Alle Versionen von Cloud Volumes ONTAP vor 9.11.1 unterstützen eine Daten-Storage-VM und eine Ziel-Storage-VM, die für die Notfallwiederherstellung verwendet wird. Sie können die Zielspeicher-VM für den Datenzugriff aktivieren, wenn es auf der Quellspeicher-VM zu einem Ausfall kommt.

Erstellen einer Speicher-VM

Basierend auf Ihrer Konfiguration und dem Lizenztyp können Sie mithilfe der APIs mehrere Storage-VMs auf einem Einzelknotensystem oder in einer Hochverfügbarkeitskonfiguration (HA) erstellen.

Informationen zu diesem Vorgang

Wenn Sie Storage-VMs mithilfe der APIs erstellen, ändert die Konsole neben der Konfiguration der erforderlichen Netzwerkschnittstellen auch die `default-data-files` Richtlinien auf den Datenspeicher-VMs, indem Sie die folgenden Dienste aus dem NAS-Daten-LIF entfernen und sie dem iSCSI-Daten-LIF hinzufügen, das für ausgehende Verwaltungsverbindungen verwendet wird:

- `data-fpolicy-client`
- `management-ad-client`
- `management-dns-client`
- `management-ldap-client`
- `management-nis-client`

Bevor Sie beginnen

Der Konsolenagent benötigt bestimmte Berechtigungen zum Erstellen von Speicher-VMs für Cloud Volumes ONTAP HA-Paare. Die erforderlichen Berechtigungen sind enthalten in "die von NetApp bereitgestellten Richtlinien" Die

Einzelknotensystem

Verwenden Sie den folgenden API-Aufruf, um eine Storage-VM auf einem Single-Node-System zu erstellen.

```
POST /gcp/vsa/working-environments/{workingEnvironmentId}/svm
```

Fügen Sie die folgenden Parameter in den Anforderungstext ein:

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
   "mgmtLif": "optional value, to create an additional management LIF, if
you want to use the storage VM for management purposes"}
```

HA-Paar

Verwenden Sie den folgenden API-Aufruf, um eine Speicher-VM auf einem HA-Paar zu erstellen:

```
POST /gcp/ha/working-environments/{workingEnvironmentId}/svm/
```

Fügen Sie die folgenden Parameter in den Anforderungstext ein:

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
}
```

Verwalten von Speicher-VMs

Mithilfe der APIs können Sie Speicher-VMs sowohl in Einzelknoten- als auch in HA-Konfigurationen umbenennen und löschen.

Bevor Sie beginnen

Der Konsolenagent benötigt bestimmte Berechtigungen zum Verwalten von Speicher-VMs für Cloud Volumes ONTAP HA-Paare. Die erforderlichen Berechtigungen sind enthalten in "die von NetApp bereitgestellten Richtlinien" Die

Umbenennen einer Speicher-VM

Um eine Speicher-VM umzubenennen, sollten Sie die Namen der vorhandenen Speicher-VM und der neuen Speicher-VM als Parameter angeben.

Schritte

- Verwenden Sie den folgenden API-Aufruf, um eine Storage-VM auf einem Einzelknotensystem umzubenennen:

  `PUT /gcp/vsa/working-environments/{workingEnvironmentId}/svm`

  Fügen Sie die folgenden Parameter in den Anforderungstext ein:

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

- Verwenden Sie den folgenden API-Aufruf, um eine Speicher-VM auf einem HA-Paar umzubenennen:

  `PUT /gcp/ha/working-environments/{workingEnvironmentId}/svm`

  Fügen Sie die folgenden Parameter in den Anforderungstext ein:

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

Löschen einer Speicher-VM

In einer Einzelknoten- oder HA-Konfiguration können Sie eine Speicher-VM entfernen, wenn sie keine aktiven Volumes hat.

Schritte

- Verwenden Sie den folgenden API-Aufruf, um eine Storage-VM auf einem Einzelknotensystem zu löschen:

```
DELETE /gcp/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}
```

- Verwenden Sie den folgenden API-Aufruf, um eine Speicher-VM auf einem HA-Paar zu löschen:

```
DELETE /gcp/ha/working-environments/{workingEnvironmentId}/svm/{svmName}
```

Ähnliche Informationen

- "Vorbereiten der Verwendung der API"
- "Cloud Volumes ONTAP -Workflows"
- "Abrufen der erforderlichen Kennungen"
- "Verwenden Sie die REST-APIs für die NetApp Console"

Einrichten der Speicher-VM-Notfallwiederherstellung für Cloud Volumes ONTAP

Die NetApp Console bietet keine Einrichtungs- oder Orchestrierungsunterstützung für die Notfallwiederherstellung von Storage-VMs (SVM). Verwenden Sie zum Ausführen dieser Aufgaben den ONTAP System Manager oder die ONTAP CLI.

Wenn Sie die SnapMirror SVM-Replikation zwischen zwei Cloud Volumes ONTAP Systemen einrichten, muss die Replikation zwischen zwei HA-Paarsystemen oder zwei Einzelknotensystemen erfolgen. Sie können keine SnapMirror SVM-Replikation zwischen einem HA-Paar und einem Einzelknotensystem einrichten.

Anweisungen zur ONTAP -CLI finden Sie in den folgenden Dokumenten.

- "Expresshandbuch zur Vorbereitung der SVM-Notfallwiederherstellung"
- "SVM Disaster Recovery Express-Handbuch"

Sicherheit und Datenverschlüsselung

Verschlüsseln Sie Volumes auf Cloud Volumes ONTAP mit NetApp -Verschlüsselungslösungen

Cloud Volumes ONTAP unterstützt NetApp Volume Encryption (NVE) und NetApp Aggregate Encryption (NAE). NVE und NAE sind softwarebasierte Lösungen, die eine FIPS 140-2-konforme Data-at-Rest-Verschlüsselung von Volumes ermöglichen. "Erfahren Sie mehr über diese Verschlüsselungslösungen" .

Sowohl NVE als auch NAE werden mit einem externen Schlüsselmanager unterstützt.

] endif::aws[] ifdef::azure[] endif::azure[] ifdef::gcp[] endif::gcp[] ifdef::aws[] endif::aws[] ifdef::azure[] endif::azure[] ifdef::gcp[] endif::gcp[

Verwalten Sie Cloud Volumes ONTAP Verschlüsselungsschlüssel mit dem AWS Key Management Service

Sie können"Schlüsselverwaltungsdienst (KMS) von AWS" um Ihre ONTAP Verschlüsselungsschlüssel in einer von AWS bereitgestellten Anwendung zu schützen.

Die Schlüsselverwaltung mit AWS KMS kann mit der CLI oder der ONTAP REST API aktiviert werden.

Beachten Sie bei der Verwendung des KMS, dass standardmäßig das LIF eines Daten-SVM zur Kommunikation mit dem Cloud-Schlüsselverwaltungsendpunkt verwendet wird. Zur Kommunikation mit den Authentifizierungsdiensten von AWS wird ein Knotenverwaltungsnetzwerk verwendet. Wenn das Clusternetzwerk nicht richtig konfiguriert ist, kann der Cluster den Schlüsselverwaltungsdienst nicht richtig nutzen.

Bevor Sie beginnen

- Cloud Volumes ONTAP muss in der Version 9.12.0 oder höher ausgeführt werden.
- Sie müssen die Volume Encryption (VE)-Lizenz installiert haben und
- Sie müssen die Lizenz Multi-tenant Encryption Key Management (MTEKM) installiert haben.
- Sie müssen ein Cluster- oder SVM-Administrator sein
- Sie müssen über ein aktives AWS-Abonnement verfügen

Sie können nur Schlüssel für eine Daten-SVM konfigurieren.

Konfiguration

AWS

1. Sie müssen eine"gewähren" für den AWS KMS-Schlüssel, der von der IAM-Rolle zur Verwaltung der Verschlüsselung verwendet wird. Die IAM-Rolle muss eine Richtlinie enthalten, die die folgenden Vorgänge zulässt:
   - `DescribeKey`
   - `Encrypt`
   - `Decrypt`Informationen zum Erstellen eines Zuschusses finden Sie unter"AWS-Dokumentation" .
2. "Fügen Sie der entsprechenden IAM-Rolle eine Richtlinie hinzu."Die Politik sollte die `DescribeKey` , `Encrypt` , Und `Decrypt` Operationen.

Cloud Volumes ONTAP

1. Wechseln Sie zu Ihrer Cloud Volumes ONTAP Umgebung.
2. Wechseln Sie zur erweiterten Berechtigungsstufe:
   `set -privilege advanced`
3. Aktivieren Sie den AWS-Schlüsselmanager:
   `security key-manager external aws enable -vserver` *`data_svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. Geben Sie bei der entsprechenden Aufforderung den geheimen Schlüssel ein.
5. Bestätigen Sie, dass AWS KMS richtig konfiguriert wurde:
   `security key-manager external aws show -vserver` *`svm_name`*

Verwalten Sie Cloud Volumes ONTAP Verschlüsselungsschlüssel mit Azure Key Vault

Sie können Azure Key Vault (AKV) verwenden, um Ihre ONTAP Verschlüsselungsschlüssel in einer in Azure bereitgestellten Anwendung zu schützen. Weitere Informationen finden Sie im"Microsoft-Dokumentation" .

AKV kann zum Schutz von NetApp Volume Encryption (NVE)-Schlüsseln nur für Daten-SVMs verwendet werden. Weitere Informationen finden Sie im "ONTAP-Dokumentation" .

Die Schlüsselverwaltung mit AKV kann mit der CLI oder der ONTAP REST API aktiviert werden.

Beachten Sie bei der Verwendung von AKV, dass standardmäßig ein Daten-SVM-LIF zur Kommunikation mit dem Cloud-Schlüsselverwaltungsendpunkt verwendet wird. Zur Kommunikation mit den Authentifizierungsdiensten des Cloud-Anbieters (login.microsoftonline.com) wird ein Knotenverwaltungsnetzwerk verwendet. Wenn das Clusternetzwerk nicht richtig konfiguriert ist, kann der Cluster den Schlüsselverwaltungsdienst nicht richtig nutzen.

Bevor Sie beginnen

- Cloud Volumes ONTAP muss in der Version 9.10.1 oder höher ausgeführt werden.
- Volume Encryption (VE)-Lizenz installiert (NetApp Volume Encryption-Lizenz wird automatisch auf jedem Cloud Volumes ONTAP -System installiert, das beim NetApp -Support registriert ist)
- Sie müssen über eine Multi-Tenant Encryption Key Management (MT_EK_MGMT)-Lizenz verfügen.
- Sie müssen ein Cluster- oder SVM-Administrator sein
- Ein aktives Azure-Abonnement

Einschränkungen

- AKV kann nur auf einem Daten-SVM konfiguriert werden
- NAE kann nicht mit AKV verwendet werden. NAE erfordert einen extern unterstützten KMIP-Server.
- Cloud Volumes ONTAP -Knoten fragen AKV alle 15 Minuten ab, um die Zugänglichkeit und Schlüsselverfügbarkeit zu bestätigen. Dieser Abfragezeitraum ist nicht konfigurierbar und nach vier aufeinanderfolgenden Fehlschlägen beim Abfrageversuch (insgesamt 1 Stunde) werden die Volumes offline gestellt.

Konfigurationsprozess

Die beschriebenen Schritte beschreiben, wie Sie Ihre Cloud Volumes ONTAP -Konfiguration bei Azure registrieren und wie Sie einen Azure Key Vault und Schlüssel erstellen. Wenn Sie diese Schritte bereits abgeschlossen haben, stellen Sie sicher, dass Sie die richtigen Konfigurationseinstellungen haben, insbesondere inErstellen eines Azure Key Vault und fahren Sie dann fort mitCloud Volumes ONTAP Konfiguration .

- Azure-Anwendungsregistrierung
- Erstellen des geheimen Azure-Clientschlüssels
- Erstellen eines Azure Key Vault
- Verschlüsselungsschlüssel erstellen
- Erstellen eines Azure Active Directory-Endpunkts (nur HA)
- Cloud Volumes ONTAP Konfiguration

Azure-Anwendungsregistrierung

1. Sie müssen Ihre Anwendung zunächst im Azure-Abonnement registrieren, das Cloud Volumes ONTAP für den Zugriff auf den Azure Key Vault verwenden soll. Wählen Sie im Azure-Portal **App-Registrierungen** aus.
2. Wählen Sie **Neue Registrierung**.
3. Geben Sie Ihrer Anwendung einen Namen und wählen Sie einen unterstützten Anwendungstyp aus. Für die Verwendung von Azure Key Vault ist der standardmäßige Einzelmandant ausreichend. Wählen Sie **Registrieren**.
4. Wählen Sie im Azure-Übersichtsfenster die Anwendung aus, die Sie registriert haben. Kopieren Sie die **Anwendungs-ID (Client-ID)** und die **Verzeichnis-ID (Mandant-ID)** an einen sicheren Ort. Sie werden später im Registrierungsprozess benötigt.

Erstellen des geheimen Azure-Clientschlüssels

1. Wählen Sie im Azure-Portal für Ihre Azure Key Vault-App-Registrierung den Bereich **Zertifikate und Geheimnisse** aus.
2. Wählen Sie **Neues Client-Geheimnis**. Geben Sie einen aussagekräftigen Namen für Ihr Client-Geheimnis ein. NetApp empfiehlt eine Ablauffrist von 24 Monaten. Ihre spezifischen Cloud-Governance-Richtlinien erfordern jedoch möglicherweise eine andere Einstellung.
3. Klicken Sie auf **Hinzufügen**, um das Clientgeheimnis zu erstellen. Kopieren Sie die in der Spalte **Wert** aufgeführte geheime Zeichenfolge und speichern Sie sie an einem sicheren Ort zur späteren Verwendung inCloud Volumes ONTAP Konfiguration . Der geheime Wert wird nicht erneut angezeigt, nachdem Sie die Seite verlassen.

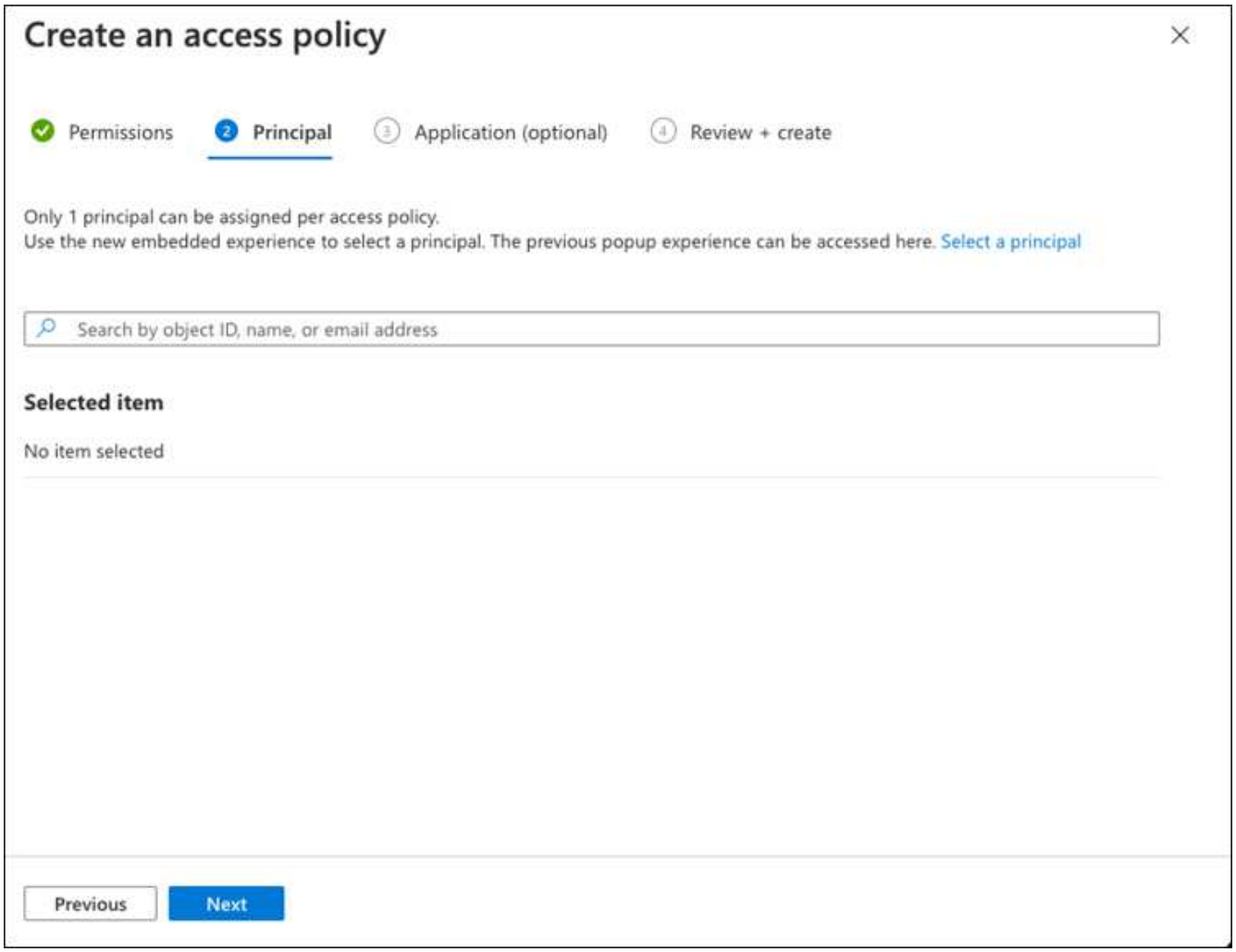
Erstellen eines Azure Key Vault

1. Wenn Sie über einen vorhandenen Azure Key Vault verfügen, können Sie diesen mit Ihrer Cloud Volumes ONTAP Konfiguration verbinden; Sie müssen dabei allerdings die Zugriffsrichtlinien an die Einstellungen anpassen.
2. Navigieren Sie im Azure-Portal zum Abschnitt **Schlüsseltresore**.
3. Klicken Sie auf **+Erstellen** und geben Sie die erforderlichen Informationen ein, einschließlich Ressourcengruppe, Region und Preisstufe. Geben Sie außerdem die Anzahl der Tage ein, die gelöschte Tresore aufbewahrt werden sollen, und wählen Sie **Löschschutz aktivieren** für den Schlüsseltresor aus.
4. Wählen Sie **Weiter** aus, um eine Zugriffsrichtlinie auszuwählen.
5. Wählen Sie die folgenden Optionen aus:
   a. Wählen Sie unter **Zugriffskonfiguration** die **Tresorzugriffsrichtlinie** aus.
   b. Wählen Sie unter **Ressourcenzugriff Azure Disk Encryption für die Volumeverschlüsselung** aus.
6. Wählen Sie **+Erstellen** aus, um eine Zugriffsrichtlinie hinzuzufügen.
7. Klicken Sie unter **Aus einer Vorlage konfigurieren** auf das Dropdown-Menü und wählen Sie dann die Vorlage **Schlüssel-, Geheimnis- und Zertifikatsverwaltung** aus.
8. Wählen Sie jedes der Dropdown-Berechtigungsmenüs (Schlüssel, Geheimnis, Zertifikat) und dann **Alle auswählen** oben in der Menüliste, um alle verfügbaren Berechtigungen auszuwählen. Sie sollten haben:
   - **Schlüsselberechtigungen**: 20 ausgewählt
   - **Geheime Berechtigungen**: 8 ausgewählt
   - **Zertifikatberechtigungen**: 16 ausgewählt

Create an access policy
1 Permissions
2 Principal
3 Application (optional)
4 Review + create
Configure from a template
Key, Secret, & Certificate Management
Key permissions
Key Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Cryptographic Operations
Select all
Decrypt
Encrypt
Unwrap Key
Wrap Key
Verify
Sign
Privileged Key Operations
Select all
Purge
Release
Rotation Policy Operations
Select all
Rotate
Get Rotation Policy
Set Rotation Policy
Secret permissions
Secret Management Operations
Select all
Get
List
Set
Delete
Recover
Backup
Restore
Privileged Secret Operations
Select all
Purge
Certificate permissions
Certificate Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Manage Contacts
Manage Certificate Authorities
Get Certificate Authorities
List Certificate Authorities
Set Certificate Authorities
Delete Certificate Authorities
Privileged Certificate Operations
Select all
Purge
Previous
Next

9. Klicken Sie auf **Weiter**, um die **Principal**-Azure-registrierte Anwendung auszuwählen, die Sie inAzure-Anwendungsregistrierung . Wählen Sie **Weiter**.

   Pro Richtlinie kann nur ein Auftraggeber zugewiesen werden.



10. Klicken Sie zweimal auf **Weiter**, bis Sie bei **Überprüfen und erstellen** ankommen. Klicken Sie dann auf **Erstellen**.
11. Wählen Sie **Weiter**, um zu den **Netzwerkoptionen** zu gelangen.
12. Wählen Sie die entsprechende Netzwerkzugriffsmethode oder wählen Sie **Alle Netzwerke** und **Überprüfen + Erstellen**, um den Schlüsseltresor zu erstellen. (Die Netzwerkzugriffsmethode kann durch eine Governance-Richtlinie oder Ihr Cloud-Sicherheitsteam im Unternehmen vorgeschrieben sein.)
13. Notieren Sie die Key Vault-URI: Navigieren Sie im von Ihnen erstellten Key Vault zum Menü „Übersicht“ und kopieren Sie die **Vault-URI** aus der rechten Spalte. Sie benötigen dies für einen späteren Schritt.

Verschlüsselungsschlüssel erstellen

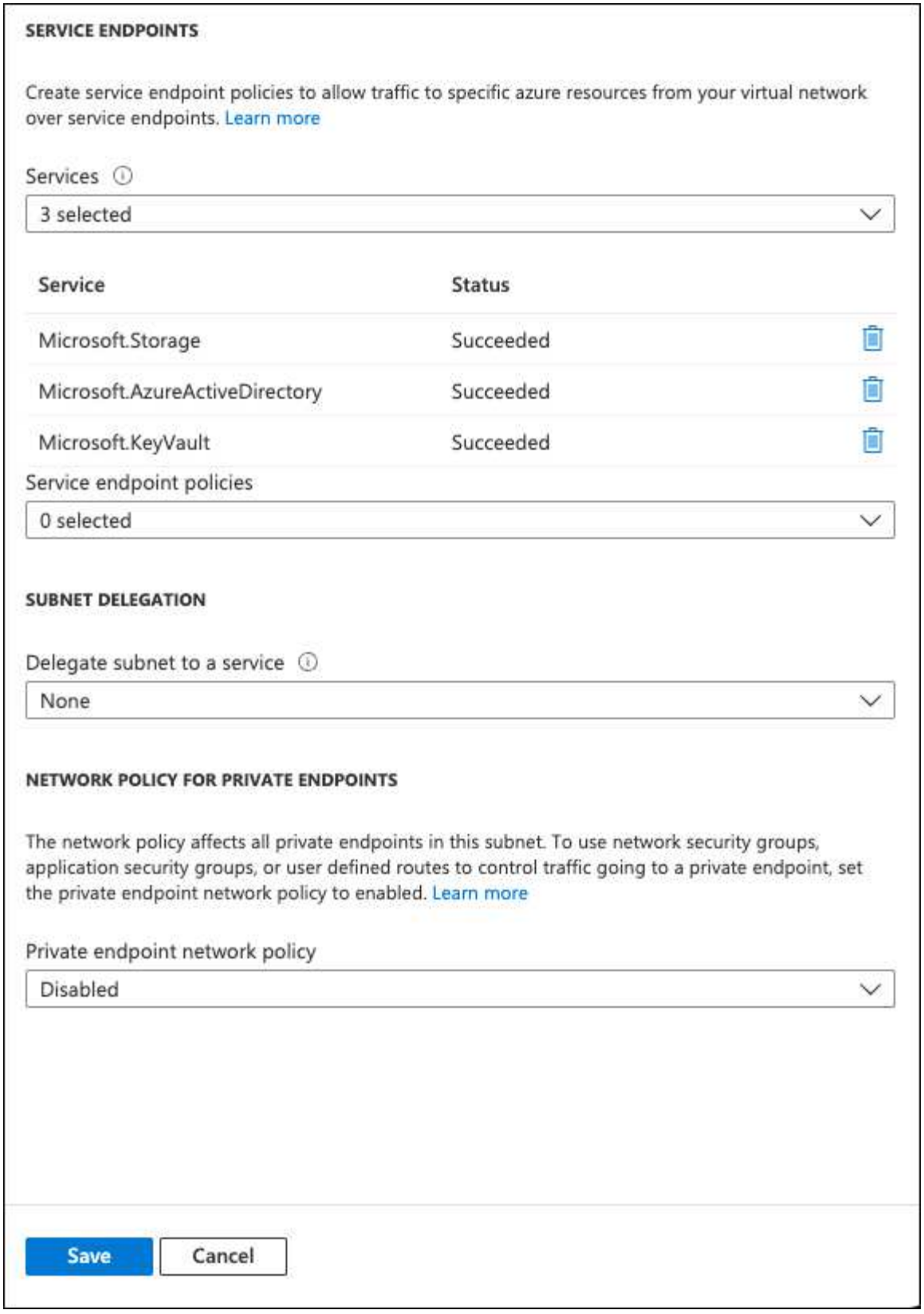
1. Navigieren Sie im Menü für den Schlüsseltresor, den Sie für Cloud Volumes ONTAP erstellt haben, zur Option **Schlüssel**.
2. Wählen Sie **Generieren/Importieren**, um einen neuen Schlüssel zu erstellen.
3. Belassen Sie die Standardoption auf **Generieren**.
4. Geben Sie die folgenden Informationen an:

- Name des Verschlüsselungsschlüssels
- Schlüsseltyp: RSA
- RSA-Schlüsselgröße: 2048
- Aktiviert: Ja

5. Wählen Sie **Erstellen** aus, um den Verschlüsselungsschlüssel zu erstellen.
6. Kehren Sie zum Menü **Schlüssel** zurück und wählen Sie den Schlüssel aus, den Sie gerade erstellt haben.
7. Wählen Sie die Schlüssel-ID unter **Aktuelle Version** aus, um die Schlüsseleigenschaften anzuzeigen.
8. Suchen Sie das Feld **Schlüsselkennung**. Kopieren Sie die URI bis zur hexadezimalen Zeichenfolge, jedoch nicht einschließlich dieser.

Erstellen eines Azure Active Directory-Endpunkts (nur HA)

1. Dieser Vorgang ist nur erforderlich, wenn Sie Azure Key Vault für ein HA Cloud Volumes ONTAP -System konfigurieren.
2. Navigieren Sie im Azure-Portal zu **Virtuelle Netzwerke**.
3. Wählen Sie das virtuelle Netzwerk aus, in dem Sie das Cloud Volumes ONTAP -System bereitgestellt haben, und wählen Sie auf der linken Seite der Seite das Menü **Subnetze** aus.
4. Wählen Sie den Subnetznamen für Ihre Cloud Volumes ONTAP -Bereitstellung aus der Liste aus.
5. Navigieren Sie zur Überschrift **Service-Endpunkte**. Wählen Sie im Dropdown-Menü Folgendes aus:
   - **Microsoft.AzureActiveDirectory**
   - **Microsoft.KeyVault**
   - **Microsoft.Storage** (optional)



6. Wählen Sie **Speichern**, um Ihre Einstellungen zu speichern.

Cloud Volumes ONTAP Konfiguration

1. Stellen Sie mit Ihrem bevorzugten SSH-Client eine Verbindung zum Cluster-Management-LIF her.
2. Rufen Sie den erweiterten Berechtigungsmodus in ONTAP auf:

```
set advanced -con off
```

3. Identifizieren Sie die gewünschte Daten-SVM und überprüfen Sie ihre DNS-Konfiguration:
`vserver services name-service dns show`

   a. Wenn ein DNS-Eintrag für die gewünschte Daten-SVM vorhanden ist und dieser einen Eintrag für das Azure-DNS enthält, ist keine Aktion erforderlich. Wenn dies nicht der Fall ist, fügen Sie einen DNS-Servereintrag für die Daten-SVM hinzu, der auf Azure DNS, privates DNS oder den lokalen Server verweist. Dies sollte mit dem Eintrag für die Cluster-Admin-SVM übereinstimmen:
   `vserver services name-service dns create -vserver SVM_name -domains domain -name-servers IP_address`

   b. Überprüfen Sie, ob der DNS-Dienst für die Daten-SVM erstellt wurde:
   `vserver services name-service dns show`

4. Aktivieren Sie Azure Key Vault mithilfe der Client-ID und der Mandanten-ID, die nach der Anwendungsregistrierung gespeichert wurden:
`security key-manager external azure enable -vserver SVM_name -client-id Azure_client_ID -tenant-id Azure_tenant_ID -name key_vault_URI -key-id full_key_URI`

   > Der `_full_key_URI` Wert muss die `<https:// <key vault host name>/keys/<key label>` Format.

5. Nach erfolgreicher Aktivierung des Azure Key Vault geben Sie die `client secret value` wenn Sie dazu aufgefordert werden.

6. Überprüfen Sie den Status des Schlüsselmanagers:
`security key-manager external azure check` Die Ausgabe sieht folgendermaßen aus:

```
::*> security key-manager external azure check

Vserver: data_svm_name
Node: akvlab01-01

Category: service_reachability
    Status: OK

Category: ekmip_server
    Status: OK

Category: kms_wrapped_key_status
    Status: UNKNOWN
    Details: No volumes created yet for the vserver. Wrapped KEK status
will be available after creating encrypted volumes.

3 entries were displayed.
```

Wenn die `service_reachability` Status ist nicht `OK` , kann die SVM den Azure Key Vault-Dienst nicht mit der erforderlichen Konnektivität und allen erforderlichen Berechtigungen erreichen. Stellen Sie sicher, dass Ihre Azure-Netzwerkrichtlinien und das Routing Ihr privates virtuelles Netzwerk nicht daran hindern,

den öffentlichen Endpunkt von Azure Key Vault zu erreichen. Wenn dies der Fall ist, sollten Sie die Verwendung eines privaten Azure-Endpunkts in Betracht ziehen, um innerhalb des virtuellen Netzwerks auf den Schlüsseltresor zuzugreifen. Möglicherweise müssen Sie auch einen statischen Hosteintrag auf Ihrem SVM hinzufügen, um die private IP-Adresse für Ihren Endpunkt aufzulösen.

Der `kms_wrapped_key_status` werde berichten `UNKNOWN` bei der Erstkonfiguration. Sein Status ändert sich zu `OK` nachdem das erste Volume verschlüsselt wurde.

7. OPTIONAL: Erstellen Sie ein Testvolumen, um die Funktionalität von NVE zu überprüfen.

   `vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size -state online -policy default`

   Bei korrekter Konfiguration erstellt Cloud Volumes ONTAP automatisch das Volume und aktiviert die Volume-Verschlüsselung.

8. Bestätigen Sie, dass das Volume korrekt erstellt und verschlüsselt wurde. Wenn dies der Fall ist, `-is -encrypted` Der Parameter wird wie folgt angezeigt: `true` .
   `vol show -vserver SVM_name -fields is-encrypted`
9. Optional: Wenn Sie die Anmeldeinformationen im Azure Key Vault-Authentifizierungszertifikat aktualisieren möchten, verwenden Sie den folgenden Befehl:
   `security key-manager external azure update-credentials -vserver v1 -authentication-method certificate`

Weiterführende Links

- "Richten Sie Cloud Volumes ONTAP für die Verwendung eines vom Kunden verwalteten Schlüssels in Azure ein"
- "Microsoft Azure-Dokumentation: Informationen zu Azure Key Vault"
- "ONTAP -Befehlsreferenzhandbuch"

Verwalten Sie Cloud Volumes ONTAP Verschlüsselungsschlüssel mit Google Cloud KMS

Sie können"Schlüsselverwaltungsdienst (Cloud KMS) der Google Cloud Platform" zum Schutz Ihrer Cloud Volumes ONTAP Verschlüsselungsschlüssel in einer auf der Google Cloud Platform bereitgestellten Anwendung.

Die Schlüsselverwaltung mit Cloud KMS kann mit der ONTAP CLI oder der ONTAP REST API aktiviert werden.

Beachten Sie bei der Verwendung von Cloud KMS, dass standardmäßig das LIF eines Daten-SVM zur Kommunikation mit dem Cloud-Schlüsselverwaltungsendpunkt verwendet wird. Zur Kommunikation mit den Authentifizierungsdiensten des Cloud-Anbieters (oauth2.googleapis.com) wird ein Knotenverwaltungsnetzwerk verwendet. Wenn das Clusternetzwerk nicht richtig konfiguriert ist, kann der Cluster den Schlüsselverwaltungsdienst nicht richtig nutzen.

Bevor Sie beginnen

- Auf Ihrem System sollte Cloud Volumes ONTAP 9.10.1 oder höher ausgeführt werden.
- Sie müssen eine Daten-SVM verwenden. Cloud KMS kann nur auf einer Daten-SVM konfiguriert werden.
- Sie müssen ein Cluster- oder SVM-Administrator sein

- Die Volume Encryption (VE)-Lizenz sollte auf der SVM installiert werden
- Ab Cloud Volumes ONTAP 9.12.1 GA sollte auch die Multi-Tenant Encryption Key Management (MTEKM)-Lizenz installiert werden
- Ein aktives Google Cloud Platform-Abonnement ist erforderlich

Konfiguration

Google Cloud

1. In Ihrer Google Cloud-Umgebung"Erstellen Sie einen symmetrischen GCP-Schlüsselring und Schlüssel" .
2. Weisen Sie dem Cloud KMS-Schlüssel und dem Cloud Volumes ONTAP Dienstkonto eine benutzerdefinierte Rolle zu.
   a. Erstellen Sie die benutzerdefinierte Rolle:

```
gcloud iam roles create kmsCustomRole
    --project=<project_id>
    --title=<kms_custom_role_name>
    --description=<custom_role_description>

--permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersio
ns.list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVer
sions.useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,clou
dkms.locations.get,cloudkms.locations.list,resourcemanager.projects.g
et
    --stage=GA
```

   b. Weisen Sie die von Ihnen erstellte benutzerdefinierte Rolle zu:
   `gcloud kms keys add-iam-policy-binding` *`key_name`* `--keyring` *`key_ring_name`* `--location` *`key_location`* `--member serviceAccount:_service_account_Name_ --role projects/`*`customer_project_id`*`/roles/kmsCustomRole`

> Wenn Sie Cloud Volumes ONTAP 9.13.0 oder höher verwenden, müssen Sie keine benutzerdefinierte Rolle erstellen. Sie können die vordefinierten[`cloudkms.cryptoKeyEncrypterDecrypter` ^] Rolle.

3. JSON-Schlüssel des Dienstkontos herunterladen:
   `gcloud iam service-accounts keys create key-file --iam-account=`*`sa-name`*`@`*`project-id`*`.iam.gserviceaccount.com`

Cloud Volumes ONTAP

1. Stellen Sie mit Ihrem bevorzugten SSH-Client eine Verbindung zum Cluster-Management-LIF her.
2. Wechseln Sie zur erweiterten Berechtigungsstufe:
   `set -privilege advanced`
3. Erstellen Sie ein DNS für die Daten-SVM.
   `dns create -domains c.<`*`project`*`>.internal -name-servers` *`server_address`* `-vserver` *`SVM_name`*

4. CMEK-Eintrag erstellen:
   `security key-manager external gcp enable -vserver SVM_name -project-id project -key-ring-name key_ring_name -key-ring-location key_ring_location -key-name key_name`
5. Geben Sie bei der entsprechenden Aufforderung den JSON-Schlüssel des Dienstkontos aus Ihrem GCP-Konto ein.
6. Bestätigen Sie, dass der Aktivierungsprozess erfolgreich war:
   `security key-manager external gcp check -vserver svm_name`
7. OPTIONAL: Erstellen Sie ein Volume zum Testen der Verschlüsselung `vol create volume_name -aggregate aggregate -vserver vserver_name -size 10G`

Fehlerbehebung

Wenn Sie Fehler beheben müssen, können Sie die Rohprotokolle der REST-API in den letzten beiden Schritten oben verfolgen:

1. `set d`
2. `systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

Aktivieren Sie NetApp Ransomware-Schutzlösungen für Cloud Volumes ONTAP

Ransomware-Angriffe können ein Unternehmen Zeit, Ressourcen und Ansehen kosten. Mit der NetApp Console können Sie zwei NetApp -Lösungen für Ransomware implementieren: Schutz vor gängigen Ransomware-Dateierweiterungen und Autonomous Ransomware Protection (ARP). Diese Lösungen bieten effektive Tools für Sichtbarkeit, Erkennung und Behebung.

Schutz vor gängigen Ransomware-Dateierweiterungen

Mit der in der Konsole verfügbaren Einstellung „Ransomware-Schutz“ können Sie die ONTAP FPolicy-Funktionalität zum Schutz vor gängigen Ransomware-Dateierweiterungstypen nutzen.

Schritte

1. Doppelklicken Sie auf der Seite **Systeme** auf den Namen des Cloud Volumes ONTAP -Systems, das Sie für den Ransomware-Schutz konfigurieren.
2. Klicken Sie auf der Registerkarte „Übersicht“ auf den Bereich „Funktionen“ und dann auf das Stiftsymbol neben „Ransomware-Schutz“.
3. Implementieren Sie die NetApp -Lösung für Ransomware:

   a. Klicken Sie auf **Snapshot-Richtlinie aktivieren**, wenn Sie Volumes haben, für die keine Snapshot-Richtlinie aktiviert ist.

      Die NetApp Snapshot-Technologie bietet die branchenweit beste Lösung zur Beseitigung von Ransomware. Der Schlüssel zu einer erfolgreichen Wiederherstellung ist die Wiederherstellung aus nicht infizierten Backups. Snapshot-Kopien sind schreibgeschützt, wodurch eine Beschädigung durch Ransomware verhindert wird. Sie können auch die Granularität bereitstellen, um Bilder einer einzelnen Dateikopie oder einer vollständigen Disaster-Recovery-Lösung zu erstellen.

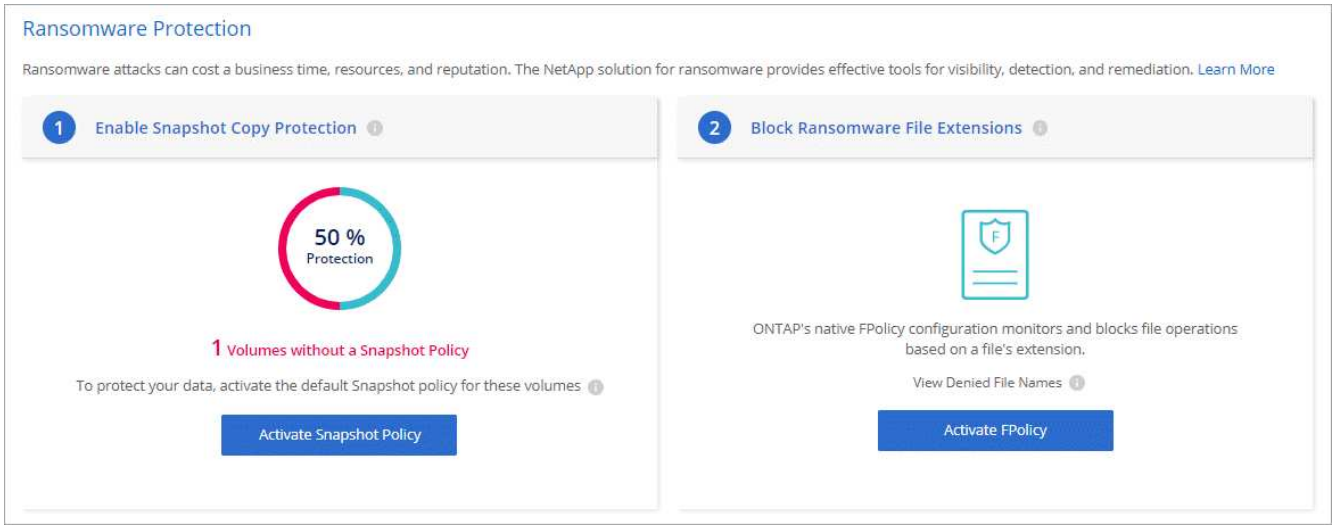
b. Klicken Sie auf **FPolicy aktivieren**, um die FPolicy-Lösung von ONTAP zu aktivieren, die Dateivorgänge basierend auf der Dateierweiterung blockieren kann.

   Diese präventive Lösung verbessert den Schutz vor Ransomware-Angriffen, indem sie gängige Ransomware-Dateitypen blockiert.

   Der Standardbereich von FPolicy blockiert Dateien mit den folgenden Erweiterungen:

   Mikro, verschlüsselt, gesperrt, Krypto, Krypta, Crinf, R5a, XRNT, XTBL, R16M01D05, pzdc, gut, LOL!, OMG!, RDM, RRK, encryptedRS, crjoker, EnCiPhErEd, LeChiffre

   Dieser Bereich wird erstellt, wenn Sie FPolicy auf Cloud Volumes ONTAP aktivieren. Die Liste basiert auf gängigen Ransomware-Dateitypen. Sie können die blockierten Dateierweiterungen mithilfe der Befehle *vserver fpolicy policy scope* aus der Cloud Volumes ONTAP CLI anpassen.



Autonomer Ransomware-Schutz

Cloud Volumes ONTAP unterstützt die Funktion Autonomous Ransomware Protection (ARP), die Analysen von Workloads durchführt, um proaktiv abnormale Aktivitäten zu erkennen und davor zu warnen, die auf einen Ransomware-Angriff hindeuten könnten.

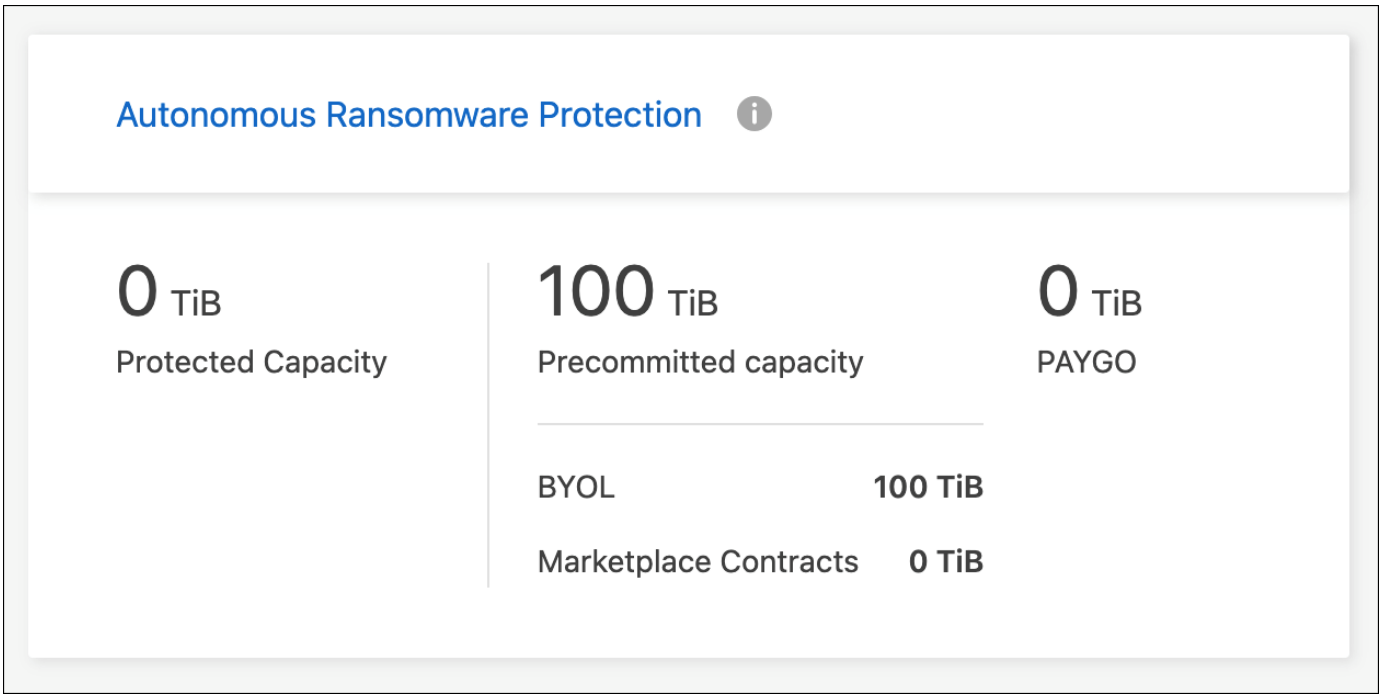
Unabhängig vom Dateierweiterungsschutz, der durch die "Ransomware-Schutzeinstellungen" Die ARP-Funktion verwendet eine Arbeitslastanalyse, um den Benutzer auf der Grundlage erkannter „abnormaler Aktivitäten“ vor potenziellen Angriffen zu warnen. Sowohl die Ransomware-Schutzeinstellung als auch die ARP-Funktion können zusammen für einen umfassenden Ransomware-Schutz verwendet werden.

Die ARP-Funktion steht für die Verwendung mit Bring Your Own License (BYOL) und Marktplatzabonnements für Ihre Lizenzen ohne zusätzliche Kosten zur Verfügung.

ARP-fähige Volumes haben den festgelegten Status „Lernmodus“ oder „Aktiv“.

Die ARP-Konfiguration für Volumes erfolgt über ONTAP System Manager und ONTAP CLI.

Weitere Informationen zum Aktivieren von ARP mit ONTAP System Manager und der ONTAP CLI finden Sie im "ONTAP -Dokumentation: Autonomen Ransomware-Schutz aktivieren" .



Erstellen Sie manipulationssichere Snapshot-Kopien von WORM-Dateien auf Cloud Volumes ONTAP

Sie können manipulationssichere Snapshot-Kopien von WORM-Dateien (Write Once, Read Many) auf einem Cloud Volumes ONTAP System erstellen und die Snapshots für einen bestimmten Aufbewahrungszeitraum unverändert aufbewahren. Diese Funktionalität wird durch die SnapLock -Technologie unterstützt und bietet eine zusätzliche Ebene für Datenschutz und Compliance.

Bevor Sie beginnen

Stellen Sie sicher, dass das Volume, das Sie zum Erstellen von Snapshot-Kopien verwenden, ein SnapLock -Volume ist. Informationen zum Aktivieren des SnapLock Schutzes auf Volumes finden Sie im "ONTAP Dokumentation: SnapLock konfigurieren" .

Schritte

1. Erstellen Sie Snapshot-Kopien vom SnapLock -Volume. Informationen zum Erstellen von Snapshot-Kopien mithilfe der CLI oder des System Managers finden Sie im "ONTAP -Dokumentation: Übersicht zum Verwalten lokaler Snapshot-Kopien" .

   Die Snapshot-Kopien übernehmen die WORM-Eigenschaften des Volumes und sind somit manipulationssicher. Die zugrunde liegende SnapLock -Technologie stellt sicher, dass ein Snapshot bis zum Ablauf der angegebenen Aufbewahrungsfrist vor Bearbeitung und Löschung geschützt bleibt.

2. Sie können den Aufbewahrungszeitraum ändern, wenn diese Snapshots bearbeitet werden müssen. Weitere Informationen finden Sie im "ONTAP -Dokumentation: Festlegen der Aufbewahrungszeit" .

   Obwohl eine Snapshot-Kopie für einen bestimmten Aufbewahrungszeitraum geschützt ist, kann das Quellvolume von einem Clusteradministrator gelöscht werden, da der WORM-Speicher in Cloud Volumes ONTAP nach dem Modell eines „vertrauenswürdigen Speicheradministrators“ betrieben wird. Darüber hinaus kann ein vertrauenswürdiger Cloud-Administrator die WORM-Daten löschen, indem er die Cloud-Speicherressourcen bearbeitet.

Weiterführende Links

- Weitere Informationen zu WORM finden Sie unter"Erfahren Sie mehr über WORM-Speicher auf Cloud Volumes ONTAP" Die
- Informationen zur Abrechnung von SnapLock -Volumes finden Sie unter"Lizenzierung und Abrechnung in Cloud Volumes ONTAP" Die

Systemadministration

Upgrade von Cloud Volumes ONTAP

Aktualisieren Sie Cloud Volumes ONTAP über die NetApp Console, um Zugriff auf die neuesten Funktionen und Verbesserungen zu erhalten. Sie sollten Cloud Volumes ONTAP -Systeme vorbereiten, bevor Sie die Software aktualisieren.

Upgradeübersicht

Bevor Sie mit dem Upgrade-Prozess für Cloud Volumes ONTAP beginnen, sollten Sie sich über Folgendes im Klaren sein.

Upgrade nur von der Konsole

Sie sollten Cloud Volumes ONTAP nicht mithilfe des ONTAP System Manager oder der ONTAP CLI aktualisieren, sondern nur mithilfe der Konsole. Andernfalls könnte die Systemstabilität beeinträchtigt werden.

Die Konsole bietet zwei Möglichkeiten zum Upgrade von Cloud Volumes ONTAP:

- Indem Sie den Upgrade-Benachrichtigungen folgen, die im System angezeigt werden
- Indem Sie das Upgrade-Image an einem HTTPS-Speicherort platzieren und der Konsole dann die URL mitteilen

Unterstützte Upgradepfade

Die Cloud Volumes ONTAP-Version, auf die Sie aktualisieren können, hängt von der Version ab, die Sie derzeit verwenden. Jede generische Version oder Patch-Version in einer Veröffentlichung in den folgenden Tabellen stellt die Basisversion dar, die für ein Upgrade verfügbar ist. Einzelheiten zu den verfügbaren Patches finden Sie in der "versionierte Versionshinweise" für jede Version.

Unterstützte Upgrade-Pfade für AWS

Aktuelle Version	Versionen, auf die Sie direkt upgraden können
9.17.1 P1	9.18.1
9.16.1	9.17.1 P1
9.15.1	9.16.1
9.15.0	9.15.1
9.14.1	9.15.1
	9.15.0
9.14.0	9.14.1

Aktuelle Version	Versionen, auf die Sie direkt upgraden können
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1
9.11.1	9.12.1
	9.12.0
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9,8	9.9.1
9,7	9,8
9,6	9,7
9,5	9,6
9,4	9,5
9,3	9,4
9,2	9,3
9,1	9,2
9,0	9,1
8,3	9,0

Unterstützte Upgradepfade für Azure

Aktuelle Version	Versionen, auf die Sie direkt upgraden können
9.17.1 P1	9.18.1
9.16.1 P3	9.17.1 P1
9.15.1 P10	9.16.1 P3
9.14.1 P13	9.15.1 P10
9.13.1 P16	9.14.1 P13

Aktuelle Version	Versionen, auf die Sie direkt upgraden können
9.12.1 P18	9.13.1 P16
9.11.1 P20	9.12.1 P18

Wenn Sie eine niedrigere Version von Cloud Volumes ONTAP in Azure haben, müssen Sie zuerst auf die nächste Version aktualisieren und den unterstützten Upgradepfaden folgen, um Ihre Zielversion zu erreichen. Wenn Sie beispielsweise Cloud Volumes ONTAP 9.7 P7 haben, folgen Sie diesem Upgrade-Pfad:

- 9,7 P7 → 9,8 P18
- 9.8 P18 → 9.9.1 P15
- 9.9.1 P15 → 9.10.1 P12
- 9.10.1 P12 → 9.11.1 P20

Unterstützte Upgrade-Pfade für Google Cloud

Aktuelle Version	Versionen, auf die Sie direkt upgraden können
9.17.1 P1	9.18.1
9.16.1	9.17.1 P1
9.15.1	9.16.1
9.15.0	9.15.1
9.14.1	9.15.1
	9.15.0
9.14.0	9.14.1
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1
9.11.1	9.12.1
	9.12.0
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1

Aktuelle Version	Versionen, auf die Sie direkt upgraden können
9,8	9.9.1
9,7	9,8
9,6	9,7
9,5	9,6
9,4	9,5
9,3	9,4
9,2	9,3
9,1	9,2
9,0	9,1
8,3	9,0

Beachten Sie Folgendes:

- Die unterstützten Upgradepfade für Cloud Volumes ONTAP unterscheiden sich von denen für einen lokalen ONTAP Cluster.
- Wenn Sie ein Upgrade durchführen, indem Sie den in einem System angezeigten Benachrichtigungen folgen, werden Sie von der Konsole aufgefordert, ein Upgrade auf eine Version durchzuführen, die diesen unterstützten Upgradepfaden folgt.
- Wenn Sie ein Upgrade durchführen, indem Sie ein Upgrade-Image an einem HTTPS-Speicherort platzieren, achten Sie darauf, diesen unterstützten Upgrade-Pfaden zu folgen.
- In einigen Fällen müssen Sie möglicherweise mehrere Upgrades durchführen, um Ihre Zielversion zu erreichen.

  Wenn Sie beispielsweise Version 9.8 ausführen und auf 9.10.1 aktualisieren möchten, müssen Sie zuerst auf Version 9.9.1 und dann auf 9.10.1 aktualisieren.

Patch-Veröffentlichungen

Ab Januar 2024 sind Patch-Upgrades nur verfügbar, wenn ein Patch-Release für die drei neuesten Versionen von Cloud Volumes ONTAP vorliegt. Gelegentlich sind Patchversionen zur Bereitstellung verfügbar, wenn die RC- oder GA-Version nicht zur Bereitstellung verfügbar ist.

Wir verwenden die neueste GA-Version, um die drei neuesten Versionen zu bestimmen, die in der Konsole angezeigt werden sollen. Wenn die aktuelle GA-Version beispielsweise 9.13.1 ist, werden Patches für 9.11.1–9.13.1 in der Konsole angezeigt.

Für Patch-Versionen 9.11.1 oder niedriger müssen Sie ein manuelles Upgrade-Verfahren verwenden, indem SieHerunterladen des ONTAP Images .

Als allgemeine Regel für Patch-Releases können Sie von einer niedrigeren Patch-Version auf jede höhere Patch-Version in derselben oder der nächsten Cloud Volumes ONTAP Version aktualisieren.

Hier sind einige Beispiele:

- 9.13.0 → 9.13.1 P15

- 9.12.1 → 9.13.1 P2

Zurücksetzen oder Herabstufen

Das Zurücksetzen oder Downgrade von Cloud Volumes ONTAP auf eine frühere Version wird nicht unterstützt.

Support-Registrierung

Cloud Volumes ONTAP muss beim NetApp -Support registriert sein, um die Software mit einer der auf dieser Seite beschriebenen Methoden zu aktualisieren. Dies gilt sowohl für Pay-as-you-go (PAYGO) als auch für Bring Your Own License (BYOL). Sie müssen"PAYGO-Systeme manuell registrieren" , während BYOL-Systeme standardmäßig registriert sind.

Ein System, das nicht für den Support registriert ist, erhält dennoch die Software-Update-Benachrichtigungen, die in der Konsole angezeigt werden, wenn eine neue Version verfügbar ist. Sie müssen das System jedoch registrieren, bevor Sie die Software aktualisieren können.

