



NetApp Workload Factory Dokumentation

Workload Factory for NetApp Console

NetApp
October 07, 2026

This PDF was generated from <https://docs.netapp.com/de-de/data-services-workloads/index.html> on October 07, 2026. Always check docs.netapp.com for the latest.

Inhalt

NetApp Workload Factory Dokumentation	1
Versionshinweise	2
Neuerungen bei Workload Factory in der NetApp Console	2
Bekannte Einschränkungen für FSx for ONTAP Workloads in NetApp Workload Factory	2
Bekannte Einschränkungen von FSx for ONTAP Storage-Workloads	2
Bekannte Einschränkungen von FSx for ONTAP Datenbank-Workloads	4
Bekannte Einschränkungen für EDA-Workloads	7
Los geht's	8
Informationen zu NetApp Workload Factory	8
Features	8
Unterstützte Cloud-Anbieter	8
Sicherheit	9
Kosten	9
Wie Workload Factory funktioniert	9
Tools zur Verwendung von NetApp Workload Factory	10
Schnellstart für NetApp Workload Factory	11
Registrierung und Anmeldung bei Workload Factory über die NetApp Console	11
Erste Schritte mit Amazon FSx for NetApp ONTAP	11
Erste Schritte mit OCI NetApp Storage Service	11
Erste Schritte mit Google Cloud NetApp Volumes	11
Registrierung und Anmeldung bei Workload Factory über die NetApp Console	11
Informationen zu NetApp Workload Factory-Links	12
Warum Links von Vorteil sind	12
Wie Links funktionieren	12
Kosten	12
Wenn ein Link erforderlich ist	13
Verwandte Informationen	13
Berechtigungen für NetApp Workload Factory	13
Warum Berechtigungen verwenden	13
Wie Berechtigungen verwendet werden	14
Amazon FSx for NetApp ONTAP	15
FSx for ONTAP für Storage-Workloads verwenden	15
Informationen zu Amazon FSx for NetApp ONTAP in NetApp Workload Factory	15
Einsparmöglichkeiten mit FSx for ONTAP in NetApp Workload Factory	17
Speicherressourcen erstellen	22
Verbindung zu einem FSx for ONTAP-Dateisystem mit einem Lambda-Link herstellen	38
Cache-Volumes in NetApp Workload Factory erkennen	45
Zugriff auf Ihre FSx for ONTAP Dateisystemdaten	46
Schutz Ihrer Daten	46
Arten des Datenschutzes in NetApp Workload Factory	46
Snapshots bieten Schutz für Daten	49
Backups bieten Schutz für Daten in der NetApp Workload Factory	58
Replikation zum Schutz von Daten verwenden	60

Schützen Sie Ihre FSx for ONTAP Daten mit NetApp Autonomous Ransomware Protection mit KI.	82
Klonen eines Volumes in NetApp Workload Factory	85
Schützen Sie Ihre FSx for ONTAP Daten mit einem Cyber-Tresor	86
FSx für ONTAP in Workload Factory verwalten	86
Analysieren Sie FSx for ONTAP-Ereignisse in NetApp Workload Factory	86
Best Practices für Dateisysteme implementieren	89
Verfolgen Sie Kosten und erhalten Sie Berichte zu Ressourcen in NetApp Workload Factory	104
Volumes verwalten	106
Blockspeicher verwalten	134
Dateisysteme verwalten	139
Storage-VMs verwalten	146
FSx for ONTAP für Datenbank-Workloads	149
Informationen zu NetApp Workload Factory for Databases	149
Schnellstart für NetApp Workload Factory für Datenbanken	153
Informationen zu Einsparungen in NetApp Workload Factory for Databases	154
Datenbankressourcen erstellen	166
Ressourcen verwalten	186
Datenbankressourcen schützen, überwachen und optimieren	193
Einsatz von FSx for ONTAP für EDA-Workloads	215
Erfahren Sie mehr über Workload Factory für EDA	215
Schnellstart für Workload Factory für EDA	216
Workload Factory für EDA-Anforderungen	217
EDA-Speicherübersicht	218
Projektnutzungsanalyse	228
Verwendung der Perforce Integration	234
Einsatz von FSx for ONTAP für VMware Workloads	241
Informationen zu NetApp Workload Factory für VMware	241
Schnellstart für die Migration zu Amazon EVS mithilfe des VMware workloads migration advisor	244
Schnellstart für die Migration zu Amazon EC2 mit dem VMware workloads migration advisor	245
Schnellstart für die Migration zu VMware Cloud on AWS mithilfe des VMware workloads migration advisor	246
Schnellstart für die Migration zu Google Cloud VMware Engine mit dem VMware workloads migration advisor	247
Überblick über das VMware Planungszentrum	248
Verwendung des VMware Planungszentrums	250
Referenz	281
Performance für FSx for ONTAP in NetApp Workload Factory	281
Sicherheit für FSx for ONTAP in NetApp Workload Factory	281
Google Cloud NetApp Volumes	282
Informationen zu Google Cloud NetApp Volumes	282
Features	282
Kosten	282
Unterstützte Regionen	282
Hilfe erhalten	282
Verwandte Links	282

Schnellstart für Google Cloud NetApp Volumes	283
Einrichtung von Google Cloud NetApp Volumes	283
Ein Servicekonto einrichten	284
Gemeinsam genutzte VPC	285
Fehlerbehebung	285
Zuweisung von Rollen für Google Cloud NetApp Volumes	285
Zuweisen von Rollen zum Mitglied des Servicekontos	285
Hinzufügen von Google Cloud NetApp Volumes Anmeldedaten zu NetApp Workload Factory	286
Überblick	286
Konfigurationsanalyse für Google Cloud NetApp Volumes	288
Analyseanforderungen	288
Bewährte Verfahren und Empfehlungen für Speicher-Workloads	288
Gut strukturierte Google Cloud NetApp Volumes Konfigurationen implementieren	289
Über diese Aufgabe	289
Bevor Sie beginnen	290
Empfehlungen zu Konfigurationsproblemen anzeigen	290
Konfigurationsanalyse verwerfen	290
Eine verworfene Konfigurationsanalyse reaktivieren	291
OCI NetApp Storage Service	292
Informationen zu OCI NetApp Storage Service in NetApp Workload Factory	292
Features	292
Tools zur Verwendung von NetApp Workload Factory	293
Hilfe erhalten	293
Schnellstart für Oracle Cloud Infrastructure NetApp Storage Service in NetApp Workload Factory	293
Hinzufügen von Oracle Cloud Infrastructure-Anmeldeinformationen zu NetApp Workload Factory	294
Erstellen oder Auffinden von Oracle Cloud Infrastructure NetApp Storage Service-Systemen in NetApp Console	295
Ein vorhandenes Cloud Storage-System entdecken	295
Herstellen einer Verbindung mit einem Oracle Cloud Infrastructure NetApp Storage Service Storage-System über einen Link	295
Über diese Aufgabe	296
Neuen Link erstellen	296
Einsatz des Terraform-Stacks in OCI Resource Manager	299
Registrierung der Funktion in Workload Factory	299
Weitere Möglichkeiten, dieselbe Vorlage anzuwenden	299
Zuordnung eines bestehenden Links zu einem OCI NetApp Storage Service System	300
OCI NetApp Storage Service Berechtigungen für NetApp Workload Factory	301
Wie Workload Factory die Berechtigungen von OCI NetApp Storage Service nutzt	301
Mandantenübergreifende Vertrauensstellung	301
IAM-Richtlinien für OCI NSS	301
Workload Factory verwalten	303
Wie NetApp Workload Factory gut strukturierte Workloads unterstützt	303
So funktioniert es	303
Warum es wichtig ist	303
Beginnen Sie mit Workload Factory, um Fehlkonfigurationen von Workloads zu erkennen und zu	

beheben	303
Konfiguration der Benachrichtigungen für NetApp Workload Factory	304
Workload Factory-Benachrichtigungen konfigurieren	304
Abonnement des Amazon SNS Themas	306
Benachrichtigungen filtern	306
Benachrichtigungstypen und -meldungen	307
Überwachung von NetApp Workload Factory Vorgängen mit Tracker	312
Abläufe nachverfolgen und überwachen	313
API-Anfrage anzeigen	313
Einen fehlgeschlagenen Vorgang wiederholen	313
Einen fehlgeschlagenen Vorgang bearbeiten und erneut versuchen	313
Links der NetApp Workload Factory verwalten	314
Anzeigen der mit Ihrem Konto verknüpften Links	314
Einen Link bearbeiten	314
Einen Link authentifizieren	314
Das Passwort für die Link-Authentifizierung aktualisieren	315
Link entfernen	316
KI-Funktionen für FSx für ONTAP in NetApp Workload Factory managen	317
Über KI-Funktionen	317
Konfigurationsoptionen	317
Bevor Sie beginnen	317
KI-Funktionen konfigurieren	318
Budgetkontrolle und Kreditlimits	318
AWS GovCloud Überlegungen	318
Auswirkungen auf bestehende Sitzungen	319
Verwandte Informationen	319
Benutzerdefinierte Dashboards für FSx für ONTAP	319
Informationen zu benutzerdefinierten Dashboards für FSx for ONTAP in NetApp Workload Factory	319
Ein benutzerdefiniertes Dashboard in NetApp Workload Factory erstellen	322
Benutzerdefinierte Dashboards in NetApp Workload Factory verwalten	323
Fehlerbehebung bei benutzerdefinierten Dashboards in NetApp Workload Factory	325
Automatisierung von Aufgaben mit Codebox	326
Informationen zur Codebox-Automatisierung in NetApp Workload Factory	326
Verwendung von Codebox für die Automatisierung in NetApp Workload Factory	327
Verwendung von CloudShell in NetApp Workload Factory	330
Über diese Aufgabe	330
CloudShell Befehle	331
Bevor Sie beginnen	332
Einsetzen von CloudShell	332
Umbenennen einer CloudShell Sitzungsregisterkarte	334
Registerkarte für doppelte CloudShell Sitzungen	334
Schließen der CloudShell Sitzungstabs	334
Registerkarten von CloudShell Sitzungen aufteilen	334
Einstellungen für eine CloudShell Sitzung aktualisieren	335
Entfernen von Anmeldeinformationen aus NetApp Workload Factory	335

Wissen und Unterstützung	336
Für Support bei der NetApp Console registrieren	336
Übersicht der Supportregistrierung	336
Die NetApp Console für den NetApp Support registrieren	336
NSS-Zugangsdaten für Cloud Volumes ONTAP Support zuordnen	338
Hilfe zu NetApp Console Cloud-Services	340
Support für einen Dateidienst eines Cloud-Anbieters erhalten	340
Selbsthilfeoptionen verwenden	340
Einen Fall beim NetApp Support erstellen	340
Verwalten Sie Ihre Supportfälle	343
Rechtliche Hinweise	344
Copyright	344
Marken	344
Patente	344
Datenschutzrichtlinie	344
Open Source	344

NetApp Workload Factory Dokumentation

Versionshinweise

Neuerungen bei Workload Factory in der NetApp Console

Hier finden Sie Informationen zu den Neuerungen in Workload Factory in der NetApp Console, darunter Aktualisierungen und Verbesserungen für das Workload-Management, die Service-Administration, Storage-Funktionen, Berechtigungen und mehr.

[[30-september-2026]]
== 30. September 2026

Erstveröffentlichung von Oracle Cloud Infrastructure NetApp Storage Service für Workload Factory

Die erste Version des OCI NetApp Storage Service (OCI NSS) für Workload Factory bietet Onboarding, Systemerkennung, Anmeldeinformationsverwaltung sowie die Erstellung und Zuordnung von Links. Für die Beantragung des Zugriffs auf OCI NSS ist ein Support-Ticket bei Oracle erforderlich.

Workload Factory Dokumentation für NetApp Console Benutzer

Detaillierte Dokumentation für Workload Factory finden Sie in der NetApp Console, einschließlich Anleitungen für Onboarding, Systemerkennung, Management von Anmeldeinformationen sowie Erstellung und Zuordnung von Links.

Bekannte Einschränkungen für FSx for ONTAP Workloads in NetApp Workload Factory

Bekannte Einschränkungen kennzeichnen Plattformen, Geräte oder Funktionen, die von dieser Produktversion nicht unterstützt werden oder nicht korrekt mit ihr zusammenarbeiten. Die folgenden Einschränkungen gelten speziell für Amazon FSx for NetApp ONTAP in NetApp Workload Factory. Überprüfen Sie diese Einschränkungen sorgfältig.

Bekannte Einschränkungen von FSx for ONTAP Storage-Workloads

Regionale Unterstützung

Die folgenden AWS-Regionen werden nicht unterstützt:

- China Regionen
- Secret Cloud
- Top Secret Cloud

Einschränkungen beim Hinzufügen von HA-Paaren

- Dieser Vorgang kann etwa 30 Minuten dauern.
- Das Hinzufügen von HA-Paaren schränkt die folgenden Vorgänge ein: das Hinzufügen weiterer HA-Paare, die Provisionierung von IOPS, die Erhöhung der SSD-Kapazität und die Aktualisierung der Durchsatzkapazität.

Unterstützung von Regionen für Durchsatzkapazität

Scale-up-Bereitstellungen

Scale-up Konfigurationen werden in allen Regionen bis zu 2 GB/s unterstützt. Die folgenden Regionen unterstützen für Scale-up Bereitstellungen eine maximale Durchsatzkapazität von bis zu 4 GB/s: Region US East (Ohio), Region US East (N. Virginia), Region US West (Oregon) und Europe (Irland).

Scale-out-Bereitstellungen

Die folgenden Regionen unterstützen für Scale-out-Bereitstellungen eine maximale Durchsatzkapazität von bis zu 6 GB/s: US East (N. Virginia und Ohio), US West (N. California und Oregon), Europa (Frankfurt, Irland und Stockholm) und Asien-Pazifik (Singapur und Sydney).

Kapazitätsmanagement

- Die automatische Vergrößerung von Volumes wird für das iSCSI-Protokoll derzeit nicht unterstützt.
- Wenn die automatische Kapazitätsmanagement-Funktion aktiv ist, ist eine manuelle Kapazitätserhöhung nicht zulässig.
- Die Deaktivierung des automatischen Kapazitätsmanagements ist nur mit denselben Berechtigungen möglich, die zum Aktivieren verwendet wurden.
- Wenn das automatische Kapazitätsmanagement aktiviert ist, ist ein Link erforderlich, um sicherzustellen, dass die Volume-Inodes zusammen mit der Storage-Kapazität zunehmen.

Storage VMs

Die Anzahl der Storage VMs ist pro SKU begrenzt. Das Erstellen von Storage VMs über diese Beschränkung hinaus wird in Workload Factory nicht unterstützt.¹

Informationen zur maximalen Anzahl von SVMs pro Dateisystem finden Sie ["Verwaltung von FSx for ONTAP Storage Virtual Machines"](#) in der AWS-Dokumentation.

iSCSI Protokollunterstützung

- Das iSCSI-Protokoll ist nur für FlexVol Volumes verfügbar. ¹
- Die Verkleinerung von Volumes wird für iSCSI-Volumes nicht unterstützt.

Datenschutz

- Schnappschüsse können nicht gelöscht werden.
- Wenn Sie ein Dateisystem replizieren, verwenden alle Volumes im Dateisystem dieselbe Replikationsrichtlinie.
- Bei Replikationsbeziehungen mit langfristiger Aufbewahrung steht für die Wiederherstellung nur der letzte Snapshot zur Verfügung.
- Folgende Funktionen werden bei unveränderlichen Snapshots nicht unterstützt:
 - Konsistenzgruppen
 - FabricPool
 - FlexCache Volumes
 - SMtape

- SnapMirror Active Sync
- SnapMirror Richtlinienregeln mit dem Parameter „-schedule“
- SnapMirror synchron
- SVM Datenmobilität (wird für die Migration oder Verlagerung einer SVM von einem Quell-Cluster zu einem Ziel-Cluster verwendet)

Storage-Einsparungsrechner

Der Speichereinsparungsrechner berechnet keine Kosteneinsparungen für die folgenden Konfigurationen:

- FSx for Windows File Server: HDD Storage-Typ
- Elastic Block Store (EBS): st1, sc1 und Standard-Volumentypen
- Elastic File System (EFS): Bursting-Durchsatzmodus

Unterstützung für AWS Secrets Manager

AWS Secrets Manager wird bei Verwendung eines Console Agenten nicht unterstützt.

Beschränkung der Amazon S3 Zugriffspunkte

Die maximale Anzahl an S3-Zugriffspunkten pro storage VM beträgt 4.000.

Einschränkungen bei der Migrationsreplikation von Storage-VMs

- Workload Factory unterstützt keine Migrationsreplikation für Storage-VMs zwischen FSx for ONTAP-Dateisystemen der ersten und zweiten Generation.
- Die Replikation bei Systemumschaltung wird für Volumes mit S3-Zugriffspunkten oder ONTAP S3-Konfigurationen, einschließlich object-store-server, buckets, users, groups oder policies auf dem vserver, nicht unterstützt.

Hinweis:

1. Gilt für Amazon FSx for NetApp ONTAP

Bekannte Einschränkungen von FSx for ONTAP Datenbank-Workloads

Unterstützung für die Instanzerkennung

Workload Factory unterstützt die Erkennung von PostgreSQL-Instanzen, die ausschließlich auf Amazon Linux Betriebssystemen laufen, und von Oracle-Instanzen, die ausschließlich auf Red Hat Enterprise Linux laufen.

Unterstützung für AMI Image-Versionen

Wir zeigen pro SQL-Version nur bis zu vier aktuelle Versionen oder Revisionen von AMI-Images an. Die Installation von einem AMI-Image, das älter als die vier neuesten Versionen ist, ist nicht zulässig.

Benutzerdefiniertes AMI

Das Deployment mit einem benutzerdefinierten AMI setzt voraus, dass Installationsmedien im Image vorhanden sind. Dies ist für die FCI-Konfiguration aus folgenden Gründen erforderlich:

- Deinstallation und Neukonfiguration zur Bildung des FCI-Clusters
- Bei Auswahl einer anderen Sortierung als der im Image für das eigenständige Deployment festgelegten

Im Rahmen des Deployment installiert Workload Factory kein benutzerdefiniertes AMI mit mehreren Microsoft SQL Server Instanzen. Im Rahmen des Deployment wird nur die Standardinstanz von Microsoft SQL Server ausgewählt und konfiguriert.

Rollback und erneuter Versuch bei fehlgeschlagenen Deployments

Rollback und Wiederholung fehlgeschlagener Deployments werden in Workload Factory nicht unterstützt. Ein fehlgeschlagener Stack kann über die CloudFormation Konsole in AWS zurückgesetzt oder erneut versucht werden.

Rollback von Active Directory- und DNS-Ressourcen

Die folgenden DNS-Ressourcen werden beim Zurücksetzen eines Tests oder eines fehlgeschlagenen Deployments über die CloudFormation Konsole in AWS nicht aus Active Directory und DNS entfernt:

- Jeder Knoten des SQL Deployments an seine Verwaltungs-IP-Adresse
- Zuordnung des Windows Cluster Namens zu den reservierten sekundären IP-Adressen von EC2-Instanzen in Fällen von FCI
- SQL FCI Name für die beiden reservierten IP-Adressen von beiden EC2-Instanzen im FCI

Sie müssen diese Einträge manuell bereinigen oder warten, bis die Domäne veraltete Einträge löscht.

Unterstützung für die Konfiguration von Always On Verfügbarkeitsgruppen

Das Managen von Konfigurationen für Always On availability groups wird in Workload Factory nicht unterstützt.

Benutzerdefinierte Verschlüsselungsschlüssel

Benutzerdefinierte Verschlüsselungsschlüssel für FSx for ONTAP sind nicht nach der Anwendbarkeit auf den Service aufgelistet. Der geeignete Schlüssel muss ausgewählt werden. AWS managed keys werden anhand der Anwendbarkeit auf den Service gefiltert.

CloudFormation Vorlage

Eine heruntergeladene oder kodierte von Codebox generierte CloudFormation Vorlage (YAML-Datei) hat eine begrenzte Aufbewahrungsdauer von sieben Tagen.

Sandbox-Unterstützung

Die maximale Anzahl von Sandbox-Klonen, die von einem Datenbankserver erstellt werden können, beträgt 90.

Erkennung und Verwaltung von Microsoft SQL Server

Die Erkennung von Microsoft SQL Server wird nicht gespeichert. Bei jedem Zugriff auf Databases in Workload Factory wird die Microsoft SQL Server Erkennung erneut ausgeführt, um SQL-Installationen in der Region zu identifizieren.

Einsparpotenziale

Auf der Registerkarte „Inventar“ werden die angezeigten geschätzten Kosten für jede Microsoft SQL-Instanz auf der Ebene des FSx for ONTAP Dateisystems berechnet und nicht für die Volumes, auf denen die SQL-Instanz gehostet wird.

Mehrere FSx for ONTAP Dateisysteme

Workload Factory unterstützt weder das Erstellen noch das Speichern von Konfigurationen für Microsoft SQL Server mit mehreren FSx for ONTAP Dateisystemen. Unterstützt wird nur ein Deployment für eine einzelne FSx for ONTAP Dateisystemkonfiguration.

Optimierungsbeschränkungen

Optimierung der Compute-Dimensionierung

Beim Wechsel zu bestimmten Instanztypen kann die Netzwerkkonfiguration zurückgesetzt werden, was während der Optimierung zu Verbindungsabbrüchen zwischen Knoten und somit zum Fehlschlagen von Aufträgen führen kann. Gegebenenfalls ist ein manueller Eingriff erforderlich, um die DNS-Einstellungen und iSCSI-Sitzungen zu überprüfen und zu aktualisieren. Weitere Informationen zu den Einschränkungen bei der Größenänderung von EC2 sind unter ["Amazon Elastic Compute Cloud Dokumentation"](#) verfügbar.

Optimierung der ONTAP und OS Konfiguration

Die Massenoptimierung für mehr als eine SQL Server-Instanz wird für die ONTAP Konfiguration und die OS-Konfiguration nicht unterstützt.

Bewertung von Betriebssystem-Patches zur Optimierung

Die zur Optimierung durchgeführte Bewertung von Betriebssystem-Patches funktioniert möglicherweise nicht in einem privaten Netzwerk. Die Bewertung basiert auf AWS Patch Manager. Zum Verständnis des Patchens von Windows EC2-Instanzen in einem privaten Netzwerk siehe den AWS Cloud Operations Blog ["Patchen von Windows EC2-Instanzen in privaten Subnetzen mit AWS Systems Manager"](#).

Bewertung der regionsübergreifenden Replikation

- Die Optimierungsbewertung kann nicht feststellen, ob regionsübergreifende Replikation (CRR) verwendet wird, wenn sich das Zieldateisystem FSx for ONTAP in einem anderen AWS-Konto befindet.
- Workload Factory bewertet nur die CRR-Konfiguration des Quell-Dateisystems in FSx for ONTAP.

Berechnung der On-Premises-Einsparungen

Die Berechnungen der Kosten und prozentualen Einsparungen für die Volume-Größe von Microsoft SQL Server On-Premises Storage werden nicht berücksichtigt.

Authentifizierung des Datenbankhosts bei der Ermittlung von Einsparungen

In einigen Fällen werden bei eingeschränkten Berechtigungen nach erfolgreicher Authentifizierung auf der Seite „Ersparnisse entdecken“ keine Daten geladen.

Integration mit NetApp Backup and Recovery

Nach dem Hinzufügen von Hosts zu NetApp Backup and Recovery zum Schutz schlägt die Datenbankerkennung manchmal fehl.

Registrierung von Oracle auf SUSE Linux Enterprise Server 12

Bei der Registrierung von Oracle Database auf SUSE Linux Enterprise Server 12 installiert Workload Factory keine Python-Abhängigkeiten. Die erforderliche Python-Version muss manuell konfiguriert werden. Workload Factory erfordert mindestens Version 3.6; empfohlen wird jedoch Version 3.11.

Bekannte Einschränkungen für EDA-Workloads

Erforderliche Bedienerberechtigungen

NetApp Workload Factory für EDA benötigt Operator-Berechtigungen, um korrekt zu funktionieren.

Los geht's

Informationen zu NetApp Workload Factory

NetApp Workload Factory ist eine leistungsstarke Plattform für das Lebenszyklusmanagement, die Ihnen dabei hilft, Ihre Workloads mithilfe von Amazon FSx for NetApp ONTAP, Google Cloud NetApp Volumes und Oracle Cloud Infrastructure NetApp Storage Service zu optimieren.

Ein Workload umfasst eine Kombination aus Ressourcen, Code und Services oder Applikationen, die einem bestimmten Geschäftsziel dienen. Dies kann von einer kundenorientierten Applikation bis hin zu einem Backend-Prozess reichen. Workloads können eine Teilmenge der Ressourcen innerhalb eines einzelnen AWS-Kontos umfassen oder sich über mehrere Konten erstrecken.

Features

Die Workload Factory Plattform bietet folgende Hauptfunktionen.

Flexible und kostengünstige Storage

Storage-Systeme in der Cloud erkennen, einsetzen und managen. Ihr Cloud Storage Anbieter stellt Ihnen den vollen Funktionsumfang von ONTAP als nativen Managed Service zur Verfügung und sorgt so für ein konsistentes Hybrid Cloud Erlebnis.

Migration lokaler vSphere Umgebungen zu VMware Cloud on AWS

Der VMware Cloud on AWS Migration Advisor ermöglicht die Analyse Ihrer aktuellen VM-Konfigurationen in On-Premises vSphere Umgebungen, die Erstellung eines Plans zum Einsetzen empfohlener VM-Layouts in VMware Cloud on AWS und die Verwendung angepasster Amazon FSx for NetApp ONTAP Dateisysteme als externe Datenspeicher.

Verwaltung des Datenbanklebenszyklus

Erkennung von Datenbank-Workloads und Analyse von Kosteneinsparungen mit Amazon FSx for NetApp ONTAP; Nutzung von Storage- und Applikationsvorteilen bei der Migration von SQL server-Datenbanken zu FSx for ONTAP Storage; Einsatz von SQL servern, Datenbanken und Datenbankklonen, die Best Practices der Anbieter implementieren; Verwendung eines Infrastructure as Code-Co-Piloten zur Automatisierung von Vorgängen; sowie kontinuierliche Überwachung und Optimierung von SQL server-Umgebungen zur Verbesserung von Performance, Verfügbarkeit, Schutz und Kosteneffizienz.

Ask Me AI Assistant

Sie können dem KI-Assistenten Fragen zur Verwaltung und zum Betrieb Ihrer Storage-Systeme stellen. Mithilfe des Model Context Protocol (MCP) kommuniziert Ask Me sicher mit externen Umgebungen und fragt API-Tools ab, um Antworten bereitzustellen, die auf Ihre spezifische Storage-Umgebung zugeschnitten sind.



Kontoadministratoren können KI-Funktionen aktivieren oder deaktivieren. Wenn ein Administrator sie deaktiviert, steht der Ask Me KI-Assistent nicht zur Verfügung. ["Informationen zur Verwaltung von KI-Funktionen"](#).

Unterstützte Cloud-Anbieter

Mit Workload Factory können Sie Cloud Storage managen und Workload-Funktionen in Amazon FSx for

NetApp ONTAP, Google Cloud NetApp Volumes und Oracle Cloud Infrastructure NetApp Storage Service (OCI NSS) nutzen.

Sicherheit

Sicherheit für NetApp Workload Factory hat für NetApp höchste Priorität. NetApp Workload Factory hat ["SOC2 Type 1 Compliance, SOC2 Type 2 Compliance und HIPAA Compliance"](#) erhalten.

Kosten

Workload Factory ist kostenlos nutzbar. Die Kosten, die Sie an Ihren Cloud-Anbieter zahlen, hängen von den Storage- und Workload-Services ab, die Sie einsetzen möchten. Dazu gehören die Kosten für Storage-Systeme, Infrastruktur, Services und mehr.

Wie Workload Factory funktioniert

Workload Factory umfasst eine webbasierte Konsole, die über die SaaS-Schicht bereitgestellt wird, ein Konto, Berechtigungsrichtlinien, die den Zugriff auf Ihre Cloud-Umgebung steuern, die Konnektivität zwischen Workload Factory und Ihren Cloud-Konten und vieles mehr.

Software-as-a-Service

Workload Factory ist über die ["NetApp Console"](#) zugänglich. Diese SaaS-Lösung ermöglicht Ihnen den automatischen Zugriff auf die neuesten Funktionen, sobald sie veröffentlicht werden, sowie den einfachen Wechsel zwischen Ihren Workload Factory Konten und Links.

Registrierung und Zugriffsverwaltung

Für die Nutzung von NetApp Console ist eine Anmeldung mit Ihren NetApp Support Site Zugangsdaten oder die Erstellung eines NetApp Console Logins erforderlich. Der erste Benutzer wird zum Unternehmensadministrator und verwaltet Benutzerkonten und Berechtigungen. Rollen können später aktualisiert und weitere Administratoren hinzugefügt werden.

- ["Es wird erläutert, wie Sie sich bei NetApp Console registrieren und anmelden."](#)
- ["Informationen zu NetApp Console Identity Access Management"](#)

Berechtigungen

Workload Factory bietet flexible Berechtigungsrichtlinien, mit denen Sie den Zugriff auf Ihre Cloud-Umgebung präzise steuern und Workload Factory auf Grundlage Ihrer IT-Richtlinien schrittweise Vertrauensstufen zuweisen können.

["Weitere Informationen zu den Berechtigungsrichtlinien von Workload Factory"](#)

Codebox Automatisierung

Codebox ist ein Co-Pilot für Infrastructure as Code (IaC), der Entwickler und DevOps-Ingenieure bei der Generierung des benötigten Codes für alle von Workload Factory unterstützten Vorgänge unterstützt. Zu den Codeformaten gehören die Workload Factory REST API, CLIs von Cloud-Anbietern, Terraform und mehr.

Codebox schafft einen klaren Weg zur Bereitschaft für die Ausführung und bietet gleichzeitig einen Automatisierungskatalog für eine schnelle künftige Wiederverwendung.

Der Codebox Bereich zeigt den IaC an, der durch einen bestimmten Job Flow Vorgang generiert und mit einem grafischen Assistenten oder einer dialogorientierten Chat-Oberfläche abgeglichen wird. Codebox unterstützt zur einfachen Navigation und Analyse die Farbcodierung und die Suche, erlaubt jedoch keine Bearbeitung. Der IaC kann nur kopiert oder im Automation Catalog gespeichert werden.

["Weitere Informationen zu Codebox"](#)

Gut konzipierte Workloads

Workload Factory unterstützt Sie bei der Wartung und dem Betrieb zuverlässiger, sicherer, effizienter und kostengünstiger Storage- und Datenbankkonfigurationen, die mit dem AWS Well-Architected Framework übereinstimmen. Workload Factory scannt täglich FSx for ONTAP Dateisysteme sowie SQL Server- und Oracle-Datenbankbereitstellungen, um Einblicke in potenzielle Fehlkonfigurationen zu liefern, und empfiehlt entweder manuelle oder automatisierte Maßnahmen zur Behebung von Problemen.

["Weitere Informationen zu gut strukturierten Workloads"](#)

Tools zur Verwendung von NetApp Workload Factory

Sie können NetApp Workload Factory mit den folgenden Tools verwenden:

- **NetApp Console:** NetApp Console bietet eine hybride Benutzeroberfläche, sodass Sie Workload Factory zusammen mit anderen NetApp Datenservices verwenden können.
- **Ask Me:** Mit dem KI-Assistenten Ask Me können Sie Fragen stellen und mehr über Workload Factory erfahren, ohne die NetApp Console zu verlassen.
- **CloudShell CLI:** Workload Factory umfasst eine CloudShell CLI zum Managen und Betreiben von AWS- und NetApp Umgebungen über verschiedene Konten hinweg mit einer einzigen browserbasierten CLI.
- **REST API:** Mit den Workload Factory REST APIs können Sie Ihre Storage-Systeme und andere Ressourcen einsetzen und managen.
- **NetApp Terraform provider:** Mit Terraform lassen sich Infrastruktur-Workflows erstellen und managen, die in NetApp Console for Workload Factory generiert werden.

REST-APIs

Workload Factory ermöglicht Ihnen die Optimierung, Automatisierung und den Betrieb Ihrer Cloud Storage-Systeme für bestimmte Workloads. Jeder Workload stellt eine zugehörige REST-API bereit. Zusammen bilden diese Workloads und APIs eine flexible und erweiterbare Entwicklungsplattform, die Sie zur Verwaltung Ihrer Storage-Systeme verwenden können.

Die Verwendung der Workload Factory REST APIs bietet mehrere Vorteile:

- Die APIs wurden auf Basis der REST-Technologie und aktueller Best Practices entwickelt. Zu den Kerntechnologien gehören HTTP und JSON.
- Die Workload Factory Authentifizierung basiert auf dem OAuth2-Standard. NetApp nutzt die Service-Implementierung von Auth0.
- Die webbasierte Konsole von Workload Factory verwendet dieselben zentralen REST-APIs, sodass zwischen den beiden Zugriffspfaden Konsistenz besteht.

["Anzeige der Workload Factory REST API-Dokumentation"](#)

Schnellstart für NetApp Workload Factory

NetApp Workload Factory ist für Benutzer als Cloud-Datendienst über NetApp Console zugänglich. Der Einstieg in Workload Factory erfolgt durch die Registrierung und die Erstellung eines Kontos in NetApp Console sowie durch das Hinzufügen von Anmeldeinformationen für den Cloud-Provider, damit Workload Factory Ihre Ressourcen direkt managen und Ihre Workloads optimieren kann.

Bevor Sie beginnen, sollten Sie mit ["Workload Factory"](#) vertraut sein.

Registrierung und Anmeldung bei Workload Factory über die NetApp Console

["Registrierung und Anmeldung bei Workload Factory über die NetApp Console"](#)

Im nächsten Schritt erfolgt der Einstieg über den Link **Quick start** Ihres Cloud-Providers.

Erste Schritte mit Amazon FSx for NetApp ONTAP

["Schnellstart für Amazon FSx for NetApp ONTAP"](#)

Erste Schritte mit OCI NetApp Storage Service

["Schnellstart für OCI NetApp Storage Service"](#)

Erste Schritte mit Google Cloud NetApp Volumes

["Schnellstart für Google Cloud NetApp Volumes"](#)

Registrierung und Anmeldung bei Workload Factory über die NetApp Console

NetApp Workload Factory ist über NetApp Console zugänglich. Für die Nutzung der Console ist eine Registrierung oder Anmeldung mit Ihren NetApp Support Site Zugangsdaten erforderlich, alternativ kann ein NetApp Console Login erstellt werden. Wenn Sie die erste Person aus Ihrem Unternehmen sind, die sich registriert, erstellen Sie als Administrator eine neue Organisation. Wenn Ihr Unternehmen bereits über eine Organisation verfügt, ist eine Registrierung oder Anmeldung mit Ihren vorhandenen NetApp Support Site Zugangsdaten oder über das Single Sign-On (SSO) Ihres Unternehmens möglich.

Nicht aufgelöste Direktive in <stdin> - include::https://raw.githubusercontent.com/NetAppDocs/console-setup-admin/main/_include/task-sign-up-saas.adoc[]

Ergebnis

Sie sind nun angemeldet und können Workload Factory zum Managen Ihrer Storage-Systeme und Workloads nutzen. Der Zugriff auf Workload Factory erfolgt über **Workloads** im Hauptmenü.

Informationen zu NetApp Workload Factory-Links

Eine NetApp Workload Factory Verknüpfung stellt eine Vertrauensbeziehung und Konnektivität zwischen einem Workload Factory Konto und einem oder mehreren Cloud Storage-Systemen her. Dadurch können Sie bestimmte Funktionen des Storage-Systems direkt über ONTAP REST API Aufrufe überwachen und managen, die über die API Ihres Cloud-Anbieters nicht verfügbar sind.

Für den Einstieg in Workload Factory benötigen Sie keinen Link, aber in einigen Fällen müssen Sie einen Link erstellen, um alle Funktionen und Workload-Funktionen von Workload Factory freizuschalten.

Warum Links von Vorteil sind

Links sind vorteilhaft, da sie Workload Factory die Durchführung von Operationen ermöglichen, die über die API Ihres Cloud-Anbieters nicht nativ verfügbar sind. Links ermöglichen erweiterte ONTAP Funktionen und Automatisierung, was das Management Ihrer Cloud Storage-Systeme verbessert.

Hier sind einige Vorteile der Verwendung von Links:

- Mit dieser Verbindung kann die NetApp Console ONTAP Befehle direkt an Ihr Cloud Storage-System senden, wodurch erweiterte ONTAP Funktionen verfügbar werden, die über das hinausgehen, was Ihr Cloud-Anbieter nativ anbietet.
- Links nutzen entfernte serverlose Funktionen, um Code als Reaktion auf Ereignisse auszuführen. Dieser serverlose Ansatz beseitigt die Abhängigkeit von einer Instanz, die in Ihrer VPC läuft.

Wie Links funktionieren

Links nutzen serverlose Remote-Computing Services wie AWS Lambda und Oracle Cloud Infrastructure Functions. Diese Services führen Code als Reaktion auf Ereignisse aus und managen die dafür benötigten Rechenressourcen. Die von Ihnen erstellten Links sind Teil Ihres NetApp Kontos und mit dem entsprechenden Cloud-Anbieterkonto verknüpft.

Nachdem Sie einen Link erstellt haben, können Sie ihn mit einem oder mehreren Cloud Storage-Systemen verknüpfen. Jedes Cloud Storage-System kann nur mit einem Link im selben NetApp Konto verknüpft werden. Wenn Sie mehrere NetApp Konten haben, kann ein einzelnes Cloud Storage-System unter verschiedenen NetApp Konten mit zusätzlichen Links verknüpft werden.

Sie erstellen und verknüpfen Links auf der Seite „Links“ in der NetApp Console für Ihre Cloud-Storage-Systeme.

Sie können Links mithilfe von Anmeldedaten authentifizieren, die im Anmeldedatenservice von Workload Factory gespeichert sind, oder mit dem Anmeldedatenservice Ihres Cloud-Anbieters. Workload Factory unterstützt das Ändern von Authentifizierungsmodi nicht.

Kosten

Für jede Transaktion, die der serverlose Compute-Service Ihres Cloud-Anbieters durchführt, fallen Gebühren an. Da der Service als Vermittler zwischen den beiden Systemen fungiert, entstehen Kosten sowohl beim Senden einer Anfrage an die ONTAP REST API im Dateisystem als auch beim Zurücksenden der Antwort an Workload Factory.

- ["Weitere Informationen zu den Kosten im Zusammenhang mit der Nutzung von AWS Lambda."](#)

- ["Weitere Informationen zu den Kosten im Zusammenhang mit der Nutzung von Oracle Cloud Infrastructure Functions"](#)

Wenn ein Link erforderlich ist

Workload Factory benötigt eine Verbindung, um bestimmte Informationen anzuzeigen und einige Aufgaben auszuführen. Wenn Sie versuchen, einen Vorgang auszuführen, der eine Verbindung erfordert, und Sie dem Cloud Storage-System keine Verbindung zugeordnet haben, benachrichtigt Workload Factory Sie darüber, dass der Vorgang eine Verbindung erfordert.

Zu den Funktionen, die eine Verknüpfung erfordern, gehören:

- Status gut konzipierter Konfigurationen von Cloud-Storage-Systemen für proaktive Wartung, Zuverlässigkeit und Kosten-Leistungs-Optimierung
- ONTAP EMS Ereignisüberwachung und Alarmierung
- NetApp Autonomous Ransomware Protection (ARP/AI)
- Verbesserte ganzheitliche Transparenz der Kapazität über Cloud Storage Systeme hinweg
- Datenreplizierung, Verwaltung und Überwachung von Volumes und Storage-VMs
- Bereitstellung und Verwaltung von SMB/CIFS-Freigaben und NFS-Exportrichtlinien
- Verwaltung von iSCSI-Volumes auf einem Cloud Storage-System
- Erstellung und Verwaltung von Snapshot-Richtlinien für benutzerdefinierte Schutz-SLA
- Verbesserungen im Inode-Management für automatisches Kapazitätsmanagement
- Automatisches Volumenwachstum für elastische Skalierung
- Klonerstellung und -verwaltung für die sofortige, direkte Datenklonierung
- Anzeige zusätzlicher Metriken direkt aus Ihrem Cloud Storage-System, z. B. der Systemversion
- Anzeige der Details zu Speicher-VMs und Cluster-LIFs, einschließlich Rollen, Endpunkten, Knoten, IP-Adressen und Status

Verwandte Informationen

Informationen zum Erstellen und Verknüpfen von Links für:

- ["Amazon FSx for NetApp ONTAP"](#)
- ["OCI NetApp Storage Service"](#)

Berechtigungen für NetApp Workload Factory

Um die Funktionen und Services von NetApp Workload Factory zu nutzen, müssen Sie Berechtigungen erteilen, damit Workload Factory Operationen in Ihrer Cloud-Umgebung durchführen kann.

Warum Berechtigungen verwenden

Wenn Sie Berechtigungen erteilen, weist Workload Factory der Instanz eine Richtlinie mit Berechtigungen zum Managen von Ressourcen und Prozessen in Ihrem Konto beim Cloud-Provider zu. Dadurch kann Workload Factory verschiedene Vorgänge ausführen, von der Erkennung Ihrer Storage-Umgebungen bis hin zum

Einsetzen von Cloud-Ressourcen wie Volumes im Storage-Management.

Bei FSx for ONTAP Datenbank-Workloads beispielsweise scannt Workload Factory, wenn es über die erforderlichen Berechtigungen verfügt, alle EC2-Instanzen in einem bestimmten Konto und einer bestimmten Region und filtert alle Windows-basierten Maschinen. Wenn der AWS Systems Manager (SSM) Agent auf dem Host installiert ist und ausgeführt wird und die Netzwerkkonfiguration von System Manager korrekt ist, kann Workload Factory auf die Windows-Maschine zugreifen und überprüfen, ob die SQL Server-Software installiert ist.

Wie Berechtigungen verwendet werden

Workload Factory verwendet Berechtigungen, um bestimmte Aufgaben auszuführen. Berechtigungen sind in festgelegten Berechtigungsrichtlinien zusammengefasst. Berechtigungsrichtlinien werden in "[die Codebox](#)" angezeigt und sind als JSON kopierbar. Jeder Cloud-Anbieter verfügt über eigene Berechtigungsrichtlinien, die auf die spezifischen Anforderungen und Funktionen dieser Cloud-Umgebung zugeschnitten sind. Diese Dokumentation enthält Berechtigungsreferenzen für jeden Cloud-Anbieter.

Berechtigungsverweise nach Cloud-Anbieter

Auf den folgenden Seiten finden sich Informationen zu den Berechtigungsanforderungen Ihres Cloud-Anbieters:

- "[Amazon FSx for NetApp ONTAP](#)"
- "[OCI NetApp Storage Service](#)"

Amazon FSx for NetApp ONTAP

FSx for ONTAP für Storage-Workloads verwenden

Informationen zu Amazon FSx for NetApp ONTAP in NetApp Workload Factory

Amazon FSx for NetApp ONTAP ist ein vollständig gemanagter, Cloud-basierter Daten-Storage-Service, der fortschrittliche Datenmanagement-Funktionen und hochskalierbare Performance bietet. FSx for ONTAP ermöglicht das Erstellen und Managen von Dateisystemen als Storage-Backend für alle Ihre Workloads innerhalb von NetApp Workload Factory.

FSx for ONTAP bietet die gleichen Funktionen, Performance und administrativen Möglichkeiten, die NetApp Kunden heute vor Ort nutzen, kombiniert mit der Einfachheit, Agilität, Sicherheit und Skalierbarkeit eines nativen AWS-Service.

FSx for ONTAP ist die *Storage*-Komponente in Workload Factory.

Features

FSx for ONTAP bietet folgende Funktionen:

- **Vollständig verwalteter Service:** bietet einen vollständig verwalteten Service, der in die Workload Factory Konsole integriert ist.
- **Hohe Verfügbarkeit:** bietet hohe Verfügbarkeit für jedes FSx for ONTAP Dateisystem und unterstützt Deployments in einzelnen und mehreren Availability Zones.
- **Automatisierte Snapshots:** schützt Daten mit automatisierten, effizienten Snapshots, die nahezu sofort verfügbare, speichereffiziente, zeitpunktgenaue, schreibgeschützte Kopien des Dateisystems oder von Volumes sind.
- **Volume-Replikation:** Ermöglicht Notfallwiederherstellung durch regionsübergreifende Replikation innerhalb von Amazon Web Services.
- **Effiziente Backups:** sorgen mit einer Kopie der Daten in einer anderen Region für Notfälle für eine zusätzliche Schutzebene.
- **Schnelles Klonen:** beschleunigt die Applikationsentwicklung durch schnelles Klonen.
- **Unterstützung mehrerer Protokolle:** Unterstützung der Protokolle Network File System (NFS), Server Message Block (SMB) und Internet Small Computer Systems Interface (iSCSI).
- **Hoher Durchsatz:** Bietet eine hohe Performance, um geringe Latenzzeiten für Workloads zu gewährleisten, die auf FSx for ONTAP Dateisystemen ausgeführt werden.
- **In-memory Cache und NVMe Cache:** umfasst einen einzigartigen In-memory Cache und NVMe Cache, der die Performance häufig abgerufener Daten steigert.
- **Hunderttausende IOPS:** bietet mit SSD-Festplatten Hunderttausende von IOPS und stellt so sicher, dass Ihr Storage und Ihre Workloads zeitnah Ergebnisse erhalten.
- **Thin Provisioning:** ermöglicht die Provisionierung von Kapazität im Voraus und spart Kosten, bis mehr Kapazität benötigt wird.
- **Datendeduplizierung und -komprimierung:** Entfernt doppelte Daten und komprimiert Daten, um den für FSx for ONTAP Dateisysteme erforderlichen physischen Storage zu reduzieren, was zu Kosteneinsparungen führt.

- **Data Tiering:** ermöglicht die Reduzierung der Storage-Kosten durch das Verschieben von seltener abgerufenen Daten vom primären Storage-Tier mit Performance SSDs auf das Storage-Tier des sekundären Kapazitätspools.

Zusätzliche Funktionen in Workload Factory

- **Speicherkostenvergleichsrechner:** Vergleicht Ihre Speicherkosten für Amazon Elastic Block Store (EBS), Elastic File System (EFS) und FSx for Windows File Server Storage mit den Kosten für FSx for ONTAP. Mit dem Rechner lässt sich anzeigen, wie Storage-Konfigurationen für FSx for ONTAP potenzielle Einsparungen bieten, und der Umstieg auf FSx for ONTAP Storage planen.
- **Workload Factory Benutzeroberfläche:** bietet die Bereitstellungsmodusoptionen *Quick create* und *Advanced create*. Quick create umfasst AWS-, NetApp- und branchenübliche Best Practices für Ihre Speicherkonfigurationen.
- **Codebox:** stellt Entwicklern einen Code-Viewer für FSx for ONTAP Vorgänge, Codevorlagen zum Kopieren und Herunterladen sowie einen Automatisierungskatalog zur Wiederverwendung von Code bereit.

Tools zur Verwendung von NetApp Workload Factory

Sie können NetApp Workload Factory mit den folgenden Tools verwenden:

- **Workload Factory console:** Die Workload Factory console bietet einen visuellen, ganzheitlichen Überblick über Ihre Anwendungen und Projekte.
- **NetApp Console:** Die NetApp Console bietet eine hybride Benutzeroberfläche, die die Nutzung von Workload Factory zusammen mit anderen NetApp Datenservices ermöglicht.
- **Ask me:** Mit dem KI-Assistenten Ask me können Sie Fragen stellen und mehr über Workload Factory erfahren, ohne die Workload Factory Konsole zu verlassen. Ask me ist über das Hilfemenü von Workload Factory verfügbar.
- **CloudShell CLI:** Workload Factory umfasst eine CloudShell CLI, um AWS- und NetApp Umgebungen kontenübergreifend über eine einzige browserbasierte CLI zu managen und zu betreiben. Der Zugriff auf CloudShell erfolgt über die obere Leiste der Workload Factory Konsole.
- **REST API:** Mit den Workload Factory REST APIs können Sie Ihre FSx for ONTAP Dateisysteme und andere AWS Ressourcen einsetzen und managen.
- **CloudFormation:** Mit AWS CloudFormation-Code lassen sich die in der Workload Factory Konsole definierten Aktionen ausführen, um AWS- und Drittanbieterressourcen aus dem CloudFormation-Stack in Ihrem AWS-Konto zu modellieren, zu provisionieren und zu managen.
- **NetApp Terraform Provider:** Mit Terraform können Infrastruktur-Workflows erstellt und verwaltet werden, die in der Workload Factory Konsole generiert wurden.

Kosten

AWS verwaltet Ihr Konto für FSx for ONTAP, nicht Workload Factory. Weitere Informationen finden Sie unter ["Preisgestaltung für Amazon FSx for NetApp ONTAP"](#).

Regionen

Workload factory wird in allen kommerziellen Regionen unterstützt, in denen FSx for ONTAP unterstützt wird. ["Unterstützte Amazon Regionen"](#)

Die folgenden AWS-Regionen werden nicht unterstützt:

- China Regionen
- Secret Cloud
- Top Secret Cloud

Hilfe erhalten

Amazon FSx for NetApp ONTAP ist eine Lösung von AWS. Bei Fragen oder technischen Supportproblemen im Zusammenhang mit Ihrem Dateisystem FSx for ONTAP, Ihrer Infrastruktur oder einer Lösung, die diesen Service verwendet, können Sie im Support Center Ihrer AWS Management Console einen Support-Fall bei AWS eröffnen. Dabei wählen Sie den Service „FSx for ONTAP“ und die entsprechende Kategorie aus. Anschließend geben Sie die übrigen Informationen an, die zum Erstellen Ihres AWS Support-Falls erforderlich sind.

Informationen zu allgemeinen Fragen zu Workload Factory oder zu Workload Factory Applikationen und Services finden Sie in ["Hilfe für FSx for ONTAP for Workload Factory"](#).

Einsparmöglichkeiten mit FSx for ONTAP in NetApp Workload Factory

Einsparungen für Ihre Storage-Workloads, die Amazon Elastic Block Store (EBS), Elastic File System (EFS) und FSx for Windows File Server im Vergleich zu FSx for NetApp ONTAP nutzen.

NetApp Workload Factory umfasst einen Rechner für Storage-Einsparungen, mit dem Amazon Storage-Umgebungen mit FSx for ONTAP verglichen werden können. Einsparungen können mit oder ohne Angabe Ihrer AWS-Zugangsdaten geprüft und die Konfigurationseinstellungen für Ihre Storage-Umgebung angepasst werden. Wenn Sie AWS-Zugangsdaten angeben, können Sie beispielsweise eine oder mehrere Instanzen von Amazon Elastic Block Store auswählen und Workload Factory den Vergleich automatisch durchführen lassen. Ob manuell oder automatisch, der Rechner ermittelt, welcher Storage-Service die niedrigsten Kosten für Ihre Storage-Anforderungen bietet.

Wenn der Storage-Rechner ermittelt, dass FSx for ONTAP der kostengünstigste Storage ist, können Sie FSx for ONTAP Konfigurationen erstellen oder speichern und die Codebox verwenden, um Infrastructure-as-Code-Vorlagen zu generieren, unabhängig von den Berechtigungen, die Sie Workload Factory erteilen.

Taschenrechneroptionen

Für den Kostenvergleich zwischen Ihren Systemen und FSx for ONTAP stehen zwei Rechneroptionen zur Verfügung: Anpassung und automatische Erkennung für Ihre Amazon Storage Umgebungen.

Einsparungen durch individuelle Anpassung lassen sich erzielen, indem Sie die Konfigurationseinstellungen für eine Storage-Umgebung angeben, einschließlich Anwendungsfall, Region, Anzahl der Volumes oder Dateisysteme, Storage-Menge, Snapshot-Frequenz, pro Snapshot geänderte Menge, bereitgestellte IOPS, Durchsatz und mehr.

Einsparmöglichkeiten für erkannte Storage Umgebungen: Workload Factory stellt die Verbindung zu Ihren bestehenden AWS Storage Umgebungen her und übernimmt die Details zur automatischen Vergleichsberechnung in den Rechner. Für die Nutzung des automatischen Modus ist die Erteilung von Automatisierungsberechtigungen erforderlich. Der Anwendungsfall kann geändert werden, alle anderen Details werden jedoch in der Berechnung automatisch ermittelt.

Zusätzlich besteht die Möglichkeit, ["AWS Anmeldeinformationen hinzufügen"](#), um die Genauigkeit der Rechneranalyse zu verbessern. **Calculate savings based on existing resources** ist auszuwählen. Anschließend erfolgt die Weiterleitung zur Seite „Add credentials“. Nach dem Hinzufügen der

Anmeldeinformationen sind die vorhandenen Ressourcen auszuwählen, die mit FSx for ONTAP verglichen werden sollen, und anschließend ist **Explore savings** auszuwählen.

Einsparpotenziale durch individuelle Anpassung

Die folgenden Schritte sind auf der Registerkarte für Ihre Storage Auswahl zu finden.

Amazon Elastic Block Store (EBS)

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Unter **FSx for ONTAP** erfolgt die Auswahl von **Einsparmöglichkeiten erkunden** und anschließend der Registerkarte **Amazon Elastic Block Store (EBS)**.
4. Im Storage-Einsparungsrechner sind die folgenden Angaben erforderlich:
 - a. **Anwendungsfall**: Erforderlich. Die Auswahl eines Anwendungsfalls erfolgt im Dropdown-Menü. Der ausgewählte Anwendungsfall bestimmt die Dateisystemeigenschaften von FSx for ONTAP für den Vergleich.
 - b. **Region**: Optional. Wählen Sie die Region für Ihre EBS-Konfiguration aus dem Dropdown-Menü aus.
 - c. **EBS Volume-Typ**: Optional. Der für Ihre Konfiguration verwendete EBS Volume-Typ wird ausgewählt.
 - d. **Anzahl der Volumes**: Optional. Anzahl der Volumes in Ihrer EBS-Konfiguration angeben.
 - e. **Storage-Menge pro Volume (TiB)**: Optional. Eingabe der Storage-Menge pro Volume in TiB.
 - f. **Snapshot-Frequenz**: Optional. Die Snapshot-Frequenz für Ihre EBS-Konfiguration wird ausgewählt.
 - g. **Pro Snapshot geänderte Menge (GiB)**: Optional. Nur für Snapshot-Storage. Die pro Snapshot geänderte Menge in GiB angeben.
 - h. **Provisionierte IOPS pro Volume**: Optional. Für gp3-, io1- und io2-Volumes. Die provisionierten IOPS pro Volume eingeben.
 - i. **Durchsatz (MiB/s)**: Optional. Nur für gp3 Volumes. Der Durchsatz ist in MiB/s pro Volume einzugeben.

Amazon FSx for Windows File Server

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Unter **FSx for ONTAP** erfolgt die Auswahl von **Einsparmöglichkeiten erkunden** und anschließend der Registerkarte **Amazon Elastic Block Store (EBS)**.
4. Im Storage-Einsparungsrechner sind die folgenden Angaben erforderlich:
 - a. **Anwendungsfall**: Erforderlich. Die Auswahl eines Anwendungsfalls erfolgt im Dropdown-Menü. Der ausgewählte Anwendungsfall bestimmt die Dateisystemeigenschaften von FSx for ONTAP für den Vergleich.

- b. **Region:** Optional. Wählen Sie die Region für Ihre FSx for Windows File Server Konfiguration aus dem Dropdown-Menü aus.
- c. **Deployment-Typ:** Optional. Wählen Sie **Single Availability Zone** oder **Multiple Availability Zones**.
- d. **Speichertyp:** Standardmäßig ist der SSD-Speichertyp ausgewählt.
- e. **Speicherkapazität (TiB):** Optional. Eingabe der Storage-Kapazität für die Konfiguration.
- f. **Einsparungen durch Deduplizierung (%):** Optional. Hier wird der erwartete prozentuale Kapazitätseinsparungswert durch Deduplizierung angegeben.
- g. **Snapshot-Frequenz:** Optional. Für Ihre Konfiguration steht eine Auswahl der Snapshot-Frequenz zur Verfügung.
- h. **Pro Snapshot geänderte Menge (GiB):** Optional. Nur für Snapshot-Storage. Die pro Snapshot geänderte Menge in GiB angeben.
- i. **Bereitgestellte SSD IOPS:** Optional. Eingabe der bereitgestellten SSD IOPS.
- j. **Durchsatz (MiB/s):** Optional. Eingabe des Durchsatzes in MiB/s.

Amazon Elastic File System (EFS)

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Unter **FSx for ONTAP** erfolgt die Auswahl von **Einsparmöglichkeiten erkunden** und anschließend der Registerkarte **Amazon Elastic Block Store (EBS)**.
4. Im Storage-Einsparungsrechner sind die folgenden Angaben erforderlich:
 - a. **Anwendungsfall:** Erforderlich. Die Auswahl eines Anwendungsfalls erfolgt im Dropdown-Menü. Der ausgewählte Anwendungsfall bestimmt die Dateisystemeigenschaften von FSx for ONTAP für den Vergleich.
 - b. **Region:** Optional. Wählen Sie die Region für Ihre FSx for Windows File Server Konfiguration aus dem Dropdown-Menü aus.
 - c. **Dateisystemtyp:** Optional. Zur Auswahl stehen **Regional** oder **One zone**.
 - d. **Speicherkapazität (TiB):** Optional. Speicherkapazität der EFS-Konfiguration eingeben.
 - e. **Häufig abgerufene Daten (%):** Optional. Eingabe des Prozentsatzes der Daten, auf die häufig zugegriffen wird.
 - f. **Durchsatzmodus:** Optional. Zur Auswahl stehen **Bereitgestellter Durchsatz** oder **Elastischer Durchsatz**.
 - g. **Durchsatz (MiB/s):** Optional. Angabe des Durchsatzes in MiB/s.

Nach Angabe der Details für Ihre Storage-System-Konfiguration lassen sich die auf der Seite bereitgestellten Berechnungen und Empfehlungen prüfen.

Zusätzlich wird der Bericht am Ende der Seite sichtbar, sobald eine der folgenden Optionen ausgewählt ist:

- **PDF-Export**
- **Per E-Mail senden**
- **Berechnungen anzeigen**

Um zu FSx für ONTAP zu wechseln, folgen Sie den Anweisungen unter [FSx for ONTAP Dateisysteme einsetzen](#).

Einsparungen für erkannte Storage-Umgebungen

Bevor Sie beginnen

Damit Workload Factory Amazon Elastic Block Store (EBS), Elastic File System (EFS) und FSx for Windows File Server Storage-Umgebungen in Ihrem AWS-Konto erkennt, müssen Sie ["Berechtigungen für Ansicht, Planung und Analyse erteilen"](#) in Ihrem AWS-Konto.



Diese Berechnungsoption unterstützt keine Berechnungen für EBS-Snapshots und FSx for Windows File Server Schattenkopien. Wenn Sie Einsparungen durch Anpassungen ermitteln möchten, können Sie Details zu EBS- und FSx for Windows File Server Snapshots angeben.

Die folgenden Schritte sind auf der Registerkarte für Ihre Storage Auswahl zu finden.

Amazon Elastic Block Store (EBS)

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** erfolgt die Auswahl von **Explore savings** und anschließend der Registerkarte **Amazon Elastic Block Store (EBS)**.
4. Auf der Registerkarte **Elastic Block Store (EBS)** erfolgt die Auswahl der Instanz(en) für den Vergleich mit FSx for ONTAP sowie die Auswahl von **Explore savings**.
5. Der Speichereinsparungsrechner wird angezeigt. Die folgenden Merkmale des Storage-Systems werden basierend auf den von Ihnen ausgewählten Instanzen vorausgefüllt:
 - a. **Anwendungsfall**: Der Anwendungsfall für Ihre Konfiguration. Sie können den Anwendungsfall bei Bedarf ändern.
 - b. **Ausgewählte Volumes**: die Anzahl der Volumes in der EBS Konfiguration
 - c. **Gesamte Storage-Menge (TiB)**: die Storage-Menge pro Volumen in TiB
 - d. **Gesamt bereitgestellte IOPS**: für gp3-, io1- und io2-Volumes
 - e. **Gesamtdurchsatz (MiB/s)**: nur für gp3 Volumes

Amazon FSx for Windows File Server

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Unter **FSx for ONTAP** erfolgt die Auswahl von **Explore savings** und anschließend der Registerkarte **Amazon FSx for Windows File Server**.
4. Auf der Registerkarte **Amazon FSx for Windows File Server** können Sie die Instanz(en) auswählen, die mit FSx for ONTAP verglichen werden sollen, und **Einsparungen erkunden** wählen.
5. Der Speichereinsparungsrechner wird angezeigt. Die folgenden Eigenschaften des Storage-Systems sind basierend auf dem Deployment-Typ der von Ihnen ausgewählten Instanz(en) vorausgefüllt:

- a. **Anwendungsfall:** Der Anwendungsfall für Ihre Konfiguration. Sie können den Anwendungsfall bei Bedarf ändern.
- b. **Ausgewählte Dateisysteme**
- c. **Gesamte Storage-Menge (TiB)**
- d. **Bereitgestellte SSD IOPS**
- e. **Durchsatz (MiB/s)**

Amazon Elastic File System (EFS)

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Unter **FSx for ONTAP** erfolgt die Auswahl von **Explore savings** und anschließend der Registerkarte **Amazon Elastic File System (EFS)**.
4. Auf der Registerkarte **Elastic File System (EFS)** können Sie die Instanz(en) für den Vergleich mit FSx for ONTAP sowie **Explore savings** auswählen.
5. Der Speichereinsparungsrechner wird angezeigt. Die folgenden Merkmale des Storage-Systems werden basierend auf den von Ihnen ausgewählten Instanzen vorausgefüllt:
 - a. **Anwendungsfall:** Der Anwendungsfall für Ihre Konfiguration. Sie können den Anwendungsfall bei Bedarf ändern.
 - b. **Gesamtanzahl der Dateisysteme**
 - c. **Gesamte Storage-Menge (TiB)**
 - d. **Bereitgestellter Gesamtdurchsatz (MiB/s)**
 - e. **Gesamter elastischer Durchsatz - Lesen (GiB)**
 - f. **Gesamter elastischer Durchsatz - Schreiben (GiB)**

Nach Angabe der Details für Ihre Storage-System-Konfiguration lassen sich die auf der Seite bereitgestellten Berechnungen und Empfehlungen prüfen.

Zusätzlich wird der Bericht am Ende der Seite sichtbar, sobald eine der folgenden Optionen ausgewählt ist:

- **PDF-Export**
- **Per E-Mail senden**
- **Berechnungen anzeigen**

Bereitstellung von FSx for ONTAP Dateisystemen

Wenn Sie zu FSx for ONTAP wechseln möchten, um Kosteneinsparungen zu erzielen, können Sie **Create** auswählen, um das/die Dateisystem(e) direkt über den Assistenten **Create an FSx for ONTAP file system** zu erstellen, oder **Save** auswählen, um die empfohlene(n) Konfiguration(en) für später zu speichern.

Deployment-Methoden

Mit Berechtigungen für die *Erstellung von Dateisystemen* können Sie das Dateisystem FSx for ONTAP direkt aus Workload Factory einsetzen. Sie können den Inhalt auch aus dem Codebox-Fenster kopieren und das System mit einer der Codebox-Methoden einsetzen.

Mit den Berechtigungen *view*, *planning*, and *analysis* können Sie den Inhalt aus dem Codebox Fenster kopieren und das FSx for ONTAP Dateisystem mithilfe einer der Codebox Methoden einsetzen.

Speicherressourcen erstellen

Cloud Storage-Systeme in NetApp Console erstellen oder erkennen

Cloud Storage-Systeme erstellen oder entdecken, um Volumes und zusätzliche Datenservices über die NetApp Console hinzuzufügen und zu managen.

Ein Storage-System erstellen

Der erste Schritt besteht darin, ein Storage-System zu erstellen. Wenn Sie bereits ein Storage-System in der Konsole Ihres Cloud-Anbieters erstellt haben, können Sie [es mit der NetApp Console entdecken](#).

Über diese Aufgabe

Eine Storage VM wird erstellt, wenn Sie ein Dateisystem erstellen.

Bevor Sie beginnen

Bevor Sie Ihr FSx for ONTAP Dateisystem erstellen, benötigen Sie Folgendes:

- Der ARN einer IAM-Rolle, die Workload Factory die Berechtigungen erteilt, die zum Erstellen eines FSx for ONTAP Dateisystems erforderlich sind. ["Erfahren Sie, wie Sie einem AWS-Konto Berechtigungen erteilen"](#).
- Die Regions- und VPC-Informationen für den Ort, an dem Sie die FSx for ONTAP Instanz erstellen.

Erstellen eines FSx for ONTAP Dateisystems

Sie können ein FSx for ONTAP Dateisystem mit *Quick create* oder *Advanced create* erstellen. Sie können auch die folgenden in der Codebox verfügbaren Tools verwenden: REST API, CloudFormation und Terraform. ["Informationen zur Verwendung von Codebox für die Automatisierung"](#).



Wenn Sie Terraform aus Codebox verwenden, werden im kopierten oder heruntergeladenen Code `fsxadmin` und `vsadmin` Passwörter ausgeblendet. Sie müssen die Passwörter erneut eingeben, wenn Sie den Code ausführen.

Schnellerstellung

Mit Quick create können Sie eine empfohlene Best-Practice-Konfiguration verwenden. Die meisten Einstellungen können Sie nach dem Erstellen eines FSx for ONTAP file system ändern.

Schritte

1. Im Menü der NetApp Console werden **Storage** und dann **Management** ausgewählt.
2. Auf der Seite „Systeme“ erfolgt die Auswahl der Option „System hinzufügen“.
3. Als Standort wird **Amazon Web Services** ausgewählt und anschließend für Amazon FSx for NetApp ONTAP **Add new**.
4. Auf der Seite „FSx for ONTAP Dateisystem erstellen“ erfolgt die Auswahl von **Quick create**.

Sie können auch eine gespeicherte Konfiguration laden.

5. Unter „Allgemeine Dateisystemkonfiguration“ sind folgende Angaben erforderlich:

- a. **AWS-Anmeldeinformationen:** Hier können Sie AWS-Anmeldeinformationen in Workload Factory hinzufügen oder ohne Anmeldeinformationen fortfahren.
- b. **Dateisystemname:** Feld für die Eingabe eines Namens für das Dateisystem.
- c. **Region & VPC:** Auswahl der Region und der VPC für das Dateisystem.
- d. **Deployment-Typ:** Auswahl eines Deployment-Typs.

- Single Availability Zone (Single-AZ) Deployment: stellt Verfügbarkeit durch die Überwachung von Hardwareausfällen und den automatischen Austausch von Infrastrukturkomponenten im Fehlerfall bereit. Erreicht eine hohe Ausfallsicherheit durch die automatische Replikation Ihrer Daten innerhalb einer Verfügbarkeitszone, um sie vor Komponentenausfällen zu schützen.

Diese Konfiguration wird für High-Performance-Workloads empfohlen oder wenn Workloads zunächst klein beginnen und schrittweise auf einen Durchsatz von 72 GB/s und 2,4 Millionen IOPS skalieren.

- Deployment mit mehreren Availability Zones (Multi-AZ): gewährleistet die kontinuierliche Verfügbarkeit von Daten, selbst wenn eine Availability Zone nicht verfügbar ist. Ein Multi-AZ-Dateisystem ist für geschäftskritische Produktions-Workloads konzipiert, die eine hohe Verfügbarkeit gemeinsam genutzter ONTAP Dateidaten erfordern und Storage mit integrierter Replikation über Availability Zones hinweg benötigen.

Diese Konfiguration mit einem einzelnen HA-Paar wird für Workloads empfohlen, die einen Durchsatz von bis zu 6 GB/s oder 200.000 IOPS erfordern.

- e. **Tags:** Optional können Sie bis zu 50 Tags hinzufügen.

6. Unter **Dateisystemdetails** sind die folgenden Angaben erforderlich:

- a. **SSD Storage-Kapazität:** Hier lassen sich die Speicherkapazität und die Einheit der Speicherkapazität angeben.
 - Bei Bereitstellungen der ersten Generation kann die Kapazität nach der Erstellung des Dateisystems nicht mehr verringert werden.
 - Bei Deployments der zweiten Generation können Sie die Kapazität nach der Erstellung des Dateisystems erhöhen.
- b. **ONTAP-Zugangsdaten:** Optional. In diesem Schritt werden Ihr ONTAP-Benutzername und Ihr Passwort eingegeben. Das Passwort kann jetzt oder später festgelegt werden.

Falls der von Ihnen angegebene Benutzer nicht der fsxadmin-Benutzer ist und Sie später das fsxadmin-Passwort zurücksetzen müssen, können Sie dies über die AWS-Konsole tun.

- c. **SMB/CIFS-Einrichtung:** Optional. Wenn Sie das SMB/CIFS-Protokoll für den Zugriff auf Volumes verwenden möchten, müssen Sie Active Directory für die Storage VM während der Dateisystemerstellung konfigurieren. Für die Storage VM, die für dieses Dateisystem erstellt wird, sind die folgenden Details erforderlich.
 - i. **Active Directory-Domäne für den Beitritt:** Eingabe des vollqualifizierten Domainnamens (FQDN) für das Active Directory.
 - ii. **DNS-IP-Adressen:** Es können bis zu drei durch Kommas getrennte DNS-IP-Adressen eingegeben werden.
 - iii. **SMB Server NetBIOS-Name:** Der SMB Server NetBIOS-Name des Active Directory-Computerobjekts, das für Ihre Storage VM erstellt werden soll. Dies ist der Name dieser Storage VM im Active Directory.

- iv. **Benutzername:** Hier wird der Benutzername des Dienstkontos in Ihrem bestehenden Active Directory eingegeben.

Die Eingabe erfolgt ohne Domänenpräfix oder -suffix. Für `EXAMPLE\ADMIN` kommt `ADMIN` zum Einsatz.

- v. **Passwort:** Das Passwort für das Dienstkonto eingeben.
- vi. **Abteilung:** Optional können Sie den Namen der Abteilung eingeben, in der Sie das Computerkonto für FSx for ONTAP erstellen möchten. Die OU ist der eindeutige Pfadname der Abteilung, mit der Sie das Dateisystem verknüpfen möchten.
- vii. **Delegierte Administratorengruppe:** Optional können Sie den Namen der Gruppe in Ihrem Active Directory eingeben, die Ihr Dateisystem verwalten kann.

Wenn Sie AWS Managed Microsoft AD verwenden, müssen Sie eine Gruppe wie `AWS Delegated FSx Administrators`, `AWS Delegated Administrators` oder eine benutzerdefinierte Gruppe mit delegierten Berechtigungen für die Abteilung angeben.

Wenn Sie einem selbstverwalteten AD beitreten, verwenden Sie den Namen der Gruppe in Ihrem AD. Die Standardgruppe ist `Domain Admins`.

- 7. In der **Zusammenfassung** lässt sich die von Ihnen definierte Konfiguration überprüfen. Bei Bedarf können Sie jetzt vor dem Speichern oder Erstellen des Dateisystems jede Einstellung ändern.
- 8. Speichern oder Erstellen des Dateisystems.

Ergebnis

Wenn Sie das Dateisystem erstellt haben, erscheint die neue FSx for ONTAP Konfiguration auf der Seite „Systeme“.

Es gibt verschiedene Möglichkeiten, Ihre FSx for ONTAP Dateisysteme zu managen, etwa über Workloads in der NetApp Console, mit ONTAP System Manager und mit AWS CloudFormation.

Erweiterte Erstellung

Mit **Advanced create** legen Sie alle Konfigurationsoptionen fest, einschließlich Verfügbarkeit, Sicherheit, Backups und Wartung.

Schritte

- 1. Im Menü der NetApp Console werden **Storage** und dann **Management** ausgewählt.
- 2. Auf der Seite „Systeme“ erfolgt die Auswahl der Option „System hinzufügen“.
- 3. Als Standort wird **Amazon Web Services** ausgewählt und anschließend für Amazon FSx for NetApp ONTAP **Add new**.
- 4. Auf der Seite „FSx for ONTAP Dateisystem erstellen“ ist **Advanced create** auszuwählen.

Sie können auch eine gespeicherte Konfiguration laden.

- 5. Unter „Allgemeine Dateisystemkonfiguration“ sind folgende Angaben erforderlich:
 - a. **AWS-Anmeldeinformationen:** Hier können Sie AWS-Anmeldeinformationen in Workload Factory hinzufügen oder ohne Anmeldeinformationen fortfahren.
 - b. **Dateisystemname:** Feld für die Eingabe eines Namens für das Dateisystem.
 - c. **Region & VPC:** Auswahl der Region und der VPC für das Dateisystem.

d. **Deployment-Typ:** Auswahl eines Deployment-Typs und der Dateisystemgeneration. Die Verfügbarkeit eines Dateisystems der zweiten Generation hängt von der ausgewählten Region ab. Wenn die ausgewählte Region keine FSx for ONTAP Dateisysteme der zweiten Generation unterstützt, wird der Deployment-Typ auf die erste Generation umgestellt.

- **Single Availability Zone (Single-AZ) Deployment:** stellt Verfügbarkeit durch die Überwachung von Hardwareausfällen und den automatischen Austausch von Infrastrukturkomponenten im Fehlerfall bereit. Erreicht eine hohe Ausfallsicherheit durch die automatische Replikation Ihrer Daten innerhalb einer Verfügbarkeitszone, um sie vor Komponentenausfällen zu schützen.

Dateisystemgenerierung: Eine der folgenden Optionen ist auszuwählen:

- **Zweite Generation:** Diese Konfiguration wird für Workloads mit hoher Performance oder für Workloads empfohlen, die klein beginnen und schrittweise auf einen Durchsatz von 72 GB/s und 2,4 Millionen IOPS skalieren.
- **Erste Generation:** Diese Konfiguration eignet sich ideal für Workloads, die bis zu 4 GB/s oder 160.000 IOPS benötigen. Dateisysteme der ersten Generation können nur die Kapazität erhöhen.
- **Deployment mit mehreren Availability Zones (Multi-AZ):** gewährleistet die kontinuierliche Verfügbarkeit von Daten, selbst wenn eine Availability Zone nicht verfügbar ist. Ein Multi-AZ-Dateisystem ist für geschäftskritische Produktions-Workloads konzipiert, die eine hohe Verfügbarkeit gemeinsam genutzter ONTAP Dateidaten erfordern und Storage mit integrierter Replikation über Availability Zones hinweg benötigen.

Dateisystemgenerierung: Eine der folgenden Optionen ist auszuwählen:

- **Zweite Generation:** Diese Konfiguration mit einem einzelnen HA-Paar wird für Workloads empfohlen, die einen Durchsatz von bis zu 6 GB/s oder 200.000 IOPS erfordern. In einer Multi-AZ-Umgebung und einem Dateisystem der zweiten Generation kann die Kapazität je nach Workload-Anforderungen erhöht oder verringert werden.
- **Erste Generation:** Diese Konfiguration eignet sich ideal für Workloads, die bis zu 4 GB/s oder 160.000 IOPS benötigen. Dateisysteme der ersten Generation können nur die Kapazität erhöhen.

e. **Tags:** Optional können Sie bis zu 50 Tags hinzufügen.

6. Unter Dateisystemdetails sind die folgenden Angaben erforderlich:

a. **SSD Storage-Kapazität:** Hier lassen sich die Speicherkapazität und die Einheit der Speicherkapazität angeben.

- Bei Bereitstellungen der ersten Generation kann die Kapazität nach der Erstellung des Dateisystems nicht mehr verringert werden.
- Bei Deployments der zweiten Generation lässt sich die Kapazität anpassen.

b. **Durchsatzkapazität pro HA-Paar:** Auswahl der Durchsatzkapazität entsprechend der Anzahl der HA-Paare. Dateisysteme der ersten Generation unterstützen nur ein HA-Paar.

c. **Bereitgestellte IOPS:** Zur Auswahl steht eine der folgenden Optionen:

- **Automatisch:** Bei der automatischen Einstellung werden für jedes erstellte GiB 3 IOPS hinzugefügt.
- **Benutzerseitig bereitgestellt:** Für „Benutzerseitig bereitgestellt“ wird der IOPS-Wert eingegeben.

d. **ONTAP-Zugangsdaten:** Optional. In diesem Schritt werden Ihr ONTAP-Benutzername und Ihr Passwort eingegeben. Das Passwort kann jetzt oder später festgelegt werden.

Falls der von Ihnen angegebene Benutzer nicht der fsxadmin-Benutzer ist und Sie später das fsxadmin-Passwort zurücksetzen müssen, können Sie dies über die AWS-Konsole tun.

- e. **Anmeldeinformationen der Storage VM:** Optional. Eintrag Ihres Benutzernamens. Das Passwort kann spezifisch für dieses Dateisystem sein, oder es kann dasselbe Passwort verwendet werden, das für die ONTAP-Anmeldeinformationen eingegeben wurde. Das Passwort kann jetzt oder später festgelegt werden.
- f. **SMB/CIFS-Einrichtung:** Optional. Wenn Sie das SMB/CIFS-Protokoll für den Zugriff auf Volumes verwenden möchten, müssen Sie Active Directory für die Storage VM während der Dateisystemerstellung konfigurieren. Für die Storage VM, die für dieses Dateisystem erstellt wird, sind die folgenden Details erforderlich.
 - i. **Active Directory-Domäne für den Beitritt:** Eingabe des vollqualifizierten Domainnamens (FQDN) für das Active Directory.
 - ii. **DNS-IP-Adressen:** Es können bis zu drei durch Kommas getrennte DNS-IP-Adressen eingegeben werden.
 - iii. **SMB Server NetBIOS-Name:** Der SMB Server NetBIOS-Name des Active Directory-Computerobjekts, das für Ihre Storage VM erstellt werden soll. Dies ist der Name dieser Storage VM im Active Directory.
 - iv. **Benutzername:** Hier wird der Benutzername des Dienstkontos in Ihrem bestehenden Active Directory eingegeben.

Die Eingabe erfolgt ohne Domänenpräfix oder -suffix. Für `EXAMPLE\ADMIN` kommt `ADMIN` zum Einsatz.

- v. **Passwort:** Das Passwort für das Dienstkonto eingeben.
- vi. **Abteilung:** Optional können Sie den Namen der Abteilung eingeben, in der Sie das Computerkonto für FSx for ONTAP erstellen möchten. Die OU ist der eindeutige Pfadname der Abteilung, mit der Sie das Dateisystem verknüpfen möchten.
- vii. **Delegierte Administratorengruppe:** Optional können Sie den Namen der Gruppe in Ihrem Active Directory eingeben, die Ihr Dateisystem verwalten kann.

Wenn Sie AWS Managed Microsoft AD verwenden, müssen Sie eine Gruppe wie `AWS Delegated FSx Administrators`, `AWS Delegated Administrators` oder eine benutzerdefinierte Gruppe mit delegierten Berechtigungen für die Abteilung angeben.

Wenn Sie einem selbstverwalteten AD beitreten, verwenden Sie den Namen der Gruppe in Ihrem AD. Die Standardgruppe ist `Domain Admins`.

7. Unter Netzwerk & Sicherheit sind die folgenden Angaben erforderlich:

- a. **Sicherheitsgruppe:** Eine neue Sicherheitsgruppe erstellen oder eine vorhandene verwenden.

Informationen zu den Sicherheitsgruppenprotokollen, Ports und Rollen einer neuen Sicherheitsgruppe finden Sie unter [Details zur Sicherheitsgruppe](#).

- b. **Verfügbarkeitszonen:** Auswahl von Verfügbarkeitszonen und Subnetzen.
 - Für Knoten 1 der Clusterkonfiguration: Es sind eine Verfügbarkeitszone und ein Subnetz auszuwählen.
 - Für den Clusterkonfigurationsknoten 2 erfolgt die Auswahl einer Verfügbarkeitszone und eines Subnetzes.

- c. **VPC Routentabellen:** Unter **VPC Routentabellen** wird die VPC Routentabelle ausgewählt, um den Clientzugriff auf Volumes zu aktivieren.
 - d. **Endpunkt-IP-Adressbereich:** Für den **Endpunkt-IP-Adressbereich** ist **Floating IP address range outside your VPC** oder **Enter an IP address range** auszuwählen und ein IP-Adressbereich einzugeben.
 - e. **Verschlüsselung:** Auswahl des Namens des Verschlüsselungsschlüssels aus der Dropdown-Liste.
8. Unter „Datensicherung und Wartung“ sind folgende Angaben erforderlich:
- a. **Volume-Backups:** Tägliche automatische Backups sind standardmäßig aktiviert. Deaktivieren, falls gewünscht.
 - i. **Aufbewahrungsdauer für automatische Backups:** Geben Sie die Anzahl der Tage an, für die automatische Backups aufbewahrt werden sollen.
 - ii. **Tägliches automatisches Sicherungsfenster:** Zur Auswahl stehen **Keine Präferenz** (eine tägliche Sicherungsstartzeit wird für Sie ausgewählt) oder **Startzeit für tägliche Sicherungen auswählen**; anschließend ist eine Startzeit anzugeben.
 - b. **Wöchentliches Wartungsfenster:** Zur Auswahl stehen entweder **Keine Präferenz** (eine Startzeit für das wöchentliche Wartungsfenster wird für Sie ausgewählt) oder **Startzeit für 30-minütiges wöchentliches Wartungsfenster**; zusätzlich ist eine Startzeit anzugeben.
9. Speichern oder Erstellen des Dateisystems.

Ergebnis

Wenn Sie das Dateisystem erstellt haben, erscheint die neue FSx for ONTAP Konfiguration auf der Seite „Systeme“.

Es gibt verschiedene Möglichkeiten, Ihre FSx for ONTAP Dateisysteme zu managen, etwa über Workloads in der NetApp Console, mit ONTAP System Manager und mit AWS CloudFormation.

Ein vorhandenes Cloud Storage-System entdecken

Wenn Sie Ihre Zugangsdaten für Ihren Cloud-Storage-Anbieter zuvor in Workload Factory angegeben haben, können Sie Ihre Storage-Systeme auf der Seite Discoverable systems automatisch erkennen. Dort können Sie auch verfügbare Datenservices prüfen.

Über diese Aufgabe

Sie können ein Cloud Storage-System innerhalb eines Kontos nur einmal erkennen und es einem Arbeitsbereich zuordnen. Das Storage-System kann später entfernt und einem anderen Arbeitsbereich neu zugeordnet werden.

Schritte

1. Im Menü NetApp Console erfolgt die Auswahl von **Storage**, dann **Management** und anschließend **Discoverable systems**.
2. Die Anzahl der ermittelten Cloud Storage-Systeme wird angezeigt. Die Auswahl erfolgt über **Discover**.
3. Zum Hinzufügen zur Seite „Systeme“ ist die Auswahl eines oder mehrerer Storage-Systeme und von **Discover** erforderlich.



- Wenn Sie ein unbenanntes Storage-System auswählen, erhalten Sie eine Aufforderung, einen Namen für das System einzugeben.

- Wenn Sie ein Storage-System auswählen, für dessen Management über die Console nicht die erforderlichen Anmeldeinformationen vorhanden sind, wird eine Aufforderung angezeigt, Anmeldeinformationen mit den erforderlichen Berechtigungen auszuwählen.
- Für die Erkennung werden die folgenden Regionen nicht unterstützt: Regionen in China, GovCloud (US) Regionen, Secret Cloud und Top Secret Cloud.

Ergebnis

Die Console zeigt Ihr erkanntes System auf der Seite „Systeme“ an. Sie können Ihre Storage-Systeme auf verschiedene Weise managen, beispielsweise über Workloads in der NetApp Console sowie mit ONTAP System Manager oder mit den Storage-Management-Tools Ihres Cloud-Providers.

Erstellen einer Storage VM für ein FSx for ONTAP Dateisystem

In NetApp Workload Factory kann für Ihre Workloads eine Storage VM (SVM) für ein FSx for ONTAP Dateisystem erstellt werden, um virtuell auf Storage und Datenservices zuzugreifen.

Über diese Aufgabe

Storage VMs sind isolierte Dateiserver, mit denen Sie auf die Daten aus jedem Workload in Workload Factory Storage zugreifen können. Jede SVM verfügt über eigene administrative Anmeldeinformationen und Endpunkte für die Administration und den Zugriff auf Daten.

Bei SVMs binden Ihre Clients und Workstations beim Zugriff auf Daten in FSx for ONTAP über den Endpunkt (die IP-Adresse) der SVM ein Volume, eine CIFS/SMB-Freigabe oder eine von einer SVM gehostete iSCSI-LUN ein.

Bevor Sie beginnen

Die unterstützte Anzahl von Storage VMs pro Dateisystem kann überprüft werden. Die maximale Anzahl von SVMs pro Dateisystem ist in ["Verwaltung von FSx for ONTAP Storage Virtual Machines"](#) der AWS-Dokumentation angegeben.

Eine Storage VM erstellen

Sie können eine Storage VM über die Workload Factory Konsole erstellen. Sie können auch die folgenden Tools verwenden, die in der Codebox verfügbar sind: REST API, CloudFormation und Terraform.

["Informationen zur Verwendung von Codebox für die Automatisierung"](#).



Wenn Sie Terraform aus Codebox verwenden, werden im kopierten oder heruntergeladenen Code `fsxadmin` und `vsadmin` Passwörter ausgeblendet. Sie müssen die Passwörter erneut eingeben, wenn Sie den Code ausführen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** erfolgt die Auswahl von **Manage** im Aktionsmenü des Dateisystems.
4. In der Dateisystemübersicht befindet sich unter „Speicher-VMs“ die Option „Storage VM erstellen“.
5. Auf der Seite „Storage VM erstellen“ sind unter „Storage VM Konfiguration“ die folgenden Angaben erforderlich:

- a. **Name:** Ein Name für die Storage VM.
- b. **Anmeldeinformationen für die Storage VM:** Hier wird ein Passwort für den Benutzer dieser Storage VM `vsadmin` oder es werden die Benutzeranmeldeinformationen des Dateisystems `fsxadmin` verwendet.
- c. **Sicherheitsstil des Root-Volumes:** Die Auswahl des Sicherheitsstils des Root-Volumes richtet sich nach dem Typ der Clients, die auf Ihre Daten zugreifen: UNIX (Linux-Clients), NTFS (Windows-Clients) oder Gemischt.
- d. **Tags:** Optional können Sie bis zu 50 Tags hinzufügen.

6. **Erstellen** auswählen.

Erstellung eines FSx for ONTAP Volume in Workload Factory

Nach der Einrichtung Ihres FSx for ONTAP Dateisystems ist es in Workload Factory möglich, FSx for ONTAP Volumes als virtuelle Ressourcen zur Gruppierung Ihrer Daten zu erstellen.

Über diese Aufgabe

FSx for ONTAP Volumes gruppieren Daten virtuell, bestimmen, wie Daten gespeichert werden, und legen die Art des Zugriffs auf Ihre Daten fest. Volumes verbrauchen keine Dateisystem-Storage-Kapazität. Die Daten, die in einem Volume gespeichert sind, verbrauchen in erster Linie SSD-Storage. Abhängig von der Tiering-Richtlinie des Volumes können die Daten auch Capacity Pool Storage verbrauchen. Die Größe eines Volumes wird bei der Erstellung festgelegt und kann später geändert werden.

Für Ihre Volumes kommen möglicherweise die folgenden Protokolle zum Einsatz:

- SMB/CIFS: Dateispeicherprotokoll für Windows-Betriebssysteme
- NFS: Dateispeicherprotokoll für Unix-Betriebssysteme
- iSCSI: Blockspeicherprotokoll

S3-Endpunkte können an ein FSx for ONTAP Volume angebunden werden. Mithilfe eines S3-Zugriffspunkts können Sie über die AWS S3 APIs auf Dateidaten zugreifen, die sich auf SMB/CIFS- oder NFS-Volumes befinden. Dadurch können Sie Ihre vorhandenen Daten mit GenAI, ML und Analysen aus AWS Services integrieren, die S3-Zugriffspunkte unterstützen.

Details zu den Volume-Einstellungen

Unveränderliche Dateien

Diese Funktion, auch bekannt als SnapLock, ist standardmäßig deaktiviert. Die Aktivierung unveränderlicher Dateien verhindert das Löschen oder Überschreiben von Daten für einen festgelegten Zeitraum. Die Aktivierung dieser Funktion ist nur bei der Volume-Erstellung möglich. Nachdem die Funktion aktiviert wurde, kann sie nicht mehr deaktiviert werden. Dies ist eine Premium-Funktion für FSx for ONTAP, für die zusätzliche Kosten anfallen. Weitere Informationen dazu finden sich unter ["Wie SnapLock funktioniert"](#) in der Dokumentation zu Amazon FSx for NetApp ONTAP.

- **Aufbewahrungsmodi:** Sie können zwischen zwei Aufbewahrungsmodi wählen - *Enterprise* oder *Compliance*.
 - Im *Enterprise*-Modus kann ein Administrator für unveränderliche Dateien oder SnapLock eine Datei während ihrer Aufbewahrungsfrist löschen.
 - Im *Compliance*-Modus kann eine WORM-Datei erst nach Ablauf ihrer Aufbewahrungsfrist gelöscht

werden. Ebenso kann das unveränderliche Volume erst gelöscht werden, nachdem die Aufbewahrungsfristen aller darin enthaltenen Dateien abgelaufen sind.

- **Aufbewahrungsdauer:** Die Aufbewahrungsdauer hat zwei Einstellungen: *Aufbewahrungsrichtlinie* und *Aufbewahrungszeiträume*. Die *Aufbewahrungsrichtlinie* legt fest, wie lange Dateien in einem unveränderlichen WORM-Zustand aufbewahrt werden. Sie können eine eigene Aufbewahrungsrichtlinie angeben oder die Standard-Aufbewahrungsrichtlinie (nicht angegeben) verwenden, die 30 Jahre beträgt. Die minimalen und maximalen *Aufbewahrungszeiträume* definieren den zulässigen Zeitraum für das Sperren von Dateien.



Auch nach Ablauf der Aufbewahrungsfrist können Sie eine WORM-Datei nicht mehr ändern. Sie können sie nur löschen oder eine neue Aufbewahrungsfrist festlegen, um den WORM-Schutz wieder zu aktivieren.

- **Autocommit:** Sie haben die Möglichkeit, die Autocommit-Funktion zu aktivieren. Die Autocommit-Funktion überführt eine Datei auf einem SnapLock Volume in den WORM-Status, wenn die Datei für die Dauer des Autocommit-Zeitraums nicht geändert wurde. Die Autocommit-Funktion ist standardmäßig deaktiviert. Die Dateien, für die Autocommit verwendet werden soll, müssen sich auf einem SnapLock Volume befinden.
- **Privilegiertes Löschen:** Ein SnapLock Administrator kann das privilegierte Löschen auf einem SnapLock Enterprise Volume aktivieren, um das Löschen einer Datei vor Ablauf ihrer Aufbewahrungsfrist zu ermöglichen. Diese Funktion ist standardmäßig deaktiviert.
- **Volume-Append-Modus:** Vorhandene Daten in einer WORM-geschützten Datei können nicht geändert werden. Unveränderliche Dateien ermöglichen jedoch die Aufrechterhaltung des Schutzes vorhandener Daten mithilfe von WORM-anhängbaren Dateien. Beispielsweise können Protokolldateien generiert oder Audio- oder Videostreaming-Daten bewahrt werden, während Daten inkrementell in diese Dateien geschrieben werden. "[Weitere Informationen zum Volume-append-Modus](#)" in der Amazon FSx for NetApp ONTAP Dokumentation.

Bevor Sie beginnen

Vor dem Erstellen eines Volumes sind die folgenden Voraussetzungen zu beachten:

- Sie benötigen ein FSx for ONTAP Dateisystem in der Workload Factory Konsole.
- Sie müssen über eine Storage VM verfügen.
- Für den Protokollzugriff ist Folgendes erforderlich:
 - Um den Zugriff auf das Volume zu konfigurieren, muss eine Verknüpfung hergestellt werden. "[Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen](#)". Nach der Verknüpfung ist eine Rückkehr zu diesem Vorgang erforderlich.
 - Sie müssen den Zugriff für das von Ihnen gewählte Protokoll konfigurieren, entweder SMB/CIFS, NFS oder iSCSI.

Erstellen Sie ein Volumen

Sie können ein Volume mithilfe der folgenden in der Codebox verfügbaren Tools erstellen: REST API, CloudFormation und Terraform. "[Informationen zur Verwendung von Codebox für die Automatisierung](#)".



Wenn Sie Terraform aus Codebox verwenden, werden im kopierten oder heruntergeladenen Code `fsxadmin` und `vsadmin` Passwörter ausgeblendet. Sie müssen die Passwörter erneut eingeben, wenn Sie den Code ausführen.

Schritte

1. Melden Sie sich bei der "NetApp Console" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Volumes explorer**.
3. **Volume erstellen** auswählen.
4. Auf der Seite „Volume erstellen“ werden unter „Allgemeine Details“ die folgenden Angaben gemacht:
 - a. **Volume-Name:** Ein Name für das Volume.
 - b. **Name der Storage VM:** Optional können Sie einen Namen für die Storage VM eingeben.
 - c. **Volume-Stil:** Auswahl von **FlexVol** oder **FlexGroup** Volume.
 - Ein *FlexVol Volume* ist eine Art von logischem Speicher in ONTAP, mit dem Sie Daten verwalten können. FlexVol Volumes können zwischen Aggregaten oder Knoten innerhalb derselben Storage Virtual Machine (SVM) verschoben werden, ohne den Client-Zugriff zu unterbrechen. Der FlexVol Volume-Stil ist standardmäßig ausgewählt.
 - Ein FlexGroup-Volume ist ein horizontal skalierbarer NAS-Container, der hohe Leistung sowie automatische Lastverteilung und Skalierbarkeit bietet. Es besteht aus mehreren Mitgliedsvolumes (Bestandteilen), die als zugrundeliegende FlexVol Volumes den Datenverkehr transparent teilen.
 - d. **Volumengröße:** Hier werden die Volumengröße und die Einheit angegeben.

Optional können Sie die automatische Vergrößerung des Volumes aktivieren. Diese Option ist verfügbar, wenn Sie **Dateizugriff** als Volume-Zugriffstyp auswählen.

+ FlexGroup Volume hängt die Größe vom Anzahl der Bestandteile ab und erfordert 100 GiB pro Bestandteil.
 - a. **Automatische Volume-Erweiterung:** Optional lässt sich die automatische Volume-Erweiterung aktivieren, um die Kapazität des Volumes automatisch zu erweitern, bis das Volume die maximale Größe erreicht. Diese Funktion trägt einem steigenden Datenaufkommen Rechnung und gewährleistet einen unterbrechungsfreien Betrieb.

Die maximale Größe und Einheit für das Volumenwachstum werden angegeben. Die maximale Wachstumsgröße darf nicht kleiner als die aktuelle Volumengröße sein.
 - b. **Tags:** Optional können Sie bis zu 50 Tags hinzufügen.
5. Unter „Zugriff“ (nur für Dateisysteme mit zugehörigen Verknüpfungen) sind die folgenden Details erforderlich:
 - a. **Zugriffstyp:** Zur Auswahl stehen **Dateizugriff** oder **Blockzugriff**. Zusätzliche Felder zur Konfiguration des Volume-Zugriffs unterscheiden sich je nach Auswahl.
 - **Dateizugriff:** Mehrere autorisierte Benutzer und Geräte erhalten über SMB/CIFS-, NFS- oder Dualprotokolle (SMB/NFS) Zugriff auf das Volume.

Die folgenden Felder sind auszufüllen, um den Dateizugriff auf das Volume einzurichten.
 - b. **NFS-Exportrichtlinie:** Folgende Angaben sind für die Bereitstellung des NFS-Zugriffs erforderlich:
 - i. **Zugriffskontrolle:** Im Dropdown-Menü kann eine **Benutzerdefinierte Exportrichtlinie**, eine **Vorhandene Exportrichtlinie** oder **Kein Zugriff auf das Volume** ausgewählt werden.
 - ii. **Name der Exportrichtlinie:**

Wenn eine benutzerdefinierte Exportrichtlinie ausgewählt wurde, erfolgt die Auswahl eines vorhandenen Richtliniennamens im Dropdown-Menü.

Bei Auswahl einer bestehenden Exportrichtlinie ist ein neuer Richtlinienname erforderlich.

- i. **Exportrichtlinienregel hinzufügen:** Optional können Sie für eine benutzerdefinierte Exportrichtlinie Exportrichtlinienregeln zur Richtlinie hinzufügen.
- c. **SMB/CIFS-Freigabe:** Folgendes ist anzugeben:
 - i. **Name:** Hier wird der Name der SMB/CIFS-Freigabe eingegeben, um Zugriff bereitzustellen.
 - ii. **Berechtigungen:** „Vollzugriff“, „Lesen/Schreiben“, „Lesen“ oder „Kein Zugriff“ auswählen und anschließend die Benutzer oder Gruppen durch ein Semikolon (;) getrennt eingeben. Bei Benutzern oder Gruppen muss die Groß-/Kleinschreibung beachtet werden, und die Domäne des Benutzers muss im Format „domain\username“ angegeben werden.
- d. **Sicherheitsstil:** Bei Dual-Protokoll-Volumes kommt entweder der UNIX- oder der NTFS-Sicherheitsstil zum Einsatz. UNIX ist der Standard-Sicherheitsstil für Dual-Protokoll-Volumes. Ausführliche Informationen zur Benutzerzuordnung in diesem Zusammenhang finden Sie im AWS-Blogartikel ["Ermöglichung von Multiprotokoll-Workloads mit Amazon FSx for NetApp ONTAP"](#).
 - **Blockzugriff:** ermöglicht Hosts, auf denen kritische Geschäftsanwendungen ausgeführt werden, den Zugriff auf das Volume über das iSCSI-Protokoll. Der Blockzugriff ist nur verfügbar, wenn das Dateisystem-Scale-Out-Deployment maximal sechs HA-Paare umfasst.

Zum Einrichten des Blockzugriffs auf das Volume sind die folgenden Felder auszufüllen.

A. **iSCSI Konfiguration:** Die folgenden Details sind erforderlich, um iSCSI für den Blockzugriff auf das Volume zu konfigurieren.

- I. Zur Auswahl stehen **Neue Initiatorgruppe erstellen** oder **Vorhandene Initiatorgruppe zuordnen**.
 - II. Die Auswahl des **Host operating system** erfolgt im Dropdown-Menü.
 - III. Eingabe eines **Namens der Initiatorgruppe** für eine neue Initiatorgruppe.
 - IV. Unter Host-Initiatoren lassen sich ein oder mehrere iSCSI Qualified Names (IQNs) als Host-Initiatoren hinzufügen.
- e. **S3-Zugriffspunkt:** Optional können Sie einen S3-Zugriffspunkt anbinden, um auf FSx for ONTAP-Dateisystemdaten zuzugreifen, die sich auf NFS- oder SMB/CIFS-Volumes befinden, über die AWS S3-APIs. Nur der Dateizugriffstyp wird unterstützt. Folgende Details sind anzugeben:
- **Name des S3 access point:** Geben Sie den Namen des S3 access point ein.
 - **Benutzer:** Wählen Sie einen vorhandenen Benutzer mit Zugriff auf das Volume aus oder erstellen Sie einen neuen Benutzer.
 - **Benutzertyp:** Wählen Sie **UNIX** oder **Windows** als Benutzerart.
 - **Netzwerkconfiguration:** Wählen Sie **Internet** oder **Virtual private cloud (VPC)**. Die Wahl des Netzwerktyps bestimmt, ob der Zugriffspunkt über das Internet erreichbar ist oder auf eine bestimmte VPC beschränkt ist.
 - **Inventartabelle aktivieren:** Wenn Sie die Inventartabelle für das Volume aktivieren, generiert das System Metadaten für alle Objekte, die über den S3-Zugriffspunkt zugänglich sind, und es fallen AWS S3-Anfragekosten an. Weitere Informationen finden Sie unter ["Amazon S3 Preisdokumentation"](#).
- f. **S3 access point tags:** Optional können Sie bis zu 50 Tags hinzufügen oder entfernen.
6. Unter „Effizienz und Schutz“ sind folgende Details anzugeben:
- a. **Speichereffizienz:** Standardmäßig aktiviert. Mit dieser Option lässt sich die Funktion deaktivieren.

ONTAP erreicht Storage-Effizienz durch Deduplizierung und Komprimierung. Deduplizierung entfernt doppelte Datenblöcke. Die Datenkomprimierung komprimiert die Datenblöcke, um den erforderlichen physischen Storage zu reduzieren.

- b. **Snapshot-Richtlinie:** Hier wird die Snapshot-Richtlinie ausgewählt, mit der die Häufigkeit und Aufbewahrungsdauer von Snapshots festgelegt werden.

Im Folgenden sind die Standardrichtlinien von AWS aufgeführt. Vorhandene Snapshot-Richtlinien werden angezeigt, wenn ["einen Link verknüpfen"](#).

default

Diese Richtlinie erstellt automatisch Snapshots nach folgendem Zeitplan, wobei die ältesten Snapshot-Kopien gelöscht werden, um Platz für neuere Kopien zu schaffen:

- Maximal sechs stündliche Momentaufnahmen, die fünf Minuten nach der vollen Stunde erstellt werden.
- Maximal zwei tägliche Schnappschüsse, aufgenommen von Montag bis Samstag jeweils 10 Minuten nach Mitternacht.
- Maximal zwei wöchentliche Snapshots, die jeden Sonntag um 0:15 Uhr erstellt werden.



Die Snapshot-Zeitpunkte basieren auf der Zeitzone des Dateisystems, die standardmäßig auf koordinierte Weltzeit (UTC) eingestellt ist. Informationen zum Ändern der Zeitzone finden Sie ["Anzeige und Einstellung der Systemzeitzone"](#) in der NetApp Supportdokumentation.

default-1weekly

Diese Richtlinie funktioniert auf die gleiche Weise wie die `default` vorherige Richtlinie, mit der Ausnahme, dass sie nur eine Momentaufnahme aus dem Wochenplan beibehält.

none

Diese Richtlinie erstellt keine Snapshots. Sie können diese Richtlinie Volumes zuweisen, um zu verhindern, dass automatisch Snapshots erstellt werden.

- c. **Tiering-Richtlinie:** Auswahl der Tiering-Richtlinie für die im Volume gespeicherten Daten.

Balanced (Auto) ist die Standard-Tiering-Richtlinie beim Erstellen eines Volumes mit der Workload Factory Konsole. Weitere Informationen zu Volume-Tiering-Richtlinien finden sich in ["Volume-Speicherkapazität"](#) der AWS FSx for NetApp ONTAP Dokumentation. Zu beachten ist, dass Workload Factory in der Workload Factory Konsole anwendungsfallbasierte Namen für Tiering-Richtlinien verwendet und die FSx for ONTAP Tiering-Richtliniennamen in Klammern aufführt.

- d. **Unveränderliche Dateien:** Durch Aktivieren der Funktion für unveränderliche Dateien werden die Dateien in diesem Volume dauerhaft in einen unveränderlichen WORM-Zustand (write-once-read-many) versetzt. Folgende Details sind erforderlich:

- i. Zum Aktivieren von **Unveränderliche Dateien mit SnapLock** auswählen.
- ii. Wählen Sie das Kontrollkästchen aus, um zuzustimmen und fortzufahren.
- iii. Wählen Sie **Enable**.
- iv. **Aufbewahrungsmodus:** Auswahl des Modus **Enterprise** oder **Compliance**.
- v. **Aufbewahrungszeitraum:**

- Auswahl der Aufbewahrungsrichtlinie:
 - **Nicht spezifiziert:** Legt die Aufbewahrungsrichtlinie auf 30 Jahre fest.
 - **Zeitraum angeben:** Hier wird die Anzahl der Sekunden, Minuten, Stunden, Tage, Monate oder Jahre eingegeben, um eine eigene Aufbewahrungsrichtlinie festzulegen.
- Auswahl der minimalen und maximalen Aufbewahrungsfristen:
 - **Minimum:** Die Anzahl der Sekunden, Minuten, Stunden, Tage, Monate oder Jahre zum Festlegen der Mindestaufbewahrungsdauer.
 - **Maximum:** Anzahl der Sekunden, Minuten, Stunden, Tage, Monate oder Jahre zum Festlegen der maximalen Aufbewahrungsdauer.
- vi. **Autocommit:** Aktiviert oder deaktiviert Autocommit. Wenn Sie Autocommit aktivieren, geben Sie den Autocommit-Zeitraum an.
- vii. **Privilegiertes Löschen:** Deaktiviert oder aktiviert. Wenn privilegiertes Löschen aktiviert ist, kann ein SnapLock Administrator eine Datei löschen, bevor deren Aufbewahrungsfrist abläuft.
- viii. **Volume-Anfügemodus:** Deaktiviert oder aktiviert. Ermöglicht das Hinzufügen neuer Inhalte zu WORM-Dateien.
- e. **ARP/AI:** NetApp Autonomous Ransomware Protection with AI (ARP/AI) ist standardmäßig aktiviert, wenn ein Link mit dem Dateisystem verknüpft ist. ["Weitere Informationen zu ARP/KI"](#). Voraussetzung zum Fortfahren ist die Zustimmung zu der Erklärung.

Wenn die Funktion nicht verfügbar ist, liegt das aus einem der folgenden Gründe vor:

- Es ist kein Link mit dem Dateisystem verknüpft. ["Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen"](#). Nach der Verknüpfung ist eine Rückkehr zu diesem Vorgang erforderlich.
 - Volumes mit unveränderlichen Dateien und Volumes mit dem NVMe-Protokoll werden für ARP/AI nicht unterstützt. iSCSI Volumes werden ab ONTAP 9.17.1 unterstützt.
 - Das Dateisystem verfügt bereits über eine ARP/AI-Richtlinie.
7. Geben Sie unter „Erweiterte Konfiguration“ die folgenden Details ein. Die Felder in diesem Abschnitt unterscheiden sich je nach gewähltem Volume-Stil.
- a. **Verbindungspfad:** Hier wird der Speicherort im Namespace der Storage VM angegeben, an dem das Volume eingehängt wird. Der Standard-Verbindungspfad ist `/<volume-name>`.
 - b. **Aggregatname:** Nur für FlexVol volumes. Wählen Sie das Aggregat aus, das das neue Volume aufnehmen soll.
 - c. **Aggregatliste:** Nur für FlexGroup Volumes. Hinzufügen oder Entfernen von Aggregaten. Die Mindestanzahl an Aggregaten beträgt eins.
 - d. **Anzahl der Bestandteile:** Nur für FlexGroup Volumes. Eingabe der Anzahl der Bestandteile pro Aggregat. Pro Bestandteil werden 100 GiB benötigt.
8. **Erstellen** auswählen.

Verwandte Informationen

- ["Anpassen der Volumenkapazität in Workload Factory"](#)
- ["Ändern der Volume-Tiering-Richtlinie in Workload Factory"](#)
- ["Verwalten von S3-Zugriffspunkten in Workload Factory"](#)

Erstellen Sie eine Initiatorgruppe für ein Dateisystem in NetApp Workload Factory

Verwenden Sie NetApp Workload Factory, um Initiatorgruppen zu erstellen und den Hostzugriff auf SAN-Blockgeräte zu verwalten.

Über diese Aufgabe

Initiatorgruppen, oder Initiatorgruppen (igroups), verbinden Blockgeräte (LUNs) mit den Rechenressourcen, die darauf zugreifen dürfen. Im Gegensatz zu NFS oder CIFS, wo ein Volume allgemein zugänglich ist und Benutzerberechtigungen den Zugriff steuern, werden Berechtigungen für Blockspeicher auf Maschinenebene verwaltet. Typischerweise kann jeweils nur ein System auf ein Blockgerät zugreifen.

Eine Initiatorgruppe dient als Berechtigungsebene für Blockspeicher. Wenn sich ein Server mit dem Speichersystem verbindet, identifiziert er sich mit seinem iSCSI qualified (IQN) Host-Initiator. Wenn dieser IQN zu einer oder mehreren Initiatorgruppen gehört, erhält der Server Zugriff auf alle LUNs, die diesen Initiatorgruppen zugeordnet sind. Sowohl eine Initiatorgruppe als auch eine iSCSI-Hostverbindung sind erforderlich, damit iSCSI ordnungsgemäß funktioniert.

Bevor Sie beginnen

Sie müssen eine Verknüpfung herstellen, um Initiatorgruppen zu erstellen. ["Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen"](#). Nach der Verknüpfung kann zu diesem Vorgang zurückgekehrt werden.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Auf der Seite FSx for ONTAP erfolgt die Auswahl der Registerkarte **Block devices**.
4. Wählen Sie den Ressourcentyp **Create initiator group** und anschließend **Create igroup**.
5. Führen Sie im Dialogfeld **Initiatorgruppe erstellen** Folgendes aus:
 - **igroup name**: Geben Sie einen Namen für die Initiatorgruppe ein.
 - **igroup description**: (Optional) Geben Sie eine Beschreibung für die Initiatorgruppe ein.
 - **Name der Storage-VM**: Wählen Sie die Storage-VM für die Initiatorgruppe aus.
 - **Blockgerätename**: Wählen Sie ein oder mehrere Blockgeräte aus, die der Initiatorgruppe zugeordnet werden sollen. Die aufgelisteten Blockgeräte sind diejenigen, die noch keinem Host-Initiator zugeordnet wurden.
 - **Betriebssystemtyp**: Wählen Sie Linux, VMware oder Windows für den Betriebssystemtyp aus.
 - **Host-Initiatoren**: Fügen Sie der Initiatorgruppe einen oder mehrere iSCSI Qualified (IQN) Host-Initiatoren hinzu.
6. **Erstellen** auswählen.

Verwandte Informationen

["Verwalten des Blockspeichers für ein FSx for ONTAP file system"](#)

Erstellung eines Blockgeräts für ein Dateisystem in NetApp Workload Factory

Blockgeräte können erstellt werden, um die Applikationsanforderungen Ihres Geschäftsbereichs zu unterstützen. Blockgeräte können in einem bestehenden Volume erstellt, ein neues Volume für das neue Blockgerät angelegt oder ein neues Volume aus

einem Snapshot für das neue Blockgerät erstellt werden.

Über diese Aufgabe

Für Block-Devices in NetApp Workload Factory werden nur FlexVol Volumes unterstützt. Sie können Block-Devices mithilfe des iSCSI-Protokolls erstellen.

Die Blockgröße muss kleiner sein als die verfügbare Größe des FlexVol volume.

Bevor Sie beginnen

- Sie müssen eine Verknüpfung herstellen, um Blockgeräte zu erstellen. ["Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen"](#). Nach der Verknüpfung kann zu diesem Vorgang zurückgekehrt werden.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In FSx for ONTAP erfolgt zunächst die Auswahl des Dateisystems, für das ein Blockgerät erstellt werden soll, und anschließend die Auswahl der Registerkarte **Block devices**.
4. Anschließend ist **Blockgerät erstellen** auszuwählen.
5. Unter **Volume details** erfolgen die folgenden Schritte:
 - a. **Volume-Name:** Zur Auswahl steht eine der folgenden Optionen.
 - Neues Volume erstellen und den Namen des Volumes eingeben.
 - Ein vorhandenes Volume auswählen.
 - Aus einem Volume-Snapshot erstellen. Den Namen des Quellvolumes und den Snapshot-Namen auswählen. Nur Volumes ohne Blockgeräte sind verfügbar.
 - b. **Aggregatname:** Wählen Sie das Aggregat aus, das das neue Volume aufnehmen soll.
 - c. **Storage VM:** Auswahl einer Storage VM.
 - d. **Volumestil:** Der standardmäßige Volumestil ist **FlexVol**.
 - e. **Volumengröße:** Größe des Volumens eingeben und Einheit auswählen. Die maximale Größe pro FlexVol volume beträgt 100 TiB.
 - f. **Automatische Volumenerweiterung:** Optional lässt sich die automatische Volumenerweiterung aktivieren, damit sich das Volumen automatisch vergrößert, wenn es seine Kapazitätsgrenze erreicht. Die maximale Erweiterungsgröße beträgt 300 TiB.
 - g. **Tags:** Optional lassen sich Tags hinzufügen, um Ihr Blockgerät zu organisieren und zu kategorisieren.
6. Unter **Details zum Blockgerät** sind folgende Schritte erforderlich:
 - a. **Blockgerätename:** Hier geben Sie einen Namen für das Blockgerät ein.
 - b. **Blockgerätegröße:** Geben Sie die Größe des Blockgeräts ein und wählen Sie die Einheit aus. Die Blockgerätegröße muss kleiner als die verfügbare Volumengröße sein.
7. Unter **Zugriff** sind die folgenden Schritte auszuführen:
 - a. **iSCSI Konfiguration:** Eine der folgenden Optionen ist auszuwählen.
 - **Neue Initiatorgruppe erstellen:** Angabe des Host-Betriebssystems und des Namens der Initiatorgruppe sowie Hinzufügen eines oder mehrerer Host-Initiatoren mit iSCSI qualified name (IQN).

- **Vorhandene Initiatorgruppe zuordnen:** Auswahl einer vorhandenen Initiatorgruppe, Angabe des Host-Betriebssystems und Auswahl eines oder mehrerer iSCSI qualified name (IQN) Host-Initiatoren.

8. Unter **Effizienz und Schutz** ist Folgendes erforderlich:

- a. **Speichereffizienz:** Standardmäßig aktiviert. Mit dieser Option lässt sich die Funktion deaktivieren.

ONTAP erreicht Storage-Effizienz durch Deduplizierung und Komprimierung. Deduplizierung entfernt doppelte Datenblöcke. Die Datenkomprimierung komprimiert die Datenblöcke, um den erforderlichen physischen Storage zu reduzieren.

- b. **Snapshot-Richtlinie:** Hier wird die Snapshot-Richtlinie ausgewählt, mit der die Häufigkeit und Aufbewahrungsdauer von Snapshots festgelegt werden.

Im Folgenden sind die Standardrichtlinien von AWS aufgeführt. Vorhandene Snapshot-Richtlinien werden angezeigt, wenn ["einen Link verknüpfen"](#).

default

Diese Richtlinie erstellt automatisch Snapshots nach folgendem Zeitplan, wobei die ältesten Snapshot-Kopien gelöscht werden, um Platz für neuere Kopien zu schaffen:

- Maximal sechs stündliche Momentaufnahmen, die fünf Minuten nach der vollen Stunde erstellt werden.
- Maximal zwei tägliche Schnappschüsse, aufgenommen von Montag bis Samstag jeweils 10 Minuten nach Mitternacht.
- Maximal zwei wöchentliche Snapshots, die jeden Sonntag um 0:15 Uhr erstellt werden.



Die Snapshot-Zeitpunkte basieren auf der Zeitzone des Dateisystems, die standardmäßig auf koordinierte Weltzeit (UTC) eingestellt ist. Informationen zum Ändern der Zeitzone finden Sie ["Anzeige und Einstellung der Systemzeitzone"](#) in der NetApp Supportdokumentation.

default-1weekly

Diese Richtlinie funktioniert auf die gleiche Weise wie die `default` vorherige Richtlinie, mit der Ausnahme, dass sie nur eine Momentaufnahme aus dem Wochenplan beibehält.

none

Diese Richtlinie erstellt keine Snapshots. Sie können diese Richtlinie Volumes zuweisen, um zu verhindern, dass automatisch Snapshots erstellt werden.

- c. **Tiering-Richtlinie:** Auswahl der Tiering-Richtlinie für die im Volume gespeicherten Daten.

Balanced (Auto) ist die Standard-Tiering-Richtlinie beim Erstellen eines Volumes mit der Workload Factory Konsole. Weitere Informationen zu Volume-Tiering-Richtlinien finden sich in ["Volume-Speicherkapazität"](#) der AWS FSx for NetApp ONTAP Dokumentation. Zu beachten ist, dass Workload Factory in der Workload Factory Konsole anwendungsfallbasierte Namen für Tiering-Richtlinien verwendet und die FSx for ONTAP Tiering-Richtliniennamen in Klammern aufführt.

- d. **ARP/AI:** NetApp Autonomous Ransomware Protection with AI (ARP/AI) ist standardmäßig aktiviert, wenn ein Link mit dem Dateisystem verknüpft ist. ["Weitere Informationen zu ARP/KI"](#). Voraussetzung zum Fortfahren ist die Zustimmung zu der Erklärung.

Wenn die Funktion nicht verfügbar ist, liegt das aus einem der folgenden Gründe vor:

- Es ist kein Link mit dem Dateisystem verknüpft. ["Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen"](#). Nach der Verknüpfung ist eine Rückkehr zu diesem Vorgang erforderlich.
- ARP/AI unterstützt keine Volumes mit unveränderlichen Dateien und keine Volumes mit dem NVMe-Protokoll.
- Das Dateisystem verfügt bereits über eine ARP/AI-Richtlinie.

9. **Erstellen** auswählen.

Verwandte Informationen

["Verwalten des Blockspeichers für ein FSx for ONTAP file system"](#)

Verbindung zu einem FSx for ONTAP-Dateisystem mit einem Lambda-Link herstellen

Für die Durchführung erweiterter ONTAP Managementvorgänge wird eine Verbindung zwischen Ihrem Workload Factory Konto und einem oder mehreren FSx for ONTAP Dateisystemen eingerichtet. Dies umfasst die Verknüpfung neuer und bestehender Lambda Links sowie die Authentifizierung der Links. Die Linkverknüpfung ermöglicht die Überwachung und Verwaltung bestimmter Funktionen direkt vom FSx for ONTAP Dateisystem aus, die über die Amazon FSx for ONTAP API nicht verfügbar sind.

["Weitere Informationen zu Links"](#).

Über diese Aufgabe

Links nutzen AWS Lambda, um Code als Reaktion auf Ereignisse auszuführen und die dafür benötigten Rechenressourcen automatisch zu verwalten. Die von Ihnen erstellten Links sind Teil Ihres NetApp Kontos und mit einem AWS Konto verknüpft.

Beim Definieren eines FSx for ONTAP Dateisystems können Sie in Ihrem Konto eine Verknüpfung erstellen. Diese Verknüpfung verwenden Sie für dieses Dateisystem und können sie auch für andere FSx for ONTAP Dateisysteme nutzen. Sie können eine Verknüpfung auch später einem Dateisystem zuordnen.

Links erfordern Authentifizierung. Sie können Links mithilfe von Anmeldeinformationen authentifizieren, die im Workload Factory Anmeldeinformationsdienst oder mit Ihren Anmeldeinformationen, die in AWS Secrets Manager gespeichert sind, hinterlegt sind. Pro Link wird nur ein Authentifizierungsverfahren unterstützt. Wenn beispielsweise die Link-Authentifizierung mit AWS Secrets Manager ausgewählt wird, kann das Authentifizierungsverfahren später nicht mehr geändert werden.

Die Link-Konnektivität für GovCloud Konten wird unterstützt. Workload Factory verwendet GovCloud Authentifizierungsschlüssel und ermöglicht so einen sicheren, agentenlosen Zugriff auf Ihre Cloud Storage-Systeme über von GovCloud genehmigte Mechanismen.



AWS Secrets Manager wird bei Verwendung eines Console Agenten nicht unterstützt.

Einen neuen Link verknüpfen

Das Verknüpfen eines neuen Links umfasst die Linkerstellung und die Zuordnung.

In diesem Workflow haben Sie zwei Möglichkeiten, Links zu erstellen – automatisch oder manuell. Wenn Sie

ein AWS GovCloud Konto haben, müssen Sie einen neuen Link manuell erstellen.

- Automatisch: Erstellt einen Link mit automatischer Registrierung über Workload Factory. Ein automatisch erstellter Link benötigt Tokens für die Workload Factory Automatisierung und der CloudFormation-Code ist kurzlebig. Er kann maximal sechs Stunden lang verwendet werden.
- Manuell: Erstellt einen Link mit manueller Registrierung mithilfe von entweder CloudFormation oder Terraform aus der Codebox. Der Code bleibt erhalten und gibt Ihnen mehr Zeit, den Vorgang abzuschließen. Dies ist nützlich, wenn mit verschiedenen Teams wie Security und DevOps zusammengearbeitet wird, die möglicherweise zunächst die Berechtigungen erteilen müssen, die für die Fertigstellung der Linkerstellung erforderlich sind.

Bevor Sie beginnen

- Es sollte berücksichtigt werden, welche Option zur Linkerstellung verwendet wird.
- Sie benötigen mindestens ein FSx for ONTAP Dateisystem in Workload Factory. Um FSx for ONTAP Dateisysteme zu ermitteln, ist ein AWS-Konto mit Berechtigungen für FSx for ONTAP Instanzen sowie ["Anmeldeinformationen in Workload Factory hinzufügen"](#) mit den Berechtigungen *view, planning, and analysis* für das Storage management erforderlich.
- Die folgenden Ports müssen in der Sicherheitsgruppe, die dem FSx for ONTAP Dateisystem zugeordnet ist, für die Verbindung offen sein.
 - Für die Workload Factory Konsole: Port 443 (HTTPS)
 - Für CloudShell und FSx für ONTAP Notfallmanagementsystem (EMS) Ereignisanalyse: Port 22 (SSH)
- Die Verbindung muss zu folgendem Endpunkt möglich sein: <https://api.workloads.netapp.com>. Die webbasierte Konsole kontaktiert diesen Endpunkt, um mit den Workload Factory APIs zu interagieren und FSx for ONTAP Workloads zu verwalten und zu betreiben.
- Sie benötigen in Ihrem AWS-Konto die folgenden Berechtigungen, wenn Sie mithilfe eines CloudFormation Stacks einen Link hinzufügen:

▼ Details

```
[
  "cloudformation:GetTemplateSummary",
  "cloudformation:CreateStack",
  "cloudformation:DescribeStacks",
  "cloudformation:ListStacks",
  "cloudformation:DescribeStackEvents",
  "cloudformation:ListStackResources",
  "ec2:DescribeSubnets",
  "ec2:DescribeSecurityGroups",
  "ec2:DescribeVpcs",
  "iam:ListRoles",
  "iam:GetRolePolicy",
  "iam:GetRole",
  "iam>DeleteRolePolicy",
  "iam:CreateRole",
  "iam:DetachRolePolicy",
  "iam:PutRolePolicy",
  "iam>DeleteRole",
  "iam:AttachRolePolicy",
```

```

"lambda:InvokeFunction",
"lambda:GetFunction",
"lambda:CreateFunction",
"lambda>DeleteFunction",
"iam:PassRole",
"lambda:TagResource",
"ecr:BatchGetImage",
"ecr:GetDownloadUrlForLayer",
"lambda:AddPermission",
"lambda:RemovePermission",
"cloudformation:DeleteStack",
"kms:CreateGrant",
"kms:GenerateDataKey"
]

```

Automatisch erstellen

Verwenden Sie CloudFormation, um den Link innerhalb von Workload Factory automatisch zu erstellen und zu registrieren.



