



Verwenden Sie Amazon FSX für NetApp ONTAP

Amazon FSx for NetApp ONTAP

NetApp
February 11, 2026

Inhalt

Verwenden Sie Amazon FSX für NetApp ONTAP	1
Entdecken Sie Einsparungen mit FSx für ONTAP in der NetApp Workload Factory	1
Berechnungsoptionen	1
Entdecken Sie Einsparungen durch Anpassung	1
Entdecken Sie die Einsparungen bei erkannten Speicherumgebungen	4
Implementieren von FSX für ONTAP-Dateisysteme	6
Verfolgen Sie die Kosten Ihrer Ressourcen in NetApp Workload Factory	6
Verwenden Sie Links	7
Erfahren Sie mehr über NetApp Workload Factory-Links	7
Stellen Sie über einen Lambda-Link eine Verbindung zu einem FSX für ONTAP-Dateisystem her	9
Verwalten von Workload Factory-Links	16
Cache-Volumes in Workload Factory entdecken	19
Volumes managen	20
Erstellen Sie ein FSx für ONTAP -Volume in Workload Factory	20
Zugriff auf Ihre FSX for ONTAP-Dateisystemdaten	26
Blockspeicherressourcen erstellen	27
Erstellen Sie eine Initiatorgruppe für ein Dateisystem in NetApp Workload Factory	27
Erstellen eines Blockgeräts für ein Dateisystem in NetApp Workload Factory	28
Erstellen Sie eine Storage-VM für ein FSX für ONTAP-Filesystem	30
Erstellen einer Storage-VM	30
Sichern Sie Ihre Daten	31
Arten der Datensicherung in NetApp Workload Factory	31
Verwenden von Snapshots	33
Verwenden Sie Backups im Objektspeicher	37
Verwenden der Replikation	39
Schützen Sie Ihre Daten mit NetApp Autonomous Ransomware Protection mit KI	43
Klonen eines Volumes in NetApp Workload Factory	47
Verwenden Sie lokale ONTAP Clusterdaten in NetApp Workload Factory	47
Schützen Sie Ihre Daten mit einem Cyber-Tresor	51

Verwenden Sie Amazon FSX für NetApp ONTAP

Entdecken Sie Einsparungen mit FSx für ONTAP in der NetApp Workload Factory

Erkunden Sie die Einsparmöglichkeiten bei Ihren Storage-Workloads, die Amazon Elastic Block Store (EBS), Elastic File System (EFS) und FSX für Windows File-Server gegen FSX für NetApp ONTAP verwenden.

NetApp Workload Factory enthält einen Speichereinsparungsrechner zum Vergleichen von Amazon-Speicherumgebungen mit FSx für ONTAP. Sie können mit oder ohne Angabe Ihrer AWS-Anmeldeinformationen Einsparungen ermitteln und die Konfigurationseinstellungen für Ihre Speicherumgebung anpassen. Wenn Sie AWS-Anmeldeinformationen angeben, können Sie beispielsweise eine oder mehrere Instanzen von Amazon Elastic Block Store auswählen und den Vergleich automatisch von Workload Factory durchführen lassen. Ob manuell oder automatisch, der Rechner ermittelt, welcher Speicherdiensst für Ihren Speicherbedarf die niedrigsten Kosten bietet.

Wenn der Speicherrechner ermittelt, dass FSx für ONTAP der kostengünstigste Speicher ist, können Sie FSx für 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.

Berechnungsoptionen

Für den Vergleich der Kosten zwischen Ihren Systemen und FSX for ONTAP stehen zwei Rechner-Optionen zur Verfügung – Anpassung und automatische Erkennung für Ihre Amazon Storage-Umgebungen.

Einsparungen durch Anpassung: Sie stellen die Konfigurationseinstellungen für eine Storage-Umgebung bereit, einschließlich Anwendungsfall, Region, Anzahl von Volumes oder File-Systemen, Storage-Menge, Snapshot-Häufigkeit, geänderter Menge pro Snapshot, bereitgestellter IOPS, Durchsatz und mehr.

Erkunden Sie die Einsparungen für erkannte Speicherumgebungen: Workload Factory stellt eine Verbindung zu Ihren vorhandenen AWS-Speicherumgebungen her und überträgt die Details zum automatischen Vergleich in den Rechner. Sie müssen Automatisierungsberechtigungen erteilen, um den automatischen Modus zu verwenden. Sie können den Anwendungsfall ändern, alle anderen Details werden jedoch automatisch in der Berechnung ermittelt.

Darüber hinaus können Sie ["AWS-Anmelde Daten hinzufügen"](#) die Genauigkeit der Rechenanalyse verbessern. Wählen Sie **Einsparungen basierend auf vorhandenen Ressourcen berechnen**. Sie werden zur Seite Anmeldeinformationen hinzufügen weitergeleitet. Nachdem Sie Anmelde Daten hinzugefügt haben, wählen Sie die vorhandenen Ressourcen aus, um sie mit FSX for ONTAP zu vergleichen, und wählen Sie **Einsparungen erkunden** aus.

Entdecken Sie Einsparungen durch Anpassung

Führen Sie die Schritte unter der Registerkarte für Ihre Speicherauswahl aus.

Amazon Elastic Block Store (EBS)

Schritte

1. Melden Sie sich mit einem der "[Konsolenerfahrungen](#)" an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Menü „Speicher“ die Option „Einsparungen entdecken“ und anschließend die Registerkarte „Amazon Elastic Block Store (EBS)“.
4. Geben Sie im Rechner für Storage-Einsparungen folgende Informationen an:
 - a. **Anwendungsfall:** Erforderlich. Wählen Sie im Dropdown-Menü einen Anwendungsfall aus. Der ausgewählte Anwendungsfall legt die Eigenschaften des Filesystems FSX für ONTAP für den Vergleich fest.
 - b. **Region:** Optional. Wählen Sie im Dropdown-Menü die Region für Ihre EBS-Konfiguration aus.
 - c. **Wählen Sie EBS Volume-Typ:** Optional. Wählen Sie den EBS Volume-Typ aus, der für Ihre Konfiguration verwendet wird.
 - d. **Anzahl der Volumen:** Optional. Geben Sie die Anzahl der Volumes in Ihrer EBS-Konfiguration ein.
 - e. **Speichermenge pro Volumen (tib):** Optional. Geben Sie die Storage-Menge pro Volume in tib ein.
 - f. **Snapshot-Frequenz:** Optional. Wählen Sie die Snapshot-Frequenz für Ihre EBS-Konfiguration aus.
 - g. **Betrag pro Snapshot geändert (gib):** Optional. Nur für Snapshot-Speicher. Geben Sie den pro Snapshot geänderten Betrag in gib ein.
 - h. **Bereitgestellte IOPS pro Volume:** Optional. Für gp3-, io1- und io2-Volumen. Geben Sie die bereitgestellten IOPS pro Volume ein.
 - i. **Durchsatz (MiB/s):** Optional. Nur für gp3-Volumes. Geben Sie den Durchsatz in MiB/s pro Volume ein.

Amazon FSX für Windows File Server

Schritte

1. Melden Sie sich mit einem der "[Konsolenerfahrungen](#)" an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Menü „Speicher“ die Option „Einsparungen entdecken“ und anschließend die Registerkarte „Amazon Elastic Block Store (EBS)“.
4. Geben Sie im Rechner für Storage-Einsparungen folgende Informationen an:
 - a. **Anwendungsfall:** Erforderlich. Wählen Sie im Dropdown-Menü einen Anwendungsfall aus. Der ausgewählte Anwendungsfall legt die Eigenschaften des Filesystems FSX für ONTAP für den Vergleich fest.
 - b. **Region:** Optional. Wählen Sie im Dropdown-Menü die Region für Ihre FSX for Windows File Server-Konfiguration aus.
 - c. **Deployment-Typ:** Optional. Wählen Sie **einzelne Verfügbarkeitszone** oder **mehrere Verfügbarkeitszonen**.
 - d. **Speichertyp:** Der SSD-Speichertyp ist standardmäßig ausgewählt.

- e. **Speicherkapazität (tib)**: Optional. Geben Sie die Speicherkapazität für die Konfiguration ein.
- f. **Deduplizierungseinsparungen (%)**: Optional. Geben Sie den Prozentsatz der zu erwartenden Kapazitätseinsparungen durch die Deduplizierung ein.
- g. **Snapshot-Frequenz**: Optional. Wählen Sie die Snapshot-Frequenz für Ihre Konfiguration aus.
- h. **Betrag pro Snapshot geändert (gib)**: Optional. Nur für Snapshot-Speicher. Geben Sie den pro Snapshot geänderten Betrag in gib ein.
- i. **Bereitgestellte SSD-IOPS**: Optional. Geben Sie die bereitgestellten SSD-IOPS ein.
- j. **Durchsatz (MiB/s)**: Optional. Geben Sie den Durchsatz in MiB/s. ein

Amazon Elastic File System (EFS)

Schritte

1. Melden Sie sich mit einem der "[Konsolenerfahrungen](#)" an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Menü „Speicher“ die Option „Einsparungen entdecken“ und anschließend die Registerkarte „Amazon Elastic Block Store (EBS)“.
4. Geben Sie im Rechner für Storage-Einsparungen folgende Informationen an:
 - a. **Anwendungsfall**: Erforderlich. Wählen Sie im Dropdown-Menü einen Anwendungsfall aus. Der ausgewählte Anwendungsfall legt die Eigenschaften des Filesystems FSX für ONTAP für den Vergleich fest.
 - b. **Region**: Optional. Wählen Sie im Dropdown-Menü die Region für Ihre FSX for Windows File Server-Konfiguration aus.
 - c. **Dateisystemtyp**: Optional. Wählen Sie **Regional** oder **One Zone**.
 - d. **Speicherkapazität (tib)**: Optional. Geben Sie die Speicherkapazität der EFS-Konfiguration ein.
 - e. **Daten, auf die häufig zugegriffen wird (%)**: Optional. Geben Sie den Prozentsatz der Daten ein, auf die häufig zugegriffen wird.
 - f. **Durchsatzmodus**: Optional. Wählen Sie **bereitgestellter Durchsatz** oder **Elastischer Durchsatz**.
 - g. **Durchsatz (MiB/s)**: Optional. Geben Sie den Durchsatz in MiB/s. ein

Nachdem Sie Details zur Konfiguration des Speichersystems angegeben haben, überprüfen Sie die Berechnungen und Empfehlungen auf der Seite.

Scrollen Sie außerdem nach unten zum Ende der Seite, um den Bericht anzuzeigen, indem Sie eine der folgenden Optionen auswählen:

- **PDF exportieren**
- **Per E-Mail senden**
- **Die Berechnungen anzeigen**

Um zu FSX für ONTAP zu wechseln, folgen Sie den Anweisungen zu [Implementieren von FSX für ONTAP-Dateisysteme](#).

Entdecken Sie die Einsparungen bei erkannten Speicherumgebungen

Bevor Sie beginnen

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



Diese Rechneroption unterstützt keine Berechnungen für EBS-Snapshots und FSx für Windows File Server-Schattenkopien. Wenn Sie die Einsparungen durch die Anpassung untersuchen, können Sie Snapshot-Details zu EBS und FSx für Windows File Server anbieten.

Führen Sie die Schritte unter der Registerkarte für Ihre Speicherauswahl aus.

Amazon Elastic Block Store (EBS)

Schritte

1. Melden Sie sich mit einem der ["Konsolenerfahrungen"](#) an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Menü „Speicher“ die Option „Einsparungen entdecken“ und anschließend die Registerkarte „Amazon Elastic Block Store (EBS)“.
4. Wählen Sie auf der Registerkarte **Elastic Block Store (EBS)** die Instanz(en) aus, die Sie mit FSX for ONTAP vergleichen möchten, und wählen Sie **Einsparungen erkunden** aus.
5. Der Rechner für Storage-Einsparungen wird angezeigt. Die folgenden Merkmale des Speichersystems werden basierend auf den 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. **Gesamtspeichermenge (tib):** Die Speichermenge pro Volume in tib
 - d. **Insgesamt bereitgestellte IOPS:** Für gp3-, io1- und io2-Volumes
 - e. **Gesamtdurchsatz (MiB/s):** Nur für gp3-Volumes

Amazon FSX für Windows File Server

Schritte

1. Melden Sie sich mit einem der ["Konsolenerfahrungen"](#) an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Menü „Speicher“ die Option „Einsparungen entdecken“ und anschließend die Registerkarte „Amazon FSx für Windows-Dateiserver“.
4. Wählen Sie auf der Registerkarte **Amazon FSX für Windows-Dateiserver** die Instanz(en) aus, die mit FSX für ONTAP verglichen werden soll, und wählen Sie **Einsparungen erkunden**.
5. Der Rechner für Storage-Einsparungen wird angezeigt. Die folgenden Merkmale des Speichersystems werden basierend auf dem Bereitstellungstyp der ausgewählten Instanz(en) vorausgefüllt:
 - a. **Anwendungsfall:** Der Anwendungsfall für Ihre Konfiguration. Sie können den Anwendungsfall bei Bedarf ändern.
 - b. **Ausgewählte Dateisysteme**
 - c. **Gesamtspeichermenge (tib)**
 - d. **Bereitgestellte SSD-IOPS**
 - e. **Durchsatz (MiB/s)**

Amazon Elastic File System (EFS)

Schritte

1. Melden Sie sich mit einem der ["Konsolenerfahrungen"](#) an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Menü „Speicher“ die Option „Einsparungen erkunden“ und anschließend die

Registerkarte „Amazon Elastic File System (EFS)“.

4. Wählen Sie auf der Registerkarte * Elastic File System (EFS)* die Instanz(en) aus, die mit FSX for ONTAP verglichen werden sollen, und wählen Sie **Einsparungen erkunden**.
5. Der Rechner für Storage-Einsparungen wird angezeigt. Die folgenden Merkmale des Speichersystems werden basierend auf den ausgewählten Instanzen vorausgefüllt:
 - a. **Anwendungsfall:** Der Anwendungsfall für Ihre Konfiguration. Sie können den Anwendungsfall bei Bedarf ändern.
 - b. **Gesamte Dateisysteme**
 - c. **Gesamtspeichermenge (tib)**
 - d. **Gesamtbereitgestellter Durchsatz (MiB/s)**
 - e. **Gesamtelastischer Durchsatz - Lesen (gib)**
 - f. **Gesamtelastischer Durchsatz – Schreiben (gib)**

Nachdem Sie Details zur Konfiguration des Speichersystems angegeben haben, überprüfen Sie die Berechnungen und Empfehlungen auf der Seite.

Scrollen Sie außerdem nach unten zum Ende der Seite, um den Bericht anzuzeigen, indem Sie eine der folgenden Optionen auswählen:

- **PDF exportieren**
- **Per E-Mail senden**
- **Die Berechnungen anzeigen**

Implementieren von FSX für ONTAP-Dateisysteme

Wenn Sie zu FSX für ONTAP wechseln möchten, um Kosteneinsparungen zu erzielen, wählen Sie **Erstellen**, um das Dateisystem direkt aus dem Assistenten zum Erstellen eines FSX für ONTAP-Dateisystems zu erstellen, oder wählen Sie **Speichern**, um die empfohlenen Konfigurationen für später zu speichern.

Bereitstellungsmethoden

Im *Automate*-Modus können Sie das FSx for ONTAP -Dateisystem direkt von Workload Factory aus bereitstellen. Sie können den Inhalt auch aus dem Codebox-Fenster kopieren und das System mit einer der Codebox-Methoden bereitstellen.

Im *BAS/C*-Modus können Sie den Inhalt aus dem Codebox-Fenster kopieren und das Dateisystem FSX for ONTAP mit einer der Codebox-Methoden bereitstellen.

Verfolgen Sie die Kosten Ihrer Ressourcen in NetApp Workload Factory.

Mit NetApp Workload Factory können Sie die Kosten und die Nutzung des FSx for ONTAP -Dateisystems in einer konsolidierten Ansicht verfolgen. Die Kostendaten helfen Ihnen, Budgets zu verwalten und Ressourcen effektiv zu optimieren. AWS Cost Explorer liefert die Kostendaten.

Über diese Aufgabe

Kosten- und Nutzungsdaten für Ihre FSx for ONTAP -Dateisystemressourcen werden mit den folgenden

Berechtigungen aus dem AWS Cost Explorer extrahiert:

- ce:GetCostAndUsage
- ce:GetTags

Bevor Sie beginnen

"[Erteilen Sie Anmeldeinformationen mit der Berechtigungsrichtlinie „Ansicht, Planung und Analyse“.](#)" in Workload Factory, um FSx für ONTAP Kosten zu verfolgen.

Schritte

1. Melden Sie sich mit einem der ["Konsolenerfahrungen"](#) an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Im Menü „Speicher“ wählen Sie **Kosten**.
4. Filtern Sie auf der Kostenseite die Kosten- und Kapazitätsdaten für Ihre FSx for ONTAP -Ressourcen, indem Sie Folgendes angeben:
 - a. **AWS-Konten:** Wählen Sie die Konten aus, für die Sie die Kostendaten anzeigen möchten.
 - b. **Anmeldeinformationen:** Wählen Sie Anmeldeinformationen mit den Berechtigungen *Anzeigen, Planen und Analysieren* aus.
 - c. **Regionen:** Wählen Sie die AWS-Regionen aus, für die Sie Kostendaten anzeigen möchten.
 - d. **Kostendatenbereich:** Wählen Sie den Zeitraum aus, in dem die Kostendaten angezeigt werden sollen.
5. Sehen Sie sich die **Kostendetails** für Ihre FSx for ONTAP -Ressourcen an.

Verwenden Sie Links

Erfahren Sie mehr über NetApp Workload Factory-Links

Ein NetApp Workload Factory-Link erstellt eine Vertrauensbeziehung und Konnektivität zwischen einem Workload Factory-Konto und einem oder mehreren FSx for ONTAP -Dateisystemen. Auf diese Weise können Sie bestimmte Dateisystemfunktionen direkt über die ONTAP REST-API-Aufrufe überwachen und verwalten, die über die Amazon FSx for ONTAP -API nicht verfügbar sind.

Sie benötigen keinen Link, um mit Workload Factory zu beginnen, 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 von Vorteil, da sie es Workload Factory ermöglichen, Vorgänge auszuführen, die über die Amazon FSx for ONTAP -API nicht nativ verfügbar sind. Links ermöglichen erweiterte ONTAP Funktionen und -Automatisierungen, die die Verwaltung von FSx für ONTAP Dateisysteme verbessern.

Hier sind einige Vorteile der Verwendung von Links:

- Über die Verknüpfung kann die NetApp Konsole ONTAP -Befehle direkt an Ihr FSx für ONTAP Dateisystem senden und so erweiterte ONTAP Funktionen bereitstellen, die über das hinausgehen, was AWS nativ bietet.

- Links nutzen AWS Lambda, um Code als Reaktion auf Ereignisse auszuführen. Dieser serverlose Ansatz beseitigt die Abhängigkeit von einer in Ihrer VPC ausgeführten Instanz.

