Sichern Sie Ihre Daten

Amazon FSx for NetApp ONTAP

NetApp
February 11, 2026

Inhalt

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

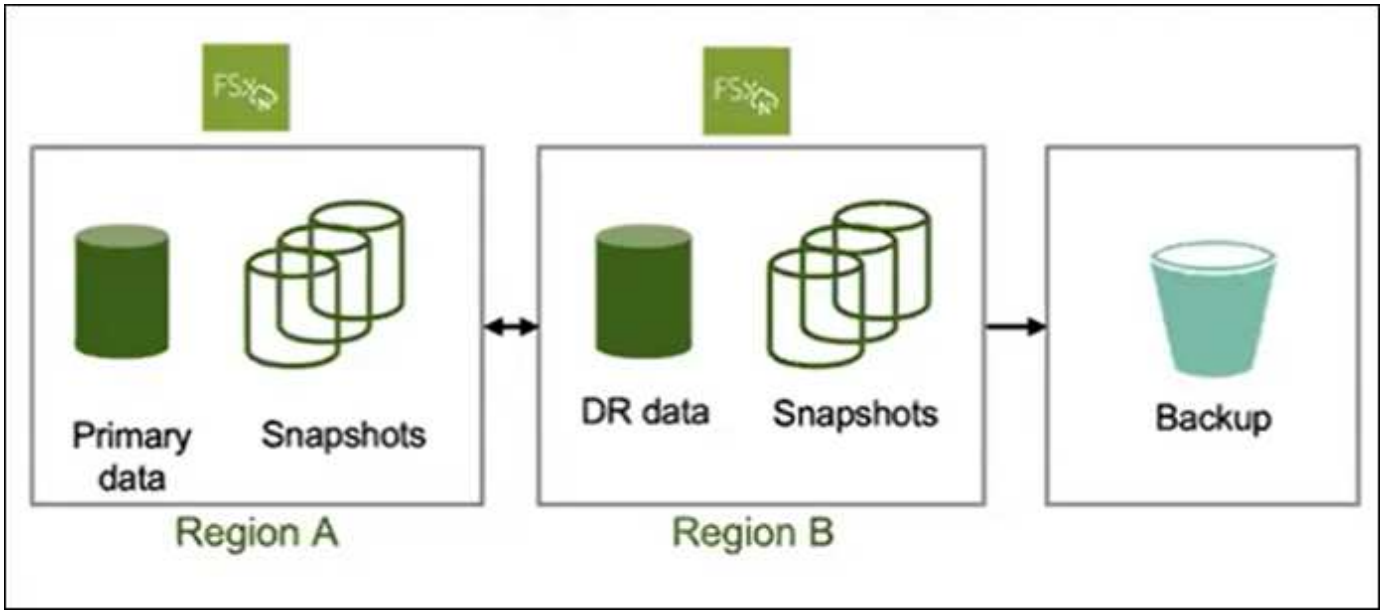
Durch Replizierung wird eine sekundäre Kopie Ihrer Daten in einem anderen FSX für ONTAP Filesystem erstellt und die sekundären Daten werden kontinuierlich aktualisiert. Ihre Daten bleiben aktuell und verfügbar, beispielsweise für Disaster Recovery.

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 wiederherzustellenden 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 Zieldateisystem 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 Zieldateisystem 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 *MirrorAllSnapshots* genannt. *MirrorAllSnapshots* 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 anwendungsfallbasierte 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 *MirrorAllSnapshots*. 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 Zieletiketten 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 anormalen 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 anormal 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 aufzubewahrenden 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 heroder **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.

Gesperrte 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.

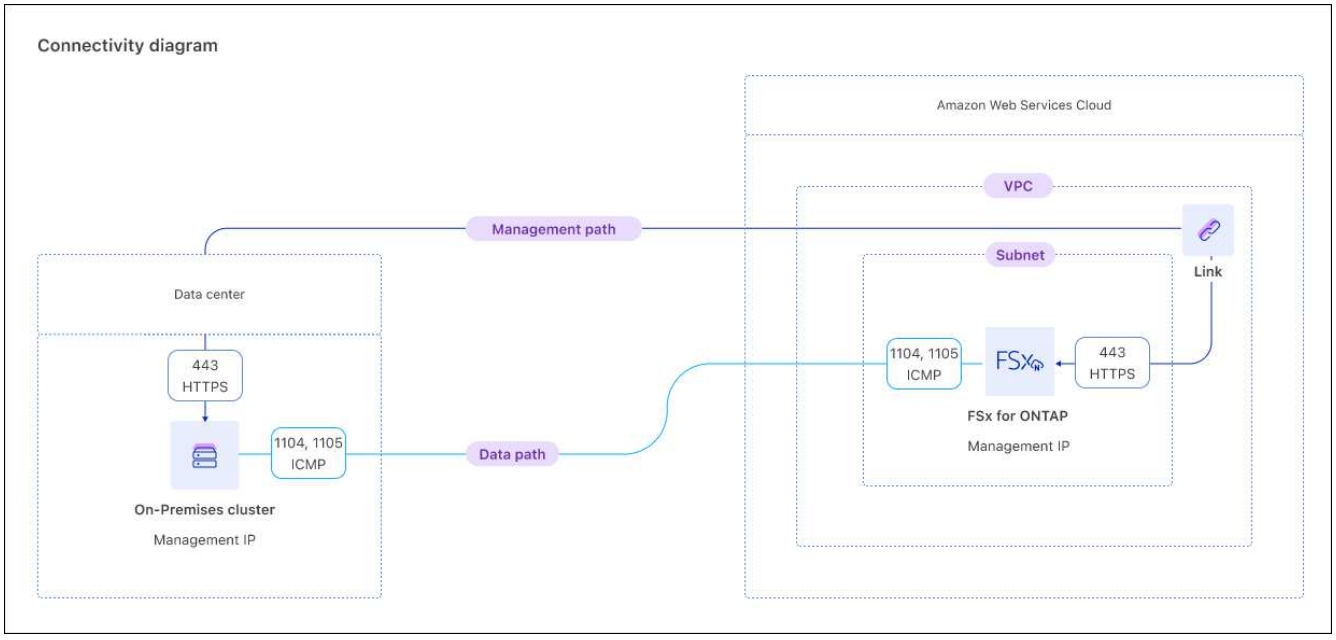
Ermitteln eines lokalen ONTAP Clusters

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 anzeigenReplizieren 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 for 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 *Kühltage* 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:
        - **Richtlinienname**: 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