Die automatische Linkerstellung wird für AWS GovCloud accounts nicht unterstützt.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü  **Administration > Links**.
3. Auf der Seite „Links“ **Erstellen und verknüpfen** auswählen.
4. Im Dialogfeld „Verknüpfung zuordnen“ das Dateisystem auswählen, das mit der Verknüpfung verknüpft werden soll, und **Weiter** auswählen.
5. **Neuen Link erstellen** auswählen und dann **Weiter** auswählen.
6. Auf der Seite „Link erstellen“ die Option **Automatisch erstellen** auswählen und anschließend Folgendes angeben:
 - a. **Linkname**: Geben Sie den Namen ein, den Sie für diesen Link verwenden möchten. Der Name muss innerhalb Ihres Kontos eindeutig sein.
 - b. **AWS Secrets Manager**: Optional. Ermöglicht es Workload Factory, FSx for ONTAP Zugangsdaten aus Ihrem AWS Secrets Manager abzurufen.

Der Link-Bereitstellungsstack fügt der Lambda-Berechtigungsrichtlinie automatisch den folgenden Standard-ARN-Regex für den Secret Manager hinzu:

```
arn:aws:secretsmanager:<link_deployment_region>:<link_deployment_account_id>:secret:FSxSecret*.
```

Sie können entweder Geheimnisse entsprechend den Standardberechtigungen erstellen oder Ihre benutzerdefinierten Berechtigungen für die Linkrichtlinie zuweisen.

Konfigurieren des VPC Private Endpoint für AWS Secrets Manager ist standardmäßig deaktiviert. Die Auswahl dieser Option speichert das Secret über den VPC Private Endpoint, anstatt es lokal zu

speichern.

a. **Linkberechtigungen:** Eine der folgenden Optionen für Linkberechtigungen kann ausgewählt werden:

- **Automatisch:** Diese Option sorgt dafür, dass der AWS CloudFormation Code automatisch die Lambda-Berechtigungsrichtlinie und die Ausführungsrolle erstellt.
- **Benutzerdefinierte Ausführungsrolle:** Diese Option weist der Lambda-Verbindung eine bestimmte Lambda-Ausführungsrolle und die zugehörigen Richtlinien zu. Für die Lambda-Berechtigungsrichtlinie sind die folgenden Berechtigungen erforderlich. Die `secretsmanager:GetSecretValue` Berechtigung ist nur erforderlich, wenn AWS Secrets Manager aktiviert ist.

```
"ec2:CreateNetworkInterface",  
"ec2:DescribeNetworkInterfaces",  
"ec2:DeleteNetworkInterface",  
"ec2:AssignPrivateIpAddresses",  
"ec2:UnassignPrivateIpAddresses",
```

Geben Sie den ARN der Lambda-Ausführungsrolle in das Textfeld ein.

b. **Tags:** Optional können Sie diesem Link Tags hinzufügen, um Ihre Ressourcen besser zu kategorisieren. Beispielsweise könnte ein Tag hinzugefügt werden, der diesen Link als von Amazon FSx für ONTAP File Systems verwendet kennzeichnet.

Workload Factory ruft automatisch das AWS-Konto, den Standort und die Sicherheitsgruppe basierend auf dem FSx for ONTAP-Dateisystem ab.

7. **Erstellen** auswählen.

Das Dialogfeld „Weiterleitung zu CloudFormation“ wird angezeigt und erläutert, wie der Link aus dem AWS CloudFormation Service erstellt wird.

8. **Weiter** auswählen, um die AWS Management Console zu öffnen und sich dann beim AWS-Konto für dieses FSx for ONTAP Dateisystem anzumelden.

9. Auf der Seite „Quick create stack“ erfolgt unter „Capabilities“ die Auswahl von „Ich bestätige, dass AWS CloudFormation IAM-Ressourcen erstellen kann“.

Die CloudFormation-Vorlage erteilt Lambda beim Start drei Berechtigungen. Workload Factory verwendet diese Berechtigungen bei der Nutzung von Links.

```
"lambda:InvokeFunction",  
"lambda:GetFunction",  
"lambda:UpdateFunctionCode"
```

10. **Stapel erstellen** auswählen und dann **Weiter** auswählen.

Sie können den Status der Linkerstellung auf der Ereignisseite verfolgen. Dies sollte nicht länger als fünf Minuten dauern.

11. Zurück in der Workload Factory Oberfläche ist zu sehen, dass die Verknüpfung mit dem FSx for ONTAP Dateisystem verbunden ist.

Manuell erstellen

Sie können mithilfe zweier Infrastructure-as-Code (IaC) Tools aus der Codebox eine Verknüpfung erstellen: CloudFormation oder Terraform. Mit dieser Option wird der ARN für die Verknüpfung aus AWS CloudFormation extrahiert und hier angegeben. Workload Factory registriert die Verknüpfung manuell für Sie.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü  **Administration > Links**.
3. Auf der Seite „Links“ **Erstellen und verknüpfen** auswählen.
4. Im Dialogfeld „Verknüpfung zuordnen“ das Dateisystem auswählen, das mit der Verknüpfung verknüpft werden soll, und **Weiter** auswählen.
5. **Neuen Link erstellen** auswählen und dann **Weiter** auswählen.
6. Auf der Seite „Link erstellen“ **Manuell erstellen** auswählen und dann CloudFormation oder Terraform aus dem Codefeld auswählen.
7. Unter „Details und Anmeldeinformationen“ sind folgende Angaben zu machen:
 - a. **Linkname**: Geben Sie den Namen ein, den Sie für diesen Link verwenden möchten. Der Name muss innerhalb Ihres Kontos eindeutig sein.
 - b. **AWS Secrets Manager**: Immer aktiviert für GovCloud-Konten. Optional für andere Konten. Ermöglicht es Workload Factory, FSx for ONTAP Zugangsdaten aus Ihrem AWS Secrets Manager abzurufen.

Sie können entweder Geheimnisse entsprechend den Standardberechtigungen erstellen oder Ihre benutzerdefinierten Berechtigungen für die Linkrichtlinie zuweisen.

Konfigurieren des VPC Private Endpoint für AWS Secrets Manager ist standardmäßig deaktiviert. Die Auswahl dieser Option speichert das Secret über den VPC Private Endpoint, anstatt es lokal zu speichern.

- c. **Linkberechtigungen**: Eine der folgenden Optionen für Linkberechtigungen kann ausgewählt werden:
 - **Automatisch**: Diese Option sorgt dafür, dass der AWS CloudFormation Code automatisch die Lambda-Berechtigungsrichtlinie und die Ausführungsrolle erstellt.
 - **Benutzerdefiniert**: Wählen Sie diese Option, um eine bestimmte Lambda-Ausführungsrolle und die zugehörigen Richtlinien dem Lambda-Link zuzuweisen. Für die Lambda-Berechtigungsrichtlinie sind die folgenden Berechtigungen erforderlich. Die ``secretsmanager:GetSecretValue`` Berechtigung ist nur bei Verwendung von AWS Secrets Manager erforderlich.

```
"ec2:CreateNetworkInterface",  
"ec2:DescribeNetworkInterfaces",  
"ec2:DeleteNetworkInterface",  
"ec2:AssignPrivateIpAddresses",
```



```
"ec2:UnassignPrivateIpAddresses"
```

Geben Sie den ARN der Lambda-Ausführungsrolle in das Textfeld ein.

- d. **Tags:** Optional können Sie diesem Link Tags hinzufügen, um Ihre Ressourcen besser zu kategorisieren. Beispielsweise könnte ein Tag hinzugefügt werden, der diesen Link als von Amazon FSx für ONTAP File Systems verwendet kennzeichnet.
- e. **Linkregistrierung:** Wählen Sie CloudFormation oder Terraform aus, um Anweisungen zur Registrierung des Links zu erhalten, und folgen Sie diesen Anweisungen.

Die CloudFormation-Vorlage erteilt Lambda beim Start drei Berechtigungen. Workload Factory verwendet diese Berechtigungen bei der Nutzung von Links.

```
"lambda:InvokeFunction",  
"lambda:GetFunction",  
"lambda:UpdateFunctionCode"
```

+

- i. Nachdem Sie den Stack erfolgreich erstellt haben, fügen Sie den Lambda-ARN in das Textfeld in der Workload Factory-Konsole ein. Workload Factory ruft automatisch das AWS-Konto, den Standort und die Sicherheitsgruppe basierend auf dem FSx for ONTAP-Dateisystem ab.
- ii. **Erstellen** auswählen.

Sie können den Status der Linkerstellung auf der Ereignisseite verfolgen. Dies sollte nicht länger als fünf Minuten dauern.

Ergebnis

Workload Factory verknüpft die Verbindung mit dem FSx for ONTAP-Dateisystem. Erweiterte ONTAP Operationen sind möglich.

Eine bestehende Verbindung mit einem FSx for ONTAP Dateisystem verknüpfen

Nachdem ein Link erstellt wurde, wird er einem oder mehreren FSx for ONTAP Dateisystemen zugeordnet.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Auf der Seite „FSx for ONTAP“ erfolgt die Auswahl von **Associate link** im Aktionsmenü des Dateisystems, dem ein Link zugeordnet werden soll.
4. Auf der Seite „Link verknüpfen“ **Vorhandenen Link verknüpfen** auswählen, den Link auswählen und **Weiter** auswählen.
5. Den Authentifizierungsmodus auswählen.
 - Workload Factory: Das Passwort zweimal eingeben.
 - AWS Secrets Manager: den geheimen ARN eingeben.

Es sollte sichergestellt sein, dass der Secret-ARN die folgenden Schlüssel-Wert-Paare enthält, wobei

filesystemID optional ist.

- `filesystemID` = `FSx_filesystem_id` (optional)
- `user` = `FSx_user`
- `Passwort` = Benutzerpasswort



Die Authentifizierung mit AWS Secrets Manager erfordert einen Benutzer, entweder den von Ihnen angegebenen `FSx_user` oder einen anderen Benutzer, der im FSx for ONTAP Dateisystem erstellt wurde. Der Standardbenutzer ist `fsxadmin`, wenn Sie keinen Benutzer angeben.

6. **Anwenden** auswählen.

Ergebnis

Der Link ist mit dem FSx for ONTAP Dateisystem verknüpft. Erweiterte ONTAP Operationen sind möglich.

Verwandte Informationen

["Weitere Informationen zu Links"](#).

Probleme mit der AWS Secrets Manager Authentifizierung beheben

Problem

Der Link hat keine Berechtigung, das Geheimnis abzurufen.

Lösung: Berechtigungen nach der Aktivierung des Links hinzufügen. In der AWS-Konsole anmelden, den Lambda-Link suchen und die zugehörige Berechtigungsrichtlinie bearbeiten.

Problem

Das Geheimnis wurde nicht gefunden.

Lösung: Der korrekte geheime ARN ist bereitzustellen.

Problem

Das Geheimnis liegt nicht im richtigen Format vor.

Lösung: Zu AWS Secrets Manager wechseln und das Format bearbeiten.

Das Geheimnis sollte die folgenden Schlüssel-Wert-Paare enthalten:

- `filesystemID` = `FSx_filesystem_id`
- `Benutzername` = `FSx_user`
- `Passwort` = Benutzerpasswort

Problem

Das Geheimnis enthält keine gültigen ONTAP-Anmeldeinformationen für die Dateisystemauthentifizierung.

Lösung: Geben Sie Anmeldeinformationen an, die FSx for ONTAP Dateisysteme im AWS Secrets Manager authentifizieren können.

Cache-Volumes in NetApp Workload Factory erkennen

Die Ermittlung und Anzeige von Cache Volumes, die mit Cache-Beziehungen verknüpft sind, ist möglich, ohne die NetApp Workload Factory Konsole zu verlassen. Cache-Beziehungen werden auch als ONTAP FlexCache Beziehungen bezeichnet. Workload Factory erkennt vorhandene Cache-Beziehungen mithilfe der FlexCache Technologie, der Remote-Caching-Funktion von NetApp ONTAP, die den Datenzugriff beschleunigt und WAN-Latenz, Bandbreite und Kosten für leseintensive Workloads reduziert, insbesondere wenn Clients wiederholt auf dieselben Daten zugreifen müssen.

["Weitere Informationen zur Datenreplikation mit FlexCache."](#)

Über diese Aufgabe

Die Link-Zuordnung ist erforderlich, um Cache-Beziehungen zu ermitteln.

Eine Cache-Beziehung kann zwischen Volumes auf zwei ONTAP Systemen bestehen, beispielsweise zwischen einem FSx for ONTAP Dateisystem und einem Cloud Volumes ONTAP System. Auch innerhalb eines einzelnen FSx for ONTAP Dateisystems kann eine Cache-Beziehung zwischen verschiedenen Volumes bestehen.

Bevor Sie beginnen

Vor Beginn sind folgende Punkte zu beachten.

- Sie müssen eine Verknüpfung herstellen, um Cache-Beziehungen in einem Dateisystem zu ermitteln. ["Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen"](#). Nach der Verknüpfung ist eine Rückkehr zu diesem Vorgang erforderlich.
- Es muss eine bestehende Cache-Beziehung vorliegen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** wird die Registerkarte **Cache relationships** ausgewählt.
4. Ihre Cache-Volumes sind in der Tabelle aufgeführt. Die Tabelle enthält folgende Informationen zu jedem Cache-Volume:
 - **Ursprungscluster**: Der Ursprungs- oder Quellcluster der FlexCache Beziehung.
 - **Ursprungs-Volume**: Das Ursprungs- oder Quell-Volume der FlexCache Beziehung.
 - **Ursprungs Storage VM**: Die Ursprungs- oder Quell-Storage VM des Volumes.
 - **Cache Volume**: Das Cache- oder Ziel-Volume der FlexCache Beziehung.
 - **Cache storage VM**: Die Cache- oder Ziel-Storage-VM des Volumes.
 - **Status**: Der Status der FlexCache Beziehung.
 - **Verfügbarer Storage im Cache**: Die Menge des verfügbaren Storage auf dem Cache Volume.
 - **Cache-Dateisystem**: Das Dateisystem des Cache-Volumes.
 - **Schreibmodi**: Der Schreibmodus der FlexCache Beziehung.
 - **DR Cache**: Gibt an, ob die FlexCache Beziehung ein Disaster-Recovery-Cache (DR-Cache) ist.

- **Exportrichtlinie:** Die Exportrichtlinie des Cache-Volumes.

Verwandte Informationen

["Verwalten von Cache Volumes"](#)

Zugriff auf Ihre FSx for ONTAP Dateisystemdaten

Sie können von Ihrem lokalen Netzwerk aus auf Ihre FSx for ONTAP Dateisysteme zugreifen, indem Sie Volumes für NAS-Clients und iSCSI-LUNs für SAN-Clients einbinden.

["Zugriff auf Daten"](#) Die Amazon FSx for NetApp ONTAP Dokumentation enthält Themen dazu, wie Sie auf Daten zugreifen können, als Referenz.

Der Mountpunkt für Volumes kann auch in NetApp Workload Factory abgerufen werden.

Abrufen des Mountpunkts für Volumes in NetApp Workload Factory

Der Mountpunkt eines Volumes wird benötigt, um eine Freigabe auf einer CIFS-Freigabe oder einem NFS-Client einzubinden.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Volumes explorer > FSx for ONTAP**.
3. Wählen Sie das Aktionsmenü für das Volume, dann **Grundlegende Aktionen** und anschließend **Einbindungsbefehl anzeigen**.
4. Im Dialogfeld „Mount-Befehl“ kann **Copy** ausgewählt werden, um den Befehl für den NFS-Mountpunkt oder die CIFS-Freigabe zu kopieren. Anschließend erfolgt die Eingabe des kopierten Befehls im Terminal.
5. **Schließen** auswählen.

Verbindung zu NAS-Clients herstellen

- ["Einbinden eines Volumes auf Linux-Clients"](#)
- ["Einbinden eines Volumes auf Windows Clients"](#)
- ["Einbinden eines Volumes auf macOS Clients"](#)

Verbindung zu SAN-Clients herstellen

- ["Einbinden einer iSCSI LUN auf Linux-Clients"](#)
- ["Einbinden einer iSCSI-LUN auf Windows-Clients"](#)

Schutz Ihrer Daten

Arten des Datenschutzes in NetApp Workload Factory

FSx für ONTAP unterstützt Snapshots, NetApp Autonomous Ransomware Protection with AI, Replikation und Backups für den Datenschutz. Wir empfehlen, eine Kombination von

Datenschutztypen zu verwenden, um auf das Unvermeidliche vorbereitet zu sein und Ihre Daten zu schützen.

Arten der Datensicherung

Der Schutz Ihrer Workloads trägt dazu bei, dass Sie sich jederzeit von Datenverlust erholen können. Vor der Auswahl der Funktionen, die Sie verwenden möchten, ist es hilfreich, die verschiedenen Arten des Datenschutzes zu kennen.

Snapshots

Ein Snapshot erstellt als Snapshot-Kopie ein schreibgeschütztes, zeitpunktgenaues Image eines Volumes innerhalb des Quellvolumes. Mithilfe dieser Snapshot-Kopie können Sie einzelne Dateien wiederherstellen oder den gesamten Inhalt eines Volumes wiederherstellen. Snapshots bilden die Grundlage aller Backup-Methoden. Die auf Ihrem Volume erstellte Snapshot-Kopie wird verwendet, um das replizierte Volume und die Backup-Datei mit den am Quellvolume vorgenommenen Änderungen zu synchronisieren.

NetApp Autonomous Ransomware Protection with AI

NetApp Autonomous Ransomware Protection with AI (ARP/AI) verwendet Workload-Analyse in NAS-Umgebungen (NFS/SMB), um anormale Aktivitäten zu erkennen und davor zu warnen, die auf einen Ransomware-Angriff hindeuten könnten. Bei Verdacht auf einen Angriff erstellt ARP/AI zusätzlich zu dem bestehenden Schutz durch geplante Snapshots neue, unveränderliche Snapshots.

Replication

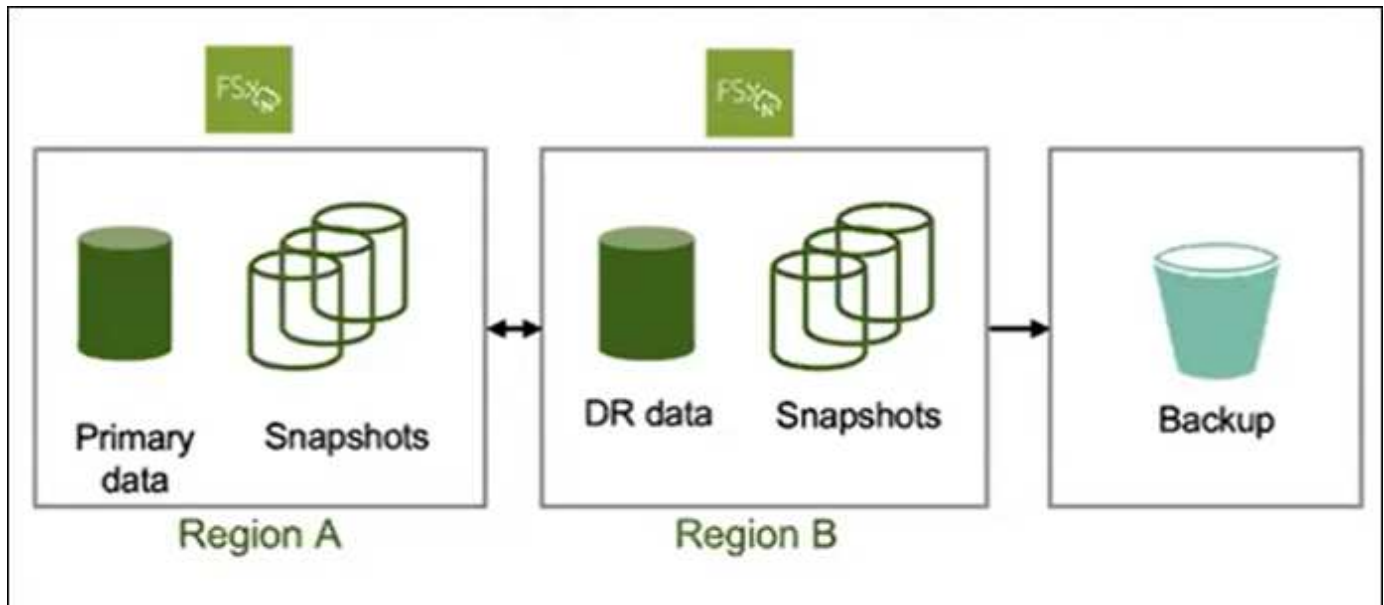
Die Replikation erstellt eine zweite Kopie Ihrer Daten auf einem anderen FSx for ONTAP Dateisystem und aktualisiert diese Kopie kontinuierlich. Ihre Daten bleiben somit stets aktuell und sind jederzeit verfügbar, beispielsweise für die Notfallwiederherstellung.

Sie können wahlweise sowohl replizierte Volumes auf einem anderen FSx for ONTAP Dateisystem als auch Backup-Dateien in der Cloud erstellen. Alternativ können Sie auch nur replizierte Volumes oder Backup-Dateien erstellen, es ist Ihre Wahl.

Backups

Sie können Sicherungen Ihrer Daten in der Cloud erstellen, um Schutz und langfristige Aufbewahrung zu gewährleisten. Bei Bedarf können Sie ein Volume, einen Ordner oder einzelne Dateien aus der Sicherung im selben oder in einem anderen Arbeitsdateisystem wiederherstellen.

Das folgende Diagramm veranschaulicht den Datenschutz für FSx for ONTAP Storage mithilfe von Snapshots, Replikation über Regionen hinweg und Backup in Objektspeicher.



Bewährte Verfahren zum Schutz Ihrer Workload-Daten

FSx for ONTAP bietet mehrere Datenschutzoptionen, die kombiniert werden können, um Ihre ausgewählten Wiederherstellungspunkt- und Wiederherstellungszeitziele zu erreichen. Für den bestmöglichen Schutz empfehlen wir, sowohl Volume-Snapshots als auch Volume-Backups zu verwenden.

Ein Wiederherstellungspunktziel (RPO) beschreibt, wie aktuell die letzte Kopie Ihrer Daten garantiert ist, was davon abhängt, wie häufig die Kopien erstellt werden. Ein Wiederherstellungszeitziel (RTO) definiert, wie lange die Wiederherstellung Ihrer Daten dauert.

Schutz Ihrer Workload-Daten mit Snapshots

Snapshots sind virtuelle zeitpunktgenaue Versionen eines Volume, die regelmäßig erstellt werden. Sie können mit Standard-Dateisystembefehlen auf Snapshots zugreifen. Snapshots bieten ein RPO von nur einer Stunde. Die RTO hängt von der Menge der wiederherzustellenden Daten ab und wird in erster Linie durch die Durchsatzbegrenzung des Volume begrenzt. Snapshots ermöglichen Benutzern außerdem die Wiederherstellung bestimmter Dateien und Verzeichnisse, was die RTO weiter verringert. Snapshots belegen nur zusätzlichen Volume-Speicherplatz für Änderungen, die am Volume vorgenommen werden.

Schutz Ihrer Workload-Daten mit NetApp Autonomous Ransomware Protection with AI

NetApp Autonomous Ransomware Protection with AI (ARP/AI) dient als wichtige zusätzliche Verteidigungsebene, falls die Antivirensoftware ein Eindringen nicht erkannt hat. Durch das Festlegen einer ARP/AI-Richtlinie wird die Funktion für alle Storage VMs sowie alle vorhandenen und neu erstellten Volumes aktiviert. Nach der Aktivierung erkennt und schützt ARP/AI alle Volumes und Storage VMs. Wenn eine Dateierweiterung als ungewöhnlich gekennzeichnet wird, ist eine Bewertung der Warnung erforderlich.

Der Schutz Ihrer Workload-Daten erfolgt mit Volume-Replikation

Die Volume-Replikation erstellt eine Kopie der neuesten Daten eines Volumes einschließlich aller seiner Snapshots in einer anderen Region. Falls mehrstündige RTOs für die vollständige Wiederherstellung eines Volumes aus einem Volume-Backup nicht vertretbar sind, sollte eine Volume-Replikation in Betracht gezogen werden. Die Volume-Replikation stellt zwar sicher, dass aktuelle Daten in einer anderen Region zur Nutzung verfügbar sind, jedoch müssen Ihre Clients so angepasst werden, dass sie das Volume in der anderen Region verwenden.

Der Schutz Ihrer Workload-Daten mit Backups

Volume Backups erstellen unabhängige zeitpunktgenaue Kopien Ihres Volumes. Sie dienen der Speicherung älterer Backups und stellen die notwendige zweite Datenkopie bereit. Tägliche, wöchentliche und monatliche Backup-Zeitpläne ermöglichen Recovery Point Objectives (RPOs) ab einem Tag. Volume Backups können nur als Ganzes wiederhergestellt werden. Die Erstellung eines Volumes aus einem Backup (RTO) kann je nach Backup-Größe Stunden bis mehrere Tage dauern.

Empfehlungen zum Schutz Ihrer Workloaddaten

Die folgenden Empfehlungen betreffen den Schutz Ihrer Workload-Daten.

- Für die Notfallwiederherstellung eignet sich die Volume-Replikation: Wenn Ihre Applikation eine niedrige RTO erfordert, empfiehlt sich die Verwendung der Volume-Replikation, um Ihre Daten in eine andere Region zu replizieren.
- Die Verwendung von Volume-Backups in Verbindung mit Snapshots stellt sicher, dass Sie Ihre Dateien aus Snapshots wiederherstellen und im Falle eines Volume-Verlusts mithilfe von Backups eine vollständige Wiederherstellung durchführen können.
- Eine Volume-Backup-Richtlinie sollte so festgelegt werden, dass sie die Anforderungen Ihres Unternehmens hinsichtlich Backup-Alter und -Häufigkeit erfüllt. Wir empfehlen, für jedes Volume mindestens zwei tägliche Backups aufzubewahren.
- Ein Snapshot-Zeitplan sollte festgelegt werden: Ältere Snapshots werden mit geringerer Wahrscheinlichkeit zur Wiederherstellung von Daten verwendet. Wir empfehlen, einen Snapshot-Zeitplan zu definieren, der den abnehmenden Nutzen der Aufbewahrung älterer Snapshots im Verhältnis zu den Kosten für zusätzliche Snapshot-Kapazität berücksichtigt.
- Die Aktivierung einer ARP/AI-Richtlinie für Ihr Dateisystem oder einzelne Volumes fügt eine zusätzliche Schutzebene hinzu, um Ihre Daten vor Ransomware-Angriffen zu schützen.

Snapshots bieten Schutz für Daten.

Snapshots bieten Schutz für Daten in NetApp Workload Factory

Schutz von Volume-Daten vor versehentlichem Löschen oder Beschädigung durch das Erstellen und Verwalten von Snapshots in NetApp Workload Factory. Es besteht die Möglichkeit, einen Snapshot eines Volumes nach Bedarf zu erstellen, eine Snapshot-Richtlinie zu definieren, um die Erstellung und Aufbewahrung von Snapshots für Storage-VMs zu automatisieren, sowie ein Volume aus einem vorhandenen Snapshot wiederherzustellen, um Daten zu einem bestimmten Zeitpunkt wiederherzustellen.

Einen On-Demand-Snapshot eines Volumes erstellen

Erstellen eines manuellen Snapshots eines FSx for ONTAP-Volumes in NetApp Workload Factory. Snapshots sind zeitpunktgenaue Versionen des Inhalts Ihres Volumes.

Snapshots sind Ressourcen von Volumes und stellen Momentaufnahmen Ihrer Daten dar, die nur Speicherplatz für geänderte Daten belegen. Da sich Daten im Laufe der Zeit ändern, benötigen Snapshots mit zunehmendem Alter in der Regel mehr Speicherplatz.

FSx for ONTAP Volumes verwenden Just-in-Time Copy-on-Write, sodass unveränderte Dateien in Snapshots keine Kapazität des Volumes belegen.



Snapshots sind keine Kopien Ihrer Daten. Wenn Sie Kopien Ihrer Daten erstellen möchten, sollten Sie die Funktionen für Volume-Backups oder Volume-Replikation verwenden.

Bevor Sie beginnen

Sie müssen eine Verknüpfung herstellen, um einen manuellen Snapshot eines Volumes zu erstellen. ["Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen"](#). Nach der Verknüpfung ist eine Rückkehr zu diesem Vorgang erforderlich.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** können Sie im Aktionsmenü des Dateisystems, das das Volume enthält, für das ein Snapshot erstellt werden soll, **Manage** auswählen.
4. In der Dateisystemübersicht erfolgt die Auswahl der Registerkarte **Volumes**.
5. Auf der Registerkarte **Volumes** wird das Aktionsmenü für das Volume ausgewählt, das mit Snapshots geschützt werden soll.
6. Die Auswahl erfolgt über **Datenschutzmaßnahmen** und anschließend **Snapshots verwalten**.
7. Auf der Seite „Snapshots verwalten“ erfolgt die Auswahl der Option **Snapshot erstellen**.
8. Im Dialogfeld „Snapshot erstellen“ erfolgen die folgenden Schritte:
 - a. Die Eingabe eines Snapshot-Namens erfolgt im Feld **Snapshot name**.
 - b. Optional ist die Auswahl einer Bezeichnung oder das Erstellen einer neuen Bezeichnung möglich.
 - c. Die **Aufbewahrungsfrist** ist als Anzahl von Stunden, Tagen, Monaten oder Jahren anzugeben.
 - d. Optional: **Diesen Snapshot unveränderlich machen**, damit der Snapshot während des Aufbewahrungszeitraums nicht gelöscht werden kann.

Die Aussage zu unveränderlichen Snapshots akzeptieren.

9. **Erstellen** auswählen.

Erstellen einer Snapshot-Richtlinie für Storage-VMs

Mit Workload Factory lässt sich eine benutzerdefinierte Snapshot-Richtlinie für Storage VMs erstellen, um die Erstellung und Aufbewahrung von Snapshots zu managen. Eine Snapshot-Richtlinie definiert, wie das System Snapshots für eine Storage VM erstellt. Sie können eine Snapshot-Richtlinie für eine Storage VM in einem FSx for ONTAP Dateisystem erstellen. Die Richtlinie kann auch für mehrere Storage VMs freigegeben werden.

Sie können eine benutzerdefinierte Snapshot-Richtlinie erstellen, die sich von den drei integrierten Snapshot-Richtlinien für FSx for ONTAP unterscheidet:

- default
- default-1weekly
- none

Standardmäßig ist jedes Volume der `default` Snapshot-Richtlinie des Dateisystems zugeordnet. Wir empfehlen, diese Richtlinie für die meisten Workloads zu verwenden.

Durch die Anpassung einer Richtlinie können Sie festlegen, wann Snapshots erstellt werden, wie viele Kopien aufbewahrt werden und wie sie benannt werden.

Bevor Sie beginnen

- Sobald eine Snapshot-Richtlinie erstellt wurde, kann ihre Zuordnung zu den Storage VM(s) nicht mehr geändert werden, die Richtlinie kann jedoch jederzeit zu Volumes hinzugefügt oder von diesen entfernt werden.
- Vor der Verwendung von Snapshots sind folgende Aspekte bezüglich der Snapshot-Kapazität zu berücksichtigen:
 - Für die meisten Datensätze reichen zusätzliche 20 % Kapazität aus, um Snapshots bis zu vier Wochen lang aufzubewahren. Mit zunehmendem Alter der Daten sinkt die Wahrscheinlichkeit ihrer Verwendung für Wiederherstellungen.
 - Das Überschreiben aller Daten in einem Snapshot verbraucht erhebliche Volume-Kapazität, was bei der Provisionierung der Volume-Kapazität berücksichtigt werden muss.
- Um eine benutzerdefinierte Snapshot-Richtlinie zu erstellen, muss eine Verknüpfung hergestellt werden. ["Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen"](#). Nach der Verknüpfung ist eine Rückkehr zu diesem Vorgang erforderlich.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2.  Im Menü ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** erfolgt die Auswahl von **Manage** über das Aktionsmenü des Dateisystems mit dem Volume.
4. In der Dateisystemübersicht erfolgt die Auswahl der Registerkarte **Storage VMs**.
5. Auf der Registerkarte **Speicher-VMs** befindet sich im Aktionsmenü für das Volume, das durch geplante Snapshots geschützt werden soll, unter **Erweiterte Aktionen** die Option **Snapshot-Richtlinien verwalten**.
6. Auf der Seite „Snapshot-Richtlinienverwaltung“ erfolgt die Auswahl von **Snapshot-Richtlinie erstellen**.
7. Im Feld **Name der Snapshot-Richtlinie** wird ein Name für die Snapshot-Richtlinie angegeben.
8. Optional können Sie eine Beschreibung für die Snapshot-Richtlinie eingeben.
9. Unter **Richtlinienzeitplan und Kopien** lässt sich festlegen, wann Snapshots erstellt werden. Zum Beispiel jede Minute oder stündlich.

Sie können mehrere Frequenzen auswählen.
10. Unter **Anzahl der Kopien** wird die Anzahl der zu behaltenden Kopien angegeben.

Die maximale Anzahl an Kopien beträgt 1.023.
11. Optional: Unter **Namenskonvention** lässt sich ein **Präfix** für die Richtlinie eingeben.
12. Das **Aufbewahrungsetikett** wird automatisch ausgefüllt.

Diese Bezeichnung bezieht sich auf die SnapMirror-Replikationsbezeichnung, die verwendet wird, um nur bestimmte Snapshots für die Replikation vom Quell- zum Zieldateisystem auszuwählen.
13. Optional ist es möglich, für alle benötigten Zeitpläne **Unveränderliche Snapshots** zu aktivieren, die **Aufbewahrungsdauer** für jeden Zeitplan festzulegen und die Erklärung zu akzeptieren, um fortzufahren.

Die Aktivierung unveränderlicher Snapshots sperrt alle Snapshots in dieser Snapshot-Richtlinie, damit sie

während des Aufbewahrungszeitraums nicht gelöscht werden können.

14. **Über Storage VMs hinweg teilen:** Standardmäßig aktiviert. Wenn diese Option aktiviert ist, wird die Snapshot-Richtlinie von allen Storage VMs im Dateisystem gemeinsam verwendet. Bei Deaktivierung wird eine Snapshot-Richtlinie für eine einzelne Storage VM erstellt.
15. **Erstellen** auswählen.

Wiederherstellung eines Volumes aus einem Snapshot

Sie können Daten aus einem Snapshot auf ein vorhandenes Volume oder auf ein neues Volume wiederherstellen. Die Wiederherstellung ermöglicht eine zeitpunktgenaue Wiederherstellung, wenn ein Volume gelöschte oder beschädigte Dateien enthält.

Die Erstellung eines neuen Volumes aus einem Snapshot erzeugt innerhalb weniger Sekunden eine Kopie des gesamten Volumes, unabhängig von dessen Größe. Die neu erstellte Kopie stellt ein neues Volume dar.

Bevor Sie beginnen

Vor dem Erstellen eines Volumes aus einem Snapshot sind die folgenden Einschränkungen zu berücksichtigen:

- Ein Volume kann nur dann aus einem Snapshot wiederhergestellt werden, wenn bereits eine Snapshot-Kopie des Volumes vorhanden ist.
- Änderungen an Berechtigungsmodellen: Wenn Sie mit diesem Vorgang den NAS-Protokolltyp wechseln, kann dadurch auch das Berechtigungsmodell geändert werden, das der Sicherheitsstil bereitstellt. Es können Probleme mit Dateizugriffsberechtigungen auftreten, die sich nur manuell mit Administratorzugriff mithilfe der NAS-Client-Tools für Berechtigungseinstellungen beheben lassen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** erfolgt die Auswahl von **Manage** über das Aktionsmenü des Dateisystems mit dem Volume.
4. In der Dateisystemübersicht erfolgt die Auswahl der Registerkarte **Volumes**.
5. Auf der Registerkarte **Volumes** erfolgt die Auswahl des Aktionsmenüs für das Volume, das aus einem Snapshot wiederhergestellt werden soll.
6. Die Auswahl erfolgt über **Datenschutzmaßnahmen** und anschließend **Snapshots verwalten**.
7. Auf der Seite „Snapshots verwalten“ kann im Aktionsmenü der wiederherzustellende Snapshot und anschließend **Wiederherstellen** ausgewählt werden.
8. Im Dialogfeld „Volume aus einem Snapshot wiederherstellen“ können Sie aus den folgenden Optionen auswählen:

- Auswahl der Option **Als neues Volume wiederherstellen**.

Im Feld **Name des wiederhergestellten Volumes** ist ein eindeutiger Name für das wiederherzustellende Volume einzugeben.

- Wiederherstellung von Daten aus einem Snapshot in ein vorhandenes Volume. Dieser Vorgang löscht endgültig alle Daten, die nach dem Erstellungszeitpunkt des Snapshots geändert wurden.

Zum Fortfahren ist die Annahme der Erklärung erforderlich.

9. Wiederherstellen auswählen.

Verwalten von Snapshot-Richtlinien für Volumes in NetApp Workload Factory

Die Verwaltung von Snapshot-Richtlinien für FSx for ONTAP Volumes in Workload Factory. Eine Snapshot-Richtlinie definiert, wie das System Snapshots für ein Volume erstellt.

Snapshot-Verwaltungsvorgänge wie das Zuweisen, Ändern und Löschen von Snapshot-Richtlinien für Volumes in einem FSx for ONTAP Dateisystem werden auf der Ebene der Storage VM verwaltet. Snapshot-Richtlinien können von einer einzelnen Storage VM oder von allen Storage VMs gemeinsam genutzt werden.

Für einige Verwaltungsaufgaben ist es erforderlich, eine Verknüpfung mit dem FSx for ONTAP Dateisystem herzustellen. ["Informationen zu Workload Factory Links"](#).

Standardmäßig ist jedes Volume der `default` Snapshot-Richtlinie des Dateisystems zugeordnet. Wir empfehlen, diese Richtlinie für die meisten Workloads zu verwenden.

Zuweisung einer Snapshot-Richtlinie zu einem Volume

Sie können einem einzelnen Volume eine Snapshot-Richtlinie zuweisen, um geplante Snapshots für das Volume zu erstellen.

Bevor Sie beginnen

Sie müssen einen Link verknüpfen, um eine Snapshot-Richtlinie zuzuweisen. ["Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen"](#). Nach der Verknüpfung ist eine Rückkehr zu diesem Vorgang erforderlich.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Storage**.
3. Im Menü „Storage“ erfolgt die Auswahl von **Inventory**.
4. Im Aktionsmenü des Dateisystems, das das Volume enthält, dem Sie eine Snapshot-Richtlinie zuweisen möchten, ist **Manage** auszuwählen.
5. In der Dateisystemübersicht erfolgt die Auswahl der Registerkarte **Storage VMs**.
6. Auf der Registerkarte **Speicher-VMs** wird im Aktionsmenü der Storage VM, die das mit geplanten Snapshots zu schützende Volume enthält, **Erweiterte Aktionen** und anschließend **Snapshot-Richtlinien verwalten** ausgewählt.
7. Auf der Seite „Snapshot-Richtlinienverwaltung“ erfolgt die Auswahl von **Richtlinie dem Volume zuweisen** über das Aktionsmenü der Snapshot-Richtlinie.
8. Im Dialogfeld „Snapshot-Richtlinie zuweisen“ erfolgt die Auswahl einer Snapshot-Richtlinie für das Volume sowie die Überprüfung des Richtlinienzeitplans.

Wenn die Richtlinie unveränderliche Snapshots enthält und Sie sie verwenden möchten, müssen Sie die Erklärung akzeptieren.

9. **Assign** ist auszuwählen.

Ergebnis

Die Snapshot-Richtlinie ist dem Volume zugewiesen.

Ändern einer Snapshot-Richtlinie

Sie können den Namen, den Zeitplan und die Anzahl der aufzubewahrenden Kopien der Snapshot-Richtlinie ändern sowie unveränderliche Snapshots aktivieren oder deaktivieren. Die gemeinsame Nutzung von Richtlinien über Storage VMs hinweg kann nicht aktiviert oder deaktiviert werden. Diese Option ist nur bei der Erstellung der Snapshot-Richtlinie verfügbar.

Bevor Sie beginnen

Um vorhandene Snapshot-Richtlinien anzuzeigen, muss ein Link zugeordnet werden. ["Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen"](#). Nach der Verknüpfung ist eine Rückkehr zu diesem Vorgang erforderlich.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Storage**.
3. Im Menü „Storage“ erfolgt die Auswahl von **Inventory**.
4. Im Dateisystem erfolgt die Auswahl des Aktionsmenüs und anschließend von **Verwalten**.
5. In der Dateisystemübersicht erfolgt die Auswahl der Registerkarte **Storage VMs**.
6. Auf der Registerkarte **Speicher-VMs** wird im Aktionsmenü der Storage VM, die das mit geplanten Snapshots zu schützende Volume enthält, **Erweiterte Aktionen** und anschließend **Snapshot-Richtlinien verwalten** ausgewählt.
7. Auf der Seite zur Snapshot-Richtlinienverwaltung ist im Menü „Aktionen“ für die zu ändernde Snapshot-Richtlinie **Bearbeiten** auszuwählen.
8. Im Dialogfeld „Snapshot-Richtlinie bearbeiten“ können die erforderlichen Änderungen an der Snapshot-Richtlinie vorgenommen werden.
9. **Anwenden** auswählen.

Ergebnis

Die Snapshot-Richtlinie wurde aktualisiert.

Aktivierung unveränderlicher Snapshots

Snapshots sperren, damit sie während der Aufbewahrungsfrist nicht gelöscht werden.

Bevor Sie beginnen

Sie müssen eine Verknüpfung herstellen, um unveränderliche Snapshots zu aktivieren. ["Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen"](#). Nach der Verknüpfung ist eine Rückkehr zu diesem Vorgang erforderlich.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Volumes explorer**.
3. Die Auswahl erfolgt im Aktionsmenü des Volumes, für das Snapshots gesperrt werden sollen.
4. Die Auswahl erfolgt über **Datenschutzaktionen, Snapshots** und anschließend **Snapshot unveränderlich machen**.

5. Im Dialogfeld „Snapshot unveränderlich erstellen“ erfolgt Folgendes:
 - a. **Snapshot-Name**: Auswahl des zu sperrenden Snapshots.
 - b. Die **Aufbewahrungsfrist** wird in Stunden, Tagen, Monaten oder Jahren festgelegt.
 - c. Die Aussage akzeptieren.
6. **Anwenden** auswählen.

Ergebnis

Der Volume Snapshot ist nun gesperrt.

Langfristige Snapshot-Aufbewahrung in NetApp Workload Factory aktivieren

In NetApp Workload Factory können Sie Snapshots zur Langzeitaufbewahrung aktivieren, wodurch Sie bestimmte Snapshots für die langfristige Notfallwiederherstellung replizieren können.

Die Langzeitaufbewahrung ermöglicht den Weiterbetrieb von Geschäftsservices auch im Falle eines vollständigen Standortausfalls und unterstützt das transparente Failover von Anwendungen mithilfe einer sekundären Kopie.

Die gleichen Schritte gelten auch für das Aktivieren und Bearbeiten von Snapshots zur Langzeitaufbewahrung.

Wenn ein lokaler ONTAP Cluster das Ziel der Replikationsbeziehung ist, wird das Ändern von Snapshots für die Langzeitaufbewahrung nicht unterstützt.



Die Bearbeitung der Langzeitaufbewahrung ist beim Replizieren von Storage-VM-Daten und Konfigurationseinstellungen nicht möglich.

Schritte

1. Melden Sie sich bei der **"NetApp Console"** an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Im Menü **FSx for ONTAP** wählen Sie zunächst **Inventory** und anschließend im Aktionsmenü des zu aktualisierenden Dateisystems **Manage** aus.
4. Wählen Sie in der Dateisystemübersicht die Registerkarte **Replikationsbeziehungen** aus.
5. Auf der Registerkarte „Replikationsbeziehungen“ können Sie das Aktionsmenü des Zeitplans der Replikationsbeziehung auswählen, der geändert werden soll.
6. Die Option **Langzeitspeicherung bearbeiten** auswählen.
7. Im Dialogfeld „Langzeitaufbewahrung bearbeiten“ können Sie Snapshots für die Langzeitaufbewahrung aktivieren oder deaktivieren.
8. Wenn Sie Snapshots für die langfristige Aufbewahrung deaktivieren, wird dieser Vorgang durch Auswahl von **Apply** abgeschlossen.
9. Wenn Sie Snapshots für die Langzeitaufbewahrung aktivieren, können Sie entweder eine bestehende Richtlinie auswählen oder eine neue Richtlinie erstellen.
 - a. Zur Verwendung einer bestehenden Richtlinie erfolgt die Auswahl im Dropdown-Menü.
 - b. Für die Erstellung einer neuen Richtlinie sind folgende Angaben erforderlich:
 - i. **Richtliniename**: Geben Sie einen Richtliniennamen ein.
 - ii. **Snapshot-Richtlinien**: Auswahl einer oder mehrerer Snapshot-Richtlinien.

- iii. **Zu behaltende Kopien:** Anzahl der Snapshot-Kopien, die auf dem Zielsystem beibehalten werden sollen.

10. **Anwenden** auswählen.

Eine Snapshot-Richtlinie von einem Volume entfernen

Eine Snapshot-Richtlinie kann von einem Volume entfernt werden, wenn keine Snapshots des Volumes mehr benötigt werden oder wenn eine Snapshot-Richtlinie gelöscht werden soll, die mehreren Volumes zugewiesen ist. Um [eine Snapshot-Richtlinie löschen](#), muss eine solche Richtlinie, die mehr als einem Volume zugewiesen ist, manuell aus allen Volumes entfernt werden.

Bevor Sie beginnen

Sie müssen einen Link verknüpfen, um eine Snapshot-Richtlinie zu entfernen. "[Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen](#)". Nach der Verknüpfung ist eine Rückkehr zu diesem Vorgang erforderlich.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Im Menü **FSx for ONTAP** wählen Sie zunächst **Inventory** und anschließend im Aktionsmenü des zu aktualisierenden Dateisystems **Manage** aus.
4. In der Dateisystemübersicht erfolgt die Auswahl der Registerkarte **Storage VMs**.
5. Auf der Registerkarte **Speicher-VMs** wird im Aktionsmenü der Storage VM, die das mit geplanten Snapshots zu schützende Volume enthält, **Erweiterte Aktionen** und anschließend **Snapshot-Richtlinien verwalten** ausgewählt.
6. Auf der Seite „Snapshot-Richtlinienverwaltung“ erfolgt die Auswahl von **Richtlinie dem Volume zuweisen** über das Aktionsmenü der Snapshot-Richtlinie.
7. Im Dialogfeld „Snapshot-Richtlinie zuweisen“ entfernt die Auswahl von **Keine** die Snapshot-Richtlinie.
8. **Assign** ist auszuwählen.

Ergebnis

Das Volume hat keine Snapshot-Richtlinie mehr.

Löschen einer Snapshot-Richtlinie

Eine Snapshot-Richtlinie kann gelöscht werden, wenn sie nicht mehr benötigt wird.

Wenn eine Snapshot-Richtlinie mehreren Volumes zugewiesen ist, müssen Sie manuell [es entfernen](#) von allen Volumes löschen, um die Snapshot-Richtlinie zu löschen. Alternativ können Sie [eine andere Snapshot-Richtlinie zuweisen](#) für die Volumes tun.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Im Menü **FSx for ONTAP** wählen Sie zunächst **Inventory** und anschließend im Aktionsmenü des zu aktualisierenden Dateisystems **Manage** aus.
4. In der Dateisystemübersicht erfolgt die Auswahl der Registerkarte **Storage VMs**.

5. Die Auswahl erfolgt auf der Registerkarte **Storage VMs** im Aktionsmenü der Storage VM mit der zu löschenden Snapshot-Richtlinie: zuerst **Advanced actions**, dann **Manage snapshot policies**.
6. Auf der Seite für die Snapshot-Richtlinienverwaltung erfolgt das Löschen über das Aktionsmenü der entsprechenden Snapshot-Richtlinie durch Auswahl von **Löschen**.
7. Im Dialogfeld „Löschen“ erfolgt das Löschen der Richtlinie über **Löschen**.

Snapshots eines FSx for ONTAP Volume managen

Das Bearbeiten der Snapshot-Einstellungen, das Aktivieren des Verzeichniszugriffs und das Löschen von Snapshots dienen dazu, Ihre Snapshots und den Datenschutz in Workload Factory zu managen.

Eine Momentaufnahme bearbeiten

Sie können den Namen, die Bezeichnung und die Aufbewahrungsdauer eines Snapshots bearbeiten. Falls der Snapshot noch nicht unveränderlich ist, können Sie ihn unveränderlich machen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Volumes explorer**.
3. Wählen Sie das Aktionsmenü für das Volume mit dem Snapshot aus, das bearbeitet werden soll.
4. Die Auswahl erfolgt über **Datenschutzmaßnahmen** und anschließend **Snapshots verwalten**.
5. Auf der Seite „Snapshots verwalten“ steht im Aktionsmenü des zu bearbeitenden Snapshots die Option **Bearbeiten** zur Verfügung.
6. Im Dialogfeld „Snapshot bearbeiten“ können Sie Folgendes bearbeiten:
 - a. Den Namen ändern.
 - b. Die Bezeichnung ändern.
 - c. Die Aufbewahrungsfrist ändern.
 - d. Optional: **Diesen Snapshot unveränderlich machen**, damit der Snapshot während des Aufbewahrungszeitraums nicht gelöscht werden kann.

Wenn der Snapshot bereits unveränderlich ist, können Sie diese Einstellung nicht bearbeiten.

Die Aussage zu unveränderlichen Snapshots akzeptieren.

7. **Anwenden** auswählen.

Zugriff auf eine Momentaufnahme

Durch Aktivieren des Zugriffs auf das Snapshot-Verzeichnis erhalten Benutzer die Möglichkeit, selbstständig auf Snapshots zuzugreifen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Volumes explorer**.

3. Wählen Sie das Aktionsmenü für das Volume mit dem Snapshot aus, auf das zugegriffen werden soll.
4. Die Auswahl erfolgt über **Datenschutzmaßnahmen** und anschließend **Snapshots verwalten**.
5. Auf der Seite „Manage snapshots“ lässt sich im Aktionsmenü des gewünschten Snapshots **Access** auswählen.
6. Im Dialogfeld „Snapshot-Zugriff“ ermöglicht die Auswahl von **Zugriff auf das Snapshot-Verzeichnis aktivieren** den Zugriff auf diesen Volume-Snapshot und alle Snapshots des Volumes.
 - Für NFS Volumes: Unter **NFS access path** ist der NFS-Pfad für den Snapshot zu sehen.
 - Für SMB/CIFS Volumes: Unter **SMB access path** ist der SMB-Pfad für den Snapshot zu sehen.
7. Den Zugriffspfad kopieren.
8. **Anwenden** auswählen.

Daten aus einem Snapshot wiederherstellen

Sie haben die Möglichkeit, Daten aus einem Snapshot in ein vorhandenes Volume oder in ein neues Volume wiederherzustellen.

["Wiederherstellung eines Volumes aus einem Snapshot"](#)

Einen Snapshot löschen

Durch das Löschen eines Snapshot wird Speicherplatz frei.

Unveränderliche Snapshots können erst nach Ablauf der Aufbewahrungsfrist gelöscht werden.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Volumes explorer**.
3. Wählen Sie das Aktionsmenü für das Volume mit dem zu löschenden Snapshot aus.
4. Die Auswahl erfolgt über **Datenschutzmaßnahmen** und anschließend **Snapshots verwalten**.
5. Auf der Seite „Snapshots verwalten“ erfolgt die Auswahl von **Löschen** im Aktionsmenü des zu löschenden Snapshots.
6. Im Dialogfeld „Snapshot löschen“ ist „delete“ einzugeben.
7. **Löschen** auswählen, um den Löschvorgang zu bestätigen.

Verwandte Informationen

- ["Erstellen Sie einen Snapshot"](#)
- ["Erstellen einer Snapshot-Richtlinie"](#)
- ["Wiederherstellung eines Volumes aus einem Snapshot"](#)

Backups bieten Schutz für Daten in der NetApp Workload Factory

Schutz der Volume-Daten vor versehentlichem Löschen, Beschädigung und anderen Datenverlusten durch das Erstellen und Wiederherstellen von Backups in der NetApp Workload Factory. Es besteht die Möglichkeit, einen Backup-Zeitplan einzurichten, ein bedarfsgesteuertes Backup eines Volumes außerhalb der regulären Backups zu erstellen

und ein Volume aus einem vorhandenen Backup auf jedes FSx for ONTAP Dateisystem im eigenen AWS-Konto wiederherzustellen.

Eine bedarfsgesteuerte Sicherung eines Volumes erstellen

Erstellung einer manuellen Sicherung eines Volumes außerhalb der regelmäßig geplanten Sicherungen in NetApp Workload Factory.

Über diese Aufgabe

Volume-Backups werden pro Volume erstellt, sodass jedes Backup nur die Daten in einem bestimmten Volume enthält.

Volume-Backups sind inkrementell, was bedeutet, dass nur die Daten auf dem Volume gespeichert werden, die sich nach Ihrem letzten Backup geändert haben. Dadurch werden die für die Erstellung des Backups benötigte Zeit und der für das Backup benötigte Speicherplatz minimiert, was Speicherkosten spart, da keine Daten dupliziert werden.

Bevor Sie beginnen

Um Backups Ihrer Volumes zu erstellen, müssen sowohl Ihr Volume als auch Ihr Dateisystem über ausreichend verfügbare SSD Storage Kapazität verfügen, um den Backup-Snapshot zu speichern. Beim Erstellen eines Backup-Snapshots darf die zusätzlich vom Snapshot belegte Storage-Kapazität nicht dazu führen, dass die SSD Storage Auslastung des Volumes 98 % überschreitet. In diesem Fall schlägt das Backup fehl.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Volumes explorer**.
3. Wählen Sie das Aktionsmenü für das zu sichernde Volume aus.
4. Wählen Sie **Datenschutzmaßnahmen, Volume-Backups** und anschließend **manuelle Sicherung**.
5. Im Dialogfeld „Manuelle Datensicherung“ wird ein Name für das Backup eingegeben.
6. Die Option **Sichern** wird ausgewählt.

Verwaltung des Sicherungsplans für ein FSx for ONTAP Dateisystem

Backup-Zeitplan für ein FSx for ONTAP Dateisystem in NetApp Workload Factory managen.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** erfolgt die Auswahl von **Manage** im Aktionsmenü des Dateisystems, für das der Sicherungszeitplan aktualisiert werden soll.
4. Wählen Sie unter Information das Stiftsymbol neben **Volume backups** aus. Das Stiftsymbol erscheint neben dem Dropdown-Pfeil, wenn der Mauszeiger über die Zeile **Volume backups** bewegt wird.
5. Geben Sie im Dialogfeld **Volume backups** Folgendes an:
 - a. **Tägliche automatische Backups:** Hier kann die Funktion aktiviert oder deaktiviert werden. Wird die Funktion deaktiviert, ist **Anwenden** auszuwählen. Wird die Funktion aktiviert, sind die folgenden Schritte auszuführen.

- b. **Aufbewahrungsdauer für automatische Backups:** Geben Sie die Anzahl der Tage an, für die automatische Backups aufbewahrt werden sollen.
- c. **Tägliches automatisches Sicherungsfenster:** Zur Auswahl stehen entweder **Keine Präferenz** (eine tägliche Sicherungsstartzeit wird für Sie ausgewählt) oder **Startzeit für tägliche Sicherungen auswählen**; anschließend ist eine Startzeit anzugeben.
- d. **Wöchentliches Wartungsfenster:** Zur Auswahl stehen entweder **Keine Präferenz** (eine Startzeit für das wöchentliche Wartungsfenster wird für Sie ausgewählt) oder **Startzeit für 30-minütiges wöchentliches Wartungsfenster**; zusätzlich ist eine Startzeit anzugeben.

6. **Anwenden** auswählen.

Wiederherstellung eines Volumes aus einem Backup in NetApp Workload Factory

In NetApp Workload Factory können Sie ein Volume aus einer Sicherung in einem beliebigen FSx for ONTAP Dateisystem in Ihrem AWS-Konto wiederherstellen.

Workload Factory ermittelt, ob Sie über ausreichend Kapazität für die Wiederherstellung verfügen und kann automatisch SSD Storage-Tier-Kapazität hinzufügen, wenn dies nicht der Fall ist.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Volumes explorer**.
3. Wählen Sie das Aktionsmenü für das Volume aus, das aus einer Sicherung wiederhergestellt werden soll.
4. Wählen Sie **Data protection actions**, **Volume backups** und anschließend **Restore from a backup**.
5. Im Dialogfeld „Aus einer Sicherung wiederherstellen“ sind folgende Angaben erforderlich:
 - a. **Zieldateisystem:** Auswahl des Zieldateisystems aus dem Dropdown-Menü.
 - b. **Ziel Storage VM:** Auswahl der Ziel Storage VM aus dem Dropdown-Menü.
 - c. **Sicherungsname:** Auswahl des Sicherungsnamens aus dem Dropdown-Menü.
 - d. **Name des wiederhergestellten Volume:** Eingabe des Namens des wiederhergestellten Volume.
6. Die Dateisystemkapazität für den Wiederherstellungsvorgang ist zu überprüfen.

Bei begrenzter Dateisystemkapazität können folgende Probleme auftreten:

- Die Wiederherstellung kann die belegte Kapazität über den von Ihnen festgelegten Schwellenwert hinaus erhöhen. Die Wiederherstellung kann abgeschlossen werden. Es kann in Betracht gezogen werden, ["Manuelles Hinzufügen von SSD Storage-Tier-Kapazität"](#) oder Workload Factory so auszuwählen, dass automatisch SSD-Storage-Tier-Kapazität hinzugefügt wird.
- Für die Wiederherstellung wird zusätzliche SSD-Kapazität benötigt. Um fortzufahren, müssen Sie auswählen, dass Workload Factory automatisch SSD Storage-Tier-Kapazität hinzufügt.

7. **Wiederherstellen** auswählen.

Replikation zum Schutz von Daten verwenden

Daten zu FSx für ONTAP in NetApp Workload Factory replizieren

Daten in NetApp Workload Factory werden repliziert, um gegen Datenverlust zu schützen, falls in der Region, in der sich Ihre Daten befinden, eine Katastrophe eintritt.

Die Datenreplikation wird zwischen FSx for ONTAP Dateisystemen und lokalen ONTAP Systemen oder Cloud Volumes ONTAP unterstützt. Workload Factory unterstützt außerdem kaskadierende Replikation, um den Datenschutz auf tertiäre Systeme auszuweiten oder Ihre Daten zu migrieren.

Beim Replizieren von Speicher-VM-Daten und Konfigurationseinstellungen müssen Sie zuerst die Replikationsbeziehung erstellen und initialisieren und dann mindestens einmal warten, bis die Daten synchronisiert sind, bevor Sie den Umstellungsvorgang abschließen können.

Standardreplikation

Die Replikation schützt Ihre Daten, wenn eine Katastrophe Ihre Region betrifft; sie kann auch für Migrationszwecke verwendet werden.

Die Replikation umfasst das Erstellen und Initialisieren einer Replikationsbeziehung. Um die Replikation einzurichten, erstellen Sie die Replikationsbeziehung. Um die Daten zwischen Quell- und Zielspeichersystemen zu übertragen, initialisieren Sie die Replikationsbeziehung. Bei der Migration von Speicher-VM-Daten und Konfigurationseinstellungen müssen Sie außerdem den Cutover-Vorgang abschließen.

Replizierte Volumes im Zieldateisystem sind Data Protection (DP) Volumes und folgen dem Namensformat: {OriginalVolumeName}_copy.

Wenn Sie ein Quellvolume mit unveränderlichen Dateien replizieren, bleiben das Ziel-Volume und das Dateisystem gesperrt, bis die Aufbewahrungsfrist des Quellvolumes abgelaufen ist. Die Funktion für unveränderliche Dateien ist verfügbar, wenn Sie ["ein Volume erstellen"](#) für ein FSx for ONTAP-Dateisystem verwenden.



Sie können ein Quellvolume (lesen/schreiben) oder ein Datensicherungsvolume (DP) replizieren. Kaskadierende Replikation wird unterstützt, aber ein dritter Hop wird nicht unterstützt. Weitere Informationen zu ["kaskadierende Replikation"](#).

Migrationsanwendungsfälle

Für die Migration können Sie die Daten und Konfigurationseinstellungen einer Storage-VM replizieren. Wenn Sie Daten und Konfigurationseinstellungen gemeinsam migrieren, stellen Sie sicher, dass die letzte Replikation des Volumes innerhalb der letzten 24 Stunden abgeschlossen wurde. Sie müssen alle Volumes in derselben Storage-VM auswählen, um diese Funktion zu nutzen. Die Tiering-Richtlinie für alle Volumes entspricht standardmäßig der Tiering-Richtlinie des Quell-Volumes, was für Migrationsanwendungsfälle empfohlen wird.

Workload Factory unterstützt die Migrationsreplikation für Speicher-VMs zwischen den folgenden Speichersystemen.

- On-premises ONTAP Systeme und FSx für ONTAP Dateisysteme
- Cloud Volumes ONTAP und FSx für ONTAP Dateisysteme
- FSx für ONTAP und FSx für ONTAP file systems
 - Erste zu erster Generation
 - Sekunde zu zweiter Generation

Für die Migration der Speicher-VM-Daten und Konfigurationseinstellungen müssen drei Vorgänge durchgeführt werden.

1. [Replikationsbeziehung erstellen](#), wählen Sie **Migration** als Anwendungsfall und wählen Sie **Speicher-VM-Konfiguration replizieren** aus.
2. [Initialisiere die Replikationsbeziehung](#) um die Daten vom Quell- zum Zielspeichersystem zu übertragen.
3. [Umstellung der Replikation für Migrationsanwendungsfälle](#) um Daten und Konfigurationseinstellungen dauerhaft vom Quelldateisystem auf das Ziel-FSx for ONTAP-Dateisystem zu migrieren.

Schritt 1: Replikationsbeziehung erstellen

Replizieren Sie Daten zwischen zwei FSx for ONTAP-Dateisystemen, zwischen einem lokalen ONTAP-System und einem FSx for ONTAP-Dateisystem oder zwischen Cloud Volumes ONTAP und einem FSx for ONTAP-Dateisystem.

Bevor Sie beginnen

Überprüfen Sie diese Anforderungen, bevor Sie beginnen.

- Stellen Sie sicher, dass ein FSx for ONTAP-Dateisystem für das Ziel in der Replikationsbeziehung zur Verfügung steht.
- Öffnen Sie die TCP-Ports 11104 und 11105 für sicheren Datentransfer und Verwaltung zwischen Speichersystemen. ICMP ist optional, kann aber bei Netzwerkprüfungen und Fehlerbehebung hilfreich sein.
- Das FSx for ONTAP-Dateisystem, das Sie für die Replikationsbeziehung verwenden, muss über eine zugeordnete Verknüpfung verfügen. ["Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen"](#). Nach der Verknüpfung kann zu diesem Vorgang zurückgekehrt werden.
- Für die Datenreplikierung von einem lokalen ONTAP-System zu einem FSx for ONTAP-Dateisystem stellen Sie sicher, dass das lokale ONTAP-System erkannt wurde.
- Die Replikation wird nicht unterstützt für Volumes, die sich in einem anderen Status als verfügbar, erstellt oder falsch konfiguriert befinden, und wenn die ONTAP-Version nicht kompatibel ist.
- Stellen Sie bei Migrationsfällen sicher, dass die letzte Replikation für das Volume innerhalb der letzten 24 Stunden abgeschlossen wurde, bevor Sie eine Replikationsbeziehung mit den Storage-VM-Daten und Konfigurationseinstellungen erstellen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Die Auswahl des Dateisystems, das die zu replizierenden Volumes enthält, erfolgt auf der Seite FSx for ONTAP.
4. Entweder werden alle Volumes in einem Dateisystem oder nur ausgewählte Volumes repliziert.
 - Zum Replizieren aller Volumes in einem Dateisystem kann in der Dateisystemübersicht die Option **Daten replizieren** ausgewählt werden.
 - Für die Replikation ausgewählter Volumes erfolgt die Auswahl der Registerkarte **Volumes** in der Dateisystemübersicht.

In der Tabelle „Volumes“ können ein oder mehrere Volumes ausgewählt und anschließend **Daten replizieren** ausgewählt werden.

5. Auf der Seite „Daten replizieren“ sind unter „Replikationsziel“ die folgenden Angaben erforderlich:

a. **Anwendungsfall:** Für die Replikation ist einer der folgenden Anwendungsfälle auszuwählen. Je nach ausgewähltem Anwendungsfall füllt Workload Factory das Formular mit empfohlenen Werten gemäß Best Practices aus. Die empfohlenen Werte können übernommen oder beim Ausfüllen des Formulars geändert werden.

- Künstliche Intelligenz (KI) und maschinelles Lernen (ML): Replizieren Sie Ihre lokalen ONTAP-Daten zu FSx for ONTAP und erstellen Sie S3-Zugriffspunkte, um das Training von KI und ML in der Cloud zu unterstützen
- Migration: überträgt Ihre Daten in das Zielspeichersystem FSx for ONTAP

Replikation der Speicher-VM-Konfiguration: Optional können Sie die Replikation der Speicher-VM-Daten und -Konfigurationseinstellungen für eine einzelne Speicher-VM auswählen. Bei der Migration von Daten und Einstellungen müssen alle Volumes innerhalb der letzten 24 Stunden repliziert und anschließend gleichzeitig umgeschaltet werden.

Die Tiering-Richtlinie für alle Volumes entspricht standardmäßig der Tiering-Richtlinie des Quell-Volumes, was für Migrationsanwendungsfälle empfohlen wird.

Während der Migration greifen Clients auf Daten des Quell-ONTAP-Datensystems zu. Nach der Umstellung sind die Volumes über die Ziel-FSx for ONTAP-Datensystem-IP-Adressen verfügbar. Aktualisieren Sie alle Clients oder Ressourcen, die noch die alte IP-Adresse verwenden.

- Hot Disaster Recovery: gewährleistet hohe Verfügbarkeit und schnelle Wiederherstellung kritischer Workloads im Katastrophenfall
- Kalt- oder Archiv-Disaster-Recovery:
 - Kalte Notfallwiederherstellung: verwendet längere Wiederherstellungszeitvorgaben (RTO) und Wiederherstellungspunktvorgaben (RPO), um die Kosten zu senken
 - Archiv: repliziert Daten für Langzeit-Storage und Compliance
- Sonstige

Darüber hinaus bestimmt die Auswahl des Anwendungsfalls die Replikationsrichtlinie oder die SnapMirror Richtlinie (ONTAP). Die zur Beschreibung von Replikationsrichtlinien verwendeten Begriffe stammen aus "[ONTAP 9 Dokumentation](#)".

- Für Migrationen und andere Zwecke heißt die Replikationsrichtlinie *MirrorAllSnapshots*. *MirrorAllSnapshots* ist eine asynchrone Richtlinie zum Spiegeln aller Snapshots und des zuletzt aktiven Dateisystems.
- Für die Hot-, Cold- oder Archiv-Notfallwiederherstellung wird die Replikationsrichtlinie als *MirrorAndVault* bezeichnet. *MirrorAndVault* ist eine asynchrone Vault-Richtlinie für die Spiegelung des neuesten aktiven Dateisystems sowie täglicher und wöchentlicher Snapshots.

Für alle Anwendungsfälle gilt: Wenn Sie Snapshots für die langfristige Aufbewahrung aktivieren, ist die Standardreplikationsrichtlinie *MirrorAndVault*.

b. **FSx for ONTAP file system:** Wählen Sie Anmeldeinformationen, Region und FSx for ONTAP file system name für das Ziel-FSx for ONTAP file system aus.

c. **Name der Speicher-VM:** Wählen Sie die Speicher-VM aus. Die von Ihnen ausgewählte Speicher-VM ist das Ziel für alle ausgewählten Volumes in dieser Replikationsbeziehung.

Wenn die Namen der Quell- und Ziel-Storage-VMs identisch sind, erstellen wir einen Dateisystemalias für die Ziel-Storage-VM-Namen, um Peering-Konflikte zu vermeiden.

- d. **Volume-Name:** Der Ziel-Volume-Name wird automatisch im folgenden Format `{OriginalVolumeName}_copy` generiert. Sie können den automatisch generierten Volume-Namen verwenden oder einen anderen Volume-Namen eingeben.
- e. **Tiering-Richtlinie:** Die Tiering-Richtlinie für die im Ziel-Volume gespeicherten Daten wird ausgewählt. Standardmäßig wird die für den ausgewählten Anwendungsfall empfohlene Tiering-Richtlinie verwendet.

Balanced (Auto) ist die Standard-Tiering-Richtlinie beim Erstellen eines Volumes mit der Workload Factory Konsole. Weitere Informationen zu Volume-Tiering-Richtlinien finden sich in "[Volume-Speicherkapazität](#)" der AWS FSx for NetApp ONTAP Dokumentation. Zu beachten ist, dass Workload Factory in der Workload Factory Konsole anwendungsfallbasierte Namen für Tiering-Richtlinien verwendet und die FSx for ONTAP Tiering-Richtliniennamen in Klammern aufführt.

Wenn Sie den Migrations-Anwendungsfall ausgewählt haben, kopiert Workload Factory automatisch die Tiering-Richtlinie des Quellvolumes auf das Ziel-Volume. Sie können die Option zum Kopieren der Tiering-Richtlinie deaktivieren und eine Tiering-Richtlinie auswählen, die für das zur Replikation ausgewählte Volume gilt.

- a. **Maximale Transferrate: Begrenzt** auswählen und das maximale Transferlimit in MB/s eingeben. Alternativ **Unbegrenzt** auswählen.

Ohne eine Begrenzung können die Netzwerk- und Applikation Performance sinken. Alternativ empfehlen wir für kritische Workloads, beispielsweise solche, die primär für die Notfallwiederherstellung verwendet werden, eine unbegrenzte Transferrate für FSx for ONTAP file systems.

6. Unter Replikationseinstellungen sind die folgenden Angaben erforderlich:

- a. **Replikationsbeziehung initialisieren:** Wählen Sie, ob die Replikationsbeziehung direkt nach ihrer Erstellung oder später initialisiert werden soll. Beachten Sie, dass die Initialisierung zeitaufwändig sein kann, und Sie möchten den Basistransfer möglicherweise außerhalb der Spitzenzeiten durchführen.

Um die Initialisierung später manuell durchzuführen, beachten Sie die Anweisungen in [Schritt 2: Replikationsbeziehung initialisieren](#).

- b. **Replikationsintervall:** Hier wird die Häufigkeit ausgewählt, mit der Snapshots vom Quell-Volume auf das Ziel-Volume übertragen werden.
- c. **Langzeitaufbewahrung:** Optional können Snapshots für die Langzeitaufbewahrung aktiviert werden. Die Langzeitaufbewahrung ermöglicht den Weiterbetrieb von Geschäfts-Services auch bei einem vollständigen Standortausfall und unterstützt Applikationen dabei, mithilfe einer sekundären Kopie transparent ein Failover durchzuführen.

Replikationen ohne Langzeitaufbewahrung verwenden die Richtlinie *MirrorAllSnapshots*. Durch Aktivieren der Langzeitaufbewahrung wird der Replikation die Richtlinie *MirrorAndVault* zugewiesen.

Wenn Sie die Langzeitaufbewahrung aktivieren, können Sie eine vorhandene Richtlinie auswählen oder eine neue Richtlinie erstellen, um die zu replizierenden Snapshots und die Anzahl der aufzubewahrenden Snapshots festzulegen.



Für die Langzeitarchivierung sind übereinstimmende Quell- und Zielbezeichnungen erforderlich. Auf Wunsch kann Workload Factory fehlende Bezeichnungen für Sie erstellen.

- **Eine bestehende Richtlinie auswählen:** Wählen Sie eine bestehende Richtlinie aus.

- **Neue Richtlinie erstellen:** Geben Sie einen **Richtliniennamen** an.
- d. **Unveränderliche Snapshots:** Optional. Die Auswahl von **Enable immutable snapshots** verhindert, dass im Rahmen dieser Richtlinie erstellte Snapshots während des Aufbewahrungszeitraums gelöscht werden.
 - Die **Aufbewahrungsfrist** wird in Stunden, Tagen, Monaten oder Jahren festgelegt.
 - **Snapshot-Richtlinien:** Wählen Sie in der Tabelle die Häufigkeit der Snapshot-Richtlinie und die Anzahl der aufzubewahrenden Kopien aus. Sie können mehrere Snapshot-Richtlinien auswählen.
- e. **S3-Zugriffspunkt:** Optional können Sie einen S3-Zugriffspunkt anbinden, um auf FSx for ONTAP-Dateisystemdaten zuzugreifen, die sich auf NFS- oder SMB/CIFS-Volumes befinden, über die AWS S3-APIs. Nur der Dateizugriffstyp wird unterstützt. Folgende Details sind anzugeben:
 - **Name des S3 access point:** Geben Sie den Namen des S3 access point ein.
 - **Benutzer:** Wählen Sie einen vorhandenen Benutzer mit Zugriff auf das Volume aus oder erstellen Sie einen neuen Benutzer.
 - **Benutzertyp:** Wählen Sie **UNIX** oder **Windows** als Benutzerart.
 - **Netzwerkconfiguration:** Wählen Sie **Internet** oder **Virtual private cloud (VPC)**. Die Wahl des Netzwerktyps bestimmt, ob der Zugriffspunkt über das Internet erreichbar ist oder auf eine bestimmte VPC beschränkt ist.
 - **Inventartabelle aktivieren:** Wenn Sie die Inventartabelle für das Volume aktivieren, generiert das System Metadaten für alle Objekte, die über den S3-Zugriffspunkt zugänglich sind, und es fallen AWS S3-Anfragekosten an. Weitere Informationen finden Sie unter "[Amazon S3 Preisdokumentation](#)".
- f. **S3 access point tags:** Optional können Sie bis zu 50 Tags hinzufügen.

7. **Erstellen** auswählen.

Ergebnis

Die Replikationsbeziehung erscheint im Tab **Replikationsbeziehungen** im Ziel-FSx for ONTAP-Dateisystem.

Wenn Sie eine Replikationsbeziehung für Migrationszwecke erstellt haben, müssen Sie alle Volumes und ihre zugehörige Storage-VM umstellen, um die Migration der Storage-VM-Daten und Konfigurationseinstellungen auf das Ziel-FSx for ONTAP-Dateisystem abzuschließen.

Schritt 2: Replikationsbeziehung initialisieren

Initialisieren Sie eine Replikationsbeziehung zwischen Quell- und Ziel-Volume, um den Snapshot und alle Datenblöcke in NetApp Workload Factory zu übertragen.

Bei der Initialisierung wird ein *Basistransfer* durchgeführt: Es wird ein Snapshot des Quell-Volumes erstellt, anschließend werden der Snapshot und alle darin referenzierten Datenblöcke auf das Ziel-Volume übertragen.

Bevor Sie beginnen

Überlegen Sie sich gut, wann Sie diesen Vorgang durchführen. Die Initialisierung kann zeitaufwändig sein. Es empfiehlt sich, den Basistransfer außerhalb der Spitzenzeiten durchzuführen.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Wählen Sie in **FSx for ONTAP** das Aktionsmenü des zu aktualisierenden Dateisystems und anschließend

Verwalten.

4. Wählen Sie in der Dateisystemübersicht die Registerkarte **Replikationsbeziehungen** aus.
5. Wählen Sie auf der Registerkarte „Replikationsbeziehungen“ das Aktionsmenü der zu initialisierenden Replikationsbeziehung aus.
6. Wählen Sie **Initialisieren**.
7. Im Dialogfeld „Beziehung initialisieren“ wählen Sie **Initialisieren**.

Wenn der Replikationsstatus **Leerlauf** anzeigt, ist der Datentransfer abgeschlossen.

Schritt 3: Umstellung der Replikation für Migrationsanwendungsfälle

Nachdem die Replikationsbeziehung für einen Migrationsanwendungsfall erstellt wurde, muss die Replikation umgestellt werden, um die Migration der Storage-VM-Daten und Konfigurationseinstellungen auf das Ziel-FSx for ONTAP-Dateisystem abzuschließen. Die Umstellung der Replikation migriert Daten und Storage-VM-Konfigurationseinstellungen dauerhaft vom Quellsystem auf das Ziel-FSx for ONTAP-Dateisystem. Während der Umstellung werden die Daten ein letztes Mal repliziert. Die Quell-Storage-VM wird offline geschaltet, wenn die Umstellung beginnt.

Planen Sie den Cutover-Vorgang

Berücksichtigen Sie Folgendes bei der Planung des Umstellungsprozesses für Migrationsanwendungsfälle.

- **Unterstützung der Replikationsversion:** Quell- und Zielspeichersysteme müssen dieselbe ONTAP Hauptversion aufweisen. Wenn beispielsweise auf dem Quellsystem ONTAP Version 9.18.1 ausgeführt wird, muss auch auf dem Zielsystem eine Version von 9.18.1 ausgeführt werden.
- **Konfigurationseinstellungen für Storage-VMs:**
 - Beim Umstellungsvorgang werden nicht alle Konfigurationseinstellungen der Speicher-VM auf die Ziel-Speicher-VM migriert. Beispielsweise werden iSCSI-, Broadcast-Domain-MTU- und DNS-Einstellungen nicht migriert. Aktualisieren Sie diese Einstellungen nach der Umstellung manuell auf der Ziel-Speicher-VM. Weitere Informationen finden Sie im [Konfigurationseinstellungen nach der Umstellung aktualisieren](#) Abschnitt.
 - Wenn Ihre Storage-VM die Domänentunnel-Authentifizierung verwendet, richten Sie vor Beginn der Migration einen Domänentunnel auf dem Zieldateisystem ein und aktivieren Sie ihn.
- **Klone:** Klone werden als einzelne Volumes migriert und belegen daher mehr Speicherplatz auf dem Ziel-FSx for ONTAP-Dateisystem. Erwägen Sie, die Klone vor der Umstellung zu löschen, um eine erhöhte Kapazität auf dem Ziel zu vermeiden.
- **Cache-Volumes:** Für ONTAP FlexCache 9.17.x oder älter. Quell-Speicher-VMs, die Cache-Volumes enthalten, werden bei der Umstellung nicht unterstützt. Entfernen Sie die ONTAP FlexCache-Beziehung vor der Umstellung, um Migrationsfehler zu vermeiden.
- **AWS S3-Zugriffspunkte:** Die Cutover-Replikation für Migrationsanwendungsfälle wird für Volumes mit S3-Zugriffspunkten nicht unterstützt. Löschen Sie die S3-Zugriffspunkte vom Quellvolume, um Migrationsfehler zu vermeiden.
- **ONTAP S3-Konfigurationen:** Die Cutover-Replikation für Migrationsszenarien wird für vServer mit ONTAP S3-Konfigurationen nicht unterstützt. Entfernen Sie ONTAP S3-Konfigurationen, einschließlich object-store-server, Buckets, Benutzer, Gruppen oder Richtlinien, vom vServer, um Migrationsfehler zu vermeiden.
- **LUN-Seriennummern und iSCSI-Ziel-IQN:** Die LUN-Seriennummern und der iSCSI-Ziel-IQN ändern sich während der Umstellung.

Bevor Sie beginnen

Überprüfen Sie diese Anforderungen, bevor Sie beginnen.

- Unterbinden Sie jeglichen Clientzugriff auf Ihre Storage-VM, bevor Sie die Replikation umstellen.
- Stellen Sie sicher, dass alle Quellvolumes keine Daten mehr bereitstellen, bevor Sie die Replikation umstellen.
- Stellen Sie sicher, dass die Daten zwischen Quell- und Ziel-Volume synchronisiert sind, bevor Sie die Replikation umstellen.
- Das FSx for ONTAP-Dateisystem, das Sie für die Replikationsbeziehung verwenden, muss über eine zugeordnete Verknüpfung verfügen. ["Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen"](#). Nach der Verknüpfung kann zu diesem Vorgang zurückgekehrt werden.
 - Die folgenden Ports müssen in der Sicherheitsgruppe, die dem FSx for ONTAP-Dateisystem zugeordnet ist, für die Verbindungsherstellung geöffnet sein: Port 443 (HTTPS) und Port 22 (SSH).

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Wählen Sie in **FSx for ONTAP** das Dateisystem aus, das die Volume(s) enthält, die repliziert werden sollen.
4. Wählen Sie die Registerkarte **Replication relationships** aus.
5. Wählen Sie in der Tabelle Replication relationships die Replikationsbeziehung aus, die umgestellt werden soll, und wählen Sie dann **Cut over replication** aus.
6. Überprüfen Sie die Informationen im Dialogfeld Cut over replication und geben Sie dann *cut over* ein, um zu bestätigen.
7. Wählen Sie **Cut over** aus.

Ergebnis

Nach Einleitung der Umstellung wird die Quellspeicher-VM offline genommen.

Konfigurationseinstellungen nach der Umstellung aktualisieren

Nachdem Sie die Replikation für Migrationsszenarien umgestellt haben, aktualisieren Sie die folgenden Speicher-VM-Konfigurationseinstellungen auf der Ziel-Speicher-VM.

- Für iSCSI:
 - Initiatorgruppe neu erstellen
 - LUN-Zuordnung aktualisieren
 - Melden Sie sich an jedem SAN-Client an und aktualisieren Sie die iSCSI/MPIO-Einstellungen für das neue Ziel und entfernen Sie die alten vserver-Ziel-IPs
- Überprüfen Sie, ob die MTU-Einstellungen der Broadcast-Domäne wie erwartet sind
- Überprüfen Sie, ob die DNS-Einstellungen den Erwartungen entsprechen
- Cache-Beziehungen (ONTAP FlexCache-Beziehungen) neu erstellen, falls im Quellspeicher-VM Cache-Volumes vorhanden waren.

Falls erforderlich, ["die Tiering-Richtlinie ändern"](#) für das/die Ziel-Volume nach der Umstellung.

Kaskadenreplikation für Datensicherungsvolumes

NetApp Workload Factory unterstützt die Replikation von Datensicherungs-Volumes, auch als *Kaskadenbereitstellungen* bezeichnet. Eine *Kaskadenbereitstellung* besteht aus einer Kette von Beziehungen, bei der ein Quell-Volume auf ein sekundäres Volume (erster Hop) gespiegelt wird und das sekundäre Volume auf ein tertiäres Volume (zweiter Hop). Falls das sekundäre Volume nicht verfügbar ist, können Sie die Beziehung zwischen dem primären und dem tertiären Volume synchronisieren, ohne einen neuen Basistransfer durchzuführen.

Diese Funktion wird für FSx for ONTAP file systems mit ONTAP Version 9.6 und höher unterstützt. Weitere Informationen finden Sie unter ["ONTAP Dokumentation für kompatible ONTAP Versionen"](#).

Weitere Informationen zu ["wie Kaskadenbereitstellungen funktionieren"](#).

Bevor Sie beginnen

Vor Beginn ist Folgendes zu beachten:

- Zu beachten ist, dass die Resynchronisierung von Volumes, die Teil einer Kaskadenkonfiguration sind, länger dauern kann.
- Wenn das Quellvolume der Beziehung ein Datensicherungsvolume ist und das Ziel einer anderen Beziehung darstellt, wird die Umkehrung der Replikationsbeziehung nicht unterstützt.
- Eine Replik eines Datensicherungsvolumes (oder ein zweiter Hop) wird unterstützt. Es gilt nicht als Best Practice, eine zweite Replik eines Datensicherungsvolumes (oder einen dritten Hop) zu erstellen.
- Öffnen Sie die TCP-Ports 11104 und 11105 für sicheren Datentransfer und Verwaltung zwischen Speichersystemen. ICMP ist optional, kann aber bei Netzwerkprüfungen und Fehlerbehebung hilfreich sein.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** erfolgt die Auswahl von **Manage** über das Aktionsmenü des Dateisystems, das die zu replizierenden Volumes enthält.
4. In der Dateisystemübersicht erfolgt die Auswahl der Registerkarte **Volumes**.
5. In der Tabelle „Volumes“ erfolgt die Auswahl eines oder mehrerer Data Protection Volumes (DP/replizierte Volumes); anschließend wird **Daten replizieren** gewählt.
6. Auf der Seite „Daten replizieren“ sind unter „Replikationsziel“ die folgenden Angaben erforderlich:
 - a. **Anwendungsfall:** Für die Replikation ist einer der folgenden Anwendungsfälle auszuwählen. Je nach ausgewähltem Anwendungsfall füllt Workload Factory das Formular mit empfohlenen Werten gemäß Best Practices aus. Die empfohlenen Werte können übernommen oder beim Ausfüllen des Formulars geändert werden.
 - Künstliche Intelligenz (KI) und maschinelles Lernen (ML): Replizieren Sie Ihre lokalen ONTAP-Daten zu FSx for ONTAP und erstellen Sie S3-Zugriffspunkte, um das Training von KI und ML in der Cloud zu unterstützen
 - Migration: überträgt Ihre Daten in das Zieldateisystem FSx for ONTAP

Replikation der Speicher-VM-Konfiguration: Optional können Sie die Replikation der Speicher-VM-Daten und -Konfigurationseinstellungen für eine einzelne Speicher-VM auswählen. Bei der Migration von Daten und Einstellungen müssen alle Volumes innerhalb der letzten 24 Stunden

repliziert und anschließend gleichzeitig umgeschaltet werden.

Die Tiering-Richtlinie für alle Volumes entspricht standardmäßig der Tiering-Richtlinie des Quell-Volumes, was für Migrationsanwendungsfälle empfohlen wird.

Während der Migration greifen Clients auf Daten des Quell-ONTAP-Dateisystems zu. Nach der Umstellung sind die Volumes über die Ziel-FSx for ONTAP-Dateisystem-IP-Adressen verfügbar. Aktualisieren Sie alle Clients oder Ressourcen, die noch die alte IP-Adresse verwenden.

- Hot Disaster Recovery: gewährleistet hohe Verfügbarkeit und schnelle Wiederherstellung kritischer Workloads im Katastrophenfall
- Kalt- oder Archiv-Disaster-Recovery:
 - Kalte Notfallwiederherstellung: verwendet längere Wiederherstellungszeitvorgaben (RTO) und Wiederherstellungspunktvorgaben (RPO), um die Kosten zu senken
 - Archiv: repliziert Daten für Langzeit-Storage und Compliance
- Sonstige

Darüber hinaus bestimmt die Auswahl des Anwendungsfalls die Replikationsrichtlinie oder die SnapMirror Richtlinie (ONTAP). Die zur Beschreibung von Replikationsrichtlinien verwendeten Begriffe stammen aus ["ONTAP 9 Dokumentation"](#).

- Für Migrationen und andere Zwecke heißt die Replikationsrichtlinie *MirrorAllSnapshots*. *MirrorAllSnapshots* ist eine asynchrone Richtlinie zum Spiegeln aller Snapshots und des zuletzt aktiven Dateisystems.
- Für die Hot-, Cold- oder Archiv-Notfallwiederherstellung wird die Replikationsrichtlinie als *MirrorAndVault* bezeichnet. *MirrorAndVault* ist eine asynchrone Vault-Richtlinie für die Spiegelung des neuesten aktiven Dateisystems sowie täglicher und wöchentlicher Snapshots.

Für alle Anwendungsfälle gilt: Wenn Sie Snapshots für die langfristige Aufbewahrung aktivieren, ist die Standardreplikationsrichtlinie *MirrorAndVault*.

- b. **FSx for ONTAP file system:** Wählen Sie Anmeldeinformationen, Region und FSx for ONTAP file system name für das Ziel-FSx for ONTAP file system aus.
- c. **Name der Speicher-VM:** Wählen Sie die Speicher-VM aus. Die von Ihnen ausgewählte Speicher-VM ist das Ziel für alle ausgewählten Volumes in dieser Replikationsbeziehung.

Wenn die Namen der Quell- und Ziel-Storage-VMs identisch sind, erstellen wir einen Dateisystemalias für die Ziel-Storage-VM-Namen, um Peering-Konflikte zu vermeiden.

- d. **Volume-Name:** Der Ziel-Volume-Name wird automatisch im folgenden Format `{OriginalVolumeName}_copy` generiert. Sie können den automatisch generierten Volume-Namen verwenden oder einen anderen Volume-Namen eingeben.
- e. **Tiering-Richtlinie:** Die Tiering-Richtlinie für die im Ziel-Volume gespeicherten Daten wird ausgewählt. Standardmäßig wird die für den ausgewählten Anwendungsfall empfohlene Tiering-Richtlinie verwendet.

Balanced (Auto) ist die Standard-Tiering-Richtlinie beim Erstellen eines Volumes mit der Workload Factory Konsole. Weitere Informationen zu Volume-Tiering-Richtlinien finden sich in ["Volume-Speicherkapazität"](#) der AWS FSx for NetApp ONTAP Dokumentation. Zu beachten ist, dass Workload Factory in der Workload Factory Konsole anwendungsfallbasierte Namen für Tiering-Richtlinien verwendet und die FSx for ONTAP Tiering-Richtliniennamen in Klammern aufführt.

Wenn Sie den Migrations-Anwendungsfall ausgewählt haben, kopiert Workload Factory automatisch die Tiering-Richtlinie des Quellvolumen auf das Ziel-Volumen. Sie können die Option zum Kopieren der Tiering-Richtlinie deaktivieren und eine Tiering-Richtlinie auswählen, die für das zur Replikation ausgewählte Volumen gilt.

- a. **Maximale Transferrate: Begrenzt** auswählen und das maximale Transferlimit in MB/s eingeben. Alternativ **Unbegrenzt** auswählen.

Ohne eine Begrenzung können die Netzwerk- und Applikation Performance sinken. Alternativ empfehlen wir für kritische Workloads, beispielsweise solche, die primär für die Notfallwiederherstellung verwendet werden, eine unbegrenzte Transferrate für FSx for ONTAP file systems.

7. Unter Replikationseinstellungen sind die folgenden Angaben erforderlich:

- a. **Replikationsbeziehung initialisieren:** Wählen Sie, ob die Replikationsbeziehung direkt nach ihrer Erstellung oder später initialisiert werden soll. Beachten Sie, dass die Initialisierung zeitaufwändig sein kann, und Sie möchten den Basistransfer möglicherweise außerhalb der Spitzenzeiten durchführen.

Um die Initialisierung später manuell durchzuführen, beachten Sie die Anweisungen in [Schritt 2: Replikationsbeziehung initialisieren](#).

- b. **Replikationsintervall:** Hier wird die Häufigkeit ausgewählt, mit der Snapshots vom Quell-Volumen auf das Ziel-Volumen übertragen werden.
- c. **Langzeitaufbewahrung:** Optional können Snapshots für die Langzeitaufbewahrung aktiviert werden. Die Langzeitaufbewahrung ermöglicht den Weiterbetrieb von Geschäfts-Services auch bei einem vollständigen Standortausfall und unterstützt Applikationen dabei, mithilfe einer sekundären Kopie transparent ein Failover durchzuführen.

Replikationen ohne Langzeitaufbewahrung verwenden die Richtlinie *MirrorAllSnapshots*. Durch Aktivieren der Langzeitaufbewahrung wird der Replikation die Richtlinie *MirrorAndVault* zugewiesen.

Wenn Sie die Langzeitaufbewahrung aktivieren, können Sie eine vorhandene Richtlinie auswählen oder eine neue Richtlinie erstellen, um die zu replizierenden Snapshots und die Anzahl der aufzubewahrenden Snapshots festzulegen.



Für die Langzeitarchivierung sind übereinstimmende Quell- und Zielbezeichnungen erforderlich. Auf Wunsch kann Workload Factory fehlende Bezeichnungen für Sie erstellen.

- **Eine bestehende Richtlinie auswählen:** Wählen Sie eine bestehende Richtlinie aus.
- **Neue Richtlinie erstellen:** Geben Sie einen **Richtliniennamen** an.
- d. **Unveränderliche Snapshots:** Optional. Die Auswahl von **Enable immutable snapshots** verhindert, dass im Rahmen dieser Richtlinie erstellte Snapshots während des Aufbewahrungszeitraums gelöscht werden.
 - Die **Aufbewahrungsfrist** wird in Stunden, Tagen, Monaten oder Jahren festgelegt.
 - **Snapshot-Richtlinien:** Wählen Sie in der Tabelle die Häufigkeit der Snapshot-Richtlinie und die Anzahl der aufzubewahrenden Kopien aus. Sie können mehrere Snapshot-Richtlinien auswählen.
- e. **S3-Zugriffspunkt:** Optional können Sie einen S3-Zugriffspunkt anbinden, um auf FSx for ONTAP-Dateisystemdaten zuzugreifen, die sich auf NFS- oder SMB/CIFS-Volumen befinden, über die AWS S3-APIs. Nur der Dateizugriffstyp wird unterstützt. Folgende Details sind anzugeben:

- **Name des S3 access point:** Geben Sie den Namen des S3 access point ein.
- **Benutzer:** Wählen Sie einen vorhandenen Benutzer mit Zugriff auf das Volume aus oder erstellen Sie einen neuen Benutzer.
- **Benutzertyp:** Wählen Sie **UNIX** oder **Windows** als Benutzerart.
- **Netzwerkkonfiguration:** Wählen Sie **Internet** oder **Virtual private cloud (VPC)**. Die Wahl des Netzwerktyps bestimmt, ob der Zugriffspunkt über das Internet erreichbar ist oder auf eine bestimmte VPC beschränkt ist.
- **Inventartabelle aktivieren:** Wenn Sie die Inventartabelle für das Volume aktivieren, generiert das System Metadaten für alle Objekte, die über den S3-Zugriffspunkt zugänglich sind, und es fallen AWS S3-Anfragekosten an. Weitere Informationen finden Sie unter ["Amazon S3 Preisdokumentation"](#).

f. **S3 access point tags:** Optional können Sie bis zu 50 Tags hinzufügen.

8. **Erstellen** auswählen.

Ergebnis

Das replizierte Volume bzw. die replizierten Volumes erscheinen auf der Registerkarte **Replikationsbeziehungen** im FSx for ONTAP Zielsystem.

Verwandte Informationen

["Die Tiering-Richtlinie ändern"](#) für das/die Ziel-Volume nach der Umstellung.

Replikation von On-Premises ONTAP Clusterdaten in NetApp Workload Factory

Lokale ONTAP Daten in der NetApp Workload Factory erkennen und replizieren, sodass sie als Backup in der Cloud genutzt werden können.

Über diese Aufgabe

Um Daten aus einem lokalen ONTAP Cluster zu nutzen, müssen Sie zunächst den lokalen ONTAP Cluster ermitteln. Nachdem Sie einen lokalen ONTAP Cluster ermittelt haben, können Sie die Daten für jeden der folgenden Anwendungsfälle verwenden.

Anwendungsfälle

- **Backup und Migration in die Cloud:** In ein FSx for ONTAP Dateisystem replizierte lokale ONTAP Volume-Daten können als Backup in der Cloud verwendet werden.
- **Data Tiering:** Nach der Replikation können selten genutzte On-Premises-ONTAP-Volume-Daten vom SSD Storage-Tier auf das Storage-Tier des Kapazitätspools verschoben werden.

Erkennung eines lokalen ONTAP Clusters

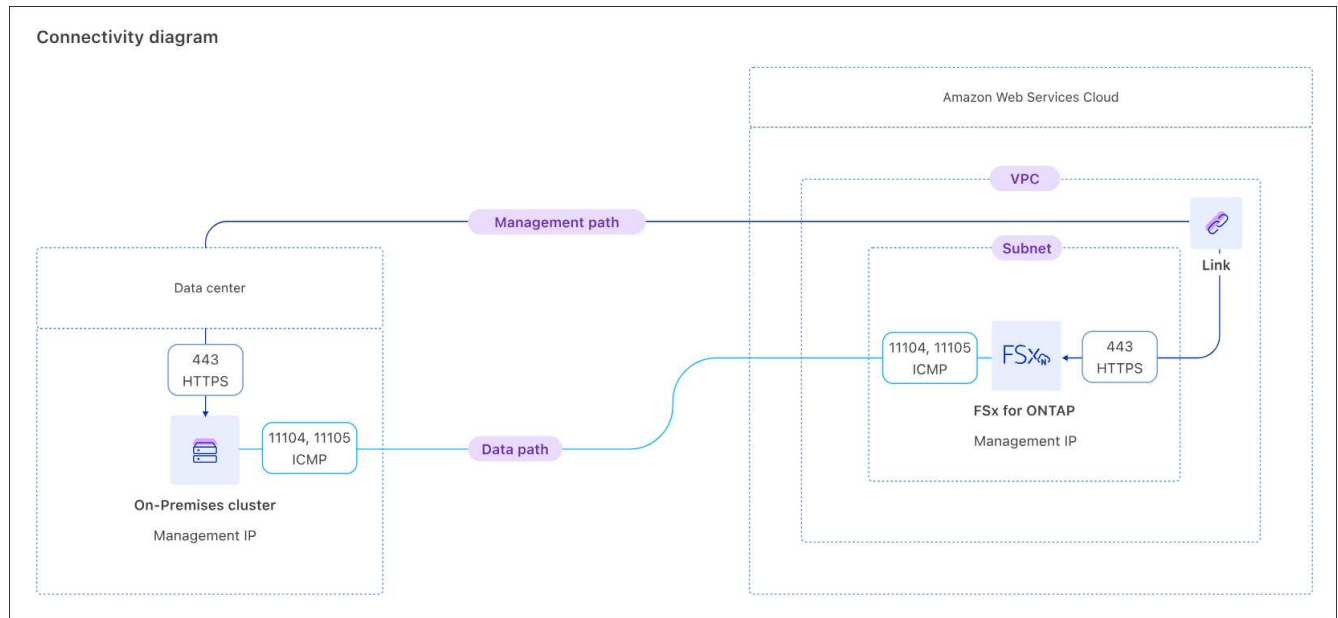
Die Erkennung eines lokalen ONTAP Clusters in NetApp Workload Factory ermöglicht die Replizierung der Daten in ein Amazon FSx for NetApp ONTAP Dateisystem.

Bevor Sie beginnen

Vor Beginn sollte Folgendes vorhanden sein:

- Ein FSx for ONTAP Dateisystem zur Replikation.
- Eine verbundene Verbindung, die mit dem erkannten lokalen Cluster verknüpft wird. Wenn keine Verbindung vorhanden ist, ist es erforderlich, ["einen erstellen"](#).

- ONTAP Benutzeranmeldeinformationen mit erforderlichen Berechtigungen.
- On-premises ONTAP Version 9.8 und höher.
- Die Konnektivität zeigt das folgende Diagramm.



Schritte

1. Melden Sie sich bei der "NetApp Console" an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Im Menü **FSx for ONTAP** ist **On-premises ONTAP** auszuwählen.
4. **Discover** auswählen.
5. Nach Prüfung der Voraussetzungen erfolgt die Auswahl von **Weiter**.
6. Auf der Seite „Discover ONTAP on-premises“ sind unter **Clusterkonfiguration** die folgenden Angaben erforderlich:

- a. **Link:** Auswahl eines Links. Der Link wird mit dem lokalen Cluster verknüpft, um eine Verbindung zwischen dem Cluster und Workload Factory herzustellen.

Falls Sie noch keinen Link erstellt haben, können Sie zunächst den Anweisungen folgen und anschließend zu diesem Vorgang zurückkehren, um den Link auszuwählen.

- b. **Cluster-IP-Adresse:** IP-Adresse des lokalen ONTAP Clusters, der repliziert werden soll.
- c. **ONTAP-Zugangsdaten:** Bitte geben Sie Folgendes an:
 - GovCloud accounts: Geben Sie die ARN mit ONTAP Zugangsdaten ein.
 - Alle anderen Konten: Geben Sie die ONTAP-Anmeldeinformationen für den lokalen ONTAP Cluster ein. Stellen Sie sicher, dass der Benutzer über die erforderlichen Berechtigungen verfügt.

7. Mit **Discover** lässt sich der Discovery-Prozess starten.

Ergebnis

Der lokale ONTAP Cluster wurde erkannt und wird nun auf der Registerkarte **On-Premises ONTAP** angezeigt.

Sie können die Daten jetzt in Ihrem lokalen ONTAP Cluster anzeigen und [Replizieren der Daten in ein FSx for](#)

Volume-Daten aus einem lokalen ONTAP Cluster replizieren

Volume-Daten aus einem lokalen ONTAP Cluster werden in ein FSx for ONTAP Dateisystem repliziert. Nach der Replikation können die Daten zur Anreicherung von KI-Wissensdatenbanken verwendet werden.

Bevor Sie beginnen

- Sie müssen einen lokalen ONTAP Cluster ermitteln, um seine Volume-Daten zu replizieren.
- Für die Replikation als Ziel ist ein verfügbares FSx for ONTAP Dateisystem erforderlich.
- Sowohl der lokale ONTAP Cluster als auch das FSx for ONTAP Dateisystem, das Sie für die Replikationsbeziehung verwenden, müssen über eine zugeordnete Verbindung verfügen. ["Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen"](#). Nach der Verknüpfung ist eine Rückkehr zu diesem Vorgang erforderlich.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Im Menü **FSx for ONTAP** ist **On-premises ONTAP** auszuwählen.
4. Zum Auffinden von Volumes nach Storage VM steht in der Dropdown-Liste **Storage VM auswählen** zur Verfügung.
5. Ein oder mehrere Volumes zur Replikation auswählen und anschließend **Replizieren** wählen.
6. Auf der Seite „Replikation erstellen“ sind unter „Replikationsziel“ die folgenden Angaben erforderlich:
 - a. **FSx for ONTAP file system:** Wählen Sie Anmeldeinformationen, Region und FSx for ONTAP file system name für das Ziel-FSx for ONTAP file system aus.
 - b. **Name der Storage VM:** Die Auswahl der Storage VM erfolgt im Dropdown-Menü.
 - c. **Volume-Name:** Der Ziel-Volume-Name wird automatisch im folgenden Format `{OriginalVolumeName}_copy` generiert. Sie können den automatisch generierten Volume-Namen verwenden oder einen anderen Volume-Namen eingeben.
 - d. **Tiering-Daten:** Auswahl der Tiering-Richtlinie für die im Ziel-Volume gespeicherten Daten.
 - **Auto:** Die Standard-Tiering-Richtlinie beim Erstellen eines Volumes mit der Workload Factory FSx for ONTAP Benutzeroberfläche. Tiering aller kalten Daten, einschließlich Benutzerdaten und Snapshots, auf das Capacity Pool Storage-Tier für einen bestimmten Zeitraum.
 - **Nur Snapshot:** Es werden nur Snapshot-Daten auf das Storage-Tier des Capacity Pool verschoben.
 - **None:** Alle Daten Ihres Volumes bleiben auf dem primären Storage-Tier.
 - **Alle:** Kennzeichnet sämtliche Benutzerdaten und Snapshot-Daten als kalt und speichert sie im Storage-Tier des Kapazitätspools.

Einige Tiering-Richtlinien haben eine zugehörige Mindestkühlzeit, die festlegt, wie lange, also wie viele *cooling days*, Benutzerdaten in einem Volume inaktiv bleiben müssen, damit die Daten als „kalt“ gelten und in den Capacity Pool Storage-Tier verschoben werden. Die Kühlzeit beginnt, wenn Daten auf die Festplatte geschrieben werden.

Weitere Informationen zu Volume-Tiering-Richtlinien bietet ["Volume-Speicherkapazität"](#) die AWS FSx for NetApp ONTAP Dokumentation.

- a. **Maximale Transferrate:** Bei Auswahl von **Begrenzt** ist die maximale Transferrate in MiB/s einzugeben. Alternativ steht **Unbegrenzt** zur Auswahl.

Ohne Begrenzung könnte die Netzwerk- und Applikations-Performance nachlassen. Alternativ empfehlen wir für FSx for ONTAP Dateisysteme bei kritischen Workloads, zum Beispiel solchen, die in erster Linie für die Notfallwiederherstellung verwendet werden, eine unbegrenzte Transferrate.

7. Unter Replikationseinstellungen sind die folgenden Angaben erforderlich:

- a. **Replikationsintervall:** Hier wird die Häufigkeit ausgewählt, mit der Snapshots vom Quell-Volume auf das Ziel-Volume übertragen werden.
- b. **Langzeitaufbewahrung:** Optional können Snapshots für die Langzeitaufbewahrung aktiviert werden.

Wenn Sie die Langzeitaufbewahrung aktivieren, können Sie eine vorhandene Richtlinie auswählen oder eine neue Richtlinie erstellen, um die zu replizierenden Snapshots und die Anzahl der aufzubewahrenden Snapshots festzulegen.

- Für eine vorhandene Richtlinie ist **Vorhandene Richtlinie auswählen** auszuwählen, und anschließend ist die vorhandene Richtlinie im Dropdown-Menü auszuwählen.
- Für eine neue Richtlinie ist **Neue Richtlinie erstellen** auszuwählen, und anschließend sind die folgenden Angaben erforderlich:
 - **Richtliniennamen:** Geben Sie einen Richtliniennamen ein.
 - **Snapshot-Richtlinien:** Wählen Sie in der Tabelle die Häufigkeit der Snapshot-Richtlinie und die Anzahl der aufzubewahrenden Kopien aus. Sie können mehrere Snapshot-Richtlinien auswählen.

8. **Erstellen** auswählen.

Ergebnis

Die Replikationsbeziehung erscheint im Tab **Replikationsbeziehungen** im Ziel-FSx for ONTAP-Dateisystem.

Entfernen eines lokalen ONTAP Clusters aus NetApp Workload Factory

Bei Bedarf ist das Entfernen eines lokalen ONTAP-Clusters aus NetApp Workload Factory möglich.

Bevor Sie beginnen

Sie müssen "[Löschen aller bestehenden Replikationsbeziehungen](#)" für alle Volumes im lokalen ONTAP Cluster überprüfen, bevor Sie den Cluster entfernen, damit keine fehlerhaften Beziehungen zurückbleiben.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Im Menü **FSx for ONTAP** ist **On-premises ONTAP** auszuwählen.
4. Auswahl des lokalen ONTAP Clusters, der entfernt werden soll.
5. Im Menü „Aktionen“ ist die Option **Aus Workload Factory entfernen** auszuwählen.

Ergebnis

Der lokale ONTAP Cluster wurde aus NetApp Workload Factory entfernt.

Eine Storage VM auf ein anderes FSx for ONTAP Dateisystem replizieren

Die Replikation einer Storage VM auf ein anderes FSx for ONTAP Dateisystem in NetApp Workload Factory bietet eine zusätzliche Schutzebene für den Datenzugriff im Falle eines Datenverlusts. Bei diesem Vorgang werden alle Volumes einer Storage VM auf ein anderes FSx for ONTAP Dateisystem repliziert.

Bevor Sie beginnen

Um eine Storage-VM auf ein anderes FSx for ONTAP File System zu replizieren, muss eine Verknüpfung hergestellt werden. ["Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen"](#). Nach der Verknüpfung ist eine Rückkehr zu diesem Vorgang erforderlich.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** wird im Aktionsmenü des Dateisystems mit der zu replizierenden Storage-VM die Option **Manage** ausgewählt.
4. In der Dateisystemübersicht erfolgt unter Storage VMs die Auswahl von **Manage**.
5. Auf dem Bildschirm „Storage VMs managen“ wird im Aktionsmenü der Storage VM, für die eine SVM repliziert werden soll, **Erweiterte Aktionen > Storage VM replizieren** ausgewählt.
6. Auf der Seite „Daten replizieren“ sind unter „Replikationsziel“ die folgenden Angaben erforderlich:

- a. **FSx for ONTAP file system:** Wählen Sie Anmeldeinformationen, Region und FSx for ONTAP file system name für das Ziel-FSx for ONTAP file system aus.
- b. **Name der Storage VM:** Die Auswahl der Storage VM erfolgt im Dropdown-Menü.
- c. **Volume-Name:** Der Name des Ziel-Volume wird automatisch im folgenden Format generiert {OriginalVolumeName}_copy.
- d. **Tiering-Richtlinie:** Auswahl der Tiering-Richtlinie für die im Ziel-Volume gespeicherten Daten.

Auto ist die Standard-Tiering-Richtlinie beim Erstellen eines Volumes über die Workload Factory FSx for ONTAP Benutzeroberfläche. Weitere Informationen zu Volume-Tiering-Richtlinien enthält ["Volume-Speicherkapazität"](#) die AWS FSx for NetApp ONTAP Dokumentation.

- e. **Maximale Transferrate: Begrenzt** auswählen und das maximale Transferlimit in MB/s eingeben. Alternativ **Unbegrenzt** auswählen.

Ohne Begrenzung könnte die Netzwerk- und Applikations-Performance nachlassen. Alternativ empfehlen wir für FSx for ONTAP Dateisysteme bei kritischen Workloads, zum Beispiel solchen, die in erster Linie für die Notfallwiederherstellung verwendet werden, eine unbegrenzte Transferrate.

7. Unter Replikationseinstellungen sind die folgenden Angaben erforderlich:
 - a. **Replikationsintervall:** Hier wird die Häufigkeit ausgewählt, mit der Snapshots vom Quell-Volume auf das Ziel-Volume übertragen werden.
 - b. **Langzeitaufbewahrung:** Optional können Snapshots für die Langzeitaufbewahrung aktiviert werden.

Wenn Sie die Langzeitaufbewahrung aktivieren, können Sie eine vorhandene Richtlinie auswählen oder eine neue Richtlinie erstellen, um die zu replizierenden Snapshots und die Anzahl der aufzubewahrenden Snapshots festzulegen.

- i. Für **Choose an existing policy** ist eine bestehende Richtlinie aus dem Dropdown-Menü auszuwählen.
- ii. Für **Neue Richtlinie erstellen** sind die folgenden Angaben erforderlich:
 - A. **Richtliniennamen:** Geben Sie einen Richtliniennamen ein.
 - B. **Snapshot-Richtlinien:** Wählen Sie in der Tabelle die Häufigkeit der Snapshot-Richtlinie und die Anzahl der aufzubewahrenden Kopien aus. Sie können mehrere Snapshot-Richtlinien auswählen.

8. **Erstellen** auswählen.

Ergebnis

Alle Volumes innerhalb der Storage VM werden auf das Zielsystem repliziert.

Replikationsverzögerungen in NetApp Workload Factory verfolgen

Die Nachverfolgung kann aktiviert werden, um Replikationsverzögerungen in Ihrem Konto zu überwachen. Workload Factory benachrichtigt Sie, wenn Verzögerungen einen festgelegten Schwellenwert überschreiten. Standardmäßig beträgt der Schwellenwert 150 % des Replikationsintervalls, um normale Übertragungszeiten zu ermöglichen und Fehlalarme zu reduzieren. Der Schwellenwert kann an Ihr RPO angepasst werden, sodass Benachrichtigungen erfolgen, wenn Verzögerungen diesen überschreiten. Die Daten können außerdem zur weiteren Analyse in eine CSV-Datei exportiert werden.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Wählen Sie in **FSx for ONTAP** das Aktionsmenü des zu aktualisierenden Dateisystems und anschließend **Verwalten**.
4. Wählen Sie in der Dateisystemübersicht die Registerkarte **Replikationsbeziehungen** aus.
5. Wählen Sie **Tracking aktivieren**.
6. Im Dialogfeld „Replikationsverzögerungsverlauf aktivieren“ wählen Sie **Enable**.
7. Zurück in der Kachel „Replikationsverzögerungsverlauf“ wählen Sie **Schwellenwert anpassen**, um Ihren bevorzugten Schwellenwert festzulegen.
8. Im Dialogfeld „Verzögerungsschwellenwert anpassen“ geben Sie die Schwelle in Stunden und Minuten ein.
9. Optional können Sie **Benachrichtigungen bei Verzögerungen aktivieren** auswählen, um Benachrichtigungen zu erhalten, wenn Replikationsverzögerungen den Schwellenwert überschreiten.

Benachrichtigungen erfolgen per E-Mail und beinhalten:

- Quelldateisystem
- Quellvolumen
- Zielsystem
- Zielvolumen
- Schwellenwert für Verzögerungszeit wurde überschritten

- Link zur Replikationsbeziehung

10. **Anwenden** auswählen.

Verwandte Informationen

["Replikationsbeziehungen verwalten"](#)

Verwalten Sie Ihre Replikationsbeziehungen in NetApp Workload Factory

Verwalten Sie Ihre Replikationsbeziehungen in NetApp Workload Factory. Sie können Replikationsbeziehungen zwischen Quell- und Ziel-Volumes anhalten, fortsetzen, umkehren, stoppen und löschen. Außerdem können Sie den Replikationszeitplan des Quell-Volumes ändern und die maximale Transferrate für Ihre Replikationsbeziehungen begrenzen.

Änderung des Replikationszeitplans eines Quell-Volumes

Änderung des Replikationszeitplans des Quell-Volumes in einer Replikationsbeziehung in NetApp Workload Factory.

Die Häufigkeit der Übertragung von Snapshots vom Quell-Volume auf das replizierte Volume richtet sich nach den erforderlichen Recovery Point Objectives (RPOs).

Wenn ein lokaler ONTAP Cluster das Ziel der Replikationsbeziehung ist, kann der Replikationszeitplan nicht geändert werden.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Storage**.
3. Im Menü „Storage“ erfolgt die Auswahl von **Inventory**.
4. In **Inventory** wird das Aktionsmenü des zu aktualisierenden Dateisystems und anschließend **Manage** ausgewählt.
5. Wählen Sie in der Dateisystemübersicht die Registerkarte **Replikationsbeziehungen** aus.
6. Auf der Registerkarte „Replikationsbeziehungen“ können Sie das Aktionsmenü des Zeitplans der Replikationsbeziehung auswählen, der geändert werden soll.
7. Die Auswahl erfolgt über **Replikationsintervall bearbeiten**.
8. Im Dialogfeld „Replikationsintervall bearbeiten“ lässt sich die Häufigkeit der Snapshot-Übertragung vom Quell-Volumen auswählen. Zur Auswahl stehen die folgenden Häufigkeiten:
 - Alle 5 Minuten
 - Stündlich
 - Alle 8 Stunden
 - Täglich
 - Wöchentlich
9. **Anwenden** auswählen.

Begrenzung der maximalen Transferrate einer Replikationsbeziehung

Die Begrenzung der maximalen Transferrate ist optional, aber empfehlenswert. Ohne eine Begrenzung könnten die Netzwerk- und Applikations-Performance sinken.

Alternativ empfehlen wir für kritische Workloads, beispielsweise solche, die primär für die Notfallwiederherstellung verwendet werden, eine unbegrenzte Transferrate für FSx for ONTAP Dateisysteme.

Bevor Sie beginnen

Dabei ist zu berücksichtigen, wie viel Bandbreite für die Replikation zugewiesen werden soll.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Storage**.
3. Im Menü „Storage“ erfolgt die Auswahl von **Inventory**.
4. In **Inventory** wird das Aktionsmenü des zu aktualisierenden Dateisystems und anschließend **Manage** ausgewählt.
5. Wählen Sie in der Dateisystemübersicht die Registerkarte **Replikationsbeziehungen** aus.
6. Auf der Registerkarte „Replikationsbeziehungen“ ist das Aktionsmenü der Replikationsbeziehung auszuwählen, für die die maximale Transferrate begrenzt werden soll.
7. Danach erfolgt die Auswahl von **Maximale Transferrate bearbeiten**.
8. Im Dialogfeld „Maximale Transferrate bearbeiten“ wird **Begrenzt** ausgewählt und das maximale Übertragungslimit in MB/s eingegeben.

Alternativ können Sie **Unbegrenzt** auswählen.

9. **Anwenden** auswählen.

Snapshot-Daten in einer Replikationsbeziehung manuell aktualisieren

Eine Replikationsbeziehung verfügt über einen festgelegten Replikationszeitplan, aber Sie können die zwischen Quell- und Ziel-Volumes übertragenen Snapshot-Daten in NetApp Workload Factory jederzeit manuell aktualisieren.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Storage**.
3. Im Menü „Storage“ erfolgt die Auswahl von **Inventory**.
4. In **Inventory** wird das Aktionsmenü des zu aktualisierenden Dateisystems und anschließend **Manage** ausgewählt.
5. Wählen Sie in der Dateisystemübersicht die Registerkarte **Replikationsbeziehungen** aus.
6. Auf der Registerkarte „Replikationsbeziehungen“ das Aktionsmenü der zu aktualisierenden Replikationsbeziehung auswählen.
7. Wählen Sie **Aktualisieren**.
8. Im Dialogfeld „Aktualisieren“ wählen Sie **Aktualisieren** aus.

Replikationsbeziehung unterbrechen

Durch das Anhalten einer Replikationsbeziehung werden geplante Replikationsaktualisierungen vom Quell-Volume zum Ziel-Volume beendet. Das Ziel-Volume wechselt von schreibgeschützt zu lesen/schreiben. Beide Volumes verwenden weiterhin den neuesten Replikations-Snapshot als neue Basis für die spätere Resynchronisierung.

Bevor Sie beginnen

Wenn Sie eine laufende Übertragung anhalten, bleibt die Übertragung davon unberührt, und die Beziehung wechselt bis zum Abschluss der Übertragung in den Status „Quiescing“. Wenn die aktuelle Übertragung abbricht, ist sie nun eine zukünftige Übertragung und wird nicht neu gestartet.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Storage**.
3. Im Menü „Storage“ erfolgt die Auswahl von **Inventory**.
4. In **Inventory** wird das Aktionsmenü des zu aktualisierenden Dateisystems und anschließend **Manage** ausgewählt.
5. Wählen Sie in der Dateisystemübersicht die Registerkarte **Replikationsbeziehungen** aus.
6. Auf der Registerkarte „Replikationsbeziehungen“ können Sie im Aktionsmenü die Replikationsbeziehung auswählen, die angehalten werden soll.
7. **Pause (Quiesce)** ist auszuwählen.
8. Im Dialogfeld **Beziehung stilllegen** wählen Sie die Option **Stilllegen**.

Ergebnis

Die Beziehung wird angehalten, und ihr Status lautet „Pausiert“.

Eine pausierte Replikationsbeziehung fortsetzen

Wenn Sie eine Replikationsbeziehung wiederherstellen, werden alle Änderungen am Ziel-Volume, die während der Unterbrechung der Replikation vorgenommen wurden, gelöscht. Das Ziel-Volume wechselt vom lesen/schreiben in den Nur-Lese-Modus und empfängt wieder Aktualisierungen vom Quell-Volume im geplanten Replikationsintervall.



Alle Daten, die zwischen der letzten Datenreplizierung und dem Zeitpunkt, zu dem das ursprüngliche Quell-Volume deaktiviert wird, auf das ursprüngliche Quell-Volume geschrieben werden, bleiben nicht erhalten.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Storage**.
3. Im Menü „Storage“ erfolgt die Auswahl von **Inventory**.
4. In **Inventory** wird das Aktionsmenü des zu aktualisierenden Dateisystems und anschließend **Manage** ausgewählt.
5. Wählen Sie in der Dateisystemübersicht die Registerkarte **Replikationsbeziehungen** aus.
6. Auf der Registerkarte „Replikationsbeziehungen“ erfolgt die Auswahl der fortzusetzenden

Replikationsbeziehung über das Aktionsmenü.

7. **Resume** wird ausgewählt.
8. Im Dialogfeld „Resume relationship“ **Resume** auswählen.

Ergebnis

Die Beziehung wird fortgesetzt, und ihr Status wird als "Replicated" angezeigt.

Umkehrung einer Replikationsbeziehung

Eine Replikationsbeziehung umkehren, sodass das Ziel-Volume zum Quell-Volume wird.

Folgende umgekehrte Operationen werden unterstützt:

- Zwei FSx für ONTAP Dateisysteme
- Ein FSx for ONTAP Dateisystem und ein lokales ONTAP System

Nachdem Sie die Replikation angehalten und Änderungen am Ziel-Volume vorgenommen haben, können Sie diese Änderungen zurück auf das Quell-Volume replizieren. Dieser Vorgang ist in einem Disaster-Recovery-Szenario üblich, in dem Sie eine Zeit lang auf dem Ziel-Volume arbeiten und anschließend die Rollen der Volumes wechseln möchten.

Wenn Sie eine Replikation umkehren und fortsetzen, werden die Quell- und Zielrollen Ihrer Volumes vertauscht; das Ziel-Volume wird zum neuen Quell-Volume und das Quell-Volume zum neuen Ziel-Volume. Der Umkehrvorgang überschreibt außerdem den Inhalt des neuen Ziel-Volumes mit dem Inhalt des neuen Quell-Volumes. Wenn Sie eine Replikation zweimal umkehren, stellt sich die ursprüngliche Replikationsrichtung wieder her.