Wie Links funktionieren

Links nutzen AWS Lambda Lambda führt Code als Reaktion auf Ereignisse aus und verwaltet automatisch die für diesen Code erforderlichen Rechenressourcen. Die von Ihnen erstellten Links sind Teil Ihres NetApp Kontos und mit einem AWS Konto verknüpft.

Nachdem Sie einen Link erstellt haben, können Sie ihn mit einem oder mehreren FSx for ONTAP -Dateisystemen verknüpfen. Jedes Dateisystem kann nur einem Link im selben NetApp-Konto zugeordnet werden. Wenn Sie mehrere NetApp-Konten haben, kann ein einziges Dateisystem mit zusätzlichen Links unter verschiedenen NetApp-Konten verknüpft werden.

Sie erstellen und verknüpfen Links aus der Speicherarbeitslast in Workload Factory.

Sie können Links mithilfe von Anmeldeinformationen authentifizieren, die im Anmeldeinformationsdienst von Workload Factory gespeichert sind, oder mithilfe Ihrer Anmeldeinformationen, die im AWS Secrets Manager gespeichert sind. Die Workload Factory unterstützt keine Änderung des Authentifizierungsmodus.

Kosten

Für jede von Lambda durchgeführte Transaktion fallen Gebühren an. Da Lambda als Proxy zwischen den beiden Systemen fungiert, fallen Gebühren an, wenn Lambda eine Anfrage an die ONTAP REST API auf einem Dateisystem sendet und wenn es die Antwort zurück an Workload Factory sendet.

["Informieren Sie sich über die Kosten bei der Nutzung von AWS Lambda"](#)

Wenn ein Link erforderlich ist

Workload Factory benötigt einen Link, um bestimmte Informationen anzuzeigen und bestimmte Aufgaben auszuführen. Wenn Sie versuchen, einen Vorgang auszuführen, der einen Link erfordert, und Sie keinen Link mit dem FSx for ONTAP Dateisystem verknüpft haben, benachrichtigt Sie Workload Factory, dass für den Vorgang ein Link erforderlich ist.

Zu den Funktionen, für die ein Link erforderlich ist, gehören:

- Gut strukturierter Status der FSx for ONTAP Dateisystemkonfigurationen für proaktive Wartung, Zuverlässigkeit und Kosten-Leistungs-Optimierung
- ONTAP EMS Ereignisüberwachung und Alarmierung
- Autonomer Ransomware-Schutz (ARP/AI) von NetApp
- Verbesserte ganzheitliche Kapazitätsbeobachtung über FSx für ONTAP Dateisysteme
- Datenreplikation, Verwaltung und Überwachung von Volume- und Storage-VMs
- Bereitstellung und Verwaltung von SMB/CIFS-Freigaben und NFS-Exportrichtlinien
- Verwaltung von iSCSI-Volumes auf einem FSX für ONTAP-Dateisystem
- Erstellen und Verwalten von Snapshot-Richtlinien für benutzerdefinierte Schutz-SLAs
- Verbesserungen der Inode-Verwaltung für automatisches Kapazitätsmanagement
- Automatisches Volumenwachstum für elastische Skalierung
- Erstellen und Verwalten von Klonen für sofortiges, direktes Klonen von Daten

- Anzeige zusätzlicher Metriken direkt aus ONTAP, wie z. B. die ONTAP Version

Erfahren Sie, wie man "["Verbinden Sie einen Link mit einem FSx für ONTAP Dateisystem"](#)".

Stellen Sie über einen Lambda-Link eine Verbindung zu einem FSx für ONTAP-Dateisystem her

Um erweiterte ONTAP Verwaltungsvorgänge durchzuführen, richten Sie eine Verbindung zwischen Ihrem Workload Factory-Konto und einem oder mehreren FSx for ONTAP-Dateisystemen ein. Dabei werden neue und bestehende Lambda-Links verknüpft und die Links authentifiziert. Mithilfe der Link-Zuordnung können Sie bestimmte Funktionen direkt vom FSx for ONTAP-Dateisystem aus überwachen und verwalten, 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 nach diesem Code erforderlichen Computing-Ressourcen automatisch zu managen. Die von Ihnen erstellten Links sind Teil Ihres NetApp Kontos und mit einem AWS Konto verknüpft.

Sie können in Ihrem Konto einen Link erstellen, wenn Sie ein FSx für ONTAP Dateisystem definieren. Der Link wird für dieses Dateisystem verwendet und kann für andere FSx for ONTAP Dateisysteme verwendet werden. Sie können auch später einen Link für ein Dateisystem zuordnen.

Für Links ist eine Authentifizierung erforderlich. Sie können Links mithilfe von Anmeldeinformationen authentifizieren, die im Anmeldeinformationsdienst von Workload Factory gespeichert sind, oder mithilfe Ihrer Anmeldeinformationen, die im AWS Secrets Manager gespeichert sind. Pro Link wird nur eine Authentifizierungsmethode unterstützt. Wenn Sie beispielsweise die Link-Authentifizierung mit AWS Secrets Manager auswählen, können Sie die Authentifizierungsmethode später nicht mehr ändern.



AWS Secrets Manager wird bei Verwendung eines Konsolenagenten nicht unterstützt.

Neuen Link zuordnen

Die Verknüpfung eines neuen Links umfasst die Erstellung und Verknüpfung.

Sie haben in diesem Workflow zwei Möglichkeiten, Links zu erstellen – automatisch oder manuell. Sie müssen einen AWS CloudFormation-Stack in Ihrem AWS-Konto starten, um den Link zu erstellen.

- Automatisch: Erstellt einen Link mit automatischer Registrierung über Workload Factory. Ein automatisch erstellter Link erfordert Token für die Workload Factory-Automatisierung und der CloudFormation-Code ist kurzlebig. Die Nutzungsdauer beträgt maximal sechs Stunden.
- Manuell: Erstellt einen Link mit manueller Registrierung mithilfe von CloudFormation oder Terraform aus der Codebox. Der Code bleibt bestehen und gibt Ihnen mehr Zeit, den Vorgang abzuschließen. Dies ist nützlich, wenn Sie mit verschiedenen Teams wie Security und DevOps arbeiten, die möglicherweise zuerst die erforderlichen Berechtigungen erteilen müssen, um die Linkerstellung abzuschließen.

Bevor Sie beginnen

- Sie sollten überlegen, welche Link-Erstelloption Sie verwenden.
- Sie benötigen mindestens ein FSx for ONTAP Dateisystem in Workload Factory. Um FSx for ONTAP

Dateisysteme zu erkennen, benötigen Sie ein AWS-Konto mit Berechtigungen für FSx for ONTAP Instanzen und "[Anmeldeinformationen in Workload Factory hinzufügen](#)" mit den Berechtigungen *view, planning, and analysis* für die Speicherverwaltung.

- Die folgenden Ports müssen in der mit dem FSx for ONTAP-Dateisystem verknüpften Sicherheitsgruppe für die Link-Konnektivität geöffnet sein.
 - Für die Workload Factory-Konsole: Port 443 (HTTPS)
 - Für die Ereignisanalyse des Notfallmanagementsystems (EMS) mit CloudShell und FSx für ONTAP : 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 müssen über die folgenden Berechtigungen in Ihrem AWS-Konto verfügen, wenn Sie einen Link mit einem CloudFormation-Stack hinzufügen:

```
"cloudformation:GetTemplateSummary",
"cloudformation>CreateStack",
"cloudformation>DeleteStack",
"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>PassRole",
"iam>PutRolePolicy",
"iam>DeleteRole",
"iam>AttachRolePolicy",
"lambda>AddPermission",
"lambda>RemovePermission",
"lambda>InvokeFunction",
"lambda>GetFunction",
"lambda>CreateFunction",
"lambda>DeleteFunction",
"lambda>TagResource",
"codestar-connections>GetSyncConfiguration",
"ecr>BatchGetImage",
"ecr>GetDownloadUrlForLayer"
```

Automatisch erstellen

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

Schritte

1. Melden Sie sich mit einem der ["Konsolenerfahrungen"](#) an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Speichermenü **FSx für ONTAP** aus.
4. Wählen Sie in **FSx for ONTAP** das Aktionsmenü des Dateisystems aus, dem Sie einen Link zuordnen möchten, und wählen Sie dann **Link zuordnen**.
5. Wählen Sie im Dialogfeld „Verknüpfung zuordnen“ die Option **Neuen Link erstellen** und wählen Sie **Weiter**.
6. Geben Sie auf der Seite „Link erstellen“ Folgendes an:
 - 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 Workload Factory, FSx für ONTAP -Zugriffsdaten von Ihrem AWS Secrets Manager abzurufen.

Der Link-Bereitstellungsstapel fügt der Lambda-Berechtigungsrichtlinie automatisch den folgenden standardmäßigen ARN-Regex des geheimen Managers hinzu:

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

Sie können entweder Geheimnisse im Einklang mit den Standardberechtigungen erstellen oder Ihre benutzerdefinierten Berechtigungen für die Link-Richtlinie zuweisen.

Konfigurieren des privaten VPC-Endpunkts zu AWS Secrets Manager ist standardmäßig deaktiviert. Bei Auswahl dieser Option wird das Secret über den privaten VPC-Endpunkt gespeichert, anstatt es lokal zu speichern.

- a. **Linkberechtigungen:** Wählen Sie eine der folgenden Optionen für Linkberechtigungen:
 - **Automatisch:** Wählen Sie diese Option, damit der AWS CloudFormation-Code automatisch die Lambda-Berechtigungsrichtlinie und Ausführungsrolle erstellt.
 - **Vom Benutzer bereitgestellt:** Wählen Sie diese Option, um dem Lambda-Link eine bestimmte Lambda-Ausführungsrolle und die zugehörigen Richtlinien zuzuweisen. Für die Lambda-Berechtigungsrichtlinie sind die folgenden Berechtigungen erforderlich. Die `secretsmanager:GetSecretValue` Die Berechtigung ist nur erforderlich, wenn Sie AWS Secrets Manager aktiviert haben.

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

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

- b. **Tags:** Fügen Sie optional alle Tags hinzu, die Sie mit diesem Link verknüpfen möchten, damit Sie Ihre Ressourcen einfacher kategorisieren können. Sie könnten beispielsweise ein Tag hinzufügen, das diesen Link als von FSX für ONTAP-Dateisystemen verwendet identifiziert.

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

7. Wählen Sie **Erstellen**.

Das Dialogfeld „Zu CloudFormation umleiten“ wird angezeigt und erläutert, wie der Link vom AWS CloudFormation-Dienst erstellt wird.

8. Wählen Sie **Weiter**, um die AWS-Verwaltungskonsole zu öffnen, und melden Sie sich dann beim AWS-Konto für dieses FSX for ONTAP-Dateisystem an.
9. Wählen Sie auf der Seite „schneller Stapel erstellen“ unter „Funktionen“ **Ich bestätige, dass AWS CloudFormation IAM-Ressourcen erstellen könnte**.

Beachten Sie, dass Lambda drei Berechtigungen erteilt werden, wenn Sie die CloudFormation-Vorlage starten. Workload Factory verwendet diese Berechtigungen bei der Verwendung von Links.

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

10. Wählen Sie **Stapel erstellen** und dann **Weiter**.

Sie können den Status der Linkerstellung auf der Seite „Ereignisse“ überwachen. Dies sollte nicht länger als 5 Minuten dauern.

11. Kehren Sie zur Workload Factory-Schnittstelle zurück und Sie werden sehen, dass der Link mit dem FSx for ONTAP -Dateisystem verknüpft ist.

Manuell erstellen

Sie können eine Verknüpfung mit zwei Infrastructure-as-Code (IaC)-Tools aus der Codebox erstellen: CloudFormation oder Terraform. Mit dieser Option extrahieren Sie die ARN für den Link aus AWS CloudFormation und melden sie hier. Workload Factory registriert den Link manuell für Sie.

Schritte

1. Melden Sie sich mit einem der ["Konsolenerfahrungen"](#) an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Speichermenü **FSx für ONTAP** aus.
4. Wählen Sie unter **FSx for ONTAP** das Aktionsmenü des Dateisystems aus, dem Sie einen Link zuordnen möchten, und wählen Sie dann **Link zuordnen**.
5. Wählen Sie im Dialogfeld „Verknüpfung zuordnen“ die Option **Neuen Link erstellen** und wählen Sie **Weiter**.
6. Wählen Sie auf der Seite „Link erstellen“ CloudFormation oder Terraform aus der Codebox aus und geben Sie dann Folgendes ein:

- Linkname:** Geben Sie den Namen ein, den Sie für diesen Link verwenden möchten. Der Name muss innerhalb Ihres Kontos eindeutig sein.
- AWS Secrets Manager:** Optional. Ermöglicht Workload Factory, FSx für ONTAP -Zugriffsdaten von Ihrem AWS Secrets Manager abzurufen.

Der Link-Bereitstellungsstapel fügt der Lambda-Berechtigungsrichtlinie automatisch den folgenden standardmäßigen ARN-Regex des geheimen Managers hinzu:

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

Sie können entweder Geheimnisse im Einklang mit den Standardberechtigungen erstellen oder Ihre benutzerdefinierten Berechtigungen für die Link-Richtlinie zuweisen.

Konfigurieren des privaten VPC-Endpunkts zu AWS Secrets Manager ist standardmäßig deaktiviert. Bei Auswahl dieser Option wird das Secret über den privaten VPC-Endpunkt gespeichert, anstatt es lokal zu speichern.

- Linkberechtigungen:** Wählen Sie eine der folgenden Optionen für Linkberechtigungen:
 - Automatisch:** Wählen Sie diese Option, damit der AWS CloudFormation-Code automatisch die Lambda-Berechtigungsrichtlinie und Ausführungsrolle erstellt.
 - Vom Benutzer bereitgestellt:** Wählen Sie diese Option, um dem Lambda-Link eine bestimmte Lambda-Ausführungsrolle und die zugehörigen Richtlinien zuzuweisen. Für die Lambda-Berechtigungsrichtlinie sind die folgenden Berechtigungen erforderlich. Die `secretsmanager:GetSecretValue` Die Berechtigung ist nur erforderlich, wenn Sie AWS Secrets Manager aktiviert haben.

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

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

- Tags:** Fügen Sie optional alle Tags hinzu, die Sie mit diesem Link verknüpfen möchten, damit Sie Ihre Ressourcen einfacher kategorisieren können. Sie könnten beispielsweise ein Tag hinzufügen, das diesen Link als von FSX für ONTAP-Dateisystemen verwendet identifiziert.
- Linkregistrierung:** Wählen Sie CloudFormation oder Terraform für die Anweisungen zur Registrierung des Links aus und folgen Sie den Anweisungen.

Beachten Sie, dass Lambda drei Berechtigungen erteilt werden, wenn Sie die CloudFormation-Vorlage starten. Workload Factory verwendet diese Berechtigungen bei der Verwendung von Links.

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

+ Nachdem Sie den Stapel erfolgreich erstellt haben, fügen Sie die Lambda-ARN in das Textfeld ein.

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

7. Wählen Sie **Erstellen**.

Sie können den Status der Linkerstellung auf der Seite „Ereignisse“ überwachen. Dies sollte nicht länger als 5 Minuten dauern.

8. Kehren Sie zur Workload Factory-Schnittstelle zurück und Sie werden sehen, dass der Link mit dem FSx for ONTAP -Dateisystem verknüpft ist.

Ergebnis

Workload Factory verknüpft den Link mit dem FSx for ONTAP Dateisystem. Sie können erweiterte ONTAP -Operationen durchführen.

Verknüpfen Sie einen vorhandenen Link mit einem FSX for ONTAP-Dateisystem

Nachdem Sie einen Link erstellt haben, verknüpfen Sie ihn mit einem oder mehreren FSX for ONTAP- Dateisystemen.

Schritte

1. Melden Sie sich mit einem der ["Konsolenerfahrungen"](#) an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Speichermenü **FSx für ONTAP** aus.
4. Wählen Sie in **FSx für ONTAP** das Aktionsmenü des Dateisystems aus, dem Sie einen Link zuordnen möchten, und wählen Sie dann **Link zuordnen**.
5. Wählen Sie auf der Link-Seite „Mitarbeiter“ die Option **vorhandenen Link verknüpfen**, wählen Sie den Link aus und wählen Sie **Weiter**.
6. Wählen Sie den Authentifizierungsmodus aus.
 - Workload Factory: Geben Sie das Passwort zweimal ein.
 - AWS Secrets Manager: Geben Sie den geheimen ARN ein.

Stellen Sie sicher, dass die geheime ARN die folgenden gültigen Schlüsselpaare enthält, wobei die *filesystemID* optional ist.

- Dateisystem-ID = FSx_Dateisystem-ID (optional)
- Benutzer = FSx_Benutzer
- Passwort = user_password



Für die Authentifizierung mit AWS Secrets Manager ist ein Benutzer erforderlich, entweder der von Ihnen angegebene *FSx_user* oder ein anderer Benutzer, der auf dem FSx for ONTAP Dateisystem erstellt wurde. Der Standardbenutzer ist *fsxadmin* wenn Sie keinen Benutzer angeben.

7. Wählen Sie **Anwenden**.

Ergebnis

Der Link ist mit dem Dateisystem FSX für ONTAP verknüpft. Sie können erweiterte ONTAP-Vorgänge ausführen.

Fehlerbehebung bei Problemen mit der AWS Secrets Manager-Link-Authentifizierung

Problem

Der Link verfügt nicht über die erforderlichen Berechtigungen zum Abrufen des Geheimnisses.

Auflösung: Berechtigungen hinzufügen, nachdem der Link aktiv ist. Melden Sie sich bei der AWS-Konsole an, suchen Sie den Lambda-Link und bearbeiten Sie die angehängte Berechtigungsrichtlinie.

Problem

Das Geheimnis wurde nicht gefunden.

Auflösung: Geben Sie das korrekte Geheimnis ARN.

Problem

Das Geheimnis liegt nicht im richtigen Format vor.

Auflösung: Gehen Sie zu AWS Secrets Manager und bearbeiten Sie das Format.

Das Secret sollte die folgenden Schlüssel-gültigen Paare enthalten:

- FilesystemID = FSX_Filesystem_id
- Benutzername = FSx_user
- Passwort = user_password

Problem

Der Schlüssel enthält keine gültigen ONTAP-Anmeldeinformationen für die Dateisystemauthentifizierung.

- **Auflösung*:** Geben Sie Anmeldeinformationen an, die FSX für ONTAP-Dateisysteme im AWS Secrets Manager authentifizieren können.

Verwalten von Workload Factory-Links

Verwalten Sie Links, die Sie mit Ihrem Workload Factory-Konto verknüpft haben. Sie können Links anzeigen, die mit einem FSx for ONTAP -Dateisystem verknüpft sind, Kennwörter für die Link-Authentifizierung angeben und Links aus der Workload Factory-Konsole entfernen.

["Weitere Informationen zu Links"](#) Oder ["Erstellen und Zuordnen eines Links"](#).