Upgrades des HA-Mediators

Die Konsole aktualisiert die Mediatorinstanz auch nach Bedarf während des Cloud Volumes ONTAP Upgradeprozesses.

Upgrades in AWS mit den EC2-Instanztypen c4, m4 und r4

Cloud Volumes ONTAP unterstützt die EC2-Instanztypen c4, m4 und r4 nicht mehr. Mit diesen Instanztypen können Sie vorhandene Bereitstellungen auf Cloud Volumes ONTAP Versionen 9.8–9.12.1 aktualisieren. Bevor Sie ein Upgrade durchführen, empfehlen wir Ihnen,Ändern Sie den Instanztyp . Wenn Sie den Instanztyp nicht ändern können, müssen Sieermöglichen eine verbesserte Vernetzung bevor Sie ein Upgrade durchführen. Lesen Sie die folgenden Abschnitte, um mehr über das Ändern des Instanztyps und das Aktivieren von Enhanced Networking zu erfahren.

In Cloud Volumes ONTAP mit Version 9.13.0 und höher können Sie kein Upgrade mit den EC2-Instanztypen c4, m4 und r4 durchführen. In diesem Fall müssen Sie die Anzahl der Festplatten reduzieren und dannÄndern Sie den Instanztyp oder stellen Sie eine neue HA-Paar-Konfiguration mit den EC2-Instanztypen c5, m5 und r5 bereit und migrieren Sie die Daten.

Ändern des Instanztyps

Die EC2-Instance-Typen c4, m4 und r4 ermöglichen mehr Festplatten pro Knoten als die EC2-Instance-Typen c5, m5 und r5. Wenn die Festplattenanzahl pro Knoten für die von Ihnen ausgeführte c4-, m4- oder r4-EC2-Instance unter der maximalen Festplattenzuteilung pro Knoten für c5-, m5- und r5-Instances liegt, können Sie den EC2-Instance-Typ in c5, m5 oder r5 ändern.

"Überprüfen Sie die Festplatten- und Tiering-Grenzen nach EC2-Instanz" "Ändern Sie den EC2-Instanztyp für Cloud Volumes ONTAP"

Wenn Sie den Instanztyp nicht ändern können, befolgen Sie die Schritte inErweiterte Vernetzung ermöglichen .

Erweiterte Vernetzung ermöglichen

Um ein Upgrade auf Cloud Volumes ONTAP Version 9.8 und höher durchzuführen, müssen Sie *Enhanced Networking* auf dem Cluster aktivieren, auf dem der Instanztyp c4, m4 oder r4 ausgeführt wird. Informationen zum Aktivieren von ENA finden Sie im Knowledge Base-Artikel"So aktivieren Sie Enhanced Networking wie SR-IOV oder ENA auf AWS Cloud Volumes ONTAP Instanzen" .

Vorbereiten des Upgrades

Bevor Sie ein Upgrade durchführen, müssen Sie überprüfen, ob Ihre Systeme bereit sind, und alle erforderlichen Konfigurationsänderungen vornehmen.

- Planen Sie Ausfallzeiten ein
- ob die automatische Rückgabe noch aktiviert ist
- SnapMirror Übertragungen aussetzen
- ob Aggregate online sind
- dass sich alle LIFs auf den Home-Ports befinden

Planen Sie Ausfallzeiten ein

Wenn Sie ein Einzelknotensystem aktualisieren, wird das System durch den Aktualisierungsvorgang für bis zu 25 Minuten offline geschaltet, wobei die E/A unterbrochen wird.

In vielen Fällen verläuft die Aktualisierung eines HA-Paares unterbrechungsfrei und die E/A erfolgt ohne Unterbrechung. Während dieses unterbrechungsfreien Upgrade-Prozesses wird jeder Knoten gleichzeitig aktualisiert, um den Clients weiterhin E/A-Vorgänge bereitzustellen.

Sitzungsorientierte Protokolle können bei Upgrades in bestimmten Bereichen negative Auswirkungen auf Clients und Anwendungen haben. Einzelheiten finden Sie im "ONTAP-Dokumentation"

Überprüfen Sie, ob die automatische Rückgabe noch aktiviert ist

Die automatische Rückgabe muss für ein Cloud Volumes ONTAP HA-Paar aktiviert sein (dies ist die Standardeinstellung). Wenn dies nicht der Fall ist, schlägt der Vorgang fehl.

"ONTAP -Dokumentation: Befehle zum Konfigurieren der automatischen Rückgabe"

SnapMirror Übertragungen aussetzen

Wenn ein Cloud Volumes ONTAP -System über aktive SnapMirror Beziehungen verfügt, sollten Sie die Übertragungen am besten aussetzen, bevor Sie die Cloud Volumes ONTAP -Software aktualisieren. Durch das Aussetzen der Übertragungen werden SnapMirror Fehler verhindert. Sie müssen die Übertragungen vom Zielsystem aussetzen.

Obwohl NetApp Backup and Recovery eine Implementierung von SnapMirror zum Erstellen von Sicherungsdateien verwendet (SnapMirror Cloud genannt), müssen Sicherungen beim Upgrade eines Systems nicht ausgesetzt werden.

Informationen zu diesem Vorgang

Diese Schritte beschreiben die Verwendung von ONTAP System Manager für Version 9.3 und höher.

Schritte

1. Melden Sie sich vom Zielsystem aus beim System Manager an.

   Sie können sich beim System Manager anmelden, indem Sie in Ihrem Webbrowser auf die IP-Adresse des Cluster-Management-LIF zeigen. Sie finden die IP-Adresse im Cloud Volumes ONTAP System.

Der Computer, von dem aus Sie auf die Konsole zugreifen, muss über eine Netzwerkverbindung zu Cloud Volumes ONTAP verfügen. Beispielsweise müssen Sie sich möglicherweise von einem Jump-Host aus, der sich im Netzwerk Ihres Cloud-Anbieters befindet, bei der Konsole anmelden.

2. Klicken Sie auf **Schutz > Beziehungen**.
3. Wählen Sie die Beziehung aus und klicken Sie auf **Operationen > Quiesce**.

Überprüfen, ob Aggregate online sind

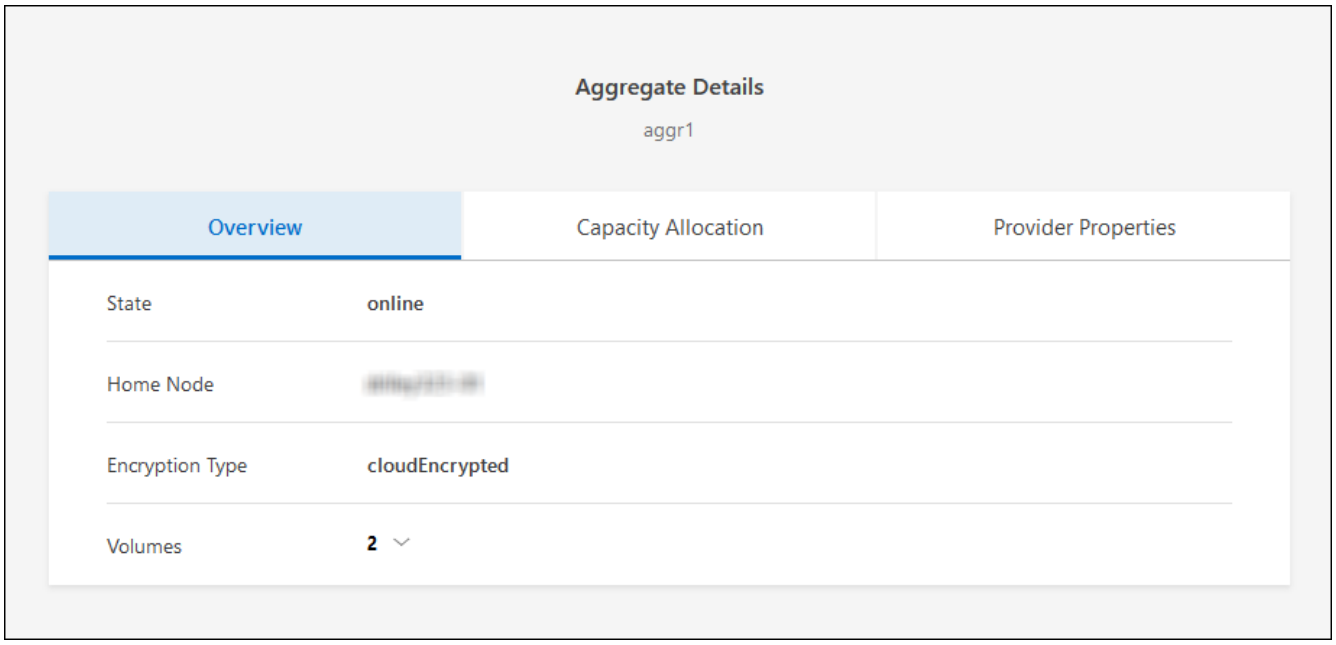
Aggregate für Cloud Volumes ONTAP müssen online sein, bevor Sie die Software aktualisieren. Aggregate sollten in den meisten Konfigurationen online sein, aber wenn nicht, sollten Sie sie online bringen.

Informationen zu diesem Vorgang

Diese Schritte beschreiben die Verwendung von ONTAP System Manager für Version 9.3 und höher.

Schritte

1. Klicken Sie im Cloud Volumes ONTAP -System auf die Registerkarte **Aggregates**.
2. Klicken Sie auf der gewünschten Aggregatkachel auf das ••• Symbol und wählen Sie dann **Aggregierte Details anzeigen** aus.



3. Wenn das Aggregat offline ist, verwenden Sie ONTAP System Manager, um das Aggregat online zu bringen:
   a. Klicken Sie auf **Speicher > Aggregate und Datenträger > Aggregate**.
   b. Wählen Sie das Aggregat aus und klicken Sie dann auf **Weitere Aktionen > Status > Online**.

Stellen Sie sicher, dass sich alle LIFs auf den Home-Ports befinden

Vor dem Upgrade müssen sich alle LIFs auf den Home-Ports befinden. Weitere Informationen finden Sie in der ONTAP -Dokumentation."Stellen Sie sicher, dass sich alle LIFs in den Heimathäfen befinden." .

Wenn ein Upgrade-Fehler auftritt, lesen Sie den Knowledge Base (KB)-Artikel"Das Upgrade von Cloud

Volumes ONTAP schlägt fehl" .

Upgrade von Cloud Volumes ONTAP

Die Konsole benachrichtigt Sie, wenn eine neue Version zum Upgrade verfügbar ist. Von dieser Benachrichtigung aus können Sie den Upgrade-Prozess starten. Weitere Informationen finden Sie unter Upgrade von Konsolenbenachrichtigungen .

Eine weitere Möglichkeit, Software-Upgrades durchzuführen, besteht in der Verwendung eines Bildes auf einer externen URL. Diese Option ist hilfreich, wenn die Konsole nicht auf den S3-Bucket zugreifen kann, um die Software zu aktualisieren, oder wenn Ihnen ein Patch zur Verfügung gestellt wurde. Weitere Informationen finden Sie unter Upgrade von einem unter einer URL verfügbaren Bild .

Upgrade von Konsolenbenachrichtigungen

Die Konsole zeigt in Cloud Volumes ONTAP Arbeitsumgebungen eine Benachrichtigung an, wenn eine neue Version von Cloud Volumes ONTAP verfügbar ist:

Bevor Sie Cloud Volumes ONTAP über die Benachrichtigungen aktualisieren können, müssen Sie über ein NetApp Support Site-Konto verfügen.

Sie können den Upgrade-Prozess über diese Benachrichtigung starten. Der Prozess wird automatisiert, indem das Software-Image aus einem S3-Bucket abgerufen, das Image installiert und dann das System neu gestartet wird.

Bevor Sie beginnen

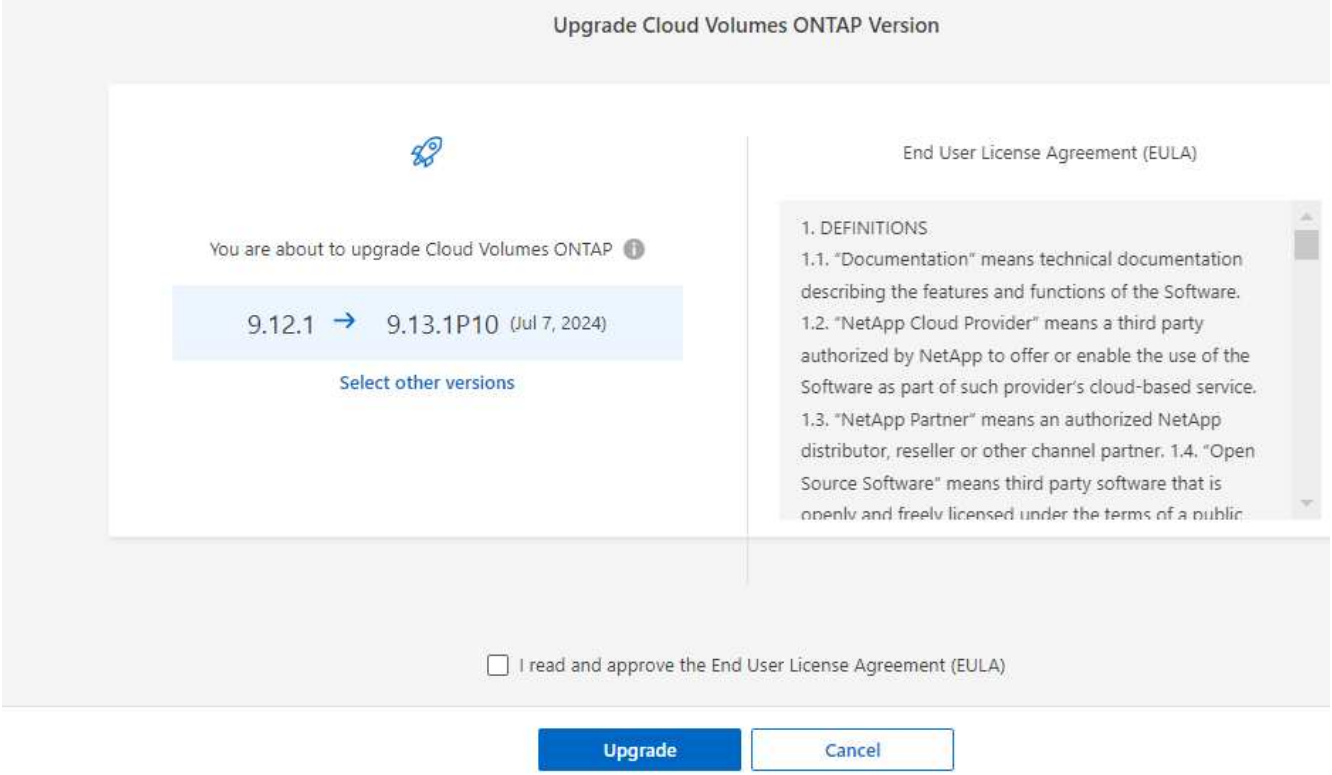
Auf dem Cloud Volumes ONTAP System dürfen keine Vorgänge wie die Erstellung von Volumes oder Aggregaten ausgeführt werden.

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Wählen Sie ein Cloud Volumes ONTAP System aus.

   Wenn eine neue Version verfügbar ist, wird im Reiter „Übersicht“ eine Benachrichtigung angezeigt:

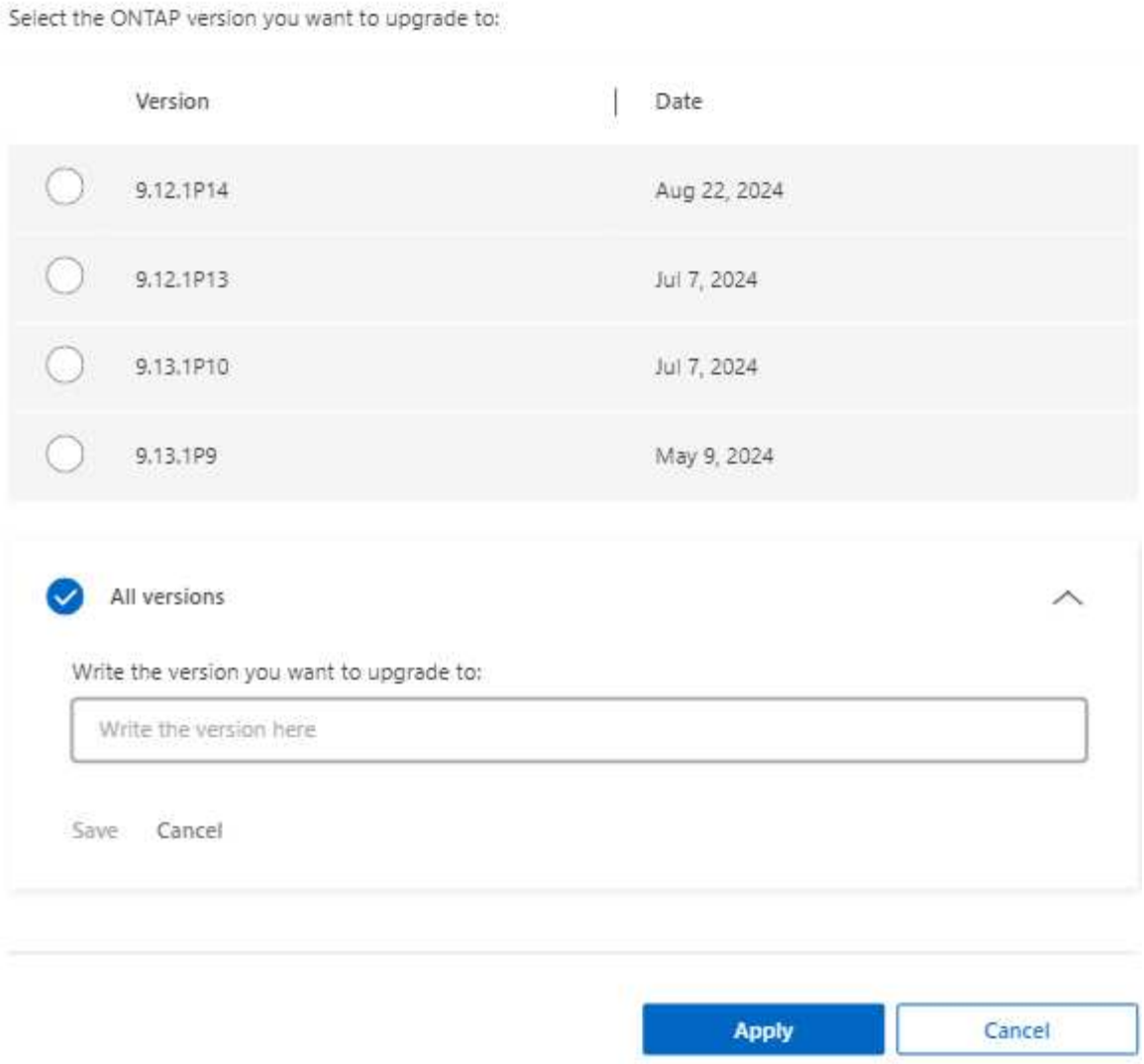
3. Wenn Sie die installierte Version von Cloud Volumes ONTAP aktualisieren möchten, klicken Sie auf **Jetzt aktualisieren!** Standardmäßig wird Ihnen die neueste, kompatible Version zum Upgrade angezeigt.



Wenn Sie auf eine andere Version aktualisieren möchten, klicken Sie auf **Andere Versionen auswählen**. Sie sehen die neuesten Cloud Volumes ONTAP Versionen aufgelistet, die auch mit der auf Ihrem System installierten Version kompatibel sind. Beispielsweise ist die auf Ihrem System installierte Version 9.12.1P3 und die folgenden kompatiblen Versionen sind verfügbar:

- 9.12.1P4 bis 9.12.1P14
- 9.13.1 und 9.13.1P1 Sie sehen 9.13.1P1 als Standardversion für das Upgrade und 9.12.1P13, 9.13.1P14, 9.13.1 und 9.13.1P1 als die anderen verfügbaren Versionen.

4. Optional können Sie auf **Alle Versionen** klicken, um eine andere Version einzugeben, auf die Sie aktualisieren möchten (z. B. den nächsten Patch der installierten Version). Einen kompatiblen Upgrade-Pfad für Ihre aktuelle Cloud Volumes ONTAP Version finden Sie unter"Unterstützte Upgradepfade" .
5. Klicken Sie auf **Speichern** und dann auf **Übernehmen**



.

6. Lesen Sie auf der Seite „Upgrade Cloud Volumes ONTAP“ die EULA und wählen Sie dann **Ich habe die EULA gelesen und stimme ihr zu** aus.
7. Wählen Sie **Upgrade**.
8. Um den Fortschritt anzuzeigen, wählen Sie im Cloud Volumes ONTAP -System **Audit** aus.

Ergebnis

Die Konsole startet das Software-Upgrade. Sie können Aktionen auf dem System ausführen, wenn das Software-Update abgeschlossen ist.

Nach Abschluss

Wenn Sie SnapMirror Übertragungen ausgesetzt haben, verwenden Sie System Manager, um die Übertragungen fortzusetzen.

Upgrade von einem unter einer URL verfügbaren Bild

Sie können das Cloud Volumes ONTAP -Software-Image auf dem Konsolen-Agenten oder auf einem HTTP-Server platzieren und dann das Software-Upgrade von der Konsole aus starten. Sie können diese Option verwenden, wenn die Konsole nicht auf den S3-Bucket zugreifen kann, um die Software zu aktualisieren.

Bevor Sie beginnen

- Auf dem Cloud Volumes ONTAP System dürfen keine Vorgänge wie die Erstellung von Volumes oder Aggregaten ausgeführt werden.
- Wenn Sie HTTPS zum Hosten von ONTAP -Images verwenden, kann das Upgrade aufgrund von SSL-Authentifizierungsproblemen fehlschlagen, die durch fehlende Zertifikate verursacht werden. Die Problemumgehung besteht darin, ein von einer Zertifizierungsstelle signiertes Zertifikat zu generieren und zu installieren, das für die Authentifizierung zwischen ONTAP und der Konsole verwendet werden soll.

  Gehen Sie zur NetApp Knowledge Base, um schrittweise Anleitungen anzuzeigen:

  "NetApp KB: So konfigurieren Sie die Konsole als HTTPS-Server zum Hosten von Upgrade-Images"

Schritte

1. Optional: Richten Sie einen HTTP-Server ein, der das Cloud Volumes ONTAP -Software-Image hosten kann.

   Wenn Sie über eine VPN-Verbindung zum virtuellen Netzwerk verfügen, können Sie das Cloud Volumes ONTAP -Software-Image auf einem HTTP-Server in Ihrem eigenen Netzwerk platzieren. Andernfalls müssen Sie die Datei auf einem HTTP-Server in der Cloud platzieren.

2. Wenn Sie Ihre eigene Sicherheitsgruppe für Cloud Volumes ONTAP verwenden, stellen Sie sicher, dass die ausgehenden Regeln HTTP-Verbindungen zulassen, damit Cloud Volumes ONTAP auf das Software-Image zugreifen kann.

   Die vordefinierte Cloud Volumes ONTAP Sicherheitsgruppe lässt standardmäßig ausgehende HTTP-Verbindungen zu.

3. Besorgen Sie sich das Software-Image von "die NetApp Support Site" .
4. Kopieren Sie das Software-Image in ein Verzeichnis auf dem Konsolenagenten oder auf einem HTTP-Server, von dem die Datei bereitgestellt wird.

   Es stehen zwei Wege zur Verfügung. Der richtige Pfad hängt von der Version Ihres Konsolenagenten ab.

   - `/opt/application/netapp/cloudmanager/docker_occm/data/ontap/images/`
   - `/opt/application/netapp/cloudmanager/ontap/images/`
5. Klicken Sie auf dem System auf das ••• Symbol und klicken Sie dann auf * Cloud Volumes ONTAP aktualisieren*.
6. Geben Sie auf der Seite „Cloud Volumes ONTAP -Version aktualisieren“ die URL ein und klicken Sie dann auf **Image ändern**.

   Wenn Sie das Software-Image in den Konsolen-Agenten im oben angezeigten Pfad kopiert haben, geben Sie die folgende URL ein:

   http://<Private IP-Adresse des Konsolenagenten>/ontap/images/<Bilddateiname>

   In der URL muss **Bilddateiname** dem Format „cot.image.9.13.1P2.tgz“ entsprechen.

7. Klicken Sie zur Bestätigung auf **Weiter**.

Ergebnis

Die Konsole startet das Software-Update. Sobald die Softwareaktualisierung abgeschlossen ist, können Sie

Aktionen auf dem System ausführen.

Nach Abschluss

Wenn Sie SnapMirror Übertragungen ausgesetzt haben, verwenden Sie System Manager, um die Übertragungen fortzusetzen.

Beheben von Downloadfehlern bei Verwendung eines Google Cloud NAT-Gateways

Der Konsolenagent lädt automatisch Softwareupdates für Cloud Volumes ONTAP herunter. Der Download kann fehlschlagen, wenn Ihre Konfiguration ein Google Cloud NAT-Gateway verwendet. Sie können dieses Problem beheben, indem Sie die Anzahl der Teile begrenzen, in die das Software-Image unterteilt ist. Sie müssen die APIs verwenden, um diesen Schritt abzuschließen.

Schritt

1. Senden Sie eine PUT-Anfrage an `/occm/`config mit dem folgenden JSON als Text:

```
{
  "maxDownloadSessions": 32
}
```

Der Wert für *maxDownloadSessions* kann 1 oder eine beliebige Ganzzahl größer als 1 sein. Wenn der Wert 1 ist, wird das heruntergeladene Bild nicht geteilt.

Beachten Sie, dass 32 ein Beispielwert ist. Der Wert, den Sie verwenden sollten, hängt von Ihrer NAT-Konfiguration und der Anzahl der Sitzungen ab, die Sie gleichzeitig haben können.

"Erfahren Sie mehr über den API-Aufruf /occm/config" .

Registrieren Sie Cloud Volumes ONTAP Pay-as-you-go-Systeme

Support von NetApp ist in Cloud Volumes ONTAP Pay-as-you-go (PAYGO)-Systemen enthalten, Sie müssen den Support jedoch zunächst aktivieren, indem Sie die Systeme bei NetApp registrieren.

Die Registrierung eines PAYGO-Systems bei NetApp ist erforderlich, um die ONTAP -Software mit einer der folgenden Methoden zu aktualisieren"auf dieser Seite beschrieben" .

Ein System, das nicht für den Support registriert ist, erhält dennoch die Software-Update-Benachrichtigungen, die in der NetApp Console angezeigt werden, wenn eine neue Version verfügbar ist. Sie müssen das System jedoch registrieren, bevor Sie die Software aktualisieren können.

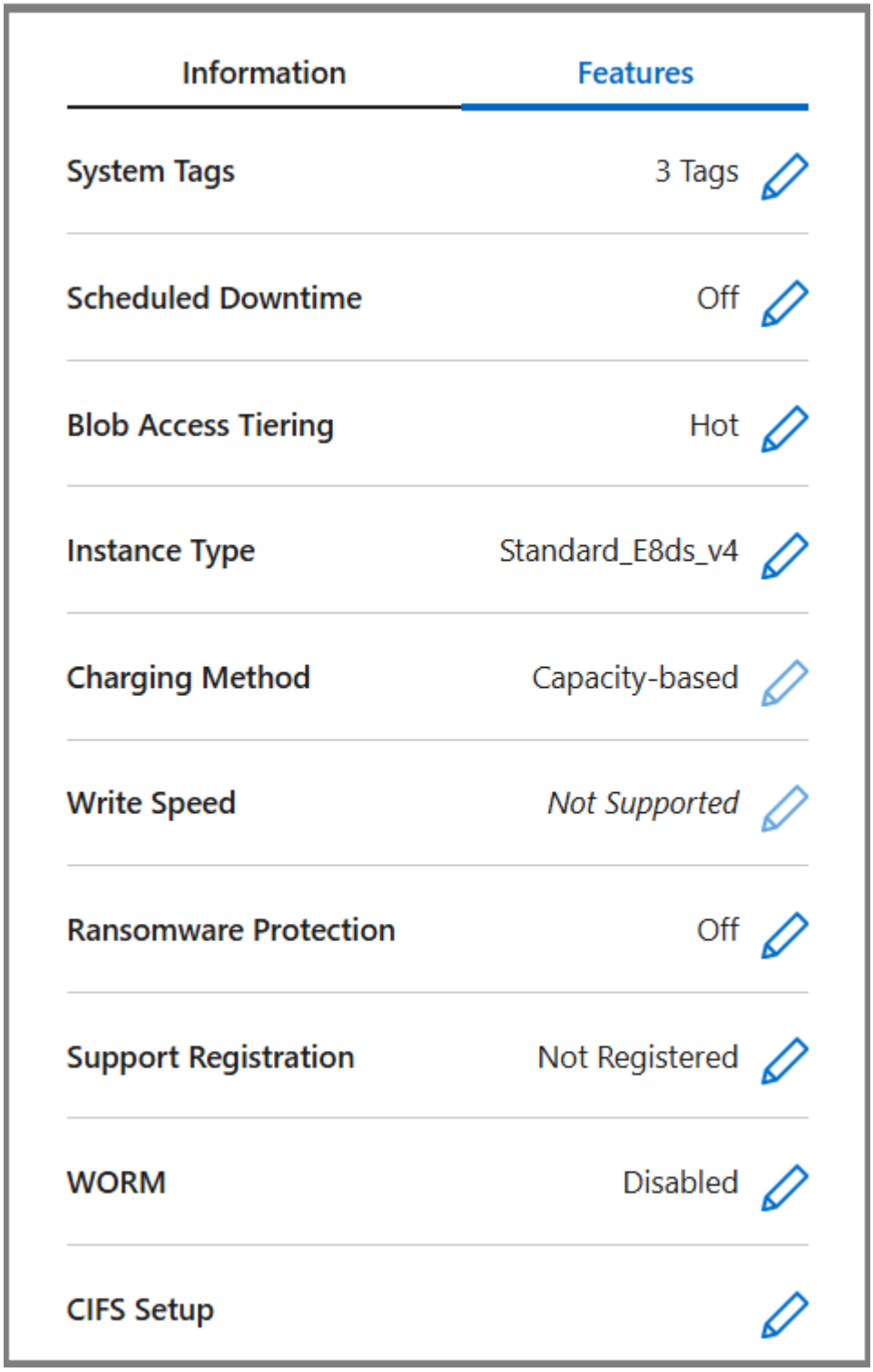
Schritte

1. Wenn Sie Ihr NetApp Support Site-Konto noch nicht zur Konsole hinzugefügt haben, gehen Sie zu **Kontoeinstellungen** und fügen Sie es jetzt hinzu.

   "Erfahren Sie, wie Sie NetApp Support Site-Konten hinzufügen" .

2. Doppelklicken Sie auf der Seite **Systeme** auf den Namen des Systems, das Sie registrieren möchten.
3. Klicken Sie auf der Registerkarte „Übersicht“ auf den Bereich „Funktionen“ und dann auf das Stiftsymbol

neben „Support-Registrierung“.



4. Wählen Sie ein NetApp Support Site-Konto aus und klicken Sie auf **Registrieren**.

Ergebnis

Das System ist bei NetApp registriert.

Konvertieren Sie eine knotenbasierte Cloud Volumes ONTAP -Lizenz in eine kapazitätsbasierte Lizenz

Nach dem Ende der Verfügbarkeit (EOA) Ihrer knotenbasierten Lizenzen sollten Sie mithilfe des Lizenzkonvertierungstools in der NetApp Console auf eine kapazitätsbasierte Lizenzierung umsteigen.

Bei jährlichen oder längerfristigen Verpflichtungen empfiehlt NetApp , dass Sie sich vor dem EOA-Datum (11. November 2024) oder dem Ablaufdatum der Lizenz an Ihren NetApp -Vertreter wenden, um sicherzustellen, dass die Voraussetzungen für den Übergang erfüllt sind. Wenn Sie keinen langfristigen Vertrag für einen Cloud Volumes ONTAP Knoten haben und Ihr System mit einem On-Demand-Pay-as-you-go-Abonnement (PAYGO) betreiben, ist es wichtig, Ihre Konvertierung vor dem Ende des Supports (EOS) am 31. Dezember 2024 zu planen. In beiden Fällen sollten Sie sicherstellen, dass Ihr System die Anforderungen erfüllt, bevor Sie das Lizenzkonvertierungstool in der NetApp Console für einen nahtlosen Übergang verwenden.

Informationen zu EOA und EOS finden Sie unter"Ende der Verfügbarkeit von knotenbasierten Lizenzen" .

Informationen zu diesem Vorgang

- Wenn Sie das Lizenzkonvertierungstool verwenden, erfolgt der Übergang vom knotenbasierten zum kapazitätsbasierten Lizenzierungsmodell vor Ort und online, sodass keine Datenmigration oder Bereitstellung zusätzlicher Cloud-Ressourcen erforderlich ist.
- Es handelt sich um einen unterbrechungsfreien Vorgang, bei dem es weder zu Dienstunterbrechungen noch zu Anwendungsausfallzeiten kommt.
- Die Konto- und Anwendungsdaten in Ihrem Cloud Volumes ONTAP System bleiben erhalten.
- Die zugrunde liegenden Cloud-Ressourcen bleiben nach der Konvertierung unberührt.
- Das Tool zur Lizenzkonvertierung unterstützt alle Bereitstellungstypen, z. B. Einzelknoten, Hochverfügbarkeit (HA) in einer einzelnen Verfügbarkeitszone (AZ), HA in mehreren AZ, Bring Your Own License (BYOL) und PAYGO.
- Das Tool unterstützt alle knotenbasierten Lizenzen als Quelle und alle kapazitätsbasierten Lizenzen als Ziel. Wenn Sie beispielsweise eine knotenbasierte PAYGO Standard-Lizenz besitzen, können Sie diese in jede beliebige kapazitätsbasierte Lizenz umwandeln, die Sie über den Marktplatz erworben haben. NetApp hat den Erwerb, die Verlängerung und die Erneuerung von BYOL-Lizenzen eingeschränkt. Weitere Informationen finden Sie unter "Eingeschränkte Verfügbarkeit der BYOL-Lizenzierung für Cloud Volumes ONTAP" .
- Die Konvertierung wird für alle Cloud-Anbieter, AWS, Azure und Google Cloud unterstützt.
- Nach der Konvertierung wird die Seriennummer der knotenbasierten Lizenz durch ein kapazitätsbasiertes Format ersetzt. Dies geschieht als Teil der Konvertierung und wird auf Ihrem NetApp Support Site (NSS)-Konto angezeigt.
- Wenn Sie zum kapazitätsbasierten Modell wechseln, werden Ihre Daten weiterhin am selben Ort wie bei der knotenbasierten Lizenzierung aufbewahrt. Dieser Ansatz garantiert, dass es während der gesamten Umstellung zu keiner Unterbrechung der Datenplatzierung kommt und die Grundsätze der Datensouveränität gewahrt bleiben.

Bevor Sie beginnen

- Sie sollten über ein NSS-Konto mit Kundenzugriff oder Administratorzugriff verfügen.
- Ihr NSS-Konto sollte mit den Benutzeranmeldeinformationen registriert sein, die Sie für den Zugriff auf die Konsole verwendet haben.
- Das Cloud Volumes ONTAP -System sollte mit dem NSS-Konto mit Kundenzugriff oder Administratorzugriff verknüpft werden.

- Sie sollten über eine gültige kapazitätsbasierte Lizenz verfügen, entweder eine BYOL-Lizenz oder ein Marktplatzabonnement.
- Eine kapazitätsbasierte Lizenz sollte in Ihrem Konto verfügbar sein. Bei dieser Lizenz kann es sich um ein Marktplatzabonnement oder ein BYOL-/Privatangebotspaket handeln, das in der Konsole unter * Licenses and subscriptions* verfügbar ist.
- Machen Sie sich mit den folgenden Kriterien vertraut, bevor Sie ein Zielpaket auswählen:
  - Wenn das Konto über eine kapazitätsbasierte BYOL-Lizenz verfügt, sollte das ausgewählte Zielpaket mit den kapazitätsbasierten BYOL-Lizenzen des Kontos übereinstimmen:
    - Wann `Professional` als Zielpaket ausgewählt ist, sollte das Konto über eine BYOL-Lizenz mit einem Professional-Paket verfügen:
    - Wann `Essentials` als Zielpaket ausgewählt ist, sollte das Konto über eine BYOL-Lizenz mit dem Essentials-Paket verfügen.
  - Wenn das Zielpaket nicht mit der BYOL-Lizenzverfügbarkeit des Kontos übereinstimmt, bedeutet dies, dass die kapazitätsbasierte Lizenz das ausgewählte Paket möglicherweise nicht enthält. In diesem Fall werden Ihnen die Kosten über Ihr Marktplatz-Abonnement in Rechnung gestellt.
  - Liegt keine kapazitätsbasierte BYOL-Lizenz vor, sondern nur ein Marktplatz-Abonnement, sollten Sie darauf achten, dass das gewählte Paket in Ihrem kapazitätsbasierten Marktplatz-Abonnement enthalten ist.
  - Wenn in Ihrer vorhandenen kapazitätsbasierten Lizenz nicht genügend Kapazität vorhanden ist und Sie über ein Marktplatzabonnement verfügen, bei dem die zusätzliche Kapazitätsnutzung in Rechnung gestellt wird, wird Ihnen die zusätzliche Kapazität über Ihr Marktplatzabonnement in Rechnung gestellt.
  - Wenn in Ihrer vorhandenen kapazitätsbasierten Lizenz nicht genügend Kapazität vorhanden ist und Sie kein Marktplatzabonnement haben, um die zusätzliche Kapazitätsnutzung in Rechnung zu stellen, kann die Konvertierung nicht erfolgen. Sie sollten ein Marktplatzabonnement hinzufügen, um die zusätzliche Kapazität in Rechnung zu stellen oder die verfügbare Kapazität Ihrer aktuellen Lizenz zu erweitern.
  - Wenn das Zielpaket nicht mit der BYOL-Lizenzverfügbarkeit des Kontos übereinstimmt und auch wenn Ihre vorhandene kapazitätsbasierte Lizenz nicht über genügend Kapazität verfügt, werden Ihnen die Kosten über Ihr Marktplatzabonnement in Rechnung gestellt.

Wenn eine dieser Voraussetzungen nicht erfüllt ist, findet die Lizenzumwandlung nicht statt. In Einzelfällen kann die Lizenz zwar umgewandelt, aber nicht genutzt werden. Klicken Sie auf das Informationssymbol, um die Probleme zu identifizieren und Korrekturmaßnahmen zu ergreifen.

Schritte

1. Doppelklicken Sie auf der Seite **Systeme** auf den Namen des Systems, für das Sie den Lizenztyp ändern möchten.
2. Klicken Sie auf der Registerkarte „Übersicht“ auf den Bereich „Funktionen“.
3. Aktivieren Sie das Stiftsymbol neben **Lademethode**. Wenn die Lademethode für Ihr System `Node Based` , können Sie es auf Kapazitätsladung umstellen.

   Das Symbol ist deaktiviert, wenn Ihr Cloud Volumes ONTAP System bereits nach Kapazität belastet ist oder wenn eine der Anforderungen nicht erfüllt ist.

4. Überprüfen Sie auf dem Bildschirm **Knotenbasierte Lizenzen in kapazitätsbasierte Lizenzen umwandeln** den Systemnamen und die Quelllizenzdetails.
5. Wählen Sie das Zielpaket für die Konvertierung der vorhandenen Lizenz aus:

    - Wesentliches. Der Standardwert ist `Essentials` .
    - Professional
6. Wenn Sie über eine BYOL-Lizenz verfügen, können Sie das Kontrollkästchen aktivieren, um die knotenbasierte Lizenz nach Abschluss der Konvertierung aus der Konsole zu löschen. Wenn die Konvertierung noch läuft, wird durch Aktivieren dieses Kontrollkästchens die Lizenz nicht aus der Konsole entfernt. Diese Option ist für Marktplatzabonnements nicht verfügbar.
7. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Auswirkungen der Änderung verstehen, und klicken Sie dann auf **Weiter**.

Nach Abschluss

Zeigen Sie die neue Lizenzseriennummer an und überprüfen Sie die Änderungen im Menü * Licenses and subscriptions* der Konsole.

Preisgestaltung in verschiedenen Hyperskalaren

Einzelheiten zu den Preisen finden Sie auf der "NetApp Console Website" .

Informationen zu privaten Angeboten in bestimmten Hyperskalaren erhalten Sie unter:

- AWS – awspo@netapp.com
- Azure – azurepo@netapp.com
- Google Cloud – gcppo@netapp.com

Starten und Stoppen eines Cloud Volumes ONTAP -Systems

Sie können Cloud Volumes ONTAP über die NetApp Console stoppen und starten, um Ihre Cloud-Computing-Kosten zu verwalten.

Planen automatischer Shutdowns von Cloud Volumes ONTAP

Möglicherweise möchten Sie Cloud Volumes ONTAP während bestimmter Zeitintervalle herunterfahren, um Ihre Rechenkosten zu senken. Anstatt dies manuell zu tun, können Sie die Konsole so konfigurieren, dass Systeme zu bestimmten Zeiten automatisch heruntergefahren und neu gestartet werden.

Informationen zu diesem Vorgang

- Wenn Sie ein automatisches Herunterfahren Ihres Cloud Volumes ONTAP Systems planen, verschiebt die Konsole das Herunterfahren, wenn eine aktive Datenübertragung läuft.

  Es fährt das System herunter, nachdem die Übertragung abgeschlossen ist.

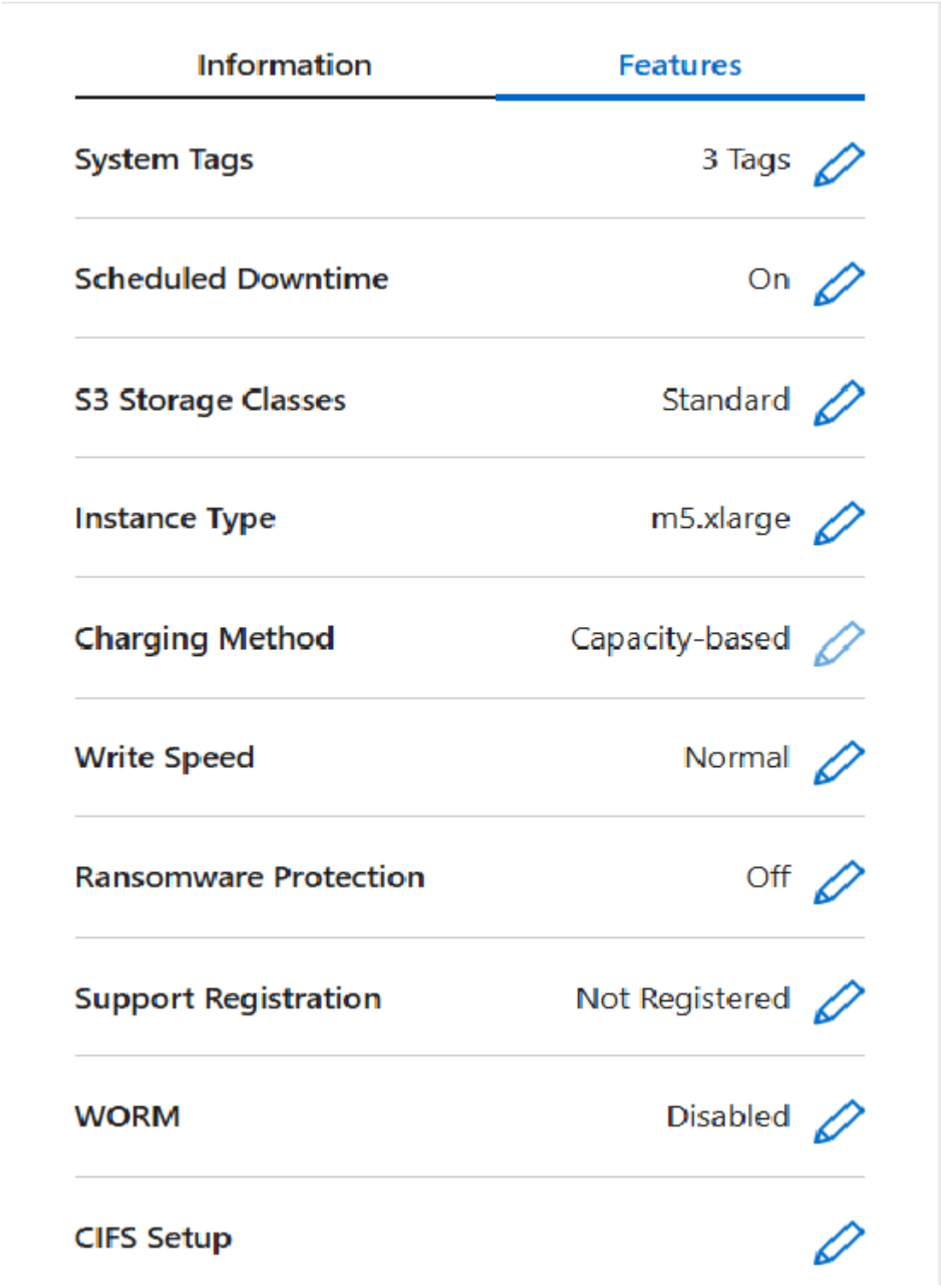
- Diese Aufgabe plant das automatische Herunterfahren beider Knoten in einem HA-Paar.
- Beim Ausschalten von Cloud Volumes ONTAP durch geplante Herunterfahren werden keine Snapshots von Boot- und Root-Festplatten erstellt.

  Snapshots werden nur dann automatisch erstellt, wenn ein manuelles Herunterfahren durchgeführt wird, wie im nächsten Abschnitt beschrieben.

Schritte

1. Doppelklicken Sie auf der Seite **Systeme** auf das Cloud Volumes ONTAP -System.

2. Klicken Sie auf der Registerkarte „Übersicht“ auf das Bedienfeld „Funktionen“ und dann auf das Stiftsymbol neben „Geplante Ausfallzeit“*.



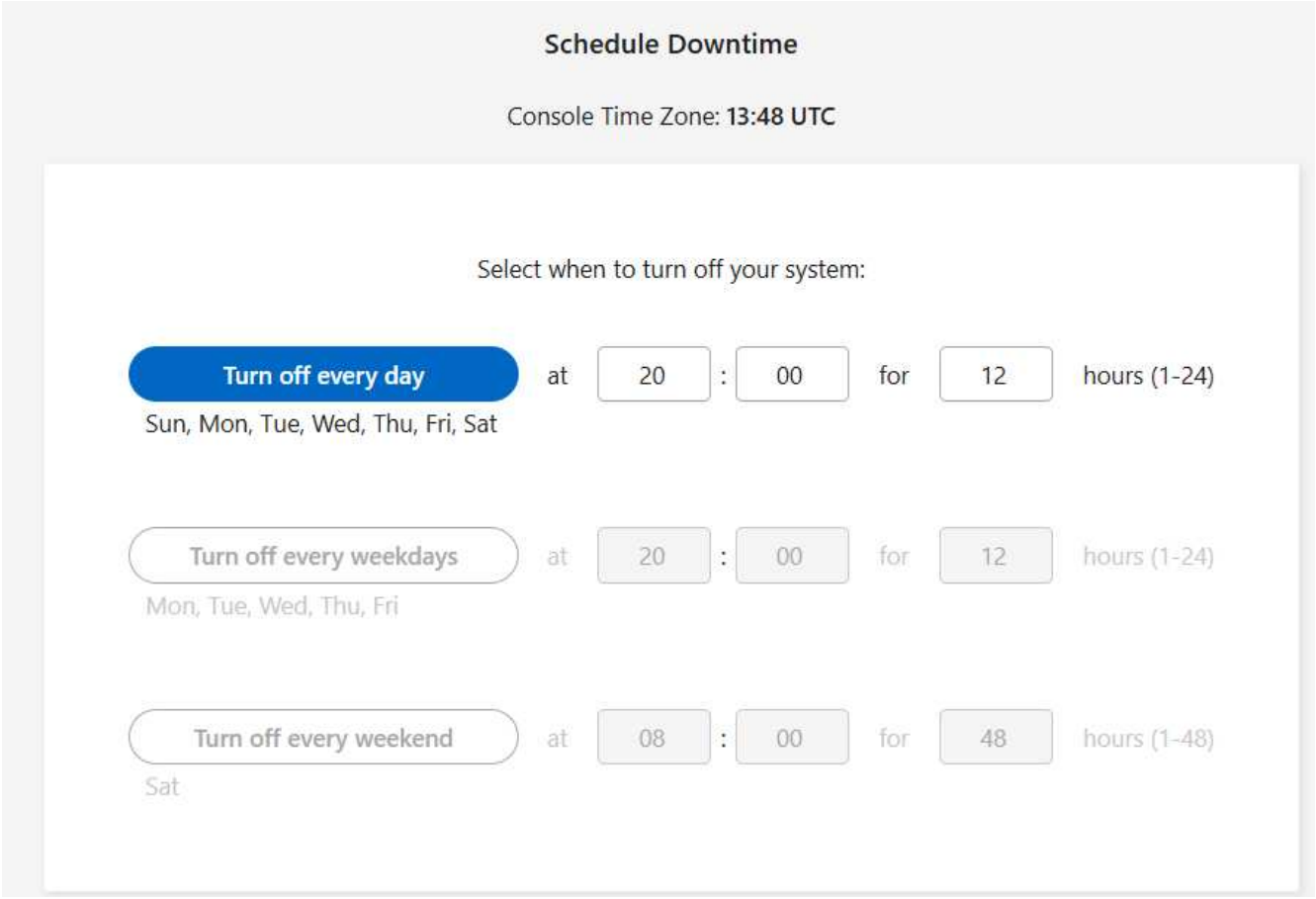
3. Geben Sie den Zeitplan für das Herunterfahren an:

   a. Wählen Sie, ob Sie das System jeden Tag, jeden Wochentag, jedes Wochenende oder eine beliebige Kombination der drei Optionen herunterfahren möchten.

   b. Geben Sie an, wann und für wie lange Sie das System ausschalten möchten.

      Beispiel

Das folgende Bild zeigt einen Zeitplan, der die Konsole anweist, das System jeden Samstag um 20:00 Uhr (20:00 Uhr) für 12 Stunden herunterzufahren. Die Konsole startet das System jeden Montag um 0:00 Uhr neu



4. Klicken Sie auf **Speichern**.

Ergebnis

Der Zeitplan wird gespeichert. Der entsprechende Eintrag „Geplante Ausfallzeit“ im Bereich „Funktionen“ zeigt „Ein“ an.

Stoppen von Cloud Volumes ONTAP

Durch das Stoppen von Cloud Volumes ONTAP sparen Sie sich anfallende Rechenkosten und erstellen Snapshots der Root- und Boot-Festplatten, die bei der Fehlerbehebung hilfreich sein können.

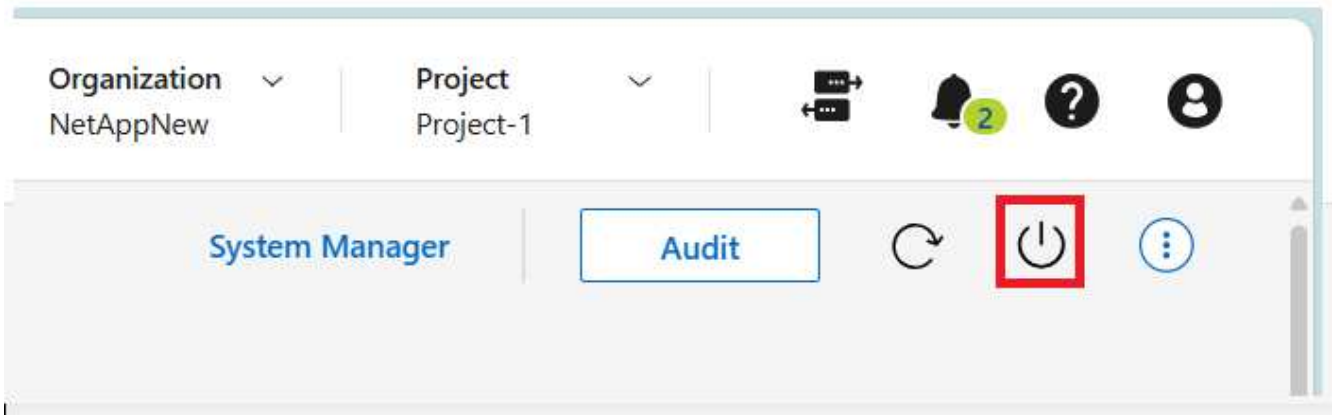
> Um Kosten zu sparen, löscht die Konsole regelmäßig ältere Snapshots von Root- und Boot-Festplatten. Sowohl für die Root- als auch für die Boot-Festplatte werden nur die beiden aktuellsten Snapshots beibehalten.

Informationen zu diesem Vorgang

Wenn Sie ein HA-Paar stoppen, fährt die Konsole beide Knoten herunter.

Schritte

1. Klicken Sie im System auf das Symbol **Ausschalten**.



2. Lassen Sie die Option zum Erstellen von Snapshots aktiviert, da die Snapshots eine Systemwiederherstellung ermöglichen können.
3. Klicken Sie auf **Ausschalten**.

   Das Anhalten des Systems kann einige Minuten dauern. Sie können Systeme zu einem späteren Zeitpunkt von der Seite **Systeme** aus neu starten.

   Beim Neustart werden automatisch Snapshots erstellt.

Synchronisieren Sie die Cloud Volumes ONTAP -Systemzeit mithilfe des NTP-Servers

Um eine genaue Zeitsynchronisierung zu gewährleisten, müssen Sie einen Network Time Protocol (NTP)-Server für Ihre Cloud Volumes ONTAP Systeme einrichten. Stellen Sie sicher, dass Sie bei allen Cloud-Anbietern einen NTP-Server für Ihre Cloud Volumes ONTAP Systeme konfigurieren, um eine konsistente Zeitsynchronisierung innerhalb Ihres Netzwerks zu gewährleisten.

Wenn Sie keinen NTP-Server konfigurieren, kann es zu Serviceunterbrechungen und ungenauer Zeitsynchronisierung kommen.

Sie können einen NTP-Server wie folgt angeben:

- "Die NetApp Console API".
- Der ONTAP CLI-Befehl "Cluster-Zeitdienst-NTP-Server erstellen"Die

Weiterführende Links

- Wissensdatenbankartikel (KB): "Wie nutzt ein CVO-Cluster NTP?"
- "Vorbereiten der Verwendung der API"
- "Cloud Volumes ONTAP -Workflows"
- "Abrufen der erforderlichen Kennungen"
- "Verwenden Sie die REST-APIs für die NetApp Console"

Ändern Sie die Schreibgeschwindigkeit des Systems

Sie können in der NetApp Console eine normale oder hohe Schreibgeschwindigkeit für Cloud Volumes ONTAP auswählen. Die Standardschreibgeschwindigkeit ist normal. Sie können auf eine hohe Schreibgeschwindigkeit umstellen, wenn für Ihre Arbeitslast eine schnelle Schreibleistung erforderlich ist.