HINWEIS:

- Alle Daten, die zwischen der letzten Datenreplizierung und dem Zeitpunkt, zu dem das ursprüngliche Quell-Volume deaktiviert wird, auf das ursprüngliche Quell-Volume geschrieben werden, bleiben nicht erhalten.
- Die umgekehrte Replikation ist beim Replizieren von Storage-VM-Daten und Konfigurationseinstellungen nicht verfügbar.

Bevor Sie beginnen

Es ist wichtig, dass Sie die aktuelle und zukünftige Rolle Ihrer Quell- und Ziel-Volumes kennen, da Änderungen auf dem neuen Ziel-Volume durch das neue Quell-Volume überschrieben werden. Bei falscher Verwendung kann es zu unbeabsichtigtem Datenverlust kommen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Storage**.
3. Im Menü „Storage“ erfolgt die Auswahl von **Inventory**.
4. In **Inventory** wird das Aktionsmenü des zu aktualisierenden Dateisystems und anschließend **Manage** ausgewählt.
5. Wählen Sie in der Dateisystemübersicht die Registerkarte **Replikationsbeziehungen** aus.

6. Auf der Registerkarte „Replikationsbeziehungen“ ist das Aktionsmenü der Replikationsbeziehung auszuwählen, die umgekehrt werden soll.
7. Die Auswahl erfolgt über **Reverse relationship**.
8. Im Dialogfeld „Beziehung umkehren“ erfolgt die Auswahl der Option **Umkehren**.

Eine Replikationsbeziehung beenden

Eine Replikationsbeziehung in NetApp Workload Factory wird beendet. Geplante Replikationsaktualisierungen vom Quellvolume zum Ziel-Volume werden dadurch angehalten. Das Ziel-Volume wechselt von schreibgeschützt zu lesen/schreiben.

Schritte

1. Melden Sie sich bei der "NetApp Console" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Storage**.
3. Im Menü „Storage“ erfolgt die Auswahl von **Inventory**.
4. In **Inventory** wird das Aktionsmenü des zu aktualisierenden Dateisystems und anschließend **Manage** ausgewählt.
5. Wählen Sie in der Dateisystemübersicht die Registerkarte **Replikationsbeziehungen** aus.
6. Auf der Registerkarte „Replikationsbeziehungen“ können Sie das Aktionsmenü der Replikationsbeziehung auswählen, die beendet werden soll.
7. **Break** auswählen.
8. Im Dialogfeld „Replikation unterbrechen“ wird die Option **Unterbrechen** ausgewählt.

Ergebnis

Der Replikationsstatus des Volumes ändert sich in **Broken**. Das Ziel-Volume wird beschreibbar.

Eine Replikationsbeziehung löschen

Löschen einer Replikationsbeziehung in NetApp Workload Factory. Beim Löschen einer Replikationsbeziehung wird die Replikationsbeziehung zwischen dem Quell- und dem Ziel-Volume entfernt. Nach dem Löschen der Replikationsbeziehung existieren beide Volumes weiterhin unabhängig voneinander mit den aktuell enthaltenen Daten.

Wenn Sie eine Replikationsbeziehung löschen, löscht FSx for ONTAP auch die gemeinsamen Replikations-Snapshots des Quell- und Ziel-Volume.

Schritte

1. Melden Sie sich bei der "NetApp Console" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Storage**.
3. Im Menü „Storage“ erfolgt die Auswahl von **Inventory**.
4. In **Inventory** wird das Aktionsmenü des zu aktualisierenden Dateisystems und anschließend **Manage** ausgewählt.
5. Wählen Sie in der Dateisystemübersicht die Registerkarte **Replikationsbeziehungen** aus.
6. Auf der Registerkarte „Replikationsbeziehungen“ ist das Aktionsmenü der zu löschenden Replikationsbeziehung auszuwählen.

7. Wählen Sie **Delete**.
8. Im Dialogfeld „Beziehung löschen“ ist **Löschen** auszuwählen.

Schützen Sie Ihre FSx for ONTAP Daten mit NetApp Autonomous Ransomware Protection mit KI.

Schützen Sie Ihre Daten mit NetApp Autonomous Ransomware Protection mit KI (ARP/AI). Es werden Aktivitäten in NAS (NFS/SMB) und SAN-Umgebungen überwacht, um ungewöhnliches Verhalten zu erkennen, das auf einen Ransomware-Angriff hindeuten könnte. Wenn eine Bedrohung erkannt wird, erstellt ARP/AI automatisch neue unveränderliche Snapshots, sodass Ihre Daten wiederhergestellt werden können.

Über diese Aufgabe

ARP/AI dient zum Schutz vor Denial-of-Service-Angriffen, bei denen Angreifer Daten zurückhalten, bis ein Lösegeld gezahlt wird. ARP/AI bietet Echtzeit-Ransomware-Erkennung auf der Grundlage von:

- Identifizierung der eingehenden Daten als verschlüsselt oder im Klartext.
- Analysen, die Folgendes erkennen:
 - **Entropie:** Eine Bewertung der Zufälligkeit von Daten in einer Datei (wird sowohl in NAS als auch in SAN Umgebungen verwendet)
 - **Dateierweiterungstypen:** Eine Erweiterung, die nicht dem normalen Erweiterungstyp entspricht (nur in NAS-Umgebungen verwendet)
 - **Datei-IOPS:** Ein Anstieg ungewöhnlicher Volumenaktivität mit Datenverschlüsselung (wird nur in NAS-Umgebungen verwendet)

ARP/AI kann die Ausbreitung der meisten Ransomware-Angriffe bereits nach der Verschlüsselung einer geringen Anzahl von Dateien erkennen, automatisch Maßnahmen zum Schutz der Daten ergreifen und Sie darüber informieren, dass ein mutmaßlicher Angriff stattfindet.

Die ARP/AI-Funktion wird automatisch entsprechend der ONTAP Version aktualisiert, mit der Amazon FSx for NetApp ONTAP ausgeführt wird, sodass Sie keine manuellen Aktualisierungen vornehmen müssen.

Lern- und Aktivmodi

Das Verhalten von ARP/AI hängt vom Protokoll und vom Volume-Typ ab:

- **NAS Volumes (NFS/SMB):** ARP/AI ist sofort nach der Aktivierung aktiv. Es nutzt ein vortrainiertes KI-Modell, um Ransomware-Bedrohungen umgehend zu erkennen.
- **SAN Volumes (ab ONTAP 9.17.1):** ARP/AI bietet sofortigen Schutz, auch während der ersten Evaluierungsphase. Während dieses 2- bis 4-wöchigen Zeitraums lernt das System die normale Verschlüsselungsaktivität und legt Alarmschwellen fest. Gleichzeitig überwacht es weiterhin Ihre Daten, erkennt Bedrohungen und sendet Warnmeldungen.
- **Aktiver Modus:** Wenn der aktive Modus aktiviert ist, erstellt FSx for ONTAP ARP/AI-Snapshots, um Ihre Daten zu schützen, wenn eine mögliche Bedrohung erkannt wird.

Wenn das System eine Dateierweiterung als ungewöhnlich kennzeichnet, sollte die Warnung überprüft werden. Auf die Warnung kann reagiert werden, um die Daten zu schützen, oder sie kann als Fehlalarm markiert werden, falls die Aktivität erwartet wird.

Wenn Sie eine Warnung als Fehlalarm markieren, aktualisiert das System seine Warnungseinstellungen. Wenn beispielsweise eine neue Dateierweiterung eine Warnung auslöst und Sie diese als Fehlalarm

markieren, erhalten Sie beim nächsten Auftreten dieser Dateierweiterung keine Warnung.

Nicht unterstützte Konfigurationen

Die folgenden Konfigurationen unterstützen die Verwendung von ARP/AI nicht.

- NVMe Volumes
- iSCSI Volumes mit ONTAP Versionen vor 9.17.1

Aktivierung von ARP/AI für ein Dateisystem oder ein Volume

Durch die Aktivierung von ARP/AI für ein Dateisystem werden automatisch alle aktuellen und neuen NAS Volumes (NFS/SMB) geschützt. Ab ONTAP 9.17.1 werden auch SAN Volumes (iSCSI) unterstützt. ARP/AI kann auch für bestimmte Volumes aktiviert werden.

Wenn ARP/AI nach der Aktivierung einen tatsächlichen Angriff erkennt, erstellt Workload Factory automatisch eine Snapshot-Richtlinie. Diese Richtlinie kann bis zu sechs Snapshots alle vier Stunden erstellen. Jeder Snapshot ist für 2-5 Tage gesperrt.

Bevor Sie beginnen

Um ARP/AI für ein Dateisystem oder ein Volume zu aktivieren, muss eine Verknüpfung hergestellt werden. ["Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen"](#). Nach der Verknüpfung ist eine Rückkehr zu diesem Vorgang erforderlich.

Aktivierung von ARP/AI für ein Dateisystem

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Im Menü **FSx for ONTAP** wählen Sie **Inventory** und anschließend im Aktionsmenü des Dateisystems zum Aktivieren von ARP/AI **Manage** aus.
4. Unter Information erfolgt die Auswahl des Stiftsymbols neben **Autonomous Ransomware Protection**. Das Stiftsymbol erscheint neben dem Pfeil, wenn sich der Mauszeiger über der Zeile **Autonomous Ransomware Protection** befindet.
5. Auf der Seite NetApp Autonomous Ransomware Protection with AI (ARP/AI) sind folgende Schritte auszuführen:
 - a. Aktivierung oder Deaktivierung der Funktion.
 - b. **Automatische Snapshot-Erstellung**: Auswahl der maximalen Anzahl der aufzubewahrenden Snapshots und des Zeitintervalls zwischen den Snapshot-Erstellungen. Standardmäßig sind 6 Snapshots alle 4 Stunden festgelegt.
 - c. **Unveränderliche Snapshots**: Hier werden die Standardaufbewahrungsdauer in Stunden und die maximale Anzahl an Tagen ausgewählt, für die unveränderliche Snapshots aufbewahrt werden sollen. Diese Option wird aktiviert, um sicherzustellen, dass Snapshots erst nach Ablauf der angegebenen Aufbewahrungsdauer gelöscht oder geändert werden können.
 - d. **Erkennung**: Optional können Sie einen oder mehrere der folgenden Parameter auswählen, um automatisch nach Anomalien zu suchen und sie zu erkennen.
6. Zum Fortfahren ist die Annahme der Erklärung erforderlich.
7. Mit **Anwenden** werden die Änderungen gespeichert.

Aktivierung von ARP/AI für ein Volume

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Volumes explorer**.
3. Im Aktionsmenü des Volumes die Option zum Aktivieren von ARP/AI auswählen, dann **Data protection actions** und anschließend **Manage ARP/AI**.
4. Im Dialogfeld „Manage ARP/AI“ gehen Sie wie folgt vor:
 - a. Aktivierung oder Deaktivierung der Funktion.
 - b. **Erkennung**: Optional können Sie einen oder mehrere der folgenden Parameter auswählen, um automatisch nach Anomalien zu suchen und sie zu erkennen.
5. Zum Fortfahren ist die Annahme der Erklärung erforderlich.
6. Mit **Anwenden** werden die Änderungen gespeichert.

Validierung von Ransomware-Angriffen

Feststellung, ob es sich bei einem Angriff um einen Fehlalarm oder einen echten Ransomware-Vorfall handelt.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Im Menü **FSx for ONTAP** erfolgt zunächst die Auswahl von **Inventar** und anschließend die des Dateisystems, für das die Validierung auf Ransomware-Angriffe erfolgen soll.
4. In der Dateisystemübersicht erfolgt die Auswahl der Registerkarte **Volumes**.
5. Auf der Kachel **Autonomous Ransomware Protection** erfolgt die Auswahl von **Analyze attacks**.
6. Anhand des heruntergeladenen Berichts zu den Angriffseignissen lässt sich prüfen, ob Dateien oder Ordner kompromittiert wurden, und anschließend feststellen, ob ein Angriff stattgefunden hat.
7. Wenn kein Angriff stattgefunden hat, können Sie in der Tabelle für das entsprechende Volume **Fehlalarm** und anschließend **Schließen** auswählen.
8. Falls ein Angriff erfolgt ist, wählen Sie in der Tabelle für das Volume **Real attack** aus. Das Dialogfeld „Restore compromised volume data“ wird geöffnet. Sie können sofort mit [Ihre Daten wiederherstellen](#) fortfahren oder **Close** auswählen und später zurückkehren, um den Wiederherstellungsprozess abzuschließen.

Daten nach einem Ransomware-Angriff wiederherstellen

Wenn das System einen möglichen Angriff erkennt, erstellt und sperrt es eine Momentaufnahme des Volumes zu diesem Zeitpunkt.

Falls der Angriff später bestätigt wird, können Sie die betroffenen Dateien oder das gesamte Volume aus dem Snapshot wiederherstellen.

Gesperrte Snapshots können erst nach Ablauf der Aufbewahrungsfrist gelöscht werden. Wenn sich der Angriff später als Fehlalarm herausstellt, wird der gesperrte Snapshot gelöscht.

Da das System die betroffenen Dateien und den Zeitpunkt des Angriffs identifiziert, ist es möglich, nur die

betroffenen Dateien aus verfügbaren Snapshots wiederherzustellen, anstatt das gesamte Volume wiederherzustellen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Im Menü **FSx for ONTAP** erfolgt die Auswahl von **Inventory** und anschließend des Dateisystems, für das Daten wiederhergestellt werden sollen.
4. In der Dateisystemübersicht erfolgt die Auswahl der Registerkarte **Volumes**.
5. Auf der Kachel **Autonomous Ransomware Protection** erfolgt die Auswahl von **Analyze attacks**.
6. Wenn ein Angriff stattgefunden hat, erfolgt in der Tabelle für das entsprechende Volume die Auswahl von **Echter Angriff**.
7. Im Dialogfeld „Daten eines kompromittierten Volumes wiederherstellen“ sind die Anweisungen zum Wiederherstellen auf Dateiebene oder auf Volume-Ebene zu befolgen. In den meisten Fällen werden Dateien und nicht ein gesamtes Volume wiederhergestellt.
8. Nach Abschluss der Wiederherstellung kann **Schließen** ausgewählt werden.

Ergebnis

Die kompromittierten Daten wurden wiederhergestellt.

Klonen eines Volumes in NetApp Workload Factory

In NetApp Workload Factory lässt sich ein Volume klonen, um für Tests ein lesen/schreiben Volume des ursprünglichen Volumes zu erstellen.

Der Klon spiegelt den aktuellen, zeitpunktgenauen Stand der Daten wider. Sie können Klone auch verwenden, um zusätzlichen Benutzern Zugriff auf Daten zu gewähren, ohne ihnen Zugriff auf Produktionsdaten zu gewähren.

Über diese Aufgabe

Volume-Klonen wird nur für FlexClone Volumes unterstützt.

Beim Klonen eines Volumes wird ein beschreibbares Volume mit Verweisen auf Snapshots des übergeordneten Volumes erstellt. Die Klonerstellung erfolgt innerhalb weniger Sekunden. Die geklonten Daten befinden sich nicht auf dem geklonten Volume, sondern auf dem übergeordneten Volume. Alle nach der Klonerstellung in das Volume geschriebenen neuen Daten befinden sich auf dem Klon.

Damit ein geklontes Volume alle Daten des übergeordneten Volumes sowie alle nach der Erstellung zum Klon hinzugefügten neuen Daten enthält, müssen Sie ["den Klon aufteilen"](#) den Klon vom übergeordneten Volume trennen. Außerdem können Sie ein übergeordnetes Volume nicht löschen, wenn es einen Klon hat. Ein Klon muss aufgeteilt werden, bevor ein übergeordnetes Volume gelöscht werden kann.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Volumes explorer**.
3. Wählen Sie das Aktionsmenü des Volumes aus, das geklont werden soll.

4. Zuerst **Datenschutzaktionen**, dann **Volume klonen** auswählen.
5. Im Dialogfeld „Volume klonen“ können Sie einen Namen für den Volume-Klon eingeben.
6. Wählen Sie **Clone** aus.

Schützen Sie Ihre FSx for ONTAP Daten mit einem Cyber-Tresor

Ein Cyber-Vault-Volume ist ein isolierter, sicherer Storage-Bereich zum Speichern von Sicherungskopien Ihrer Daten, der sie vor Ransomware-Angriffen und anderen Cyberbedrohungen schützt. Zur Vault-Erstellung gehören das Erstellen eines Cyber-Vault-Volumes, das Deaktivieren aller Client-Protokolle, das Einrichten einer Replikationsbeziehung zwischen dem Quell-Volume und dem Cyber-Vault-Volume sowie das Erstellen unveränderlicher Snapshots auf dem Cyber-Vault-Volume.

Was ist ein Cyber-Vault?

Ein Cyber-Vault ist eine spezielle Methode zum Schutz von Daten, bei der kritische Daten in einer isolierten Umgebung getrennt von der primären IT-Infrastruktur gespeichert werden.

Der Cyber-Vault ist ein vom Netzwerk isolierter, unveränderlicher und unauslöschlicher Datenspeicher, der vor Bedrohungen des Hauptnetzwerks wie Malware, Ransomware oder Insider-Bedrohungen geschützt ist. Ein solcher Cyber-Vault lässt sich durch unveränderliche und unauslöschliche Snapshots realisieren.

Bei herkömmlichen Methoden für Air-Gap-Backups werden Speicherplatz geschaffen und primäre und sekundäre Speichermedien physisch getrennt. Durch die Auslagerung der Speichermedien an einen externen Standort und/oder die Unterbrechung der Verbindung haben Angreifer keinen Zugriff auf die Daten. Dies schützt die Daten, kann aber zu längeren Wiederherstellungszeiten führen.

FSx for ONTAP Cyber-Vaults

Amazon FSx for NetApp ONTAP wird als Cyber-Vault-Quelle und -Ziel unterstützt.

Implementierung

Workload Factory unterstützt Sie bei der Erstellung einer Cyber-Vault-Architektur. Nachdem Sie NetApp kontaktiert haben, um Ihr Interesse an der Implementierung eines Cyber-Vault auszudrücken, nimmt ein NetApp Spezialist Kontakt mit Ihnen auf, um Ihre Anforderungen zu besprechen.

Zum Einstieg senden Sie eine E-Mail an ng-FSx-CyberVault@netapp.com.

Verwandte Informationen

Weitere Informationen zu Cyber-Vaults und zur Einrichtung dieser Architektur finden Sie im ["ONTAP Cyber-Vault-Dokumentation"](#).

FSx für ONTAP in Workload Factory verwalten

Analysieren Sie FSx for ONTAP-Ereignisse in NetApp Workload Factory

Identifizieren und beheben Sie Dateisystemprobleme von FSx for ONTAP schnell mit dem intelligenten Ereignisanalysator in NetApp Workload Factory. Der Ereignisanalysator extrahiert und analysiert automatisch FSx for ONTAP Event Management System (EMS)- und Latenzereignisse und nutzt dabei Agentic AI mit Amazon Bedrock-Integration.

Über diese Aufgabe

Speicheradministratoren reagieren auf FSx for ONTAP-Ereignisse oft erst nach Kundenbeschwerden oder durch die Pflege benutzerdefinierter Skripte und Alarmer. Dieser reaktive Ansatz kann die Effizienz verringern, die Problemlösung verzögern und Ausfallzeiten erhöhen.

Der Ereignisanalysator extrahiert automatisch die folgenden Ereignistypen aus FSx for ONTAP-Dateisystemen:

- **EMS-Ereignisse:** Fehler-, Alarm- und Notfallereignisse aus dem ONTAP Event Management System.
- **Latenzereignisse:** Lese- und Schreiblatenzereignisse. Latenzereignisse können ohne eine Linkverbindung angezeigt werden.

Mit der Amazon Bedrock-Integration verwendet Workload Factory KI, um Ereignisse zu analysieren und umsetzbare Erkenntnisse bereitzustellen, damit die Integrität und Leistung Ihrer FSx for ONTAP File Systems erhalten bleibt.

Zu den wichtigsten Vorteilen gehören:

- **Erweiterte Fehlerbehebung:** KI identifiziert, analysiert und liefert automatisch Erkenntnisse zur Behebung von FSx for ONTAP EMS- und Latenzereignissen, wodurch manuelle Untersuchungszeit reduziert wird.
- **Bewährte Vorgehensweise zur Fehlerbehebung:** Der Ereignisanalysator liefert klare, umsetzbare Schritte zur Behebung von FSx for ONTAP EMS- und Latenzereignissen.

Bei der Verwendung des Ereignisanalysators haben Sie die volle Kontrolle über Ihre Umgebung, während Sie von fortschrittlichen KI-Analysen profitieren.

Damit Workload Factory Ereignisse analysieren kann, müssen Sie Amazon Bedrock aktivieren, das Modell auswählen, das Workload Factory verwendet, einen privaten Endpunkt zur Verbindung mit Amazon Bedrock erstellen, Berechtigungen hinzufügen und eine Enterprise-Lizenz erstellen.

"Preise für Amazon Bedrock"



Wenn Ihr Kontoadministrator die KI-Funktionen deaktiviert hat, wird eine Meldung angezeigt und die KI-Analyse kann nicht genutzt werden. Die Kontaktaufnahme erfolgt über Ihren Administrator oder ["Informationen zur KI-Administration"](#).

Datenschutz und Datensicherheit

Ihr Datenschutz und Ihre Sicherheit werden geschützt durch:

- **Datenhoheit:** Alle Daten und Aggregationen verbleiben innerhalb Ihres AWS-Kontos und werden über einen privaten VPC-Endpunkt (Amazon Bedrock) kommuniziert, ohne öffentliche Internetverbindung.
- **Kein KI-Training:** Kundendaten werden nicht zum Trainieren oder Verbessern von Modellen verwendet. Amazon Bedrock verarbeitet Ereignisse in Echtzeit, trainiert aber nicht mit Ihren Daten. Ergebnisse werden nur in Ihrer Umgebung gespeichert.

Weitere Einzelheiten finden Sie unter ["Amazon Bedrock Datenschutzdokumentation"](#).

Bevor Sie beginnen

Um Latenzereignisse anzuzeigen, sind die folgenden Schritte erforderlich:

- ["Berechtigungen für Ansicht, Planung und Analyse erteilen"](#) in Ihrem AWS-Konto.

- ["Verbindung zum Dateisystem über einen Link herstellen"](#).

Um EMS- und Latenzereignisse zu analysieren und KI-gestützte Erkenntnisse und Empfehlungen zu erhalten, stellen Sie Folgendes sicher:

- Sie haben ["Berechtigungen für Operationen und Fehlerbehebung"](#) in Ihrem AWS-Konto.
- Du hast ["über einen Link mit dem Dateisystem verbunden"](#).
- Port 22 (SSH) ist in der Sicherheitsgruppe geöffnet, die Ihrem FSx for ONTAP file system zugeordnet ist.

Zusätzliche Anforderungen (das System fordert Sie während der Ereignisanalyse dazu auf):

- **Amazon Bedrock Aktivierung**

Konfigurieren Sie die Amazon Bedrock APIs für jedes AWS-Konto. Die Amazon Bedrock APIs werden verwendet, um Einblicke in FSx for ONTAP-Ereignisse zu gewinnen.

Empfohlenes Modell: `anthropic.claude-sonnet-4-20250514-v1:0`. Geben Sie den ARN des Inferenzprofils für Ihre ausgewählte Region an.

- **Link zu Workload Factory**

Erstellen und verknüpfen Sie einen Link mit einem FSx for ONTAP-Dateisystem, um KI-gestützte Ereignisanalysen zu ermöglichen. Ein Link stellt eine Vertrauensbeziehung zwischen Workload Factory und einem oder mehreren FSx for ONTAP-Dateisystemen her und nutzt AWS Lambda.

["Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen"](#). Nach der Verknüpfung ist eine Rückkehr zu diesem Vorgang erforderlich.

- **AWS IAM Berechtigungen**

Fügen Sie der mit der Workload Factory IAM-Rolle verknüpften Richtlinie die folgenden Berechtigungen hinzu.

- `bedrock:InvokeModel`
- `bedrock:InvokeModelWithResponseStream`

Diese Berechtigungen ermöglichen Workload Factory, Bedrock-Modelle zur Fehleruntersuchung und Anleitung zur Behebung aufzurufen. Dieses Profil gewährleistet außerdem sicheren KI-Zugriff für maßgeschneiderte Erkenntnisse.

Fügen Sie außerdem die folgenden Berechtigungen für die mit Workload Factory verknüpften AWS credentials hinzu:

- `bedrock:GetInferenceProfile`
- `bedrock:ListInferenceProfiles`

Diese Berechtigungen bestätigen die Verfügbarkeit des Modells.

Ereignisse für FSx für ONTAP anzeigen und analysieren

Verwenden Sie die Workload Factory-Konsole, um EMS- und Latenzereignisse für FSx for ONTAP-Dateisysteme anzuzeigen und zu analysieren.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Im Menü „Storage“ erfolgt die Auswahl von **Analysis**.
4. Wählen Sie im Analysebildschirm die AWS-Konten, Anmeldeinformationen und Regionen aus, die die FSx for ONTAP-Dateisysteme enthalten, die Sie anzeigen möchten.

Es werden nur FSx for ONTAP-Dateisysteme angezeigt, die Ereignisse enthalten.

5. Wählen Sie das FSx for ONTAP-Dateisystem aus, das Sie anzeigen möchten.

Die Ereignistabelle zeigt alle Ereignisse für dieses Dateisystem an.

6. Prüfen Sie die Ereignisdetails in der Tabelle.
7. Um Ereignisse zu analysieren, gehen Sie wie folgt vor:
 - Um mehrere Ereignisse zu analysieren, wählen Sie die Kontrollkästchen neben den Ereignissen aus und wählen Sie dann **Analysieren** in der Tabelle.
 - Um ein Ereignis zu analysieren und Erkenntnisse im Seitenbereich anzuzeigen, wählen Sie den Ereignisnamen aus und wählen Sie dann im Bereich **Analysieren** aus. Die Erkenntnisse und Empfehlungen werden im Bereich angezeigt.
 - Um ein einzelnes Ereignis aus der Tabelle zu analysieren, wählen Sie in der Ereigniszeile **Analysieren** aus und anschließend den Ereignisnamen, um die Erkenntnisse und Empfehlungen anzuzeigen.

Falls erforderlich, sind die Einrichtungsvoraussetzungen für die KI-Analyse anhand der Anweisungen auf dem Bildschirm zu vervollständigen, um fehlende Voraussetzungen zu erfüllen.

Verwandte Informationen

- ["Legen Sie Schwellenwerte für die Volumenlatenz in Workload Factory fest."](#)

Best Practices für Dateisysteme implementieren

Konfigurationsanalyse für FSx for ONTAP Dateisysteme

NetApp Workload Factory analysiert Amazon FSx for NetApp ONTAP-Dateisystemkonfigurationen regelmäßig, um festzustellen, ob Konfigurationsprobleme vorliegen. Werden Probleme gefunden, zeigt Workload Factory an, worin die Probleme bestehen, und erklärt, was geändert werden muss, damit Ihr Dateisystemspeicher optimale Leistung, Kosteneffizienz und die Einhaltung bewährter Verfahren erreicht.

Zu den wichtigsten Fähigkeiten gehören:

- Tägliche Konfigurationsanalyse
- Automatische Best-Practice-Validierungen
- Proaktive Beobachtbarkeit
- Erkenntnisse in die Praxis umsetzen
- AWS Well-Architected Framework Berater

So funktioniert es

Workload Factory analysiert täglich Ihre Workloads, die auf unterstützten Cloud-Speichersystem-Bereitstellungen ausgeführt werden. Die Analyse liefert den Status einer Well-Architected-Architektur, Erkenntnisse und Empfehlungen.

Nach Abschluss der täglichen Analyse werden die Konfigurationen im Well-architected Dashboard für die Bereitstellung als „optimiert“ oder „nicht optimiert“ angezeigt. Konfigurationsprobleme sind nach Kategorie sowie in einer Liste mit Problemen und Empfehlungen zu finden. Empfehlungen zu den Konfigurationsproblemen können überprüft werden. Workload Factory kann einige Probleme automatisch beheben, andere erfordern manuelle Eingriffe. In diesem Fall stellt Workload Factory detaillierte Anweisungen bereit, um die empfohlenen Änderungen umzusetzen.

Sie können die Analyse von Konfigurationen, die für Ihre Umgebungen nicht relevant sind, ausblenden. Dadurch werden unnötige Warnmeldungen und ungenaue Optimierungsergebnisse vermieden.

Es besteht auch die Möglichkeit, benutzerdefinierte Regeln in einfacher Sprache zu erstellen, um Ihre Umgebungen anhand der Standards Ihres Unternehmens und der NetApp Best Practices zu validieren. Regeln können mit einem Probelauf getestet und anschließend für die Ausführung in Ihren Umgebungen terminiert werden. ["Weitere Informationen zu benutzerdefinierten Regeln"](#).

Warum es wichtig ist

Workload Factory wendet Best Practices auf große Storage-, Datenbank- und VMware-Umgebungen an, indem kontinuierliche Bewertungen mit Empfehlungseinblicken und Fehlerbehebungen kombiniert werden. Automatisierte Korrekturen reduzieren menschliche Fehler, gewährleisten einheitliches Management und erhalten Leistung und Zuverlässigkeit über Ihre Workload-Infrastrukturen hinweg.

Analyseanforderungen

Für eine vollständige Dateisystemanalyse sind die folgenden Schritte erforderlich:

- Stellen Sie eine Verknüpfung her. Die Verknüpfungskonnektivität ermöglicht es Workload Factory, alle Dateisystemkonfigurationen wie Datenschutz und Leistung zu analysieren.

["Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen"](#).

- Gewähren Sie *view, planning, and analysis*-Berechtigungen in Ihrem AWS-Konto.

["Erfahren Sie, wie Sie einem AWS-Konto Berechtigungen erteilen"](#).

Bewährte Verfahren und Empfehlungen für Speicher-Workloads

Das gut strukturierte Dashboard bewertet Speicherkonfigurationen anhand der ONTAP Best Practices und des AWS Well-Architected Framework. Die Bewertung empfiehlt außerdem Verbesserungen und Fehlerbehebungen.

Die gut strukturierte Analyse kategorisiert Konfigurationen in den folgenden Säulen des Rahmenwerks: *Zuverlässigkeit, Sicherheit, operative Exzellenz, Kostenoptimierung und Leistungseffizienz*.

Zuverlässigkeit

Zuverlässigkeit gewährleistet, dass Arbeitslasten ihre beabsichtigten Funktionen korrekt und konsistent erfüllen, selbst wenn es zu Störungen kommt.

- **Volume Backups**

Die Sicherung Ihrer Volumes unterstützt die Einhaltung von Aufbewahrungs- und Compliance-Anforderungen. Verwenden Sie Volume-Backups, um automatisierte Backups und Aufbewahrung für Ihre Daten einzurichten.

- **Snapshot Policy**

Lokale Snapshots für effiziente Datensicherung und schnelle Wiederherstellung einplanen. Snapshots sind sofortige, zeitpunktgenaue Abbilder Ihrer Volumes. Diese Empfehlung gilt nicht für Datenbankumgebungen.

- **Applikationskonsistente Snapshots**

Für Datenbankumgebungen empfiehlt sich die Verwendung applikationskonsistenter Snapshots mit NetApp SnapCenter, um präzise und zuverlässige Momentaufnahmen Ihrer Volume-Daten zu einem bestimmten Zeitpunkt zu erstellen. Dadurch laufen Ihre Anwendungen reibungslos und Ihre Daten bleiben sicher. SnapCenter vereinfacht die Erstellung von Backups und unterstützt die schnelle und korrekte Wiederherstellung von Daten, wodurch Ausfallzeiten reduziert und Ihre wichtigsten Workloads geschützt werden.

- **Regionenübergreifende Replikation**

Die regionsübergreifende Replikation stellt sicher, dass Ihre Daten in eine andere AWS-Region repliziert werden, was eine erhöhte Datenbeständigkeit und Verfügbarkeit bietet. Die Einrichtung der regionsübergreifenden Replikation unterstützt Notfallwiederherstellung und Compliance.

- **SSD-Kapazitätsreserve**

Die SSD-Speicherebene sollte eine Auslastung von maximal 80 % nicht überschreiten. Dies kann sich auf Lese- und Schreibvorgänge auf Ihrer Kapazitätspool-Speicherebene auswirken und die Durchsatzkapazität Ihres Dateisystems beeinträchtigen. Wenn die Kapazität erschöpft ist, werden Datenvolumes schreibgeschützt. Dienste, die versuchen, neue Daten zu schreiben, schlagen ebenfalls fehl.

- **Replikationsrichtlinienbezeichnungen**

Die Snapshot-Richtlinienbezeichnungen des Quellvolumes und die Replikationsrichtlinienbezeichnungen müssen übereinstimmen, um die Datenzuverlässigkeit zu gewährleisten.

- **Dateiobjektkapazität**

Um die Speicherkapazitätsgrenze des Volumes nicht zu erreichen, sollte der Schwellenwert für die Dateikapazität erhöht werden. Eine geringe Dateikapazität (Inodes) verhindert das Schreiben weiterer Daten auf das Volume. Workload Factory empfiehlt, die Dateikapazitätsauslastung unter 80 % zu halten, um die Erstellung neuer Dateien zu ermöglichen.

Sicherheit

Sicherheit betont den Schutz von Daten, Systemen und Vermögenswerten durch Risikobewertungen und Risikominderungsstrategien.

- **Schutz vor Ransomware (ARP/AI)**

NetApp Autonomous Ransomware Protection mit KI (ARP/AI) hilft, Ihre Volumes vor Ransomware-Bedrohungen zu schützen. Workload Factory empfiehlt, ARP/AI für alle Volumes zu aktivieren.

- **Nicht autorisierter iSCSI-Volume-Zugriff**

Volumes, die Anwendungsdaten über iSCSI bereitstellen, sollten nicht gleichzeitig NAS-Zugriff ermöglichen. Workload Factory empfiehlt, iSCSI-Volumes von der Verwendung anderer Protokolle auszuschließen.

Operative Exzellenz

Operative Exzellenz konzentriert sich auf die Bereitstellung der optimalsten Architektur und des größten Geschäftswerts.

- **Automatisches Kapazitätsmanagement**

Automatisches Kapazitätsmanagement sollte aktiviert werden, um regelmäßig sicherzustellen, dass die SSD-Ebene den Schwellenwert nicht überschreitet.

- **Freier Volumenkapazitätsspielraum**

Die Volume-Auslastung sollte unter 80 % gehalten werden, um potenzielle Auswirkungen auf das Lesen/Schreiben von Anwendungen zu vermeiden. Die Kapazität kann manuell oder mit der automatischen Vergrößerung des Volumens erhöht werden.

- **FlexCache Schreibmodus**

Für optimale Leistung sollte der Schreibmodus der Cache-Beziehung am besten an Ihre Arbeitslast angepasst werden. Der Write-Around-Modus bietet eine bessere Leistung bei leseintensiven Arbeitslasten mit kleinen Dateien, während der Write-Back-Modus eine bessere Leistung bei schreibintensiven Arbeitslasten mit großen Dateien bietet.

- **FlexCache Replika-Größe**

Automatische Größenanpassung und Scrubbing auf Cache-Volumes sorgen für eine optimale Größe und richten den Cache auf häufig genutzte Daten aus, was eine maximale Effizienz ermöglicht.

- **Für den Host sichtbare Kapazitätsberichterstattung**

Die host-sichtbare Kapazitätsberichterstattung ermöglicht eine bessere Transparenz der Speichernutzung auf Volume-Ebene.

- **Betriebssystem (OS) Typ**

Bestätigen Sie, dass der Wert für den Betriebssystemtyp (OS) der ONTAP LUN mit dem Partitionierungsschema des Betriebssystems übereinstimmt, um eine E/A-Ausrichtung zu erreichen. Eine fehlerhafte Konfiguration kann die Leistung verringern.

- **Speicherplatzmanagement für Blockgeräte**

Blockgerätespeicher-Einstellungen für von Datenbank-Hostinstanzen verwendete LUNs konfigurieren, um Schreibfehler zu vermeiden und die Speichereffizienz auf FSx for ONTAP zu verbessern. Diese Konfiguration gilt für die empfohlene Kombination von Einstellungen für Thin-Provisioned Volumes: Speicherplatzreservierung, Speicherplatzzuweisung und fraktionelle Reserve.

- **Thin Provisioning**

Thin Provisioning für FSx for ONTAP Volumes, die Datenbankinstanzen hosten, konfigurieren. Mit diesem Ansatz kann mehr logische Daten gespeichert werden, als physisch verfügbar sind.

Kostenoptimierung

Kostenoptimierung hilft Ihnen, den größtmöglichen Nutzen für Ihr Unternehmen zu erzielen und gleichzeitig die Kosten niedrig zu halten.

- **Kalte Datenauslagerung**

Cold-Data-Tiering aktivieren, um die Auslastung der SSD-Speicher-Tier zu reduzieren. Eine Tiering-Richtlinie auf jedes Volume anwenden, das auf allgemeine Datenspeicherung ausgerichtet ist. Für Datenbank-Volumes Cold-Data-Tiering dort aktivieren, wo es angemessen ist. FSx for ONTAP scannt die Daten kontinuierlich nach kalten Daten und verschiebt diese ohne Unterbrechung in die Capacity Pool-Tier.

- **Speichereffizienzen**

Speichereffizienzmaßnahmen wie Verdichtung, Komprimierung und Deduplizierung ermöglichen eine optimierte Speicherauslastung und eine Reduzierung der Kosten der SSD-Ebene.

- **Ablauf der Backups**

Alle manuell erstellten Backups von gelöschten Volumes sowie alle Backups, die älter als zwei Wochen sind, sollten gelöscht werden. Diese Backups verfallen nicht automatisch, können die Kosten erhöhen und die Komplexität steigern, wenn sie nicht mehr für SLA oder Wiederherstellung benötigt werden.

- **Ablauf der Snapshot**

Alte oder manuell erstellte Snapshots, die nicht mehr benötigt werden, können gelöscht werden. Das Entfernen dieser Snapshots kann Kosten senken und die Datenmenge reduzieren, insbesondere wenn sie nicht für die SLA oder Wiederherstellungsanforderungen erforderlich sind.

- **Inaktive Blockgeräte**

Wenn ein Blockgerät sieben Tage lang nicht verwendet wird, empfiehlt es sich, die Blockgerätedaten zu archivieren oder das ungenutzte Blockgerät zu löschen, um Kosten zu senken.

- **Überdimensionierte SSD-Kapazität**

Überschüssige SSD-Kapazität verursacht unnötige Kosten. Die SSD-Ebene kann reduziert werden, während ein freier Speicherplatzpuffer von 20 % beibehalten wird. Der Vorgang kann Stunden bis Tage dauern, und während dieser Zeit werden keine anderen Dateisystemoperationen unterstützt.

- **Inaktive NAS-Volumes**

Die Konfigurationsanalyse identifiziert NAS Volumes, die nicht aktiv genutzt werden, und schlägt vor, die Volumes zu löschen oder zu archivieren, um Kosten zu reduzieren.

Performance-Effizienz

Leistungseffizienz trägt dazu bei, dass Ihre Speicherressourcen effektiv genutzt werden und Arbeitslasten optimal ausgeführt werden.

- **FlexGroup Volumes-Ausgleich**

Rebalancieren Sie Ihre FlexGroup Volumes, um die Effizienz zu verbessern. Nach dem Scale-out kann die Kapazitäts- und Arbeitslastverteilung innerhalb des Volumes ungleichmäßig werden.

- **FlexVol Volumes-Ausgleich**

Rebalancieren Sie Ihre FlexVol Volumes, um die Effizienz zu verbessern. Nach dem Scale-out kann die Kapazitäts- und Arbeitslastverteilung innerhalb des Volumes ungleichmäßig werden.

Was kommt als Nächstes

["Gut strukturierte Dateisystemkonfigurationen implementieren"](#)

Gut strukturierte FSx for ONTAP Dateisystemkonfigurationen implementieren

Mit Workload Factory lassen sich Best Practices für Ihre FSx for ONTAP Dateisysteme umsetzen. Der Well-Architected-Status kann einfach überprüft werden, und Probleme mit Ihren Konfigurationen können erkannt und behoben werden, um die Architektur aller Systeme zu verbessern, die nicht für Zuverlässigkeit, Sicherheit, Effizienz, Performance und Kosten optimiert sind.

["Informationen zur Konfigurationsanalyse und zum Well-Architected-Status."](#)

Über diese Aufgabe

Workload Factory analysiert täglich die Bereitstellungsconfigurationen des Amazon FSx for NetApp ONTAP-Dateisystems.

Da die Anforderungen an Speicherkonfigurationen variieren, kann die Analyse bestimmter Konfigurationen, die für Ihre Speicherumgebung nicht relevant sind, ausgeschlossen werden.

Die Link-Konnektivität ermöglicht es Workload Factory, Probleme mit Leistung, Datenschutz und Konfigurationen zu erkennen. ["Verbindung zu einem FSx for ONTAP Dateisystem über einen Link herstellen"](#) für die umfassendste Analyse Ihrer Dateisystemressourcen.

Was analysiert wird

Workload Factory analysiert den gut entwickelten Status der folgenden Konfigurationen für FSx for ONTAP Dateisysteme:

- Zuverlässigkeit: Volume Backups, Snapshot-Richtlinie, regionsübergreifende Replikation, SSD-Kapazitätsreserve, Replikationsrichtlinienbezeichnungen und Dateiobjektkapazität
- Sicherheit: Ransomware-Schutz (ARP/AI) und unautorisierter iSCSI-Volume-Zugriff
- Operative Exzellenz: automatisches Kapazitätsmanagement, Speicherplatzreserve für Volumes, FlexCache Write-Modus, FlexCache Replikatgröße, host-seitige Kapazitätsberichte, Betriebssystemtyp, Blockgeräte Speicherplatzmanagement und Thin Provisioning
- Kostenoptimierung: Kaltdaten-Tiering, Speichereffizienzen, Backup-Ablauf, Snapshot-Ablauf, inaktive Blockgeräte, überprovisionierte SSD-Kapazität und inaktive NAS-Volumes
- Leistungseffizienz: FlexGroup Volumes Rebalancierung und FlexVol Volumes Rebalancierung

Bevor Sie beginnen

- Sie müssen ["Berechtigungen für Operationen und Behebung gewähren"](#) in Ihrem AWS-Konto angemeldet sein.
- ["Verbindung zu einem FSx for ONTAP Dateisystem über einen Link herstellen"](#) für die umfassendste Analyse Ihrer Dateisystemressourcen.

Ein Konfigurationsproblem beheben

Sie können Konfigurationsprobleme für ein FSx for ONTAP Dateisystem oder für ausgewählte Volumes in einem Dateisystem beheben. Für die Behebung lassen sich eine oder mehrere Konfigurationen auswählen.

Korrekturmaßnahmen können zu Ausfallzeiten von Instanzen oder Serviceunterbrechungen führen. Jede Empfehlung sollte sorgfältig geprüft werden, bevor ein Konfigurationsproblem behoben wird.

Schritte

1. Melden Sie sich bei der "NetApp Console" an.
2. Im Menü , **Workloads > Well-architected > FSx for ONTAP** auswählen.
3. Für jede Konfiguration **Anzeigen und Reparieren** auswählen. Eine sorgfältige Prüfung der Empfehlung ist wichtig.

Die Empfehlung erläutert bewährte Vorgehensweisen und potenzielle Fallstricke nicht optimierter Konfigurationen.

4. Ressourcen auswählen und dann **Fix**.

Manche Reparaturvorgänge sind nur für bestimmte Operationen und nicht immer für mehr als eine Ressource verfügbar. Beispielsweise können Sie die Konfiguration möglicherweise nur für ein einzelnes Volume korrigieren, nicht aber für mehrere Volumes.

5. Die Maßnahmen geben Aufschluss über die Folgen dieser Korrektur, wie etwa Instanz-Ausfallzeiten oder Serviceunterbrechungen.
6. **Fix** auswählen, wenn Workload Factory die empfohlenen Änderungen anwenden soll.

Ergebnis

Der Reparaturvorgang wird gestartet. Im Menü „Kontoeinstellungen“ die Option „Tracker“ auswählen, um den Status des Vorgangs anzuzeigen.

Konfigurationsanalyse verwerfen

Eine Konfigurationsanalyse für eine oder mehrere Ressourcen wird unbegrenzt gestoppt. Die Analyse kann bei Bedarf erneut gestartet werden.

Abbrechen beendet die Konfigurationsanalyse für ein oder mehrere FSx for ONTAP Dateisysteme oder Volumes. Die Analyse kann jederzeit neu gestartet werden.

Eine Konfigurationsanalyse für Konfigurationen verwerfen

Schritte

1. Melden Sie sich bei der "NetApp Console" an.
2. Im Menü , **Workloads > Well-architected > FSx for ONTAP** auswählen.
3. Unter „Konfigurationen“ die Konfiguration identifizieren, die nicht auf Ihre Umgebung zutrifft.
4. Wählen Sie **...** und dann **Verwerfen** aus.
5. Im Dialogfeld „Konfiguration verwerfen“ wählen Sie **Verwerfen**, um die Analyse für die Konfiguration zu stoppen.

Eine Konfigurationsanalyse für Ihre Ressourcen verwerfen

Schritte

1. Melden Sie sich bei der "NetApp Console" an.
2. Im Menü , **Workloads > Well-architected > FSx for ONTAP** auswählen.
3. Im FSx for ONTAP well-architected Dashboard unter Konfigurationen die Konfiguration auswählen, die nicht auf Ihre Umgebung zutrifft.
4. Auf der Konfigurationsseite die Ressource(n) auswählen, die aus der Konfigurationsanalyse entfernt werden sollen.
 - Für eine Ressource:  auswählen und anschließend **Verwerfen** wählen.
 - Für mehrere Ressourcen: Die Ressourcen auswählen und dann neben Bulk action auf **Dismiss** klicken.
5. Im Dialogfeld „Ressourcen verwerfen“ **Verwerfen** auswählen, um die Analyse zu beenden.

Ergebnis

Workload Factory stoppt die Konfigurationsanalyse für ausgewählte Konfigurationen.

Eine verworfene Konfigurationsanalyse reaktivieren

Eine verworfene Konfigurationsanalyse kann jederzeit reaktiviert werden. Sie können eine oder mehrere Konfigurationen oder Ressourcen reaktivieren.

Eine Konfigurationsanalyse für Konfigurationen reaktivieren

Schritte

1. Melden Sie sich bei der "NetApp Console" an.
2. Im Menü , **Workloads > Well-architected > FSx for ONTAP** auswählen.
3. Wählen Sie **Verworfen Konfigurationen** aus.
4. Identifizieren Sie die Konfiguration(en), die Sie reaktivieren möchten, und wählen Sie **Reaktivieren** aus.

Eine Konfigurationsanalyse für Ihre Ressourcen erneut aktivieren

Schritte

1. Melden Sie sich bei der "NetApp Console" an.
2. Im Menü , **Workloads > Well-architected > FSx for ONTAP** auswählen.
3. Im FSx for ONTAP well-architected Dashboard unter Konfigurationen die Konfiguration auswählen, die nicht auf Ihre Umgebung zutrifft.
4. Auf der Konfigurationsseite **Ausgeschlossene Konfigurationen** auswählen.
5. Wählen Sie die Ressource(n) aus, die reaktiviert werden sollen.
 - Für eine Ressource:  auswählen und dann **Reaktivieren** auswählen.
 - Für mehrere Ressourcen: Die Ressourcen auswählen und dann neben Bulk action auf **Reaktivieren** klicken.

Ergebnis

Workload Factory reaktiviert die Konfigurationsanalyse und führt jeden Tag eine neue Analyse durch.

Benutzerdefinierte Regeln

Informationen zu benutzerdefinierten Regeln in der NetApp Console

Mit benutzerdefinierten Regeln lassen sich im Well-architected Dashboard eigene Architekturstandards sowie NetApp Best Practices festlegen, überprüfen und durchsetzen.

Überblick

Mit dem Errichter können benutzerdefinierte Best-Practice-Regeln in einfacher Sprache erstellt werden. Diese Regeln werden für alle Ihre Ressourcen überprüft.

Individuelle Regeln helfen Ihnen, die Standards, Risikogrenzen und betrieblichen Anforderungen Ihrer Organisation durchzusetzen, Aspekte, die generische Anbieterregeln möglicherweise nicht vollständig abdecken.



Wenn Ihr Kontoadministrator die KI-Funktionen deaktiviert hat, ist der Rule builder nicht verfügbar und Sie können keine benutzerdefinierten Regeln erstellen. ["Informationen zur Verwaltung von KI-Funktionen"](#).

Funktionsweise benutzerdefinierter Regeln

Benutzerdefinierte Regeln nutzen einen KI-gestützten Prozess, der Ihre Anweisungen in natürlicher Sprache in klare, strukturierte Regeln umwandelt. Die KI fungiert als Übersetzer und Prüfer. Es wird eine Regel vorgeschlagen, erläutert, wie die Anfrage verstanden wurde, und um Zustimmung gebeten, bevor die Regel gespeichert oder eingeplant wird.

Dieser Prozess stellt sicher, dass:

- Die Regellogik ist klar definiert und auf Fehler überprüft.
- Es wird kein Freiformcode ausgeführt
- Sie können genau sehen, was bewertet wird, bevor Sie die Regel genehmigen

Einschränkungen

Für benutzerdefinierte Regeln gelten folgende Einschränkungen:

- Automatische Korrekturen sind nicht verfügbar. Nicht konforme Ressourcen sind anhand der bereitgestellten Anleitung selbst zu korrigieren.
- Jede Regel kann nur einen Ressourcentyp prüfen. Um mehrere Ressourcentypen zu prüfen, sind separate Regeln zu erstellen.
- Das kürzeste Auswertungsintervall beträgt 1 Stunde, um übermäßiges Scannen zu vermeiden.
- Regeln haben nur Lesezugriff und können keine Änderungen an Ihrer Umgebung vornehmen.

Regeldefinitionsmodell

Jede benutzerdefinierte Regel besteht aus den folgenden Komponenten:

Regelname

Ein benutzerdefinierter Name für die Regel.

Beschreibung

Ihre Begründung, warum diese Regel für Ihre Organisation wichtig ist.

Ressourcentyp

Die auszuwertende FSx-Ressource (Dateisystem, Volume oder Cache). Derzeit ein Ressourcentyp pro Regel.

Terminplaner

Wie oft die Regel ausgewertet wird (mindestens 1 Stunde, Standard 24 Stunden).

Bedingungslogik

Die zu prüfenden Kriterien.

Bewertungsumfang

Welche Ressourcen werden bewertet (alle relevanten Ressourcen im Geltungsbereich).

Sanierungslogik

Manuelle Anleitung zum Umgang mit nicht konformen Ressourcen.

Regellebenszyklus

Benutzerdefinierte Regeln durchlaufen die folgenden Zustände:

Entwurf

Es wird eine Regel erstellt. Es findet keine Auswertung statt.

Trockenlauf

Einmalige Auswertung zur Vorschau, welche Ressourcen betroffen wären. Wird zur Validierung vor der Terminplanung verwendet.

Geplant (Aktiviert)

Die Regel ist aktiv und wird gemäß dem festgelegten Zeitplan ausgeführt.

Deaktiviert

Die Regel ist pausiert, aber nicht gelöscht. Kann wieder aktiviert werden.

Gelöscht

Die Regel wurde dauerhaft entfernt.

Beispiele für benutzerdefinierte Regeln

Die folgenden Beispiele veranschaulichen gängige benutzerdefinierte Regeln:

Schutz des Produktionsvolumens

„Alle Volumes mit dem Tag ‚Prod‘ müssen über eine Snapshot-Richtlinie verfügen.“

Diese Regel erstellt automatisch Snapshots zum Schutz der Produktionsvolumina gemäß den Unternehmensanforderungen.

Archivvolumen Tiering

„Allen Volumes mit dem Tag ‚Archive‘ sollte die Tiering-Richtlinie auf ‚All‘ gesetzt sein.“

Diese Regel senkt die Kosten, indem archivierte Daten automatisch in kostengünstigeren Speicher verschoben werden.

Namensstandards für Dateisysteme

„Alle Dateisysteme müssen der Namenskonvention 'fsx-{environment}-{application}' folgen.“

Diese Regel validiert, dass Dateisysteme den organisatorischen Namenskonventionen entsprechen, was eine einfachere Verwaltung und Kostenverteilung ermöglicht.

Nächste Schritte

["Eine benutzerdefinierte Regel erstellen"](#)

Benutzerdefinierte Regel in NetApp Workload Factory erstellen

Benutzerdefinierte Regeln können durch Beschreibungen in einfacher Sprache erstellt werden. Der KI-Errichter in NetApp Workload Factory wandelt Ihre Anfrage in eine validierte Regel um, die Ihre FSx for ONTAP Ressourcen prüft.

Über diese Aufgabe

Der Regelerstellungsprozess führt Sie Schritt für Schritt durch die Regeldefinition, die Überprüfung der KI-Interpretation und die Ergebniskontrolle vor der Planung regelmäßiger Auswertungen. Sie behalten dabei in jedem Schritt die Kontrolle. Das System schlägt basierend auf Ihrer Eingabe eine Regel vor, aber nichts wird umgesetzt, bevor Sie sie bestätigen.



Wenn Ihr Kontoadministrator die KI-Funktionen deaktiviert hat, können Sie keine benutzerdefinierten Regeln erstellen. Eine Kontaktaufnahme ist über Ihren Administrator oder ["Informationen zur KI-Administration"](#) möglich.

Einschränkungen

Für benutzerdefinierte Regeln gelten folgende Einschränkungen:

- Automatische Korrekturen sind nicht verfügbar. Nicht konforme Ressourcen sind anhand der bereitgestellten Anleitung selbst zu korrigieren.
- Jede Regel kann nur einen Ressourcentyp prüfen. Um mehrere Ressourcentypen zu prüfen, sind separate Regeln zu erstellen.
- Das kürzeste Auswertungsintervall beträgt 1 Stunde, um übermäßiges Scannen zu vermeiden.
- Regeln haben nur Lesezugriff und können keine Änderungen an Ihrer Umgebung vornehmen.

Beispiele für benutzerdefinierte Regeln

Die folgenden Beispiele veranschaulichen gängige benutzerdefinierte Regeln:

Schutz des Produktionsvolumens

„Alle Volumes mit dem Tag ‚Prod‘ müssen über eine Snapshot-Richtlinie verfügen.“

Diese Regel erstellt automatisch Snapshots zum Schutz der Produktionsvolumina gemäß den Unternehmensanforderungen.

Archivvolumen Tiering

„Allen Volumes mit dem Tag ‚Archive‘ sollte die Tiering-Richtlinie auf ‚All‘ gesetzt sein.“

Diese Regel senkt die Kosten, indem archivierte Daten automatisch in kostengünstigeren Speicher verschoben werden.

Namensstandards für Dateisysteme

„Alle Dateisysteme müssen der Namenskonvention 'fsx-{environment}-{application}' folgen.“

Diese Regel validiert, dass Dateisysteme den organisatorischen Namenskonventionen entsprechen, was eine einfachere Verwaltung und Kostenverteilung ermöglicht.

Bevor Sie beginnen

Bevor Sie benutzerdefinierte Regeln erstellen und ausführen können, müssen Sie Folgendes haben:

- Sie haben AWS-Anmeldeinformationen mit Lesezugriff konfiguriert. "[AWS-Anmeldeinformationen zur Workload Factory hinzufügen](#)".
- Sie verfügen über ONTAP Zugangsdaten mit Anzeigeberechtigungen. "[ONTAP-Anmeldeinformationen zur Workload Factory hinzufügen](#)".
- Sie haben einen Link oder einen Console Agent für die Konnektivität zum Cloud Storage-System konfiguriert. "[Link erstellen und zuordnen](#)" oder "[einen Console Agent einsetzen](#)".
- Sie verstehen, dass die Erstellung benutzerdefinierter Regeln den Bedrock AI-Dienst von NetApp verwendet.

Regel erstellen

Mit dem Rule Errichter lassen sich benutzerdefinierte Best-Practice-Regeln in einfacher Sprache erstellen. Diese Regeln werden für alle Ihre Ressourcen geprüft.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Well-architected**.
3. Im Menü „Well-architected“ die Option **Rule builder** auswählen.

Wenn Sie den Errichter öffnen, werden Beispielaufforderungen angezeigt, die beim Schreiben Ihrer benutzerdefinierten Regel unterstützen. Es besteht die Möglichkeit, **Aufforderung kopieren** auszuwählen, um eine Beispielaufforderung in das Textfeld des KI-Dialogs zu übernehmen.

4. Geben Sie im Feld **Regel erstellen** Ihre Regelbeschreibung in natürlicher Sprache ein. Seien Sie so spezifisch wie möglich in Bezug auf:
 - Welcher Ressourcentyp überprüft wird (Dateisystem, Volume oder Cache).
 - Welche Bedingung validiert wird.

- Welcher Schwellenwert definiert die Compliance.
- Warum diese Regel wichtig ist (optional, aber empfohlen).

5. Wählen Sie .

Die KI analysiert Ihre Eingabeaufforderung und generiert eine Regeldefinition.

KI-Interpretation überprüfen

Der Regelgenerator zeigt Folgendes an:

- **Interpretation (geparst)**: Wie die KI Ihre Eingabeaufforderung in einfacher Sprache verstanden hat.
- **Regeldefinition**: Die strukturierte Regel einschließlich Ressourcentyp, Bedingungslogik und Auswertungskriterien.
- **Begründung**: Warum die KI Ihre Eingabeaufforderung auf diese Weise interpretiert hat.
- **Konfidenzindikator**: Wie sicher das System in der Interpretation ist.

Schritte

1. Die Interpretation sollte überprüft werden, um sicherzustellen, dass sie der beabsichtigten Bedeutung entspricht.

Zu prüfen ist, ob die Regeldefinition korrekt ist. Falls die Auslegung unklar oder fehlerhaft ist, kann das System Fragen stellen wie: * Welche Ressource sollte geprüft werden? * Welcher Wert oder Grenzwert definiert die Einhaltung? * Wie häufig sollte die Regel ausgeführt werden?

2. Antworten auf die klärenden Fragen der KI.

Die KI bittet Sie möglicherweise, aus mehreren Optionen auszuwählen, um Ihre Bedürfnisse besser zu verstehen. Jede Frage wird beantwortet und **Weiter** ausgewählt, oder **Überspringen** wird gewählt, um optionale Fragen zu überspringen.

3. Nachdem Sie alle Fragen beantwortet haben, wählen Sie **Weiter**, um Ihre Regel zu erstellen.

Testen der Regel

Vor der Planung der Regel kann ein einmaliger Test durchgeführt werden, um zu sehen, welche Ressourcen davon betroffen sind.

Schritte

1. **Regel validieren** auswählen.

Das System bewertet alle Ressourcen im Geltungsbereich anhand Ihrer Regellogik.

2. Validierungsergebnisse anzeigen:

- **Bewertete Ressourcen**: Gesamtzahl der überprüften Ressourcen
- **Konform**: Ressourcen, die die Regelkriterien erfüllen
- **Nicht konform**: Ressourcen, die die Kriterien nicht erfüllen
- **Fehlgeschlagene Auswertungen**: Ressourcen, die nicht ausgewertet werden konnten (mit Fehlerdetails)

3. Wenn einige Ressourcen die Auswertung nicht bestanden haben, können die Fehlerursachen eingesehen

werden:

- **AWS-Anmeldeinformationsfehler:** Leseberechtigungen reichen für bestimmte Ressourcen möglicherweise nicht aus
- **Verbindungsfehler:** Die Verbindung oder der Agent ist möglicherweise nicht für bestimmte Dateisysteme konfiguriert
- **ONTAP-Berechtigungsfehler:** Der Viewer-Benutzer hat möglicherweise keinen Zugriff auf bestimmte Ressourcen

Regel speichern oder planen

Nachdem Sie Ihre Regel getestet haben, können Sie sie als Entwurf speichern oder so festlegen, dass sie regelmäßig ausgeführt wird.

Schritte

1. Führen Sie einen der folgenden Schritte aus:

- Um eine regelmäßige Auswertung zu planen, die Auswertungshäufigkeit festlegen (mindestens 1 Stunde, Standard 24 Stunden) und **Planen** auswählen. Die Regel ist aktiviert und wird gemäß dem definierten Zeitplan ausgeführt.
- Um ohne Terminplanung zu speichern, **Als Entwurf speichern** auswählen. Die Regel wird gespeichert, aber nicht ausgewertet, bis sie geplant wird.
- Um die Regel zu verwerfen, **Verwerfen** auswählen, um die Regelerstellung abubrechen und neu zu beginnen.

Ergebnis

Ihre benutzerdefinierte Regel wurde erstellt und ist im Regelkatalog aufgeführt. Wenn Sie einen Zeitplan festlegen, werden Ihre FSx for ONTAP Ressourcen mit der angegebenen Häufigkeit geprüft.

Fehlerbehebung

Keine Dateisysteme verfügbar

Richten Sie Ihre AWS-Zugangsdaten ein und stellen Sie sicher, dass Ihre Umgebung mindestens ein FSx for ONTAP Dateisystem enthält. Der Rule Builder benötigt ein Dateisystem, um Regeln anzuwenden.

Interpretation mit geringer Sicherheit

Es werden weitere Informationen benötigt. Die Fragen können beantwortet oder die Aufgabenstellung mit klaren Details zu Ressourcentyp, Einschränkungen und Bedingungen neu formuliert werden.

Teilweise Validierungsfehler

Überprüfen Sie, welche Ressourcen fehlgeschlagen sind und warum. Häufige Ursachen sind fehlende Link- oder Agenteneinstellungen oder unzureichende Berechtigungen. Das Problem beheben und anschließend erneut validieren.

Mehrdeutige Eingabeaufforderung

Beschreiben Sie genauer, was Sie prüfen möchten. Geben Sie den Ressourcentyp, die Bedingung und den Schwellenwert an. Zur Unterstützung dienen die Beispiele für Eingabeaufforderungen.

Die Regel zielt auf mehrere Ressourcentypen ab

Für jeden Ressourcentyp ist eine separate Regel zu erstellen. Pro Regel wird nur ein Ressourcentyp unterstützt.

Nächste Schritte

"Benutzerdefinierte Regeln verwalten"

Benutzerdefinierte Regeln für NetApp Workload Factory managen

Der Regelkatalog ist eine zentrale Anlaufstelle zum Managen all Ihrer benutzerdefinierten Regeln. Die Details jeder Regel, deren Ergebnisse sowie die Möglichkeit, sie zu aktivieren oder zu deaktivieren, sind einsehbar.

Regelkatalog anzeigen

Der Regelkatalog zeigt alle von Ihnen erstellten Regeln, deren Status, Zeitplan und neuesten Ergebnisse an.

Schritte

1. Melden Sie sich mit einem der ["Konsolenerlebnisse"](#) an.
2. Wählen Sie das Menü  und anschließend **Rule builder**.
3. **Ihre Regeln ansehen** öffnet den Regelkatalog.

Regelergebnisse anzeigen

Die Ergebnisse zeigen, welche Ressourcen Ihrer Regel folgen und welche nicht.

Schritte

1. Im Regelkatalog auf die Regel klicken, die überprüft werden soll.
2. Die Registerkarte **Alle Laufergebnisse** auswählen.
3. Mit **Details anzeigen** werden die Ergebnisse für jeden Durchlauf angezeigt.

Wenn die Überprüfung für einige Elemente fehlgeschlagen ist, zeigt die Fehlermeldung den Grund an. Häufige Gründe sind Verbindungsprobleme, fehlende Berechtigungen oder eine nicht eingerichtete Verknüpfung.

Benutzerdefinierte Regel bearbeiten

Sie können die Logik, den Zeitplan oder andere Einstellungen einer Regel jederzeit ändern. Wenn Sie eine Regel bearbeiten, wird der Regel Errichter mit den aktuellen Einstellungen der Regel geöffnet.

Schritte

1. Im Regelkatalog wählen Sie die Regel aus, die Sie bearbeiten möchten.
2. Klicken Sie auf **Bearbeiten**.

Die Regel wechselt in den Entwurfsmodus, und der Regel-Errichter öffnet sich.

3. Die Regelvorgabe kann bearbeitet oder das Gespräch genutzt werden, um die Regel zu verbessern.
4. Überprüfung der aktualisierten Interpretation und Regeldefinition der KI.

Das System zeigt an, was sich gegenüber der aktuellen Regel geändert hat, einschließlich aller API-Aufrufe oder Logik.

5. Je nach den vorgenommenen Änderungen ist einer der folgenden Schritte auszuführen:

- Bei nur geringfügigen Änderungen kann die Regel mit **Save** aktualisiert werden.
- Wenn wesentliche Änderungen vorgenommen wurden, können die Änderungen mit **Regel validieren** getestet werden; anschließend kann mit **Planen** die Regel gespeichert und geplant oder mit **Als Entwurf speichern** ohne Planung gespeichert werden.
- Zum Verwerfen der Änderungen ist **Zur vorherigen Version zurückkehren** auszuwählen. Die Regel kehrt zu ihrer ursprünglichen Definition zurück und verlässt den Bearbeitungsmodus.

Verfolgen Sie Kosten und erhalten Sie Berichte zu Ressourcen in NetApp Workload Factory

Verfolgen Sie die Kosten und die Nutzung des FSx for ONTAP-Dateisystems in einer konsolidierten Ansicht in der NetApp Workload Factory-Konsole. Die Kostendaten unterstützen Sie bei der Budgetverwaltung und Ressourcenoptimierung. Workload Factory generiert außerdem Kostenberichte für Ihre FSx for ONTAP-Dateisystemressourcen, die Sie mit Stakeholdern teilen können.

Über diese Aufgabe

Workload Factory verfolgt die Kosten und die Nutzung des FSx for ONTAP-Dateisystems, indem es Kostendaten vom AWS Cost Explorer abrufen. Die folgenden Kostendetails werden erfasst: Nutzungsart, Nutzungs-SKU, Bereitstellungstyp, Nutzung und Gesamtkosten.

Für individuelle Ressourcen berechnet Workload Factory die Kosten durch Kombination der tatsächlichen Nutzung der Performance-Tier, eines anteiligen Kostenanteils der Performance-Tier-Kosten für bereitgestellten, aber ungenutzten Speicherplatz, der nach Kapazität verteilten Performance-Zuweisungen und der Nutzung des Kapazitätspools. Jede Komponente wird mit ihrem Preis pro Einheit für die jeweilige Dimension multipliziert, und die Ergebnisse werden summiert, um die Gesamtkosten für jede Ressource zu ermitteln.

Im Kosten-Dashboard können Sie Kosten- und Nutzungsdaten nach AWS-Konten, Anmeldeinformationen, einer oder mehreren Regionen und Zeiträumen filtern, damit Sie den Verbrauch Ihres FSx for ONTAP Dateisystems nachvollziehen können. Die Daten werden stets monatsweise angezeigt.

Wir rufen Kosten- und Nutzungsdaten für Ihre Dateisystemressourcen für FSx for ONTAP über AWS Cost Explorer mit den folgenden Berechtigungen ab: `ce:GetCostAndUsage` und `ce:GetTags`. Wir berechnen die Gesamtkosten mithilfe der AWS Cost Explorer API und unserer Schätzungen.

AWS-Zuordnungs-Tag-Schlüssel und Tag-Schlüssel-Werte bieten eine zusätzliche Filterebene, um spezifische Kosten zu ermitteln. Ein Tag besteht aus einem Schlüssel und einem Wert. Zum Filtern nach Tag-Schlüsseln und Tag-Schlüsselwerten weisen Sie Ihren FSx for ONTAP Dateisystemen Tags zu. ["Erfahren Sie mehr über AWS-Kostenverteilungs-Tags."](#)

Zusätzlich zu den Kostendaten im Kosten-Dashboard können Sie Kostenberichte für Ihre FSx for ONTAP-Dateisystemressourcen erstellen. Die Daten im Kostenbericht enthalten Informationen zu spezifischen Dateisystemen und Volumes. Der Bericht ist eine herunterladbare PDF-Datei, die mit Stakeholdern geteilt werden kann.

Kosten nachverfolgen

Die in der Workload Factory-Konsole im Kosten-Dashboard angezeigten Kosten basieren auf den Daten von AWS Cost Explorer, die alle 24 Stunden aktualisiert werden.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen:

- Sie müssen ["Zugangsdaten mit der Berechtigungsrichtlinie für Anzeigen, Planen und Analysieren gewähren"](#) in Workload Factory die FSx for ONTAP-Kosten nachverfolgen.
- Um nach AWS-Zuordnungs-Tags zu filtern, stellen Sie sicher, dass Ihren FSx for ONTAP File Systems Tags zugewiesen sind.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads** > **Storage** > **FSx for ONTAP** auszuwählen.
3. Im Menü **FSx for ONTAP** erfolgt die Auswahl von **Cost**.
4. Filtern Sie im Kosten-Dashboard die Kosten- und Kapazitätsdaten Ihrer FSx for ONTAP-Ressourcen, indem Sie Folgendes angeben:
 - a. **AWS Konten**: Auswahl der Konten, für die Kostendaten angezeigt werden sollen.
 - b. **Anmeldeinformationen**: Anmeldeinformationen mit den Berechtigungen *Anzeigen, Planen und Analysieren* auswählen.
 - c. **Regionen**: Auswahl der AWS-Regionen, für die Kostendaten angezeigt werden sollen.
 - d. **Kostendatenbereich**: Auswahl des Zeitraums für die anzuzeigenden Kostendaten.
 - e. **Zuordnungs-Tag-Schlüssel**: (Optional) Wählen Sie einen Zuordnungs-Tag-Schlüssel und dessen Wert aus, um einen detaillierten Kostenbericht für alle FSx for ONTAP-Dateisysteme zu erstellen, die dem AWS-Tag zugeordnet sind.
 - f. **Zuordnungs-Tag-Werte**: (Optional) Wählen Sie den Zuordnungs-Tag-Schlüsselwert aus, der dem Zuordnungs-Tag-Schlüssel zugeordnet ist, um einen detaillierten Kostenbericht für alle FSx for ONTAP-Dateisysteme zu generieren, die dem AWS-Tag zugeordnet sind.
5. Die **Kostendetails** für Ihre FSx for ONTAP Ressourcen können angezeigt werden.

Generieren Sie Kostenberichte für Ihre FSx for ONTAP-Ressourcen

Erstellen Sie Kostenberichte für spezifische FSx for ONTAP-Dateisystemressourcen, um diese mit den Stakeholdern zu teilen.

Schritte

1. Im Kosten-Dashboard wählen Sie **Bericht generieren**.
2. Geben Sie im Berichtsfenster folgende Informationen an:
 - a. **Dateisystem**: Wählen Sie ein oder mehrere FSx for ONTAP-Dateisysteme aus, die in den Bericht aufgenommen werden sollen.
 - b. **Volume**: (Optional) Wählen Sie ein oder mehrere Volumes aus, die in den Bericht aufgenommen werden sollen.

Ergebnis

Es wird ein PDF-Bericht generiert, der heruntergeladen werden kann.

Volumes verwalten

Kapazität von Volumes in der NetApp Workload Factory verwalten

Die Volume-Kapazität sollte an den sich ändernden Bedarf angepasst werden. Die Volume-Größe kann manuell angepasst oder die automatische Größenanpassung für Volumes aktiviert werden, damit Workload Factory die Volume-Kapazität verwaltet. Das Gleichgewicht der FlexVol- oder FlexGroup-Volume-Kapazität kann überprüft und die Volume-Kapazität neu verteilt werden, um Dateien gleichmäßig auf alle FlexVol-Volumes in einem Node oder auf alle Bestandteile zu verteilen, sodass alle Nodes an der Arbeitslast eines einzelnen FlexGroup-Volumes beteiligt sind.

Automatisches Vergrößern des Volume bearbeiten

Aktivieren Sie die automatische Größenanpassung des Volumes, damit NetApp Workload Factory die Volumenkapazität für Sie verwaltet. Diese Funktion kann jederzeit deaktiviert werden.



Die automatische Vergrößerung von Volumes wird für iSCSI Volumes nicht unterstützt.

Bevor Sie beginnen

Um die automatische Volumenvergrößerung zu aktivieren, muss eine Verknüpfung hergestellt werden.

["Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen"](#).

Nach der Verknüpfung ist eine Rückkehr zu diesem Vorgang erforderlich.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Volumes explorer**.
3. Wählen Sie das Aktionsmenü für das Volume aus, das Sie ändern möchten.
4. Die Auswahl erfolgt über **Grundlegende Aktionen** und dann **Volume-Autogrow festlegen**.
5. Im Dialogfeld „Automatisches Wachstum einstellen“ wird durch Aktivieren der Option „Volume automatisch erweitern“ die Volume-Kapazität automatisch vergrößert, bis das Volume die maximale Größe erreicht. Diese Funktion berücksichtigt steigendes Datenaufkommen und gewährleistet einen unterbrechungsfreien Betrieb.

Hier werden die maximale Wachstumsgröße des Volumes und die Einheit angegeben. Die maximale Wachstumsgröße kann nicht kleiner sein als die Größe des aktuellen Volumes.

6. **Anwenden** auswählen.

Volume-Kapazität manuell anpassen

Sie können die Speicherkapazität anpassen, indem Sie die bereitgestellte Größe eines Volumes erhöhen oder verringern. Die folgende Tabelle zeigt die minimalen und maximalen Volume-Größen nach Volume-Typ:

Volumentyp	Mindestgröße	Maximale Größe
FlexVol volume	20 MiB	300 TiB
FlexGroup-Volume	800 GiB	2 PiB

Bei einer iSCSI-LUN erhöht eine Vergrößerung des Volumes auch die Größe der Host-LUN. Nach der Erhöhung der Volume-Kapazität ist gemäß der Anleitung des Host-Betriebssystems die neue Größe der LUN zu ermitteln und das Dateisystem der LUN zu erweitern.

Die Volume-Größe kann nur bei NFS- und SMB/CIFS-Volumes verringert werden.

Bevor Sie beginnen

Um die Volume-Kapazität anzupassen, muss ein Link zugeordnet werden. ["Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen"](#). Nach der Verknüpfung ist eine Rückkehr zu diesem Vorgang erforderlich.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Volumes explorer**.
3. Wählen Sie das Aktionsmenü für das Volume aus, das Sie ändern möchten.
4. **Grundlegende Aktionen** und anschließend **Volume-Kapazität anpassen** auswählen.
5. Im Dialogfeld „Volumenkapazität anpassen“ lassen sich **Bereitgestellte Kapazität** und Einheit festlegen.
6. Mit **Anpassen** werden die Änderungen übernommen.

Kapazität von FlexVol- und FlexGroup-Volumes neu ausbalancieren

Die Neuverteilung der Volume-Kapazität wird für FlexVol Volumes und FlexGroup Volumes unterstützt. Bei der Neuverteilung eines Volumes wird die Kapazität neu verteilt, wenn sich im Laufe der Zeit durch das Hinzufügen neuer Dateien und das Wachstum von Dateien Ungleichgewichte entwickeln. Nachdem Sie den Neuverteilungsvorgang manuell gestartet haben, wählen wir die Dateien aus und verschieben sie automatisch und unterbrechungsfrei. Volume-Übertragungsvorgänge verbrauchen Dateisystemressourcen.

Die einzelnen Volumenarten und Neuausgleichsvorgänge unterscheiden sich wie folgt.

FlexVol Volumes

FlexVol volumes sind logische Container, die Flexibilität beim Managen von Daten bieten und Erweiterung, Verkleinerung, Verschiebung und effizientes Kopieren ermöglichen. Sie können in NAS- und SAN-Umgebungen verwendet werden.

Ein FlexVol volume kann in einem FSx for ONTAP Dateisystem im Verhältnis zu anderen FlexVol volumes innerhalb eines Knotens ausbalanciert werden. Wenn das Dateisystem nur ein einziges FlexVol volume hat, ist eine Neuausrichtung nicht möglich. Wenn das Dateisystem mehr als ein FlexVol volume pro Knoten hat und ein einzelnes FlexVol volume ausgewählt ist, wird das FlexVol volume im Kontext aller FlexVols ausbalanciert, aber nur das ausgewählte volume kann verschoben werden.

FlexGroup Volumes

FlexGroup Volumes hingegen sind skalierbare NAS-Container, die für hohe Performance und automatische Lastverteilung ausgelegt sind. Sie bestehen aus mehreren Mitglieds-Volumes (Bestandteilen), die den Datenverkehr transparent gemeinsam nutzen. FlexGroup Volumes bieten enorme Kapazität und übertreffen die FlexVol Grenzen mit bis zu 60 PB Kapazität und 400 Milliarden Dateien. Sie vereinfachen das Management, indem sie einen Container mit einem einzigen Namespace bereitstellen.

In einem Scale-out-Dateisystem FSx for ONTAP mit zwei oder mehr Hochverfügbarkeitspaaren (HA) wird die Kapazität auf mehrere Komponenten verteilt. Jede Komponente ist ein Container, der die maximale Größe einer einzelnen Datei festlegt. FSx for ONTAP verteilt Dateien gleichmäßig auf alle Komponenten, sodass alle Knoten an der Arbeitslast eines einzelnen FlexGroup Volumens beteiligt sind.

Wenn die Bestandteile nicht gleichmäßig auf alle Knoten verteilt sind, verringert sich die Performance des FlexGroup volume.

Die Überprüfung der Kapazität des FlexGroup volume umfasst die Bewertung des aktuellen Layouts der Bestandteile. Beim Neuausbalancieren der Kapazität des volume entwirft NetApp Workload Factory ein neues Layout der Bestandteile mit einer geraden Anzahl von Bestandteilen, um die Daten gleichmäßig auf alle HA-Paare zu verteilen. Der Service führt den Neuausgleichsplan aus, was wiederum die Lese- und Schreibvorgänge verbessert.



Rebalancing wird für SAN Volumes wie iSCSI und NVMe nicht unterstützt.

Die Ausgewogenheit Ihrer Volumes prüfen

Prüfen der Balance von FlexVol oder FlexGroup Volumes in einem FSx for ONTAP Dateisystem.

Bevor Sie beginnen

- FlexGroup Volume-Balance ist nur für FSx for ONTAP Dateisysteme verfügbar, die ein Scale-out Deployment mit mindestens zwei HA-Paaren verwenden.
- Um den Kontostand eines Volumens zu prüfen, müssen Sie ["Einen Link erstellen und zuordnen oder einen vorhandenen Link mit dem Dateisystem verknüpfen"](#). Nach der Verknüpfung ist eine Rückkehr zu diesem Vorgang erforderlich.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Unter **FSx for ONTAP** erfolgt die Auswahl von **Manage** im Aktionsmenü des Dateisystems, das die neu zu verteilenden Volumes enthält.
4. In der Dateisystemübersicht erfolgt die Auswahl der Registerkarte **Volumes**.
5. Auf der Registerkarte „Volumes“ oben in der Tabelle die Option „Volume-Balance prüfen“ auswählen.
6. Im Fenster „Volume balance“ wird der Bilanzstatus von Folgendem geprüft:
 - FlexGroup Volumes
 - FlexVol Volumes

Wenn ein Volume unausgeglichen ist, sollten Sie [es neu ausbalancieren](#) in Betracht ziehen.

Volumenkapazität neu ausbalancieren

Ausgleichen eines oder mehrerer unausgeglichener Volumes.



Ein Workload Factory Administrator kann [Rebalancing stoppen](#) während des Vorgangs.

Bevor Sie beginnen

- [Prüfung der Balance eines Volumes](#) vor dem Neuausgleich der Volumes.
- Um ein Volume neu auszubalancieren, muss ["Einen Link erstellen und zuordnen oder einen vorhandenen Link mit dem Dateisystem verknüpfen"](#) werden. Nach der Verknüpfung ist eine Rückkehr zu diesem Vorgang erforderlich.
- Vorhandene Snapshots auf Volumes, die neu ausbalanciert werden, werden teilweise unvollständig und

können nicht zur Wiederherstellung von Volume-Daten verwendet werden, neue Snapshots, die nach der Neuausbalancierung erstellt werden, können jedoch zur Wiederherstellung von Volume-Daten verwendet werden.

- FlexVol Volumes sollten idealerweise gemeinsam neu ausbalanciert werden, um alle Volume-Ressourcen gleichmäßig auszubalancieren. Abgewählte Volumes nehmen nicht aktiv am Ausbalancierungsvorgang teil.

FlexVol volume

Ein FlexVol volume kann in einem FSx for ONTAP Dateisystem im Verhältnis zu anderen FlexVol volumes innerhalb eines Knotens ausbalanciert werden. Wenn das Dateisystem mehr als ein FlexVol volume pro Knoten hat und ein einzelnes FlexVol volume ausgewählt wird, dann wird das FlexVol volume im Kontext aller FlexVols ausbalanciert, aber nur das ausgewählte volume darf verschoben werden.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
 2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
 3. In **FSx for ONTAP** erfolgt die Auswahl von **Manage** im Aktionsmenü des Dateisystems, das das neu auszugleichende Volume enthält.
 4. In der Dateisystemübersicht erfolgt die Auswahl der Registerkarte **Volumes**.
 5. Auf der Registerkarte „Volumes“ oben in der Tabelle die Option „Volume-Balance prüfen“ auswählen.
 6. Im Fenster „Volumes balance“ kann optional in der Bilanzübersicht für FlexVol die Option **Datenverteilung** ausgewählt werden, um die genutzte Kapazität pro Aggregat anzuzeigen.
 7. Mit **Neu ausbalancieren** lassen sich ein oder mehrere unausgeglichene Volumes neu ausbalancieren.
 8. Im Rebalance-Assistenten führen Sie die Schritte nacheinander aus.
 - a. **Maximale Transferrate**: Optional. Standardmäßig deaktiviert. Die Drosselung begrenzt die Bandbreite einer Volume-Verschiebung in Ihrem Dateisystem und verlangsamt den ausgehenden Datenverkehr der Volume-Replikation.

Eingabe des Drosselwerts in MB/s.
- Weiter** auswählen.
- a. Nach der Prüfung der aktuellen und vorgeschlagenen Layouts aller FlexVol volumes wird **Weiter** ausgewählt.
 - b. Vor Beginn der Rebalancing-Operation sollten die Auswirkungen und der Hinweis sorgfältig geprüft werden.
9. Auswahl der Option **Rebalance**.

Ergebnis

Das FlexVol Volumen wird neu verteilt. Nach Abschluss des Vorgangs wird das Dateisystem wieder auf den ursprünglichen Wert gedrosselt.

FlexGroup-Volume

Die Daten werden über die Mitgliedsvolumes hinweg neu verteilt, um das FlexGroup Volume wieder auszubalancieren. Je nach gewähltem Layout kann der Vorgang zum Neuausbalancieren zusätzliche FlexGroup Mitgliedsvolumes hinzufügen und die Größe der provisionierten Volumes erhöhen.

Schritte

1. Melden Sie sich bei der **"NetApp Console"** an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** erfolgt die Auswahl von **Manage** im Aktionsmenü des Dateisystems, das das neu auszugleichende Volume enthält.
4. In der Dateisystemübersicht erfolgt die Auswahl der Registerkarte **Volumes**.
5. Auf der Registerkarte „Volumina“ befindet sich oben in der Tabelle die Option **FlexGroup Balance prüfen**.
6. Im Fenster „Balance“ von FlexGroup steht **Neu ausgleichen** zur Verfügung, um ein oder mehrere unausgeglichene Volumes neu auszubalancieren.
7. Im Rebalance-Assistenten ist das bevorzugte Datenverteilungslayout auszuwählen.
 - **Performance-optimiert** (empfohlen): Erhöht die Anzahl der FlexGroup Member Volumes und die provisionierte Größe des Volumes. Entspricht der NetApp Best Practice.
 - **Eingeschränkt**: unterstützt Volumes in einer Replikationsbeziehung. Die Anzahl der FlexGroup Mitglieds volumes und die Größe der bereitgestellten Volumes bleiben unverändert. Standardmäßig ausgewählt, wenn alle ausgewählten Volumes an einer Replikationsbeziehung beteiligt sind.
 - **Manuell**: Auswahl der gewünschten Anzahl von FlexGroup Mitglieds volumes pro HA-Paar. Abhängig von Ihrer Auswahl können sich die Anzahl der FlexGroup Mitglieds volumes und die bereitgestellte Größe des Volumes erhöhen.
8. **Drosselung**: Optional. Standardmäßig deaktiviert. Die Drosselung begrenzt optional die Bandbreite einer Volume-Verschiebung in Ihrem Dateisystem und verlangsamt den ausgehenden Datenverkehr der Volume-Replikation.

Eingabe des Drosselwerts in MB/s.
9. Eine Layoutvergleichsansicht auswählen und dann **Weiter** auswählen.
 - Vergleich des Volume Layouts
 - FSx for ONTAP Layoutvergleich
10. Optional können Sie vor dem Rebalancing eine Liste der Volume-Verschiebungen herunterladen.
11. Auswahl der Option **Rebalance**.

Ergebnis

FlexGroup Mitglieds volumes werden beim Rebalancing nacheinander verschoben. Nach Abschluss des Vorgangs wird das Dateisystem wieder auf den ursprünglichen Wert gedrosselt.

Beenden eines Neuausgleichsvorgangs für ein Volume

Ein Rebalancing-Vorgang lässt sich jederzeit stoppen; dies führt zu keinen Betriebsunterbrechungen. Beim Stoppen des Vorgangs werden aktive Volume-Verschiebungen abgebrochen.

Sie können später einen weiteren Neuverteilungsvorgang starten.

Schritte

1. Nachdem Sie den Rebalancing-Vorgang gestartet haben, ist auf der Seite „Volume balance“ die Option **Stop rebalancing** auszuwählen.

2. Im Dialogfeld „Neubalancierung stoppen“ wird **Stopp** ausgewählt.

Ergebnis

Der Neuausgleich des Volumes stoppt, und aktive Volume-Verschiebungen brechen ab.

Legen Sie Schwellenwerte für die Volumenlatenz in der NetApp Workload Factory fest.

Legen Sie Latenzschwellenwerte für Volumes fest, um Benachrichtigungen zu erhalten, wenn die lesen- oder schreiben-Latenz die angegebenen Werte überschreitet.

Über diese Aufgabe

Sie können Latenzschwellenwerte pro Volume konfigurieren, um die Leistung zu überwachen und Benachrichtigungen zu erhalten, wenn die Latenzwerte Ihre definierten Grenzwerte überschreiten. Workload Factory überwacht sowohl die Lese- als auch die Schreiblatenz und generiert Benachrichtigungen, sobald einer der Schwellenwerte überschritten wird.

Wenn Sie Latenzschwellenwerte festlegen, überwacht Workload Factory Folgendes:

- **Leseverzögerung:** Löst eine Warnung aus, wenn Lesevorgänge den angegebenen Schwellenwert in Millisekunden überschreiten.
- **Schreiblatenz:** Löst eine Warnung aus, wenn Schreibvorgänge den angegebenen Schwellenwert in Millisekunden überschreiten.

Die Latenzüberwachung verwendet die folgenden Standardparameter:

- **IOPS-Schwellenwert:** 100 IOPS (lesen und schreiben)
- **Zeitraum:** 10 Minuten

Es wird eine Warnung generiert, wenn der Latenzschwellenwert überschritten und der IOPS-Schwellenwert innerhalb des angegebenen Zeitraums erreicht wird.



Sie können Latenzereignisse anzeigen und Benachrichtigungen erhalten, ohne eine Linkverbindung zu haben. Um jedoch Ereignisse zu analysieren und KI-gestützte Erkenntnisse und Empfehlungen zu erhalten, müssen Sie ["Stellen Sie über einen Link eine Verbindung zum Dateisystem her."](#)

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Volumes explorer**.
3. Wählen Sie das Aktionsmenü des Volumes aus, für das Latenzschwellenwerte festgelegt werden sollen.
4. Wählen Sie **Alerts actions** und anschließend **Latenzschwelle festlegen**.
5. Konfigurieren Sie im Dialogfeld „Latenzschwelle festlegen“ Folgendes:
 - a. **Leselatenz:** Geben Sie den Schwellenwert in Millisekunden (ms) für Lesevorgänge ein.
 - b. **Schreiblatenz:** Geben Sie den Schwellenwert in Millisekunden (ms) für Schreibvorgänge ein.
6. Wählen Sie **Speichern**, um die Latenzschwellenwerte anzuwenden.

Ergebnis

Workload Factory überwacht das Volume und generiert Warnmeldungen, wenn die Lese- oder Schreiblatenz

die konfigurierten Schwellenwerte überschreitet. Sie können Latenzereignisse aus der "[Analysebildschirm](#)" einsehen.

Verwandte Informationen

- "[Analysieren Sie FSx for ONTAP-Ereignisse in NetApp Workload Factory](#)"
- "[Anpassen der Volumenkapazität in Workload Factory](#)"

Volume-Einstellungen in NetApp Workload Factory verwalten

Die FSx for ONTAP Volume-Einstellungen in NetApp Workload Factory können an die Anforderungen Ihres Unternehmens angepasst werden. Volume-Tags lassen sich verwalten, um Ressourcen zu kategorisieren, die Einstellungen zur Speichereffizienz können aktualisiert werden, um Speicherplatz und Kosten zu optimieren, und die Einstellungen für unveränderliche Dateien ermöglichen die Steuerung der Datenaufbewahrung und den Schutz vor unbefugten Änderungen.

Volume-Tags managen

Tags können Ihnen helfen, Ihre Ressourcen zu kategorisieren. In NetApp Workload Factory können Sie Volume-Tags für Volumes in FSx for ONTAP jederzeit hinzufügen, bearbeiten und entfernen.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Volumes explorer**.
3. Wählen Sie das Aktionsmenü für das Volume aus, für das Sie Tags ändern möchten.
4. Anschließend erfolgt unter **Grundlegende Aktionen** die Auswahl von **Volume-Tags bearbeiten**.
5. Auf der Seite „Volume Tags bearbeiten“ können Sie Tags hinzufügen, bearbeiten oder entfernen.

Die maximale Anzahl an Tags, die Sie einem Volume zuweisen können, beträgt 50.

6. **Anwenden** auswählen.

Aktualisierung der Volume-Speichereffizienz

Die Speichereffizienzeinstellung kann nach der Volume-Erstellung aktualisiert werden.

Die Funktion für Storage-Effizienz umfasst Deduplizierung, Datenkomprimierung und Datenverdichtung, um optimale Platzeinsparungen auf einem FlexVol volume zu erzielen. Die Deduplizierung entfernt doppelte Datenblöcke. Die Datenkomprimierung komprimiert die Datenblöcke, um die Menge an erforderlichem physischem Storage zu reduzieren. Die Datenverdichtung speichert mehr Daten auf kleinerem Raum, um die Storage-Effizienz zu erhöhen.

Wenn Sie beim Erstellen eines Volumes die Speichereffizienz nicht aktiviert haben, können Sie diese Einstellung jederzeit aktivieren, um potenziell Speicherplatz und Kosten zu sparen.

Volumes nutzen Thin Provisionierung, unabhängig davon, ob Sie Storage-Effizienz aktivieren oder deaktivieren.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Volumes explorer**.
3. Wählen Sie das Aktionsmenü des Volumes aus, für das die Speichereffizienzeinstellung aktualisiert werden soll.
4. Die Auswahl von **Advanced actions** und anschließend **Set storage efficiency**.
5. Die Speichereffizienz des Volumes kann aktiviert oder deaktiviert werden.
6. Mit **Apply** wird die Änderung gespeichert.

Verwalten unveränderlicher Dateien für ein Volume in NetApp Workload Factory

Wenn die Funktion aktiviert ist, können Sie bestimmte Einstellungen für unveränderliche Dateien eines Volumes aktualisieren, z. B. die Aufbewahrungsrichtlinie und -zeiträume, den Autocommit-Zeitraum und den Anhängemodus des Volumes.

Die Aktivierung unveränderlicher Dateien ist nur während ["Volume-Erstellung"](#) möglich.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Volumes explorer**.
3. Wählen Sie das Aktionsmenü des Volumes aus, das aktualisiert werden soll.
4. Die Auswahl erfolgt über **Datenschutzmaßnahmen** und anschließend über **Unveränderliche Dateien verwalten**.
5. Auf der Seite „Unveränderliche Dateien verwalten“ können Sie Folgendes aktualisieren:
 - **Aufbewahrungsdauer: Nicht angegeben** oder **Zeitraum angeben** auswählen.
 - **Nicht spezifiziert:** Der standardmäßige Mindestzeitraum beträgt "0" Jahre, und der standardmäßige Höchstzeitraum beträgt "30 years".
 - **Zeitraum festlegen:** Option zur Definition der Aufbewahrungsrichtlinie, der minimalen und maximalen Aufbewahrungsdauer, der Autocommit-Funktion und der Funktion für den Volume-Anhängemodus. Folgende Details sind erforderlich:
 - **Aufbewahrungsrichtlinie:** Dieser Zeitraum muss größer oder gleich der Mindestaufbewahrungsfrist und kleiner oder gleich der Höchstaufbewahrungsfrist sein.
 - **Minimale und maximale Zeiträume:** Mit diesen Einstellungen werden die minimalen und maximalen Zeiträume festgelegt, um Dateien in diesem Volume in einen unveränderlichen WORM-Zustand zu überführen.
 - **Autocommit:** Die Funktion aktiviert oder deaktiviert das automatische Committen von Dateien in WORM, die während des Autocommit-Zeitraums nicht geändert wurden.
 - **Privilegiertes Löschen:** Aktivierung oder Deaktivierung der Funktion. Durch die Aktivierung der Funktion kann ein SnapLock Administrator ein noch nicht abgelaufenes WORM-Volume löschen. Diese Funktion wird nur im Enterprise-Aufbewehrungsmodus unterstützt.
 - **Volume Append Modus:** Die Funktion kann aktiviert oder deaktiviert werden. Wenn der Volume Append Modus aktiviert ist, können Sie WORM-Dateien neue Inhalte hinzufügen.
6. Auf **Anwenden** klicken.

Verwandte Informationen

- ["Erstellung eines Volume in Workload Factory"](#)
- ["Kapazität von Volumes in Workload Factory verwalten"](#)
- ["Ändern der Volume-Tiering-Richtlinie in Workload Factory"](#)
- ["Verwalten von S3-Zugriffspunkten in Workload Factory"](#)

FSx for ONTAP Cache Volumes mit NetApp Workload Factory managen

Die NetApp Workload Factory Konsole dient zum Managen von Cache-Volumes für FSx for ONTAP Dateisysteme. Caching, eine Methode zur temporären Speicherung von Daten, verbessert die Datenzugriffs-Performance durch die Verkürzung der Abrufzeit. Sie können den Cache-Namen bearbeiten, die Kapazität anpassen, die Exportrichtlinie ändern, eine Caching-Methode auswählen, den Cache vorab befüllen oder Cache-Volumes löschen.

Über diese Aufgabe

In der NetApp Workload Factory Konsole können Sie Cache-Volumes managen, die mit Cache-Beziehungen verknüpft sind.

Bevor Sie beginnen

- Sie müssen eine Verknüpfung herstellen, um Cache-Volumes und Beziehungen zu verwalten. ["Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen"](#). Nach der Verknüpfung kann zu diesem Vorgang zurückgekehrt werden.
- Zum Bearbeiten ist ein vorhandenes Cache Volume erforderlich.

Den Namen des Cache-Volumes bearbeiten

Sie können den Namen eines vorhandenen Cache-Volumes jederzeit ändern.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In FSx for ONTAP erfolgt die Auswahl von **Manage** im Aktionsmenü des Dateisystems mit dem Cache-Volume.
4. In der Dateisystemübersicht ist die Registerkarte **Cache-Beziehungen** zu wählen.
5. Im Aktionsmenü erfolgt die Auswahl des Cache-Volumes, das geändert werden soll; anschließend wird **Cache-Namen bearbeiten** ausgewählt.
6. Im Dialogfeld **Cache-Namen bearbeiten** wird der neue Name für das Cache-Volume eingegeben und anschließend **Anwenden** ausgewählt.

Kapazität eines Cache-Volumes anpassen

Sie können die Kapazität eines vorhandenen Cache-Volumes jederzeit anpassen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.

2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In FSx for ONTAP erfolgt die Auswahl von **Manage** im Aktionsmenü des Dateisystems mit dem Cache-Volume.
4. In der Dateisystemübersicht ist die Registerkarte **Cache-Beziehungen** zu wählen.
5. Im Aktionsmenü für das Cache-Volume, das Sie ändern möchten, erfolgt anschließend die Auswahl von **Cache-Kapazität anpassen**.
6. Im Dialogfeld **Cache-Kapazität anpassen** kann die neue Kapazität für das Cache-Volume prozentual oder in Einheiten eingegeben und anschließend **Apply** ausgewählt werden.

Bearbeiten der Exportrichtlinie für Cache-Volumes

Der Mount-Pfad oder die Exportrichtlinie eines vorhandenen Cache-Volume kann geändert werden.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In FSx for ONTAP erfolgt die Auswahl von **Manage** im Aktionsmenü des Dateisystems mit dem Cache-Volume.
4. In der Dateisystemübersicht ist die Registerkarte **Cache-Beziehungen** zu wählen.
5. Für das Cache-Volume, das Sie ändern möchten, erfolgt im Aktionsmenü anschließend die Auswahl von **Exportrichtlinie bearbeiten**.
6. Im Dialogfeld **Exportrichtlinie bearbeiten** lässt sich der Mount-Pfad ändern oder eine andere Exportrichtlinie zur Zuweisung an das Cache-Volume auswählen.
7. **Anwenden** auswählen.

Ändern der Caching-Methode für ein Cache-Volume

Sie können die Funktionsweise des Caches für ein bestehendes Cache-Volume auf Write-Around oder Write-Back ändern.

Weitere Informationen zu ["Schreibmodi"](#).

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In FSx for ONTAP erfolgt die Auswahl von **Manage** im Aktionsmenü des Dateisystems mit dem Cache-Volume.
4. In der Dateisystemübersicht ist die Registerkarte **Cache-Beziehungen** zu wählen.
5. Im Menü „Aktionen“ für das Cache-Volume, das geändert werden soll, erfolgt die Auswahl von **Caching-Methode ändern**.
6. Im Dialogfeld **Caching-Methode ändern** erfolgt die Auswahl der neuen Caching-Methode und anschließend von **Anwenden**.

Vorbefüllen eines Cache-Volumes

Es ist sinnvoll, das Cache-Volume vor der Verwendung mit Daten aus dem Ursprungsvolume zu füllen, damit zwischengespeicherte Daten schneller verfügbar sind.

Schritte

1. Melden Sie sich bei der "NetApp Console" an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In FSx for ONTAP erfolgt die Auswahl von **Manage** im Aktionsmenü des Dateisystems mit dem Cache-Volume.
4. In der Dateisystemübersicht ist die Registerkarte **Cache-Beziehungen** zu wählen.
5. Im Menü „Aktionen“ lässt sich für das Cache-Volume, das geändert werden soll, die Option **Cache vorbereiten** auswählen.
6. Im Dialogfeld **Cache vorbereiten** erfolgt die Angabe des Pfads zum Datensatz für die Vorbereitung, anschließend die Auswahl von **Anwenden**.

Löschen eines Cache-Volumes

Wenn Sie ein Cache-Volume löschen, heben Sie dessen Cache-Beziehung auf. Zwischengespeicherte Daten sind dann nicht mehr verfügbar.

Schritte

1. Melden Sie sich bei der "NetApp Console" an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In FSx for ONTAP erfolgt die Auswahl von **Manage** im Aktionsmenü des Dateisystems mit dem Cache-Volume.
4. In der Dateisystemübersicht ist die Registerkarte **Cache-Beziehungen** zu wählen.
5. Im Aktionsmenü des Cache-Volumes, das Sie löschen möchten, erfolgt anschließend die Auswahl von **Cache-Volume löschen**.
6. Im Dialogfeld **Cache-Volume löschen** ist die Löschung zu bestätigen; anschließend ist **Löschen** auszuwählen.

Ändern der Tiering-Richtlinie eines Volumes in NetApp Workload Factory

In NetApp Workload Factory können Sie die Tiering-Richtlinie ändern, um Daten automatisch vom primären Hochleistungs-Storage-Tier auf das sekundäre Kapazitätspool-Storage-Tier neu zuzuweisen.

Über diese Aufgabe

Sie können die Tiering-Richtlinie eines Volumes jederzeit ändern. Die Tiering-Richtlinie ist pro Volume definiert.

Die Entscheidung, wo Ihre Daten gespeichert werden, hat Auswirkungen auf Ihre Kosteneinsparungen.

FSx for ONTAP verfügt über zwei Storage-Tiers zum Speichern von Volumendaten:

- **SSD Storage-Tier:** Dieses primäre Storage-Tier ist für die Daten vorgesehen, auf die Sie am häufigsten zugreifen, auch bekannt als *heiße* Daten. Das Speichern von Daten auf dem primären Storage-Tier ist

teurer als auf dem sekundären Storage-Tier.

- **Storage-Tier für Kapazitätspools:** Dieser sekundäre Storage-Tier ist für archivierte Daten oder selten abgerufene Daten vorgesehen, auch als *kalte* Daten bezeichnet.

Weitere Informationen zu Storage-Tiers finden Sie in "[Verwaltung der Storage-Kapazität](#)" AWS für FSx for NetApp ONTAP Dokumentation.

Bevor Sie beginnen

Die verfügbaren Tiering-Richtlinien sollten vor dem Ändern der Tiering-Richtlinie überprüft werden.

- **Ausgewogen (Automatisch):** Standardmäßige Tiering-Richtlinie beim Erstellen eines Volumes über die Benutzeroberfläche. Häufig genutzte Daten verbleiben im SSD Storage-Tier, selten genutzte Daten und Snapshots werden nach Ablauf der Abkühlphase in das Kapazitätspool Storage-Tier verschoben. Empfohlen für allgemeine primäre Workloads.
- **Kostenoptimiert (Alle):** Lagert alle Snapshots und Daten in den Storage-Tier des Kapazitätspools aus. Empfohlen für sekundäre Ziele.
- **Leistungsoptimiert (nur Snapshots):** Tiers speichern nur Snapshot-Daten im Storage-Tier des Kapazitätspools. Empfohlen für Workloads mit niedriger Latenz, wie z. B. unternehmenskritische Datenbanken.
- **Keine:** Behält die Volumendaten im SSD Storage-Tier und verhindert, dass sie in das Kapazitätspool Storage-Tier verschoben werden.

Einige Tiering-Richtlinien haben eine zugehörige Mindestkühlzeit, die festlegt, wie lange, also wie viele *cooling days*, Benutzerdaten in einem Volume inaktiv bleiben müssen, damit die Daten als „kalt“ gelten und in den Capacity Pool Storage-Tier verschoben werden. Die Kühlzeit beginnt, wenn Daten auf die Festplatte geschrieben werden.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Die Auswahl erfolgt im Menü  **Workloads > Volumes explorer > FSx for ONTAP**.
3. Wählen Sie das Aktionsmenü des Volumes aus, für das die Tiering-Richtlinie geändert werden soll.
4. Die Auswahl erfolgt zunächst über **Advanced actions** und dann über **Change tiering policy**.
5. Auf der Seite „Tiering-Richtlinie ändern“ kann die Tiering-Richtlinie des Quell-Volumes kopiert oder eine der folgenden Tiering-Richtlinien ausgewählt werden:
 - **Ausgeglichen (Auto):** Anzahl der Kühlstage eingeben.
 - **Kostenoptimiert (Alle)**
 - **Leistungsoptimiert (nur Snapshots):** Anzahl der Kühlstage eingeben.
 - **Keine**
6. **Anwenden** auswählen.

Managen der NFS-Exportrichtlinie für ein Volume in NetApp Workload Factory

Managen der NFS-Exportrichtlinie für ein Volume, das die Protokolltypen NFSv3 oder NFSv4.1 in NetApp Workload Factory verwendet.

Über diese Aufgabe

Das Managen der Exportrichtlinie eines Volumes umfasst das Hinzufügen von Exportrichtlinienregeln, die

Client-Spezifikationen, Zugriffskontrolle, Superuser-Zugriff und die NFS-Version detailliert beschreiben. Sie können mehrere Exportrichtlinien hinzufügen und diese priorisieren.

Bevor Sie beginnen

Festlegung der Client-Spezifikationen für die Exportrichtlinienregeln. Gültige Werte für die Client-Spezifikation sind wie folgt:

- IP-Adressen
- IP-Adressen mit Subnetzmasken
- IP-Adressen mit Netzwerkmaske
- Ein Netzgruppenname, dem das Zeichen „@“ vorangestellt ist
- Ein Domainname, dem ein Punkt „.“ vorangestellt ist.
- Hostnamen

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Volumes explorer**.
3. Wählen Sie das Aktionsmenü für das Volume aus, für das die NFS-Exportrichtlinie geändert werden soll.
4. Die Auswahl erfolgt über **Advanced actions** und anschließend **Edit NFS export policy**.
5. Auf der Seite „NFS-Exportrichtlinie bearbeiten“ sind die folgenden Angaben erforderlich:
 - a. **Zugriffskontrolle:** Zur Auswahl stehen **Benutzerdefinierte Exportrichtlinie** oder **Vorhandene Exportrichtlinie**.

Alternativ können Sie **Kein Zugriff auf das Volume** auswählen.
 - b. **Name der Exportrichtlinie:** Optional können Sie einen Namen für die Exportrichtlinie eingeben.
 - c. **Exportrichtlinienregel hinzufügen:** Die folgenden Details sind anzugeben, und die Richtlinien beginnen mit Regel Nr. 1 als Prioritätsregel:
 - i. **Client-Spezifikation:** Mehrere Werte werden durch Kommas getrennt.
 - ii. **Zugriffskontrolle:** Im Dropdown-Menü stehen **lesen/schreiben**, **Nur lesen** und **Kein Zugriff** zur Auswahl.
 - iii. **Superuser-Zugriff:** Auswahl von **Ja** oder **Nein**.
 - iv. **NFS-Version:** Zur Auswahl stehen **Alle**, **NFSv3** oder **NFSv4**.
6. **Anwenden** auswählen.

Verwalten der SMB/CIFS-Freigabe für ein Volume in NetApp Workload Factory

Die Verwaltung einer SMB/CIFS-Freigabe eines Volumes in Workload Factory umfasst das Erstellen und Löschen von SMB/CIFS-Freigaben sowie das Festlegen der Benutzer und Gruppen, denen Zugriff gewährt wird, und des Levels der Berechtigungen, die ihnen erteilt werden.

Bevor Sie beginnen

Bevor Sie beginnen, sind die folgenden Schritte auszuführen:

- Um SMB/CIFS-Freigaben zu verwalten, muss eine Verknüpfung hergestellt werden. "[Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen](#)". Nach der Verknüpfung ist eine Rückkehr zu diesem Vorgang erforderlich.
- Zu bestimmen sind die Benutzer oder Gruppen, denen Zugriff gewährt werden soll, sowie die Level an Berechtigungen, die ihnen erteilt werden sollen.

Erstellen einer SMB/CIFS-Freigabe für ein Volume

Die folgenden Schritte dienen zum Erstellen einer SMB/CIFS-Freigabe für ein Volume.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Volumes explorer**.
3. Wählen Sie das Aktionsmenü des Volumes aus, für das die SMB-Freigabe geändert werden soll.
4. Die Auswahl erfolgt über **Advanced actions** und anschließend **Manage SMB/CIFS shares**.
5. Auf der Seite **Manage SMB/CIFS shares** erfolgt die Auswahl von **Create SMB/CIFS share**.
6. Im Dialogfeld „SMB/CIFS-Freigabe erstellen“ sind folgende Angaben erforderlich:
 - a. **Name:** Feld für den Namen der SMB/CIFS-Freigabe.
 - b. **Pfad:** Es ist möglich, den Pfad entweder mit dem Standard-Volumenamen zu definieren oder eine Freigabe für ein internes Verzeichnis anzugeben.

Gültige Pfadeingaben für den Volume-Namen, zum Beispiel "avocado", lauten wie folgt:

- /avocado
- /avocado/folder
- /avocado/folder/subfolder
- /avocado/file-name

Gültige Pfadeingaben für den Freigabenamen, zum Beispiel „Server“, lauten wie folgt:

- \\Server
- \\Server\Projects
- \\Server\Projekte\Gemeinsame Ressourcen

- c. **Berechtigungen:** „Vollzugriff“, „Lesen/Schreiben“, „Lesen“ oder „Kein Zugriff“ auswählen und anschließend die Benutzer oder Gruppen durch ein Semikolon (;) getrennt eingeben. Bei Benutzern oder Gruppen muss die Groß-/Kleinschreibung beachtet werden, und die Domäne des Benutzers muss im Format „domain\username“ angegeben werden.

7. **Erstellen** auswählen.

SMB/CIFS-Freigabe für ein Volume ändern

Nachfolgend sind die Schritte zum Ändern der SMB/CIFS-Freigabeeinstellungen für ein Volume beschrieben.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
- 2.

Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.

3. Auf der Registerkarte **FSx for ONTAP** wird im Aktionsmenü des Dateisystems mit dem zu aktualisierenden Volume die Option **Manage** ausgewählt.
4. In der Dateisystemübersicht erfolgt die Auswahl der Registerkarte **Volumes**.
5. Auf der Registerkarte „Volumes“ erfolgt die Auswahl des Aktionsmenüs des Volumes, für das die SMB-Freigabe geändert werden soll.
6. Die Auswahl erfolgt über **Advanced actions** und anschließend **Manage SMB/CIFS shares**.
7. Auf der Seite „SMB/CIFS-Freigaben verwalten“ die Option **Anzeigen und bearbeiten** auswählen.
8. Änderung der SMB/CIFS-Zugriffsberechtigungen oder der Benutzer bzw. Gruppen, denen Berechtigungen erteilt werden sollen.

Änderungen könnten dazu führen, dass aktuelle Benutzer oder Gruppen den Zugriff auf die SMB/CIFS-Freigabe verlieren.

9. Mit **Anwenden** werden die Änderungen gespeichert.

Löschen einer SMB/CIFS-Freigabe für ein Volume

Nachfolgend sind die Schritte zum Löschen einer SMB/CIFS-Freigabe für ein Volume aufgeführt.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Auf der Registerkarte **FSx for ONTAP** wird im Aktionsmenü des Dateisystems mit dem zu aktualisierenden Volume die Option **Manage** ausgewählt.
4. In der Dateisystemübersicht erfolgt die Auswahl der Registerkarte **Volumes**.
5. Auf der Registerkarte „Volumes“ erfolgt die Auswahl des Aktionsmenüs des Volumes, für das die SMB-Freigabe geändert werden soll.
6. Die Auswahl erfolgt über **Advanced actions** und anschließend **Manage SMB/CIFS shares**.
7. Auf der Seite „SMB/CIFS-Freigaben managen“ kann im Aktionsmenü der SMB/CIFS-Freigabe die Option **Delete** ausgewählt werden.

Durch das Löschen der SMB/CIFS-Freigabe ist diese nicht mehr verfügbar und für alle Benutzer, die sie einbinden möchten, nicht mehr zugänglich.

8. Im Dialogfeld „SMB/CIFS-Freigabe löschen“ bestätigt die Auswahl von **Löschen** die Löschung.

Management von S3-Zugriffspunkten

Erstellen Sie S3-Zugriffspunkte für ein Volume in NetApp Workload Factory

Erstellen und Zuordnen von S3-Zugriffspunkten für ein Volume in NetApp Workload Factory.

Über diese Aufgabe

Amazon FSx for NetApp ONTAP ermöglicht NFS- und SMB-Dateisystemen den Zugriff auf S3-Daten und die

Anbindung an AWS-Services wie Amazon Bedrock, SageMaker, Athena, AWS Glue und mehr. Sie können AWS-Services mit all Ihren Objektspeicherdaten verbinden.

Binden Sie S3-Zugriffspunkte an NFS- und SMB-Volumes in einem FSx for ONTAP-Dateisystem an, damit AWS-Services auf Dateien zugreifen können, als befänden sie sich in einem S3-Bucket. Definieren Sie beim Anbinden des Zugriffspunkts eine eindeutige ID, wählen Sie den Dateizugriffstyp (UNIX oder Windows) aus und fügen Sie einen Benutzernamen für die Zugriffsberechtigung hinzu.

Nachdem Sie den S3-Zugriffspunkt eingebunden haben, wird er in der AWS Management Console mit einem eindeutigen Alias angezeigt. Verwenden Sie diesen Alias als S3-Bucket-Namen für AWS Services, wie Amazon Bedrock, um auf Dateien im FSx for ONTAP Volume zuzugreifen.

Sie können mehrere S3-Zugriffspunkte an ein einzelnes FSx for ONTAP volume anhängen, jeder mit einer eindeutigen Zugangsstufe, um eine Verbindung zu mehreren AWS Services herzustellen.

Bevor Sie beginnen

Bitte erfüllen Sie die folgenden Anforderungen, bevor Sie beginnen.

- Sie benötigen ein bestehendes Volume mit einem S3-Zugangspunkt. ["Erstellen Sie ein Volume mit einem S3-Zugriffspunkt"](#)
- Sie müssen ["Anmeldeinformationen mit der Berechtigungsrichtlinie operations and remediation gewähren"](#) in Workload Factory sein, um diese Aufgabe abzuschließen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Volumes explorer**.
3. Wählen Sie das Aktionsmenü für das Volume, das Sie verwenden möchten, dann **Erweiterte Aktionen** und anschließend **S3-Zugriffspunkte verwalten**.
4. Auf der Seite „S3-Zugriffspunkte verwalten“ wählen Sie **S3-Zugriffspunkt erstellen und zuordnen**.
5. Geben Sie auf der Seite **S3-Zugriffspunkt erstellen und verbinden** die folgenden Informationen an:
 - **Name des S3 access point**: Geben Sie den Namen des S3 access point ein.
 - **Benutzer**: Wählen Sie einen vorhandenen Benutzer mit Zugriff auf das Volume aus oder erstellen Sie einen neuen Benutzer.
 - **Benutzertyp**: Wählen Sie **UNIX** oder **Windows** als Benutzerart.
 - **Netzwerkconfiguration**: Wählen Sie **Internet** oder **Virtual private cloud (VPC)**. Die Wahl des Netzwerktyps bestimmt, ob der Zugriffspunkt über das Internet erreichbar ist oder auf eine bestimmte VPC beschränkt ist. Um die Journal-Tabellenfunktion zu nutzen, müssen Sie **Internet** als Netzwerkconfiguration auswählen.
 - **Inventartabelle**: Optional. Erfordert die `getObject` Berechtigung. Aktivieren Sie die Inventartabelle auf dem Volume, um Metadaten für alle Objekte zu generieren, die über den S3-Zugriffspunkt zugänglich sind, und es entstehen AWS S3-Anfragekosten. Weitere Informationen finden Sie unter ["Amazon S3 Preisdokumentation"](#). Die Tabelle wird alle 24 Stunden aktualisiert.
 - **S3 access point tags**: Optional können Sie bis zu 50 Tags hinzufügen oder entfernen.
6. **Erstellen** auswählen.

Verwandte Informationen

Optional können Sie die Journaltabellenfunktion mit S3-Zugriffspunkten in Workload Factory verwenden. Die Journaltabelleninfrastruktur erfasst und speichert Audit-Protokolle von Benutzerzugriffsereignissen und

Objektoperationen über Amazon FSx for ONTAP volume access points hinweg. Um die Journaltabellenfunktion zu aktivieren, müssen Sie die erforderliche AWS-Infrastruktur einrichten, einschließlich AWS CloudTrail, AWS CloudWatch, AWS S3 Buckets, AWS CloudWatch Protokollgruppen sowie AWS Identity and Access Management (IAM)-Rollen und -Richtlinien. ["Richten Sie die Journaltabelleninfrastruktur für NetApp Workload Factory ein."](#)

Weitere verwandte Themen:

["Bearbeiten oder Löschen von S3-Zugriffspunkten für ein Volume in NetApp Workload Factory"](#)

Verwaltung der S3-Zugriffspunkte für ein Volume in NetApp Workload Factory

Aktualisierung der S3-Zugriffspunktdetails oder Löschen von S3-Zugriffspunkten für ein Volume in NetApp Workload Factory.

Sie können die **Inventartabelle** für den Zugriffspunkt aktivieren oder deaktivieren. Die Inventartabelle generiert Metadaten für alle Objekte, auf die der S3-Zugriffspunkt zugreifen kann, und verursacht AWS S3-Anfragekosten. Weitere Informationen finden Sie unter ["Amazon S3 Preisdokumentation"](#).

S3 Zugriffspunkte für ein Volume bearbeiten

Bearbeiten Sie die S3-Zugriffspunkte für ein Volume in NetApp Workload Factory.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü  **Workloads > Storage > Volumes explorer**.
3. Wählen Sie das Aktionsmenü für das Volume aus, für das Sie die S3-Zugriffspunkte bearbeiten möchten, dann **Erweiterte Aktionen** und anschließend **S3-Zugriffspunkte verwalten**.
4. Wählen Sie auf dem Bildschirm **S3-Zugriffspunkte verwalten** das Menü Aktionen und dann **Zugriffspunkt bearbeiten** aus.
5. Nehmen Sie Aktualisierungen vor und wählen Sie dann **Anwenden**.

Um die Infrastruktur für die Journaltabellenfunktion einzurichten, müssen Sie **Internet** als Netzwerkconfiguration für den S3-Zugriffspunkt auswählen. ["Erfahren Sie, wie Sie die Journaltabelleninfrastruktur für NetApp Workload Factory einrichten."](#)

Details zum S3-Zugriffspunkt für ein Volume anzeigen

Zeigen Sie Details zu S3-Zugriffspunkten wie Alias, ARN und S3-URI an. Mit aktivierten Inventar- und Journaltabellen können Sie Metadaten und Audit-Protokolle von Benutzerzugriffsereignissen und Objektoperationen über alle S3-Zugriffspunkte hinweg einsehen.

Über diese Aufgabe

Wenn die Inventartabelle für das Volume aktiviert ist, können Sie Zugriffspunkt-, Inventartabellen- und Bucket-Details der vorhandenen S3-Zugriffspunkte, die mit dem Volume verbunden sind, anzeigen. Das System stellt außerdem einen Link zur Inventartabelle in der AWS Management Console bereit.

Wenn die Protokolltabelle aktiviert ist, generiert Workload Factory Protokolle zu Zugriffspunkten in einer Tabelle, die Ihnen als Referenz dient. Die Tabelle enthält CloudTrail-Ereignisse, Trails (eine Aufzeichnung der AWS-Aktivitäten), CloudTrail-Filter, CloudWatch-Protokollgruppen und mehr.

Sie können die Zugangspunktdetails kopieren, um sie in anderen Anwendungen zu verwenden.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Storage > Volumes explorer**.
3. Im Aktionsmenü des Volumes, für das Details angezeigt werden sollen, erfolgt zunächst die Auswahl von **Erweiterte Aktionen** und anschließend **Details anzeigen**.

Die Details werden unter vier Registerkarten angezeigt: **Zugriffspunkt**, **Inventartabelle**, **Journaltabelle** und **Table bucket**.

4. Wenn der Status für Inventar- oder Journaltabellen aktiviert ist, Ihnen aber die `get:Object` Berechtigung fehlt, folgen Sie den Anweisungen im Dialogfeld, um die erforderliche Berechtigung hinzuzufügen.
5. Wenn der Status der Journaltabelle „Ausstehend“ ist, müssen Sie die CloudTrail-ARN angeben, um die Journaltabelle mit der erstellten Infrastruktur zu verbinden. Befolgen Sie die Anweisungen zur Bereitstellung des CloudFormation-Stacks mithilfe der AWS CLI oder der AWS Management Console und kehren Sie anschließend zur Workload Factory Konsole zurück, um die CloudTrail-ARN einzugeben.

Löschen Sie die S3-Zugriffspunkte für ein Volume in NetApp Workload Factory

Löschen Sie vorhandene S3-Zugriffspunkte von einem Volume in NetApp Workload Factory.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Storage > Volumes explorer**.
3. Wählen Sie das Aktionsmenü für das Volume aus, für das Sie S3-Zugriffspunkte verwalten möchten, dann **Erweiterte Aktionen** und anschließend **S3-Zugriffspunkte verwalten**.
4. Wählen Sie das Aktionsmenü für den S3-Zugriffspunkt, den Sie löschen möchten, und wählen Sie dann **Löschen**.
5. Im Dialogfeld **S3-Zugriffspunkt löschen** wählen Sie **Löschen**, um den S3-Zugriffspunkt vom Volume zu löschen.

Workload Factory löscht weder die Inventar- noch die Journaltabelle, aber Sie können sie manuell über die AWS Management Console entfernen.

Verwandte Informationen

- ["Einrichtung der Journaltabelleninfrastruktur"](#)

Einrichtung der Journaltabelleninfrastruktur für NetApp Workload Factory

Richten Sie die Journaltabelleninfrastruktur ein, um Audit-Logs von Benutzerzugriffsereignissen und Objektoperationen über Amazon FSx for ONTAP Volumezugriffspunkte hinweg zu erfassen und zu speichern. Mehrere Schritte sind erforderlich, um die Infrastruktur für AWS-Services wie AWS CloudTrail, AWS CloudWatch, AWS S3 Buckets, AWS CloudWatch log group, AWS Identity and Access Management (IAM) und AWS S3 Tables einzurichten, damit die Protokollereignisse korrekt durch die Pipeline gelangen und von Workload Factory gelesen werden.