Zeigen Sie die mit Ihrem Konto verknüpften Links an

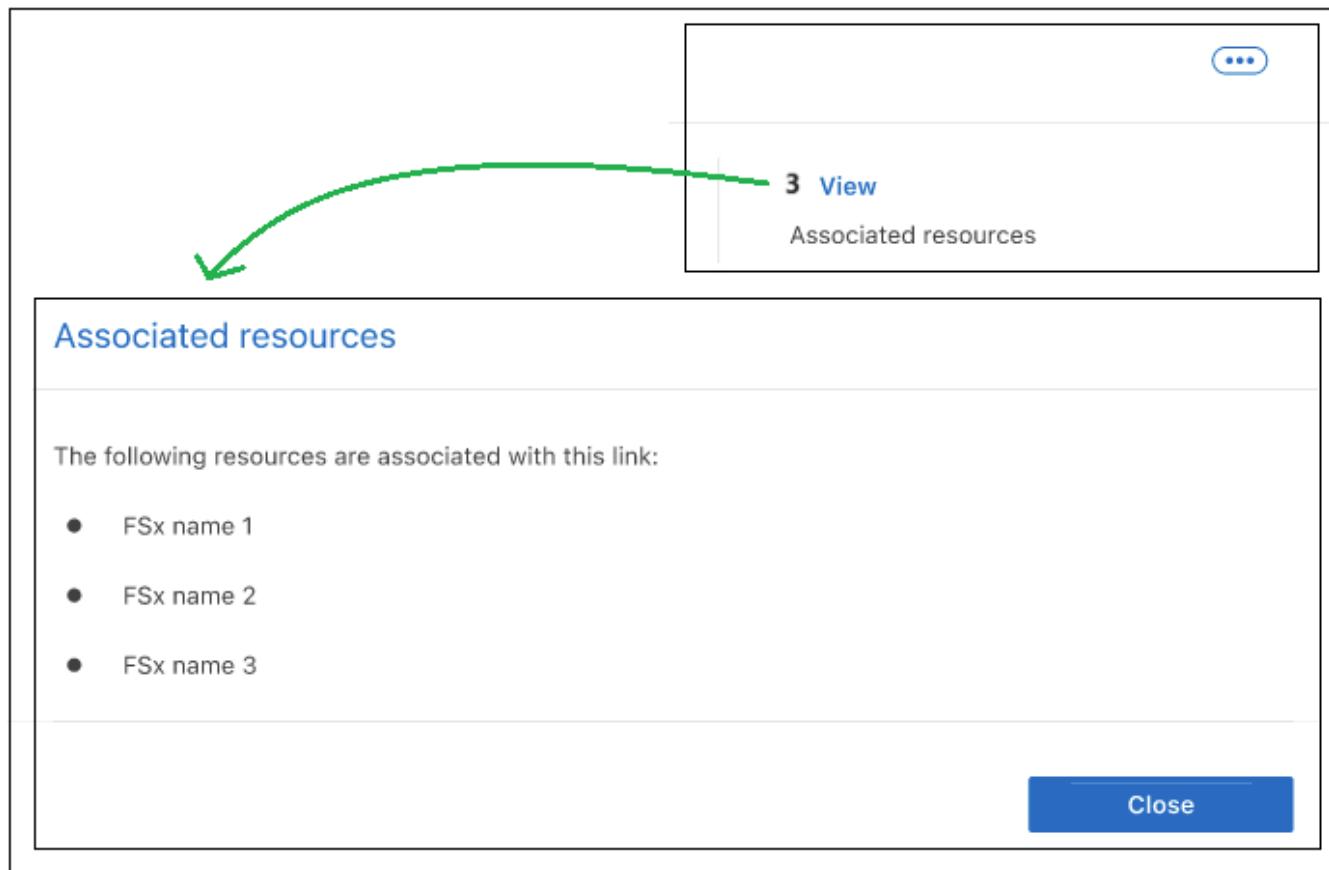
Sie können die Links anzeigen, die derzeit mit Ihrem Konto verknüpft sind.

Schritte

1. Melden Sie sich mit einem der ["Konsolenerfahrungen"](#) an.
2. Wählen Sie im Speichermenü **Verwaltung** und dann **Links**.

Vorhandene Links werden auf der Seite „Links“ angezeigt.

3. Um die FSx für ONTAP-Dateisysteme anzuzeigen, die mit einem Link verknüpft sind, wählen Sie die Schaltfläche **Ansicht** im Abschnitt „zugewiesene Ressourcen“ aus.



4. Wenn Sie den Amazon Resource Name (ARN) für den Link benötigen, können Sie neben dem ARN-Feld das *copy*-Symbol auswählen.

Bearbeiten Sie einen Link

Sie können einen Link nicht über die Workload Factory-Schnittstelle bearbeiten. Wenn Sie eine Änderung an einem Link vornehmen müssen, müssen Sie einen neuen Link erstellen und diesen Link dann Ihrem Dateisystem zuordnen.



Sie können die Lambda-Netzwerkkonfiguration (z. B. VPC, Subnetze und Sicherheitsgruppen) über die AWS Konsole bearbeiten. Die Änderungen werden dann in der UI für das Linkmanagement übernommen. Diese Änderungen können jedoch zu Verbindungsproblemen zwischen Lambda und ONTAP führen und werden nicht empfohlen.

Authentifizieren Sie einen Link

Geben Sie ein Administratorkennwort für Workload Factory-Anmeldeinformationen oder eine geheime ARN von AWS Secrets Manager ein, um die Verbindung mit einem FSx for ONTAP Dateisystem herzustellen.

AWS Secrets Manager wird bei Verwendung eines Konsolenagenten nicht unterstützt.



Pro Link wird nur eine Authentifizierungsmethode unterstützt. Wenn Sie beispielsweise die Verbindungsauthentifizierung mit AWS Secrets Manager auswählen, können Sie die Authentifizierungsmethode später nicht mehr ändern.

Schritte

1. Melden Sie sich mit einem der "Konsolenerfahrungen" an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Speichermenü **FSx für ONTAP** aus.
4. Wählen Sie in **FSx for ONTAP** das Aktionsmenü des Dateisystems aus, dem Sie einen Link zuordnen möchten, und wählen Sie dann **Verwalten**.
5. Wählen Sie in der Dateisystemübersicht **Authenticate the Link** aus.
6. Wählen Sie auf der Seite „Authentifizieren“ einen Authentifizierungsmodus aus:
 - Workload Factory: Geben Sie das Passwort zweimal ein.
 - AWS Secrets Manager: Geben Sie den geheimen ARN ein.
7. Wählen Sie **Anwenden**.

Ergebnis

Der Link ist authentifiziert, und Sie können erweiterte ONTAP-Vorgänge durchführen

Aktualisieren Sie das Passwort für die Link-Authentifizierung

Wenn das Administratorkennwort ungültig ist, aktualisieren Sie das Kennwort, um den Link mit dem Dateisystem FSX für ONTAP zu verbinden.

Schritte

1. Melden Sie sich mit einem der "Konsolenerfahrungen" an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Speichermenü **FSx für ONTAP** aus.
4. Wählen Sie in **FSx for ONTAP** das Aktionsmenü des Dateisystems aus, dem Sie einen Link zuordnen möchten, und wählen Sie dann **Verwalten**.
5. Wählen Sie in der Dateisystemübersicht **Passwort aktualisieren**.
6. Geben Sie auf der Seite Authentifizierungs-Link das neue Passwort zweimal ein.
7. Wählen Sie **Anwenden**.

Ergebnis

Das Passwort wird aktualisiert, und der Link ist jetzt mit dem Dateisystem FSX für ONTAP verbunden.

Entfernen Sie eine Verknüpfung

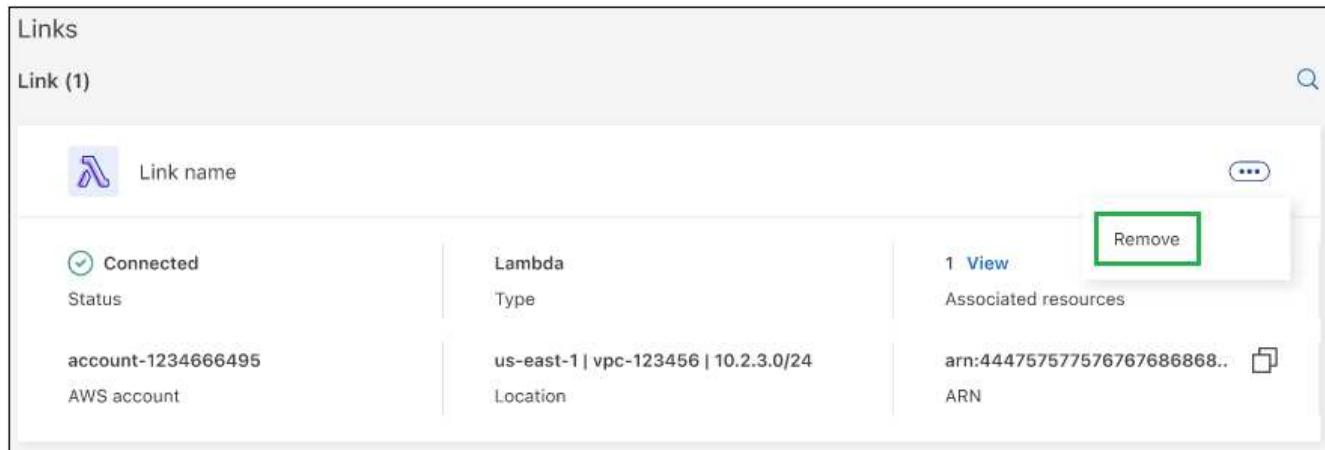
Sie können einen Link entfernen, den Sie in Ihrer Umgebung nicht mehr verwenden. Alle FSX für ONTAP-Dateisysteme oder andere Ressourcen, die den Link verwendeten, können bestimmte Funktionen nicht nutzen, nachdem der Link entfernt wurde.

Beachten Sie, dass der Link nur aus Workload Factory gelöscht wird – er wird nicht aus Ihrer AWS-Umgebung gelöscht. Sie müssen die Lambda-Funktion aus Ihrem AWS-Konto löschen, nachdem Sie die Verknüpfung in

Workload Factory entfernt haben.

Schritte

1. Melden Sie sich mit einem der "Konsolenerfahrungen" an.
 2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
 3. Wählen Sie im Speichermenü **Verwaltung** und dann **Links**.
- Vorhandene Links werden auf der Seite „Links“ angezeigt.
4. Wählen Sie auf der Seite „Links“ das Aktionsmenü des zu entfernenden Links und dann **Entfernen**.



Link name	...
 account-1234666495	
Connected	 View
Status	Associated resources
AWS account	arn:44475757757676868686..
Lambda	
Type	Location
us-east-1 vpc-123456 10.2.3.0/24	arn
AWS account	Location

5. Wenn Sie sicher sind, wählen Sie erneut **Entfernen**.

Informationen hierzu finden Sie in der AWS-Dokumentation unter "[Lambda-Funktion löschen](#)".

Cache-Volumes in Workload Factory entdecken

Entdecken und zeigen Sie Cache-Volumes an, die mit Cache-Beziehungen verknüpft sind, 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. Dabei handelt es sich um die Remote-Caching-Funktion von NetApp ONTAP, die den Datenzugriff beschleunigt und die WAN-Latenz, Bandbreite und Kosten für leseintensive Workloads reduziert, insbesondere wenn Clients wiederholt auf dieselben Daten zugreifen müssen.

["Erfahren Sie mehr über die Replikation von Daten mit FlexCache."](#)

Über diese Aufgabe

Zum Erkennen von Cache-Beziehungen ist eine Link-Zuordnung erforderlich.

Eine Cache-Beziehung kann zwischen Volumes auf zwei ONTAP Systemen bestehen, beispielsweise einem FSx für ONTAP Dateisystem und einem Cloud Volumes ONTAP System. Eine Cache-Beziehung kann auch innerhalb eines einzelnen FSx for ONTAP Dateisystems von Volume zu Volume bestehen.

Bevor Sie beginnen

Beachten Sie Folgendes, bevor Sie beginnen.

- Sie müssen einen Link zuordnen, um Cache-Beziehungen auf einem Dateisystem zu erkennen. "[Erfahren Sie, wie Sie einen vorhandenen Link zuordnen oder einen neuen Link erstellen und zuordnen.](#)" . Kehren Sie nach der Verknüpfung zu diesem Vorgang zurück.
- Sie müssen über eine bestehende Cache-Beziehung verfügen.

Schritte

1. Melden Sie sich mit einem der "[Konsolenerfahrungen](#)" an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Speichermenü **FSx für ONTAP** aus.
4. Wählen Sie unter **FSx for ONTAP** die Registerkarte **Cache-Beziehungen** aus.
5. Ihre Cache-Volumes werden in der Tabelle angezeigt. Die Tabelle enthält die folgenden Informationen zu jedem Cache-Volume:
 - **Ursprungscluster**: Der Ursprungs- oder Quellcluster der FlexCache -Beziehung.
 - **Ursprungsvolumen**: Das Ursprungs- oder Quellvolumen der FlexCache -Beziehung.
 - **Ursprungsspeicher-VM**: Die Ursprungs- oder Quellspeicher-VM des Volumes.
 - **Cache-Volumen**: Das Cache- oder Zielvolumen der FlexCache -Beziehung.
 - **Cache-Speicher-VM**: Der Cache oder die Ziel-Speicher-VM des Volumes.
 - **Status**: Der Status der FlexCache -Beziehung.
 - **Verfügbarer Speicher im Cache**: Die Menge des verfügbaren Speichers auf dem Cache-Volume.
 - **Cache-Dateisystem**: Das Dateisystem des Cache-Volumes.
 - **Schreibmodi**: Der Schreibmodus der FlexCache Beziehung.
 - **DR-Cache**: Gibt an, ob es sich bei der FlexCache -Beziehung um einen Disaster Recovery (DR)-Cache handelt.
 - **Exportrichtlinie**: Die Exportrichtlinie des Cache-Volumes.

Ähnliche Informationen

["Cache-Volumes verwalten"](#)

Volumes managen

Erstellen Sie ein FSx für ONTAP -Volume in Workload Factory

Nachdem Sie Ihr FSx for ONTAP Dateisystem eingerichtet haben, erstellen Sie FSx for ONTAP -Volumes in Workload Factory als virtuelle Ressourcen zum Gruppieren Ihrer Daten.

Über diese Aufgabe

FSx für ONTAP-Volumes gruppieren Daten virtuell, bestimmen, wie Daten gespeichert werden, und bestimmen die Art des Zugriffs auf Ihre Daten. Volumes verbrauchen keine Storage-Kapazität des Filesystems. Die in einem Volume gespeicherten Daten belegen primär SSD-Storage. Je nach der Tiering-Richtlinie des Volumes können die Daten auch Kapazitäts-Pool-Storage in Anspruch nehmen. Sie legen die Größe eines Volumes fest, wenn Sie es erstellen, und Sie können die Größe später ändern.

Die folgenden Protokolle können für Ihre Volumes verwendet werden:

- SMB/CIFS: Dateispeicherprotokoll für Windows-Betriebssysteme
- NFS: File-Storage-Protokoll für Unix Betriebssysteme
- iSCSI: Block-Storage-Protokoll

S3-Endpunkte können an ein FSx for ONTAP Volume angehängt werden. Mithilfe eines S3-Zugriffspunkts können Sie über die AWS S3-APIs auf Dateidaten zugreifen, die sich auf SMB/CIFS- oder NFS-Volumes befinden. Dies ermöglicht Ihnen die Integration Ihrer vorhandenen Daten mit GenAI, ML und Analysen von AWS-Diensten, die S3-Zugriffspunkte unterstützen.

Details zu den Lautstärkeeinstellungen

Unveränderliche Dateien

Diese Funktion, auch als SnapLock bekannt, ist standardmäßig deaktiviert. Durch die Aktivierung unveränderlicher Dateien wird das Löschen oder Überschreiben von Daten für einen festgelegten Zeitraum verhindert. Die Aktivierung dieser Funktion ist nur während der Volume-Erstellung möglich. Nachdem die Funktion aktiviert wurde, kann sie nicht mehr deaktiviert werden. Dies ist eine Premiumfunktion für FSx für ONTAP, für die eine zusätzliche Gebühr anfällt. Weitere Informationen finden Sie unter "[So funktioniert SnapLock](#)" in der Amazon FSx for NetApp ONTAP -Dokumentation.

- **Aufbewahrungsmodi:** Sie können zwischen zwei Aufbewahrungsmodi wählen – *Enterprise* oder *Compliance*.
 - Im *Enterprise*-Modus können unveränderliche Dateien oder SnapLock, Administratoren eine Datei während des Aufbewahrungszeitraums löschen.
 - Im *Compliance*-Modus kann eine WORM-Datei nicht vor Ablauf der Aufbewahrungsfrist gelöscht werden. Auf ähnliche Weise kann das unveränderliche Volume erst gelöscht werden, wenn die Aufbewahrungsfristen für alle Dateien innerhalb des Volume abgelaufen sind.
- **Aufbewahrungszeitraum:** Für den Aufbewahrungszeitraum gibt es zwei Einstellungen: *Aufbewahrungsrichtlinie* und *Aufbewahrungszeiträume*. Die *Aufbewahrungsrichtlinie* definiert, wie lange Dateien in einem unveränderlichen WORM-Zustand aufbewahrt werden. Sie können Ihre eigene Aufbewahrungsrichtlinie angeben oder die Standardaufbewahrungsrichtlinie (nicht angegeben) verwenden, die 30 Jahre beträgt. Die minimalen und maximalen *Aufbewahrungsfristen* definieren den zulässigen Zeitraum für das Sperren von Dateien.



Selbst wenn die Aufbewahrungsfrist abgelaufen ist, können Sie keine WORM-Datei ändern. Sie können sie nur löschen oder einen neuen Aufbewahrungszeitraum festlegen, um den WORM-Schutz erneut zu aktivieren.

- **Autocommit:** Sie haben die Möglichkeit, die Autocommit-Funktion zu aktivieren. Die Autocommit-Funktion übergibt eine Datei auf einem SnapLock -Volume in den WORM-Status, wenn sich die Datei während der Dauer des Autocommit-Zeitraums nicht geändert hat. Die Autocommit-Funktion ist standardmäßig deaktiviert. Sie müssen sicherstellen, dass sich die Dateien, die Sie automatisch festschreiben möchten, 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 der Aufbewahrungsfrist der Datei zu ermöglichen. Diese Funktion ist standardmäßig deaktiviert.
- **Volume-Anfügemodus:** Sie können vorhandene Daten in einer WORM-geschützten Datei nicht ändern. Unveränderliche Dateien ermöglichen Ihnen jedoch, den Schutz vorhandener Daten mithilfe von WORM-anhängbaren Dateien aufrechtzuerhalten. Sie können beispielsweise Protokolldateien erstellen oder Audio- oder Video-Streaming-Daten aufbewahren, während Sie inkrementell Daten in diese Dateien

schreiben. "["Erfahren Sie mehr über den Volume-Append-Modus"](#) in der Amazon FSx for NetApp ONTAP -Dokumentation.