Hohe Schreibgeschwindigkeiten werden bei allen Arten von Einzelknotensystemen und einigen HA-Paarkonfigurationen unterstützt. Unterstützte Konfigurationen anzeigen in der "Versionshinweise zu Cloud Volumes ONTAP"

Bevor Sie die Schreibgeschwindigkeit ändern, sollten Sie"die Unterschiede zwischen den normalen und hohen Einstellungen verstehen" .

Informationen zu diesem Vorgang

- Stellen Sie sicher, dass keine Vorgänge wie die Erstellung von Volumes oder Aggregaten ausgeführt werden.
- Beachten Sie, dass diese Änderung das Cloud Volumes ONTAP -System neu startet. Dies ist ein störender Prozess, der Ausfallzeiten für das gesamte System erfordert.

Schritte

1. Doppelklicken Sie auf der Seite **Systeme** auf den Namen des Systems, für das Sie die Schreibgeschwindigkeit konfigurieren.
2. Klicken Sie auf der Registerkarte „Übersicht“ auf das Bedienfeld „Funktionen“ und dann auf das Stiftsymbol neben „Schreibgeschwindigkeit“.
3. Wählen Sie **Normal** oder **Hoch**.

   Wenn Sie „Hoch“ wählen, müssen Sie die Aussage „Ich verstehe …“ lesen und durch Ankreuzen des Kästchens bestätigen.

   Die Schreibgeschwindigkeitsoption **Hohe** wird mit Cloud Volumes ONTAP HA-Paaren in Google Cloud ab Version 9.13.0 unterstützt.

4. Klicken Sie auf **Speichern**, überprüfen Sie die Bestätigungsnachricht und klicken Sie dann auf **Genehmigen**.

Ändern Sie das Administratorkennwort für den Cloud Volumes ONTAP -Cluster

Cloud Volumes ONTAP umfasst ein Cluster-Administratorkonto. Sie können das Kennwort für dieses Konto bei Bedarf über die NetApp Console ändern.

Sie sollten das Kennwort für das Administratorkonto nicht über den ONTAP System Manager oder die ONTAP CLI ändern. Das Passwort wird nicht in der Konsole angezeigt. Dies hat zur Folge, dass die Konsole die Instanz nicht ordnungsgemäß überwachen kann.

Informationen zu diesem Vorgang

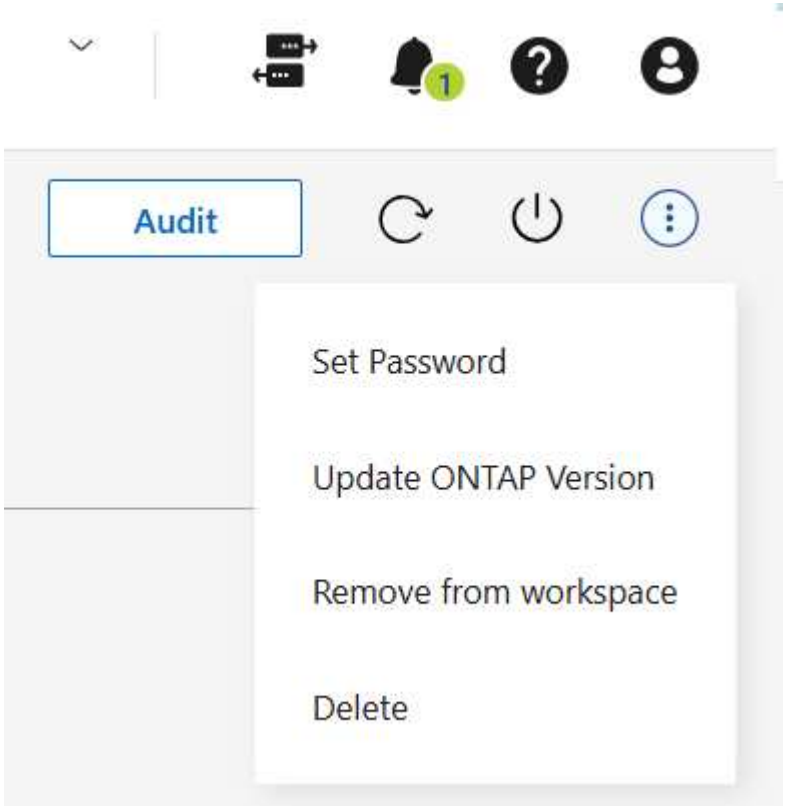
Das Passwort muss einige Regeln beachten. Das neue Passwort:

- Sollte das Wort nicht enthalten `admin`

- Muss zwischen acht und 50 Zeichen lang sein
- Muss mindestens einen englischen Buchstaben und eine Ziffer enthalten
- Sollte diese Sonderzeichen nicht enthalten: `/ ( ) { } [ ] # : % " ? \`

Schritte

1. Doppelklicken Sie auf der Seite **Systeme** auf den Namen des Cloud Volumes ONTAP -Systems.
2. Klicken Sie oben rechts in der Konsole auf das ••• Symbol und wählen Sie **Passwort festlegen**.



Systeme hinzufügen, entfernen oder löschen

Fügen Sie der NetApp Console ein vorhandenes Cloud Volumes ONTAP -System hinzu

Sie können bestehende Cloud Volumes ONTAP-Systeme zur NetApp Console zur zentralen Verwaltung erkennen und hinzufügen. Wenn Sie ein System mit einem Konto einbinden, wird das System mit diesem Konto registriert. In Umgebungen mit mehreren Konten oder Organisationen können Sie nur Systeme erkennen und verwalten, die mit Ihrem Console-Anmeldekonto registriert sind.

Bei der Arbeit mit Systemregistrierungen ist darauf zu achten, dass alle Aktionen innerhalb derselben Organisation und desselben Kontos durchgeführt werden, in denen die Systeme ursprünglich integriert wurden. Beispielsweise können Sie ein Cloud Volumes ONTAP System auf einen neuen Console Agent verschieben, wenn die Migration innerhalb derselben Organisation erfolgt.

Sie können keine Systeme entdecken, anzeigen oder verwalten, die bei einem anderen Konto oder einer anderen Organisation registriert sind.

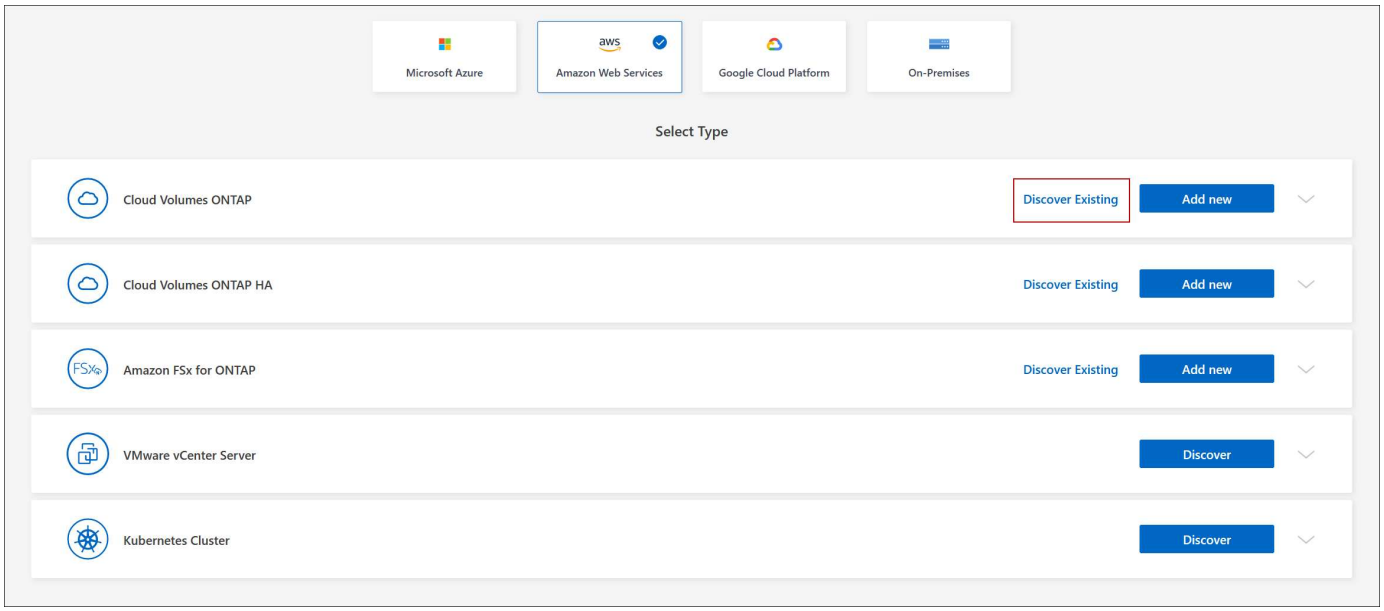
Bevor Sie beginnen

Sie müssen das Kennwort für das Cloud Volumes ONTAP Administratorbenutzerkonto kennen.

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Klicken Sie auf der Seite **System** auf **System hinzufügen**.
3. Wählen Sie den Cloud-Anbieter aus, bei dem sich das System befindet.
4. Wählen Sie den Typ des hinzuzufügenden Cloud Volumes ONTAP Systems aus.
5. Klicken Sie auf den Link, um ein vorhandenes System zu entdecken.

+



1. Wählen Sie auf der Seite „Region“ eine Region aus. Sie können die Systeme sehen, die in der ausgewählten Region ausgeführt werden.

   Cloud Volumes ONTAP -Systeme werden auf dieser Seite als Instanzen dargestellt. Aus der Liste können Sie nur die Instanzen auswählen, die mit dem aktuellen Konto registriert sind.

2. Geben Sie auf der Seite „Anmeldeinformationen“ das Kennwort für den Cloud Volumes ONTAP Administratorbenutzer ein und wählen Sie dann **Los**.

Ergebnis

Die Konsole fügt die Cloud Volumes ONTAP -Systeme zur Seite **Systeme** hinzu.

Entfernen eines Cloud Volumes ONTAP -Systems aus der NetApp Console

Sie können ein Cloud Volumes ONTAP -System entfernen, um es auf ein anderes System zu verschieben oder um Erkennungsprobleme zu beheben.

Informationen zu diesem Vorgang

Durch das Entfernen eines Cloud Volumes ONTAP -Systems wird es aus der NetApp Console entfernt. Das Cloud Volumes ONTAP -System wird dadurch nicht gelöscht. Sie können das System später bei Bedarf erneut entdecken.

Schritte

1. Doppelklicken Sie auf der Seite **Systeme** auf das System, das Sie entfernen möchten.
2. Klicken Sie oben rechts in der Konsole auf das ••• Symbol und wählen Sie **Aus Arbeitsbereich entfernen**.
3. Klicken Sie im Fenster **Aus Arbeitsbereich entfernen** auf **Entfernen**.

Ergebnis

Die Konsole entfernt das System. Benutzer können das gelöschte System jederzeit auf der Seite **Systeme** wiederfinden.

Löschen eines Cloud Volumes ONTAP -Systems aus der NetApp Console

Sie sollten Cloud Volumes ONTAP -Systeme immer aus der NetApp Console und nicht aus der Anwendung Ihres Cloud-Anbieters löschen. Wenn Sie beispielsweise eine lizenzierte Cloud Volumes ONTAP Instanz bei Ihrem Cloud-Anbieter kündigen, können Sie den Lizenzschlüssel nicht für eine andere Instanz verwenden. Sie müssen das Cloud Volumes ONTAP -System aus der Konsole löschen, um die Lizenz freizugeben.

Wenn Sie ein System löschen, beendet die Konsole Cloud Volumes ONTAP Instanzen und löscht Festplatten und Snapshots.

> Andere Ressourcen, wie beispielsweise von NetApp Backup and Recovery verwaltete Backups und Instanzen für NetApp Data Classification, werden beim Löschen eines Systems nicht gelöscht. Sie müssen sie manuell löschen. Wenn Sie dies nicht tun, fallen für diese Ressourcen weiterhin Kosten an.

Wenn die Konsole Cloud Volumes ONTAP bei Ihrem Cloud-Anbieter bereitstellt, aktiviert sie den Kündigungsschutz auf den Instanzen. Diese Option hilft, eine versehentliche Beendigung zu verhindern.

Schritte

1. Wenn Sie die Sicherung und Wiederherstellung auf dem System aktiviert haben, prüfen Sie, ob die gesicherten Daten noch benötigt werden, und dann "Löschen Sie ggf. die Backups" Die

   Backup und Recovery sind konzeptionell unabhängig von Cloud Volumes ONTAP . Backup and Recovery löscht Backups nicht automatisch, wenn Sie ein Cloud Volumes ONTAP -System löschen, und in der Benutzeroberfläche gibt es derzeit keine Unterstützung zum Löschen der Backups, nachdem das System gelöscht wurde.

2. Wenn Sie die Datenklassifizierung auf diesem System aktiviert haben und kein anderes System diesen Dienst verwendet, müssen Sie die Instanz für den Dienst löschen.

   "Weitere Informationen zur Datenklassifizierungsinstanz" .

3. Löschen Sie das Cloud Volumes ONTAP -System.
   a. Doppelklicken Sie auf der Seite **Systeme** auf den Namen des Cloud Volumes ONTAP Systems, das Sie löschen möchten.
   b. Klicken Sie oben rechts in der Konsole auf das ••• Symbol und wählen Sie **Löschen**.
   c. Geben Sie den Namen des Systems ein, das Sie löschen möchten, und klicken Sie dann auf **Löschen**. Das Löschen eines Systems kann bis zu fünf Minuten dauern.

Backup und Recovery sind nur für Cloud Volumes ONTAP Professional-Lizenzen kostenlos. Dieser kostenlose Vorteil gilt nicht für gelöschte Umgebungen. Wenn gesicherte Kopien der Cloud Volumes ONTAP -Umgebung in einer Backup- und Recovery-Instanz aufbewahrt werden, werden Ihnen die gesicherten Kopien in Rechnung gestellt, bis sie gelöscht werden.

AWS -Verwaltung

Ändern Sie den EC2-Instanztyp für ein Cloud Volumes ONTAP System in AWS

Sie können aus mehreren Instanzen oder Typen wählen, wenn Sie Cloud Volumes ONTAP in AWS starten. Sie können den Instanztyp jederzeit ändern, wenn Sie feststellen, dass er für Ihre Anforderungen zu klein oder zu groß ist.

Informationen zu diesem Vorgang

- Die automatische Rückgabe muss für ein Cloud Volumes ONTAP HA-Paar aktiviert sein (dies ist die Standardeinstellung). Wenn dies nicht der Fall ist, schlägt der Vorgang fehl.

  "ONTAP 9-Dokumentation: Befehle zum Konfigurieren der automatischen Rückgabe"

- Das Ändern des Instanztyps kann sich auf die AWS-Servicegebühren auswirken.
- Der Vorgang startet Cloud Volumes ONTAP.

  Bei Single-Node-Systemen wird die I/O unterbrochen.

  Bei HA-Paaren erfolgt die Änderung ohne Unterbrechung. HA-Paare stellen weiterhin Daten bereit.

Die NetApp Console ändert jeweils einen Knoten, indem sie die Übernahme einleitet und auf die Rückgabe wartet. Das Qualitätssicherungsteam von NetApp hat während dieses Vorgangs sowohl das Schreiben als auch das Lesen von Dateien getestet und konnte auf der Clientseite keine Probleme feststellen. Beim Ändern der Verbindungen wurden auf der E/A-Ebene einige Wiederholungsversuche beobachtet, die Anwendungsschicht konnte die Neuverdrahtung der NFS/CIFS-Verbindungen jedoch bewältigen.

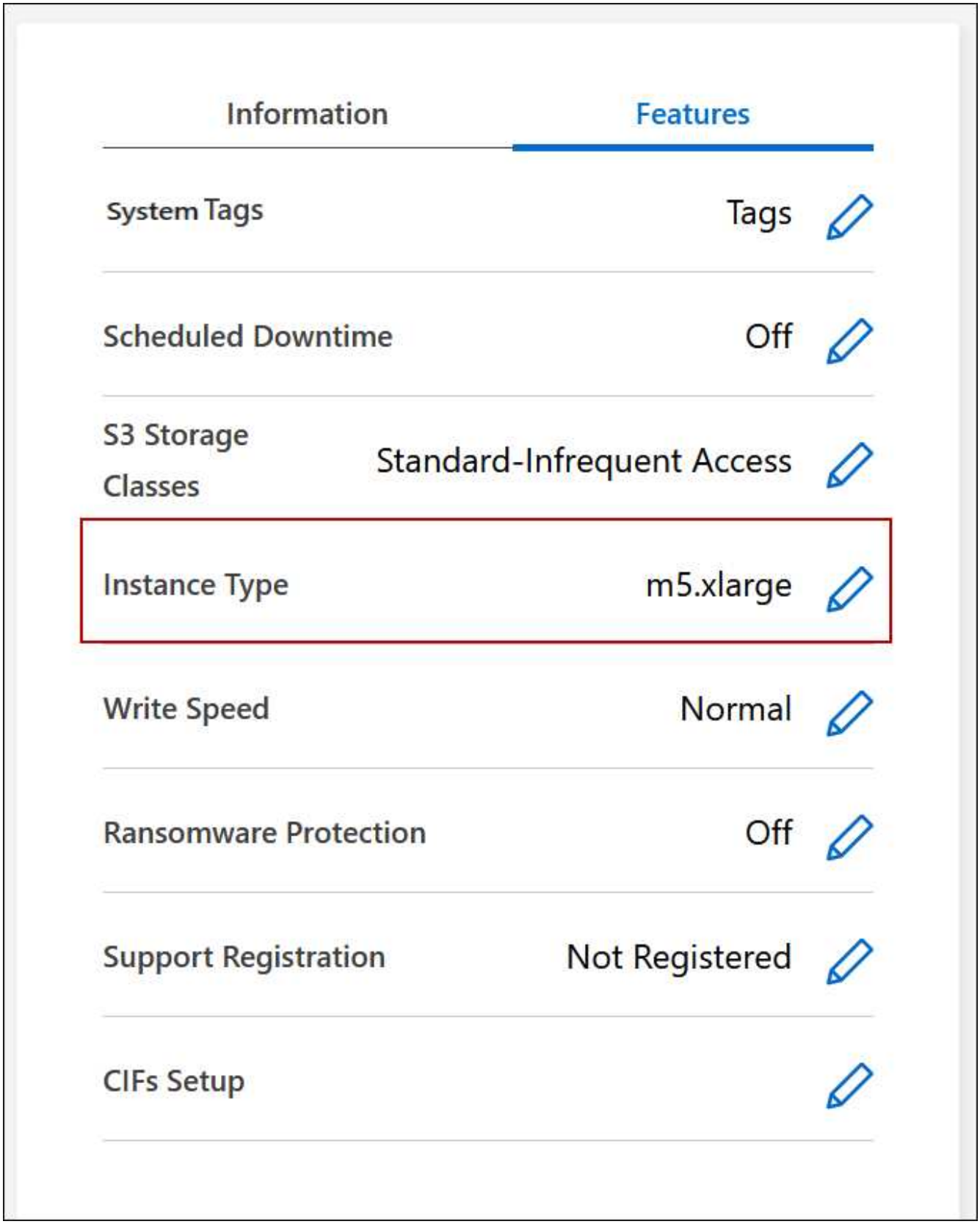
Referenz

Eine Liste der unterstützten Instanztypen in AWS finden Sie unter"Unterstützte EC2-Instanzen" .

Wenn Sie den Instanztyp von c4-, m4- oder r4-Instanzen nicht ändern können, lesen Sie den KB-Artikel"Konvertieren einer AWS Xen CVO-Instanz in Nitro (KVM)" .

Schritte

1. Wählen Sie auf der Seite **Systeme** das System aus.
2. Klicken Sie auf der Registerkarte „Übersicht“ auf den Bereich „Funktionen“ und dann auf das Stiftsymbol neben „Instanztyp“ .



Wenn Sie eine knotenbasierte Pay-as-you-go-Lizenz (PAYGO) verwenden, können Sie optional eine andere Lizenz und einen anderen Instanztyp auswählen, indem Sie auf das Stiftsymbol neben **Lizenztyp** klicken.

3. Wählen Sie einen Instanztyp aus, aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die

Auswirkungen der Änderung verstehen, und klicken Sie dann auf **Ändern**.

Ergebnis

Cloud Volumes ONTAP wird mit der neuen Konfiguration neu gestartet.

Routentabellen für Cloud Volumes ONTAP HA-Paare in mehreren AWS AZs ändern

Sie können die AWS-Routentabellen ändern, die Routen zu den Floating-IP-Adressen für ein HA-Paar enthalten, das in mehreren AWS Availability Zones (AZs) bereitgestellt wird. Sie können dies tun, wenn neue NFS- oder CIFS-Clients auf ein HA-Paar in AWS zugreifen müssen.

Schritte

1. Wählen Sie auf der Seite **Systeme** das System aus.
2. Klicken Sie auf der Registerkarte „Übersicht“ auf den Bereich „Funktionen“ und dann auf das Stiftsymbol neben „Routentabellen“.
3. Ändern Sie die Liste der ausgewählten Routentabellen und klicken Sie dann auf **Speichern**.

Ergebnis

Die NetApp Console sendet eine AWS-Anfrage zum Ändern der Routentabellen.

Azure-Verwaltung

Ändern des Azure-VM-Typs für Cloud Volumes ONTAP

Sie können aus mehreren VM-Typen wählen, wenn Sie Cloud Volumes ONTAP in Microsoft Azure starten. Sie können den VM-Typ jederzeit ändern, wenn Sie feststellen, dass er für Ihre Anforderungen zu klein oder zu groß ist.

Informationen zu diesem Vorgang

- Die automatische Rückgabe muss für ein Cloud Volumes ONTAP HA-Paar aktiviert sein (dies ist die Standardeinstellung). Wenn dies nicht der Fall ist, schlägt der Vorgang fehl.

  "ONTAP 9-Dokumentation: Befehle zum Konfigurieren der automatischen Rückgabe"

- Das Ändern des VM-Typs kann sich auf die Servicegebühren von Microsoft Azure auswirken.
- Der Vorgang startet Cloud Volumes ONTAP.

  Bei Single-Node-Systemen wird die I/O unterbrochen.

  Bei HA-Paaren erfolgt die Änderung ohne Unterbrechung. HA-Paare stellen weiterhin Daten bereit.

  Die NetApp Console ändert jeweils einen Knoten, indem sie die Übernahme einleitet und auf die Rückgabe wartet. Das Qualitätssicherungsteam von NetApp hat während dieses Vorgangs sowohl das Schreiben als auch das Lesen von Dateien getestet und konnte auf der Clientseite keine Probleme feststellen. Beim Ändern der Verbindungen wurden auf der E/A-Ebene einige Wiederholungsversuche beobachtet, die Anwendungsschicht konnte die Neuverdrahtung der NFS/CIFS-Verbindungen jedoch bewältigen.

Schritte

1. Wählen Sie auf der Seite **Systeme** das System aus.
2. Klicken Sie auf der Registerkarte „Übersicht“ auf den Bereich „Funktionen“ und dann auf das Stiftsymbol neben „VM-Typ“.

   Wenn Sie eine knotenbasierte Pay-as-you-go-Lizenz (PAYGO) verwenden, können Sie optional eine andere Lizenz und einen anderen VM-Typ auswählen, indem Sie auf das Stiftsymbol neben **Lizenztyp** klicken.

3. Wählen Sie einen VM-Typ aus, aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Auswirkungen der Änderung verstehen, und klicken Sie dann auf **Ändern**.

Ergebnis

Cloud Volumes ONTAP wird mit der neuen Konfiguration neu gestartet.

Außerkraftsetzen von CIFS-Sperren für Cloud Volumes ONTAP HA-Paare in Azure

Der Organisations- oder Kontoadministrator kann in der NetApp Console eine Einstellung aktivieren, die Probleme mit der Rückgabe von Cloud Volumes ONTAP -Speicher während Azure-Wartungsereignissen verhindert. Wenn Sie diese Einstellung aktivieren, blockiert Cloud Volumes ONTAP CIFS-Sperren und setzt aktive CIFS-Sitzungen zurück.

Informationen zu diesem Vorgang

Microsoft Azure plant regelmäßige Wartungsereignisse auf seinen virtuellen Maschinen. Wenn bei einem Cloud Volumes ONTAP HA-Paar ein Wartungsereignis auftritt, leitet das HA-Paar die Speicherübernahme ein. Wenn während dieses Wartungsereignisses aktive CIFS-Sitzungen vorhanden sind, können die Sperren der CIFS-Dateien die Speicherrückgabe verhindern.

Wenn Sie diese Einstellung aktivieren, wird Cloud Volumes ONTAP die Sperren blockieren und die aktiven CIFS-Sitzungen zurücksetzen. Dadurch kann das HA-Paar während dieser Wartungsereignisse die Speicherrückgabe abschließen.

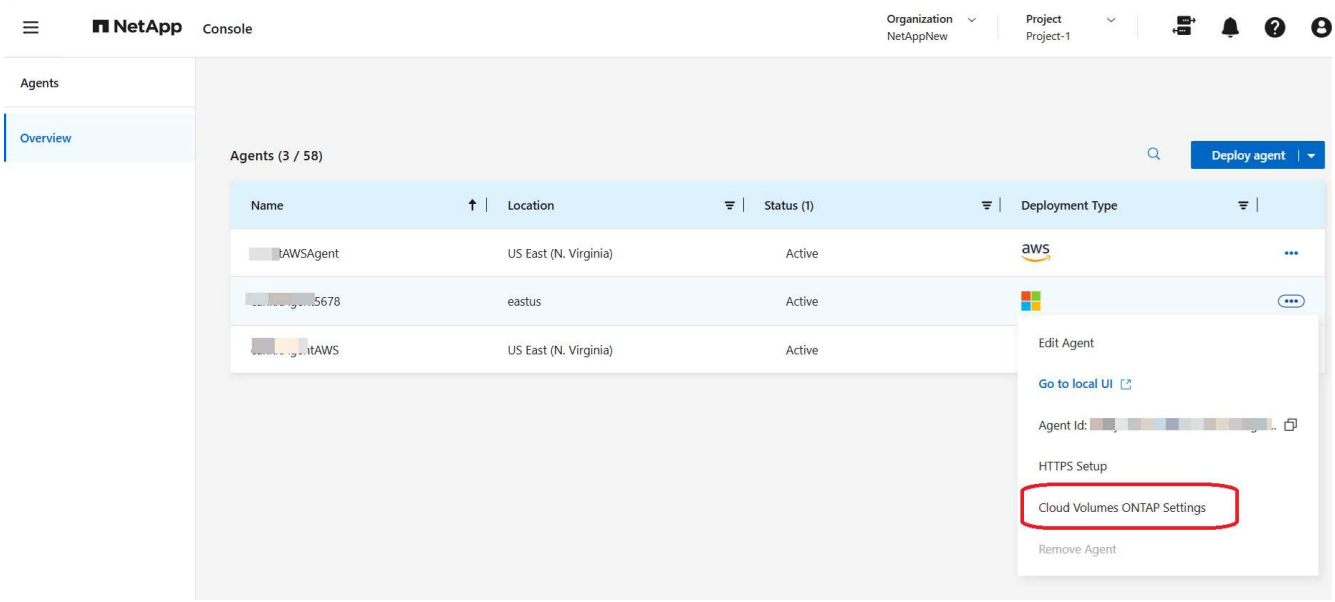
Dieser Vorgang kann für CIFS-Clients störend sein. Daten, die nicht von CIFS-Clients festgeschrieben werden, können verloren gehen.

Bevor Sie beginnen

Sie müssen einen Konsolenagenten erstellen, bevor Sie die Konsoleneinstellungen ändern können. "Erfahren Sie mehr" .

Schritte

1. Gehen Sie im linken Navigationsbereich zu **Administration > Agenten**.
2. Klicken Sie auf das ••• Symbol für den Konsolenagenten, der Ihr Cloud Volumes ONTAP -System verwaltet.
3. Wählen Sie * Cloud Volumes ONTAP -Einstellungen*.



4. Klicken Sie unter **Azure** auf **Azure CIFS-Sperren für Azure HA-Systeme**.
5. Klicken Sie auf das Kontrollkästchen, um die Funktion zu aktivieren, und klicken Sie dann auf **Speichern**.

Verwenden Sie einen Azure Private Link oder Service-Endpunkte für Cloud Volumes ONTAP Systeme

Cloud Volumes ONTAP verwendet einen Azure Private Link für Verbindungen zu den zugehörigen Speicherkonten. Bei Bedarf können Sie Azure Private Links deaktivieren und stattdessen Dienstendpunkte verwenden.

Überblick

Standardmäßig aktiviert die NetApp Console einen Azure Private Link für Verbindungen zwischen Cloud Volumes ONTAP und den zugehörigen Speicherkonten. Ein Azure Private Link sichert Verbindungen zwischen Endpunkten in Azure und bietet Leistungsvorteile.

Bei Bedarf können Sie Cloud Volumes ONTAP so konfigurieren, dass anstelle eines Azure Private Link Dienstendpunkte verwendet werden.

Bei beiden Konfigurationen beschränkt die Konsole immer den Netzwerkzugriff für Verbindungen zwischen Cloud Volumes ONTAP und Speicherkonten. Der Netzwerkzugriff ist auf das VNet beschränkt, in dem Cloud Volumes ONTAP bereitgestellt wird, und das VNet, in dem der Konsolenagent bereitgestellt wird.

Deaktivieren Sie Azure Private Links und verwenden Sie stattdessen Dienstendpunkte

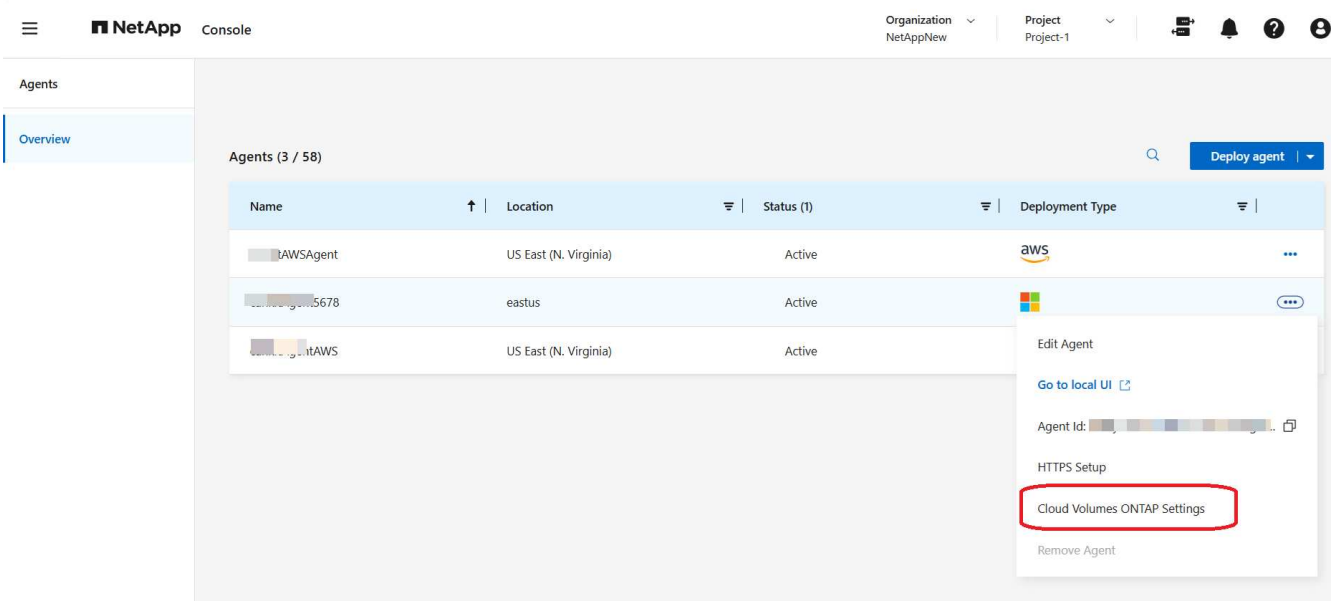
Falls Ihr Unternehmen dies erfordert, können Sie eine Einstellung in der Konsole ändern, sodass Cloud Volumes ONTAP so konfiguriert wird, dass Service-Endpunkte anstelle eines Azure Private Link verwendet werden. Das Ändern dieser Einstellung gilt für neue Cloud Volumes ONTAP -Systeme, die Sie erstellen. Service-Endpunkte werden nur unterstützt in"Azure-Regionspaare" zwischen dem Konsolenagenten und Cloud Volumes ONTAP VNets.

Der Konsolenagent sollte in derselben Azure-Region wie die von ihm verwalteten Cloud Volumes ONTAP -Systeme oder in der "Azure-Regionenpaar" für die Cloud Volumes ONTAP -Systeme.

Schritte

1. Gehen Sie im linken Navigationsbereich zu **Administration > Agenten**.

2. Klicken Sie auf das ••• Symbol für den Konsolenagenten, der Ihr Cloud Volumes ONTAP -System verwaltet.
3. Wählen Sie * Cloud Volumes ONTAP -Einstellungen*.



4. Klicken Sie unter **Azure** auf **Azure Private Link verwenden**.
5. Deaktivieren Sie **Private Link-Verbindung zwischen Cloud Volumes ONTAP und Speicherkonten**.
6. Klicken Sie auf **Speichern**.

Nach Abschluss

Wenn Sie Azure Private Links deaktiviert haben und der Konsolen-Agent einen Proxyserver verwendet, müssen Sie den direkten API-Verkehr aktivieren.

"Erfahren Sie, wie Sie den direkten API-Verkehr auf dem Konsolenagenten aktivieren"

Arbeiten mit Azure Private Links

In den meisten Fällen müssen Sie nichts tun, um Azure Private Links mit Cloud Volumes ONTAP einzurichten. Die Konsole verwaltet Azure Private Links für Sie. Wenn Sie jedoch eine vorhandene Azure Private DNS-Zone verwenden, müssen Sie eine Konfigurationsdatei bearbeiten.

Voraussetzung für benutzerdefiniertes DNS

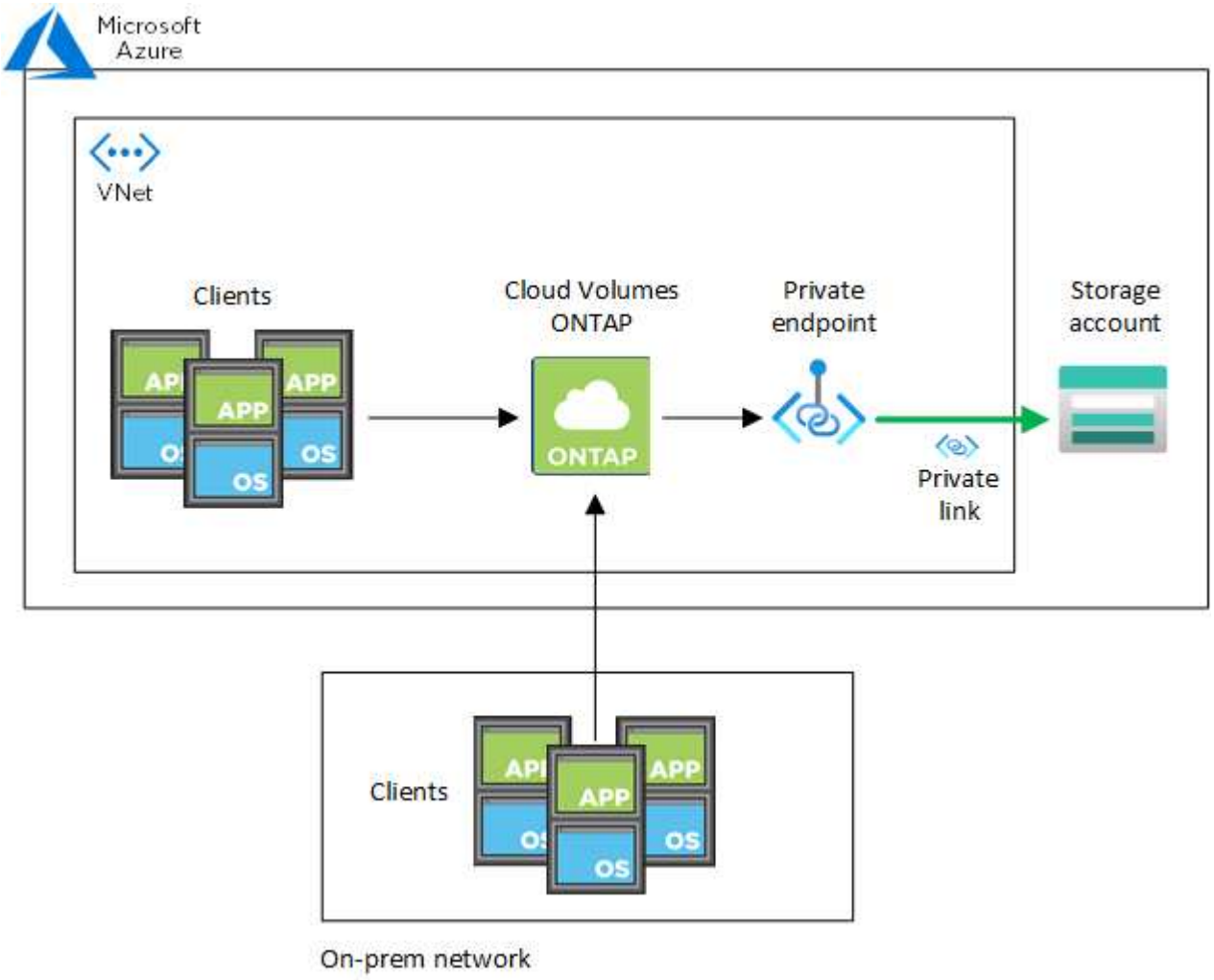
Wenn Sie mit benutzerdefiniertem DNS arbeiten, müssen Sie optional von Ihren benutzerdefinierten DNS-Servern eine bedingte Weiterleitung zur privaten Azure-DNS-Zone erstellen. Weitere Informationen finden Sie unter"Azure-Dokumentation zur Verwendung einer DNS-Weiterleitung" .

Funktionsweise von Private Link-Verbindungen

Wenn die Konsole Cloud Volumes ONTAP in Azure bereitstellt, erstellt sie einen privaten Endpunkt in der Ressourcengruppe. Der private Endpunkt ist mit Speicherkonten für Cloud Volumes ONTAP verknüpft. Daher erfolgt der Zugriff auf den Cloud Volumes ONTAP -Speicher über das Microsoft-Backbone-Netzwerk.

Der Clientzugriff erfolgt über die private Verbindung, wenn sich Clients im selben VNet wie Cloud Volumes ONTAP, in Peering-VNets oder in Ihrem lokalen Netzwerk befinden, wenn eine private VPN- oder ExpressRoute-Verbindung zum VNet verwendet wird.

Hier ist ein Beispiel, das den Clientzugriff über eine private Verbindung innerhalb desselben VNet und von einem lokalen Netzwerk aus zeigt, das entweder über eine private VPN- oder ExpressRoute-Verbindung verfügt.



Wenn der Konsolenagent und die Cloud Volumes ONTAP -Systeme in unterschiedlichen VNets bereitgestellt werden, müssen Sie VNet-Peering zwischen dem VNet einrichten, in dem der Konsolenagent bereitgestellt wird, und dem VNet, in dem die Cloud Volumes ONTAP -Systeme bereitgestellt werden.

Geben Sie Details zu Ihrem Azure Private DNS an

Wenn Sie "Privates Azure-DNS" , dann müssen Sie auf jedem Konsolenagenten eine Konfigurationsdatei ändern. Andernfalls kann die Konsole die Azure Private Link-Verbindung zwischen Cloud Volumes ONTAP und den zugehörigen Speicherkonten nicht herstellen.

Beachten Sie, dass der DNS-Name den Azure DNS-Benennungsanforderungen entsprechen muss. "wie in der Azure-Dokumentation gezeigt" .

Schritte

1. Stellen Sie per SSH eine Verbindung zum Konsolenagent-Host her und melden Sie sich an.
2. Navigieren Sie zum `/opt/application/netapp/cloudmanager/docker_occm/data` Verzeichnis.

3. Bearbeiten `app.conf` durch Hinzufügen der `user-private-dns-zone-settings` Parameter mit den folgenden Schlüsselwort-Wert-Paaren:

```
"user-private-dns-zone-settings" : {
   "resource-group" : "<resource group name of the DNS zone>",
   "subscription" : "<subscription ID>",
   "use-existing" : true,
   "create-private-dns-zone-link" : true
}
```

   Der `subscription` Das Schlüsselwort ist nur erforderlich, wenn sich die private DNS-Zone in einem anderen Abonnement befindet als das des Konsolenagenten.

4. Speichern Sie die Datei und melden Sie sich vom Konsolenagenten ab.

   Ein Neustart ist nicht erforderlich.

Rollback bei Fehlern aktivieren

Wenn die Konsole im Rahmen bestimmter Aktionen keinen Azure Private Link erstellen kann, führt sie die Aktion ohne die Azure Private Link-Verbindung aus. Dies kann beim Erstellen eines neuen Systems (einzelner Knoten oder HA-Paar) passieren oder wenn die folgenden Aktionen auf einem HA-Paar stattfinden: Erstellen eines neuen Aggregats, Hinzufügen von Datenträgern zu einem vorhandenen Aggregat oder Erstellen eines neuen Speicherkontos beim Überschreiten von 32 TiB.

Sie können dieses Standardverhalten ändern, indem Sie das Rollback aktivieren, wenn die Konsole den Azure Private Link nicht erstellen kann. Auf diese Weise können Sie sicherstellen, dass Sie die Sicherheitsvorschriften Ihres Unternehmens vollständig einhalten.

Wenn Sie das Rollback aktivieren, stoppt die Konsole die Aktion und führt ein Rollback aller Ressourcen durch, die im Rahmen der Aktion erstellt wurden.

Sie können das Rollback über die API oder durch Aktualisieren der Datei app.conf aktivieren.

Rollback über die API aktivieren

Schritt

1. Verwenden Sie die `PUT /occm/config` API-Aufruf mit folgendem Anforderungstext:

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

Rollback durch Aktualisieren von app.conf aktivieren

Schritte

1. Stellen Sie per SSH eine Verbindung zum Host des Konsolenagenten her und melden Sie sich an.
2. Navigieren Sie zum folgenden Verzeichnis: /opt/application/netapp/cloudmanager/docker_occm/data
3. Bearbeiten Sie app.conf, indem Sie den folgenden Parameter und Wert hinzufügen:

```
 "rollback-on-private-link-failure": true
. Speichern Sie die Datei und melden Sie sich vom Konsolenagenten ab.
```

Ein Neustart ist nicht erforderlich.

Verschieben einer Azure-Ressourcengruppe für Cloud Volumes ONTAP in der Azure-Konsole

Cloud Volumes ONTAP unterstützt das Verschieben von Azure-Ressourcengruppen, der Workflow erfolgt jedoch nur in der Azure-Konsole.

Sie können ein Cloud Volumes ONTAP -System innerhalb desselben Azure-Abonnements von einer Ressourcengruppe in eine andere Ressourcengruppe in Azure verschieben. Das Verschieben von Ressourcengruppen zwischen verschiedenen Azure-Abonnements wird nicht unterstützt.

Schritte

1. Entfernen Sie das Cloud Volumes ONTAP -System. Weitere Informationen finden Sie unter "Entfernen von Cloud Volumes ONTAP -Systemen" .
2. Führen Sie die Ressourcengruppenverschiebung in der Azure-Konsole aus.

   Um den Umzug abzuschließen, lesen Sie"Verschieben von Ressourcen in eine neue Ressourcengruppe oder ein neues Abonnement in der Dokumentation von Microsoft Azure" .
3. Suchen Sie auf der Seite **Systeme** nach dem System.
4. Suchen Sie in den Informationen zum System nach der neuen Ressourcengruppe.

Ergebnis

Das System und seine Ressourcen (VMs, Datenträger, Speicherkonten, Netzwerkschnittstellen, Snapshots) befinden sich in der neuen Ressourcengruppe.

Trennen Sie den SnapMirror -Datenverkehr in Azure

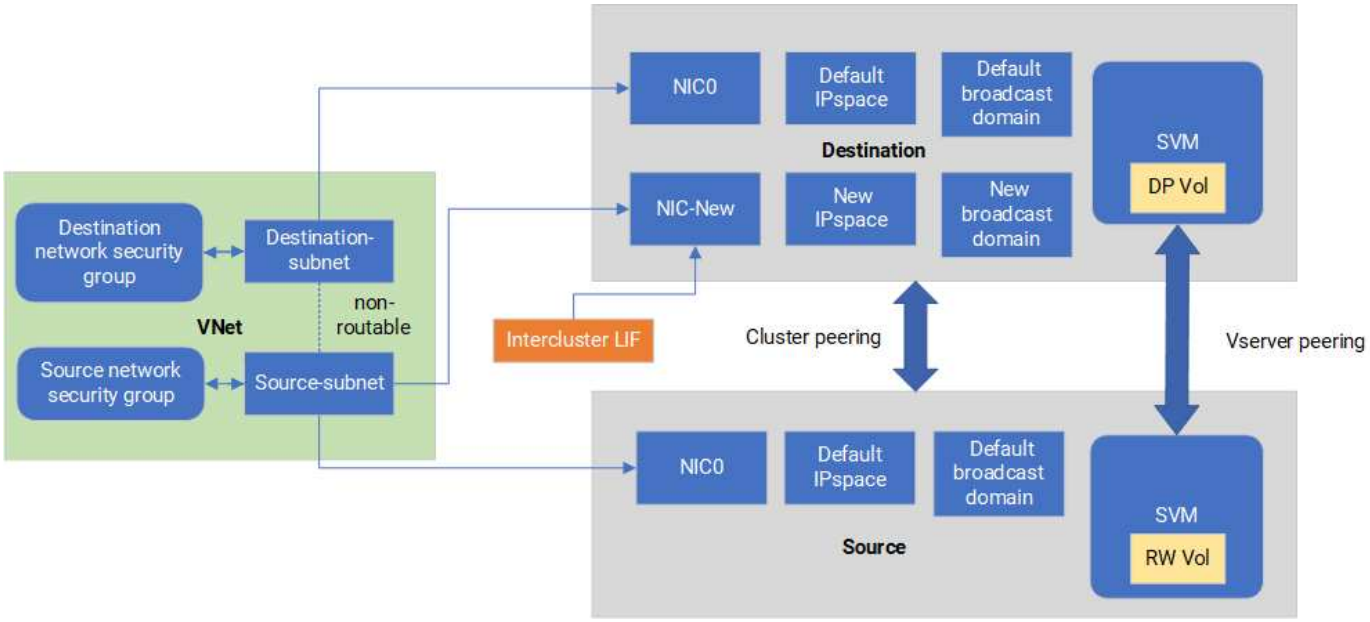
Mit Cloud Volumes ONTAP in Azure können Sie den SnapMirror Replikationsdatenverkehr vom Daten- und Verwaltungsdatenverkehr trennen. Um den SnapMirror -Replikationsverkehr von Ihrem Datenverkehr zu trennen, fügen Sie eine neue Netzwerkschnittstellenkarte (NIC), ein zugehöriges Intercluster-LIF und ein nicht routbares Subnetz hinzu.

Informationen zur SnapMirror -Verkehrstrennung in Azure

Standardmäßig konfiguriert die NetApp Console alle NICs und LIFs in einer Cloud Volumes ONTAP Bereitstellung im selben Subnetz. In solchen Konfigurationen verwenden der SnapMirror Replikationsverkehr sowie der Daten- und Verwaltungsverkehr dasselbe Subnetz. Durch die Trennung des SnapMirror -Verkehrs wird ein zusätzliches Subnetz genutzt, das nicht an das vorhandene Subnetz weitergeleitet werden kann, das für den Daten- und Verwaltungsverkehr verwendet wird.

Abbildung 1

Die folgenden Diagramme zeigen die Trennung des SnapMirror -Replikationsdatenverkehrs mit einer zusätzlichen Netzwerkkarte, einem zugehörigen Intercluster-LIF und einem nicht routingfähigen Subnetz in einer Einzelknotenbereitstellung. Eine HA-Paarbereitstellung unterscheidet sich geringfügig.



Bevor Sie beginnen

Beachten Sie die folgenden Überlegungen:

- Sie können einem Cloud Volumes ONTAP Einzelknoten oder einer HA-Paar-Bereitstellung (VM-Instanz) zur SnapMirror Verkehrstrennung nur eine einzelne Netzwerkkarte hinzufügen.
- Um eine neue Netzwerkkarte hinzuzufügen, muss der von Ihnen bereitgestellte VM-Instanztyp über eine ungenutzte Netzwerkkarte verfügen.
- Die Quell- und Zielcluster sollten Zugriff auf dasselbe virtuelle Netzwerk (VNet) haben. Der Zielcluster ist ein Cloud Volumes ONTAP -System in Azure. Der Quellcluster kann ein Cloud Volumes ONTAP -System in Azure oder ein ONTAP System sein.

Schritt 1: Erstellen Sie eine zusätzliche Netzwerkkarte und verbinden Sie sie mit der Ziel-VM

Dieser Abschnitt enthält Anweisungen zum Erstellen einer zusätzlichen Netzwerkkarte und zum Anschließen an die Ziel-VM. Die Ziel-VM ist das Einzelknoten- oder HA-Paarsystem in Cloud Volumes ONTAP in Azure, in dem Sie Ihre zusätzliche Netzwerkkarte einrichten möchten.

Schritte

1. Stoppen Sie den Knoten in der ONTAP CLI.

```
dest::> halt -node <dest_node-vm>
```

2. Überprüfen Sie im Azure-Portal, ob der Status der VM (Knoten) „Beendet“ lautet.

```
az vm get-instance-view --resource-group <dest-rg> --name <dest-vm>
--query instanceView.statuses[1].displayStatus
```

3. Verwenden Sie die Bash-Umgebung in Azure Cloud Shell, um den Knoten zu stoppen.
   a. Stoppen Sie den Knoten.

```
az vm stop --resource-group <dest_node-rg> --name <dest_node-vm>
```

b. Heben Sie die Zuordnung des Knotens auf.

```
az vm deallocate --resource-group <dest_node-rg> --name <dest_node-vm>
```

4. Konfigurieren Sie Netzwerksicherheitsgruppenregeln, um die beiden Subnetze (Quellcluster-Subnetz und Zielcluster-Subnetz) untereinander nicht routbar zu machen.
   a. Erstellen Sie die neue Netzwerkkarte auf der Ziel-VM.
   b. Suchen Sie die Subnetz-ID für das Subnetz des Quellclusters.

```
az network vnet subnet show -g <src_vnet-rg> -n <src_subnet> --vnet -name <vnet> --query id
```

   c. Erstellen Sie die neue Netzwerkkarte auf der Ziel-VM mit der Subnetz-ID für das Subnetz des Quellclusters. Hier geben Sie den Namen für die neue Netzwerkkarte ein.

```
az network nic create -g <dest_node-rg> -n <dest_node-vm-nic-new> --subnet <id_from_prev_command> --accelerated-networking true
```

   d. Speichern Sie die private IP-Adresse. Diese IP-Adresse, <new_added_nic_primary_addr>, wird verwendet, um ein Intercluster-LIF inBroadcast-Domäne, Intercluster-LIF für die neue NIC .
5. Schließen Sie die neue Netzwerkkarte an die VM an.

```
az vm nic add -g <dest_node-rg> --vm-name <dest_node-vm> --nics <dest_node-vm-nic-new>
```

6. Starten Sie die VM (den Knoten).

```
az vm start --resource-group <dest_node-rg>  --name <dest_node-vm>
```

7. Gehen Sie im Azure-Portal zu **Netzwerk** und bestätigen Sie, dass die neue Netzwerkkarte, z. B. nic-new, vorhanden ist und der beschleunigte Netzwerkbetrieb aktiviert ist.

```
az network nic list --resource-group azure-59806175-60147103-azure-rg --query "[].{NIC: name, VM: virtualMachine.id}"
```

Wiederholen Sie bei HA-Paar-Bereitstellungen die Schritte für den Partnerknoten.

Schritt 2: Erstellen Sie einen neuen IPspace, eine neue Broadcast-Domäne und ein Intercluster-LIF für die neue Netzwerkkarte

Ein separater IP-Bereich für LIFs zwischen Clustern bietet eine logische Trennung zwischen Netzwerkfunktionen für die Replikation zwischen Clustern.

Verwenden Sie für die folgenden Schritte die ONTAP CLI.

Schritte

1. Erstellen Sie den neuen IPspace (new_ipspace).

```
dest::> network ipspace create -ipspace <new_ipspace>
```

2. Erstellen Sie eine Broadcast-Domäne im neuen IPspace (new_ipspace) und fügen Sie den nic-new-Port hinzu.

```
dest::> network port show
```

3. Bei Einzelknotensystemen ist der neu hinzugefügte Port *e0b*. Bei HA-Paar-Bereitstellungen mit verwalteten Datenträgern ist der neu hinzugefügte Port *e0d*. Bei HA-Paar-Bereitstellungen mit Seitenblobs ist der neu hinzugefügte Port *e0e*. Verwenden Sie den Node-Name, nicht den VM-Name. Finden Sie den Node-Name, indem Sie `node show` ausführen.

```
dest::> broadcast-domain create -broadcast-domain <new_bd> -mtu 1500
-ipspace <new_ipspace> -ports <dest_node-cot-vm:e0b>
```

4. Erstellen Sie ein Intercluster-LIF auf der neuen Broadcast-Domäne (new_bd) und auf der neuen NIC (nic-new).

```
dest::> net int create -vserver <new_ipspace> -lif <new_dest_node-ic-
lif> -service-policy default-intercluster -address
<new_added_nic_primary_addr> -home-port <e0b> -home-node <node> -netmask
<new_netmask_ip> -broadcast-domain <new_bd>
```

5. Überprüfen Sie die Erstellung des neuen Intercluster-LIF.

```
dest::> net int show
```

Wiederholen Sie bei HA-Paar-Bereitstellungen die Schritte für den Partnerknoten.

Schritt 3: Überprüfen des Cluster-Peerings zwischen Quell- und Zielsystemen

Dieser Abschnitt enthält Anweisungen zum Überprüfen des Peerings zwischen den Quell- und Zielsystemen.

Verwenden Sie für die folgenden Schritte die ONTAP CLI.