Über diese Aufgabe

Die Journaltabellenfunktion erfasst S3-Datenebenenereignisse (PutObject, GetObject, DeleteObject usw.) für überwachte FSx for ONTAP S3-Zugriffspunkte. Sie nutzt eine Kette von AWS-Services, die in Ihrem AWS-Konto bereitgestellt werden. Wenn Sie die Infrastruktur korrekt einrichten, stellt sie eine Verbindung zum FSx for ONTAP-Volumen-Zugriffspunkt her und richtet die Pipeline ein, die Benutzerzugriffs- und Objektoperations-Audit-Ereignisse in der Journaltabelle erfasst.

Die folgende Tabelle listet die AWS-Services auf, die Teil der Infrastruktur sind, ihre jeweiligen Ressourcennamensmuster und den Zweck des Services in der Pipeline.

AWS-Service	Ressourcennamensmuster	Zweck
AWS CloudFormation	netapp-metadata-*	Stellt die gesamte Infrastruktur als Stack bereit
AWS S3-Bucket	netapp-metadata-cloudtrail-events-logs-{uuid}	Speichert rohe CloudTrail-Protokolldateien
AWS CloudTrail	netapp-metadata-journal-data-events-trail-{uuid}	Erfasst S3-Datenereignisse für bestimmte Zugriffspunkte
AWS CloudWatch-Protokollgruppe	netapp-metadata-journal-data-events-{uuid}	Empfängt CloudTrail-Ereignisse als strukturierte Protokolleinträge
IAM-Rollen	- netapp-metadata-cloudtrail-cw-role-{uuid} - netapp-metadata-s3table-integration-role-{uuid}	Aktive Integration
ObservabilityAdmin	S3TableIntegration	Bridges CloudWatch Logs in eine S3 Tables-Tabelle
S3-Tabellen	aws-cloudwatch Bucket → logs.aws_cloudtrail__data	Speichert strukturierte, abfragbare CloudTrail-Ereignisse im Iceberg-Format

Das {uuid} ist eine zufällige 8-stellige Kennung, die beim Erstellen der Vorlage generiert wird.

Bevor Sie beginnen

Um die Journaltabellenfunktion zu aktivieren, führen Sie folgende Schritte aus:

- Sie haben ein bestehendes Volume mit einem S3-Zugangspunkt. "[Erstellen Sie ein Volume mit einem S3-Zugriffspunkt](#)"
- Stellen Sie die Netzwerkkonfiguration für den S3-Zugangspunkt auf **Internet** ein. "[Netzwerkkonfiguration für den S3-Zugangspunkt bearbeiten](#)".
- "[Gewähren Sie die Berechtigungen für operations and remediation](#)" zu Ihren Workload Factory-Anmeldeinformationen.
- Fügen Sie dem AWS-Konto, das Sie zum Ausführen der CloudFormation-Bereitstellung verwenden, die folgenden IAM-Richtlinienberechtigungen hinzu, um die Journaltabelle einzurichten.

▼ IAM-Richtlinienberechtigungen für die Journaltabelleneinrichtung

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "CFNStack",
    "Effect": "Allow",
    "Action": [
      "cloudformation:CreateStack",
      "cloudformation:DescribeStacks",
      "cloudformation:DescribeStackEvents"
    ],
    "Resource": "arn:aws:cloudformation:*:*:stack/netapp-
metadata-*/*"
  },
  {
    "Sid": "StarResources",
    "Effect": "Allow",
    "Action": [
      "cloudformation:GetTemplateSummary",
      "cloudtrail:DescribeTrails",
      "logs:DescribeLogGroups",
      "logs:ListSourcesForS3TableIntegration",
      "observabilityadmin:CreateS3TableIntegration",
      "observabilityadmin:GetS3TableIntegration",
      "observabilityadmin:TagResource",
      "observabilityadmin:ListTagsForResource"
    ],
    "Resource": "*"
  },
  {
    "Sid": "S3Bucket",
    "Effect": "Allow",
    "Action": [
      "s3:CreateBucket",
      "s3:PutBucketPolicy",
      "s3:PutBucketTagging"
    ],
    "Resource": "arn:aws:s3:::netapp-metadata-*"
  },
  {
    "Sid": "IAMRoles",
    "Effect": "Allow",
    "Action": [
      "iam:CreateRole",
      "iam:PutRolePolicy",
      "iam:TagRole",
      "iam:GetRole"
    ]
  }
]

```

```

    ],
    "Resource": "arn:aws:iam::*:role/netapp-metadata-*"
  },
  {
    "Sid": "PassRole",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/netapp-metadata-*",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": [
          "cloudtrail.amazonaws.com",
          "logs.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid": "CloudTrail",
    "Effect": "Allow",
    "Action": [
      "cloudtrail:CreateTrail",
      "cloudtrail:StartLogging",
      "cloudtrail:AddTags",
      "cloudtrail:PutEventSelectors"
    ],
    "Resource": "arn:aws:cloudtrail::*:trail/netapp-metadata-*"
  },
  {
    "Sid": "CWLogGroup",
    "Effect": "Allow",
    "Action": [
      "logs:CreateLogGroup",
      "logs>DeleteLogGroup",
      "logs:PutRetentionPolicy",
      "logs:TagResource",
      "logs:AssociateSourceToS3TableIntegration"
    ],
    "Resource": "arn:aws:logs::*:log-group/netapp-metadata-*"
  },
  {
    "Sid": "S3Table",
    "Effect": "Allow",
    "Action": [
      "s3tables>CreateTableBucket",

```

```

        "s3tables:PutTableBucketEncryption",
        "s3tables:PutTableBucketPolicy"
    ],
    "Resource": "arn:aws:s3tables:*:*:bucket/aws-cloudwatch"
}
]
}

```

Einrichtung der Journaltabelleninfrastruktur

Richten Sie die Infrastruktur so ein, dass AWS-Serviceereignisse vom S3-Zugriffspunkt in der Journaltabelle erfasst werden.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** erfolgt die Auswahl von **Manage** im Aktionsmenü des Dateisystems mit dem zu aktualisierenden Volume.
4. In der Dateisystemübersicht erfolgt die Auswahl der Registerkarte **Volumes**.
5. Wählen Sie auf der Registerkarte „Volumes“ das Aktionsmenü für das Volume aus, für das Sie S3-Zugriffspunkte verwalten möchten, dann wählen Sie **Erweiterte Aktionen** und anschließend **S3-Zugriffspunkte verwalten**.
6. Wählen Sie auf dem Bildschirm **S3-Zugriffspunkte verwalten** das Menü Aktionen und dann **Zugriffspunkt bearbeiten** aus.
7. Im Dialogfeld **S3-Zugriffspunkt bearbeiten** stellen Sie sicher, dass die Netzwerkkonfiguration auf **Internet** eingestellt ist.
8. Folgen Sie den Anweisungen im Dialogfeld, um die Infrastruktur für die Journaltabellenfunktion einzurichten.
9. Laden Sie die CloudFormation-Vorlage herunter.
10. Stellen Sie den CloudFormation Stack in Ihrem AWS-Konto bereit.
 - a. Speichern Sie die JSON-Vorlage in einer Datei.
 - b. Stellen Sie die Vorlage mithilfe der AWS CLI oder der AWS Management Console bereit.
 - c. Warten Sie, bis der Stapel den `CREATE_COMPLETE` Status erreicht hat.
 - d. Ermitteln Sie den CloudTrail ARN aus den Stack-Ausgaben.
11. Kehren Sie zur Workload Factory-Konsole zurück und dann zurück zum Volume, für das Sie S3-Zugriffspunkte verwalten möchten.
12. Wählen Sie im Menü für Volume-Aktionen die Option **Details anzeigen** aus.
13. Geben Sie im Tab **Journaltabelle** die CloudTrail ARN ein.
14. **Anwenden** auswählen.

Sollte einer der Schritte fehlschlagen, [Fehlerbehebung bei der Infrastruktureinrichtung für die Journaltabelle](#) oder wenden Sie sich an den NetApp Support, um Hilfe zu erhalten.

Beheben Sie Probleme bei der Infrastruktureinrichtung für die Journaltabelle

Mithilfe der AWS Management Console oder der AWS CLI können Sie Fehler während der CloudFormation-Stack-Bereitstellung und der von ihr erstellten Ressourcen beheben.

Nach Behebung des Problems übermitteln Sie den CloudTrail ARN erneut, um die Einrichtung der Journaltabelle neu zu starten.

Häufige CloudFormation Bereitstellungsfehler

Unzureichende IAM-Berechtigungen

Die Rolle/der Benutzer, der die Bereitstellung durchführt, benötigt bestimmte Berechtigungen. Siehe [Bevor Sie beginnen](#) für die vollständige Richtlinie.

Falls der Stack mit einem `AccessDenied` oder `InsufficientPermission` Fehler fehlschlägt, überprüfen Sie die Stack-Ereignisse und suchen Sie im `ResourceStatusReason` Feld nach der fehlenden Berechtigung.

CloudTrail-Limit

AWS legt standardmäßig ein Limit von 5 Trails pro Region fest. Wenn das Konto bereits 5 Trails enthält, schlägt die `FsxDataEventTrail` die Ressource mit folgender Fehlermeldung fehl: `Maximum number of trails (5) exceeded`. Sie können die Anzahl der Trails auf regionaler Ebene mit folgendem Befehl überprüfen:

```
aws cloudtrail describe-trails \
  --no-include-shadow-trails \
  --region <region> \
  --query "length(trailList)"
```

Auflösungsoptionen

- Option 1: Löschen Sie einen nicht verwendeten Pfad in der Region, um Platz zu schaffen.
- Option 2: Verwenden Sie einen vorhandenen Trail. Entfernen Sie die `FsxDataEventTrail`, `CloudTrailBucket`, `CloudTrailBucketPolicy`, und `CloudTrailToCloudWatchRole` Ressourcen aus der Vorlage, bevor Sie den CloudFormation Stack erneut bereitstellen. Übergeben Sie dann den ARN Ihres vorhandenen Trails während des Initialisierungsschritts. Der vorhandene Trail muss eine CloudWatch Loggruppe konfiguriert haben, eine mit der Loggruppe verknüpfte `S3TableIntegration` besitzen und Datenereignisse protokollieren.

Die S3-Tabellenintegration ist bereits vorhanden.

Wenn das Konto bereits eine `S3TableIntegration` für die Datenquelle `aws_cloudtrail` besitzt, schlägt die Ressource `LogsToS3TableIntegration` fehl.

Auflösung

Entfernen Sie die `LogsToS3TableIntegration` und `S3TableIntegrationRole` Ressourcen aus der Vorlage, bevor Sie den CloudFormation-Stack erneut bereitstellen. Das System verwendet automatisch die bestehende Integration, solange Sie diese für `aws_cloudtrail data events` konfigurieren.

Um zu prüfen, ob eine Integration bereits besteht:

```
aws observabilityadmin list-s3-table-integrations --region <your-region>
```

S3-Bucket-Name existiert bereits

Der Bucket-Name `netapp-metadata-cloudtrail-events-logs-{uuid}` ist weltweit eindeutig. Bei einer Namenskollision muss die Vorlage erneut angefordert werden, um eine neue UUID zu erhalten.

IAM-Rolle existiert bereits

Falls bei einer vorherigen Teilbereitstellung IAM-Rollen mit dem `netapp-metadata-*` Namensmuster zurückgeblieben sind, schlägt die Rollenerstellung im Stack fehl. Löschen Sie zuerst die verwaisten Rollen:

```
aws iam delete-role-policy \
  --role-name netapp-metadata-cloudtrail-cw-role-<uuid> \
  --policy-name <policy-name>
aws iam delete-role \
  --role-name netapp-metadata-cloudtrail-cw-role-<uuid>
```

Fehler nach Aktivierung der Journaltabelle

Nach der Übermittlung des CloudTrail ARN validiert Workload Factory die gesamte Ressourcenpipeline, indem automatisch ein Seed- (Test-)Ereignis gesendet wird. Bei Erfolg wird das Seed-Ereignis in der S3 Tables-Tabelle angezeigt. Der Test dauert etwa 10 Minuten.

Wenn die Testvalidierung fehlschlägt, erhalten Sie möglicherweise eine der folgenden Fehlermeldungen:

Fehlermeldung	Bedeutung
Die Tabelle <code>aws_cloudtrail__data</code> wurde nicht in {bucket} erstellt. Überprüfen Sie die Berechtigungen für <code>s3table</code> .	S3TableIntegration hat die von CloudWatch verwaltete Tabelle nicht erstellt. Die Pipeline zwischen CloudWatch Logs und S3-Tabellen ist unterbrochen.
Die Tabelle ist vorhanden, aber das Journal-Seed-Ereignis wird nicht angezeigt. Überprüfen Sie CloudTrail und CloudWatch Berechtigungen.	Die Tabelle existiert, aber das entsprechende Seed-Ereignis ist nie eingetroffen. Die Pipeline ist zwischen CloudTrail und der S3 Tables-Tabelle unterbrochen.
Die Einrichtung des Journals ist fehlgeschlagen. ...	Beim Hintergrundprozess (Seed/Poll) ist ein Fehler aufgetreten. Prüfen Sie die nachfolgende Meldung für Details.

Lösungsschritte

Wenn das Journal den Status „FEHLGESCHLAGEN“ erreicht, verfolgen Sie das Ausgangsereignis durch die Pipeline-Phasen, um genau zu ermitteln, wo es abgebrochen wurde. Jeder Schritt ist einer bestimmten AWS-Ressource zugeordnet, die von der Vorlage erstellt wurde.

1. Überprüfen Sie den CloudTrail S3-Bucket.

Der Trail schreibt Rohereignisprotokolle in den S3-Bucket `netapp-metadata-cloudtrail-events-logs`. Suchen Sie nach den neuesten Protokolldateien.

Wenn keine Protokolldateien vorhanden sind, erfasst CloudTrail keine Ereignisse. Überprüfen Sie Folgendes:

- Der Trail wird protokolliert (`IsLogging: true`)
- Die erweiterten Ereigniselektoren enthalten den korrekten Zugriffspunkt-ARN
- Die erweiterten Ereigniselektoren umfassen die Filter für `eventCategory = Data` und `resources.type = AWS::S3::AccessPoint`

2. Überprüfen Sie die CloudWatch Log Group.

Der Pfad übermittelt außerdem Ereignisse an die CloudWatch Log Group. Der Name der Log Group beginnt mit `netapp-metadata-journal-data-events-<uuid>`.

- Wenn die Protokollgruppe leer ist, liefert CloudTrail keine Ereignisse an CloudWatch. Überprüfen Sie, ob die `CloudTrailToCloudWatchRole` IAM-Rolle existiert und über `logs:CreateLogStream` und `logs:PutLogEvents` Berechtigungen verfügt und ob der Trail mit den korrekten `CloudWatchLogsLogGroupArn` und `CloudWatchLogsRoleArn` konfiguriert ist.
- Wenn das Ausgangsereignis in der Protokollgruppe erscheint, liegt das Problem in einem nachfolgenden Schritt – fahren Sie mit Schritt 3 fort.

3. Überprüfen Sie die Tabelle S3 Tables (`aws-cloudwatch`).

Die `S3TableIntegration` erstellt automatisch einen Tabellen-Bucket namens `aws-cloudwatch` und füllt eine Tabelle unter `logs.aws_cloudtrail__data`. Diese Tabelle wird erst erstellt, nachdem das erste Ereignis verarbeitet wurde.

- Wenn der `aws-cloudwatch`-Tabellen-Bucket nicht existiert, dann fehlen die `S3TableIntegrationRole` Berechtigungen. Es benötigt `s3tables:CreateTableBucket`, `s3tables:PutTableBucketEncryption` und `s3tables:PutTableBucketPolicy` — alle beschränkt auf `arn:aws:s3tables:*:*:bucket/aws-cloudwatch`.
- Wenn der Tabellen-Bucket existiert, aber `logs.aws_cloudtrail__data` nicht, dann leitet die Integration keine Ereignisse weiter. Die Integration muss `Status: ACTIVE` anzeigen und `aws_cloudtrail` als Protokollquelle einbinden.
- Existiert die Tabelle, ist das entsprechende Ereignis aber nicht darin enthalten, befindet es sich möglicherweise noch in der Übertragung. Die Datenaufnahme in S3-Tabellen kann eine gewisse Latenz aufweisen. Warten Sie einige Minuten. Sollte das Ereignis nach 15–20 Minuten immer noch nicht angezeigt werden, ist die Integration möglicherweise fehlgeschlagen.

4. Fragen Sie das Seed-Ereignis direkt ab.

- Öffnen Sie die S3-Tabellen in der AWS-Managementkonsole.
- Navigieren Sie zum `aws-cloudwatch table bucket` → `aws_cloudtrail__data table` und verwenden Sie die Schaltfläche **Vorschau**, um eine Schnellabfrage direkt im Browser auszuführen.
- Wenn das Ereignis in der Tabelle vorhanden ist, das Journal aber immer noch `FAILED` anzeigt, dann ist das Abfragefenster möglicherweise abgelaufen, bevor das Ereignis eingetreten ist.

Nachdem das Problem behoben wurde, kehren Sie zur Workload Factory-Konsole zurück. Versuchen Sie es [Initialisierung der Journaltabelleneinrichtung](#) erneut, indem Sie den Trail-ARN erneut übermitteln.

- Sollte die Einrichtung weiterhin fehlschlagen, wenden Sie sich an den NetApp Support, um Unterstützung zu erhalten.

Berechtigungsreferenz für die Einrichtung der Journaltabelle

Die IAM-Rolle, die den CloudFormation-Stack zur Aktivierung der Journaltabellenfunktion bereitstellt, benötigt die folgenden Berechtigungen. Siehe [Bevor Sie beginnen](#) für eine kopierbare JSON-Richtlinie mit den erforderlichen Berechtigungen.

Stapeloperationen

Berechtigung	Ressource	Warum
cloudformation:CreateStack	arn:aws:cloudformation:*:*:stack/netapp-metadata-/	Erstellen Sie den Stapel
cloudformation:DescribeStacks	arn:aws:cloudformation:*:*:stack/netapp-metadata-/	Stack-Status überwachen
cloudformation:DescribeStackEvents	arn:aws:cloudformation:*:*:stack/netapp-metadata-/	Diagnose von Fehlern auf Ressourcenebene cloudformation:GetTemplateSummary * Vorabprüfung der Vorlage

CloudTrail

Berechtigung	Ressource	Warum
cloudtrail:CreateTrail	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	Erstelle den Pfad
cloudtrail:StartLogging	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	Protokollierung aktivieren
cloudtrail:AddTags	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	Identifikationsetikett anbringen
cloudtrail:PutEventSelectors	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	Datenerfassungsereignisse konfigurieren
cloudtrail:DescribeTrails	*	Trail-ARN für Stack-Ausgabe auflösen

S3

Berechtigung	Ressource	Warum
s3:CreateBucket	arn:aws:s3:::netapp-metadata-*	Erstelle den CloudTrail Log-Bucket
s3:PutBucketPolicy	arn:aws:s3:::netapp-metadata-*	Erlauben Sie CloudTrail, Protokolle zu schreiben
s3:PutBucketTagging	arn:aws:s3:::netapp-metadata-*	Identifikationsetikett anbringen

IAM

Berechtigung	Ressource	Warum
iam:CreateRole	arn:aws:iam:*:*:role/netapp-metadata-*	Erstellen Sie beide IAM-Rollen

Berechtigung	Ressource	Warum
iam:PutRolePolicy	arn:aws:iam::*:role/netapp-metadata-*	Inline-Richtlinien anhängen
iam:TagRole	arn:aws:iam::*:role/netapp-metadata-*	Identifikationsetikett anbringen
iam:GetRole	arn:aws:iam::*:role/netapp-metadata-*	Bestätigen, dass die Rolle aktiv ist
iam:PassRole	arn:aws:iam::*:role/netapp-metadata-* (Bedingung: PassedToService = cloudtrail.amazonaws.com, logs.amazonaws.com)	Rollen an CloudTrail und CloudWatch Logs übergeben

CloudWatch Logs

Berechtigung	Ressource	Warum
Protokolle:CreateLogGroup	arn:aws:logs::*:log-group/netapp-metadata-*	Protokollgruppe erstellen
Protokolle>DeleteLogGroup	arn:aws:logs::*:log-group/netapp-metadata-*	Protokollgruppe bereinigen, falls die Erstellung fehlgeschlagen ist
Protokolle:PutRetentionPolicy	arn:aws:logs::*:log-group/netapp-metadata-*	30-tägige Aufbewahrungsfrist festlegen
Protokolle:TagResource	arn:aws:logs::*:log-group/netapp-metadata-*	Identifikationsetikett anbringen
logs:AssociateSourceToS3TableIntegration	arn:aws:logs::*:log-group/netapp-metadata-*	Verknüpfen Sie die CloudTrail-Quelle mit S3-Tabellen
Protokolle:DescribeLogGroups	*	Prüfen Sie, ob die Protokollgruppe existiert
logs:ListSourcesForS3TableIntegration	*	Integrationsassoziation bestätigen

ObservabilityAdmin

Berechtigung	Ressource	Warum
observabilityadmin:CreateS3TableIntegration	*	Erstellen Sie die CloudWatch → S3-Tabellen-Brücke
observabilityadmin:GetS3TableIntegration	*	Bestätigen Sie, dass die Integration aktiv ist.
observabilityadmin:TagResource	*	Identifikationsetikett anbringen
observabilityadmin:ListTagsForResource	*	Drifterkennung

S3-Tabellen

Berechtigung	Ressource	Warum
s3tables:CreateTableBucket	arn:aws:s3tables:*:*:bucket/aws-cloudwatch	Erstellen Sie den S3-Tables-Bucket (über die Integrationsrolle)
s3tables:PutTableBucketEncryption	arn:aws:s3tables:*:*:bucket/aws-cloudwatch	AES256-Verschlüsselung einstellen
s3tables:PutTableBucketPolicy	arn:aws:s3tables:*:*:bucket/aws-cloudwatch	Zugriff auf CloudWatch Logs zulassen

Aufteilen eines geklonten Volume in NetApp Workload Factory

Trennen eines geklonten FlexVol Volumes von seinem übergeordneten Volume, um den Klon in ein normales lesen/schreiben FlexVol Volume in NetApp Workload Factory umzuwandeln.

Die Daten sind während der Aufteilung sowohl auf dem Klon als auch auf dem übergeordneten System zugänglich. Der Aufteilungsprozess aktualisiert lediglich Metadaten und erfordert nur minimale IO. Es werden keine Datenblöcke kopiert.

Über diese Aufgabe

Der Vorgang der Klonteilung umfasst Folgendes:

- Neue Snapshot-Kopien des FlexClone Volumes können während des Split-Vorgangs nicht erstellt werden.
- Ein FlexClone volume kann nicht vom übergeordneten Volume getrennt werden, wenn es Teil einer Datensicherungsbeziehung ist.
- Wenn das FlexClone Volume während eines laufenden Aufteilungsvorgangs offline genommen wird, wird der Aufteilungsprozess ausgesetzt; wenn das FlexClone Volume wieder online geschaltet wird, setzt sich der Aufteilungsprozess fort.
- Nach der Aufteilung benötigen sowohl das übergeordnete FlexVol Volume als auch der Klon den vollen Speicherplatz, der durch ihre Volume-Garantien bestimmt wird.
- Nachdem ein FlexClone volume von seinem übergeordneten Volume getrennt wurde, können die beiden nicht wieder zusammengeführt werden.

Bevor Sie beginnen

Vor dem Aufteilen eines geklonten Volume ist Folgendes zu beachten:

- Um ein geklontes Volume aufzuteilen, muss eine Verknüpfung hergestellt werden. ["Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen"](#). Nach der Verknüpfung ist eine Rückkehr zu diesem Vorgang erforderlich.
- Das FlexClone volume muss online sein, wenn der Split-Vorgang beginnt.
- Das übergeordnete Volume muss online sein, damit die Aufteilung erfolgreich ist.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Volumes explorer**.

3. Wählen Sie das Aktionsmenü des Volumes mit dem zu trennenden geklonten Volume aus.
4. Auszuwählen sind **Datenschutzaktionen** und anschließend **Geklontes Volume aufteilen**.
5. Im Dialogfeld „Volume teilen“ ist die Option **Löschen** auszuwählen.

Ergebnis

Der Klon des Volumes ist aufgeteilt und erscheint auf der Registerkarte „Volumes“.

Löschen eines Volumes in NetApp Workload Factory

Ein nicht mehr benötigtes Volume in Ihrem FSx for ONTAP Dateisystem kann gelöscht werden, um Speicherplatz freizugeben. Dieser Vorgang ist unumkehrbar.

Bevor Sie beginnen

Vor dem Löschen eines Volume ist Folgendes zu berücksichtigen:

- Replikationsbeziehungen: Sie müssen "[Löschen aller bestehenden Replikationsbeziehungen](#)" dieses Volume überprüfen, bevor Sie es löschen, damit keine fehlerhaften Beziehungen zurückbleiben.
- Lokale Snapshots: Alle mit diesem FSx for ONTAP Dateisystem verknüpften Snapshots werden dauerhaft gelöscht.
- Volume backups: Die Volume-Backup-Kopien bleiben erhalten und können weiterhin verwendet werden.
- Unveränderliche Dateien und Snapshots: Volumes, die unveränderliche Dateien und Snapshots enthalten, können erst nach Ablauf der Aufbewahrungsfrist gelöscht werden.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Volumes explorer**.
3. Das Aktionsmenü des zu löschenden Volumes auswählen.
4. Die Auswahl erfolgt über **Grundlegende Aktionen** und anschließend **Volume löschen**.
5. Im Dialogfeld „Volume löschen“ sind folgende Schritte erforderlich:
 - a. Optional können Sie **Volume sichern** auswählen, um das Volume vor dem Löschen zu sichern.

Die Sicherungskopie bleibt im Dateisystem erhalten, bis Sie sie manuell löschen.
 - b. **Continue** ist auszuwählen.
 - c. Zum Löschen des Volume ist „delete“ einzugeben.
 - d. Zur Bestätigung ist **Löschen** auszuwählen.

Blockspeicher verwalten

Blockspeicher für ein Dateisystem in NetApp Workload Factory verwalten

Verwenden Sie NetApp Workload Factory, um die Verwaltung Ihrer Blockspeicherressourcen, einschließlich Initiatorgruppen und Blockgeräten, zu vereinfachen und den Clientzugriff auf FSx for ONTAP Blockgeräte zu steuern, um optimale Leistung zu erzielen und die Kosten zu minimieren.

Über diese Aufgabe

Über die Workload Factory-Konsole können Sie Initiatorgruppen (igroups) verwalten, um den Clientzugriff auf Blockgeräte zu steuern. Außerdem können Sie Details zu Blockgeräten anzeigen, die Kapazität erhöhen, Klone erstellen, den Clientzugriff verwalten, Daten inaktiver Blockgeräte archivieren und Blockgeräte löschen.

Prüfen Sie das Blockspeicherdiagramm, um Folgendes zu überprüfen:

- Clientverbindungen
- Blockgerätestatus
- Knoten-Client-Beziehung
- Möglicherweise fehlerhafte Clientverbindungen

Bevor Sie beginnen

- Sie müssen eine Verknüpfung herstellen, um Initiatorgruppen zu verwalten. "[Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen](#)". Nach der Verknüpfung kann zu diesem Vorgang zurückgekehrt werden.
- Sie müssen über eine vorhandene Initiatorgruppe oder ein Blockgerät verfügen, um sie anzuzeigen und zu verwalten.

Initiatorgruppen verwalten

Sie können Initiatorgruppen-Details anzeigen, den Clientzugriff verwalten und Initiatorgruppen löschen.

Clientzugriff für eine Initiatorgruppe verwalten

Verwalten Sie den Clientzugriff für eine bestehende Initiatorgruppe jederzeit.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** die Registerkarte **Blockgeräte** auswählen.
4. Wählen Sie den Ressourcentyp **Initiator groups (igroups)** aus, um vorhandene Initiatorgruppen anzuzeigen.
5. Gehen Sie zum Aktionsmenü für das Blockgerät und wählen Sie **Clientzugriff verwalten**.
6. Überprüfen Sie die für die Initiatorgruppe angezeigten Client-Zugriffsdetails.
7. Um Änderungen am Clientzugriff vorzunehmen, wählen Sie **Clientzugriff bearbeiten**.
8. Im Dialogfeld **Clientzugriff bearbeiten** können Sie Folgendes bearbeiten:
 - **Initiatorgruppenname**
 - **Initiatorgruppe Beschreibung**
 - **Name der Storage-VM**
 - **Name des Blockgeräts**
 - **Betriebssystemtyp**
 - **Host-Initiatoren**
9. **Anwenden** auswählen.

Eine Initiatorgruppe löschen

Löschen Sie eine Initiatorgruppe, wenn sie nicht mehr benötigt wird.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** die Registerkarte **Blockgeräte** auswählen.
4. Wählen Sie den Ressourcentyp **Initiator groups (igroups)** aus, um vorhandene Initiatorgruppen anzuzeigen.
5. Gehen Sie zum Aktionsmenü des Blockgeräts und wählen Sie dann **Initiatorgruppe löschen**.
6. Geben Sie im Dialogfeld „Initiatorgruppe (igroup) löschen“ „delete“ ein, um zu bestätigen, dass Sie die Initiatorgruppe löschen möchten, und wählen Sie dann **Löschen** aus.

Blockgeräte für eine Initiatorgruppe verwalten

Blockgeräte oder LUNs (logische Einheitennummern) sind Volumes mit Dateisystemen in einer SAN-Umgebung, die über ein Netzwerk für Hosts zugänglich sind.

Sie können Blockgeräte für FSx for ONTAP Dateisysteme managen, die das iSCSI-Protokoll verwenden.

Details des Blockgeräts

Die Details eines vorhandenen Blockgeräts lassen sich jederzeit anzeigen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** die Registerkarte **Blockgeräte** auswählen.
4. Im Aktionsmenü für das Blockgerät kann anschließend **Details anzeigen** ausgewählt werden.

Allgemeine Details sowie Informationen zu Verbrauch, Zugriff und Schutz für das Blockgerät werden angezeigt.

Clientzugriff für ein Blockgerät managen

Sie können den Clientzugriff für ein vorhandenes Blockgerät jederzeit managen, indem Sie Initiatorgruppen erstellen und Blockgeräte sowie Host-Initiatoren hinzufügen oder entfernen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** die Registerkarte **Blockgeräte** auswählen.
4. Sie wechseln zum Aktionsmenü des Blockgeräts und wählen anschließend **Clientzugriff verwalten** aus.
5. Falls keine Initiatorgruppe existiert, erstellen Sie eine neue Initiatorgruppe, indem Sie **Map igroup > Create igroup** auswählen, und gehen Sie dann wie folgt vor:

- a. **Blockgerätename:** Unter diesem Feld wird ein Blockgerätename eingegeben. Mehrere Blockgeräte können zur Zuordnung zur Initiatorgruppe ausgewählt werden.
 - b. **Betriebssystemtyp:** Der Betriebssystemtyp wird ausgewählt.
 - c. **Name der Initiatorgruppe:** Hier wird ein Name der Initiatorgruppe eingegeben.
 - d. **Beschreibung der Initiatorgruppe:** Optional ist die Eingabe einer Beschreibung der Initiatorgruppe möglich.
 - e. **Host-Initiatoren:** Eingabe von einem oder mehreren Host-Initiatoren. Diese Initiatoren müssen dem Format iSCSI Qualified Name (IQN) entsprechen.
 - f. **Erstellen** auswählen.
6. Wenn bereits eine Initiatorgruppe (igroup) existiert, wählen Sie **Initiatorgruppe zuordnen > Vorhandene Initiatorgruppe zuordnen**, um Blockgeräte und Host-Initiatoren zur Initiatorgruppe hinzuzufügen oder daraus zu entfernen, und wählen Sie dann **Zuordnen**.

Erhöhung der Kapazität eines Blockgeräts

Die Kapazität eines bestehenden Blockgeräts kann jederzeit erhöht werden.

Schritte

1. Melden Sie sich bei der "NetApp Console" an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** die Registerkarte **Blockgeräte** auswählen.
4. Anschließend können Sie im Aktionsmenü des Blockgeräts **Kapazität erhöhen** auswählen.
5. Die neue Kapazität für das Blockgerät und die Einheit werden eingegeben.
6. Zum Anwenden der Änderungen **Erhöhen** auswählen.



Nach der Vergrößerung des Blockgeräts befolgen Sie die Vorgehensweise Ihres Host-Betriebssystems, um die neue Größe zu ermitteln und das Dateisystem zu erweitern.

Klonen eines Blockgeräts

Sie können jederzeit einen Klon eines bestehenden Blockgeräts erstellen. Ein Blockgeräte-Klon ist eine beschreibbare Kopie des Original-Blockgeräts, die dieselben Datenblöcke verwendet, bis Änderungen entweder am Original oder am Klon vorgenommen werden. Das Klonen eines Blockgeräts ist eine schnelle und effiziente Methode, um wiederverwendbare Kopien Ihrer Daten zu erstellen, ohne zusätzlichen Storage zu verbrauchen.

Schritte

1. Melden Sie sich bei der "NetApp Console" an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** die Registerkarte **Blockgeräte** auswählen.
4. Navigieren Sie zum Aktionsmenü des Blockgeräts und wählen Sie dann **Blockgerät klonen**.
5. Geben Sie im Dialogfeld „Blockgerät klonen“ einen Namen für das geklonte Blockgerät ein.
6. Optional kann die automatische Löschung aktiviert werden, um das geklonte Blockgerät automatisch zu löschen, wenn der Speicherplatz auf dem Volume knapp wird.

7. **iSCSI-Konfiguration:** Optional. Um den Blockgeräteklon mit Host-Initiatoren zu verbinden, erstellen Sie entweder eine neue Initiatorgruppe oder ordnen Sie ihn einer vorhandenen Initiatorgruppe zu.
- **Neue Initiatorgruppe erstellen:** Wählen Sie diese Option, um eine neue Initiatorgruppe für den Klon des Blockgeräts zu erstellen. Geben Sie die folgenden Details ein:
 - i. **Host-Betriebssystem:** Wählen Sie den Typ des Host-Betriebssystems aus.
 - ii. **Name der Initiatorgruppe:** Geben Sie einen Initiatorgruppen-Namen ein.
 - iii. **Host-Initiatoren:** Eingabe von einem oder mehreren Host-Initiatoren. Diese Initiatoren müssen dem Format iSCSI Qualified Name (IQN) entsprechen.
 - **Zuordnung zu einer bestehenden Initiatorgruppe:** Wählen Sie diese Option, um den Klon des Blockgeräts einer bestehenden Initiatorgruppe zuzuordnen. Wählen Sie eine oder mehrere Initiatorgruppen aus, denen das Blockgerät zugeordnet werden soll.
8. Wählen Sie **Klonen**, um den Klon des Blockgeräts zu erstellen.

Archivieren Sie die Daten eines inaktiven Blockgeräts

Blockgeräte, die keinem Client mehr zugeordnet sind oder sieben Tage lang nicht verwendet wurden, werden als inaktive Blockgeräte eingestuft. Sie können die Daten eines inaktiven Blockgeräts in die Kapazitätspool-Ebene archivieren, um SSD-Kapazität zurückzugewinnen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** die Registerkarte **Blockgeräte** auswählen.
4. Unter „Verwaiste Geräte“ erfolgt die Auswahl von „Kapazität anzeigen und zurückgewinnen“.
5. Auf dem Bildschirm „Speicherplatz für ungenutzte Blockgeräte freigeben“ können Sie ein oder mehrere Blockgeräte auswählen, um die Daten zu archivieren und die Kapazität zurückzugewinnen.
6. **Archiv** auswählen.

Löschen eines Blockgeräts

Blockgeräte, die keinem Client zugeordnet sind oder sieben Tage lang nicht verwendet wurden, sind inaktive Blockgeräte. Durch diesen Vorgang wird die Zuordnung des ausgewählten Blockgeräts aufgehoben und es gelöscht. Wenn das Host-FlexVol-Volume keine Blockgeräte enthält, wird es von Workload Factory gelöscht.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** die Registerkarte **Blockgeräte** auswählen.
4. Unter „Verwaiste Geräte“ erfolgt die Auswahl von „Kapazität anzeigen und zurückgewinnen“.
5. Auf dem Bildschirm „Speicherplatz für ungenutzte Blockgeräte freigeben“ können Sie ein oder mehrere Blockgeräte auswählen, um die Daten zu archivieren und die Kapazität zurückzugewinnen.
6. Wählen Sie **Delete**.

Verwandte Informationen

- ["Erstellen einer Initiatorgruppe für ein FSx for ONTAP file system"](#)
- ["Erstellung eines Blockgeräts für ein FSx for ONTAP Dateisystem"](#)

Wenden Sie ONTAP-Tags auf Blockgeräte in NetApp Workload Factory an

Nutzen Sie das native EC2-Benutzerdatenskript von NetApp Workload Factory, um Blockgeräte während der AWS EC2-Instance-Bereitstellung automatisch zu erstellen und zu taggen. Fügen Sie das EC2-Benutzerdatenskript der Vorlage des Assistenten zum Starten von Instances hinzu, wenn Sie eine EC2-Instance über die AWS EC2-Konsole bereitstellen. Nach der Bereitstellung verwendet Workload Factory die vom Skript erfassten Metadaten, um Ihren Blockgeräten ONTAP-Tags zuzuweisen. Mithilfe dieser Tags können Sie erkennen, welcher Host welches Blockgerät verwendet, sodass Sie die Nutzung bei der Fehlerbehebung oder im Rahmen von Audits schnell dem zuständigen Host zuordnen können.

Über diese Aufgabe

Das EC2-Benutzerdatenskript erstellt Blockgeräte und wendet während der EC2-Instanzbereitstellung EC2-Tags auf ONTAP-Ebene auf die Blockgeräte an.

Das dem Blockgerät zugewiesene *EC2-Tag* enthält den EC2-Namen, die EC2-ID und den Mount-Pfad für das/die Blockgerät(e) innerhalb der EC2-Instanz.

Schritte

1. Folgen Sie ["Die Amazon Elastic Compute Cloud-Anleitung zum Starten einer EC2-Instanz"](#) dem Assistenten zum Starten der Instanz in der AWS EC2-Konsole.
2. Fügen Sie das EC2-Benutzerdatenskript zur Vorlage des Assistenten zum Starten von Instanzen hinzu, um Blockgeräte automatisch zu erstellen und zu kennzeichnen.

Gehen Sie zu unserem GitHub-Repository [FSx-ONTAP-sample-scripts](#), um die ["EC2-Benutzerdatenskript"](#) zu erhalten.

3. Starten Sie die Instanz.

Das EC2-Benutzerdatenskript wendet automatisch ONTAP-Tags auf neue Blockspeichergeräte an, die auf der EC2-Instanz gehostet werden.

4. Bei bestehenden EC2-Instanzen werden Benutzerdatenskripte erst nach einem Neustart wirksam.

Ergebnis

EC2-Tags erscheinen in der Blockgerätetabelle innerhalb des zugehörigen FSx for ONTAP file system.

Verwandte Informationen

- ["Erstellen Sie Initiatorgruppen \(igroups\) für ein Dateisystem in NetApp Workload Factory"](#)
- ["Blockspeicher für ein Dateisystem in NetApp Workload Factory verwalten"](#)

Dateisysteme verwalten

Dateisystemkapazität in NetApp Workload Factory anpassen

Die SSD-Speicherkapazität eines FSx for ONTAP Dateisystems kann an die Anforderungen von Workloads mit unterschiedlichen aktiven Arbeitssätzen in NetApp Workload Factory angepasst werden. Die Kapazität lässt sich manuell erhöhen, wenn die Nutzung den festgelegten Schwellenwert überschreitet, oder verringern, wenn die Arbeitssätze nicht genutzt werden, um Kosten zu sparen. Alternativ ist es möglich, das automatische Kapazitätsmanagement zu aktivieren, sodass Workload Factory inkrementellen Storage bei sich ändernden Anforderungen im Zeitverlauf hinzufügt und die manuelle Überwachung entfällt.



Die Verringerung der SSD Storage Kapazität wird nur für Dateisysteme der zweiten Generation unterstützt.

Dateisystemkapazität manuell anpassen

Mit elastischer Dateisystemkapazität können Sie die Kapazität Ihrer Dateisysteme dynamisch an die Bedürfnisse Ihrer Workloads anpassen.

Über diese Aufgabe

Eine Änderung der Dateisystemkapazität wirkt sich auf die IOPS Ihres FSx for ONTAP file system aus.

Bei der automatischen "[IOPS provisionieren](#)" Aktualisierung eines Dateisystems erhöht oder verringert sich die Anzahl der IOPS um 3 IOPS mit jeder Erhöhung oder Verringerung der SSD-Kapazität um 1 GiB.

Wenn Sie "[IOPS provisionieren](#)" manuell vorgehen, müssen Sie möglicherweise Ihre IOPS-Zuweisung erhöhen, um die erhöhte Dateisystemkapazität zu unterstützen.

Informationen zu SSD Storage-Kapazitätsgrenzen finden Sie "[Kontingente](#)" in der AWS FSx for NetApp ONTAP Dokumentation.

Bevor Sie beginnen

Um die Kapazität eines Dateisystems anzupassen, müssen Sie zuerst [automatisches Kapazitätsmanagement deaktivieren](#).

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Storage**.
3. Im Dashboard steht die Option **SSD-Kapazität anpassen** zur Auswahl.
4. Sie wählen das Dateisystem aus, dessen Kapazität Sie anpassen möchten, und anschließend **Weiter**.
5. Im Dialogfeld „SSD-Kapazität anpassen“ erfolgt die Eingabe einer Zahl für **Bereitgestellte Kapazität**.
6. Die Einheit für die provisionierte Kapazität auswählen.
7. **Anwenden** auswählen.

Automatische Kapazitäts- und Inode-Verwaltung aktivieren

Die Aktivierung von Kapazitätsmanagement und Inode-Management ermöglicht es der NetApp Workload Factory, automatisch inkrementellen Storage, ein FSx for ONTAP File System und Inodes (Dateien) zu einem

Volume hinzuzufügen, wenn sich der Kapazitätsbedarf im Laufe der Zeit ändert. Diese Funktionen machen die manuelle Überwachung von Kapazität und Inodes überflüssig.

Nur ein Konto kann diese Funktionen verwalten.

Automatisches Kapazitätsmanagement und Kapazitätsbenachrichtigungen aktivieren

Aktivieren Sie das automatische Kapazitätsmanagement, um inkrementellen Storage eines FSx for ONTAP-Dateisystems automatisch bis zur maximalen Größenbegrenzung hinzuzufügen. Richten Sie Benachrichtigungen ein, um Warnungen zu erhalten, wenn das Dateisystem einen bestimmten Kapazitätsschwellenwert erreicht.

Über diese Aufgabe

Workload Factory scannt das FSx for ONTAP-Dateisystem alle 30 Minuten, um zu prüfen, ob inkrementeller Storage hinzugefügt werden muss.

Die maximale SSD Storage-Kapazität für alle FSx for ONTAP Dateisysteme beträgt 524.288 GiB. Informationen zur Beantragung einer Kontingenterhöhung enthält "[Kontingente](#)" in der AWS FSx for NetApp ONTAP Dokumentation.

Bevor Sie beginnen

Vor Beginn ist Folgendes zu beachten:

- Sie müssen "[Zugangsdaten mit der Berechtigungsrichtlinie für Anzeigen, Planen und Analysieren gewähren](#)" in Workload Factory sein, um diese Aufgabe abzuschließen.
- Um sicherzustellen, dass die Anzahl der Volume-Inodes mit der Speicherkapazität zunimmt, muss eine Verknüpfung hergestellt werden. "[Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen](#)". Nach der Verknüpfung ist eine Rückkehr zu diesem Vorgang erforderlich.
- Sie sollten diese Funktion während der Datenmigration nicht aktivieren, da AWS eine Mindestabkühlphase von sechs Stunden zwischen SSD-Kapazitätserhöhungen vorschreibt. Diese Einschränkung kann Anpassungen verzögern, daher ist eine entsprechende Planung erforderlich.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Storage**.
3. Im Menü „Storage“ erfolgt die Auswahl von **Inventory**.
4. Unter **Inventar** erfolgt die Auswahl des Dateisystems, für das die automatische Kapazität aktiviert werden soll.

Das **Elastizitätsdiagramm** zeigt sowohl den Durchsatz als auch die SSD-Kapazität für das ausgewählte Dateisystem an.

5. Nach der Auswahl von **SSD** erfolgt die Auswahl von **Manage**.
6. Wählen Sie die Kapazitätsmanagement-Methode. Zur Auswahl stehen inkrementelle und adaptive Modi.
 - **Inkrementell:** Erhöht die Kapazität um einen festen Betrag bei Erreichen bestimmter Schwellenwerte.
 - **Schwellenwert:** Legen Sie einen Schwellenwert fest, der unterhalb der inkrementellen Erhöhung liegt, um eine Benachrichtigung vom Workload Factory Benachrichtigungsdienst auszulösen. Der Standardwert beträgt 70%.

Die Schwellenwerteinstellung ist nur verfügbar, wenn Sie ["den Workload Factory Benachrichtigungsdienst aktiviert"](#).

- **Schrittweise Erhöhung:** Geben Sie die maximale prozentuale Erhöhung für das FSx for ONTAP-Dateisystem ein. Der Standardwert beträgt 80%.

Dies ist der Schwellenwert, ab dem Workload Factory einen Auftrag zur Kapazitätserhöhung auslöst. Wenn beispielsweise das Dateisystem 80 % der Kapazität erreicht, erhöht Workload Factory die Kapazität.

- **Adaptiv:** Prognostiziert und ändert die Kapazität auf Basis historischer Daten.
 - **Rückblick:** Legen Sie den Analysezeitraum in Stunden fest, um zu bestimmen, wie viele historische Daten für Kapazitätsprognosen berücksichtigt werden sollen. Der Standardwert beträgt 120 Stunden.
 - **Planen Sie im Voraus:** Legen Sie die Pufferzeit in Stunden fest, um sicherzustellen, dass die Kapazität erhöht wird, bevor sie tatsächlich benötigt wird. Der Standardwert beträgt 48 Stunden.

7. Wählen Sie **Automatisches Kapazitätsmanagement** und die Berechtigungen *view, planning, and analysis* aus.

Alternativ kann die Funktion deaktiviert werden. Wenn die Dateisystemkapazität erhöht werden muss, muss zuerst das automatische Kapazitätsmanagement deaktiviert werden.

8. Wählen Sie **Kapazitätsbenachrichtigungen aktivieren**, um Benachrichtigungen zu erhalten, wenn die Kapazität den von Ihnen festgelegten Schwellenwert erreicht und wenn NetApp Workload Factory eine automatische Kapazitätserhöhung durchführt. Der Standardwert beträgt 70%.

Die Einstellung für Kapazitätsbenachrichtigungen ist nur verfügbar, wenn Sie ["den Workload Factory Benachrichtigungsdienst aktiviert"](#) und wenn automatisches Kapazitätsmanagement aktiviert ist.

9. **Anwenden** auswählen.

Ergebnis

Alle 30 Minuten wird ein Dateisystemscan durchgeführt, um festzustellen, ob zusätzliche Kapazität benötigt wird.

Aktivierung der automatischen Inode-Verwaltung für ein Dateisystem

Aktivieren Sie die automatische Inode-Verwaltung, um die Anzahl der Inodes (Dateien) pro Volume bis zum zulässigen Limit zu erhöhen.

Über diese Aufgabe

Workload Factory scannt das FSx for ONTAP Dateisystem alle 30 Minuten, um die verfügbaren Volume-Inodes zu überprüfen und zu prüfen, ob inkrementelle Inodes hinzugefügt werden müssen. Die Anzahl erhöht sich basierend auf den Schwellenwerten der automatischen Inode-Verwaltung.



Terraform-Nutzer: Terraform hat eine Einschränkung, die erfordert, dass alle Operationen innerhalb von Terraform abgeschlossen werden. Inode-Management wird in Terraform nicht unterstützt, die automatische Inode-Verwaltung lässt sich jedoch in der Workload Factory Konsole aktivieren.

Bevor Sie beginnen

Vor Beginn ist Folgendes zu beachten:

- Um Volume-Inodes automatisch zu verwalten, muss eine Verknüpfung hergestellt werden. ["Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen"](#). Nach der Verknüpfung ist eine Rückkehr zu diesem Vorgang erforderlich.
- Die automatische Inode-Verwaltung kann mit einem Warnschwellenwert eingerichtet werden, der eine Benachrichtigung vom Benachrichtigungsdienst von Workload Factory auslöst. Um diese Funktion zu nutzen, müssen Sie zunächst ["den Benachrichtigungsdienst von Workload Factory aktivieren"](#).
- Sie müssen ["Zugangsdaten mit der Berechtigungsrichtlinie für Anzeigen, Planen und Analysieren gewähren"](#) in Workload Factory sein, um diese Aufgabe abzuschließen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. Auf der Seite „FSx for ONTAP“ erfolgt die Auswahl von **Inventory**.
4. Im **Inventar** können Sie das Aktionsmenü des Dateisystems auswählen, für das die automatische Inode-Verwaltung aktiviert werden soll.
5. Auswahl von **Manage**.
6. Unter „Informationen“ befindet sich neben **Automatische Inode-Verwaltung** das Stiftsymbol. Das Stiftsymbol erscheint neben dem Dropdown-Pfeil, wenn sich der Mauszeiger über der Zeile **Automatische Inode-Verwaltung** befindet.
7. Im Dialogfeld **Automatische Inode-Verwaltung** sind folgende Angaben erforderlich:
 - a. **Anmeldeinformationen:** Im Dropdown-Menü werden Anmeldeinformationen mit *Automate*-Berechtigungen ausgewählt.
 - b. Die Aktivierung der **automatischen Inode-Verwaltung** erfolgt über die Schaltfläche „Aktivieren“.

Alternativ lässt sich die Funktion deaktivieren. Wenn die Anzahl der Inodes erhöht werden muss, muss zuerst die automatische Inode-Verwaltung deaktiviert werden.
 - c. **Warnschwelle:** Die Warnschwelle ist niedriger als die Schwellenerhöhung festzulegen, ab der eine Benachrichtigung vom Workload Factory Benachrichtigungsdienst ausgelöst wird. Der Standardwert beträgt 70 %.

Die Einstellung des Warnschwellenwerts ist nur verfügbar, wenn Sie ["den Workload Factory Benachrichtigungsdienst aktiviert"](#).
 - d. **Schwellenwerterhöhung:** Hier wird die maximale prozentuale Erhöhung der Anzahl der Inodes (Dateien) pro Volume eingegeben. Der Standardwert beträgt 80 %.
 - e. **Schrittweise Erhöhung:** Prozentsatz für die schrittweise Erhöhung der Anzahl der Inodes (Dateien). Der Standardwert ist 10%.
8. **Anwenden** auswählen.

Ergebnis

Alle 30 Minuten erfolgt ein Dateisystem-Scan, um festzustellen, ob die Volumes zusätzliche Inodes (Dateien) je Volume benötigen.

FSx for ONTAP Dateiseinstellungen in NetApp Workload Factory verwalten

Die Einstellungen eines FSx for ONTAP Dateisystems in NetApp Workload Factory

lassen sich verwalten. Tags für das Dateisystem können verwaltet, das fsxadmin Passwort bei Bedarf zurückgesetzt und die Durchsatzkapazität nach Bedarf aktualisiert werden.

Verwaltung von FSx for ONTAP Dateisystem-Tags

Tags können Ihnen bei der Kategorisierung Ihrer Ressourcen helfen. Sie können Tags für ein Dateisystem jederzeit in NetApp Workload Factory hinzufügen, bearbeiten und entfernen.

Schritte

1. Melden Sie sich bei der "NetApp Console" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Storage**.
3. Im Menü „Storage“ erfolgt die Auswahl von **Inventory**.
4. Im **Inventar** erfolgt die Auswahl von **Dateisystem-Tags verwalten** im Aktionsmenü des zu aktualisierenden Dateisystems.
5. Im Dialogfeld **Dateisystem-Tags verwalten** können Sie nach Bedarf Tags hinzufügen, bearbeiten oder entfernen.

Die maximale Anzahl von Tags, die Sie einem Dateisystem zuweisen können, beträgt 50.

6. **Anwenden** auswählen.

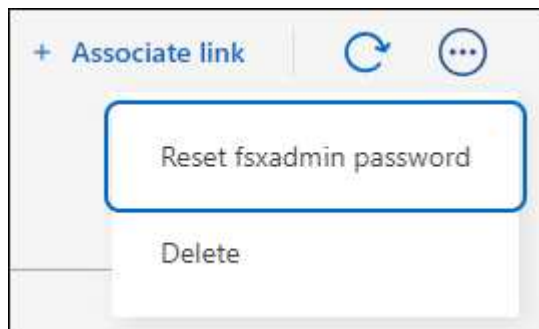
Das fsxadmin-Passwort eines FSx for ONTAP Dateisystems zurücksetzen

Das fsxadmin-Passwort in NetApp Workload Factory wird bei Bedarf zurückgesetzt.

Wenn Sie bei der Erstellung des Dateisystems einen alternativen Benutzer angegeben haben, können Sie das fsxadmin-Passwort nur in der AWS-Konsole zurücksetzen.

Schritte

1. Melden Sie sich bei der "NetApp Console" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Storage**.
3. Im Menü „Storage“ erfolgt die Auswahl von **Inventory**.
4. Im **Inventory** im Aktionsmenü des Dateisystems, für das das fsxadmin Passwort zurückgesetzt werden soll, **Manage** auswählen.
5. Die Auswahl des Menüs „Aktionen“ erfolgt in der Dateisystemübersicht.



6. Die Option **Reset fsxadmin password** ist auszuwählen.
7. Im Dialogfeld zum Zurücksetzen des fsxadmin Passworts wird ein neues fsxadmin Passwort eingegeben und zur Bestätigung erneut eingegeben.
8. **Anwenden** auswählen.

Aktualisierung der Durchsatzkapazität für ein FSx for ONTAP Dateisystem

Bei Bedarf lässt sich die Durchsatzkapazität für ein FSx for ONTAP Dateisystem in NetApp Workload Factory aktualisieren.

Informationen zu den Durchsatzkapazitätsgrenzen sind "[Kontingente](#)" in der AWS FSx for NetApp ONTAP Dokumentation enthalten.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Storage**.
3. Im Menü „Storage“ erfolgt die Auswahl von **Inventory**.
4. Im **Inventory** erfolgt die Auswahl von **Manage** im Aktionsmenü des Dateisystems, für das die Durchsatzkapazität aktualisiert werden soll.
5. Unter „Informationen“ erfolgt die Auswahl des Stiftsymbols neben **Durchsatzkapazität**. Das Stiftsymbol wird neben dem Dropdown-Pfeil angezeigt, wenn sich der Mauszeiger über der Zeile **Durchsatzkapazität** befindet.
6. Im Dialogfeld „Durchsatzkapazität“ erfolgt die Auswahl der benötigten Durchsatzkapazität.
7. **Anwenden** speichert die Änderungen.

SSD IOPS für ein FSx for ONTAP Dateisystem provisionieren

Automatisches oder manuelles Provisionieren von SSD IOPS für ein FSx for ONTAP Dateisystem in NetApp Workload Factory.

Über diese Aufgabe

Sie können die automatische SSD IOPS Provisionierung für ein FSx Dateisystem aktivieren oder IOPS manuell provisionieren.

Automatisch provisionierte IOPS werden mit drei IOPS pro GiB berechnet.

Wenn Sie IOPS manuell provisionieren, müssen Sie die IOPS möglicherweise vor "[Erhöhung der Dateisystemkapazität](#)" erhöhen.

Informationen zu IOPS-Grenzwerten finden Sie "[Kontingente](#)" in der AWS FSx for NetApp ONTAP Dokumentation.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** erfolgt die Auswahl von **Manage** im Aktionsmenü des Dateisystems, für das IOPS provisioniert werden sollen.

4. Unter Informationen kann das Stiftsymbol ausgewählt werden, das neben dem Dropdown-Pfeil erscheint, wenn sich der Mauszeiger über der Zeile **IOPS-Zuweisung** befindet.
5. Im Dialogfeld „Provisioned IOPS“ ist **Automatic** oder **User provisioned** auszuwählen.
6. Bei Auswahl von **User provisioned** ist der gewünschte **IOPS-Wert** anzugeben.
7. **Anwenden** auswählen.

Löschen eines Dateisystems in NetApp Workload Factory

Um ein Dateisystem in NetApp Workload Factory zu löschen, müssen Sie zuerst alle Volumes, storage VMs oder Replikationsbeziehungen löschen, die mit dem Dateisystem verknüpft sind.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** erfolgt die Auswahl des Aktionsmenüs des FSx for ONTAP Dateisystems, das gelöscht werden soll.
4. Auswahl von **Manage**.
5. Auf der Registerkarte **Übersicht** ist das Menü „Aktionen“ auszuwählen.
6. Wählen Sie **Delete**.
7. Im Dialogfeld „FSx for ONTAP Dateisystem löschen“ erfolgt die Eingabe des Namens des zu löschenden FSx for ONTAP Dateisystems.
8. Zur Bestätigung ist **Löschen** auszuwählen.

Storage-VMs verwalten

Speicher-VM-Einstellungen in NetApp Workload Factory verwalten

Die Einstellungen einer Storage-VM in NetApp Workload Factory lassen sich verwalten. Die Konfiguration und Aktualisierung von Active Directory für eine Storage-VM, die Aktualisierung des Storage-VM-Kennworts sowie die Verwaltung von Tags für die Storage-VM sind möglich.

AD für eine Storage-VM in NetApp Workload Factory konfigurieren und aktualisieren

Konfigurieren und Aktualisieren von Active Directory für eine Storage VM in einem FSx for ONTAP Dateisystem in NetApp Workload Factory.

Die gleichen Schritte gelten für die Konfiguration und Aktualisierung von Active Directory für eine Storage VM.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** wird im Aktionsmenü des Dateisystems mit der zu aktualisierenden storage VM **Manage** ausgewählt.

4. In der Dateisystemübersicht erfolgt unter Storage VMs die Auswahl von **Manage**.
5. Auf dem Bildschirm „Storage VMs managen“ ist im Aktionsmenü der Storage VM, für die Active Directory konfiguriert werden soll, **Basic actions > Manage AD configuration** auszuwählen.
6. Auf der Seite „AD Konfiguration managen“ sind die folgenden Angaben erforderlich:
 - a. **Active Directory-Domäne für den Beitritt:** Als Wert dient der vollqualifizierte Domain-Name (FQDN) Ihres Active Directory.
 - b. **DNS IP-Adressen:** Es können bis zu drei durch Kommas getrennte IP-Adressen eingegeben werden.
 - c. **NetBIOS-Name des SMB-Servers:** Der NetBIOS-Name des SMB-Servers des für Ihre Storage VM zu erstellenden Active Directory-Computerobjekts. Dies ist der Name dieser SVM in Active Directory.
 - d. **Benutzername:** Hier wird der Benutzername des Dienstkontos in Ihrem bestehenden Active Directory eingegeben.

Die Eingabe erfolgt ohne Domänenpräfix oder -suffix. Für `EXAMPLE\ADMIN` kommt `ADMIN` zum Einsatz.

- e. **Passwort:** Das Passwort für das Dienstkonto eingeben.
- f. **Organisationseinheit (OU):** Eingabe der Organisationseinheit.

Die OU ist der eindeutige Pfadname der Organisationseinheit, mit der Sie Ihr Dateisystem verbinden möchten.

- g. **Delegierte Administratorengruppe:** Optional ist die Eingabe der delegierten Dateisystemadministratorengruppe möglich.

Die Gruppe der delegierten Administratoren ist der Name der Gruppe in Ihrem Active Directory, die Ihr Dateisystem verwalten kann.

Wenn Sie AWS Managed Microsoft AD verwenden, müssen Sie eine Gruppe wie `AWS Delegated FSx Administrators`, `AWS Delegated Administrators` oder eine benutzerdefinierte Gruppe mit delegierten Berechtigungen für die Abteilung angeben.

Wenn Sie eine Verbindung zu einem selbstverwalteten Active Directory herstellen, verwenden Sie den Namen der Gruppe in Ihrem Active Directory. Die Standardgruppe ist `Domain Admins`.

7. **Anwenden** auswählen.

Managen von Storage VM-Tags

Tags helfen Ihnen bei der Kategorisierung Ihrer Ressourcen. Sie können Tags für eine Storage VM jederzeit in NetApp Workload Factory hinzufügen, bearbeiten und entfernen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** wird im Aktionsmenü des Dateisystems mit der zu aktualisierenden storage VM **Manage** ausgewählt.
4. In der Dateisystemübersicht erfolgt unter Storage VMs die Auswahl von **Manage**.
5. Im Bildschirm „Manage storage VMs“ wird im Aktionsmenü der Storage VM, deren Tags bearbeitet werden

sollen, **Basic actions** > **Edit storage VM tags** ausgewählt.

6. Auf der Seite „Storage VM-Tags bearbeiten“ können Sie Tags hinzufügen, bearbeiten oder entfernen.

Die maximale Anzahl von Tags, die Sie einer storage VM zuweisen können, beträgt 50.

7. **Anwenden** auswählen.

Zurücksetzen des Storage VM Passworts in NetApp Workload Factory

Das Kennwort für eine Storage-VM in NetApp Workload Factory lässt sich bei Bedarf zurücksetzen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads** > **Storage** > **FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** wird im Aktionsmenü des Dateisystems mit dem zurückzusetzenden Storage VM Passwort **Manage** ausgewählt.
4. In der Dateisystemübersicht erfolgt unter Storage VMs die Auswahl von **Manage**.
5. Auf dem Bildschirm „Storage VMs managen“ erfolgt die Auswahl von **Grundlegende Aktionen** > **Kennwort zurücksetzen** im Aktionsmenü der Storage VM, für die das Kennwort zurückgesetzt werden soll.
6. Im Dialogfeld „Passwort zurücksetzen“ sind folgende Angaben erforderlich:
 - a. **Neues Passwort:** Eingabe eines neuen Passworts für die Storage VM.
 - b. **Passwort bestätigen:** Das neue Passwort zur Bestätigung erneut eingeben.

Löschen einer Storage VM in NetApp Workload Factory

Eine Storage VM (SVM), die nicht mehr benötigt wird, kann aus einer FSx for ONTAP Dateisystemkonfiguration gelöscht werden.

Bevor Sie beginnen

Vor dem Löschen einer Storage VM sind folgende Punkte zu beachten:

- Es muss sichergestellt sein, dass keine Applikationen auf die Daten in der SVM zugreifen.
- Löschen aller Nicht-Root-Volumes, die an die SVM angehängt sind.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads** > **Storage** > **FSx for ONTAP** auszuwählen.
3. Wählen Sie in **FSx for ONTAP** das Aktionsmenü des zu aktualisierenden Dateisystems und anschließend **Verwalten**.
4. In der Dateisystemübersicht erfolgt unter Storage VMs die Auswahl von **Manage**.
5. Auf dem Bildschirm „Storage-VMs verwalten“ erfolgt die Auswahl des Aktionsmenüs der zu löschenden Storage-VM.
6. Ausgewählt wird die Option **Storage VM löschen**.
7. Im Dialogfeld „Storage VM löschen“ ist zum Löschen der Storage VM „delete“ einzugeben.

8. Zur Bestätigung ist **Löschen** auszuwählen.

FSx for ONTAP für Datenbank-Workloads

Informationen zu NetApp Workload Factory for Databases

NetApp Workload Factory for Databases ist ein End-to-End-Service für Datenbank-Deployment und -Wartung mit integrierten Best Practices für Optimierung, automatisches Thin Cloning sowie Überwachungs- und Fehlerbehebungsfunktionen.

Was ist NetApp Workload Factory für Datenbanken?

NetApp Workload Factory for Databases erkennt, bewertet, plant, stellt bereit und migriert Microsoft SQL Server-, PostgreSQL- und Oracle-Daten zu Amazon FSx for NetApp ONTAP (FSx for ONTAP)-Bereitstellungen, die darauf optimiert sind, Ihre Anforderungen an Leistung und Kosten zu erfüllen und gleichzeitig die Best Practices der Branche einzuhalten. NetApp Workload Factory for Databases optimiert und verwaltet kontinuierlich Datenbanken auf FSx for ONTAP.

["Weitere Informationen zu Workload Factory"](#).

Vorteile von Workload Factory für selbstverwaltete Datenbanken

Workload Factory bietet Best Practices und Automatisierung für selbstverwaltete Datenbanken.

Best Practices

- Integriertes Wissen aus AWS Cloud, Microsoft Windows und SQL Servern sowie NetApp ONTAP für SQL Server Deployments auf EC2 Instanzen.
- Deployment mit optimierten Gesamtbetriebskosten.
- Durchgängige Deployment-Automatisierung, die den Best Practices von AWS, Microsoft und ONTAP folgt.
- Der Deployment-Modus *Quick create* hilft Ihnen, potenzielle Fallstricke bei der manuellen Konfiguration zu vermeiden.

Automatisierung mit Workload Factory Codebox

Workload Factory führt mit der integrierten *Codebox* eine integrierte Automatisierung ein. Die Codebox bietet folgende Vorteile der Automatisierung:

- **Generierung von Code-Snippets:** Workload Factory generiert Infrastructure-as-Code (IaC)-Snippets während der Ressourcenerstellung und ermöglicht so die nahtlose Integration in bestehende Orchestrierungs-Workflows.
- **Infrastructure-as-code co-pilot:** Die Codebox ist ein Infrastructure-as-code (IaC) co-pilot, der Entwicklern und DevOps dabei hilft, Code zu generieren, um jeden von Workload Factory unterstützten Vorgang auszuführen.
- **Code-Viewer und Automatisierungskatalog:** Die Codebox bietet einen Code-Viewer zur schnellen Analyse von Automatisierung und einen Automatisierungskatalog zur schnellen späteren Wiederverwendung.

Workload Factory for Databases Funktionen

Workload Factory für Datenbanken bietet folgende Funktionen:

- **Kostenschätzung:** Ermitteln Sie mögliche Kosteneinsparungen mit dem Einsparungsrechner, der die Kosten für Speicher, Rechenleistung, SQL-Lizenzierung, Snapshots und Klone für bestehende Microsoft SQL Server- und Oracle-Bereitstellungen mit Elastic Block Store, FSx for Windows File Server und On-Premises im Vergleich zu FSx for ONTAP schätzt und detailliert aufschlüsselt.
- **Einfache, schnelle Bereitstellungen:** Vereinfachen und optimieren Sie die Bereitstellung von Hosts, Datenbanken und Sandboxes mit integrierten NetApp-, Microsoft- und Amazon-Best Practices, die die Komplexität der manuellen Konfiguration für Microsoft SQL Server- und PostgreSQL-Instanzen auf AWS eliminieren.
 - Stellen Sie über die Workload Factory-Konsole im *Schnellmodus* oder *Erweiterten Modus* bereit, oder erstellen, wiederverwenden und passen Sie AWS-CloudFormation-Vorlagen über die Codebox an, um zukünftige Bereitstellungen in mehreren Umgebungen zu ermöglichen.
 - Erstellen Sie bedarfsgesteuerte, isolierte Datenbanken mit Speicherkonfigurationen und Sandbox-Klonen, die für Tests, Integration, Diagnose und Schulungen verwendet werden können, ohne die Produktionsdaten zu beeinträchtigen.
- **Ausgereifte Bewertungsfunktion:** Durch kontinuierliches Scannen Ihrer Microsoft SQL Server- und Oracle-Umgebungen erhalten Sie einen umfassenden Bericht mit Erkenntnissen, Optimierungspotenzialen und Empfehlungen, der Ihnen hilft, operative Exzellenz, Sicherheit, Zuverlässigkeit, Leistungseffizienz und Kostenoptimierung auf Basis der AWS Best Practices zu erreichen.
- **Fehleranalyse:** Analysieren und beheben Sie Protokollfehler mit dem KI-Analysator, um detaillierte Fehlermeldungen, Schritte zur Fehlerbehebung und Empfehlungen zur Problemlösung zu erhalten.
- **Zentrale Verwaltung:** Verwalten Sie Ihre Microsoft SQL Server-, Oracle- und PostgreSQL-Ressourcen auf FSx for ONTAP von einem Ort aus. In Workload Factory erhalten Sie Einblick in die angeschlossene Infrastruktur, AWS-Konten, Anmeldeinformationen, verbundene FSx for ONTAP-Dateisysteme, Speichernutzung einschließlich NFS-Volumes und iSCSI-LUNs, Schutzstatus, Leistung, Well-Architected-Status und Fehleranalyse.

Vorteile von Amazon FSx for ONTAP für selbst gemanagte Datenbanken

- **Beständigkeit, Verfügbarkeit und Zuverlässigkeit:** FSx for ONTAP bietet zahlreiche Funktionen, die die Beständigkeit und Verfügbarkeit von selbstverwalteten Datenbanken verbessern, die auf FSx for ONTAP gehostet werden, z. B. Hochverfügbarkeit zur Unterstützung von Deployments in Single und Multiple Availability Zones, anwendungsorientierte Snapshots, verbesserte Notfallwiederherstellung durch Replikation und effiziente Datensicherung.
- **Performance und Skalierbarkeit:** FSx for ONTAP bietet Performance-Optimierung mit hohem Durchsatz, geringer Latenz, Hochgeschwindigkeits-Netzwerkverbindungen und Skalierbarkeit mit mehreren Dateisystemen, um die für eine Workload erforderliche Gesamt-Performance zu skalieren.
- **Datenmanagement und Effizienz:** FSx for ONTAP bietet zahlreiche Funktionen zur Verbesserung des Datenmanagements und der Effizienz, wie z. B. speichereffiziente Thin Clones, Thin Provisionierung, Komprimierung und Deduplizierung sowie die Auslagerung selten genutzter Daten in den Kapazitätspool.

["Informationen zu FSx for ONTAP for Workload Factory"](#).

Tools zur Verwendung von NetApp Workload Factory

Sie können NetApp Workload Factory mit den folgenden Tools verwenden:

- **Workload Factory console:** Die Workload Factory console bietet einen visuellen, ganzheitlichen Überblick

über Ihre Anwendungen und Projekte.

- **NetApp Console:** Die NetApp Console bietet eine hybride Benutzeroberfläche, die die Nutzung von Workload Factory zusammen mit anderen NetApp Datenservices ermöglicht.
- **Ask me:** Mit dem KI-Assistenten Ask me können Sie Fragen stellen und mehr über Workload Factory erfahren, ohne die Workload Factory Konsole zu verlassen. Ask me ist über das Hilfemenü von Workload Factory verfügbar.
- **CloudShell CLI:** Workload Factory umfasst eine CloudShell CLI, um AWS- und NetApp Umgebungen kontenübergreifend über eine einzige browserbasierte CLI zu managen und zu betreiben. Der Zugriff auf CloudShell erfolgt über die obere Leiste der Workload Factory Konsole.
- **REST API:** Mit den Workload Factory REST APIs können Sie Ihre FSx for ONTAP Dateisysteme und andere AWS Ressourcen einsetzen und managen.
- **CloudFormation:** Mit AWS CloudFormation-Code lassen sich die in der Workload Factory Konsole definierten Aktionen ausführen, um AWS- und Drittanbieterressourcen aus dem CloudFormation-Stack in Ihrem AWS-Konto zu modellieren, zu provisionieren und zu managen.
- **NetApp Terraform Provider:** Mit Terraform können Infrastruktur-Workflows erstellt und verwaltet werden, die in der Workload Factory Konsole generiert wurden.

Unterstützte Konfigurationen

Sie können Workload Factory mit den folgenden Datenbank-Engines, Versionen, Betriebssystemen und Bereitstellungsmodellen verwenden und dabei die Best Practices von AWS, NetApp ONTAP, Microsoft SQL Server, Oracle und PostgreSQL befolgen.

Engine	Version	Betriebssystem	Deployment-Modell
Microsoft SQL Server	SQL Server 2016	Windows Server 2016	FCI, Standalone
Microsoft SQL Server	SQL Server 2019	Windows Server 2016	FCI, Standalone
Microsoft SQL Server	SQL Server 2022	Windows Server 2016	FCI, Standalone
Microsoft SQL Server	SQL Server 2016	Windows Server 2019	FCI, Standalone
Microsoft SQL Server	SQL Server 2019	Windows Server 2019	FCI, Standalone
Microsoft SQL Server	SQL Server 2022	Windows Server 2019	FCI, Standalone
Microsoft SQL Server	SQL Server 2016	Windows Server 2022	FCI, Standalone
Microsoft SQL Server	SQL Server 2019	Windows Server 2022	FCI, Standalone
Microsoft SQL Server	SQL Server 2022	Windows Server 2022	FCI, Standalone
Microsoft SQL Server	SQL Server 2017	Beliebig	FCI, Standalone
Microsoft SQL Server	SQL Server 2016, 2017,2019, 2022	Beliebig	FCI, Standalone
Microsoft SQL Server	SQL Server 2016, 2017,2019, 2022	Beliebig	Always On- Verfügbarkeitsgruppe
Oracle	19c	RHEL, SuSe Linux	Eigenständig (Einzel- /Mehrmandantenfähig)
Oracle	21c	RHEL, SuSe Linux	Eigenständig (Einzel- /Mehrmandantenfähig)

Engine	Version	Betriebssystem	Deployment-Modell
Oracle	19c	RHEL, SuSe Linux	Eigenständig (Einzel-/Mehrmandantenfähig)
Oracle	21c	RHEL, SuSe Linux	Eigenständig (Einzel-/Mehrmandantenfähig)
Oracle	19c	RHEL, SuSe Linux	Standalone mit ASM (Einzel-/Mehrmandanten)
Oracle	21c	RHEL, SuSe Linux	Standalone mit ASM (Einzel-/Mehrmandanten)
Oracle	19c, 21c	RHEL, SuSe Linux	Data Guard
PostgreSQL	PostgreSQL 15	Amazon Linux 2023 AMI	HA, Standalone Instanz
PostgreSQL	PostgreSQL 16	Amazon Linux 2023 AMI	HA, Standalone Instanz

Integrierte AWS Services

Die Datenbanken umfassen die folgenden integrierten AWS-Dienste:

- CloudFormation
- Simple Notification Service
- CloudWatch
- System Manager
- Secrets Manager

Regionen

Databases wird in allen kommerziellen Regionen unterstützt, in denen FSx for ONTAP unterstützt wird.

["Unterstützte Amazon Regionen"](#)

Die folgenden AWS-Regionen werden nicht unterstützt:

- China Regionen
- Secret Cloud
- Top Secret Cloud

Hilfe erhalten

Amazon FSx for NetApp ONTAP ist eine Lösung von AWS. Bei Fragen oder technischen Supportproblemen im Zusammenhang mit Ihrem Dateisystem FSx for ONTAP, Ihrer Infrastruktur oder einer Lösung, die diesen Service verwendet, können Sie im Support Center Ihrer AWS Management Console einen Support-Fall bei AWS eröffnen. Dabei wählen Sie den Service „FSx for ONTAP“ und die entsprechende Kategorie aus. Anschließend geben Sie die übrigen Informationen an, die zum Erstellen Ihres AWS Support-Falls erforderlich sind.

Allgemeine Fragen zu Workload Factory oder Workload Factory Anwendungen und Services finden Sie unter ["Hilfe zu NetApp Workload Factory for Databases"](#).

Schnellstart für NetApp Workload Factory für Datenbanken

Mit NetApp Workload Factory for Databases können Sie sofort mit den Berechtigungen für Ansicht, Planung und Analyse beginnen. Wenn Sie Workload Factory zum Ermitteln von Hosts, zum Managen von Ressourcen und für weitere Funktionen nutzen möchten, können Sie in wenigen Schritten beginnen.

Sie benötigen ein AWS-Konto, um Databases nutzen zu können.

Die folgenden Schritte erleichtern den Einstieg.

1

Anmeldung bei NetApp Workload Factory

Sie müssen ["Registrierung"](#) und sich bei der NetApp Console anmelden.

2

Hinzufügen von Anmeldeinformationen und Berechtigungen für die Datenbank-Workload

["Manuelles Hinzufügen von Anmeldeinformationen zu einem Konto"](#) Dazu gehört die Auswahl der Datenbank-Workload-Funktion und die Auswahl derjenigen ["Berechtigungsrichtlinien"](#), die Ihren Bedürfnissen entspricht.

3

Ressourcen erkennen oder einsetzen

Mithilfe von Anmeldeinformationen und IAM-Richtlinien können Sie vorhandene Datenbankressourcen im Inventar oder ["einen Microsoft SQL Server einsetzen"](#) oder ["einen PostgreSQL Server einsetzen"](#) ermitteln. Das Inventar bietet eine einheitliche Schnittstelle zum Managen von Ressourcen.

4

Möglichkeiten zur Kosteneinsparung erkunden

Wenn Sie Datenbanken lokal oder auf AWS mit Storage auf Amazon Elastic Block Store (EBS) oder FSx for Windows File Server betreiben, können Sie ["den Explore Sparrechner verwenden"](#) die Kosten analysieren und Migrationen effektiv planen.

5

Gut konzipierte Datenbankkonfigurationen implementieren

Workload Factory for Databases analysiert regelmäßig Microsoft SQL Server- und Oracle-Bereitstellungen auf Amazon FSx for NetApp ONTAP Storage über das Well-Architected Dashboard. Um Probleme im Well-Architected Dashboard für Ihre Datenbankressourcen zu beheben, müssen Sie zunächst ["Instanzen registrieren"](#).

Nach der Registrierung der Instanzen können Sie den Well-Architected-Status anzeigen und Maßnahmen ergreifen, um ["gut konzipierte Datenbankkonfigurationen implementieren"](#) in Workload Factory.

Was kommt als Nächstes

Wenn Sie Ressourcen mit FSx for ONTAP Dateisystem-Storage in Ihrem Datenbankinventar registriert haben, können Sie ["eine Benutzerdatenbank erstellen"](#) oder ["Host klonen, um eine Sandbox zu erstellen"](#).

Informationen zu Einsparungen in NetApp Workload Factory for Databases

Einsparungen in NetApp Workload Factory for Databases für Ihre Datenbank-Workloads lassen sich durch den Vergleich der Kosten für die Nutzung von Microsoft SQL Server auf Amazon Elastic Block Store (EBS), FSx for Windows File Server und lokalem Storage mit FSx for ONTAP Storage analysieren.

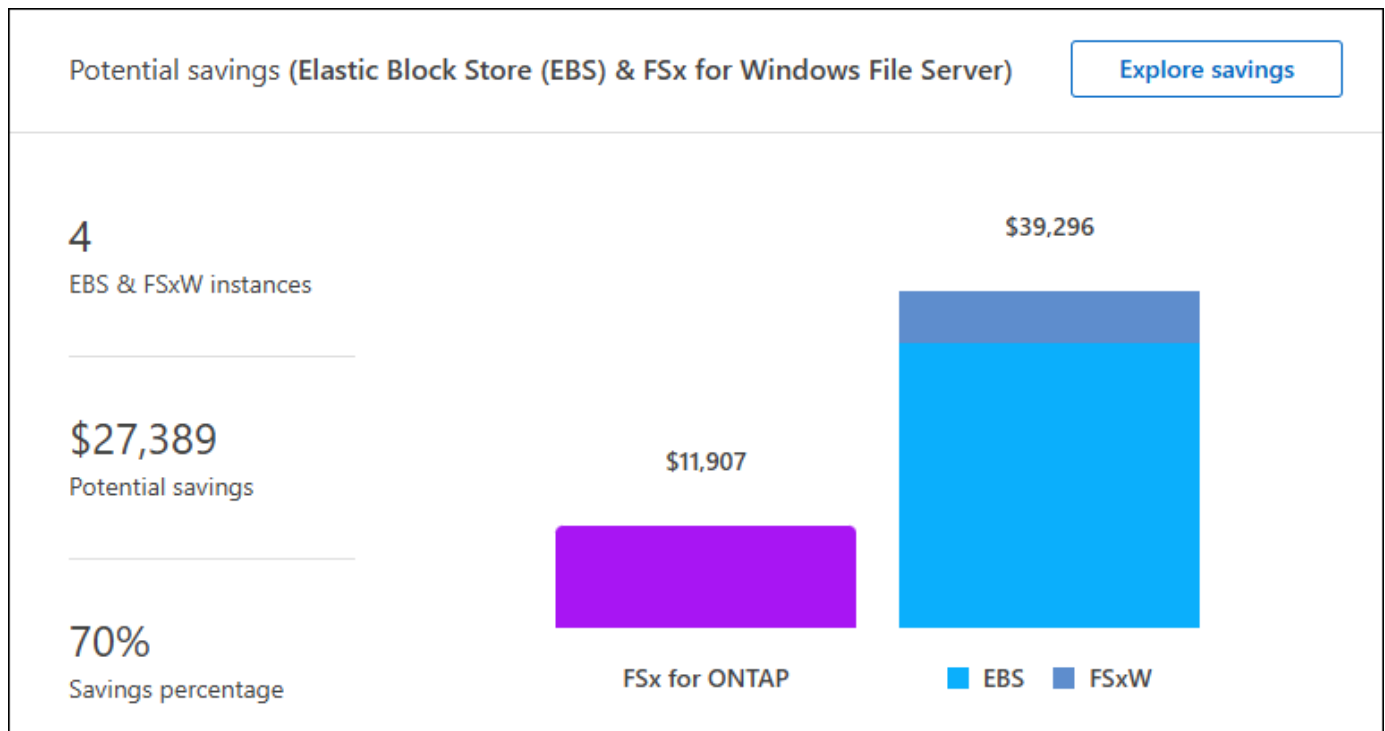
Über diese Aufgabe

Sie können Einsparmöglichkeiten für Ihre Datenbank-Workloads auf EBS, FSx for Windows File Server und lokalem Speicher mithilfe des Dashboards, der Registerkarte „Inventar“ oder der Registerkarte „Einsparungen erkunden“ untersuchen. In allen Fällen können Sie den Einsparungsrechner verwenden, um verschiedene Kostenkomponenten für den Betrieb von Microsoft SQL Server-Workloads wie Storage, Compute, SQL-Lizenz, Snapshots und Klone für Ihre Datenbank-Workloads auf FSx for ONTAP-Dateisystemen mit Elastic Block Store (EBS), FSx for Windows File Server und lokalem Speicher zu vergleichen.

Wenn Workload Factory Kosteneinsparungen bei FSx for ONTAP findet, können Sie Microsoft SQL über FSx for ONTAP direkt aus dem Einsparungsrechner in der Workload Factory-Konsole bereitstellen. Wenn Sie mehrere Microsoft SQL Server-Instanzen über Elastic Block Store, FSx for Windows File Server oder lokalen Speicher haben, empfehlen wir eine FSx for ONTAP-Konfiguration mit einer einzelnen SQL-Instanz.

Potenzielle Einsparungen für alle Datenbank-Workloads

Rufen Sie das Datenbank-**Dashboard** in der Workload Factory-Konsole auf, um sich einen Überblick über die potenziellen Kosteneinsparungen beim Ausführen all Ihrer Datenbank-Workloads auf FSx for ONTAP zu verschaffen. Die Kachel **Potenzielle Einsparungen** zeigt Ihre Datenbank-Workloads auf EBS und FSx for Windows File Server, potenzielle Kosteneinsparungen, Einsparungsprozentsatz und ein Balkendiagramm an.

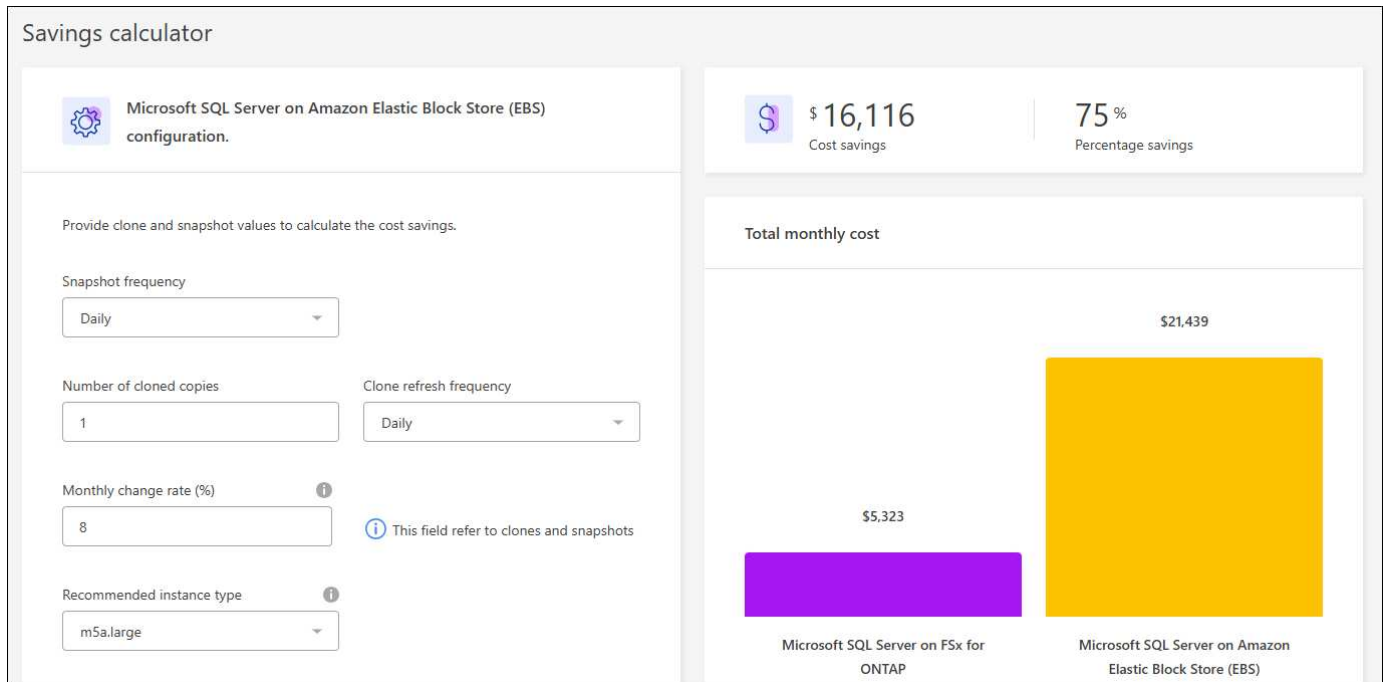


Einsparungsrechner

Sie können den Kostenrechner nutzen, um verschiedene Kostenkomponenten für den Betrieb von Microsoft SQL Server-Workloads wie Speicher, Rechenleistung, SQL-Lizenz, Snapshots und Klone für Ihre Datenbank-Workloads auf FSx for ONTAP-Dateisystemen mit Elastic Block Store (EBS), FSx for Windows File Server und

lokalem Speicher zu vergleichen. FSx for ONTAP-Dateisysteme könnten die kostengünstigste Option für Ihre Datenbank-Workloads sein.

Der Rechner zeigt an, ob die Storage für die Datenbank Workloads auf diesen Microsoft SQL Servern geringer ausfallen würde, wenn Sie ein FSx for ONTAP Dateisystem verwenden würden. [Informationen zur Verwendung des Taschenrechners.](#)



SQL Server Deployment-Analyse

Der Rechner prüft Ihre SQL Server-Bereitstellung, um sicherzustellen, dass die verwendeten Ressourcen und Funktionen der SQL Server-Edition entsprechen. Hier sind die wichtigsten Faktoren und Bedingungen, die der Rechner prüft, bevor er ein Downgrade auf die Standard Edition empfiehlt:

Bereitstellungsmodell

Der Rechner bewertet das Deployment-Modell und prüft, ob die Enterprise edition erforderlich ist.

Zugewiesene Ressourcen

Der Rechner bewertet die Bedingungen der folgenden lizenzabhängigen zugeteilten Ressourcen:

- Target Instance vCPUs: Die Instanz verfügt über 48 oder weniger virtuelle CPUs.
- Speicherzuweisung: Die Instanz verfügt über 128GB oder weniger Arbeitsspeicher.

Nutzung von Unternehmensfunktionen

Der Rechner überprüft, ob eine oder mehrere der folgenden Enterprise-Funktionen verwendet werden:

- Enterprise-Funktionen auf Datenbankebene
- Online-Indexoperationen
- Resource Governor
- Peer-to-Peer- oder Oracle-Replikation
- R/Python-Erweiterungen

- Speicheroptimierte TempDB

Wenn die bewertete SQL Server-Instanz keine der oben genannten Enterprise-Funktionen nutzt und die Ressourcenbeschränkungen erfüllt, empfiehlt der Rechner, die Lizenz auf die Standard Edition herabzustufen. Der Rechner hilft Ihnen, die SQL Server-Lizenzkosten zu optimieren, ohne Leistung oder Funktionalität zu reduzieren.

Taschenrechneroptionen

Für den Kostenvergleich zwischen Ihren Systemen und FSx for ONTAP stehen zwei Rechneroptionen zur Verfügung: Anpassung und Erkennung.

Einsparungen lassen sich durch individuelle Anpassung erzielen: Sie legen die Konfigurationseinstellungen für Microsoft SQL Server auf Amazon EC2 mit EBS oder FSx for Windows File Server fest, einschließlich Region, Deployment-Modell, SQL Server Edition, monatlicher Änderungsrate, Snapshot-Frequenz und mehr.

Einsparungen für erkannte Hosts prüfen: Workload Factory stellt eine Verknüpfung zu Ihren vorhandenen Microsoft SQL Servern her und übernimmt die Details in den Rechner für einen automatischen Vergleich. Sie müssen Berechtigungen für *Anzeige*, *Planung* und *Analyse* gewähren, um diese Rechneroption nutzen zu können. Sie können den Anwendungsfall ändern, alle weiteren Details werden jedoch in der Berechnung automatisch bestimmt.

Zusätzlich kann ["AWS Anmeldeinformationen hinzufügen"](#) die Genauigkeit der Rechneranalyse verbessert werden. Anschließend erfolgt die Auswahl von **Calculate savings based on existing resources**. Daraufhin erfolgt eine Weiterleitung zur Seite **Add credentials**. Nach dem Hinzufügen der Anmeldeinformationen erfolgt die Auswahl der vorhandenen Ressourcen für den Vergleich mit FSx for ONTAP sowie die Auswahl von **Explore savings**.

Einsparpotenziale durch individuelle Anpassung

Passen Sie die Felder im Rechner an, um eine möglichst genaue Einsparungsschätzung zu erhalten.

Individuelle Einsparungen für Microsoft SQL Server-Hosts

Die folgenden Schritte sind auf der Registerkarte für Ihren Storage-Typ aufgeführt.

Amazon Elastic Block Store (EBS)

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Die Auswahl erfolgt im Menü Datenbanken über **Einsparungen erkunden** und anschließend **Microsoft SQL Server auf EBS**.
4. Im Sparrechner werden die folgenden Details benötigt:
 - a. **Region**: Auswahl einer Region aus dem Dropdown-Menü.
 - b. **Deployment-Modell**: Auswahl eines Deployment-Modells aus dem Dropdown-Menü.
 - c. **SQL Server Edition**: Die SQL Server Edition wird im Dropdown-Menü ausgewählt.
 - d. **Monatliche Änderungsrate (%)**: Prozentsatz, um den sich Klon- und Snapshot-Daten durchschnittlich pro Monat ändern.

- e. **Snapshot-Frequenz:** Auswahl einer Snapshot-Frequenz aus dem Dropdown-Menü.
- f. **Anzahl der geklonten Kopien:** Eingabe der Anzahl der geklonten Kopien in der EBS Konfiguration.
- g. **Monatliche SQL BYOL-Kosten (\$):** Optional ist die Eingabe der monatlichen SQL BYOL-Kosten in Dollar möglich.
- h. Unter EC2-Spezifikationen sind folgende Angaben erforderlich:
 - **Maschinenbeschreibung:** Optional können Sie einen Namen eingeben, der die Maschine beschreibt.
 - **Instanztyp:** Auswahl des EC2-Instanztyps im Dropdown-Menü.
- i. Unter „Volume-Typen“ sind für mindestens einen Volume-Typ die folgenden Details erforderlich. IOPS und Durchsatz gelten für Volumes mit bestimmten Festplattentypen.
 - **Anzahl der Volumes**
 - **Storage-Kapazität pro Volume (GiB)**
 - **Bereitgestellte IOPS pro Volume**
 - **Durchsatz MB/s**
- j. Wenn Sie das Bereitstellungsmodell Always On availability ausgewählt haben, sind Angaben zu **Secondary EC2 specifications** und **Volume types** erforderlich.

Amazon FSx for Windows File Server

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Im Menü **Databases** erfolgt die Auswahl von **Explore savings** und anschließend von **Microsoft SQL Server on FSx for Windows**.
4. Im Sparrechner werden die folgenden Details benötigt:
 - a. **Region:** Auswahl einer Region aus dem Dropdown-Menü.
 - b. **Deployment-Modell:** Auswahl eines Deployment-Modells aus dem Dropdown-Menü.
 - c. **SQL Server Edition:** Die SQL Server Edition wird im Dropdown-Menü ausgewählt.
 - d. **Monatliche Änderungsrate (%):** Prozentsatz, um den sich Klon- und Snapshot-Daten durchschnittlich pro Monat ändern.
 - e. **Snapshot-Frequenz:** Auswahl einer Snapshot-Frequenz aus dem Dropdown-Menü.
 - f. **Anzahl der geklonten Kopien:** Eingabe der Anzahl der geklonten Kopien in der EBS Konfiguration.
 - g. **Monatliche SQL BYOL-Kosten (\$):** Optional ist die Eingabe der monatlichen SQL BYOL-Kosten in Dollar möglich.
 - h. Unter den Einstellungen für FSx for Windows File Server sind folgende Angaben erforderlich:
 - **Deployment-Typ:** Auswahl des Deployment-Typs im Dropdown-Menü.
 - **Speichertyp:** SSD-Storage ist der unterstützte Speichertyp.
 - **Gesamte Storage-Kapazität:** Eingabe der Storage-Kapazität und Auswahl der Kapazitätseinheit für die Konfiguration.
 - **Bereitgestellte SSD-IOPS:** Die für die Konfiguration bereitgestellten SSD-IOPS werden

eingegeben.

- **Durchsatz (MB/s)**: Eingabe des Durchsatzes in MB/s.
- i. Unter EC2-Spezifikationen erfolgt die Auswahl des **Instanztyps** im Dropdown-Menü.

Nach der Angabe der Details für die Hostkonfiguration Ihrer Datenbank folgt eine Überprüfung der auf der Seite angezeigten Berechnungen und Empfehlungen.

Zusätzlich wird der Bericht am Ende der Seite sichtbar, sobald eine der folgenden Optionen ausgewählt ist:

- **PDF-Export**
- **Per E-Mail senden**
- **Berechnungen anzeigen**

Um zu FSx für ONTAP zu wechseln, folgen Sie den Anweisungen unter [Microsoft SQL Server auf AWS EC2 mit FSx für ONTAP-Dateisysteme bereitstellen](#).

Einsparungen für Oracle-Hosts auf EBS anpassen

Passen Sie die Felder im Rechner an, um die genaueste Kosteneinsparungsschätzung für Ihre Oracle-Hosts zu erhalten, die auf Amazon Elastic Block Store (EBS) laufen.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Im Menü Datenbanken erfolgt die Auswahl von **Einsparungen erkunden** und anschließend **Oracle on EBS**.
4. Im Sparrechner werden die folgenden Details benötigt:
 - a. **Region**: Auswahl einer Region aus dem Dropdown-Menü.
 - b. **Deployment-Modell**: Auswahl eines Deployment-Modells aus dem Dropdown-Menü.
 - c. **Oracle edition**: Wählen Sie die Oracle edition aus dem Dropdown-Menü aus.
 - d. **Monatliche Änderungsrate (%)**: Prozentsatz, um den sich Klon- und Snapshot-Daten durchschnittlich pro Monat ändern.
 - e. **Snapshot-Frequenz**: Auswahl einer Snapshot-Frequenz aus dem Dropdown-Menü.
 - f. **Anzahl der geklonten Kopien**: Eingabe der Anzahl der geklonten Kopien in der EBS Konfiguration.
 - g. **Monatliche Oracle BYOL-Kosten (\$)**: Optional können Sie die monatlichen Oracle BYOL-Kosten in Dollar eingeben.
 - h. Unter EC2-Spezifikationen sind folgende Angaben erforderlich:
 - **Maschinenbeschreibung**: Optional können Sie einen Namen eingeben, der die Maschine beschreibt.
 - **Instanztyp**: Auswahl des EC2-Instanztyps im Dropdown-Menü.
 - i. Unter „Volume-Typen“ sind für mindestens einen Volume-Typ die folgenden Details erforderlich. IOPS und Durchsatz gelten für Volumes mit bestimmten Festplattentypen.
 - **Anzahl der Volumes**

- **Storage-Kapazität pro Volume (GiB)**
- **Bereitgestellte IOPS pro Volume**
- **Durchsatz MB/s**

j. Wenn Sie das Bereitstellungsmodell Always On availability ausgewählt haben, sind Angaben zu **Secondary EC2 specifications** und **Volume types** erforderlich.

Nach der Angabe der Details für die Hostkonfiguration Ihrer Datenbank folgt eine Überprüfung der auf der Seite angezeigten Berechnungen und Empfehlungen.

Zusätzlich wird der Bericht am Ende der Seite sichtbar, sobald eine der folgenden Optionen ausgewählt ist:

- **PDF-Export**
- **Per E-Mail senden**
- **Berechnungen anzeigen**

Einsparungen für erkannte Hosts

Workload Factory gibt die erkannten Host-Merkmale ein, damit Sie automatisch Einsparmöglichkeiten entdecken können.

Bevor Sie beginnen

Bevor Sie beginnen, müssen folgende Voraussetzungen erfüllt sein:

- "[Berechtigungen für Ansicht, Planung und Analyse gewähren](#)" in Ihrem AWS-Konto, um Elastic Block Store (EBS)- und FSx for Windows-Systeme unter dem Tab **Explore savings** zu erkennen und die Einsparungsberechnung im Einsparungsrechner anzuzeigen.
- Um Empfehlungen für Instanztypen zu erhalten und die Kostengenaugkeit zu verbessern, sind die folgenden Schritte erforderlich:
 - a. Amazon CloudWatch und AWS Compute Optimizer Berechtigungen gewähren.
 - i. Die Anmeldung bei der AWS Management Console und das Öffnen des IAM-Service erfolgen.
 - ii. Bearbeitung der Richtlinie für die IAM-Rolle. Kopieren und Hinzufügen der folgenden Berechtigungen für Amazon CloudWatch und AWS Compute Optimizer.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "compute-optimizer:GetEnrollmentStatus",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "compute-optimizer:PutRecommendationPreferences",
      "Resource": "*"
    },
    {
```

```

    "Effect": "Allow",
    "Action": "compute-optimizer:GetEffectiveRecommendationPreferences",
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "compute-optimizer:GetEC2InstanceRecommendations",
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "autoscaling:DescribeAutoScalingGroups",
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "autoscaling:DescribeAutoScalingInstances",
    "Resource": "*"
  }
]
}

```

- b. Das abrechnungsrelevante AWS-Konto wird für AWS Compute Optimizer aktiviert.

Entdecken Sie Einsparungen für erkannte Microsoft SQL Server Hosts

Die folgenden Schritte sind auf der Registerkarte für Ihren Storage-Typ aufgeführt.

Amazon Elastic Block Store (EBS)

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Wählen Sie im Menü Datenbanken **Explore savings** aus.
4. Wählen Sie in „Einsparungen entdecken“ die Registerkarte **SQL Server auf Elastic Block Store (EBS)** aus.

Wenn Workload Factory EBS-Hosts erkennt, werden Sie zur Registerkarte „Einsparmöglichkeiten erkunden“ weitergeleitet. Wenn keine EBS-Hosts erkannt werden, werden Sie zum Rechner weitergeleitet, um [Einsparmöglichkeiten durch individuelle Anpassung](#).

5. Unter **Explore savings** können Sie einen oder mehrere auf EBS ausgeführte Datenbank-Hosts auswählen und anschließend **Explore savings** auswählen.
6. Falls erforderlich, können Sie den Datenbankhost mit SQL Server-Anmeldeinformationen, Windows-Anmeldeinformationen oder durch das Hinzufügen fehlender SQL Server-Berechtigungen authentifizieren.

Wenn die Seite **Explore savings** nach erfolgreicher Authentifizierung keine Daten lädt, kann durch Auswählen der Registerkarte **Inventory** ein erneutes Laden der Daten veranlasst werden; anschließend kann die Registerkarte **Explore savings** erneut ausgewählt werden.

7. Im Savings calculator können Sie die folgenden Details zu Klonen und Snapshots in Ihrem EBS-Speicher angeben, um eine genauere Kosteneinsparungsschätzung zu erhalten.
 - a. **Snapshot-Frequenz**: Im Menü wird eine Snapshot-Frequenz ausgewählt.
 - b. **Aktualisierungsfrequenz der Klone**: Im Menü lässt sich die Frequenz auswählen, mit der die Klone aktualisiert werden.
 - c. **Anzahl der geklonten Kopien**: Eingabe der Anzahl der geklonten Kopien in der EBS Konfiguration.
 - d. **Monatliche Änderungsrate**: Eingabe des Prozentsatzes, um den sich Klon- und Snapshot-Daten durchschnittlich pro Monat ändern.
 - e. **Hosts hinzufügen**: Optional können Sie bis zu fünf erkannte EBS-Hosts auswählen, die in die Einsparungsberechnung einbezogen werden sollen.

Workload Factory konsolidiert mehrere SQL Server-Hosts zu einer einzigen FSx for ONTAP Konfigurationsempfehlung, um Kosteneinsparungen zu optimieren, es sei denn, die ausgewählten EBS-Hosts überschreiten die Durchsatz-, Kapazitäts- oder IOPS-Grenzwerte für ein einzelnes FSx for ONTAP Dateisystem.

Amazon FSx for Windows File Server

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Wählen Sie im Menü Datenbanken **Explore savings** aus.
4. Wählen Sie in „Explore savings“ die Registerkarte **SQL Server auf FSx für Windows** aus.

Wenn Workload Factory FSx for Windows-Hosts erkennt, werden Sie zum Tab „Einsparungen erkunden“ weitergeleitet. Wenn keine FSx for Windows-Hosts erkannt werden, werden Sie zum Rechner weitergeleitet [Einsparungsmöglichkeiten durch individuelle Anpassung](#).

5. Auf der Registerkarte „Explore savings“ erfolgt die Auswahl von **Explore savings** für den Datenbank-Host bei Verwendung von FSx for Windows File Server Storage.
6. Falls erforderlich, können Sie den Datenbankhost mit SQL Server-Anmeldeinformationen, Windows-Anmeldeinformationen oder durch das Hinzufügen fehlender SQL Server-Berechtigungen authentifizieren.

Wenn die Seite **Explore savings** nach erfolgreicher Authentifizierung keine Daten lädt, kann durch Auswählen der Registerkarte **Inventory** ein erneutes Laden der Daten veranlasst werden; anschließend kann die Registerkarte **Explore savings** erneut ausgewählt werden.

7. Im Kosteneinsparungsrechner können Sie optional die folgenden Details zu Klonen (Schattenkopien) und Snapshots in Ihrem FSx for Windows Storage angeben, um eine genauere Kosteneinsparungsschätzung zu erhalten.
 - a. **Snapshot-Frequenz**: Im Menü wird eine Snapshot-Frequenz ausgewählt.

Wenn Workload Factory Schattenkopien von FSx for Windows erkennt, wird der Standardwert auf **Täglich** gesetzt. Wenn keine Schattenkopien erkannt werden, wird der Standardwert auf **Keine**

Snapshot-Frequenz gesetzt.

- b. **Aktualisierungsfrequenz der Klone:** Im Menü lässt sich die Frequenz auswählen, mit der die Klone aktualisiert werden.
- c. **Anzahl der geklonten Kopien:** Geben Sie die Anzahl der geklonten Kopien in der FSx for Windows Konfiguration an.
- d. **Monatliche Änderungsrate:** Eingabe des Prozentsatzes, um den sich Klon- und Snapshot-Daten durchschnittlich pro Monat ändern.

Microsoft SQL Server On-Premises

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Wählen Sie im Menü Datenbanken **Explore savings** aus.
4. In „Explore savings“ wählen Sie als Engine-Typ **Microsoft SQL Server** aus.
5. Wählen Sie als Nächstes die Registerkarte **SQL Server on-premises** aus.
6. Wählen Sie auf der Registerkarte „SQL Server On-Premises“ die Option **Assessment script > Assessment script information** aus und überprüfen Sie die bereitgestellten Informationen.
7. Wählen Sie **Download assessment script**.

Das Skript ist ein Datenerfassungstool, das auf PowerShell basiert. Es sammelt Konfigurations- und Leistungsdaten von SQL Server und lädt diese anschließend in Workload Factory hoch. Der Migrationsberater wertet die Daten aus und plant die FSx for ONTAP-Bereitstellung für Ihre SQL Server-Umgebung.

8. Führen Sie das Skript auf dem SQL Server-Host mit einem Benutzer aus, der über ausreichende Berechtigungen verfügt.
9. Wählen Sie **Skriptergebnisse hochladen** auf der Registerkarte „SQL Server lokal“ in Workload Factory aus.
10. Wählen Sie auf der Registerkarte „SQL Server On-Premises“ bis zu fünf Datenbank-Hosts aus und klicken Sie anschließend auf **Einsparungen erkunden**, um eine Kostenanalyse der SQL Server On-Premises-Hosts im Vergleich zu FSx für ONTAP durchzuführen.
11. Im Sparrechner ist die Region für den lokalen Host auszuwählen.
12. Für eine genauere Schätzung der Kosteneinsparungen können optional die folgenden Details zu Klonen (Schattenkopien) und Snapshots in Ihrer lokalen Datenbankumgebung angegeben werden.
 - a. **Snapshot-Frequenz:** Im Menü wird eine Snapshot-Frequenz ausgewählt.

Wenn Workload Factory Schattenkopien von FSx for Windows erkennt, wird der Standardwert auf **Täglich** gesetzt. Wenn keine Schattenkopien erkannt werden, wird der Standardwert auf **Keine Snapshot-Frequenz** gesetzt.

- b. **Aktualisierungsfrequenz der Klone:** Im Menü lässt sich die Frequenz auswählen, mit der die Klone aktualisiert werden.
- c. **Anzahl der geklonten Kopien:** Die Anzahl der geklonten Kopien in der On-Premises-Konfiguration.
- d. **Monatliche Änderungsrate:** Eingabe des Prozentsatzes, um den sich Klon- und Snapshot-Daten

durchschnittlich pro Monat ändern.

13. Für genauere Ergebnisse empfiehlt sich eine Aktualisierung der Compute-Informationen sowie der Details zu Storage und Performance.

Workload Factory konsolidiert mehrere lokale SQL Server-Hosts zu einer einzigen FSx for ONTAP-Konfigurationsempfehlung, um Kosteneinsparungen zu optimieren, es sei denn, die ausgewählten lokalen Hosts überschreiten die Durchsatz-, Kapazitäts- oder IOPS-Grenzwerte für ein einzelnes FSx for ONTAP-Dateisystem.

Entfernung des On-Premises-Hosts

Nachdem Sie die Einsparmöglichkeiten für einen lokalen Microsoft SQL Server Host geprüft haben, können Sie den Eintrag für diesen Host aus Workload Factory entfernen. Anschließend kann im Aktionsmenü des lokalen Microsoft SQL Server Hosts **Delete** ausgewählt werden.

Nach der Angabe der Details für die Hostkonfiguration Ihrer Datenbank folgt eine Überprüfung der auf der Seite angezeigten Berechnungen und Empfehlungen.

Zusätzlich wird der Bericht am Ende der Seite sichtbar, sobald eine der folgenden Optionen ausgewählt ist:

- **PDF-Export**
- **Per E-Mail senden**
- **Berechnungen anzeigen**

Um zu FSx für ONTAP zu wechseln, folgen Sie den Anweisungen unter [Microsoft SQL Server auf AWS EC2 mit FSx für ONTAP-Dateisysteme bereitstellen](#).

Entdecken Sie die Einsparungen für erkannte Oracle-Hosts

Die folgenden Schritte sind auf der Registerkarte für Ihren Storage-Typ aufgeführt.

Amazon Elastic Block Store (EBS)

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Wählen Sie im Menü Datenbanken **Explore savings** aus.
4. Wählen Sie unter „Einsparungen entdecken“ die Registerkarte **Oracle on Elastic Block Store (EBS)** aus.

Wenn Workload Factory EBS-Hosts erkennt, werden Sie zur Registerkarte „Einsparmöglichkeiten erkunden“ weitergeleitet. Wenn keine EBS-Hosts erkannt werden, werden Sie zum Rechner weitergeleitet, um [Einsparmöglichkeiten durch individuelle Anpassung](#).

5. Unter **Explore savings** können Sie einen oder mehrere auf EBS ausgeführte Datenbank-Hosts auswählen und anschließend **Explore savings** auswählen.
6. Falls erforderlich, authentifizieren Sie den Datenbank-Host mit Oracle-Anmeldeinformationen oder fügen Sie fehlende Oracle-Berechtigungen hinzu.

Wenn die Seite **Explore savings** nach erfolgreicher Authentifizierung keine Daten lädt, kann durch

Auswählen der Registerkarte **Inventory** ein erneutes Laden der Daten veranlasst werden; anschließend kann die Registerkarte **Explore savings** erneut ausgewählt werden.

7. Im Savings calculator können Sie die folgenden Details zu Klonen und Snapshots in Ihrem EBS-Speicher angeben, um eine genauere Kosteneinsparungsschätzung zu erhalten.
 - a. **Snapshot-Frequenz**: Im Menü wird eine Snapshot-Frequenz ausgewählt.
 - b. **Aktualisierungsfrequenz der Klone**: Im Menü lässt sich die Frequenz auswählen, mit der die Klone aktualisiert werden.
 - c. **Anzahl der geklonten Kopien**: Eingabe der Anzahl der geklonten Kopien in der EBS Konfiguration.
 - d. **Monatliche Änderungsrate**: Eingabe des Prozentsatzes, um den sich Klon- und Snapshot-Daten durchschnittlich pro Monat ändern.
 - e. **Hosts hinzufügen**: Optional können Sie bis zu fünf erkannte EBS-Hosts auswählen, die in die Einsparungsberechnung einbezogen werden sollen.

Workload Factory konsolidiert mehrere Oracle-Hosts zu einer einzigen FSx for ONTAP-Konfigurationsempfehlung, um Kosteneinsparungen zu optimieren, es sei denn, die ausgewählten EBS-Hosts überschreiten die Durchsatz-, Kapazitäts- oder IOPS-Grenzwerte für ein einzelnes FSx for ONTAP-Dateisystem.

Oracle Server vor Ort

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Wählen Sie im Menü Datenbanken **Explore savings** aus.
4. In „Explore savings“ wählen Sie als Engine-Typ **Microsoft SQL Server** aus.
5. Wählen Sie anschließend die Registerkarte **Oracle Server on-premises** aus.
6. Wählen Sie auf der Registerkarte **Oracle Server on-premises** die Option **Assessment script > Assessment script information** und überprüfen Sie die bereitgestellten Informationen.
7. Wählen Sie **Download assessment script**.

Das Skript ist ein Datenerfassungstool, das auf PowerShell basiert. Es sammelt Konfigurations- und Leistungsdaten des Oracle Servers.

8. Führen Sie das Skript auf dem Oracle-Host mit einem Benutzer aus, der über ausreichende Berechtigungen verfügt.
9. Wählen Sie **Skriptergebnisse hochladen** und laden Sie anschließend die Skriptausgabedatei in die Workload Factory console hoch. Der Migrationsberater analysiert die Daten und plant die FSx for ONTAP-Bereitstellung für Ihre Oracle Server environment.
10. Wählen Sie auf der Registerkarte „Oracle Server On-Premises“ den lokalen Oracle Server aus und wählen Sie dann **Einsparungen erkunden**, um eine Kostenanalyse für FSx for ONTAP durchzuführen.
11. Im Sparrechner ist die Region für den lokalen Host auszuwählen.
12. Für eine genauere Schätzung der Kosteneinsparungen können optional die folgenden Details zu Klonen (Schattenkopien) und Snapshots in Ihrer lokalen Datenbankumgebung angegeben werden.
 - a. **Snapshot-Frequenz**: Im Menü wird eine Snapshot-Frequenz ausgewählt.

Wenn Workload Factory Schattenkopien von FSx for Windows erkennt, wird der Standardwert auf **Täglich** gesetzt. Wenn keine Schattenkopien erkannt werden, wird der Standardwert auf **Keine Snapshot-Frequenz** gesetzt.

- b. **Aktualisierungsfrequenz der Klone:** Im Menü lässt sich die Frequenz auswählen, mit der die Klone aktualisiert werden.
 - c. **Anzahl der geklonten Kopien:** Die Anzahl der geklonten Kopien in der On-Premises-Konfiguration.
 - d. **Monatliche Änderungsrate:** Eingabe des Prozentsatzes, um den sich Klon- und Snapshot-Daten durchschnittlich pro Monat ändern.
13. Für genauere Ergebnisse empfiehlt sich eine Aktualisierung der Compute-Informationen sowie der Details zu Storage und Performance.

Workload Factory konsolidiert mehrere lokale Oracle-Datenbanken zu einer einzigen FSx for ONTAP-Konfigurationsempfehlung, um Kosteneinsparungen zu optimieren, es sei denn, die ausgewählten lokalen Datenbanken überschreiten die Durchsatz-, Kapazitäts- oder IOPS-Grenzwerte für ein einzelnes FSx for ONTAP-Dateisystem.

Entfernung des On-Premises-Hosts

Nachdem Sie die Einsparmöglichkeiten für einen lokalen Oracle-Host geprüft haben, können Sie den Eintrag des lokalen Oracle-Hosts aus Workload Factory entfernen. Wählen Sie das Aktionsmenü des lokalen Oracle-Hosts und dann **Löschen**.

Nach der Angabe der Details für die Hostkonfiguration Ihrer Datenbank folgt eine Überprüfung der auf der Seite angezeigten Berechnungen und Empfehlungen.

Zusätzlich wird der Bericht am Ende der Seite sichtbar, sobald eine der folgenden Optionen ausgewählt ist:

- **PDF-Export**
- **Per E-Mail senden**
- **Berechnungen anzeigen**

Microsoft SQL Server auf AWS EC2 mit FSx for ONTAP einsetzen

Wenn Sie zu FSx for ONTAP wechseln möchten, um Kosteneinsparungen zu erzielen, können Sie durch Klicken auf **Create** die empfohlene(n) Konfiguration(en) direkt über den Assistenten zum Erstellen eines neuen Microsoft SQL server erstellen oder durch Klicken auf **Save** die empfohlene(n) Konfiguration(en) für später speichern.



Workload Factory unterstützt weder das Speichern noch das Erstellen mehrerer FSx for ONTAP Dateisysteme.

Deployment-Methoden

Mit Berechtigungen für die *database host creation* können Sie den neuen Microsoft SQL server auf AWS EC2 mit FSx for ONTAP direkt aus Workload Factory einsetzen. Sie können auch den Inhalt aus dem Codebox-Fenster kopieren und die empfohlene Konfiguration mit einer der Codebox-Methoden einsetzen.

Ohne Berechtigungen können Sie den Inhalt aus dem Codebox-Fenster kopieren und die empfohlene Konfiguration mithilfe einer der Codebox-Methoden einsetzen.

Verwandte Informationen

Datenbankressourcen erstellen

Erstellen eines Microsoft SQL Servers in NetApp Workload Factory für Datenbanken

Die Erstellung eines neuen Microsoft SQL Server oder Datenbankhosts in Workload Factory for Databases erfordert ein FSx for ONTAP Dateisystem Deployment und Ressourcen für Active Directory.

Über diese Aufgabe

Vor dem Erstellen eines Microsoft SQL Server aus Workload Factory sollten die verfügbaren Storage Deployment-Typen für die Datenbankhostkonfiguration, die Microsoft Multi-path I/O-Konfiguration, das Active Directory-Deployment, die Netzwerkdetails und die Anforderungen für den Abschluss dieses Vorgangs bekannt sein.

Nach dem Deployment sind [Aktivierung der Remoteverbindung auf dem Microsoft SQL Server](#) erforderlich.

FSx for ONTAP Dateisystem Deployments

Zum Erstellen eines neuen Microsoft SQL Server ist ein FSx for ONTAP Dateisystem als Storage-Backend erforderlich. Sie können ein vorhandenes FSx for ONTAP Dateisystem verwenden oder ein neues Dateisystem erstellen. Wenn Sie ein vorhandenes FSx for ONTAP Dateisystem als Storage-Backend für Ihren Datenbankserver auswählen, erstellen wir eine neue Storage VM für die Microsoft SQL Workloads.

FSx for ONTAP-Dateisysteme verfügen über zwei Microsoft SQL Server Deployment-Modelle: *Failover Cluster Instance (FCI)* oder *Standalone*. Je nach ausgewähltem FSx for ONTAP Deployment-Modell werden für das FSx for ONTAP-Dateisystem unterschiedliche Ressourcen erstellt.

- **Failover Cluster Instance (FCI) Microsoft SQL Deployment:** Bei Auswahl eines neuen FSx for ONTAP Dateisystems für das FCI Deployment wird ein FSx for NetApp ONTAP Dateisystem mit Multiple Availability Zone bereitgestellt. Für ein FCI Deployment werden separate Volumes und LUNs für Daten-, Protokoll- und tempdb-Dateien erstellt. Für den Windows-Cluster werden zusätzlich ein weiteres Volume und eine weitere LUN als Quorum- oder Zeugendatenträger erstellt.
- **Eigenständiges Microsoft SQL Deployment:** Beim Erstellen eines neuen Microsoft SQL Server wird ein FSx for ONTAP Dateisystem mit einer Single Availability Zone erstellt. Zusätzlich erstellt das System separate Volumes und LUNs für Daten-, Protokoll- und tempdb-Dateien.

Microsoft Multi-path I/O Konfiguration

Beide Deployment Modelle für Microsoft SQL Server erfordern die Erstellung von LUNs mithilfe des iSCSI Storage Protokolls. Workload Factory konfiguriert Microsoft Multi-path I/O (MPIO) im Rahmen der Konfiguration von LUNs für SQL Server über FSx for ONTAP. MPIO wird auf der Grundlage von Best Practices von AWS und NetApp konfiguriert.

Weitere Informationen sind unter ["SQL Server Hochverfügbarkeits-Deployments mit Amazon FSx for NetApp ONTAP"](#) verfügbar.

Active Directory

Für Active Directory (AD) tritt während des Deployments Folgendes auf:

- Wenn kein vorhandenes SQL-Dienstkonto angegeben wird, wird in der Domäne ein neues Microsoft SQL-Dienstkonto erstellt.

- Der Windows-Cluster, die Knotenhostnamen und der Microsoft SQL FCI-Name werden dem Microsoft SQL-Dienstkonto als verwaltete Computer hinzugefügt.
- Dem Windows Clustereintrag werden Berechtigungen zum Hinzufügen von Computern zur Domäne zugewiesen.

Benutzerverwaltete Active Directory-Sicherheitsgruppen

Wenn Sie während des Microsoft SQL Server Deployments in Workload Factory „user-managed Active Directory“ auswählen, müssen Sie eine Sicherheitsgruppe angeben, die den Datenverkehr zwischen den EC2-Instanzen und dem Verzeichnisdienst für das Deployment ermöglicht. Workload Factory ordnet die Sicherheitsgruppe für user-managed Active Directory nicht automatisch zu, wie dies bei AWS Managed Microsoft AD der Fall ist.

Rollback der Ressource

Wenn Sie ein Rollback Ihrer Domain Name System (DNS)-Ressourcen durchführen, werden die Ressourceneinträge in AD und DNS nicht automatisch entfernt. Die Einträge können wie folgt vom DNS-Server und aus AD entfernt werden.

- Bei benutzerverwaltetem AD zunächst ["Entfernen des AD-Computers"](#). Anschließend erfolgt über den DNS-Manager die Verbindung zum DNS-Server, und ["Löschen der DNS-Ressourceneinträge"](#).
- Für AWS Managed Microsoft AD ["Installation der AD-Verwaltungstools"](#). Als Nächstes ["Entfernen des AD-Computers"](#). Zum Schluss erfolgt über den DNS-Manager die Verbindung mit dem DNS-Server und ["Löschen der DNS-Ressourceneinträge"](#).

Bevor Sie beginnen

Vor der Erstellung eines neuen Datenbankhosts müssen die folgenden Voraussetzungen erfüllt sein.

Anmeldeinformationen und Berechtigungen

Sie müssen ["Berechtigungen für die Erstellung des Datenbankhosts"](#) in Ihrem AWS-Konto einen neuen Datenbankhost in Workload Factory erstellen.

Active Directory

Für die Verbindung mit Active Directory benötigen Sie Administratorrechte mit folgenden Berechtigungen:

- Beitritt zur Domäne
- Erstellung von Computerobjekten
- Objekte in der Standard-Organisationseinheit (OU) erstellen
- Alle Eigenschaften auslesen
- Der Domänenbenutzer muss auf den AD-Knoten über lokale Administratorrechte verfügen.
- Erstellung eines Microsoft SQL Server-Dienstbenutzers in AD, falls noch keiner vorhanden ist

Schritt 1: Einen Datenbankserver erstellen

Zum Abschließen dieser Aufgabe in Workload Factory mit Berechtigungen für den Modus *Automate* können die Deployment-Modi *Quick create* oder *Advanced create* verwendet werden. Außerdem können die folgenden in der Codebox verfügbaren Tools verwendet werden: REST API, AWS CLI, AWS CloudFormation und Terraform. ["Informationen zur Verwendung von Codebox für die Automatisierung"](#).