Bevor Sie beginnen

Überprüfen Sie die folgenden Voraussetzungen, bevor Sie ein Volume erstellen:

- Sie müssen über ein FSx for ONTAP -Dateisystem in der Workload Factory-Konsole verfügen.
- Sie benötigen eine Storage-VM.
- Für den Zugriff auf das Protokoll müssen Sie Folgendes ausführen:
 - Um den Zugriff auf das Volume zu konfigurieren, müssen Sie einen Link zuordnen. "["Erfahren Sie, wie Sie einen vorhandenen Link zuordnen oder einen neuen Link erstellen und zuordnen."](#)". Kehren Sie nach dem Verknüpfen zu diesem Vorgang zurück.
 - Sie müssen den Zugriff für das von Ihnen ausgewählte Protokoll konfigurieren, entweder SMB/CIFS, NFS oder iSCSI.

Erstellen eines Volumes

Sie können ein Volume mit den folgenden Tools in der Codebox erstellen: REST API, CloudFormation und Terraform. "["Erfahren Sie, wie Sie Codebox für die Automatisierung verwenden"](#)".



Bei der Verwendung von Terraform aus der Codebox werden der Code, den Sie kopieren oder herunterladen, ausgeblendet `fsxadmin` und `vsadmin` Passwörter. Sie müssen die Passwörter erneut eingeben, wenn Sie den Code ausführen.

Schritte

1. Melden Sie sich mit einem der "["Konsolenerfahrungen"](#) an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Speichermenü **FSx für ONTAP** aus.
4. Wählen Sie in **FSx für ONTAP** das Aktionsmenü des Dateisystems aus, in dem Sie ein Volume erstellen möchten, und wählen Sie **Volume erstellen**.
5. Geben Sie auf der Seite Volume erstellen unter Allgemeine Details die folgenden Details ein:
 - a. **Volumenname:** Geben Sie einen Namen für das Volume ein.
 - b. **Name der Speicher-VM:** Geben Sie optional einen Namen der Speicher-VM ein.
 - c. **Lautstärkestil:** Wählen Sie **FlexVol** oder **FlexGroup** Lautstärke.

Standardmäßig ist ein FlexVol-Volume-Stil ausgewählt.

Die Größe des FlexGroup-Volumes hängt von der Anzahl der Bestandteile ab und erfordert 100 GiB pro Bestandteil.

- a. **Volumengröße:** Geben Sie die Volumengröße und Einheit ein.
Aktivieren Sie optional Volume Autogrow. Diese Option ist verfügbar, wenn Sie **Dateizugriff** als Zugriffstyp für das Volume auswählen.
- b. **Volume-Autogrow:** Aktivieren Sie optional die Funktion „Volume-Autogrow“, um die Volume-Kapazität automatisch zu erweitern, bis das Volume die maximale Größe erreicht. Diese Funktion trägt der

steigenden Datennutzung Rechnung und gewährleistet einen unterbrechungsfreien Betrieb.

Geben Sie die maximale Größe und Einheit für das Volumewachstum an. Sie können die maximale Wachstumsgröße nicht kleiner als die aktuelle Volumegröße einstellen

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

6. Geben Sie unter Zugriff (nur für Dateisysteme mit zugehörigen Links) die folgenden Details an:

a. **Zugriffstyp:** Wählen Sie **Dateizugriff** oder **Zugriff sperren**. Weitere Felder zur Konfiguration des Volume-Zugriffs unterscheiden sich je nach Auswahl.

- **Dateizugriff:** Ermöglicht mehreren autorisierten Benutzern und Geräten den Zugriff auf das Volume mittels SMB/CIFS, NFS oder dualen Protokollen (SMB/NFS).

Füllen Sie die folgenden Felder aus, um den Dateizugriff auf das Volume einzurichten.

b. **NFS-Exportpolitik:** Geben Sie die folgenden Details an, um NFS-Zugriff zu ermöglichen:

i. **Zugriffskontrolle:** Wählen Sie eine **Benutzerdefinierte Exportrichtlinie, bestehende Exportpolitik** oder **kein Zugriff auf das Volume** aus dem Dropdown-Menü.

ii. **Name der Exportpolitik:**

Wenn Sie eine benutzerdefinierte Exportrichtlinie ausgewählt haben, wählen Sie im Dropdown-Menü einen vorhandenen Richtliniennamen aus.

Wenn Sie eine vorhandene Exportrichtlinie ausgewählt haben, geben Sie einen neuen Richtliniennamen ein.

i. **Export Policy Rule** hinzufügen: Optional können Sie für eine benutzerdefinierte Export Policy Regeln zur Export Policy hinzufügen.

c. **SMB/CIFS-Freigabe:** Geben Sie Folgendes an:

i. **Name:** Geben Sie den SMB/CIFS-Freigabenamen ein, um Zugriff zu gewähren.

ii. **Berechtigungen:** Wählen Sie Vollzugriff, Lesen/Schreiben, Lesen oder keinen Zugriff und geben Sie dann die Benutzer oder Gruppen getrennt durch ein Semikolon (;) ein. Bei Benutzern oder Gruppen wird zwischen Groß- und Kleinschreibung unterschieden, und die Domäne des Benutzers muss im Format „Domain\username“ enthalten sein.

d. **Sicherheitsstil:** Wählen Sie für Dual-Protokoll-Volumes entweder den UNIX- oder NTFS-Sicherheitstil aus. UNIX ist der Standard-Sicherheitstil für Dual-Protokoll-Volumes. Eine detaillierte Anleitung zum User Mapping finden Sie in diesem Kontext im AWS Blog-Artikel ["Aktivieren von Multiprotokoll-Workloads mit Amazon FSX for NetApp ONTAP"](#).

- **Blockzugriff:** Ermöglicht Hosts, die kritische Geschäftsanwendungen ausführen, den Zugriff auf das Volume über das iSCSI-Protokoll. Der Block-Zugriff ist nur verfügbar, wenn die horizontal skalierbare Filesystem-Implementierung maximal sechs HA-Paare umfasst.

Füllen Sie die folgenden Felder aus, um den Blockzugriff auf das Volume einzurichten.

A. **iSCSI-Konfiguration:** Geben Sie die folgenden Details an, um iSCSI für den Blockzugriff auf das Volume zu konfigurieren.

I. Wählen Sie **Neue Initiatorgruppe erstellen** oder **vorhandene Initiatorgruppe zuordnen** aus.

II. Wählen Sie das **Host-Betriebssystem** aus dem Dropdown-Menü aus.

- III. Geben Sie einen **Initiatorgruppennamen** für eine neue Initiatorgruppe ein.
- IV. Fügen Sie unter Host-Initiatoren einen oder mehrere iSCSI Qualified Name (IQN)-Hostinitiatoren hinzu.
- e. **S3-Zugriffspunkt**: Optional kann ein S3-Zugriffspunkt angehängt werden, um über AWS S3-APIs auf FSx for ONTAP -Dateisystemdaten zuzugreifen, die sich auf NFS- oder SMB/CIFS-Volumes befinden. Es wird nur der Dateizugriffstyp unterstützt. Bitte geben Sie folgende Details an:
- **Name des S3-Zugangspunkts**: Geben Sie den Namen des S3-Zugangspunkts ein.
 - **Benutzer**: Wählen Sie einen vorhandenen Benutzer mit Zugriff auf das Volume aus oder erstellen Sie einen neuen Benutzer.
 - **Benutzertyp**: Wählen Sie als Benutzertyp **UNIX** oder **Windows** aus.
 - **Netzwerkkonfiguration**: Wählen Sie **Internet** oder **Virtual private cloud (VPC)**. Der von Ihnen gewählte Netzwerktyp bestimmt, ob der Zugangspunkt aus dem Internet erreichbar ist oder auf eine bestimmte VPC beschränkt ist.
 - **Metadaten aktivieren**: Durch die Aktivierung von Metadaten wird eine S3-Tabelle erstellt, die alle über den S3-Zugangspunkt zugänglichen Objekte enthält, die Sie für Audits, Governance, Automatisierung, Analyse und Optimierung verwenden können. Die Aktivierung von Metadaten verursacht zusätzliche AWS-Kosten. Weitere Informationen finden Sie unter "[Amazon S3 Preisdokumentation](#)".
- f. **S3 access point tags**: Optional können Sie bis zu 50 Tags hinzufügen oder entfernen.

7. Geben Sie unter Effizienz und Sicherung folgende Informationen an:

- a. **Speichereffizienz**: Standardmäßig aktiviert. Wählen Sie diese Option, um die Funktion zu deaktivieren.
- ONTAP erreicht Speichereffizienz durch Deduplizierungs- und Komprimierungsfunktionen. Deduplizierung eliminiert doppelte Datenblöcke. Bei der Datenkomprimierung werden die Datenblöcke komprimiert, damit sie die erforderliche Menge an physischem Storage reduzieren können.
- b. **Snapshot Policy**: Wählen Sie die Snapshot Policy aus, um die Häufigkeit und Aufbewahrung von Snapshots festzulegen.

Nachfolgend sind die Standardrichtlinien von AWS aufgeführt. Um vorhandene Snapshot-Richtlinien anzuzeigen, müssen Sie "["Verknüpfen Sie eine Verknüpfung"](#) Die

default

Diese Richtlinie erstellt automatisch Snapshots nach dem folgenden Zeitplan. Die ältesten Snapshot-Kopien werden gelöscht, um Platz für neuere Kopien zu schaffen:

- Maximal sechs stündliche Snapshots wurden fünf Minuten nach der Stunde erstellt.
- Maximal zwei Snapshots täglich von Montag bis Samstag um 10 Minuten nach Mitternacht.
- Maximal zwei wöchentliche Schnapschüsse, die jeden Sonntag um 15 Minuten nach Mitternacht erstellt wurden.



Snapshot-Zeiten basieren auf der Zeitzone des Dateisystems, die standardmäßig auf Coordinated Universal Time (UTC) eingestellt ist. Informationen zum Ändern der Zeitzone finden Sie in "["Anzeigen und Einstellen der Systemzeitzone"](#) der NetApp-Supportdokumentation.

default-1weekly

Diese Richtlinie funktioniert auf die gleiche Weise wie die `default` Richtlinie, außer dass nur ein Snapshot aus dem wöchentlichen Zeitplan aufbewahrt wird.

none

Diese Richtlinie erstellt keine Snapshots. Sie können diese Richtlinie Volumes zuweisen, um die automatische Erstellung von Snapshots zu verhindern.

c. **Tiering Policy:** Wählen Sie die Tiering Policy für die auf dem Volume gespeicherten Daten.

Ausgewogen (Auto) ist die Standard-Tiering-Richtlinie beim Erstellen eines Volumes über die Workload Factory-Konsole. Weitere Informationen zu den Richtlinien für die Mengenstaffelung finden Sie unter "[Speicherkapazität für Volumes](#)" in der AWS FSx for NetApp ONTAP Dokumentation. Beachten Sie, dass Workload Factory in der Workload Factory-Konsole anwendungsfallbasierte Namen für Tiering-Richtlinien verwendet und FSx for ONTAP Tiering-Richtliniennamen in Klammern angibt.

d. **Unveränderliche Dateien:** Durch Aktivieren der Funktion „Unveränderliche Dateien“ werden Dateien in diesem Volume dauerhaft in einen unveränderlichen WORM-Status (Write-Once-Read-Many) versetzt. Geben Sie die folgenden Details an:

- i. Aktivieren Sie **unveränderliche Dateien mit SnapLock**.
- ii. Wählen Sie das Feld aus, um zuzustimmen und fortzufahren.
- iii. Wählen Sie **Enable**.
- iv. **Retention Mode:** Wählen Sie **Enterprise** oder **Compliance** Modus.
- v. **Aufbewahrungsfrist:**

- Wählen Sie die Aufbewahrungsrichtlinie aus:
 - **Unspezifiziert:** Setzt die Aufbewahrungspolitik auf 30 Jahre.
 - **Zeitraum angeben:** Geben Sie die Anzahl der Sekunden, Minuten, Stunden, Tage, Monate oder Jahre ein, um Ihre eigene Aufbewahrungsrichtlinie festzulegen.
- Wählen Sie die Mindest- und Höchstaufbewahrungszeiträume aus:
 - **Minimum:** Geben Sie die Anzahl der Sekunden, Minuten, Stunden, Tage, Monate oder Jahre ein, um die Mindestaufbewahrungszeit festzulegen.
 - **Maximum:** Geben Sie die Anzahl der Sekunden, Minuten, Stunden, Tage, Monate oder Jahre ein, um die maximale Aufbewahrungszeit festzulegen.

vi. **Autocommit:** Deaktivieren oder aktivieren Sie Autocommit. Wenn Sie die automatische Übertragung aktivieren, legen Sie den Zeitraum für die automatische Übertragung fest.

vii. **Privilegiertes Löschen:** Deaktivieren oder aktivieren. Wenn Sie das privilegierte Löschen aktivieren, kann ein SnapLock Administrator eine Datei löschen, bevor ihre Aufbewahrungszeit abläuft.

viii. **Volume Append-Modus:** Deaktivieren oder aktivieren. Ermöglicht das Hinzufügen neuer Inhalte zu WORM-Dateien.

e. **ARP/AI:** NetApp Autonomous Ransomware Protection mit AI (ARP/AI) ist standardmäßig aktiviert, wenn ein Link mit dem Dateisystem verknüpft ist. "[Erfahren Sie mehr über ARP/AI](#)". Akzeptieren Sie die Aussage, um fortzufahren.

Wenn die Funktion nicht verfügbar ist, kann dies einen der folgenden Gründe haben:

- Dem Dateisystem ist kein Link zugeordnet. "[Erfahren Sie, wie Sie einen vorhandenen Link](#)

zuordnen oder einen neuen Link erstellen und zuordnen.". Kehren Sie nach dem Verknüpfen zu diesem Vorgang zurück.

- Volumes mit unveränderlichen Dateien und Volumes mit iSCSI- und NVMe-Protokollen werden für ARP/AI nicht unterstützt.
- Das Dateisystem verfügt bereits über eine ARP/AI-Richtlinie.

8. Geben Sie unter Erweiterte Konfiguration Folgendes an:

- a. **Verbindungspfad:** Geben Sie den Speicherort im Namespace der Speicher-VM ein, an dem das Volume gemountet wird. Der Standard-Verbindungspfad ist /<volume-name>.
- b. **Aggregatliste:** Nur für FlexGroup Volumes. Hinzufügen oder Entfernen von Aggregaten. Die Mindestanzahl an Aggregaten ist eins.
- c. **Anzahl der Komponenten:** Nur für FlexGroup-Volumes. Geben Sie die Anzahl der Bestandteile pro Aggregat ein. Pro Komponente sind 100 gib erforderlich.

9. Wählen Sie **Erstellen**.

Ähnliche Informationen

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

Zugriff auf Ihre FSX for ONTAP-Dateisystemdaten

Sie können von vor Ort auf Ihre FSX for ONTAP-Dateisysteme zugreifen, indem Sie Volumes für NAS-Clients mounten und iSCSI-LUNs für SAN-Clients mounten.

["Datenzugriff"](#) In der Dokumentation zu Amazon FSX for NetApp ONTAP finden Sie Informationen dazu, wie Sie auf Daten für Ihre Referenz zugreifen.

Sie können den Einhängepunkt für Volumes auch in NetApp Workload Factory abrufen.

Holen Sie sich den Mount-Punkt für Volumes in NetApp Workload Factory

Holen Sie sich den Mount-Punkt für ein Volume, um eine Freigabe auf einer CIFS-Freigabe oder einem NFS-Client zu mounten.

Schritte

1. Melden Sie sich mit einem der "[Konsolenerfahrungen](#)" an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie in **FSx for ONTAP** das Aktionsmenü des Dateisystems mit dem Volume und wählen Sie dann **Verwalten**.
4. Wählen Sie in der Dateisystemübersicht die Registerkarte **Volumes** aus.
5. Wählen Sie auf der Registerkarte „Volumes“ das Aktionsmenü für das Volume, dann **Grundlegende Aktionen** und dann **Mount-Befehl anzeigen**.
6. Wählen Sie im Dialogfeld Mount-Befehl **Copy** aus, um den Befehl entweder für den NFS-Mount-Punkt oder die CIFS-Freigabe zu kopieren. Sie geben den kopierten Befehl in Ihrem Terminal ein.
7. Wählen Sie **Schließen**.

Stellen Sie eine Verbindung mit NAS-Clients her

- "[Mounten Sie ein Volume auf Linux-Clients](#)"
- "[Mounten Sie ein Volume auf Windows-Clients](#)"
- "[Mounten Sie ein Volume auf macOS Clients](#)"

Stellen Sie eine Verbindung mit SAN-Clients her

- "[Mounten Sie eine iSCSI-LUN auf Linux-Clients](#)"
- "[Mounten Sie eine iSCSI-LUN auf Windows-Clients](#)"

Blockspeicherressourcen erstellen

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 vorhandenen Link zuordnen oder einen neuen Link erstellen und zuordnen.](#)". Nachdem Sie die Verknüpfung hergestellt haben, kehren Sie zu diesem Vorgang zurück.

Schritte

1. Melden Sie sich mit einem der "[Konsolenerfahrungen](#)" an.
2. Wählen Sie in der Kachel „Speicher“ die Option „Zum Speicher gehen“ aus.
3. Wählen Sie im Speichermenü **FSx für ONTAP** aus.
4. Wählen Sie in **FSx for ONTAP** die Registerkarte **Blockgeräte** aus.
5. Wählen Sie den Ressourcentyp **Create initiator group** und anschließend **Create igrup**.
6. 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.

7. Wählen Sie **Erstellen**.

Ähnliche Informationen

["Verwalten der Initiatorgruppen für ein FSx for ONTAP-Dateisystem"](#)

Erstellen eines Blockgeräts für ein Dateisystem in NetApp Workload Factory

Erstellen Sie Blockgeräte, um die Anforderungen Ihrer Geschäftsanwendungen (LOB) zu erfüllen.

Über diese Aufgabe

In NetApp Workload Factory werden für Blockgeräte ausschließlich FlexVol -Volumes unterstützt. Sie können Blockgeräte mithilfe des iSCSI-Protokolls erstellen.

Die Blockgröße muss kleiner sein als die verfügbare FlexVol volume Volumengröße.

Bevor Sie beginnen

- Sie müssen einen Link zuordnen, um Blockgeräte zu erstellen. ["Erfahren Sie, wie Sie einen vorhandenen Link zuordnen oder einen neuen Link erstellen und zuordnen."](#) Die Nachdem Sie die Verknüpfung hergestellt haben, kehren Sie zu diesem Vorgang zurück.