Schritte

1. Überprüfen Sie, ob das Intercluster-LIF des Zielclusters das Intercluster-LIF des Quellclusters anpingen kann. Da der Zielcluster diesen Befehl ausführt, ist die Ziel-IP-Adresse die LIF-IP-Adresse zwischen den Clustern auf der Quelle.

```
dest::> ping -lif <new_dest_node-ic-lif> -vserver <new_ipspace>
-destination <10.161.189.6>
```

2. Überprüfen Sie, ob das Intercluster-LIF des Quellclusters das Intercluster-LIF des Zielclusters anpingen kann. Das Ziel ist die IP-Adresse der neuen Netzwerkkarte, die am Ziel erstellt wurde.

```
src::> ping -lif <src_node-ic-lif> -vserver <src_svm> -destination
<10.161.189.18>
```

Wiederholen Sie bei HA-Paar-Bereitstellungen die Schritte für den Partnerknoten.

Schritt 4: SVM-Peering zwischen Quell- und Zielsystem erstellen

Dieser Abschnitt enthält Anweisungen zum Erstellen eines SVM-Peerings zwischen dem Quell- und dem Zielsystem.

Verwenden Sie für die folgenden Schritte die ONTAP CLI.

Schritte

1. Erstellen Sie Cluster-Peering auf dem Ziel unter Verwendung der Quell-Intercluster-LIF-IP-Adresse als `-peer-addrs` . Listen Sie für HA-Paare die Quell-Intercluster-LIF-IP-Adresse für beide Knoten als `-peer -addrs` .

```
dest::> cluster peer create -peer-addrs <10.161.189.6> -ipspace
<new_ipspace>
```

2. Geben Sie die Passphrase ein und bestätigen Sie sie.
3. Erstellen Sie Cluster-Peering auf der Quelle unter Verwendung der LIF-IP-Adresse des Zielclusters als `peer-addrs` . Listen Sie für HA-Paare die Ziel-Intercluster-LIF-IP-Adresse für beide Knoten als `-peer -addrs` .

```
src::> cluster peer create -peer-addrs <10.161.189.18>
```

4. Geben Sie die Passphrase ein und bestätigen Sie sie.
5. Überprüfen Sie, ob der Cluster gepeert wurde.

```
src::> cluster peer show
```

Bei erfolgreichem Peering wird im Verfügbarkeitsfeld **Verfügbar** angezeigt.

6. Erstellen Sie SVM-Peering auf dem Ziel. Sowohl Quell- als auch Ziel-SVMs sollten Daten-SVMs sein.

```
dest::> vserver peer create -vserver <dest_svm> -peer-vserver <src_svm>
-peer-cluster <src_cluster> -applications snapmirror``
```

7. Akzeptieren Sie SVM-Peering.

```
src::> vserver peer accept -vserver <src_svm> -peer-vserver <dest_svm>
```

8. Überprüfen Sie, ob die SVM gepeert wurde.

```
dest::> vserver peer show
```

Peer-Status zeigt*`peered` * und Peering-Anwendungen zeigt*`snapmirror` *.

Schritt 5: Erstellen Sie eine SnapMirror -Replikationsbeziehung zwischen dem Quell- und Zielsystem

Dieser Abschnitt enthält Anweisungen zum Erstellen einer SnapMirror -Replikationsbeziehung zwischen dem Quell- und dem Zielsystem.

Um eine vorhandene SnapMirror -Replikationsbeziehung zu verschieben, müssen Sie zuerst die vorhandene SnapMirror -Replikationsbeziehung auflösen, bevor Sie eine neue SnapMirror -Replikationsbeziehung erstellen.

Verwenden Sie für die folgenden Schritte die ONTAP CLI.

Schritte

1. Erstellen Sie ein datengeschütztes Volume auf der Ziel-SVM.

```
dest::> vol create -volume <new_dest_vol> -vserver <dest_svm> -type DP
-size <10GB> -aggregate <aggr1>
```

2. Erstellen Sie die SnapMirror Replikationsbeziehung auf dem Ziel, die die SnapMirror -Richtlinie und den Zeitplan für die Replikation enthält.

```
dest::> snapmirror create -source-path src_svm:src_vol  -destination
-path  dest_svm:new_dest_vol -vserver dest_svm -policy
MirrorAllSnapshots -schedule 5min
```

3. Initialisieren Sie die SnapMirror Replikationsbeziehung auf dem Ziel.

```
dest::> snapmirror initialize -destination-path  <dest_svm:new_dest_vol>
```

4. Überprüfen Sie in der ONTAP CLI den SnapMirror Beziehungsstatus, indem Sie den folgenden Befehl ausführen:

```
dest::> snapmirror show
```

   Der Beziehungsstatus ist `Snapmirrored` und die Gesundheit der Beziehung ist `true` .

5. Optional: Führen Sie in der ONTAP CLI den folgenden Befehl aus, um den Aktionsverlauf für die SnapMirror -Beziehung anzuzeigen.

```
dest::> snapmirror show-history
```

Optional können Sie die Quell- und Zielvolumes mounten, eine Datei auf die Quelle schreiben und überprüfen, ob das Volume auf das Ziel repliziert wird.

Google Cloud-Verwaltung

Ändern Sie den Google Cloud-Maschinentyp für Cloud Volumes ONTAP

Sie können aus mehreren Maschinentypen wählen, wenn Sie Cloud Volumes ONTAP in Google Cloud starten. Sie können die Instanz oder den Maschinentyp jederzeit ändern, wenn Sie feststellen, dass er für Ihre Anforderungen zu klein oder zu groß ist.

Informationen zu diesem Vorgang

- Die automatische Rückgabe muss für ein Cloud Volumes ONTAP HA-Paar aktiviert sein (dies ist die Standardeinstellung). Wenn dies nicht der Fall ist, schlägt der Vorgang fehl.

  "ONTAP 9-Dokumentation: Befehle zum Konfigurieren der automatischen Rückgabe"

- Das Ändern des Maschinentyps kann sich auf die Servicegebühren von Google Cloud auswirken.
- Der Vorgang startet Cloud Volumes ONTAP.

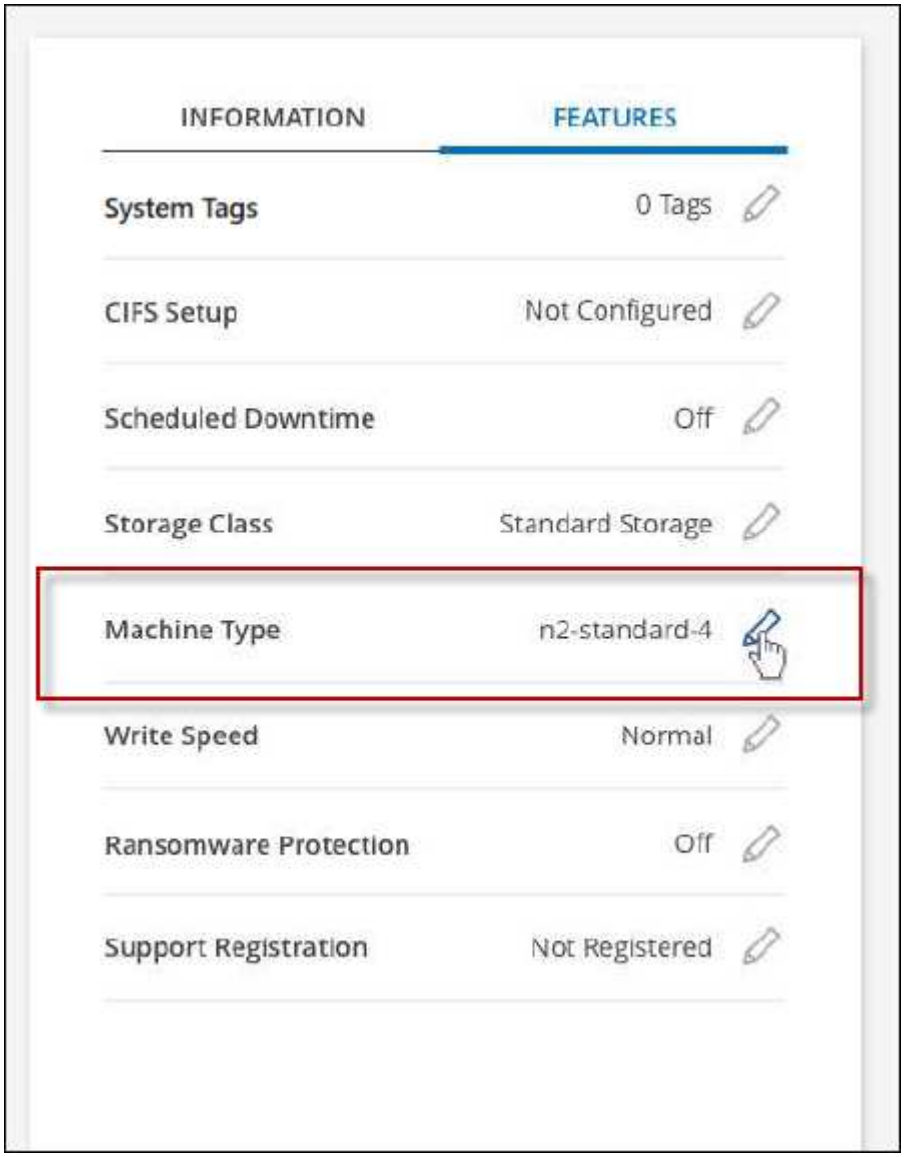
  Bei Single-Node-Systemen wird die I/O unterbrochen.

  Bei HA-Paaren erfolgt die Änderung ohne Unterbrechung. HA-Paare stellen weiterhin Daten bereit.

> Die NetApp Console ändert jeweils einen Knoten, indem sie die Übernahme einleitet und auf die Rückgabe wartet. Das Qualitätssicherungsteam von NetApp hat während dieses Vorgangs sowohl das Schreiben als auch das Lesen von Dateien getestet und konnte auf der Clientseite keine Probleme feststellen. Beim Ändern der Verbindungen wurden auf der E/A-Ebene einige Wiederholungsversuche beobachtet, die Anwendungsschicht konnte die Neuverdrahtung der NFS/CIFS-Verbindungen jedoch bewältigen.

Schritte

1. Wählen Sie auf der Seite **Systeme** das System aus.
2. Klicken Sie auf der Registerkarte „Übersicht“ auf den Bereich „Funktionen“ und dann auf das Stiftsymbol neben „Maschinentyp“.



Wenn Sie eine knotenbasierte Pay-as-you-go-Lizenz (PAYGO) verwenden, können Sie optional eine andere Lizenz und einen anderen Maschinentyp auswählen, indem Sie auf das Stiftsymbol neben **Lizenztyp** klicken.

1. Wählen Sie einen Maschinentyp aus, aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Auswirkungen der Änderung verstehen, und klicken Sie dann auf **Ändern**.

Ergebnis

Cloud Volumes ONTAP wird mit der neuen Konfiguration neu gestartet.

Konvertieren Sie bestehende Cloud Volumes ONTAP-Bereitstellungen in Infrastructure Manager

Ab dem 9. Februar 2026 können neue Cloud Volumes ONTAP-Bereitstellungen in Google Cloud den Google Cloud Infrastructure Manager nutzen. Google wird den Google Cloud Deployment Manager zugunsten des Infrastructure Manager einstellen. Daher müssen

Sie ein Übergangstool manuell ausführen, um Ihre bestehenden Cloud Volumes ONTAP-Bereitstellungen vom Deployment Manager auf den Infrastructure Manager umzustellen. Dies ist ein einmaliger Vorgang, nach dem Ihre Systeme automatisch den Infrastructure Manager verwenden.

Informationen zu diesem Vorgang

Das Übergangstool ist in der "NetApp Support-Website" verfügbar und erstellt die folgenden Artefakte:

- Terraform-Artefakte, gespeichert in `conversion_output/deployment_name`.
- Zusammenfassung der Konvertierung, gespeichert in `conversion_output/batch_summary_<deployment_name>_<timestamp>.json`.
- Debug-Protokolle, gespeichert im `<gcp project number>-<region>-blueprint-config/<cvo name>` Verzeichnis. Sie benötigen diese Protokolle zur Fehlerbehebung. Der `<gcp project number>-<region>-blueprint-config` Bucket speichert die Terraform-Protokolle.

> Cloud Volumes ONTAP-Systeme, die Infrastructure Manager verwenden, speichern Daten und Datensätze in Google Cloud Storage-Buckets. Für diese Buckets können zusätzliche Kosten anfallen, aber bearbeiten oder löschen Sie die Buckets oder deren Inhalt nicht:
>
> - `gs://netapp-cvo-infrastructure-manager-<project id>`: für ONTAP Versionen und SVM Terraform Templates, die für neue Cloud Volumes ONTAP Deployments verwendet werden. Innerhalb davon enthält der `dm-to-im-convert` bucket die Cloud Volumes ONTAP Terraform Dateien.
> - `<gcp project number>-<region>-blueprint-config`: zum Speichern von Google Cloud Terraform-Artefakten.

Bevor Sie beginnen

- Stellen Sie sicher, dass Ihr Cloud Volumes ONTAP System 9.16.1 oder höher ist.
- Stellen Sie sicher, dass keine der Cloud Volumes ONTAP Ressourcen oder deren Eigenschaften manuell über die Google Cloud Console bearbeitet wurden.
- Stellen Sie sicher, dass die Google Cloud APIs aktiviert sind. Siehe "Google Cloud APIs aktivieren". Stellen Sie sicher, dass Sie neben den anderen APIs auch die Google Cloud Quotas API aktivieren.
- Stellen Sie sicher, dass das Dienstkonto des NetApp Console-Agenten über alle erforderlichen Berechtigungen verfügt. Siehe "Google Cloud-Berechtigungen für den Konsolenagenten".

  Für Bereitstellungen im privaten Modus stellen Sie sicher, dass diese zusätzlichen Voraussetzungen erfüllt sind:

  - Stellen Sie sicher, dass Sie die neueste Version des Console-Agenten verwenden. Laden Sie das Produktinstallationsprogramm von der NetApp Support Site herunter und installieren Sie den Agenten anschließend manuell auf Ihrem Host, damit der Agent die Infrastructure Manager APIs nutzen kann.
  - Wenn Sie das Tool im privaten Modus ausführen, stellen Sie sicher, dass Sie neben den anderen APIs auch die Cloud Build API aktiviert haben. "Google Cloud APIs aktivieren".
  - Stellen Sie sicher, dass Sie die Netzwerkkonfigurationen abgeschlossen und den Worker-Pool für private Bereitstellungen erstellt haben. Siehe "Infrastructure Manager-Konfiguration für private Modus-Bereitstellungen".

- Das Konvertierungstool verwendet die folgenden Domänen. Aktivieren Sie diese auf Port 443 in Ihrem Netzwerk:

Domäne	Hafen	Protokoll	Richtung	Zweck
cloudresourcemanager.googleapis.com	443	TCP	EGRESS	Projektvalidierung
deploymentmanager.googleapis.com	443	TCP	EGRESS	Bereitstellungserkennung
config.googleapis.com	443	TCP	EGRESS	Infrastructure Manager API
storage.googleapis.com	443	TCP	EGRESS	GCS bucket-Operationen
iam.googleapis.com	443	TCP	EGRESS	Validierung des Dienstkontos
compute.googleapis.com	443	TCP	EGRESS	Compute API-Aufrufe, die von Google Cloud und Terraform Import und Plan verwendet werden
cloudbuild.googleapis.com	443	TCP	EGRESS	Build-Operationen sind nur im privaten Modus erforderlich
openidconnect.googleapis.com	443	TCP	EGRESS	Authentifizierung
oauth2.googleapis.com	443	TCP	EGRESS	OAuth2-Token-Austausch
registry.terraform.io	443	TCP	EGRESS	Terraform Provider-Registry
releases.hashicorp.com	443	TCP	EGRESS	Terraform-Binärdateien herunterladen
apt.releases.hashicorp.com	443	TCP	EGRESS	HashiCorp APT-Repository
us-central1-docker.pkg.dev	443	TCP	EGRESS	GCP Artifact Registry
metadata.google.internal	80	HTTP	Intern	VM-Metadaten & Authentifizierungstoken
pypi.org	443	TCP	EGRESS	Python Package Index
files.pythonhosted.org	443	TCP	EGRESS	Python-Paket-Downloads
checkpoint-api.hashicorp.com	443	TCP	EGRESS	Terraform-Versionsprüfung

Domäne	Hafen	Protokoll	Richtung	Zweck
download.docker.com	443	TCP	EGRESS	Docker APT-Repository
security.ubuntu.com	80/443	TCP	EGRESS	Ubuntu-Sicherheitsupdates
*.gce.archive.ubuntu.com	80	TCP	EGRESS	Ubuntu-Paketspiegel

Bereiten Sie die Umgebung für die Ausführung des Tools vor

Führen Sie diese Schritte aus, bevor Sie das Tool ausführen.

Schritte

1. Erstellen Sie eine Rolle und hängen Sie sie an ein Dienstkonto an:
   a. Erstellen Sie eine YAML-Datei mit den folgenden Berechtigungen:

```
title: NetApp Dm TO IM Convert Solution
description: Permissions for the service account associated with the
VM where the tool will run.
stage: GA
includedPermissions:
- compute.addresses.get
- compute.disks.get
- compute.forwardingRules.get
- compute.healthChecks.get
- compute.instanceGroups.get
- compute.instances.get
- compute.regionBackendServices.get
- config.deployments.create
- config.deployments.get
- config.deployments.getLock
- config.deployments.lock
- config.deployments.unlock
- config.deployments.update
- config.deployments.delete
- config.deployments.updateState
- config.operations.get
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- iam.serviceAccounts.get
- storage.buckets.create
- storage.objects.create
- storage.objects.delete
- storage.objects.get
- storage.objects.list
```

Zusätzliche Berechtigung für Bereitstellungen im privaten Modus einschließen

Wenn Sie das Tool im privaten Modus ausführen, fügen Sie die `cloudbuild.workerpools.get` Berechtigung auch zur YAML-Datei hinzu.

b. Erstellen Sie eine benutzerdefinierte Rolle in Google Cloud mit den in der YAML-Datei definierten Berechtigungen.
`gcloud iam roles create dmtoim_convert_tool_role --project=PROJECT_ID \ --file=YAML_FILE_PATH` Weitere Informationen finden Sie unter "Erstellen und Verwalten benutzerdefinierter Rollen".

c. Weisen Sie die benutzerdefinierte Rolle dem Dienstkonto zu, das Sie zum Erstellen der VM verwenden.

d. Fügen Sie die `roles/iam.serviceAccountUser` Rolle zu diesem Dienstkonto hinzu. Siehe "Übersicht der Servicekonten".

2. Erstellen Sie eine VM mit den folgenden Konfigurationen. Sie führen das Tool auf dieser VM aus.
   - Maschinentyp: Google Compute Engine machine type e2-medium
   - Betriebssystem: Wählen Sie je nach Ihren Anforderungen eines dieser Images aus:
     - Ubuntu 25.10 AMD64 Minimal (Image: ubuntu-minimal-2510-amd64)
     - SUSE Linux Enterprise Server 15 SP7 x86_64
   - Netzwerk: Firewall, die HTTP und HTTPs zulässt
   - Festplattengröße: 20GB
   - Sicherheit: Dienstkonten: das von Ihnen erstellte Servicekonto
   - Sicherheit: Zugriffsbereich - Zugriffssatz für jede API:
     - Cloud Platform: Aktiviert
     - Compute Engine: Nur lesen
     - Speicher: Nur lesen (Standard)
     - Google Cloud Logging (ehemals Stackdriver Logging) API: Write only (default)
     - Stackdriver Monitoring (jetzt Teil von Google Cloud Operations) API: Nur Schreiben (default)
     - Service Management: Schreibgeschützt (Standard)
     - Service Control: Aktiviert (Standard)
     - Google Cloud Trace (ehemals Stackdriver Trace): Nur Schreiben (Standard)
3. Stellen Sie über SSH eine Verbindung zur neu erstellten VM her: `gcloud compute ssh dmtoim-convert-executor-vm --zone <region where VM is deployed>`
4. Laden Sie das Konvertierungstool von der "NetApp Support-Website" mit Ihren NSS-Zugangsdaten herunter: `wget <download link from NetApp Support site>`
5. Entpacken Sie die heruntergeladene TAR-Datei: `unzip <downloaded file name>`

Ubuntu

1. Laden Sie diese erforderlichen Pakete herunter und installieren Sie sie:
   - Docker: 28.2.2 build 28.2.2-0ubuntu1 oder höher
   - Terraform: 1.14.1 oder höher
   - Python: 3.13.7, python3-pip, python3 venv

   ```
   sudo apt-get update
   sudo apt-get install python3-pip python3-venv -y
   wget -O - https://apt.releases.hashicorp.com/gpg | sudo gpg
   --dearmor -o /usr/share/keyrings/hashicorp-archive-keyring.gpg
   echo "deb [arch=$(dpkg --print-architecture) signed-
   by=/usr/share/keyrings/hashicorp-archive-keyring.gpg]
   https://apt.releases.hashicorp.com noble main" | sudo tee
   /etc/apt/sources.list.d/hashicorp.list
   sudo apt update && sudo apt install terraform
   sudo apt-get install -y docker.io
   sudo systemctl start docker
   ```

   Google Cloud CLI `gcloud` ist auf der VM vorinstalliert.

SUSE Linux Enterprise Server

1. Python einrichten: `sudo update-alternatives --install /usr/bin/python3 python3 /usr/bin/python3.11 2`
2. Installieren Sie pip3, um das Paket zu installieren: `python3.11 -m ensurepip --upgrade`
3. Terraform installieren:

   ```
   wget
   https://releases.hashicorp.com/terraform/1.7.4/terraform_1.7.4_linux
   _amd64.zip
   unzip terraform_1.7.4_linux_amd64.zip
   sudo mv terraform /usr/local/bin/
   rm terraform_1.7.4_linux_amd64.zip
   ```

4. Installieren Sie das Google Cloud SDK (gcloud)

   ```
   curl https://sdk.cloud.google.com | bash
   exec -l $SHELL
   ```

Führen Sie das Konvertierungstool aus

Diese Schritte gelten sowohl für Ubuntu als auch für SUSE Linux Enterprise Server zum Ausführen des Konvertierungstools.

Schritte

1. Fügen Sie den aktuellen Benutzer der Docker-Gruppe hinzu, damit das Tool Docker ohne `sudo` Privilegien verwenden kann.

```
sudo usermod -aG docker $USER
newgrp docker
```

2. Installieren Sie das Konvertierungstool:

```
cd <folder where you extracted the tool>
 ./install.sh
```

   Dadurch wird das Tool in einer isolierten Umgebung installiert, `dmconvert-venv` und es wird überprüft, ob alle erforderlichen Softwarepakete installiert sind.

3. Geben Sie die Umgebung ein, in der das Tool installiert ist: `source dmconvert-venv/bin/activate`
4. Führen Sie das Konvertierungstool als `non-sudo` Benutzer aus. Stellen Sie sicher, dass Sie dasselbe Dienstkonto wie das Dienstkonto des Console-Agenten verwenden und dass das Dienstkonto alle "Erforderliche Berechtigungen für Google Cloud Infrastructure Manager" besitzt.

```
dmconvert \
--project-id=<the Google Cloud project ID for the Cloud Volumes ONTAP
deployment> \
--cvo-name=<Cloud Volumes ONTAP system name> \
--service-account=<the service account attached to the Console agent>
```

Führen Sie das Tool im privaten Modus für Bereitstellungen aus

Geben Sie den `--worker-pool` Parameter an, um das Tool in privaten Bereitstellungsmodi auszuführen. Weitere Informationen zur Konfiguration des Worker-Pools finden Sie unter "Infrastructure Manager-Konfiguration für private Modus-Bereitstellungen".

```
dmconvert \
--project-id=<the Google Cloud project ID for the Cloud Volumes
ONTAP deployment> \
--cvo-name=<Cloud Volumes ONTAP system name> \
--service-account=<the service account attached to the Console
agent> \
--worker-pool=<worker pool name>
```

Nach Abschluss

Das Tool zeigt eine Liste aller Cloud Volumes ONTAP-Systeme und SVM-Details an. Wenn der Vorgang abgeschlossen ist, können Sie die Status aller konvertierten Systeme sehen. Jedes konvertierte System erscheint in der Google Console unter Infrastructure Manager im *<system-name-imdeploy>* Format, was darauf hinweist, dass die Console nun die Infrastructure Manager APIs zur Verwaltung dieses Cloud Volumes ONTAP-Systems verwendet.

Nach der Konvertierung darf das Bereitstellungsobjekt für Deployment Manager in der Google Cloud Console nicht gelöscht werden. Dieses Bereitstellungsobjekt enthält Informationen, die Sie möglicherweise benötigen, um das konvertierte System zurückzusetzen.

Wenn Sie die Konvertierung rückgängig machen müssen, müssen Sie dieselbe VM verwenden. Wenn Sie alle Systeme konvertiert haben und nicht zum Deployment Manager zurückkehren müssen, können Sie die VM löschen.

Die Konvertierung rückgängig machen

Wenn Sie die Konvertierung nicht fortsetzen möchten, können Sie zum Deployment Manager zurückkehren, indem Sie die folgenden Schritte ausführen:

Schritte

1. Führen Sie auf demselben VM, die Sie zum Ausführen des Tools erstellt haben folgenden Befehl aus:

```
dmconvert \
--project-id=<the Google Cloud project ID for the Cloud Volumes ONTAP
deployment> \
--cvo-name=<Cloud Volumes ONTAP system name> \
--service-account=<the service account attached to the Console agent> \
--rollback
```

2. Warten Sie, bis der Rollback abgeschlossen ist.

Weiterführende Links

- "NetApp Console Agent 4.2.0 Versionshinweise"
- "Erforderliche Berechtigungen für Google Cloud Infrastructure Manager"

Verwalten Sie Cloud Volumes ONTAP mit System Manager

Erweiterte Speicherverwaltungsfunktionen in Cloud Volumes ONTAP stehen über den ONTAP System Manager zur Verfügung, eine Verwaltungsoberfläche, die mit ONTAP -Systemen bereitgestellt wird. Sie können direkt von der NetApp Console auf den System Manager zugreifen.

Features

Sie können mit ONTAP System Manager in der Konsole verschiedene Speicherverwaltungsfunktionen ausführen. Die folgende Liste enthält einige dieser Funktionen (ohne Anspruch auf Vollständigkeit):

- Erweiterte Speicherverwaltung: Verwalten Sie Konsistenzgruppen, Freigaben, Qtrees, Kontingente und Speicher-VMs.
- Volumenverschiebung: "Verschieben Sie ein Volume in ein anderes Aggregat."
- Netzwerkverwaltung: Verwalten Sie IP-Bereiche, Netzwerkschnittstellen, Portsets und Ethernet-Ports.
- FlexGroup -Volumes verwalten: Sie können FlexGroup Volumes nur über den System Manager erstellen und verwalten. Die Konsole unterstützt die Erstellung von FlexGroup Volumes nicht.
- Ereignisse und Jobs: Zeigen Sie Ereignisprotokolle, Systemwarnungen, Jobs und Prüfprotokolle an.
- Erweiterter Datenschutz: Schützen Sie Speicher-VMs, LUNs und Konsistenzgruppen.
- Hostverwaltung: Richten Sie SAN-Initiatorgruppen und NFS-Clients ein.
- ONTAP S3 Objektspeicherverwaltung: ONTAP S3 Speicherverwaltungsfunktionen in Cloud Volumes ONTAP sind nur im System Manager und nicht in der Console verfügbar.

Unterstützte Konfigurationen

- Erweitertes Speichermanagement über ONTAP System Manager ist in Cloud Volumes ONTAP 9.10.0 und höher in Standard-Cloud-Regionen verfügbar.
- Die System Manager-Integration wird in GovCloud-Regionen oder in Regionen ohne ausgehenden Internetzugang nicht unterstützt.

Einschränkungen

Einige Funktionen, die in der System Manager-Schnittstelle angezeigt werden, werden von Cloud Volumes ONTAP nicht unterstützt:

- NetApp Cloud Tiering: Cloud Volumes ONTAP unterstützt kein Cloud Tiering. Sie sollten die Datenschichtung im Objektspeicher beim Erstellen von Volumes direkt aus der Standardansicht einrichten.
- Ebenen: Die Aggregatverwaltung (einschließlich lokaler und Cloud-Ebenen) wird vom System Manager nicht unterstützt. Sie müssen Aggregate direkt aus der Standardansicht verwalten.
- Firmware-Upgrades: Cloud Volumes ONTAP unterstützt keine automatischen Firmware-Updates von der Seite **Cluster > Einstellungen** des System Managers.
- Rollenbasierte Zugriffskontrolle: Die rollenbasierte Zugriffskontrolle vom System Manager wird nicht unterstützt.

- SMB Continuous Availability (CA): Cloud Volumes ONTAP unterstützt nicht "ständig verfügbare SMB-Aktien" für einen unterbrechungsfreien Betrieb.

Konfigurieren der Authentifizierung für den Zugriff auf den System Manager

Als Administrator können Sie die Authentifizierung für Benutzer aktivieren, die über die Konsole auf ONTAP System Manager zugreifen. Sie können die richtige Zugriffsberechtigungsebene basierend auf den ONTAP Benutzerrollen bestimmen und die Authentifizierung nach Bedarf aktivieren oder deaktivieren. Wenn Sie die Authentifizierung aktivieren, müssen Benutzer ihre ONTAP Benutzeranmeldeinformationen jedes Mal eingeben, wenn sie von der Konsole aus auf den System Manager zugreifen oder wenn die Seite neu geladen wird, da die Konsole die Anmeldeinformationen nicht intern speichert. Wenn Sie die Authentifizierung deaktivieren, können Benutzer mit den Administratoranmeldeinformationen auf den System Manager zugreifen.

Diese Einstellung gilt für jeden Konsolenagenten für die ONTAP Benutzer in Ihrer Organisation oder Ihrem Konto, unabhängig vom Cloud Volumes ONTAP System.

Erforderliche Berechtigungen

Um die Konsolen-Agent-Einstellungen für die Cloud Volumes ONTAP Benutzerauthentifizierung ändern zu können, müssen Ihnen die Administratorrechte der Organisation oder des Kontos zugewiesen sein.

Schritte

1. Gehen Sie im linken Navigationsbereich zu **Administration > Agenten**.
2. Klicken Sie auf das ••• Symbol für den gewünschten Konsolenagenten und wählen Sie **Konsolenagenten bearbeiten**.
3. Aktivieren Sie unter **Benutzeranmeldeinformationen erzwingen** das Kontrollkästchen **Aktivieren/Deaktivieren**. Standardmäßig ist die Authentifizierung deaktiviert.

   Wenn Sie diesen Wert auf **Aktivieren** setzen, wird die Authentifizierung zurückgesetzt und Sie müssen alle vorhandenen Workflows ändern, um diese Änderung zu berücksichtigen.

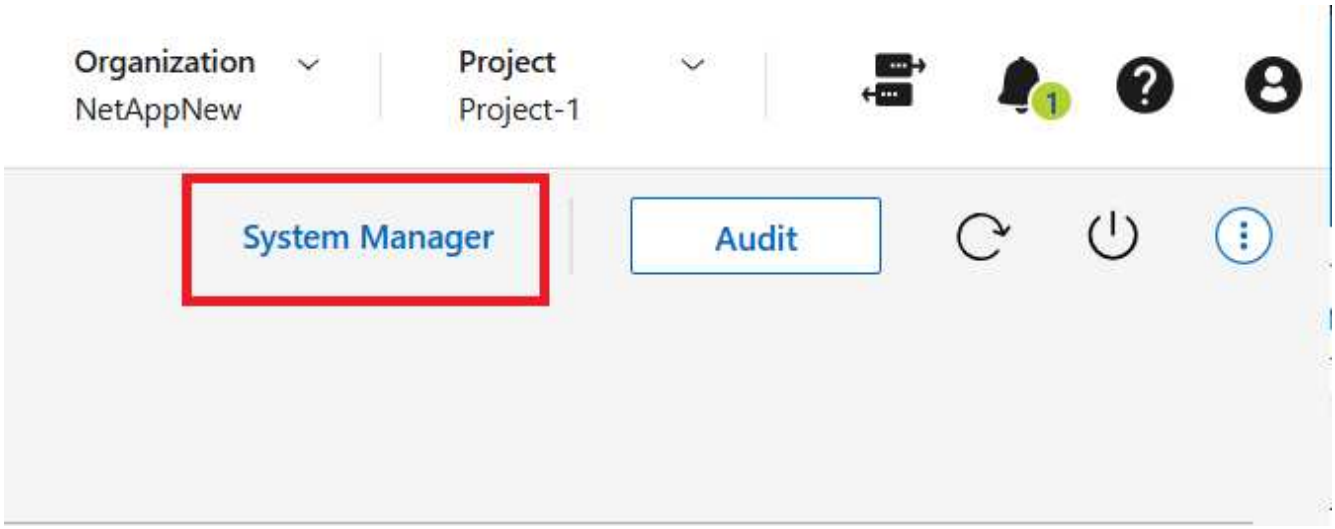
4. Klicken Sie auf **Speichern**.

Erste Schritte mit System Manager

Sie können von einem Cloud Volumes ONTAP ONTAP -System auf ONTAP System Manager zugreifen.

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Doppelklicken Sie auf der Seite **Systeme** auf das gewünschte Cloud Volumes ONTAP -System.
3. Klicken Sie auf **System Manager**.



4. Geben Sie bei entsprechender Aufforderung Ihre ONTAP Benutzeranmeldeinformationen ein und klicken Sie auf **Anmelden**.
5. Wenn eine Bestätigungsmeldung angezeigt wird, lesen Sie diese durch und klicken Sie auf **Schließen**.

Verwenden Sie System Manager, um Ihr Cloud Volumes ONTAP System zu verwalten. Sie können auf **Zurück** klicken, um zur Konsole zurückzukehren.

Hilfe zur Verwendung von System Manager

Wenn Sie Hilfe bei der Verwendung von System Manager mit Cloud Volumes ONTAP benötigen, können Sie sich an die "ONTAP-Dokumentation" für schrittweise Anleitungen. Hier sind einige Links zur ONTAP -Dokumentation, die hilfreich sein könnten:

- "ONTAP -Rollen, -Anwendungen und -Authentifizierung"
- "Verwenden Sie System Manager, um auf einen Cluster zuzugreifen" .
- "Volume- und LUN-Verwaltung"
- "Netzwerkmanagement"
- "Datenschutz"
- "Erstellen Sie kontinuierlich verfügbare SMB-Freigaben"

Verwalten von Cloud Volumes ONTAP über die CLI

Mit der Cloud Volumes ONTAP CLI können Sie alle Verwaltungsbefehle ausführen und sie ist eine gute Wahl für erweiterte Aufgaben oder wenn Sie mit der Verwendung der CLI vertrauter sind. Sie können über Secure Shell (SSH) eine Verbindung zur CLI herstellen.

Bevor Sie beginnen

Der Host, von dem aus Sie per SSH eine Verbindung zu Cloud Volumes ONTAP herstellen, muss über eine Netzwerkverbindung zu Cloud Volumes ONTAP verfügen. Beispielsweise müssen Sie möglicherweise eine SSH-Verbindung von einem Jump-Host herstellen, der sich im Netzwerk Ihres Cloud-Anbieters befindet.

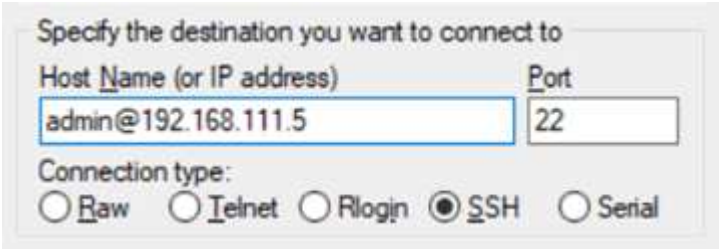
Bei der Bereitstellung in mehreren AZs verwenden Cloud Volumes ONTAP HA-Konfigurationen eine Floating-IP-Adresse für die Clusterverwaltungsschnittstelle, was bedeutet, dass kein externes Routing verfügbar ist. Sie müssen die Verbindung von einem Host aus herstellen, der Teil derselben Routingdomäne ist.

Schritte

1. Identifizieren Sie in der NetApp Console die IP-Adresse der Cluster-Verwaltungsschnittstelle:
   a. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
   b. Wählen Sie auf der Seite **Systeme** das Cloud Volumes ONTAP -System aus.
   c. Kopieren Sie die Clusterverwaltungs-IP-Adresse, die im rechten Bereich angezeigt wird.
2. Verwenden Sie SSH, um mit dem Administratorkonto eine Verbindung zur IP-Adresse der Clusterverwaltungsschnittstelle herzustellen.

   Beispiel

   Das folgende Bild zeigt ein Beispiel mit PuTTY:



3. Geben Sie bei der Anmeldeaufforderung das Kennwort für das Administratorkonto ein.

   Beispiel

```
Password: ********
COT2::>
```

Systemzustand und Ereignisse

Überprüfen Sie das AutoSupport -Setup für Cloud Volumes ONTAP

AutoSupport überwacht proaktiv den Zustand Ihres Systems und sendet Nachrichten an den technischen Support von NetApp . Standardmäßig ist AutoSupport auf jedem Knoten aktiviert, um Nachrichten über das HTTPS-Transportprotokoll an den technischen Support zu senden. Am besten überprüfen Sie, ob AutoSupport diese Nachrichten senden kann.

Der einzige erforderliche Konfigurationsschritt besteht darin, sicherzustellen, dass Cloud Volumes ONTAP über eine ausgehende Internetverbindung verfügt. Einzelheiten finden Sie in den Netzwerkanforderungen Ihres Cloud-Anbieters.

AutoSupport Anforderungen

Cloud Volumes ONTAP -Knoten erfordern ausgehenden Internetzugang für NetApp AutoSupport, das den Zustand Ihres Systems proaktiv überwacht und Nachrichten an den technischen Support von NetApp sendet.

Routing- und Firewall-Richtlinien müssen HTTPS-Verkehr zu den folgenden Endpunkten zulassen, damit Cloud Volumes ONTAP AutoSupport Nachrichten senden kann:

- https://mysupport.netapp.com/aods/asupmessage
- https://mysupport.netapp.com/asupprod/post/1.0/postAsup

Wenn zum Senden von AutoSupport -Nachrichten keine ausgehende Internetverbindung verfügbar ist, konfiguriert die NetApp Console Ihre Cloud Volumes ONTAP Systeme automatisch so, dass der Konsolenagent als Proxyserver verwendet wird. Die einzige Voraussetzung besteht darin, sicherzustellen, dass die Sicherheitsgruppe des Konsolenagenten *eingehende* Verbindungen über Port 3128 zulässt. Sie müssen diesen Port öffnen, nachdem Sie den Konsolenagenten bereitgestellt haben.

Wenn Sie strenge ausgehende Regeln für Cloud Volumes ONTAP definiert haben, müssen Sie auch sicherstellen, dass die Sicherheitsgruppe Cloud Volumes ONTAP ausgehende Verbindungen über Port 3128 zulässt.

Wenn Sie ein HA-Paar verwenden, benötigt der HA-Mediator keinen ausgehenden Internetzugang.

Nachdem Sie überprüft haben, dass ausgehender Internetzugang verfügbar ist, können Sie AutoSupport testen, um sicherzustellen, dass es Nachrichten senden kann. Anweisungen hierzu finden Sie im "ONTAP -Dokumentation: AutoSupport einrichten" .

Fehlerbehebung bei Ihrer AutoSupport -Konfiguration

Wenn keine ausgehende Verbindung verfügbar ist und die Konsole Ihr Cloud Volumes ONTAP -System nicht so konfigurieren kann, dass der Konsolenagent als Proxy-Server verwendet wird, erhalten Sie von der Konsole eine Benachrichtigung, dass Ihr System nicht in der Lage ist, AutoSupport Nachrichten zu senden. Befolgen Sie diese Schritte, um dieses Problem zu beheben.

Schritte

1. Stellen Sie eine sichere Verbindung (über SSH) zum Cloud Volumes ONTAP System her, um die ONTAP CLI zu verwenden.

   "Erfahren Sie, wie Sie per SSH auf Cloud Volumes ONTAP zugreifen" .

2. Überprüfen Sie den detaillierten Status des AutoSupport Subsystems:

   ```
   autosupport check show-details
   ```

   Die Antwort sieht folgendermaßen aus:

```
    Category: smtp
          Component: mail-server
             Status: failed
             Detail: SMTP connectivity check failed for destination:
                     mailhost. Error: Could not resolve host -
'mailhost'
            Corrective Action: Check the hostname of the SMTP server

    Category: http-https
        Component: http-put-destination
            Status: ok
            Detail: Successfully connected to:
                    <https://support.netapp.com/put/AsupPut/>.

          Component: http-post-destination
             Status: ok
             Detail: Successfully connected to:

https://support.netapp.com/asupprod/post/1.0/postAsup.

    Category: on-demand
          Component: ondemand-server
             Status: ok
             Detail: Successfully connected to:
                     https://support.netapp.com/aods/asupmessage.

    Category: configuration
            Component: configuration
                Status: ok
                Detail: No configuration issues found.
    5 entries were displayed.
```

Wenn der Status der Kategorie http-https ist `OK` Das bedeutet, dass AutoSupport ordnungsgemäß konfiguriert ist und Nachrichten gesendet werden können.

3. Falls nicht, überprüfen Sie die Proxy-URL für jeden Cloud Volumes ONTAP -Knoten:

   ```
   autosupport show -fields proxy-url
   ```

4. Wenn der Proxy-URL-Parameter leer ist, konfigurieren Sie Cloud Volumes ONTAP so, dass der Konsolenagent als Proxy verwendet wird:

   ```
   autosupport modify -proxy-url http://<console agent private ip>:3128
   ```

5. Überprüfen Sie den AutoSupport Status erneut:

   ```
   autosupport check show-details
   ```

6. Wenn der Status weiterhin „Fehlgeschlagen“ lautet, überprüfen Sie, ob eine Verbindung zwischen Cloud Volumes ONTAP und dem Konsolenagenten über Port 10 besteht. `3128`Die
7. Wenn der Status nach der Überprüfung immer noch fehlgeschlagen ist, stellen Sie eine SSH-Verbindung zum Konsolenagenten her.

   "Erfahren Sie mehr über die Verbindung zur Linux-VM für den Konsolen-Agenten"

8. Gehe zu `/opt/application/netapp/cloudmanager/docker_occm/data/`Die
9. Öffnen Sie die Proxy-Konfigurationsdatei `squid.conf`Die Dies ist die Struktur der Datei:

```
        http_port 3128
        acl netapp_support dst support.netapp.com
        http_access allow netapp_support
        request_header_max_size 21 KB
        reply_header_max_size 21 KB
        http_access deny all
        httpd_suppress_version_string on
```

10. Falls Ihre Datei keinen Eintrag für den CIDR-Block des Cloud Volumes ONTAP Systems enthält, fügen Sie einen neuen Eintrag hinzu und erlauben Sie den Zugriff:

    ```
    acl cvonet src <cidr>

    http_access allow cvonet
    ```

    Hier ist ein Beispiel:

```
        http_port 3128
        acl netapp_support dst support.netapp.com
        acl cvonet src <cidr>
        http_access allow netapp_support
        http_access allow cvonet
        request_header_max_size 21 KB
        reply_header_max_size 21 KB
        http_access deny all
        httpd_suppress_version_string on
```

11. Nach der Bearbeitung der Konfigurationsdatei muss der Proxy-Container neu gestartet werden. `sudo`Die Je nachdem, ob Sie Docker oder Podman verwenden, führen Sie folgende Befehle aus:

    Für Docker: Führen Sie Folgendes aus `docker restart squid`Die

    Wenn Sie Podman verwenden, führen Sie Folgendes aus: `podman restart squid`Die

12. Kehren Sie zur ONTAP CLI zurück und überprüfen Sie, ob Cloud Volumes ONTAP AutoSupport Nachrichten senden kann:

    ```
    autosupport check show-details
    ```

Weiterführende Links

- "Netzwerkanforderungen für Cloud Volumes ONTAP in AWS"
- "Netzwerkanforderungen für Cloud Volumes ONTAP in Azure"
- "Netzwerkanforderungen für Cloud Volumes ONTAP in Google Cloud"

EMS für Cloud Volumes ONTAP -Systeme konfigurieren

Das Event Management System (EMS) sammelt und zeigt Informationen zu Ereignissen an, die auf ONTAP -Systemen auftreten. Um Ereignisbenachrichtigungen zu erhalten, können Sie Ereignisziele (E-Mail-Adressen, SNMP-Trap-Hosts oder Syslog-Server) und Ereignisrouten für einen bestimmten Ereignisschweregrad festlegen.

Sie können EMS mithilfe der CLI konfigurieren. Anweisungen hierzu finden Sie im "ONTAP -Dokumentation: EMS-Konfigurationsübersicht" .

Konzepte

Lizenzierung

Lizenzierung für Cloud Volumes ONTAP

Für Cloud Volumes ONTAP sind mehrere Lizenzierungsoptionen verfügbar. Jede Option ermöglicht Ihnen die Auswahl eines Verbrauchsmodells, das Ihren Anforderungen entspricht.

Lizenzübersicht

Für Neukunden stehen folgende Lizenzierungsoptionen zur Verfügung.

Kapazitätsbasierte Lizenzierung
: Bezahlen Sie für mehrere Cloud Volumes ONTAP -Systeme in Ihrem NetApp -Konto nach bereitgestellter Kapazität. Beinhaltet die Möglichkeit, zusätzliche Cloud-Datendienste zu erwerben. Weitere Informationen zu Verbrauchsmodellen oder Kaufoptionen bei kapazitätsbasierten Lizenzen finden Sie unter:"Erfahren Sie mehr über kapazitätsbasierte Lizenzen" Die

Keystone Abonnement
: Ein Abonnementdienst mit nutzungsabhängiger Bezahlung, der ein nahtloses Hybrid-Cloud-Erlebnis für Hochverfügbarkeitspaare (HA) bietet.

In den folgenden Abschnitten finden Sie weitere Einzelheiten zu jeder dieser Optionen.

Für die Nutzung lizenzierter Funktionen ohne Lizenz wird kein Support angeboten.

Kapazitätsbasierte Lizenzierung

Mit kapazitätsbasierten Lizenzpaketen können Sie für Cloud Volumes ONTAP pro TiB Kapazität bezahlen. Die Lizenz ist mit Ihrem NetApp -Konto verknüpft und ermöglicht Ihnen, mehrere Systeme über die Lizenz abzurechnen, sofern über die Lizenz genügend Kapazität verfügbar ist.

Sie könnten beispielsweise eine einzelne 20-TiB-Lizenz erwerben, vier Cloud Volumes ONTAP Systeme bereitstellen und dann jedem System ein 5-TiB-Volume zuweisen, sodass insgesamt 20 TiB zur Verfügung stehen. Die Kapazität steht den Volumes auf jedem in diesem Konto bereitgestellten Cloud Volumes ONTAP System zur Verfügung.

Die kapazitätsbasierte Lizenzierung ist in Form eines *Pakets* verfügbar. Wenn Sie ein Cloud Volumes ONTAP -System bereitstellen, können Sie je nach Ihren Geschäftsanforderungen aus mehreren Lizenzpaketen wählen.

Während die tatsächliche Nutzung und Messung der in der NetApp Console verwalteten Produkte und Services immer in GiB und TiB berechnet wird, werden die Begriffe GB/GiB und TB/TiB synonym verwendet. Dies spiegelt sich in den Einträgen im Cloud-Marktplatz, Preisangeboten, Eintragsbeschreibungen und in anderen unterstützenden Dokumenten wider.

Pakete

Für Cloud Volumes ONTAP sind die folgenden kapazitätsbasierten Pakete verfügbar. Weitere Informationen zu kapazitätsbasierten Lizenzpaketen finden Sie unter"Erfahren Sie mehr über kapazitätsbasierte Lizenzen" .

Eine Liste der unterstützten VM-Typen mit den folgenden kapazitätsbasierten Paketen finden Sie unter:

- "Unterstützte Konfigurationen in Azure"
- "Unterstützte Konfigurationen in Google Cloud"

Freemium

Bietet alle Cloud Volumes ONTAP -Funktionen kostenlos von NetApp (Gebühren des Cloud-Anbieters fallen weiterhin an). Ein Freemium-Paket hat folgende Eigenschaften:

- Es ist keine Lizenz oder kein Vertrag erforderlich.
- Support von NetApp ist nicht enthalten.
- Sie sind auf 500 GiB bereitgestellte Kapazität pro Cloud Volumes ONTAP System beschränkt.
- Mit dem Freemium-Angebot können Sie pro NetApp -Konto bis zu 10 Cloud Volumes ONTAP Systeme für jeden Cloud-Anbieter nutzen.
- Wenn die bereitgestellte Kapazität für ein Cloud Volumes ONTAP -System 500 GiB überschreitet, konvertiert die Konsole das System in ein Essentials-Paket.

  Sobald ein System auf das Essentials-Paket umgestellt wird,"Mindestladezeit" gilt dafür.

  Ein Cloud Volumes ONTAP -System, das in ein Essentials-Paket konvertiert wurde, kann nicht wieder auf Freemium umgestellt werden, selbst wenn die bereitgestellte Kapazität auf weniger als 500 GiB reduziert wird. Andere Systeme mit weniger als 500 GiB bereitgestellter Kapazität bleiben bei Freemium (sofern sie mit dem Freemium-Angebot bereitgestellt wurden).

Grundausstattung

Sie können nach Kapazität in verschiedenen Konfigurationen bezahlen:

- Wählen Sie Ihre Cloud Volumes ONTAP -Konfiguration:
  - Ein einzelner Knoten oder ein HA-System
  - Datei- und Blockspeicher oder Sekundärdaten für die Notfallwiederherstellung (DR)
- Fügen Sie gegen Aufpreis beliebige Cloud-Datendienste von NetApp hinzu

Professional

Bezahlen Sie nach Kapazität für jede Art von Cloud Volumes ONTAP Konfiguration mit unbegrenzten Backups.

- Bietet Lizenzierung für jede Cloud Volumes ONTAP -Konfiguration

  Einzelknoten oder HA mit Kapazitätsabrechnung für primäre und sekundäre Volumes zum gleichen Tarif

- Beinhaltet unbegrenzte Volume-Backups mit NetApp Backup and Recovery, jedoch nur für Cloud Volumes ONTAP Systeme, die das Professional-Paket verwenden.

Für Backup und Recovery ist ein Pay-as-you-go-Abonnement (PAYGO) erforderlich. Für die Nutzung dieses Dienstes fallen jedoch keine Gebühren an. Weitere Informationen zum Einrichten der Lizenzierung für Backup und Recovery finden Sie unter "Einrichten der Lizenzierung für Backup und Recovery" .

- Fügen Sie gegen Aufpreis beliebige Cloud-Datendienste von NetApp hinzu

Verfügbarkeit kapazitätsbasierter Lizenzen

Die Verfügbarkeit der PAYGO- und BYOL-Lizenzen für Cloud Volumes ONTAP Systeme erfordert, dass der Konsolenagent betriebsbereit ist.

"Erfahren Sie mehr über Konsolenagenten" .

NetApp hat den Erwerb, die Verlängerung und die Erneuerung von BYOL-Lizenzen eingeschränkt. Weitere Informationen finden Sie unter "Eingeschränkte Verfügbarkeit der BYOL-Lizenzierung für Cloud Volumes ONTAPP" .

Erste Schritte

Erfahren Sie, wie Sie mit der kapazitätsbasierten Lizenzierung beginnen:

- "Einrichten der Lizenzierung für Cloud Volumes ONTAP in AWS"
- "Einrichten der Lizenzierung für Cloud Volumes ONTAP in Azure"
- "Einrichten der Lizenzierung für Cloud Volumes ONTAP in Google Cloud"

Keystone Abonnement

Ein Abonnementdienst mit nutzungsabhängiger Bezahlung, der ein nahtloses Hybrid-Cloud-Erlebnis für diejenigen bietet, die OpEx-Verbrauchsmodelle gegenüber vorab zu zahlenden Investitionskosten oder Leasing bevorzugen.

Die Abrechnung basiert auf der Größe Ihrer zugesagten Kapazität für ein oder mehrere Cloud Volumes ONTAP HA-Paare in Ihrem Keystone Abonnement.

Die bereitgestellte Kapazität für jedes Volume wird aggregiert und regelmäßig mit der zugesagten Kapazität Ihres Keystone Abonnements verglichen. Überschreitungen werden als Burst für Ihr Keystone Abonnement berechnet.

"Erfahren Sie mehr über NetApp Keystone" .

Unterstützte Konfigurationen

Keystone Subscriptions werden mit HA-Paaren unterstützt. Diese Lizenzierungsoption wird derzeit nicht mit Single-Node-Systemen unterstützt.

Kapazitätsgrenze

Im kapazitätsbasierten Lizenzmodell unterstützt jedes Cloud Volumes ONTAP System die Einstufung in Objektspeicher und die gesamte abgestufte Kapazität kann bis zum Bucket-Limit des Cloud-Anbieters skaliert werden. Obwohl die Lizenz keine Kapazitätsbeschränkungen vorsieht, befolgen Sie die "Best Practices für FabricPool" um optimale Leistung, Zuverlässigkeit und Kosteneffizienz bei der Konfiguration und Verwaltung der Tiering-Ebene sicherzustellen.

Informationen zu den Kapazitätsgrenzen der einzelnen Cloud-Anbieter finden Sie in deren Dokumentation:

- "AWS-Dokumentation"
- "Azure-Dokumentation für verwaltete Datenträger"Und "Azure-Dokumentation für Blob Storage"
- "Google Cloud-Dokumentation"

Erste Schritte

Erfahren Sie, wie Sie mit einem Keystone -Abonnement beginnen:

- "Einrichten der Lizenzierung für Cloud Volumes ONTAP in AWS"
- "Einrichten der Lizenzierung für Cloud Volumes ONTAP in Azure"
- "Einrichten der Lizenzierung für Cloud Volumes ONTAP in Google Cloud"

Knotenbasierte Lizenzierung

Die knotenbasierte Lizenzierung ist das Lizenzierungsmodell der vorherigen Generation, mit dem Sie Cloud Volumes ONTAP pro Knoten lizenzieren konnten. Dieses Lizenzmodell ist für Neukunden nicht verfügbar. Das Laden nach Knoten wurde durch die oben beschriebenen Lademethoden nach Kapazität ersetzt.

NetApp hat das Ende der Verfügbarkeit (EOA) und des Supports (EOS) der knotenbasierten Lizenzierung geplant. Nach EOA und EOS müssen knotenbasierte Lizenzen in kapazitätsbasierte Lizenzen umgewandelt werden.

Weitere Informationen finden Sie unter "Kundenmitteilung: CPC-00589" .

Ende der Verfügbarkeit von knotenbasierten Lizenzen

Ab dem 11. November 2024 wurde die begrenzte Verfügbarkeit von knotenbasierten Lizenzen beendet. Der Support für die knotenbasierte Lizenzierung endet am 31. Dezember 2024.