Wenn Sie Terraform aus Codebox verwenden, blendet der Code, den Sie kopieren oder herunterladen, `fsxadmin` und `vsadmin` Passwörter aus. Bei der Ausführung des Codes

müssen Sie die Passwörter erneut eingeben. Zusätzlich zu den Berechtigungen für den *Automate*-Modus benötigt das Benutzerkonto die folgenden Berechtigungen: `iam:TagRole` und `iam:TagInstanceProfile`. ["Informationen zur Verwendung von Terraform aus Codebox"](#).

Während des Deployments aktiviert Workload Factory CredSSP für die Delegierung von Anmeldeinformationen an Skripte zur Provisionierung von SQL. Wenn die Gruppenrichtlinie die CredSSP-Delegierung für alle Domänencomputer blockiert, schlägt das Deployment fehl. Nach dem Deployment deaktiviert Workload Factory CredSSP.

Schnellerstellung



In *Quick create* ist FCI das standardmäßige Deployment-Modell, Windows 2016 die Standard-Windows-Version und SQL 2019 Standard Edition die Standard-SQL-Version.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. In der Datenbankübersicht erfolgt die Auswahl von **Deploy host** und anschließend von **Microsoft SQL Server** im Menü.
4. Die Option **Quick create** auswählen.
5. Unter **AWS settings** sind folgende Angaben erforderlich:

- a. **AWS-Anmeldeinformationen:** Auswahl von AWS-Anmeldeinformationen mit automatisierten Berechtigungen zum Einsetzen des neuen Datenbankhosts.

AWS-Anmeldeinformationen mit Berechtigungen zum Erstellen von Datenbankhosts ermöglichen es Workload Factory, den neuen Datenbankhost über Ihr AWS-Konto innerhalb von workload factory einzusetzen und zu managen.

AWS-Anmeldeinformationen mit den Berechtigungen *view, planning und analysis* ermöglichen es Workload Factory, eine CloudFormation Vorlage zu generieren, die in der AWS CloudFormation Konsole verwendet werden kann.

Wenn in Workload Factory keine AWS-Anmeldeinformationen verknüpft sind und der neue Server in Workload Factory erstellt werden soll, ist **Option 1** zu verwenden, um zur Seite „Anmeldeinformationen“ zu gelangen. Dort erfolgt das manuelle Hinzufügen der erforderlichen Anmeldeinformationen und der Berechtigungen für die *Erstellung von Datenbankhosts* bei Datenbank-Workloads.

Wenn Sie das Formular zum Erstellen eines neuen Servers in Workload Factory ausfüllen möchten, um eine vollständige YAML-Dateivorlage für das Deployment in AWS CloudFormation herunterzuladen, ist **Option 2** zu verwenden, damit die erforderlichen Berechtigungen zum Erstellen des neuen Servers in AWS CloudFormation vorhanden sind. Die erforderlichen Anmeldeinformationen sowie die Berechtigungen für *Ansicht, Planung und Analyse* für Datenbank-Workloads sind manuell hinzuzufügen.

Optional können Sie eine teilweise ausgefüllte YAML-Dateivorlage aus der Codebox herunterladen, um den Stack außerhalb von Workload Factory ohne Anmeldeinformationen oder Berechtigungen zu erstellen. Für den Download der YAML-Datei steht in der Codebox im Dropdown-Menü **CloudFormation** zur Auswahl.

b. **Region & VPC:** Auswahl einer Region und eines VPC-Netzwerks.

Es ist sicherzustellen, dass Deployment-Subnetze vorhandenen Schnittstellenendpunkten zugeordnet sind und dass Sicherheitsgruppen den Zugriff auf das HTTPS-Protokoll (443) für die ausgewählten Subnetze ermöglichen.

AWS-Service-Schnittstellenendpunkte (SQS, FSx, EC2, CloudWatch, CloudFormation, SSM) und der S3-Gateway-Endpunkt werden während des Deployments erstellt, sofern sie nicht gefunden werden.

VPC DNS Attribute `EnableDnsSupport` und `EnableDnsHostnames` werden so geändert, dass die Auflösung von Endpunktadressen aktiviert wird, falls sie nicht bereits auf `true` gesetzt sind.

Bei Verwendung eines VPC-übergreifenden DNS muss die Sicherheitsgruppe für Endpunkte in der anderen VPC, in der sich das DNS befindet, Port 443 für Deployment Subnetze zulassen. Andernfalls ist beim Beitritt zu einem VPC-übergreifenden Active Directory ein DNS-Resolver aus der lokalen VPC bereitzustellen. In einer Umgebung mit mehreren replizierten Domain Controllers kann, wenn einige Domain Controllers vom Subnetz aus nicht erreichbar sind, **Zu CloudFormation umleiten** ausgewählt und `Preferred domain controller` eingegeben werden, um die Verbindung zu Active Directory herzustellen.

c. **Verfügbarkeitszonen:** Verfügbarkeitszonen und Subnetze werden gemäß dem Failover Cluster Instance (FCI) Deployment-Modell ausgewählt.



FCI Deployments werden nur auf FSx for ONTAP Konfigurationen mit Multiple Availability Zone (MAZ) unterstützt.

- i. Im Feld **Clusterkonfiguration - Knoten 1** erfolgt die Auswahl der primären Verfügbarkeitszone für die MAZ FSx for ONTAP Konfiguration aus dem Dropdown-Menü **Verfügbarkeitszone** sowie eines Subnetzes aus der primären Verfügbarkeitszone aus dem Dropdown-Menü **Subnetz**.
- ii. Im Feld **Clusterkonfiguration - Knoten 2** wird die sekundäre Availability Zone für die MAZ FSx for ONTAP Konfiguration im Dropdown-Menü **Availability zone** ausgewählt sowie ein Subnetz aus der sekundären Availability Zone im Dropdown-Menü **Subnet**.

6. Unter **Anwendungseinstellungen** werden ein Benutzername und ein Passwort für die **Datenbankzugangsdaten** eingegeben.

Für GovCloud-Konten geben Sie den Wert für den AWS SSM Parameter-ARN im folgenden Format ein:

```
{ fsx: { "username": "fsxadmin", "password": "pass" } }.
```

Der Wert wird im Parameter Store unter Parameterdetails in der AWS Management Console bereitgestellt. Der AWS SSM-Parametertyp muss „Secure String“ sein, mit dem Namen im Format `/netapp/wlmdb/<anyname>`. Weitere Informationen zum Abrufen von SSM-Parametern finden Sie unter ["AWS GovCloud-Dokumentation"](#).

7. Unter **Konnektivität** sind folgende Angaben erforderlich:

a. **Schlüsselpaar:** Auswahl eines Schlüsselpaars.

b. **Active Directory:**

- i. Im Feld **Domänenname** wird ein Name für die Domäne ausgewählt oder eingegeben.
 - A. Bei AWS-verwalteten Active Directories erscheinen Domännennamen im Dropdown-Menü.

- B. Bei einem benutzerverwalteten Active Directory erfolgt die Eingabe eines Namens im Feld **Suchen und Hinzufügen**; anschließend wird **Hinzufügen** ausgewählt.
- ii. Im Feld **DNS-Adresse** wird die DNS-IP-Adresse für die Domain eingegeben. Es können bis zu 3 IP-Adressen hinzugefügt werden.

Bei von AWS verwalteten Active Directories werden die DNS-IP-Adressen im Dropdown-Menü angezeigt.

- iii. Im Feld **Benutzername** ist der Benutzername für die Active Directory-Domäne einzugeben.
- iv. Im Feld **Passwort** geben Sie ein Passwort für die Active Directory-Domäne ein.

Für GovCloud-Konten geben Sie den AWS SSM Parameter-ARN-Wert für Active Directory-Anmeldeinformationen im folgenden Format ein:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Der AWS SSM-Parametertyp muss „Secure String“ sein, mit dem Namen im Format `/netapp/wlmdb/<anyname>`. Weitere Informationen zum Abrufen von SSM-Parametern finden Sie unter ["AWS GovCloud-Dokumentation"](#).

8. Unter **Infrastruktureinstellungen** sind die folgenden Angaben erforderlich:

- a. **FSx for ONTAP System**: Ein neues FSx for ONTAP Dateisystem erstellen oder ein vorhandenes FSx for ONTAP Dateisystem verwenden.

- i. **Neues FSx for ONTAP erstellen**: Eingabe von Benutzername und Passwort.

Für GovCloud-Konten geben Sie den AWS SSM Parameter-ARN-Wert für FSx for ONTAP-Anmeldeinformationen im folgenden Format ein:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Der AWS SSM-Parametertyp muss „Secure String“ sein, mit dem Namen im Format `/netapp/wlmdb/<anyname>`. Weitere Informationen zum Abrufen von SSM-Parametern finden Sie unter ["AWS GovCloud-Dokumentation"](#).

Ein neues FSx for ONTAP Dateisystem kann die Installationszeit um 30 Minuten oder mehr verlängern.

- i. **Vorhandenes FSx für ONTAP**: Wählen Sie den FSx für ONTAP Namen aus und geben Sie einen Benutzernamen und ein Passwort für das Dateisystem ein.

Für bestehende FSx for ONTAP Dateisysteme sind die folgenden Punkte zu beachten:

- Die an FSx for ONTAP angehängte Routing-Gruppe ermöglicht, Routen zu den Subnetzen für das Deployment zu verwenden.
- Die Sicherheitsgruppe erlaubt Datenverkehr aus den für das Deployment verwendeten Subnetzen, insbesondere über die TCP-Ports HTTPS (443) und iSCSI (3260).

- b. **Datenträgergröße**: Die Kapazität des Datenträgers und die Kapazitätseinheit angeben.

9. Zusammenfassung:

- a. **Vorschau der Standardeinstellungen**: Prüfung der von Quick create festgelegten Standardkonfigurationen.
- b. **Geschätzte Kosten**: Enthält eine Schätzung der Kosten, die Ihnen entstehen könnten, wenn Sie die angezeigten Ressourcen einsetzen.

10. Klicken Sie auf **Create**.

Alternativ können Sie, falls Sie eine dieser Standardeinstellungen jetzt ändern möchten, den Datenbankserver mit **Advanced create** erstellen.

Sie können auch **Konfiguration speichern** auswählen, um den Host später einzusetzen.

Erweiterte Erstellung

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. In der Datenbankübersicht erfolgt die Auswahl von **Deploy host** und anschließend von **Microsoft SQL Server** im Menü.
4. **Advanced create** ist auszuwählen.
5. Für **Deployment-Modell** stehen **Failover Cluster Instance** oder **Single instance** zur Auswahl.
6. Unter **AWS settings** sind folgende Angaben erforderlich:

- a. **AWS-Anmeldeinformationen:** Auswahl von AWS-Anmeldeinformationen mit automatisierten Berechtigungen zum Einsetzen des neuen Datenbankhosts.

AWS-Anmeldeinformationen mit Berechtigungen zum Erstellen von Datenbankhosts ermöglichen es Workload Factory, den neuen Datenbankhost über Ihr AWS-Konto innerhalb von workload factory einzusetzen und zu managen.

AWS-Anmeldeinformationen mit den Berechtigungen *view, planning und analysis* ermöglichen es Workload Factory, eine CloudFormation Vorlage zu generieren, die in der AWS CloudFormation Konsole verwendet werden kann.

Wenn in Workload Factory keine AWS-Anmeldeinformationen verknüpft sind und der neue Server in Workload Factory erstellt werden soll, ist **Option 1** zu verwenden, um zur Seite „Anmeldeinformationen“ zu gelangen. Dort erfolgt das manuelle Hinzufügen der erforderlichen Anmeldeinformationen und der Berechtigungen für die *Erstellung von Datenbankhosts* bei Datenbank-Workloads.

Wenn Sie das Formular zum Erstellen eines neuen Servers in Workload Factory ausfüllen möchten, um eine vollständige YAML-Dateivorlage für das Deployment in AWS CloudFormation herunterzuladen, ist **Option 2** zu verwenden, damit die erforderlichen Berechtigungen zum Erstellen des neuen Servers in AWS CloudFormation vorhanden sind. Die erforderlichen Anmeldeinformationen sowie die Berechtigungen für *Ansicht, Planung und Analyse* für Datenbank-Workloads sind manuell hinzuzufügen.

Optional können Sie eine teilweise ausgefüllte YAML-Dateivorlage aus der Codebox herunterladen, um den Stack außerhalb von Workload Factory ohne Anmeldeinformationen oder Berechtigungen zu erstellen. Für den Download der YAML-Datei steht in der Codebox im Dropdown-Menü **CloudFormation** zur Auswahl.

- b. **Region & VPC:** Auswahl einer Region und eines VPC-Netzwerks.

Sicherheitsgruppen für einen vorhandenen Schnittstellenendpunkt müssen den Zugriff über das HTTPS-Protokoll (443) auf die ausgewählten Subnetze zulassen.

AWS Service-Schnittstellenendpunkte (SQS, FSx, EC2, CloudWatch, Cloud Formation, SSM) und der S3-Gateway-Endpunkt werden während des Deployment erstellt, wenn sie nicht gefunden werden.

Die VPC-DNS-Attribute `EnableDnsSupport` und `EnableDnsHostnames` werden so geändert, dass die Auflösung von Endpunktadressen ermöglicht wird, falls sie nicht bereits auf `true` festgelegt sind.

- c. **Verfügbarkeitszonen:** Verfügbarkeitszonen und Subnetze sind entsprechend dem ausgewählten Deployment-Modell auszuwählen. Subnetze sollten aus Gründen der Hochverfügbarkeit nicht dieselbe Routingtabelle verwenden.



FCI Deployments werden nur auf FSx for ONTAP Konfigurationen mit Multiple Availability Zone (MAZ) unterstützt.

- Für Einzelinstanzbereitstellungen:
 - Im Feld **Clusterkonfiguration - Knoten 1** stehen im Dropdown-Menü **Verfügbarkeitszone** eine Verfügbarkeitszone und im Dropdown-Menü **Subnetz** ein Subnetz zur Auswahl.
- Für FCI Deployments:
 - Im Feld **Clusterkonfiguration - Knoten 1** erfolgt die Auswahl der primären Verfügbarkeitszone für die MAZ FSx for ONTAP Konfiguration aus dem Dropdown-Menü **Verfügbarkeitszone** sowie eines Subnetzes aus der primären Verfügbarkeitszone aus dem Dropdown-Menü **Subnetz**.
 - Im Feld **Clusterkonfiguration - Knoten 2** wird die sekundäre Availability Zone für die MAZ FSx for ONTAP Konfiguration im Dropdown-Menü **Availability zone** ausgewählt sowie ein Subnetz aus der sekundären Availability Zone im Dropdown-Menü **Subnet**.

- d. **Sicherheitsgruppe:** Eine Arbeitslast-Sicherheitsgruppe wird erstellt, um die für die Kommunikation zwischen Microsoft SQL und Windows-Cluster auf den Knoten erforderlichen Ports und Protokolle zuzulassen. Zusätzlich können Sie eine oder mehrere Sicherheitsgruppen auswählen.

7. Unter **Anwendungseinstellungen** sind folgende Angaben erforderlich:

- a. Unter **SQL Server Installationsart** erfolgt die Auswahl von **License included AMI** oder **Use custom AMI**.
- i. Bei Auswahl von **License included AMI** sind folgende Angaben erforderlich:
- A. **Betriebssystem:** Zur Auswahl stehen **Windows server 2016**, **Windows server 2019** oder **Windows server 2022**.
 - B. **Datenbankedition:** Zur Auswahl stehen **SQL Server Standard Edition** oder **SQL Server Enterprise Edition**.
 - C. **Datenbankversion:** Zur Auswahl stehen **SQL Server 2016**, **SQL Server 2019** oder **SQL Server 2022**.
 - D. **SQL Server AMI:** Auswahl eines SQL Server AMI aus dem Dropdown-Menü.
- ii. Wenn **Benutzerdefiniertes AMI verwenden** ausgewählt wird, erfolgt die Auswahl eines AMI im Dropdown-Menü.
- b. **SQL Server Sortierung:** Auswahl eines Sortierungssatzes für den Server.



Falls die ausgewählte Kollation für die Installation nicht kompatibel ist, empfehlen wir Ihnen, die Standardkollation „SQL_Latin1_General_CP1_CI_AS“ auszuwählen.

- c. **Datenbankname:** Eingabe des Namens des Datenbankclusters.

- d. **Datenbank-Anmeldeinformationen:** Eingabe eines Benutzernamens und Kennworts für ein neues Dienstkonto oder Verwendung der Anmeldedaten eines vorhandenen Dienstkontos im Active Directory.

Optional: Auswahl von **Use managed service account** für das SQL Server-Dienstkonto. Diese Option eignet sich, wenn Ihre Umgebung MSA (Managed Service Account) oder Group Managed Service Accounts (gMSA) verwendet und die Kennwortverwaltung von Active Directory übernommen wird.

Für GovCloud-Konten geben Sie den Wert für den AWS SSM Parameter-ARN im folgenden Format ein:

```
{fsx:{"username":"fsxadmin","password":"pass"}}
```

Der Wert wird im Parameter Store unter Parameterdetails in der AWS Management Console bereitgestellt. Der AWS SSM-Parametertyp muss „Secure String“ sein, mit dem Namen im Format /netapp/wlmdb/<anyname>. Weitere Informationen zum Abrufen von SSM-Parametern finden Sie unter ["AWS GovCloud-Dokumentation"](#).

8. Unter **Konnektivität** sind folgende Angaben erforderlich:

a. **Schlüsselpaar:** Auswahl eines Schlüsselpaars für eine sichere Verbindung zu Ihrer Instanz.

b. **Active Directory:** Folgende Angaben zu Active Directory sind erforderlich:

- i. Im Feld **Domänenname** wird ein Name für die Domäne ausgewählt oder eingegeben.

A. Bei AWS-verwalteten Active Directories erscheinen Domänennamen im Dropdown-Menü.

B. Bei einem benutzerverwalteten Active Directory erfolgt die Eingabe eines Namens im Feld **Suchen und Hinzufügen**; anschließend wird **Hinzufügen** ausgewählt.

- ii. Im Feld **DNS-Adresse** wird die DNS-IP-Adresse für die Domain eingegeben. Es können bis zu 3 IP-Adressen hinzugefügt werden.

Bei von AWS verwalteten Active Directories werden die DNS-IP-Adressen im Dropdown-Menü angezeigt.

- iii. Geben Sie den Benutzernamen und das Kennwort für die Active Directory-Domain ein.

Für GovCloud-Konten geben Sie den AWS SSM Parameter-ARN-Wert für Active Directory-Anmeldeinformationen im folgenden Format ein:

```
{fsx:{"username":"fsxadmin","password":"pass"}}
```

Der AWS SSM-Parametertyp muss „Secure String“ sein, mit dem Namen im Format /netapp/wlmdb/<anyname>. Weitere Informationen zum Abrufen von SSM-Parametern finden Sie unter ["AWS GovCloud-Dokumentation"](#).

- iv. **Bevorzugter Domänencontroller:** Optional lässt sich der bevorzugte Domänencontroller angeben, der für den Beitritt zu Active Directory verwendet werden soll.

v. **Bevorzugter Pfad der Organisationseinheit:** Optional kann die bevorzugte Organisationseinheit (OU) im Active Directory angegeben werden, die für den Beitritt verwendet werden soll.

- vi. **Ziel Active Directory-Gruppe:** Optional kann die Ziel Active Directory-Gruppe angegeben werden, der die Computer hinzugefügt werden sollen.

9. Unter **Infrastruktureinstellungen** sind die folgenden Angaben erforderlich:

a. **DB-Instanztyp:** Im Dropdown-Menü wird der Typ der Datenbankinstanz ausgewählt.

- b. **FSx for ONTAP System:** Ein neues FSx for ONTAP Dateisystem erstellen oder ein vorhandenes FSx for ONTAP Dateisystem verwenden.

- i. **Neues FSx for ONTAP erstellen:** Eingabe von Benutzername und Passwort.

Für GovCloud-Konten geben Sie den AWS SSM-Parameter-ARN-Wert für die FSx for ONTAP-Anmeldeinformationen im folgenden Format ein:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Der AWS SSM-Parametertyp muss „Secure String“ sein, mit dem Namen im Format `/netapp/wlmdb/<anyname>`. Weitere Informationen zum Abrufen von SSM-Parametern finden Sie unter ["AWS GovCloud-Dokumentation"](#).

Ein neues FSx for ONTAP Dateisystem kann die Installationszeit um 30 Minuten oder mehr verlängern.

- ii. **Vorhandenes FSx for ONTAP auswählen:** Im Dropdown-Menü werden der Name von FSx for ONTAP ausgewählt sowie ein Benutzername und ein Passwort für das Dateisystem eingegeben.

Für bestehende FSx for ONTAP Dateisysteme sind die folgenden Punkte zu beachten:

- Die an FSx for ONTAP angehängte Routing-Gruppe ermöglicht, Routen zu den Subnetzen für das Deployment zu verwenden.
- Die Sicherheitsgruppe erlaubt Datenverkehr aus den für das Deployment verwendeten Subnetzen, insbesondere über die TCP-Ports HTTPS (443) und iSCSI (3260).

- c. **Snapshot-Richtlinie:** Standardmäßig aktiviert. Snapshots werden täglich erstellt und 7 Tage lang aufbewahrt.

Die Snapshots sind den Volumes zugewiesen, die für SQL-Workloads erstellt wurden.

- d. **Datenträgergröße:** Die Kapazität des Datenträgers und die Kapazitätseinheit angeben.

- e. **Provisionierte IOPS:** Zur Auswahl stehen **Automatisch** oder **vom Benutzer provisioniert**. Bei Auswahl von **vom Benutzer provisioniert** ist der IOPS-Wert anzugeben.

- f. **Durchsatzkapazität:** Die Durchsatzkapazität wird im Dropdown-Menü ausgewählt.

In bestimmten Regionen können Sie eine Durchsatzkapazität von 4 GB/s auswählen. Zum Provisionieren einer Durchsatzkapazität von 4 GB/s muss Ihr FSx for ONTAP Dateisystem mit einer SSD Storage Kapazität von mindestens 5.120 GiB und 160.000 SSD IOPS konfiguriert sein.

- g. **Verschlüsselung:** Wählen Sie einen Schlüssel aus Ihrem Konto oder aus einem anderen Konto. Sie müssen den ARN des Verschlüsselungsschlüssels aus einem anderen Konto eingeben.

Benutzerdefinierte Verschlüsselungsschlüssel für FSx for ONTAP werden basierend auf der Dienstkompatibilität nicht aufgeführt. Die Auswahl eines geeigneten FSx-Verschlüsselungsschlüssels ist erforderlich. Nicht-FSx-Verschlüsselungsschlüssel führen dazu, dass die Servererstellung fehlschlägt.

Die von AWS verwalteten Schlüssel werden anhand ihrer Anwendbarkeit für den jeweiligen Dienst gefiltert.

- h. **Tags:** Optional lassen sich bis zu 40 Tags hinzufügen.

- i. **Simple Notification Service:** Optional können Sie den Simple Notification Service (SNS) für diese Konfiguration aktivieren, indem Sie im Dropdown-Menü ein SNS-Topic für Microsoft SQL

Server auswählen.

- i. Die Aktivierung des Simple Notification Service ist erforderlich.
- ii. Die Auswahl einer ARN erfolgt über das Dropdown-Menü.
- j. **CloudWatch Überwachung:** Optional können Sie die CloudWatch Überwachung aktivieren.

Wir empfehlen, CloudWatch für die Fehlersuche im Fehlerfall zu aktivieren. Die Ereignisse, die in der AWS CloudFormation Konsole angezeigt werden, sind allgemein gehalten und geben nicht die eigentliche Ursache an. Alle detaillierten Protokolle werden im `C:\cfn\logs` Ordner in den EC2 Instanzen gespeichert.

In CloudWatch wird eine Protokollgruppe mit dem Namen des Stacks erstellt. Unter der Protokollgruppe wird für jeden Validierungsknoten und SQL-Knoten ein Protokollstream angezeigt. CloudWatch zeigt den Skriptfortschritt an und liefert Informationen, anhand derer Sie erkennen können, ob und wann ein Deployment fehlschlägt.

- a. **Ressourcen-Rollback:** Für diese Funktion gibt es derzeit keine Unterstützung.

10. Zusammenfassung

- a. **Geschätzte Kosten:** Enthält eine Schätzung der Kosten, die Ihnen entstehen könnten, wenn Sie die angezeigten Ressourcen einsetzen.

11. Mit **Erstellen** wird der neue Datenbankhost eingesetzt.

Alternativ können Sie die Konfiguration speichern.

Schritt 2: Aktivierung der Remote-Verbindung auf dem Microsoft SQL Server

Nach der Serverbereitstellung aktiviert Workload Factory die Remote-Verbindung zum Microsoft SQL Server nicht. Die Aktivierung der Remote-Verbindung erfolgt in den folgenden Schritten.

Schritte

1. Die Verwendung der Computeridentität für NTLM ist in der Microsoft-Dokumentation unter ["Netzwerksicherheit: Lokalem System die Verwendung der Computeridentität für NTLM erlauben"](#) beschrieben.
2. Die dynamische Portkonfiguration lässt sich anhand von ["Beim Herstellen einer Verbindung zu SQL Server ist ein netzwerkbezogener oder instanzspezifischer Fehler aufgetreten"](#) in der Microsoft-Dokumentation überprüfen.
3. Die Sicherheitsgruppe muss die erforderliche Client-IP oder das Subnetz zulassen.

Was kommt als Nächstes

Jetzt können Sie ["Erstellen einer Datenbank in Workload Factory for Databases"](#).

Einen PostgreSQL-Server in der NetApp Workload Factory für Datenbanken erstellen

Die Erstellung eines neuen PostgreSQL-Servers oder Datenbankhosts in NetApp Workload Factory for Databases erfordert ein FSx for ONTAP Dateisystem-Deployment und Ressourcen für Active Directory.

Über diese Aufgabe

Bevor Sie einen PostgreSQL-Server aus der Workload Factory erstellen, sollten Sie sich über die verfügbaren

Storage Deployment-Typen für die Datenbankhostkonfiguration, die Betriebsmodi der Workload Factory und die Anforderungen für die Durchführung dieses Vorgangs informieren.

FSx for ONTAP Dateisystem Deployments

Für die Erstellung eines neuen PostgreSQL-Servers wird ein FSx for ONTAP Dateisystem als Storage-Backend benötigt. Sie können ein vorhandenes FSx for ONTAP Dateisystem verwenden oder ein neues Dateisystem erstellen. Wenn Sie ein vorhandenes FSx for ONTAP Dateisystem als Storage-Backend für Ihren Datenbankserver auswählen, erstellen wir eine neue Storage VM für die PostgreSQL-Workloads.

+ FSx for ONTAP Dateisysteme haben zwei PostgreSQL Server Deployment-Modelle: *High Availability (HA)* oder *Einzelinstanz*. Für das FSx for ONTAP Dateisystem entstehen je nach ausgewähltem FSx for ONTAP Deployment-Modell unterschiedliche Ressourcen.

- **High Availability (HA) Deployment:** Ein FSx for NetApp ONTAP Dateisystem mit mehreren Availability Zones wird eingesetzt, wenn ein neues FSx for ONTAP Dateisystem für ein HA Deployment ausgewählt wird. Für ein HA Deployment werden separate Volumes und LUNs für Daten-, Protokoll- und tempdb-Dateien erstellt. Für den Quorum- oder Zeugendatenträger für den Windows-Cluster werden ein zusätzliches Volume und eine zusätzliche LUN erstellt. Das HA Deployment konfiguriert die Streaming-Replikation zwischen den primären und sekundären PostgreSQL-Servern.
- **Single instance Deployment:** Ein FSx for ONTAP Dateisystem in einer einzelnen Availability Zone wird erstellt, wenn ein neuer PostgreSQL Server erstellt wird. Zusätzlich werden separate Volumes und LUNs für Daten-, Protokoll- und tempdb-Dateien erstellt.

Bevor Sie beginnen

Sie müssen ["Berechtigungen für die Erstellung des Datenbankhosts"](#) in Ihrem AWS-Konto haben, um einen neuen Datenbankhost in Workload Factory zu erstellen.

Einen PostgreSQL-Server erstellen

Sie können die Deployment-Modi „Quick create“ oder „Advanced create“ verwenden, um diese Aufgabe in workload factory mit den Berechtigungen des Modus „Automate“ abzuschließen. Außerdem können die folgenden in der Codebox verfügbaren Tools verwendet werden: REST API, AWS CLI, AWS CloudFormation und Terraform. ["Informationen zur Verwendung von Codebox für die Automatisierung"](#).



Wenn Sie Terraform aus Codebox verwenden, werden im Code, den Sie kopieren oder herunterladen, Passwörter ausgeblendet `fsxadmin` und `vsadmin`. Sie müssen die Passwörter erneut eingeben, wenn Sie den Code ausführen. Zusätzlich zu den Berechtigungen für den *Automate*-Modus müssen Sie für das Benutzerkonto die folgenden Berechtigungen einschließen: `iam:TagRole` und `iam:TagInstanceProfile`. ["Informationen zur Verwendung von Terraform aus Codebox"](#).

Schnellerstellung



Bei der *Schnellerstellung* ist HA das Standard-Deployment-Modell, Windows 2016 die Standard-Windows-Version und SQL 2019 Standard Edition die Standard-SQL-Version.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.

3. In der Datenbankübersicht erfolgt die Auswahl von **Host einsetzen** und anschließend im Menü von **PostgreSQL Server**.
4. Die Option **Quick create** auswählen.
5. Unter **Landing zone** sind die folgenden Angaben erforderlich:

- a. **AWS-Anmeldeinformationen:** Auswahl von AWS-Anmeldeinformationen mit automatisierten Berechtigungen zum Einsetzen des neuen Datenbankhosts.

AWS-Anmeldeinformationen mit Berechtigungen zum Erstellen von Datenbankhosts ermöglichen es Workload Factory, den neuen Datenbankhost über Ihr AWS-Konto innerhalb von workload factory einzusetzen und zu managen.

AWS-Anmeldeinformationen mit den Berechtigungen *view, planning und analysis* ermöglichen es Workload Factory, eine CloudFormation Vorlage zu generieren, die in der AWS CloudFormation Konsole verwendet werden kann.

Wenn in Workload Factory keine AWS-Anmeldeinformationen verknüpft sind und der neue Server in Workload Factory erstellt werden soll, ist **Option 1** zu verwenden, um zur Seite „Anmeldeinformationen“ zu gelangen. Dort erfolgt das manuelle Hinzufügen der erforderlichen Anmeldeinformationen und der Berechtigungen für die *Erstellung von Datenbankhosts* bei Datenbank-Workloads.

Wenn Sie das Formular zum Erstellen eines neuen Servers in Workload Factory ausfüllen möchten, um eine vollständige YAML-Dateivorlage für das Deployment in AWS CloudFormation herunterzuladen, ist **Option 2** zu verwenden, damit die erforderlichen Berechtigungen zum Erstellen des neuen Servers in AWS CloudFormation vorhanden sind. Die erforderlichen Anmeldeinformationen sowie die Berechtigungen für *Ansicht, Planung und Analyse* für Datenbank-Workloads sind manuell hinzuzufügen.

Optional können Sie eine teilweise ausgefüllte YAML-Dateivorlage aus der Codebox herunterladen, um den Stack außerhalb von Workload Factory ohne Anmeldeinformationen oder Berechtigungen zu erstellen. Für den Download der YAML-Datei steht in der Codebox im Dropdown-Menü **CloudFormation** zur Auswahl.

- b. **Region & VPC:** Auswahl einer Region und eines VPC-Netzwerks.

Sicherheitsgruppen für einen vorhandenen Schnittstellenendpunkt müssen den Zugriff über das HTTPS-Protokoll (443) auf die ausgewählten Subnetze zulassen.

AWS-Service-Schnittstellenendpunkte (SQS, FSx, EC2, CloudWatch, CloudFormation, SSM) und der S3-Gateway-Endpunkt werden während des Deployments erstellt, sofern sie nicht gefunden werden.

VPC DNS Attribute `EnableDnsSupport` und `EnableDnsHostnames` werden so geändert, dass die Auflösung von Endpunktadressen aktiviert wird, falls sie nicht bereits auf `true` gesetzt sind.

- c. **Verfügbarkeitszonen:** Auswahl von Verfügbarkeitszonen und Subnetzen.



HA Deployments werden nur für Multiple Availability Zone (MAZ) FSx for ONTAP Konfigurationen unterstützt.

Aus Gründen der Hochverfügbarkeit sollten Subnetze nicht dieselbe Routingtabelle verwenden.

- i. Im Feld **Clusterkonfiguration - Knoten 1** erfolgt die Auswahl der primären

Verfügbarkeitszone für die MAZ FSx for ONTAP Konfiguration aus dem Dropdown-Menü **Verfügbarkeitszone** sowie eines Subnetzes aus der primären Verfügbarkeitszone aus dem Dropdown-Menü **Subnetz**.

- ii. Im Feld **Clusterkonfiguration - Knoten 2** wird die sekundäre Availability Zone für die MAZ FSx for ONTAP Konfiguration im Dropdown-Menü **Availability zone** ausgewählt sowie ein Subnetz aus der sekundären Availability Zone im Dropdown-Menü **Subnet**.

6. Unter **Anwendungseinstellungen** werden ein Benutzername und ein Passwort für die **Datenbankzugangsdaten** eingegeben.
7. Unter **Konnektivität** wird ein Schlüsselpaar ausgewählt, um eine sichere Verbindung zu Ihrer Instanz herzustellen.
8. Unter **Infrastruktureinstellungen** sind die folgenden Angaben erforderlich:
 - a. **FSx for ONTAP System**: Ein neues FSx for ONTAP Dateisystem erstellen oder ein vorhandenes FSx for ONTAP Dateisystem verwenden.

- i. **Neues FSx for ONTAP erstellen**: Eingabe von Benutzername und Passwort.

Für GovCloud-Konten geben Sie den AWS SSM Parameter-ARN-Wert für FSx for ONTAP-Anmeldeinformationen im folgenden Format ein:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Der AWS SSM-Parametertyp muss „Secure String“ sein, mit dem Namen im Format `/netapp/wlmdb/<anyname>`. Weitere Informationen zum Abrufen von SSM-Parametern finden Sie unter ["AWS GovCloud-Dokumentation"](#).

Ein neues FSx for ONTAP Dateisystem kann die Installationszeit um 30 Minuten oder mehr verlängern.

- i. **Vorhandenes FSx for ONTAP auswählen**: Im Dropdown-Menü werden der Name von FSx for ONTAP ausgewählt sowie ein Benutzername und ein Passwort für das Dateisystem eingegeben.

Für bestehende FSx for ONTAP Dateisysteme sind die folgenden Punkte zu beachten:

- Die an FSx for ONTAP angehängte Routing-Gruppe ermöglicht, Routen zu den Subnetzen für das Deployment zu verwenden.
- Die Sicherheitsgruppe erlaubt Datenverkehr aus den für das Deployment verwendeten Subnetzen, insbesondere über die TCP-Ports HTTPS (443) und iSCSI (3260).

- b. **Datenträgergröße**: Die Kapazität des Datenträgers und die Kapazitätseinheit angeben.

9. Zusammenfassung:

- a. **Vorschau der Standardeinstellungen**: Prüfung der von Quick create festgelegten Standardkonfigurationen.
 - b. **Geschätzte Kosten**: Enthält eine Schätzung der Kosten, die Ihnen entstehen könnten, wenn Sie die angezeigten Ressourcen einsetzen.

10. Klicken Sie auf **Create**.

Alternativ können Sie, falls Sie eine dieser Standardeinstellungen jetzt ändern möchten, den Datenbankserver mit Advanced create erstellen.

Sie können auch **Konfiguration speichern** auswählen, um den Host später einzusetzen.

Erweiterte Erstellung

Schritte

1. Melden Sie sich bei der "NetApp Console" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. In der Datenbankübersicht erfolgt die Auswahl von **Host einsetzen** und anschließend im Menü von **PostgreSQL Server**.
4. **Advanced create** ist auszuwählen.
5. Unter **Bereitstellungsmodell** steht entweder **Standalone-Instanz** oder **Hochverfügbarkeit (HA)** zur Auswahl.
6. Unter **Landing zone** sind die folgenden Angaben erforderlich:
 - a. **AWS-Anmeldeinformationen**: Auswahl von AWS-Anmeldeinformationen mit automatisierten Berechtigungen zum Einsetzen des neuen Datenbankhosts.

AWS-Anmeldeinformationen mit Berechtigungen zum Erstellen von Datenbankhosts ermöglichen es Workload Factory, den neuen Datenbankhost über Ihr AWS-Konto innerhalb von workload factory einzusetzen und zu managen.

AWS-Anmeldeinformationen mit den Berechtigungen *view, planning und analysis* ermöglichen es Workload Factory, eine CloudFormation Vorlage zu generieren, die in der AWS CloudFormation Konsole verwendet werden kann.

Wenn in Workload Factory keine AWS-Anmeldeinformationen verknüpft sind und der neue Server in Workload Factory erstellt werden soll, ist **Option 1** zu verwenden, um zur Seite „Anmeldeinformationen“ zu gelangen. Dort erfolgt das manuelle Hinzufügen der erforderlichen Anmeldeinformationen und der Berechtigungen für die *Erstellung von Datenbankhosts* bei Datenbank-Workloads.

Wenn Sie das Formular zum Erstellen eines neuen Servers in Workload Factory ausfüllen möchten, um eine vollständige YAML-Dateivorlage für das Deployment in AWS CloudFormation herunterzuladen, ist **Option 2** zu verwenden, damit die erforderlichen Berechtigungen zum Erstellen des neuen Servers in AWS CloudFormation vorhanden sind. Die erforderlichen Anmeldeinformationen sowie die Berechtigungen für *Ansicht, Planung und Analyse* für Datenbank-Workloads sind manuell hinzuzufügen.

Optional können Sie eine teilweise ausgefüllte YAML-Dateivorlage aus der Codebox herunterladen, um den Stack außerhalb von Workload Factory ohne Anmeldeinformationen oder Berechtigungen zu erstellen. Für den Download der YAML-Datei steht in der Codebox im Dropdown-Menü **CloudFormation** zur Auswahl.

- b. **Region & VPC**: Auswahl einer Region und eines VPC-Netzwerks.

Sicherheitsgruppen für einen vorhandenen Schnittstellenendpunkt müssen den Zugriff über das HTTPS-Protokoll (443) auf die ausgewählten Subnetze zulassen.

AWS Service-Schnittstellenendpunkte (SQS, FSx, EC2, CloudWatch, Cloud Formation, SSM) und der S3-Gateway-Endpunkt werden während des Deployment erstellt, wenn sie nicht gefunden werden.

Die VPC-DNS-Attribute `EnableDnsSupport` und `EnableDnsHostnames` werden so geändert, dass die Auflösung von Endpunktadressen ermöglicht wird, falls sie nicht bereits auf `true` festgelegt sind.

c. **Verfügbarkeitszonen:** Auswahl von Verfügbarkeitszonen und Subnetzen.

Für Einzelinstanz-Deployments

Im Feld **Clusterkonfiguration - Knoten 1** ist eine Verfügbarkeitszone aus dem Dropdown-Menü **Verfügbarkeitszone** und ein Subnetz aus dem Dropdown-Menü **Subnetz** auszuwählen.

Für HA Deployments

- i. Im Feld **Clusterkonfiguration - Knoten 1** erfolgt die Auswahl der primären Verfügbarkeitszone für die MAZ FSx for ONTAP Konfiguration aus dem Dropdown-Menü **Verfügbarkeitszone** sowie eines Subnetzes aus der primären Verfügbarkeitszone aus dem Dropdown-Menü **Subnetz**.
 - ii. Im Feld **Clusterkonfiguration - Knoten 2** wird die sekundäre Availability Zone für die MAZ FSx for ONTAP Konfiguration im Dropdown-Menü **Availability zone** ausgewählt sowie ein Subnetz aus der sekundären Availability Zone im Dropdown-Menü **Subnetz**.
- d. **Sicherheitsgruppe:** Es wird eine Arbeitslast-Sicherheitsgruppe erstellt, um die für PostgreSQL erforderlichen Ports und Protokolle zuzulassen. Zusätzlich können Sie eine oder mehrere Sicherheitsgruppen auswählen.
7. Unter **Anwendungseinstellungen** sind folgende Angaben erforderlich:
- a. Die Auswahl des **Betriebssystems** erfolgt über das Dropdown-Menü.
 - b. Die **PostgreSQL Version** wird im Dropdown-Menü ausgewählt.
 - c. **Name des Datenbankservers:** Eingabe des Namens des Datenbankclusters.
 - d. **Datenbank-Anmeldeinformationen:** Eingabe eines Benutzernamens und Kennworts für ein neues Dienstkonto oder Verwendung der Anmeldeinformationen eines vorhandenen Dienstkontos im Active Directory.

Für GovCloud-Konten geben Sie den AWS SSM Parameter-ARN-Wert für die Anmeldeinformationen im folgenden Format ein:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Der AWS SSM-Parametertyp muss „Secure String“ sein, mit dem Namen im Format `/netapp/wlmdb/<anyname>`. Weitere Informationen zum Abrufen von SSM-Parametern finden Sie unter ["AWS GovCloud-Dokumentation"](#).

8. Unter **Konnektivität** wird ein Schlüsselpaar ausgewählt, um eine sichere Verbindung zu Ihrer Instanz herzustellen.
9. Unter **Infrastruktureinstellungen** sind die folgenden Angaben erforderlich:
- a. **DB-Instanztyp:** Im Dropdown-Menü wird der Typ der Datenbankinstanz ausgewählt.
 - b. **FSx for ONTAP System:** Ein neues FSx for ONTAP Dateisystem erstellen oder ein vorhandenes FSx for ONTAP Dateisystem verwenden.
 - i. **Neues FSx for ONTAP erstellen:** Eingabe von Benutzername und Passwort.

Für GovCloud-Konten geben Sie den AWS SSM-Parameter-ARN-Wert für die FSx for ONTAP-Anmeldeinformationen im folgenden Format ein:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Der AWS SSM-Parametertyp muss „Secure String“ sein, mit dem Namen im Format `/netapp/wlmdb/<anyname>`. Weitere Informationen zum Abrufen von SSM-Parametern finden Sie unter ["AWS GovCloud-Dokumentation"](#).

Ein neues FSx for ONTAP Dateisystem kann die Installationszeit um 30 Minuten oder mehr verlängern.

- ii. **Vorhandenes FSx for ONTAP auswählen:** Im Dropdown-Menü werden der Name von FSx for ONTAP ausgewählt sowie ein Benutzername und ein Passwort für das Dateisystem eingegeben.

Für bestehende FSx for ONTAP Dateisysteme sind die folgenden Punkte zu beachten:

- Die an FSx for ONTAP angehängte Routing-Gruppe ermöglicht, Routen zu den Subnetzen für das Deployment zu verwenden.
 - Die Sicherheitsgruppe erlaubt Datenverkehr aus den für das Deployment verwendeten Subnetzen, insbesondere über die TCP-Ports HTTPS (443) und iSCSI (3260).
- c. **Snapshot-Richtlinie:** Standardmäßig aktiviert. Snapshots werden täglich erstellt und 7 Tage lang aufbewahrt.

Die Snapshots sind Volumes zugewiesen, die für PostgreSQL Workloads erstellt wurden.

- d. **Datenträgergröße:** Die Kapazität des Datenträgers und die Kapazitätseinheit angeben.
- e. **Provisionierte IOPS:** Zur Auswahl stehen **Automatisch** oder **vom Benutzer provisioniert**. Bei Auswahl von **vom Benutzer provisioniert** ist der IOPS-Wert anzugeben.
- f. **Durchsatzkapazität:** Die Durchsatzkapazität wird im Dropdown-Menü ausgewählt.

In bestimmten Regionen können Sie eine Durchsatzkapazität von 4 GB/s auswählen. Zum Provisionieren einer Durchsatzkapazität von 4 GB/s muss Ihr FSx for ONTAP Dateisystem mit einer SSD Storage Kapazität von mindestens 5.120 GiB und 160.000 SSD IOPS konfiguriert sein.

- g. **Verschlüsselung:** Wählen Sie einen Schlüssel aus Ihrem Konto oder aus einem anderen Konto. Sie müssen den ARN des Verschlüsselungsschlüssels aus einem anderen Konto eingeben.

Benutzerdefinierte Verschlüsselungsschlüssel für FSx for ONTAP werden basierend auf der Dienstkompatibilität nicht aufgeführt. Die Auswahl eines geeigneten FSx-Verschlüsselungsschlüssels ist erforderlich. Nicht-FSx-Verschlüsselungsschlüssel führen dazu, dass die Servererstellung fehlschlägt.

Die von AWS verwalteten Schlüssel werden anhand ihrer Anwendbarkeit für den jeweiligen Dienst gefiltert.

- h. **Tags:** Optional lassen sich bis zu 40 Tags hinzufügen.
- i. **Simple Notification Service:** Optional können Sie den Simple Notification Service (SNS) für diese Konfiguration aktivieren, indem Sie im Dropdown-Menü ein SNS-Thema für PostgreSQL auswählen.
 - i. Die Aktivierung des Simple Notification Service ist erforderlich.
 - ii. Die Auswahl einer ARN erfolgt über das Dropdown-Menü.
- j. **CloudWatch Überwachung:** Optional können Sie die CloudWatch Überwachung aktivieren.

Wir empfehlen, CloudWatch für die Fehlersuche im Fehlerfall zu aktivieren. Die Ereignisse, die in der AWS CloudFormation Konsole angezeigt werden, sind allgemein gehalten und geben nicht die eigentliche Ursache an. Alle detaillierten Protokolle werden im `C:\cfn\logs` Ordner in den EC2 Instanzen gespeichert.

In CloudWatch wird eine Protokollgruppe mit dem Namen des Stacks erstellt. Unter der Protokollgruppe wird für jeden Validierungsknoten und SQL-Knoten ein Protokollstream angezeigt. CloudWatch zeigt den Skriptfortschritt an und liefert Informationen, anhand derer Sie erkennen können, ob und wann ein Deployment fehlschlägt.

a. **Ressourcen-Rollback:** Für diese Funktion gibt es derzeit keine Unterstützung.

10. Zusammenfassung

a. **Geschätzte Kosten:** Enthält eine Schätzung der Kosten, die Ihnen entstehen könnten, wenn Sie die angezeigten Ressourcen einsetzen.

11. Mit **Erstellen** wird der neue Datenbankhost eingesetzt.

Alternativ können Sie die Konfiguration speichern.

Was kommt als Nächstes

Sie können Benutzer, Fernzugriff und Datenbanken auf dem eingesetzten PostgreSQL Server manuell konfigurieren.

Erstellen einer Microsoft SQL Datenbank in NetApp Workload Factory for Databases

Durch das Erstellen einer neuen Microsoft SQL Datenbank können Sie die Ressource in NetApp Workload Factory for Databases managen.

Über diese Aufgabe

Bei der Erstellung der Datenbank werden im FSx for ONTAP Dateisystem zwei neue Volumes erstellt, die aus unabhängigen LUNs bestehen und Daten- und Protokolldateien für die Datenbank hosten. Die Datenbankdateien in der neuen Datenbank sind thin-provisioniert und belegen nur wenige MB der der neuen Datenbank insgesamt zugewiesenen Größe.

Wenn Sie Storage für die Datenbank trennen möchten, können Sie dies mithilfe eines virtuellen Mountpunkts tun. Der virtuelle Mountpunkt ermöglicht es Ihnen, Datenbanken auf wenigen gemeinsamen Laufwerken auf dem Host zu konsolidieren.

Zum Erstellen einer Datenbank in workload factory sind die Berechtigungen *Anzeigen*, *Planen* und *Analysieren* erforderlich. Alternativ können Sie eine teilweise ausgefüllte Codevorlage kopieren oder herunterladen, um den Vorgang außerhalb von workload factory abzuschließen. ["Informationen zu den Berechtigungen von Workload Factory"](#), um zu entscheiden, welchen Modus Sie verwenden möchten.



Microsoft SQL Servers, die das SMB-Protokoll verwenden, unterstützen keine Datenbankerstellung.

Bevor Sie beginnen

Folgende Voraussetzungen sind zu erfüllen, bevor eine neue Datenbank erstellt wird.

- **Anmeldeinformationen und Berechtigungen:** Sie müssen ["AWS-Kontoanmeldeinformationen und Berechtigungen für Operationen und Behebungen"](#) besitzen, um eine neue Datenbank in Workload Factory zu erstellen.

Alternativ lässt sich die Codebox verwenden, um eine Vorlage zu kopieren, sodass Sie mithilfe der REST API eine Datenbank außerhalb von workload factory einsetzen können. ["Weitere Informationen zur Codebox Automatisierung"](#).

- **Windows-Host:** Sie müssen auf dem Microsoft SQL Server über genügend Laufwerksbuchstaben verfügen, um neue Laufwerke für die neue Datenbank zu erstellen, wenn Sie den Modus *Quick create* verwenden.
- **Microsoft SQL Server:** Voraussetzung ist ein verwalteter Microsoft SQL Server in workload factory for Databases zum Hosten der neuen Datenbank.
- **AWS Systems Manager:** Es muss sichergestellt sein, dass die NT Authority\SYSTEM Benutzerrechte im Microsoft SQL Host über AWS Systems Manager aktiviert sind.

Erstellen einer Datenbank

In Workload Factory kann diese Aufgabe mit den Deployment-Modi *Quick create* oder *Advanced create* abgeschlossen werden.

Schnellerstellung

Schritte

1. Melden Sie sich bei der "NetApp Console" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Im Menü Datenbanken wird **Inventar** ausgewählt.
4. Im Inventar wird **Microsoft SQL Server** als Typ der Datenbank-Engine ausgewählt.
5. Auswahl eines Datenbankservers mit einer verwalteten SQL server Instanz, in dem die Datenbank erstellt wird.
6. Anschließend erfolgt im Aktionsmenü der verwalteten Instanz die Auswahl von **Benutzerdatenbank erstellen**.
7. Auf der Seite „Benutzerdatenbank erstellen“ sind unter „Datenbankinformationen“ die folgenden Angaben zu machen:
 - a. **Datenbankname:** Namen für die Datenbank eingeben.
 - b. **Sortierung:** Auswahl einer Sortierung für die Datenbank. Die Standardsortierung "SQL_Latin1_General_CP1_CI_AS" auf Microsoft SQL Server ist ausgewählt.
8. Unter Dateieinstellungen sind die folgenden Angaben erforderlich:
 - a. **Dateieinstellungsmodus:** Auswahl von **Schnell erstellen**.
 - b. **Dateinamen & Pfad:**
 - **Name der Datendatei:** Name der Datendatei eingeben.
 - **Name der Protokolldatei:** Eingabe des Namens der Protokolldatei.
 - c. **Dateigrößen:** Eingabe der Datengröße und der Protokollgröße für die Datenbank.
9. Klicken Sie auf **Create**.

Alternativ können Sie, wenn Sie eine dieser Standardeinstellungen jetzt ändern möchten, den **Dateieinstellungsmodus** in **Erweiterte Erstellung** ändern.

Erweiterte Erstellung

Schritte

1. Melden Sie sich bei der "NetApp Console" an.
- 2.

Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.

3. Im Menü Datenbanken wird **Inventar** ausgewählt.
4. Im Inventar wird **Microsoft SQL Server** als Typ der Datenbank-Engine ausgewählt.
5. Auswahl eines Datenbankservers mit einer verwalteten SQL server Instanz, in dem die Datenbank erstellt wird.
6. Anschließend erfolgt im Aktionsmenü der verwalteten Instanz die Auswahl von **Benutzerdatenbank erstellen**.
7. Die Auswahl fällt auf **Create user database**.
8. Auf der Seite „Benutzerdatenbank erstellen“ sind unter „Datenbankinformationen“ die folgenden Angaben zu machen:
 - a. **Datenbankname**: Namen für die Datenbank eingeben.
 - b. **Sortierung**: Auswahl der Sortierung für die Datenbank. Die Standardsortierung "SQL_Latin1_General_CP1_CI_AS" auf Microsoft SQL Server ist ausgewählt.
9. Unter Dateieinstellungen sind die folgenden Angaben erforderlich:
 - a. **Modus für Dateieinstellungen**: **Advanced create** auswählen.
 - b. **Dateinamen & Pfad**:
 - i. **Datendatei**: Auswahl eines Laufwerksbuchstabens und Eingabe des Namens der Datendatei.

Optional kann das Kontrollkästchen für **Virtual mount point** aktiviert werden.
 - ii. **Protokolldatei**: Auswahl eines Laufwerksbuchstabens und Eingabe des Namens der Protokolldatei.

Optional kann das Kontrollkästchen für **Virtual mount point** aktiviert werden.
 - c. **Dateigrößen**: Eingabe der Datengröße und der Protokollgröße für die Datenbank.
10. Klicken Sie auf **Create**.

Wenn Sie den Datenbank-Host erstellt haben, können Sie den Fortschritt des Auftrags auf der Registerkarte **Job monitoring** überprüfen.

Erstellung eines Sandbox-Klons in NetApp Workload Factory for Databases

Das Erstellen eines Sandbox-Klons einer Datenbank in NetApp Workload Factory for Databases ermöglicht die Verwendung des Klons für Entwicklung, Tests, Integration, Analysen, Schulungen, Qualitätssicherung und mehr, ohne die Quelldatenbank zu verändern.

Über diese Aufgabe

Ein Sandbox-Klon wird aus dem aktuellsten Snapshot der Quelldatenbank erstellt. Er kann auf demselben Microsoft SQL Server wie die Quelldatenbank oder auf einem anderen Microsoft SQL Server geklont werden, sofern beide dasselbe FSx for ONTAP-Dateisystem verwenden.

Bevor Sie beginnen

Bevor Sie einen Sandbox-Klon erstellen, müssen Sie die folgenden Voraussetzungen erfüllen.

- **Anmeldeinformationen und Berechtigungen:** Es müssen "[AWS-Kontoanmeldeinformationen und Berechtigungen für Operationen und Behebungen](#)" vorhanden sein, um einen Sandbox-Klon in Workload Factory zu erstellen.

Alternativ können Sie die Codebox verwenden, um eine teilweise ausgefüllte Vorlage zu kopieren oder eine fertige Vorlage zu erstellen, sodass Sie den Sandbox-Klon außerhalb der Workload Factory mithilfe der REST-API erstellen können "[Weitere Informationen zur Codebox Automatisierung](#)".

- **Microsoft SQL Server:** Sie benötigen einen verwalteten Microsoft SQL Server in Workload Factory for Databases zum Hosten des neuen Sandbox-Klons.
- **AWS Systems Manager:** Es muss sichergestellt sein, dass die NT Authority\SYSTEM Benutzerrechte im Microsoft SQL Host über AWS Systems Manager aktiviert sind.
- **Quelldatenbank:** Sie benötigen eine für den Klon verfügbare Quelldatenbank.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Unter Databases die Registerkarte **Sandboxes** auswählen.
4. Im Reiter „Sandboxes“ ist **Neue Sandbox erstellen** auszuwählen.
5. Auf der Seite „Neue Sandbox erstellen“ sind unter „Datenbankquelle“ folgende Angaben erforderlich:
 - a. **Quelldatenbank-Host:** Auswahl des Quelldatenbank-Hosts.
 - b. **Quell-Datenbankinstanz:** Auswahl der Quell-Datenbankinstanz.
 - c. **Quelldatenbank:** Auswahl der Datenbank, die geklont werden soll.
6. Unter „Datenbankziel“ sind folgende Angaben erforderlich:
 - a. **Ziel-Datenbankhost:** Der für den Sandbox-Klon ausgewählte Zieldatenbankhost befindet sich in derselben VPC und weist dasselbe FSx for ONTAP Dateisystem wie der Quellhost auf.
 - b. **Zieldatenbankinstanz:** Auswahl der Zieldatenbankinstanz für den Sandbox-Klon.
 - c. **Zieldatenbank:** Eingabe eines Namens für den Sandbox-Klon.
7. **Einbinden:** Beim Klonen einer SQL-Datenbank mit mehreren Daten- und/oder Protokolldateien kloniert Workload Factory alle Dateien unter dem automatisch zugewiesenen oder definierten Laufwerksbuchstaben.

Wählen Sie eine der folgenden Optionen:

- a. **Automatische Montagepunktzuweisung**
- b. **Definition des Mountpunktpfads**

Zum Definieren des Mountpunktpfads sind die folgenden Angaben erforderlich:

- Eingabe des Laufwerksbuchstabens für den Datendateipfad.
- Der Laufwerksbuchstabe für den Pfad der Protokolldatei ist anzugeben.

8. **Tag definieren:** Auswahl eines Tags zur Definition des Sandbox-Klons.
9. Klicken Sie auf **Create**.

Zum Überprüfen des Fortschritts des Auftrags dient die Registerkarte **Auftragsüberwachung**.

Ressourcen verwalten

Ressourcenmanagement in NetApp Workload Factory für Datenbanken

Die Verwaltung von Ressourcen in NetApp Workload Factory for Databases ermöglicht die Nutzung erweiterter Funktionen, darunter die Erstellung von Datenbanken und Klonen, Ressourcenauslastung und Überwachung. Darüber hinaus können Sie den Well-Architected-Status Ihrer Datenbankkonfigurationen analysieren und Best Practices für die Konfiguration implementieren, um die Performance zu verbessern und die Betriebskosten zu senken. Die Ressourcenverwaltung ist nur für Microsoft SQL Server- und Oracle-Umgebungen vorgesehen, die auf FSx for ONTAP file system storage ausgeführt werden.

Sie müssen ["Ressourcen registrieren"](#), um eine der folgenden Managementaufgaben auszuführen.

Zu den Managementaufgaben gehören:

- Anzeigen von Datenbanken im Inventar
- ["Erstellen einer Datenbank"](#)
- ["Erstellen eines Datenbankklons \(Sandbox\)"](#)
- ["Implementierung gut strukturierter Datenbankkonfigurationen"](#)

Ressourcen in NetApp Workload Factory für Datenbanken registrieren

Instanzen für Microsoft SQL Server und Datenbanken für Oracle registrieren, sodass Ressourcen verwaltet, Datenbanken und Sandbox-Klone erstellt, Fehlerprotokollanalysen durchgeführt und Konfigurationen in NetApp Workload Factory for Databases optimiert werden können.

Sie können Ihre Ressourcen nur registrieren, wenn sie auf FSx für ONTAP Dateisystemspeicher laufen.

Zur Aufgabe

Die Registrierung einer Instanz (SQL Server) oder Datenbank (Oracle) umfasst zwei Schritte: Instanz- oder Datenbank-Authentifizierung und Vorbereitung. Authentifizierung ist der Prozess der Überprüfung der Anmeldeinformationen für die Instanz oder Datenbank. Die Vorbereitung umfasst die Installation von AWS-, NetApp- und PowerShell-Modulen auf der Instanz oder Datenbank, um die Mindestanforderungen für Workload Factory for Databases-Funktionen wie ["Erstellen einer Datenbank"](#), ["Erstellen einer Sandbox"](#), ["Fehlerprotokollanalyse"](#) oder ["die Well-Architected Bewertung"](#) zu erfüllen.

Workload Factory unterstützt nur die Registrierung und Verwaltung von Microsoft SQL Server-Instanzen und Oracle-Datenbanken. Abhängig von den in Workload Factory ausgewählten AWS-Kontodaten werden PostgreSQL-Hosts im Inventar angezeigt. Derzeit unterstützt Workload Factory nicht registrierte PostgreSQL-Instanzen, die nur auf Amazon Linux-Betriebssystemen ausgeführt werden.

Bevor Sie beginnen

Folgendes ist erforderlich, bevor Sie eine Instanz oder Datenbank registrieren:

- Stellen Sie sicher, dass die Hosts der Ressourcen, die Sie registrieren möchten, im Inventar angezeigt werden. ["Berechtigungen für Operationen und Remediation gewähren"](#) in Ihrem AWS-Konto.

- Stellen Sie eine Verknüpfung mit dem FSx for ONTAP Dateisystem her, das die Ressourcen hostet, die Sie registrieren möchten. ["Informationen dazu, wie ein bestehender Link verknüpft oder ein neuer Link erstellt und verknüpft werden kann."](#) Nach der Verknüpfung kann zu diesem Vorgang zurückgekehrt werden.

Registrieren einer Instanz in einem privaten Netzwerk

Um eine Instanz oder Datenbank in einem privaten Netzwerk ohne externe Verbindung zu registrieren, stellen Sie die erforderlichen Endpunkte in der VPC bereit und ordnen Sie sie den entsprechenden Subnetzen zu. Erlauben Sie Port 443 in der Security Group für Interface-Endpunkte.

- `s3 Gateway/endpoint`
- `ssm`
- `ssmmessages`
- `fsx`

Wenn Sie einen Proxyserver für ausgehende EC2-Verbindungen verwenden, erlauben Sie den Zugriff auf diese Domains für Managementvorgänge:

- `.microsoft.com` (SQL Server)
- `.powershellgallery.com` (SQL Server)
- `.aws.amazon.com`
- `.amazonaws.com`

Registrieren einer Microsoft SQL Server-Instanz

Die Registrierung einer Instanz umfasst zwei Schritte: Authentifizierung und Vorbereitung. Es ist möglich, eine einzelne Instanz oder mehrere Instanzen zu registrieren.

Workload Factory unterstützt die Registrierung für Failover Cluster Instance (FCI) und Standalone-Bereitstellung für SQL Server.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Im Menü Datenbanken wird **Inventar** ausgewählt.
4. Im Inventar ist **Microsoft SQL Server** als Engine-Typ auszuwählen.
5. Auswahl der Registerkarte **Instanzen**.
6. Hier wird ausgewählt, ob eine einzelne Instanz oder mehrere Instanzen registriert werden sollen.
7. Um Instanzen zu authentifizieren (Schritt 1), führen Sie die folgenden Schritte aus und wählen Sie dann **Weiter**:
 - a. Wählen Sie **Die gleichen Anmeldeinformationen für alle Instanzen verwenden** oder **Anmeldeinformationen manuell verwalten** aus.
 - b. Authentifizieren Sie SQL Server und Windows, indem Sie Benutzername und Passwort angeben.

Wenn die Instanzen authentifiziert sind, wählen Sie **Weiter**.

8. Zur Vorbereitung (Schritt 2) stellen Sie sicher, dass die Instanz(en) die Mindestanforderungen erfüllen.

Um die Mindestanforderungen zu erfüllen, müssen auf der Instanz die AWS- und NetApp PowerShell-Module sowie die PowerShell 7-Module installiert sein, und Sie müssen die Voraussetzungen für mindestens eine der unter „Voraussetzungsprüfung“ aufgeführten Funktionen erfüllen.

- a. Überprüfen Sie die Voraussetzungen in der **Prerequisite check view**.

Sie müssen alle Voraussetzungen für eine einzelne Fähigkeit wie **Review well-architected issues and recommendations** erfüllen, um die Instanz zu registrieren.

- b. Wählen Sie für jede Funktion **Setup details** aus, um mehr über die Voraussetzungen der jeweiligen Funktion zu erfahren, und folgen Sie den Anweisungen auf dem Bildschirm, um etwaige fehlende Voraussetzungen für eine Funktion zu erfüllen.

Um Workload Factory zu "[Gut konzipierte Probleme überprüfen und beheben](#)" aktivieren, erfüllen Sie alle Voraussetzungen unter **Überprüfung von gut strukturierten Problemen und Empfehlungen** und **Behebung von gut strukturierten Problemen**.

9. Nachdem Sie alle Voraussetzungen erfüllt haben, **Register** Sie die Instanz(en).

Ergebnis

Die Instanzregistrierung wird gestartet. Wählen Sie die Registerkarte **Job monitoring**, um den Fortschritt zu verfolgen.

Registrierung einer Oracle Datenbank

Die Registrierung einer Instanz umfasst zwei Schritte: Datenbank Authentifizierung und Vorbereitung. Es ist möglich, eine einzelne Instanz oder mehrere Datenbanken zu registrieren.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Die Auswahl erfolgt im Menü  **Workloads > Datenbanken**.
3. Im Menü Datenbanken wird **Inventar** ausgewählt.
4. Wählen Sie im Inventory **Oracle** als Engine-Typ aus.
5. Auszuwählen ist die Registerkarte **Datenbanken**.
6. Zur Registrierung stehen eine einzelne Datenbank oder mehrere Datenbanken zur Auswahl.
7. Um Datenbanken zu authentifizieren (Schritt 1), gehen Sie wie folgt vor und wählen Sie dann **Weiter**:
 - a. Wählen Sie **Die gleichen Anmeldeinformationen für alle Instanzen verwenden** oder **Anmeldeinformationen manuell verwalten** aus.
 - b. Authentifizieren Sie den Oracle-Benutzer und den Automatic Storage Management (ASM) Grid-Benutzer (falls zutreffend), indem Sie Benutzernamen und Passwörter angeben.

Wenn die Datenbanken authentifiziert sind, wählen Sie **Next**.

8. Zur Vorbereitung (Schritt 2) stellen Sie sicher, dass die Datenbank(en) die erforderlichen Voraussetzungen erfüllen. Sind alle erforderlichen Module installiert und die Voraussetzungen erfüllt, wählen Sie **Weiter**, um die Datenbank zu registrieren. Andernfalls folgen Sie diesen Schritten.
 - a. Überprüfen Sie die Voraussetzungen in der **Prerequisite check view**.

Sie müssen alle Voraussetzungen für eine einzelne Funktion wie **Review well-architected issues and recommendations** erfüllen, um die Datenbank zu registrieren.

- b. Wählen Sie für jede Funktion **Setup details** aus, um mehr über die Voraussetzungen der jeweiligen Funktion zu erfahren, und folgen Sie den Anweisungen auf dem Bildschirm, um etwaige fehlende Voraussetzungen für eine Funktion zu erfüllen.

Um Workload Factory "[Gut konzipierte Probleme überprüfen und beheben](#)" für Ihre Datenbanken nutzen zu können, müssen Sie alle Voraussetzungen erfüllen, die unter **Überprüfung von Problemen und Empfehlungen in der Architektur** und **Behebung von Problemen in der Architektur** aufgeführt sind.

9. Nachdem Sie die Voraussetzungen erfüllt haben, **Register** Sie die Datenbank(en).

Ergebnis

Die Datenbankregistrierung wird gestartet. Wählen Sie die Registerkarte **Job monitoring**, um den Fortschritt zu verfolgen.

Was kommt als Nächstes

Nach der Registrierung können Sie diese Aufgaben ausführen.

- Datenbanken aus dem Inventar anzeigen
- "[Erstellen einer Datenbank](#)"
- "[Erstellung eines Datenbankklons \(Sandbox\)](#)"
- "[Umfassende, gut durchdachte Bewertung von Datenbankkonfigurationen](#)"

Datenbank-Klone in der NetApp Workload Factory für Datenbanken verwalten

Sandbox-Klone lassen sich in der NetApp Workload Factory for Databases verwalten, sodass Entwicklungs- und Testumgebungen zuverlässig und kostengünstig bleiben. Die Integrität der Daten eines Klons kann überprüft, ein Klon mit der CI/CD-Pipeline verbunden werden, um die Softwarebereitstellung zu automatisieren, oder ein Klon kann aktualisiert, zurückgesetzt oder aufgeteilt werden, um ihn an aktuelle Entwicklungsanforderungen anzupassen. Wird ein Klon nicht mehr benötigt, kann er gelöscht werden, um Speicherplatz freizugeben.

Integrität der Sandbox-Daten überprüfen

Mit einer Integritätsprüfung lässt sich feststellen, ob die Sandbox-Klondaten in NetApp Workload Factory for Databases intakt oder beschädigt sind.

Über diese Aufgabe

Wenn Sie einen Sandbox-Klon aus einer ausgelasteten Quelldatenbank erstellen, sind die Daten des Klons möglicherweise nicht mit dem aktuellsten Snapshot der Quelldatenbank synchronisiert. Dieser Vorgang prüft die Integrität aller Objekte im Sandbox-Klon, um festzustellen, ob die Daten des Sandbox-Klons aktuell sind.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.

3. Im Menü „Datenbanken“ erfolgt die Auswahl von **Sandboxes**.
4. Wählen Sie in Sandboxes das Aktionsmenü des Sandbox-Klons aus, dessen Integrität überprüft werden soll.
5. Die Option **Integritätsprüfung ausführen** auswählen.
6. Im Dialogfeld „Integritätsprüfung“ ist **Integritätsprüfung** auszuwählen.
7. Der Status der Integritätsprüfung ist in Sandboxes oder in der Jobüberwachung ersichtlich.

Falls die Integritätsprüfung fehlschlägt, empfehlen wir Ihnen, den Sandbox-Klon nicht zu verwenden und einen neuen Sandbox-Klon zu erstellen.

Einen Sandbox-Klon mit CI/CD verbinden

Die Verbindung eines Sandbox-Klons mit einer Continuous Integration- und Continuous Delivery (CI/CD)-Pipeline über REST API-Code verbessert die Software-Delivery durch Automatisierung in NetApp Workload Factory for Databases.

Über diese Aufgabe

Für die automatische Bereitstellung einer neuen Softwareversion für Ihren Datenbankklon ist eine Verbindung mit einer CI/CD-Pipeline erforderlich. Für die Herstellung dieser Verbindung kann der in diesem Vorgang bereitgestellte REST API Code verwendet werden.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Im Menü „Datenbanken“ erfolgt die Auswahl von **Sandboxes**.
4. In Sandboxes erfolgt die Verbindung mit CI/CD-Tools über das Aktionsmenü des Sandbox-Klons.
5. **Connect to CI/CD tools** auswählen.
6. Im CI/CD-Dialog können Sie den REST API-Code kopieren oder herunterladen, der für die Verbindung mit den CI/CD-Tools benötigt wird.
7. Klicken Sie auf **Schließen**.

Löschen eines Datenbankklons

Wenn ein Sandbox-Klon in NetApp Workload Factory for Databases nicht mehr benötigt wird und Storage-Kapazität freigegeben werden soll, kann er gelöscht werden.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Im Menü „Datenbanken“ erfolgt die Auswahl von **Sandboxes**.
4. In Sandboxes erfolgt die Auswahl des Aktionsmenüs des Sandbox-Klons, den Sie löschen möchten.
5. Wählen Sie **Delete**.
6. Im Dialogfeld „Löschen“ dient die Auswahl von **Löschen** zur Bestätigung des Löschvorgangs.

Aktualisieren eines Datenbankklons

Ein Datenbank-(Sandbox)-Klon in NetApp Workload Factory for Databases kann so aktualisiert werden, dass er der Quelldatenbank zum aktuellen oder zu einem früheren Zeitpunkt entspricht.

Über diese Aufgabe

Beim Aktualisieren eines Klons wird der Klon entweder auf den aktuellen Stand der Quelldatenbank oder auf einen Snapshot der Quelldatenbank aktualisiert, der zu einem früheren Zeitpunkt erstellt wurde. Alle am Sandbox Klon vorgenommenen Änderungen werden gelöscht.

Bevor Sie beginnen

Eine Aktualisierung ist nur möglich, wenn die Quelldatenbank aktiv ist.

Zum Aktualisieren eines Datenbankklons aus einem Snapshot muss die Quelldatenbank für den Vorgang über mindestens einen Snapshot verfügen.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Im Menü „Datenbanken“ erfolgt die Auswahl von **Sandboxes**.
4. In Sandboxes erfolgt die Auswahl des Aktionsmenüs des Sandbox-Klons, den Sie aktualisieren möchten.
5. Wählen Sie **Aktualisieren**.
6. Im Dialogfeld „Aktualisieren“ kann eine der folgenden Optionen ausgewählt werden:
 - a. **Auf aktuelle Uhrzeit aktualisieren**
 - b. **Aktualisierung zu einem Zeitpunkt**

Für diese Option erfolgt die Auswahl des Datenbank-Snapshots, auf den aktualisiert werden soll, im Dropdown-Menü.

7. Klicken Sie auf **Aktualisieren**.

Einen Datenbankklon zurücksetzen

Einen Datenbank-(Sandbox)-Klon in NetApp Workload Factory for Databases auf seine ursprüngliche Version zum Zeitpunkt der Erstellung zurücksetzen.

Beim Klonen einer Datenbank wird bei der Erstellung zunächst ein *Baseline*-Klon erstellt. Die Daten in der geklonten Datenbank entsprechen zum Zeitpunkt der Erstellung den Daten der Quelldatenbank. Da sich die Daten in einem Datenbankklon im Laufe der Zeit ändern, kann es sinnvoll sein, die Daten auf die Baseline zurückzusetzen, die bei der ersten Erstellung des Klons bestand. Dieser Vorgang wird als Zurücksetzen eines Klons auf die Baseline bezeichnet. Das Zurücksetzen eines Klons auf die Baseline statt das Erstellen eines neuen Klons spart Speicherplatz; dabei werden jedoch alle am Datenbankklon vorgenommenen Änderungen gelöscht.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Im Menü „Datenbanken“ erfolgt die Auswahl von **Sandboxes**.

4. In Sandboxes erfolgt die Auswahl des Aktionsmenüs des Datenbankklons, der zurückgesetzt werden soll.
5. **Re-baseline** auswählen.
6. Im Dialogfeld **Re-baseline** erfolgt die Auswahl von **Re-baseline**.

Aufteilen eines Datenbankklons

In NetApp Workload Factory for Databases wird durch das Trennen eines Datenbankklons von seiner Quelldatenbank eine neue Datenbank erstellt, die eine bestimmte Menge an Storage-Kapazität belegt. Nach Abschluss der Trennung wird der Klon gelöscht, und die neue Datenbank erscheint im Inventory.

Bevor Sie beginnen

Zu berücksichtigen ist, wie viel Storage-Kapazität für die neue Datenbank erforderlich ist. Falls erforderlich, ["Erhöhung der Dateisystemkapazität"](#) für das FSx for ONTAP file system, bevor Sie beginnen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Im Menü „Datenbanken“ erfolgt die Auswahl von **Sandboxes**.
4. In Sandboxes kann das Aktionsmenü des Datenbankklons ausgewählt werden, der getrennt werden soll.
5. **Split** auswählen.
6. Im Dialogfeld „Teilen“ ist die Option **Teilen** auszuwählen.

Verbindungsinformationen eines Klons anzeigen

Die Verbindungsinformationen eines Datenbankklons in NetApp Workload Factory for Databases anzeigen und kopieren.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Im Menü „Datenbanken“ erfolgt die Auswahl von **Sandboxes**.
4. In Sandboxes können Sie im Aktionsmenü des Sandbox-Klons dessen Verbindungsinformationen anzeigen.
5. Die Option **Verbindungsinformationen anzeigen** auswählen.
6. Im Dialogfeld „Verbindungsinformationen anzeigen“ können Sie die Verbindungsinformationen bei Bedarf kopieren.
7. **Schließen** auswählen.

Eine Ressource in NetApp Workload Factory für Datenbanken abmelden

Sie können eine Ressource, z. B. eine Microsoft SQL Server Instanz oder eine Oracle Datenbank, abmelden, wenn Sie über die NetApp Workload Factory Konsole keine Ressourcen mehr einsetzen oder überwachen möchten. Das Abmelden von Ressourcen entfernt auch die von der Instanz genutzte Storage-Kapazität von FSx for ONTAP.

Sie können die Ressource erneut registrieren.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Im Menü Datenbanken wird **Inventar** ausgewählt.
4. Im Inventar erfolgt die Auswahl des Engine-Typs: **Microsoft SQL Server**, **Oracle** oder **PostgreSQL**.
5. Die Ressource, die abgemeldet werden soll, ist zu suchen, das Aktionsmenü auszuwählen und anschließend **Abmelden** zu wählen.

Datenbankressourcen schützen, überwachen und optimieren

Fehlerprotokolle in der NetApp Workload Factory für Datenbanken analysieren

Mit dem intelligenten Fehlerprotokollanalysator lassen sich Fehlerprotokolle von Microsoft SQL Server und Oracle Datenbanken automatisch interpretieren, sodass Probleme schnell identifiziert und behoben werden können. Die Agentic AI-basierte Analyse erfordert eine Integration mit Amazon Bedrock.

Über diese Aufgabe

Die Analyse und Behebung von Fehlerprotokollen tragen zur Aufrechterhaltung von Systemstatus und Performance von SQL Server Instanzen und Oracle Datenbanken bei. Die effektive Interpretation von Fehlerprotokollen erfordert sorgfältige Analyse und Fachkenntnisse. Manuelle Überwachung, Fehlererkennung und Ursachenanalyse sind zeitaufwendig und fehleranfällig. Diese Herausforderungen können die Problemlösung verzögern, Ausfallzeiten verlängern und zu betrieblichen Ineffizienzen führen. Der intelligente Fehlerprotokollanalysator begegnet diesen Herausforderungen mit folgenden wesentlichen Vorteilen:

- Intelligente Gruppierung: Fehler werden intelligent nach Einzigartigkeit, Schweregrad und Kategorie konsolidiert, wodurch der Prozess der Fehlerbehebung vereinfacht und schnellere, effektivere Lösungen ermöglicht werden.
- KI-gestützte Untersuchung: KI analysiert Fehler proaktiv und liefert klare, umsetzbare Erkenntnisse, die die Problemidentifizierung beschleunigen, ohne tiefgreifende Fachkenntnisse zu erfordern.
- Fehleranreicherung: Ergänzt Fehlerprotokolle um externe Verweise und bietet so kontextbezogene Klarheit, um das Verständnis und die Entscheidungsfindung zu verbessern.
- Bewährte Verfahren zur Fehlerbehebung: Bietet maßgeschneiderte Empfehlungen zur Behebung von Problemen bei SQL Server-Workloads, die auf FSx for ONTAP ausgeführt werden, und ermöglicht es Benutzern aller Erfahrungsstufen, Probleme sicher zu lösen.

Wenn Sie den Fehlerprotokollanalysator verwenden, behalten Sie die volle Kontrolle über Ihre Umgebung und profitieren gleichzeitig von fortschrittlicher KI-Analyse.

Um den Fehlerprotokollanalysator zu verwenden, müssen Sie Amazon Bedrock aktivieren, das von Workload Factory verwendete Modell auswählen, einen privaten Endpunkt zur Verbindung mit Amazon Bedrock erstellen, Berechtigungen hinzufügen und eine Unternehmenslizenz erstellen.

["Preise für Amazon Bedrock"](#)



Wenn Ihr Kontoadministrator die KI-Funktionen deaktiviert hat, wird eine Meldung angezeigt und

die KI-Analyse kann nicht genutzt werden. Die Kontaktaufnahme erfolgt über Ihren Administrator oder ["Informationen zur KI-Administration"](#).

Datenschutz und Datensicherheit

Diese Funktion gewährleistet Datenschutz und Datensicherheit durch folgende Maßnahmen:

Datenhoheit

Protokolldaten und Aggregationen verbleiben innerhalb Ihres AWS-Kontos und werden über einen privaten VPC-Endpoint (Amazon Bedrock) übertragen, wodurch eine Offenlegung im öffentlichen Internet ausgeschlossen ist.

Kein KI-Training

Kundendaten werden nicht zum Trainieren oder Verbessern von Modellen verwendet. Amazon Bedrock verarbeitet Protokolle in Echtzeit, trainiert aber nicht mit Ihren Daten. Die Ergebnisse werden nur zu Referenzzwecken in Ihrer Umgebung gespeichert. Weitere Details enthält die ["Amazon Bedrock Datenschutzdokumentation"](#).

Bevor Sie beginnen

Um den Fehlerprotokollanalysator verwenden zu können, müssen Sie folgende Voraussetzungen erfüllen:

- Sie müssen ["Berechtigungen für Ansicht, Planung und Analyse erteilen"](#) in Ihrem AWS-Konto, um einen neuen Datenbank-Host in Workload Factory zu erstellen.
- ["Registrierung von Ressourcen"](#) in Workload Factory.
- Folgende Voraussetzungen müssen ebenfalls erfüllt sein. Im Rahmen der Schritte zur Analyse von Protokollfehlern werden Sie aufgefordert, diese Voraussetzungen zu erfüllen.

- **Amazon Bedrock Aktivierung**

Amazon Bedrock ist erforderlich, damit der auf dem SQL Server- oder Oracle-Host von Workload Factory ausgeführte KI-Agent eine nahtlose Verbindung zu Bedrock herstellen und KI-basierte Erkenntnisse für die identifizierten Fehlerprotokolle abrufen kann.

- **Netzwerk**

Der Amazon Bedrock VPC endpoint gewährleistet die private Kommunikation Ihres SQL Server- oder Oracle-Hosts mit den Amazon Bedrock APIs und verhindert die Erreichbarkeit über das öffentliche Internet. Der Amazon Bedrock VPC endpoint muss dem Subnetz des SQL Server- oder Oracle-Hosts zugeordnet sein (Beispiel: vpce-050cb2f33a1380ffd).

- **AWS IAM Berechtigungen**

Für die EC2-Instanzprofilrolle, die dem SQL Server- oder Oracle-Host zugeordnet ist, und für die AWS-Anmeldeinformationen, die mit Workload Factory verknüpft sind, sind die folgenden Berechtigungen erforderlich.

- EC2-Instanzprofilrolle mit der Berechtigung "bedrock:InvokeModel"

Diese Berechtigung ermöglicht es der EC2-Instanz auf dem entsprechenden SQL Server oder Oracle Host, Bedrock Modelle für die proaktive Fehleranalyse und Hinweise zur Fehlerbehebung aufzurufen. Dieses Profil gewährleistet zudem einen sicheren KI-Zugriff für maßgeschneiderte Erkenntnisse.

- AWS-Anmeldeinformationen, die mit Workload Factory verknüpft sind: Berechtigungen "bedrock:GetFoundationModelAvailability" und "bedrock:ListInferenceProfiles"

Diese Berechtigungen überprüfen die Verfügbarkeit und Konfiguration des Modells in der Region des SQL Server oder Oracle Hosts und gewährleisten eine zuverlässige, regionsspezifische Performance.

◦ Oracle Benutzerberechtigung

Die folgende Berechtigung gewährt Lesezugriff auf erweiterte Diagnosewarnungen und ermöglicht so die Extraktion von Fehler-/Trace-Details aus Protokollen zur KI-gestützten Mustererkennung und -behebung: `V$DIAG_ALERT_EXT`. Diese Berechtigung ist nur für Oracle Datenbanken erforderlich.

Fehlerprotokolle analysieren

Mit der Workload Factory console lassen sich SQL Server-Fehlerprotokolle analysieren.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Im Menü Datenbanken wird **Inventar** ausgewählt.
4. Im Inventar erfolgt die Auswahl von **Microsoft SQL Server** oder **Oracle** als Typ der Datenbank-Engine.
5. Auf der Registerkarte „Instanzen“ können Sie die spezifische SQL Server Instanz oder Oracle Datenbank, die Sie analysieren möchten, suchen und dann im Menü **Fehler untersuchen** auswählen.
6. Auf der Registerkarte **Fehleruntersuchung** sind die folgenden Voraussetzungen wie in der Konsole beschrieben zu erfüllen:
 - Amazon Bedrock
 - Netzwerk: Privater Endpunkt für Amazon Bedrock
 - Berechtigungen für die EC2-Instanzprofilrolle
 - Anmeldeinformationen im Zusammenhang mit Workload Database Management (wlmdb)
7. Wenn die Voraussetzungen erfüllt sind, steht mit **Investigate now** der Fehlerprotokollanalysator zur Verfügung, um Einblicke in Ihre SQL Server-Fehlerprotokolle zu gewinnen.

Nach dem Scan zeigt die Konsole Fehler an und bietet damit einen umfassenden Überblick über die vom Smart Fehlerprotokollanalysator erkannten Probleme.

8. Mit Filtern können Sie die angezeigten Fehler anhand von Kriterien wie Schweregrad, Zeitrahmen und Fehlercode oder anhand infrastrukturorientierter Tags wie Compute, Storage, Netzwerk und Sicherheit eingrenzen.
9. Eine Überprüfung der detaillierten Fehlerinformationen, einschließlich der ursprünglichen Fehlermeldung, der KI-basierten Erklärung und der vorgeschlagenen Schritte zur Behebung der Fehler, ist möglich.

Bewährte Konfigurationsmethoden implementieren

Informationen zur Konfigurationsanalyse in NetApp Workload Factory für Datenbanken

Workload Factory for Databases analysiert regelmäßig Datenbankkonfigurationen, um festzustellen, ob Probleme mit Microsoft SQL Server und Oracle Bereitstellungen auf

Amazon FSx for NetApp ONTAP Storage vorliegen. Wenn Probleme gefunden werden, zeigt Workload Factory an, worin diese bestehen, und erläutert, welche Änderungen erforderlich sind, damit Ihre Datenbankkonfigurationen optimale Leistung, Kosteneffizienz und die Einhaltung bewährter Verfahren erreichen.

Workload Factory bietet Best Practices und Empfehlungen für gut strukturierte Datenbank-Workloads. Die Analyse der optimalen Architektur bewertet Konfigurationen und Einstellungen von Microsoft SQL Server und Oracle Database in Bezug auf Speicher, Rechenleistung, Anwendung, Ausfallsicherheit und Klonen.

So funktioniert es

Workload Factory analysiert täglich Ihre Workloads, die auf unterstützten Cloud-Speichersystem-Bereitstellungen ausgeführt werden. Die Analyse liefert den Status einer Well-Architected-Architektur, Erkenntnisse und Empfehlungen.

Nach Abschluss der täglichen Analyse werden die Konfigurationen im Well-architected Dashboard für die Bereitstellung als „optimiert“ oder „nicht optimiert“ angezeigt. Konfigurationsprobleme sind nach Kategorie sowie in einer Liste mit Problemen und Empfehlungen zu finden. Empfehlungen zu den Konfigurationsproblemen können überprüft werden. Einige Probleme können automatisch von Workload Factory behoben werden, während andere manuelle Eingriffe erfordern. In diesem Fall stellt Workload Factory detaillierte Anweisungen bereit, um die empfohlenen Änderungen umzusetzen.

Sie können die Analyse von Konfigurationen, die für Ihre Umgebungen nicht relevant sind, ausblenden. Dadurch werden unnötige Warnmeldungen und ungenaue Optimierungsergebnisse vermieden.

Es besteht auch die Möglichkeit, benutzerdefinierte Regeln in einfacher Sprache zu erstellen, um Ihre Umgebungen anhand der Standards Ihres Unternehmens und der NetApp Best Practices zu validieren. Regeln können mit einem Probelauf getestet und anschließend für die Ausführung in Ihren Umgebungen terminiert werden. "[Weitere Informationen zu benutzerdefinierten Regeln](#)".

Warum es wichtig ist

Workload Factory wendet Best Practices auf große Storage-, Datenbank- und VMware-Umgebungen an, indem kontinuierliche Bewertungen mit Empfehlungseinblicken und Fehlerbehebungen kombiniert werden. Automatisierte Korrekturen in der NetApp Console reduzieren menschliche Fehler, gewährleisten einheitliches Management und erhalten Leistung und Zuverlässigkeit über Ihre Workload-Infrastrukturen hinweg.

Optionen zur Analyse Ihrer Datenbankumgebung

Workload Factory bietet folgende Optionen zur Analyse Ihrer Datenbankumgebung:

- **Einmalige Bewertung:** Führen Sie eine "[einmalige Bewertung](#)" Bewertung durch, um den Status Ihrer gut strukturierten Microsoft SQL Server-Instanzen oder Oracle-Datenbanken zu ermitteln, ohne Anmeldeinformationen zu speichern oder Ressourcen zu registrieren.

Für die einmalige Bewertung sind die Anmeldeinformationen für die Microsoft SQL Server Instanzen oder Oracle Datenbanken, die analysiert werden sollen, nur einmal bereitzustellen.

- **Kontinuierliche Bewertung:** Workload Factory analysiert Ihre Datenbankumgebung regelmäßig, gibt fortlaufend Empfehlungen zur Optimierung Ihrer Konfigurationen und behebt Probleme automatisch.

Für die kontinuierliche Bewertung ist es erforderlich, Ihre Ressourcen zu registrieren, einen Link zuzuordnen und Berechtigungen in Ihrem AWS-Konto zu erteilen.

Best Practices für Microsoft SQL Server

Die folgenden Best Practices und Empfehlungen gelten für Microsoft SQL Server Workloads.

Storage

Speicherebene

Die primäre SSD-Ebene eignet sich für leistungskritische SQL-Workloads.

▼ Details

Für optimale Leistung sollte die primäre SSD-Ebene für FSx for ONTAP Volumes verwendet werden. Die Kapazitätspool-Ebene kann die Leistung verringern und die Latenz erhöhen. Die primäre SSD-Ebene ist für Hochleistungs-Workloads ausgelegt, während die Kapazitätspool-Ebene auf Kosteneffizienz optimiert ist und möglicherweise nicht die Leistungsanforderungen von SQL Server Workloads erfüllt.

Dateisystem-Spielraum

Es sollte ausreichend freie Kapazität oberhalb der Gesamtvolumengröße vorhanden sein.

▼ Details

Es sollte ausreichend Dateisystemkapazität über der Gesamtgröße Ihres Volumes vorhanden sein. Zu wenig freier Speicherplatz verursacht Leistungsprobleme, zu viel verschwendet Speicher und erhöht die Kosten.

Log-Laufwerkgröße

Protokolllaufwerke dimensionieren und überwachen, um Rollbacks und Ausfälle zu vermeiden.

▼ Details

Die Größe und Überwachung des SQL Server-Protokolllaufwerks verhindert Transaktions-Rollbacks, Datenbanknichtverfügbarkeit, Datenbeschädigung und Leistungsprobleme, die durch ein volles Protokolllaufwerk verursacht werden.

Größe des TempDB-Laufwerks

TempDB so dimensionieren, dass Engpässe und Zeitüberschreitungen vermieden werden.

▼ Details

Die TempDB sollte dimensioniert und überwacht werden, um Leistung und Stabilität aufrechtzuerhalten. Zu wenig Speicherplatz in der TempDB kann zu verlangsamten Abfragen, Anwendungstimeouts und Systemabstürzen führen.

Platzierung von Daten- und Protokolldateien

Separate .mdf und .ldf Pfade.

▼ Details

Daten- und Protokolldateien sollten auf unterschiedlichen Laufwerken gespeichert werden, um die parallele E/A, die Flexibilität beim Backup und das Wiederherstellungsverhalten zu verbessern. Für kleinere Datenbanken wird empfohlen, die LUN-Pfade für Daten und Protokolle auf verschiedene Volumes zu trennen.

TempDB Platzierung

Ein separates Laufwerk verwenden.

▼ Details

Platzieren Sie TempDB auf einem separaten Laufwerk, um E/A-Konflikte zu vermeiden und die Leistung und Stabilität von SQL Server zu verbessern.

Thin Provisioning

Speicherplatz wird nach Bedarf zugewiesen.

▼ Details

Thin Provisioning für FSx for ONTAP Volumes konfigurieren, um den Speicherplatz besser zu nutzen und Kosten zu senken. Thin Provisioning ermöglicht die bedarfsgerechte Zuweisung von Speicherplatz, anstatt die gesamte Kapazität auf einmal zu reservieren.

Automatische Größenanpassung und Modus für automatische Größenanpassung

Volumen werden automatisch vergrößert.

▼ Details

Automatische Größenanpassung aktivieren und den Modus auf `grow` setzen, damit Volumes automatisch vergrößert werden, bevor sie voll und schreibgeschützt werden.

Blockgeräte Speicherplatzmanagement

Blockgerätespeicherplatzeinstellungen für von SQL Server verwendete LUNs konfigurieren.

▼ Details

Blockgerätespeicherplatzeinstellungen für LUNs, die von Microsoft SQL Server Instanzen verwendet werden, können konfiguriert werden, um Schreibfehler zu verhindern und die Speichereffizienz auf FSx for ONTAP zu verbessern.

Snapshot Copy-Reserve und automatisches Löschen

Speicherplatz für aktive Daten vorhalten.

▼ Details

Die Snapshot-Kopierreserve wird auf 0 % gesetzt und die automatische Snapshot-Löschung aktiviert, um Speicherplatz für aktive Daten zu schützen.

Speicherplatzmanagement

Das Volume sollte erweitert werden, bevor Snapshot-Kopien gelöscht werden.

▼ Details

Wenn der Speicherplatz knapp wird, das Volume erweitern, bevor Snapshot-Kopien gelöscht werden. Die Erweiterung des Volumes verhindert „Volume voll“-Fehler, reduziert Schreibfehler und erhält Snapshot-Wiederherstellungspunkte.

Tiering / TCO-Optimierung

Snapshot-Daten auf Tier-Ebene unter Verwendung der Snapshot-Only-Tiering-Richtlinie.

▼ Details

Verwenden Sie die Snapshot-only-Tiering-Richtlinie, die nur Snapshot-Daten in die Kapazitätsebene verschiebt, während aktive Daten in der SSD-Ebene verbleiben. Dieser Ansatz erhält die Performance mit niedriger Latenz für SQL-Workloads und senkt gleichzeitig die Speicherkosten. Snapshot-Daten werden nach einer 7-tägigen Abkühlphase in die Kapazitätsebene verschoben.

Storage Effizienz

Deduplizierung, Komprimierung und Verdichtung verwenden.

▼ Details

Deduplizierung, Komprimierung und Verdichtung können aktiviert werden, um den Speicherbedarf und die Kosten zu reduzieren, während die Leistung erhalten bleibt.

OS

ONTAP LUN OS-Typ auf die Hostpartitionierung abstimmen.

▼ Details

Der Wert für das ONTAP LUN-Betriebssystem ist auf das Partitionierungsschema des Hosts abzustimmen, um eine korrekte I/O-Ausrichtung sicherzustellen.

MPIO-Richtlinie, Sitzungen, Status und Zeitüberschreitungseinstellungen

Multipath I/O (MPIO) Richtlinie, Sitzungen, Status und Zeitüberschreitungseinstellungen konfigurieren.

▼ Details

Multipath I/O (MPIO) für Resilienz und Durchsatz konfigurieren. Fünf MPIO-Sitzungen pro Ziel-Interface für SQL Server auf iSCSI-LUNs verwenden, den Pfadstatus überwachen und den Host-Zeitüberschreitung auf 60 Sekunden setzen.

NTFS-Zuordnungseinheitsgröße

Auf 64K gesetzt.

▼ Details

Die NTFS-Zuordnungseinheitsgröße sollte auf 64 KB festgelegt werden, um die Festplatteneffizienz zu verbessern und die Fragmentierung bei SQL Server Workloads zu reduzieren.

Geplante lokale Snapshots

Geplante Snapshots deaktivieren.

▼ Details

Geplante Snapshots für FSx for ONTAP Volumes, die von Microsoft SQL Server verwendet werden, sollten deaktiviert werden. Stattdessen empfiehlt sich die externe Verwaltung von Snapshots mit Tools wie NetApp SnapCenter, die applikationskonsistente Backups erstellen und Datenbeschädigung bei Wiederherstellungsvorgängen verhindern.

Compute

Compute Rightsizing

Die EC2-Instanzgröße wird an den Arbeitslastbedarf angepasst.

▼ Details

Die Größe der SQL Server EC2 Instanz wird entsprechend der Arbeitslast angepasst. Bei Unterdimensionierung wird die Größe erhöht und bei Überdimensionierung reduziert, um Kosten und Leistung auszugleichen.

Betriebssystem-Patch

Aktuelle Betriebssystem-Patches anwenden.

▼ Details

Die neuesten Betriebssystem-Patches werden angewendet, um Sicherheit und Zuverlässigkeit zu verbessern.

Netzwerkadaptereinstellungen

Empfangsseitenskalierung (RSS) konfigurieren.

▼ Details

Receive Side Scaling (RSS) konfigurieren, um die Netzwerkverarbeitung auf mehrere CPUs zu verteilen und so die Netzwerkleistung zu verbessern. Die Einstellungen sollten vor der Produktivsetzung validiert werden.

MTU-Ausrichtung

Maximale Übertragungseinheit (MTU) über Host- und Speicherpfade hinweg angleichen.

▼ Details

Die EC2-MTU-Einstellungen (Maximum Transmission Unit) mit den FSx for ONTAP-Pfaden abgleichen, um Fragmentierung zu vermeiden und einen stabilen Durchsatz aufrechtzuerhalten.

Anwendung

Lizenz

Die Lizenznutzung für kostenpflichtige Funktionen kann überprüft werden.

▼ Details

Die SQL Server-Lizenznutzung auf Hostebene kann überprüft werden. Wenn kostenpflichtige Funktionen nicht verwendet werden, ist die Lizenz nicht optimiert und kann die Kosten erhöhen.

Microsoft SQL Server Patch

Die neuesten SQL Server Patches anwenden.

▼ Details

Die neuesten SQL Server Patches anwenden, um die Sicherheit und Systemzuverlässigkeit zu erhöhen.

MAXDOP

Arbeitslast-getestete Werte verwenden.

▼ Details

Konfigurieren Sie MAXDOP, um die Abfrageleistung zu optimieren. Werte von 4, 8 oder 16 funktionieren in der Regel gut. Testen Sie Ihre Arbeitslast und überwachen Sie auf Parallelitäts-Wartetypen wie CXPACKET.

Resilienz

Applikationskonsistente Snapshots

Applikationskonsistente Snapshots mit NetApp SnapCenter verwenden.

▼ Details

Mit applikationskonsistenten Snapshots und NetApp SnapCenter lassen sich präzise und zuverlässige Momentaufnahmen Ihrer Volume-Daten zu einem bestimmten Zeitpunkt erstellen. SnapCenter vereinfacht die Datensicherung und unterstützt eine schnelle Wiederherstellung von Daten, wodurch Ausfallzeiten reduziert und kritische Workloads geschützt werden.

Regionsübergreifende Replikation

Schutz vor regionalen Ausfällen.

▼ Details

Die regionsübergreifende Replikation (CRR) kann zur Verbesserung der Datenverfügbarkeit und der Notfallwiederherstellung in Ihrer SQL Server-Umgebung beitragen. CRR schützt vor regionalen Ausfällen und gewährleistet die Geschäftskontinuität durch die Replikation von Daten an verschiedenen Standorten.

Sicherungskonfiguration

FSx für ONTAP Backups oder AWS Backup konfigurieren.

▼ Details

FSx für ONTAP Backups oder AWS Backup kann so konfiguriert werden, dass Aufbewahrungs- und Compliance-Anforderungen erfüllt werden und doppelte Backup-Workflows vermieden werden.

Cluster Quorum

Quorum für Failover Cluster-Instanzen konfigurieren.

▼ Details

Das Quorum für SQL Server Failover Cluster Instances sollte korrekt konfiguriert werden, damit der Cluster erwartete Knotenausfälle tolerieren kann.

Laufwerksbuchstabe

Die Laufwerksbuchstaben sollten auf allen Knoten einheitlich bleiben.

▼ Details

Verwenden Sie in Ihrer SQL Server Hochverfügbarkeitsumgebung auf allen Knoten dieselben Laufwerksbuchstaben. Dies vereinfacht die Verwaltung und trägt dazu bei, dass das Failover korrekt funktioniert.

Heartbeat-Einstellungen

Heartbeat für ein stabiles Failover-Verhalten abstimmen.

▼ Details

Die Heartbeat-Einstellungen können so angepasst werden, dass unnötige Failover vermieden werden und echte Fehler dennoch schnell erkannt werden.

Gemeinsamer Speicher

Beide Knoten müssen auf gemeinsam genutzte iSCSI-LUNs zugreifen können.

▼ Details

Im FCI-Bereitstellungsmodell müssen alle gemeinsam genutzten Datenträger (iSCSI LUNs) von beiden Knoten aus erreichbar sein, damit Failover funktioniert.

SQL Server Dienst

Dienstkonto und Startabhängigkeiten validieren.

▼ Details

Die Berechtigungen des Dienstkontos, der Starttyp und die Abhängigkeiten sollten validiert werden, um ein zuverlässiges Hochverfügbarkeitsverhalten sicherzustellen.

Klonen

Klonbereinigung

Alte Klone regelmäßig entfernen.

▼ Details

Veraltete Klone regelmäßig entfernen, um Speicherkosten und betrieblichen Aufwand zu reduzieren. Alte und ungenutzte Klone verursachen hohe Kosten.

Oracle Best Practices

Die folgenden Best Practices und Empfehlungen gelten für Oracle Workloads.

Storage

Dateisystem-Spielraum

Es sollte ausreichend freie Kapazität oberhalb der Gesamtvolumengröße vorhanden sein.

▼ Details

Es sollte ausreichend Dateisystemkapazität über der Gesamtgröße Ihres Volumes vorhanden sein. Zu wenig freier Speicherplatz verursacht Leistungsprobleme, zu viel verschwendet Speicher und erhöht die Kosten.

Thin Provisioning

Speicherplatz wird nach Bedarf zugewiesen.

▼ Details

Thin Provisioning für FSx for ONTAP Volumes konfigurieren, um den Speicherplatz besser zu nutzen und Kosten zu senken. Thin Provisioning ermöglicht die bedarfsgerechte Zuweisung von Speicherplatz, anstatt die gesamte Kapazität auf einmal zu reservieren.

Automatische Größenanpassung und Modus für automatische Größenanpassung

Volumen werden automatisch vergrößert.

▼ Details

Automatische Größenanpassung aktivieren und den Modus auf `grow` setzen, damit Volumes automatisch vergrößert werden, bevor sie voll und schreibgeschützt werden.

Blockgeräte Speicherplatzmanagement

Blockgerätespeicherplatzeinstellungen für von SQL Server verwendete LUNs konfigurieren.

▼ Details

Die Einstellungen für den Blockgerätespeicherplatz der von Oracle Datenbanken verwendeten LUNs können so konfiguriert werden, dass Schreibfehler vermieden und die Speichereffizienz auf FSx für ONTAP verbessert werden.

Snapshot Copy-Reserve und automatisches Löschen

Speicherplatz für aktive Daten vorhalten.

▼ Details

Die Snapshot-Kopierreserve wird auf 0 % gesetzt und die automatische Snapshot-Löschung aktiviert, um Speicherplatz für aktive Daten zu schützen.

Speicherplatzmanagement

Das Volume sollte erweitert werden, bevor Snapshot-Kopien gelöscht werden.

▼ Details

Wenn der Speicherplatz knapp wird, das Volume erweitern, bevor Snapshot-Kopien gelöscht werden. Die Erweiterung des Volumes verhindert „Volume voll“-Fehler, reduziert Schreibfehler und erhält Snapshot-Wiederherstellungspunkte.

Tiering / TCO-Optimierung

Snapshot-Daten auf Tier-Ebene unter Verwendung der Snapshot-Only-Tiering-Richtlinie.

▼ Details

Verwenden Sie die Snapshot-only-Tiering-Richtlinie, die nur Snapshot-Daten in die Kapazitätsebene verschiebt, während aktive Daten in der SSD-Ebene verbleiben. Dieser Ansatz erhält die Performance mit niedriger Latenz für SQL-Workloads und senkt gleichzeitig die Speicherkosten. Snapshot-Daten werden nach einer 7-tägigen Abkühlphase in die Kapazitätsebene verschoben.

Storage Effizienz

Deduplizierung, Komprimierung und Verdichtung verwenden.

▼ Details

Deduplizierung, Komprimierung und Verdichtung können aktiviert werden, um den Speicherbedarf und die Kosten zu reduzieren, während die Leistung erhalten bleibt.

Swap-Speicher

Swap-Speicher basierend auf RAM festlegen.

▼ Details

Richten Sie den Auslagerungsspeicher entsprechend der Menge an RAM ein, damit das System den Speicherdruck bewältigen und Verlangsamungen oder Abstürze vermeiden kann.

Archiv, Daten, Kontrolle, Redo und temporäre Platzierung

Für jeden Typ von Oracle-Datei sollte ein dediziertes Volume verwendet werden, um E/A-Muster zu isolieren und die Leistung zu verbessern.

▼ Details

Archivprotokolle, Datendateien, Kontrolldateien, Redo-Logs und temporäre Dateien sollten auf separaten Laufwerken platziert werden, um E/A-Muster zu isolieren und die Ausfallsicherheit zu verbessern. Redundante Kopien sind bei Bedarf auf separaten Datenträgern aufzubewahren.

Oracle Binärplatzierung

Ein separates Volume verwenden.

▼ Details

Oracle-Binärdateien auf einem dedizierten Volume ablegen, um E/A-Konflikte zu reduzieren. Diese Trennung vereinfacht Software-Updates und minimiert das Risiko versehentlicher Änderungen oder Datenbeschädigung.

Geplante lokale Snapshots

Lokale geplante Snapshots werden deaktiviert.

▼ Details

Geplante Snapshots für FSx for ONTAP Volumes, die von Oracle verwendet werden, sollten deaktiviert werden, um Speicherplatz zu sparen und Kosten zu senken. Stattdessen empfiehlt sich die externe Verwaltung von Snapshots mit Tools wie NetApp SnapCenter, die applikationskonsistente Backups erstellen und Datenbeschädigung bei Wiederherstellungsvorgängen verhindern.

NFS rootonly

Für dNFS deaktivieren.

▼ Details

Der ONTAP `nfs-rootonly` Parameter für dNFS sollte deaktiviert werden. `nfs-rootonly` Dadurch werden NFS-Verbindungen auf privilegierte Ports (<1024) beschränkt. Da dNFS-Prozesse in NFSv4+ nicht als Root ausgeführt werden und höhere Ports verwenden, ermöglicht das Deaktivieren dieses Parameters die notwendigen Verbindungen.

Exportrichtlinie für Binärdateien

Superuser- und Setuid-Berechtigungen sind in die dedizierte Exportrichtlinie für Oracle-Binärdateien einzubeziehen.

▼ Details

Stellen Sie sicher, dass die Exportrichtlinie Superuser- und Setuid-Berechtigungen enthält, wenn sich Oracle-Binärdateien auf einer NFS-Freigabe befinden. Superuser-Zugriff (root) ermöglicht es NFS-Clients, als root zuzuordnen, was für die Ausführung von Binärdateien erforderlich ist.

ASM Setup

Oracle Automatic Storage Management (ASM) für iSCSI-basierten Speicher auf FSx für ONTAP einrichten.

▼ Details

Oracle Automatic Storage Management (ASM) kann für iSCSI-basierte Speicher, die auf FSx for ONTAP laufen, eingesetzt werden, um die Performance zu optimieren, die Speicherverwaltung zu vereinfachen und die Skalierbarkeit für Oracle Database Bereitstellungen zu erhöhen.

Nur-ASM-Konfigurationen

- **ASM Daten-Festplattengruppe, ASM Logs-Festplattengruppe, ASM FRA-Festplattengruppe und ASM Archive-Festplattengruppe LUNs**

LUNs werden auf Ressourcen der Automatic Storage Management (ASM) Festplattengruppe verteilt.

▼ Details

Verteilen Sie LUNs auf Festplattengruppen für Daten, Wiederherstellungsprotokoll und Archivprotokoll des Automatic Storage Management (ASM), um optimale Leistung und Redundanz zu erzielen.

- **ASM externe Redundanz**

Oracle ASM Festplattengruppen mit EXTERNAL Redundanz konfigurieren.

▼ Details

Oracle ASM Festplattengruppen mit EXTERNAL Redundanz für FSx for ONTAP iSCSI LUNs konfigurieren, um die integrierte Hochverfügbarkeit von FSx for ONTAP zu nutzen, die Speichereffizienz zu optimieren und Kosten zu senken, indem auf Oracle-Ebene auf Daten-Spiegelung verzichtet wird.

- **ASM Filtertreiber und ASMLib logische Blockgrößenanpassung**

Oracle ASM Filter Driver (AFD) und ASMLib so konfigurieren, dass die logische Blockgröße des zugrunde liegenden FSx für ONTAP Storage verwendet wird.

▼ Details

Der Oracle ASM Filter Driver (AFD) und ASMLib sind in der ASMLib Konfigurationsdatei so einzurichten, dass die logische Blockgröße des zugrunde liegenden FSx for ONTAP Storage verwendet wird. Dies

stellt sicher, dass AFD und ASMLib die I/O-Operationen an die Blockgröße des Storage ausrichten, wodurch die Leistung durch Minimierung der Latenz und Reduzierung unnötigen I/O-Overheads optimiert wird.

TCP Slot-Tabelle

Für NFS-basierte Oracle-Workloads auf 128 festgelegt.

▼ Details

Die Kernelparameter für die TCP-Slottabelle sollten für Oracle-Workloads, die auf NFS ausgeführt werden, auf 128 gesetzt werden. Diese Konfiguration ermöglicht mehr gleichzeitige I/O-Operationen und reduziert die Latenz in Szenarien mit hohem Durchsatz wie dem Oracle-Dateizugriff. Kernelparameter steuern die maximale Anzahl ausstehender NFS-Anfragen über TCP und wirken wie die Warteschlangentiefe in Fibre Channel-Setups. Die Standardwerte unter Linux, die typischerweise auf 16 gesetzt sind, unterstützen keine optimale Datenbankleistung.

NFS Mountoptionen – Datenbankdateien

NFS-Mount-Optionen, die die Leistung für Datenbankdateien optimieren, bieten eine optimale Performance.

▼ Details

Optimierte NFS-Mount-Optionen für Datenbankdateien verwenden. Wichtige Parameter sind `rw` für lesen/schreiben-Zugriff, `bg` für Hintergrund-Mounting, `hard` für unbegrenzte Wiederholungsversuche bei Fehlern und `proto=tcp` für zuverlässige Zustellung. Die Werte `rsize` und `wsizesize` von 262144 verbessern große E/A-Operationen und erhöhen den Durchsatz, während `nointr` lang andauernde Aufgaben nicht unterbricht. Diese Konfiguration verbessert die Datenbankleistung und Resilienz, insbesondere in Umgebungen mit hohem Durchsatz.

NFS-Mountoptionen für ADR home

NFS-Mount-Optionen, die die Leistung für das ADR-Home-Verzeichnis optimieren, bieten eine optimale Performance.

▼ Details

Optimierte NFS-Mountoptionen für das Automatic Diagnostic Repository (ADR) Home- oder Stammverzeichnis verwenden. Das ADR-Home speichert Protokolle und Traces, die von ähnlichen Zuverlässigkeitsoptionen wie zentrale Datenbankdateien profitieren, jedoch nicht die `nointr` Mountoption benötigen, da die Vorgänge weniger unterbrechungsempfindlich sind.

NFSv4 Domänennamen

NFSv4-Domänennamen zwischen Host und NFS-Server müssen übereinstimmen.

▼ Details

NFSv4-Domänennamen zwischen dem Host (`/etc/idmapd.conf` oder `hostname -d` und dem NFS-Server (`v4-id-domain` in ONTAP abgleichen).

NFS Caching-Optionen

Host-Caching darf in eigenständigen Bereitstellungen nicht deaktiviert werden.

▼ Details

NFS-Mountoptionen, die das Host-Caching deaktivieren, wie `actimeo=0` und `noac`, sollten in eigenständigen Oracle-Bereitstellungen ausgelassen werden, um Effizienz und Zuverlässigkeit zu verbessern. Diese Optionen gelten für Clusterumgebungen, um die Cache-Konsistenz sicherzustellen, aber in Einzelinstanzumgebungen umgehen sie unnötig das Caching und können die Leistung erheblich verringern.

dNFS-Aktivierung

dNFS wird aktiviert.

▼ Details

Direct NFS (dNFS) kann in der Oracle-Umgebung aktiviert werden, um die Leistung und Zuverlässigkeit des NFS-Speichers zu verbessern.

dNFS konsistente IP-Auflösung

Die Namensauflösung im Round-Robin-Verfahren sollte vermieden werden.

▼ Details

Die Verwendung von Direct NFS (dNFS) mit jeglicher Art von Round-Robin-Namensauflösung, einschließlich DNS, DDNS, NIS oder anderen Methoden, sollte vermieden werden. Dies schließt die in ONTAP verfügbare DNS-Lastverteilungsfunktion ein. Eine konsistente IP-Adressauflösung erhält die Stabilität der Datenbank und verhindert potenzielle Abstürze oder Datenbeschädigung.

dNFS Konfigurationsdatei

Inhalte `oranfstab` validieren.

▼ Details

Der Inhalt der `oranfstab`-Datei sollte überprüft und aktualisiert werden, um eine korrekte Nutzung von Direct NFS (dNFS) sicherzustellen. Die `oranfstab`-Datei ist unerlässlich für die Konfiguration erweiterter dNFS-Funktionen wie Multipathing und spezifischer NFS-Optionen. Eine korrekte Konfiguration verbessert die Effizienz des Datenzugriffs und der Datenverwaltung.

dNFS ohne gemeinsamen Cache

Verwenden Sie `nosharecache` für bestimmte Multi-Mount-Fälle.

▼ Details

Die ``nosharecache`` Mount-Option ist für Umgebungen zu konfigurieren, in denen Direct NFS (dNFS) aktiviert ist und ein Quellvolume mehrmals auf einem einzelnen Server mit verschachtelten NFS-Mounts eingebunden wird. Diese Konfiguration verhindert das Teilen des Caches zwischen den Mounts und stellt so Datenkonsistenz sowie optimale Performance sicher.

Compute

Betriebssystem-Patch

Aktuelle Patches anwenden.

▼ Details

Die neuesten Betriebssystem-Patches werden angewendet, um Sicherheit und Zuverlässigkeit zu verbessern.

Transparente riesige Seiten

Transparente riesige Seiten (THP) deaktivieren.

▼ Details

Transparent Huge Pages (THP) sollten auf Datenbank-Hosts mit Oracle Datenbanken deaktiviert werden, um potenzielle Leistungseinbußen zu vermeiden und das Speichermanagement zu verbessern.

Erweiterte TCP-Optionen

Erweiterte Optionen des Transmission Control Protocol (TCP) aktivieren.

▼ Details

TCP-Zeitstempel, SACK und Window Scaling sollten für optimale Netzwerkleistung und Zuverlässigkeit aktiviert sein.

Dateisystem-I/O-Optionen

Festlegen `filesystemio_options = setall`.

▼ Details

Für optimale E/A-Leistung `filesystemio_options = setall` einstellen. Die Größe des System Global Area (SGA) sollte gegebenenfalls angepasst werden, wenn von gepufferter E/A abgewichen wird.

Multiblock Lesezähler

Der `db_file_multiblock_read_count` Parameter wird entfernt.

▼ Details

Den `db_file_multiblock_read_count` Parameter aus der textbasierten FILE `init.ora` oder der serververwalteten binären SPFILE (`spfile<SID>.ora`) für Oracle Datenbanken entfernen, um Leistungsprobleme zu vermeiden und Oracle die automatische Verwaltung dieser Einstellung zu überlassen.

Oracle Critical Patch Updates

Aktuelle CPU-Updates anwenden.

▼ Details

Installieren Sie die neuesten Oracle Critical Patch Updates, um Sicherheitslücken zu schließen und die Integrität Ihrer Datenbankumgebung zu gewährleisten. Überprüfen und installieren Sie regelmäßig Patches, um sich vor potenziellen Bedrohungen zu schützen und die Einhaltung bewährter Sicherheitspraktiken sicherzustellen.

Resilienz

Applikationskonsistente Snapshots

Applikationskonsistente Snapshots mit NetApp SnapCenter verwenden.

▼ Details

Mit applikationskonsistenten Snapshots und NetApp SnapCenter lassen sich präzise und zuverlässige Momentaufnahmen Ihrer Volume-Daten zu einem bestimmten Zeitpunkt erstellen. SnapCenter vereinfacht die Datensicherung und unterstützt eine schnelle Wiederherstellung von Daten, wodurch Ausfallzeiten reduziert und kritische Workloads geschützt werden.

Regionsübergreifende Replikation

Schutz vor regionalen Ausfällen.

▼ Details

Die regionsübergreifende Replikation (CRR) kann aktiviert werden, um die Datenverfügbarkeit und die Notfallwiederherstellung für Ihre Oracle-Datenbanken zu verbessern. CRR schützt vor regionalen Ausfällen und gewährleistet die Geschäftskontinuität durch die Replikation von Daten an verschiedenen Standorten.

Sicherungskonfiguration

FSx für ONTAP Backups oder AWS Backup konfigurieren.

▼ Details

FSx für ONTAP Backups oder AWS Backup kann so konfiguriert werden, dass Aufbewahrungs- und Compliance-Anforderungen erfüllt werden und doppelte Backup-Workflows vermieden werden.

Klonen

Klonbereinigung

Alte Klone regelmäßig entfernen.

▼ Details

Veraltete Klone regelmäßig entfernen, um Speicherkosten und betrieblichen Aufwand zu reduzieren. Alte und ungenutzte Klone verursachen hohe Kosten.

Was kommt als Nächstes

["Gut konzipierte Datenbankkonfigurationen implementieren"](#)

Gut strukturierte Datenbankkonfigurationen in NetApp Workload Factory implementieren

Nutzen Sie die Erkenntnisse und Empfehlungen der Konfigurationsanalyse, um mit NetApp Workload Factory Best Practices für Ihre Datenbankkonfigurationen mit Microsoft SQL Server und Oracle zu implementieren. Sie können den gut entwickelten Status einfach überprüfen, sich über Probleme mit Datenbankkonfigurationen informieren und Konfigurationen beheben, die nicht hinsichtlich Zuverlässigkeit, Sicherheit, Effizienz, Leistung und Kosten optimiert sind.

Sie können auch die Analyse von Konfigurationen ausblenden, die nicht auf Ihre Umgebung zutreffen, um zusätzliche Warnmeldungen und ungenaue Ergebnisse zu vermeiden.

["Informationen zur Konfigurationsanalyse und zum Well-Architected-Status in Workload Factory."](#)

Über diese Aufgabe

Workload Factory analysiert täglich Datenbankkonfigurationen. Die tägliche Analyse liefert gut strukturierte Statusberichte, Erkenntnisse und Empfehlungen.

Viele Empfehlungen stehen zur Verfügung, wenn Sie Ihrem AWS-Konto die Berechtigungen *Anzeigen*, *Planen* und *Analysieren* erteilen. Wenn Sie die Berechtigungen *Betrieb* und *Behebung* erteilen, sind alle Empfehlungen verfügbar, und Konfigurationsprobleme können automatisch behoben werden, um Best Practices zu erfüllen.

Probleme können im Datenbankinventar oder im Well-architected Dashboard innerhalb der Workload Factory Konsole überprüft und behoben werden. Da die Anforderungen an Datenbankkonfigurationen variieren, lässt sich die Analyse spezifischer Konfigurationen, die für Ihre Datenbankumgebung nicht zutreffen, ausblenden. So werden unnötige Warnmeldungen und ungenaue Optimierungsergebnisse vermieden.

Optional können Sie eine einmalige Bewertung durchführen, um die Best Practices für Ihre Datenbankkonfigurationen zu überprüfen, ohne Anmeldeinformationen zu speichern oder Ressourcen zu registrieren.

Es besteht auch die Möglichkeit, benutzerdefinierte Regeln in einfacher Sprache zu erstellen, um Ihre Umgebungen anhand der Standards Ihres Unternehmens und der NetApp Best Practices zu validieren. Regeln können mit einem Probelauf getestet und anschließend für die Ausführung in Ihren Umgebungen geplant werden. ["Weitere Informationen zu benutzerdefinierten Regeln."](#)

Was analysiert wird

Workload Factory analysiert den Well-Architected-Status der folgenden Konfigurationen:

Für Microsoft SQL Server Instanzen:

- **Speicherdimensionierung:** umfasst Storage-Tier, Dateisystem-Spielraum, Protokolllaufwerkgröße und TempDB-Laufwerkgröße
- **Speicherlayout:** umfasst die Platzierung von Benutzerdatendateien, die Platzierung von Protokolldateien und die Platzierung von TempDB
- **Storage-Konfiguration:** umfasst Kapazitätsmanagement, Thin Provisionierung, Tiering-Richtlinie, Snapshots, den Microsoft Multipath I/O (MPIO)-Status und die MPIO-Einstellung für die Zeitüberschreitung
- **Compute:** umfasst die richtige Dimensionierung, Betriebssystem-Patches und Netzwerkadaptoreinstellungen wie Receive Side Scaling (RSS), TCP-Offloading und MTU-Ausrichtung
- **Anwendung:** Enthält Microsoft SQL Server-Lizenzen, Microsoft SQL Server-Patch und MAXDOP-Einstellungen
- **Ausfallsicherheit:** umfasst lokale Snapshots, Backup-Konfiguration, regionsübergreifende Replikation (CRR), Microsoft SQL High Availability und Klonbereinigung
- **Klone:** enthält Optionen zum Aktualisieren und Löschen von Klonen (Sandboxes), die innerhalb oder außerhalb von Workload Factory erstellt wurden und älter als 60 Tage sind

Für Oracle Datenbanken:

- **Speicherdimensionierung:** beinhaltet die Zuweisung von Auslagerungsspeicher und den verfügbaren Platz im Dateisystem
- **Speicherkonfiguration:** Umfasst Kapazitätsmanagement, Thin Provisioning, Tiering-Richtlinie, Snapshots, Speichereffizienzen und Betriebssystemkonfigurationen für Bereitstellungen mit NFS oder iSCSI mit oder ohne Automatic Storage Management (ASM), einschließlich Microsoft Multipath I/O (MPIO) Status und Einstellungen sowie die folgenden dNFS-Einstellungen: dNFS-Aktivierung, dNFS konsistente IP-Auflösung, dNFS Konfigurationsdatei und dNFS `nosharecache`
- **Storage-Layout:** umfasst die Platzierung von Wiederherstellungsprotokollen, temporären Tabellenbereichen, Datendateien, Archivprotokollen, Kontrolldateien und Binärdateien sowie die Anzahl der LUNs in ASM-Disk-Gruppen.
- **Compute:** beinhaltet Betriebssystem-Patches
- **Anwendung:** Enthält kritische Patch-Updates von Oracle
- **Ausfallsicherheit:** umfasst regionsübergreifende Replikation (CRR), applikationskonsistente Snapshots, Backup-Konfiguration und Klonbereinigung

Die Well-Architected-Analyse für Oracle benachrichtigt Sie, wenn eine Konfiguration von anderen abhängt, und listet Maßnahmen zur Optimierung verknüpfter Konfigurationen auf.