Schritte

1. Melden Sie sich mit einem der ["Konsolenerfahrungen"](#) an.
2. Wählen Sie in der Kachel „Speicher“ die Option „Zum Speicher gehen“ aus.
3. Wählen Sie im Speichermenü **FSx für ONTAP** aus.
4. Wählen Sie in **FSx for ONTAP** die Registerkarte **Blockgeräte** aus.
5. Wählen Sie **Blockgerät erstellen**.
6. Gehen Sie unter **Volumendetails** wie folgt vor:
 - a. **Volume-Name:** Wählen Sie eine der folgenden Optionen aus.
 - Erstellen Sie ein neues Volume und geben Sie einen Namen für das Volume ein.
 - Wählen Sie ein vorhandenes Volume aus.
 - b. **Speicher-VM:** Wählen Sie eine Speicher-VM aus.
 - c. **Lautstärkestil:** Der Standard-Lautstärkestil ist * FlexVol*.
 - d. **Volumengröße:** Geben Sie die Volumengröße ein und wählen Sie die Einheit aus. Die maximale Größe pro FlexVol volume beträgt 100 TiB.
 - e. **Automatische Volume-Vergrößerung:** Optional können Sie die automatische Volume-Vergrößerung aktivieren, damit das Volume automatisch an Größe zunimmt, sobald es seine Kapazitätsgrenze erreicht. Die maximale Wachstumsgröße beträgt 300 TiB.
 - f. **Tags:** Optional können Sie Tags hinzufügen, um Ihr Blockgerät zu organisieren und zu kategorisieren.
7. Führen Sie unter **Details zum Blockgerät** folgende Schritte aus:
 - a. **Blockgerätename:** Geben Sie einen Namen für das Blockgerät ein.

- b. **Blockgerätegröße**: Geben Sie die Größe des Blockgeräts ein und wählen Sie die Einheit aus. Die Größe des Blockgeräts muss kleiner sein als die verfügbare Speicherkapazität.
8. Gehen Sie unter **Zugriff** wie folgt vor:
- iSCSI-Konfiguration**: Wählen Sie eine der folgenden Optionen.
 - **Neue Initiatorgruppe erstellen**: Geben Sie das Host-Betriebssystem und den Namen der Initiatorgruppe an und fügen Sie einen oder mehrere iSCSI Qualified Name (IQN) Host-Initiatoren hinzu.
 - **Vorhandene Initiatorgruppe zuordnen**: Wählen Sie eine vorhandene Initiatorgruppe aus, geben Sie das Host-Betriebssystem an und wählen Sie einen oder mehrere iSCSI Qualified Name (IQN) Host-Initiatoren aus.
9. Unter **Effizienz und Schutz** sind folgende Maßnahmen zu ergreifen:
- Speichereffizienz**: Standardmäßig aktiviert. Wählen Sie diese Option, um die Funktion zu deaktivieren.

ONTAP erreicht Speichereffizienz durch Deduplizierungs- und Komprimierungsfunktionen. Deduplizierung eliminiert doppelte Datenblöcke. Bei der Datenkomprimierung werden die Datenblöcke komprimiert, damit sie die erforderliche Menge an physischem Storage reduzieren können.
 - Snapshot Policy**: Wählen Sie die Snapshot Policy aus, um die Häufigkeit und Aufbewahrung von Snapshots festzulegen.
- Nachfolgend sind die Standardrichtlinien von AWS aufgeführt. Um vorhandene Snapshot-Richtlinien anzuzeigen, müssen Sie [xref:."/Verknüpfen Sie eine Verknüpfung"Die](#)
- default**
- Diese Richtlinie erstellt automatisch Snapshots nach dem folgenden Zeitplan. Die ältesten Snapshot-Kopien werden gelöscht, um Platz für neuere Kopien zu schaffen:
- Maximal sechs stündliche Snapshots wurden fünf Minuten nach der Stunde erstellt.
 - Maximal zwei Snapshots täglich von Montag bis Samstag um 10 Minuten nach Mitternacht.
 - Maximal zwei wöchentliche Schnappschüsse, die jeden Sonntag um 15 Minuten nach Mitternacht erstellt wurden.
-  Snapshot-Zeiten basieren auf der Zeitzone des Dateisystems, die standardmäßig auf Coordinated Universal Time (UTC) eingestellt ist. Informationen zum Ändern der Zeitzone finden Sie in ["Anzeigen und Einstellen der Systemzeitzone"](#) der NetApp-Supportdokumentation.
- default-1weekly**
- Diese Richtlinie funktioniert auf die gleiche Weise wie die **default** Richtlinie, außer dass nur ein Snapshot aus dem wöchentlichen Zeitplan aufbewahrt wird.
- none**
- Diese Richtlinie erstellt keine Snapshots. Sie können diese Richtlinie Volumes zuweisen, um die automatische Erstellung von Snapshots zu verhindern.
- c. **Tiering Policy**: Wählen Sie die Tiering Policy für die auf dem Volume gespeicherten Daten.
- Ausgewogen (Auto)* ist die Standard-Tiering-Richtlinie beim Erstellen eines Volumes über die Workload

Factory-Konsole. Weitere Informationen zu den Richtlinien für die Mengenstaffelung finden Sie unter "[Speicherkapazität für Volumes](#)" in der AWS FSx für NetApp ONTAP Dokumentation. Beachten Sie, dass Workload Factory in der Workload Factory-Konsole anwendungsfallbasierte Namen für Tiering-Richtlinien verwendet und FSx for ONTAP Tiering-Richtliniennamen in Klammern angibt.

- d. **ARP/AI:** NetApp Autonomous Ransomware Protection mit AI (ARP/AI) ist standardmäßig aktiviert, wenn ein Link mit dem Dateisystem verknüpft ist. "[Erfahren Sie mehr über ARP/AI](#)". Akzeptieren Sie die Aussage, um fortzufahren.

Wenn die Funktion nicht verfügbar ist, kann dies einen der folgenden Gründe haben:

- Dem Dateisystem ist kein Link zugeordnet. "[Erfahren Sie, wie Sie einen vorhandenen Link zuordnen oder einen neuen Link erstellen und zuordnen.](#)". Kehren Sie nach dem Verknüpfen zu diesem Vorgang zurück.
- Für ARP/AI werden keine Volumes mit unveränderlichen Dateien und Volumes mit dem NVMe-Protokoll unterstützt.
- Das Dateisystem verfügt bereits über eine ARP/AI-Richtlinie.

10. Wählen Sie **Erstellen**.

Ähnliche Informationen

["Verwalten der Blockgeräte für ein FSx for ONTAP -Dateisystem"](#)

Erstellen Sie eine Storage-VM für ein FSX für ONTAP-Filesystem

Erstellen Sie eine Storage-VM (SVM) für ein FSx for ONTAP Dateisystem, um virtuell auf Speicher- und Datendienste für Ihre Workloads in NetApp Workload Factory zuzugreifen.

Über diese Aufgabe

Storage-VMs sind isolierte Dateiserver, mit denen Sie auf die Daten der einzelnen Workloads im Workload Factory Storage zugreifen können. Jede SVM verfügt über eigene Administratoranmeldeinformationen und Endpunkte für die Verwaltung und den Zugriff auf Daten.

Wenn Sie mit SVMs auf Daten in FSX for ONTAP zugreifen, mounten Ihre Clients und Workstations über den Endpunkt (IP-Adresse) der SVM ein Volume, eine CIFS/SMB-Freigabe oder eine iSCSI-LUN, die von einer SVM gehostet wird.

Bevor Sie beginnen

Überprüfen Sie die unterstützte Anzahl von Storage-VMs pro Dateisystem. "[Management von FSX für ONTAP Storage Virtual Machines](#)" In der AWS-Dokumentation finden Sie Informationen zur maximalen Anzahl von SVMs pro Filesystem.

Erstellen einer Storage-VM

Sie können eine Speicher-VM über die Workload Factory-Konsole erstellen. Sie können auch die folgenden in der Codebox verfügbaren Tools verwenden: REST API, CloudFormation und Terraform. "[Erfahren Sie, wie Sie Codebox für die Automatisierung verwenden](#)" .



Bei der Verwendung von Terraform aus der Codebox werden der Code, den Sie kopieren oder herunterladen, ausgeblendet `fsxadmin` und `vsadmin` Passwörter. Sie müssen die Passwörter erneut eingeben, wenn Sie den Code ausführen.

Schritte

1. Melden Sie sich mit einem der "Konsolenerfahrungen" an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Speichermenü **FSx für ONTAP** aus.
4. Wählen Sie in **FSx for ONTAP** das Aktionsmenü des Dateisystems und anschließend **Verwalten**.
5. Wählen Sie in der Dateisystemübersicht unter „Speicher-VMs“ die Option „Speicher-VM erstellen“.
6. Geben Sie auf der Seite „Speicher-VM erstellen“ unter „Speicher-VM-Konfiguration“ Folgendes an:
 - a. **Name:** Geben Sie einen Namen für die Speicher-VM ein.
 - b. **Speicher-VM-Anmeldeinformationen:** Geben Sie ein Passwort für den Benutzer dieser Speicher-VM ein `vsadmin` oder verwenden Sie die Benutzeranmeldeinformationen des Dateisystems `fsxadmin`.
 - c. **Sicherheitsstil des Root-Volumes:** Wählen Sie den Sicherheitstyp des Root-Volumes abhängig von der Art 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.
7. Wählen Sie **Erstellen**.

Sichern Sie Ihre Daten

Arten der Datensicherung in NetApp Workload Factory

FSx für ONTAP unterstützt Snapshots, NetApp Autonomous Ransomware Protection mit KI, Replikation und Backups zum Datenschutz. Wir empfehlen Ihnen, eine Kombination verschiedener Datenschutzarten zu verwenden, um sich auf das Unvermeidliche vorzubereiten und Ihre Daten zu schützen.

Arten der Datensicherung

Datensicherung Ihrer Workloads gewährleistet, dass nach jedem Datenverlust jederzeit ein Recovery durchgeführt werden kann. Informieren Sie sich über die Arten der Datensicherung, bevor Sie die zu verwendenden Funktionen auswählen.

Snapshots

Ein Snapshot erstellt ein schreibgeschütztes, zeitpunktgenaues Image eines Volumes innerhalb des Quell-Volumes als Snapshot-Kopie. Sie können die Snapshot-Kopie verwenden, um einzelne Dateien wiederherzustellen oder den gesamten Inhalt eines Volumes wiederherzustellen. Snapshots sind die Grundlage aller Sicherungsmethoden. Mithilfe der Snapshot Kopie, die auf dem Volume erstellt wird, werden das replizierte Volume und die Backup-Datei bei den Änderungen am Quell-Volume synchronisiert.

Autonomer Ransomware-Schutz von NetApp mit KI

NetApp Autonomous Ransomware Protection mit KI (ARP/AI) nutzt Workload-Analysen in NAS-Umgebungen (NFS/SMB), um ungewöhnliche Aktivitäten zu erkennen und davor zu warnen, die auf einen Ransomware-Angriff hindeuten könnten. Bei Verdacht auf einen Angriff erstellt ARP/AI zusätzlich zum bestehenden Schutz

durch geplante Snapshots auch neue, unveränderliche Snapshots.

Replizierung

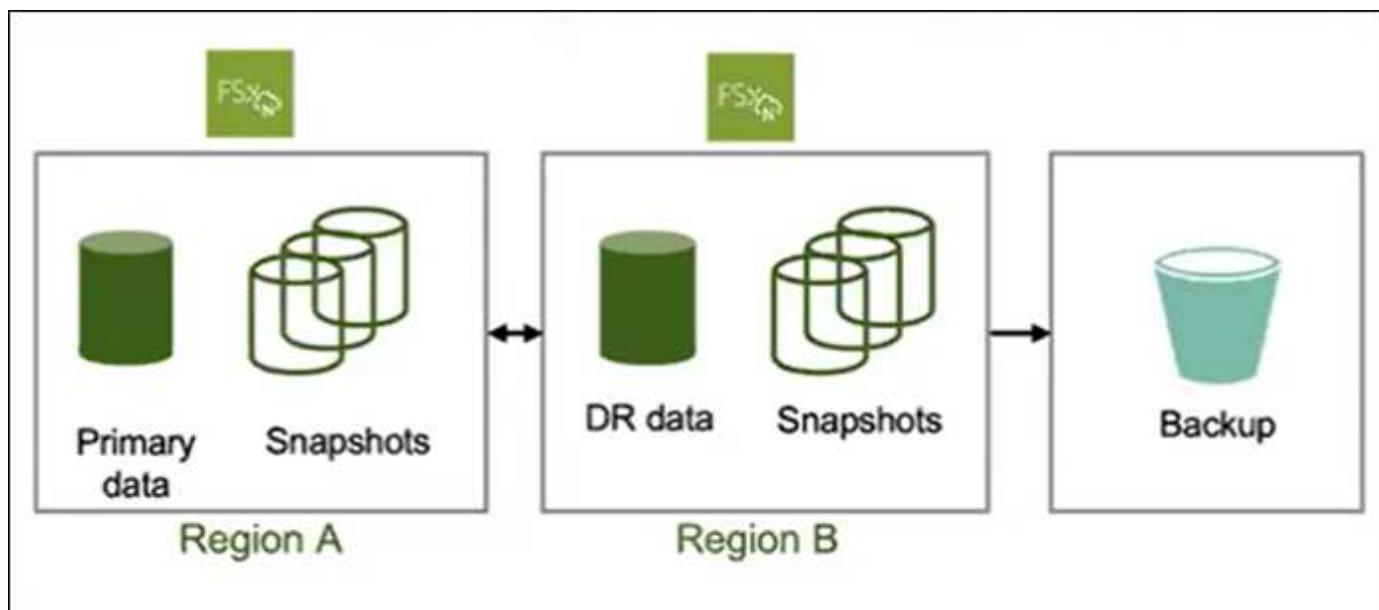
Durch Replizierung wird eine sekundäre Kopie Ihrer Daten in einem anderen FSX für ONTAP Dateisystem erstellt und die sekundären Daten werden kontinuierlich aktualisiert. Ihre Daten bleiben aktuell und verfügbar, beispielsweise für Disaster Recovery.

Sie können sowohl replizierte Volumes auf einem anderen FSX für ONTAP-Dateisystem als auch Backup-Dateien in der Cloud erstellen. Oder Sie haben die Wahl, ob Sie nur replizierte Volumes oder Backup-Dateien erstellen möchten.

Backups

Sie können Backups Ihrer Daten in der Cloud zur Sicherung und zur langfristigen Aufbewahrung erstellen. Bei Bedarf können Sie ein Volume, einen Ordner oder einzelne Dateien aus dem Backup in demselben oder einem anderen funktionierenden Dateisystem wiederherstellen.

Das folgende Diagramm zeigt eine visuelle Darstellung der Datensicherung für FSX für ONTAP Storage durch Snapshots, regionsübergreifende Replizierung und Backup in Objekt-Storage.



Best Practices zum Schutz Ihrer Workload-Daten

FSX für ONTAP bietet mehrere Datensicherungsoptionen, die miteinander kombiniert werden können, um die Recovery-Zeitpunkte und -Zeiten Ihrer Wahl zu erreichen. Für den bestmöglichen Schutz empfehlen wir, sowohl Volume-Snapshots als auch Volume-Backups zu verwenden.

Ein Recovery-Zeitpunkt (Recovery Point Objective, RPO) beschreibt, wie häufig die neueste Kopie Ihrer Daten garantiert wird. Ein Recovery-Zeitvorgabe (Recovery Time Objective, RTO) definiert, wie lange die Wiederherstellung Ihrer Daten dauert.

Schützen Sie Ihre Workload-Daten mit Snapshots

Snapshots sind virtuelle Point-in-Time-Versionen eines Volumes, die nach einem Zeitplan erstellt werden. Sie können mithilfe von standardmäßigen Dateisystembefehlen auf Snapshots zugreifen. Snapshots stellen einen RPO von nur einer Stunde bereit. Die RTO hängt von der wiederherstellenden Datenmenge ab und ist in erster Linie durch das Volume-Durchsatzlimit begrenzt. Snapshots ermöglichen Benutzern auch die Wiederherstellung spezifischer Dateien und Verzeichnisse, wodurch die RTO noch weiter verringert wird.

Snapshots verbrauchen nur zusätzlichen Volume-Speicherplatz für Änderungen, die am Volume vorgenommen werden.

Schützen Sie Ihre Workload-Daten mit NetApp Autonomous Ransomware Protection mit KI

NetApp Autonomous Ransomware Protection mit KI (ARP/AI) fungiert als wichtige zusätzliche Verteidigungsebene, wenn die Antivirensoftware einen Eindringling nicht erkennen konnte. Durch das Festlegen einer ARP/AI-Richtlinie wird diese für alle Speicher-VMs und alle vorhandenen und neu erstellten Volumes aktiviert. Nach der Aktivierung erkennt und schützt ARP/AI alle Volumes und Speicher-VMs. Wenn eine Dateierweiterung als abnormal gekennzeichnet ist, sollten Sie die Warnung auswerten.

Schutz von Workload-Daten durch Volume-Replizierung

Volume Replication erstellt eine Kopie der neuesten Daten eines Volumes einschließlich aller Snapshots in einer anderen Region. Wenn Sie sich keine mehrstündigen RTOs für eine vollständige Volume-Wiederherstellung von einem Volume-Backup leisten können, sollten Sie eine Volume-Replikation in Erwägung ziehen. Die Volume-Replikation stellt zwar sicher, dass aktuelle Daten in einer anderen Region zur Verfügung stehen, Sie müssen jedoch Ihre Clients anpassen, um das Volume in der anderen Region zu verwenden.

Schutz von Workload-Daten durch Backups

Volume Backups ermöglichen unabhängige, zeitpunktgenaue Kopien Ihres Volumes. Sie können dazu verwendet werden, alte Backups zu speichern und die erforderliche zweite Kopie Ihrer Daten bereitzustellen. Tägliche, wöchentliche und monatliche Backup-Zeitpläne ermöglichen die Einhaltung von RPOs ab einem Tag. Volume Backups können nur als Ganzes wiederhergestellt werden. Das Erstellen eines Volumes aus einem Backup (RTO) kann je nach Größe des Backups Stunden bis viele Tage dauern.

Empfehlungen zum Schutz Ihrer Workload-Daten

Berücksichtigen Sie die folgenden Empfehlungen zum Schutz Ihrer Workload-Daten.