Wenn Sie über einen gültigen knotenbasierten Vertrag verfügen, der über das EOA-Datum hinausgeht, können Sie die Lizenz bis zum Ablauf des Vertrags weiter verwenden. Nach Ablauf des Vertrages ist eine Umstellung auf das kapazitätsbasierte Lizenzmodell erforderlich. Wenn Sie keinen langfristigen Vertrag für einen Cloud Volumes ONTAP Knoten haben, ist es wichtig, Ihre Konvertierung vor dem EOS-Datum zu planen.

In dieser Tabelle erfahren Sie mehr über die einzelnen Lizenztypen und die Auswirkungen von EOA darauf:

Lizenztyp	Auswirkungen nach EOA
Gültige knotenbasierte Lizenz, erworben über Bring Your Own License (BYOL)	Die Lizenz bleibt bis zum Ablauf gültig. Vorhandene, ungenutzte knotenbasierte Lizenzen können für die Bereitstellung neuer Cloud Volumes ONTAP -Systeme verwendet werden.
Abgelaufene knotenbasierte Lizenz, die über BYOL erworben wurde	Sie sind nicht berechtigt, mit dieser Lizenz neue Cloud Volumes ONTAP -Systeme bereitzustellen. Die vorhandenen Systeme funktionieren möglicherweise weiterhin, Sie erhalten jedoch nach dem EOS-Datum keinen Support oder keine Updates für Ihre Systeme.

Lizenztyp	Auswirkungen nach EOA
Gültige knotenbasierte Lizenz mit PAYGO-Abonnement	Sie erhalten nach dem EOS-Datum NetApp Support mehr, bis Sie zu einer kapazitätsbasierten Lizenz wechseln.

Ausschlüsse

NetApp ist sich bewusst, dass bestimmte Situationen besondere Berücksichtigung erfordern. EOA und EOS der knotenbasierten Lizenzierung gelten in den folgenden Fällen nicht:

- Kunden aus dem öffentlichen Sektor der USA
- Bereitstellungen im privaten Modus
- Bereitstellungen von Cloud Volumes ONTAP in AWS in der Region China

Für diese speziellen Szenarien bietet NetApp Unterstützung bei der Erfüllung der einzigartigen Lizenzanforderungen im Einklang mit vertraglichen Verpflichtungen und betrieblichen Anforderungen.

Auch in diesen Szenarien sind neue knotenbasierte Lizenzen und Lizenzverlängerungen ab dem Genehmigungsdatum maximal ein Jahr gültig.

Lizenzkonvertierung

Die Konsole ermöglicht eine nahtlose Konvertierung von knotenbasierten Lizenzen in kapazitätsbasierte Lizenzen über das Lizenzkonvertierungstool. Informationen zum EOA der knotenbasierten Lizenzierung finden Sie unter"Ende der Verfügbarkeit von knotenbasierten Lizenzen" .

Vor der Umstellung ist es gut, sich mit den Unterschieden zwischen den beiden Lizenzmodellen vertraut zu machen. Die knotenbasierte Lizenzierung umfasst eine feste Kapazität für jede ONTAP Instanz, was die Flexibilität einschränken kann. Die kapazitätsbasierte Lizenzierung hingegen ermöglicht einen gemeinsamen Speicherpool über mehrere Instanzen hinweg, bietet dadurch mehr Flexibilität, optimiert die Ressourcennutzung und reduziert das Risiko finanzieller Nachteile bei der Neuverteilung von Workloads. Die kapazitätsbasierte Abrechnung passt sich nahtlos an veränderte Speicheranforderungen an.

Informationen zur Durchführung dieser Konvertierung finden Sie unter"Konvertieren Sie eine knotenbasierte Cloud Volumes ONTAP Lizenz in eine kapazitätsbasierte Lizenz" .

Die Umstellung eines Systems von kapazitätsbasierter auf knotenbasierte Lizenzierung wird nicht unterstützt.

Erfahren Sie mehr über kapazitätsbasierte Lizenzen für Cloud Volumes ONTAP

Sie sollten mit den Abrechnungs- und Kapazitätsnutzungsregeln für kapazitätsbasierte Lizenzen vertraut sein.

Verbrauchsmodelle oder Lizenzkaufoptionen

Kapazitätsbasierte Lizenzpakete sind mit folgenden Verbrauchsmodellen bzw. Kaufoptionen erhältlich:

- **BYOL**: Bringen Sie Ihre eigene Lizenz mit (BYOL). Eine von NetApp erworbene Lizenz, mit der Cloud Volumes ONTAP bei jedem Cloud-Anbieter bereitgestellt werden kann.

NetApp hat den Erwerb, die Verlängerung und die Erneuerung von BYOL-Lizenzen eingeschränkt. Weitere Informationen finden Sie unter "Eingeschränkte Verfügbarkeit der BYOL-Lizenzierung für Cloud Volumes ONTAP" .

- **PAYGO**: Ein Pay-as-you-go-Abonnement (PAYGO) ist ein stündliches Abonnement vom Marktplatz Ihres Cloud-Anbieters.
- **Jährlich**: Ein Jahresvertrag vom Marktplatz Ihres Cloud-Anbieters.

Beachten Sie Folgendes:

- Wenn Sie eine Lizenz von NetApp (BYOL) erwerben, müssen Sie zusätzlich das PAYGO-Angebot vom Marktplatz Ihres Cloud-Anbieters abonnieren. NetApp hat die BYOL-Lizenzierung eingeschränkt. Wenn Ihre BYOL-Lizenzen ablaufen, müssen Sie sie durch Abonnements vom Cloud-Marktplatz ersetzen.

  Ihre Lizenz wird immer zuerst in Rechnung gestellt. In den folgenden Fällen wird Ihnen jedoch der Stundensatz auf dem Marktplatz in Rechnung gestellt:

  - Wenn Sie Ihre lizenzierte Kapazität überschreiten
  - Wenn die Laufzeit Ihrer Lizenz abläuft
- Wenn Sie einen Jahresvertrag von einem Marktplatz haben, werden *alle* von Ihnen bereitgestellten Cloud Volumes ONTAP Systeme über diesen Vertrag abgerechnet. Sie können einen jährlichen Marktplatzvertrag nicht mit BYOL kombinieren.
- Nur Einzelknotensysteme mit BYOL werden in China-Regionen unterstützt. Bereitstellungen in China-Regionen sind von den BYOL-Lizenzbeschränkungen ausgenommen.

Änderung der Lizenzpakete

Nach der Bereitstellung können Sie das Paket für ein Cloud Volumes ONTAP -System ändern, das eine kapazitätsbasierte Lizenzierung verwendet. Wenn Sie beispielsweise ein Cloud Volumes ONTAP -System mit dem Essentials-Paket bereitgestellt haben, können Sie es auf das Professional-Paket umstellen, wenn sich Ihre Geschäftsanforderungen ändern.

"Erfahren Sie, wie Sie die Lademethode ändern" .

Informationen zum Konvertieren von knotenbasierten Lizenzen in kapazitätsbasierte Lizenzen finden Sie unter

Wie Ihnen die unterstützten Speichertypen und Pakete in Rechnung gestellt werden

Die Abrechnung in Cloud Volumes ONTAP basiert auf einer Reihe von Faktoren, wie z. B. Paketen und Volumentypen. Kapazitätsbasierte Lizenzpakete sind mit Cloud Volumes ONTAP 9.7 und höher verfügbar.

Einzelheiten zu den Preisen finden Sie auf der "NetApp Console Website" .

Speicher-VMs

- Für zusätzliche datenbereitstellende Storage-VMs (SVMs) fallen keine zusätzlichen Lizenzkosten an, es wird jedoch eine Mindestkapazitätsgebühr von 4 TiB pro datenbereitstellender SVM erhoben.
- Die Kosten für Disaster Recovery-SVMs richten sich nach der bereitgestellten Kapazität.

HA-Paare

Bei HA-Paaren wird Ihnen nur die bereitgestellte Kapazität auf einem Knoten in Rechnung gestellt. Für Daten,

die synchron auf den Partnerknoten gespiegelt werden, fallen keine Kosten an.

FlexClone und FlexCache -Volumes

- Für die von FlexClone -Volumes genutzte Kapazität werden Ihnen keine Kosten berechnet.
- Quell- und Ziel- FlexCache -Volumes werden als Primärdaten betrachtet und entsprechend dem bereitgestellten Speicherplatz berechnet.

Lese-/Schreibvolumes

Wenn Sie ein beschreibbares (Lese-/Schreib-)Volume erstellen oder verwenden, wird es als primäres Volume betrachtet und die bereitgestellte Kapazität wird auf Basis der Mindestgebühr pro Storage VM (SVM) berechnet. Beispiele hierfür sind FlexVol Lese-/Schreibvolumes, SnapLock -Auditvolumes und CIFS/NFS-Auditvolumes. Alle vom Benutzer erstellten Datenmengen werden gemäß Ihrem Abonnement und Pakettyp abgerechnet. Für ONTAP interne Volumes, die automatisch erstellt werden und keine Daten speichern können, wie z. B. SVM-Root-Volumes, werden keine Gebühren erhoben.

Essentials-Pakete

Beim Essentials-Paket erfolgt die Abrechnung nach Bereitstellungstyp (HA oder Einzelknoten) und Volumetyp (primär oder sekundär). Die Preisgestaltung erfolgt in der folgenden Reihenfolge (absteigend): *Essentials Primary HA*, *Essentials Primary Single Node*, *Essentials Secondary HA* und *Essentials Secondary Single Node*. Wenn Sie alternativ einen Marktplatzvertrag erwerben oder ein privates Angebot annehmen, sind die Kapazitätsgebühren für alle Bereitstellungs- und Volumentypen gleich.

Die Lizenzierung basiert vollständig auf dem Volume-Typ, der in Cloud Volumes ONTAP Systemen erstellt wird:

- Essentials Single Node: Lese-/Schreib-Volumes, die auf einem Cloud Volumes ONTAP System mit nur einem ONTAP Knoten erstellt wurden.
- Essentials HA: Lese-/Schreib-Volumes mit zwei ONTAP -Knoten, die für einen unterbrechungsfreien Datenzugriff auf einander umschalten können.
- Essentials Secondary Single Node: Volumes vom Typ Data Protection (DP) (normalerweise schreibgeschützte SnapMirror oder SnapVault -Zielvolumes), die auf einem Cloud Volumes ONTAP System unter Verwendung nur eines ONTAP Knotens erstellt wurden.

  > Wenn ein schreibgeschütztes/DP-Volume zu einem primären Volume wird, betrachtet die Konsole es als primäre Daten und die Gebühren werden basierend auf der Zeit berechnet, die das Volume im Lese-/Schreibmodus war. Wenn das Volume wieder schreibgeschützt/DP ist, wird es wieder als sekundäres Datenvolumen betrachtet und entsprechend mit der am besten passenden Lizenz in der Konsole abgerechnet.

- Essentials Secondary HA: Volumes vom Typ Data Protection (DP) (normalerweise schreibgeschützte SnapMirror oder SnapVault -Zielvolumes), die auf einem Cloud Volumes ONTAP -System unter Verwendung von zwei ONTAP Knoten erstellt werden, die für einen unterbrechungsfreien Datenzugriff auf einander umschalten können.

Kapazitätsgrenze

Im kapazitätsbasierten Lizenzmodell unterstützt jedes Cloud Volumes ONTAP System die Einstufung in Objektspeicher und die gesamte abgestufte Kapazität kann bis zum Bucket-Limit des Cloud-Anbieters skaliert werden. Obwohl die Lizenz keine Kapazitätsbeschränkungen vorsieht, befolgen Sie die "Best Practices für FabricPool" um optimale Leistung, Zuverlässigkeit und Kosteneffizienz bei der Konfiguration und Verwaltung

der Tiering-Ebene sicherzustellen.

Informationen zu den Kapazitätsgrenzen der einzelnen Cloud-Anbieter finden Sie in deren Dokumentation:

- "AWS-Dokumentation"
- "Azure-Dokumentation für verwaltete Datenträger"Und "Azure-Dokumentation für Blob Storage"
- "Google Cloud-Dokumentation"

Maximale Anzahl an Systemen

Bei kapazitätsbasierter Lizenzierung ist die maximale Anzahl von Cloud Volumes ONTAP-Systemen auf 24 pro NetApp Console-Organisation beschränkt. Ein ist ein Cloud Volumes ONTAP HA-Paar, ein Cloud Volumes ONTAP Einzelknotensystem oder eine beliebige zusätzliche Speicher-VM, die Sie erstellen. Die Standard-Speicher-VM wird nicht auf das Limit angerechnet. Dieses Limit gilt für alle Lizenzmodelle.

Nehmen wir beispielsweise an, Sie haben drei Systeme:

- Ein Cloud Volumes ONTAP -System mit einem Knoten und einer Speicher-VM (dies ist die Standard-Speicher-VM, die beim Bereitstellen von Cloud Volumes ONTAP erstellt wird)

  Dieses System zählt als ein System.

- Ein Cloud Volumes ONTAP -System mit einem Knoten und zwei Speicher-VMs (die Standard-Speicher-VM plus eine zusätzliche Speicher-VM, die Sie erstellt haben)

  Dieses System zählt als zwei Systeme: eines für das Einzelknotensystem und eines für die zusätzliche Storage-VM.

- Ein Cloud Volumes ONTAP HA-Paar mit drei Storage-VMs (die Standard-Storage-VM plus zwei zusätzliche Storage-VMs, die Sie erstellt haben)

  Dieses System zählt als drei Systeme: eines für das HA-Paar und zwei für die zusätzlichen Speicher-VMs.

Das sind insgesamt sechs Systeme. Sie hätten dann Platz für weitere 14 Systeme in Ihrer Organisation.

Bei größeren Installationen mit mehr als 24 Systemen wenden Sie sich bitte an Ihren Kundenbetreuer oder Ihr Vertriebsteam.

"Informieren Sie sich über Speicherlimits für AWS, Azure und Google Cloud" .

Mindestgebühr

Für jede datenbereitstellende Speicher-VM mit mindestens einem primären (Lese-/Schreib-)Volume wird eine Mindestgebühr von 4 TiB erhoben. Wenn die Summe der primären Volumes weniger als 4 TiB beträgt, berechnet die Konsole dieser Speicher-VM die Mindestgebühr von 4 TiB.

Wenn Sie noch keine Volumes bereitgestellt haben, fällt die Mindestgebühr nicht an.

Beim Essentials-Paket fällt die Gebühr für die Mindestkapazität von 4 TiB nicht für Speicher-VMs an, die nur sekundäre (Datenschutz-)Volumes enthalten. Wenn Sie beispielsweise über eine Speicher-VM mit 1 TiB sekundärer Daten verfügen, werden Ihnen nur die Kosten für dieses 1 TiB Daten in Rechnung gestellt. Beim Pakettyp „Professional“ gilt unabhängig vom Volume-Typ die Mindestkapazitätsberechnung von 4 TiB.

Abrechnungseinstellungen und Überschreitungen

Im Abschnitt * Licenses and subscriptions* in der Konsole können Sie auswählen, wie die Abrechnung erfolgen soll. Überschreitungen entstehen, wenn Ihre Nutzung die in Ihrem Lizenzpaket oder Jahresabonnement festgelegte Kapazität überschreitet.

- * NetApp -Lizenzen zuerst*: Bei diesem Modell wird Ihre Nutzung zunächst auf die Kapazität Ihres Lizenzpakets (BYOL) angerechnet. Wenn Sie Ihre Lizenzkapazität überschreiten, werden die Mehrkosten auf Basis Ihres jährlichen Marktplatz-Abonnements oder Ihrer stündlichen Marktplatz-Abrechnungssätze (PAYGO) berechnet. Wenn Ihre BYOL-Lizenz abläuft, müssen Sie über die Cloud-Marktplätze auf ein kapazitätsbasiertes Lizenzierungsmodell umsteigen. Weitere Informationen finden Sie unter "Konvertieren Sie eine knotenbasierte Cloud Volumes ONTAP -Lizenz in eine kapazitätsbasierte Lizenz"Die
- **Nur für Marketplace-Abonnements**: Bei diesem Modell wird Ihre Nutzung zunächst über Ihr jährliches Marketplace-Abonnement abgerechnet. Jegliche zusätzliche Nutzung wird zu den stundenweisen On-Demand-Tarifen des Marktplatzes abgerechnet (PAYGO). Nicht genutzte Lizenzkapazität wird bei der Abrechnung nicht berücksichtigt.

Weitere Informationen zu den Abrechnungseinstellungen finden Sie unter "Erfahren Sie mehr über die Abrechnungseinstellungen für Lizenzen und Abonnements."Die

Wie Überschreitungen bei Essentials-Lizenzen abgerechnet werden

Wenn Sie eine Essentials-Lizenz von NetApp (BYOL) erwerben und die lizenzierte Kapazität für ein bestimmtes Essentials-Paket überschreiten, berechnet die Console die Mehrkosten einer höherpreisigen Essentials-Lizenz (sofern Sie über eine solche mit verfügbarer Kapazität verfügen). Die Konsole nutzt zunächst die verfügbare Kapazität, für die Sie bezahlt haben, bevor sie den Marktplatz in Rechnung stellt. Falls mit Ihrer BYOL-Lizenz keine Kapazität verfügbar ist, wird die überschrittene Kapazität zu den stündlichen On-Demand-Tarifen des Marktplatzes (PAYGO) abgerechnet und Ihrer monatlichen Rechnung hinzugefügt.

Wenn Sie hingegen einen jährlichen Marktplatzvertrag oder ein privates Angebot mit mehreren Essentials-Paketen haben und Ihre Nutzung die zugesicherte Kapazität für einen Bereitstellungs- und Volumentyp eines bestimmten Pakets überschreitet, berechnet die Console die Mehrkosten einem höherpreisigen Essentials-Paket auf Basis seiner verfügbaren Kapazität. Sobald diese Kapazität erschöpft ist, wird der verbleibende Mehrverbrauch zu den stündlichen PAYGO-Tarifen (Pay-as-you-go) des Marktplatzes abgerechnet und Ihrer monatlichen Rechnung hinzugefügt.

Informationen zu den Gebühren für Essentials-Lizenzen finden Sie unter"Essentials-Pakete" Die

Hier ist ein Beispiel. Angenommen, Sie verfügen über die folgenden Lizenzen für das Essentials-Paket:

- Eine 500 TiB *Essentials Secondary HA*-Lizenz mit 500 TiB zugesicherter Kapazität
- Eine 500 TiB *Essentials Single Node*-Lizenz mit nur 100 TiB zugesicherter Kapazität

Weitere 50 TiB werden auf einem HA-Paar mit sekundären Volumes bereitgestellt. Anstatt diese 50 TiB PAYGO in Rechnung zu stellen, verrechnet die Konsole die 50 TiB Überschreitung mit der *Essentials Single Node*-Lizenz. Diese Lizenz ist teurer als *Essentials Secondary HA*, nutzt jedoch eine Lizenz, die Sie bereits erworben haben, und verursacht keine zusätzlichen Kosten auf Ihrer monatlichen Rechnung.

Unter **Verwaltung > Licenses and subscriptions** können Sie sehen, dass 50 TiB von der *Essentials Single Node*-Lizenz abgezogen werden.

Hier ist ein weiteres Beispiel. Angenommen, Sie verfügen über die folgenden Lizenzen für das Essentials-Paket:

- Eine 500 TiB *Essentials Secondary HA*-Lizenz mit 500 TiB zugesicherter Kapazität
- Eine 500 TiB *Essentials Single Node*-Lizenz mit nur 100 TiB zugesicherter Kapazität

Weitere 100 TiB werden auf einem HA-Paar mit primären Volumes bereitgestellt. Die von Ihnen erworbene Lizenz verfügt nicht über die zugesagte Kapazität von *Essentials Primary HA*. Die Lizenz „Essentials Primary HA“ ist teurer als die Lizenzen „Essentials Primary Single Node“ und „Essentials Secondary HA“.

In diesem Beispiel berechnet die Konsole für die zusätzlichen 100 TiB Überschreitungen zum Marktpreis. Die Überschreitungsgebühren werden auf Ihrer monatlichen Rechnung erscheinen.

Storage

Unterstützte Client-Protokolle für Cloud Volumes ONTAP

Cloud Volumes ONTAP unterstützt die Clientprotokolle iSCSI, NFS, SMB, NVMe-TCP und S3.

iSCSI

iSCSI ist ein Blockprotokoll, das in Standard-Ethernet-Netzwerken ausgeführt werden kann. Die meisten Client-Betriebssysteme bieten einen Software-Initiator, der über einen Standard-Ethernet-Port läuft.

NFS

NFS ist das traditionelle Dateizugriffsprotokoll für UNIX- und LINUX-Systeme. Clients können mithilfe der Protokolle NFSv3, NFSv4 und NFSv4.1 auf Dateien in ONTAP -Volumes zugreifen. Sie können den Dateizugriff mit Berechtigungen im UNIX-Stil, Berechtigungen im NTFS-Stil oder einer Mischung aus beiden steuern.

Clients können über die Protokolle NFS und SMB auf dieselben Dateien zugreifen.

KMU

SMB ist das traditionelle Dateizugriffsprotokoll für Windows-Systeme. Clients können mithilfe der Protokolle SMB 2.0, SMB 2.1, SMB 3.0 und SMB 3.1.1 auf Dateien in ONTAP -Volumes zugreifen. Genau wie bei NFS wird eine Mischung aus Berechtigungsstilen unterstützt.

S3

Cloud Volumes ONTAP unterstützt S3 als Option für Scale-Out-Speicher. Durch die Unterstützung des S3-Protokolls können Sie den S3-Clientzugriff auf Objekte konfigurieren, die in einem Bucket in einer Speicher-VM (SVM) enthalten sind.

"ONTAP -Dokumentation: Erfahren Sie, wie S3-Multiprotokoll funktioniert" . "ONTAP Dokumentation: Erfahren Sie, wie Sie S3-Objektspeicherdienste in ONTAP konfigurieren und verwalten" .

NVMe-TCP

Ab ONTAP Version 9.12.1 wird NVMe-TCP von allen Cloud-Anbietern unterstützt. Cloud Volumes ONTAP unterstützt NVMe-TCP als Blockprotokoll für Storage VMs (SVMs) während der Bereitstellung und installiert die erforderlichen NVMe-Lizenzen automatisch.

Die NetApp Console bietet keine Verwaltungsfunktionen für NVMe-TCP.

Weitere Informationen zur Konfiguration von NVMe über ONTAP finden Sie im "ONTAP -Dokumentation: Konfigurieren einer Storage-VM für NVMe" .

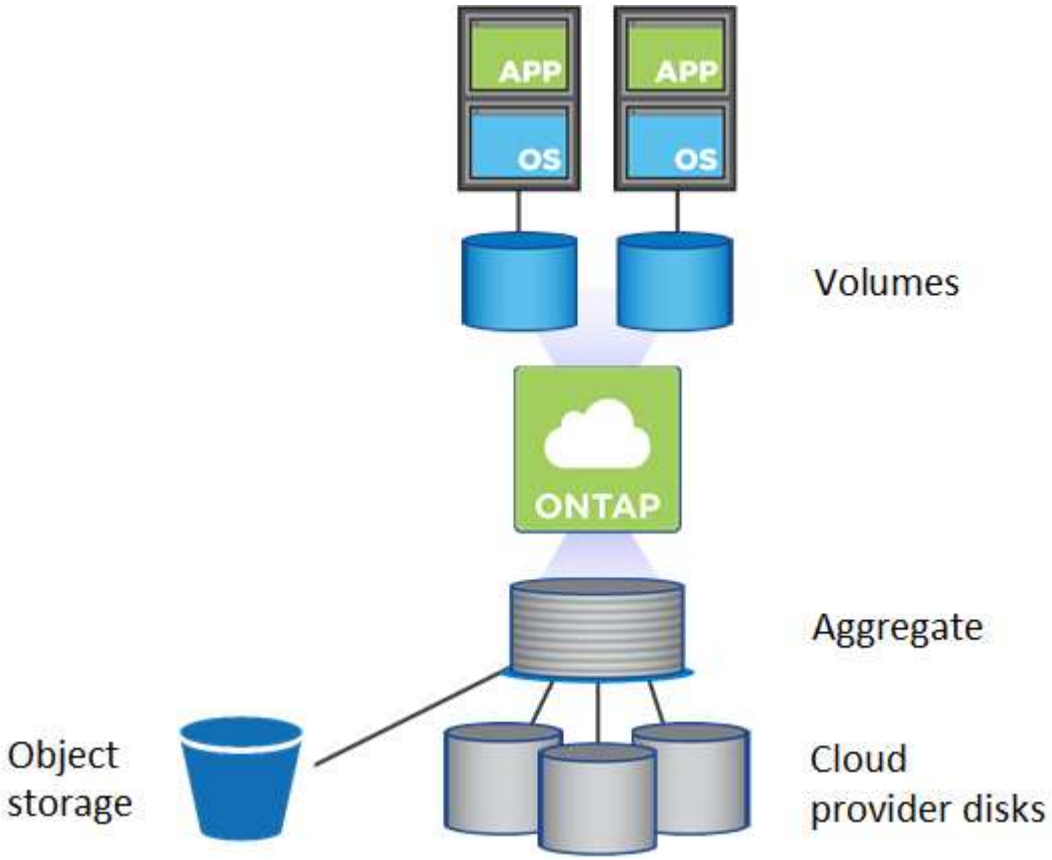
Für Cloud Volumes ONTAP -Cluster verwendete Festplatten und Aggregate

Wenn Sie verstehen, wie Cloud Volumes ONTAP Cloud-Speicher verwendet, können Sie Ihre Speicherkosten besser einschätzen.

Sie müssen alle Festplatten und Aggregate in der NetApp Console erstellen und löschen. Sie sollten diese Aktionen nicht von einem anderen Verwaltungstool aus durchführen. Dies kann die Systemstabilität beeinträchtigen, die Möglichkeit, in Zukunft Festplatten hinzuzufügen, einschränken und möglicherweise zu überflüssigen Gebühren des Cloud-Anbieters führen.

Überblick

Cloud Volumes ONTAP verwendet den Speicher des Cloud-Anbieters als Datenträger und gruppiert sie in ein oder mehrere Aggregate. Aggregate stellen Speicher für ein oder mehrere Volumes bereit.



Es werden mehrere Arten von Cloud-Festplatten unterstützt. Sie wählen den Datenträgertyp beim Erstellen eines Volumes und die Standarddatenträgergröße beim Bereitstellen von Cloud Volumes ONTAP.

Die Gesamtmenge des von einem Cloud-Anbieter erworbenen Speichers ist die *Rohkapazität*. Die *nutzbare Kapazität* ist geringer, da etwa 12 bis 14 Prozent Overhead sind, der für die Nutzung von Cloud Volumes ONTAP reserviert ist. Wenn die Konsole beispielsweise ein 500-GiB-Aggregat erstellt, beträgt die nutzbare Kapazität 442,94 GiB.

AWS-Speicher

In AWS verwendet Cloud Volumes ONTAP EBS-Speicher für Benutzerdaten und lokalen NVMe-Speicher als Flash-Cache auf einigen EC2-Instanztypen.

EBS-Speicher

In AWS kann ein Aggregat bis zu 6 Festplatten enthalten, die alle dieselbe Größe haben. Wenn Sie jedoch über eine Konfiguration verfügen, die die Funktion „Amazon EBS Elastic Volumes“ unterstützt, kann ein Aggregat bis zu 8 Festplatten enthalten. "Erfahren Sie mehr über die Unterstützung für Elastic Volumes" .

Die maximale Festplattengröße beträgt 16 TiB.

Der zugrunde liegende EBS-Festplattentyp kann entweder eine Allzweck-SSD (gp3 oder gp2), eine SSD mit bereitgestellten IOPS (io1) oder eine durchsatzoptimierte Festplatte (st1) sein. Sie können eine EBS-Festplatte mit Amazon Simple Storage Service (Amazon S3) koppeln, um "kostengünstiger Objektspeicher".

Bei Verwendung von durchsatzoptimierten HDDs (st1) wird das Tiering von Daten in Objektspeicher nicht empfohlen.

Lokaler NVMe-Speicher

Einige EC2-Instanztypen umfassen lokalen NVMe-Speicher, den Cloud Volumes ONTAP als"Flash-Cache" .

Weiterführende Links

- "AWS-Dokumentation: EBS-Volume-Typen"
- "Erfahren Sie, wie Sie Datenträgertypen und Datenträgergrößen für Ihre Systeme in AWS auswählen"
- "Überprüfen Sie die Speicherlimits für Cloud Volumes ONTAP in AWS"
- "Überprüfen Sie die unterstützten Konfigurationen für Cloud Volumes ONTAP in AWS"

Azure-Speicher

In Azure kann ein Aggregat bis zu 12 Datenträger gleicher Größe enthalten. Der Datenträgertyp und die maximale Datenträgergröße hängen davon ab, ob Sie ein Einzelknotensystem oder ein HA-Paar verwenden:

Einzelknotensysteme

Einzelknotensysteme können diese Arten von Azure Managed Disks verwenden:

- *Premium SSD Managed Disks* bieten hohe Leistung für I/O-intensive Workloads zu höheren Kosten.
- *Premium SSD v2 Managed Disks* bieten im Vergleich zu Premium SSD Managed Disks eine höhere Leistung mit geringerer Latenz zu geringeren Kosten sowohl für einzelne Knoten als auch für HA-Paare.
- *Standard-SSD-Managed Disks* bieten konsistente Leistung für Workloads, die niedrige IOPS erfordern.
- *Standard HDD Managed Disks* sind eine gute Wahl, wenn Sie keine hohen IOPS benötigen und Ihre Kosten senken möchten.

  Jeder verwaltete Datenträgertyp hat eine maximale Datenträgergröße von 32 TiB.

  Sie können einen verwalteten Datenträger mit Azure Blob Storage koppeln, um"kostengünstiger Objektspeicher" .

HA-Paare

HA-Paare verwenden zwei Arten von Festplatten, die bei höheren Kosten eine hohe Leistung für E/A-intensive Workloads bieten:

- *Premium-Seitenblobs* mit einer maximalen Festplattengröße von 8 TiB
- *Managed Disks* mit einer maximalen Diskgröße von 32 TiB

Weiterführende Links

- "Erfahren Sie, wie Sie Datenträgertypen und Datenträgergrößen für Ihre Systeme in Azure auswählen"
- "Starten Sie ein Cloud Volumes ONTAP HA-Paar in Azure"
- "Microsoft Azure-Dokumentation: Azure-verwaltete Datenträgertypen"
- "Microsoft Azure-Dokumentation: Übersicht über Azure-Seitenblobs"
- "Überprüfen Sie die Speicherlimits für Cloud Volumes ONTAP in Azure"

Google Cloud-Speicher

In Google Cloud kann ein Aggregat bis zu 6 Festplatten enthalten, die alle dieselbe Größe haben. Die maximale Festplattengröße beträgt 64 TiB.

Der Datenträgertyp kann entweder *Zonal SSD Persistent Disks*, *Zonal Balanced Persistent Disks* oder *Zonal Standard Persistent Disks* sein. Sie können persistente Festplatten mit einem Google Storage-Bucket koppeln, um"kostengünstiger Objektspeicher" .

Weiterführende Links

- "Google Cloud-Dokumentation: Speicheroptionen"
- "Überprüfen Sie die Speicherlimits für Cloud Volumes ONTAP in Google Cloud"

RAID-Typ

Der RAID-Typ für jedes Cloud Volumes ONTAP -Aggregat ist RAID0 (Striping). Cloud Volumes ONTAP verlässt sich hinsichtlich der Festplattenverfügbarkeit und -haltbarkeit auf den Cloud-Anbieter. Es werden keine anderen RAID-Typen unterstützt.

Hotspares

RAID0 unterstützt nicht die Verwendung von Hotspares zur Redundanz.

Das Erstellen ungenutzter Festplatten (Hot Spares), die an eine Cloud Volumes ONTAP Instanz angeschlossen sind, ist ein unnötiger Aufwand und kann die Bereitstellung zusätzlichen Speicherplatzes bei Bedarf verhindern. Daher wird es nicht empfohlen.

Erfahren Sie mehr über die Unterstützung für AWS Elastic Volumes mit Cloud Volumes ONTAP

Die Unterstützung der Amazon EBS Elastic Volumes-Funktion mit einem Cloud Volumes ONTAP -Aggregat bietet eine bessere Leistung und zusätzliche Kapazität und ermöglicht es der NetApp Console, die zugrunde liegende Festplattenkapazität bei Bedarf automatisch zu erhöhen.

Vorteile

- Dynamisches Festplattenwachstum

  Die Konsole kann die Größe von Festplatten dynamisch erhöhen, während Cloud Volumes ONTAP ausgeführt wird und Festplatten noch angeschlossen sind.

- Bessere Leistung

  Mit Elastic Volumes aktivierte Aggregate können bis zu acht Festplatten haben, die gleichmäßig über zwei RAID-Gruppen verteilt genutzt werden. Diese Konfiguration bietet mehr Durchsatz und konstante Leistung.

- Größere Aggregate

  Die Unterstützung von acht Festplatten bietet eine maximale Gesamtkapazität von 128 TiB. Diese Grenzwerte sind höher als die Grenzwerte von sechs Datenträgern und 96 TiB für Aggregate, die nicht mit der Funktion „Elastic Volumes“ aktiviert sind.

  Beachten Sie, dass die Gesamtkapazitätsgrenzen des Systems gleich bleiben.

"AWS-Dokumentation: Erfahren Sie mehr über Elastic Volumes von AWS"

Unterstützte Konfigurationen

Die Funktion „Amazon EBS Elastic Volumes“ wird mit bestimmten Cloud Volumes ONTAP Versionen und bestimmten EBS-Festplattentypen unterstützt.

Cloud Volumes ONTAP Version

Die Elastic Volumes-Funktion wird mit *neuen* Cloud Volumes ONTAP Systemen unterstützt, die ab Version 9.11.0 erstellt wurden. Die Funktion wird von vorhandenen Cloud Volumes ONTAP Systemen, die vor 9.11.0 bereitgestellt wurden, *nicht* unterstützt.

Beispielsweise wird die Funktion „Elastic Volumes“ nicht unterstützt, wenn Sie ein Cloud Volumes ONTAP 9.9.0-System erstellt und dieses System später auf Version 9.11.0 aktualisiert haben. Es muss sich um ein neues System handeln, das mit Version 9.11.0 oder höher bereitgestellt wird.

EBS-Festplattentypen

Die Funktion „Elastic Volumes“ wird automatisch auf aggregierter Ebene aktiviert, wenn General Purpose SSDs (gp3) oder Provisioned IOPS SSDs (io1) verwendet werden. Die Funktion „Elastic Volumes“ wird bei Aggregaten, die einen anderen Datenträgertyp verwenden, nicht unterstützt.

Erforderliche AWS-Berechtigungen

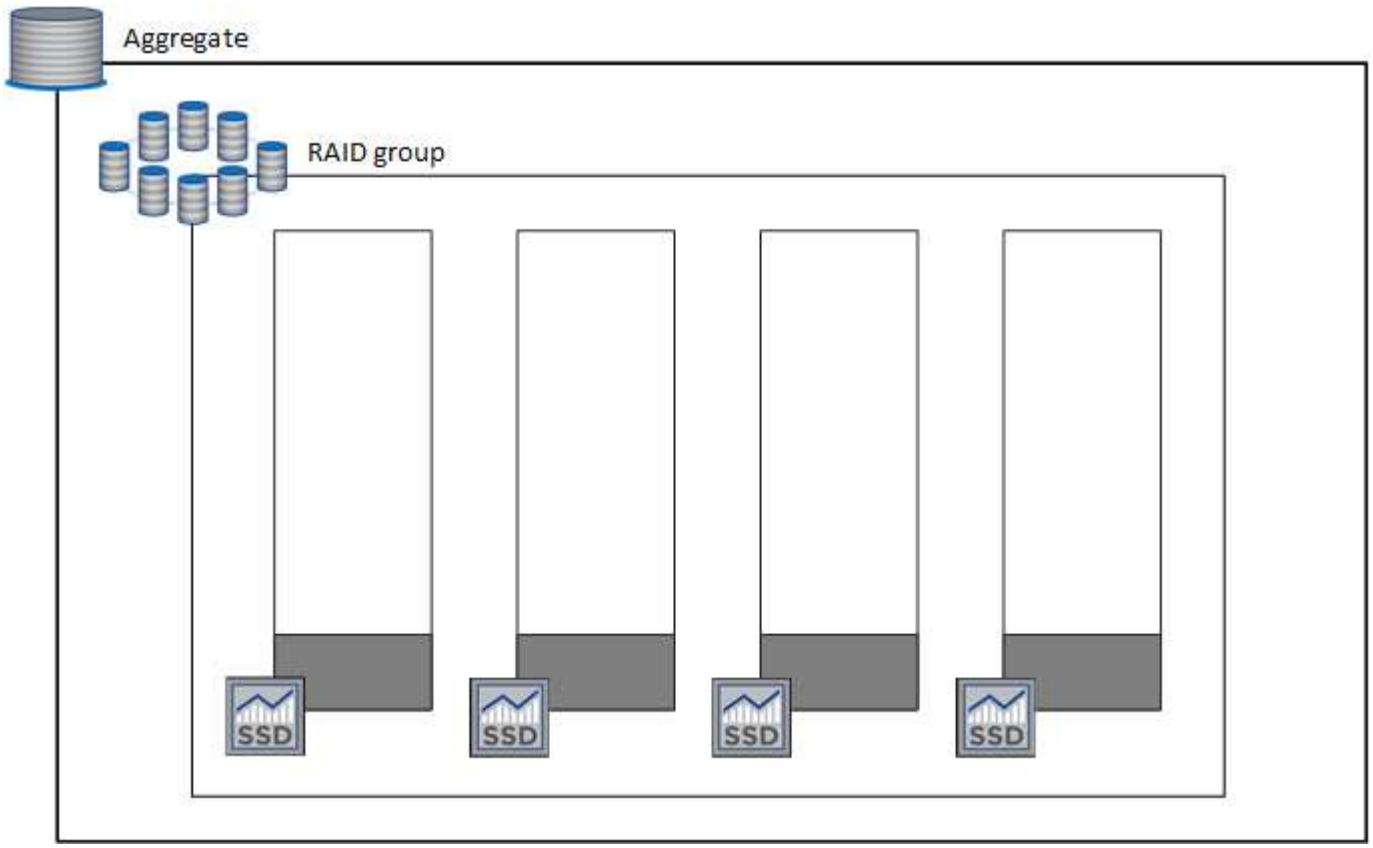
Ab der Version 3.9.19 benötigt der Konsolenagent die folgenden Berechtigungen, um die Elastic Volumes-Funktion auf einem Cloud Volumes ONTAP Aggregat zu aktivieren und zu verwalten:

- ec2:DescribeVolumesModifications
- ec2:ModifyVolume

Diese Berechtigungen sind enthalten in "die von NetApp bereitgestellten Richtlinien"

So funktioniert die Unterstützung für Elastic Volumes

Ein Aggregat mit aktivierter Elastic Volumes-Funktion besteht aus einer oder zwei RAID-Gruppen. Jede RAID-Gruppe verfügt über vier identische Festplatten mit der gleichen Kapazität. Hier ist ein Beispiel für ein 10-TiB-Aggregat mit vier Festplatten mit jeweils 2,5 TiB:



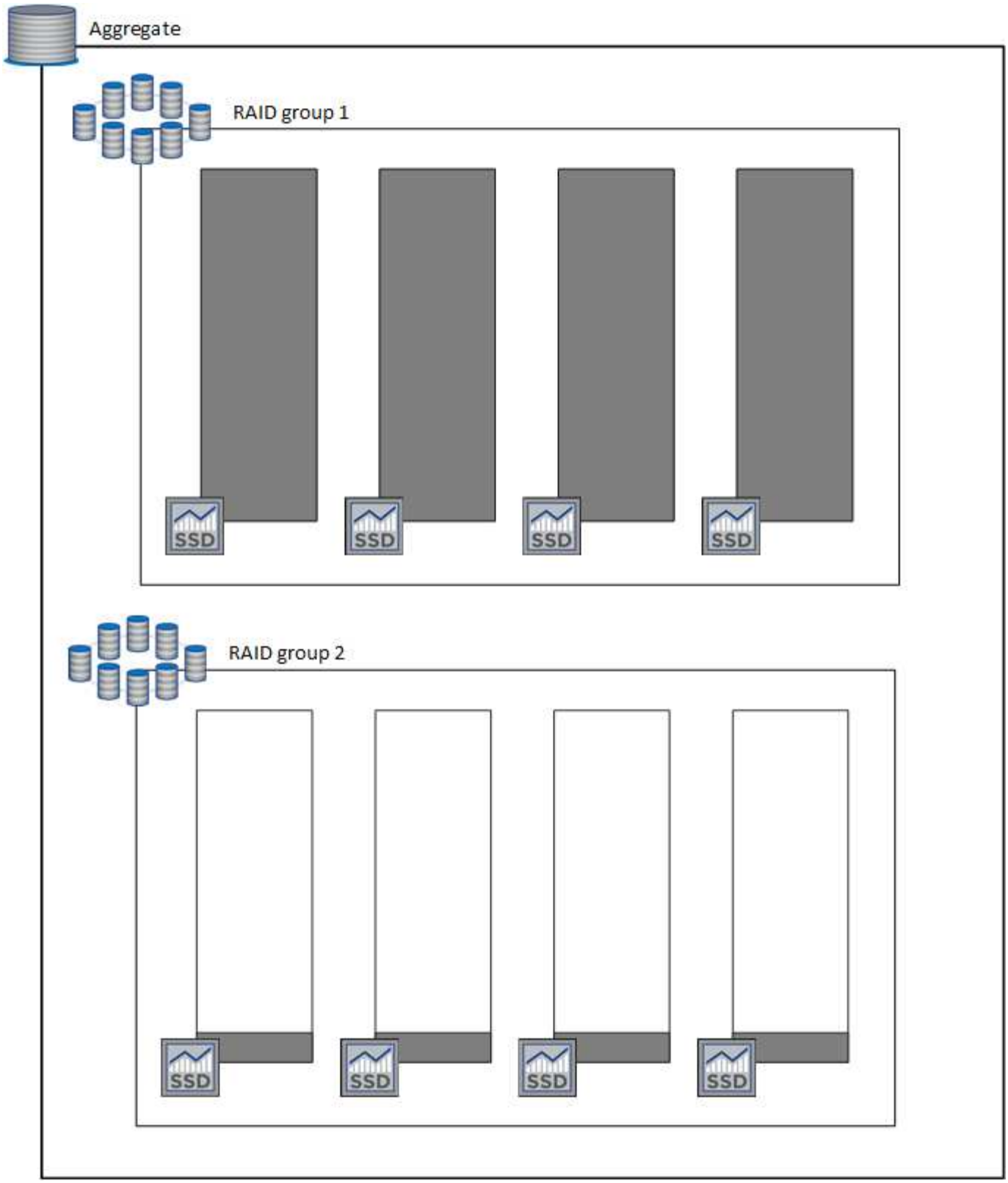
Wenn die Konsole ein Aggregat erstellt, beginnt sie mit einer RAID-Gruppe. Wenn zusätzliche Kapazität benötigt wird, wird die Gesamtkapazität vergrößert, indem die Kapazität aller Festplatten in der RAID-Gruppe um den gleichen Betrag erhöht wird. Die Kapazitätserhöhung beträgt entweder mindestens 256 GiB oder 10 % der Aggregatgröße.

Wenn Sie beispielsweise ein 1-TiB-Aggregat haben, ist jede Festplatte 250 GiB groß. 10 % der Kapazität des Aggregats betragen 100 GiB. Das ist weniger als 256 GiB, daher wird die Größe des Aggregats um das Minimum von 256 GiB (oder 64 GiB für jede Festplatte) erhöht.

Die Konsole erhöht die Größe der Festplatten, während das Cloud Volumes ONTAP -System ausgeführt wird und die Festplatten noch angeschlossen sind. Die Änderung erfolgt ohne Unterbrechung.

Wenn ein Aggregat 64 TiB (oder 16 TiB auf jeder Festplatte) erreicht, erstellt die Konsole eine zweite RAID-Gruppe für zusätzliche Kapazität. Diese zweite RAID-Gruppe funktioniert genauso wie die erste: Sie verfügt über vier Festplatten mit genau der gleichen Kapazität und kann auf bis zu 64 TiB erweitert werden. Das bedeutet, dass ein Aggregat eine maximale Kapazität von 128 TiB haben kann.

Hier ist ein Beispiel für ein Aggregat mit zwei RAID-Gruppen. Die Kapazitätsgrenze der ersten RAID-Gruppe wurde erreicht, während die Festplatten der zweiten RAID-Gruppe über reichlich freien Speicherplatz verfügen.



Was passiert, wenn Sie ein Volume erstellen?

Wenn Sie ein Volume erstellen, das gp3- oder io1-Datenträger verwendet, erstellt die Konsole das Volume auf einem Aggregat wie folgt:

- Wenn ein vorhandenes gp3- oder io1-Aggregat vorhanden ist, bei dem Elastic Volumes aktiviert sind, erstellt die Konsole das Volume auf diesem Aggregat.

- Wenn es mehrere gp3- oder io1-Aggregate gibt, bei denen Elastic Volumes aktiviert sind, erstellt die Konsole das Volume auf dem Aggregat, das die geringste Menge an Ressourcen benötigt.
- Wenn das System nur über gp3- oder io1-Aggregate verfügt, die nicht für Elastic Volumes aktiviert sind, wird das Volume auf diesem Aggregat erstellt.

  Obwohl dieses Szenario unwahrscheinlich ist, ist es in zwei Fällen möglich:

  - Sie haben die Funktion „Elastic Volumes“ beim Erstellen eines Aggregats aus der API explizit deaktiviert.
  - Sie haben über die Benutzeroberfläche ein neues Cloud Volumes ONTAP -System erstellt. In diesem Fall ist die Funktion „Elastic Volumes“ im ersten Aggregat deaktiviert. RezensionEinschränkungen unten, um mehr zu erfahren.

- Wenn keines der vorhandenen Aggregate über genügend Kapazität verfügt, erstellt die Konsole das Aggregat mit aktivierten Elastic Volumes und erstellt dann das Volume auf diesem neuen Aggregat.

  Die Größe des Aggregats richtet sich nach der gewünschten Volumengröße zuzüglich 10 % Kapazität.

Kapazitätsverwaltungsmodus

Der Kapazitätsverwaltungsmodus für einen Konsolenagenten funktioniert mit Elastic Volumes ähnlich wie mit anderen Aggregattypen:

- Wenn der automatische Modus aktiviert ist (dies ist die Standardeinstellung), erhöht die Konsole automatisch die Größe der Aggregate, wenn zusätzliche Kapazität benötigt wird.
- Wenn Sie den Kapazitätsverwaltungsmodus auf „Manuell“ ändern, fordert die Konsole Ihre Zustimmung zum Kauf zusätzlicher Kapazität an.

"Erfahren Sie mehr über den Kapazitätsverwaltungsmodus" .

Einschränkungen

Das Erhöhen der Größe eines Aggregats kann bis zu 6 Stunden dauern. Während dieser Zeit kann die Konsole keine zusätzliche Kapazität für dieses Aggregat anfordern.

So arbeiten Sie mit Elastic Volumes

Mit Elastic Volumes können Sie folgende Aufgaben ausführen:

- Erstellen Sie ein neues System, bei dem Elastic Volumes auf dem ersten Aggregat aktiviert sind, wenn Sie gp3- oder io1-Festplatten verwenden.

  "Erfahren Sie, wie Sie ein Cloud Volumes ONTAP -System erstellen"

- Erstellen Sie ein neues Volume auf einem Aggregat, für das Elastic Volumes aktiviert ist.

  Wenn Sie ein Volume erstellen, das gp3- oder io1-Datenträger verwendet, erstellt die Konsole das Volume automatisch auf einem Aggregat, für das Elastic Volumes aktiviert sind. Weitere Einzelheiten finden Sie unterwenn Sie ein Volume erstellen? .

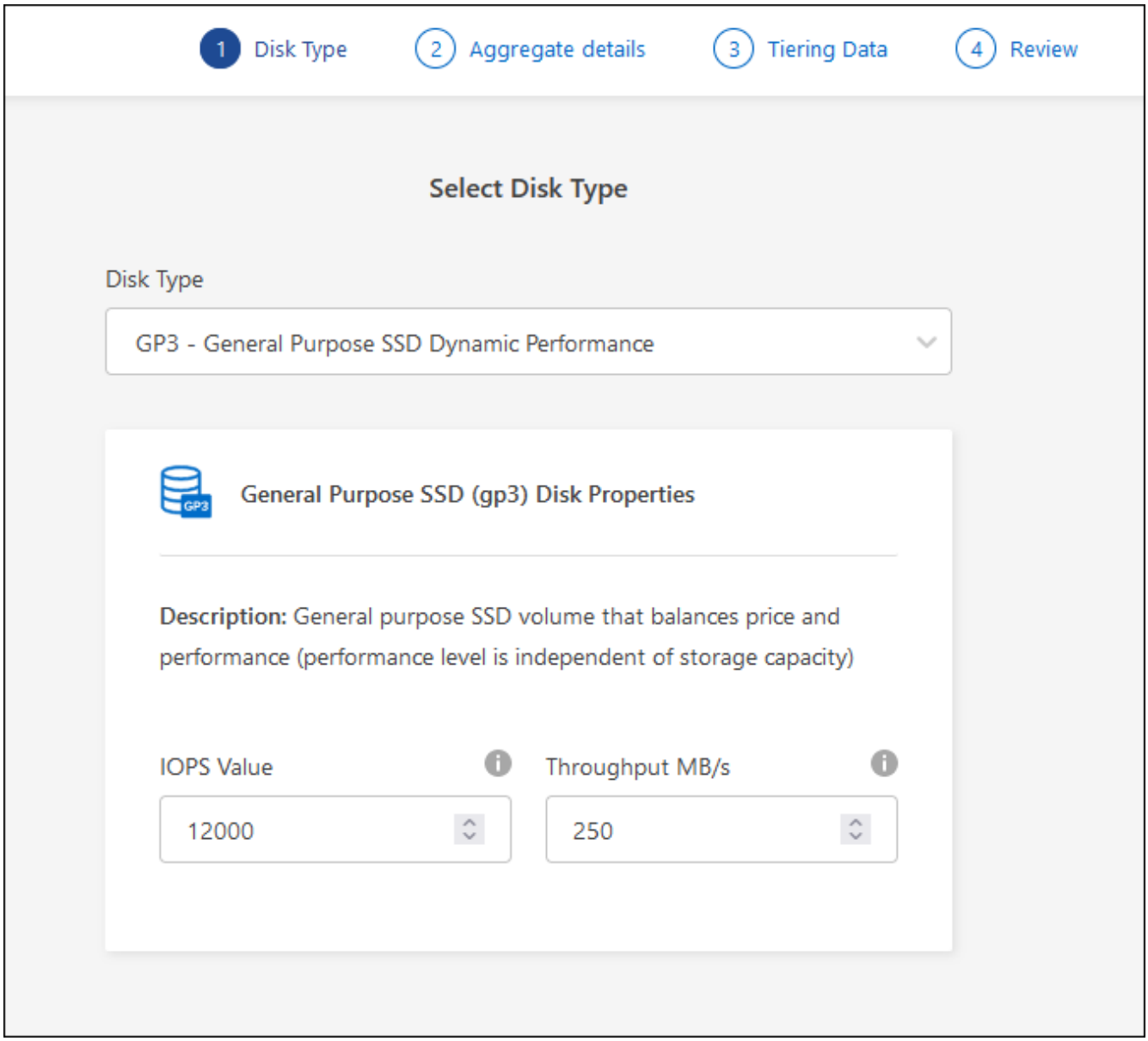
  "Erfahren Sie, wie Sie Volumes erstellen" .

- Erstellen Sie ein neues Aggregat mit aktivierten Elastic Volumes

Elastic Volumes wird automatisch auf neuen Aggregaten aktiviert, die gp3- oder io1-Festplatten verwenden, sofern das Cloud Volumes ONTAP System ab Version 9.11.0 erstellt wurde.

Wenn Sie das Aggregat erstellen, werden Sie von der Konsole aufgefordert, die Kapazitätsgröße des Aggregats anzugeben. Dies unterscheidet sich von anderen Konfigurationen, bei denen Sie eine Festplattengröße und -anzahl auswählen.

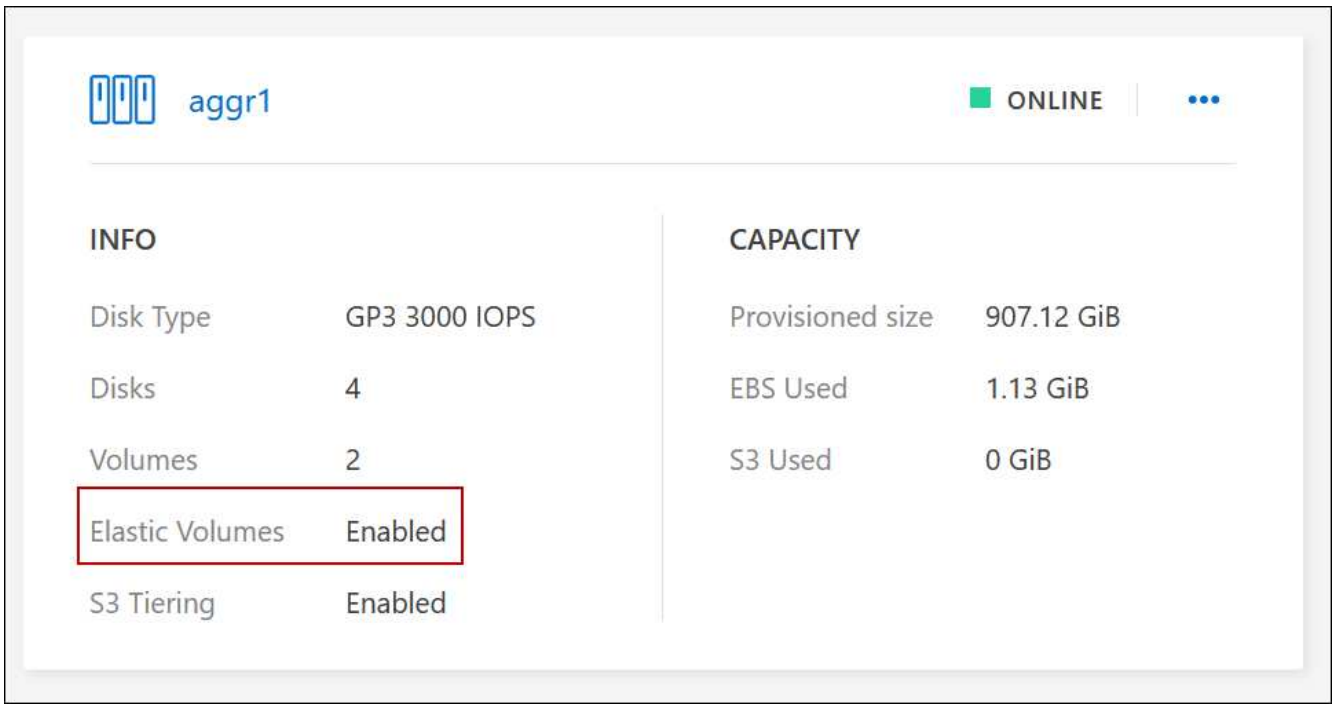
Der folgende Screenshot zeigt ein Beispiel eines neuen Aggregats, das aus GP3-Festplatten besteht.