Führen Sie eine einmalige Bewertung Ihrer Konfigurationen durch

Führen Sie eine einmalige Bewertung durch, um den Well-Architected-Status Ihrer Microsoft SQL Server-Instanzen oder Oracle-Datenbanken zu ermitteln, ohne Anmeldeinformationen zu speichern oder Ressourcen zu registrieren.

Sie können das Skript ausführen und die Ergebnisse mehrmals hochladen. Workload Factory aktualisiert den Well-Architected-Status und die Erkenntnisse mit jedem Upload.

Für jede Konfiguration werden der aktuelle Wert und der empfohlene Wert angezeigt.

Microsoft SQL Server-Instanzen

Schritte

1. Melden Sie sich mit einem der "[Konsolenerlebnisse](#)" an.
2. Wählen Sie das Menü  und dann **Datenbanken** aus.
3. Wählen Sie im **Inventar SQL Server** als Engine-Typ aus.
4. Wählen Sie **Einmalige Bewertung > Mehr über die Bewertung erfahren**. Lesen Sie die Informationen zur einmaligen Bewertung.
5. Wählen Sie **Download script**.
 - a. Kopieren Sie das Skript auf Ihren Microsoft SQL Server host.
 - b. Führen Sie das Skript in PowerShell aus. Ein Skript sammelt Metadaten von allen Instanzen.
6. Wählen Sie **Einmalige Bewertung > Hochladen**. Suchen Sie die Datei und laden Sie sie in die Workload Factory console hoch.
7. Sehen Sie sich die Empfehlungen für jede Konfiguration an. Workload Factory enthält Best Practices und weist in den Empfehlungen auf potenzielle Probleme hin, die bei nicht optimierten Konfigurationen auftreten können.

Oracle-Datenbanken

Schritte

1. Melden Sie sich mit einem der "[Konsolenerlebnisse](#)" an.
2. Wählen Sie das Menü  und dann **Datenbanken** aus.
3. Wählen Sie im **Inventar** als Engine-Typ **Oracle** aus.
4. Wählen Sie **Einmalige Bewertung > Mehr über die Bewertung erfahren**. Lesen Sie die Informationen zur einmaligen Bewertung.
5. Wählen Sie **Download script**.
 - a. Kopieren Sie das Python-Skript auf Ihren Oracle-Datenbank-Host.
 - b. Führen Sie das Skript in der entsprechenden Shell aus. Ein Skript sammelt Metadaten aus allen Datenbanken.
6. Wählen Sie **Einmalige Bewertung > Hochladen**. Suchen Sie die Datei und laden Sie sie in die Workload Factory console hoch.
7. Sehen Sie sich die Empfehlungen für jede Konfiguration an. Workload Factory enthält Best Practices und weist in den Empfehlungen auf potenzielle Probleme hin, die bei nicht optimierten Konfigurationen auftreten können.

Eine On-Demand-Bewertung durchführen

Wenn Sie in Ihrem AWS-Konto die Berechtigungen „Operationen“ und „Problembehebung“ erteilen, kann eine bedarfsgesteuerte Bewertung Ihrer Oracle-Datenbanken durchgeführt werden. Für diese Bewertung ist keine Registrierung von Ressourcen erforderlich.

Schritte

1. Melden Sie sich mit einem der "[Konsolenerlebnisse](#)" an.
2. Wählen Sie das Menü  und dann **Datenbanken** aus.
3. Wählen Sie im **Inventar** als Engine-Typ **Oracle** aus.
4. **Anzeigen und korrigieren** auswählen.
5. Im Tab „Well-architected Status“ **Jetzt analysieren** auswählen.
6. Sehen Sie sich die Empfehlungen für jede Konfiguration an. Workload Factory enthält Best Practices und weist in den Empfehlungen auf potenzielle Probleme hin, die bei nicht optimierten Konfigurationen auftreten können.

Bevor Sie mit dem Beheben, Verwerfen und Reaktivieren von Konfigurationen beginnen

Die folgenden Anforderungen sind für die kontinuierliche Bewertung Ihrer Datenbankumgebung und die automatische Behebung von Konfigurationsproblemen notwendig. Diese Anforderungen sind für die einmalige Bewertung nicht erforderlich.

- Sie müssen "[Berechtigungen für Operationen und Behebung gewähren](#)" in Ihrem AWS-Konto angemeldet sein.
- Die Ressource muss in Workload Factory registriert werden und der Speichertyp muss FSx for ONTAP sein. "[Informationen zur Registrierung von Ressourcen](#)."
- Prüfen Sie jede Empfehlung, bevor Sie eine Einstellung oder Konfiguration beheben. Testen Sie bei RSS und MAXDOP die empfohlenen Einstellungen, um die Leistung zu überprüfen, bevor Sie Ihre Produktionsumgebung ändern.

Ein Konfigurationsproblem beheben

Behebung von Konfigurationsproblemen für SQL Server- oder Oracle-Umgebungen, die auf FSx for ONTAP Storage ausgeführt werden.



Die Korrektur einer Konfiguration kann zu Ausfallzeiten oder Serviceunterbrechungen führen. Stellen Sie sicher, dass Sie die Empfehlung sorgfältig prüfen, bevor Sie sich entscheiden, eine Konfiguration zu korrigieren.

Schritte

1. Melden Sie sich mit einem der "[Konsolenerlebnisse](#)" an.
2. Wählen Sie das Menü  und dann **Datenbanken** aus.
3. Im **Inventar** erfolgt die Auswahl des Engine-Typs: Microsoft SQL Server oder Oracle.
4. Auswahl der Ressourcen zur Behebung bestimmter Konfigurationen.
 - Bei Auswahl von Microsoft SQL Server ist die Registerkarte **Instances** auszuwählen.
 - Wenn Oracle ausgewählt wurde, ist die Registerkarte **Databases** auszuwählen.
5. Mit **View and fix** lassen sich Konfigurationsprobleme für die Instanz anzeigen.
6. Auf der Statusseite „Well-Architected“ der Instanz können die Ergebnisse der Analyse überprüft werden.

Sie können Konfigurationsprobleme nach Kategorien, Unterkategorien, Status, Schweregrad und Tags filtern.

Wählen Sie **Export PDF**, um einen Bericht mit den Ergebnissen herunterzuladen.

7. Über den Pfeil im Dropdown-Menü lässt sich die Empfehlung für jede Konfiguration anzeigen. Die Empfehlungen umfassen bewährte Vorgehensweisen, potenzielle Probleme nicht optimierter Konfigurationen und wichtige Hinweise. Eine sorgfältige Prüfung der Empfehlung ist wichtig.
8. Wenn die Option verfügbar ist, können Konfigurationsprobleme mit **View and fix** angezeigt und behoben werden.

Alle auswählen ist die Standardeinstellung, es können jedoch auch bestimmte Ressourcen zur Behebung ausgewählt werden.

- a. Prüfen Sie bei allen Konfigurationen außer der Klonbereinigung die Empfehlungsdetails, um die Auswirkungen der Problembehebung zu ermitteln. Einige Maßnahmen zur Behebung können zu Ausfallzeiten oder Serviceunterbrechungen führen.
- b. Für die Klonbereinigung lassen sich geklonte Datenbanken (Sandboxes) zum Aktualisieren oder Löschen auswählen.
 - Durch das Aktualisieren eines Klons wird dieser mit seiner Quelldatenbank synchronisiert. Die Aktualisierung ist nur für Klone verfügbar, die in Workload Factory erstellt wurden.
 - Das Löschen eines Klons entfernt ihn dauerhaft, gibt Speicherplatz im Storage frei und senkt die Kosten. Sie können Klone löschen, die innerhalb und außerhalb von Workload Factory erstellt wurden.

9. **Weiter** auswählen, um das Konfigurationsproblem zu beheben.

Ergebnis

Workload Factory beginnt mit der Behebung des Problems bzw. der Probleme. Auf der Registerkarte **Job monitoring** wird der Status des Vorgangs angezeigt.

Die Analyse von Datenbankkonfigurationen ablehnen

Verwerfen Sie die Analyse bestimmter Datenbankkonfigurationen, die nicht auf Ihre Datenbankumgebung zutreffen, um unnötige Warnmeldungen und ungenaue Optimierungsergebnisse zu vermeiden. Sie können eine verworfene Konfigurationsanalyse jederzeit wieder aktivieren.

Schritte

1. Melden Sie sich mit einem der "[Konsolenerlebnisse](#)" an.
2. Wählen Sie das Menü  und dann **Datenbanken** aus.
3. Im Menü Datenbanken wird **Inventar** ausgewählt.
4. Im Inventar ist der Datenbank-Engine-Typ **Microsoft SQL Server** oder **Oracle** auszuwählen.
5. In der SQL Server-Instanz oder Oracle Datenbank mit der Konfiguration, die zurückgestellt werden soll, erfolgt die Auswahl des Aktionsmenüs und anschließend von **Well-architected**.
6. Auf der Seite „Well-architected-Analyse“ können Sie zu der Konfiguration, deren Bearbeitung aufgeschoben werden soll, nach unten scrollen und dann das Aktionsmenü sowie anschließend **Dismiss** auswählen.
7. Im Konfigurationsdialog „Verwerfen“ erfolgt die Bestätigung des Verwerfens durch Auswahl der Option **Verwerfen** und anschließende erneute Auswahl von **Verwerfen**.

Ergebnis

Workload Factory stoppt die Konfigurationsanalyse.

Sie können die Analyse jederzeit reaktivieren. Die Konfiguration wird nicht mehr in die Gesamtoptimierungsbewertung einbezogen.

Eine verworfene Konfigurationsanalyse reaktivieren

Eine verworfene Konfigurationsanalyse kann jederzeit reaktiviert werden. Eine oder mehrere Konfigurationen können zur Reaktivierung ausgewählt werden.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Im Menü Datenbanken wird **Inventar** ausgewählt.
4. Im Inventar ist der Datenbank-Engine-Typ **Microsoft SQL Server** oder **Oracle** auszuwählen.
5. In der SQL Server-Instanz oder Oracle Datenbank mit der Konfiguration, die zurückgestellt werden soll, erfolgt die Auswahl des Aktionsmenüs und anschließend von **Well-architected**.
6. Auf der Seite für die Well-architected-Analyse werden bei Auswahl von **Dismissed configuration** nur verworfene Konfigurationen angezeigt.
7. Über **Reaktivieren** lässt sich die Konfigurationsanalyse für die verschobene oder verworfene Konfiguration neu starten.

Ergebnis

Workload Factory reaktiviert die Konfigurationsanalyse und führt sie von nun an täglich aus.

Verwandte Informationen

- ["Informationen zur Konfigurationsanalyse für Datenbankressourcen und den Well-Architected-Status in Workload Factory"](#)
- ["Verbindung zu einem FSx for ONTAP Dateisystem über einen Link herstellen"](#)
- ["Informationen zu benutzerdefinierten Regeln"](#)

Microsoft SQL Server Workloads mit NetApp Workload Factory für Datenbanken schützen

Der Schutz Ihrer Microsoft SQL Server Anwendungsdaten erfolgt mit NetApp Backup and Recovery über die NetApp Workload Factory Konsole. Mit dieser Integration lassen sich die folgenden Schutzziele erreichen: Workloads mit lokalen Snapshots auf lokalem primärem Amazon FSx for NetApp ONTAP (FSx for ONTAP) Storage sichern und Workloads auf sekundären FSx for ONTAP Storage replizieren.

Über diese Aufgabe

Workload Factory automatisiert die Ressourcenerkennung, die Überprüfung der Voraussetzungen sowie die Konfiguration und Installation des Plug-ins für Microsoft SQL Server, um den Schutz Ihrer Workloads mit NetApp Backup and Recovery vorzubereiten. Das Plug-in ist eine hostseitige Komponente der NetApp Software, mit der Sie Ihre Microsoft SQL Server Workloads schützen können.

NetApp Backup and Recovery nutzt die NetApp SnapMirror Datenreplizierungstechnologie, um sicherzustellen, dass alle Backups durch die Erstellung von Snapshot-Kopien und deren Übertragung an die Backup-Speicherorte vollständig synchronisiert sind.

Weitere Informationen zum Schutz mit Backup und Recovery finden Sie im ["Überblick über den Schutz von Microsoft SQL Workloads mit Backup and Recovery"](#).

Bevor Sie beginnen

Die folgenden Anforderungen müssen erfüllt sein, um Microsoft SQL Server Workloads mit Backup and Recovery zu schützen.

- Es muss sichergestellt sein, dass Ihre Umgebung ["die Anforderungen für Backup and Recovery SQL Server"](#) entspricht.
- ["Vollständige NetApp Console Anforderungen"](#) einschließlich der Einrichtung, der Zuweisung von IAM-Rollen und der Installation eines Console agent.

Wenn Sie als Unternehmensadministrator Zugriff auf das NetApp Konto haben, wird Ihnen die `backup and recovery super admin` Rolle automatisch zugewiesen, wenn Sie [Vorbereitung auf den Schutz mit NetApp Backup and Recovery](#).

- Festlegen der Hostauflösung auf dem Connector

Für die Erkennung von Datenbanken ist eine Hostauflösung auf dem Connector erforderlich. Auf dem gehosteten Gerät wird die Zuordnung der IP-Adresse zum Hostnamen in der `/etc/hosts` Datei eingetragen.

- ["Einrichtung der Lizenzierung für NetApp Backup and Recovery"](#)

Vorbereitung auf den Schutz mit NetApp Backup and Recovery

Zum Schutz Ihrer Microsoft SQL Server-Ressourcen mit NetApp Backup and Recovery ist der Vorbereitungsprozess abzuschließen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Im Menü Datenbanken wird **Inventar** ausgewählt.
4. Im Inventar ist **Microsoft SQL Server** als Engine-Typ auszuwählen.
5. Die zu schützende Instanz suchen und dann im Menü **Protect** auswählen.
6. Falls eine Aufforderung angezeigt wird, sind Windows-Anmeldeinformationen mit Administratorrechten erforderlich.

Für die Nutzung von NetApp Backup and Recovery zum Schutz müssen SQL Server-Instanzen in Workload Factory mit Windows-Anmeldeinformationen registriert werden.

7. Wenn mehrere Console agents aktiv und verfügbar sind, können Sie den **Console agent** auswählen, bei dem der Workload registriert und geschützt werden soll.
8. Zur Vorbereitung der Datensicherung registriert Workload Factory Ihre SQL Server Ressourcen automatisch in Backup and Recovery, konfiguriert und installiert das Plug-in for Microsoft SQL Server und ermittelt Ressourcen, die die Voraussetzungen für den Schutz Ihrer SQL Server Instanz erfüllen. Der Prozess beginnt mit der Auswahl von **Start**.
9. Nach Erfüllung der Voraussetzungen kann **Redirect** ausgewählt werden, um auf Backup and Recovery zuzugreifen.

Was kommt als Nächstes

In Backup and Recovery können Sie eine Richtlinie erstellen, um Ihre Microsoft SQL Server Instanz und Datenbanken zu schützen.

["Informationen zum Erstellen einer Richtlinie zum Schutz Ihrer Microsoft SQL Server Instanz und Ihrer Datenbanken"](#).

Zugehörige Informationen bietet die ["Dokumentation zu Datensicherung und Wiederherstellung"](#) zur Verwaltung von Microsoft SQL Server Workloads.

Schutz für Microsoft SQL Server Ressourcen bearbeiten

Sie können den Schutz für Microsoft SQL Server Instanzen und Datenbanken bearbeiten, die bereits in NetApp Backup and Recovery geschützt sind. Durch die Bearbeitung des Schutzes können Sie die Datensicherungsstrategie oder den Zeitplan für Ihre geschützten Microsoft SQL Server Instanzen ändern.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Im Menü Datenbanken wird **Inventar** ausgewählt.
4. Im Inventar ist **Microsoft SQL Server** als Engine-Typ auszuwählen.
5. Auszuwählen ist die Registerkarte **Datenbanken**.
6. Die Datenbank, für die der Schutz bearbeitet werden soll, ist zu suchen, und anschließend ist im Menü **Schutz bearbeiten** auszuwählen.

Sie werden in der NetApp Console zu Backup and Recovery weitergeleitet, wo Sie die Datensicherungsstrategie oder den Zeitplan ändern können.

Einsatz von FSx for ONTAP für EDA-Workloads

Erfahren Sie mehr über Workload Factory für EDA

Workload Factory für EDA unterstützt Sie bei der Verwaltung von Amazon FSx für ONTAP über mehrere Dateisysteme hinweg. Die Leistung wird verbessert und die Kosten werden gesenkt, indem Speichereinstellungen automatisch angepasst, Latenzprobleme erkannt und Einblicke in Ihre EDA-Projekte bereitgestellt werden.

Es ist so konzipiert, dass es sich in Ihre Infrastructure as Code (IaC) Frameworks integrieren lässt.

Workload Factory for EDA bietet Dashboards, Automatisierungstools und Hilfsprogramme, die bei der Verwaltung mehrerer FSx for ONTAP Dateisysteme unterstützen.

Es bietet Folgendes:

- **"Übersichts-Dashboard"**: Bietet eine zentrale Übersicht über Ihren FSx for ONTAP Cluster, sodass Sie Zustand, Kapazität und Durchsatz überwachen können. Damit lässt sich entscheiden, wo neue Volumes platziert werden, wann eine Erhöhung von Kapazität oder Durchsatz sinnvoll ist, und es werden automatische Kapazitätsempfehlungen bereitgestellt oder die automatische Skalierung kann aktiviert werden. Auch eine Überprüfung früherer Entscheidungen ist möglich, um nachzuvollziehen, wie sich die

Empfehlungen des Systems im Laufe der Zeit verändert haben.

- ["Volume-Latenz überwachen"](#) Überwacht die Lese- und Schreiblatenz von Volumes und ermöglicht die Festlegung von Warn- und kritischen Schwellenwerten. Bei Überschreitung dieser Schwellenwerte erfolgt eine Benachrichtigung per E-Mail oder SNS. Enthält eine automatisierte Basisanalyse anhand von ONTAP QoS Delay Center-Metriken sowie eine optionale KI-Analyse für komplexere Probleme, die eine tiefere Ursachenidentifikation erfordern.
- ["Latenztrends analysieren"](#) Synchronisierte Leistungsdiagramme für Latenz, IOPS und Durchsatz zeigen, wie sich diese Metriken im Zeitverlauf verändern. So lassen sich Muster erkennen, feststellen, ob Probleme wiederholt oder nur einmalig auftreten, und fundierte Entscheidungen zu Korrekturen treffen.
- ["Projekt-Dashboard"](#): Zeigt die Speichernutzung all Ihrer FSx for ONTAP Dateisysteme an einem Ort an, unterstützt bei der Kapazitätsplanung, Kostenschätzung und zeigt, wie jedes Projekt Speicher verwendet.
- ["CI/CD"](#): Beschleunigt Software-Builds durch schnelles Klonen von FSx for ONTAP Volumes.

Schnellstart für Workload Factory für EDA

Beginnen Sie mit Workload Factory for EDA, indem Sie Ihre Umgebung einrichten, Überwachungs-Dashboards aktivieren und die Latenzanalyse konfigurieren, um die FSx for ONTAP Performance für Ihre EDA-Workloads zu optimieren.

1

Anmeldung bei Workload Factory

Sie müssen sich ["Registrieren und anmelden"](#) bei der NetApp Console anmelden.

2

Hinzufügen von Anmeldeinformationen und Berechtigungen für die EDA-Workload

["Manuelles Hinzufügen von Anmeldeinformationen zu einem Konto"](#) was die Auswahl der EDA Workload-Funktion und ["Erstellung der IAM-Richtlinien für die erforderlichen Berechtigungen"](#) umfasst.

3

Einrichten Ihrer Umgebung zur Erfüllung der EDA-Anforderungen

Sie benötigen ein bereitgestelltes und erkanntes FSx for ONTAP Dateisystem, das mindestens ein Volume enthält, das als NFS-Freigabe konfiguriert wurde.

["Weitere Informationen zu den EDA-Anforderungen"](#).

4

Aktivieren Sie das Übersichts-Dashboard

Aktivieren Sie das Übersichts-Dashboard, um den Zustand, die Kapazität und den Durchsatz Ihrer FSx for ONTAP Cluster zu überwachen. Bestätigen Sie die Zustimmungsanfrage, damit Workload Factory mit der Erfassung von CloudWatch Metriken beginnen kann.

["Erfahren Sie, wie Sie das Übersichts-Dashboard aktivieren"](#).

5

Konfigurieren Sie das Projects-Dashboard

Konfigurieren Sie das Projects-Dashboard, um Systemzustand, Leistung und Speichernutzung zu überwachen und so Ihre EDA-Umgebung effektiv zu optimieren.

["Erfahren Sie, wie Sie das Projects-Dashboard konfigurieren."](#)

6

FSx für ONTAP Latenzanalyse konfigurieren

Latenzschwellenwerte können eingerichtet werden, um Leistungsprobleme proaktiv zu identifizieren und zu beheben, bevor sie die Simulationslaufzeit beeinflussen. Warn- und kritische Benachrichtigungen lassen sich konfigurieren, E-Mail- oder SNS-Benachrichtigungen ermöglichen den Empfang von Echtzeit-Benachrichtigungen, automatisierte Basisanalysen können genutzt und optional KI-Analysen für komplexe Szenarien eingesetzt werden.

["Erfahren Sie, wie Sie die Latenzüberwachung konfigurieren"](#). Sobald Ereignisse erkannt wurden, können Sie ["Latenztrends analysieren"](#) das interaktive Diagramm verwenden.

7

Integrieren mit anderen Diensten

Integrieren Sie EDA mit anderen Diensten wie einem Serviceportal oder Perforce Helix Core mithilfe der Workload Factory REST API.

["Informationen zur Integration von EDA in Perforce"](#).

Was kommt als Nächstes?

- ["Latenzüberwachung für FSx für ONTAP konfigurieren"](#)
- ["Konfigurieren Sie das Projects-Dashboard"](#)
- ["Erfahren Sie mehr über EDA-Workloads"](#)
- ["Holen Sie sich Hilfe bei EDA"](#)

Workload Factory für EDA-Anforderungen

Vor der Verwendung von NetApp Workload Factory für EDA sollten NetApp Workload Factory und AWS ordnungsgemäß eingerichtet sein. Dazu gehören Ihre AWS-Anmeldeinformationen, ein bereitgestelltes FSx for ONTAP-Dateisystem und weitere Voraussetzungen.

Workload Factory-Anmeldung und -Konto

Sie müssen ["bei NetApp Console registrieren und anmelden."](#)

AWS Anmeldeinformationen und Berechtigungen

Sie müssen AWS-Zugangsdaten mit lesen/schreiben-Berechtigungen zu Workload Factory hinzufügen, was bedeutet, dass Sie Workload Factory für EDA im Modus *lesen/schreiben* verwenden werden.

Die Berechtigungen *Basic* und *Read-only* werden derzeit nicht unterstützt.



Für die Nutzung der Latenzüberwachungsfunktion, die CloudWatch-Metriken zur Analyse der Volumenleistung erfasst, werden auch AWS-Anmeldeinformationen benötigt. Benachrichtigungen über Latenzereignisse sind verfügbar, wenn die Benachrichtigungseinstellungen in den Workload Factory Einstellungen konfiguriert sind. Eine optionale KI-Analyse für komplexe Latenzszenarien ist verfügbar, wenn die von NetApp verwaltete KI-Analyse aktiviert ist. ["Erfahren Sie mehr über Latenzüberwachung"](#).

FSx for ONTAP Dateisystem

Sie benötigen mindestens ein FSx for ONTAP Dateisystem:

- EDA verwendet das Dateisystem zum Speichern der Projekte und Arbeitsbereiche, die Sie erstellen.

Dieses FSx for ONTAP Dateisystem muss FlexVol Volumes verwenden. FlexGroup Volumes werden nicht unterstützt.

- Sie müssen die AWS-Region, die VPC und das Subnetz kennen, in dem sich das AWS FSx for ONTAP Dateisystem befindet.
- Sie benötigen mindestens ein Volume im Dateisystem mit folgender Konfiguration:
 - Das Volume muss als NFS-Freigabe konfiguriert sein.
 - Das Dateisystem muss mit einem Link konfiguriert werden. ["Weitere Informationen zu Links"](#).
- Zu berücksichtigen sind die Tag-Schlüssel/Wert-Paare, die auf die AWS-Ressourcen angewendet werden sollen, die Teil dieses Deployment sind (optional).

["Informationen zum Erkennen oder Erstellen von FSx for ONTAP Dateisystemen."](#)

EDA-Speicherübersicht

Erfahren Sie mehr über das Übersichts-Dashboard in Workload Factory für EDA

Das Übersichts-Dashboard bietet IT-Administratoren eine zentrale Plattform zur Überwachung von EDA-Workloads über mehrere FSx for ONTAP Dateisysteme hinweg. Damit lassen sich Systemzustand und Auslastung schnell überprüfen, geeignete Speicherorte für neue Volumes oder Jobs auswählen, Volumes oder SVMs identifizieren, die möglicherweise verschoben werden müssen, sowie den Zeitpunkt erkennen, zu dem eine Kapazitäts- oder Durchsatzserhöhung erforderlich ist.

Überblick

Das Dashboard „Übersicht“ erfasst CloudWatch-Metriken für alle FSx for ONTAP-Dateisysteme, die mit Ihren konfigurierten AWS-Anmeldeinformationen verknüpft sind.

Es beinhaltet:

- **Cluster-Gesundheitsstatus:** Eine Zusammenfassung oben hebt Latenzereignisse, SSD-Auslastung, Durchsatzmodusstatus, Kapazitätsempfehlungen und ONTAP EMS-Ereignisse in Ihren Dateisystemen hervor.
- **Clustertabelle:** Eine durchsuchbare Tabelle, die Nutzung und Leistung für jedes Cluster anzeigt. Es besteht die Möglichkeit, die Daten zu filtern und zu sortieren, zwischen Seiten zu wechseln und sie als CSV-Datei zu exportieren.

Es hilft Ihnen:

- Neue Volumes platzieren und Workloads neu verteilen
- Kapazitäts- oder Durchsatzskalierung planen
- Überwachung des Clusterzustands im großen Maßstab

- Treffen Sie fundierte Entscheidungen über die Volumenplatzierung
- Identifizieren Sie Cluster, die sich ihren Kapazitätsgrenzen nähern

Dashboard-Komponenten

Cluster-Gesundheitsstatus

Der Clusterstatus bietet eine schnelle Übersicht über die Aktivität der von Ihnen ausgewählten Dateisysteme. Dies erscheint nur, wenn mindestens eine FSx for ONTAP Verbindung zu Ihren Dateisystemen besteht.

Der Gesundheitszustand umfasst folgende Bereiche:

Latenz

Zeigt die Anzahl der in den ausgewählten Dateisystemen gefundenen Latenzereignisse an. Diese Information erscheint nur, wenn die Latenzüberwachung aktiviert ist.

Elastizität des Dateisystems

- **SSD-Kapazität:** Zeigt, wie viele Dateisysteme Automate, Recommend oder None zur Verwaltung der SSD-Kapazität verwenden.
- **Durchsatz:** Zeigt, wie viele Dateisysteme Automate, Recommend oder None zur Durchsatzverwaltung verwenden.

ONTAP-Ereignisse

Zeigt die Anzahl der erkannten EMS-Ereignisse an, kategorisiert nach Kapazität, Verfügbarkeit & Schutz sowie Sicherheit & Sonstiges.

Clustertabelle

Die Clustertabelle bietet eine detaillierte Ansicht jedes FSx for ONTAP-Dateisystems, gefiltert nach Ihrer aktiven Region und Ihren AWS-Kontoeinstellungen. Die Daten werden aus CloudWatch-Metriken gewonnen.

Nutzen Sie die Tabelle, um:

- Identifizieren Sie Dateisysteme, die sich ihren Kapazitätsgrenzen nähern (Spalte „SSD-Nutzung“)
- Vergleichen Sie den Durchsatzbedarf mit der bereitgestellten Durchsatz-SKU (Spalte „Durchsatznutzung P99“)
- Leistungskennzahlen über mehrere Cluster hinweg verfolgen
- Prüfen Sie den Link-Konfigurationsstatus (Spalte „Zugehöriger Link“) – Die Gültigkeit der Verbindung wird täglich überprüft.
- Wählen Sie mehrere Cluster für Massenaktualisierungen von Parametern aus

Ein Dateisystem kann ausgewählt werden, um Clusterdetails einschließlich Clusterinformationen, SSD-Kapazitätswerte und das Diagramm „SSD-Kapazität im Zeitverlauf“ anzuzeigen.

SSD Kapazitätsmanagement

Managementmodi

Nur benachrichtigen (Empfohlen-Modus)

Workload Factory analysiert, wie Sie Ihre SSDs verwenden, und schlägt vor, wann die Kapazität erhöht werden sollte. Diese Vorschläge werden überprüft und es wird entschieden, ob sie angewendet werden.

Dadurch bleibt die volle Kontrolle über Kapazitätsänderungen erhalten, während dennoch von der automatisierten Analyse profitiert wird.

Automatisieren

Workload Factory fügt automatisch zusätzlichen SSD-Speicherplatz hinzu, sobald festgelegte Nutzungsgrenzen erreicht sind. Dies geschieht automatisch, sodass keine manuelle Arbeit erforderlich ist. Dies eignet sich gut für Umgebungen, die eine automatische Verwaltung bevorzugen.

Keine

Wenn das SSD Kapazitätsmanagement nicht aktiviert ist, gibt das System keine Kapazitätsempfehlungen ab und führt keine automatisierten Aktionen durch. Diese Option ist geeignet, wenn Sie die Kapazität selbst verwalten möchten.

SSD-Verwaltungsparameter

Parameter steuern, wie das Kapazitätsmanagementsystem Ihre SSD-Nutzung analysiert und darauf reagiert:

Schwellenwert (10-90%)

Der SSD-Auslastungsgrad, ab dem Kapazitätsempfehlungen oder Automatisierungsaktionen ausgelöst werden. Beispielsweise bedeutet ein Schwellenwert von 80 %, dass Empfehlungen oder Aktionen erfolgen, sobald die SSD-Auslastung 80 % erreicht. Diese Einstellung ist sowohl im Recommend- als auch im Automate-Modus verfügbar.

Rückblick (1-200 Stunden)

Der Zeitraum, der zur Analyse historischer SSD-Nutzungsmuster verwendet wird. Ein längerer Betrachtungszeitraum liefert mehr historischen Kontext für Kapazitätsentscheidungen. Nur im Automate-Modus verfügbar.

Vorschau (1-200 Stunden)

Der Zeitraum, der zur Prognose des zukünftigen Kapazitätsbedarfs verwendet wird. Ein längerer Prognosezeitraum plant das Kapazitätswachstum weiter in die Zukunft. Nur im Automate-Modus verfügbar.

Sie können diese Parameter für jedes Dateisystem einzeln festlegen oder die Massенbearbeitung verwenden, um dieselben Einstellungen auf mehrere Dateisysteme anzuwenden.

Durchsatzmanagement

Sie können das Verhalten der elastischen Durchsatzsteigerung für ein oder mehrere Dateisysteme konfigurieren.

Managementmodi

Nur benachrichtigen (Empfohlen-Modus)

Workload Factory bewertet die Durchsatzbelastung und stellt Empfehlungen zur Verfügung, die Sie anwenden können.

Automatisieren

Workload Factory erhöht den Durchsatz automatisch, wenn die konfigurierten Bedingungen erfüllt sind.

Keine

Wenn Sie die Durchsatzverwaltung nicht aktiviert haben, gibt das System keine Empfehlungen und führt keine automatisierten Aktionen durch. Diese Option ist geeignet, wenn Sie die Kapazität selbst verwalten möchten.

Durchsatzparameter

Der Dialog zur Durchsatzkonfiguration umfasst Folgendes:

- **Auslastungsschwelle** (50-100%, Standard 80%): Prozentsatz der Durchsatzauslastung, der Empfehlungen oder Automatisierungen auslöst.

Erweiterte Durchsatzparameter sind im erweiterbaren Abschnitt **Advanced configuration** verfügbar.

- **Auswertungszeitraum (Stunden)** (12-72 Stunden, Standard 24)
- **Überschrittene Kennzahlen (%)** (Standard 66%): Prozentualer Schwellenwert zur Feststellung eines Verstoßes
- **Zeitfenster für aufeinanderfolgende Verstöße (Stunden)** (1-5 Stunden, Standard 2)
- **Kennzahlen für aufeinanderfolgende Verstöße (%)** (Standardwert 95%)
- **Minimale Latenz (ms)** (Standard 10 ms)
- **SKU mit maximalem Durchsatz** (Standard None)

Empfehlungen zur Elastizität des Dateisystems

Wenn Workload Factory sich im Automate- oder Recommend-Modus befindet, überprüft es automatisch jedes FSx for ONTAP Dateisystem und führt einen Kapazitätsempfehlungsalgorithmus aus. Das System scannt regelmäßig, um festzustellen, ob die SSD-Kapazität oder der Durchsatz angepasst werden sollte.

Wenn eine Empfehlung identifiziert wird:

- Sie erhalten eine sofortige Benachrichtigung basierend auf Ihren Workload Factory Benachrichtigungseinstellungen.
- Dateisysteme mit Empfehlungen lassen sich durch Filtern der Tabelle „Cluster“ identifizieren.
- Die Benutzeroberfläche zeigt die Gesamtzahl der Dateisysteme an, für die aktuell aktive Empfehlungen vorliegen.

Die Empfehlung erläutert die vorgeschlagene Änderung und deren Begründung, beispielsweise: *Wir empfehlen, die SSD-Größe basierend auf Ihrem SSD-Nutzungsmuster des Dateisystems zu erhöhen.*

Benachrichtigungen werden für Ereignisse zur Storage Kapazität gesendet, darunter Empfehlungen, erfolgreiche Kapazitätserhöhungen, Warnmeldungen und Fehler bei Kapazitätsprüfungen oder Erhöhungsvorgängen. Fehlerbenachrichtigungen erläutern die Ursache, z. B. fehlende Berechtigungen, eine bereits laufende Dateisystemaktualisierung, eine AWS-Wartezeit nach einer kürzlich erfolgten Storage Änderung, das Erreichen der maximalen Kapazität oder nicht verfügbare CloudWatch Daten.

Kapazitätsentscheidungspunkte verstehen

Das SSD-Nutzungsdiagramm zeigt an, wann das System Kapazitätsempfehlungen ausgesprochen oder automatische Maßnahmen ergriffen hat. Diese Markierungen zeigen, wie sich der Kapazitätsmanagement-Algorithmus im Zeitverlauf verhalten hat.

Empfehlungsentscheidungspunkte

Diese Punkte erscheinen, wenn das System erkennt, dass mehr SSD-Kapazität benötigt wird. Wenn die Kapazität nicht erhöht wurde, können diese Punkte bis zu alle 30 Minuten erscheinen. Das Diagramm zeigt jeden Entscheidungspunkt, wenn möglich. Wenn der gewählte Zeitraum zu dicht ist, werden die Punkte zusammengefasst.

Entscheidungspunkte für die Automatisierung

Diese Meldungen erscheinen, wenn das Automatisierungssystem versucht, die SSD-Kapazität zu erhöhen. Sie zeigen, ob die Aktion erfolgreich war oder fehlgeschlagen ist.

Das SSD-Nutzungsverlaufsdiagramm dient dazu:

- Anzeigen, wie oft die Speichergröße geändert werden muss
- Es kann festgestellt werden, ob der Automatisierungsmodus oder der Empfehlungsmodus besser zu den Nutzungsmustern passt.
- Wiederholte Speicherengpässe erkennen
- Zukünftiger Speicherbedarf kann auf Grundlage des Wachstums im Zeitverlauf geplant werden.
- Untersuchung der Gründe für das Scheitern der Automatisierungsversuche

Verwandte Informationen

- ["Aktivieren Sie das Übersichts-Dashboard"](#)
- ["Nutzen Sie das Übersichts-Dashboard"](#)

Aktivieren Sie das Übersichts-Dashboard in Workload Factory für EDA

Das Übersichts-Dashboard kann aktiviert werden, um CloudWatch-Metriken für Ihre FSx for ONTAP Dateisysteme zu erfassen. Im Dashboard werden Clusterzustand, Kapazität und Durchsatz an einem Ort angezeigt.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen, bevor Sie das Dashboard aktivieren.

AWS-Anmeldeinformationen mit Ansichtsberechtigungen

Sie müssen in Workload Factory AWS-Anmeldeinformationen mit mindestens Leseberechtigungen (View) für General Storage konfigurieren. *View, planning, and analysis* Anmeldeinformationen werden nicht unterstützt, da sie nicht die erforderlichen Leseberechtigungen für CloudWatch Metriken enthalten.

Wenn Sie keine Anmeldeinformationen mit Anzeigeberechtigungen konfiguriert haben, werden Sie beim Öffnen der Registerkarte „Übersicht“ auf die AWS-Anmeldeinformations-Einrichtungsseite weitergeleitet.

Wenn Sie noch keine AWS-Zugangsdaten konfiguriert haben, siehe ["AWS-Anmeldeinformationen hinzufügen"](#).

Dashboard aktivieren

Nachdem Workload Factory die Anmeldeinformationen mit Ansichtsberechtigungen überprüft hat, wird das Dashboard aktiviert, um CloudWatch-Metriken für Ihre FSx for ONTAP Dateisysteme zu erfassen.



Nachdem Sie Ihre Einwilligung erteilt haben, kann die Erfassung der Messwerte etwas Zeit in Anspruch nehmen. Das Dashboard benachrichtigt Sie, während die erste Erfassung läuft.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > EDA**.

3. Wählen Sie die Registerkarte **Overview** aus.
4. Falls keine Anmeldeinformationen mit Leseberechtigungen gefunden werden, wählen Sie **Anmeldeinformationen hinzufügen** und folgen Sie den Anweisungen, um AWS-Anmeldeinformationen mit Leseberechtigungen zu konfigurieren. Kehren Sie anschließend zur Registerkarte **Übersicht** zurück.
5. Lesen Sie die Zustimmungsaufforderung, in der die CloudWatch-Metriken beschrieben werden, die für Ihre FSx for ONTAP Dateisysteme erfasst werden.
6. Wählen Sie **Activate**, um das Dashboard zu aktivieren und mit der Metrikenerfassung zu beginnen.

Ergebnis

Workload Factory beginnt mit der Erfassung von CloudWatch Metriken für alle FSx for ONTAP Dateisysteme, die mit Ihren AWS-Anmeldeinformationen verknüpft sind. Das Dashboard wird aktualisiert, sobald die Metriken verfügbar sind. Während der Datenerfassung erscheint eine Benachrichtigung.

Nächste Schritte

Nach der Aktivierung des Dashboards können Sie:

- ["Nutzen Sie das Übersichts-Dashboard"](#) um den Zustand und die Kapazität des Clusters zu überwachen
- ["SSD-Kapazitätsmanagementmodi aktivieren und konfigurieren"](#) (Empfehlen, Automatisieren oder Keine)
- ["Durchsatzmanagementmodi aktivieren und konfigurieren"](#) (Empfehlen, Automatisieren oder Keine)
- Richten Sie Filter ein, um sich auf bestimmte Regionen oder AWS accounts zu konzentrieren.

Nutzen Sie das Übersichts-Dashboard in Workload Factory für EDA

Das Übersichts-Dashboard bietet eine Übersicht über den Zustand und die Kapazität Ihrer FSx for ONTAP Dateisysteme. Eine Filterung der Daten, das Anzeigen von Kapazitätsempfehlungen, das Anpassen von SSD- und Durchsatzeinstellungen sowie das Überprüfen von Leistungstrends unterstützen bei der Entscheidung, wo Volumes platziert werden und wann eine Kapazitätserweiterung sinnvoll ist.

Bevor Sie beginnen

Sie müssen ["Das Übersichts-Dashboard wurde aktiviert"](#) haben, bevor Sie es zur Überwachung Ihrer Dateisysteme verwenden können.

Dashboard filtern

Verwenden Sie die Filter oben im Dashboard, um bestimmte Dateisysteme anzuzeigen. Die Filter gelten für die Abschnitte Latenz, Auslastung, ONTAP-Ereignisse und die Clustertabelle.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > EDA**.
3. Wählen Sie die Registerkarte **Overview** aus.
4. Nutzen Sie die verfügbaren Filter, um Ihre Ansicht einzugrenzen:
 - **AWS-Konten:** Filtern Sie nach einem oder mehreren AWS-Konten, die mit Ihren konfigurierten Anmeldeinformationen verknüpft sind

- **Anmeldeinformationen:** Filtern Sie nach bestimmten AWS-Anmeldeinformationen, falls Sie mehrere konfiguriert haben
 - **Regionen:** Filtern Sie nach einer oder mehreren AWS-Regionen
5. Wenn Sie die Filterauswahl aktualisieren, werden alle Informationen aktualisiert, sodass nur die übereinstimmenden Dateisysteme angezeigt werden.

Cluster-Gesundheitsstatus anzeigen

Ganz oben im Dashboard wird eine Zusammenfassung des Zustands und der Aktivität der ausgewählten Dateisysteme angezeigt. Dies erscheint nur, wenn mindestens eine FSx for ONTAP Verbindung zu Ihren Dateisystemen besteht.

Über diese Aufgabe

Der Gesundheitszustand des Clusters umfasst folgende Schlüsselbereiche:

- **Latenz:** Anzahl der erkannten Latenzereignisse
- **Elastizität des Dateisystems:**
 - **SSD-Kapazität:** Zeigt, wie viele Dateisysteme Automate, Recommend oder None zur Verwaltung der SSD-Kapazität verwenden.
 - **Durchsatz:** Zeigt, wie viele Dateisysteme Automate, Recommend oder None zur Durchsatzverwaltung verwenden.
- **ONTAP-Ereignisse:** Anzahl der EMS-Ereignisse nach Kategorie (Kapazität, Verfügbarkeit & Schutz, Sicherheit & Sonstiges)

Schritte

1. Überprüfen Sie den Cluster-Gesundheitsstatus oben im Dashboard.
2. So zeigen Sie Latenzereignisse an:
 - Wählen Sie **Überprüfen**, um zur Registerkarte **Latenz** zu gelangen.
 - Wenn die Latenzüberwachung nicht konfiguriert ist, wählen Sie **Konfigurieren**, um Latenzschwellenwerte festzulegen

Weitere Informationen zur Latenzüberwachung finden Sie unter "[Latenzüberwachung konfigurieren](#)".

3. Um ONTAP-Ereignisse für Ihre FSx for ONTAP-Dateisysteme anzuzeigen, wählen Sie **Review**.

Die ONTAP-Ereignisansichtskarte zeigt die Anzahl der EMS-Ereignisse nach Kategorie (Kapazität, Verfügbarkeit & Schutz sowie Sicherheit & Sonstiges) an. Eine vollständige Liste der überwachten EMS-Ereignisse finden Sie unter "[ONTAP CLI-Dokumentation](#)".

Kapazitäts- oder Durchsatzempfehlungen anzeigen und anwenden

Workload Factory führt automatisch Empfehlungen für jedes FSx for ONTAP Dateisystem durch. Dateisysteme mit Empfehlungen lassen sich durch Filtern der Clusters-Tabelle finden.

Schritte

1. In der Tabelle **Cluster** nach den relevanten Zeit- oder Detailspalten filtern.

Dateisysteme mit Kapazitäts- oder Durchsatzempfehlungen erscheinen oben in der Tabelle.

2. Ein Dateisystemname in der Tabelle öffnet die Clusterdetails.

3. Die Empfehlung und die Grafik werden angezeigt.

Die Empfehlung erläutert die vorgeschlagene Änderung und die Begründung dafür. Zum Beispiel: *Wir empfehlen, die SSD-Größe basierend auf Ihrem SSD-Nutzungsmuster des Dateisystems zu erhöhen.*

Die Grafik zeigt die aktuelle Nutzung zusammen mit den historischen Trends.

4. Wählen Sie oben rechts im Diagramm den Zeitraum aus, um die angezeigte Periode zu ändern.

Das Diagramm zeigt außerdem Empfehlungs- und Automatisierungsentscheidungspunkte an (sofern der Automatisierungsmodus aktiviert ist). Bewegen Sie den Mauszeiger über einen Entscheidungspunkt, um Details zur Kapazitätsempfehlung oder Automatisierungsaktion in diesem Moment anzuzeigen.

5. Um die Empfehlung umzusetzen, befolgen Sie die in der Empfehlungsmitteilung enthaltenen Anweisungen.

SSD-Verwaltungsmodus ändern

Für jedes Dateisystem kann festgelegt werden, wie die SSD-Kapazität verwaltet wird: manuelle Empfehlungen erhalten oder automatische Skalierung zulassen.

Schritte

1. Suchen Sie in der Tabelle „Cluster“ den Dateisystemnamen. Öffnen Sie daneben **...** und wählen Sie **SSD-Kapazitätsmanagement ändern** aus.
2. **SSD Kapazitätsmanagement aktivieren** auswählen und anschließend **Anwenden** auswählen.
3. Wählen Sie Ihren bevorzugten Modus:
 - **Nur benachrichtigen (Empfohlen-Modus)**
 - **Automatisieren**
4. Die Parameter für das SSD-Kapazitätsmanagement konfigurieren:
 - **Schwellenwert (%)**: SSD-Auslastung in Prozent, die eine Empfehlung auslöst
 - **Rückblick (%)**: Historische Nutzungsdatenperiode für die Analyse
 - **Vorausschau (%)**: Prognostizierte Nutzung für die zukünftige Kapazitätsplanung
5. **Anwenden** auswählen.

Ergebnis

Das Dateisystem wechselt sofort in den neuen Modus. Bei Auswahl von „Empfehlen“ oder „Automatisieren“ verwendet das System die festgelegten Einstellungen, um die Speicherkapazität zu analysieren und Entscheidungen zu treffen.

Durchsatzmanagementmodus ändern

Für jedes Dateisystem kann festgelegt werden, wie die Durchsatzsteigerung verwaltet wird.

Schritte

1. Auf der Registerkarte **Übersicht** sind in der Tabelle „Cluster“ ein oder mehrere Dateisysteme auszuwählen.
2. **Durchsatzmanagement ändern** auswählen.
3. **Durchsatzmanagement aktivieren** auswählen und dann **Anwenden** auswählen.
4. Wählen Sie Ihren bevorzugten Modus:

- **Nur benachrichtigen (Empfohlen-Modus)**

- **Automatisieren**

5. Im Dialog werden die Parameter für das Durchsatzmanagement konfiguriert:

- **Auswertungszeitraum (Stunden):** Zeitraum für die Analyse von Durchsatzmustern
- **Überschrittene Kennzahlen (%):** Prozentualer Schwellenwert zur Feststellung einer Überschreitung
- **Zeitraum aufeinanderfolgender Verstöße (Stunden):** Dauer aufeinanderfolgender Verstöße vor einer Maßnahme
- **Minimale Latenz (ms):** Latenzschwellenwert zur Bestimmung der Durchsatzsteigerung
- **Maximaler Durchsatz (SKUs):** Maximal zulässige SKU für den Durchsatz

6. **Anwenden** auswählen.

Ergebnis

Die ausgewählten Dateisysteme wechseln sofort in den neuen Durchsatzmodus.

Parameter für das Massенbearbeitungsmanagement

Einstellungen für mehrere Dateisysteme gleichzeitig ändern, sodass die gleichen Einstellungen für alle Cluster gelten.

Schritte

1. Wählen Sie auf der Registerkarte **Übersicht** die Dateisysteme aus, die Sie in der Tabelle bearbeiten möchten.



Sie können einzelne Dateisysteme auswählen oder mithilfe des Kontrollkästchens in der Kopfzeile alle sichtbaren Dateisysteme auswählen.

2. **SSD-Kapazitätsmanagement ändern** oder **Durchsatzmanagement ändern** oberhalb der Tabelle auswählen.
3. Wählen Sie Ihren bevorzugten Modus.
4. Im Bearbeitungsdialog können die Parameter nach Bedarf angepasst werden.

Jedes Parameterfeld enthält eine QuickInfo, die seinen Zweck und den gültigen Bereich beschreibt. Der Dialog zeigt die aktuellen Werte oder Standardwerte basierend auf Ihrer Auswahl an.

5. Wählen Sie **Anwenden**, um die Änderungen auf alle ausgewählten Dateisysteme anzuwenden.

Ergebnis

Die Parameter werden für alle ausgewählten Dateisysteme aktualisiert. Dateisysteme im Recommend- oder Automate-Modus verwenden die neuen Parameter sofort für Analysen und Entscheidungsfindung.

Analysieren Sie Kapazitätstrends und Entscheidungspunkte

Das SSD-Nutzungsdiagramm zeigt, wie sich die Speichernutzung im Laufe der Zeit verändert und ermöglicht das Erkennen von Mustern.

Über diese Aufgabe

Die Entscheidungspunkte im Diagramm zeigen an, wann:

- **Empfehlungsentscheidungspunkte:** Der Kapazitätsempfehlungsalgorithmus hat festgestellt, dass

zusätzliche SSD-Kapazität benötigt wird.

- **Automatisierungsentscheidungspunkte:** Das Automatisierungssystem hat versucht, die SSD-Kapazität zu erhöhen. Diese Punkte zeigen, ob die Aktion erfolgreich war oder fehlgeschlagen ist.

Schritte

1. Auf der Registerkarte **Übersicht** wird in der Tabelle ein Dateisystemname ausgewählt.
2. Sehen Sie sich das SSD-Nutzungsdiagramm an, das die historischen Kapazitätstrends aufzeigt.
3. Wählen Sie verschiedene Zeiträume aus, um das Kapazitätsverhalten über verschiedene Zeiträume hinweg anzuzeigen.
4. Bewegen Sie den Mauszeiger über Entscheidungspunkte im Diagramm, um Details zu Empfehlungen oder Automatisierungsaktionen zu bestimmten Zeitpunkten anzuzeigen.
5. Nutzen Sie die Erkenntnisse aus dem Diagramm, um:
 - Verstehen, wie häufig Kapazitätsanpassungen erforderlich sind
 - Prüfen Sie, ob der Automatisierungs- oder der Empfehlungsmodus besser zu Ihren Arbeitslastmustern passt
 - Wiederkehrende Kapazitätsengpässe identifizieren
 - Planen Sie zukünftigen Kapazitätsbedarf basierend auf Wachstumstrends
 - Fehlerbehebung bei fehlgeschlagenen Automatisierungsversuchen

Häufige Fehlerursachen sind: unzureichende AWS-Berechtigungen, ein bereits laufendes Dateisystem-Update, innerhalb der letzten 6 Stunden geänderter Storage, Erreichen der maximalen SSD-Kapazität oder nicht verfügbare CloudWatch Metriken.

Verwenden Sie die Clustertabelle

Die Clustertabelle bietet eine detaillierte Übersicht über jedes FSx for ONTAP Dateisystem mit Leistungs- und Nutzungsmetriken.

Schritte

1. Überprüfen Sie auf der Registerkarte **Übersicht** die Clustertabelle.
2. Verwenden Sie das Suchfeld, um bestimmte Dateisysteme anhand ihres Namens zu finden.
3. Wählen Sie Spaltenüberschriften aus, um die Daten zu sortieren.
4. Verwenden Sie die **SSD-Auslastung**, um Dateisysteme zu identifizieren, die sich ihrer Kapazitätsgrenze nähern.
5. Verwenden Sie die **Durchsatzauslastung (P99)**, um den Durchsatzbedarf mit der bereitgestellten Durchsatz-SKU zu vergleichen.

Bewegen Sie den Mauszeiger über die Durchsatz-Spaltenüberschriften, um Berechnungsdetails anzuzeigen.

6. Um Spalten anzupassen, wählen Sie das Symbol für die Spalteneinstellungen und wählen Sie aus, welche Spalten angezeigt werden sollen.
7. Um Daten zu exportieren, wählen Sie das Export-Symbol, um eine CSV-Datei herunterzuladen.

Best Practices

Beachten Sie diese Empfehlungen bei der Verwendung des Übersichts-Dashboards:

- **Regelmäßige Überwachung:** Das Dashboard sollte regelmäßig überprüft werden, um Trends zu erkennen, bevor sie zu Problemen werden.
- **Klare Schwellenwerte festlegen:** SSD-Nutzungsschwellenwerte und Durchsatzparameter auswählen, die zur jeweiligen Arbeitslast und zu den Kapazitätsplänen passen.
- **Filter verwenden:** Regions- und Kontofilter können angewendet werden, um sich auf die Teile der Infrastruktur zu konzentrieren, die überprüft werden sollen.
- **Empfehlungen schnell prüfen:** Die Tabelle „Cluster“ kann gefiltert werden, um Dateisysteme mit Kapazitäts- oder Durchsatzempfehlungen zu finden. Diese können überprüft und entsprechende Maßnahmen ergriffen werden, um Speicherplatzmangel zu vermeiden.
- **Den richtigen Modus wählen:** Der Modus **Empfehlen** eignet sich, wenn Kapazitäts- oder Durchsatzänderungen selbst genehmigt werden sollen. Der Modus **Automatisieren** ist geeignet, wenn das System Kapazität oder Durchsatz automatisch verwalten soll.
- **Entscheidungspunkte beobachten:** Entscheidungspunkte in den Kapazitätsdiagrammen prüfen, um zu sehen, wie das System Entscheidungen trifft, und bestätigen, dass die Einstellungen für die eigenen Anforderungen geeignet sind.
- **Massenbearbeitung:** Bei der Verwaltung vieler Dateisysteme sorgt die Massenbearbeitung für konsistente Einstellungen.

Verwandte Informationen

- ["Erfahren Sie mehr über das Overview Dashboard"](#)
- ["Aktivieren Sie das Übersichts-Dashboard"](#)
- ["Latenzüberwachung konfigurieren"](#)

Projektnutzungsanalyse

Erfahren Sie mehr über das Projects-Dashboard in Workload Factory für EDA

Das Projects Dashboard ermöglicht IT-Administratoren und Projektmanagern die Übersicht darüber, wie Projekte Speicher in FSx for ONTAP File Systems und Volumes nutzen. Es zeigt Speichernutzungsmuster an, sodass Projekte mit dem höchsten Ressourcenverbrauch erkannt, Kosten nachverfolgt und der Speicher angepasst werden können, bevor Kapazitäts- oder Leistungsprobleme EDA-Simulationen beeinträchtigen.

So funktioniert das Projekt-Dashboard

Das Dashboard „Projekte“ zeigt CloudWatch Kennzahlen für alle FSx for ONTAP Volumes an, die mit Ihren AWS-Anmeldeinformationen verknüpft sind. Es können bis zu fünf Filter mithilfe von AWS-Tags erstellt werden, um die Daten nach Projekt, Team, Anwendung oder anderen Kategorien zu organisieren und anzuzeigen.

Das Dashboard hilft Ihnen dabei:

- Kapazität planen und Kosten verstehen
- Daten dienen als Grundlage für Entscheidungen zur Ressourcenzuweisung.
- Projekte mit hohem Ressourcenverbrauch erkennen
- Kosten nach Projekt oder Team nachverfolgen
- Speicher anpassen, bevor Probleme auftreten

Für die proaktive Überwachung der Latenzleistung siehe ["Erfahren Sie mehr über Latenzüberwachung"](#).

Erfasste CloudWatch-Metriken

Das Dashboard erfasst und zeigt die folgenden CloudWatch Kennzahlen an:

- **Bereitgestellte Kapazität:** Metrik auf Volumenebene, die die bereitgestellte Speicherkapazität darstellt.
- **Ausgenutzte Kapazität:** Metrik auf Volumenebene, die den genutzten Speicher darstellt.
- **Durchschnittlicher/Maximaler Durchsatz:** Berechnet als Durchschnitt bzw. Maximum der Summe von DataReadBytes und DataWriteBytes über den angegebenen Zeitraum.
- **Durchschnittliche/Maximale IOPS:** Berechnet als Durchschnitt bzw. Maximum der Summe von DataReadOperations, DataWriteOperations und MetadataOperations über den angegebenen Zeitraum.

Benutzerdefinierte Filter

Benutzerdefinierte Filter helfen dabei, Dashboard-Daten so zu organisieren, dass sie den Arbeitsabläufen Ihres Unternehmens entsprechen. Filter können nach Projekt, Team oder Kostenstelle gesetzt werden, sodass die benötigten Daten schnell gefunden werden, ohne irrelevante Informationen durchsuchen zu müssen. Dadurch wird die Kapazitätsplanung, Kostenverfolgung und Leistungsüberwachung erleichtert.

Sie können bis zu fünf benutzerdefinierte Filter basierend auf Ihren AWS-Tags konfigurieren.

- **Filterbezeichnung:** Der Name, der im Dashboard angezeigt wird
- **AWS-Tag-Schlüsselname:** Der tatsächliche AWS-Tag-Schlüssel, der auf Ihren Ressourcen verwendet wird
- **Auswahltyp:** Einzelauswahl oder Mehrfachauswahl

Wenn Sie keine benutzerdefinierten Filter konfigurieren, stehen die Standardfilter Dateisystem, Volume-Typ und Zeitbereich weiterhin zur Verfügung, sodass Sie Ihre Dashboards anzeigen und verwenden können.

AWS-Tags

AWS-Tags sind Metadaten für Ihre AWS-Ressourcen. Sie helfen Ihnen, Ihre AWS-Ressourcen auf verschiedene Weise zu kategorisieren, beispielsweise nach Projekt, Anwendung oder Geschäftsbereich.

Um benutzerdefinierte Filter zu verwenden, fügen Sie Ihren FSx for ONTAP Volumes AWS-Tags hinzu, die Ihren Anforderungen entsprechen, z. B. Tags für Projekte, Teams oder Geschäftsbereiche.

Weitere Informationen zum Taggen finden Sie unter ["Was sind Tags?"](#) und ["AWS Resource Groups Tagging API Referenz"](#).

Volumendetails

Das Dashboard bietet verschiedene Ansichtsmodi, mit denen Sie Ihre Speichermetriken auf unterschiedlichen Detailebenen analysieren können.

Gesamtansicht

Die Gesamtansicht (Standard) zeigt kombinierte Metriken für alle Volumes an, die Ihren ausgewählten Filtern entsprechen. Sie bietet einen schnellen Überblick über die gesamte Speicherleistung, einschließlich Gesamtkapazität, IOPS und Durchsatz.

Nutzen Sie diese Ansicht, um:

- Allgemeine Trends verstehen
- Planen Sie für den zukünftigen Kapazitätsbedarf
- Bericht über den gesamten Ressourcenverbrauch in allen Projekten oder Teams

Volumenansicht

Die Volumenansicht zeigt, wie einzelne Volumes im Zeitverlauf arbeiten. Es werden die Top 10 Volumes für jede Metrik angezeigt. Dies erleichtert die Übersicht darüber, welche Volumes die meisten Ressourcen nutzen und wie sie sich im ausgewählten Zeitraum verhalten.

Nutzen Sie diese Ansicht, um:

- Ermitteln, was die Leistung verlangsamt
 - Speichervolumes identifizieren, bei denen möglicherweise eine Größenanpassung erforderlich ist
 - Anzeigen, welche Projekte oder Arbeitslasten die meisten Ressourcen verwenden

Volumenmetriken angezeigt

Wenn Sie einzelne Volumes anzeigen, zeigt das Dashboard die Top 10 Volumes aus Ihrer Gesamtzahl an Volumes für jede Kennzahl an:

- **Verwendete Kapazität des Volumens:** Zeigt Volumen mit der aktuell höchsten verwendeten Kapazität an.
- **IOPS:** Zeigt Volumes mit den höchsten durchschnittlichen IOPS im ausgewählten Zeitraum an.
- **Durchsatz:** Zeigt die Volumes mit dem höchsten durchschnittlichen Durchsatz im ausgewählten Zeitraum an.



Das Dashboard zeigt nur die Top 10 Volumes für jede Kennzahl an. Wenn Sie mehr als 10 Volumes haben, werden einige Volumes möglicherweise nicht in der Detailansicht angezeigt.

Wenn in mehreren Metriken die gleichen Volumes vorkommen, verwendet das Dashboard in der Legende die gleichen Farben, sodass diese Volumes in den verschiedenen Metriken leicht nachverfolgt werden können.

Interaktive Volumendaten

Fahren Sie mit dem Mauszeiger über das Diagramm, um die genauen Werte zu bestimmten Zeitpunkten anzuzeigen. Dies erleichtert die Verknüpfung von Leistungsänderungen mit Ereignissen oder Zeiträumen. Die detaillierten Daten können dabei unterstützen, Leistungsprobleme zu erkennen, die Wirksamkeit von Optimierungen zu bestätigen und anderen die Ressourcennutzung zu erläutern.

Wenn Sie mit dem Mauszeiger über eine beliebige Volumenlinie in den Diagrammen fahren, können Sie Folgendes anzeigen:

- **Ausgenutzte Kapazität des Volumens:** Volumenname, genutzte Kapazität zu diesem Zeitpunkt und zugewiesene Kapazität
- **IOPS:** Name des Volumens, durchschnittliche IOPS für den Zeitraum und maximale IOPS für den Zeitraum
- **Durchsatz:** Volume-Name, durchschnittlicher Durchsatz für den Zeitraum und maximaler Durchsatz für den Zeitraum

Verwandte Informationen

- ["Konfigurieren Sie das Projects-Dashboard"](#)
- ["Nutzen Sie das Projekt-Dashboard"](#)

Konfigurieren Sie das Projects-Dashboard in Workload Factory für EDA

Im Projekt-Dashboard lassen sich benutzerdefinierte Filter einrichten, um Daten so zu organisieren, dass sie den Geschäftsprozessen entsprechen, zum Beispiel nach Projekt, Team oder Kostenstelle. Dadurch werden Kosten übersichtlicher dargestellt, es lässt sich erkennen, welche Ressourcen die meiste Kapazität nutzen, und fundiertere Entscheidungen zu Budgets und Personal können getroffen werden. Wenn die Filter der Struktur Ihrer Organisation entsprechen, lassen sich die benötigten Daten schnell finden und Kapazität, Kosten sowie Leistung effizienter verwalten.

Bevor Sie beginnen

Um benutzerdefinierte Filter zu verwenden, AWS-Tags zu Ihren FSx for ONTAP Volumes entsprechend Ihren Anforderungen hinzufügen, wie zum Beispiel Tags für Projekte, Teams oder Geschäftsbereiche.

Benutzerdefinierte Filter konfigurieren



Nur der erste Administrator, der das Projects Dashboard öffnet, kann benutzerdefinierte Filter erstellen, ändern oder löschen. Alle anderen Benutzer, einschließlich anderer Administratoren, können die Filter nur anzeigen.

Über diese Aufgabe

Sie können bis zu fünf benutzerdefinierte Filter mithilfe Ihrer AWS-Tags konfigurieren. Jeder Filter benötigt Folgendes: eine Filterbezeichnung, einen AWS-Tag-Schlüssel und einen Auswahltyp (einzeln oder mehrfach).

Wenn Sie keine benutzerdefinierten Filter konfigurieren, stehen Ihnen die Standardfilter, Dateisystem, Volume-Typ und Zeitbereich weiterhin zur Verfügung, sodass Sie Ihre Dashboards weiterhin anzeigen und verwenden können.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > EDA**.
3. Wählen Sie **Projekte** aus.

Falls Sie Ihr Dashboard noch nicht konfiguriert haben, werden Sie automatisch dazu aufgefordert.

4. **Filter hinzufügen** auswählen.
5. Fügen Sie für jeden benutzerdefinierten Filter, den Sie erstellen möchten, die Details hinzu:
 - Filterbezeichnung (der Anzeigename im Dashboard)
 - AWS-Tag-Schlüsselname (der tatsächliche Tag-Schlüssel, der für Ihre Ressourcen verwendet wird)
 - Auswahltyp (Einzel- oder Mehrfachauswahl)



Die Filter werden im Dashboard in der von Ihnen festgelegten Reihenfolge angezeigt.

Die am häufigsten verwendeten Filter sollten oben platziert werden, damit sie leichter zugänglich sind.

6. **Anwenden** auswählen.

Sie können einen benutzerdefinierten Filter löschen, indem Sie das Papierkorbsymbol neben diesem Filter auswählen, bevor Sie Ihre Änderungen anwenden.

7. Um Ihre Änderungen nach dem Anwenden von Tags oder Filtern anzuzeigen, wählen Sie das Aktualisierungssymbol im Dashboard aus.

8. Die spätere Bearbeitung der Dashboard Konfiguration erfolgt über **Configure**.

Ergebnis

Wenn diese Tags angewendet werden, beginnt Workload Factory mit dem Sammeln und Anzeigen der zugehörigen CloudWatch-Metriken. Das Dashboard unterstützt bei der Organisation von Ressourcen, der Nachverfolgung von Kosten und dem Filtern von Elementen entsprechend der jeweiligen Anforderungen.

Verwandte Informationen

- ["Erfahren Sie mehr über das Projects-Dashboard"](#)
- ["Nutzen Sie das Projekt-Dashboard"](#)

Nutzen Sie das Projekt-Dashboard in Workload Factory für EDA

Das Projects Dashboard bietet eine Übersicht über die Speichernutzung Ihrer FSx for ONTAP File Systems und Volumes. Die Daten lassen sich nach Projekt, Team oder Anwendung filtern. Sowohl die Gesamtleistung als auch die Leistung pro Volume werden angezeigt, was die Kapazitätsplanung unterstützt und eine effizientere Ressourcennutzung ermöglicht.

Bevor Sie beginnen

Sie sollten ["konfigurierte benutzerdefinierte Filter"](#) für das Projekt-Dashboard haben. Falls Sie keine benutzerdefinierten Filter konfiguriert haben, können Sie weiterhin die Standardfilter (Dateisystem, Volume-Typ und Zeitbereich) verwenden.

Dashboard filtern

Durch Filter können Sie sich auf bestimmte Gruppen von Speicherressourcen konzentrieren. Dies erleichtert das Erkennen von Trends, das Auffinden von Problemen und das Erstellen von Berichten für Stakeholder. Durch die Kombination mehrerer Filter lassen sich gezielte Fragen beantworten, wie zum Beispiel: „Wie viel Speicher verwendet das ASIC project team?“ oder „Welche Volumes in der US-West Region haben die höchsten IOPS?“

Über diese Aufgabe

Sie können die auf dem Dashboard angezeigten Informationen mithilfe einer Kombination aus Standardfiltern und von Ihnen konfigurierten benutzerdefinierten Filtern filtern.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
- 2.

Die Auswahl erfolgt im Menü , **Workloads > EDA**.

3. Wählen Sie **Projekte** aus.
4. Wählen Sie die Filter aus, die Sie aus den verfügbaren Optionen anwenden möchten:
 - Standardfilter (Dateisystem, Volume-Typ, Zeitbereich)
 - Alle von Ihnen konfigurierten benutzerdefinierten Filter
5. Wählen Sie das Aktualisierungssymbol, um die Dashboard-Informationen basierend auf Ihren Filterauswahlen zu aktualisieren.
6. Eine Erläuterung der auf einer Karte angezeigten Informationen erhalten Sie, indem Sie das Informationssymbol dieser Karte auswählen.

Volumendetails anzeigen

Die Betrachtung sowohl der Gesamtleistung des Volumens als auch der einzelnen Volumina hilft bei der Kapazitätsplanung und Leistungsverbesserung. Die Gesamtansicht zeigt allgemeine Trends. Die Volumenansicht ermöglicht das Auffinden bestimmter Volumina, die möglicherweise Aufmerksamkeit, Optimierung oder zusätzliche Ressourcen benötigen.

Aggregierte Volumenstatistiken anzeigen

Die Gesamtansicht zeigt kombinierte Kennzahlen für alle Volumen, die Ihren Filtern entsprechen.

Schritte

1. Nach dem Öffnen des Tabs **Projects** sollte der Tab **Total** ausgewählt sein. Dies ist die Standardansicht.
2. Überprüfen Sie die angezeigten Kennzahlen:
 - Gesamtkapazität über alle Volumina hinweg
 - Aggregierte IOPS
 - Aggregierter Durchsatz
3. Diese Ansicht zeigt Trends und unterstützt die Planung des zukünftigen Kapazitätsbedarfs.

Anzeige der individuellen Volume-Performance

Die Volumenansicht zeigt, wie jedes Volumen im Zeitverlauf arbeitet. Es werden die zehn wichtigsten Volumina für jede Kennzahl hervorgehoben.

Schritte

1. Auf der Registerkarte **Projects** die Registerkarte **Volume** auswählen.
2. Überprüfen Sie die Volumen Kennzahlen:
 - **Verwendete Kapazität des Volumens:** Zeigt Volumen mit der höchsten aktuell verwendeten Kapazität an
 - **IOPS:** Zeigt die Volumes mit den höchsten durchschnittlichen IOPS im ausgewählten Zeitraum
 - **Durchsatz:** Zeigt Volumes mit dem höchsten durchschnittlichen Durchsatz im ausgewählten Zeitraum an



Wenn Sie mehr als 10 Volumes haben, werden die übrigen nicht in der Detailansicht angezeigt.

3. Bewegen Sie den Mauszeiger über eine beliebige Volumenlinie in den Diagrammen, um detaillierte Informationen anzuzeigen:
 - **Ausgenutzte Kapazität des Volumes:** Volumenname, genutzte Kapazität zu diesem Zeitpunkt und zugewiesene Kapazität
 - **IOPS:** Name des Volumes, durchschnittliche IOPS für den Zeitraum und maximale IOPS für den Zeitraum
 - **Durchsatz:** Volume-Name, durchschnittlicher Durchsatz für den Zeitraum und maximaler Durchsatz für den Zeitraum
4. Mit der Legende lässt sich jedes Volume identifizieren. Die gleichen Volumes werden in allen Metriken mit denselben Farben dargestellt, sodass sie einfach nachverfolgt werden können.

Ergebnis

Diese Daten können verwendet werden, um:

- Nutzungsmuster analysieren
- Mögliche Engpässe erkennen
- Volumen finden, die möglicherweise in der Größe angepasst werden müssen
- Anzeigen, welche Projekte oder Arbeitslasten die meisten Ressourcen verwenden

Best Practices

Beachten Sie diese Empfehlungen bei der Verwendung des Projects-Dashboards:

- Das Dashboard sollte regelmäßig überprüft werden, damit Muster erkannt werden, bevor sie zu Problemen werden.
- Mehrere Filter können gleichzeitig verwendet werden, um spezifische Fragen zur Ressourcennutzung zu beantworten.
- Beide Ansichten bieten Vorteile: Total dient der Kapazitätsplanung, Volume hilft bei der Identifizierung und Behebung von Problemen.
- Den Zeitraum ändern, um zu erkennen, ob die Veränderungen normal sind oder Teil eines wachsenden Trends.
- Normale Leistungswerte werden aufgezeichnet, sodass ungewöhnliches Verhalten später leichter erkannt werden kann.
- Nutzen Sie die Erkenntnisse aus den Daten, um Ressourcen anzupassen, Volumes zu vergrößern oder die Leistung zu verbessern, bevor Arbeitslasten beeinträchtigt werden.

Verwandte Informationen

- ["Erfahren Sie mehr über das Projects-Dashboard"](#)
- ["Konfigurieren Sie das Projects-Dashboard"](#)
- ["Erfahren Sie mehr über Latenzüberwachung"](#)

Verwendung der Perforce Integration

Erfahren Sie mehr über die Perforce-Integration in Workload Factory für EDA

Die Integration von Perforce in CI/CD-Pipelines verbessert den Entwicklungsprozess

durch die Automatisierung von Builds, Tests und Deployments und führt so zu einer schnelleren und zuverlässigeren Softwarebereitstellung.

Continuous Integration und Continuous Deployment (CI/CD) in EDA ist ein Tool zur schnellen Erstellung von Entwicklungsumgebungen für Softwareentwickler. Es ermöglicht die schnelle Einrichtung persönlicher Entwicklungsumgebungen, spart Zeit und ermöglicht Selfservice für Entwickler, während DevOps Teams die Kontrolle über die Infrastruktur behalten. Mit CI/CD können Softwareentwickler schnell Arbeitsbereiche erstellen, ohne dass spezieller Storage oder Kenntnisse der Entwicklungsinfrastruktur erforderlich sind.

Was ist CI/CD?

Durch den Einsatz von CI/CD können Sie die Verwaltung und Interaktion der Entwickler mit verschiedenen Versionen ihrer Software optimieren. Es arbeitet mit Perforce Helix Core zusammen, um Softwareversionen sofort zu klonen und Arbeitsbereiche für Entwicklung, Qualitätssicherung und CI/CD zu erstellen.

Sie können ganz einfach ein Projekt erstellen und ein Volume zuweisen, das Ihre Softwareumgebung und deren Artefakte repräsentiert. Während Sie Ihre Software aktualisieren, können Sie Snapshots des Volumes erstellen, die den Zustand Ihrer Software zu diesem Zeitpunkt erfassen. Sie können sofort auf jede Softwareversion zugreifen, ohne erneut synchronisieren zu müssen, und sparen dadurch Zeit und Ressourcen.

Mithilfe der Snapshot- und Klonfunktionen von NetApp ONTAP können Sie schnell auf verschiedene Versionen Ihrer Software zugreifen und so Updates schneller entwickeln und veröffentlichen. Weitere Informationen zu Workload Factory finden Sie in der Dokumentation ["Workload Factory Übersicht"](#).

CI/CD-Funktionen

- Projekte erstellen, bearbeiten und entfernen. Weitere Informationen unter ["Projekte managen"](#).
- Snapshots definierter Softwareversionen erstellen. Siehe ["Projektversionen managen"](#).
- Arbeitsbereiche erstellen und löschen (basierend auf Klonen). Weitere Informationen unter ["Einen Arbeitsbereich erstellen"](#).
- Zugriffsrichtlinien ermöglichen die Steuerung des Zugriffs auf ein Projekt.
- Analyse der Kapazitätsauslastung jedes Projekts.
- Steuerung von Klongrößenbeschränkungen und der Klonaufbewahrung für jedes Projekt.
- Integration mit Versionskontrollsystemen wie Perforce. Weitere Informationen finden Sie unter ["Integration mit Perforce"](#).

Projekte und Arbeitsbereiche in EDA

Sie können ein Projekt erstellen und ein Volume zuweisen, das Ihre Softwareumgebung und deren Artefakte repräsentiert. Bei jeder neuen Softwareversion müssen Sie die Volume-Daten erneut synchronisieren und einen Projekt-Snapshot erstellen, um den Volume-Status als bekannte Version zu kennzeichnen. Das Projekt-Quellvolume kann fortlaufende Updates erhalten und mehrere Snapshots zur Kennzeichnung verschiedener Versionen enthalten. Jeder Snapshot kann sofort als instant clone verwendet werden, ein dediziertes oder gemeinsam genutztes, bearbeitbares Repository, das Entwicklern, QA oder Build-Prozessen zur Verfügung steht. Ein Klon im Kontext einer bestimmten Softwareversion ist ein workspace.

Automatisierung mit Workload Factory Codebox

Workload Factory führt mit der integrierten *Codebox* eine integrierte Automatisierung ein. Die Codebox bietet folgende Vorteile der Automatisierung:

- **Generierung von Code-Snippets:** Infrastructure-as-Code (IaC)-Snippets entstehen während der

Ressourcenerstellung und ermöglichen eine nahtlose Integration in bestehende Orchestrierungs-Workflows.

- **Infrastructure-as-code co-pilot:** Die Codebox ist ein Infrastructure-as-code (IaC) co-pilot, der Entwicklern und DevOps dabei hilft, Code zu generieren, um jeden von Workload Factory unterstützten Vorgang auszuführen.
- **Code-Viewer und Automatisierungskatalog:** Die Codebox bietet einen Code-Viewer zur schnellen Analyse von Automatisierung und einen Automatisierungskatalog zur schnellen späteren Wiederverwendung.

Kosten

Die Nutzung der CI/CD-Funktionalität von Workload Factory ist kostenlos.

Lizenzierung

Für die Nutzung der CI/CD-Funktionen von Workload Factory sind keine speziellen Lizenzen von NetApp erforderlich.

Regionen

EDA wird in allen kommerziellen Regionen unterstützt, in denen FSx for ONTAP unterstützt wird. "[Unterstützte Amazon Regionen](#)"

Die folgenden AWS-Regionen werden nicht unterstützt:

- China Regionen
- Secret Cloud
- Top Secret Cloud

Hilfe erhalten

Amazon FSx for NetApp ONTAP ist eine AWS Erstanbieterlösung. Für Support lässt sich im Support Center Ihrer AWS Management Console ein Fall öffnen. Dort werden "FSx for ONTAP" und die Kategorie ausgewählt, anschließend werden die erforderlichen Informationen angegeben.

Antworten auf allgemeine Fragen zu Workload Factory oder Workload Factory Anwendungen und Services finden sich in "[Hilfe zu EDA for Workload Factory](#)".

EDA-Projekte in Workload Factory für EDA verwalten

EDA-Projekte können verwaltet werden, um zu steuern, wie Ihr Code und Ihre Artefakte für jedes Projekt in NetApp Workload Factory for EDA gemanagt werden.

Ein Projekt erstellen

Sie können ein neues EDA-Projekt erstellen, um die Datenschutzfunktionen Ihres FSx for ONTAP Dateisystems für Ihren Code und Ihre Artefakte zu nutzen.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Die Auswahl erfolgt im Menü , **Workloads > EDA**.

3. Hier wird **CI/CD** ausgewählt.
4. Wählen Sie **Projekt hinzufügen** aus.
5. Auf der Seite „Projekt erstellen“ sind folgende Angaben erforderlich:
 - a. **Projektname**: Einen Namen für das Projekt eingeben.
 - b. **Beschreibung**: Eine Beschreibung für das Projekt eingeben.
 - c. **Dateisystem**: Folgendes ist anzugeben:
 - i. **Anmeldeinformationen**: Wählen Sie die zu verwendenden Amazon AWS-Anmeldeinformationen aus. EDA verwendet diese Anmeldeinformationen, um FSx for ONTAP-Dateisysteme zu ermitteln, die Sie mit diesem Projekt verwenden können, und um Klone und Snapshots von Projekten zu erstellen.
 - ii. **Region**: Wählen Sie die Region aus, in der sich dieses FSx for ONTAP-Dateisystem befindet.
 - iii. **FSx for ONTAP-Dateisystem**: Wählen Sie ein FSx for ONTAP-Dateisystem aus, das mit diesem Projekt verwendet werden soll.

Sie können nur Dateisysteme auswählen, die mit einem Link konfiguriert sind. "[Weitere Informationen zu Links](#)".
 - iv. **Volume auswählen**: Auswahl eines Volumes, auf dem das Projekt gespeichert wird; EDA verwendet dieses Volume als Software-Repository.

Sie können nur Volumes auswählen, die als NFS-Freigabe konfiguriert sind.
 - d. **Betriebsrichtlinien**: Grenzwerte für Projektklone:
 - i. **Maximale Aufbewahrungsdauer in Tagen**: Hier kann die maximale Anzahl von Tagen festgelegt werden, für die ein Klon aufbewahrt werden soll. Nach Ablauf dieser Anzahl von Tagen entfernt Workload Factory den Klon.
 - ii. **Maximale Anzahl von Klonen pro Benutzer oder Gruppe**: Die maximale Anzahl von Klonen eingeben, die für einen Benutzer oder eine Gruppe bereitgestellt werden können.
 - iii. **Maximale Klongröße in GiB**: Hier wird die maximale Größe eines Projektklons in GiB eingegeben.
 - e. **Zugriffsrichtlinien**: Explizite Gewährung des Projektzugriffs an bestimmte Benutzer oder Gruppen:
 - i. **Geltungsbereich der Richtliniendurchsetzung**: Mit der Eingabe einzelner IP-Adressen oder IP-Adressbereiche lässt sich der Projektzugriff auf genau diese IP-Adressen oder Bereiche beschränken.

Beispiel: 172.16.0.0/24
 - ii. **Benutzer- oder Gruppenkennungen**: Mit der Eingabe von Benutzer- oder Gruppenkennungen lässt sich der Projektzugriff auf diese Benutzer oder Gruppen beschränken.

Beispiel: User1234
6. **Erstellen** auswählen.

Ergebnis

Das Projekt wurde erstellt und erscheint in der Projektliste auf der Projektseite.

Vorhandene Projekte anzeigen

Sie können bestehende Projekte anzeigen, die in NetApp Workload Factory for EDA erstellt wurden, indem Sie diese Schritte ausführen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > EDA**.
3. Hier wird **CI/CD** ausgewählt.
4. Die Option **Zur Projektseite** auswählen.
5. Auf der Seite „Projekte“ sind die vorhandenen Projekte aufgelistet.

Ein Projekt bearbeiten

Sie können die Einstellungen eines Projekts jederzeit bearbeiten.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > EDA**.
3. Hier wird **CI/CD** ausgewählt.
4. Die Option **Zur Projektseite** auswählen.
5. Auf der Seite „Projekte“ wählen Sie für das Projekt, das Sie bearbeiten möchten, **...** und anschließend **Bearbeiten** aus.
6. Alle erforderlichen Änderungen an der Projektkonfiguration vornehmen.
7. **Speichern** auswählen.

Arbeitsbereiche eines Projekts anzeigen

Ein Klon oder Snapshot eines Projekts wird als Arbeitsbereich bezeichnet. Wenn Sie einen Arbeitsbereich erstellen, wird dieser so lange gespeichert, wie es die Betriebsrichtlinie des Projekts zulässt. Vorhandene Arbeitsbereiche für ein Projekt können mit den folgenden Schritten angezeigt werden.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > EDA**.
3. Hier wird **CI/CD** ausgewählt.
4. Die Option **Zur Projektseite** auswählen.
5. Auf der Seite „Projekte“ wird ein Projekt ausgewählt und **Anzeigen** ausgewählt.
6. Der Status und die Details aller Arbeitsbereiche für dieses Projekt werden angezeigt.
7. Wenn für einen Arbeitsbereich Benachrichtigungen oder Warnungen angezeigt werden, sehen Sie den Grund, wenn Sie den Mauszeiger über das Benachrichtigungs- oder Warnsymbol bewegen.

Ein Projekt löschen

Sie können ein Projekt löschen, wenn es nicht mehr erforderlich ist, indem Sie diese Schritte befolgen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > EDA**.
3. Hier wird **CI/CD** ausgewählt.
4. Die Option **Zur Projektseite** auswählen.
5. Auf der Seite „Projekte“ wählen Sie für das Projekt, das Sie löschen möchten, **...** aus.
6. Wählen Sie **Delete**.
7. Im Bestätigungsdialog erfolgt die Auswahl von **Löschen**.

Ergebnis

Das Projekt wird gelöscht, und der gesamte zugehörige Code sowie alle Artefakte werden aus dem Volume gelöscht. Snapshots und Klone des Projekts bleiben erhalten.

Versionen von Workload Factory für EDA-Projekte verwalten

Arbeiten Sie mit verschiedenen Versionen Ihrer EDA-Projekte, indem Sie direkt in Workload Factory bedarfsgesteuerte Snapshots und Klone erstellen. Snapshots und Klone eines Projekts werden im Dateisystem gespeichert, das dem Projekt bei seiner Erstellung zugeordnet war. Sie können Snapshots und Klone auch mit dem ["Workload Factory REST-API"](#) verwalten.

Erstellen einer Snapshot-Kopie eines Projekts

Sie können einen Snapshot eines Projekts erstellen, indem Sie diese Schritte befolgen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > EDA**.
3. Hier wird **CI/CD** ausgewählt.
4. Die Option **Zur Projektseite** auswählen.
5. Auf der Seite „Projekte“ wählen Sie **...** für das Projekt aus, von dem Sie einen Snapshot erstellen möchten.
6. Im daraufhin angezeigten Menü erfolgt die Auswahl von **Snapshot erstellen**.
7. Im Dialogfeld **Snapshot erstellen** wählen Sie einen Namen für den Snapshot aus und dann **Erstellen**.

Einen Klon eines Projekts erstellen

Das Klonen eines EDA-Projekts aus einem Snapshot erfolgt in diesen Schritten. Wenn Sie einen Klon erstellen, wird ein neues bearbeitbares Volume erstellt, das den Klon enthält.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > EDA**.
3. Hier wird **CI/CD** ausgewählt.
4. Die Option **Zur Projektseite** auswählen.
5. Auf der Seite „Projekte“ wählen Sie  für das Projekt aus, das Sie klonen möchten.
6. Im daraufhin angezeigten Menü können Sie **Create a clone** auswählen.
7. Gehen Sie im Dialogfeld **Klon erstellen** wie folgt vor:
 - a. Einen Namen für den Klon eingeben.

Der Standardname für den Klon ist der Projektname mit einem Suffix aus dem aktuellen Datum und der aktuellen Uhrzeit.

- b. Es ist ein Snapshot auszuwählen, der als Basis für den Klon verwendet werden soll.
- c. **Erstellen** auswählen.

Ergebnis

Workload Factory erstellt einen neuen Klon des Projekts, und der Klon erscheint als neues Projekt auf der Seite „Projekte“.

Erstellung eines EDA-Arbeitsbereichs

Ein Workspace in NetApp Workload Factory für EDA ist eine Perforce-Darstellung eines Projekts zu einem bestimmten Zeitpunkt. Workspaces werden auf Basis eines Projekt-Snapshots erstellt. Sie können neue Workspaces innerhalb eines EDA-Projekts erstellen. Die Erstellung von Workspaces ist über die Perforce-Benutzeroberfläche möglich.

Bevor Sie beginnen

Voraussetzung ist, dass EDA in den Perforce Helix Visual Client integriert ist. Weitere Informationen finden Sie unter ["Integration von EDA mit Perforce"](#).

Schritte

1. Bei Perforce anmelden.
2. Im Perforce-Menü erfolgt die Auswahl von **Ansicht > WF**.

In der Perforce-Benutzeroberfläche erscheint der Anmeldebildschirm von Workload Factory.
3. Melden Sie sich mit einem der ["Konsolenerlebnisse"](#) an.
4. Wählen Sie das Menü  und wählen Sie dann **EDA** aus.
5. Hier wird **CI/CD** ausgewählt.
6. **Projekt erstellen** wird ausgewählt, anschließend **Arbeitsbereich erstellen**.
7. Auf der Seite „Arbeitsbereichsprojekt erstellen“ sind folgende Angaben erforderlich:
 - a. Als Grundlage für den Arbeitsbereich ist ein Snapshot auszuwählen.
 - b. Sie geben einen Namen für den Arbeitsbereich ein.
 - c. Optional können Sie eine Benutzerkennung eingeben, um den Arbeitsbereich zu beanspruchen. Diese

Kennung sollte mit der Perforce-Benutzer-ID des Entwicklers übereinstimmen, der diesen Arbeitsbereich verwenden wird.

8. **Erstellen** auswählen.

Ergebnis

Der Arbeitsbereich wurde erstellt und erscheint in der Liste der Arbeitsbereiche auf der Seite „Workspaces“.

Workload Factory für EDA mit Perforce integrieren

Die Integration von EDA in den Perforce Helix Visual Client (P4V) ermöglicht es Entwicklern, Ihre Arbeitsbereiche über die Perforce CLI zu managen. Dies ermöglicht es Entwicklern, schnell zwischen Projekten und Arbeitsbereichen zu wechseln und so während der Entwicklung Zeit zu sparen.

Schritte

1. Download der "[P4V Integrationsdatei](#)".
2. In P4V erfolgt die Navigation zu **Tools > Manage Tools > HTML tabs**.
3. Die Option **HTML-Tabs importieren** auswählen.
4. Die P4V-Integrations-XML-Datei auswählen und **Importieren** wählen.
5. **Workload Factory** ist unter **Ansicht > Workload Factory** verfügbar.

Ergebnis

Die Web-Benutzeroberfläche von NetApp Workload Factory für EDA wird im P4V Client als HTML-Registerkarte angezeigt.

Was kommt als Nächstes?

["EDA-Projekte erstellen und managen"](#).

Einsatz von FSx for ONTAP für VMware Workloads

Informationen zu NetApp Workload Factory für VMware

NetApp Workload Factory für VMware bietet Tools, um Ihre Daten von lokalen Systemen zu Amazon Elastic VMware Service (EVS), VMware Cloud on AWS (VMC), Amazon EC2 oder Google Cloud VMware Engine zu migrieren.

Was ist NetApp Workload Factory für VMware?

NetApp Workload Factory für VMware bietet ein Planungszentrum und Migrationsberater, mit denen Sie Ihre aktuellen virtuellen Maschinenkonfigurationen in lokalen vSphere-Umgebungen analysieren können. Die Migrationsberater erstellen anschließend einen Plan zur Bereitstellung empfohlener VM-Layouts auf Amazon EVS, Amazon EC2, VMware Cloud on AWS vSphere-Clustern oder Google Cloud VMware Engine, wobei benutzerdefinierter Cloud-nativer Speicher als externe Datenspeicher verwendet wird. Für AWS-Umgebungen umfasst dies Amazon FSx for NetApp ONTAP Dateisysteme. Für Google Cloud-Umgebungen umfasst dies Google Cloud NetApp Volumes. Das Planungszentrum, das als Workload Factory für VMware Dashboard fungiert, ermöglicht Ihnen die Verwaltung gespeicherter VM-Inventardatensätze und gespeicherter Migrationspläne sowie die Bereitstellung aller von Ihnen gespeicherten Migrationspläne.

Amazon FSx for NetApp ONTAP ist ein externer NFS-Datenspeicher, der auf dem NetApp ONTAP-

Dateisystem basiert und an Amazon EVS- oder Amazon EC2-Instanzen oder VMware Cloud on AWS vSphere-Cluster angebunden werden kann. Ähnlich bietet Google Cloud NetApp Volumes externe NFS-Datenspeicher für Google Cloud VMware Engine-Umgebungen. Es ist nicht erforderlich, zusätzliche Hosts hinzuzufügen, um den verfügbaren Speicher zu erhöhen; stattdessen nutzen Sie einfach diese Cloud-nativen Speichervolumes als externe Datenspeicher zur Ergänzung von vSAN-Datenspeichern. Dies bietet Ihnen eine flexible, leistungsstarke, virtualisierte Speicherinfrastruktur, die unabhängig von den Rechenressourcen skaliert.

Weitere Informationen zu Workload Factory sind in ["Workload Factory Übersicht"](#) enthalten.

Wie die VMware Migrationsberater funktionieren

Die Migrationsberater können Ihnen dabei helfen, lokale virtuelle Maschinen (VMs) und deren Daten, die auf beliebigen von VMware unterstützten Datenspeichern laufen, zu Amazon EVS, Amazon EC2, VMware Cloud oder Google Cloud VMware Engine Datenspeichern zu migrieren, einschließlich zusätzlicher NFS-Datenspeicher auf einem FSx for ONTAP Dateisystem oder Google Cloud NetApp Volumes.

Ein einzelner vSphere Cluster auf VMware Cloud on AWS unterstützt bis zu vier (4) angehängte FSx for ONTAP Volumes.

Was Sie mit den Migrationsberatern tun können

Die Migrationsberater bieten folgende Funktionen:

- Analyse der aktuellen On-Premises-VM-Konfigurationen
- Ermitteln Sie, welche VMs zu Amazon EC2, Amazon EVS, VMware Cloud on AWS oder Google Cloud VMware Engine migriert werden sollen
- Ermitteln Sie den benötigten Speicherplatz auf Cloud-nativen Speichervolumes, die als externe VM-Datenspeicher verwendet werden
- Anhand des resultierenden Berichts lassen sich die Deployment Schritte nachvollziehen.
- Führen Sie die eigentliche Bereitstellung durch (für Amazon EC2, Amazon EVS und VMware Cloud on AWS)

Der Migrationsberater unterstützt die Konfigurationsplanung für einen einzelnen Amazon EVS, Amazon EC2 oder VMware Cloud on AWS Cluster, der mit Amazon FSx for NetApp ONTAP Dateisystemen verbunden ist, oder einen Google Cloud VMware Engine Cluster, der mit Google Cloud NetApp Volumes verbunden ist.

Vorteile der Nutzung der Migrationsberater

Die Migration von Teilen Ihrer aktuellen Infrastruktur zu Amazon EC2, Amazon EVS, VMware Cloud on AWS oder Google Cloud VMware Engine unter Verwendung von Cloud-nativem Speicher als externen NFS-Datenspeichern bietet die folgenden Vorteile:

- Kostenoptimierung durch Entkopplung von Host und Storage sowie fortschrittliche Dateneffizienz
- Die Möglichkeit, die Storage-Kapazität nach Bedarf zu erweitern, ohne zusätzliche Host-Instanzen erwerben zu müssen
- NetApp ONTAP Datenmanagementfunktionen in der Cloud, wie z. B. speichereffiziente Snapshots, Klonen, Komprimierung, Deduplizierung, Verdichtung und Replikation
- Reduzierung des Verwaltungsaufwands für Hardware-Aktualisierungen
- Möglichkeit zur Änderung des Datendurchsatzes, der IOPS und der Größe des Dateisystems sowie zur Vergrößerung oder Verkleinerung der Größe von Volumes

- Hohe Verfügbarkeit für Deployments über mehrere Availability Zones (AZ)
- Kosten- und Latenzreduzierung durch Single-AZ-Konfigurationen mit VPC-Peering ohne Transit Gateway

Tools zur Verwendung von NetApp Workload Factory

Sie können NetApp Workload Factory mit den folgenden Tools verwenden:

- **Workload Factory console:** Die Workload Factory console bietet einen visuellen, ganzheitlichen Überblick über Ihre Anwendungen und Projekte.
- **NetApp Console:** Die NetApp Console bietet eine hybride Benutzeroberfläche, die die Nutzung von Workload Factory zusammen mit anderen NetApp Datenservices ermöglicht.
- **Ask me:** Mit dem KI-Assistenten Ask me können Sie Fragen stellen und mehr über Workload Factory erfahren, ohne die Workload Factory Konsole zu verlassen. Ask me ist über das Hilfemenü von Workload Factory verfügbar.
- **CloudShell CLI:** Workload Factory umfasst eine CloudShell CLI, um AWS- und NetApp Umgebungen kontenübergreifend über eine einzige browserbasierte CLI zu managen und zu betreiben. Der Zugriff auf CloudShell erfolgt über die obere Leiste der Workload Factory Konsole.
- **REST API:** Mit den Workload Factory REST APIs können Sie Ihre FSx for ONTAP Dateisysteme und andere AWS Ressourcen einsetzen und managen.
- **CloudFormation:** Mit AWS CloudFormation-Code lassen sich die in der Workload Factory Konsole definierten Aktionen ausführen, um AWS- und Drittanbieterressourcen aus dem CloudFormation-Stack in Ihrem AWS-Konto zu modellieren, zu provisionieren und zu managen.
- **NetApp Terraform Provider:** Mit Terraform können Infrastruktur-Workflows erstellt und verwaltet werden, die in der Workload Factory Konsole generiert wurden.

Gut strukturierte Analyse für EVS-Umgebungen

Die Registerkarte „Optimierte Architektur“ bietet eine automatisierte tägliche Analyse Ihrer Amazon Elastic VMware Service (EVS)-Umgebungen, um die Einhaltung der AWS- und NetApp-Best Practices sicherzustellen. Die Registerkarte identifiziert Konfigurationsprobleme und bietet detaillierte Hinweise zur Behebung, damit Sie optimalen Betrieb, Sicherheit und Kosteneffizienz gewährleisten können.

Automatische Scans werden mithilfe der AWS-APIs durchgeführt – es sind keine vSphere-Anmeldeinformationen erforderlich. Die Ergebnisse sind nach Konfigurationsbereich geordnet, wobei jeder Befund Status, Schweregrad, Details zu den betroffenen Ressourcen und Schritt-für-Schritt-Anleitungen zur Behebung enthält.

["Implementieren Sie gut strukturierte EVS-Konfigurationen in Workload Factory".](#)

Kosten

Die Nutzung von Workload Factory für VMware ist kostenlos.

Sie müssen für AWS-Ressourcen bezahlen, die Sie auf der Grundlage der Empfehlungen der Migrationsberater einsetzen.

Lizenzierung

Für die Nutzung von Workload Factory for VMware sind keine speziellen Lizenzen von NetApp erforderlich.

Regionen

Workload Factory wird in allen kommerziellen Regionen unterstützt, in denen FSx for ONTAP unterstützt wird. ["Unterstützte Amazon Regionen"](#)

Die folgenden AWS-Regionen werden nicht unterstützt:

- China Regionen
- Secret Cloud
- Top Secret Cloud

Schnellstart für die Migration zu Amazon EVS mithilfe des VMware workloads migration advisor

Der Einstieg in den VMware migration advisor unterstützt die Migration Ihrer aktuellen Infrastruktur zu Amazon EVS unter Verwendung von Amazon FSx for ONTAP als externen NFS-Datenspeichern.

Bevor Sie beginnen, sollten Sie mit dem ["Berechtigungen für NetApp Workload Factory"](#) vertraut sein.

1

Anmeldung bei Workload Factory

Sie müssen ["ein Konto bei Workload Factory einrichten"](#) und sich bei der NetApp Console anmelden.

2

Hinzufügen von Anmeldeinformationen und Berechtigungen

Die Auswahl des Produkts ["Berechtigungsrichtlinien"](#), das Ihren Anforderungen entspricht.

Wenn Sie sich entscheiden, keine Berechtigungen zu erteilen, können Sie Workload Factory for Databases verwenden, um teilweise fertiggestellte Codebeispiele aus dem ["Berechtigungsrichtlinien"](#) zu kopieren.

Wenn Sie Berechtigungen erteilen möchten, müssen Sie ["Anmeldeinformationen manuell zu einem Konto hinzufügen"](#) wobei Sie Workload-Funktionen wie Datenbanken und VMware auswählen und die IAM-Richtlinien für die erforderlichen Berechtigungen erstellen.

["Informationen zum Hinzufügen von Anmeldeinformationen und Berechtigungen"](#).

3

Hochladen von VM Inventardaten

Im Planungszentrum können Sie Inventardetails zu Ihrer aktuellen VM-Umgebung hochladen. Zum Erfassen Ihrer aktuellen VM-Konfiguration und zum Hochladen der Daten in das Planungszentrum stehen das Datenerfassungsskript, RVTools oder NetApp Data Infrastructure Insights zur Verfügung.

["So laden Sie VM-Inventardaten hoch"](#).

4

Erstellung eines Deployment-Plans mit dem VMware migration advisor

Der VMware migration advisor ermöglicht die manuelle Konfiguration der VM-Umgebung, die auf der Amazon Elastic VMWare Service Infrastruktur unter Verwendung eines Amazon FSx for ONTAP Dateisystems als externem NFS-Datenspeicher erstellt werden soll.

"Es wird erläutert, wie der VMware migration advisor zum Erstellen eines Deployment-Plans verwendet wird."

5

Einsetzen des empfohlenen FSx for ONTAP Dateisystems

Das neue FSx for ONTAP Dateisystem wird eingesetzt, um die Datenspeicher für Ihre VMs in Ihrer Amazon EC2-Infrastruktur bereitzustellen.

"Informationen dazu, wie Sie Ihr neues Dateisystem FSx for ONTAP einsetzen".

6

Überprüfen Sie gut strukturierte Erkenntnisse für Ihre EVS-Umgebung

Wenn Ihre EVS-Umgebung erkannt wird, führt Workload Factory automatisch täglich Well-Architected-Scans durch, um Konfigurationsprobleme zu identifizieren und Empfehlungen zur Behebung bereitzustellen.

"Erfahren Sie, wie Sie gut strukturierte Konfigurationen implementieren".

Schnellstart für die Migration zu Amazon EC2 mit dem VMware workloads migration advisor

Mit dem VMware migration advisor kann Ihre aktuelle Infrastruktur mithilfe von Amazon FSx for ONTAP als externen NFS-Datstores zu Amazon EC2 migriert werden.

Bevor Sie beginnen, sollten Sie mit dem ["Berechtigungen für FSx for ONTAP für NetApp Workload Factory"](#) vertraut sein.

1

Anmeldung bei Workload Factory

Sie müssen ["ein Konto bei Workload Factory einrichten"](#) und sich bei der NetApp Console anmelden.

2

Hinzufügen von Anmeldeinformationen und Berechtigungen

Die Auswahl des Produkts ["Berechtigungsrichtlinien"](#), das Ihren Anforderungen entspricht.

Wenn Sie keine Berechtigungen erteilen, können Sie Workload Factory for Databases verwenden, um teilweise fertiggestellte Codebeispiele zu kopieren.

Wenn Sie Berechtigungen erteilen möchten, müssen Sie ["Anmeldeinformationen manuell zu einem Konto hinzufügen"](#), einschließlich der Auswahl von Workload-Funktionen wie Databases und AI sowie der Erstellung der IAM-Richtlinien für die erforderlichen Berechtigungen.

["Informationen zum Hinzufügen von Anmeldeinformationen und Berechtigungen"](#).

3

Hochladen von VM Inventardaten

Im Planungszentrum können Sie Inventardetails zu Ihrer aktuellen VM-Umgebung hochladen. Zum Erfassen Ihrer aktuellen VM-Konfiguration und zum Hochladen der Daten in das Planungszentrum stehen das Datenerfassungsskript, RVTools oder NetApp Data Infrastructure Insights zur Verfügung.

["So laden Sie VM-Inventardaten hoch"](#).

4

Erstellung eines Deployment-Plans mit dem VMware migration advisor

Nach dem Start des VMware migration advisor wählen Sie die VMs aus, die Sie mithilfe eines Amazon FSx for ONTAP Dateisystems als externe NFS-Dataspaces in die Amazon EC2 Infrastruktur migrieren möchten. Vor dem Speichern des Plans sind noch einige Änderungen möglich.

["Es wird erläutert, wie der VMware migration advisor zum Erstellen eines Deployment-Plans verwendet wird."](#)

5

Einsetzen des empfohlenen FSx for ONTAP Dateisystems

Das neue FSx for ONTAP Dateisystem wird eingesetzt, um die Datenspeicher für Ihre VMs in Ihrer Amazon EC2-Infrastruktur bereitzustellen.

["Informationen dazu, wie Sie Ihr neues Dateisystem FSx for ONTAP einsetzen"](#).

Schnellstart für die Migration zu VMware Cloud on AWS mithilfe des VMware workloads migration advisor

Erste Schritte mit dem VMware migration advisor, um Ihre aktuelle Infrastruktur mithilfe von Amazon FSx for ONTAP als externe NFS-Datenspeicher in VMware Cloud on AWS zu migrieren.

Bevor Sie beginnen, sollten Sie mit dem ["Berechtigungen für FSx for ONTAP für NetApp Workload Factory"](#) vertraut sein.

1

Anmeldung bei Workload Factory

Sie müssen ["ein Konto bei Workload Factory einrichten"](#) und sich bei der NetApp Console anmelden.

2

Hinzufügen von Anmeldeinformationen und Berechtigungen

Die Auswahl des Produkts ["Berechtigungsrichtlinien"](#), das Ihren Anforderungen entspricht.

Wenn Sie keine Berechtigungen erteilen, können Sie Workload Factory for Databases verwenden, um teilweise fertiggestellte Codebeispiele zu kopieren.

Wenn Sie Berechtigungen erteilen möchten, müssen Sie ["Anmeldeinformationen manuell zu einem Konto hinzufügen"](#), einschließlich der Auswahl von Workload-Funktionen wie Databases und AI sowie der Erstellung der IAM-Richtlinien für die erforderlichen Berechtigungen.

["Informationen zum Hinzufügen von Anmeldeinformationen und Berechtigungen"](#).

3

Hochladen von VM Inventardaten

Im Planungszentrum können Sie Inventardetails zu Ihrer aktuellen VM-Umgebung hochladen. Zum Erfassen Ihrer aktuellen VM-Konfiguration und zum Hochladen der Daten in das Planungszentrum stehen das Datenerfassungsskript, RVTools oder NetApp Data Infrastructure Insights zur Verfügung.

["So laden Sie VM-Inventardaten hoch"](#).

4

Erstellung eines Deployment-Plans mit dem VMware migration advisor

Im VMware migration advisor lassen sich die VMs auswählen, die mithilfe eines Amazon FSx for ONTAP Dateisystems als externe NFS Datastores in die neue VMware Cloud on AWS Infrastruktur migriert werden sollen. Vor dem Speichern des Plans können noch einige Änderungen vorgenommen werden.

["Es wird erläutert, wie der VMware migration advisor zum Erstellen eines Deployment-Plans verwendet wird."](#)

5

Einsetzen des empfohlenen FSx for ONTAP Dateisystems

Sie setzen das neue FSx for ONTAP Dateisystem ein, das die Datenspeicher für Ihre VMs in Ihrer VMware Cloud on AWS Infrastruktur bereitstellt.

["Informationen dazu, wie Sie Ihr neues Dateisystem FSx for ONTAP einsetzen"](#).

6

Verbindung Ihrer FSx for ONTAP Dateisysteme mit VMware Cloud on AWS

Ihr Software-Defined Data Center (SDDC) bietet Netzwerkoptionen für die Verbindung mit dem FSx for ONTAP Dateisystem durch Nutzung der VPC Peering Funktion, um die Netzwerkkonnektivität auf die externen NFS Storage-Volumes zu erweitern.

["Informationen zum Verbinden Ihrer FSx for ONTAP Dateisysteme"](#).

7

Migration von Daten von Ihren alten Systemen auf Ihre neuen FSx for ONTAP Dateisysteme

Zum Verschieben Ihrer Daten vom Storage Ihrer alten virtuellen Maschinen auf die mit Ihren neuen virtuellen Maschinen verbundenen FSx for NetApp ONTAP volumes eignet sich ein externes Tool wie VMware HCX (Hybrid Cloud Extension).

["Weitere Informationen zur Migration Ihrer Daten"](#).

Schnellstart für die Migration zu Google Cloud VMware Engine mit dem VMware workloads migration advisor

Beginnen Sie mit dem VMware Migration Advisor, um Ihre aktuelle Infrastruktur zu Google Cloud VMware Engine zu migrieren und dabei Google Cloud NetApp Volumes als externe NFS-Datenspeicher zu verwenden.

Bevor Sie beginnen, sollten Sie mit dem ["Berechtigungen für FSx for ONTAP für NetApp Workload Factory"](#) vertraut sein.

1

Anmeldung bei Workload Factory

Sie müssen ["ein Konto bei Workload Factory einrichten"](#) und sich bei der NetApp Console anmelden.

2

Hinzufügen von Anmeldeinformationen und Berechtigungen

Die Auswahl des Produkts ["Berechtigungsrichtlinien"](#), das Ihren Anforderungen entspricht.

Wenn Sie keine Berechtigungen erteilen, können Sie Workload Factory für VMware verwenden, um teilweise fertiggestellte Codebeispiele zu kopieren.

Wenn Sie sich dafür entscheiden, Berechtigungen zu erteilen, müssen Sie ["Anmeldeinformationen manuell zu einem Konto hinzufügen"](#); dazu gehört auch, ein GCP-Dienstkonto mit den erforderlichen Berechtigungen zum Anzeigen und Managen von Google Cloud NetApp Volumes Ressourcen, der VPC Konfiguration und der Google Cloud VMware Engine Datenspeicheranbindung bereitzustellen.

["Informationen zum Hinzufügen von Anmeldeinformationen und Berechtigungen"](#).

3

Hochladen von VM Inventardaten

Im Planungszentrum können Sie Inventardetails zu Ihrer aktuellen VM-Umgebung hochladen. Zum Erfassen Ihrer aktuellen VM-Konfiguration und zum Hochladen der Daten in das Planungszentrum stehen das Datenerfassungsskript, RVTools oder NetApp Data Infrastructure Insights zur Verfügung.

["So laden Sie VM-Inventardaten hoch"](#).

4

Erstellung eines Deployment-Plans mit dem VMware migration advisor

Starten Sie den VMware Migration Advisor und konfigurieren Sie die VM-Umgebung, die Sie auf der Google Cloud VMware Engine-Infrastruktur unter Verwendung von Google Cloud NetApp Volumes als externe NFS-Datenspeicher erstellen möchten.

["Es wird erläutert, wie der VMware migration advisor zum Erstellen eines Deployment-Plans verwendet wird."](#).

Überblick über das VMware Planungszentrum

Das VMware Planning Center ermöglicht Ihnen, neue VM Inventardaten hochzuladen und neue Migrationspläne zu erstellen sowie die VM Inventardaten und Migrationspläne zu managen, die Sie bereits mit NetApp Workload Factory gespeichert haben.

VM-Inventardaten managen

Im Planungszentrum können Sie VM-Inventardaten erstellen und managen.

VM-Inventardaten hochladen

Sie können VM-Inventardaten hochladen, wenn Sie bereit sind, Workload Factory zu verwenden, um Migrationsoptionen für Amazon AWS Umgebungen zu erkunden. Anweisungen dazu finden Sie unter ["VM-Inventardaten hochladen"](#).

Datensatz umbenennen

Sie können den Namen eines gespeicherten Datensatzes ändern.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > VMware** auszuwählen.

Das Planungszentrum ist zu sehen.

3. Im Menü „Aktionen“ (...) ist für den Datensatz, der umbenannt werden soll, die Option **Umbenennen** auszuwählen.
4. Für den Datensatz wird ein neuer Name eingegeben und **Speichern** ausgewählt.

Einen Datensatz löschen

Wenn ein Datensatz nicht mehr benötigt wird, können Sie ihn jederzeit löschen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads** > **VMware** auszuwählen.

Das Planungszentrum ist zu sehen.
3. Für den Datensatz, der gelöscht werden soll, erfolgt die Auswahl von **Löschen** im Menü „Aktionen“ (...).
4. Die Aktion wird durch Auswählen von **Delete** bestätigt.

Migrationspläne verwalten

Im Migrationscenter können Sie Migrationspläne erstellen und managen.

Provisionierung eines Migrationsplans

Sie können einen Migrationsplan auswählen und provisionieren, sodass die VMs in die Amazon AWS Umgebung Ihrer Wahl migriert werden.

Schritte

1. Die Anmeldung bei Workload Factory erfolgt mit einem der ["Konsolenerlebnisse"](#).
2. Im Menü  erfolgt anschließend die Auswahl von **VMware**.

Das Planungszentrum ist zu sehen.
3. Die Option **Migrationspläne** auswählen.
4. Im Menü „Aktionen“ (...) ist der Migrationsplan auszuwählen, der provisioniert werden soll, und anschließend **Provision**.
5. Je nach Migrationsplan sind die Anweisungen zum Einsetzen des Dateisystems zu beachten:
 - ["Deployment des Dateisystems für Amazon VMware Cloud Pläne"](#)
 - ["Dateisystem für Amazon EC2 Pläne einsetzen"](#)
 - ["Deployment des Dateisystems für Amazon Elastic VMware Service Pläne"](#)

Kommentar für einen Migrationsplan bearbeiten

Falls eine Änderung von Kommentardetails für einen Migrationsplan erforderlich ist, kann der Kommentar im Planungszentrum bearbeitet werden.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
- 2.

Im Menü  ist **Workloads > VMware** auszuwählen.

Das Planungszentrum ist zu sehen.

3. Die Option **Migrationspläne** auswählen.
4. Im Menü „Aktionen“ (...) lässt sich für den Migrationsplan, der bearbeitet werden soll, **Kommentar bearbeiten** auswählen.
5. Nach Eingabe eines Kommentars **Speichern** auswählen.

Erstellung eines PDF- oder CSV-Berichts zu einem Migrationsplan

Erstellung eines PDF- oder CSV-Berichts mit den Details eines Migrationsplans.

Schritte

1. Melden Sie sich bei der "NetApp Console" an.
2. Im Menü  ist **Workloads > VMware** auszuwählen.

Das Planungszentrum ist zu sehen.
3. Die Option **Migrationspläne** auswählen.
4. Im Menü „Aktionen“ (...) lässt sich für den Migrationsplan, für den ein PDF- oder CSV-Bericht erstellt werden soll, **Plan herunterladen (PDF)** oder **VM-Bericht herunterladen (CSV)** auswählen.
5. Für den Bericht einen Namen eingeben und **Speichern** auswählen.

Einen Migrationsplan löschen

Wenn ein Migrationsplan nicht mehr benötigt wird, können Sie ihn jederzeit löschen.

Schritte

1. Melden Sie sich bei der "NetApp Console" an.
2. Im Menü  ist **Workloads > VMware** auszuwählen.

Das Planungszentrum ist zu sehen.
3. Die Option **Migrationspläne** auswählen.
4. Im Menü „Aktionen“ (...) kann für den Migrationsplan, der gelöscht werden soll, **Löschen** ausgewählt werden.
5. Bestätigen Sie die Aktion, indem Sie **Löschen** auswählen.

Verwendung des VMware Planungszentrums

Hochladen von VM-Inventardaten in NetApp Workload Factory

Bevor Sie einen Migrationsplan erstellen können, müssen Sie Ihre VM-Inventardaten hochladen.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads** > **VMware** auszuwählen.

Das Planungszentrum wird angezeigt. Im Planungszentrum können Sie Ihre VM-Inventardaten hochladen, frühere Inventardaten-Uploads einsehen und eine Migration mithilfe beliebiger VM-Inventardatensätze planen.

3. Die Auswahl erfolgt über **Upload VM inventory**.
4. Es ist die zu verwendende Datenerfassungsmethode auszuwählen:

Verwendung von RVTools (Schnellbewertung)

RVTools ist eine Windows Applikation, die mit VCenter und ESX server (5.x bis 8.0) interagiert, um Informationen über Ihre virtuellen VMware-Umgebungen zu erfassen. Sie sammelt Informationen über VMs, CPU, Arbeitsspeicher, Festplatten, Cluster, ESX-Hosts, Datastores und mehr. Sie können diese Informationen in eine xlsx-Datei exportieren, um sie mit dem Migrationsberater zu verwenden.

["Weitere Informationen zu RVTools"](#)

Schritte

1. Sie wählen die Kachel **RVTools** und anschließend **Weiter** aus.

Die Seite **Prepare for AWS Cloud onboarding** wird angezeigt.

2. Geben Sie einen Namen für den VM-Inventar-Datensatz ein, den Sie erstellen werden.
3. RVTools 4.4.2 oder höher lässt sich von der ["RVTools Website"](#) herunterladen und installieren
4. RVTools wird gestartet, und die Anmeldung beim Ziel VCenter Server erfolgt.

Damit werden Informationen zu diesem VCenter Server erfasst.

5. Der Export Ihrer VMware-Informationen in eine xlsx- oder xls-Datei ist möglich.

Einzelheiten enthält das Kapitel „Befehlszeilenparameter“ in der ["Die RVTools Dokumentation befindet sich im Abschnitt „Ressourcen“"](#).

6. Zunächst erfolgt die Auswahl von , anschließend die Auswahl der exportierten RVTools-Datei.
7. Die Option **Upload** auswählen.
8. Wählen Sie **Fertigstellen**.

Datensammler verwenden (detaillierte Planung)

Das Skript NetApp Migration advisor VM collector sammelt VM-Konfigurationsinformationen aus Ihrem vCenter, ähnlich wie RVTools, erfasst jedoch aktuelle VM-Performance-Daten, um tatsächliche Lese- und Schreib-IOPS sowie Durchsatzstatistiken bereitzustellen. Das Skript kann in einem von zwei Modi verwendet werden:

- Stündliche Datenerfassung
- Tägliche Datenerfassung

Zum Kopieren des VM-Collector-Skripts des Migration advisor aus dem Codebox-Fenster ist der Start des Migration advisor erforderlich.

Bevor Sie beginnen

Das System, auf dem Sie das Collector-Skript ausführen, muss folgende Anforderungen erfüllen:

- Microsoft PowerShell 7.0 oder höher muss installiert sein. Unter "[Microsoft PowerShell Dokumentation](#)" finden Sie Informationen, falls PowerShell installiert werden muss.
- VMware PowerCLI muss installiert sein. Das "[VMware PowerCLI Dokumentation](#)" enthält Informationen, falls PowerCLI installiert werden muss.
- Die SSL-Zertifikatsprüfung muss deaktiviert sein.
- PowerShell muss die Ausführung unsignierter Skripte ermöglichen.

Wenn Sie langfristige Statistiken von Ihren VMs erfassen möchten (tägliche Statistiken), müssen Sie in der vSphere Managementkonsole (VMware-Managementumgebung) Statistiken auf Level 3 oder höher aktiviert haben.

Schritte

1. Es erfolgt die Auswahl der Kachel **Datensammler** und anschließend von **Weiter**.

Das Fenster Codebox wird auf der rechten Seite der Seite angezeigt.

2. Im Codebox-Fenster steht entweder  zum Speichern des Datenerfassungsskripts des Migration Advisor (mit dem Namen "list-vms.ps1") auf dem Zielsystem oder  zum Kopieren des Skripts zur Verfügung, damit es auf dem entsprechenden System eingefügt werden kann.

3. Mit den folgenden Schritten lassen sich die Konfigurationen Ihrer aktuellen VMs erfassen:

- a. Die Anmeldung erfolgt bei dem System, auf dem Sie den Datensammler heruntergeladen haben und auf dem PowerShell sowie PowerCLI installiert sind.
- b. Die Verbindung zu Ihrem VMware vCenter Server erfolgt durch Ausführen des folgenden Befehls:

```
Connect-VIServer -server <server_IP>
```

Anstelle von <server_IP> ist die IP-Adresse oder der Hostname Ihres VMware-Servers anzugeben.

- c. Beim Ausführen des heruntergeladenen Datenerfassungsskripts ist die Datenerfassungsoption für stündliche oder tägliche VM-Statistiken anzugeben.

```
./list-vms.ps1 -PerformanceStatisticsTimePeriod <LastHour |  
LastDay>
```

Dabei gilt:

- **LastHour** erfasst IOPS- und Durchsatzdaten der letzten 1 Stunde in 20-Sekunden-Intervallen.
- **LastDay** erfasst IOPS- und Durchsatzdaten der letzten 24 Stunden in 5-Minuten-Intervallen.

Optional können Sie das Datenerfassungsskript auch ohne Angabe von Optionen ausführen; dadurch können Sie den Datenerfassungszeitraum im interaktiven Menü auswählen.

+ Das Skript erzeugt im aktuellen Arbeitsverzeichnis eine komprimierte Datei mit einem Zeitstempel im Namen. Die .zip-Datei enthält eine Liste aller VMs und ihrer Eigenschaften sowie deren IOPS- und

Durchsatzdaten.

4. Die Option **Upload** auswählen.

Verwendung von NetApp Data Infrastructure Insights (detaillierte Planung)

NetApp Data Infrastructure Insights ist ein Tool zur Überwachung von Cloud-Infrastrukturen, das Ihnen Transparenz in Ihre gesamte Infrastruktur bietet. Sie müssen die temporäre API-Kommunikation zwischen dem Migrationsberater und Data Infrastructure Insights aktivieren, damit der Migrationsberater Informationen über Ihre VMware-Infrastruktur erfassen kann.

["Weitere Informationen zu Data Infrastructure Insights"](#)

Schritte

1. Die Auswahl erfolgt über die Kachel **Data Infrastructure Insights** und anschließend über **Next**.

Die Seite **Prepare for AWS Cloud onboarding** wird angezeigt.

2. Geben Sie einen Namen für den VM-Inventar-Datensatz ein, den Sie erstellen werden.
3. Eingabe des Tenant-Endpunkts für Data Infrastructure Insights.

Dies sollte die URL sein, die Sie für den Zugriff auf Data Infrastructure Insights verwenden.

4. Falls Sie noch kein API-Zugriffstoken für Data Infrastructure Insights generiert haben, folgen Sie den Anweisungen auf der Seite, um eines zu erstellen. Andernfalls erfolgt die Eingabe Ihres API-Zugriffstokens in das Textfeld „API Access Token eingeben“.
5. Die Option **Upload** auswählen.

Workload Factory sammelt Informationen aus Data Infrastructure Insights.

Was kommt als Nächstes?

Im Planungszentrum lassen sich Ihre hochgeladenen VM-Inventardaten managen oder ein Deployment-Plan erstellen.

- ["Das VMware workloads planning center erkunden"](#)
- ["Erstellung eines Amazon VMware Cloud Deployment-Plans"](#)
- ["Erstellung eines Deployment-Plans für Amazon Elastic VMware Service"](#)
- ["Erstellung eines Amazon EC2 Deployment-Plans"](#)
- ["Erstellen Sie einen Google Cloud VMware Engine-Bereitstellungsplan"](#)

Migration zu Amazon Elastic VMware Service

Einsparungen für Amazon Elastic VMware Service mit NetApp Workload Factory

Sie erhalten einen Überblick über potenzielle Einsparungen bei der Migration Ihrer VMware-Workloads zu Amazon Elastic VMware Service (EVS). Der Kostenrechner ermöglicht den Vergleich der Kosten für die Nutzung von Amazon EVS mit und ohne Amazon FSx for NetApp ONTAP als Storage.

Wenn der Kostenrechner ermittelt, dass der kostengünstigste Storage FSx for ONTAP ist, können Sie eine detaillierte Bewertung erstellen, die einen Migrationsplan bereitstellt, den Sie vor der Verwendung prüfen

können. Anschließend können Sie mit der Codebox Infrastructure-as-Code-Vorlagen generieren.

Einsparpotenziale für EVS-Umgebungen

Mit den folgenden Schritten lassen sich mögliche Einsparungen bei einer geplanten Migration in eine Amazon EVS-Umgebung ermitteln.



Vor dem Fortfahren bietet der Haftungsausschluss am unteren Rand des Einsparungsrechners weitere Informationen dazu, wie die Preisschätzungen berechnet werden.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.

2. Im Menü  ist **Workloads** > **VMware** auszuwählen.

Das Planungszentrum ist zu sehen.