- Verwenden Sie die Volume-Replikation für die Notfallwiederherstellung: Wenn Ihre Anwendung eine niedrige RTO erfordert, sollten Sie die Verwendung der Volume-Replikation in Betracht ziehen, um Ihre Daten in eine andere Region zu replizieren.
- Verwenden Sie Volume-Backups in Verbindung mit Snapshots: Durch die gemeinsame Verwendung der beiden Funktionen wird sichergestellt, dass Sie Ihre Dateien aus Snapshots wiederherstellen und im Falle eines Volume-Verlusts mithilfe von Backups vollständige Wiederherstellungen durchführen können.
- Definieren Sie eine Volume Backup-Richtlinie: Vergewissern Sie sich, dass die Backup-Richtlinie die Anforderungen Ihres Unternehmens im Hinblick auf das Alter und die Häufigkeit des Backups erfüllt. Wir empfehlen, mindestens zwei tägliche Backups für jedes Volume zu erstellen.
- Definieren Sie einen Snapshot-Zeitplan: Ältere Snapshots werden weniger wahrscheinlich zur Wiederherstellung von Daten verwendet. Wir empfehlen Ihnen, einen Snapshot-Zeitplan zu definieren, der die abnehmenden Ergebnisse der Aufbewahrung älterer Snapshots im Vergleich zu den Kosten für zusätzliche Snapshot-Kapazität berücksichtigt.
- Aktivieren Sie eine ARP/AI-Richtlinie für Ihr Dateisystem oder einzelne Volumes, um eine zusätzliche Schutzebene hinzuzufügen und Ihre Daten vor Ransomware-Angriffen zu schützen.

Verwenden von Snapshots

Erstellen Sie einen manuellen Snapshot eines FSX für ONTAP-Volumes

Erstellen Sie einen manuellen Snapshot eines FSx für ONTAP -Volumes in NetApp

Workload Factory. Snapshots sind zeitpunktbezogene Versionen des Inhalts Ihres Volumes.

Snapshots sind Ressourcen von Volumes und sofortige Erfassung von Daten, die nur für geänderte Daten Speicherplatz verbrauchen. Da sich die Daten im Laufe der Zeit ändern, belegen Snapshots in der Regel mit zunehmendem Alter mehr Speicherplatz.

FSX für ONTAP-Volumes verwenden Just-in-Time Copy-on-Write, sodass unveränderte Dateien in Snapshots keine Kapazität des Volumes beanspruchen.



Snapshots sind keine Kopien Ihrer Daten. Wenn Sie Kopien Ihrer Daten erstellen möchten, sollten Sie FSX für ONTAP-Backups oder Volume-Replizierungsfunktionen in Erwägung ziehen.

Bevor Sie beginnen

Sie müssen einen Link zuordnen, um einen manuellen Snapshot eines Volumes zu erstellen. "[Erfahren Sie, wie Sie einen vorhandenen Link zuordnen oder einen neuen Link erstellen und zuordnen.](#)". Kehren Sie nach dem Verknüpfen zu diesem Vorgang zurück.

Schritte

1. Melden Sie sich mit einem der "[Konsolenerfahrungen](#)" an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Speichermenü **FSx für ONTAP** aus.
4. Wählen Sie in **FSx for ONTAP** das Aktionsmenü des Dateisystems aus, das das Volume enthält, für das ein Snapshot erstellt werden soll, und wählen Sie dann **Verwalten**.
5. Wählen Sie in der Dateisystemübersicht die Registerkarte **Volumes** aus.
6. Wählen Sie auf der Registerkarte **Volumes** das Aktionsmenü für das Volume aus, das mit Snapshots geschützt werden soll.
7. Wählen Sie **Datenschutzaktionen** und dann **Snapshots verwalten**.
8. Wählen Sie auf der Seite „Snapshots verwalten“ die Option „Snapshot erstellen“ aus.
9. Führen Sie im Dialogfeld „Snapshot erstellen“ die folgenden Schritte aus:
 - a. Geben Sie im Feld **Snapshot-Name** einen Snapshot-Namen ein.
 - b. Wählen Sie optional ein Etikett aus oder erstellen Sie ein neues Etikett.
 - c. Legen Sie die **Aufbewahrungsfrist** als Anzahl von Stunden, Tagen, Monaten oder Jahren fest.
 - d. Optional: **Machen Sie diesen Snapshot unveränderlich**, um zu verhindern, dass der Snapshot während der Aufbewahrungsfrist gelöscht wird.
- Akzeptieren Sie die Aussage zu unveränderlichen Snapshots.

10. Wählen Sie **Erstellen**.

Erstellen einer Snapshot-Richtlinie für Speicher-VMs in Workload Factory

Erstellen Sie eine benutzerdefinierte Snapshot-Richtlinie für Speicher-VMs in Workload Factory, um die Erstellung und Aufbewahrung von Snapshots zu verwalten. Eine Snapshot-Richtlinie definiert, wie das System Snapshots für eine Speicher-VM erstellt. Sie können eine Snapshot-Richtlinie für eine Speicher-VM in einem FSx for ONTAP

-Dateisystem erstellen. Sie können die Richtlinie auch für mehrere Speicher-VMs freigeben.

Über diese Aufgabe

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

- default
- default-1weekly
- none

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

Durch das Anpassen einer Richtlinie können Sie festlegen, wann Snapshots erstellt werden sollen, wie viele Kopien aufbewahrt werden sollen und wie sie benannt werden sollen.

Bevor Sie beginnen

- Sobald eine Snapshot-Richtlinie erstellt wurde, kann ihre Zuordnung zu den Speicher-VM(s) nicht geändert werden, Sie können die Richtlinie jedoch immer hinzufügen oder aus Volumes entfernen.
- Beachten Sie Folgendes über die Snapshot-Kapazität, bevor Sie Snapshots verwenden:
 - Bei den meisten Datensätzen reicht eine zusätzliche Kapazität von 20 % aus, um Snapshots für bis zu vier Wochen aufzubewahren. Je älter die Daten werden, desto wahrscheinlicher wird die Verwendung für Wiederherstellungen.
 - Das Überschreiben aller Daten in einem Snapshot erfordert eine erhebliche Volume-Kapazität, was für die Bereitstellung von Volume-Kapazität von Bedeutung ist.
- Um eine benutzerdefinierte Snapshot-Richtlinie zu erstellen, müssen Sie einen Link zuordnen. ["Erfahren Sie, wie Sie einen vorhandenen Link zuordnen oder einen neuen Link erstellen und zuordnen."](#). Kehren Sie nach dem Verknüpfen zu diesem Vorgang zurück.

Schritte

1. Melden Sie sich mit einem der ["Konsolenerfahrungen"](#) an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Speichermenü **FSx für ONTAP** aus.
4. Wählen Sie in **FSx for ONTAP** das Aktionsmenü des Dateisystems mit dem Volume und wählen Sie dann **Verwalten**.
5. Wählen Sie in der Dateisystemübersicht die Registerkarte **Storage VMs** aus.
6. Wählen Sie auf der Registerkarte **Storage-VMs** das Aktionsmenü für das Volume aus, das mit geplanten Snapshots geschützt werden soll, dann **Erweiterte Aktionen** und dann **Snapshot-Richtlinien verwalten**.
7. Wählen Sie auf der Seite Snapshot Policy Management **Create Snapshot Policy** aus.
8. Geben Sie im Feld **Snapshot Policy Name** einen Namen für die Snapshot Policy ein.
9. Geben Sie optional eine Beschreibung für die Snapshot-Richtlinie ein.
10. Wählen Sie unter **Policy schedule and copies** aus, wann Snapshots erstellt werden sollen. Zum Beispiel jede Minute oder jede Stunde.

Sie können mehr als eine Frequenz auswählen.

11. Geben Sie unter **Anzahl der Kopien** die Anzahl der Kopien ein, die beibehalten werden sollen.

Die maximale Anzahl von Kopien beträgt 1,023.

12. Optional: Geben Sie unter **Namenskonventionen** ein **Präfix** für die Richtlinie ein.

13. **Retention Label** wird automatisch ausgefüllt.

Dieses Label bezieht sich auf das SnapMirror- oder Replikationslabel, mit dem nur angegebene Snapshots für die Replikation vom Quell- zum Zielsystem ausgewählt werden.

14. Optional: Aktivieren Sie **unveränderliche Snapshots** für alle benötigten Zeitpläne, legen Sie die **Aufbewahrungsfrist** für jeden Zeitplan fest und akzeptieren Sie die Anweisung, um fortzufahren.

Wenn Sie unveränderliche Snapshots aktivieren, werden alle Snapshots in dieser Snapshot-Richtlinie gesperrt, um zu verhindern, dass die Snapshots während des Aufbewahrungszeitraums gelöscht werden.

15. **Freigabe über Storage-VMs:** Standardmäßig aktiviert. Wenn diese Option aktiviert ist, wird die Snapshot-Richtlinie für alle Storage-VMs im File-System freigegeben. Deaktivieren Sie, um eine Snapshot-Richtlinie für eine einzelne Storage-VM zu erstellen.

16. Wählen Sie **Erstellen**.

Wiederherstellen eines Volumes aus einem Snapshot in Workload Factory

In Workload Factory können Sie Daten aus einem Snapshot auf einem vorhandenen oder einem neuen Volume wiederherstellen. Der Wiederherstellungsvorgang ermöglicht eine zeitpunktbezogene Wiederherstellung, wenn ein Volume gelöschte oder beschädigte Dateien enthält.

Über diese Aufgabe

Sie haben die Möglichkeit, Daten aus einem Snapshot auf einem vorhandenen oder einem neuen Volume wiederherzustellen.

Durch die Erstellung eines neuen Volumes aus einem Snapshot wird innerhalb weniger Sekunden eine Kopie eines gesamten Volumes erstellt, unabhängig von der Volumegröße. Die neu erstellte Kopie stellt ein neues Volume dar.

Bevor Sie beginnen

Beachten Sie die folgenden Einschränkungen, bevor Sie ein Volume aus einem Snapshot erstellen:

- Sie können ein Volume nur aus einem Snapshot wiederherstellen, wenn Sie über eine vorhandene Snapshot-Kopie des Volumes verfügen.
- Änderungen an Berechtigungsmodellen: Wenn Sie diesen Vorgang zum Umschalten des Protokolltyps des Network-Attached Storage (NAS) verwenden, kann er auch das Berechtigungsmodell wechseln, das der Sicherheitstyp bereitstellt. Es kann zu Problemen mit Dateizugriffsberechtigungen kommen, die Sie nur manuell mit Administratorzugriff mithilfe der NAS-Client-Tools für die Berechtigungseinstellung beheben können.

Schritte

1. Melden Sie sich mit einem der "Konsolenerfahrungen" an.

2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Speichermenü **FSx für ONTAP** aus.
4. Wählen Sie in **FSx for ONTAP** das Aktionsmenü des Dateisystems mit dem Volume und wählen Sie dann **Verwalten**.
5. Wählen Sie in der Dateisystemübersicht die Registerkarte **Volumes** aus.
6. Wählen Sie auf der Registerkarte **Volumes** das Aktionsmenü für das Volume aus, das aus einem Snapshot wiederhergestellt werden soll.
7. Wählen Sie **Datenschutzaktionen** und dann **Snapshots verwalten**.
8. Wählen Sie auf der Seite „Snapshots verwalten“ das Aktionsmenü für den wiederherzustellenden Snapshot und dann **Wiederherstellen** aus.
9. Wählen Sie im Dialogfeld „Volume aus einem Snapshot wiederherstellen“ eine der folgenden Optionen aus:
 - Wählen Sie mit dem Schalter „Als neues Volume wiederherstellen“ aus.
Geben Sie im Feld **restored Volume Name** einen eindeutigen Namen für das wiederherzustellende Volume ein.
 - Stellen Sie Daten aus einem Snapshot auf einem vorhandenen Volume wieder her. Dieser Vorgang löscht dauerhaft alle Daten, die nach der Erstellung des Snapshots geändert wurden.Akzeptieren Sie die Aussage, um fortzufahren.

10. Wählen Sie **Wiederherstellen**.

Verwenden Sie Backups im Objektspeicher

Erstellen Sie eine manuelle Sicherung eines Volumes in NetApp Workload Factory

Erstellen Sie eine manuelle Sicherung eines Volumes außerhalb regelmäßig geplanter Sicherungen in NetApp Workload Factory.

Über diese Aufgabe

FSX für ONTAP-Backups erfolgen pro Volume, sodass jedes Backup nur die Daten in einem bestimmten Volume enthält.

FSX für ONTAP-Backups sind inkrementell, was bedeutet, dass nur die Daten auf dem Volume, die sich nach Ihrem letzten Backup geändert haben, gespeichert werden. Dies minimiert die zur Erstellung des Backups benötigte Zeit und den für das Backup benötigten Storage-Bedarf. Dadurch sparen Sie Storage-Kosten, da Daten nicht dupliziert werden.

Bevor Sie beginnen

Um Backups Ihrer Volumes zu erstellen, müssen sowohl das Volume als auch das Dateisystem über ausreichend SSD-Speicherkapazität verfügen, um den Backup-Snapshot zu speichern. Bei der Erstellung eines Backup-Snapshots kann die zusätzliche Speicherkapazität, die durch den Snapshot verbraucht wird, nicht dazu führen, dass das Volume SSD-Storage-Auslastung von über 98 % überschreitet. In diesem Fall schlägt die Sicherung fehl.

Schritte

1. Melden Sie sich mit einem der "Konsolenerfahrungen" an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Speichermenü **FSx für ONTAP** aus.
4. Wählen Sie in **FSx for ONTAP** das Aktionsmenü des Dateisystems mit dem Volume und wählen Sie dann **Verwalten**.
5. Wählen Sie in der Dateisystemübersicht die Registerkarte **Volumes** aus.
6. Wählen Sie auf der Registerkarte **Volumes** das Aktionsmenü für das zu sichernde Volume aus.
7. Wählen Sie **Data Protection Actions, FSX for ONTAP Backup** und dann **Manual Backup**.
8. Geben Sie im Dialogfeld Manuelle Sicherung einen Namen für das Backup ein.
9. Wählen Sie **Backup**.

Wiederherstellen eines Volumes aus einer Sicherung in NetApp Workload Factory

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

Workload Factory legt fest, ob Sie über genügend Kapazität für die Wiederherstellung verfügen, und kann automatisch SSD-Speicher-Tier-Kapazität hinzufügen, wenn nicht.

Schritte

1. Melden Sie sich mit einem der "Konsolenerfahrungen" an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Speichermenü **FSx für ONTAP** aus.
4. Wählen Sie in **FSx for ONTAP** das Aktionsmenü des Dateisystems mit dem Volume und wählen Sie dann **Verwalten**.
5. Wählen Sie in der Dateisystemübersicht die Registerkarte **Volumes** aus.
6. Wählen Sie auf der Registerkarte **Volumes** das Aktionsmenü für das Volume aus, das aus einer Sicherung wiederhergestellt werden soll.
7. Wählen Sie **Data Protection Actions, FSX for ONTAP Backup** und dann **Restore from a Backup**.
8. Geben Sie im Dialogfeld Wiederherstellen von einem Backup Folgendes an:
 - a. **Zieldateisystem**: Wählen Sie das Zieldateisystem aus dem Dropdown-Menü aus.
 - b. **Ziel-Speicher-VM**: Wählen Sie die Ziel-Speicher-VM aus dem Dropdown-Menü.
 - c. **Sicherungsname**: Wählen Sie den Sicherungsnamen aus dem Dropdown-Menü.
 - d. **Name des wiederhergestellten Volumes**: Geben Sie den Namen des wiederhergestellten Volumes ein.
9. Überprüfen Sie die Dateisystemkapazität für den Wiederherstellungsvorgang.

Wenn die Kapazität des Dateisystems begrenzt ist, kann Folgendes auftreten:

- Durch die Wiederherstellung kann die genutzte Kapazität den von Ihnen angegebenen Schwellenwert überschreiten. Sie können den Wiederherstellungsvorgang abschließen. In Betracht ziehen "[Manuelles Hinzufügen von SSD-Storage-Tier-Kapazität](#)" oder wählen Sie „Workload Factory“ aus, um automatisch SSD-Speicherebenenkapazität hinzuzufügen.

- Die Wiederherstellung erfordert zusätzliche SSD-Kapazität. Um fortzufahren, müssen Sie für Workload Factory auswählen, dass automatisch SSD-Speicherebenenkapazität hinzugefügt wird.

10. Wählen Sie **Wiederherstellen**.

Verwenden der Replikation

Erstellen einer Replikationsbeziehung in NetApp Workload Factory

Erstellen Sie eine Replikationsbeziehung für ein FSx for ONTAP-Dateisystem in NetApp Workload Factory, um Datenverlust im Falle einer unvorhergesehenen Katastrophe zu vermeiden. Die Replikation wird zwischen zwei FSx for ONTAP-Dateisystemen sowie zwischen einem lokalen ONTAP-System und einem FSx for ONTAP-Dateisystem unterstützt.

Über diese Aufgabe

Die Replikation schützt Ihre Daten, wenn eine Katastrophe Ihre Region betrifft.

Dieser Vorgang erstellt eine Replikationsbeziehung für Quellvolumes in einem FSx for ONTAP File System oder einem On-Premises ONTAP System.

Replizierte Volumes im Zielsystem sind Datensicherungs-Volumes (DP) und folgen dem Namensformat: {OriginalVolumeName}_copy.

Wenn Sie ein Quell-Volume mit unveränderlichen Dateien replizieren, bleiben das Ziel-Volume und das Dateisystem gesperrt, bis die Aufbewahrungsfrist der unveränderlichen Dateien im Quell-Volume endet. Die Funktion für unveränderliche Dateien ist verfügbar, wenn Sie ["Erstellen Sie ein Volume"](#) für ein FSx for ONTAP-Dateisystem.

-  • Die Replikation wird für Block-Volumes mit iSCSI- oder NVMe-Protokollen nicht unterstützt.
- Sie können ein Quell-Volume (Lese-/Schreibvorgänge) oder ein Datensicherungs-Volume replizieren. Eine kaskadierende Replikation wird unterstützt, ein dritter Hop aber nicht. Erfahren Sie mehr über ["Kaskadierende Replizierung"](#).

Bevor Sie beginnen

Überprüfen Sie diese Anforderungen, bevor Sie beginnen.

- Sie müssen über ein FSx for ONTAP-Dateisystem verfügen, das als Ziel in der Replikationsbeziehung verwendet wird.
- Das FSx for ONTAP-Dateisystem, das Sie für die Replikationsbeziehung verwenden, muss über eine zugeordnete Verknüpfung verfügen. ["Erfahren Sie, wie Sie einen vorhandenen Link zuordnen oder einen neuen Link erstellen und zuordnen."](#). Nachdem Sie die Verknüpfung hergestellt haben, kehren Sie zu diesem Vorgang zurück.
- Für die Datenreplizierung von einem lokalen ONTAP-System zu einem FSx for ONTAP-Dateisystem stellen Sie sicher, dass das lokale ONTAP-System erkannt wurde.

Führen Sie diese Schritte aus, um bestimmte oder alle Volumes in einem Dateisystem zu replizieren.

Schritte

1. Melden Sie sich mit einem der ["Konsolenerfahrungen"](#) an.

2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Speichermenü **FSx für ONTAP** aus.
4. Wählen Sie unter **FSx for ONTAP** das Aktionsmenü des Dateisystems aus, das die zu replizierenden Volumes enthält, und wählen Sie dann **Verwalten**.
5. Replizieren Sie entweder alle Volumes in einem Dateisystem oder replizieren Sie ausgewählte Volumes.
 - Um alle Volumes in einem Dateisystem zu replizieren: Wählen Sie in der Dateisystemübersicht **Daten replizieren**.
 - Um ausgewählte Volumes zu replizieren: Wählen Sie in der Dateisystemübersicht die Registerkarte **Volumes** aus.