"Erfahren Sie, wie Sie Aggregate erstellen" .

- Identifizieren Sie Aggregate, bei denen Elastic Volumes aktiviert sind

  Wenn Sie zur Seite „Erweiterte Zuordnung“ gehen, können Sie feststellen, ob die Funktion „Elastic Volumes“ auf einem Aggregat aktiviert ist. Im folgenden Beispiel sind für aggr1 Elastic Volumes aktiviert.



- Kapazität zu einem Aggregat hinzufügen

  Während die Konsole bei Bedarf automatisch Kapazität zu Aggregaten hinzufügt, können Sie die Kapazität auch manuell selbst erhöhen.

  "Erfahren Sie, wie Sie die Gesamtkapazität erhöhen" .

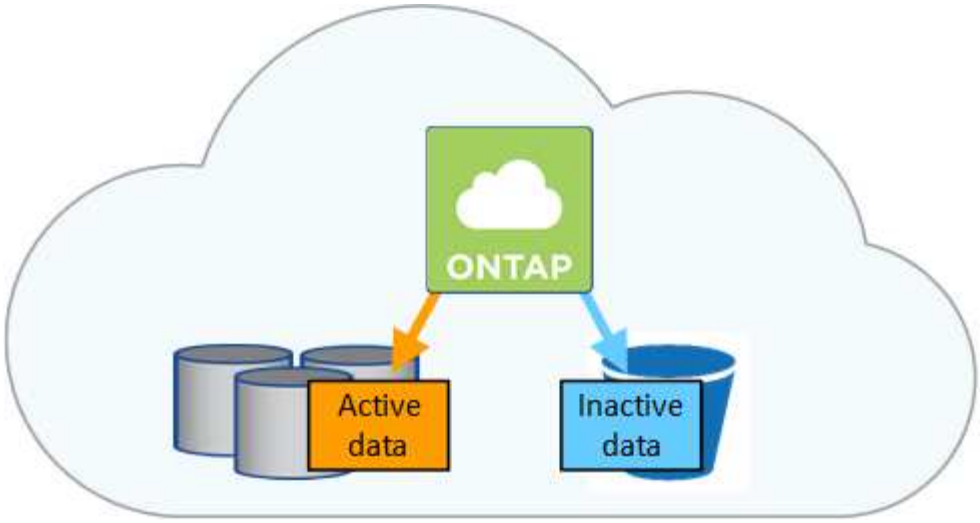
- Replizieren Sie Daten in ein Aggregat, für das Elastic Volumes aktiviert ist

  Wenn das Cloud Volumes ONTAP -Zielsystem Elastic Volumes unterstützt, wird ein Zielvolume auf einem Aggregat platziert, auf dem Elastic Volumes aktiviert sind (sofern Sie eine gp3- oder io1-Festplatte auswählen).

  "Erfahren Sie, wie Sie die Datenreplikation einrichten"

Erfahren Sie mehr über Data Tiering mit Cloud Volumes ONTAP in AWS, Azure oder Google Cloud

Reduzieren Sie Ihre Speicherkosten, indem Sie die automatische Einstufung inaktiver Daten in kostengünstigen Objektspeicher ermöglichen. Aktive Daten verbleiben auf Hochleistungs-SSDs oder -HDDs, während inaktive Daten auf kostengünstigen Objektspeicher ausgelagert werden. Dadurch können Sie Speicherplatz auf Ihrem primären Speicher zurückgewinnen und den sekundären Speicher verkleinern.



Die Datenschichtung wird durch die FabricPool -Technologie ermöglicht. Cloud Volumes ONTAP bietet Daten-Tiering für alle Cloud Volumes ONTAP Cluster ohne zusätzliche Lizenz. Wenn Sie die Datenschichtung aktivieren, fallen für die in den Objektspeicher verschobenen Daten Gebühren an. Einzelheiten zu den Kosten für die Objektspeicherung finden Sie in der Dokumentation Ihres Cloud-Anbieters.

Daten-Tiering in AWS

Wenn Sie Data Tiering in AWS aktivieren, verwendet Cloud Volumes ONTAP EBS als Performance-Tier für häufig genutzte Daten und Amazon Simple Storage Service (Amazon S3) als Kapazitäts-Tier für inaktive Daten.

Leistungsstufe

Die Leistungsstufe kann aus General Purpose SSDs (gp3 oder gp2) oder Provisioned IOPS SSDs (io1) bestehen.

Bei Verwendung von durchsatzoptimierten HDDs (st1) wird das Tiering von Daten in Objektspeicher nicht empfohlen.

Kapazitätsstufe

Ein Cloud Volumes ONTAP -System ordnet inaktive Daten einem einzelnen S3-Bucket zu.

Die NetApp Console erstellt für jedes System einen einzelnen S3-Bucket und nennt ihn Fabric-Pool-*Cluster Unique Identifier*. Es wird nicht für jedes Volume ein anderer S3-Bucket erstellt.

Wenn die Konsole den S3-Bucket erstellt, verwendet sie die folgenden Standardeinstellungen:

- Speicherklasse: Standard
- Standardverschlüsselung: Deaktiviert
- Öffentlichen Zugriff blockieren: Den gesamten öffentlichen Zugriff blockieren
- Objektbesitz: ACLs aktiviert
- Bucket-Versionierung: Deaktiviert
- Objektsperre: Deaktiviert

Speicherklassen

Die Standardspeicherklasse für mehrstufige Daten in AWS ist *Standard*. Standard ist ideal für häufig abgerufene Daten, die in mehreren Verfügbarkeitszonen gespeichert sind.

Wenn Sie nicht vorhaben, auf die inaktiven Daten zuzugreifen, können Sie Ihre Speicherkosten senken, indem Sie die Speicherklasse in eine der folgenden ändern: *Intelligent Tiering*, *One-Zone Infrequent Access*, *Standard-Infrequent Access* oder *S3 Glacier Instant Retrieval*. Wenn Sie die Speicherklasse ändern, beginnen inaktive Daten in der Standardspeicherklasse und wechseln in die von Ihnen ausgewählte Speicherklasse, wenn nach 30 Tagen nicht auf die Daten zugegriffen wird.

Wenn Sie auf die Daten zugreifen, sind die Zugriffskosten höher. Berücksichtigen Sie dies daher, bevor Sie die Speicherklasse ändern. "Amazon S3-Dokumentation: Weitere Informationen zu Amazon S3-Speicherklassen" .

Sie können beim Erstellen des Systems eine Speicherklasse auswählen und diese später jederzeit ändern. Anweisungen zum Ändern der Speicherklasse finden Sie unter"Verschieben Sie inaktive Daten in kostengünstige Objektspeicher" .

Die Speicherklasse für die Datenschichtung gilt systemweit, nicht pro Datenträger.

Datentiering in Azure

Wenn Sie das Daten-Tiering in Azure aktivieren, verwendet Cloud Volumes ONTAP Azure Managed Disks als Leistungsebene für Hot Data und Azure Blob Storage als Kapazitätsebene für inaktive Daten.

Leistungsstufe

Die Leistungsstufe kann entweder aus SSDs oder HDDs bestehen.

Kapazitätsstufe

Ein Cloud Volumes ONTAP -System ordnet inaktive Daten einem einzelnen Blob-Container zu.

Die Konsole erstellt für jedes Cloud Volumes ONTAP -System ein neues Speicherkonto mit einem Container. Der Name des Speicherkontos ist zufällig. Es wird nicht für jedes Volume ein anderer Container erstellt.

Die Konsole erstellt das Speicherkonto mit den folgenden Einstellungen:

- Zugriffsebene: Hot
- Leistung: Standard
- Redundanz: Entsprechend der Cloud Volume ONTAP -Bereitstellung
  - Einzelne Verfügbarkeitszone: Lokal redundanter Speicher (LRS)
  - Mehrere Verfügbarkeitszonen: Zonenredundanter Speicher (ZRS)
- Konto: StorageV2 (allgemeiner Zweck v2)
- Sichere Übertragung für REST-API-Operationen erforderlich: Aktiviert
- Zugriff auf Speicherkontoschlüssel: Aktiviert
- Mindestens TLS-Version: Version 1.2
- Infrastrukturverschlüsselung: Deaktiviert

Speicherzugriffsebenen

Die Standardspeicherzugriffsebene für mehrstufige Daten in Azure ist die *Hot*-Ebene. Die Hot-Tier-Ebene ist ideal für häufig abgerufene Daten in der Kapazitätsebene.

Wenn Sie nicht vorhaben, auf die inaktiven Daten in der Kapazitätsebene zuzugreifen, können Sie die *coole* Speicherebene wählen, in der die inaktiven Daten mindestens 30 Tage lang aufbewahrt werden. Sie

können sich auch für die *kalte* Stufe entscheiden, bei der die inaktiven Daten mindestens 90 Tage lang gespeichert werden. Basierend auf Ihren Speicheranforderungen und Kostenüberlegungen können Sie die Stufe auswählen, die Ihren Anforderungen am besten entspricht. Wenn Sie die Speicherebene auf *cool* oder *cold* ändern, werden die Daten der inaktiven Kapazitätsebene direkt in die Speicherebene „cool“ oder „cold“ verschoben. Die kühlen und kalten Ebenen bieten im Vergleich zur heißen Ebene geringere Speicherkosten, sind jedoch mit höheren Zugriffskosten verbunden. Berücksichtigen Sie dies, bevor Sie die Speicherebene ändern. Siehe "Microsoft Azure-Dokumentation: Weitere Informationen zu Azure Blob Storage-Zugriffsebenen" .

Sie können eine Speicherebene auswählen, wenn Sie ein Cloud Volumes ONTAP -System hinzufügen, und diese später jederzeit ändern. Einzelheiten zum Ändern der Speicherebene finden Sie unter"Verschieben Sie inaktive Daten in kostengünstige Objektspeicher" .

Die Speicherzugriffsebene für die Datenschichtung gilt systemweit und nicht pro Datenträger.

Daten-Tiering in Google Cloud

Wenn Sie das Daten-Tiering in Google Cloud aktivieren, verwendet Cloud Volumes ONTAP persistente Festplatten als Leistungsebene für Hot Data und einen Google Cloud Storage-Bucket als Kapazitätsebene für inaktive Daten.

Leistungsstufe

Die Leistungsstufe kann entweder aus persistenten SSD-Festplatten, ausgeglichenen persistenten Festplatten oder persistenten Standardfestplatten bestehen.

Kapazitätsstufe

Ein Cloud Volumes ONTAP -System verteilt inaktive Daten auf einen einzelnen Google Cloud Storage-Bucket.

Die Konsole erstellt für jedes System einen Bucket und nennt ihn fabric-pool-*cluster unique identifier*. Es wird nicht für jedes Volume ein anderer Bucket erstellt.

Wenn die Konsole den Bucket erstellt, verwendet sie die folgenden Standardeinstellungen:

- Standorttyp: Region
- Speicherklasse: Standard
- Öffentlicher Zugriff: Vorbehaltlich der Objekt-ACLs
- Zugriffskontrolle: Feinkörnig
- Schutz: Keiner
- Datenverschlüsselung: Von Google verwalteter Schlüssel

Speicherklassen

Die Standardspeicherklasse für mehrstufige Daten ist die Klasse *Standard Storage*. Bei seltenem Datenzugriff können Sie Ihre Speicherkosten durch den Wechsel zu *Nearline Storage* oder *Coldline Storage* senken. Wenn Sie die Speicherklasse ändern, werden nachfolgende inaktive Daten direkt in die von Ihnen ausgewählte Klasse verschoben.

> ⓘ Alle vorhandenen inaktiven Daten behalten die Standardspeicherklasse bei, wenn Sie die Speicherklasse ändern. Um die Speicherklasse für vorhandene inaktive Daten zu ändern, müssen Sie die Kennzeichnung manuell vornehmen.

Wenn Sie auf die Daten zugreifen, sind die Zugriffskosten höher. Berücksichtigen Sie dies, bevor Sie die

Speicherklasse ändern. Weitere Informationen finden Sie im "Google Cloud-Dokumentation: Speicherklassen" .

Sie können beim Erstellen des Systems eine Speicherebene auswählen und diese später jederzeit ändern. Einzelheiten zum Ändern der Speicherklasse finden Sie unter"Verschieben Sie inaktive Daten in kostengünstige Objektspeicher" .

Die Speicherklasse für die Datenschichtung gilt systemweit, nicht pro Datenträger.

Daten-Tiering und Kapazitätsgrenzen

Wenn Sie Data Tiering aktivieren, bleibt die Kapazitätsgrenze eines Systems gleich. Das Limit ist auf die Leistungsstufe und die Kapazitätsstufe verteilt.

Richtlinien für die Datenträgereinteilung

Um Data Tiering zu aktivieren, müssen Sie beim Erstellen, Ändern oder Replizieren eines Volumes eine Volume-Tiering-Richtlinie auswählen. Sie können für jedes Volume eine andere Richtlinie auswählen.

Einige Tiering-Richtlinien verfügen über eine zugehörige Mindestkühlperiode, die die Zeit festlegt, die Benutzerdaten in einem Volume inaktiv bleiben müssen, damit die Daten als „kalt“ betrachtet und in die Kapazitätsebene verschoben werden. Die Abkühlphase beginnt, wenn Daten in das Aggregat geschrieben werden.

Sie können die Mindestkühlperiode und den Standard-Gesamtschwellenwert von 50 % ändern (mehr dazu weiter unten). "Erfahren Sie, wie Sie die Kühlperiode ändern" Und "Erfahren Sie, wie Sie den Schwellenwert ändern" .

Die Konsole ermöglicht Ihnen beim Erstellen oder Ändern eines Volumes die Auswahl aus den folgenden Volume-Tiering-Richtlinien:

Nur Schnappschuss

Nachdem ein Aggregat 50 % seiner Kapazität erreicht hat, verschiebt Cloud Volumes ONTAP kalte Benutzerdaten von Snapshot-Kopien, die nicht mit dem aktiven Dateisystem verknüpft sind, in die Kapazitätsebene. Die Abkühlzeit beträgt ca. 2 Tage.

Beim Lesen werden kalte Datenblöcke auf der Kapazitätsebene zu heißen Datenblöcken und werden auf die Leistungsebene verschoben.

Alle

Alle Daten (ohne Metadaten) werden sofort als „kalt“ markiert und so schnell wie möglich in den Objektspeicher verschoben. Es ist nicht erforderlich, 48 Stunden zu warten, bis neue Blöcke in einem Volume kalt werden. Beachten Sie, dass Blöcke, die sich vor dem Festlegen der Richtlinie „Alle“ im Volume befanden, 48 Stunden benötigen, um kalt zu werden.

Beim Lesen bleiben kalte Datenblöcke auf der Cloud-Ebene kalt und werden nicht auf die Leistungsebene zurückgeschrieben. Diese Richtlinie ist ab ONTAP 9.6 verfügbar.

Automatisch

Nachdem ein Aggregat 50 % seiner Kapazität erreicht hat, ordnet Cloud Volumes ONTAP kalte Datenblöcke in einem Volume einer Kapazitätsebene zu. Zu den kalten Daten gehören nicht nur Snapshot-Kopien, sondern auch kalte Benutzerdaten aus dem aktiven Dateisystem. Die Kühlperiode beträgt ca. 31 Tage.

Diese Richtlinie wird ab Cloud Volumes ONTAP 9.4 unterstützt.

Beim Lesen durch zufällige Lesevorgänge werden die kalten Datenblöcke in der Kapazitätsebene heiß und werden in die Leistungsebene verschoben. Beim Lesen durch sequenzielle Lesevorgänge, wie sie beispielsweise bei Index- und Antivirenscans auftreten, bleiben die kalten Datenblöcke kalt und werden nicht in die Leistungsebene verschoben.

Keine

Behält die Daten eines Volumes in der Leistungsstufe und verhindert, dass sie in die Kapazitätsstufe verschoben werden.

Replikation

Wenn Sie ein Volume replizieren, können Sie wählen, ob die Daten in den Objektspeicher verschoben werden sollen. Wenn Sie dies tun, wendet die Konsole die **Backup**-Richtlinie auf das Datensicherungsvolume an. Ab Cloud Volumes ONTAP 9.6 ersetzt die Tiering-Richtlinie **All** die Sicherungsrichtlinie. Wenn eine Replikationsbeziehung gelöscht wird, behält das Zielvolume die Tiering-Richtlinie bei, die während der Replikation gültig war.

Das Ausschalten von Cloud Volumes ONTAP wirkt sich auf die Abkühlphase aus

Datenblöcke werden durch Kühlscans gekühlt. Bei diesem Vorgang wird die Blocktemperatur nicht verwendeter Blöcke auf den nächstniedrigeren Wert verschoben (abgekühlt). Die standardmäßige Abkühlzeit hängt von der Volume-Tiering-Richtlinie ab:

- Auto: 31 Tage
- Nur Schnappschuss: 2 Tage

Damit der Kühlungsscan funktioniert, muss Cloud Volumes ONTAP ausgeführt werden. Wenn Cloud Volumes ONTAP ausgeschaltet wird, wird auch die Kühlung gestoppt. Dadurch kann es zu längeren Abkühlzeiten kommen.

Wenn Cloud Volumes ONTAP ausgeschaltet ist, bleibt die Temperatur jedes Blocks erhalten, bis Sie das System neu starten. Wenn beispielsweise die Temperatur eines Blocks beim Ausschalten des Systems 5 beträgt, beträgt die Temperatur auch beim erneuten Einschalten des Systems noch immer 5.

Einrichten von Daten-Tiering

Anweisungen und eine Liste der unterstützten Konfigurationen finden Sie unter"Verschieben Sie inaktive Daten in kostengünstige Objektspeicher" .

Cloud Volumes ONTAP -Speicherverwaltung

Die NetApp Console bietet eine vereinfachte und erweiterte Verwaltung des Cloud Volumes ONTAP Speichers.

Sie müssen alle Datenträger und Aggregate direkt von der Konsole aus erstellen und löschen. Sie sollten diese Aktionen nicht von einem anderen Verwaltungstool aus durchführen. Dies kann die Systemstabilität beeinträchtigen, die Möglichkeit, in Zukunft Festplatten hinzuzufügen, einschränken und möglicherweise zu überflüssigen Gebühren des Cloud-Anbieters führen.

Speicherbereitstellung

Die Konsole vereinfacht die Speicherbereitstellung für Cloud Volumes ONTAP, indem sie Festplatten kauft und Aggregate für Sie verwaltet. Sie müssen nur Volumes erstellen. Sie können eine erweiterte Zuordnungsoption verwenden, um Aggregate selbst bereitzustellen, wenn Sie möchten.

Vereinfachte Bereitstellung

Aggregate stellen Cloud-Speicher für Volumes bereit. Die Konsole erstellt Aggregate für Sie, wenn Sie eine Instanz starten und zusätzliche Volumes bereitstellen.

Wenn Sie ein Volume erstellen, führt die Konsole eine von drei Aktionen aus:

- Es platziert das Volume auf einem vorhandenen Aggregat, das über ausreichend freien Speicherplatz verfügt.
- Es platziert das Volume auf einem vorhandenen Aggregat, indem es weitere Festplatten für dieses Aggregat kauft.

+ Im Fall eines Aggregats in AWS, das Elastic Volumes unterstützt, erhöht es auch die Größe der Festplatten in einer RAID-Gruppe. "Erfahren Sie mehr über die Unterstützung für Elastic Volumes" .

- Es kauft Festplatten für ein neues Aggregat und platziert das Volume auf diesem Aggregat.

Die Konsole ermittelt anhand mehrerer Faktoren, wo ein neues Volume platziert werden soll: der maximalen Größe eines Aggregats, der Aktivierung von Thin Provisioning und den Schwellenwerten für den freien Speicherplatz von Aggregaten.

Auswahl der Datenträgergröße für Aggregate in AWS

Wenn die Konsole neue Aggregate für Cloud Volumes ONTAP in AWS erstellt, erhöht sie die Festplattengrößen schrittweise mit zunehmender Anzahl der Aggregate, um die Systemkapazität zu maximieren, bevor die AWS-Datenfestplattenlimits erreicht werden.

Beispielsweise kann die Konsole die folgenden Datenträgergrößen auswählen:

Gesamtzahl	Festplattengröße	Maximale Gesamtkapazität
1	500 GiB	3 TiB
4	1 TiB	6 TiB
6	2 TiB	12 TiB

Dieses Verhalten gilt nicht für Aggregate, die die Funktion „Amazon EBS Elastic Volumes“ unterstützen. Aggregate mit aktivierten Elastic Volumes bestehen aus einer oder zwei RAID-Gruppen. Jede RAID-Gruppe verfügt über vier identische Festplatten mit der gleichen Kapazität. "Erfahren Sie mehr über die Unterstützung für Elastic Volumes" .

Sie können die Festplattengröße mithilfe der erweiterten Zuordnungsoption selbst auswählen.

Erweiterte Zuordnung

Sie können auch Aggregate verwalten. "Von der Seite **Erweiterte Zuordnung**" können Sie neue Aggregate erstellen, die eine bestimmte Anzahl von Datenträgern enthalten, Datenträger zu einem vorhandenen Aggregat hinzufügen und Volumes in bestimmten Aggregaten erstellen.

Kapazitätsmanagement

Der Organisations- oder Kontoadministrator kann die Konsole so konfigurieren, dass Sie über Entscheidungen zur Speicherkapazität benachrichtigt werden oder ob die Kapazitätsanforderungen automatisch für Sie verwaltet werden sollen.

Dieses Verhalten wird durch den *Kapazitätsverwaltungsmodus* auf einem Konsolenagenten bestimmt. Der Kapazitätsverwaltungsmodus wirkt sich auf alle Cloud Volumes ONTAP Systeme aus, die von diesem Konsolenagenten verwaltet werden. Wenn Sie einen anderen Konsolenagenten haben, kann dieser anders konfiguriert werden.

Automatisches Kapazitätsmanagement

Der Kapazitätsverwaltungsmodus ist standardmäßig auf „Automatisch“ eingestellt. In diesem Modus überprüft die Konsole alle 15 Minuten das Verhältnis des freien Speicherplatzes, um festzustellen, ob das Verhältnis des freien Speicherplatzes unter den angegebenen Schwellenwert fällt. Wenn mehr Kapazität benötigt wird, leitet es den Kauf neuer Festplatten ein, löscht nicht verwendete Festplattensammlungen (Aggregate), verschiebt Volumes nach Bedarf zwischen Aggregaten und versucht, Festplattenausfälle zu verhindern.

Die folgenden Beispiele veranschaulichen die Funktionsweise dieses Modus:

- Wenn ein Aggregat die Kapazitätsschwelle erreicht und Platz für weitere Festplatten hat, kauft die Konsole automatisch neue Festplatten für dieses Aggregat, damit die Volumes weiter wachsen können.

Im Fall eines Aggregats in AWS, das Elastic Volumes unterstützt, erhöht es auch die Größe der Festplatten in einer RAID-Gruppe. "Erfahren Sie mehr über die Unterstützung für Elastic Volumes" .

+ * Wenn ein Aggregat die Kapazitätsschwelle erreicht und keine zusätzlichen Festplatten unterstützen kann, verschiebt die Konsole automatisch ein Volume von diesem Aggregat zu einem Aggregat mit verfügbarer Kapazität oder zu einem neuen Aggregat.

+ Wenn die Konsole ein neues Aggregat für das Volume erstellt, wählt sie eine Datenträgergröße, die der Größe dieses Volumes entspricht.

+ Beachten Sie, dass jetzt auf dem ursprünglichen Aggregat freier Speicherplatz verfügbar ist. Dieser Speicherplatz kann von vorhandenen oder neuen Volumes genutzt werden. In diesem Szenario kann der Speicherplatz nicht an den Cloud-Anbieter zurückgegeben werden.

- Wenn ein Aggregat länger als 12 Stunden keine Volumes enthält, wird es von der Konsole gelöscht.

Verwaltung von LUNs mit automatischer Kapazitätsverwaltung

Die automatische Kapazitätsverwaltung der Konsole gilt nicht für LUNs. Beim Erstellen einer LUN wird die Autogrow-Funktion deaktiviert.

Manuelles Kapazitätsmanagement

Wenn der Organisations- oder Kontoadministrator den **Kapazitätsverwaltungsmodus** auf manuell einstellt, werden Sie von der Konsole aufgefordert, geeignete Maßnahmen für Kapazitätsentscheidungen zu ergreifen. Für den manuellen Modus gelten die gleichen Beispiele wie für den automatischen Modus, aber es liegt an Ihnen, die Aktionen zu akzeptieren.

Mehr erfahren

"Erfahren Sie, wie Sie den Kapazitätsverwaltungsmodus ändern" .

Schreibgeschwindigkeit

Mit der NetApp Console können Sie für die meisten Cloud Volumes ONTAP Konfigurationen zwischen normaler oder hoher Schreibgeschwindigkeit wählen. Bevor Sie eine Schreibgeschwindigkeit auswählen, sollten Sie die Unterschiede zwischen den normalen und hohen Einstellungen sowie die Risiken und Empfehlungen bei der Verwendung einer hohen Schreibgeschwindigkeit verstehen.

Normale Schreibgeschwindigkeit

Wenn Sie die normale Schreibgeschwindigkeit wählen, werden die Daten direkt auf die Festplatte geschrieben. Wenn Daten direkt auf die Festplatte geschrieben werden, verringert sich die Wahrscheinlichkeit eines Datenverlusts im Falle eines ungeplanten Systemausfalls oder eines kaskadierenden Fehlers mit einem ungeplanten Systemausfall (nur HA-Paare).

Die normale Schreibgeschwindigkeit ist die Standardoption.

Hohe Schreibgeschwindigkeit

Wenn Sie eine hohe Schreibgeschwindigkeit wählen, werden die Daten im Speicher gepuffert, bevor sie auf die Festplatte geschrieben werden, was eine schnellere Schreibleistung ermöglicht. Aufgrund dieses Cachings besteht die Möglichkeit eines Datenverlusts, wenn es zu einem ungeplanten Systemausfall kommt.

Die Datenmenge, die bei einem ungeplanten Systemausfall verloren gehen kann, entspricht der Spanne der letzten beiden Konsistenzpunkte. Ein Konsistenzpunkt ist der Vorgang des Schreibens gepufferter Daten auf die Festplatte. Ein Konsistenzpunkt tritt auf, wenn das Schreibprotokoll voll ist oder nach 10 Sekunden (je nachdem, was zuerst eintritt). Die Leistung des von Ihrem Cloud-Anbieter bereitgestellten Speichers kann sich jedoch auf die Verarbeitungszeit des Konsistenzpunkts auswirken.

Wann sollte eine hohe Schreibgeschwindigkeit verwendet werden?

Eine hohe Schreibgeschwindigkeit ist eine gute Wahl, wenn für Ihre Arbeitslast eine schnelle Schreibleistung erforderlich ist und Sie das Risiko eines Datenverlusts im Falle eines ungeplanten Systemausfalls oder eines kaskadierenden Fehlers mit einem ungeplanten Systemausfall (nur HA-Paare) verkraften können.

Empfehlungen bei Verwendung hoher Schreibgeschwindigkeit

Wenn Sie eine hohe Schreibgeschwindigkeit aktivieren, sollten Sie den Schreibschutz auf Anwendungsebene sicherstellen oder sicherstellen, dass die Anwendungen einen Datenverlust tolerieren können, falls dieser auftritt.

Hohe Schreibgeschwindigkeit mit einem HA-Paar in AWS

Wenn Sie eine hohe Schreibgeschwindigkeit auf einem HA-Paar in AWS aktivieren möchten, sollten Sie den Unterschied in den Schutzstufen zwischen einer Bereitstellung mit mehreren Availability Zones (AZ) und einer Bereitstellung mit einer einzelnen AZ verstehen. Die Bereitstellung eines HA-Paares über mehrere AZs hinweg bietet mehr Ausfallsicherheit und kann dazu beitragen, das Risiko eines Datenverlusts zu verringern.

"Erfahren Sie mehr über HA-Paare in AWS" .

Konfigurationen, die eine hohe Schreibgeschwindigkeit unterstützen

Nicht alle Cloud Volumes ONTAP -Konfigurationen unterstützen eine hohe Schreibgeschwindigkeit. Diese Konfigurationen verwenden standardmäßig die normale Schreibgeschwindigkeit.

AWS

Wenn Sie ein Einzelknotensystem verwenden, unterstützt Cloud Volumes ONTAP hohe Schreibgeschwindigkeiten bei allen Instanztypen.

Ab der Version 9.8 unterstützt Cloud Volumes ONTAP eine hohe Schreibgeschwindigkeit mit HA-Paaren bei Verwendung fast aller unterstützten EC2-Instanztypen, mit Ausnahme von m5.xlarge und r5.xlarge.

"Erfahren Sie mehr über die von Cloud Volumes ONTAP unterstützten Amazon EC2-Instanzen" .

Azurblau

Wenn Sie ein Einzelknotensystem verwenden, unterstützt Cloud Volumes ONTAP hohe Schreibgeschwindigkeiten mit allen VM-Typen.

Wenn Sie ein HA-Paar verwenden, unterstützt Cloud Volumes ONTAP ab der Version 9.8 eine hohe Schreibgeschwindigkeit mit mehreren VM-Typen. Gehen Sie zum "Versionshinweise zu Cloud Volumes ONTAP" um die VM-Typen anzuzeigen, die eine hohe Schreibgeschwindigkeit unterstützen.

Google Cloud

Wenn Sie ein Einzelknotensystem verwenden, unterstützt Cloud Volumes ONTAP hohe Schreibgeschwindigkeiten mit allen Maschinentypen.

Wenn Sie ein HA-Paar verwenden, unterstützt Cloud Volumes ONTAP ab der Version 9.13.0 eine hohe Schreibgeschwindigkeit mit mehreren VM-Typen. Gehen Sie zum "Versionshinweise zu Cloud Volumes ONTAP" um die VM-Typen anzuzeigen, die eine hohe Schreibgeschwindigkeit unterstützen.

"Erfahren Sie mehr über die von Cloud Volumes ONTAP unterstützten Google Cloud-Maschinentypen" .

So wählen Sie eine Schreibgeschwindigkeit aus

Sie können eine Schreibgeschwindigkeit wählen, wenn Sie ein neues Cloud Volumes ONTAP System hinzufügen und Sie können"Ändern Sie die Schreibgeschwindigkeit für ein vorhandenes System" .

Was ist bei Datenverlust zu erwarten?

Kommt es aufgrund hoher Schreibgeschwindigkeit zu Datenverlust, meldet das Event Management System (EMS) die folgenden zwei Ereignisse:

- Cloud Volumes ONTAP 9.12.1 oder höher

```
 NOTICE nv.data.loss.possible: An unexpected shutdown occurred while in
high write speed mode, which possibly caused a loss of data.
* Cloud Volumes ONTAP 9.11.0 bis 9.11.1
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown with High Write Speed mode"
```

```
 ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect..
* Cloud Volumes ONTAP 9.8 bis 9.10.1
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown"
```

```
ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect.
```

In diesem Fall sollte Cloud Volumes ONTAP in der Lage sein, hochzufahren und ohne Benutzereingriff weiterhin Daten bereitzustellen.

So stoppen Sie den Datenzugriff bei Datenverlust

Wenn Sie sich Sorgen über Datenverlust machen und möchten, dass die Anwendungen bei Datenverlust nicht mehr ausgeführt werden und der Datenzugriff nach der ordnungsgemäßen Behebung des Datenverlustproblems wieder aufgenommen wird, können Sie dieses Ziel mit der Option NVFAIL der CLI erreichen.

So aktivieren Sie die NVFAIL-Option

```
vol modify -volume <vol-name> -nvfail on
```

So überprüfen Sie die NVFAIL-Einstellungen

```
vol show -volume <vol-name> -fields nvfail
```

So deaktivieren Sie die NVFAIL-Option

```
vol modify -volume <vol-name> -nvfail off
```

Wenn ein Datenverlust auftritt, sollte ein NFS- oder iSCSI-Volume mit aktiviertem NVFAIL die Bereitstellung von Daten einstellen (CIFS, ein zustandsloses Protokoll, hat keine Auswirkungen). Weitere Einzelheiten finden Sie unter "Auswirkungen von NVFAIL auf den Zugriff auf NFS-Volumes oder LUNs" .

So überprüfen Sie den NVFAIL-Status

```
vol show -fields in-nvfailed-state
```

Nachdem das Problem des Datenverlusts ordnungsgemäß behoben wurde, können Sie den NVFAIL-Status löschen und das Volume ist für den Datenzugriff verfügbar.

So löschen Sie den NVFAIL-Status

```
vol modify -volume <vol-name> -in-nvfailed-state false
```

Flash-Cache

Einige Cloud Volumes ONTAP -Konfigurationen umfassen lokalen NVMe-Speicher, den Cloud Volumes ONTAP für eine bessere Leistung als *Flash Cache* verwendet.

Was ist Flash Cache?

Flash Cache beschleunigt den Datenzugriff durch intelligentes Echtzeit-Caching kürzlich gelesener Benutzerdaten und NetApp Metadaten. Es eignet sich für Workloads mit vielen zufälligen Lesevorgängen, darunter Datenbanken, E-Mail und Dateidienste.

Unterstützte Konfigurationen

Flash Cache wird mit bestimmten Cloud Volumes ONTAP -Konfigurationen unterstützt. Unterstützte Konfigurationen anzeigen in der "Versionshinweise zu Cloud Volumes ONTAP"

Einschränkungen

- Beim Konfigurieren von Flash Cache für Cloud Volumes ONTAP 9.12.0 oder früher in AWS muss die Komprimierung auf allen Volumes deaktiviert werden, um die Leistungsverbesserungen von Flash Cache nutzen zu können. Wenn Sie Cloud Volumes ONTAP 9.12.1 oder höher bereitstellen oder ein Upgrade darauf durchführen, müssen Sie die Komprimierung nicht deaktivieren.

  Überspringen Sie die Auswahl der Speichereffizienzeinstellungen, wenn Sie ein Volume über die NetApp Console erstellen, oder erstellen Sie ein Volume und dann "Deaktivieren Sie die Datenkomprimierung mithilfe der CLI" .

- Das erneute Aufwärmen des Caches nach einem Neustart wird von Cloud Volumes ONTAP nicht unterstützt.

Verwandte Themen

- "Unterstützte Konfigurationen für Cloud Volumes ONTAP in AWS"
- "Unterstützte Konfigurationen für Cloud Volumes ONTAP in Azure"
- "Unterstützte Konfigurationen für Cloud Volumes ONTAP in Google Cloud"

Erfahren Sie mehr über WORM-Speicher auf Cloud Volumes ONTAP

Sie können den WORM-Speicher (Write Once, Read Many) auf einem Cloud Volumes ONTAP System aktivieren, um Dateien für einen angegebenen Aufbewahrungszeitraum unverändert aufzubewahren. Der Cloud-WORM-Speicher basiert auf der SnapLock -Technologie, was bedeutet, dass WORM-Dateien auf Dateiebene geschützt sind.

Die WORM-Funktion steht für die Verwendung mit BYOL-Lizenzen (Bring Your Own License) und Marktplatzabonnements für Ihre Lizenzen ohne zusätzliche Kosten zur Verfügung. Wenden Sie sich an Ihren NetApp -Vertriebsmitarbeiter, um WORM zu Ihrer aktuellen Lizenz hinzuzufügen.

So funktioniert WORM-Speicher

Sobald eine Datei im WORM-Speicher abgelegt wurde, kann sie nicht mehr geändert werden, auch nicht nach Ablauf der Aufbewahrungsfrist. Eine manipulationssichere Uhr stellt fest, wann die Aufbewahrungsfrist für eine WORM-Datei abgelaufen ist.

Nach Ablauf der Aufbewahrungsfrist sind Sie für die Löschung nicht mehr benötigter Dateien verantwortlich.

WORM-Speicher aktivieren

Wie Sie WORM-Speicher aktivieren, hängt von der von Ihnen verwendeten Cloud Volumes ONTAP Version ab.

Version 9.10.1 und höher

Ab Cloud Volumes ONTAP 9.10.1 haben Sie die Möglichkeit, WORM auf Volume-Ebene zu aktivieren oder zu deaktivieren.

Wenn Sie ein Cloud Volumes ONTAP -System hinzufügen, werden Sie aufgefordert, den WORM-Speicher zu aktivieren oder zu deaktivieren:

- Wenn Sie beim Hinzufügen eines Systems den WORM-Speicher aktivieren, ist WORM für jedes Volume aktiviert, das Sie über die NetApp Console erstellen. Sie können jedoch den ONTAP System Manager oder die ONTAP CLI verwenden, um Volumes zu erstellen, bei denen WORM deaktiviert ist.
- Wenn Sie den WORM-Speicher beim Hinzufügen eines Systems deaktivieren, ist WORM für jedes Volume deaktiviert, das Sie über die Konsole, den ONTAP System Manager oder die ONTAP CLI erstellen.

Version 9.10.0 und früher

Sie können WORM-Speicher auf einem Cloud Volumes ONTAP -System aktivieren, wenn Sie ein neues System hinzufügen. Für jedes Volume, das Sie über die Konsole erstellen, ist WORM aktiviert. Sie können den WORM-Speicher auf einzelnen Volumes nicht deaktivieren.

Dateien an WORM übergeben

Sie können eine Anwendung verwenden, um Dateien über NFS oder CIFS an WORM zu übergeben, oder die ONTAP CLI verwenden, um Dateien automatisch an WORM zu übergeben. Sie können auch eine WORM-Anfügedatei verwenden, um inkrementell geschriebene Daten wie Protokollinformationen aufzubewahren.

Nachdem Sie den WORM-Speicher auf einem Cloud Volumes ONTAP System aktiviert haben, müssen Sie die ONTAP CLI für die gesamte Verwaltung des WORM-Speichers verwenden. Anweisungen hierzu finden Sie im "ONTAP -Dokumentation zu SnapLock" .

Aktivieren von WORM auf einem Cloud Volumes ONTAP System

Sie können den WORM-Speicher aktivieren, wenn Sie ein Cloud Volumes ONTAP -System auf der Konsole erstellen. Sie können WORM auf einem System auch aktivieren, wenn WORM während der Erstellung nicht darauf aktiviert wurde. Nachdem Sie es aktiviert haben, können Sie WORM nicht mehr deaktivieren.

Informationen zu diesem Vorgang

- WORM wird auf ONTAP 9.10.1 und höher unterstützt.
- WORM mit Backup wird auf ONTAP 9.11.1 und höher unterstützt.

Schritte

1. Doppelklicken Sie auf der Seite **Systeme** auf den Namen des Systems, auf dem Sie WORM aktivieren möchten.
2. Klicken Sie auf der Registerkarte „Übersicht“ auf den Bereich „Funktionen“ und dann auf das Stiftsymbol neben **WORM**.

   Wenn WORM auf dem System bereits aktiviert ist, ist das Bleistiftsymbol deaktiviert.

3. Legen Sie auf der Seite **WORM** den Aufbewahrungszeitraum für die Cluster-Compliance-Clock fest.

   Weitere Informationen finden Sie im "ONTAP -Dokumentation: Initialisieren der Compliance Clock" .

4. Klicken Sie auf **Festlegen**.

Nach Abschluss

Sie können den Status von **WORM** im Bereich „Funktionen“ überprüfen. Nachdem WORM aktiviert wurde, wird die SnapLock -Lizenz automatisch auf dem Cluster installiert. Sie können die SnapLock -Lizenz im ONTAP System Manager anzeigen.

Löschen von WORM-Dateien

Sie können WORM-Dateien während der Aufbewahrungsfrist mithilfe der Funktion zum privilegierten Löschen löschen.

Anweisungen hierzu finden Sie im "ONTAP-Dokumentation" .

WORM und Daten-Tiering

Wenn Sie ein neues Cloud Volumes ONTAP 9.8-System oder höher erstellen, können Sie sowohl Data Tiering als auch WORM-Speicher zusammen aktivieren. Durch die Aktivierung der Datenschichtung mit WORM-Speicher können Sie die Daten in einem Objektspeicher in der Cloud schichten.

Sie sollten Folgendes über die Aktivierung von Daten-Tiering und WORM-Speicher wissen:

- Daten, die in den Objektspeicher eingelagert sind, umfassen nicht die ONTAP WORM-Funktionalität. Um die End-to-End-WORM-Fähigkeit sicherzustellen, müssen Sie die Bucket-Berechtigungen richtig einrichten.
- Die im Objektspeicher abgelegten Daten verfügen nicht über die WORM-Funktionalität. Das bedeutet, dass technisch gesehen jeder mit vollem Zugriff auf Buckets und Container die von ONTAP abgelegten Objekte löschen kann.
- Das Zurücksetzen oder Downgrade auf Cloud Volumes ONTAP 9.8 ist nach der Aktivierung von WORM und Tiering blockiert.

Einschränkungen

- WORM-Speicher in Cloud Volumes ONTAP wird nach dem Modell eines „vertrauenswürdigen Speicheradministrators“ betrieben. Obwohl WORM-Dateien vor Änderungen oder Modifikationen geschützt sind, können Volumes von einem Cluster-Administrator gelöscht werden, selbst wenn diese Volumes noch nicht abgelaufene WORM-Daten enthalten.
- Zusätzlich zum Modell des vertrauenswürdigen Speicheradministrators wird WORM-Speicher in Cloud Volumes ONTAP implizit auch nach dem Modell eines „vertrauenswürdigen Cloud-Administrators“ betrieben. Ein Cloud-Administrator könnte WORM-Daten vor ihrem Ablaufdatum löschen, indem er den Cloud-Speicher direkt beim Cloud-Anbieter entfernt oder bearbeitet.

Weiterführender Link

- "Erstellen Sie manipulationssichere Snapshot-Kopien für den WORM-Speicher"
- "Lizenzierung und Abrechnung in Cloud Volumes ONTAP"

Hochverfügbarkeitspaare

Erfahren Sie mehr über Cloud Volumes ONTAP HA-Paare in AWS

Eine Cloud Volumes ONTAP Hochverfügbarkeitskonfiguration (HA) bietet unterbrechungsfreien Betrieb und Fehlertoleranz. In AWS werden Daten synchron zwischen den beiden Knoten gespiegelt.

HA-Komponenten

In AWS umfassen Cloud Volumes ONTAP HA-Konfigurationen die folgenden Komponenten:

- Zwei Cloud Volumes ONTAP Knoten, deren Daten synchron untereinander gespiegelt werden.
- Eine Mediatorinstanz, die einen Kommunikationskanal zwischen den Knoten bereitstellt, um bei der Übernahme und Rückgabe von Speicher zu helfen.

Vermittler

Hier sind einige wichtige Details zur Mediator-Instanz in AWS:

Instanztyp
t3-Mikro

Festplatten
Zwei st1-Festplatten mit 8 GiB und 4 GiB

Betriebssystem
Debian 11

Für Cloud Volumes ONTAP 9.10.0 und früher wurde Debian 10 auf dem Mediator installiert.

Verbesserungen
Wenn Sie Cloud Volumes ONTAP aktualisieren, aktualisiert die NetApp Console bei Bedarf auch die Mediatorinstanz.

Zugriff auf die Instanz
Wenn Sie ein Cloud Volumes ONTAP HA-Paar über die Konsole erstellen, werden Sie aufgefordert, ein Schlüsselpaar für die Mediatorinstanz anzugeben. Sie können dieses Schlüsselpaar für den SSH-Zugriff verwenden, indem Sie `admin` Benutzer.

Drittanbieter-Agenten
Agenten oder VM-Erweiterungen von Drittanbietern werden auf der Mediatorinstanz nicht unterstützt.

Speicherübernahme und -rückgabe

Wenn ein Knoten ausfällt, kann der andere Knoten Daten für seinen Partner bereitstellen, um einen kontinuierlichen Datendienst bereitzustellen. Clients können auf dieselben Daten des Partnerknotens zugreifen, da die Daten synchron zum Partner gespiegelt wurden.

Nach dem Neustart des Knotens muss der Partner die Daten erneut synchronisieren, bevor er den Speicher zurückgeben kann. Die zum erneuten Synchronisieren der Daten benötigte Zeit hängt davon ab, wie viele

Daten geändert wurden, während der Knoten ausgefallen war.

Die Speicherübernahme, Neusynchronisierung und Rückgabe erfolgen standardmäßig automatisch. Es ist keine Benutzeraktion erforderlich.

RPO und RTO

Eine HA-Konfiguration gewährleistet die Hochverfügbarkeit Ihrer Daten wie folgt:

- Das Recovery Point Objective (RPO) beträgt 0 Sekunden. Ihre Daten sind transaktionskonsistent und es kommt zu keinem Datenverlust.
- Die Wiederherstellungszeit (RTO) beträgt 120 Sekunden. Im Falle eines Ausfalls sollten die Daten in 120 Sekunden oder weniger verfügbar sein.

HA-Bereitstellungsmodelle

Sie können die Hochverfügbarkeit Ihrer Daten sicherstellen, indem Sie eine HA-Konfiguration über mehrere Verfügbarkeitszonen (AZs) oder in einer einzelnen Verfügbarkeitszone (AZ) bereitstellen. Sie sollten sich die Einzelheiten zu jeder Konfiguration genauer ansehen, um die Konfiguration auszuwählen, die Ihren Anforderungen am besten entspricht.

Mehrere Verfügbarkeitszonen

Durch die Bereitstellung einer HA-Konfiguration in mehreren Verfügbarkeitszonen (AZs) wird eine hohe Verfügbarkeit Ihrer Daten gewährleistet, wenn bei einer AZ oder einer Instanz, auf der ein Cloud Volumes ONTAP Knoten ausgeführt wird, ein Fehler auftritt. Sie sollten verstehen, welche Auswirkungen NAS-IP-Adressen auf den Datenzugriff und das Speicher-Failover haben.

NFS- und CIFS-Datenzugriff

Wenn eine HA-Konfiguration über mehrere Verfügbarkeitszonen verteilt ist, ermöglichen *Floating IP-Adressen* den NAS-Clientzugriff. Die Floating-IP-Adressen, die für alle VPCs in der Region außerhalb der CIDR-Blöcke liegen müssen, können bei Fehlern zwischen Knoten migrieren. Sie sind für Clients außerhalb der VPC nicht nativ zugänglich, es sei denn, Sie"Einrichten eines AWS Transit Gateways" .

Wenn Sie kein Transit-Gateway einrichten können, stehen private IP-Adressen für NAS-Clients außerhalb der VPC zur Verfügung. Diese IP-Adressen sind jedoch statisch und können nicht zwischen Knoten umgeschaltet werden.

Sie sollten die Anforderungen für Floating-IP-Adressen und Routentabellen überprüfen, bevor Sie eine HA-Konfiguration über mehrere Verfügbarkeitszonen hinweg bereitstellen. Sie müssen die Floating-IP-Adressen angeben, wenn Sie die Konfiguration bereitstellen. Die privaten IP-Adressen werden automatisch erstellt.

Weitere Informationen finden Sie unter "AWS-Netzwerkanforderungen für Cloud Volumes ONTAP HA in mehreren AZs" .

iSCSI-Datenzugriff

Die VPC-übergreifende Datenkommunikation stellt kein Problem dar, da iSCSI keine Floating-IP-Adressen verwendet.

Übernahme und Rückgabe für iSCSI

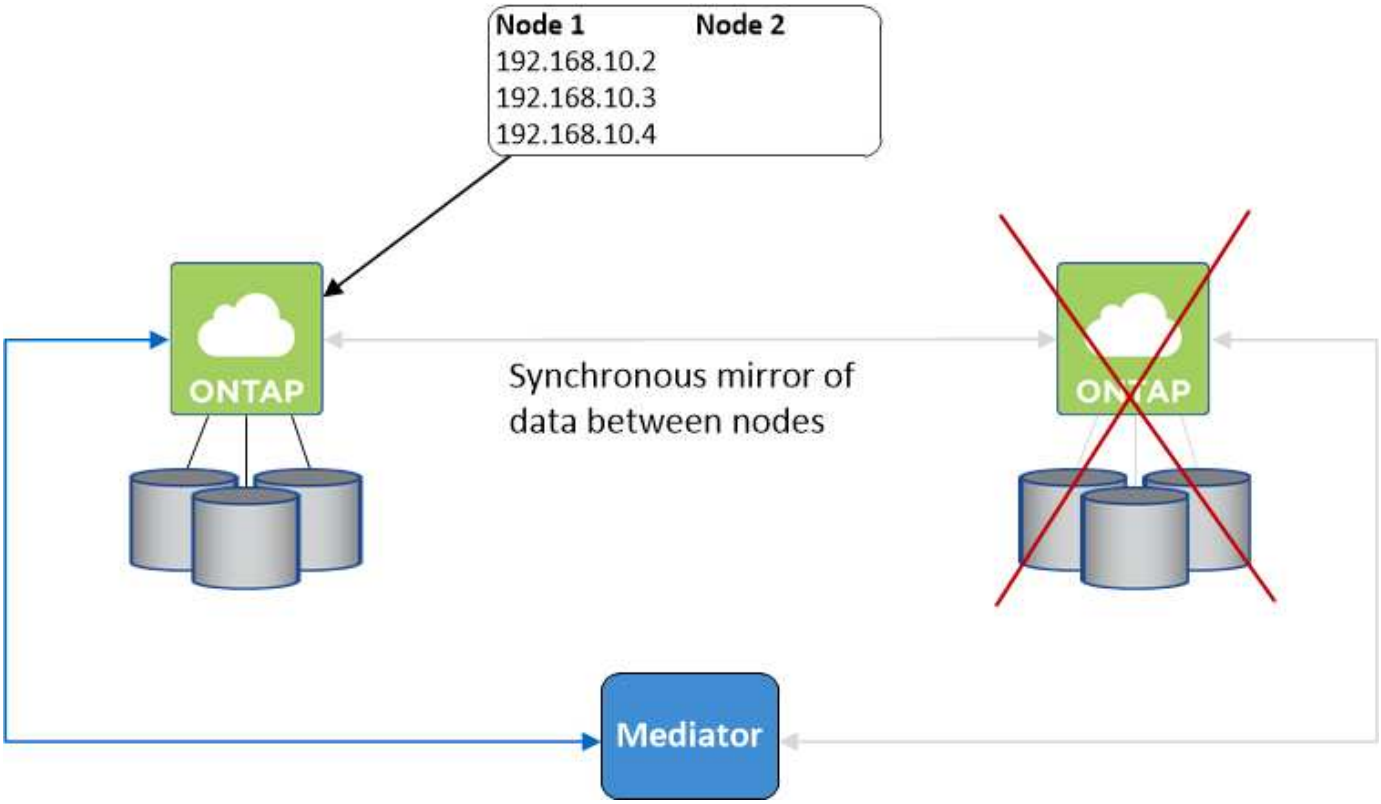
Für iSCSI verwendet Cloud Volumes ONTAP Multipath I/O (MPIO) und Asymmetric Logical Unit Access

(ALUA), um das Pfad-Failover zwischen den aktiv optimierten und nicht optimierten Pfaden zu verwalten.

Informationen darüber, welche spezifischen Hostkonfigurationen ALUA unterstützen, finden Sie im "NetApp Interoperabilitätsmatrix-Tool" und die "Leitfaden für SAN-Hosts und Cloud-Clients" für Ihr Host-Betriebssystem.

Übernahme und Rückgabe für NAS

Wenn in einer NAS-Konfiguration mit Floating-IPs eine Übernahme erfolgt, wird die Floating-IP-Adresse des Knotens, die Clients für den Datenzugriff verwenden, auf den anderen Knoten verschoben. Das folgende Bild zeigt die Speicherübernahme in einer NAS-Konfiguration mit Floating-IPs. Wenn Knoten 2 ausfällt, wird die Floating-IP-Adresse für Knoten 2 auf Knoten 1 verschoben.



Für den externen VPC-Zugriff verwendete NAS-Daten-IPs können bei Fehlern nicht zwischen Knoten migriert werden. Wenn ein Knoten offline geht, müssen Sie Volumes manuell erneut an Clients außerhalb der VPC anbinden, indem Sie die IP-Adresse auf dem anderen Knoten verwenden.

Nachdem der ausgefallene Knoten wieder online ist, mounten Sie die Clients erneut mit der ursprünglichen IP-Adresse auf den Volumes. Dieser Schritt ist erforderlich, um die Übertragung unnötiger Daten zwischen zwei HA-Knoten zu vermeiden, die erhebliche Auswirkungen auf Leistung und Stabilität haben können.

Sie können die richtige IP-Adresse in der Konsole ermitteln, indem Sie das Volume auswählen und auf **Mount Command** klicken.