3. Im VMware-Menü erfolgt die Auswahl von **Einsparmöglichkeiten entdecken**. Der Einsparungsrechner wird angezeigt.

Im Bereich **Umgebungseinstellungen** können Sie Ihre EVS Deployment-Region auswählen und die TCO- und Einsparungsprognosen entsprechend anpassen.

4. Für die Berechnung der Einsparungen dient die Dropdown-Liste **Region** zur Auswahl der EVS Deployment Region.

5. Mit den folgenden Schiebereglern lassen sich bei Bedarf Echtzeitberechnungen der Einsparungen für die von Ihnen gewählten Werte anzeigen. Bei Verwendung einer Tastatur sind mit den Pfeiltasten kleinere Anpassungen möglich:

- **Erforderliche physische CPU (Anzahl)**
- **Erforderlicher physischer Speicher (GiB)**
- **Erforderlicher VM Storage (TiB)**

6. Unter **EVS-Abrechnungsplan** erfolgt die Auswahl des von Ihnen genutzten Plans.

7. Führen Sie einen der folgenden Schritte aus:

- Zur Verwendung des Migrationsberaters ["einen Deployment-Plan erstellen"](#) für eine Amazon EVS Umgebung ist **Plan EVS migration** auszuwählen.
- Die Option **Schließen** schließt den TCO-Rechner.

Deployment-Plan für Amazon EVS manuell erstellen

Für den Zugriff auf das VMware Planning Center ist die Anmeldung bei der NetApp Workload Factory erforderlich. Dort kann manuell ein Deployment- oder Migrationsplan für Amazon EVS erstellt werden, der an Ihre Anforderungen angepasst ist.

Sie können Ihre Anforderungen an virtuelle Maschinen im Amazon Elastic VMware Service manuell festlegen und angepasste Amazon FSx for NetApp ONTAP Dateisysteme als externe Datenspeicher verwenden.

Anforderungen

- Sie benötigen einen Benutzernamen und ein Passwort, um auf Workload Factory zuzugreifen. Falls Sie

noch keinen Zugang haben, können Sie jetzt ein Konto erstellen. Die Anweisungen finden Sie ["hier"](#).

- Sie benötigen ein Abonnement für Amazon Elastic VMware Service.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads** > **VMware** auszuwählen.

Das Planungszentrum ist zu sehen.

3. Auswahl von **Manually create EVS plan**.
4. Eingabe der Anforderungen für Ihre VM-Umgebung.



Zu beachten sind die folgenden Performance-Anforderungen und Empfehlungen für die VM-Migration:

- Aus Performancegründen wird für das VM-Inventar eine Mindest-Storage-Kapazität von 10TiB empfohlen.
- Für die Datastores des Amazon Elastic VMware Service ist ein Mindestdurchsatz erforderlich, abhängig von der erforderlichen Anzahl an IOPS, die Sie für dieses Deployment angeben.
- Je nach Konfiguration des FSx for ONTAP Dateisystems ist eine Mindestanzahl externer Datastores erforderlich, damit die Amazon Elastic VMware Service Umgebung eine optimale Performance erreicht.

5. Sobald Sie bereit sind, können Sie über **Plan überprüfen** den Migrationsplan prüfen.
6. Plan überprüfen. Die einzelnen Abschnitte erweitern, um die Plandetails anzuzeigen.

Standardmäßig speichert Workload Factory den Migrationsplan im Planungszentrum. Sie können diese Option oben auf der Seite deaktivieren.

7. Optional können Sie den Migrationsplan als PDF- oder CSV-Datei exportieren, indem Sie oben rechts auf der Seite **Plan verwalten** und anschließend **Bericht herunterladen (.pdf)** oder **VM Storage Deployment (.csv)** auswählen.

Die .csv-Datei erstellt eine Übersicht aller im Migrationsplan enthaltenen VMs sowie ihrer zugewiesenen Storage Volumes.

8. Wenn Sie bereit sind, den Deployment Plan zu provisionieren, steht **Provision** zur Auswahl.

["Einsatz des von VMware Workloads empfohlenen FSx for ONTAP Dateisystems"](#).

Erstellen eines Deployment-Plans für Amazon EVS mithilfe des migration advisor

Im VMware planning center können Sie den Amazon EVS migration advisor starten, der Sie bei der Erstellung eines auf Ihre Bedürfnisse zugeschnittenen Migrationsplans unterstützt.

Sie können einen Deployment-Plan erstellen, um virtuelle Maschinen zu Amazon Elastic VMware Service zu migrieren und angepasste Dateisysteme von Amazon FSx for NetApp ONTAP als externe Datenspeicher zu

verwenden. Die Optionen im Migrationsberater können je nach dem Tool, das zur Erfassung der VM-Inventardaten verwendet wurde, variieren.

Anforderungen

- Sie benötigen einen Benutzernamen und ein Passwort, um auf Workload Factory zuzugreifen. Falls Sie noch keinen Zugang haben, können Sie jetzt ein Konto erstellen. Die Anweisungen finden Sie ["hier"](#).
- Sie benötigen ein Abonnement für Amazon Elastic VMware Service.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.

2. Im Menü  ist **Workloads** > **VMware** auszuwählen.

Das Planungszentrum ist zu sehen.

3. Sie wählen in der Liste das VM-Inventar aus, das Sie zum Erstellen eines Deployment-Plans verwenden möchten, und in dieser Zeile anschließend **Start planning**.

4. Im daraufhin erscheinenden Dropdown-Menü ist **EVS** auszuwählen.

Der Assistent **Prepare for AWS Cloud onboarding** wird angezeigt.

5. Die erforderlichen Informationen eingeben.

Angeben

1. Der Abschnitt *VM-Konfiguration hochladen* enthält Informationen zu dem Datensatz, mit dem ein Migrationsplan erstellt wird. Im Abschnitt **VM-Inventarübersicht** werden anhand der Inventardatei die Anzahl der VMs sowie die gesamte Storage-Kapazität angezeigt.

2. Im Abschnitt *Überlegungen zur VM-Inventarisierung* können Sie die Optionen auswählen, um die Liste der zu migrierenden VMs zu filtern:

- a. **Region:** Die Region auswählen, in der Amazon FSx for NetApp ONTAP Dateisysteme eingesetzt werden. Für optimale Performance und Kosteneffizienz ist dies in der Regel dieselbe Region, in der Ihr bestehendes Amazon EC2 SDDC eingesetzt wird.
- b. Für die VMs in dieser Region ist ein prognostiziertes Performance Level auszuwählen. Wir empfehlen, mit einer niedrigeren IOPS-Einstellung zu beginnen. Sie können die provisionierten SSD-IOPS erhöhen, nachdem das Dateisystem erstellt wurde, wenn Workloads migriert oder eingesetzt werden:
 - **Standard bis hohe Performance:** Für VMs mit durchschnittlichen E/A-Raten zwischen 20 und 5000 IOPS.
 - **Sehr hohe Performance:** Für VMs mit durchschnittlichen E/A-Raten von mehr als 5000 IOPS.
 - **Sehr geringe Performance:** Für VMs mit einer durchschnittlichen E/A-Rate von weniger als 20 IOPS.

3. Im Abschnitt *Überlegungen zu Zielkapazität und Schutz* stehen Ihnen einige Storage Optionen zur Auswahl:

- a. **Zu berücksichtigender VM Storage:** Auswahl, ob die für jede integrierte VM erstellten Datastores auf Basis ihrer aktuell genutzten Größe (empfohlen) oder ihrer provisionierten Größe dimensioniert werden.

Die externen Datenspeicher werden mithilfe von Dateisystem-Volumes des Amazon FSx for NetApp

ONTAP Dateisystems implementiert.

- b. **Durchschnittliches Datenreduktionsverhältnis:** Zur Auswahl stehen drei gängige Datenreduktionsverhältnisse. Verfügbar sind "1:1 - Keine Reduktion", "1:1.25 - 20 % Reduktion" oder "1:1.5 - 33 % Reduktion".

Help me decide ist auszuwählen, wenn Unklarheit darüber besteht, welches Verhältnis gewählt werden soll. Das Dialogfeld *Data reduction ratio assistant* wird angezeigt. Es sind alle Aussagen auszuwählen, die auf Ihren VM-Bestand und Ihre Storage-Umgebung zutreffen. Der Assistent empfiehlt eine geeignete Datenreduktionsrate. **Apply** ist auszuwählen, um das empfohlene Verhältnis zu verwenden.

- c. **Prozentualer Kapazitätspuffer:** Der Prozentsatz des Kapazitätswachstums, der zur Kapazität Ihrer FSx for ONTAP Dateisysteme hinzugefügt wird.

Wenn Sie einen Wert von weniger als 20 % auswählen, können Sie keine Volume-Snapshots zum Schutz und für langfristige Backups erstellen.

- d. **VM-Snapshot-Schutz:** Mit dieser Option lassen sich die VMs durch Snapshots schützen.

4. **Weiter** auswählen.

Auswählen

1. Auf der Seite **Virtuelle Maschinen auswählen** erfolgt die Auswahl der VMs aus der Liste, die in die AWS-Migration einbezogen werden sollen. Die Liste kann nach dem Energiestatus der einzelnen VMs sowie nach dem Datacenter und Cluster gefiltert werden, in dem sich die VM befindet.

In der VM-Liste können Sie auswählen, welche Arten von VM-Informationen als Spalten angezeigt werden. Beispielsweise wird durch Auswahl von *Peak read IOPS* eine Spalte mit den Spitzenwerten der Lese-IOPS für jede VM angezeigt.

2. Optional können Sie das Deployment entweder im Hinblick auf die Kosten oder auf die Wiederherstellbarkeit optimieren.
- **Kosten:** Workload Factory wählt aus der Liste VMs mit geringerer E/A-Dichte aus. Dies trägt zur Reduzierung des Ressourcenbedarfs bei.
 - **Wiederherstellungsfähigkeit:** Workload Factory wählt aus der Liste die VMs aus, die sich am einfachsten und schnellsten lokal kopieren lassen. Dies ermöglicht kurze Wiederherstellungszeiten im Falle von Störungen.

3. **Weiter** auswählen.

Design

- Auf der Seite **Speicherzuweisung der ClassReview Instanz** werden die VM-Informationen, die Regeln zur Volume-Klassifizierung, die Volume-Zuweisungen und die Liste der Volumes, die als Teil des Deployment migriert werden, überprüft. Anschließend wird **Weiter** ausgewählt.

Planprüfung

1. Auf der Seite **Plan überprüfen** werden die geschätzten monatlichen Einsparungen und Kostenschätzungen für alle VMs angezeigt, deren Migration geplant ist.

Im oberen Bereich der Seite werden die geschätzten monatlichen Einsparungen für FSx for ONTAP Dateisysteme und EBS Volumes angezeigt. Jeder Abschnitt lässt sich erweitern, um Details zur

vorgeschlagenen Dateisystemkonfiguration, zur Aufschlüsselung der geschätzten Einsparungen, zu den Annahmen und zu den technischen Haftungsausschlüssen anzuzeigen.

Standardmäßig speichert das Planungscenter den Migrationsplan automatisch in der Liste der Pläne.

- Optional können Sie den Migrationsplan als PDF- oder CSV-Datei exportieren, indem Sie oben rechts auf der Seite **Plan verwalten** und anschließend **Bericht herunterladen (.pdf)** oder **VM Storage Deployment (.csv)** auswählen.

Die .csv-Datei erstellt eine Übersicht aller im Migrationsplan enthaltenen VMs sowie ihrer zugewiesenen Storage Volumes.

- Wenn Sie bereit sind, mit dem Plan fortzufahren, wählen Sie **Provision**, um mit dem Deployment des empfohlenen Amazon FSx for NetApp ONTAP Dateisystems zu beginnen.

["Einsatz des von VMware Workloads empfohlenen FSx for ONTAP Dateisystems"](#).

Einsatz des empfohlenen FSx for ONTAP Dateisystems

Nachdem Sie überprüft haben, dass das empfohlene FSx for ONTAP Dateisystem (oder in einigen Fällen mehrere Dateisysteme) Ihren genauen Anforderungen entspricht, können Sie Workload Factory verwenden, um das System in Ihrer AWS-Umgebung einzusetzen.

Abhängig von den Richtlinien und Berechtigungen, die Sie Ihrem Workload Factory Konto hinzugefügt haben, können Sie das FSx for ONTAP Dateisystem vollständig mit Workload Factory einsetzen (im lesen/schreiben Modus). Wenn Sie über weniger Berechtigungen (schreibgeschützter Modus) oder keine Berechtigungen (Basic Modus) verfügen, müssen Sie die CloudFormation Vorlage aus der Codebox verwenden und das FSx for ONTAP Dateisystem selbst in AWS einsetzen.

Anforderungen

- Sie benötigen ein Abonnement für Amazon Elastic VMware Service.
- Sie benötigen die erforderlichen Berechtigungen, um ein FSx for ONTAP Dateisystem in Ihrem AWS-Konto zu erstellen.

Überlegungen

- Sie können die Option „Schnell erstellen“ oder „Erweitert erstellen“ verwenden. „Erweitert erstellen“ bietet einige zusätzliche Storage-Parameter, die Sie anpassen können. ["Was diese beiden Optionen bieten"](#).
- Im Abschnitt „Amazon Elastic VMware Service preferences“ können Sie die EVS Virtualisierungsumgebung auswählen, um die Verbindung zu den externen Datenspeichern herzustellen. Dadurch werden einige Felder automatisch mit den Best-Practice-Optionen für das Deployment ausgefüllt. Diese Optionen können Sie nach Bedarf anpassen.

Schritte

- Am unteren Rand der Seite **Review plan** führt die Auswahl von **Deploy** zur Anzeige der Seite „Create an FSx for ONTAP file system“.

Die meisten Felder, die Ihr FSx for ONTAP Dateisystem definieren, sind anhand der von Ihnen bereitgestellten Informationen ausgefüllt. Es gibt jedoch einige Felder, die Sie auf dieser Seite ausfüllen müssen.

2. Im Abschnitt „Allgemeine Konfiguration des Dateisystems“ erfolgt die Eingabe der folgenden Informationen:
 - a. **AWS-Anmeldeinformationen:** Wählen Sie Anmeldeinformationen aus oder fügen Sie sie hinzu, die Workload Factory die erforderlichen Berechtigungen erteilen, um Ihr FSx for ONTAP file system direkt zu erstellen. Alternativ können Sie auch den CloudFormation Code aus Codebox auswählen und das FSx for ONTAP file system in AWS selbst einsetzen.
 - b. **Dateisystemname:** Geben Sie den Namen ein, den Sie für dieses FSx for ONTAP Dateisystem verwenden möchten.
 - c. **Tags:** Optional können Sie Tags hinzufügen, um dieses FSx for ONTAP Dateisystem zu kategorisieren.
3. Im Abschnitt „Amazon Elastic VMware Service Einstellungen“ erfolgt die Auswahl der EVS-Umgebung, an die die Datastores angebunden werden, in der Liste „Environment ID“.

Dadurch werden die folgenden Felder automatisch ausgefüllt:

- **VPC**
 - **Verfügbarkeitszone**
 - **Subnetz**
 - Im Abschnitt **NFS-Datenspeicherzugriff** füllt das System das Feld **EVS-Hostverwaltung (CIDR)** automatisch aus, wenn Sie die Option **Nur EVS-Hostverwaltung** ausgewählt haben.
 - Im Abschnitt **Datastore-Einbindungsoptionen** werden die Felder **EVS Cluster VMware vCenter-Adresse** und **vSphere Administratoranmeldeinformationen Secret ARN** automatisch ausgefüllt, wenn Sie ausgewählt haben, Datastores im EVS Cluster einzubinden.
4. Im Abschnitt „Netzwerk & Sicherheit“ erfolgt die Eingabe der folgenden Informationen:
 - a. **Region & VPC:** Auswahl der Region und der VPC, in der das Dateisystem FSx for ONTAP eingesetzt wird.
 - b. **Sicherheitsgruppe** (nur erweiterte Erstellung): Bei Verwendung der Option **Erweiterte Erstellung** können Sie die Standard-Sicherheitsgruppe für die FSx for ONTAP VPC auswählen, sodass der gesamte Datenverkehr auf das FSx for ONTAP Dateisystem zugreifen kann. Sie können entweder eine neue Sicherheitsgruppe erstellen oder eine vorhandene auswählen.

Wenn Sie die Option **Sicherheitsgruppenkonfiguration an EVS NFS Datenspeicher anpassen** aktivieren, konfiguriert Workload Factory die Sicherheitsgruppe gemäß den Einstellungen für EVS NFS Datenspeicher.

Sie können der Sicherheitsgruppe eine eingehende Regel hinzufügen, die einschränkt, auf welche anderen AWS Services das FSx for ONTAP Dateisystem zugreifen kann. Dadurch wird die Anzahl der offenen Services reduziert. Dies sind die minimalen Ports und Protokolle:

Protokolle	Ports	Zweck
TCP, UDP	111	Portmapper (zum Aushandeln der in NFS-Anfragen verwendeten Ports)
TCP, UDP	635	NFS mountd (empfangt NFS-Mount-Anfragen)
TCP, UDP	2049	NFS Netzwerkdatenverkehr
TCP, UDP	4045	Network Lock Manager (NLM, lockd) - Verarbeitet Sperranforderungen.
TCP, UDP	4046	Netzwerkstatusmonitor (NSM, statd) - Benachrichtigt NFS-Clients über Neustarts des Servers für die Sperrverwaltung.

- a. **Verfügbarkeitszone:** Die Verfügbarkeitszone und das Subnetz werden ausgewählt.

Sie sollten dieselbe Verfügbarkeitszone auswählen, in der Ihr VMware SDDC bereitgestellt ist, wenn Sie Gebühren für Cross-AZ-Datenverkehr vermeiden möchten.

- b. **Encryption** (nur bei **Advanced create**): Bei Verwendung der Option **Advanced create** können Sie den Namen des AWS-Verschlüsselungsschlüssels aus der Dropdown-Liste auswählen.
- c. **NFS Datastores Zugriff** (nur bei **Advanced create**): Bei Verwendung der Option **Advanced create** können Sie auswählen, ob alle Hosts auf die Datastores zugreifen können oder ob nur der EVS Management Host auf die Datastores zugreifen kann.

5. Im Abschnitt „Dateisystemdetails“ erfolgt die Eingabe der folgenden Informationen:

- a. **ONTAP Zugangsdaten:** Eingabe von ONTAP Benutzername und Passwort.
- b. **Anmeldeinformationen für die Storage VM** (nur bei erweiterter Erstellung): Geben Sie das Kennwort für die Storage VM ein und bestätigen Sie es. Das Kennwort kann spezifisch für dieses Dateisystem sein, oder Sie können dasselbe Kennwort verwenden, das Sie für die ONTAP Anmeldeinformationen eingegeben haben.

6. Im Abschnitt „EVS Cluster Anbindung“ sind die folgenden Informationen einzugeben:

- a. **Datastore-Einbindungsoptionen:** Optional kann die Option **Datastores in den EVS Cluster einbinden** aktiviert werden, um die Datastores automatisch mit dem Amazon EVS Cluster zu verbinden. Diese Option bewirkt außerdem, dass Workload Factory die VMware ESXi Hosteinstellungen so konfiguriert, dass sie den ONTAP Best-Practice-Empfehlungen entsprechen. Vor dem Einsatz des Dateisystems können die Plandetails im Abschnitt **Summary** geprüft werden, um die geänderten Einstellungen zu sehen.
- b. **EVS Cluster vSphere Konsolendetails:** IP-Adresse oder FQDN des VMware vCenter Servers, der eine Verbindung zu Amazon EVS herstellen soll.
- c. **vSphere Administratoranmeldeinformationen Secret ARN:** Hier wird der Secret ARN für die Administratoranmeldeinformationen von vSphere ausgewählt. Diese Anmeldeinformationen werden verwendet, um Datastores einzubinden und empfohlene VMware-Einstellungen zu konfigurieren.

Falls Amazon EVS in dieser Region nicht verfügbar ist oder Ihr Konto nicht über die Berechtigungen zum Abrufen der Liste der verfügbaren secret ARNs verfügt, können Sie einen secret ARN-Wert manuell eingeben.

7. Im Abschnitt **Summary** ist die FSx for ONTAP Dateisystem- und Datastore-Konfiguration zu sehen, die der VMware Migration Advisor auf Basis Ihrer Angaben entworfen hat.
8. Über **Erstellen** lässt sich das Dateisystem FSx for ONTAP einsetzen. Dieser Vorgang kann bis zu 2 Stunden dauern.

Im Codebox-Fenster steht optional die Option **Umleiten nach CloudFormation** zur Verfügung, mit der sich das Dateisystem und die empfohlene VM-Konfiguration mithilfe eines CloudFormation Stack erstellen lassen.

In beiden Fällen können Sie den Erstellungsfortschritt in CloudFormation überwachen.

Ergebnis

Das FSx for ONTAP Dateisystem ist bereitgestellt. Sie können nun die AWS CloudFormation Vorlage in der Codebox verwenden, um die empfohlene VM-Konfiguration in Ihrer Amazon Elastic VMware Service Umgebung einzusetzen.

Migrieren zu Google Cloud VMware Engine

Erstellen Sie einen Bereitstellungsplan für Google Cloud VMware Engine mithilfe des Migrationsberaters

Vom VMware Planning Center aus können Sie den Google Cloud VMware Engine Migration Advisor starten, um einen auf Ihre Bedürfnisse zugeschnittenen Migrationsplan zu erstellen.

Sie können einen Bereitstellungsplan erstellen, um virtuelle Maschinen zu Google Cloud VMware Engine zu migrieren und angepasste Google Cloud NetApp Volumes als externe NFS-Datenspeicher zu verwenden. Die Optionen im Migrationsberater können je nach dem Tool, das zur Erfassung der VM-Inventardaten verwendet wurde, variieren.

Anforderungen

- Sie müssen ["VM-Inventar hochgeladen"](#) haben.
- Sie benötigen einen Benutzernamen und ein Passwort, um auf Workload Factory zuzugreifen. Wenn Sie keinen Zugang haben, können Sie jetzt ein Konto erstellen. Die Anweisungen ["hier,"](#) können Sie einsehen.
- Sie benötigen ein Google Cloud VMware Engine-Abonnement in einer Region, in der sowohl Google Cloud VMware Engine als auch Google Cloud NetApp Volumes Services verfügbar sind.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.

2. Im Menü  ist **Workloads > VMware** auszuwählen.

Das Planungszentrum ist zu sehen.

3. Wählen Sie **Google Cloud** aus dem Drop-down-Menü.

4. Wählen Sie in der VM-Inventartabelle neben dem Inventar, das Sie für die Erstellung eines Bereitstellungsplans verwenden möchten, **Start planning** aus.

Der Assistent **Prepare for Google Cloud onboarding** wird angezeigt.

5. Die erforderlichen Informationen eingeben.

Migrationseinstellungen konfigurieren

1. Der Abschnitt *VM-Konfiguration hochladen* enthält Informationen zu dem Datensatz, mit dem ein Migrationsplan erstellt wird. Im Abschnitt **VM-Inventarübersicht** werden anhand der Inventardatei die Anzahl der VMs sowie die gesamte Storage-Kapazität angezeigt.
2. Wählen Sie im Abschnitt *VM inventory considerations* die Optionen aus, um die Liste der VMs zu filtern und zu konfigurieren, wie der Migrationsplan gestaltet wird:
 - a. **Überlegungen zur VM-Inventarisierung:** Wählen Sie aus, welche VMs basierend auf ihrem Energiestatus einbezogen werden sollen:
 - **Eingeschaltet** (standardmäßig ausgewählt)
 - **Ausgeschaltet**
 - **Ausgesetzt**

- b. **Zu berücksichtigender VM-Speicher:** Wählen Sie, wie Sie die Google Cloud NetApp Volumes-Datenspeicher dimensionieren:
 - **Ausgelastet:** Größe der Datenspeicher basierend auf der tatsächlich genutzten Kapazität der VMs.
 - **Bereitgestellt** (default): Größe der Datenspeicher basierend auf der insgesamt bereitgestellten Kapazität der VMs.
- c. **Zu berücksichtigender VM-Speicher:** Wählen Sie aus, wie die benötigten Google Cloud VMware Engine-Cluster-Rechenressourcen berechnet werden sollen:
 - **Ausgelastet:** Berechnung basierend auf der tatsächlichen Speichernutzung durch VMs.
 - **Bereitgestellt** (Standard): Berechnung basierend auf dem gesamten Speicher, der den VMs zugewiesen wurde.
- d. **Leistungsschätzung virtueller Maschinen:** Diese Option wird nur angezeigt, wenn Sie RVTools als Datenquelle verwenden. Wählen Sie das erwartete Leistungsniveau aus:
 - **Niedrig:** 50 IOPS im Durchschnitt pro VM.
 - **Standard:** 200 IOPS im Durchschnitt pro VM (standardmäßig ausgewählt).
 - **Hoch:** 800 IOPS im Durchschnitt pro VM.

3. Im Abschnitt :

- a. **Region:** Wählen Sie die Google Cloud-Region aus, in der Google Cloud VMware Engine und Google Cloud NetApp Volumes bereitgestellt werden sollen. In der Liste werden nur Regionen angezeigt, in denen beide Dienste verfügbar sind.

4. Im Abschnitt *VM-Speicherkapazität und Schutzüberlegungen:*

- a. **Prozentuale Kapazitätsreserve:** Geben Sie den Prozentsatz der zusätzlichen Kapazität ein, die für Wachstum hinzugefügt werden soll. Der Standardwert beträgt 20 %, was auch dem empfohlenen Minimum entspricht.



Wenn Sie weniger als 20% Spielraum auswählen, wird der Snapshot-Schutz automatisch deaktiviert.

- b. **VM-Snapshot-Schutz:** Aktivieren Sie diese Option (standardmäßig aktiviert), um VMs mit Snapshots mithilfe der ONTAP default snapshot policy zu schützen.

5. **Weiter** auswählen.

Wählen Sie eine Clusterkonfiguration aus

1. Auf der Seite **Bevorzugte Google Cloud VMware Engine cluster configuration auswählen** konfigurieren Sie Ihre Google Cloud VMware Engine cluster preferences und überprüfen die empfohlenen Konfigurationen.
2. Im Abschnitt *Architecture preferences:*
 - a. **Google Cloud VMware Engine VE2 node types zulassen:** Wenn diese Option aktiviert ist (Standardeinstellung), werden sowohl VE1- als auch VE2 node types berücksichtigt. Deaktivieren Sie diese Option, um die Konfigurationen auf VE1 nodes zu beschränken.
 - b. **Allow Google Cloud NetApp Volumes Standard-Volumes:** Wenn diese Option deaktiviert ist (Standard), werden in der Konfigurationsgestaltung nur die Servicelevel Premium und Extreme verwendet, was die empfohlene Best Practice ist. Premium- und Extreme-Volumes bieten regionale Verfügbarkeit und machen sie widerstandsfähig gegen Ausfälle von Verfügbarkeitszonen. Standard-Volumes bieten nur zonale Verfügbarkeit und sind nicht gegen AZ-Ausfälle geschützt. Aktivieren Sie diese Option, um Standard-Servicelevel-Volumes einzubeziehen, was die Kosten für Workloads mit

geringerer Leistung senken kann, bei denen keine Resilienz auf AZ-Ebene erforderlich ist.

3. Im Abschnitt *Clusterkonfiguration* überprüfen Sie die verfügbaren Google Cloud VMware Engine Cluster-Konfigurationen:

Die Konfigurationen sind nach geschätzten Gesamtkosten (niedrigste bis höchste) sortiert und zeigen verschiedene Kombinationen von:

- Google Cloud VMware Engine node types (VE1 oder VE2)
- Geschätzte Gesamtkosten
- Geschätzte Einsparungen
- Knotenanzahl
- VSAN-Fehlertoleranzeinstellungen: FTT (Fault Tolerance Type) und FTM (Fault Tolerance Method)
- Überschüssige Speicherkapazität in TiB
- Nur-Speicher-Knotentyp

4. Wählen Sie Ihre bevorzugte Clusterkonfiguration aus, indem Sie auf das Optionsfeld daneben klicken.

Die erste (kostengünstigste) Konfiguration ist standardmäßig ausgewählt.

5. **Weiter** auswählen.

Wählen Sie ein VM-Layout aus

1. Auf der Seite **Automatische VM-Auswahl** überprüfen Sie das optimale Layout der virtuellen Maschine, das automatisch basierend auf Ihrer benötigten externen Speicherkapazität und Ihren Präferenzen ausgewählt wurde.
2. Überprüfen Sie den Abschnitt *VM-Inventar*, der Folgendes anzeigt:

- Gesamtzahl der VMs
- Gesamtkapazität (bereitgestellt oder genutzt basierend auf Ihrer vorherigen Auswahl)

Sie können den Abschnitt erweitern, um die folgenden Details anzuzeigen:

- Aggregierte durchschnittliche IOPS
- Aggregierter Durchsatz (MB/s)
- Aggregierte Spitzen-IOPS
- Aggregierter Spitzendurchsatz (MB/s)

3. Wählen Sie im Abschnitt *VM selection preferences* die Optimierungsmethode aus:
 - **Kosten** (Standard): Weist VMs mit der höchsten I/O-Dichte dem vSAN-Speicher zu, was dazu beiträgt, die Google Cloud NetApp Volumes-Kosten zu minimieren und gleichzeitig die Leistungsanforderungen zu erfüllen.
 - **Schutz**: Weist VMs mit der höchsten Speicherkapazität den externen Google Cloud NetApp Volumes-Datenspeichern zu, was eine bessere Wiederherstellbarkeit durch die Snapshot- und Replikationsfunktionen von Google Cloud NetApp Volumes bietet.
4. Lesen Sie den Abschnitt *Konfiguration des externen Datenspeichers*, der zeigt, wie VMs und Kapazität zwischen Google Cloud NetApp Volumes und vSAN-Speicher verteilt werden.

Sie können den Abschnitt erweitern, um die folgenden Details anzuzeigen: * Aggregierte durchschnittliche

IOPS * Aggregierter Durchsatz (MB/s) * Aggregierte Spitzen-IOPS * Aggregierter Spitzendurchsatz (MB/s)

5. In der Tabelle *VMs ausgewählt für Google Cloud NetApp Volumes NFS-Dataspaces* können Sie:

- Sehen Sie sich die automatisch ausgewählten VMs basierend auf Ihrer gewählten Optimierungsmethode an.
- Wählen oder deaktivieren Sie einzelne VMs manuell mithilfe der Kontrollkästchen aus.
- VMs nach Cluster, Betriebssystem oder Datacenter filtern.
- Sortieren Sie VMs nach jeder sichtbaren Spalte (wie VM-Name, bereitgestellte Kapazität, durchschnittliche Lese-IOPS).
- Zeigen oder verbergen Sie zusätzliche Spalten, indem Sie auf  klicken.



Wenn Sie die VM-Auswahl manuell ändern, können Sie zur automatischen Auswahl basierend auf Ihren Optimierungspräferenzen zurückkehren, indem Sie **Zurücksetzen** auswählen.

6. **Weiter** auswählen.

NFS-Datenspeicherzuweisungen überprüfen

1. Auf der Seite **Review instance store assignment** überprüfen Sie das detaillierte Datenspeicherlayout und die VM-Zuordnungen.
2. Verwenden Sie die Registerkarten **Gesamt** und **Pro Datenspeicher**, um zwischen einer Gesamtansicht und Details pro Datenspeicher zu wechseln.
3. Auf der Registerkarte **Total**:
 - a. Überprüfen Sie das Diagramm zur *Speicherkapazitätsanalyse*, das Folgendes anzeigt:
 - Google Cloud NetApp Volumes logische Kapazität
 - VM-bereitgestellte Kapazität
 - Freier Speicherplatz auf VM-Ebene (wenn bereitgestellte Kapazität ausgewählt wurde)
 - Gesamtkapazitäts-Spielraum
 - Snapshot-Pufferkapazität (falls der Snapshot-Schutz aktiviert ist)
 - b. Lesen Sie den Abschnitt *Detaillierte Informationen*, der Folgendes enthält:
 - Gesamtkapazität der bereitgestellten VMs
 - Gesamtkapazitäts-Spielraum
 - Freier Speicherplatz (wenn bereitgestellte Kapazität ausgewählt wurde)
 - Gesamtkapazität aller Google Cloud NetApp Volumes-Speicherpools
 - Google Cloud NetApp Volumes Anzahl und Typen von Speicherpools
 - Gesamtzahl der VMs und bereitgestellte Kapazität
 - Aggregierte durchschnittliche VM-IOPS (wenn verfügbar)
 - Durchschnittliche E/A-Dichte (mit Tooltip zur Berechnungserklärung)
 - Aggregierter VM-Durchschnittsdurchsatz (sofern verfügbar)
4. In den Registerkarten **Pro Datenspeicher**:

- a. Wählen Sie eine Registerkarte „Datastore“ aus, um deren Details anzuzeigen.
- b. Überprüfen Sie die Details dieses Datastores, die Folgendes umfassen:
 - Kapazitätsaufschlüsselungsdiagramm
 - Datastore-Eigenschaften:
 - Gesamte von VMs genutzte Kapazität
 - Gesamtkapazitäts-Spielraum
 - Freier Speicherplatz (wenn bereitgestellte Kapazität ausgewählt wurde)
 - Logische Kapazität des Datastores
 - Servicelevel des Datastore (Standard, Premium, Extreme)
 - Gesamtzahl der VMs und bereitgestellte Kapazität
 - Aggregierte durchschnittliche VM-IOPS (wenn verfügbar)
 - Durchschnittliche E/A-Dichte des Datenspeichers (wenn verfügbar)
 - Aggregierter VM-Durchschnittsdurchsatz (sofern verfügbar)
- c. Überprüfen Sie die Tabelle *Virtuelle Maschinen*, in der alle diesem Datenspeicher zugewiesenen VMs mit Spalten für VM-Name, Kapazität, Cluster, Betriebssystem, IOPS, Durchsatz und andere Eigenschaften angezeigt werden.

5. **Weiter** auswählen.

Überprüfen und speichern Sie Ihren Bereitstellungsplan

1. Auf der Seite **Review your migration plan** überprüfen und passen Sie Ihren Bereitstellungsplan an, bevor Sie ihn speichern.
2. Wählen Sie aus dem Dropdown-Menü Ihren Tarif aus:
 - **On-demand** (Standard): Bezahlung nach Nutzung



Die auf der Bewertungsseite angezeigten Preise passen sich basierend auf Ihrem ausgewählten Tarif an.

3. Überprüfen Sie den Abschnitt *Geschätzte Einsparungen*:
 - a. Die Vergleichstabellen der *Google Cloud VMware Engine configuration alternatives* vergleichen:
 - Geschätzte monatliche Kosten der Google Cloud VMware Engine vSAN-only-Konfiguration (Compute-Nodes + Storage-only-Nodes)
 - Geschätzte monatliche Kosten für Google Cloud VMware Engine vSAN + externen Datenspeicher (Rechenknoten + Google Cloud NetApp Volumes externe Datenspeicher)
 - Ersparnisprozentsatz und Dollarbetrag
 - b. Die Tabelle „Aufschlüsselung der geschätzten Einsparungen“ vergleicht die beiden Konfigurationen mit Details zu Knotenanzahl, Speicherkapazität, Google Cloud NetApp Volumes-Poolinformationen sowie monatlichen und jährlichen Kosteneinsparungen.
4. Überprüfen Sie den Abschnitt *Vorgeschlagene Konfiguration für Google Cloud NetApp Volumes*. Er hebt hervor:
 - Anzahl und Typen der Speicherpools
 - Gesamtkapazität des Speicherpools

- Anzahl der Datastores (Volumes)
- Aggregierter Durchsatz von Datenspeichern
- Geschätzte monatliche Kosten
 - i. Der Abschnitt *Empfohlene Konfigurationsdetails* bietet eine Aufschlüsselung nach Servicelevel (Standard, Premium, Extreme) mit Angaben zu Speicherpoolanzahl, Kapazitäten, Datenspeicheranzahl, Durchsatzdetails, Kapazitätsreserve, Snapshot-Puffer und geschätzten monatlichen Gesamtkosten.
 - ii. Im Abschnitt *Geschätzte Kostenanalyse* werden die Kosten nach Servicelevel (Standard, Premium, Extreme) aufgeschlüsselt, einschließlich Kapazitätskosten, Kaltkapazität, replizierter Daten, Backup-Nutzung und -Kapazität, mit einer insgesamt geschätzten monatlichen Gesamtkosten.
 - iii. Die Tabelle *Volume configuration* listet jedes geplante Google Cloud NetApp Volumes-Volume mit Details wie Name, Pooltyp, Protokoll (NFSv3), Kapazität, Headroom, Snapshot-Richtlinie und Tiering-Richtlinie auf.

5. Lesen Sie die Abschnitte *Annahmen zum Lösungsdesign* und *Haftungsausschluss*.

6. Wenn Sie mit dem Migrationsplan zufrieden sind, haben Sie mehrere Möglichkeiten:

- Wählen Sie oben auf der Seite **Manage plan** aus.
- Zur Auswahl steht einer der folgenden Downloads:
 - **Bericht herunterladen:** Ein umfassendes PDF-Dokument mit allen Plandetails
 - **Download instance storage deployment:** Eine CSV-Datei, die VMs ihren zugewiesenen Datenspeichern zuordnet

7. Wählen Sie **Provision**, um die Google Cloud NetApp Volumes NFS-Datenspeicher mithilfe von Terraform Infrastructure-as-Code bereitzustellen.

In einer Codebox wird der generierte Terraform-Code angezeigt. Sie können den Code in Ihre Zwischenablage kopieren oder als Datei herunterladen, um ihn in Ihrer eigenen Terraform-Umgebung auszuführen.

8. Wählen Sie **Erstellen**, um die Google Cloud NetApp Volumes NFS-Datenspeicher zu erstellen.

Migration zu Amazon EC2

Erstellung eines Deployment-Plans für Amazon EC2 mit dem VMware workloads migration advisor

Die Anmeldung bei der NetApp Workload Factory ermöglicht den Zugriff auf den VMware migration advisor. Anschließend werden die Schritte im Assistenten befolgt, um einen Deployment- oder Migrationsplan zu erstellen, der an Ihre Anforderungen angepasst ist.

Beachten Sie, dass Sie für den Zugriff auf Workload Factory einen Benutzernamen und ein Passwort benötigen. Falls Sie noch keinen Zugriff haben, können Sie jetzt ein Konto erstellen. Die Anweisungen ["hier,"](#) stehen zur Verfügung.

Erstellung eines Deployment-Plans auf Basis einer lokalen vSphere Umgebung

Sie können Ihre aktuellen Konfigurationen virtueller Maschinen aus lokalen vSphere Umgebungen auf virtuelle Maschinen in Amazon EC2 migrieren und angepasste Amazon FSx for NetApp ONTAP Dateisysteme als externe Datastores verwenden.

Anforderungen

- Sie müssen "VM-Inventar hochgeladen" haben.

Schritte

1. Melden Sie sich bei der "NetApp Console" an.

2. Im Menü  ist **Workloads** > **VMware** auszuwählen.

Das Planungszentrum ist zu sehen.

3. Falls noch kein VM-Inventar hochgeladen wurde, ist die Option **VM-Inventar hochladen** zu verwenden; die entsprechenden Anweisungen finden sich in "VM-Inventardaten hochladen".
4. In der Liste erfolgt die Auswahl eines VM-Inventardatensatzes; für den Datensatz wird anschließend das Menü **Start planning** geöffnet.
5. **AWS native compute** auswählen.

Die Seite **Prepare for AWS Cloud onboarding** wird angezeigt.

6. Im Abschnitt „VM-Konfiguration hochladen“ wählen Sie  und anschließend die von RVTools erstellte .xlsx-Datei aus.

Der Abschnitt **Details zur Datenerfassung** enthält den Datumsbereich und die Anzahl der Stunden an Daten, die mithilfe des Onboarding Advisor Datensammlers erfasst wurden.

Der Abschnitt **VM-Inventarübersicht** wird anhand der Inventardatei ausgefüllt und zeigt die Anzahl der VMs sowie die gesamte Storage-Kapazität an.

7. Im Abschnitt „Überlegungen zur VM-Inventarisierung“ erfolgt die Auswahl der Optionen zum Filtern der Liste der VMs, die migriert werden sollen.
 - a. **Region:** Die Region auswählen, in der Amazon FSx for NetApp ONTAP Dateisysteme eingesetzt werden. Für optimale Performance und Kosteneffizienz ist dies in der Regel dieselbe Region, in der Ihr bestehendes Amazon EC2 SDDC eingesetzt wird.
 - b. Für die VMs in dieser Region ist ein prognostiziertes Performance Level auszuwählen. Wir empfehlen, mit einer niedrigeren IOPS-Einstellung zu beginnen. Sie können die provisionierten SSD-IOPS erhöhen, nachdem das Dateisystem erstellt wurde, wenn Workloads migriert oder eingesetzt werden:
 - **Standard bis hohe Performance:** Für VMs mit durchschnittlichen E/A-Raten zwischen 20 und 5000 IOPS.
 - **Sehr hohe Performance:** Für VMs mit durchschnittlichen E/A-Raten von mehr als 5000 IOPS.
 - **Sehr geringe Performance:** Für VMs mit einer durchschnittlichen E/A-Rate von weniger als 20 IOPS.

8. Im Abschnitt *Zielkapazität und Schutzüberlegungen* stehen einige Storage-Optionen zur Auswahl.

- a. **Zu berücksichtigender VM Storage:** Auswahl, ob die für jede integrierte VM erstellten Datastores auf Basis ihrer aktuell genutzten Größe (empfohlen) oder ihrer provisionierten Größe dimensioniert werden.

Die externen Datenspeicher werden mithilfe von Dateisystem-Volumes des Amazon FSx for NetApp ONTAP Dateisystems implementiert.

- b. **Durchschnittliches Datenreduktionsverhältnis:** Zur Auswahl stehen drei gängige Datenreduktionsverhältnisse. Verfügbar sind "1:1 - Keine Reduktion", "1:1.25 - 20 % Reduktion" oder "1:1.5 - 33 % Reduktion".

Help me decide ist auszuwählen, wenn Unklarheit darüber besteht, welches Verhältnis gewählt werden soll. Das Dialogfeld *Data reduction ratio assistant* wird angezeigt. Es sind alle Aussagen auszuwählen, die auf Ihren VM-Bestand und Ihre Storage-Umgebung zutreffen. Der Assistent empfiehlt eine geeignete Datenreduktionsrate. **Apply** ist auszuwählen, um das empfohlene Verhältnis zu verwenden.

- c. **Prozentualer Kapazitätspuffer:** Der Prozentsatz des Kapazitätswachstums, der zur Kapazität Ihrer FSx for ONTAP Dateisysteme hinzugefügt wird.

Wenn Sie einen Wert von weniger als 20 % auswählen, können Sie keine Volume-Snapshots zum Schutz und für langfristige Backups erstellen.

- d. **VM-Snapshot-Schutz:** Mit dieser Option lassen sich die VMs durch Snapshots schützen.

9. **Weiter** auswählen.

10. Auf der Seite **Scope** erfolgt die Auswahl der VMs aus der Liste, die in die AWS-Migration einbezogen werden sollen. Die Liste kann nach dem Energiestatus der einzelnen VMs sowie nach dem Datacenter und dem Cluster gefiltert werden, in dem sich die VM befindet.

In der VM-Liste können Sie auswählen, welche VM-Informationen als Spalten angezeigt werden sollen. Wenn Sie beispielsweise „Geschätzter Instanztyp“ auswählen, wird für jede VM eine Spalte mit dem geschätzten Amazon EC2 Instanztyp basierend auf den VM-Ressourcenanforderungen angezeigt.

11. **Weiter** auswählen.

12. Auf der Seite **Klassifizieren** erfolgt die Überprüfung der VM-Informationen, der Regeln für die Volume-Klassifizierung, der Volume-Zuweisungen und der Liste der Volumes, die im Rahmen des Deployments migriert werden, und anschließend die Auswahl von **Weiter**.



Wenn ein Volume Kapazitäts- oder Performanceanforderungen hat, die die Fähigkeiten eines Amazon FSx for NetApp ONTAP Dateisystems in einer bestimmten Region übersteigen, empfiehlt der Migrationsberater, das Volume auf einem Amazon EBS Dateisystem einzusetzen.

13. Auf der Seite **Paket** werden die EC2-Instanzen und die den verschiedenen FSx for ONTAP Clustern zugewiesenen Volumes überprüft, anschließend wird **Weiter** ausgewählt.
14. Auf der Seite **Plan überprüfen** werden die geschätzten monatlichen Einsparungen und Kostenschätzungen für alle VMs angezeigt, deren Migration geplant ist.

Im oberen Bereich der Seite werden die geschätzten monatlichen Einsparungen für FSx for ONTAP Dateisysteme und EBS Volumes angezeigt. Jeder Abschnitt lässt sich erweitern, um Details zur vorgeschlagenen Dateisystemkonfiguration, zur Aufschlüsselung der geschätzten Einsparungen, zu den Annahmen und zu den technischen Haftungsausschlüssen anzuzeigen.

Standardmäßig speichert das Planungscenter den Migrationsplan automatisch in der Liste der Pläne.

Wenn Sie mit dem Migrationsplan zufrieden sind, haben Sie mehrere Möglichkeiten:

- Über **Plan herunterladen > Bericht herunterladen** lässt sich der Deployment-Plan im .pdf-Format herunterladen, sodass er zur Überprüfung verteilt werden kann.
- Über **Download plan > Download instance storage deployment** kann der externe Datastore-Deployment-Plan im .csv-Format heruntergeladen und zum Erstellen Ihrer neuen Cloud-basierten intelligenten Dateninfrastruktur verwendet werden.

- Mit **Provision** beginnt das Deployment des empfohlenen Amazon FSx for NetApp ONTAP Dateisystems.

Einsatz des empfohlenen FSx for ONTAP Dateisystems

Nachdem Sie überprüft haben, dass das empfohlene FSx for ONTAP Dateisystem (oder in einigen Fällen mehrere Dateisysteme) Ihren genauen Anforderungen entspricht, können Sie Workload Factory verwenden, um das System in Ihrer AWS-Umgebung einzusetzen.

Die Anweisungen in "[Erstellung eines FSx for ONTAP Dateisystems in NetApp Workload Factory](#)" unterstützen Sie dabei, das FSx for ONTAP Dateisystem gemäß der von Workload Factory empfohlenen Konfiguration einzusetzen. Sie können die Schritte unter **Advanced create** in den Anweisungen verwenden, um das Dateisystem vollständig anzupassen.

Migration zu VMware Cloud on AWS

Erstellung eines Deployment Plans für VMware Cloud on AWS mit dem VMware workloads migration advisor

Die Anmeldung bei der NetApp Workload Factory ermöglicht den Zugriff auf den VMware migration advisor. Anschließend werden die Schritte im Assistenten befolgt, um einen Deployment- oder Migrationsplan zu erstellen, der an Ihre Anforderungen angepasst ist.

Bei der Migration zu VMware Cloud können Sie den Migrationsberater verwenden, um Ihre aktuelle lokale vSphere Umgebung zu VMWare cloud zu migrieren.

Beachten Sie, dass Sie für den Zugriff auf Workload Factory einen Benutzernamen und ein Passwort benötigen. Falls Sie noch keinen Zugriff haben, können Sie jetzt ein Konto erstellen. Die Anweisungen "[hier](#)," stehen zur Verfügung.

Erstellung eines Deployment-Plans auf Basis einer lokalen vSphere Umgebung

Sie können Ihre aktuellen Konfigurationen virtueller Maschinen aus lokalen vSphere-Umgebungen zu virtuellen Maschinen in VMware Cloud on AWS migrieren und angepasste Amazon FSx for NetApp ONTAP Dateisysteme als externe Datenspeicher verwenden.

Anforderungen

- Sie müssen die Inventardatei aus Ihren bestehenden Systemen mithilfe des migration advisor VM collector (.csv-Datei) oder von RVTools (.xlsx-Datei) erstellt haben.
- Sie müssen Zugriff auf die Inventardatei des Systems haben, von dem aus Sie sich bei Workload Factory anmelden.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Im Menü  ist **Workloads** > **VMware** auszuwählen.

Das Planungszentrum ist zu sehen.

3. Die Auswahl erfolgt über **Plan and create VMC**.
4. Den Typ der Inventardatei auswählen, mit der Workload Factory mit Ihrer aktuellen VM-Konfiguration

befüllt wird, und anschließend **Weiter** auswählen.

- Zum Verwenden der .csv-Datei, die mit dem VMware Datensammler erstellt wurde, ist **Use the migration advisor VMware data collector** auszuwählen.
- Die Option **RVTools verwenden** dient zur Verwendung der .xlsx-Datei, die Sie mit RVTools erstellt haben.

Die Seite „Vorbereitung auf das VMware Cloud Onboarding“ wird angezeigt.

5. Im Abschnitt „VM-Konfiguration hochladen“ erfolgt die Auswahl von  und anschließend der Datei, die verwendet werden soll.

- Bei Verwendung des Migration advisor VM collector erfolgt die Auswahl der .csv-Datei.
- Die .xlsx-Datei ist auszuwählen, wenn RVTools verwendet wird.

Die Angaben im Abschnitt „VM-Übersicht“ stammen aus der Inventardatei und umfassen die Anzahl der VMs sowie die gesamte Storage-Kapazität.

6. Im Abschnitt „Überlegungen zur VM-Inventarisierung“ erfolgt die Auswahl der Optionen zum Filtern der Liste der VMs, die migriert werden sollen.

- VMs berücksichtigen:** Hier wird angegeben, welche VMs basierend auf ihrem Betriebszustand aus der .csv-Datei extrahiert werden. Es können alle VMs oder nur die VMs einbezogen werden, die eingeschaltet, ausgeschaltet oder angehalten sind.
- Zu berücksichtigender VM Storage:** Auswahl, ob die für jede integrierte VM erstellten Datastores auf Basis ihrer aktuell genutzten Größe (empfohlen) oder ihrer provisionierten Größe dimensioniert werden.

Die externen Datenspeicher werden mithilfe von Dateisystem-Volumes des Amazon FSx for NetApp ONTAP Dateisystems implementiert.

- Zu berücksichtigender VM-Speicher:** Hier wählen Sie aus, ob der für jede integrierte VM zugewiesene Speicher auf Grundlage ihrer aktuell genutzten Größe (empfohlen) oder ihrer bereitgestellten Größe dimensioniert wird.

7. Im Abschnitt *VMware Cloud on AWS deployment configuration* sind Details zur erforderlichen VMware Cloud on AWS Konfiguration einzugeben.

- Region:** Wählen Sie die Region aus, in der die VMs und Amazon FSx for NetApp ONTAP Dateisysteme eingesetzt werden.

Für optimale Performance und Kosteneffizienz ist dies in der Regel dieselbe Region, in der Ihr bestehendes VMware Cloud on AWS SDDC ausgeführt wird.

- Geschätzte Performance-Anforderungen der VM:** Diese Option ist nur bei Verwendung von RVTools verfügbar. Der VM-Collector des Migration Advisor erfasst diese Informationen aus Ihrer Umgebung. Für Ihre neuen bereitzustellenden VMs werden die folgenden durchschnittlichen Performance-Parameter pro virtueller Maschine verwendet:

- **Durchschnittliche IOPS pro VM:** Eingabe der für Ihre Dateisysteme erforderlichen Anzahl an IOPS. Falls Sie sich nicht sicher sind, kann der Standardwert von 3 IOPS pro GiB SSD Storage für Amazon FSx for ONTAP Dateisysteme verwendet werden. Wenn beispielsweise 2.000 GiB Kapazität eingesetzt werden, entspricht dies 6.000 IOPS. Es empfiehlt sich, mit einer kleineren IOPS-Einstellung zu beginnen. Die bereitgestellten SSD IOPS können nach der Erstellung des Dateisystems erhöht werden, wenn Workloads migriert oder eingesetzt werden.
- **Durchschnittliche E/A-Blockgröße:** Die Größe jedes Blocks, der Lese- oder Schreibvorgänge

enthält. Die Standardgröße beträgt 4 KB. Eine größere Blockgröße kann für umfangreiches sequentielles Lesen und Schreib-Workloads vorteilhaft sein. Eine kleinere Blockgröße kann eine bessere Performance für Workloads bieten, die kleine zufällige Schreibvorgänge in Sparse-Dateien oder in große Dateien durchführen.

- **Durchschnittliches Schreibverhältnis:** Der prozentuale Anteil der Vorgänge, bei denen es sich für Ihre Workloads um Schreibvorgänge handelt. Das Standardverhältnis beträgt 30 % Schreibvorgänge und 70 % Lesevorgänge.

8. Im Abschnitt *Überlegungen zur VM-Speicherkapazität* stehen einige Storage Optionen zur Auswahl.

- a. **Durchschnittliches Datenreduktionsverhältnis:** Zur Auswahl stehen drei gängige Werte für die Datenreduktion. Zur Auswahl stehen "1:1 - Keine Reduktion", "1:1.25 - 20 % Reduktion" oder "1:1.5 - 33 % Reduktion".
- b. **Prozentualer Kapazitätspuffer:** Der Prozentsatz des Kapazitätswachstums, der zur Kapazität Ihrer FSx for ONTAP Dateisysteme hinzugefügt wird.

Wenn Sie einen Wert von weniger als 20 % auswählen, können Sie keine Volume-Snapshots für Schutz und langfristige Backups erstellen.

9. Nach Auswahl von **Next** wird die Seite „VMware cloud on AWS node configuration“ angezeigt.

Auf dieser Seite können Sie die VMware cloud on AWS Clusterkonfiguration mithilfe einer geschätzten Kosteneinsparungsanalyse und des empfohlenen Knotentyps definieren. Folgendes kann konfiguriert werden:

- a. **vSAN Architektur:** Hier wird ausgewählt, ob die vSAN Express Storage Architecture (ESA) oder die vSAN Original Storage Architecture (OSA) verwendet werden soll.
- b. **vSAN Fehlertoleranz:** Hier wird der für die VMs erforderliche Grad an Fehlertoleranz ausgewählt. Es kann „Auto“ gewählt werden, was empfohlen wird, oder aus einer Vielzahl von RAID Leveln ausgewählt werden.
 - RAID-1 (FTT 1): besteht aus einer exakten Kopie (oder einem Spiegel) eines Satzes von Daten auf 2 oder mehr Festplatten.
 - RAID-5 (FTT 1): besteht aus Striping auf Blockebene mit verteilter Parität. Die Paritätsinformationen werden auf 3 oder mehr Laufwerke verteilt, und es kann den Ausfall einer einzelnen Festplatte überstehen.
 - RAID-5 (FTT 2): besteht aus Block-Level-Striping mit verteilter Parität - die Paritätsinformationen werden auf 4 oder mehr Laufwerke verteilt, und es kann zwei gleichzeitige Festplattenausfälle überstehen.
 - RAID-6 (FTT 2): erweitert RAID 5 durch das Hinzufügen eines weiteren Paritätsblocks; daher verwendet es Block-Level-Striping mit zwei Paritätsblöcken, die auf alle Mitgliedsfestplatten verteilt sind. Es erfordert 4 oder mehr Festplatten und kann den gleichzeitigen Ausfall von zwei Festplatten überstehen.
- c. **Auswahlliste für die Knotenkonfiguration:** Hier wird ein EC2-Instanztyp für die Knoten ausgewählt.

10. Nach Auswahl von **Weiter** werden auf der Seite „Virtuelle Maschinen auswählen“ die VMs angezeigt, die den auf der vorherigen Seite angegebenen Kriterien entsprechen.

- a. Im Abschnitt „Auswahlkriterien“ erfolgt die Auswahl der Kriterien für die VMs, die Sie einsetzen möchten:
 - Basierend auf Kosten- und Performanceoptimierung
 - Basierend auf der Möglichkeit, Ihre Daten in Wiederherstellungsszenarien mithilfe lokaler Snapshots einfach wiederherzustellen

- Basierend auf beiden Kriteriengruppen: die niedrigsten Kosten bei gleichzeitig guten Wiederherstellungsoptionen

b. Im Abschnitt „Virtuelle Maschinen“ sind die VMs ausgewählt (markiert), die den auf der vorherigen Seite angegebenen Kriterien entsprechen. Eine Auswahl oder Abwahl von VMs ist möglich, wenn auf dieser Seite weniger oder mehr VMs eingebunden/migriert werden sollen.

Der Abschnitt **Empfohlenes Deployment** wird aktualisiert, wenn Sie Änderungen vornehmen. Durch Aktivieren des Kontrollkästchens in der Überschriftenzeile lassen sich alle VMs auf dieser Seite auswählen.

c. **Weiter** auswählen.

11. Auf der Seite **Datenspeicher-Bereitstellungsplan** ist die Gesamtzahl der VMs und Datenspeicher aufgeführt, die für die Migration empfohlen wurden.

a. Bei Auswahl jedes oben auf der Seite aufgeführten Datenspeichers wird angezeigt, wie die Datenspeicher und VMs bereitgestellt werden.

Am unteren Rand der Seite sind die Quell-VM (oder mehrere Quell-VMs) aufgeführt, für die diese neue VM und dieser neue Datenspeicher bereitgestellt werden.

b. Sobald Sie verstanden haben, wie Ihre Datenspeicher bereitgestellt werden, können Sie **Weiter** auswählen.

12. Auf der Seite **Bereitstellungsplan prüfen** finden Sie die geschätzten monatlichen Kosten für alle VMs, deren Migration geplant ist.

Im oberen Bereich der Seite sind die monatlichen Kosten für alle bereitgestellten VMs und FSx for ONTAP Dateisysteme beschrieben. Die einzelnen Abschnitte lassen sich erweitern, um Details zu „Empfohlene Amazon FSx for ONTAP Dateisystemkonfiguration“, „Geschätzte Kostenaufschlüsselung“, „Volume Konfiguration“, „Dimensionierungsannahmen“ und technischen „Haftungsausschlüssen“ anzuzeigen.

13. Wenn Sie mit dem Migrationsplan zufrieden sind, haben Sie mehrere Möglichkeiten:

- Für das Deployment der FSx for ONTAP Dateisysteme zur Unterstützung Ihrer VMs wird **Deploy** verwendet. ["Informationen zum Deployment eines FSx for ONTAP Dateisystems"](#).
- Mit **Download plan > VM deployment** lässt sich der Migrationsplan im .csv-Format herunterladen, sodass Sie ihn zum Erstellen Ihrer neuen Cloud-basierten intelligenten Dateninfrastruktur verwenden können.
- Über **Download plan > Plan report** können Sie den Migrationsplan im .pdf-Format herunterladen und zur Überprüfung verteilen.
- Mit **Export plan** lässt sich der Migrationsplan als Vorlage im .json-Format speichern. Der Plan kann zu einem späteren Zeitpunkt importiert und als Vorlage für das Deployment von Systemen mit ähnlichen Anforderungen verwendet werden.

Einsatz des empfohlenen FSx for ONTAP Dateisystems

Nachdem Sie überprüft haben, dass das empfohlene FSx for ONTAP Dateisystem (oder in einigen Fällen mehrere Dateisysteme) Ihren genauen Anforderungen entspricht, können Sie Workload Factory verwenden, um das System in Ihrer AWS-Umgebung einzusetzen.

Abhängig von den Richtlinien und Berechtigungen, die Sie Ihrem Workload Factory Konto hinzugefügt haben, können Sie das FSx for ONTAP Dateisystem vollständig mit Workload Factory einsetzen (im Modus

lesen/schreiben). Wenn Sie über weniger Berechtigungen (Nur-Lese-Modus) oder keine Berechtigungen (Basismodus) verfügen, müssen Sie die CloudFormation Informationen aus der Codebox verwenden und das FSx for ONTAP Dateisystem selbst in AWS einsetzen.

Anforderungen für Deployments in VMware Cloud on AWS

- Sie müssen VMware Cloud on AWS Software-Defined Data Center (SDDC) Version 1.20 oder höher verwenden, um FSx for ONTAP Dateisysteme einzusetzen.
- Das FSx for ONTAP Dateisystem darf nicht in derselben VPC eingesetzt werden, die während des SDDC Deployment verwendet wurde. Stattdessen muss es in einer neuen Amazon VPC eingesetzt werden, die Ihnen gehört, um die Integration von VMware Cloud on AWS mit Amazon FSx for NetApp ONTAP zu ermöglichen.
- Sie müssen das Dateisystem FSx for ONTAP in derselben AWS Region wie Ihr SDDC einsetzen.

Schritte

1. Am unteren Rand der Seite **Review plan** führt die Auswahl von **Deploy** zur Anzeige der Seite „Create an FSx for ONTAP file system“.

Die meisten Felder, die Ihr FSx for ONTAP Dateisystem definieren, sind anhand der von Ihnen bereitgestellten Informationen ausgefüllt. Es gibt jedoch einige Felder, die Sie auf dieser Seite ausfüllen müssen.

Sie können die Option „Schnell erstellen“ oder „Erweitert erstellen“ verwenden. „Erweitert erstellen“ bietet einige zusätzliche Storage-Parameter, die Sie anpassen können. "[Was diese beiden Optionen bieten](#)".

2. **AWS-Anmeldeinformationen:** Wählen Sie Anmeldeinformationen aus oder fügen Sie sie hinzu, die Workload Factory die erforderlichen Berechtigungen erteilen, um Ihr FSx for ONTAP file system direkt zu erstellen. Alternativ können Sie auch den CloudFormation Code aus Codebox auswählen und das FSx for ONTAP file system in AWS selbst einsetzen.
3. **Dateisystemname:** Geben Sie den Namen ein, den Sie für dieses FSx for ONTAP Dateisystem verwenden möchten.
4. **Tags:** Optional können Sie Tags hinzufügen, um dieses FSx for ONTAP Dateisystem zu kategorisieren.
5. Im Abschnitt „Netzwerk & Sicherheit“ erfolgt die Eingabe der folgenden Informationen:

- a. **Region & VPC:** Auswahl der Region und der VPC, in der das FSx for ONTAP Dateisystem eingesetzt wird.

Beim Einsatz von VMware Cloud on AWS sollte das Deployment in einer anderen VPC als der VPC erfolgen, in der VMware Cloud on AWS eingesetzt wird.

- b. **Sicherheitsgruppe:** Bei Verwendung der Option **Erweitert erstellen** können Sie die Standard-Sicherheitsgruppe für die FSx for ONTAP VPC auswählen, sodass der gesamte Datenverkehr auf das FSx for ONTAP Dateisystem zugreifen kann.

Zum Einschränken des Zugriffs anderer AWS Services auf das Dateisystem FSx for ONTAP kann eine eingehende Regel hinzugefügt werden. Dadurch wird die Anzahl offener Services begrenzt. Dies sind die minimal erforderlichen Ports und Protokolle:

Protokolle	Ports	Zweck
TCP, UDP	111	Portmapper (zum Aushandeln der in NFS-Anfragen verwendeten Ports)
TCP, UDP	635	NFS mountd (empfängt NFS-Mount-Anfragen)

Protokolle	Ports	Zweck
TCP, UDP	2049	NFS Netzwerkdatenverkehr
TCP, UDP	4045	Network Lock Manager (NLM, lockd) - Verarbeitet Sperranforderungen.
TCP, UDP	4046	Netzwerkstatusmonitor (NSM, statd) - Benachrichtigt NFS-Clients über Neustarts des Servers für die Sperrverwaltung.

a. **Verfügbarkeitszone:** Auswahl der Verfügbarkeitszone und des Subnetzes.

Sie sollten dieselbe Verfügbarkeitszone auswählen, in der Ihr VMware SDDC bereitgestellt ist, wenn Sie Gebühren für Cross-AZ-Datenverkehr vermeiden möchten.

b. **Verschlüsselung:** Bei Verwendung der Option **Advanced create** können Sie den Namen des AWS-Verschlüsselungsschlüssels aus der Dropdown-Liste auswählen.

c. **Zugriffskontrolle für Datenspeicher:** Bei Verwendung der Option **Erweiterte Erstellung** können Sie auswählen, ob alle Hosts auf die Datenspeicher zugreifen können oder ob nur bestimmte vSphere Clusterknoten in einem bestimmten Subnetz auf die Datenspeicher zugreifen können.

6. Im Abschnitt „Dateisystemdetails“ erfolgt die Eingabe der folgenden Informationen:

a. **ONTAP Zugangsdaten:** Eingabe und Bestätigung des ONTAP Passworts.

b. **Anmeldeinformationen für die Storage VM** (nur bei erweiterter Erstellung): Geben Sie das Kennwort für die Storage VM ein und bestätigen Sie es. Das Kennwort kann spezifisch für dieses Dateisystem sein, oder Sie können dasselbe Kennwort verwenden, das Sie für die ONTAP Anmeldeinformationen eingegeben haben.

7. Im Abschnitt **Summary** ist die FSx for ONTAP Dateisystem- und Datastore-Konfiguration zu sehen, die der VMware Migration Advisor auf Basis Ihrer Angaben entworfen hat.

8. Über **Erstellen** lässt sich das Dateisystem FSx for ONTAP einsetzen. Dieser Vorgang kann bis zu 2 Stunden dauern.

Optional können Sie im Codebox-Fenster die Option **Umleiten nach CloudFormation** auswählen, um das Dateisystem mithilfe eines CloudFormation Stack zu erstellen.

In beiden Fällen können Sie den Erstellungsfortschritt in CloudFormation überwachen.

Ergebnis

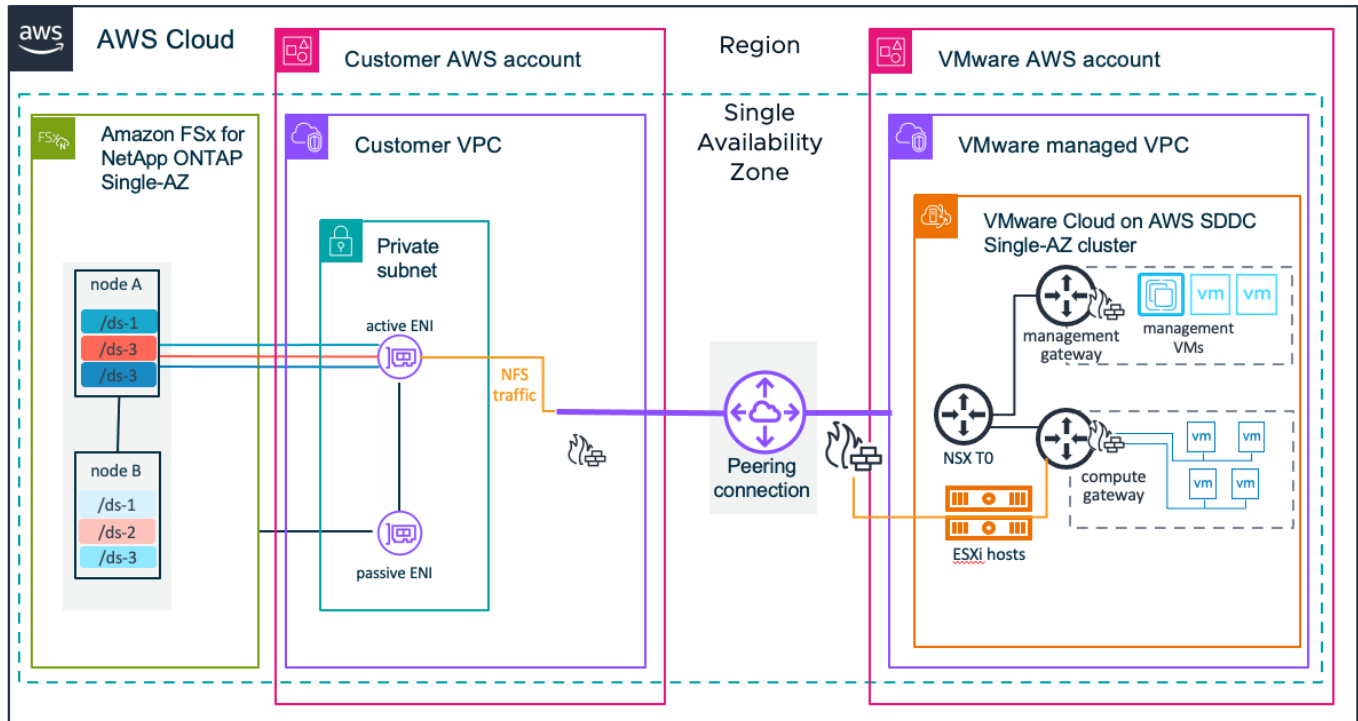
Das FSx for ONTAP Dateisystem wird eingesetzt.

Verbindung Ihrer FSx for ONTAP Dateisysteme mit VMware Cloud on AWS

Nach dem Einsatz von FSx for ONTAP Dateisystemen müssen Sie dieses System mit Ihrer VMware Cloud on AWS Infrastruktur verbinden. Ihr Software-Defined Data Center (SDDC) bietet Netzwerkoptionen für die Verbindung mit dem FSx for ONTAP Dateisystem, indem die VPC-Peering-Funktion genutzt wird, um die Netzwerkkonnektivität auf die externen NFS-Storage-Volumes zu erweitern.

["Einzelheiten enthält die Dokumentation zu Amazon VPC peering."](#)

Das folgende Diagramm zeigt die Verwendung von VPC Peering, um SDDC Cluster in einer einzelnen Availability Zone (AZ) mit FSx for ONTAP Single-AZ-Deployments zu verbinden.



Migration Ihrer Daten in die neue Infrastruktur mit NetApp Workload Factory for VMware

Mit einem Tool wie VMware Hybrid Cloud Extension (HCX) lassen sich Ihre Daten von Ihrem alten Storage virtueller Maschinen auf die FSx for NetApp ONTAP Volumes verschieben, die mit Ihren neuen virtuellen Maschinen verbunden sind. Die Kernfunktionalität von VMware HCX ermöglicht die transparente Migration von Workloads aus Ihrem lokalen Datacenter in Ihr Software-Defined Data Center (SDDC).

["Die Dokumentation zu VMware HCX"](#) für Details.

Was kommt als Nächstes?

Nachdem Sie Ihre Daten zu den externen Datastores von VMware Cloud on AWS und Amazon FSx for NetApp ONTAP migriert haben, können Sie die wichtigen Daten auf Ihrem FSx for ONTAP Dateisystem sichern und schützen, um sicherzustellen, dass Ihre Daten jederzeit verfügbar sind.

Informationen zur Verwaltung Ihres FSx for ONTAP Dateisystems finden Sie unter ["Amazon FSx for NetApp ONTAP Dokumentation"](#), wo die verfügbaren Sicherungs- und Schutzfunktionen angezeigt werden.

Optimierung von VMware Workloads auf FSx for ONTAP

Konfigurationsanalyse für EVS-Konfigurationen

Workload Factory analysiert regelmäßig Amazon Elastic VMware Service (EVS) Konfigurationen, um Abweichungen von Best Practices zu identifizieren. Nutzen Sie die Ergebnisse, um Leistung, Kosteneffizienz und Compliance zu verbessern.

Zu den wichtigsten Fähigkeiten gehören:

- Tägliche Konfigurationsanalyse

- Automatische Best-Practice-Validierungen
- Proaktive Beobachtbarkeit
- Erkenntnisse in die Praxis umsetzen

So funktioniert es

Workload Factory analysiert täglich Ihre Workloads, die auf unterstützten Cloud-Speichersystem-Bereitstellungen ausgeführt werden. Die Analyse liefert den Status einer Well-Architected-Architektur, Erkenntnisse und Empfehlungen.

Nach Abschluss der täglichen Analyse werden die Konfigurationen im Well-architected Dashboard für die Bereitstellung als „optimiert“ oder „nicht optimiert“ angezeigt. Konfigurationsprobleme sind nach Kategorie sowie in einer Liste mit Problemen und Empfehlungen zu finden. Empfehlungen zu den Konfigurationsproblemen können überprüft werden. Einige Probleme können automatisch von Workload Factory behoben werden, während andere manuelle Eingriffe erfordern. In diesem Fall stellt Workload Factory detaillierte Anweisungen bereit, um die empfohlenen Änderungen umzusetzen.

Sie können die Analyse von Konfigurationen, die für Ihre Umgebungen nicht relevant sind, ausblenden. Dadurch werden unnötige Warnmeldungen und ungenaue Optimierungsergebnisse vermieden.

Es besteht auch die Möglichkeit, benutzerdefinierte Regeln in einfacher Sprache zu erstellen, um Ihre Umgebungen anhand der Standards Ihres Unternehmens und der NetApp Best Practices zu validieren. Regeln können mit einem Probelauf getestet und anschließend für die Ausführung in Ihren Umgebungen terminiert werden. ["Weitere Informationen zu benutzerdefinierten Regeln"](#).

Warum es wichtig ist

Workload Factory wendet Best Practices auf große Storage-, Datenbank- und VMware-Umgebungen an, indem kontinuierliche Bewertungen mit Empfehlungseinblicken und Fehlerbehebungen kombiniert werden. Automatisierte Korrekturen in der NetApp Console reduzieren menschliche Fehler, gewährleisten einheitliches Management und erhalten Leistung und Zuverlässigkeit über Ihre Workload-Infrastrukturen hinweg.

Analyseanforderungen

Für eine vollständige Konfigurationsanalyse müssen Sie Folgendes tun:

- Stellen Sie eine Verknüpfung her. Die Verknüpfungskonnektivität ermöglicht es Workload Factory, alle Dateisystemkonfigurationen wie Datenschutz und Leistung zu analysieren.

["Erfahren Sie, wie Sie einen bestehenden Link verknüpfen oder einen neuen Link erstellen und verknüpfen"](#).

- Gewähren Sie *Anzeige-, Planungs- und Analyse-Berechtigungen* für VMware-Workloads.

["Erfahren Sie, wie Sie einem AWS-Konto Berechtigungen erteilen"](#)

- Sie müssen mindestens eine erkannte Amazon Elastic VMware Service-Umgebung in Ihrem AWS-Konto haben.

Bewährte Verfahren und Empfehlungen für EVS-Workloads

Workload Factory bietet Best Practices und Empfehlungen für den Betrieb gut entwickelter Amazon Elastic VMware Service (EVS) Workloads. Die Well-Architected-Analyse bewertet EVS-Konfigurationen, um sicherzustellen, dass Ihre VMware-Umgebungen für Zuverlässigkeit, Sicherheit, betriebliche Exzellenz,

Kostenoptimierung und Leistungseffizienz optimiert sind. Auf der Registerkarte „Well-Architected-Status“ in VMware finden Sie Einblicke und Empfehlungen, die Ihnen helfen, Well-Architected-Best-Practices für Ihre EVS-Umgebungen umzusetzen.

Die gut strukturierte Analyse kategorisiert Konfigurationen in den folgenden Säulen des Frameworks: *reliability* und *security*.

Zuverlässigkeit

Zuverlässigkeit gewährleistet, dass Arbeitslasten ihre beabsichtigten Funktionen korrekt und konsistent erfüllen, selbst wenn es zu Störungen kommt.

- **EVS-Umgebungsresilienz**

Stellen Sie sicher, dass Ihre EVS-Clusterknoten korrekt auf Partition Placement Groups verteilt sind. Alle Knoten sollten Mitglieder einer einzigen Partition Placement Group sein, die mit vier oder mehr Partitionen konfiguriert ist. Die richtige Partition Placement stellt sicher, dass Ihre EVS-Clusterknoten auf mehrere fehlerisolierte Hardwarepartitionen innerhalb einer AWS Availability Zone verteilt sind. Eine Fehlanordnung kann zu erheblichem Verlust an Rechenleistung oder Ausfallzeiten führen, wenn eine Partition ausfällt.

Sicherheit

Sicherheit betont den Schutz von Daten, Systemen und Vermögenswerten durch Risikobewertungen und Risikominderungsstrategien.

- **Cluster-Knoten-Verwaltung**

Stellen Sie sicher, dass Ihre EVS-Clusterknoten über einen geeigneten EC2-Stopp- und Beendigungsschutz verfügen. EVS ESXi-Knoten sollten ausschließlich mit vCenter oder anderen VMware-Verwaltungstools verwaltet werden. Ohne entsprechenden EC2-Schutz können Knoten versehentlich über die EC2-Konsole gestoppt oder beendet werden, was zur Nichtverfügbarkeit von virtuellen Maschinendaten oder zu Datenverlust führen kann.

Was kommt als Nächstes

["Implementieren Sie gut strukturierte Konfigurationen"](#)

Implementieren Sie gut strukturierte EVS-Konfigurationen

Nutzen Sie die Workload Factory-Konfigurationsanalyse, um den gut entwickelten Status Ihrer Amazon Elastic VMware Service (EVS)-Konfigurationen zu überprüfen und Probleme zu beheben, die sich auf Zuverlässigkeit, Sicherheit und Kosten auswirken.

Über diese Aufgabe

Automatische tägliche Scans aller erkannten EVS-Umgebungen mithilfe der AWS-APIs analysieren Ihre EVS-Konfiguration und identifizieren potenzielle Probleme, die die Verfügbarkeit, Ausfallsicherheit, Sicherheit oder Kostenoptimierung beeinträchtigen könnten. Die Ergebnisse sind nach Konfigurationsbereich geordnet, wobei jeder Befund Status, Schweregrad, Details zu den betroffenen Ressourcen und Schritt-für-Schritt-Anleitungen zur Behebung enthält.

Zu den wichtigsten Merkmalen gehören:

- **Automatische tägliche Scans:** Alle erkannten EVS-Umgebungen werden automatisch einmal täglich gescannt, um sicherzustellen, dass die Erkenntnisse aktuell bleiben.

- **AWS API-basiertes Scannen:** Scans nutzen AWS APIs und erfordern keine vSphere Anmeldeinformationen oder Konnektivität zu Ihrem vCenter.
- **Detaillierte Anleitung zur Problemlösung:** Jedes identifizierte Problem enthält eine klare Erklärung, den Schweregrad und schrittweise Verfahren zur Problemlösung.
- **Nur Ansichtsinformationen:** Bietet detaillierte Ergebnisse und Empfehlungen ohne automatisierte Optionen zur Problemlösung.

Verständnis von gut strukturierten Erkenntnissen

Die Registerkarte „Well-architected“ zeigt Folgendes an:

- **Konfigurationsname:** Der Konfigurationsbereich, der bewertet wird.
- **Tags:** Bezeichnungen, die die Wirkungsbereiche angeben (wie Verfügbarkeit, Ausfallsicherheit, Sicherheit).
- **Status:** Entweder "Optimized" (keine Probleme gefunden) oder "Not optimized" (Probleme gefunden).
- **Schweregrad:** Die Wichtigkeitsstufe des Findings (zum Beispiel Warning).
- **Ressourcentyp:** Der Typ der AWS-Ressource, die bewertet wird.
- **Anzahl der betroffenen Ressourcen:** Die Anzahl der von dem Problem betroffenen Ressourcen.

Scanfrequenz

Well-architected Scans werden automatisch für alle erkannten EVS-Konfigurationen durchgeführt. Wichtige Details zur Scanplanung:

- Scans erfolgen einmal pro Tag für jede EVS-Konfiguration.
- Scans für verschiedene Konfigurationen können zu unterschiedlichen Zeiten erfolgen.
- Wenn ein Scan für eine Konfiguration fehlschlägt, werden Scans für andere Konfigurationen im selben Konto dennoch versucht.
- Die Zeitstempelkarte auf der Registerkarte Well-architected-Status zeigt an, wann der letzte Scan für die aktuelle Konfiguration abgeschlossen wurde.



Die bedarfsgesteuerte Ausführung von gut strukturierten Scans wird derzeit nicht unterstützt. Alle Scans werden automatisch nach dem täglichen Zeitplan durchgeführt.

Bevor Sie beginnen

- Sie benötigen "[AWS-Anmeldeinformationen hinzugefügt](#)" mit den Berechtigungen *Anzeigen, Planen und Analysieren* für VMware Workloads.
- Sie müssen mindestens eine erkannte Amazon Elastic VMware Service-Umgebung in Ihrem AWS-Konto haben.

Greifen Sie auf die Registerkarte „Well-Architected-Status“ zu.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Im Menü  ist **Workloads > VMware** auszuwählen.

Das Planungszentrum ist zu sehen.

3. Wählen Sie im VMware-Menü **Inventory** aus.
4. Wählen Sie in der Liste **Virtualisierung environments** die gefundene EVS-Umgebung aus, für die Sie gut strukturierte Einblicke anzeigen möchten.
5. Wählen Sie die Registerkarte **Well-architected status** aus.

Folgende Elemente werden angezeigt:

- **Automatischer täglicher Analyse-Zeitstempel:** Zeigt an, wann der letzte Scan für diese Umgebung durchgeführt wurde.
- **Konfigurationen:** Organisiert die Ergebnisse nach Konfigurationsbereich und zeigt deren Status und Details an.

Gut konzipierte Assessments anzeigen

Clusterknotenverwaltung

Hierbei wird bewertet, ob auf Ihren EVS-Clusterknoten ein geeigneter EC2-Stopp- und Beendigungsschutz konfiguriert ist.

Status:

- **Optimiert:** Auf allen EVS-Knoten sind sowohl EC2-Stop-Schutz als auch Terminationsschutz konfiguriert.
- **Nicht optimiert:** Mindestens ein EVS-Knoten hat keinen EC2-Stop-Schutz oder Terminierungsschutz konfiguriert.

Warum das wichtig ist:

EVS ESXi-Knoten sollten ausschließlich mit vCenter oder anderen VMware-Verwaltungstools verwaltet werden. Ohne entsprechenden EC2-Schutz können Knoten versehentlich über die EC2-Konsole gestoppt oder beendet werden, was zur Nichtverfügbarkeit von virtuellen Maschinendaten oder zu Datenverlust führen kann.

Um detaillierte Ergebnisse anzuzeigen:

1. Suchen Sie auf der Registerkarte „Well-architected Status“ nach **Cluster node management**.
2. Wählen Sie **View**, um den Ergebnisdialog zu öffnen.

Im Dialogfeld wird Folgendes angezeigt:

- **Zusammenfassung der Findings:** Eine detaillierte Erläuterung des in Ihrer Umgebung festgestellten Problems.
- **Ressourcenübersicht:** Eine Tabelle, die alle EVS-Knoten und ihren Schutzstatus anzeigt, einschließlich:
 - Knotenkennung
 - EC2-Stoppstatus
 - EC2-Terminationsschutzstatus
- **Maßnahme erforderlich:** Schrittweise Problemlösungsverfahren.
- **Empfehlung:** Best-Practice-Leitfaden.

Behebung:

Um dieses Problem zu beheben, aktivieren Sie den Stopp- und Beendigungsschutz für Ihre EVS-Knoten:

- Befolgen Sie das in ["AWS documentation zum Aktivieren des Stoppschutzes"](#) angegebene Verfahren.
- Befolgen Sie das in ["AWS-Dokumentation zur Aktivierung des Termination Protection"](#) angegebene Verfahren.

EVS-Umgebungsresilienz

Dies bewertet, ob Ihre EVS-Clusterknoten ordnungsgemäß auf Partitionsplatzierungsgruppen verteilt sind.

Status:

- **Optimiert:** Alle Knoten sind Mitglieder einer einzigen Partition Placement Group, die mit vier oder mehr Partitionen konfiguriert ist.
- **Nicht optimiert**, wenn eine der folgenden Bedingungen zutrifft:
 - Knoten sind Mitglieder von mehr als einer Platzierungsgruppe.
 - Mindestens ein Knoten ist Mitglied einer nicht partitionierten Platzierungsgruppe.
 - Alle Knoten sind Mitglieder einer partitionierten Platzierungsgruppe mit weniger als vier Partitionen.

Warum das wichtig ist:

Die richtige Partition Placement stellt sicher, dass Ihre EVS-Clusterknoten auf mehrere fehlerisolierte Hardwarepartitionen innerhalb einer AWS Availability Zone verteilt sind. Eine Fehlanordnung kann zu erheblichem Verlust an Rechenleistung oder Ausfallzeiten führen, wenn eine Partition ausfällt.

Um detaillierte Ergebnisse anzuzeigen:

1. Suchen Sie auf der Registerkarte „Well-architected Status“ nach **EVS environment resiliency**.
2. Wählen Sie **View**, um den Ergebnisdiallog zu öffnen.

Im Dialogfeld wird Folgendes angezeigt:

- **Zusammenfassung der Ergebnisse:** Eine detaillierte Erklärung der Partitionierungsfehlausrichtung.
- **Ressourcenübersicht:** Eine Tabelle, die die EVS-Umgebungsknoten mit:
 - Knotenkennung
 - Name der Platzierungsgruppe
 - Platzierungsgruppentyp
 - Anzahl der Partitionen der Placement Groups
- **Aktion erforderlich:** Schrittweise Sanierungsverfahren
- **Empfehlung:** Best-Practice-Leitfaden

Behebung:

Um Probleme bei der Partitionsplatzierung zu beheben:

- Beim Hinzufügen neuer Knoten zur EVS-Umgebung stellen Sie die neuen Knoten mithilfe einer partitionierten Platzierungsgruppe mit mindestens vier Partitionen bereit.
- Wenn Clusterknoten ausgetauscht werden, stellen Sie sicher, dass die Ersatzknoten mithilfe einer partitionierten Platzierungsgruppe mit mindestens vier Partitionen bereitgestellt werden.
- Versuchen Sie, alle EVS-Knoten in einer einzigen Platzierungsgruppe zusammenzufassen, die mit den

oben genannten Empfehlungen übereinstimmt.

Best-Practice-Empfehlung:

Beim Erstellen oder Erweitern einer EVS-Umgebung stellen Sie alle Clusterknoten mithilfe einer einzigen partitionierten Platzierungsgruppe bereit, die mit vier oder mehr Partitionen konfiguriert ist.

Was kommt als Nächstes

Nach Überprüfung Ihrer gut strukturierten Erkenntnisse und der Umsetzung der empfohlenen Änderungen:

- Überprüfen Sie täglich die Registerkarte „Well-Architected Status“, um über den Status Ihrer Umgebung informiert zu bleiben.
- Befolgen Sie die Sanierungsverfahren für alle „Nicht optimiert“-Befunde.
- Überprüfen Sie die AWS- und NetApp-Dokumentation auf weitere Best Practices.
- Erwägen Sie, die Empfehlungen umzusetzen, bevor Sie Ihre EVS-Umgebung erweitern.

Verwandte Links

- ["Erstellen eines Deployment-Plans für Amazon EVS mithilfe des migration advisor"](#)
- ["Einsatz des empfohlenen FSx for ONTAP Dateisystems"](#)
- ["AWS placement groups Dokumentation"](#)

Referenz

Performance für FSx for ONTAP in NetApp Workload Factory

Einen Überblick über Performance finden Sie in der ["Amazon FSx for NetApp ONTAP Performance"](#)Dokumentation.

Sicherheit für FSx for ONTAP in NetApp Workload Factory

Die Dokumentation zu Amazon FSx for NetApp ONTAP enthält die folgenden Sicherheitsthemen als Referenz.

- ["Datensicherung in Amazon FSx for NetApp ONTAP"](#)
- ["Identitäts- und Zugriffsmanagement für Amazon FSx for NetApp ONTAP"](#)
- ["Dateisystemzugriffskontrolle mit Amazon VPC"](#) in der Amazon FSx for NetApp ONTAP Dokumentation

Workload Factory stellt Dokumentation zur Informationssicherheit bereit, um Sicherheits-Best-Practices innerhalb von Workload Factory und FSx for ONTAP zu verstehen und zu implementieren. ["Mehr erfahren"](#).

Google Cloud NetApp Volumes

Informationen zu Google Cloud NetApp Volumes

Google Cloud NetApp Volumes ist ein vollständig verwalteter, Cloud-basierter Datenspeicherdienst, der fortschrittliche Datenverwaltungsfunktionen und hochskalierbare Leistung bietet.

NetApp Volumes hilft dabei, die Bereitstellungszeiten zu beschleunigen, Ihre Workloads und Anwendungen zu verwalten und Workloads in die Cloud zu migrieren, während gleichzeitig die Leistung und die Funktionen des lokalen Speichers erhalten bleiben.

Features

- Lässt Unternehmensanwendungen schneller und effizienter laufen.
- Reduziert die Cloud-Storage-Kosten um bis zu 90 %.
- Erfüllt die Anforderungen an Betriebszeit, Verfügbarkeit und Sicherheit.
- Unterstützt NFS-, SMB- und Multiprotokollumgebungen.

Kosten

Von Google Cloud NetApp Volumes erstellte Volumes werden Ihrem Abonnement für den Dienst belastet, nicht über die NetApp Console.

Für die Ermittlung einer Google Cloud NetApp Volumes Region oder eines Volumes über die NetApp Console fallen keine Gebühren an.

Unterstützte Regionen

["Anzeige der unterstützten Regionen für Google Cloud NetApp Volumes"](#)

Hilfe erhalten

Für technischen Support kann eine Anfrage über das Google Cloud portal erstellt werden. Wählen Sie Ihr Google Cloud subscription und den Service **Google Cloud NetApp Volumes** unter **Storage** aus. Die erforderlichen Informationen sind zu vervollständigen.

Bei allgemeinen Fragen zu Google Cloud NetApp Volumes steht das Google Cloud Team von NetApp unter gcinfo@netapp.com per E-Mail zur Verfügung.

Bei technischen Problemen mit Ihren Cloud-Volumes können Sie über die Google Cloud Console ein Support-Ticket erstellen. Details finden Sie unter ["Support erhalten"](#).

Verwandte Links

- ["Google Cloud NetApp Volumes-Dokumentation"](#)
- ["NetApp Console Copy and Sync Dokumentation"](#)

Schnellstart für Google Cloud NetApp Volumes

Zum Einstieg in Google Cloud NetApp Volumes ist zunächst Google Cloud einzurichten und anschließend ein System zu erstellen.

1

"Einrichtung von Google Cloud NetApp Volumes"

Bei Google können Sie ein Dienstkonto erstellen.

2

"Rollen zuweisen"

Um mit Google Cloud NetApp Volumes arbeiten zu können, benötigen Sie die entsprechenden Berechtigungen, und Ihnen muss die Rolle „Google Cloud NetApp Volumes admin“ oder „Google Cloud NetApp viewer“ zugewiesen sein.

Add new roles

Associate role in organization, folder, or project

Add role

Organization, folder or project	Category	Role	
test-workspace x	Application	Google Cloud NetApp Volumes admin	

Add new roles

Cancel

Die Zuweisung der richtigen Rollen an Mitglieder erfolgt über die NetApp Console.

3

"Fügen Sie ein System hinzu"

In der NetApp Console wählen Sie nacheinander **Add System**, dann **Google Cloud Platform**, anschließend **Google Cloud NetApp Volumes** und schließlich **Discover** aus. Anzugeben sind die Details zum Servicekonto und zum Google Cloud-Projekt.

Einrichtung von Google Cloud NetApp Volumes

Die NetApp Console benötigt die entsprechenden Berechtigungen über ein Google Cloud-Dienstkonto.

Führen Sie die folgenden Aufgaben aus, damit NetApp Console auf Ihr Google Cloud-Projekt zugreifen kann.



Für diese Aufgaben können Sie die Google Cloud console oder die gcloud CLI verwenden. Um die gcloud CLI zu verwenden, müssen Sie ["Google Cloud CLI installiert"](#) zuerst haben.

- Falls noch kein bestehendes Servicekonto vorhanden ist, muss ein neues erstellt werden.
- Zugriff für Identitätsübernahme gewähren.
- Zuweisung der IAM-Rolle im gemeinsamen Projekt.

Ein Servicekonto einrichten



Änderungen an den Google Cloud-Projektberechtigungen können einige Minuten dauern, bis sie wirksam werden.

1. In der Google Cloud console, "[Zur Seite „Servicekonten“ wechseln](#)".
2. Nach Auswahl von **Projekt auswählen** wählen Sie Ihr Projekt aus und klicken auf **Öffnen**.
3. Zum Erstellen eines Dienstkontos sind die folgenden Schritte erforderlich:
 - a. Anschließend wählen Sie **Dienstkonto erstellen** aus.
 - b. Der Dienstkontoname (freundlicher Anzeigename) und eine Beschreibung werden eingegeben.

Die Google Cloud Console generiert anhand dieses Namens eine Dienstkonto-ID. Bei Bedarf lässt sich die ID bearbeiten; später ist keine Änderung mehr möglich.

- c. Der nächste Schritt ist die Auswahl von **Erstellen und fortfahren**.
- d. Wählen Sie in der Rollenliste die Rolle **Google Cloud NetApp Volumes Admin** oder **Google Cloud NetApp Volumes Viewer** aus.
- e. **Continue** ist auszuwählen.

Alternativ können Sie die Rolle auch über die gcloud CLI zuweisen:

```
gcloud projects add-iam-policy-binding <YOUR_PROJECT_ID>
--member="serviceAccount:<YOUR_SA_EMAIL>" --role="roles/netapp.admin"
```

- f. Für dieses Dienstkonto ist die Berechtigung zum Identitätswechsel zu erteilen: [credentials-sa@wf-production-netapp.iam.gserviceaccount.com](#). Weitere Informationen finden Sie unter "[Erstellung eines selbstsignierten JSON Web Token \(JWT\)](#)".

Das Dienstkonto im Besitz von NetApp wird verwendet, um ein kurzlebiges Zugriffstoken anzufordern, mit dem Sie als dieses Dienstkonto agieren können, ohne Zugriff auf seinen privaten Schlüssel zu benötigen.

Alternativ können Sie die Identitätswechselberechtigung über die gcloud CLI gewähren:

```
gcloud iam service-accounts add-iam-policy-binding <YOUR_SA_EMAIL>
--member="serviceAccount:credentials-sa@wf-production
-netapp.iam.gserviceaccount.com"
--role="roles/iam.serviceAccountTokenCreator"
--project=<YOUR_PROJECT_ID>
```

- a. Unten auf der Seite wird auf **FERTIG** geklickt, anschließend kann mit dem nächsten Schritt fortgefahren werden.

Gemeinsam genutzte VPC

Führen Sie in jedem weiteren Google Cloud-Projekt, das das Dienstkonto verwenden soll, folgende Schritte aus:

1. Auf der *IAM-Seite* erfolgt im Dropdown-Menü „Projekt“ die Auswahl des Projekts „Shared VPC host project“.
2. Sie wählen **Add Principal** aus.
3. Geben Sie im Feld „New principals“ die E-Mail-Adresse Ihres Servicekontos an.
4. Im Dropdown-Menü „Rolle auswählen“ erfolgt die Auswahl der Rolle **Google Cloud NetApp Volumes admin**.
5. Auf **Speichern** klicken.

Alternativ können Sie die IAM-Richtlinienbindung mithilfe der gcloud CLI hinzufügen:

```
gcloud projects add-iam-policy-binding <SHARED_VPC_HOST_PROJECT_ID>
--member="serviceAccount:<YOUR_SA_EMAIL>" --role="roles/netapp.admin"
```

Detaillierte Schritte sind in der Google Cloud-Dokumentation beschrieben:

- ["Erstellung und Verwaltung von Servicekonten"](#)
- ["Google Cloud NetApp Volumes Rollen und Berechtigungen"](#)
- ["Gewährung, Änderung und Entzug des Zugriffs auf Ressourcen"](#)

Fehlerbehebung

Falls ein Fehler auftritt, ist möglicherweise die Richtlinie **iam.disableCrossProjectServiceAccountUsage** erzwungen. Zur Behebung dieses Problems sind folgende Schritte erforderlich:

1. In der Google Cloud console ist dies unter ["Seite mit Unternehmensrichtlinien"](#) zu finden.
2. Die Richtlinie **Projektübergreifende Dienstkontonutzung deaktivieren** suchen und deaktivieren.

Was kommt als Nächstes?

["Zuweisung von Rollen für Google Cloud NetApp Volumes"](#).

Zuweisung von Rollen für Google Cloud NetApp Volumes

Um mit Google Cloud NetApp Volumes arbeiten zu können, müssen Sie den Mitgliedern in NetApp Console die richtigen Rollen zuweisen. Details sind unter ["Informationen zu NetApp Console Zugriffsrollen für alle Services"](#) verfügbar.

Zuweisen von Rollen zum Mitglied des Servicekontos

1. Sie melden sich bei der ["NetApp Console"](#) an.
2. Auszuwählen sind **Administration** und anschließend **Identity and access**.
3. Wählen Sie das Aktionen-Menü  neben dem Mitglied, dem Sie eine Rolle zuweisen möchten, und

wählen Sie **Rolle hinzufügen** aus.

4. Zum Hinzufügen einer Rolle sind die Schritte im Dialogfeld auszuführen:

- a. Ordner oder Projekt auswählen: Auswahl des Levels Ihrer Ressourcenhierarchie, für das das Mitglied Berechtigungen haben soll.

Wenn Sie einen Ordner auswählen, hat das Mitglied Berechtigungen für alles, was sich in diesem Ordner befindet.

- b. Im Dropdown-Menü **Kategorie** erfolgt die Auswahl der Rollenkategorie **Anwendung**. ["Informationen zu Zugriffsrollen"](#).
- c. Im Dropdown-Menü **Rolle** erfolgt die Auswahl einer Rolle, die dem Mitglied Berechtigungen für die Ressourcen zuweist, die dem ausgewählten Ordner oder Projekt zugeordnet sind.

Important: Sie müssen eine oder beide dieser Rollen hinzufügen:

- *Google Cloud NetApp Volumes Administrator* ODER
 - *Google Cloud NetApp Volumes Viewer*
- d. Rolle hinzufügen: Wenn Sie Zugriff auf zusätzliche Ordner oder Projekte innerhalb Ihres Unternehmens bereitstellen möchten, wählen Sie **Rolle hinzufügen**, geben Sie einen weiteren Ordner, ein weiteres Projekt oder eine weitere Rollenkategorie an und wählen Sie dann eine Rollenkategorie und eine entsprechende Rolle aus.

5. **Neue Rollen hinzufügen** auswählen.

Was kommt als Nächstes?

["Ein NetApp Volumes System zu Google Cloud hinzufügen"](#).

Hinzufügen von Google Cloud NetApp Volumes Anmeldedaten zu NetApp Workload Factory

Das Hinzufügen und Managen Ihrer Cloud-Anbieter-Zugangsdaten stellt sicher, dass NetApp Workload Factory über die erforderlichen Berechtigungen verfügt, um Ressourcen in Ihren Cloud-Anbieterkonten einzusetzen und zu managen.

Überblick

Sie können die Anmeldeinformationen für Google Cloud NetApp Volumes auf der Seite „Anmeldeinformationen“ in der NetApp console hinzufügen. Die Konsole bietet eine geführte Einrichtungsanleitung und einen Link zur Dokumentation, sodass Sie die erforderliche Google Cloud-Konfiguration abschließen und anschließend zurückkehren können, um das Hinzufügen der Anmeldeinformationen abzuschließen.

Mit diesem Workflow erhält Workload Factory die Berechtigungen, die zum Erkennen, Analysieren und Managen von Ressourcen in Ihrer Google Cloud-Umgebung erforderlich sind.

Die Erstellung der Zugangsdaten besteht aus drei Teilen:

- Schritt 1: Auswahl des Berechtigungsstufen-Levels, das Sie Workload Factory gewähren möchten.
- Schritt 2: Erstellen und Validieren eines Google Cloud-Dienstkontos sowie anschließendes Auswählen des zu managenden Google Cloud-Projekts.

- Schritt 3: Eingabe eines Namens für die Anmeldeinformationen sowie Hinzufügen der Anmeldeinformationen.

Bevor Sie beginnen

Sie benötigen Anmeldeinformationen, um sich bei Ihrem Google Cloud Konto anzumelden.

Schritte

1. Melden Sie sich bei der "[NetApp Konsole](#)" an.
2. Im Menü erfolgt die Auswahl von **Workloads > Administration > Credentials**.
3. Auf der Seite „Anmeldeinformationen“ ist die Option **Anmeldeinformationen hinzufügen** auszuwählen.
4. **Google Cloud NetApp Volumes** ist als Cloud-Anbieter auszuwählen.
5. Auf der Seite zum Hinzufügen von Google Cloud NetApp Volumes Anmeldeinformationen ist jeder Abschnitt unter **Berechtigungskonfiguration** auszufüllen.

Schritt 1: Berechtigungsrichtlinien erstellen

Schritte

1. Unter **Berechtigungsrichtlinien erstellen** ist **Anzeigen, planen und analysieren** standardmäßig ausgewählt. Diese Berechtigungsrichtlinie ermöglicht es Ihnen, die Storage Pools von Google Cloud NetApp Volumes anzuzeigen, Informationen zum Systemstatus zu erhalten, die Well-Architected-Analyse für Ihre Systeme abzurufen und Einsparpotenziale zu ermitteln.
2. Optional: **Betrieb und Fehlerbehebung** auswählen, wenn Workload Factory auch Google Cloud NetApp Volumes Ressourcen managen und Konfigurationsprobleme beheben soll.
3. Vor dem Fortfahren empfiehlt sich ein Blick auf die Einrichtungsanweisungen unter "[Einrichtung von Google Cloud NetApp Volumes](#)".

Schritt 2: Erstellen des Google Cloud Dienstkontos

Schritte

1. Abschnitt **Google Cloud-Umgebung einrichten** erweitern.
2. Die angezeigten Schritte 1-5 müssen abgeschlossen werden, um ein Google Cloud-Dienstkonto zu erstellen.
3. Die E-Mail-Adresse des Servicekontos kopieren.
4. Nach der Rückkehr zu Workload Factory können Sie die E-Mail-Adresse in das Feld **GCP service account** einfügen und **Validate credentials** auswählen.
5. Nach Abschluss der Validierung erfolgt im Dropdown-Menü **Projects** die Auswahl des Google Cloud-Projekts, das Workload Factory managen soll. HINWEIS: Die Projects-Liste ist erst verfügbar, nachdem die Anmeldeinformationen des Dienstkontos überprüft wurden.

Schritt 3: Den Namen der Anmeldeinformationen eingeben

Schritte

1. **Name der Anmeldeinformationen** erweitern.
2. Im Feld **Name** wird ein Name für die Anmeldedaten mit ausschließlich alphanumerischen Zeichen eingegeben. Sonderzeichen und Leerzeichen sind nicht zulässig.
3. Wählen Sie **Add**.

Ergebnis

Die Anmeldeinformationen für Google Cloud NetApp Volumes wurden Ihrem Konto hinzugefügt und stehen für unterstützte Workload Factory-Vorgänge zur Verfügung.

Konfigurationsanalyse für Google Cloud NetApp Volumes

Das Well-Architected Dashboard in der NetApp Console analysiert regelmäßig die Konfigurationen von Speichersystemen, um festzustellen, ob Konfigurationsprobleme vorliegen. Wenn Probleme gefunden werden, zeigt das Dashboard an, worin diese bestehen, und erläutert, welche Änderungen erforderlich sind, damit die Speichersysteme optimale Leistung, Kosteneffizienz und die Einhaltung bewährter Verfahren erreichen.

Zu den wichtigsten Fähigkeiten gehören:

- Tägliche Konfigurationsanalyse
- Automatische Validierung bewährter Verfahren für NetApp ONTAP Speichersysteme und Partner-Speicheranbieter
- Proaktive Beobachtbarkeit
- Erkenntnisse in die Praxis umsetzen

Analyseanforderungen

Für eine vollständige Analyse des Speicherpools sind die folgenden Schritte erforderlich:

- ["Ihr Google Cloud NetApp Volumes System zur NetApp Console hinzufügen"](#).
- Die Berechtigungen *Anzeigen*, *Planen* und *Analysieren* müssen in Ihrem Google Cloud-Konto vergeben sein.

["Informationen dazu, wie einem Google Cloud Konto Berechtigungen gewährt werden"](#)

Bewährte Verfahren und Empfehlungen für Speicher-Workloads

Workload Factory bewertet Speicherkonfigurationen anhand von Best Practices für Storage und ONTAP sowie des Google Cloud Well-Architected Framework. Die Bewertung empfiehlt außerdem Verbesserungen.

Die gut strukturierte Analyse kategorisiert Konfigurationen in den folgenden Säulen des Rahmenwerks: *Zuverlässigkeit* und *operative Exzellenz*.

Zuverlässigkeit

Zuverlässigkeit gewährleistet, dass Arbeitslasten ihre beabsichtigten Funktionen korrekt und konsistent erfüllen, selbst wenn es zu Störungen kommt.

- **Snapshot Policy**

Lokale Snapshots für effiziente Datensicherung und schnelle Wiederherstellung einplanen. Snapshots sind sofortige, zeitpunktgenaue Abbilder Ihrer Volumes.

- **SSD-Kapazitätsreserve**

Workload Factory empfiehlt, die SSD-Tier-Auslastung auf 80 % oder weniger zu halten. Einige Workloads benötigen möglicherweise zusätzlichen Kapazitätsspielraum und niedrigere Auslastungsziele. Wenn die

empfohlene Reserve überschritten wird, steigt das Risiko von Leistungseinbußen und Serviceproblemen, insbesondere wenn die Kapazität nicht rechtzeitig erweitert wird. Diese Einstellung kann für einen oder mehrere Speicherpools ausgeblendet und bei Bedarf später wieder aktiviert werden.

Operative Exzellenz

Operative Exzellenz konzentriert sich auf die Bereitstellung der optimalsten Architektur und des größten Geschäftswerts.

- **Freier Volumenkapazitätsspielraum**

Workload Factory empfiehlt, die Volume-Auslastung unter 80 % zu halten, um das Risiko von Speicherplatzengpässen zu minimieren. Wenn ein Volume schneller als erwartet wächst, könnte eine schnelle Erweiterung erforderlich sein. Dadurch kann das Risiko von Auswirkungen auf Anwendungen steigen, insbesondere bei plötzlichem oder sprunghaftem Wachstum. Dieses Risiko ist geringer, wenn Thin Provisioning und automatische Kapazitätsmanagement verwendet werden. Für ein oder mehrere Volumes kann diese Funktion deaktiviert und bei Bedarf später wieder aktiviert werden.

Was kommt als Nächstes

["Gut strukturierte Google Cloud NetApp Volumes Konfigurationen implementieren"](#)

Gut strukturierte Google Cloud NetApp Volumes Konfigurationen implementieren

Mit den Erkenntnissen und Empfehlungen aus der Konfigurationsanalyse lässt sich NetApp nutzen, um Best Practices für Ihre Google Cloud NetApp Volumes Speicherpools, die auf Google Cloud Storage laufen, umzusetzen. Der gut konzipierte Status kann einfach überprüft werden, Informationen zu Problemen mit den Konfigurationen stehen zur Verfügung, und es werden Empfehlungen gegeben, um die Architektur von Speicherpools zu verbessern, die nicht auf Zuverlässigkeit, Sicherheit, Leistung und Kosten optimiert sind.

["Informationen zur Konfigurationsanalyse und zum Well-Architected-Status."](#)

Über diese Aufgabe

NetApp analysiert Google Cloud NetApp Volumes Speicherpool-Bereitstellungen in Google Cloud täglich. Die tägliche Analyse liefert den Well-Architected-Status sowie Einblicke und Empfehlungen, um Konfigurationsprobleme nachvollziehen zu können, damit die Speicherpools den Best Practices entsprechen.

Nach Abschluss der täglichen Analyse zeigt das Dashboard die Gesamtzahl der Ressourcen mit Well-Architected-Status, die Anzahl der Ressourcen in einem kritischen Zustand und die Anzahl der Ressourcen in einem Warnzustand an. Die Konfigurationen werden nach den Säulen des Well-Architected-Frameworks kategorisiert: Zuverlässigkeit, operative Exzellenz, Kostenoptimierung, Leistungseffizienz und Sicherheit. Das Dashboard enthält außerdem eine Tabelle, in der alle Konfigurationen, der Well-Architected-Status dieser Konfigurationen, der Schweregrad, die Kategorie, der Ressourcentyp (Volume oder Speicherpool), betroffene Ressourcen und die Option zum Anzeigen der Empfehlung aufgeführt sind, wenn die Konfiguration nicht optimiert ist.

Bevor Sie beginnen

- Sie müssen "[einen Google Cloud NetApp Volumes Storage-Pool hinzufügen](#)" zur NetApp Console wechseln, um den Status der gut strukturierten Konfiguration und Empfehlungen für Konfigurationsprobleme anzuzeigen.

Empfehlungen zu Konfigurationsproblemen anzeigen

Nach Abschluss der täglichen Analyse können Sie Empfehlungen zu Konfigurationsproblemen einsehen. Empfehlungen erläutern bewährte Vorgehensweisen und potenzielle Risiken nicht optimierter Konfigurationen. Es besteht außerdem die Möglichkeit, eine CSV-Datei mit den Empfehlungen herunterzuladen.

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Wählen Sie im NetApp Console-Menü die Option **Workloads** und dann **Well-architected** aus.
3. Im Dashboard „Well-architected“ kann für jede Konfiguration die Option **Ansicht** ausgewählt werden.

Optional können Sie eine CSV-Datei mit den Empfehlungen für alle Konfigurationen herunterladen.

4. Die Empfehlung wird überprüft.

Konfigurationsanalyse verwerfen

Eine Konfigurationsanalyse für einen Google Cloud NetApp Volumes Speicherpool oder für ausgewählte Volumes wird gestoppt. Die Analyse kann bei Bedarf erneut gestartet werden.

Eine Konfigurationsanalyse für einen Speicherpool verwerfen

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Wählen Sie im NetApp Console-Menü die Option **Workloads** und dann **Well-architected** aus.
3. Im Dashboard „Well-architected“ kann für jede Konfiguration die Option **Ansicht** ausgewählt werden.
4. Suchen Sie unter Configurations die Konfiguration, die nicht auf Ihre Umgebung zutrifft, und wählen Sie dann **Dismiss**.
5. Im Dialogfeld „Konfiguration verwerfen“ **Verwerfen** auswählen, um die Konfigurationsanalyse zu beenden.

Eine Konfigurationsanalyse für ein Volume abbrechen

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Wählen Sie im NetApp Console-Menü die Option **Workloads** und dann **Well-architected** aus.
3. Im Dashboard „Well-architected“ kann für jede Konfiguration die Option **Ansicht** ausgewählt werden.
4. Unter „Konfigurationen“ die Konfiguration für die ausgewählten Volumes zum Verwerfen identifizieren und dann **Anzeigen** auswählen.
5. Die Volumes, die aus der Konfigurationsanalyse ausgeschlossen werden, identifizieren.
 - Für ein Volume: das Menü „Aktionen“ auswählen und dann **Volume ausblenden** auswählen.
 - Für mehrere Volumes: Die Volumes auswählen und dann neben **Bulk action** auf **Dismiss** klicken.

6. **Verwerfen** auswählen, um die Analyse für die Konfiguration zu beenden.
7. Im Dialogfeld „Volumes verwerfen“ **Verwerfen** auswählen, um zu bestätigen.

Ergebnis

Die Konfigurationsanalyse stoppt für den Speicherpool oder die ausgewählten Volumes.

Sie können die Analyse jederzeit reaktivieren.

Eine verworfene Konfigurationsanalyse reaktivieren

Eine verworfene Konfigurationsanalyse kann jederzeit reaktiviert werden. Eine oder mehrere Konfigurationen können zur Reaktivierung ausgewählt werden.

Eine Konfigurationsanalyse für einen Speicherpool reaktivieren

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Wählen Sie im NetApp Console-Menü die Option **Workloads** und dann **Well-architected** aus.
3. Wählen Sie **Verworfene Konfigurationen** aus.
4. Die gewünschte Konfiguration auswählen und **Reaktivieren** wählen.

Eine Konfigurationsanalyse für ein Volumen reaktivieren

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Wählen Sie im NetApp Console-Menü die Option **Workloads** und dann **Well-architected** aus.
3. Wählen Sie **Verworfene Konfigurationen** aus.
4. Das/die zu reaktivierende(n) Volumen wird/werden anhand der Konfigurationsanalyse identifiziert.
 - Für ein Volume: Wählen Sie das Aktionsmenü und dann **Volume reaktivieren**.
 - Für mehrere Volumes: Die Volumes auswählen und dann neben **Massenaktion** auf **Reaktivieren** klicken.

Ergebnis

Das System reaktiviert die Konfigurationsanalyse. Täglich findet eine neue Analyse statt.

OCI NetApp Storage Service

Informationen zu OCI NetApp Storage Service in NetApp Workload Factory

Oracle Cloud Infrastructure NetApp Storage Service (OCI NSS) ist ein vollständig verwalteter Service für Cloud-basierte Daten-Storage, der fortschrittliche Datenmanagement-Funktionen und hochskalierbare Performance bietet. OCI NSS ermöglicht das Erstellen und Managen von Storage-Pools als Storage-Backend für alle Ihre Workloads innerhalb von NetApp Workload Factory.

OCI NSS bietet die gleichen Funktionen, die gleiche Performance und die gleichen administrativen Möglichkeiten, die NetApp Kunden heute lokal nutzen, kombiniert mit der Einfachheit, Agilität, Sicherheit und Skalierbarkeit eines nativen Oracle Cloud-Service.

OCI NSS ist die *Storage*-Komponente in Workload Factory.

Features

OCI NSS bietet folgende Funktionen:

- **Vollständig verwalteter Service:** bietet einen vollständig verwalteten Service, der in die Workload Factory Konsole integriert ist.
- **Hohe Verfügbarkeit:** bietet hohe Verfügbarkeit für jeden OCI NSS Storage Pool und unterstützt Deployments mit einzelnen und mehreren Verfügbarkeitszonen.
- **Automatisierte Snapshots:** schützt Daten mit automatisierten, effizienten Snapshots, die nahezu sofort verfügbare, speichereffiziente, zeitpunktgenaue schreibgeschützte Kopien des Storage Pools oder der Volumes sind.
- **Volume-Replikation:** ermöglicht die Notfallwiederherstellung durch regionsübergreifende Replikation in Oracle Cloud Infrastructure.
- **Effiziente Backups:** sorgen mit einer Kopie der Daten in einer anderen Region für Notfälle für eine zusätzliche Schutzebene.
- **Schnelles Klonen:** beschleunigt die Applikationsentwicklung durch schnelles Klonen.
- **Unterstützung mehrerer Protokolle:** Unterstützung der Protokolle Network File System (NFS), Server Message Block (SMB) und Internet Small Computer Systems Interface (iSCSI).
- **Hoher Durchsatz:** bietet eine hohe Performance, um geringe Latenzzeiten für Workloads auf OCI NSS-Dateisystemen zu gewährleisten.
- **In-memory Cache und NVMe Cache:** umfasst einen einzigartigen In-memory Cache und NVMe Cache, der die Performance häufig abgerufener Daten steigert.
- **Hunderttausende IOPS:** bietet mit SSD-Festplatten Hunderttausende von IOPS und stellt so sicher, dass Ihr Storage und Ihre Workloads zeitnah Ergebnisse erhalten.
- **Thin Provisioning:** ermöglicht die Provisionierung von Kapazität im Voraus und spart Kosten, bis mehr Kapazität benötigt wird.
- **Datendeduplizierung und -komprimierung:** Doppelte Daten werden entfernt und Daten werden komprimiert, um den für OCI NSS-Dateisysteme erforderlichen physischen Storage zu reduzieren und dadurch Kosten zu sparen.

- **Data Tiering:** ermöglicht die Reduzierung der Storage-Kosten durch das Verschieben von seltener abgerufenen Daten vom primären Storage-Tier mit Performance SSDs auf das Storage-Tier des sekundären Kapazitätspools.

Tools zur Verwendung von NetApp Workload Factory

Sie können NetApp Workload Factory mit den folgenden Tools verwenden:

- **NetApp Console:** NetApp Console bietet eine hybride Benutzeroberfläche, sodass Sie Workload Factory zusammen mit anderen NetApp Datenservices verwenden können.
- **Ask Me:** Mit dem KI-Assistenten Ask Me können Sie Fragen stellen und mehr über Workload Factory erfahren, ohne die Workload Factory Konsole zu verlassen. Ask Me ist über die Workload Factory Benutzeroberfläche zugänglich.
- **CloudShell CLI:** Workload Factory umfasst eine CloudShell CLI, um AWS- und NetApp Umgebungen kontenübergreifend über eine einzige browserbasierte CLI zu managen und zu betreiben. Der Zugriff auf CloudShell erfolgt über die obere Leiste der Workload Factory Konsole.
- **REST API:** Mit den Workload Factory REST APIs können Sie Ihre OCI NSS-Systeme und -Ressourcen einsetzen und managen.
- **Oracle Cloud Infrastructure (OCI) Resource Manager:** Mit dem OCI Resource Manager lassen sich die in der Workload Factory console definierten Aktionen ausführen, um OCI- und Drittanbieterressourcen aus dem Resource Manager-Stack in Ihrem OCI-Konto zu modellieren, zu provisionieren und zu managen.
- **NetApp Terraform Provider:** Mit Terraform können Infrastruktur-Workflows erstellt und verwaltet werden, die in der Workload Factory Konsole generiert wurden.

Hilfe erhalten

Informationen zu allgemeinen Fragen über Workload Factory oder Workload Factory Applikationen und Services finden Sie unter ["Hilfe zu OCI NSS für Workload Factory"](#).

Schnellstart für Oracle Cloud Infrastructure NetApp Storage Service in NetApp Workload Factory

Der Einstieg in Oracle Cloud Infrastructure NetApp Storage Service (OCI NSS) erfolgt durch das Hinzufügen von Anmeldeinformationen und Berechtigungen, das Erstellen einer Verknüpfung bei Bedarf sowie das Erstellen oder Erkennen eines Storage-Systems.

Die folgenden Schritte erleichtern den Einstieg.

1

Anmeldeinformationen und Berechtigungen hinzufügen

["Hinzufügen von Anmeldeinformationen zu einem Konto"](#). Dies umfasst die Auswahl der Workload-Funktionen und die Erstellung der IAM-Richtlinien für die erforderlichen Berechtigungen.

Auswahl der standardmäßigen ["Ansicht, Planung und Analyse"](#) Berechtigungsrichtlinie.

2

Link erstellen

Dieser Schritt ist optional. Für einige Verwaltungsaufgaben in der NetApp Console ist ein NetApp Workload

Factory Link erforderlich. Ein *Link* nutzt OCI Functions, um eine Vertrauensbeziehung und Konnektivität zu Ihren OCI NSS Systemen herzustellen.

- ["Informationen dazu, wann ein Console Agent oder Link für die OCI NSS-Verwaltung erforderlich ist"](#)
- ["Informationen zum Erstellen eines Links"](#)

3

OCI NetApp Storage Service-System erkennen oder hinzufügen

Zu Beginn des Managements Ihrer OCI NSS-Ressourcen in Workload Factory wird ein Storage-Pool ermittelt. Im ["NetApp Console"](#) finden Sie unter **Storage** und dann unter **Management** den Eintrag **Discoverable systems**. ["Informationen zum Erkennen eines OCI NSS Storage-Systems"](#).

Was kommt als Nächstes

Mit einem Storage Pool in Ihrem Storage Inventar können Sie Ihre OCI NSS-Ressourcen managen.

Hinzufügen von Oracle Cloud Infrastructure-Anmeldeinformationen zu NetApp Workload Factory

Das Hinzufügen und Managen Ihrer Cloud-Anbieter-Zugangsdaten stellt sicher, dass NetApp Workload Factory über die erforderlichen Berechtigungen verfügt, um Ressourcen in Ihren Cloud-Anbieterkonten einzusetzen und zu managen.

["Berechtigungen für OCI NetApp Storage Service"](#)

Über diese Aufgabe

Auf der Seite „Credentials“ können Sie einem bestehenden Workload Factory Konto Zugangsdaten hinzufügen. Dadurch erhält Workload Factory die erforderlichen Berechtigungen, um Ressourcen und Prozesse in Ihrer Cloud-Umgebung zu managen.

Bevor Sie beginnen

Sie benötigen Anmeldeinformationen, um sich bei Ihrem Oracle Cloud Infrastructure Konto anzumelden.

Schritte

1. Melden Sie sich bei der ["NetApp Konsole"](#) an.
2. Im Menü erfolgt die Auswahl von **Workloads** > **Administration** > **Credentials**.
3. Auf der Seite „Anmeldeinformationen“ ist die Option **Anmeldeinformationen hinzufügen** auszuwählen.
4. Auf der Seite „Anmeldeinformationen für den Oracle Cloud Infrastructure NetApp Storage Service hinzufügen“ ist Folgendes auszuführen:
 - a. Unter „Berechtigungskonfiguration“ werden die entsprechenden Berechtigungen für die Anmeldeinformationen des Oracle Cloud Infrastructure NetApp Storage Service ausgewählt. **Anzeigen, planen und analysieren** ist die Standardberechtigung. Diese Berechtigungsrichtlinie ermöglicht das Anzeigen von OCI NSS Storage-Pools, Informationen zum Systemstatus, den Erhalt der Well-Architected-Analyse für Ihre Systeme und die Prüfung von Einsparpotenzialen.
 - b. Die mit der Oracle Cloud Console bereitgestellten manuellen Schritte ermöglichen das Abschließen der Berechtigungskonfiguration für die OCI NSS-Anmeldeinformationen.
 - c. Unter *Name der Anmeldeinformationen* sind der Name einzugeben, der für diese Anmeldeinformationen verwendet werden soll, sowie die Mandanten-OCID.

5. Wählen Sie **Add**.

Was kommt als Nächstes

["Schnellstart für Oracle Cloud Infrastructure NetApp Storage Service in NetApp Workload Factory."](#)

Erstellen oder Auffinden von Oracle Cloud Infrastructure NetApp Storage Service-Systemen in NetApp Console

In der NetApp Console können Oracle Cloud Infrastructure NetApp Storage Service (OCI NSS) Systeme erkannt sowie Volumes und zusätzliche Datenservices gemanagt werden.

Ein vorhandenes Cloud Storage-System entdecken

Die Erkennung Ihrer Storage Systeme erfolgt auf der Seite Discoverable systems.