Wählen Sie in der Tabelle Volumes ein oder mehrere Volumes aus und wählen Sie dann **Daten replizieren** aus.
6. Geben Sie auf der Seite Daten replizieren unter Replikationsziel Folgendes an:
 - a. **Anwendungsfall:** Wählen Sie einen der folgenden Anwendungsfälle für die Replikation aus. Abhängig vom ausgewählten Anwendungsfall füllt Workload Factory das Formular gemäß Best Practices mit empfohlenen Werten aus. Sie können die empfohlenen Werte akzeptieren oder beim Ausfüllen des Formulars Änderungen vornehmen.
 - Migration: Überträgt Ihre Daten an das Ziel-FSX für ONTAP-Filesystem
 - Hot Disaster Recovery: Hohe Verfügbarkeit und schnelles Disaster Recovery für kritische Workloads
 - Disaster Recovery in kalten oder archivierten Daten:
 - Cold Disaster Recovery: Verwendet längere Recovery-Zeitvorgaben (RTO) und Recovery-Zeitpunkte (RPO) zur Senkung der Kosten
 - Archiv: Replizierung von Daten für langfristige Speicherung und Compliance
 - Sonstiges

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

- Für die Migration und andere wird die Replikationsrichtlinie *MirrorAll/Snapshots* genannt. *MirrorAll/Snapshots* ist eine asynchrone Richtlinie zur Spiegelung aller Snapshots und des aktuellen aktiven Dateisystems.
- Für Disaster Recovery mit heißen, kalten oder archivierten Daten wird die Replikationsrichtlinie *MirrorAndVault* genannt. *MirrorAndVault* ist eine asynchrone und Vault-Richtlinie zur Spiegelung des neuesten aktiven Dateisystems und der täglichen und wöchentlichen Snapshots.

Wenn Sie Snapshots für die langfristige Aufbewahrung aktivieren, lautet die standardmäßige Replikationsrichtlinie für alle Anwendungsfälle *MirrorAndVault*.

- b. * FSX für ONTAP Dateisystem*: Wählen Sie Anmeldeinformationen, Region und FSX für ONTAP Dateisystem Namen für das Ziel FSX für ONTAP Dateisystem.
- c. **Name der Speicher-VM:** Wählen Sie die Speicher-VM aus dem Dropdown-Menü aus. Die von Ihnen ausgewählte Speicher-VM ist das Ziel für alle ausgewählten Volumes in dieser Replikationsbeziehung.

- d. **Volumenname:** Der Name des Zielvolume wird automatisch im folgenden Format generiert `{OriginalVolumeName}_copy`. Sie können den automatisch generierten Volume-Namen verwenden oder einen anderen Volume-Namen eingeben.
- e. **Tiering Policy:** Wählen Sie die Tiering Policy für die auf dem Ziel-Volume gespeicherten Daten. Die Tiering-Richtlinie wird standardmäßig auf die empfohlene Tiering-Richtlinie für den ausgewählten Anwendungsfall zurückgesetzt.

Ausgeglichen (Auto) ist die Standard-Tiering-Richtlinie beim Erstellen eines Volumes mit der Workload Factory-Konsole. Weitere Informationen zu Volume-Tiering-Richtlinien finden Sie unter "[Speicherkapazität für Volumes](#)" in der AWS FSx für NetApp ONTAP -Dokumentation. Beachten Sie, dass Workload Factory in der Workload Factory-Konsole anwendungsbasierte Namen für Tiering-Richtlinien verwendet und FSx für ONTAP -Tiering-Richtliniennamen in Klammern einschließt.

Wenn Sie den Migrationsanwendungsfall ausgewählt haben, wählt Workload Factory automatisch aus, dass die Tiering-Richtlinie des Quellvolumes auf das Zielvolume kopiert werden soll. Sie können die Option zum Kopieren der Tiering-Richtlinie deaktivieren und eine Tiering-Richtlinie auswählen, die für das für die Replikation ausgewählte Volume gilt.

- a. **Max. Übertragungsrate:** Wählen Sie **Limited** und geben Sie die maximale Übertragungsgrenze in MB/s. ein Alternativ wählen Sie **Unlimited**.

Ohne Einschränkung kann die Netzwerk- und Anwendungsleistung abnehmen. Alternativ empfehlen wir eine unbegrenzte Übertragungsrate für die Dateisysteme FSX for ONTAP für kritische Workloads, zum Beispiel solche, die primär für die Disaster Recovery genutzt werden.

7. Geben Sie unter Replikationseinstellungen Folgendes an:

- a. **Replikationsintervall:** Wählen Sie die Häufigkeit, mit der Snapshots vom Quell-Volume auf das Ziel-Volume übertragen werden.
- b. **Langfristige Aufbewahrung:** Optional können Snapshots für die langfristige Aufbewahrung aktiviert werden. Dank der langfristigen Aufbewahrung können Business-Services auch bei einem vollständigen Standortausfall weiterlaufen und Applikationen mithilfe einer sekundären Kopie einen transparenten Failover unterstützen.

Replikationen ohne langfristige Aufbewahrung verwenden die Richtlinie *MirrorAllS snapshots*. Durch Aktivieren der langfristigen Aufbewahrung wird der Replikation die Richtlinie *MirrorAndVault* zugewiesen.

Wenn Sie die langfristige Aufbewahrung aktivieren, wählen Sie eine vorhandene Richtlinie aus, oder erstellen Sie eine neue Richtlinie, um die zu replizierenden Snapshots und die Anzahl der beizubehaltenden Snapshots zu definieren.



Zur langfristigen Aufbewahrung sind passende Quell- und Zieldatenetiketten erforderlich. Auf Wunsch kann Workload Factory fehlende Etiketten für Sie erstellen.

- **Wählen Sie eine vorhandene Richtlinie:** Wählen Sie eine vorhandene Richtlinie aus dem Dropdown-Menü aus.
 - **Neue Richtlinie erstellen:** Geben Sie einen **Richtliniennamen** ein.
- c. **Unveränderliche Snapshots:** Optional. Wählen Sie **Enable Immanable Snapshots** aus, um zu verhindern, dass in dieser Richtlinie ergriffene Snapshots während des Aufbewahrungszeitraums gelöscht werden.
- Legen Sie die **Aufbewahrungsfrist** in Stunden, Tagen, Monaten oder Jahren fest.

- **Snapshot-Richtlinien:** Wählen Sie in der Tabelle die Snapshot-Policy-Häufigkeit und die Anzahl der zu haltenden Kopien aus. Sie können mehrere Snapshot-Richtlinien auswählen.
- d. **S3-Zugriffspunkt:** Optional kann ein S3-Zugriffspunkt angehängt werden, um über AWS S3-APIs auf FSx for ONTAP -Dateisystemdaten zuzugreifen, die sich auf NFS- oder SMB/CIFS-Volumes befinden. Es wird nur der Dateizugriffstyp unterstützt. Bitte geben Sie folgende Details an:
 - **Name des S3-Zugangspunkts:** Geben Sie den Namen des S3-Zugangspunkts ein.
 - **Benutzer:** Wählen Sie einen vorhandenen Benutzer mit Zugriff auf das Volume aus oder erstellen Sie einen neuen Benutzer.
 - **Benutzertyp:** Wählen Sie als Benutzertyp **UNIX** oder **Windows** aus.
 - **Netzwerkkonfiguration:** Wählen Sie **Internet** oder **Virtual private cloud (VPC)**. Der von Ihnen gewählte Netzwerktyp bestimmt, ob der Zugangspunkt aus dem Internet erreichbar ist oder auf eine bestimmte VPC beschränkt ist.
 - **Metadaten aktivieren:** Durch die Aktivierung von Metadaten wird eine S3-Tabelle erstellt, die alle über den S3-Zugangspunkt zugänglichen Objekte enthält, die Sie für Audits, Governance, Automatisierung, Analyse und Optimierung verwenden können. Die Aktivierung von Metadaten verursacht zusätzliche AWS-Kosten. Weitere Informationen finden Sie unter "[Amazon S3 Preisdokumentation](#)".

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

8. Wählen Sie **Erstellen**.

Ergebnis

Die Replikationsbeziehung wird auf der Registerkarte **Replikationsbeziehungen** im Ziel-FSX für ONTAP-Dateisystem angezeigt.

Initialisieren einer Replikationsbeziehung in NetApp Workload Factory

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

Über diese Aufgabe

Die Initialisierung führt einen *Baseline* Transfer durch: Es erstellt einen Snapshot des Quell-Volumes und überträgt dann den Snapshot und alle Datenblöcke, die es auf das Ziel-Volume verweist.

Bevor Sie beginnen

Denken Sie daran, wenn Sie diesen Vorgang abschließen möchten. Initialisierung kann sehr zeitaufwendig sein. Möglicherweise möchten Sie den Basistransfer in Zeiten geringerer Auslastung durchführen.

Schritte

1. Melden Sie sich mit einem der "[Konsolenerfahrungen](#)" an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Speichermenü **FSx für ONTAP** aus.
4. Wählen Sie in **FSx for ONTAP** das Aktionsmenü des zu aktualisierenden Dateisystems und dann **Verwalten**.
5. Wählen Sie in der Dateisystemübersicht die Registerkarte **Replikationsbeziehungen** aus.
6. Wählen Sie auf der Registerkarte „Replikationsbeziehungen“ das Aktionsmenü der zu initialisierenden Replikationsbeziehung aus.

7. Wählen Sie **Initialisieren**.

8. Wählen Sie im Dialogfeld Beziehung initialisieren die Option **Initialisieren** aus.

Schützen Sie Ihre Daten mit NetApp Autonomous Ransomware Protection mit KI

Schützen Sie Ihre Daten mit NetApp Autonomous Ransomware Protection mit KI (ARP/AI), einer Funktion, die Workload-Analysen in NAS-Umgebungen (NFS/SMB) nutzt, um ungewöhnliche Aktivitäten zu erkennen und davor zu warnen, die auf einen Ransomware-Angriff hindeuten könnten. Bei Verdacht auf einen Angriff erstellt ARP/AI außerdem neue, unveränderliche Snapshots, aus denen Sie Ihre Daten wiederherstellen können.

Über diese Aufgabe

Verwenden Sie ARP/AI zum Schutz vor Denial-of-Service-Angriffen, bei denen der Angreifer Daten zurückhält, bis ein Lösegeld gezahlt wird. ARP/AI bietet Ransomware-Erkennung in Echtzeit basierend auf:

- Identifizierung der eingehenden Daten als verschlüsselt oder als Klartext.
- Analysen, die Folgendes erkennen:
 - **Entropie**: Eine Auswertung der Zufälligkeit der Daten in einer Datei
 - **Dateierweiterungstypen**: Eine Erweiterung, die nicht dem normalen Erweiterungstyp entspricht
 - **Datei-IOPS**: Ein Anstieg der abnormalen Volume-Aktivität mit Datenverschlüsselung

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

Die ARP/AI-Funktion wird automatisch entsprechend der ONTAP -Version aktualisiert, die Amazon FSx for NetApp ONTAP ausführt, sodass Sie keine manuellen Updates durchführen müssen.

Lernen und aktive Modi

ARP/AI arbeitet zunächst im *Lernmodus* und wechselt dann automatisch in den *aktiven Modus*.

- **Lernmodus**: Wenn Sie ARP/AI aktivieren, läuft es im *Lernmodus*. Im Lernmodus entwickelt das FSx for ONTAP -Dateisystem ein Warnprofil basierend auf den Analysebereichen: Entropie, Dateierweiterungstypen und Datei-IOPS. Nachdem das Dateisystem ARP/AI lange genug im Lernmodus ausgeführt hat, um die Workload-Eigenschaften zu beurteilen, wechselt Workload Factory automatisch zu ARP/AI in den *aktiven Modus* und beginnt mit dem Schutz Ihrer Daten.
- **Aktivmodus**: Nachdem ARP/AI in den *aktiven Modus* gewechselt ist, erstellt FSx for ONTAP ARP/AI-Snapshots, um die Daten zu schützen, falls eine Bedrohung erkannt wird.

Wenn im aktiven Modus eine Dateierweiterung als abnormal gekennzeichnet ist, sollten Sie die Warnmeldung auswerten. Sie können auf die Warnung reagieren, um Ihre Daten zu schützen, oder Sie können die Warnung als falsch positiv markieren. Wenn Sie eine Warnung als falsch positiv markieren, wird das Warnungsprofil aktualisiert. Wenn die Warnmeldung beispielsweise durch eine neue Dateierweiterung ausgelöst wird und Sie die Warnmeldung als falsch positiv markieren, erhalten Sie beim nächsten Mal keine Warnmeldung, wenn diese Dateierweiterung beobachtet wird.

FlexVol Volumes, die ein Blockgerät enthalten, starten ARP/AI im aktiven Modus.

Nicht unterstützte Konfigurationen

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

- iSCSI-Volumes
- NVMe Volumes

Aktivieren Sie ARP/AI für ein Dateisystem oder ein Volume

Durch die Aktivierung von ARP/AI für ein Dateisystem wird automatisch Schutz für alle vorhandenen NAS- und neu erstellten NAS-Volumes (NFS/SMB) hinzugefügt. Sie können ARP/AI auch für einzelne Volumes aktivieren.

Wenn nach der Aktivierung von ARP/AI ein Angriff stattfindet und Sie feststellen, dass es sich um einen echten Angriff handelt, richtet Workload Factory automatisch eine Snapshot-Richtlinie ein, die alle vier Stunden bis zu sechs Snapshots erstellt. Jeder Snapshot ist 2–5 Tage lang gesperrt.

Bevor Sie beginnen

Um ARP/AI für ein Dateisystem oder ein Volume zu aktivieren, müssen Sie einen Link zuordnen. ["Erfahren Sie, wie Sie einen vorhandenen Link zuordnen oder einen neuen Link erstellen und zuordnen."](#) . Kehren Sie nach der Verknüpfung zu diesem Vorgang zurück.

Aktivieren Sie ARP/AI für ein Dateisystem

Schritte

1. Melden Sie sich mit einem der ["Konsolenerfahrungen"](#) an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Speichermenü **FSx für ONTAP** aus.
4. Wählen Sie in **FSx for ONTAP** das Aktionsmenü des Dateisystems aus, um ARP/AI zu aktivieren, und wählen Sie dann **Verwalten**.
5. Wählen Sie unter „Informationen“ das Stiftsymbol neben „Autonomer Ransomware-Schutz“ aus. Das Stiftsymbol wird neben dem Pfeil angezeigt, wenn Sie mit der Maus über die Zeile **Autonomous Ransomware Protection** fahren.
6. Führen Sie auf der Seite „NetApp Autonomous Ransomware Protection with AI (ARP/AI)“ die folgenden Schritte aus:
 - a. Aktivieren oder deaktivieren Sie die Funktion.
 - b. **Automatische Snapshot-Erstellung**: Wählen Sie die maximale Anzahl der aufzubewahrenen Snapshots und das Zeitintervall zwischen der Erstellung der Snapshots. Der Standardwert beträgt 6 Snapshots alle 4 Stunden.
 - c. **Unveränderliche Snapshots**: Wählen Sie die Standardaufbewahrungsdauer in Stunden und die maximale Anzahl von Tagen für die Aufbewahrung unveränderlicher Snapshots. Aktivieren Sie diese Option, um sicherzustellen, dass Snapshots erst gelöscht oder geändert werden können, wenn der angegebene Aufbewahrungszeitraum abgelaufen ist.
 - d. **Erkennung**: Wählen Sie optional einen der folgenden Parameter aus, um automatisch zu scannen und Anomalien zu erkennen.
7. Akzeptieren Sie die Aussage, um fortzufahren.
8. Wählen Sie **Übernehmen**, um die Änderungen zu speichern.

ARP/AI für ein Volume aktivieren

Schritte

1. Melden Sie sich mit einem der ["Konsolenerfahrungen"](#) an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Speichermenü **FSx für ONTAP** aus.
4. Wählen Sie in **FSx for ONTAP** das Aktionsmenü des Dateisystems aus, um ARP/AI zu aktivieren, und wählen Sie dann **Verwalten**.
5. Wählen Sie auf der Registerkarte „Volumes“ das Aktionsmenü des Volumes aus, um ARP/AI zu aktivieren, dann **Datenschutzaktionen** und dann **ARP/AI verwalten**.
6. Führen Sie im Dialogfeld „ARP/AI verwalten“ die folgenden Schritte aus:
 - a. Aktivieren oder deaktivieren Sie die Funktion.
 - b. **Erkennung**: Wählen Sie optional einen der folgenden Parameter aus, um automatisch zu scannen und Anomalien zu erkennen.
7. Akzeptieren Sie die Aussage, um fortzufahren.
8. Wählen Sie **Übernehmen**, um die Änderungen zu speichern.

Ransomware-Angriffe validieren

Ermitteln Sie, ob ein Angriff ein falscher Alarm oder ein echter Ransomware-Vorfall ist.

Schritte

1. Melden Sie sich mit einem der "Konsolenerfahrungen" an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Speichermenü **FSx für ONTAP** aus.
4. Wählen Sie unter **FSx for ONTAP** das Dateisystem aus, für das Ransomware-Angriffe validiert werden sollen.
5. Wählen Sie in der Dateisystemübersicht die Registerkarte **Volumes** aus.
6. Wählen Sie aus der Kachel Autonomous Ransomware Protection **Analyze Attacks** aus.
7. Laden Sie den Bericht über Angriffsereignisse herunter, um zu überprüfen, ob Dateien oder Ordner kompromittiert wurden, und entscheiden Sie dann, ob ein Angriff stattgefunden hat.
8. Wenn kein Angriff stattgefunden hat, wählen Sie **False Alarm** für die Lautstärke in der Tabelle und wählen Sie dann **Schließen**.
9. Wenn ein Angriff stattgefunden hat, wählen Sie **Real Attack** für das Volumen in der Tabelle. Das Dialogfeld „kompromittierte Volume-Daten wiederherstellen“ wird geöffnet. Sie können sofort mit fortfahren **Stellen Sie Ihre Daten wieder her** oder **Schließen** auswählen und später den Wiederherstellungsprozess abschließen.

Wiederherstellung von Daten nach einem Ransomware-Angriff

Wenn ein Angriff vermutet wird, erstellt das System zu diesem Zeitpunkt einen Volume-Snapshot und sperrt diese Kopie. Sollte sich der Angriff später bestätigen, können die betroffenen Dateien oder das gesamte Volume mithilfe des ARP/AI-Snapshots wiederhergestellt werden.

Gesperzte Snapshots können erst gelöscht werden, wenn die Aufbewahrungsfrist endet. Wenn Sie sich jedoch später entscheiden, den Angriff als falsch positiv zu markieren, wird die gesperrte Kopie gelöscht.