Einzelne Verfügbarkeitszone

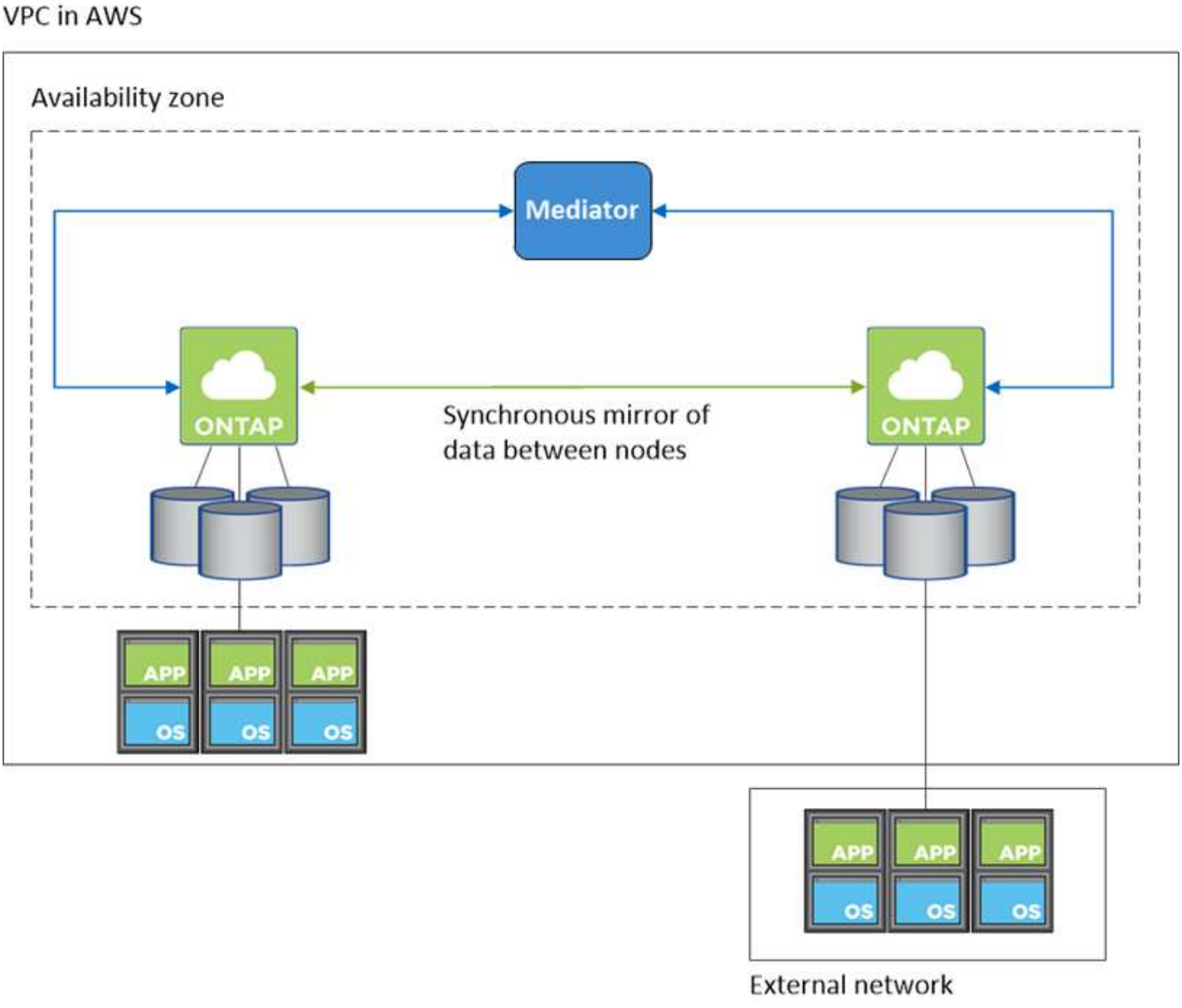
Durch die Bereitstellung einer HA-Konfiguration in einer einzelnen Verfügbarkeitszone (AZ) können Sie eine hohe Verfügbarkeit Ihrer Daten sicherstellen, wenn eine Instanz ausfällt, auf der ein Cloud Volumes ONTAP Knoten ausgeführt wird. Auf alle Daten kann nativ von außerhalb der VPC zugegriffen werden.

Die Konsole erstellt eine "AWS-Dokumentation: AWS Spread Placement Group" und startet die beiden HA-Knoten in dieser Platzierungsgruppe. Die Platzierungsgruppe verringert das Risiko gleichzeitiger Ausfälle, indem sie die Instanzen auf unterschiedliche zugrunde liegende Hardware verteilt. Diese Funktion verbessert die Redundanz aus der Perspektive der Datenverarbeitung und nicht aus der Perspektive eines Festplattenausfalls.

Datenzugriff

Da sich diese Konfiguration in einer einzelnen AZ befindet, sind keine Floating-IP-Adressen erforderlich. Sie können dieselbe IP-Adresse für den Datenzugriff innerhalb und außerhalb der VPC verwenden.

Das folgende Bild zeigt eine HA-Konfiguration in einer einzelnen AZ. Auf die Daten kann innerhalb und außerhalb der VPC zugegriffen werden.



Übernahme und Rückgabe

Für iSCSI verwendet Cloud Volumes ONTAP Multipath I/O (MPIO) und Asymmetric Logical Unit Access (ALUA), um das Pfad-Failover zwischen den aktiv optimierten und nicht optimierten Pfaden zu verwalten.

Informationen darüber, welche spezifischen Hostkonfigurationen ALUA unterstützen, finden Sie im "NetApp Interoperabilitätsmatrix-Tool" und die "Leitfaden für SAN-Hosts und Cloud-Clients" für Ihr Host-Betriebssystem.

Bei NAS-Konfigurationen können die Daten-IP-Adressen bei Fehlern zwischen HA-Knoten migrieren. Dadurch wird der Clientzugriff auf den Speicher sichergestellt.

Lokale AWS-Zonen

Bei AWS Local Zones handelt es sich um eine Infrastrukturbereitstellung, bei der Speicher, Rechenleistung, Datenbanken und andere ausgewählte AWS-Dienste in der Nähe von Großstädten und Industriegebieten angesiedelt sind. Mit AWS Local Zones können Sie AWS-Dienste näher zu sich holen, was die Latenz für Ihre Workloads verbessert und Datenbanken lokal verwaltet. Auf Cloud Volumes ONTAP,

Sie können eine einzelne AZ oder mehrere AZ-Konfigurationen in AWS Local Zones bereitstellen.

AWS Local Zones werden unterstützt, wenn die Konsole im Standard- und privaten Modus verwendet wird. Derzeit werden AWS Local Zones im eingeschränkten Modus nicht unterstützt.

Beispielkonfigurationen für AWS Local Zone

Cloud Volumes ONTAP in AWS unterstützt nur den Hochverfügbarkeitsmodus (HA) in einer einzelnen Verfügbarkeitszone. Bereitstellungen mit einem einzelnen Knoten werden nicht unterstützt.

Cloud Volumes ONTAP unterstützt kein Daten-Tiering, Cloud-Tiering und nicht qualifizierte Instanzen in AWS Local Zones.

Nachfolgend sind Beispielkonfigurationen aufgeführt:

- Einzelne Verfügbarkeitszone: Beide Clusterknoten und der Mediator befinden sich in derselben lokalen Zone.
- Mehrere Verfügbarkeitszonen In Konfigurationen mit mehreren Verfügbarkeitszonen gibt es drei Instanzen, zwei Knoten und einen Mediator. Eine der drei Instanzen muss sich in einer separaten Zone befinden. Sie können wählen, wie Sie dies einrichten.

  Hier sind drei Beispielkonfigurationen:

  - Jeder Clusterknoten befindet sich in einer anderen lokalen Zone und der Mediator in einer öffentlichen Verfügbarkeitszone.
  - Ein Clusterknoten in einer lokalen Zone, der Mediator in einer lokalen Zone und der zweite Clusterknoten befindet sich in einer Verfügbarkeitszone.
  - Jeder Clusterknoten und der Mediator befinden sich in separaten lokalen Zonen.

Unterstützte Datenträger- und Instanztypen

Der einzige unterstützte Datenträgertyp ist GP2. Die folgenden EC2-Instance-Typfamilien mit den Größen xlarge bis 4xlarge werden derzeit unterstützt:

- M5
- C5
- C5d

- R5
- R5d

> Cloud Volumes ONTAP unterstützt ausschließlich diese Konfigurationen. Die Auswahl nicht unterstützter Datenträgertypen oder nicht qualifizierter Instanzen in der AWS Local Zone-Konfiguration kann zu einem Bereitstellungsfehler führen. Data Tiering zu Amazon Simple Storage Service (Amazon S3) wird nicht unterstützt, wenn sich Ihr Cloud Volumes ONTAP System in einer AWS Local Zone befindet, da der Zugriff auf die Amazon S3-Buckets außerhalb der Local Zone mit einer höheren Latenz verbunden ist und die Aktivitäten von Cloud Volumes ONTAP beeinträchtigt.

"AWS-Dokumentation: EC2-Instanztypen in lokalen Zonen" .

Funktionsweise der Speicherung in einem HA-Paar

Anders als bei einem ONTAP Cluster wird der Speicher in einem Cloud Volumes ONTAP HA-Paar nicht zwischen den Knoten geteilt. Stattdessen werden die Daten synchron zwischen den Knoten gespiegelt, sodass die Daten im Fehlerfall verfügbar sind.

Speicherzuweisung

Wenn Sie ein neues Volume erstellen und zusätzliche Datenträger benötigt werden, weist die Konsole beiden Knoten die gleiche Anzahl an Datenträgern zu, erstellt ein gespiegeltes Aggregat und erstellt dann das neue Volume. Wenn beispielsweise zwei Festplatten für das Volume erforderlich sind, weist die Konsole zwei Festplatten pro Knoten zu, sodass insgesamt vier Festplatten vorhanden sind.

Speicherkonfigurationen

Sie können ein HA-Paar als Aktiv-Aktiv-Konfiguration verwenden, bei der beide Knoten Daten an Clients bereitstellen, oder als Aktiv-Passiv-Konfiguration, bei der der passive Knoten nur dann auf Datenanforderungen antwortet, wenn er den Speicher für den aktiven Knoten übernommen hat.

> Sie können eine Aktiv-Aktiv-Konfiguration nur einrichten, wenn Sie die Konsole in der Speichersystemansicht verwenden.

Leistungserwartungen

Eine Cloud Volumes ONTAP HA-Konfiguration repliziert Daten synchron zwischen Knoten, was Netzwerkbandbreite verbraucht. Im Vergleich zu einer Cloud Volumes ONTAP -Konfiguration mit einem einzelnen Knoten können Sie daher die folgende Leistung erwarten:

- Bei HA-Konfigurationen, die Daten von nur einem Knoten bereitstellen, ist die Leseleistung mit der Leseleistung einer Einzelknotenkonfiguration vergleichbar, während die Schreibleistung geringer ist.
- Bei HA-Konfigurationen, die Daten von beiden Knoten bereitstellen, ist die Leseleistung höher als die Leseleistung einer Einzelknotenkonfiguration und die Schreibleistung ist gleich oder höher.

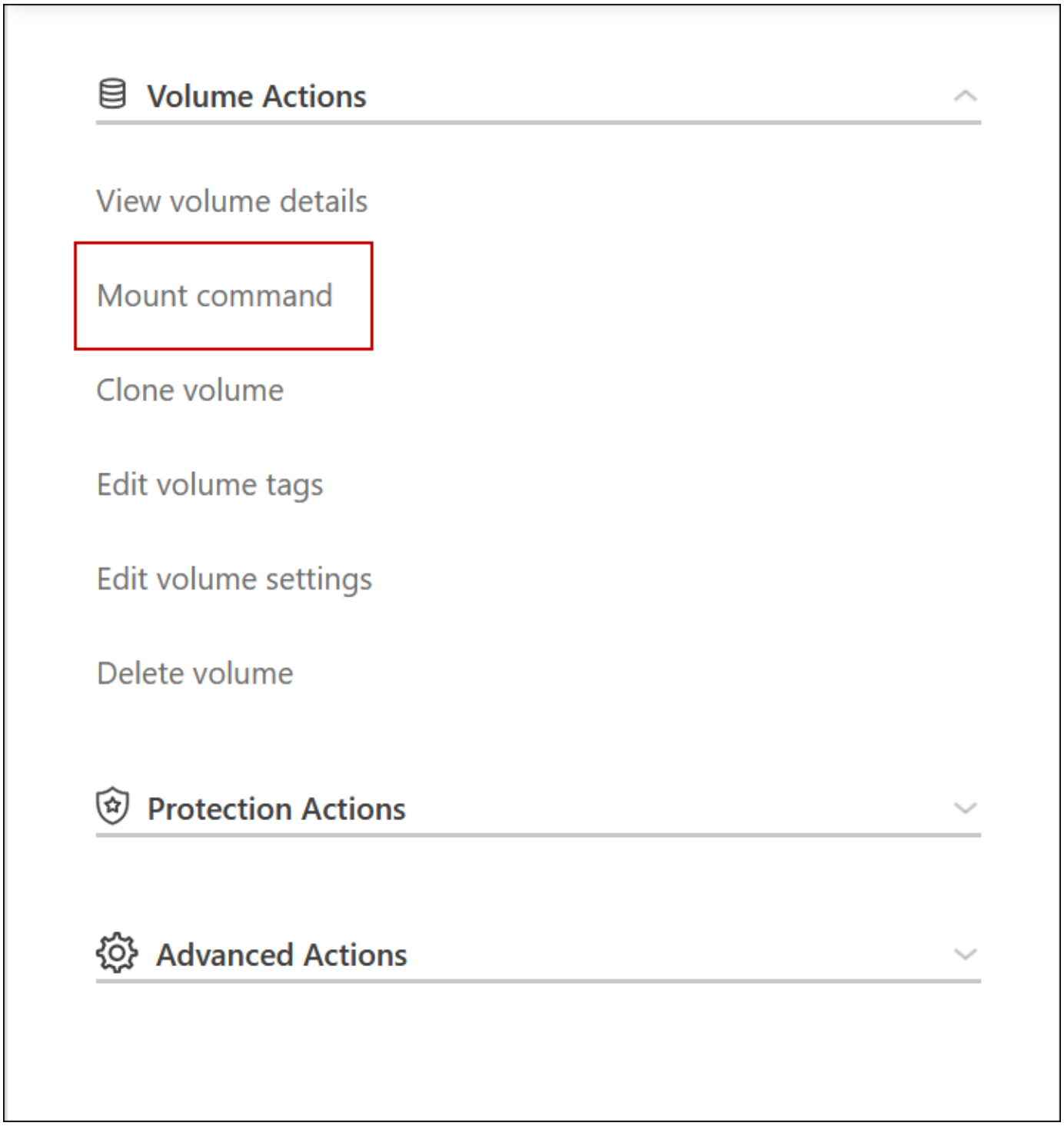
Weitere Informationen zur Leistung von Cloud Volumes ONTAP finden Sie unter"Performance" .

Clientzugriff auf Speicher

Clients sollten auf NFS- und CIFS-Volumes zugreifen, indem sie die Daten-IP-Adresse des Knotens verwenden, auf dem sich das Volume befindet. Wenn NAS-Clients über die IP-Adresse des Partnerknotens auf ein Volume zugreifen, wird der Datenverkehr zwischen beiden Knoten geleitet, was die Leistung verringert.

Wenn Sie ein Volume zwischen Knoten in einem HA-Paar verschieben, sollten Sie das Volume unter Verwendung der IP-Adresse des anderen Knotens erneut mounten. Andernfalls kann es zu Leistungseinbußen kommen. Wenn Clients NFSv4-Verweise oder Ordnerumleitungen für CIFS unterstützen, können Sie diese Funktionen auf den Cloud Volumes ONTAP Systemen aktivieren, um eine erneute Bereitstellung des Volumes zu vermeiden. Einzelheiten finden Sie in der ONTAP -Dokumentation.

Sie können die richtige IP-Adresse ganz einfach über die Option „Mount Command“ im Bereich „Volumes verwalten“ ermitteln.



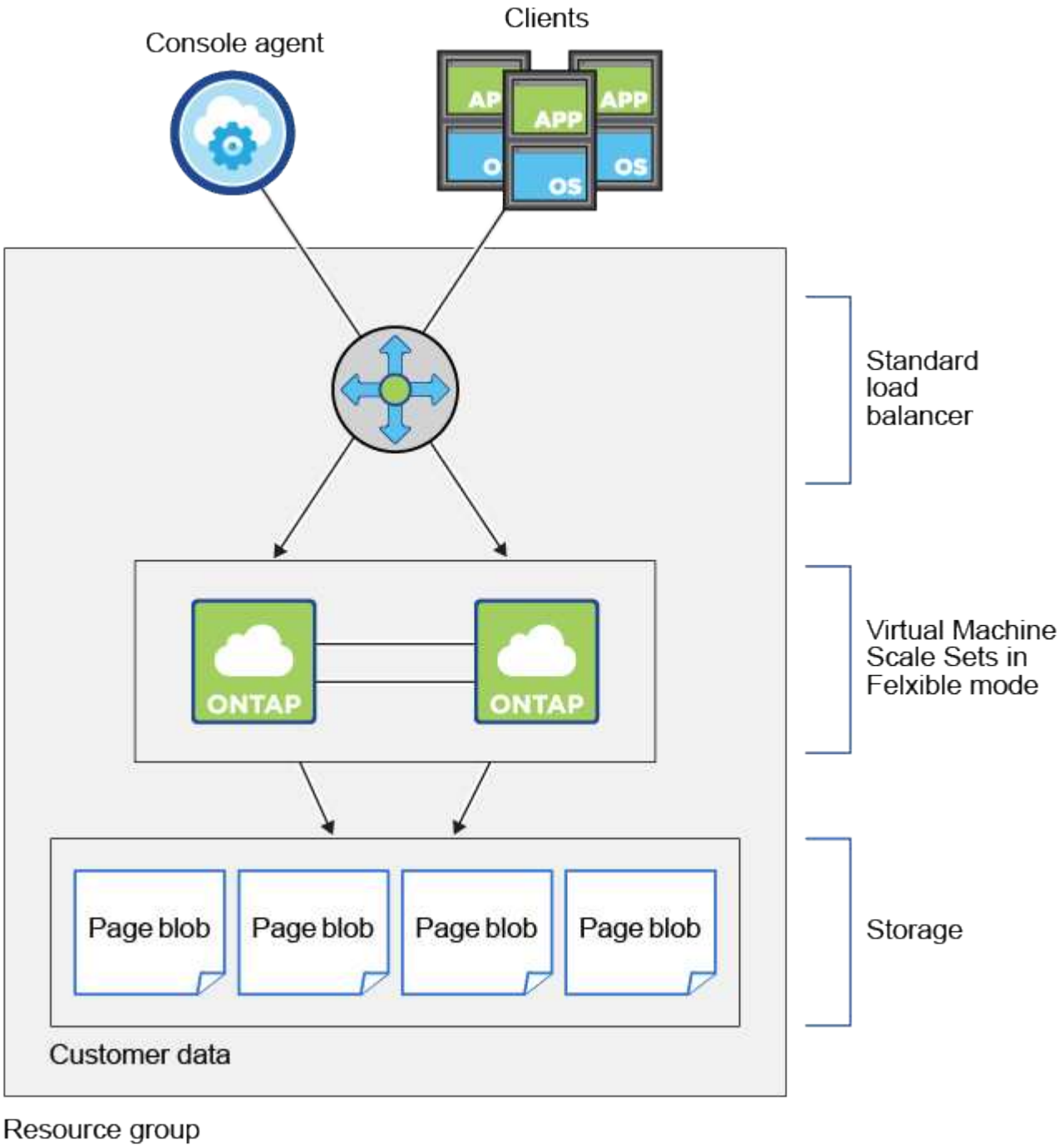
Erfahren Sie mehr über Cloud Volumes ONTAP HA-Paare in Azure

Ein Cloud Volumes ONTAP -Hochverfügbarkeitspaar (HA) bietet Unternehmenszuverlässigkeit und kontinuierlichen Betrieb im Falle von Ausfällen in Ihrer Cloud-Umgebung. In Azure wird der Speicher zwischen den beiden Knoten geteilt.

HA-Komponenten

HA-Konfiguration einer einzelnen Verfügbarkeitszone mit Seitenblobs

Eine Cloud Volumes ONTAP HA-Seitenblobkonfiguration in Azure umfasst die folgenden Komponenten:



Beachten Sie Folgendes zu den Azure-Komponenten, die die NetApp Console für Sie bereitstellt:

Azure Standard Load Balancer

Der Load Balancer verwaltet den eingehenden Datenverkehr zum Cloud Volumes ONTAP HA-Paar.

VMs in einzelnen Verfügbarkeitszonen

Ab Cloud Volumes ONTAP 9.15.1 können Sie heterogene virtuelle Maschinen (VMs) in einer einzigen Verfügbarkeitszone (AZ) erstellen und verwalten. Sie können Hochverfügbarkeitsknoten (HA) in separaten Fehlerdomänen innerhalb derselben AZ bereitstellen und so optimale Verfügbarkeit gewährleisten. Weitere Informationen zum flexiblen Orchestrierungsmodus, der diese Funktion ermöglicht, finden Sie im "Microsoft Azure-Dokumentation: Virtual Machine Scale Sets" .

Festplatten

Kundendaten befinden sich auf Premium Storage-Seitenblobs. Jeder Knoten hat Zugriff auf den Speicher des anderen Knotens. Zusätzlicher Speicher wird auch benötigt für"Boot-, Root- und Core-Daten" .

Speicherkonten

- Für verwaltete Datenträger ist ein Speicherkonto erforderlich.
- Für die Premium Storage-Seitenblobs sind ein oder mehrere Speicherkonten erforderlich, da die Datenträgerkapazitätsgrenze pro Speicherkonto erreicht ist.

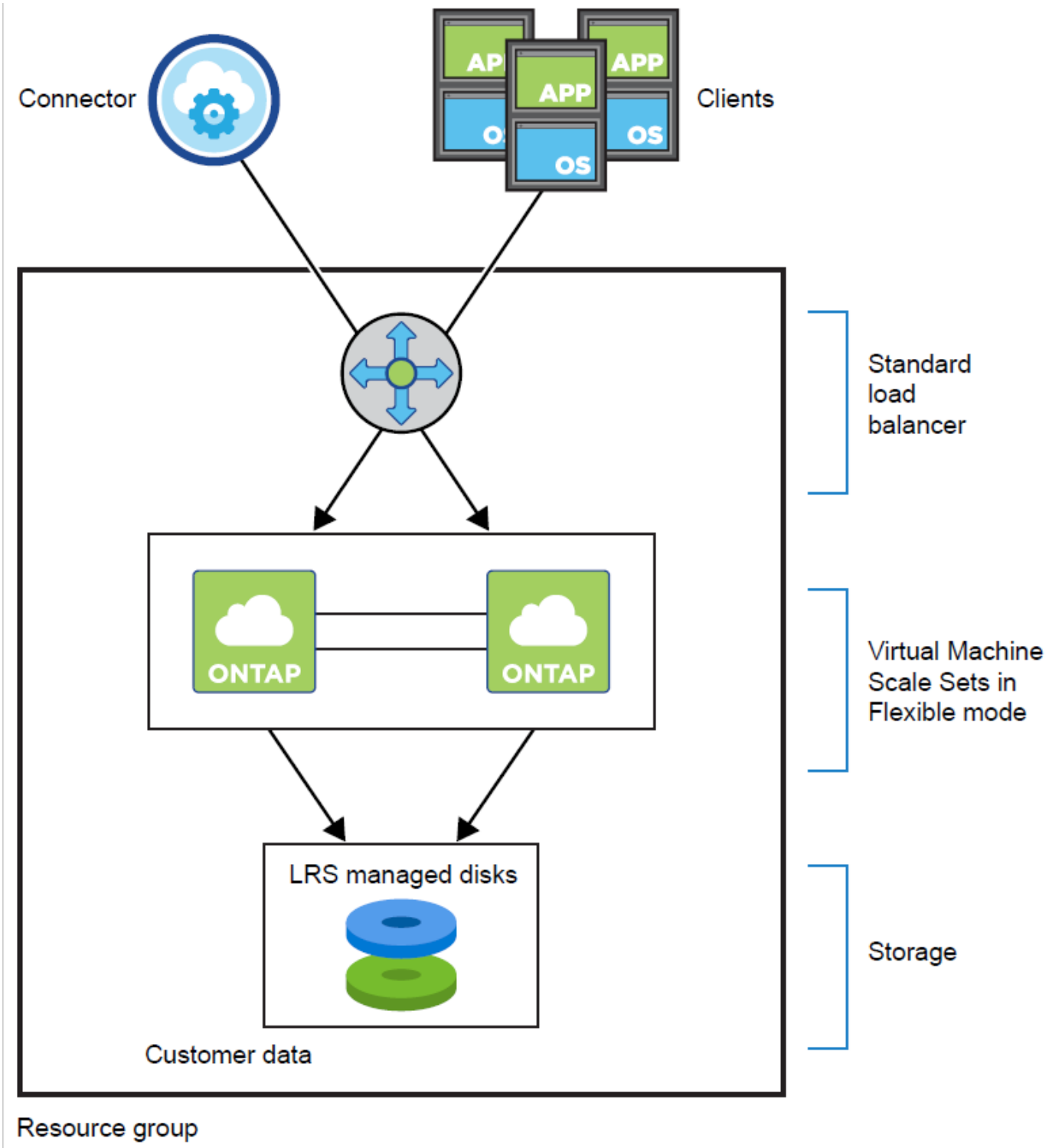
  "Microsoft Azure-Dokumentation: Azure Storage-Skalierbarkeits- und Leistungsziele für Speicherkonten" .

- Für die Datentierierung in Azure Blob Storage ist ein Speicherkonto erforderlich.
- Ab Cloud Volumes ONTAP 9.7 sind die Speicherkonten, die die Konsole für HA-Paare erstellt, allgemeine v2-Speicherkonten.
- Sie können eine HTTPS-Verbindung von einem Cloud Volumes ONTAP 9.7 HA-Paar zu Azure-Speicherkonten aktivieren, wenn Sie ein Cloud Volumes ONTAP -System hinzufügen. Beachten Sie, dass das Aktivieren dieser Option die Schreibleistung beeinträchtigen kann. Sie können die Einstellung nicht mehr ändern, nachdem Sie das System erstellt haben.

> Ab Cloud Volumes ONTAP 9.15.0P1 werden Azure-Seitenblobs für neue Bereitstellungen mit Hochverfügbarkeitspaaren nicht mehr unterstützt. Wenn Sie derzeit Azure-Seitenblobs in vorhandenen Bereitstellungen mit Hochverfügbarkeitspaaren verwenden, können Sie in den VMs der Edsv4- und Edsv5-Serie zu neueren VM-Instanztypen migrieren. "Erfahren Sie mehr über unterstützte Konfigurationen in Azure" .

HA-Konfiguration einer einzelnen Verfügbarkeitszone mit gemeinsam genutzten verwalteten Datenträgern

Eine Cloud Volumes ONTAP HA-Konfiguration mit einer einzelnen Verfügbarkeitszone, die auf einer gemeinsam genutzten verwalteten Festplatte ausgeführt wird, umfasst die folgenden Komponenten:



Beachten Sie Folgendes zu den Azure-Komponenten, die die Konsole für Sie bereitstellt:

Azure Standard Load Balancer

Der Load Balancer verwaltet den eingehenden Datenverkehr zum Cloud Volumes ONTAP HA-Paar.

VMs in einzelnen Verfügbarkeitszonen

Ab Cloud Volumes ONTAP 9.15.1 können Sie heterogene virtuelle Maschinen (VMs) in einer einzigen Verfügbarkeitszone (AZ) erstellen und verwalten. Sie können Hochverfügbarkeitsknoten (HA) in separaten Fehlerdomänen innerhalb derselben AZ bereitstellen und so optimale Verfügbarkeit gewährleisten. Weitere Informationen zum flexiblen Orchestrierungsmodus, der diese Funktion ermöglicht, finden Sie im "Microsoft

Azure-Dokumentation: Virtual Machine Scale Sets" .

Die zonale Bereitstellung verwendet Premium SSD v2 Managed Disks, wenn die folgenden Bedingungen erfüllt sind:

- Die Version von Cloud Volumes ONTAP ist 9.15.1 oder höher.
- Die ausgewählte Region und Zone unterstützen Premium SSD v2 Managed Disks. Informationen zu den unterstützten Regionen finden Sie unter "Microsoft Azure-Website: Verfügbare Produkte nach Region" .
- Das Abonnement ist für Microsoft registriert"Microsoft.Compute/VMOrchestratorZonalMultiFD-Funktion" .

Wenn Sie Premium SSD Managed Disks für eine Umgebung auswählen, die die oben genannten Kriterien erfüllt, stellt die Konsole automatisch Premium SSD v2 Managed Disks bereit. Ein Wechsel zu Premium SSD v1 Managed Disks ist nicht möglich.

Festplatten

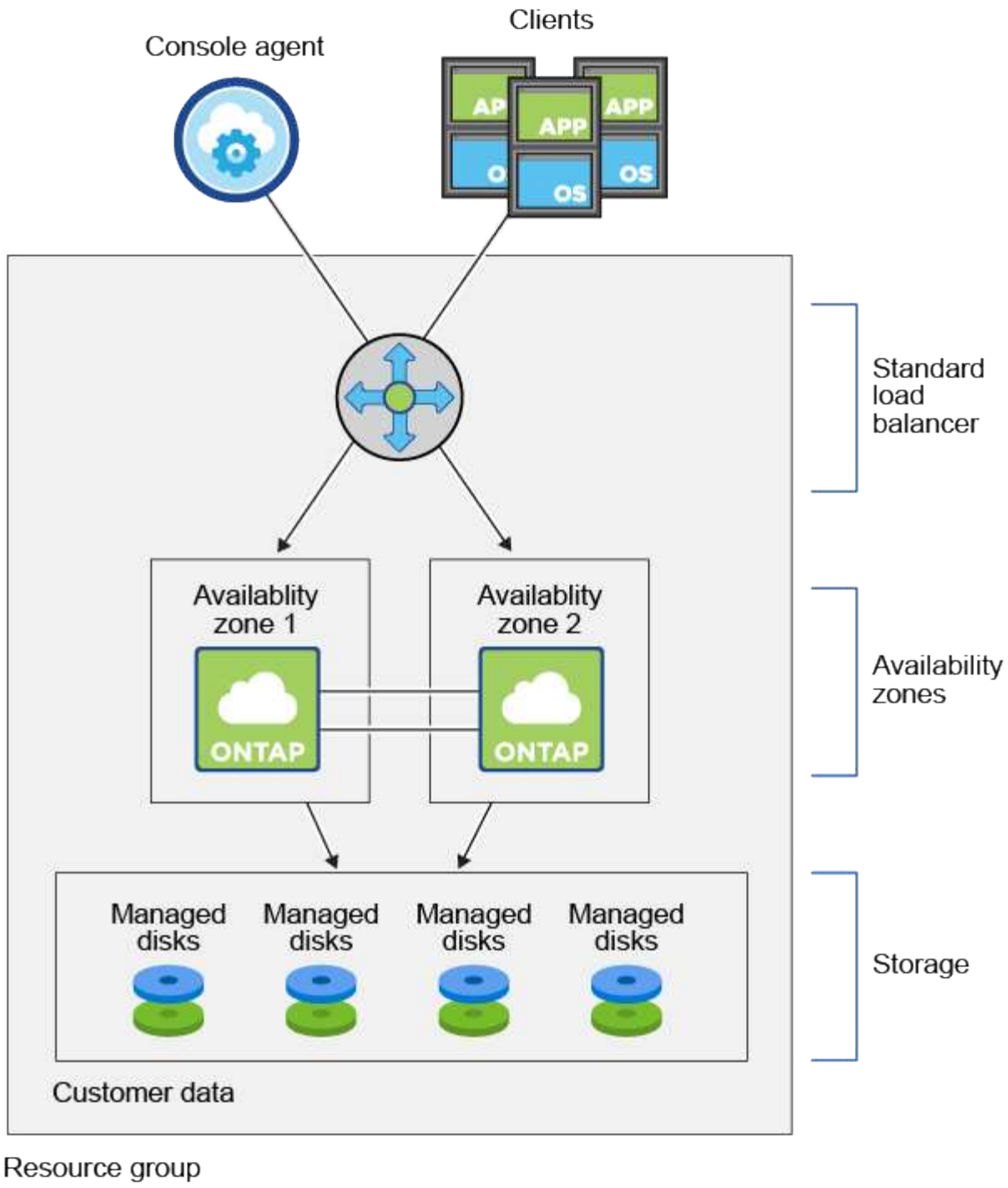
Kundendaten befinden sich auf verwalteten Festplatten mit lokal redundantem Speicher (LRS). Jeder Knoten hat Zugriff auf den Speicher des anderen Knotens. Zusätzlicher Speicher wird auch benötigt für"Boot-, Root-, Partner-Root-, Core- und NVRAM -Daten" .

Speicherkonten

Speicherkonten werden für Bereitstellungen auf Basis verwalteter Datenträger verwendet, um Diagnoseprotokolle und die Einstufung in Blob-Speicher zu verarbeiten.

HA-Konfiguration für mehrere Verfügbarkeitszonen

Eine Cloud Volumes ONTAP HA-Konfiguration mit mehreren Verfügbarkeitszonen in Azure umfasst die folgenden Komponenten:



Beachten Sie Folgendes zu den Azure-Komponenten, die die Konsole für Sie bereitstellt:

Azure Standard Load Balancer

Der Load Balancer verwaltet den eingehenden Datenverkehr zum Cloud Volumes ONTAP HA-Paar.

Verfügbarkeitszonen

Die HA-Konfiguration mit mehreren Verfügbarkeitszonen verwendet ein Bereitstellungsmodell, bei dem zwei Cloud Volumes ONTAP Knoten in unterschiedlichen Verfügbarkeitszonen bereitgestellt werden. Dadurch wird sichergestellt, dass sich die Knoten in unterschiedlichen Fehlerdomänen befinden, um Redundanz und Verfügbarkeit zu gewährleisten. Informationen dazu, wie Virtual Machine Scale Sets im flexiblen Orchestrierungsmodus Verfügbarkeitszonen in Azure nutzen können, finden Sie im "Microsoft Azure-

Dokumentation: Erstellen eines Virtual Machine Scale Set, das Verfügbarkeitszonen verwendet" .

Festplatten

Kundendaten befinden sich auf verwalteten Datenträgern mit zonenredundantem Speicher (ZRS). Jeder Knoten hat Zugriff auf den Speicher des anderen Knotens. Zusätzlicher Speicher wird auch benötigt für"Boot-, Root-, Partner-Root- und Core-Daten" .

Speicherkonten

Speicherkonten werden für Bereitstellungen auf Basis verwalteter Datenträger verwendet, um Diagnoseprotokolle und die Einstufung in Blob-Speicher zu verarbeiten.

RPO und RTO

Eine HA-Konfiguration gewährleistet die Hochverfügbarkeit Ihrer Daten wie folgt:

- Das Recovery Point Objective (RPO) beträgt 0 Sekunden. Ihre Daten sind transaktionskonsistent und es kommt zu keinem Datenverlust.
- Die Wiederherstellungszeit (RTO) beträgt 120 Sekunden. Im Falle eines Ausfalls sollten die Daten in 120 Sekunden oder weniger verfügbar sein.

Speicherübernahme und -rückgabe

Ähnlich wie bei einem physischen ONTAP Cluster wird der Speicher in einem Azure HA-Paar zwischen Knoten geteilt. Durch Verbindungen zum Speicher des Partners kann jeder Knoten im Falle einer *Übernahme* auf den Speicher des anderen zugreifen. Failover-Mechanismen für Netzwerkpfade stellen sicher, dass Clients und Hosts weiterhin mit dem verbleibenden Knoten kommunizieren. Der Partner gibt den Speicher zurück, wenn der Knoten wieder online ist.

Bei NAS-Konfigurationen werden Daten-IP-Adressen bei Fehlern automatisch zwischen HA-Knoten migriert.

Für iSCSI verwendet Cloud Volumes ONTAP Multipath I/O (MPIO) und Asymmetric Logical Unit Access (ALUA), um das Pfad-Failover zwischen den aktiv optimierten und nicht optimierten Pfaden zu verwalten.

Informationen darüber, welche spezifischen Hostkonfigurationen ALUA unterstützen, finden Sie im "NetApp Interoperabilitätsmatrix-Tool" und die "Leitfaden für SAN-Hosts und Cloud-Clients" für Ihr Host-Betriebssystem.

Die Speicherübernahme, Neusynchronisierung und Rückgabe erfolgen standardmäßig automatisch. Es ist keine Benutzeraktion erforderlich.

Speicherkonfigurationen

Sie können ein HA-Paar als Aktiv-Aktiv-Konfiguration verwenden, bei der beide Knoten Daten an Clients bereitstellen, oder als Aktiv-Passiv-Konfiguration, bei der der passive Knoten nur dann auf Datenanforderungen antwortet, wenn er den Speicher für den aktiven Knoten übernommen hat.

Erfahren Sie mehr über Cloud Volumes ONTAP HA-Paare in Google Cloud

Eine Cloud Volumes ONTAP Hochverfügbarkeitskonfiguration (HA) bietet unterbrechungsfreien Betrieb und Fehlertoleranz. In Google Cloud werden Daten synchron zwischen den beiden Knoten gespiegelt.

HA-Komponenten

Cloud Volumes ONTAP HA-Konfigurationen in Google Cloud umfassen die folgenden Komponenten:

- Zwei Cloud Volumes ONTAP Knoten, deren Daten synchron untereinander gespiegelt werden.
- Eine Mediatorinstanz, die einen Kommunikationskanal zwischen den Knoten bereitstellt, um bei der Übernahme und Rückgabe von Speicher zu helfen.
- Eine Zone oder drei Zonen (empfohlen).

  Wenn Sie drei Zonen auswählen, befinden sich die beiden Knoten und der Mediator in separaten Google Cloud-Zonen.

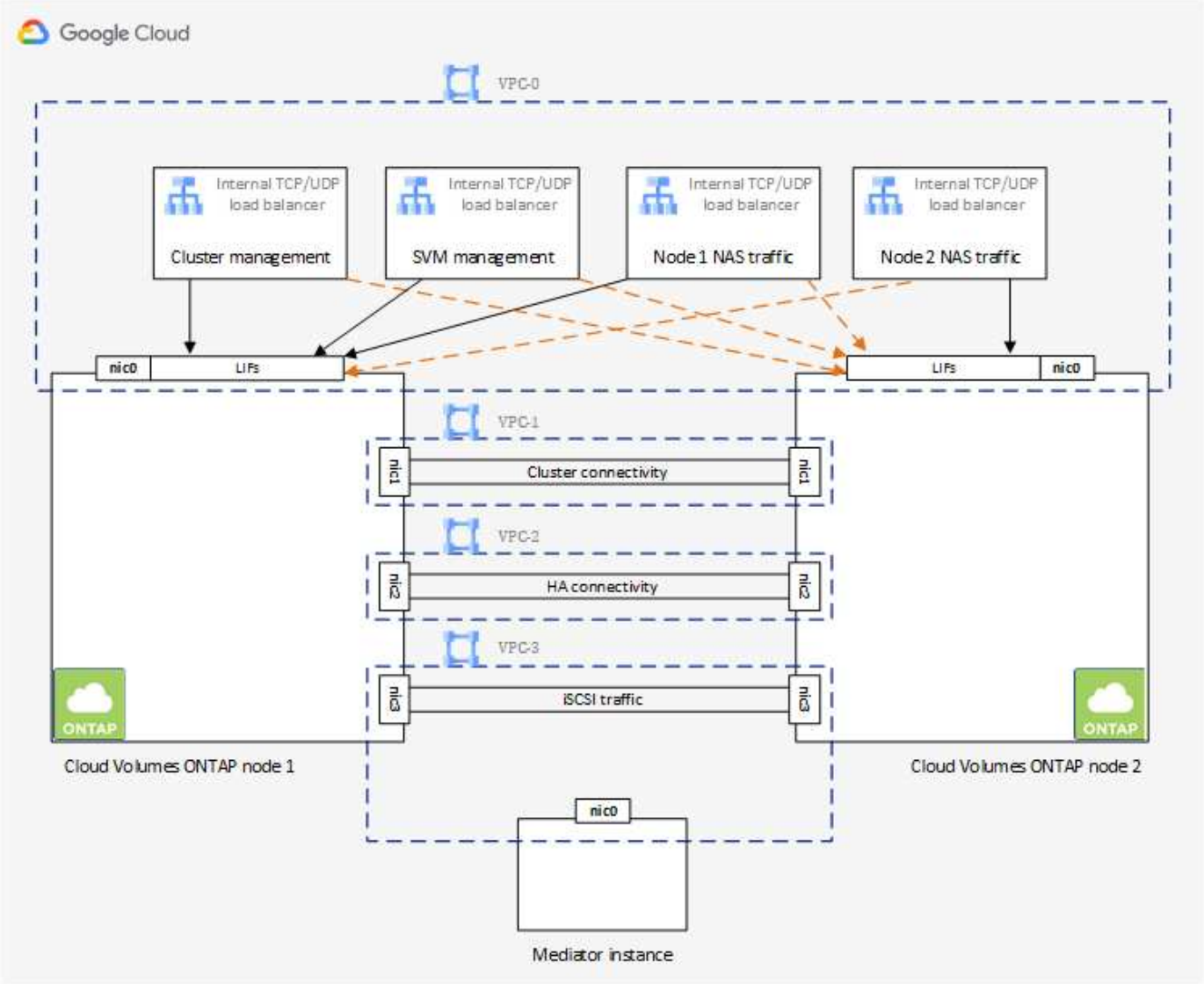
- Vier virtuelle private Clouds (VPCs).

  Die Konfiguration verwendet vier VPCs, da GCP erfordert, dass sich jede Netzwerkschnittstelle in einem separaten VPC-Netzwerk befindet.

- Vier interne Load Balancer (TCP/UDP) von Google Cloud, die den eingehenden Datenverkehr zum Cloud Volumes ONTAP HA-Paar verwalten.

"Informieren Sie sich über die Netzwerkanforderungen", einschließlich weiterer Details zu Load Balancern, VPCs, internen IP-Adressen, Subnetzen und mehr.

Das folgende Konzeptbild zeigt ein Cloud Volumes ONTAP HA-Paar und seine Komponenten:



Vermittler

Hier sind einige wichtige Details zur Mediator-Instanz in Google Cloud:

Instanztyp

e2-micro (zuvor wurde eine f1-micro-Instanz verwendet)

Festplatten

Zwei persistente Standarddatenträger mit jeweils 10 GiB

Betriebssystem

Debian 11

Für Cloud Volumes ONTAP 9.10.0 und früher wurde Debian 10 auf dem Mediator installiert.

Verbesserungen

Wenn Sie Cloud Volumes ONTAP aktualisieren, aktualisiert die NetApp Console bei Bedarf auch die Mediatorinstanz.

Zugriff auf die Instanz

Für Debian ist der Standard-Cloud-Benutzer `admin`. Google Cloud erstellt und fügt ein Zertifikat für den `admin` Benutzer hinzu, wenn der SSH-Zugriff über die Google Cloud Console oder die gcloud Befehlszeile angefordert wird. Sie können `sudo` angeben, um Root-Rechte zu erhalten.

Drittanbieter-Agenten

Agenten oder VM-Erweiterungen von Drittanbietern werden auf der Mediatorinstanz nicht unterstützt.

Speicherübernahme und -rückgabe

Wenn ein Knoten ausfällt, kann der andere Knoten Daten für seinen Partner bereitstellen, um einen kontinuierlichen Datendienst bereitzustellen. Clients können auf dieselben Daten des Partnerknotens zugreifen, da die Daten synchron zum Partner gespiegelt wurden.

Nach dem Neustart des Knotens muss der Partner die Daten erneut synchronisieren, bevor er den Speicher zurückgeben kann. Die zum erneuten Synchronisieren der Daten benötigte Zeit hängt davon ab, wie viele Daten geändert wurden, während der Knoten ausgefallen war.

Die Speicherübernahme, Neusynchronisierung und Rückgabe erfolgen standardmäßig automatisch. Es ist keine Benutzeraktion erforderlich.

RPO und RTO

Eine HA-Konfiguration gewährleistet die Hochverfügbarkeit Ihrer Daten wie folgt:

- Das Recovery Point Objective (RPO) beträgt 0 Sekunden.

  Ihre Daten sind transaktionskonsistent und es kommt zu keinem Datenverlust.

- Die Wiederherstellungszeit (RTO) beträgt 120 Sekunden.

  Im Falle eines Ausfalls sollten die Daten in 120 Sekunden oder weniger verfügbar sein.

HA-Bereitstellungsmodelle

Sie können die Hochverfügbarkeit Ihrer Daten sicherstellen, indem Sie eine HA-Konfiguration in mehreren Zonen oder in einer einzelnen Zone bereitstellen.

Mehrere Zonen (empfohlen)

Durch die Bereitstellung einer HA-Konfiguration über drei Zonen hinweg wird eine kontinuierliche Datenverfügbarkeit gewährleistet, wenn innerhalb einer Zone ein Fehler auftritt. Beachten Sie, dass die Schreibleistung im Vergleich zur Verwendung einer einzelnen Zone etwas geringer ist, aber minimal.

Einzelzone

Bei der Bereitstellung in einer einzelnen Zone verwendet eine Cloud Volumes ONTAP HA-Konfiguration eine Richtlinie für verteilte Platzierung. Diese Richtlinie stellt sicher, dass eine HA-Konfiguration vor einem einzelnen Fehlerpunkt innerhalb der Zone geschützt ist, ohne dass separate Zonen zur Fehlerisolierung verwendet werden müssen.

Dieses Bereitstellungsmodell senkt Ihre Kosten, da zwischen den Zonen keine Gebühren für den Datenausgang anfallen.

Funktionsweise der Speicherung in einem HA-Paar

Anders als bei einem ONTAP Cluster wird der Speicher in einem Cloud Volumes ONTAP HA-Paar in GCP nicht zwischen Knoten geteilt. Stattdessen werden die Daten synchron zwischen den Knoten gespiegelt, sodass die Daten im Fehlerfall verfügbar sind.

Speicherzuweisung

Wenn Sie ein neues Volume erstellen und zusätzliche Datenträger benötigt werden, weist die Konsole beiden Knoten die gleiche Anzahl an Datenträgern zu, erstellt ein gespiegeltes Aggregat und erstellt dann das neue Volume. Wenn beispielsweise zwei Festplatten für das Volume erforderlich sind, weist die Konsole zwei Festplatten pro Knoten zu, sodass insgesamt vier Festplatten vorhanden sind.

Speicherkonfigurationen

Sie können ein HA-Paar als Aktiv-Aktiv-Konfiguration verwenden, bei der beide Knoten Daten an Clients bereitstellen, oder als Aktiv-Passiv-Konfiguration, bei der der passive Knoten nur dann auf Datenanforderungen antwortet, wenn er den Speicher für den aktiven Knoten übernommen hat.

Leistungserwartungen für eine HA-Konfiguration

Eine Cloud Volumes ONTAP HA-Konfiguration repliziert Daten synchron zwischen Knoten, was Netzwerkbandbreite verbraucht. Im Vergleich zu einer Cloud Volumes ONTAP -Konfiguration mit einem einzelnen Knoten können Sie daher die folgende Leistung erwarten:

- Bei HA-Konfigurationen, die Daten von nur einem Knoten bereitstellen, ist die Leseleistung mit der Leseleistung einer Einzelknotenkonfiguration vergleichbar, während die Schreibleistung geringer ist.
- Bei HA-Konfigurationen, die Daten von beiden Knoten bereitstellen, ist die Leseleistung höher als die Leseleistung einer Einzelknotenkonfiguration und die Schreibleistung ist gleich oder höher.

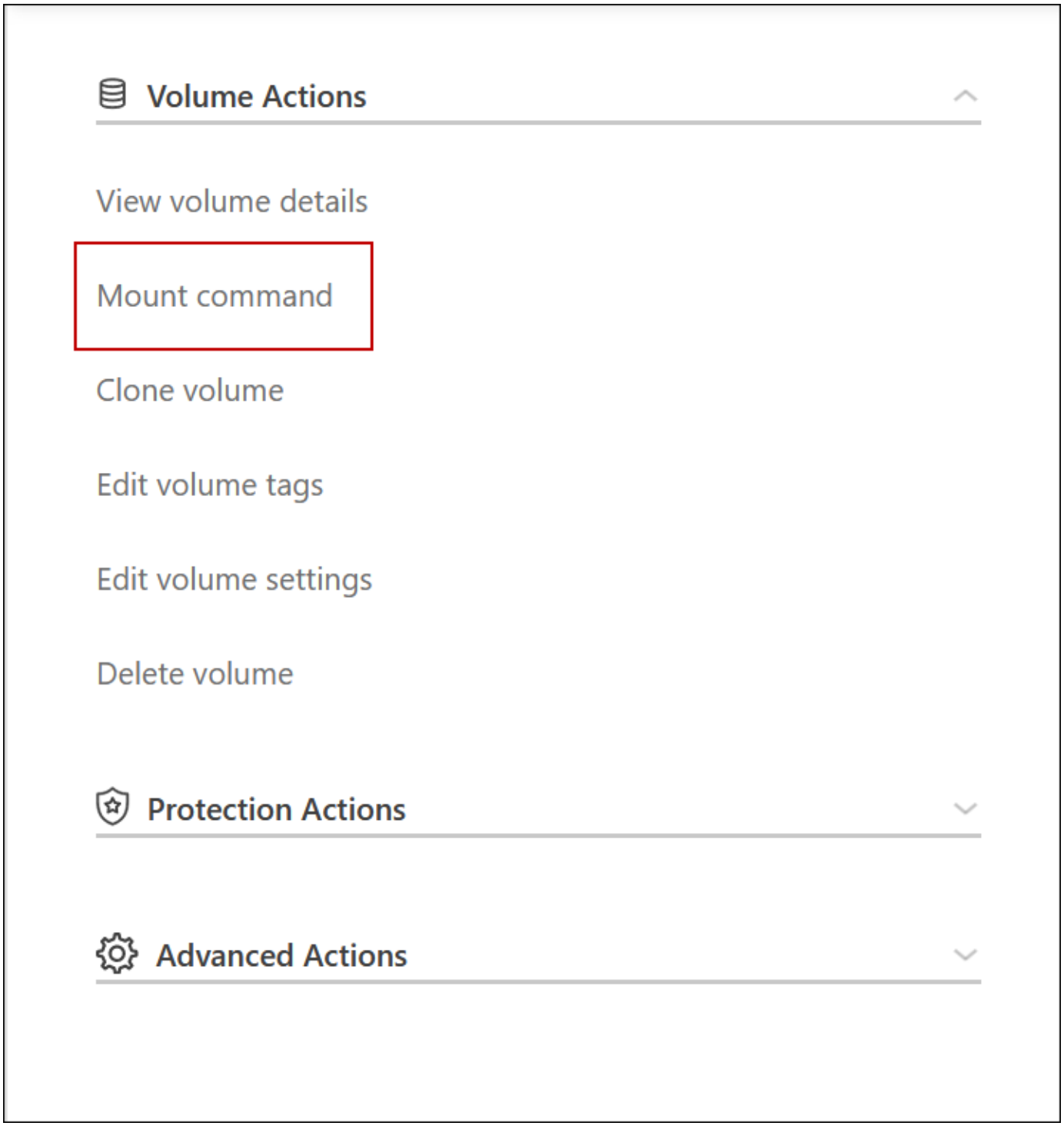
Weitere Informationen zur Leistung von Cloud Volumes ONTAP finden Sie unter"Performance" .

Clientzugriff auf Speicher

Clients sollten auf NFS- und CIFS-Volumes zugreifen, indem sie die Daten-IP-Adresse des Knotens verwenden, auf dem sich das Volume befindet. Wenn NAS-Clients über die IP-Adresse des Partnerknotens auf ein Volume zugreifen, wird der Datenverkehr zwischen beiden Knoten geleitet, was die Leistung verringert.

Wenn Sie ein Volume zwischen Knoten in einem HA-Paar verschieben, sollten Sie das Volume unter Verwendung der IP-Adresse des anderen Knotens erneut mounten. Andernfalls kann es zu Leistungseinbußen kommen. Wenn Clients NFSv4-Verweise oder Ordnerumleitungen für CIFS unterstützen, können Sie diese Funktionen auf den Cloud Volumes ONTAP Systemen aktivieren, um eine erneute Bereitstellung des Volumes zu vermeiden. Weitere Einzelheiten finden Sie in der ONTAP Dokumentation.

Sie können die richtige IP-Adresse in der Konsole ermitteln, indem Sie das Volume auswählen und auf **Mount Command** klicken.



Weiterführende Links

- "Informieren Sie sich über die Netzwerkanforderungen"
- "Erfahren Sie, wie Sie mit GCP beginnen"

Vorgänge sind nicht verfügbar, wenn ein Knoten im Cloud Volumes ONTAP HA-Paar offline ist

Wenn ein Knoten in einem HA-Paar nicht verfügbar ist, stellt der andere Knoten Daten für seinen Partner bereit, um einen kontinuierlichen Datendienst bereitzustellen. Dies wird

als *Speicherübernahme* bezeichnet. Einige Aktionen sind erst nach Abschluss der Speicherrückgabe verfügbar.

Wenn ein Knoten in einem HA-Paar nicht verfügbar ist, lautet der Status des Systems in der NetApp Console „Herabgestuft“.

Die folgenden Aktionen sind bei der Speicherübernahme nicht verfügbar:

- Support-Registrierung
- Lizenzänderungen
- Änderungen des Instanz- oder VM-Typs
- Änderungen der Schreibgeschwindigkeit
- CIFS-Einrichtung
- Ändern des Speicherorts von Konfigurationssicherungen
- Festlegen des Clusterkennworts
- Verwalten von Datenträgern und Aggregaten (erweiterte Zuweisung)

Diese Aktionen sind wieder verfügbar, nachdem die Speicherrückgabe abgeschlossen ist und der Zustand des Systems wieder in den Normalzustand zurückkehrt.

Erfahren Sie mehr über die Datenverschlüsselung und den Ransomware-Schutz von Cloud Volumes ONTAP

Cloud Volumes ONTAP unterstützt die Datenverschlüsselung und bietet Schutz vor Viren und Ransomware.

Verschlüsselung ruhender Daten

Cloud Volumes ONTAP unterstützt die folgenden Verschlüsselungstechnologien:

- NetApp -Verschlüsselungslösungen (NVE und NAE)
- AWS-Schlüsselverwaltungsdienst
- Azure Storage Service-Verschlüsselung
- Standardverschlüsselung der Google Cloud Platform

Sie können NetApp Verschlüsselungslösungen mit nativer Verschlüsselung Ihres Cloud-Anbieters verwenden, die Daten auf Hypervisor-Ebene verschlüsselt. Dadurch würde eine doppelte Verschlüsselung erreicht, die bei sehr sensiblen Daten wünschenswert sein könnte. Beim Zugriff auf die verschlüsselten Daten werden diese zweimal entschlüsselt: einmal auf Hypervisor-Ebene (mit Schlüsseln des Cloud-Anbieters) und dann erneut mithilfe von NetApp Verschlüsselungslösungen (mit Schlüsseln eines externen Schlüsselmanagers).

NetApp -Verschlüsselungslösungen (NVE und NAE)

Cloud Volumes ONTAP unterstützt "NetApp Volume Encryption (NVE) und NetApp Aggregate Encryption (NAE)" . NVE und NAE sind softwarebasierte Lösungen, die eine (FIPS) 140-2-konforme Data-at-Rest-Verschlüsselung von Volumes ermöglichen. Sowohl NVE als auch NAE verwenden die AES-256-Bit-Verschlüsselung.

- NVE verschlüsselt ruhende Daten jeweils auf einem Volume. Jedes Datenvolumen verfügt über einen eigenen, eindeutigen Verschlüsselungsschlüssel.
- NAE ist eine Erweiterung von NVE – es verschlüsselt Daten für jedes Volume und die Volumes teilen sich einen Schlüssel über das Aggregat hinweg. NAE ermöglicht außerdem die Deduplizierung gemeinsamer Blöcke über alle Volumes im Aggregat hinweg.

Cloud Volumes ONTAP unterstützt sowohl NVE als auch NAE mit externen Schlüsselverwaltungsdiensten (EKMs) von AWS, Azure und Google Cloud, einschließlich Lösungen von Drittanbietern wie Fortanix. Anders als bei ONTAP werden bei Cloud Volumes ONTAP die Verschlüsselungsschlüssel auf der Seite des Cloud-Anbieters und nicht in ONTAP generiert. Cloud Volumes ONTAP unterstützt nicht "Integrierter Schlüsselmanager".