Bevor Sie beginnen

Ihre Zugangsdaten für Ihre OCI NSS-Umgebung in Workload Factory.

Über diese Aufgabe

Sie können ein Cloud Storage-System innerhalb eines Kontos nur einmal erkennen und es einem Arbeitsbereich zuordnen. Das Storage-System kann später entfernt und einem anderen Arbeitsbereich neu zugeordnet werden.

Schritte

1. Im Menü NetApp Console erfolgt die Auswahl von **Storage**, dann **Management** und anschließend **Discoverable systems**.
2. Die Anzahl der ermittelten Cloud Storage-Systeme wird angezeigt. Die Auswahl erfolgt über **Discover**.
3. Zum Hinzufügen zur Seite „Systeme“ ist die Auswahl eines oder mehrerer Storage-Systeme und von **Discover** erforderlich.



- Wenn Sie ein unbenanntes Storage-System auswählen, erhalten Sie eine Aufforderung, einen Namen für das System einzugeben.
- Wenn Sie ein Storage-System auswählen, für dessen Management über die Console nicht die erforderlichen Anmeldeinformationen vorhanden sind, wird eine Aufforderung angezeigt, Anmeldeinformationen mit den erforderlichen Berechtigungen auszuwählen.

Ergebnis

Die Console zeigt Ihr erkanntes System auf der Seite „Systeme“ an. Sie können Ihre Storage-Systeme auf verschiedene Weise managen, beispielsweise über Workloads in der NetApp Console sowie mit ONTAP System Manager oder mit den Storage-Management-Tools Ihres Cloud-Providers.

Herstellen einer Verbindung mit einem Oracle Cloud Infrastructure NetApp Storage Service Storage-System über einen Link

Für erweiterte Storage-Management-Vorgänge ist eine Verbindung zwischen Ihrem NetApp Workload Factory Konto und einem Oracle Cloud Infrastructure NetApp Storage

Service (OCI NSS) System erforderlich. Dieser Prozess umfasst das Erstellen und Verknüpfen eines Links mit Ihrem Storage-System. Die Verknüpfung ermöglicht Ihnen, bestimmte Funktionen direkt über das OCI NSS System zu überwachen und zu managen, die über OCI APIs nicht verfügbar sind.

["Weitere Informationen zu Links"](#).

Über diese Aufgabe

Ein *Link* in Workload Factory ist eine OCI Functions Applikation in Ihrem Mandanten. Workload Factory verwendet ihn zur Kommunikation mit dem ONTAP System in einem OCI NSS Storage Pool (HTTPS 443 und SSH 22).

Links verwenden OCI Functions, um Code als Reaktion auf Ereignisse auszuführen und die für diesen Code erforderlichen Computing-Ressourcen automatisch zu managen. Die von Ihnen erstellten Links sind Teil Ihres NetApp Kontos und einem Oracle Cloud Infrastructure Konto zugeordnet.

Sie setzen den Link bzw. die Funktion mit Terraform ein und registrieren dann die Funktions-OCID in Workload Factory.

Dieser Stack wird in Ihrem Mandanten mit Ihrem OCI-Benutzer ausgeführt. Es handelt sich nicht um die mandantenübergreifende Anmeldeinformationsrichtlinie. Diese Richtlinie gehört beim Hinzufügen von Anmeldeinformationen in das Stammverzeichnis des Mandanten; sie wird zum Erstellen einer Verknüpfung nicht erneut erstellt.

Was Terraform erstellt

Ressource	Beispielname
Functions Applikation	netapp-wf-app-<suffix>
Funktion	netapp-wf-function-<suffix>
Protokollgruppe + Funktionsaufrufprotokoll	netapp-wf-link-logs-<suffix>
Dynamische Gruppe + vault-read-Richtlinie	Nur wenn Sie Local OCI Vault Authentication aktivieren (netapp-functions-dg, in der Tenancy gemeinsam genutzt)

Neuen Link erstellen

Sie können beim Definieren eines OCI NSS Systems in Ihrem Konto eine Verknüpfung erstellen. Sie verwenden die Verknüpfung für dieses Storage-System und können sie auch für andere OCI NSS Systeme nutzen. Sie können eine Verknüpfung für ein Storage-System auch später zuordnen.

Links erfordern eine Authentifizierung. Sie können Links mithilfe von Anmeldeinformationen authentifizieren, die im Anmeldeinformationsdienst von Workload Factory oder in OCI Vault gespeichert sind. Pro Link wird nur ein Authentifizierungsverfahren unterstützt. Wenn Sie beispielsweise die Link-Authentifizierung mit OCI Vault auswählen, können Sie das Authentifizierungsverfahren später nicht mehr ändern.



OCI Vault wird nicht unterstützt, wenn ein Console agent verwendet wird.

Bevor Sie beginnen

- Sie haben die Anmeldeinformationen für Workload Factory für den Mandanten hinzugefügt.
- Sie können sich bei der OCI Console für den Mandanten und die Region anmelden, in der sich der Storage-Pool befindet.
- Netzwerk:
 - Ein **privates Subnetz** im VCN, das die ONTAP Management LIF erreichen kann
 - Ein **Service Gateway** mit einer Route zu allen <Region> Services im Oracle Services Network (zum Abrufen des Funktionsabbilds erforderlich)
- Für die Gruppe, die den Stack einsetzt, ist eine IAM-Richtlinie erforderlich. Weitere Informationen zu "[OCI NSS Berechtigungen](#)".

Die Gruppe benötigt die Berechtigung, den Stack und die Funktion zu erstellen. Dabei sind <deploy-group> und <compartment-name> durch Ihre Werte zu ersetzen. Verwendet wird eine benannte Gruppe, nicht any-user.

```
Allow group <deploy-group> to manage orm-stacks in compartment
<compartment-name>
Allow group <deploy-group> to manage orm-jobs in compartment
<compartment-name>
Allow group <deploy-group> to manage functions-family in compartment
<compartment-name>
Allow group <deploy-group> to manage log-groups in compartment
<compartment-name>
Allow group <deploy-group> to use virtual-network-family in compartment
<compartment-name>
```

Wenn Sie die **lokale OCI Vault-Authentifizierung** aktivieren, ist Folgendes hinzuzufügen:

```
Allow group <deploy-group> to manage dynamic-groups in tenancy
Allow group <deploy-group> to manage policies in compartment
<compartment-name>
```

Der Stack erstellt (oder verwendet wieder) dann eine dynamische Gruppe netapp-functions-dg, damit die Funktion das Vault-Geheimnis lesen kann. Übereinstimmungsregel:

```
ALL {resource.type = 'fnfunc', resource.compartment.id = '<compartment-
ocid>'}
```

Vault-Richtlinie in dem Compartment, in dem sich die Funktion und das Secret befinden:

```
Allow dynamic-group netapp-functions-dg to read secret-bundles in
compartment <compartment-name>
Allow dynamic-group netapp-functions-dg to use keys in compartment
```

<compartment-name>

Schritte

Für die Erstellung und Registrierung des Links in Workload Factory stehen die OCI CLI oder OCI Terraform zur Verfügung.

1. Die Auswahl erfolgt im Menü  **Administration > Links**.
2. Auf der Seite „Links“ erfolgt die Auswahl von **Link erstellen und zuordnen > OCI NetApp Storage Service**.
3. Im Dialogfeld „Link hinzufügen“ unter **Details** sind die folgenden Angaben erforderlich:
 - a. **Linkname**: Geben Sie den Namen ein, den Sie für diesen Link verwenden möchten. Der Name muss innerhalb Ihres Kontos eindeutig sein.
 - b. **OCI Vault**: Optional. Ermöglicht Workload Factory das sichere Abrufen von ONTAP Anmeldedaten aus Ihrem OCI Vault.

Der Link Deployment Stack fügt der OCI Functions-Berechtigungsrichtlinie den folgenden Standard-Regex für OCI Vault Secret OCID hinzu:

```
ocid1.vaultsecret.oc1.iad.<unique_id>.ONTAPSecret*.
```

Sie können entweder Secrets erstellen, die dem Standard-Regex entsprechen, oder den Regex in der Terraform Konfigurationsdatei aktualisieren, damit er mit Ihrer Secret-OCID übereinstimmt.

- a. **Tags**: Optional lassen sich bis zu 50 Tags hinzufügen, um sie mit diesem Link zu verknüpfen und Ihre Ressourcen so einfacher zu kategorisieren. Beispielsweise lässt sich ein Tag hinzufügen, das diesen Link als von OCI NSS storage systems verwendet kennzeichnet.
- b. **Linkregistrierung**: Die Anweisungen zum Registrieren des Links finden Sie in der Workload Factory Konsole. Die Linkregistrierung erfolgt in Ihrer OCI Terraform-Umgebung. Die Anweisungen sind in der Codebox unter OCI Terraform verfügbar.
- c. **Linkzuordnung**: Hier werden das OCI NSS Storage-System für diesen Link sowie Benutzername und Passwort angegeben.
- d. **Linkberechtigungen**: Erforderliche Berechtigungen für die Benutzergruppe zum Erstellen des Links.

Erforderliche Berechtigungen für den Link

```
Allow group to manage orm-stacks in compartment id
Allow group to manage orm-jobs in compartment id
Allow group to manage dynamic-groups in tenancy
Allow group to manage policies in compartment id
Allow group to manage functions-family in compartment id
Allow group to manage log-groups in compartment id
Allow group to use virtual-network-family in compartment id
```

4. Im Dialogfeld „Link hinzufügen“ sind unter **Standort** folgende Angaben erforderlich:
 - a. **OCI tenancy**: Eingabe des OCI-Mandanten.
 - b. **Compartment**: Hier wird das Compartment eingegeben.

- c. **Region**: Die Region auswählen.
- d. **Subnetz**: Auswahl des Subnetzes.
- e. **Netzwerksicherheitsgruppe**: Die Sicherheitsgruppe wird eingegeben.

Workload Factory ruft das OCI-Konto, den Standort und die Sicherheitsgruppe automatisch anhand des ausgewählten OCI NSS Systems ab.

5. Wählen Sie **Add**.

Sie können den Status der Linkerstellung auf der Ereignisseite verfolgen. Dies sollte nicht länger als fünf Minuten dauern.

6. In der Workload Factory Benutzeroberfläche ist zu sehen, dass die Verknüpfung mit dem OCI NSS Storage-System verknüpft ist.

Einsatz des Terraform-Stacks in OCI Resource Manager

Schritte

1. In der Codebox erfolgt die Auswahl von **OCI Terraform**.
2. **Redirect to OCI Resource Manager** auswählen.
3. Im Dialogfeld erfolgt die Auswahl von **Weiter**.
4. Sie melden sich bei dem OCI-Mandanten an, der den Storage Pool enthält.
5. Überprüfung von Kompartiment, Region und Variablen (aus Workload Factory vorausgefüllt).
6. Die Option **Create** wird ausgewählt. Es ist zu warten, bis der Apply-Job erfolgreich abgeschlossen ist.
7. Im Job **Output** den Inhalt `function_ocid` kopieren.

Registrierung der Funktion in Workload Factory

Schritte

1. Rückkehr zur Seite **Link hinzufügen**.
2. Unter **Link registration** wird die Funktions-OCID eingefügt (`ocid1.fnfunc.oc1...`).
3. Wählen Sie **Add**.

Weitere Möglichkeiten, dieselbe Vorlage anzuwenden

Diese werden nur verwendet, wenn Sie den Resource Manager nicht über die Codebox verwenden.

Terraform CLI

1. Einen Ordner erstellen.
2. Sie können **OCI Terraform** aus der Codebox (`main.tf`) in diesen Ordner kopieren oder herunterladen.
3. Aus dem Ordner:

```
terraform init
terraform plan
```

```
terraform apply
```

4. Kopieren `function_ocid` des Inhalts aus der apply-Ausgabe und anschließendes Fortfahren mit [Registrieren der Funktion](#3-register-the-function-in-workload-factory).

OCI CLI

Zum Herunterladen der ZIP-Datei, zum Erstellen des Resource Manager Stack sowie zum Ausführen von Plan- und Apply-Jobs dient die Registerkarte **OCI CLI** in der Codebox.

Ergebnis

Der Link erscheint in Ihrer Liste **Links**.

Zum Entfernen der Funktion den Link in Workload Factory löschen und anschließend den Resource Manager-Stack zerstören (oder `terraform destroy` ausführen).

Ergebnis

Der Link erscheint in Ihrer Liste **Links**.

Zum Entfernen der Funktion den Link in Workload Factory löschen und anschließend den Resource Manager-Stack zerstören (oder `terraform destroy` ausführen).

Zuordnung eines bestehenden Links zu einem OCI NetApp Storage Service System

Nach dem Erstellen eines Links können Sie ihn mit einem oder mehreren OCI NetApp Storage Service-Systemen verknüpfen.

Schritte

1. Die Auswahl erfolgt im Menü , **Workloads > Storage**.
2. Die Auswahl erfolgt über **OCI NetApp Storage Service > Inventar**.
3. Im Aktionsmenü des Storage Pools, mit dem ein Link verknüpft werden soll, kann anschließend **Link zuordnen** ausgewählt werden.
4. Überprüfung der Netzwerkennung (Subnetzname oder OCID und CIDR).
5. Auswahl von **Vorhandenen Link zuordnen**.
6. Auswahl des Linknamens.
7. Auswahl des Authentifizierungsverfahrens:
 - **Workload Factory**: Geben Sie den ONTAP Admin-Benutzernamen und das Passwort an.
 - **OCI-Geheimnisverwaltung - OCI Vault Schlüssel**: zu verwenden, wenn die Link-Funktion mit Vault-Unterstützung eingesetzt wurde. Eingabe der Vault-Geheimnis-OCID.
8. **Anwenden** auswählen.

Ergebnis

Workload Factory ordnet den Link dem OCI NSS-System zu. Sie können erweiterte ONTAP-Operationen durchführen.

Verwandte Informationen

["Weitere Informationen zu Links"](#).

OCI NetApp Storage Service Berechtigungen für NetApp Workload Factory

Die für das Managen von Oracle Cloud Infrastructure NetApp Storage Service (OCI NSS)-Ressourcen mit NetApp Workload Factory erforderlichen Berechtigungen werden überprüft.

Wie Workload Factory die Berechtigungen von OCI NetApp Storage Service nutzt

Wenn Sie eine mandantenübergreifende Richtlinie erstellen, die die Workload Factory Identität in Ihren Mandanten zulässt, ruft Workload Factory die OCI APIs als diese NetApp-Identität auf, und OCI prüft jede Anfrage anhand der Berechtigungen, die Sie erteilt haben.

Sie geben weder Benutzerpasswörter noch API-Schlüssel weiter. Der Zugriff besteht nur, solange Ihre Richtlinie aktiv ist.

Mandantenübergreifende Vertrauensstellung

NetApp betreibt die `workload-factory-OCI-SN` Gruppe in einem OCI-Mandanten von NetApp. Sie richten im Root Compartment des Mandanten eine mandantenübergreifende Richtlinie ein, die dieser Gruppe einen begrenzten, expliziten Satz von Berechtigungen in Ihrem Mandanten gewährt. Jeder OCI API-Aufruf wird pro Anfrage anhand dieser Vereinbarung geprüft; Sie können sie jederzeit prüfen und widerrufen.

OCI NetApp Storage Service Mandant

Der Standard-Mandant für OCI NSS ist das Stamm-Compartment Ihres OCI-Mandanten.

Optionalerweise können Sie, wenn Sie das Prinzip der minimalen Berechtigungen anwenden möchten, in jeder Zeile „in tenancy“ durch „in compartment“ `<name>` ersetzen.

IAM-Richtlinien für OCI NSS

Workload Factory greift erst dann auf Ihren Mandanten in Oracle Cloud Infrastructure (OCI) zu, wenn Sie eine mandantenübergreifende Richtlinie hinzufügen, die den Workload Factory Service zulässt.

Diese Richtlinie wird im Root-Compartment Ihres Mandanten erstellt. Die Richtlinie führt die genauen Berechtigungen auf, die Workload Factory verwenden darf. Jede API-Anfrage wird dagegen geprüft. Die Richtlinie kann in der OCI Console eingesehen und jederzeit widerrufen werden, um den Zugriff zu beenden.

Folgende Berechtigungsrichtlinie ist verfügbar.

- **Anzeigen, planen und analysieren:** Anzeige von Ressourcen des OCI NetApp Storage Service, Informationen zum Systemstatus, Bereitstellung einer fundierten Analyse für Ihre Systeme und Aufzeigen von Einsparpotenzialen.

Die erforderlichen Richtlinien:

▼ Berechtigungsrichtlinien für OCI NetApp Storage Service

Anzeigen, planen und analysieren

```
Define tenancy NetAppWF as ocid1.tenancy.oc1..<>
```

```
Define group NetAppOpsWF as ocidl.group.oc1..<>
Admit group NetAppOpsWF of tenancy NetAppWF to inspect tenancies in
tenancy
Admit group NetAppOpsWF of tenancy NetAppWF to read compartments in
tenancy
Admit group NetAppOpsWF of tenancy NetAppWF to read instance-family
in tenancy
Admit group NetAppOpsWF of tenancy NetAppWF to read metrics in
tenancy
Admit group NetAppOpsWF of tenancy NetAppWF to read log-content in
tenancy
Admit group NetAppOpsWF of tenancy NetAppWF to use virtual-network-
family in tenancy
Admit group NetAppOpsWF of tenancy NetAppWF to read file-family in
tenancy
Admit group NetAppOpsWF of tenancy NetAppWF to manage functions-
family in tenancy
Admit group NetAppOpsWF of tenancy NetAppWF to read log-groups in
tenancy
Admit group NetAppOpsWF of tenancy NetAppWF to read netapp-storage-
pool in tenancy
Admit group NetAppOpsWF of tenancy NetAppWF to read netapp-svm in
tenancy
Admit group NetAppOpsWF of tenancy NetAppWF to read netapp-work-
request in tenancy
```

Workload Factory verwalten

Wie NetApp Workload Factory gut strukturierte Workloads unterstützt

Workload Factory unterstützt Sie bei der Wartung und dem Betrieb zuverlässiger, sicherer, effizienter und kostengünstiger Workload-Konfigurationen, die dem Well-Architected Framework Ihres Cloud-Anbieters entsprechen. Workload Factory analysiert Ihre Workloads täglich, gibt Empfehlungen und führt automatische Korrekturen durch, um einen zuverlässigen Workload-Betrieb zu fördern. Durch die Automatisierung dieses Prozesses minimiert Workload Factory menschliche Fehler und stellt Konsistenz im Workload-Management sicher.

So funktioniert es

Workload Factory analysiert täglich Ihre Workloads, die auf unterstützten Cloud-Speichersystem-Bereitstellungen ausgeführt werden. Die Analyse liefert den Status einer Well-Architected-Architektur, Erkenntnisse und Empfehlungen.

Nach Abschluss der täglichen Analyse werden die Konfigurationen im Well-architected Dashboard für die Bereitstellung als „optimiert“ oder „nicht optimiert“ angezeigt. Konfigurationsprobleme sind nach Kategorie sowie in einer Liste mit Problemen und Empfehlungen zu finden. Empfehlungen zu den Konfigurationsproblemen können überprüft werden. Einige Probleme können automatisch von Workload Factory behoben werden, während andere manuelle Eingriffe erfordern. In diesem Fall stellt Workload Factory detaillierte Anweisungen bereit, um die empfohlenen Änderungen umzusetzen.

Sie können die Analyse von Konfigurationen, die für Ihre Umgebungen nicht relevant sind, ausblenden. Dadurch werden unnötige Warnmeldungen und ungenaue Optimierungsergebnisse vermieden.

Es besteht auch die Möglichkeit, benutzerdefinierte Regeln in einfacher Sprache zu erstellen, um Ihre Umgebungen anhand der Standards Ihres Unternehmens und der NetApp Best Practices zu validieren. Regeln können mit einem Probelauf getestet und anschließend für die Ausführung in Ihren Umgebungen terminiert werden. ["Weitere Informationen zu benutzerdefinierten Regeln"](#).

Warum es wichtig ist

Workload Factory wendet Best Practices auf große Storage-, Datenbank- und VMware-Umgebungen an, indem kontinuierliche Bewertungen mit Empfehlungseinblicken und Fehlerbehebungen kombiniert werden. Automatisierte Korrekturen in der NetApp Console reduzieren menschliche Fehler, gewährleisten einheitliches Management und erhalten Leistung und Zuverlässigkeit über Ihre Workload-Infrastrukturen hinweg.

Beginnen Sie mit Workload Factory, um Fehlkonfigurationen von Workloads zu erkennen und zu beheben

Um mit Workload Factory zu beginnen, registrieren Sie sich, fügen Sie Anmeldeinformationen hinzu und stellen Sie eine Verbindung her, um AWS-Ressourcen zu verwalten und Workloads mithilfe von Amazon FSx for NetApp ONTAP zu optimieren.

["Schnellstart"](#)

Verwandte Informationen

Die folgenden Seiten bieten Anleitungen zur Implementierung gut strukturierter Konfigurationen für verschiedene NetApp Storage-Lösungen:

- ["Implementieren Sie gut strukturierte FSx for ONTAP Dateisysteme"](#)
- ["Gut konzipierte Datenbankkonfigurationen implementieren"](#)
- ["Implementieren Sie gut strukturierte EVS-Konfigurationen"](#)
- ["Gut strukturierte NetApp Volumes Konfigurationen implementieren"](#)
- ["Implementierung gut konzipierter Cloud Volumes ONTAP Systemkonfigurationen in Microsoft Azure"](#)

Konfiguration der Benachrichtigungen für NetApp Workload Factory

Sie können den NetApp Workload Factory-Benachrichtigungsdienst so konfigurieren, dass Benachrichtigungen als Warnmeldungen in der NetApp Console, an mit dem Konto verknüpfte E-Mail-Adressen oder an ein Amazon SNS-Thema gesendet werden. Benachrichtigungen, die als Warnmeldungen gesendet werden, erscheinen in der NetApp Console, wenn Sie einen Console-Agent oder -Link bereitgestellt haben. Wenn Workload Factory Benachrichtigungen an ein Amazon SNS-Thema veröffentlicht, erhalten Abonnenten dieses Themas (wie Personen oder andere Anwendungen) die Benachrichtigungen an den für das Thema konfigurierten Endpunkten (wie E-Mail oder SMS).

Workload Factory-Benachrichtigungen konfigurieren

Sie können Workload Factory-Benachrichtigungen mithilfe der NetApp Console oder der Workload Factory-Konsole konfigurieren.

Folgende Optionen stehen zum Empfangen von Benachrichtigungen zur Verfügung:

NetApp Console

- **Benachrichtigungen:** Konfigurieren Sie Workload Factory so, dass Benachrichtigungen gesendet werden, die unter dem Glockensymbol in NetApp Console angezeigt werden.
- **E-Mail:** Aktivieren Sie E-Mail-Benachrichtigungen in der NetApp Console, um Benachrichtigungen an alle mit dem Konto verknüpften E-Mail-Adressen zu erhalten, ohne dass eine Amazon SNS-Konfiguration erforderlich ist.
- **Amazon SNS:** Konfigurieren Sie Workload Factory so, dass Benachrichtigungen an ein Amazon SNS-Topic gesendet werden.

Workload Factory Konsole

- **E-Mail:** Aktivieren Sie E-Mail-Benachrichtigungen in der Workload Factory Console, um Benachrichtigungen an alle mit dem Konto verknüpften E-Mail-Adressen zu erhalten, ohne dass eine Amazon SNS-Konfiguration erforderlich ist.
- **Amazon SNS:** Konfigurieren Sie Workload Factory so, dass Benachrichtigungen mithilfe der Workload Factory Console an ein Amazon SNS-Thema gesendet werden.



Wenn Sie Benachrichtigungen in der NetApp Console konfigurieren, übernimmt diese die Zustellung der Benachrichtigungen und die Benachrichtigungsoptionen der Workload Factory Console werden deaktiviert und im Nur-Lese-Modus angezeigt. Ein Tooltip weist darauf hin, dass Benachrichtigungen von der NetApp Console verwaltet werden. Sie können Benachrichtigungen dann nur noch über die NetApp Console verwalten.

Bevor Sie beginnen

Die folgenden Voraussetzungen gelten nur bei der Konfiguration von Amazon SNS-Benachrichtigungen:

- Sie müssen Amazon SNS konfigurieren und Amazon SNS Topics mithilfe der Amazon SNS console oder der AWS CLI erstellen.
- Zu beachten ist, dass Workload Factory den Thementyp **Standard** unterstützt. Dieser Thementyp gewährleistet nicht, dass Benachrichtigungen in der Reihenfolge ihres Eingangs an die Abonnenten gesendet werden. Dies sollte daher berücksichtigt werden, wenn kritische oder Notfallbenachrichtigungen vorliegen.

Konfiguration von Benachrichtigungen aus NetApp Console

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü der NetApp Console werden **Workloads**, **Administration** und anschließend **Notifications setup** ausgewählt.
3. Aktivieren Sie auf der Seite „Benachrichtigungseinstellungen“ einen oder mehrere der folgenden Benachrichtigungstypen:
 - a. **NetApp Console-Benachrichtigungen**: Wählen Sie **NetApp Console-Benachrichtigungen aktivieren**, um Workload Factory so zu konfigurieren, dass Benachrichtigungen in der NetApp Console gesendet werden.
 - b. **E-Mail-Benachrichtigungen**: Wählen Sie **E-Mail-Benachrichtigungen aktivieren**, um Workload Factory so zu konfigurieren, dass Benachrichtigungen an alle mit dem Konto verknüpften E-Mail-Adressen gesendet werden.
 - c. **Amazon SNS-Benachrichtigungen**: Wählen Sie **SNS-Benachrichtigungen aktivieren** und folgen Sie dann den Anweisungen, um Amazon SNS aus der Amazon SNS-Konsole zu konfigurieren.

Nach dem Erstellen des Themas können Sie den Topic ARN kopieren und auf der Seite **Notifications setup** in das Feld **SNS topic ARN** eingeben.

4. Nach der Überprüfung der Konfiguration durch Senden einer Testbenachrichtigung folgt die Auswahl von **Apply**.

Konfigurieren von Benachrichtigungen aus der Workload Factory Konsole

Schritte

1. Melden Sie sich bei der ["Workload Factory Konsole"](#) an.
2. Im Menü der Workload Factory Console sind **Workloads**, **Administration** und anschließend **Notifications setup** auszuwählen.
3. Aktivieren Sie einen oder mehrere der folgenden Benachrichtigungstypen:
 - **E-Mail-Benachrichtigungen**: Wählen Sie **E-Mail-Benachrichtigungen aktivieren**. Alle mit dem Konto verknüpften E-Mail-Adressen werden im Nur-Lese-Modus angezeigt.

- **Amazon SNS-Benachrichtigungen:** Wählen Sie **SNS-Benachrichtigungen aktivieren** und folgen Sie dann den Anweisungen, um Amazon SNS aus der Amazon SNS-Konsole zu konfigurieren.

Nach der Überprüfung der Konfiguration durch Senden einer Testbenachrichtigung folgt die Auswahl von **Apply**.

Abonnement des Amazon SNS Themas

Nachdem Sie Workload Factory so konfiguriert haben, dass Benachrichtigungen an ein Thema gesendet werden, können Sie das Thema anhand der "[Anweisungen](#)" in der Amazon SNS-Dokumentation abonnieren, damit Sie Benachrichtigungen von Workload Factory erhalten.

Benachrichtigungen filtern

Sie können unnötigen Benachrichtigungsverkehr reduzieren und bestimmte Benachrichtigungstypen gezielt an bestimmte Nutzer senden, indem Sie Filter auf die Benachrichtigungen anwenden. Sie können dies mithilfe einer Amazon SNS-Richtlinie für SNS-Benachrichtigungen und mit den Benachrichtigungseinstellungen in der NetApp Console tun.

Amazon SNS Benachrichtigungen filtern

Wenn Sie ein Amazon SNS-Thema abonnieren, erhalten Sie standardmäßig alle Benachrichtigungen, die zu diesem Thema veröffentlicht werden. Wenn Sie nur bestimmte Benachrichtigungen aus dem Thema erhalten möchten, können Sie mit einer Filterrichtlinie steuern, welche Benachrichtigungen Sie erhalten. Filterrichtlinien bewirken, dass Amazon SNS dem Abonnenten nur die Benachrichtigungen zustellt, die der Filterrichtlinie entsprechen.

Sie können Amazon SNS Benachrichtigungen nach folgenden Kriterien filtern:

Beschreibung	Feldname der Filterrichtlinie	Mögliche Werte
Ressourcentyp	resourceType	• DB • Microsoft SQL Server host • PostgreSQL Server host
Arbeitslast	workload	WLMDB
Priorität	priority	• Success • Info • Recommendation • Warning • Error • Critical
Benachrichtigungstyp	notificationType	• Deployment • Well-architected

Schritte

1. In der Amazon SNS Konsole erfolgt die Bearbeitung der Abonnementdetails für das SNS Topic.
2. Im Bereich **Subscription filter policy** erfolgt die Filterung nach **Message attributes**.
3. Aktivierung der Option **Abonnementfilterrichtlinie**.
4. Die Eingabe einer JSON-Filterrichtlinie erfolgt im Feld **JSON editor**.

Beispielsweise akzeptiert die folgende JSON-Filterrichtlinie Benachrichtigungen von der Microsoft SQL Server Ressource, die mit dem WLMDB Workload in Zusammenhang stehen, die Priorität „Success“ oder „Error“ haben und Details zum Status „Well-architected“ bereitstellen:

```
{
  "accountId": [
    "account-a"
  ],
  "resourceType": [
    "Microsoft SQL Server host"
  ],
  "workload": [
    "WLMDB"
  ],
  "priority": [
    "Success",
    "Error"
  ],
  "notificationType": [
    "Well-architected"
  ]
}
```

5. **Änderungen speichern** auswählen.

Weitere Beispiele für Filterrichtlinien sind unter ["Beispielfilterrichtlinien für Amazon SNS"](#) zu finden.

Weitere Informationen zum Erstellen von Filterrichtlinien finden Sie unter ["Amazon SNS Dokumentation"](#).

Benachrichtigungen in der NetApp Console filtern

Sie können die Benachrichtigungseinstellungen der NetApp Console verwenden, um die Benachrichtigungen, die Sie in der Console erhalten, nach Schweregrad zu filtern, wie zum Beispiel Kritisch, Info oder Warnung.

Weitere Informationen zum Filtern von Benachrichtigungen in der Console enthält das ["NetApp Console-Dokumentation"](#).

Benachrichtigungstypen und -meldungen

Workload Factory sendet Benachrichtigungen für die folgenden Ereignisse:

Ereignis	Beschreibung	Benachrichtigungstyp	Schwere	Arbeitslast	Ressourcentyp
Einige Datenbankinstanzen in Ihrem Konto sind nicht optimal konzipiert	Alle Microsoft SQL Server-Instanzen in Ihrem Konto wurden auf Well-Architected-Probleme analysiert. Die Beschreibung dieses Ereignisses gibt die Anzahl der Well-Architected-Instanzen und nicht optimierten Instanzen an. Well-Architected-Statusergebnisse und Empfehlungen sind im Databases-Inventar über die Workload Factory console einsehbar.	Gut konzipiert	Empfehlung	Datenbanken	Microsoft SQL Server Instanz
Deployment des Microsoft SQL Server/PostgreSQL Servers war erfolgreich	Das Deployment des Microsoft SQL Server oder PostgreSQL Hosts war erfolgreich. Weitere Informationen sind unter der Auftragsüberwachung verfügbar.	Bereitstellung	Erfolg	Datenbanken	FSx for ONTAP, DB-Host
Microsoft SQL Server/PostgreSQL Server Deployment ist fehlgeschlagen	Das Deployment des Hosts für Microsoft SQL Server oder PostgreSQL ist fehlgeschlagen. Weitere Informationen sind unter Job Monitoring verfügbar.	Bereitstellung	Fehler	Datenbanken	FSx for ONTAP, DB-Host

Ereignis	Beschreibung	Benachrichtigungstyp	Schwere	Arbeitslast	Ressourcentyp
Erstellung der Replikationsbeziehung fehlgeschlagen	Die Erstellung einer SnapMirror Replikationsbeziehung ist fehlgeschlagen. Weitere Informationen sind im Tracker verfügbar.	Replication	Kritisch	Allgemeiner Storage	FSx for ONTAP
Fehler bei der Erstellung von FSx for ONTAP	Der Erstellungsprozess für ein Dateisystem von FSx for ONTAP ist fehlgeschlagen. Weitere Informationen finden Sie im Tracker.	FSx for ONTAP Dateisystemaktionen	Kritisch	Allgemeiner Storage	FSx for ONTAP
Erfolg der automatischen Erhöhung von SSD-Kapazität oder Inodes	Im Rahmen eines kürzlich durchgeführten automatischen Kapazitätsmanagement-Updates hat das FSx for ONTAP Dateisystem entweder die SSD-Kapazität oder die Volume-Inodes erfolgreich erhöht. Weitere Informationen sind im Tracker verfügbar.	Kapazitätsmanagement	Erfolg	Allgemeiner Storage	FSx for ONTAP Datei

Ereignis	Beschreibung	Benachrichtigungstyp	Schwere	Arbeitslast	Ressourcentyp
Fehler bei der automatischen Erhöhung der SSD-Kapazität oder Inodes	Während eines kürzlich durchgeführten automatischen Kapazitätsmanagement-Updates konnte das FSx for ONTAP Dateisystem die SSD-Kapazität oder die Volume-Inodes nicht erhöhen. Weitere Informationen sind im Tracker verfügbar.	Kapazitätsmanagement	Kritisch	Allgemeiner Storage	FSx for ONTAP Dateisysteme
FSx für ONTAP Problem erkannt	Alle FSx for ONTAP Dateisysteme wurden auf Well-Architected-Probleme hin analysiert. Der Scan hat ein oder mehrere Probleme festgestellt. Weitere Informationen enthält die Well-Architected-Analyse im Storage Dashboard der Workload Factory Konsole.	Gut konzipierte Analyse	Empfehlung	Allgemeiner Storage	FSx for ONTAP Dateisysteme
Automatisches Kapazitätsmanagement-Ereignis für FSx für ONTAP	Die SSD Performance Tier für das FSx for ONTAP Dateisystem hat den Gesamtwarnschwellenwert für Kapazität/Prozentsatz erreicht.	Kapazitätsmanagement	Warnung	Allgemeiner Storage	FSx for ONTAP Dateisysteme

Ereignis	Beschreibung	Benachrichtigungstyp	Schwere	Arbeitslast	Ressourcentyp
Automatisches Inodes-Management-Ereignis für FSx für ONTAP	Die Anzahl der Inodes für das FSx for ONTAP Volume hat den Warnschwellenwert für die Gesamtanzahl/den Gesamtprozentsatz erreicht.	Kapazitätsmanagement	Warnung	Allgemeiner Storage	FSx for ONTAP Dateisysteme
Verdächtige Datenträgeraktivität im FSx für ONTAP-Dateisystem festgestellt	NetApp Autonomous Ransomware Protection mit KI (ARP/AI) hat verdächtige Volumenaktivitäten erkannt.	Schutz vor Ransomware	Kritisch	Allgemeiner Storage	FSx for ONTAP Dateisysteme
Überschreitung des Latenzschwellenwerts festgestellt	Mindestens ein Volume im FSx for ONTAP Cluster hat den Latenzschwellenwert überschritten.	Leistungsüberwachung	Warnung	EDA	FSx for ONTAP Dateisysteme
Monatlicher Kostenbericht	Monatliche Kostenübersicht für Ihr Konto, die Ausgabentrends, ungewöhnliche Änderungen und die besten Einsparmöglichkeiten für FSx für ONTAP-Dateisysteme anzeigt.	Kostenbericht	Empfehlung	Allgemeiner Storage	FSx for ONTAP Dateisysteme
Replikationsverzögerung	Die Replikation dauert länger als erwartet.	Replication	Kritisch	Allgemeiner Storage	FSx for ONTAP Dateisysteme
Die Erstellung des benutzerdefinierten Dashboards war erfolgreich	Ihr individuelles Dashboard wurde erfolgreich erstellt und ist bereit zur Anzeige.	Benutzerdefinierte Dashboards	Erfolg	Allgemeiner Storage	Workload Factory Konto

Ereignis	Beschreibung	Benachrichtigungstyp	Schwere	Arbeitslast	Ressourcentyp
Erstellung eines benutzerdefinierten Dashboards fehlgeschlagen	Workload Factory konnte Ihr benutzerdefiniertes Dashboard nicht erstellen. Das Dashboard kann erneut erstellt werden.	Benutzerdefinierte Dashboards	Fehler	Allgemeiner Storage	Workload Factory Konto

Überwachung von NetApp Workload Factory Vorgängen mit Tracker

Die Ausführung von FSx für ONTAP, Anmeldeinformationen und Link-Vorgängen sowie den Aufgabenfortschritt mit Tracker in NetApp Workload Factory überwachen und nachverfolgen.

Über diese Aufgabe

Workload Factory bietet Tracker, eine Überwachungsfunktion, mit der der Fortschritt und Status von FSx for ONTAP, Anmeldeinformationen und Verbindungsvorgängen überwacht und verfolgt, Details zu Betriebsaufgaben und Unteraufgaben überprüft sowie etwaige Probleme oder Fehler diagnostiziert werden können.

In Tracker stehen mehrere Aktionen zur Verfügung. Aufträge können nach Zeitraum (letzte 24 Stunden, 7 Tage, 14 Tage oder 30 Tage), Arbeitslast, Status und Benutzer gefiltert, mit der Suchfunktion gefunden und die Auftragsstabelle als CSV-Datei heruntergeladen werden. Tracker kann jederzeit aktualisiert werden. Ein fehlgeschlagener Vorgang kann schnell wiederholt oder die Parameter eines fehlgeschlagenen Vorgangs bearbeitet und der Vorgang erneut ausgeführt werden.

Tracker unterstützt je nach Vorgang zwei Überwachungsebenen. Jede Aufgabe, wie beispielsweise die Bereitstellung eines Dateisystems, zeigt die Aufgabenbeschreibung, den Status, die Startzeit, die Aufgabendauer, den Benutzer, die Region, die Proxy-Ressource, die Aufgaben-ID und alle zugehörigen Unteraufgaben an. API-Antworten können angezeigt werden, um nachzuvollziehen, was während des Vorgangs passiert ist.

Tracker-Aufgabenebenen mit Beispielen

- Ebene 1 (Aufgabe): Verfolgt die Bereitstellung des Dateisystems.
- Ebene 2 (Teilaufgabe): Verfolgt die Teilaufgaben im Zusammenhang mit der Dateisystembereitstellung.

Betriebsstatus

Der Vorgangstatus in Tracker ist wie folgt: *in Bearbeitung*, *erfolgreich* und *fehlgeschlagen*.

Betriebsfrequenz

Die Betriebshäufigkeit richtet sich nach der Art des Auftrags und dem Auftragsplan.

Ereignisaufbewahrung

Ereignisse bleiben 30 Tage lang in der Benutzeroberfläche erhalten.

Abläufe nachverfolgen und überwachen

Vorgänge in der NetApp Console lassen sich mit Tracker nachverfolgen und überwachen.

Schritte

1. Melden Sie sich mit einem der "[Konsolenerlebnisse](#)" an.
2. Wählen Sie das Menü  und dann **Administration**.
3. Im Menü „Administration“ **Tracker** auswählen.
4. In Tracker können Sie mithilfe der Filter oder der Suchfunktion die Job-Ergebnisse eingrenzen. Es besteht außerdem die Möglichkeit, einen Jobbericht herunterzuladen.

API-Anfrage anzeigen

Die API-Anfrage für eine Aufgabe in Tracker ist im Codebox-Bereich einsehbar.

Schritte

1. In Tracker eine Aufgabe auswählen.
2. Das Menü „Aktionen“ auswählen und anschließend **API-Anfrage anzeigen** wählen.

Einen fehlgeschlagenen Vorgang wiederholen

Eine fehlgeschlagene Operation in Tracker wiederholen. Sie können auch die Fehlermeldung einer fehlgeschlagenen Operation kopieren.



Bei einem fehlgeschlagenen Vorgang sind nur x Wiederholungsversuche zulässig.

Schritte

1. In Tracker einen fehlgeschlagenen Vorgang auswählen.
2. Das Menü „Aktionen“ auswählen und dann **Wiederholen** auswählen.

Ergebnis

Der Vorgang wurde neu gestartet.

Einen fehlgeschlagenen Vorgang bearbeiten und erneut versuchen

Die Parameter des fehlgeschlagenen Vorgangs können bearbeitet und der Vorgang außerhalb von Tracker erneut ausgeführt werden.

Schritte

1. In Tracker einen fehlgeschlagenen Vorgang auswählen.
2. Wählen Sie das Aktionsmenü und dann **Bearbeiten und erneut versuchen**.

Sie werden auf die Seite für den Vorgang weitergeleitet, wo Sie die Parameter bearbeiten und den Vorgang erneut versuchen können.

Ergebnis

Der Vorgang wurde neu gestartet. Den Status des Vorgangs können Sie im Tracker einsehen.

Links der NetApp Workload Factory verwalten

Sie können Links verwalten, die Ihrem Workload Factory Konto zugeordnet sind. Sie können Links anzeigen, die einem FSx for ONTAP Dateisystem oder einem OCI NetApp Storage Service (OCI NSS) System zugeordnet sind, Passwörter für die Linkauthentifizierung angeben und Links aus NetApp Console entfernen.

["Weitere Informationen zu Links."](#)

Anzeigen der mit Ihrem Konto verknüpften Links

Sie können die Links anzeigen, die aktuell mit Ihrem Konto verknüpft sind.

Schritte

1. Die Auswahl erfolgt im Menü  **Administration > Links**.

Bestehende Links erscheinen auf der Seite „Links“.
2. Die mit einem Link verknüpften Storage-Systeme werden über die Schaltfläche **View** im Abschnitt Zugehörige Ressourcen angezeigt.
3. Falls Sie den Amazon Resource Name (ARN) für den Link benötigen, können Sie das Symbol *copy* neben dem ARN-Feld auswählen.

Einen Link bearbeiten

Ein Link kann über die NetApp Console nicht bearbeitet werden. Wenn eine Änderung an einem Link erforderlich ist, muss ein neuer Link erstellt und dann Ihrem Storage-System zugeordnet werden.



Die Netzwerkkonfiguration von AWS Lambda oder Oracle Cloud Functions (z. B. VPC, Subnetze und Sicherheitsgruppen) kann über die Konsole Ihres Cloud-Anbieters bearbeitet werden, und die Änderungen werden in Links oder in der Benutzeroberfläche zur Functions-Verwaltung angezeigt; diese Änderungen können jedoch zu Verbindungsproblemen zwischen AWS Lambda oder Oracle Cloud Functions und ONTAP führen und werden daher nicht empfohlen.

Einen Link authentifizieren

Die Authentifizierung eines Links erfolgt durch Angabe eines Administratorbenutzerkennworts für Workload Factory Anmeldeinformationen oder eines Secrets aus AWS Secrets Manager oder Oracle Vault.

- Für AWS Secrets Manager werden entweder der Name des Secrets oder eine AWS Secrets Manager Secret ARN benötigt, um den Link mit einem FSx for ONTAP Dateisystem zu verbinden.



AWS Secrets Manager wird bei Verwendung eines Console Agenten nicht unterstützt.

- Für Oracle Vault ist die OCID des Vault-Geheimnisses anzugeben, um die Verknüpfung mit einem OCI NetApp Storage Service System herzustellen.



Pro Link wird nur ein Authentifizierungsverfahren unterstützt. Wenn beispielsweise die Link-Authentifizierung mit AWS Secrets Manager ausgewählt wird, kann das

Authentifizierungsverfahren später nicht mehr geändert werden.

Amazon FSx for NetApp ONTAP

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** das Aktionsmenü des Dateisystems auswählen, dem ein Link zugeordnet werden soll, und anschließend **Verwalten** auswählen.
4. In der Dateisystemübersicht **Link authentifizieren** auswählen.
5. Auf der Seite „Authentifizierungslink“ ein Authentifizierungsverfahren auswählen:
 - **Workload Factory**: Die Eingabe des Passworts erfolgt zweimal.
 - **AWS Secrets Manager**: der Secret ARN.
6. **Anwenden** auswählen.

OCI NetApp Storage Service

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü , **Workloads > Storage > OCI NetApp Storage Service** ist auszuwählen.
3. Im **OCI NetApp Storage Service** ist für den Storage-Pool, dem eine Verknüpfung zugeordnet werden soll, das Aktionsmenü und anschließend **Verwalten** auszuwählen.
4. In der Übersicht des Storage-Pools erfolgt die Auswahl von **Link authentifizieren**.
5. Auf der Seite „Authentifizierungslink“ ein Authentifizierungsverfahren auswählen:
 - **Workload Factory**: Die Eingabe des Passworts erfolgt zweimal.
 - **OCI Vault**: die OCID des Secrets eingeben.
6. **Anwenden** auswählen.

Ergebnis

Die Verbindung ist authentifiziert, und Sie können erweiterte ONTAP-Operationen durchführen.

Das Passwort für die Link-Authentifizierung aktualisieren

Wenn das Administratorpasswort ungültig ist, ist eine Aktualisierung des Passworts erforderlich, um die Verbindung zu Ihrem Storage-System herzustellen.

Amazon FSx for NetApp ONTAP

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü  ist **Workloads > Storage > FSx for ONTAP** auszuwählen.
3. In **FSx for ONTAP** das Aktionsmenü des Dateisystems auswählen, dem ein Link zugeordnet werden

soll, und anschließend **Verwalten** auswählen.

4. In der Dateisystemübersicht **Passwort aktualisieren** auswählen.
5. Auf der Seite „Authentifizierung“ wird das neue Passwort zweimal eingegeben.
6. **Anwenden** auswählen.

OCI NetApp Storage Service

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Im Menü , **Workloads > Storage > OCI NetApp Storage Service** ist auszuwählen.
3. Im **OCI NetApp Storage Service** ist für den Storage-Pool, dem eine Verknüpfung zugeordnet werden soll, das Aktionsmenü und anschließend **Verwalten** auszuwählen.
4. In der Übersicht des Speicherpools kann **Kennwort aktualisieren** ausgewählt werden.
5. Auf der Seite „Authentifizierung“ wird das neue Passwort zweimal eingegeben.
6. **Anwenden** auswählen.

Ergebnis

Das Passwort wurde aktualisiert, und die Verbindung ist jetzt mit dem Storage-System hergestellt.

Link entfernen

Sie können eine Verknüpfung entfernen, die in Ihrer Umgebung nicht mehr verwendet wird. Storage-Systeme oder andere Ressourcen, die die Verknüpfung verwendet haben, können nach deren Entfernung bestimmte Funktionen nicht mehr nutzen.

Der Link wird nur aus Workload Factory gelöscht und nicht aus Ihrer AWS- oder Oracle-Umgebung entfernt.

- Für FSx for ONTAP müssen Sie die Lambda function aus Ihrem AWS-Konto löschen, nachdem Sie die Verknüpfung in Workload Factory entfernt haben.
- Für OCI NetApp Storage Service müssen Sie die Function-Instanz aus Ihrem OCI-Konto löschen, nachdem Sie den Link in Workload Factory entfernt haben.

Amazon FSx for NetApp ONTAP

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Die Auswahl erfolgt im Menü  **Administration > Links**.

Bestehende Links erscheinen auf der Seite „Links“.
3. Auf der Seite „Links“ im Aktionsmenü des zu entfernenden Links die Option **Entfernen** auswählen.
4. Wenn Sie sicher sind, wählen Sie erneut **Entfernen**.

In der AWS-Dokumentation "[die Lambda-Funktion löschen](#)" finden sich weitere Informationen.

OCI NetApp Storage Service

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü  **Administration > Links**.

Bestehende Links erscheinen auf der Seite „Links“.
3. Auf der Seite „Links“ im Aktionsmenü des zu entfernenden Links die Option **Entfernen** auswählen.
4. Wenn Sie sicher sind, wählen Sie erneut **Entfernen**.

KI-Funktionen für FSx für ONTAP in NetApp Workload Factory managen

Der Zugriff auf KI-Funktionen für FSx for ONTAP in Workload Factory lässt sich steuern. Es ist möglich, KI-Funktionen zu deaktivieren oder AWS Bedrock zu verwenden, das von NetApp verwaltet wird.

Über KI-Funktionen

Workload Factory beinhaltet mehrere KI-gestützte Funktionen, die Ihr Benutzererlebnis verbessern, wie Ask Me, benutzerdefinierte Dashboards und Analysetools für EMS, Datenbankprotokolle und Latenz.

Als Administrator von Workload Factory kann auf der Seite „KI-Einstellungen“ gesteuert werden, wie diese Funktionen KI nutzen.

Konfigurationsoptionen

Wählen Sie aus diesen Konfigurationsoptionen:

NetApp Managed Bedrock (Empfohlen)

Ein von NetApp verwalteter AWS Bedrock Service kann verwendet werden. Diese Option wird für die meisten Benutzer empfohlen.

- Ihre Daten werden nicht zum Trainieren von Modellen verwendet
- Monatliche Nutzungsguthaben sind organisationsweit gemeinsam nutzbar.
- Keine zusätzliche AWS-Einrichtung ist erforderlich.

GenAI Funktionen deaktiviert

Alle KI-Funktionen werden deaktiviert. Benutzer können „Ask Me“, Analysetools, benutzerdefinierte Dashboards, den Errichter oder andere KI-gestützte Tools nicht mehr verwenden.

Bevor Sie beginnen

- Es wird empfohlen, dass ein Kontoadministrator die KI-Funktionen einrichtet.

KI-Funktionen konfigurieren

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Im Menü der NetApp Console erfolgt die Auswahl von **Workloads > Administration > AI settings**.
3. Auf der Seite **KI-Einstellungen** kann die bevorzugte Konfiguration ausgewählt werden:
 - **NetApp-verwaltetes Bedrock (Empfohlen)**: NetApp-verwaltetes AWS Bedrock verwenden.
 - **Gen AI-Funktionen deaktiviert**: Alle KI-Funktionen sind deaktiviert.
4. **Einstellungen speichern** auswählen.

Ergebnis

Ihre Einstellungen werden gespeichert und sofort auf alle KI-Funktionen in Workload Factory angewendet. Im Tracker ist ersichtlich, wer die Einstellungen zuletzt aktualisiert hat und wann.

Wenn KI-Funktionen deaktiviert sind, sehen Nutzer eine Meldung, wenn sie versuchen, KI-gestützte Funktionen zu verwenden. Die Benutzeroberfläche bleibt sichtbar und zeigt deutlich, dass die Funktion nicht verfügbar ist.

Budgetkontrolle und Kreditlimits

NetApp verwaltet die Budgetkontrolle für KI-Funktionen bei Verwendung der standardmäßigen, von NetApp verwalteten Konfiguration.

Monatliche Kreditlimits

Jedes Konto hat ein monatliches Ausgabenlimit für jede KI-Funktion, wenn NetApp-verwaltetes Bedrock verwendet wird.

Wenn das Budget erreicht ist

Wenn Ihr Konto das monatliche Budgetlimit erreicht, führt Workload Factory Folgendes aus:

- KI-Funktionen deaktivieren und die zugehörigen Teile der Benutzeroberfläche ausgrauen
- Diese Meldung als Tooltip anzeigen: „Monatliches KI-Guthaben erreicht. Wenden Sie sich an den NetApp Support.“
- Protokollnutzung zu Nachverfolgungszwecken

Zusätzliche Gutscheine beantragen

Falls Sie mehr KI-Guthaben benötigen, wenden Sie sich an Ihren NetApp Ansprechpartner. Ihr Ansprechpartner kann das Kreditlimit entsprechend Ihres Bedarfs anpassen.



Um Ihren NetApp Ansprechpartner bezüglich Kreditlimits zu kontaktieren, kann der In-Product-Chat genutzt werden oder die "[Hilfe erhalten](#)" Seite aufgerufen werden.

AWS GovCloud Überlegungen

Wenn ein Workload Factory Konto in AWS GovCloud (US) erstellt wird, ist zu beachten, dass KI-Funktionen standardmäßig AWS Bedrock Dienste in öffentlichen AWS Regionen verwenden.

Wenn Ihre Sicherheitsanforderungen keine Verbindungen zu öffentlichen AWS Region Services zulassen, können KI-Funktionen deaktiviert werden.

Auswirkungen auf bestehende Sitzungen

Wenn Sie die KI-Einstellungen ändern, werden alle aktiven KI-Sitzungen sanft beendet. Laufende Arbeitsabläufe können abgeschlossen werden, aber neue Anfragen verwenden die aktualisierten Einstellungen.

Das Beendungsverhalten kann je nach Funktion variieren. Einzelheiten sind in der funktionspezifischen Dokumentation zu finden.

Verwandte Informationen

- ["Informationen zu den Funktionen von Workload Factory"](#)
- ["Informationen zu benutzerdefinierten Dashboards"](#)
- ["AWS-Anmeldeinformationen hinzufügen"](#)
- ["Berechtigungsreferenz"](#)

Benutzerdefinierte Dashboards für FSx für ONTAP

Informationen zu benutzerdefinierten Dashboards für FSx for ONTAP in NetApp Workload Factory

Als Cloud- und Storage-Administrator bieten benutzerdefinierte Dashboards einen klaren Überblick über die Systeme und Workloads, die Sie verwalten. Sie ermöglichen es, Ansichten zu erstellen und zu personalisieren, die Ihrer Arbeit, Ihren Prioritäten und Geschäftszielen entsprechen, anstatt auf vorgegebene Layouts beschränkt zu sein.

Benutzerdefinierte Dashboards nutzen KI, um personalisierte Ansichten Ihrer Workload Factory Umgebung zu erstellen. Es genügt, in verständlicher Sprache zu beschreiben, was überwacht werden soll, und das System erstellt automatisch visuelle Diagramme basierend auf den jeweiligen Anforderungen.

Alle Benutzer Ihres Workload Factory Kontos können alle benutzerdefinierten Dashboards einsehen. Diese gemeinsame Einrichtung unterstützt die Zusammenarbeit der Teams und ermöglicht es, dass in Ihrer Organisation dieselben betrieblichen Informationen angezeigt werden.



Wenn Ihr Kontoadministrator die KI-Funktionen deaktiviert hat, wird eine Meldung angezeigt und das Erstellen von Dashboards ist nicht möglich. Die Kontaktaufnahme erfolgt über Ihren Administrator oder ["Informationen zur KI-Administration"](#).

Warum benutzerdefinierte Dashboards verwendet werden

Workload Factory Nutzer verwalten zahlreiche Workloads, Umgebungen und Prioritäten, aber die Standard Dashboards zeigen nur vordefinierte Ansichten. Benutzerdefinierte Dashboards tragen zur Lösung verschiedener betrieblicher Herausforderungen bei:

- **Wichtige Fragen schnell beantworten:** Der Fokus liegt auf den wichtigsten Fragen oder Wissenslücken statt auf allgemeinen Systemstatistiken.

- **Überwachen Sie, was jetzt wichtig ist:** Verfolgen Sie die Kennzahlen, die Ihren aktuellen Prioritäten entsprechen, nicht einen festen Satz von Gesundheitsindikatoren.
- **Technische Daten mit Geschäftsergebnissen verknüpfen:** Es wird dargestellt, wie sich die Systemleistung auf den Betrieb und die Geschäftsziele auswirkt.
- **Vermeiden Sie das Wechseln zwischen verschiedenen Tools:** Alle relevanten Informationen sind an einem Ort verfügbar, ein Wechsel zwischen Tools, Seiten oder Exporten ist nicht erforderlich.

Möglichkeiten mit benutzerdefinierten Dashboards

Während der Einrichtung unterstützt Sie der KI-gestützte Dialog dabei, Folgendes zu definieren:

- Zu überwachende Arbeitslasten und Ressourcen
- Wichtige Kennzahlen für Ihre Arbeit
- Zeitbereiche und Vergleichszeiträume
- Ansichten nach Region, Arbeitslast oder anderen Kategorien
- Regeln oder Anforderungen, die verfolgt und angezeigt werden müssen

Dashboards anzeigen und teilen

Neue Dashboards sind standardmäßig privat, sodass nur Sie sie sehen können. Ein Dashboard kann jederzeit öffentlich gemacht werden, um es mit Ihrem Team zu teilen.

- **Private Dashboards:** Nur Sie können diese Dashboards einsehen. Diese eignen sich für persönliche Überwachung, Tests oder laufende Arbeiten.
- **Öffentliche Dashboards:** Alle Benutzer Ihres Workload Factory-Kontos können diese Dashboards einsehen. Damit lassen sich Überwachungsansichten teilen und das Team bleibt hinsichtlich Workloads, Prioritäten und Geschäftszielen auf dem gleichen Stand.

Jede Dashboard-Karte zeigt an, ob das Dashboard privat oder öffentlich ist, sodass Sie schnell sehen können, welche Dashboards geteilt sind.

["Informationen zum Ändern der Dashboard-Sichtbarkeit"](#).

Überlegungen und Einschränkungen

AWS Anmeldeinformationen und Berechtigungen

Zum Erstellen oder Anzeigen benutzerdefinierter Dashboards benötigen Sie die entsprechenden AWS IAM-Berechtigungen für die Ressourcen, die Sie überwachen möchten. Es ist sicherzustellen, dass das Workload Factory Konto über Lesezugriff auf die von den Dashboards verwendeten Datenquellen verfügt.

Zum Erstellen von Dashboards verwendet Workload Factory schreibgeschützte AWS-Anmeldeinformationen. Diese Anmeldeinformationen erlauben nur Leseaktionen wie `fsx:DescribeVolumes` und `fsx:DescribeFileSystems`, für die folgenden Dienste: EC2, FSx, CloudWatch, Resource Groups Tagging API, Backup, CloudWatch Logs, KMS und EFS.

["Informationen zum Hinzufügen von AWS-Anmeldeinformationen und zum Einrichten von IAM-Berechtigungen"](#).

Link zu FSx für ONTAP

Workload Factory benötigt eine Verbindung zu FSx for ONTAP Dateisystemen. Eine Verbindung stellt eine Vertrauensbeziehung und Konnektivität zwischen Workload Factory und einem oder mehreren FSx for ONTAP Dateisystemen her. So ist es möglich, bestimmte Dateisystemfunktionen direkt über die ONTAP REST API-Aufrufe zu überwachen und zu verwalten, die über die Amazon FSx for ONTAP API nicht verfügbar sind.

["Informationen zum Erstellen eines Links".](#)

Read-only-Design

Benutzerdefinierte Dashboards sind schreibgeschützt. Sie können weder Ihre Speicher- noch Ihre Workload-Einstellungen ändern. Dadurch ist es möglich, das System zu überwachen, ohne versehentlich Änderungen vorzunehmen.

Einschränkungen

Für benutzerdefinierte Dashboards gelten derzeit folgende Einschränkungen:

- Dashboards können nicht außerhalb Ihres Workload Factory-Kontos geteilt werden. Die Freigabe von Dashboards ist auf Benutzer innerhalb desselben Workload Factory-Kontos beschränkt.

Demo Umgebung

Wenn Sie ein Workload Factory Demoaccount verwenden, stehen einige vordefinierte Dashboards zur Verfügung. Diese helfen dabei, die Möglichkeiten benutzerdefinierter Dashboards zu erkennen. Jedes Dashboard zeigt einen typischen Überwachungsbedarf: Status der Notfallwiederherstellung, Kapazität und Kosten in verschiedenen Regionen sowie ob Speicherschutzregeln eingehalten werden.

Beispiel-Eingabeaufforderungen

Die folgenden Beispiele zeigen, wie sich Überwachungsanforderungen in einfacher Sprache beschreiben lassen:

- **Überwachung der Notfallwiederherstellung:** „Ich richte eine Notfallwiederherstellungslösung in AWS für meine On-Premises-Systeme ein. Ich möchte eine vollständige Liste meiner On-Premises-Ressourcen und den Status jeder einzelnen Ressource am Notfallwiederherstellungsstandort in der Region US East sehen, einschließlich der Information, ob sie konfiguriert, aktiv und fehlerfrei ist.“
- **Multiregionale Kapazität und Kosten:** „Ich verwalte Speicher über mehrere Cloud-Regionen und Anwendungen hinweg. Ich möchte einen klaren Überblick darüber, wie viel Speicherplatz ich zugewiesen habe, wie viel davon genutzt wird und wie hoch die Kosten sind, mit Details für jede Region und jede Anwendung.“
- **Konformität mit den Speicherschutzrichtlinien:** „Ich richte eine neue Speicherschutzstrategie gemäß den Standards meiner Organisation ein. Alle Dateisysteme anzeigen und angeben, ob sie diese Anforderungen erfüllen:
 - Datenbank-Workloads: 12 tägliche Snapshots pro Volume und 2 manipulationssichere Snapshots pro Woche.
 - NFS und SMB Freigaben: 7 tägliche Snapshots pro Volume und 1 manipulationssicherer Snapshot pro Woche.
 - ARP muss auf allen Volumes aktiviert sein.

Nächste Schritte

- ["Ein benutzerdefiniertes Dashboard erstellen"](#)
- ["Benutzerdefinierte Dashboards verwalten"](#)
- ["Fehlerbehebung bei benutzerdefinierten Dashboards"](#)

Ein benutzerdefiniertes Dashboard in NetApp Workload Factory erstellen

Individuelle Dashboards lassen sich erstellen, indem in einfacher Sprache beschrieben wird, was überwacht werden soll. Die KI unterstützt bei der Einrichtung, sodass die Dashboards zu den jeweiligen Workloads und Prioritäten passen.

Über diese Aufgabe

Benutzerdefinierte Dashboards nutzen einen KI-gestützten Dialog, um zu verstehen, was Sie visualisieren möchten. Ihre Überwachungsanforderungen werden in natürlicher Sprache beschrieben, und das System stellt klärende Fragen, damit das Dashboard Ihren Anforderungen entspricht.

Nach der Erstellung kann das Dashboard aktualisiert werden, um die aktualisierten Daten anzuzeigen.

Beachten Sie, dass benutzerdefinierte Dashboards standardmäßig schreibgeschützt sind und keine Änderungen an Ihren Speicher- oder Workload-Konfigurationen vornehmen können.



Wenn Ihr Kontoadministrator die KI-Funktionen deaktiviert hat, wird eine Meldung angezeigt und das Erstellen von Dashboards ist nicht möglich. Die Kontaktaufnahme erfolgt über Ihren Administrator oder ["Informationen zur KI-Administration"](#).

Ein Dashboard erstellen

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü der NetApp Console erfolgt die Auswahl über **Workloads > Workloads Overview > Custom dashboards**.

Wenn dies Ihr erstes Dashboard ist, sehen Sie einen leeren Bildschirm mit Beispielaufforderungen, die Ihnen den Einstieg erleichtern. Es besteht die Möglichkeit, **Aufforderung kopieren** auszuwählen, um eine Beispielaufforderung in das Textfeld des KI-Dialogs zu übernehmen.

3. **Neues Dashboard erstellen** auswählen.
4. Im KI-Dialog wird beschrieben, was überwacht werden soll.

Beschreiben Sie es in einfachen Worten. Die KI stellt einige Fragen, um Ihre Bedürfnisse besser zu verstehen.

5. Wählen Sie .

6. Antworten auf die klärenden Fragen der KI.

Die KI bittet Sie möglicherweise, aus mehreren Optionen auszuwählen, um Ihre Bedürfnisse besser zu verstehen. Jede Frage wird beantwortet und **Weiter** ausgewählt, oder **Überspringen** wird gewählt, um optionale Fragen zu überspringen.

7. Nachdem Sie alle Fragen beantwortet haben, **Weiter** auswählen, um Ihr Dashboard zu erstellen.

Ihr Dashboard wird erstellt. Dies kann einen Moment dauern.

Ergebnis

Ihr benutzerdefiniertes Dashboard wurde erstellt und dem Dashboard Katalog hinzugefügt. Standardmäßig ist das Dashboard privat und nur für Sie sichtbar. Die Sichtbarkeit kann auf öffentlich geändert werden, wenn eine Freigabe für andere Benutzer Ihres Workload Factory Kontos gewünscht ist. ["Informationen zum Ändern der Dashboard-Sichtbarkeit"](#).

Sie erhalten eine Benachrichtigung, sobald Ihr Dashboard fertig ist. Falls es nicht erstellt werden kann, erhalten Sie eine Benachrichtigung mit einem Link, um es erneut zu versuchen. ["Informationen zur Konfiguration von Benachrichtigungen"](#).

Was kommt als Nächstes

Nach der Erstellung können Sie:

- Die Dashboard-Sichtbarkeit kann geändert werden, sodass sie mit dem Team geteilt wird.
- Dashboard-Daten werden aktualisiert, damit die neuesten Informationen angezeigt werden.
- Dashboards, die nicht mehr benötigt werden, können gelöscht werden.
- Dashboard-Details anzeigen, einschließlich des Erstellers und des Zeitpunkts der letzten Aktualisierung

Verwandte Informationen

- ["Eigene benutzerdefinierte Dashboards verwalten"](#)
- ["Fehlerbehebung bei benutzerdefinierten Dashboards"](#)

Benutzerdefinierte Dashboards in NetApp Workload Factory verwalten

Verwalten Sie Ihre benutzerdefinierten Dashboards im Dashboard-Katalog. Von dort aus lassen sich Details anzeigen, Dashboards freigeben, Daten aktualisieren oder Dashboards, die nicht mehr benötigt werden, löschen.

Über diese Aufgabe

Im Dashboard-Katalog lassen sich benutzerdefinierte Dashboards anzeigen und managen. Private Dashboards sind nur für Sie sichtbar, während öffentliche Dashboards für alle Benutzer in Ihrem Workload Factory Konto sichtbar sind. Jedes Dashboard zeigt grundlegende Details wie den Namen des Erstellers, das Erstellungsdatum und eine Transparenzkennzeichnung (Privat oder Öffentlich).

Benutzerdefinierte Dashboards sind schreibgeschützt. Sie können weder Ihre Speicher- noch Ihre Workload-Einstellungen ändern.

Bevor Sie beginnen

Sie müssen mindestens ein benutzerdefiniertes Dashboard in Ihrem Workload Factory Konto haben.

Auf den Dashboard Katalog zugreifen

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü der NetApp Console erfolgt die Auswahl über **Workloads > Workloads Overview > Custom**

dashboards.

Der Dashboard Katalog zeigt alle benutzerdefinierten Dashboards in Ihrem Workload Factory Konto an.

3. Die Dashboard-Liste wird angezeigt.

Dashboard-Sichtbarkeit ändern

Ein Dashboard kann öffentlich gemacht werden, um es mit dem Team zu teilen. Durch das Setzen auf privat wird die gemeinsame Nutzung beendet.

Schritte

1. Auf der Seite **Benutzerdefinierte Dashboards** das Dashboard suchen, das aktualisiert werden soll.
2. Im Dropdown-Menü **Aktionen** ... für dieses Dashboard eine der folgenden Optionen auswählen:
 - **Dashboard teilen** – Macht das Dashboard für alle Benutzer Ihres Workload Factory Kontos sichtbar.
 - **Auf privates Dashboard umschalten** – macht das Dashboard nur für Sie sichtbar

Ergebnis

Das Dashboard wird sofort aktualisiert. Die Sichtbarkeitsanzeige auf der Dashboard-Karte zeigt den aktuellen Status.

Dashboard-Daten aktualisieren

Dashboard-Daten werden beim Öffnen eines Dashboards geladen. Eine Aktualisierung zeigt die neuesten Informationen an.

Das Dashboard lädt Daten aus Ihren Workloads neu. Die Zeitangabe „Letzte Aktualisierung“ ändert sich und zeigt an, wann die Daten aktualisiert wurden.

Ein Dashboard löschen

Dashboards, die nicht mehr benötigt werden, können gelöscht werden. Dieser Vorgang ist endgültig und kann nicht rückgängig gemacht werden.

Schritte

1. Auf der Seite **Benutzerdefinierte Dashboards** das Dashboard suchen, das entfernt werden soll.
2. Im Dropdown-Menü **Aktionen** für dieses Dashboard die Option **Löschen** auswählen.
3. Bestätigen Sie die Löschung.

Ergebnis

Das Dashboard wird dauerhaft aus Ihrem Workload Factory-Konto entfernt und alle Benutzer verlieren den Zugriff darauf.

Verwandte Informationen

- ["Zusätzliche benutzerdefinierte Dashboards erstellen"](#)
- ["Fehlerbehebung bei benutzerdefinierten Dashboards"](#)

Fehlerbehebung bei benutzerdefinierten Dashboards in NetApp Workload Factory

Diese Informationen helfen bei der Behebung häufiger Probleme, die beim Erstellen oder Verwenden benutzerdefinierter Dashboards auftreten können.

Dashboard Erstellung fehlgeschlagen

Problem: Beim Erstellen eines Dashboards wird die Fehlermeldung „Failed to understand request and generate code“ angezeigt.

Ursache: Das System konnte Ihre Anfrage nicht verstehen oder die Visualisierung anhand Ihrer Eingabe nicht erstellen.

Lösung: Folgendes kann versucht werden:

- Formulieren Sie Ihre Anfrage mit klareren Details dazu, was Sie überwachen möchten.
- Mit einer der Beispielaufforderungen in ["Ein benutzerdefiniertes Dashboard erstellen"](#) kann begonnen werden.
- Komplexe Überwachungsanforderungen können in mehrere einfachere Dashboards unterteilt werden.
- Die Arbeitslasten, Metriken, Zeitbereiche oder Dimensionen, die verfolgt werden sollen, können angegeben werden.

Das Dashboard konnte keine Daten laden

Problem: Das Dashboard wurde erstellt, aber beim Laden der Daten werden Fehler angezeigt.

Ursache: Dies geschieht üblicherweise aufgrund von Berechtigungsproblemen oder nicht verfügbaren Datenquellen.

Lösung:

- **Berechtigungen prüfen:** Stellen Sie sicher, dass Ihr Workload Factory-Konto Lesezugriff auf die vom Dashboard verwendeten Workloads und Ressourcen hat. Die Berechtigungsanforderungen sind in ["AWS Anmeldeinformationen und Berechtigungen"](#) zu finden.
- **Anmeldeinformationen überprüfen:** Bestätigen Sie, dass Ihre AWS-Anmeldeinformationen gültig sind und nicht abgelaufen sind. Details sind unter ["AWS-Anmeldeinformationen hinzufügen"](#) verfügbar.

Dashboard lädt nicht oder lädt nur langsam

Problem: Das Dashboard lädt langsam oder einige Widgets werden nicht angezeigt.

Ursache: Langsame Ladezeiten können durch Netzwerkprobleme, große Datenmengen oder vorübergehende Serviceverzögerungen verursacht werden.

Lösung:

- **Überprüfen Sie Ihre Internetverbindung:** Es sollte sichergestellt sein, dass Ihre Internetverbindung stabil ist.
- **Aktualisieren Sie Ihren Browser:** Die Seite kann neu geladen werden, um zu prüfen, ob das Dashboard korrekt geladen wird.
- **Browser-Cache und Cookies löschen:** Dies kann dazu beitragen, Ladeprobleme zu beheben, die durch veraltete oder beschädigte Daten verursacht werden.

- **Warten und erneut versuchen:** Wenn das Problem weiterhin besteht, einige Minuten abwarten und es dann erneut versuchen.

Fehlende Dashboards

Problem: Ein von Ihnen erstelltes Dashboard wird nicht mehr im Dashboard-Katalog aufgeführt.

Ursache: Ein anderer Benutzer in Ihrem Workload Factory-Konto hat sie möglicherweise gelöscht.

Lösung:

- Stellen Sie sicher, dass Sie im richtigen Workload Factory Konto angemeldet sind.
- Fragen Sie andere Benutzer Ihres Kontos, ob jemand das Dashboard gelöscht hat.
- Falls erforderlich kann das Dashboard anhand der ursprünglichen Anforderungen neu erstellt werden.

Alle Benutzer eines Workload Factory Kontos können benutzerdefinierte Dashboards anzeigen und löschen. Bei der Verwaltung gemeinsam genutzter Dashboards ist eine Abstimmung mit Ihrem Team erforderlich.

Weitere Hilfe

Falls weiterhin Probleme mit benutzerdefinierten Dashboards auftreten, enthält ["Hilfe erhalten"](#) Informationen zur Kontaktaufnahme mit dem NetApp Support.

Automatisierung von Aufgaben mit Codebox

Informationen zur Codebox-Automatisierung in NetApp Workload Factory

Codebox ist ein Infrastructure as Code (IaC) Co-Pilot, der Entwicklern und DevOps dabei hilft, den Code zu generieren, der für die Ausführung beliebiger von NetApp Workload Factory unterstützter Operationen benötigt wird. Codebox ist auf die Berechtigungsrichtlinien von Workload Factory abgestimmt und schafft einen klaren Weg zur Ausführungsbereitschaft sowie einen Automatisierungskatalog für die schnelle spätere Wiederverwendung.

Codebox Funktionen

Codebox bietet zwei wichtige IaC-Funktionen:

- Codebox Viewer zeigt den durch einen bestimmten Job-Flow-Vorgang generierten IaC-Code an, indem Einträge und Auswahlen aus dem grafischen Assistenten oder aus der Chat-Oberfläche abgeglichen werden. Codebox Viewer unterstützt zwar die Farbcodierung zur einfacheren Navigation und Analyse, erlaubt aber keine Bearbeitung, sondern lediglich das Kopieren oder Speichern von Code im Automation Catalog.
- Im *Codebox Automation Catalog* werden alle gespeicherten IaC-Jobs angezeigt, sodass Sie zur späteren Verwendung einfach darauf verweisen können. Jobs aus dem Automation Catalog werden als Vorlagen gespeichert und im Kontext der Ressourcen angezeigt, die für sie gelten.

Zusätzlich zeigt Codebox beim Einrichten der Anmeldeinformationen für Workload Factory dynamisch die AWS-Berechtigungen an, die zum Erstellen von IAM-Richtlinien erforderlich sind. Die Berechtigungen werden für jede Workload Factory-Funktion bereitgestellt, die Sie verwenden möchten (Datenbanken, AI, FSx for ONTAP usw.), und sie sind anpassbar. Die Berechtigungen lassen sich einfach aus Codebox kopieren und

dann in die AWS Management Console einfügen, damit Workload Factory über die korrekten Berechtigungen zum Managen Ihrer Workloads verfügt.

Unterstützte Codeformate

Die unterstützten Codeformate umfassen:

- Workload Factory REST-APIs
- AWS CLI
- AWS CloudFormation
- Terraform

Verwandte Informationen

["So verwenden Sie Codebox"](#).

["Workload Factory REST API Dokumentation"](#).

Verwendung von Codebox für die Automatisierung in NetApp Workload Factory

Mit Codebox können Sie den Code generieren, der zur Ausführung aller von NetApp Workload Factory unterstützten Operationen benötigt wird. Sie können Code generieren, der mithilfe von Workload Factory REST APIs, der AWS CLI und AWS CloudFormation genutzt und ausgeführt werden kann.

Codebox ist auf die Berechtigungsrichtlinien der Workload Factory abgestimmt, indem die entsprechenden Daten im Code auf Grundlage der im Workload Factory Konto für jeden Benutzer bereitgestellten AWS-Berechtigungen eingefügt werden. Der Code kann wie eine Vorlage verwendet werden, in der Sie fehlende Informationen (z. B. Anmeldeinformationen) ergänzen oder bestimmte Daten vor der Ausführung anpassen können.

Verwendung von Codebox

Während Sie in den Benutzeroberflächenassistenten in der NetApp Console Werte eingeben, können Sie sehen, wie die Daten in Codebox bei jedem ausgefüllten Feld aktualisiert werden. Wenn der Assistent abgeschlossen ist, aber bevor unten auf der Seite die Schaltfläche **Create** ausgewählt wird, kann in Codebox  zum Kopieren ausgewählt werden, um den zum Erstellen Ihrer Konfiguration erforderlichen Code zu erfassen. Dieser Screenshot aus dem Erstellen eines neuen Microsoft SQL Server zeigt beispielsweise die Assistenteneingaben für VPC und Availability Zones sowie die entsprechenden Einträge in Codebox für eine REST API Implementierung.

The screenshot shows the 'Create new Microsoft SQL server' interface. On the left, the 'Region & VPC' section is set to 'us-east-1 | US East (N. Virginia)' and 'VPC-1 | 172.30.0.0/20'. The 'Availability zones' section shows two nodes: Node 1 with 'us-east-1d' and 'HCL-CC-1 | 192.168.16.0/24', and Node 2 with 'us-east-2d' and 'HCL-CC-2 | 192.168.17.0/24'. The 'Security group' is set to 'Use an existing security group | sg-ad2b38d1'. On the right, the 'Codebox' shows a REST API call to 'https://api.workloads.netapp.com/accounts/acc' with a JSON payload. Green arrows indicate the mapping: 'us-east-1' to 'availabilityZone1', 'us-east-2d' to 'availabilityZone2', and the VPC ID to 'vpcId'.

Bei einigen Codeformaten können Sie auch die Download-Schaltfläche auswählen, um den Code in einer Datei zu speichern und auf ein anderes System zu übertragen. Bei Bedarf können Sie den Code nach dem Download bearbeiten, um ihn an andere AWS-Konten anzupassen.

Verwendung von CloudFormation Code aus Codebox

Sie können den von Codebox generierten CloudFormation Code kopieren und anschließend den Amazon Web Services CloudFormation Stack in Ihrem AWS-Konto starten. CloudFormation führt die Aktionen aus, die Sie in der Workload Factory-Benutzeroberfläche definiert haben.

Die Schritte zur Verwendung des CloudFormation Codes können unterschiedlich sein, je nachdem, ob Sie ein FSx for ONTAP Dateisystem einsetzen, Kontoanmeldedaten erstellen oder andere Workload Factory Aktionen durchführen.

Der Code in einer CloudFormation-generierten YAML-Datei läuft aus Sicherheitsgründen nach 7 Tagen ab.

Bevor Sie beginnen

- Sie benötigen Anmeldeinformationen, um sich bei Ihrem AWS account anzumelden.
- Um einen CloudFormation Stack verwenden zu können, benötigen Sie die folgenden Benutzerberechtigungen:

▼ Details

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
```

```

        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:GetTemplate",
        "cloudformation:ValidateTemplate",
        "lambda:InvokeFunction",
        "iam:PassRole",
        "iam:CreateRole",
        "iam:UpdateAssumeRolePolicy",
        "iam:AttachRolePolicy",
        "iam:CreateServiceLinkedRole"
    ],
    "Resource": "*"
}
]
}

```

Schritte

1. Nachdem Sie in NetApp Console die gewünschte Operation definiert haben, erfolgt das Kopieren des Codes in die Codebox.
2. Nach Auswahl von **Weiterleiten zu CloudFormation** wird die Seite „Weiterleiten zu CloudFormation“ angezeigt.
3. Anmeldung bei der AWS Management Console in einem weiteren Browserfenster.
4. Auf der Seite „Weiterleiten zu CloudFormation“ wählen Sie **Weiter** aus.
5. Die Anmeldung sollte bei dem AWS-Konto erfolgen, in dem der Code ausgeführt werden soll.
6. Auf der Seite „Quick create stack“ unter „Capabilities“ die Option **Ich bestätige, dass AWS CloudFormation möglicherweise ...** auswählen.
7. **Create stack** auswählen.
8. Der Fortschritt lässt sich über AWS oder Workload Factory verfolgen.

Verwendung von REST API-Code aus Codebox

Sie können die mit Codebox generierten Workload Factory REST APIs verwenden, um Ihre FSx for ONTAP Dateisysteme und andere AWS Ressourcen einzusetzen und zu managen.

Sie können die APIs von jedem Host ausführen, der curl unterstützt und über eine Internetverbindung verfügt.

Beachten Sie, dass die Authentifizierungstoken in Codebox ausgeblendet sind, aber beim Kopieren und Einfügen des API-Aufrufs eingefügt werden.

Schritte

1. Nachdem Sie die gewünschte Operation mit NetApp Console definiert haben, können Sie den API-Code in der Codebox kopieren.
2. Der Code kann in Ihr Hostsystem eingefügt und dort ausgeführt werden.

AWS CLI-Code aus Codebox verwenden

Sie können die von Codebox generierte Amazon Web Services CLI verwenden, um Ihre FSx for ONTAP Dateisysteme und andere AWS-Ressourcen einzusetzen und zu managen.

Schritte

1. Nachdem Sie mit NetApp Console den gewünschten Vorgang definiert haben, steht die AWS CLI in der Codebox zum Kopieren bereit.
2. Anmeldung bei der AWS Management Console in einem weiteren Browserfenster.
3. Der Code kann nun eingefügt und ausgeführt werden.

Terraform aus Codebox verwenden

Mit Terraform können Sie Ihre FSx for ONTAP Dateisysteme und andere AWS-Ressourcen einsetzen und managen.

Bevor Sie beginnen

- Sie benötigen ein System, auf dem Terraform installiert ist (Windows/Mac/Linux).
- Sie benötigen Anmeldeinformationen, um sich bei Ihrem AWS account anzumelden.

Schritte

1. Nachdem Sie mit NetApp Console den gewünschten Vorgang definiert haben, steht der Terraform-Code in der Codebox zum Herunterladen bereit.
2. Das heruntergeladene Skriptarchiv sollte auf das System kopiert werden, auf dem Terraform installiert ist.
3. Nach dem Entpacken der ZIP-Datei sind die Schritte in der Datei README.md zu befolgen.

Verwendung von CloudShell in NetApp Workload Factory

Mit CloudShell lassen sich AWS- oder ONTAP CLI-Befehle von überall in der NetApp Workload Factory Konsole ausführen.

Über diese Aufgabe

CloudShell ermöglicht die Ausführung von AWS CLI Befehlen oder ONTAP CLI Befehlen in einer Shell-ähnlichen Umgebung innerhalb der Workload Factory Konsole. Es simuliert Terminal-Sitzungen im Browser, stellt Terminalfunktionen bereit und leitet Nachrichten über das Workload Factory Backend weiter. Es ermöglicht die Verwendung der AWS Anmeldeinformationen und ONTAP Anmeldeinformationen, die Sie in Ihrem NetApp Konto angegeben haben.

CloudShell umfasst folgende Funktionen:

- Mehrere CloudShell Sitzungen: mehrere CloudShell Sitzungen gleichzeitig einsetzen, um mehrere Befehlssequenzen parallel auszuführen,
- Mehrere Ansichten: Aufteilen von CloudShell Tab-Sitzungen, sodass zwei oder mehr Tabs gleichzeitig horizontal oder vertikal angezeigt werden können
- Sitzungsumbenennung: Sitzungen lassen sich bei Bedarf umbenennen
- Beibehaltung des Inhalts der letzten Sitzung: Erneutes Öffnen der letzten Sitzung, wenn sie versehentlich geschlossen wurde

- Voreinstellungen: Änderung der Schriftgröße und des Ausgabetyps
- KI-generierte Fehlermeldungen für ONTAP CLI-Befehle
- Unterstützung für die Autovervollständigung: Bei der Eingabe eines Befehls lassen sich mit der Taste **Tab** verfügbare Optionen anzeigen



Wenn Ihr Kontoadministrator die KI-Funktionen deaktiviert hat, stehen keine KI-generierten Fehlermeldungen zur Verfügung. ["Informationen zur Verwaltung von KI-Funktionen"](#).

CloudShell Befehle

In der CloudShell GUI können Sie `help` eingeben, um verfügbare CloudShell Befehle anzuzeigen. Nach Eingabe des Befehls `help` erscheint die folgende Referenz.

Beschreibung

NetApp CloudShell ist eine in NetApp Workload Factory integrierte grafische Benutzeroberfläche, mit der AWS CLI Befehle oder ONTAP CLI Befehle in einer Shell-ähnlichen Umgebung ausgeführt werden können. Es simuliert Terminal-Sitzungen im Browser, stellt Terminalfunktionen bereit und leitet Nachrichten über das Backend in Workload Factory weiter. Damit können die AWS Anmeldeinformationen und ONTAP Anmeldeinformationen verwendet werden, die im NetApp Konto angegeben wurden.

Verfügbare Befehle

- `clear`
- `help`
- `[--fsx <fsxId>] <ontap-command> [parameters]`
- `aws <aws-command> <aws-sub-command> [parameters]`

Kontext

Jede Terminal-Sitzung wird in einem bestimmten Kontext ausgeführt: Anmeldeinformationen, Region und optional das FSx for ONTAP file system.

+ Alle AWS-Befehle werden im angegebenen Kontext ausgeführt. AWS-Befehle sind nur erfolgreich, wenn die angegebenen Anmeldeinformationen über Berechtigungen in der angegebenen Region verfügen.

+ Sie können ONTAP Befehle optional mit einer `fsxId` ID angeben. Wenn Sie eine `fsxId` ID mit einem einzelnen ONTAP Befehl angeben, überschreibt diese ID die ID im Kontext. Wenn die Terminalsitzung keinen FSx for ONTAP Dateisystem-ID-Kontext hat, müssen Sie mit jedem ONTAP Befehl `fsxId` angeben.

+ Zum Aktualisieren verschiedener kontextspezifischer Angaben ist Folgendes zu tun: * Zum Ändern der Anmeldedaten: `"using credentials <credentialId>"` * Zum Ändern der Region: `"using region <regionCode>"` * Zum Ändern des FSx for ONTAP Dateisystems: `"using fsx <fileSystemId>"`

Elemente werden angezeigt

- Verfügbare Anmeldeinformationen lassen sich mit `"show credentials"` anzeigen
- Um die verfügbaren Regionen anzuzeigen: `"show regions"`
- Zum Anzeigen des Befehlsverlaufs: `"show history"`

Variablen

Im Folgenden sind Beispiele für das Setzen und Verwenden von Variablen aufgeführt. Enthält ein Variablenwert Leerzeichen, sollte er in Anführungszeichen gesetzt werden.

+ * Zum Setzen einer Variable: `$<variable> = <value>` * Zum Verwenden einer Variable: `$<variable>` * Beispiel zum Setzen einer Variable: `$svm1 = svm123` * Beispiel zum Verwenden einer Variable: `--fsx FileSystem-1 volumes show --vserver $svm1` * Beispiel zum Setzen einer Variable mit Stringwert `$comment1 = "Ein Kommentar mit Leerzeichen"`

Betreiber

Shell-Operatoren wie Pipes `|`, Hintergrundausführung `&` und Umleitung `>` werden nicht unterstützt. Die Befehlsausführung schlägt fehl, wenn Sie diese Operatoren verwenden.

Bevor Sie beginnen

CloudShell funktioniert im Kontext Ihrer AWS-Anmeldeinformationen. Für die Verwendung von CloudShell muss mindestens eine AWS-Anmeldeinformation angegeben werden.



CloudShell steht Ihnen zur Verfügung, um beliebige AWS oder ONTAP CLI Befehle auszuführen. Wenn Sie jedoch im Kontext eines FSx for ONTAP Dateisystems arbeiten möchten, ist die Ausgabe des folgenden Befehls erforderlich: `using fsx <file-system-name>`.

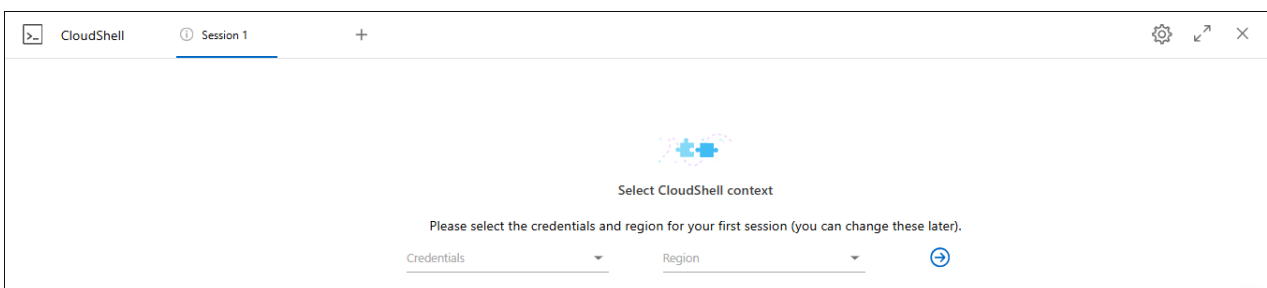
Einsetzen von CloudShell

Das Einsetzen von CloudShell ist von überall in der NetApp Workload Factory Konsole möglich. Das Einsetzen von CloudShell ist auch über die NetApp Console möglich.

Einsatz über die Workload Factory console

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü der NetApp Console steht **Workloads > Administration > CloudShell** zur Auswahl.
3. Im CloudShell Fenster werden die Anmeldeinformationen und die Region für die CloudShell Sitzung ausgewählt; anschließend wird zum Fortfahren der Pfeil ausgewählt.



4. Durch Eingabe von `help` lassen sich die verfügbaren [CloudShell Befehle](#) und Anweisungen anzeigen; alternativ können die folgenden CLI-Referenzdokumente zu verfügbaren Befehlen herangezogen werden:
 - ["AWS CLI Referenz"](#): Für Befehle im Zusammenhang mit FSx for ONTAP wird **fsx** ausgewählt.
 - ["ONTAP CLI-Referenz"](#)
5. Die Eingabe der Befehle erfolgt innerhalb der CloudShell Sitzung.

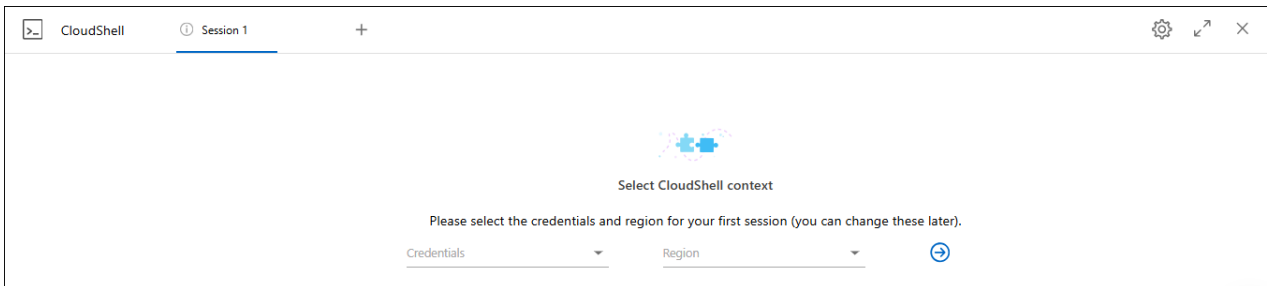
Wenn nach Ausführung eines ONTAP CLI-Befehls ein Fehler auftritt, kann über das Glühbirnensymbol eine kurze, KI-generierte Fehlerantwort mit einer Beschreibung des Fehlers, der

Fehlerursache und einer detaillierten Lösung abgerufen werden. Weitere Details sind unter **Read more** verfügbar.

Bereitstellung über die NetApp Console

Schritte

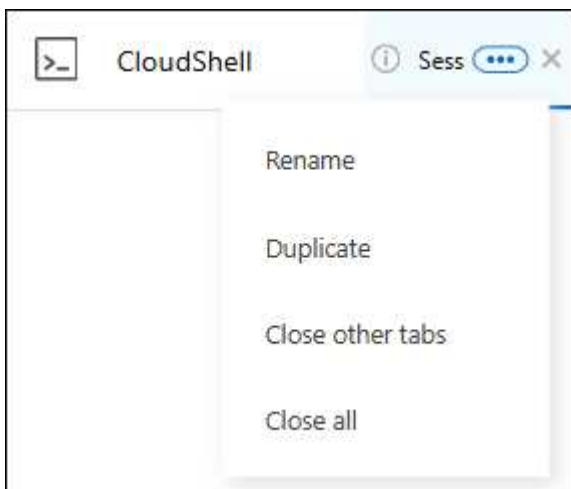
1. Melden Sie sich bei der "NetApp Console" an.
2. Im Menü der NetApp Console steht **Workloads > Administration > CloudShell** zur Auswahl.
3. Im CloudShell Fenster werden die Anmeldeinformationen und die Region für die CloudShell Sitzung ausgewählt; anschließend wird zum Fortfahren der Pfeil ausgewählt.



4. Mit `help` werden die verfügbaren CloudShell Befehle und Anweisungen angezeigt; alternativ können die folgenden CLI-Referenzdokumente zu verfügbaren Befehlen herangezogen werden:
 - "AWS CLI Referenz": Für Befehle im Zusammenhang mit FSx for ONTAP wird **fsx** ausgewählt.
 - "ONTAP CLI-Referenz"
5. Die Eingabe der Befehle erfolgt innerhalb der CloudShell Sitzung.

Wenn nach Ausführung eines ONTAP CLI-Befehls ein Fehler auftritt, kann über das Glühbirnensymbol eine kurze, KI-generierte Fehlerantwort mit einer Beschreibung des Fehlers, der Fehlerursache und einer detaillierten Lösung abgerufen werden. Weitere Details sind unter **Read more** verfügbar.

Die in diesem Screenshot dargestellten CloudShell Aufgaben lassen sich über das Aktionsmenü der Registerkarte einer geöffneten CloudShell Sitzung ausführen. Die Anweisungen für jede dieser Aufgaben folgen.



Umbenennen einer CloudShell Sitzungsregisterkarte

Sie können einen CloudShell Sitzungsreiter umbenennen, um die Sitzung leichter identifizieren zu können.

Schritte

1. Auswahl des Aktionsmenüs der Registerkarte „Sitzung“ in der CloudShell Sitzung.
2. **Umbenennen** auswählen.
3. Für die Sitzungsregisterkarte wird ein neuer Name eingegeben; anschließend wird zum Festlegen des neuen Namens außerhalb des Registerkartennamens geklickt.

Ergebnis

Der neue Name wird auf der Registerkarte der CloudShell Sitzung angezeigt.

Registerkarte für doppelte CloudShell Sitzungen

Sie können eine CloudShell Sitzungskarte duplizieren, um eine neue Sitzung mit demselben Namen, denselben Anmeldeinformationen und derselben Region zu erstellen. Der Code aus der ursprünglichen Registerkarte wird in der duplizierten Registerkarte nicht dupliziert.

Schritte

1. Auswahl des Aktionsmenüs der Registerkarte „Sitzung“ in der CloudShell Sitzung.
2. Sie wählen **Duplizieren** aus.

Ergebnis

Die neue Registerkarte erscheint mit demselben Namen wie die ursprüngliche Registerkarte.

Schließen der CloudShell Sitzungstabs

Sie können CloudShell Tabs einzeln schließen, andere Tabs, an denen Sie gerade nicht arbeiten, schließen oder alle Tabs gleichzeitig schließen.

Schritte

1. Auswahl des Aktionsmenüs der Registerkarte „Sitzung“ in der CloudShell Sitzung.
2. Wählen Sie eine der folgenden Optionen aus:
 - Im Registerkartenfenster CloudShell lässt sich mit „X“ jeweils eine Registerkarte schließen.
 - Mit **Andere Tabs schließen** werden alle anderen geöffneten Tabs mit Ausnahme des Tabs geschlossen, an dem Sie gerade arbeiten.
 - Mit **Alle Tabs schließen** werden alle Tabs geschlossen.

Ergebnis

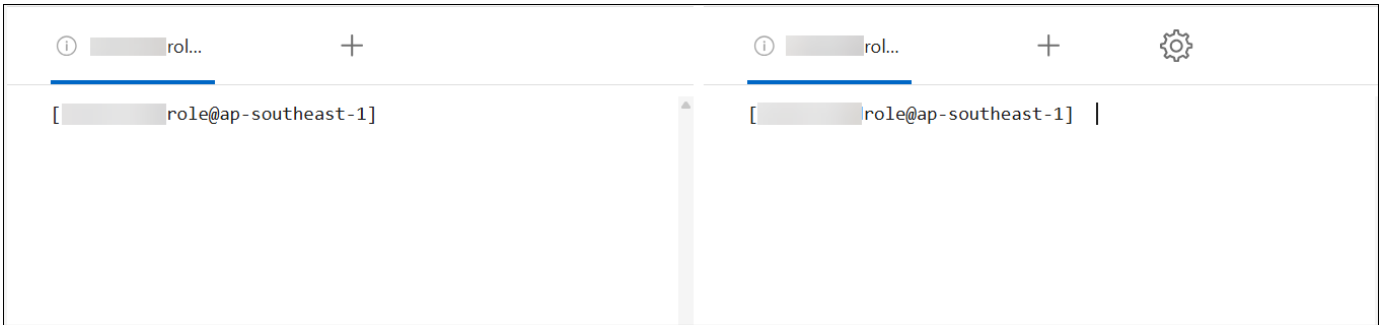
Die ausgewählten CloudShellSitzungsregisterkarten werden geschlossen.

Registerkarten von CloudShell Sitzungen aufteilen

Sie können CloudShell Sitzungstabs aufteilen, um zwei oder mehr Tabs gleichzeitig anzuzeigen.

Schritt

Durch Ziehen und Ablegen der CloudShell Sitzungsregisterkarten an den oberen, unteren, linken oder rechten Rand des CloudShell Fensters lässt sich die Ansicht teilen.



Einstellungen für eine CloudShell Sitzung aktualisieren

Sie können die Einstellungen für Schriftart und Ausgabetyt für CloudShell Sitzungen aktualisieren.

Schritte

1. Bereitstellung einer CloudShell Sitzung.
2. Auf der Registerkarte CloudShell das Symbol „Einstellungen“ auswählen.

Der Einstellungsdialog wird angezeigt.

3. Die Schriftgröße und der Ausgabetyt lassen sich nach Bedarf anpassen.



Die angereicherte Ausgabe gilt für JSON-Objekte und Tabellenformatierungen. Alle anderen Ausgaben werden als Klartext angezeigt.

4. **Anwenden** auswählen.

Ergebnis

Die CloudShell Einstellungen wurden aktualisiert.

Entfernen von Anmeldeinformationen aus NetApp Workload Factory

Wenn Sie Anmeldeinformationen nicht mehr benötigen, können Sie diese in Workload Factory löschen. Sie können nur Anmeldeinformationen löschen, die nicht mit einem FSx for ONTAP Dateisystem verknüpft sind.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Im Menü der NetApp Console erfolgt die Auswahl von **Workloads** > **Administration** > **Credentials**.
3. Auf der Seite **Anmeldeinformationen** sind folgende Schritte erforderlich:
 - In der Workload Factory Konsole wird im Aktionsmenü für einen Satz Anmeldeinformationen die Option **Remove** ausgewählt. Zur Bestätigung wird **Remove** ausgewählt.
 - In der NetApp Console wählen Sie für einen Satz von Anmeldeinformationen das Aktionsmenü und anschließend **Delete** aus. Wählen Sie zur Bestätigung **Delete** aus.

Wissen und Unterstützung

Für Support bei der NetApp Console registrieren

Für den Erhalt von technischem Support speziell für die NetApp Console und deren Storage-Lösungen und Datendienste ist eine Supportregistrierung erforderlich. Eine Supportregistrierung ist ebenfalls erforderlich, um wichtige Workflows für Cloud Volumes ONTAP Systeme zu ermöglichen.

Die Registrierung für den Support aktiviert keinen NetApp Support für einen Dateidienst eines Cloud-Anbieters. Technischer Support in Bezug auf einen Dateidienst eines Cloud-Anbieters, dessen Infrastruktur oder eine Lösung, die diesen Dienst nutzt, ist im Abschnitt „Hilfe erhalten“ der Dokumentation des jeweiligen Produkts zu finden.

- ["Amazon FSx for ONTAP"](#)
- ["Azure NetApp Files"](#)
- ["Google Cloud NetApp Volumes"](#)

Übersicht der Supportregistrierung

Es gibt zwei Registrierungsformen zur Aktivierung des Anspruchs auf Support:

- Registrierung der NetApp Console-Kontoseriennummer (der 20-stellige 960xxxxxxx-Seriennummer, die auf der Support Resources-Seite in der Console zu finden ist).

Dies dient als Ihre einzige Support-Abonnement-ID für jeden Dienst innerhalb der Console. Jedes Console-Konto muss registriert sein.

- Registrierung der Cloud Volumes ONTAP Seriennummern, die mit einem Abonnement verknüpft sind, auf dem Marktplatz Ihres Cloud-Anbieters (dies sind 20-stellige 909201xxxxxxx Seriennummern).

Diese Seriennummern werden üblicherweise als *PAYGO-Seriennummern* bezeichnet und von der NetApp Console zum Zeitpunkt der Cloud Volumes ONTAP Bereitstellung generiert.

Durch die Registrierung beider Seriennummertypen werden Funktionen wie das Erstellen von Support-Tickets und die automatische Fallgenerierung ermöglicht. Die Registrierung wird durch das Hinzufügen von NetApp Support Site (NSS)-Konten zur Konsole abgeschlossen, wie unten beschrieben.

Die NetApp Console für den NetApp Support registrieren

Um sich für den Support zu registrieren und die Supportberechtigung zu aktivieren, muss ein Benutzer Ihres NetApp Console-Kontos ein NetApp Support Site-Konto mit seinem Console-Login verknüpfen. Wie die Registrierung für den NetApp Support erfolgt, hängt davon ab, ob bereits ein NetApp Support Site-Konto (NSS-Konto) vorhanden ist.

Bestandskunde mit einem NSS-Konto

Wenn Sie ein NetApp Kunde mit einem NSS-Konto sind, ist lediglich eine Registrierung für den Support über die Console erforderlich.

Schritte

1. **Administration > Anmeldeinformationen** auswählen.
2. **Benutzeranmeldeinformationen** auswählen.
3. **NSS-Anmeldeinformationen hinzufügen** auswählen und der Authentifizierungsaufforderung der NetApp Support-Website (NSS) folgen.
4. Zur Bestätigung, dass der Registrierungsvorgang erfolgreich war, das Hilfesymbol auswählen und anschließend **Support** wählen.

Auf der Seite **Ressourcen** sollte angezeigt werden, dass Ihr Console-Konto für den Support registriert ist.

Beachten Sie, dass andere Console-Benutzer diesen Support-Registrierungsstatus nicht sehen, wenn sie kein NetApp Support Site-Konto mit ihrem Login verknüpft haben. Das bedeutet jedoch nicht, dass Ihr Konto nicht für den Support registriert ist. Solange mindestens ein Benutzer in der Organisation diese Schritte durchgeführt hat, ist Ihr Konto registriert.

Bestandskunde, aber kein NSS-Konto

Wenn Sie bereits NetApp Kunde sind und über bestehende Lizenzen und Seriennummern, aber *kein* NSS-Konto verfügen, ist es erforderlich, ein NSS-Konto zu erstellen und dieses mit Ihrem Console-Login zu verknüpfen.

Schritte

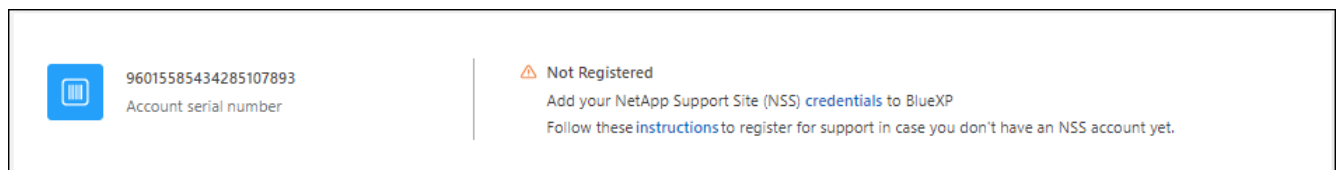
1. Ein NetApp Support Site-Konto kann erstellt werden, indem das "[NetApp Support Site Benutzerregistrierungsformular](#)" Formular ausgefüllt wird.
 - a. Es sollte die passende Benutzerstufe ausgewählt werden, die in der Regel **NetApp Customer/End User** ist.
 - b. Kopieren Sie die oben verwendete Console Account-Seriennummer (960xxxx) für das Seriennummernfeld. Dadurch wird die Kontobearbeitung beschleunigt.
2. Das neue NSS-Konto wird mit Ihrem Console-Login verknüpft, indem die Schritte unter [Bestandskunde mit einem NSS-Konto](#) abgeschlossen werden.

Ganz neu bei NetApp

Wenn Sie ganz neu bei NetApp sind und kein NSS-Konto haben, führen Sie die folgenden Schritte aus.

Schritte

1. Oben rechts in der Konsole das Hilfesymbol auswählen und anschließend **Support** wählen.
2. Die Konto-ID-Seriennummer befindet sich auf der Support-Registrierungsseite.



3. Navigieren Sie zu "[NetApp's Support-Registrierungsseite](#)" und wählen Sie **Ich bin kein registrierter NetApp Customer** aus.
4. Füllen Sie die Pflichtfelder (die mit roten Sternchen) aus.
5. Im Feld **Produktlinie** wird **Cloud Manager** ausgewählt und anschließend der entsprechende Abrechnungsanbieter.

6. Kopieren Sie Ihre Kontoseriennummer aus Schritt 2 oben, führen Sie die Sicherheitsprüfung durch und bestätigen Sie anschließend, dass Sie die globale Datenschutzrichtlinie von NetApp gelesen haben.

Um diese sichere Transaktion abzuschließen, wird umgehend eine E-Mail an die angegebene Adresse gesendet. Es empfiehlt sich, den Spam-Ordner zu überprüfen, falls die Bestätigungs-E-Mail nicht innerhalb weniger Minuten eintrifft.

7. Die Aktion wird direkt in der E-Mail bestätigt.

Mit der Bestätigung wird Ihre Anfrage an NetApp übermittelt und es wird empfohlen, ein NetApp Support Site-Konto zu erstellen.

8. Ein NetApp Support Site-Konto kann erstellt werden, indem das "[NetApp Support Site Benutzerregistrierungsformular](#)" Formular ausgefüllt wird.
 - a. Es sollte die passende Benutzerstufe ausgewählt werden, die in der Regel **NetApp Customer/End User** ist.
 - b. Bitte kopieren Sie die oben angegebene Kontoseriennummer (960xxxx) in das Feld „Seriennummer“. Dies beschleunigt die Bearbeitung.

Nachdem Sie fertig sind

NetApp sollte sich während dieses Prozesses mit Ihnen in Verbindung setzen. Dies ist eine einmalige Einführungsmaßnahme für neue Benutzer.

Sobald Sie über Ihr NetApp Support Site-Konto verfügen, kann das Konto mit Ihrem Console-Login verknüpft werden, indem die Schritte unter [Bestandskunde mit einem NSS-Konto](#) abgeschlossen werden.

NSS-Zugangsdaten für Cloud Volumes ONTAP Support zuordnen

Die Verknüpfung der NetApp Support Site-Anmeldeinformationen mit Ihrem Console-Konto ist erforderlich, um die folgenden wichtigen Workflows für Cloud Volumes ONTAP zu ermöglichen:

- Registrierung von Cloud Volumes ONTAP Systemen mit nutzungsbasierter Abrechnung für den Support

Die Angabe Ihres NSS-Kontos ist erforderlich, um den Support für Ihr System zu aktivieren und Zugang zu NetApp technischen Supportressourcen zu erhalten.

- Bereitstellung von Cloud Volumes ONTAP bei Verwendung eigener Lizenz (BYOL)

Die Angabe Ihres NSS-Kontos ist erforderlich, damit die NetApp Console Ihren Lizenzschlüssel hochladen und das Abonnement für die von Ihnen erworbene Laufzeit aktivieren kann. Dies umfasst automatische Updates für Laufzeitverlängerungen.

- Aktualisierung der Cloud Volumes ONTAP Software auf die neueste Version

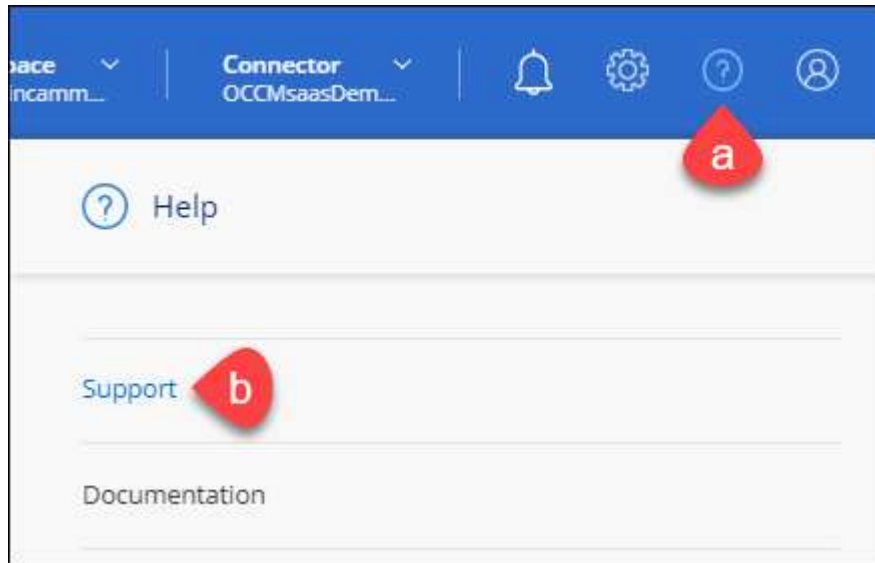
Die Verknüpfung von NSS-Anmeldeinformationen mit Ihrem NetApp Console-Konto unterscheidet sich von dem NSS-Konto, das mit einem Console-Benutzerlogin verknüpft ist.

Diese NSS-Zugangsdaten sind mit Ihrer spezifischen Console-Konto-ID verknüpft. Benutzer, die zur Console-Organisation gehören, können auf diese Zugangsdaten unter **Support > NSS Management** zugreifen.

- Wenn Sie über ein Kundenkonto 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 Kundenkonten hinzugefügt werden.

Schritte

1. Oben rechts in der Konsole das Hilfesymbol auswählen und anschließend **Support** wählen.



2. **NSS Management > Add NSS Account** auswählen.
3. Wenn Sie dazu aufgefordert werden, **Weiter** auswählen, erfolgt eine Weiterleitung zur Microsoft-Anmeldeseite.

NetApp verwendet Microsoft Entra ID als Identitätsanbieter für Authentifizierungsdienste im Zusammenhang mit Support und Lizenzierung.

4. Auf der Anmeldeseite sind die bei der NetApp Support Site registrierte E-Mail-Adresse und das Passwort anzugeben, um den Authentifizierungsprozess durchzuführen.

Diese Aktionen ermöglichen es der Konsole, Ihr NSS-Konto für Aufgaben wie das Herunterladen von Lizenzen, die Überprüfung von Software-Upgrades und zukünftige Support-Registrierungen zu nutzen.

Dabei ist Folgendes zu beachten:

- Das NSS-Konto muss ein Kundenkonto sein (kein Gast- oder temporäres Konto). Es können mehrere Kundenkonten auf NSS-Ebene vorhanden sein.
- Es kann nur ein NSS-Konto geben, wenn es sich um ein Partner-Level-Konto handelt. Wenn versucht wird, NSS-Konten auf Kundenebene hinzuzufügen und bereits ein Partner-Level-Konto existiert, erscheint die folgende Fehlermeldung:

„Der NSS-Kundentyp ist für dieses Konto nicht zulässig, da bereits NSS-Benutzer eines anderen Typs vorhanden sind.“

Das Gleiche gilt, wenn bereits NSS-Kundenkonten vorhanden sind und versucht wird, ein Partnerkonto hinzuzufügen.

- Nach erfolgreicher Anmeldung speichert NetApp den NSS-Benutzernamen.

Dies ist eine systemgenerierte ID, die Ihrer E-Mail-Adresse zugeordnet ist. Auf der Seite **NSS Management** können Sie Ihre E-Mail-Adresse über das **...** Menü anzeigen.

- Wenn Sie Ihre Anmelde-Credential-Tokens jemals aktualisieren müssen, gibt es im **...** Menü auch die Option **Anmeldeinformationen aktualisieren**.

Bei Nutzung dieser Option müssen Sie sich erneut anmelden. Beachten Sie, dass das Token für diese Konten nach 90 Tagen abläuft. Eine Benachrichtigung wird veröffentlicht, um Sie darauf hinzuweisen.

Hilfe zu NetApp Console Cloud-Services

NetApp bietet Unterstützung für NetApp Console und dessen Cloud-Services auf vielfältige Weise. Umfangreiche kostenlose Selbsthilfeoptionen wie Knowledge Base (KB)-Artikel und ein Community-Forum stehen rund um die Uhr zur Verfügung. Die Support-Registrierung umfasst technischen Remote-Support über Web-Ticketing.

Support für einen Dateidienst eines Cloud-Anbieters erhalten

Technische Unterstützung im Zusammenhang mit dem Dateidienst eines Cloud-Anbieters, seiner Infrastruktur oder einer Lösung, die diesen Dienst nutzt, finden Sie in der Dokumentation des jeweiligen Produkts.

- ["Amazon FSx for ONTAP"](#)
- ["Azure NetApp Files"](#)
- ["Google Cloud NetApp Volumes"](#)

Um technischen Support speziell für NetApp und dessen Speicherlösungen und Datendienste zu erhalten, nutzen Sie die unten beschriebenen Supportoptionen.

Selbsthilfeoptionen verwenden

Diese Optionen stehen Ihnen kostenlos 24 Stunden am Tag, 7 Tage die Woche zur Verfügung:

- Dokumentation

Die NetApp Console-Dokumentation, die Sie gerade ansehen.

- ["Wissensdatenbank"](#)

Durchsuchen Sie die NetApp Wissensdatenbank, um hilfreiche Artikel zur Fehlerbehebung zu finden.

- ["Communities"](#)

Tritt der NetApp Console-Community bei, um laufende Diskussionen zu verfolgen oder neue zu starten.

Einen Fall beim NetApp Support erstellen

Zusätzlich zu den oben genannten Selbsthilfeoptionen können Sie nach der Aktivierung des Supports mit einem NetApp Support-Spezialisten zusammenarbeiten, um etwaige Probleme zu lösen.

Bevor Sie beginnen

- Um die Funktion **Fall erstellen** nutzen zu können, müssen Sie zunächst Ihre NetApp Support Site-Anmeldeinformationen mit Ihrem Console-Login verknüpfen. ["Erfahren Sie, wie Sie die mit Ihrem Console-Login verknüpften Anmeldeinformationen verwalten."](#)
- Wenn Sie einen Fall für ein ONTAP System mit Seriennummer eröffnen, muss Ihr NSS-Konto mit der Seriennummer dieses Systems verknüpft sein.

Schritte

1. In der NetApp Console wählen Sie **Hilfe > Support**.
2. Auf der Seite **Ressourcen** steht unter Technischer Support eine der verfügbaren Optionen zur Auswahl:
 - a. **Kontaktieren Sie uns** kann ausgewählt werden, wenn ein Telefongespräch mit einer Ansprechperson gewünscht ist. Eine Weiterleitung erfolgt auf eine Seite auf netapp.com, auf der die Telefonnummern aufgeführt sind, die angerufen werden können.
 - b. **Fall erstellen** auswählen, um ein Ticket bei einem NetApp Support-Spezialisten zu eröffnen:
 - **Dienst:** Wählen Sie den Dienst aus, dem das Problem zugeordnet ist. Zum Beispiel **NetApp Console**, wenn es sich um ein technisches Supportproblem mit Workflows oder Funktionen innerhalb der Console handelt.
 - **System:** Falls zutreffend, wählen Sie **Cloud Volumes ONTAP** oder **On-Prem** und anschließend die zugehörige Arbeitsumgebung aus.

Die Liste der Systeme befindet sich im Geltungsbereich der Console-Organisation und des Console-Agenten, den Sie im oberen Banner ausgewählt haben.

- **Fallpriorität:** Die Priorität des Falls kann auf Niedrig, Mittel, Hoch oder Kritisch gesetzt werden.

Weitere Details zu diesen Prioritäten werden angezeigt, wenn der Mauszeiger über das Informationssymbol neben dem Feldnamen gehalten wird.

- **Problembeschreibung:** Eine detaillierte Beschreibung des Problems, einschließlich aller relevanten Fehlermeldungen oder durchgeführten Schritte zur Fehlerbehebung.
- **Weitere E-Mail-Adressen:** Zusätzliche E-Mail-Adressen können eingegeben werden, um eine andere Person auf dieses Problem aufmerksam zu machen.
- **Anhang (optional):** Bis zu fünf Anhänge können einzeln hochgeladen werden.

Anhänge sind auf 25 MB pro Datei beschränkt. Die folgenden Dateierweiterungen werden unterstützt: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.

ntapitdemo
NetApp Support Site Account

Service

Select

Working Enviroment

Select

Case Priority

Low - General guidance

Issue Description

Provide detailed description of problem, applicable error messages and troubleshooting steps taken.

Additional Email Addresses (Optional)

Type here

Attachment (Optional)

No files selected

Upload

Nachdem Sie fertig sind

Es erscheint ein Pop-up mit Ihrer Support-Fallnummer. Ein NetApp Support-Spezialist prüft Ihren Fall und meldet sich in Kürze bei Ihnen.

Für eine Historie Ihrer Supportfälle kann **Einstellungen > Zeitleiste** ausgewählt und nach Aktionen mit dem Namen „Supportfall erstellen“ gesucht werden. Eine Schaltfläche ganz rechts ermöglicht das Erweitern der Aktion, um Details anzuzeigen.

Es ist möglich, dass beim Versuch, einen Fall zu erstellen, die folgende Fehlermeldung angezeigt wird:

„Sie sind nicht berechtigt, einen Case für den ausgewählten Service zu erstellen.“

Dieser Fehler kann bedeuten, dass das NSS-Konto und das zugehörige Unternehmen nicht mit dem Unternehmen übereinstimmen, das für die NetApp Console-Konto-Seriennummer (z. B. 960xxxx) oder die Seriennummer der Arbeitsumgebung als Unternehmen der Registrierung geführt ist. Hilfe ist über eine der folgenden Optionen erhältlich:

- Einen nicht-technischen Fall einreichen unter <https://mysupport.netapp.com/site/help>

Verwalten Sie Ihre Supportfälle

Sie können aktive und abgeschlossene Supportfälle direkt in der Console einsehen und verwalten. Die mit Ihrem NSS-Konto und Ihrem Unternehmen verknüpften Fälle lassen sich verwalten.

Dabei ist Folgendes zu beachten:

- Das Fallmanagement-Dashboard oben auf der Seite bietet zwei Ansichten:
 - Die Ansicht auf der linken Seite zeigt die Gesamtzahl der in den letzten 3 Monaten über das von Ihnen angegebene NSS-Benutzerkonto eröffneten Fälle.
 - Die Ansicht auf der rechten Seite zeigt die Gesamtzahl der in den letzten 3 Monaten auf Unternehmensebene eröffneten Fälle basierend auf Ihrem NSS-Benutzerkonto.

Die Ergebnisse in der Tabelle spiegeln die Fälle wider, die sich auf die von Ihnen ausgewählte Ansicht beziehen.

- Sie können Spalten Ihrer Wahl hinzufügen oder entfernen und den Inhalt von Spalten wie Priorität und Status filtern. Andere Spalten bieten lediglich Sortierfunktionen.

Die folgenden Schritte enthalten weitere Details.

- Auf Ebene einzelner Fälle besteht die Möglichkeit, Fallnotizen zu aktualisieren oder einen Fall zu schließen, der sich noch nicht im Status „Abgeschlossen“ oder „Vorläufig abgeschlossen“ befindet.

Schritte

1. In der NetApp Console wählen Sie **Hilfe > Support**.
2. Wählen Sie **Fallmanagement** aus und fügen Sie gegebenenfalls Ihr NSS-Konto zur Console hinzu.

Die Seite **Fallverwaltung** zeigt offene Fälle an, die mit dem NSS-Konto verknüpft sind, das Ihrem Console-Benutzerkonto zugeordnet ist. Dies ist dasselbe NSS-Konto, das oben auf der Seite **NSS management** angezeigt wird.

3. Optional können die in der Tabelle angezeigten Informationen geändert werden:
 - Unter **Fälle der Organisation** auf **Anzeigen** auswählen, um alle mit Ihrem Unternehmen verknüpften Fälle anzuzeigen.
 - Der Datumsbereich kann geändert werden, indem entweder ein genauer Datumsbereich oder ein anderer Zeitraum ausgewählt wird.
 - Der Inhalt der Spalten filtern.
 - Ändern Sie die in der Tabelle angezeigten Spalten, indem Sie  auswählen und dann die Spalten wählen, die Sie anzeigen möchten.
4. Verwalten Sie einen bestehenden Fall, indem Sie  eine der verfügbaren Optionen auswählen:
 - **Fall ansehen**: Vollständige Details zu einem bestimmten Fall anzeigen.
 - **Fallnotizen aktualisieren**: Zusätzliche Details zu Ihrem Problem können angegeben oder **Dateien hochladen** ausgewählt werden, um bis zu fünf Dateien anzuhängen.

Anhänge sind auf 25 MB pro Datei beschränkt. Die folgenden Dateierweiterungen werden unterstützt: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.

- **Fall schließen**: Geben Sie Einzelheiten dazu an, warum Sie den Fall schließen, und wählen Sie **Fall schließen** aus.

Rechtliche Hinweise

Rechtliche Hinweise bieten Zugriff auf Urheberrechtsvermerke, Marken, Patente und mehr.

Copyright

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marken

NETAPP, das NETAPP-Logo und die auf der NetApp Trademarks-Seite aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen- und Produktnamen können Marken ihrer jeweiligen Eigentümer sein.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Patente

Eine aktuelle Liste der NetApp owned patents finden Sie unter:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Datenschutzrichtlinie

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Open Source

Hinweisdateien enthalten Informationen über Urheberrechte und Lizenzen Dritter, die in NetApp Software verwendet werden.

["Hinweis für die NetApp Console"](#)

["NetApp Workload Factory"](#)

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 IRGEND EINER 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.