Mit dem Wissen über die betroffenen Dateien und dem Zeitpunkt des Angriffs ist es möglich, die betroffenen Dateien selektiv aus verschiedenen Snapshots wiederherzustellen, anstatt das gesamte Volume einfach auf einen der Snapshots zurückzugreifen.

Schritte

1. Melden Sie sich mit einem der "Konsolenerfahrungen" an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Speichermenü **FSx für ONTAP** aus.
4. Wählen Sie unter **FSx for ONTAP** das Dateisystem aus, für das Daten wiederhergestellt werden sollen.
5. Wählen Sie in der Dateisystemübersicht die Registerkarte **Volumes** aus.
6. Wählen Sie aus der Kachel Autonomous Ransomware Protection **Analyze Attacks** aus.
7. Wenn ein Angriff stattgefunden hat, wählen Sie **Real Attack** für das Volumen in der Tabelle.
8. Befolgen Sie im Dialogfeld „kompromittierte Volume-Daten wiederherstellen“ die Anweisungen zur Wiederherstellung auf Datei- oder Volume-Ebene. In den meisten Fällen stellen Sie Dateien statt eines gesamten Volumes wieder her.
9. Nachdem Sie die Wiederherstellung abgeschlossen haben, wählen Sie **Schließen**.

Ergebnis

Die kompromittierten Daten wurden wiederhergestellt.

Klonen eines Volumes in NetApp Workload Factory

Klonen Sie ein Volume in NetApp Workload Factory, um zum Testen ein Lese-/Schreibvolume des Originalvolumes zu erstellen.

Der Klon gibt den aktuellen Point-in-Time-Zustand der Daten wieder. Darüber hinaus können Klone verwendet werden, um zusätzlichen Benutzern Zugriff auf Daten zu gewähren, ohne dass diese auf Produktionsdaten zugreifen müssen.

Über diese Aufgabe

Das Klonen von Volumes wird nur für FlexClone Volumes unterstützt.

Wenn ein Volume geklont wird, wird ein beschreibbares Volume mit Referenzen zu Snapshots vom übergeordneten Volume erstellt. Die Klonerstellung erfolgt in Sekunden. Die geklonten Daten befinden sich nicht auf dem Volume-Klon, sondern befinden sich auf dem übergeordneten Volume. Alle neuen Daten, die nach der Klonerstellung auf das Volume geschrieben werden, verbleiben im Klon.

Damit ein geklontes Volume alle Daten des übergeordneten Volume und alle neuen Daten, die nach der Erstellung dem Klon hinzugefügt werden, enthält, ist das übergeordnete Volume erforderlich ["Teilen Sie den Klon auf"](#). Außerdem können Sie ein übergeordnetes Volume nicht löschen, wenn es über einen Klon verfügt. Ein Klon muss aufgeteilt werden, bevor ein übergeordnetes Volume gelöscht werden kann.

Schritte

1. Melden Sie sich mit einem der ["Konsolenerfahrungen"](#) an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Speichermenü **FSx für ONTAP** aus.
4. Wählen Sie unter **FSx for ONTAP** das Aktionsmenü des FSx for ONTAP -Dateisystems aus, das das zu klonende Volume enthält, und wählen Sie dann **Verwalten**.
5. Wählen Sie auf der Registerkarte Übersicht des Dateisystems die Registerkarte **Volumes** aus.
6. Wählen Sie auf der Registerkarte „Volumes“ das Aktionsmenü des zu klonenden Volumes aus.
7. Wählen Sie **Data Protection actions** und dann **Clone Volume**.
8. Geben Sie im Dialogfeld Volume klonen einen Namen für den Volume-Klon ein.
9. Wählen Sie **Clone**.

Verwenden Sie lokale ONTAP Clusterdaten in NetApp Workload Factory

Entdecken und replizieren Sie lokale ONTAP -Daten in NetApp Workload Factory, damit diese zur Anreicherung von KI-Wissensdatenbanken verwendet werden können.

Über diese Aufgabe

Um Daten aus einem lokalen ONTAP Cluster zu verwenden, müssen Sie zuerst den lokalen ONTAP Cluster erkennen. Nach der Erkennung eines lokalen ONTAP-Clusters können Sie die Daten für jeden der folgenden Anwendungsfälle verwenden:

Anwendungsfälle

Beachten Sie, dass der primäre Anwendungsfall für den GenAI-Workload der Schwerpunkt dieser Aufgabenreihe ist.

- **GenAI-Workload:** Replizieren Sie On-Premises-ONTAP-Volume-Daten auf ein FSX for ONTAP-Dateisystem, damit die Daten für verwendet werden können "[Verbesserte KI-Wissensdatenbanken](#)".
- **Backup und Migration in die Cloud:** Replizierte On-Premises-ONTAP-Volume-Daten auf einem FSX für ONTAP-Dateisystem können als Backup in der Cloud verwendet werden.
- **Daten-Tiering:** Nach der Replizierung können selten verwendete Daten auf dem lokalen ONTAP-Volume vom SSD-Storage-Tier auf das Storage-Tier des Kapazitäts-Pools verschoben werden.

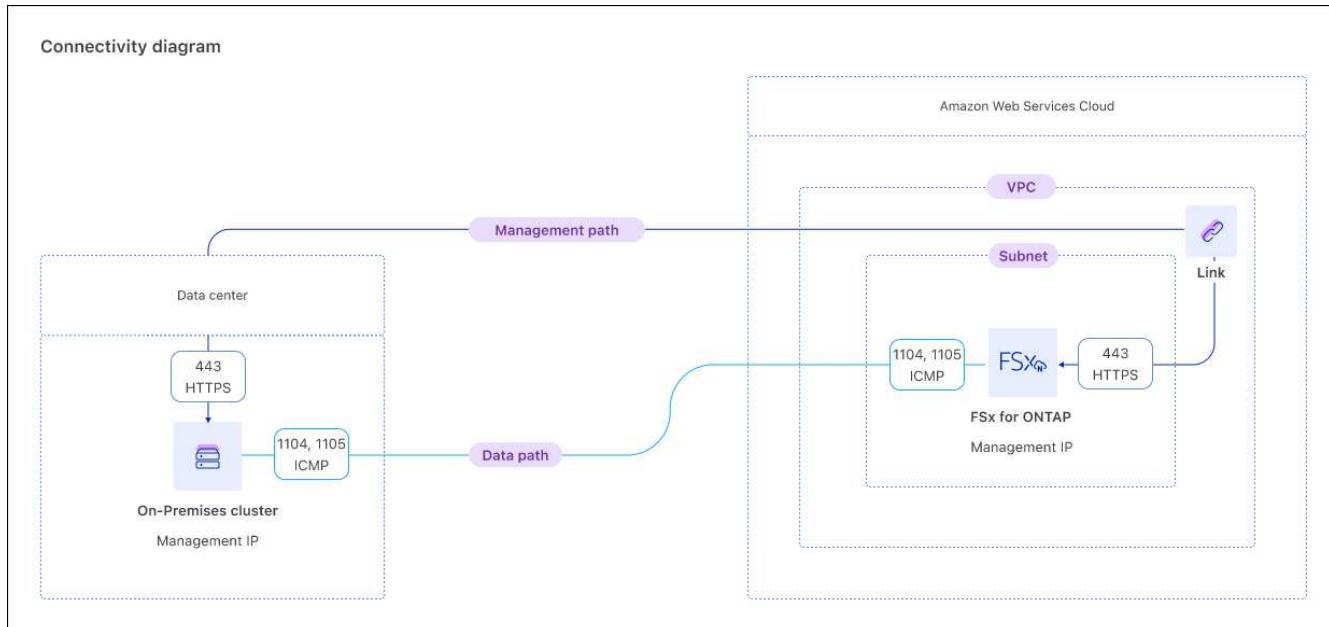
Ermitteln eines lokalen ONTAP Clusters

Entdecken Sie einen lokalen ONTAP Cluster in NetApp Workload Factory, damit Sie die Daten auf ein Amazon FSx for NetApp ONTAP Dateisystem replizieren können.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie Folgendes haben, bevor Sie beginnen:

- Ein FSX für ONTAP-Dateisystem für die Replikation.
- Eine verbundene Verbindung, die mit dem ermittelten On-Premises-Cluster verknüpft wird. Wenn Sie keinen Link haben, müssen Sie "[Erstellen Sie eine](#)".
- ONTAP-Benutzeranmeldeinformationen mit erforderlichen Berechtigungen.
- On-Premises-ONTAP Version 9.8 und höher
- Anschlussmöglichkeiten wie in der folgenden Abbildung dargestellt.



Schritte

1. Melden Sie sich mit einem der "[Konsolenerfahrungen](#)" an.
2. Wählen Sie das Menü aus und wählen Sie dann **Speicher** aus.

3. Wählen Sie die Registerkarte **On-Premise ONTAP**.
4. Wählen Sie * Entdecken*.
5. Überprüfen Sie die Voraussetzungen und wählen Sie **Weiter**.
6. Geben Sie auf der Seite ONTAP vor Ort ermitteln unter **Clusterkonfiguration** Folgendes ein:
 - a. **Link**: Wählen Sie einen Link aus. Der Link wird mit dem lokalen Cluster verknüpft, um eine Konnektivität zwischen dem Cluster und Workload Factory herzustellen.

Wenn Sie keinen Link erstellt haben, folgen Sie den Anweisungen, kehren Sie zu diesem Vorgang zurück, und wählen Sie den Link aus.
 - b. **Cluster-IP-Adresse**: Geben Sie die IP-Adresse für den lokalen ONTAP-Cluster an, der repliziert werden soll.
 - c. **ONTAP Credentials**: Geben Sie die ONTAP Credentials für den On-Premises ONTAP Cluster ein. Stellen Sie sicher, dass der Benutzer über die erforderlichen Berechtigungen verfügt.
7. Wählen Sie **Discover**, um den Erkennungsvorgang zu starten.

Ergebnis

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

Sie können jetzt die Daten in Ihrem lokalen ONTAP-Cluster und anzeigen [Replizieren Sie die Daten in ein FSX für ONTAP-Dateisystem](#).

Volume-Daten aus einem lokalen ONTAP Cluster replizieren

Replizieren von Volume-Daten von einem lokalen ONTAP-Cluster zu einem FSX für ONTAP Filesystem. Nach der Replizierung können diese Daten zur Erweiterung von KI-Wissensdatenbanken verwendet werden.

Bevor Sie beginnen

- Sie müssen ein On-Premises-ONTAP-Cluster erkennen, um seine Volume-Daten zu replizieren.
- Sie müssen über ein verfügbares FSX für ONTAP-Dateisystem verfügen, um das Ziel für die Replikation zu sein.
- Sowohl dem On-Premises-ONTAP-Cluster als auch dem für die Replikationsbeziehung verwendeten FSX für ONTAP-Dateisystem muss ein Link zugeordnet sein. ["Erfahren Sie, wie Sie einen vorhandenen Link zuordnen oder einen neuen Link erstellen und zuordnen."](#). Kehren Sie nach dem Verknüpfen zu diesem Vorgang zurück.

Schritte

1. Melden Sie sich mit einem der ["Konsolenerfahrungen"](#) an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Speichermenü **On-Premises ONTAP** aus.
4. Um Volumes nach Storage VM zu finden, können Sie **Storage VM** aus der Dropdown-Liste auswählen.
5. Wählen Sie ein oder mehrere Volumes aus, die repliziert werden sollen, und wählen Sie dann **replicate** aus.
6. Geben Sie auf der Seite Replikation erstellen unter Replikationsziel Folgendes an:
 - a. * FSX für ONTAP Dateisystem*: Wählen Sie Anmeldeinformationen, Region und FSX für ONTAP Dateisystem Namen für das Ziel FSX für ONTAP Dateisystem.

- b. **Name der Speicher-VM:** Wählen Sie die Speicher-VM aus dem Dropdown-Menü aus.
- c. **Volumenname:** Der Name des Zielvolume wird automatisch im folgenden Format generiert {OriginalVolumeName}_copy. Sie können den automatisch generierten Volume-Namen verwenden oder einen anderen Volume-Namen eingeben.
- d. **Tiering-Daten:** Wählen Sie die Tiering-Richtlinie für die im Ziel-Volume gespeicherten Daten.
 - **Auto:** Die Standard-Tiering-Richtlinie beim Erstellen eines Volumes mithilfe der Workload Factory FSx for ONTAP -Benutzeroberfläche. Ordnet alle kalten Daten, einschließlich Benutzerdaten und Snapshots, für einen bestimmten Zeitraum der Speicherebene des Kapazitätspools zu.
 - **Nur Snapshot:** Verschiebt nur Snapshot-Daten auf den Storage Tier des Kapazitäts-Pools.
 - **Keine:** Speichert alle Daten Ihres Volumes auf dem primären Storage Tier.
 - **All:** Markiert alle Benutzerdaten und Snapshot-Daten als „kalt“ und speichert sie im Kapazitäts-Pool-Speicher-Tier.

Beachten Sie, dass einige Tiering-Richtlinien über einen zugehörigen Mindestkühlzeitraum verfügen, der die Zeit bzw. die *Kühltag*e festlegt, dass Benutzerdaten in einem Volume inaktiv bleiben müssen, damit die Daten als „kalt“ gelten und in die Storage-Ebene des Kapazitäts-Pools verschoben werden. Der Kühlzeitraum beginnt, wenn Daten auf die Festplatte geschrieben werden.

Weitere Informationen zu Volume-Tiering-Richtlinien finden Sie "[Speicherkapazität für Volumes](#)" in der Dokumentation zu AWS FSX for NetApp ONTAP.

- a. **Max. Übertragungsrate:** Wählen Sie **Limited** und geben Sie die maximale Übertragungsgrenze in MiB/s. ein Alternativ wählen Sie **Unlimited**.

Ohne Einschränkung kann die Netzwerk- und Applikations-Performance abnehmen. Alternativ empfehlen wir eine unbegrenzte Übertragungsrate für die Dateisysteme FSX for ONTAP für kritische Workloads, zum Beispiel solche, die primär für die Disaster Recovery genutzt werden.

7. Geben Sie unter Replikationseinstellungen Folgendes an:

- a. **Replikationsintervall:** Wählen Sie die Häufigkeit, mit der Snapshots vom Quell-Volume auf das Ziel-Volume übertragen werden.
- b. **Langfristige Aufbewahrung:** Optional können Snapshots für die langfristige Aufbewahrung aktiviert werden.

Wenn Sie die langfristige Aufbewahrung aktivieren, wählen Sie eine vorhandene Richtlinie aus, oder erstellen Sie eine neue Richtlinie, um die zu replizierenden Snapshots und die Anzahl der beizubehaltenden Snapshots zu definieren.

- Wählen Sie für eine vorhandene Richtlinie **vorhandene Richtlinie auswählen** aus, und wählen Sie dann die vorhandene Richtlinie aus dem Dropdown-Menü aus.
- Wählen Sie für eine neue Richtlinie **Create a New Policy** aus, und geben Sie Folgendes an:
 - **Richtliniename:** Geben Sie einen Richtliniennamen ein.
 - **Snapshot-Richtlinien:** Wählen Sie in der Tabelle die Snapshot-Policy-Häufigkeit und die Anzahl der zu haltenden Kopien aus. Sie können mehrere Snapshot-Richtlinien auswählen.

8. Wählen Sie **Erstellen**.

Ergebnis

Die Replikationsbeziehung wird auf der Registerkarte **Replikationsbeziehungen** im Ziel-FSX für ONTAP-Dateisystem angezeigt.

Entfernen eines lokalen ONTAP Clusters aus der NetApp Workload Factory

Entfernen Sie bei Bedarf einen lokalen ONTAP Cluster aus der NetApp Workload Factory.

Bevor Sie beginnen

Vor dem Entfernen des Clusters müssen Sie "["Löschen Sie alle vorhandenen Replikationsbeziehungen"](#)" alle Volumes im On-Premises-ONTAP-Cluster berücksichtigen, damit keine unterbrochenen Beziehungen mehr erhalten bleiben.

Schritte

1. Melden Sie sich mit einem der "["Konsolenerfahrungen"](#)" an.
2. Wählen Sie das Menü aus  und wählen Sie dann **Speicher** aus.
3. Wählen Sie im Speichermenü **On-Premises ONTAP** aus.
4. Wählen Sie das lokale ONTAP-Cluster aus, das entfernt werden soll.
5. Wählen Sie das Aktionsmenü und wählen Sie **Aus Workload Factory entfernen**.

Ergebnis

Der lokale ONTAP Cluster wird aus der NetApp Workload Factory entfernt.

Schützen Sie Ihre Daten mit einem Cyber-Tresor.

Ein Cyber-Vault-Volume ist ein isolierter, sicherer Speicherort, der zum Speichern von Sicherungskopien Ihrer Daten verwendet wird und diese vor Ransomware-Angriffen und anderen Cyberbedrohungen schützt. Im Rahmen der Vault-Erstellung erstellen Sie ein Cyber-Vault-Volume, deaktivieren alle Client-Protokolle, richten eine Replikationsbeziehung zwischen dem Quell-Volume und dem Cyber-Vault-Volume ein und erstellen unveränderliche Snapshots auf dem Cyber-Vault-Volume.

Was ist ein Cyber-Tresor?

Ein Cyber-Tresor ist eine spezielle Datenschutztechnik, bei der kritische Daten in einer isolierten Umgebung, getrennt von der primären IT-Infrastruktur, gespeichert werden.

Der Cyber-Tresor ist ein vom Rest des Netzwerks abgeschottetes, unveränderliches und unauslöschliches Datenrepository, das immun gegen Bedrohungen ist, die das Hauptnetzwerk betreffen, wie Malware, Ransomware oder sogar Insider-Bedrohungen. Ein Cyber-Tresor lässt sich mit unveränderlichen und unauslöschlichen Snapshots realisieren.

Bei Air-Gapping-Backups mit herkömmlichen Methoden müssen Platz geschaffen und das primäre und sekundäre Medium physisch getrennt werden. Durch die Verlagerung der Medien an einen anderen Standort und/oder die Trennung der Verbindung haben böswillige Akteure keinen Zugriff auf die Daten. Dies schützt die Daten, kann jedoch zu längeren Wiederherstellungszeiten führen.

FSx für ONTAP Cyber-Tresore

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

Durchführung

Workload Factory bietet Unterstützung bei der Erstellung einer Cyber-Vault-Architektur. Nachdem Sie NetApp kontaktiert haben, um Ihr Interesse an der Implementierung eines Cyber-Vaults zu bekunden, setzt sich ein NetApp Spezialist mit Ihnen in Verbindung, um Ihre Anforderungen zu besprechen.

Senden Sie eine E-Mail an ng-FSx-CyberVault@netapp.com, um loszulegen.

Ähnliche Informationen

Weitere Informationen zu Cyber-Tresoren und deren Einrichtung finden Sie unter: ["ONTAP Cyber Vault-Dokumentation"](#) Die

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 BESCHRÄNKKT 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 BESCHRÄNKKT 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 VERTRÄGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.