Cloud Volumes ONTAP verwendet die standardmäßigen KMIP-Dienste (Key Management Interoperability Protocol), die ONTAP verwendet. Weitere Informationen zu den unterstützten Diensten finden Sie im "Interoperabilitätsmatrix-Tool" .

Wenn Sie NVE verwenden, haben Sie die Möglichkeit, den Schlüsseltresor Ihres Cloud-Anbieters zum Schutz der ONTAP Verschlüsselungsschlüssel zu verwenden:

- AWS-Schlüsselverwaltungsdienst (KMS)
- Azure-Schlüsseltresor (AKV)
- Google Cloud-Schlüsselverwaltungsdienst

Bei neuen Aggregaten ist die NetApp Aggregate Encryption (NAE) standardmäßig aktiviert, nachdem Sie einen externen Schlüsselmanager eingerichtet haben. Bei neuen Volumes, die nicht Teil eines NAE-Aggregats sind, ist NVE standardmäßig aktiviert (z. B. wenn Sie über vorhandene Aggregate verfügen, die vor der Einrichtung eines externen Schlüsselmanagers erstellt wurden).

Das Einrichten eines unterstützten Schlüsselmanagers ist der einzige erforderliche Schritt. Anweisungen zur Einrichtung finden Sie unter"Verschlüsseln Sie Volumes mit NetApp -Verschlüsselungslösungen" .

AWS-Schlüsselverwaltungsdienst

Wenn Sie ein Cloud Volumes ONTAP -System in AWS starten, können Sie die Datenverschlüsselung mithilfe des "AWS-Schlüsselverwaltungsdienst (KMS)" . Die NetApp Console fordert Datenschlüssel mithilfe eines Customer Master Key (CMK) an.

Sie können die AWS-Datenverschlüsselungsmethode nicht mehr ändern, nachdem Sie ein Cloud Volumes ONTAP System erstellt haben.

Wenn Sie diese Verschlüsselungsoption verwenden möchten, müssen Sie sicherstellen, dass das AWS KMS entsprechend eingerichtet ist. Weitere Informationen finden Sie unter"Einrichten des AWS KMS" .

Azure Storage Service-Verschlüsselung

Die Daten werden automatisch auf Cloud Volumes ONTAP in Azure verschlüsselt mit "Azure Storage Service-Verschlüsselung" mit einem von Microsoft verwalteten Schlüssel.

Sie können, wenn Sie möchten, Ihre eigenen Verschlüsselungsschlüssel verwenden. "Erfahren Sie, wie Sie Cloud Volumes ONTAP für die Verwendung eines vom Kunden verwalteten Schlüssels in Azure einrichten." .

Standardverschlüsselung der Google Cloud Platform

"Verschlüsselung ruhender Daten auf der Google Cloud Platform"ist standardmäßig für Cloud Volumes ONTAP aktiviert. Es ist keine Einrichtung erforderlich.

Während Google Cloud Storage Ihre Daten immer verschlüsselt, bevor sie auf die Festplatte geschrieben werden, können Sie mithilfe der Konsolen-APIs ein Cloud Volumes ONTAP -System erstellen, das *vom Kunden verwaltete Verschlüsselungsschlüssel* verwendet. Dies sind Schlüssel, die Sie mithilfe des Cloud Key Management Service in GCP generieren und verwalten. "Mehr erfahren" .

ONTAP -Virenscan

Sie können die integrierte Antivirenfunktion auf ONTAP -Systemen verwenden, um Daten vor der Gefährdung durch Viren oder anderen Schadcode zu schützen.

Der ONTAP Virenscan, genannt *Vscan*, kombiniert erstklassige Antivirensoftware von Drittanbietern mit ONTAP Funktionen, die Ihnen die nötige Flexibilität bieten, um zu steuern, welche Dateien wann gescannt werden.

Informationen zu den Anbietern, der Software und den von Vscan unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix" .

Informationen zum Konfigurieren und Verwalten der Antivirenfunktion auf ONTAP -Systemen finden Sie im "ONTAP 9 Antivirus-Konfigurationshandbuch" .

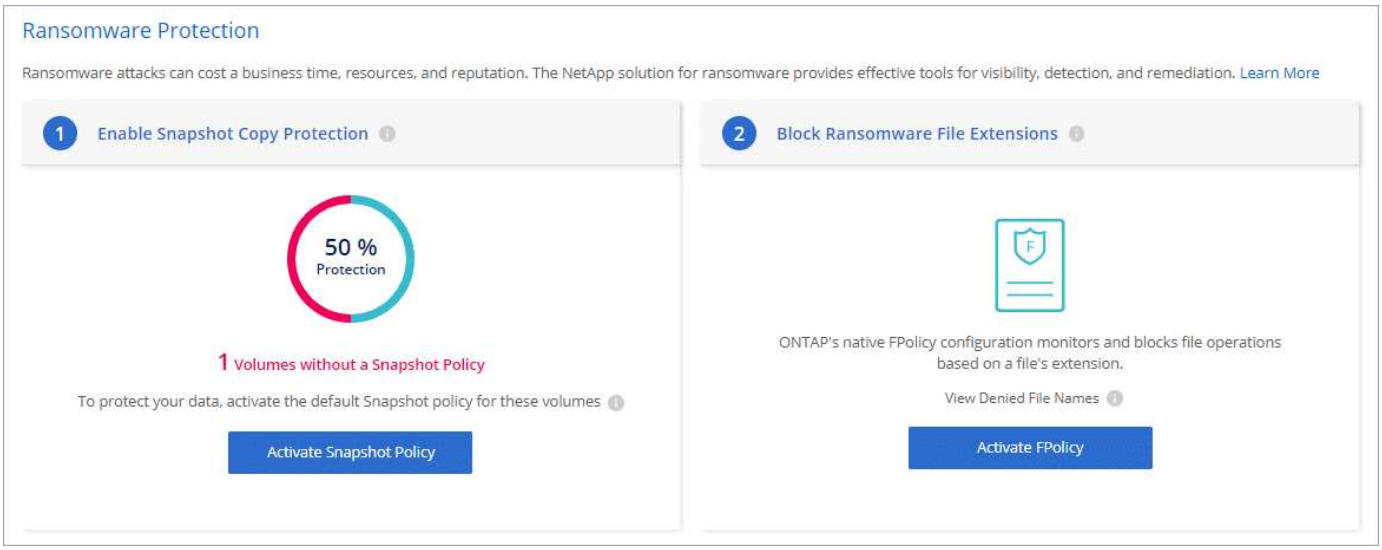
Ransomware-Schutz

Ransomware-Angriffe können ein Unternehmen Zeit, Ressourcen und Ansehen kosten. Mit der Konsole können Sie die NetApp -Lösung für Ransomware implementieren, die effektive Tools für Transparenz, Erkennung und Behebung bietet.

- Die Konsole identifiziert Volumes, die nicht durch eine Snapshot-Richtlinie geschützt sind, und ermöglicht Ihnen, die Standard-Snapshot-Richtlinie auf diesen Volumes zu aktivieren.

  Snapshot-Kopien sind schreibgeschützt, wodurch eine Beschädigung durch Ransomware verhindert wird. Sie können auch die Granularität bereitstellen, um Bilder einer einzelnen Dateikopie oder einer vollständigen Disaster-Recovery-Lösung zu erstellen.

- Mit der Konsole können Sie außerdem gängige Ransomware-Dateierweiterungen blockieren, indem Sie die FPolicy-Lösung von ONTAP aktivieren.



"Erfahren Sie, wie Sie die NetApp -Lösung für Ransomware implementieren" .

Erfahren Sie mehr über die Leistungsüberwachung für Cloud Volumes ONTAP -Workloads

Sie können die Leistungsergebnisse überprüfen, um zu entscheiden, welche Workloads für Cloud Volumes ONTAP geeignet sind.

Leistungstechnische Berichte

- Cloud Volumes ONTAP für AWS

  "NetApp Technical Report 4383: Leistungscharakterisierung von Cloud Volumes ONTAP in Amazon Web Services mit Anwendungs-Workloads"

- Cloud Volumes ONTAP für Microsoft Azure

  "NetApp Technical Report 4671: Leistungscharakterisierung von Cloud Volumes ONTAP in Azure mit Anwendungs-Workloads"

- Cloud Volumes ONTAP für Google Cloud

  "NetApp Technical Report 4816: Leistungscharakterisierung von Cloud Volumes ONTAP für Google Cloud"

CPU-Leistung

Cloud Volumes ONTAP -Knoten werden in den Überwachungstools Ihres Cloud-Anbieters als stark ausgelastet (über 90 %) angezeigt. Dies liegt daran, dass ONTAP alle der virtuellen Maschine bereitgestellten vCPUs reserviert, sodass sie bei Bedarf verfügbar sind.

Weitere Informationen finden Sie im "NetApp Knowledgebase-Artikel zur Überwachung der ONTAP CPU-Auslastung mithilfe der CLI"

Lizenzverwaltung für knotenbasiertes BYOL

Auf jedem Cloud Volumes ONTAP System mit einer knotenbasierten Bring-Your-Own-Lizenz (BYOL) muss eine Systemlizenz mit einem aktiven Abonnement installiert sein. Die NetApp Console vereinfacht den Vorgang, indem sie die Lizenzen für Sie verwaltet und vor Ablauf eine Warnung anzeigt.

Eine knotenbasierte Lizenz ist die Lizenz der vorherigen Generation für Cloud Volumes ONTAP. Eine knotenbasierte Lizenz kann von NetApp (BYOL) erworben werden und ist nur in bestimmten Fällen für Lizenzverlängerungen verfügbar.

"Erfahren Sie mehr über die Lizenzierungsoptionen von Cloud Volumes ONTAP" .

"Erfahren Sie mehr über die Verwaltung knotenbasierter Lizenzen" .

BYOL-Systemlizenzen

Knotenbasierte Lizenzen können von NetApp bezogen werden. Die Anzahl der Lizenzen, die Sie für ein Einzelknotensystem oder ein HA-Paar erwerben können, ist unbegrenzt.

NetApp hat den Erwerb, die Verlängerung und die Erneuerung von BYOL-Lizenzen eingeschränkt. Weitere Informationen finden Sie unter "Eingeschränkte Verfügbarkeit der BYOL-Lizenzierung für Cloud Volumes ONTAPP" .

Eine knotenbasierte Lizenz bietet bis zu 368 TiB Kapazität für einen einzelnen Knoten oder ein HA-Paar. Möglicherweise haben Sie mehrere Lizenzen für ein Cloud Volumes ONTAP BYOL-System erworben, um mehr als 368 TiB Kapazität zuzuweisen. Beispielsweise könnten Sie zwei Lizenzen besitzen, um Cloud Volumes ONTAP bis zu 736 TiB Kapazität zuzuweisen. Oder Sie könnten vier Lizenzen besitzen, um bis zu 1,4 PiB zu erhalten.

Beachten Sie, dass Festplattenlimits Sie daran hindern können, die Kapazitätsgrenze zu erreichen, wenn Sie nur Festplatten verwenden. Sie können das Festplattenlimit überschreiten, indem Sie"Tiering inaktiver Daten in den Objektspeicher" . Informationen zu Festplattenlimits finden Sie unter "Speicherlimits in den Cloud Volumes ONTAP Versionshinweisen" .

Lizenzmanagement für ein neues System

Wenn Sie ein knotenbasiertes BYOL-System erstellen, werden Sie von der Konsole aufgefordert, die Seriennummer Ihrer Lizenz und Ihr NetApp Support Site-Konto einzugeben. Die Konsole verwendet das Konto, um die Lizenzdatei von NetApp herunterzuladen und auf dem Cloud Volumes ONTAP System zu installieren.

"Erfahren Sie, wie Sie NetApp Support Site-Konten zur Konsole hinzufügen" .

Wenn die Konsole über die sichere Internetverbindung nicht auf die Lizenzdatei zugreifen kann, können Sie"Besorgen Sie sich die Datei selbst und laden Sie sie dann manuell in die Konsole hoch" .

Lizenzablauf

Die Konsole zeigt 30 Tage vor Ablauf einer knotenbasierten Lizenz eine Warnung an und erneut, wenn die Lizenz abläuft. Das folgende Bild zeigt eine 30-tägige Ablaufwarnung, die in der Benutzeroberfläche angezeigt wird:

Sie können das System auswählen, um die Nachricht zu überprüfen.

Die Konsole enthält eine Warnung zum Ablauf der Lizenz im Cloud Volumes ONTAP -Bericht, der Ihnen per E-Mail zugesandt wird, wenn Sie ein Organisations- oder Kontoadministrator sind und die Option aktiviert haben. Der per E-Mail versendete Bericht enthält alle zwei Wochen eine Warnung zum Ablauf der Lizenz.

Wenn Sie die Lizenz nicht rechtzeitig erneuern, schaltet sich das Cloud Volumes ONTAP System selbst ab. Wenn Sie es neu starten, fährt es sich wieder herunter.

Lizenzerneuerung

Wenn Sie ein knotenbasiertes BYOL-Abonnement verlängern, indem Sie sich an einen NetApp -Vertreter wenden, erhält die Konsole automatisch die neue Lizenz von NetApp und installiert sie auf dem Cloud Volumes ONTAP System.

Wenn die Konsole über die sichere Internetverbindung nicht auf die Lizenzdatei zugreifen kann, können Sie"Besorgen Sie sich die Datei selbst und laden Sie sie dann manuell in die Konsole hoch" .

Lizenzübertragung auf ein neues System

Eine knotenbasierte BYOL-Lizenz ist zwischen Cloud Volumes ONTAP Systemen übertragbar, wenn Sie ein vorhandenes System löschen und dann mit derselben Lizenz ein neues erstellen.

Beispielsweise möchten Sie möglicherweise ein vorhandenes lizenziertes System löschen und die Lizenz dann mit einem neuen BYOL-System bei einem anderen VPC/VNet oder Cloud-Anbieter verwenden. Beachten Sie, dass bei allen Cloud-Anbietern nur *Cloud-agnostische* Seriennummern funktionieren. Cloud-agnostische Seriennummern beginnen mit dem Präfix *908xxxx*.

Es ist wichtig zu beachten, dass Ihre BYOL-Lizenz an Ihr Unternehmen und einen bestimmten Satz von Anmeldeinformationen für die NetApp -Support-Site gebunden ist.

Erfahren Sie, wie AutoSupport und Digital Advisor für Cloud Volumes ONTAP verwendet werden

Die AutoSupport Komponente von ONTAP sammelt Telemetriedaten und sendet sie zur Analyse. Active IQ Digital Advisor (auch bekannt als Digital Advisor) analysiert die Daten von AutoSupport und bietet proaktive Betreuung und Optimierung. Mithilfe künstlicher Intelligenz kann Digital Advisor potenzielle Probleme erkennen und Ihnen bei der Lösung helfen, bevor sie sich auf Ihr Unternehmen auswirken.

Mit Digital Advisor können Sie Ihre Dateninfrastruktur in Ihrer globalen Hybrid Cloud optimieren, indem Sie über ein Cloud-basiertes Portal und eine mobile App umsetzbare prädiktive Analysen und proaktiven Support bereitstellen. Datenbasierte Erkenntnisse und Empfehlungen von Digital Advisor stehen allen NetApp -Kunden mit einem aktiven SupportEdge -Vertrag zur Verfügung (Funktionen variieren je nach Produkt und

Supportstufe).

Hier sind einige Dinge, die Sie mit Digital Advisor tun können:

- Planen Sie Upgrades.

  Digital Advisor identifiziert Probleme in Ihrer Umgebung, die durch ein Upgrade auf eine neuere Version von ONTAP behoben werden können, und die Komponente Upgrade Advisor unterstützt Sie bei der Planung eines erfolgreichen Upgrades.

- Systemgesundheit anzeigen.

  Ihr Digital Advisor -Dashboard meldet alle Wellnessprobleme und hilft Ihnen, diese zu beheben. Überwachen Sie die Systemkapazität, um sicherzustellen, dass Ihnen nie der Speicherplatz ausgeht. Zeigen Sie Supportfälle für Ihr System an.

- Leistung verwalten.

  Digital Advisor zeigt die Systemleistung über einen längeren Zeitraum an, als Sie im ONTAP System Manager sehen können. Identifizieren Sie Konfigurations- und Systemprobleme, die Ihre Leistung beeinträchtigen. Maximieren Sie die Effizienz. Zeigen Sie Kennzahlen zur Speichereffizienz an und ermitteln Sie Möglichkeiten, mehr Daten auf weniger Speicherplatz zu speichern.

- Inventar und Konfiguration anzeigen.

  Digital Advisor zeigt vollständige Inventar- und Software- und Hardwarekonfigurationsinformationen an. Informieren Sie sich über das Ablaufdatum von Serviceverträgen und verlängern Sie diese, um sicherzustellen, dass Sie weiterhin unterstützt werden.

Weiterführende Links

- "NetApp Dokumentation: Digital Advisor"
- "Starten Sie den Digital Advisor"
- "SupportEdge -Dienste"

Unterstützte Standardkonfigurationen für Cloud Volumes ONTAP

Wenn Sie wissen, wie Cloud Volumes ONTAP standardmäßig konfiguriert ist, können Sie Ihre Systeme leichter einrichten und verwalten, insbesondere wenn Sie mit ONTAP vertraut sind, da sich die Standardkonfiguration für Cloud Volumes ONTAP von der von ONTAP unterscheidet.

Standard-Setup

- Die NetApp Console erstellt bei der Bereitstellung von Cloud Volumes ONTAP eine datenbereitstellende Speicher-VM. Einige Konfigurationen unterstützen zusätzliche Speicher-VMs. "Erfahren Sie mehr über die Verwaltung von Speicher-VMs" .

  Ab der Version 3.9.5 ist die logische Speicherplatzberichterstattung auf der ersten Speicher-VM aktiviert. Wenn der Speicherplatz logisch gemeldet wird, meldet ONTAP den Volume-Speicherplatz so, dass der gesamte durch die Speichereffizienzfunktionen eingesparte physische Speicherplatz auch als verwendet

gemeldet wird. Informationen zu den Effizienzfunktionen für Inline-Speicher finden Sie im Knowledge Base-Artikel "KB: Welche Inline-Speichereffizienzfunktionen werden mit CVO unterstützt?"

- Die Konsole installiert automatisch die folgenden ONTAP Funktionslizenzen auf Cloud Volumes ONTAP:
  - CIFS
  - FlexCache
  - FlexClone
  - iSCSI
  - Multi-Tenant Encryption Key Management (MTEKM), beginnend mit Cloud Volumes ONTAP 9.12.1 GA
  - NetApp Volume Encryption (nur für Bring Your Own License (BYOL) oder registrierte Pay-as-you-go (PAYGO)-Systeme)
  - NFS ifdef::aws[] endif::aws[] ifdef::azure[] endif::azure[]
  - SnapMirror
  - SnapRestore
  - SnapVault
- Standardmäßig werden mehrere Netzwerkschnittstellen erstellt:
  - Ein Cluster-Management-LIF
  - Ein Cluster-übergreifendes LIF
- Ein SVM-Verwaltungs-LIF auf HA-Systemen in Azure
- Ein SVM-Verwaltungs-LIF auf HA-Systemen in Google Cloud
- Ein SVM-Management-LIF auf Single-Node-Systemen in AWS
- Ein Knotenverwaltungs-LIF

+ In Google Cloud wird dieses LIF mit dem Intercluster-LIF kombiniert.

- Ein iSCSI-Daten-LIF
- Ein CIFS- und NFS-Daten-LIF

> Aufgrund der Anforderungen des Cloud-Anbieters ist LIF-Failover für Cloud Volumes ONTAP standardmäßig deaktiviert. Durch die Migration eines LIF auf einen anderen Port wird die externe Zuordnung zwischen IP-Adressen und Netzwerkschnittstellen auf der Instanz unterbrochen, wodurch der LIF nicht mehr zugänglich ist.

  - Cloud Volumes ONTAP sendet Konfigurationssicherungen per HTTP an den Konsolenagenten.

    Auf die Sicherungen kann über http://ipaddress/occm/offboxconfig/ zugegriffen werden, wobei *ipaddress* die IP-Adresse des Hosts des Konsolenagenten ist.

    Sie können die Backups zur Neukonfiguration Ihres Cloud Volumes ONTAP Systems verwenden. Weitere Informationen zu Konfigurationssicherungen finden Sie im "ONTAP-Dokumentation" .

  - Die Konsole legt einige Volume-Attribute anders fest als andere Verwaltungstools (z. B. ONTAP System Manager oder ONTAP CLI).

    In der folgenden Tabelle sind die Volumeattribute aufgeführt, die von den Standardeinstellungen abweichen:

Attribut	Wert, den die Konsole konfiguriert
Autosize-Modus	wachsen
Maximale automatische Größe	1.000 Prozent Der Organisations- oder Kontoadministrator kann diesen Wert auf der Seite „Einstellungen“ ändern.
Sicherheitsstil	NTFS für CIFS-Volumes UNIX für NFS-Volumes
Platzgarantie Stil	keiner
UNIX-Berechtigungen (nur NFS)	777

+
Informationen zu diesen Attributen finden Sie unter"ONTAP *volume create* Manpage" .

Interne Festplatten für Systemdaten

Zusätzlich zum Speicher für Benutzerdaten erwirbt die Konsole auch Cloud-Speicher für Systemdaten.

AWS

- Drei Festplatten pro Knoten für Boot-, Root- und Core-Daten:
  - 47 GiB io1-Festplatte für Bootdaten
  - 140 GiB GP3-Disk für Root-Daten
  - 540 GiB GP2-Festplatte für Kerndaten
- Für HA-Paare:
  - Zwei st1-EBS-Volumes für die Mediator-Instanz, eines mit ca. 8 GiB als Root-Disk und eines mit 4 GiB als Datendiskette
  - Eine 140 GiB große gp3-Festplatte in jedem Knoten, die eine Kopie der Stammdaten des anderen Knotens enthält

    In einigen Zonen kann der verfügbare EBS-Festplattentyp nur gp2 sein.
- Ein EBS-Snapshot für jede Boot- und Root-Festplatte

  Beim Neustart werden automatisch Snapshots erstellt.
- Wenn Sie die Datenverschlüsselung in AWS mithilfe des Key Management Service (KMS) aktivieren, werden auch die Boot- und Root-Datenträger für Cloud Volumes ONTAP verschlüsselt. Dazu gehört die Bootdiskette für die Mediatorinstanz in einem HA-Paar. Die Festplatten werden mit dem CMK verschlüsselt, den Sie beim Hinzufügen eines Cloud Volumes ONTAP Systems auswählen.

In AWS befindet sich NVRAM auf der Startdiskette.

Azure (einzelner Knoten)

- Drei Premium-SSD-Festplatten:
  - Eine 10-GiB-Festplatte für Startdaten
  - Eine 140-GiB-Festplatte für Root-Daten
  - Eine 512-GiB-Festplatte für NVRAM

    Wenn die von Ihnen für Cloud Volumes ONTAP ausgewählte virtuelle Maschine Ultra-SSDs unterstützt, verwendet das System für NVRAM eine 32-GiB-Ultra-SSD anstelle einer Premium-SSD.
- Eine 1024 GiB Standard-HDD-Festplatte zum Speichern von Kernen
- Ein Azure-Snapshot für jede Startdiskette und jede Root-Diskette
- Jeder Datenträger in Azure wird standardmäßig im Ruhezustand verschlüsselt.

  Wenn die virtuelle Maschine, die Sie für Cloud Volumes ONTAP ausgewählt haben, Premium SSD v2 Managed Disk als Datenträger unterstützt, verwendet das System eine 32 GiB Premium SSD v2 Managed Disk für NVRAM und eine weitere als Root-Datenträger.

Azure (HA-Paar)

HA-Paare mit Seitenblob

- Zwei 10 GiB Premium SSD-Datenträger für das Startvolume (einer pro Knoten)
- Zwei 140 GiB Premium Storage-Seitenblobs für das Stammvolume (einer pro Knoten)
- Zwei 1024 GiB Standard-HDD-Festplatten zum Speichern von Kernen (eine pro Knoten)
- Zwei 512 GiB Premium SSD-Festplatten für NVRAM (eine pro Knoten)
- Ein Azure-Snapshot für jede Startdiskette und jede Root-Diskette

  Beim Neustart werden automatisch Snapshots erstellt.
- Jeder Datenträger in Azure wird standardmäßig im Ruhezustand verschlüsselt.

HA-Paare mit gemeinsam genutzten verwalteten Datenträgern in mehreren Verfügbarkeitszonen

- Zwei 10 GiB Premium SSD-Datenträger für das Startvolume (einer pro Knoten)
- Zwei 512 GiB Premium SSD-Datenträger für das Stammvolume (einer pro Knoten)
- Zwei 1024 GiB Standard-HDD-Festplatten zum Speichern von Kernen (eine pro Knoten)
- Zwei 512 GiB Premium SSD-Festplatten für NVRAM (eine pro Knoten)
- Ein Azure-Snapshot für jede Startdiskette und jede Root-Diskette

  Beim Neustart werden automatisch Snapshots erstellt.
- Jeder Datenträger in Azure wird standardmäßig im Ruhezustand verschlüsselt.

HA-Paare mit gemeinsam genutzten verwalteten Datenträgern in einzelnen Verfügbarkeitszonen

- Zwei 10 GiB Premium SSD-Datenträger für das Startvolume (einer pro Knoten)

- Zwei 512 GiB Premium SSD Shared Managed Disks für das Stammvolume (einer pro Knoten)
- Zwei 1024 GiB Standard-HDD-Festplatten zum Speichern von Kernen (eine pro Knoten)
- Zwei 512 GiB Premium SSD Managed Disks für NVRAM (eine pro Knoten)

Wenn Ihre virtuelle Maschine Premium SSD v2 Managed Disks als Datenträger unterstützt, verwendet sie 32 GiB Premium SSD v2 Managed Disks für NVRAM und 512 GiB Premium SSD v2 Shared Managed Disks für das Stammvolume.

Sie können HA-Paare in einer einzigen Verfügbarkeitszone bereitstellen und verwaltete SSD Premium v2-Datenträger verwenden, wenn die folgenden Bedingungen erfüllt sind:

- Die Version von Cloud Volumes ONTAP ist 9.15.1 oder höher.
- Die ausgewählte Region und Zone unterstützen Premium SSD v2 Managed Disks. Informationen zu den unterstützten Regionen finden Sie unter "Microsoft Azure-Website: Verfügbare Produkte nach Region" .
- Das Abonnement ist für Microsoft registriert"Microsoft.Compute/VMOrchestratorZonalMultiFD-Funktion" .

Google Cloud (einzelner Knoten)

- Eine persistente SSD-Festplatte mit 10 GiB für Startdaten
- Eine persistente 64-GiB-SSD-Festplatte für Root-Daten
- Eine persistente SSD-Festplatte mit 500 GiB für NVRAM
- Eine persistente Standardfestplatte mit 315 GiB zum Speichern von Kernen
- Snapshots für Boot- und Root-Daten

  Beim Neustart werden automatisch Snapshots erstellt.

- Boot- und Root-Disks sind standardmäßig verschlüsselt.

Google Cloud (HA-Paar)

- Zwei persistente 10-GiB-SSD-Festplatten für Startdaten
- Vier persistente 64-GiB-SSD-Festplatten für Root-Daten
- Zwei persistente SSD-Festplatten mit 500 GiB für NVRAM
- Zwei persistente Standard-Festplatten mit 315 GiB zum Speichern von Kernen
- Eine persistente 10-GiB-Standardfestplatte für Mediatordaten
- Eine persistente 10-GiB-Standardfestplatte für Mediator-Bootdaten
- Snapshots für Boot- und Root-Daten

  Beim Neustart werden automatisch Snapshots erstellt.

- Boot- und Root-Disks sind standardmäßig verschlüsselt.

Wo sich die Festplatten befinden

Speicherlayout:

- Die Startdaten befinden sich auf einer Festplatte, die an die Instanz oder virtuelle Maschine angeschlossen

ist.

Diese Festplatte, die das Boot-Image enthält, ist für Cloud Volumes ONTAP nicht verfügbar.

- Root-Daten, die die Systemkonfiguration und Protokolle enthalten, befinden sich in aggr0.
- Das Stammvolume der Storage Virtual Machine (SVM) befindet sich in aggr1.
- Datenvolumes befinden sich auch in aggr1.

Wissen und Unterstützung

Für Support registrieren

Um technischen Support speziell für die NetApp Console und ihre Speicherlösungen und Datendienste zu erhalten, ist eine Support-Registrierung erforderlich. Eine Support-Registrierung ist auch erforderlich, um wichtige Workflows für Cloud Volumes ONTAP Systeme zu aktivieren.

Durch die Registrierung für den Support wird kein NetApp Support für den Dateidienst eines Cloud-Anbieters aktiviert. Technischen Support für den Dateidienst eines Cloud-Anbieters, seine Infrastruktur oder eine Lösung, die den Dienst nutzt, erhalten Sie unter „Hilfe erhalten“ in der Dokumentation des jeweiligen Produkts.

- "Amazon FSx für ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Übersicht zur Support-Registrierung

Zur Aktivierung des Supportanspruchs stehen zwei Registrierungsformen zur Verfügung:

- Registrieren Sie die Seriennummer Ihres NetApp Console (Ihre 20-stellige Seriennummer 960xxxxxxxxx, die Sie auf der Seite „Supportressourcen“ in der Konsole finden).

  Dies dient als Ihre einzige Support-Abonnement-ID für alle Dienste innerhalb der Konsole. Jedes Konsolenkonto muss registriert werden.

- Registrieren Sie die mit einem Abonnement verknüpften Cloud Volumes ONTAP Seriennummern im Marktplatz Ihres Cloud-Anbieters (dies sind 20-stellige 909201xxxxxxxx-Seriennummern).

  Diese Seriennummern werden allgemein als *PAYGO-Seriennummern* bezeichnet und von der NetApp Console zum Zeitpunkt der Bereitstellung von Cloud Volumes ONTAP generiert.

Durch die Registrierung beider Seriennummerntypen werden Funktionen wie das Öffnen von Support-Tickets und die automatische Fallgenerierung ermöglicht. Die Registrierung wird abgeschlossen, indem Sie der Konsole NetApp Support Site (NSS)-Konten hinzufügen, wie unten beschrieben.

Registrieren Sie die NetApp Console für den NetApp Support

Um sich für den Support zu registrieren und den Supportanspruch zu aktivieren, muss ein Benutzer in Ihrem NetApp Console seinem Konsolen-Login ein NetApp Support-Site-Konto zuordnen. Wie Sie sich für den NetApp Support registrieren, hängt davon ab, ob Sie bereits über ein NetApp Support Site (NSS)-Konto verfügen.

Bestandskunde mit NSS-Konto

Wenn Sie ein NetApp -Kunde mit einem NSS-Konto sind, müssen Sie sich lediglich über die Konsole für den Support registrieren.

Schritte

1. Wählen Sie **Administration** > **Anmeldeinformationen**.
2. Wählen Sie **Benutzeranmeldeinformationen**.
3. Wählen Sie **NSS-Anmeldeinformationen hinzufügen** und folgen Sie der Authentifizierungsaufforderung der NetApp Support Site (NSS).
4. Um zu bestätigen, dass der Registrierungsvorgang erfolgreich war, wählen Sie das Hilfesymbol und dann **Support**.

   Auf der Seite **Ressourcen** sollte angezeigt werden, dass Ihr Konsolenkonto für den Support registriert ist.

   Beachten Sie, dass anderen Konsolenbenutzern dieser Support-Registrierungsstatus nicht angezeigt wird, wenn sie ihrem Login kein NetApp Support Site-Konto zugeordnet haben. Dies bedeutet jedoch nicht, dass Ihr Konto nicht für den Support registriert ist. Sofern ein Benutzer in der Organisation diese Schritte befolgt hat, wurde Ihr Konto registriert.

Bestandskunde, aber kein NSS-Konto

Wenn Sie bereits NetApp -Kunde mit vorhandenen Lizenzen und Seriennummern, aber *keinem* NSS-Konto sind, müssen Sie ein NSS-Konto erstellen und es mit Ihrem Konsolen-Login verknüpfen.

Schritte

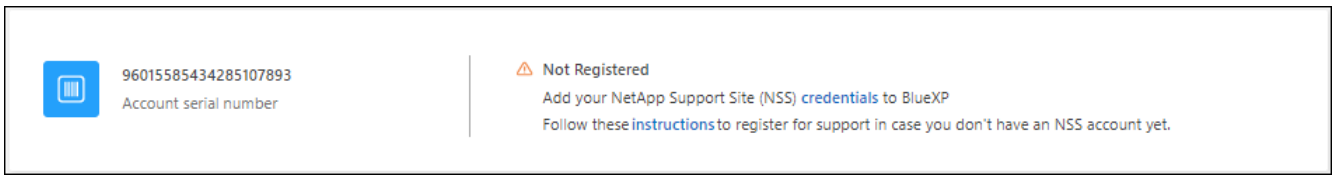
1. Erstellen Sie ein NetApp Support Site-Konto, indem Sie das "Registrierungsformular für Benutzer der NetApp Support-Site"
   a. Achten Sie darauf, die entsprechende Benutzerebene auszuwählen, in der Regel „NetApp -Kunde/Endbenutzer“.
   b. Denken Sie daran, die Seriennummer des Konsolenkontos (960xxxx) zu kopieren, die oben für das Feld „Seriennummer“ verwendet wurde. Dies beschleunigt die Kontobearbeitung.
2. Verknüpfen Sie Ihr neues NSS-Konto mit Ihrem Konsolen-Login, indem Sie die folgenden Schritte ausführenBestandskunde mit NSS-Konto .

Ganz neu bei NetApp

Wenn Sie NetApp noch nicht kennen und kein NSS-Konto haben, befolgen Sie die nachstehenden Schritte.

Schritte

1. Wählen Sie oben rechts in der Konsole das Hilfesymbol und dann **Support** aus.
2. Suchen Sie auf der Support-Registrierungsseite nach der Seriennummer Ihrer Konto-ID.



3. Navigieren Sie zu "Support-Registrierungssite von NetApp" und wählen Sie **Ich bin kein registrierter NetApp -Kunde**.
4. Füllen Sie die Pflichtfelder (mit roten Sternchen gekennzeichnet) aus.
5. Wählen Sie im Feld **Produktlinie Cloud Manager** und dann Ihren entsprechenden Abrechnungsanbieter aus.
6. Kopieren Sie die Seriennummer Ihres Kontos aus Schritt 2 oben, schließen Sie die Sicherheitsüberprüfung

ab und bestätigen Sie anschließend, dass Sie die globale Datenschutzrichtlinie von NetApp gelesen haben.

Um diese sichere Transaktion abzuschließen, wird umgehend eine E-Mail an das angegebene Postfach gesendet. Überprüfen Sie unbedingt Ihren Spam-Ordner, wenn die Bestätigungs-E-Mail nicht innerhalb weniger Minuten eintrifft.

7. Bestätigen Sie die Aktion in der E-Mail.

   Durch die Bestätigung wird Ihre Anfrage an NetApp übermittelt und es wird empfohlen, dass Sie ein NetApp Support Site-Konto erstellen.

8. Erstellen Sie ein NetApp Support Site-Konto, indem Sie das "Registrierungsformular für Benutzer der NetApp Support-Site"
   a. Achten Sie darauf, die entsprechende Benutzerebene auszuwählen, in der Regel „NetApp -Kunde/Endbenutzer“.
   b. Denken Sie daran, die oben für das Seriennummernfeld verwendete Kontoseriennummer (960xxxx) zu kopieren. Dadurch wird die Bearbeitung beschleunigt.

Nach Abschluss

NetApp sollte sich während dieses Vorgangs mit Ihnen in Verbindung setzen. Dies ist eine einmalige Onboarding-Übung für neue Benutzer.

Sobald Sie über Ihr NetApp Support Site-Konto verfügen, verknüpfen Sie das Konto mit Ihrem Konsolen-Login, indem Sie die folgenden Schritte ausführenBestandskunde mit NSS-Konto .

NSS-Anmeldeinformationen für Cloud Volumes ONTAP Support zuordnen

Um die folgenden wichtigen Workflows für Cloud Volumes ONTAP zu aktivieren, müssen Sie Ihrem Konsolenkonto Anmeldeinformationen für die NetApp Support Site zuordnen:

- Registrieren von Pay-as-you-go Cloud Volumes ONTAP Systemen für den Support

  Die Angabe Ihres NSS-Kontos ist erforderlich, um den Support für Ihr System zu aktivieren und Zugriff auf die technischen Supportressourcen von NetApp zu erhalten.

- Bereitstellen von Cloud Volumes ONTAP mit eigener Lizenz (BYOL)

  Die Angabe Ihres NSS-Kontos ist erforderlich, damit die Konsole Ihren Lizenzschlüssel hochladen und das Abonnement für die von Ihnen erworbene Laufzeit aktivieren kann. Hierzu gehören automatische Updates bei Laufzeitverlängerungen.

- Aktualisieren der Cloud Volumes ONTAP -Software auf die neueste Version

Die Zuordnung von NSS-Anmeldeinformationen zu Ihrem NetApp Console unterscheidet sich von der Zuordnung des NSS-Kontos zu einer Konsolenbenutzeranmeldung.

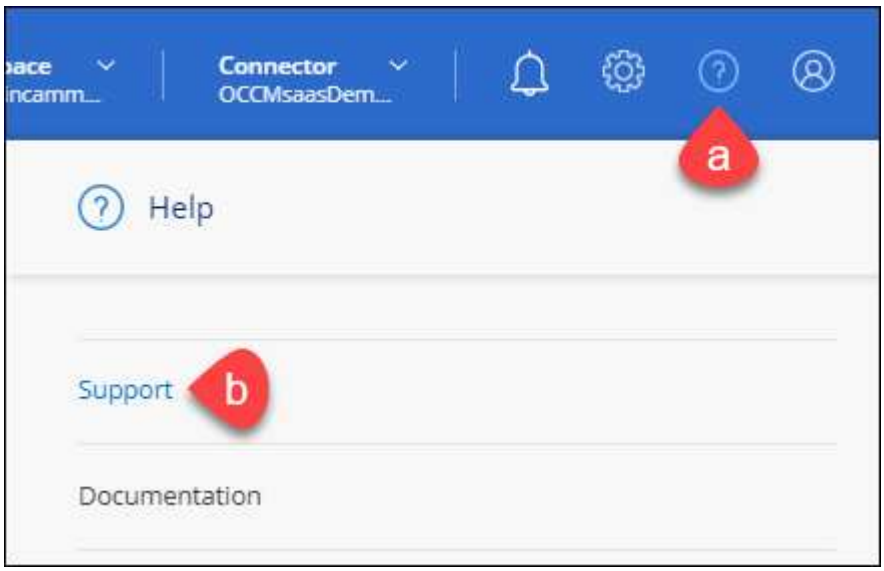
Diese NSS-Anmeldeinformationen sind mit Ihrer spezifischen Konsolenkonto-ID verknüpft. Benutzer, die zur Konsolenorganisation gehören, können über **Support > NSS-Verwaltung** auf diese Anmeldeinformationen zugreifen.

- Wenn Sie über ein Konto auf Kundenebene verfügen, können Sie ein oder mehrere NSS-Konten hinzufügen.

- Wenn Sie über ein Partner- oder Reseller-Konto verfügen, können Sie ein oder mehrere NSS-Konten hinzufügen, diese können jedoch nicht zusammen mit Konten auf Kundenebene hinzugefügt werden.

Schritte

1. Wählen Sie oben rechts in der Konsole das Hilfesymbol und dann **Support** aus.



2. Wählen Sie **NSS-Verwaltung > NSS-Konto hinzufügen**.
3. Wenn Sie dazu aufgefordert werden, wählen Sie **Weiter**, um zu einer Microsoft-Anmeldeseite weitergeleitet zu werden.

   NetApp verwendet Microsoft Entra ID als Identitätsanbieter für Authentifizierungsdienste speziell für Support und Lizenzierung.

4. Geben Sie auf der Anmeldeseite Ihre bei der NetApp Support Site registrierte E-Mail-Adresse und Ihr Kennwort ein, um den Authentifizierungsprozess durchzuführen.

   Diese Aktionen ermöglichen der Konsole, Ihr NSS-Konto für Dinge wie Lizenzdownloads, Überprüfung von Software-Upgrades und zukünftige Support-Registrierungen zu verwenden.

   Beachten Sie Folgendes:

   - Das NSS-Konto muss ein Konto auf Kundenebene sein (kein Gast- oder temporäres Konto). Sie können mehrere NSS-Konten auf Kundenebene haben.
   - Es kann nur ein NSS-Konto geben, wenn es sich bei diesem Konto um ein Konto auf Partnerebene handelt. Wenn Sie versuchen, NSS-Konten auf Kundenebene hinzuzufügen und ein Konto auf Partnerebene vorhanden ist, erhalten Sie die folgende Fehlermeldung:

     „Der NSS-Kundentyp ist für dieses Konto nicht zulässig, da bereits NSS-Benutzer eines anderen Typs vorhanden sind.“

   Dasselbe gilt, wenn Sie bereits über NSS-Konten auf Kundenebene verfügen und versuchen, ein Konto auf Partnerebene hinzuzufügen.

   - Nach erfolgreicher Anmeldung speichert NetApp den NSS-Benutzernamen.

     Dies ist eine vom System generierte ID, die Ihrer E-Mail-Adresse zugeordnet ist. Auf der Seite **NSS-Verwaltung** können Sie Ihre E-Mail-Adresse aus dem ••• Speisekarte.

- Wenn Sie Ihre Anmeldeinformationen aktualisieren müssen, gibt es auch die Option **Anmeldeinformationen aktualisieren** im ••• Speisekarte.

  Bei Verwendung dieser Option werden Sie aufgefordert, sich erneut anzumelden. Beachten Sie, dass das Token für diese Konten nach 90 Tagen abläuft. Sie werden durch eine entsprechende Benachrichtigung darauf aufmerksam gemacht.

Hilfe erhalten

NetApp bietet auf vielfältige Weise Support für die NetApp Console und ihre Cloud-Dienste. Umfangreiche kostenlose Selbsthilfeoptionen stehen rund um die Uhr zur Verfügung, beispielsweise Knowledge Base-Artikel (KB) und ein Community-Forum. Ihre Support-Registrierung beinhaltet technischen Remote-Support per Web-Ticketing.

Erhalten Sie Unterstützung für den Dateidienst eines Cloud-Anbieters

Technischen Support zu einem Dateidienst eines Cloud-Anbieters, seiner Infrastruktur oder einer Lösung, die den Dienst nutzt, finden Sie in der Dokumentation zu diesem Produkt.

- "Amazon FSx für ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Um technischen Support speziell für NetApp und seine Speicherlösungen und Datendienste zu erhalten, verwenden Sie die unten beschriebenen Supportoptionen.

Nutzen Sie Möglichkeiten zur Selbsthilfe

Diese Optionen stehen Ihnen 24 Stunden am Tag, 7 Tage die Woche kostenlos zur Verfügung:

- Dokumentation

  Die NetApp Console Konsolendokumentation, die Sie gerade anzeigen.

- "Wissensdatenbank"

  Durchsuchen Sie die NetApp Wissensdatenbank nach hilfreichen Artikeln zur Problembehebung.

- "Gemeinschaften"

  Treten Sie der NetApp Console Community bei, um aktuelle Diskussionen zu verfolgen oder neue zu starten.

Erstellen Sie einen Fall mit dem NetApp Support

Zusätzlich zu den oben genannten Self-Support-Optionen können Sie nach der Aktivierung des Supports mit einem NetApp -Support-Spezialisten zusammenarbeiten, um alle Probleme zu lösen.

Bevor Sie beginnen

- Um die Funktion **Fall erstellen** zu verwenden, müssen Sie zunächst Ihre Anmeldeinformationen für die NetApp -Support-Site mit Ihrem Konsolen-Login verknüpfen. "Erfahren Sie, wie Sie die mit Ihrer

Konsolenanmeldung verknüpften Anmeldeinformationen verwalten." .

- Wenn Sie einen Fall für ein ONTAP -System mit einer Seriennummer eröffnen, muss Ihr NSS-Konto mit der Seriennummer für dieses System verknüpft sein.

Schritte

1. Wählen Sie in der NetApp Console*Hilfe > Support*.
2. Wählen Sie auf der Seite **Ressourcen** unter „Technischer Support“ eine der verfügbaren Optionen aus:

   a. Wählen Sie **Rufen Sie uns an**, wenn Sie mit jemandem telefonieren möchten. Sie werden zu einer Seite auf netapp.com weitergeleitet, auf der die Telefonnummern aufgeführt sind, die Sie anrufen können.

   b. Wählen Sie **Fall erstellen**, um ein Ticket bei einem NetApp -Support-Spezialisten zu öffnen:

      - **Dienst**: Wählen Sie den Dienst aus, mit dem das Problem verknüpft ist. Beispiel: * NetApp Console*, wenn es sich speziell um ein technisches Supportproblem mit Workflows oder Funktionen innerhalb der Konsole handelt.
      - **System**: Wählen Sie, falls für den Speicher zutreffend, * Cloud Volumes ONTAP* oder **On-Prem** und dann die zugehörige Arbeitsumgebung aus.

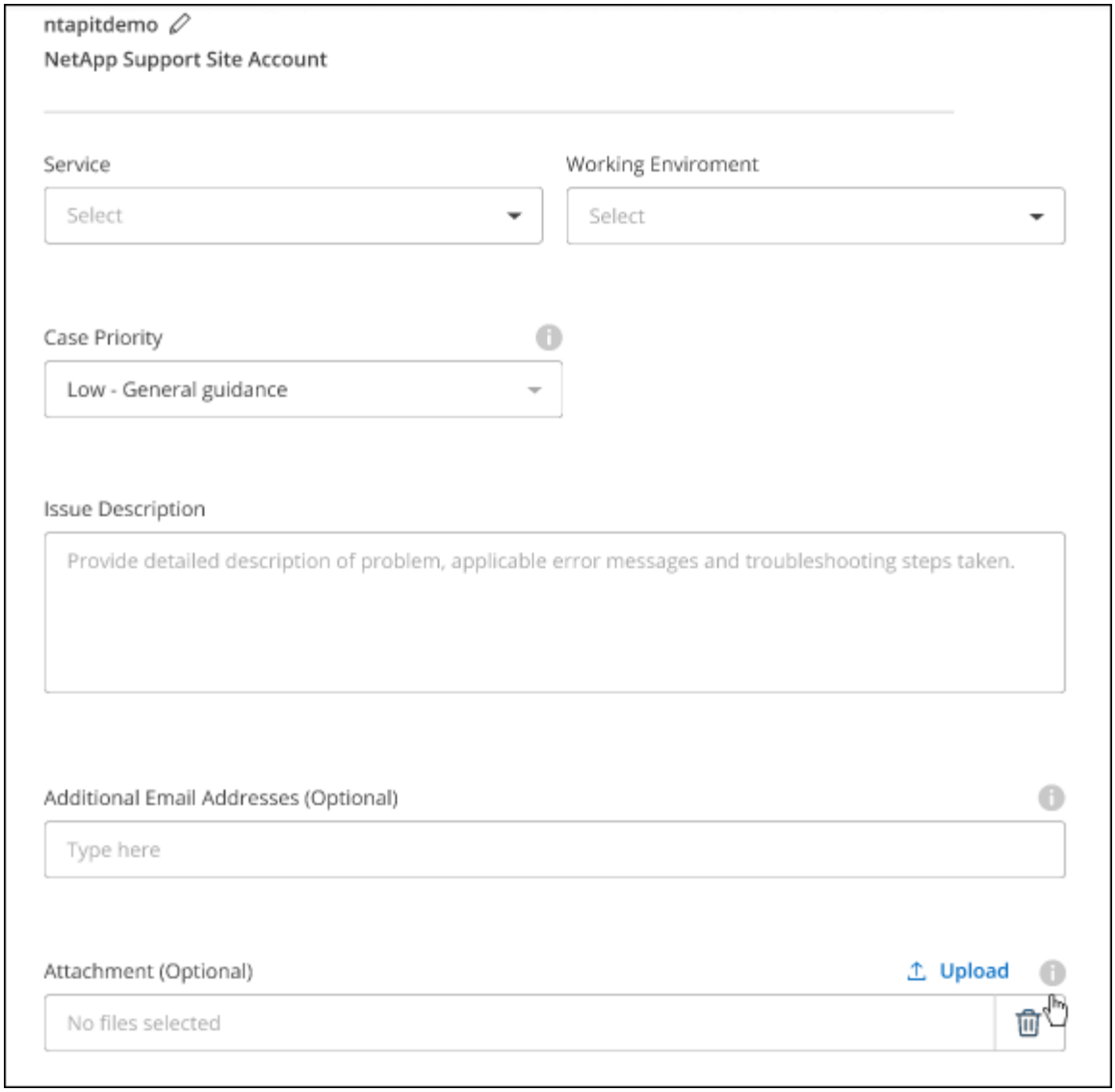
        Die Liste der Systeme liegt im Rahmen der Konsolenorganisation und des Konsolenagenten, den Sie im oberen Banner ausgewählt haben.

      - **Fallpriorität**: Wählen Sie die Priorität für den Fall. Sie kann „Niedrig“, „Mittel“, „Hoch“ oder „Kritisch“ sein.

        Um weitere Einzelheiten zu diesen Prioritäten zu erfahren, bewegen Sie die Maus über das Informationssymbol neben dem Feldnamen.

      - **Problembeschreibung**: Geben Sie eine detaillierte Beschreibung Ihres Problems an, einschließlich aller zutreffenden Fehlermeldungen oder Schritte zur Fehlerbehebung, die Sie durchgeführt haben.
      - **Zusätzliche E-Mail-Adressen**: Geben Sie zusätzliche E-Mail-Adressen ein, wenn Sie jemand anderen auf dieses Problem aufmerksam machen möchten.
      - **Anhang (optional)**: Laden Sie bis zu fünf Anhänge hoch, einen nach dem anderen.

        Anhänge sind auf 25 MB pro Datei begrenzt. Die folgenden Dateierweiterungen werden unterstützt: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.



Nach Abschluss

Es erscheint ein Popup mit Ihrer Support-Fallnummer. Ein NetApp -Support-Spezialist wird Ihren Fall prüfen und sich in Kürze bei Ihnen melden.

Um einen Verlauf Ihrer Supportfälle anzuzeigen, können Sie **Einstellungen > Zeitleiste** auswählen und nach Aktionen mit der Bezeichnung „Supportfall erstellen“ suchen. Über eine Schaltfläche ganz rechts können Sie die Aktion erweitern, um Details anzuzeigen.

Beim Versuch, einen Fall zu erstellen, kann es sein, dass die folgende Fehlermeldung angezeigt wird:

„Sie sind nicht berechtigt, einen Fall für den ausgewählten Dienst zu erstellen.“

Dieser Fehler könnte bedeuten, dass das NSS-Konto und das damit verknüpfte Unternehmen nicht dasselbe Unternehmen sind, für das die Seriennummer des NetApp Console gilt (d. h. 960xxxx) oder die Seriennummer der Arbeitsumgebung. Sie können auf eine der folgenden Arten Hilfe anfordern:

- Senden Sie einen nicht-technischen Fall an https://mysupport.netapp.com/site/help

Verwalten Sie Ihre Supportfälle

Sie können aktive und gelöste Supportfälle direkt von der Konsole aus anzeigen und verwalten. Sie können die mit Ihrem NSS-Konto und Ihrem Unternehmen verknüpften Fälle verwalten.

Beachten Sie Folgendes:

- Das Fallmanagement-Dashboard oben auf der Seite bietet zwei Ansichten:
  - Die Ansicht links zeigt die Gesamtzahl der Fälle, die in den letzten drei Monaten von dem von Ihnen angegebenen NSS-Benutzerkonto eröffnet wurden.
  - Die Ansicht rechts zeigt die Gesamtzahl der in den letzten drei Monaten auf Unternehmensebene eröffneten Fälle basierend auf Ihrem NSS-Benutzerkonto.

  Die Ergebnisse in der Tabelle spiegeln die Fälle wider, die mit der von Ihnen ausgewählten Ansicht in Zusammenhang stehen.
- Sie können interessante Spalten hinzufügen oder entfernen und den Inhalt von Spalten wie „Priorität“ und „Status“ filtern. Andere Spalten bieten lediglich Sortierfunktionen.

  Weitere Einzelheiten finden Sie in den folgenden Schritten.
- Auf Einzelfallebene bieten wir die Möglichkeit, Fallnotizen zu aktualisieren oder einen Fall zu schließen, der sich noch nicht im Status „Abgeschlossen“ oder „Ausstehend abgeschlossen“ befindet.

Schritte

1. Wählen Sie in der NetApp Console*Hilfe > Support*.
2. Wählen Sie **Fallmanagement** und fügen Sie bei entsprechender Aufforderung Ihr NSS-Konto zur Konsole hinzu.

   Auf der Seite **Fallverwaltung** werden offene Fälle angezeigt, die sich auf das NSS-Konto beziehen, das mit Ihrem Konsolenbenutzerkonto verknüpft ist. Dies ist dasselbe NSS-Konto, das oben auf der **NSS-Verwaltungsseite** angezeigt wird.
3. Ändern Sie optional die in der Tabelle angezeigten Informationen:
   - Wählen Sie unter **Fälle der Organisation** die Option **Anzeigen** aus, um alle mit Ihrem Unternehmen verknüpften Fälle anzuzeigen.
   - Ändern Sie den Datumsbereich, indem Sie einen genauen Datumsbereich oder einen anderen Zeitrahmen auswählen.
   - Filtern Sie den Inhalt der Spalten.
   - Ändern Sie die in der Tabelle angezeigten Spalten, indem Sie und wählen Sie dann die Spalten aus, die Sie anzeigen möchten.
4. Verwalten Sie einen vorhandenen Fall, indem Sie und wählen Sie eine der verfügbaren Optionen aus:
   - **Fall anzeigen**: Alle Details zu einem bestimmten Fall anzeigen.
   - **Fallnotizen aktualisieren**: Geben Sie zusätzliche Details zu Ihrem Problem an oder wählen Sie **Dateien hochladen**, um bis zu fünf Dateien anzuhängen.

     Anhänge sind auf 25 MB pro Datei begrenzt. Die folgenden Dateierweiterungen werden unterstützt: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.

- **Fall schließen**: Geben Sie Details zum Grund für das Schließen des Falls an und wählen Sie **Fall schließen** aus.

Rechtliche Hinweise

Rechtliche Hinweise bieten Zugriff auf Urheberrechtserklärungen, Marken, Patente und mehr.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marken

NETAPP, das NETAPP-Logo und die auf der NetApp -Markenseite aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen- und Produktnamen können Marken ihrer jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der Patente im Besitz von NetApp finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

Hinweisdateien enthalten Informationen zu Urheberrechten und Lizenzen Dritter, die in der NetApp -Software verwendet werden.

- "Hinweis zur NetApp Console"
- "Hinweis für Cloud Volumes ONTAP"
- "Hinweis für ONTAP"

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.