



Verwalten Sie Ihre Speicher-VMs und Daten AFX

NetApp
February 10, 2026

Inhalt

Verwalten Sie Ihre Speicher-VMs und Daten	1
Daten verwalten	1
Bereiten Sie sich auf die Verwaltung Ihrer AFX-Speichersystemdaten vor	1
Erstellen und Konfigurieren eines Volumes auf einem AFX-Speichersystem	3
Verwalten der AFX-Speichersystemvolumes	4
Erstellen und Konfigurieren eines S3-Buckets auf einem AFX-Speichersystem	4
Verwalten der AFX-Speichersystem-Buckets	5
Überwachen und Fehlerbeheben eines AFX-Speichersystems	5
Daten schützen	5
Bereiten Sie sich auf den Schutz Ihrer AFX-Speichersystemdaten vor	5
Erstellen einer Konsistenzgruppe auf einem AFX-Speichersystem	6
Verwalten von Konsistenzgruppen auf einem AFX-Speichersystem	7
Erstellen eines Snapshots auf einem AFX-Speichersystem	8
Verwalten von Snapshots auf einem AFX-Speichersystem	11
Erstellen einer Intercluster-SVM-Peer-Beziehung auf einem AFX-Speichersystem	11
Verwalten der Snapshot-Replikation auf einem AFX-Speichersystem	12
Verwalten Sie Datenschutzrichtlinien und -pläne für AFX-Speichersysteme	17
Sichere Daten	19
Bereiten Sie sich auf die Sicherung Ihrer AFX-Speichersystemdaten vor	19
Verschlüsseln Sie ruhende Daten auf einem AFX-Speichersystem	19
Sichere IP-Verbindungen auf Ihren AFX-Speichersystemen	20
Zusätzliche Verwaltung für eine AFX-Speichersystem-SVM	21
Speicherverwaltung und Leistung	21
Datenschutz	22
Sicherheit	22
ONTAP Ereignis- und Leistungsüberwachung	22
Ähnliche Informationen	23

Verwalten Sie Ihre Speicher-VMs und Daten

Daten verwalten

Bereiten Sie sich auf die Verwaltung Ihrer AFX-Speichersystemdaten vor

Bevor Sie Ihre AFX-Daten verwalten, sollten Sie mit den grundlegenden Konzepten und Funktionen vertraut sein.



Da viele der auf AFF und FAS -Systemen verfügbaren Konzepte und Verwaltungsverfahren mit denen von AFX-Speichersystemen identisch sind, kann es hilfreich sein, die Unified ONTAP -Dokumentation durchzusehen. Siehe die Links in [Ähnliche Informationen](#) für weitere Informationen.

Terminologie und Optionen

Es gibt mehrere Begriffe im Zusammenhang mit AFX-Speicher, mit denen Sie vertraut sein sollten.

FlexVolume

Ein FlexVol ist ein logischer Containertyp, der in AFX-Speichersystemen verwendet wird. FlexVol -Volumes können erweitert, verkleinert, verschoben und effizient kopiert werden. Sie können außerdem mithilfe von Qtrees in besser verwaltbare Einheiten aufgeteilt und die Ressourcennutzung mithilfe von Kontingenten begrenzt werden.

FlexGroup

Ein FlexGroup -Volume ist ein Scale-Out-NAS-Container, der sowohl hohe Leistung als auch automatische Lastverteilung bietet. Jedes besteht aus mehreren Volumes, die den Datenverkehr transparent teilen. FlexGroup -Volumes bieten mehrere Vorteile, darunter verbesserte Skalierbarkeit und Leistung sowie vereinfachte Verwaltung.

FlexCache

FlexCache ist eine ONTAP Caching-Technologie, die spärliche, beschreibbare Replikate von Volumes auf demselben oder auf verschiedenen ONTAP Clustern erstellt. Es ist darauf ausgelegt, die Datenzugriffsleistung zu verbessern, indem die Daten näher an die Benutzer gebracht werden, was zu einem schnelleren Durchsatz bei geringerem Platzbedarf führen kann. FlexCache ist besonders nützlich für leseintensive Workflows und hilft, den Datenverkehr von stark beanspruchten Volumes zu entlasten.

S3-Bucket

Ein S3-Bucket ist ein Speichercontainer, der Objekte oder Daten in der Cloud enthält. Bei ONTAP ist ein S3-NAS-Bucket eine Zuordnung zwischen einem S3-Bucket-Namen und einem NAS-Pfad, wodurch S3 auf jeden Teil eines SVM-Namespaces mit vorhandenen Volumes und Verzeichnisstruktur zugreifen kann.

Datencontainer

Im Kontext eines AFX-Systems ist ein Datencontainer ein allgemeiner Begriff und kann entweder ein Volume oder ein S3-Bucket sein.

Qtree

Ein Qtree ist eine logische Unterteilung innerhalb eines Datenträgers, die Sie zum Verwalten und Organisieren von Daten erstellen können. Sie können die Eigenschaften und den Sicherheitsstil (NTFS oder UNIX) festlegen und die Exportrichtlinien des übergeordneten Volumes übernehmen oder eigene haben. Qtrees können Dateien und Verzeichnisse enthalten und werden häufig verwendet, um

Berechtigungen und Kontingente innerhalb eines Volumes detaillierter zu verwalten.

Quote

Ein Kontingent in ONTAP ist eine Begrenzung der Speicherplatzmenge oder der Anzahl der Dateien, die von einem Benutzer, einer Gruppe oder einem Qtree verwendet werden können. Kontingente werden verwendet, um die Ressourcennutzung innerhalb eines Speichersystems zu verwalten und zu steuern. So wird sichergestellt, dass kein einzelner Benutzer oder keine einzelne Anwendung eine übermäßige Menge an Ressourcen verbraucht.

NFS-Sitzungsbündelung

NFS-Trunking ist eine Technologie, die es NFS v4.1-Clients ermöglicht, mehrere Verbindungen zu verschiedenen LIFs auf dem NFS-Server zu öffnen. Dies erhöht die Datenübertragungsgeschwindigkeit und bietet Ausfallsicherheit durch mehrere Pfade beim Export von Datenmengen an Clients mit Trunking-Funktion. Die LIFs müssen sich auf demselben Knoten befinden, um am Trunk teilnehmen zu können.

Um Trunking zu aktivieren, müssen Sie eine für NFS konfigurierte SVM haben und NFSv4.1 sollte aktiviert sein. Außerdem müssen alle NFSv4.x-Clients nach einer Konfigurationsänderung neu gemountet werden, was zu Störungen führen kann. Die Support- und Konfigurationsverfahren für NFS-Trunking sind für alle ONTAP Systeme gleich. Erfahren Sie mehr über ["NFS-Trunking"](#)

Dateisystemanalyse

File System Analytics (FSA) ist eine ONTAP -Funktion, die Echtzeit-Einblicke in die Dateinutzung und Speicherkapazitätstrends innerhalb von FlexGroup oder FlexVol -Volumes bietet. Es macht externe Tools überflüssig, indem es Einblicke in die Speichernutzung und Optimierungsmöglichkeiten bietet. FSA bietet detaillierte Ansichten auf verschiedenen Ebenen der Dateisystemhierarchie eines Volumes, einschließlich der SVM-, Volume-, Verzeichnis- und Dateiebene.

Optionen zur Datenmigration

Es gibt mehrere Optionen zur Datenmigration. Der Schwerpunkt liegt auf der Migration externer Daten in einen AFX-Cluster.

Datenmigration aus AFF oder FAS Systemen

Ein vollständig integrierter Migrationspfad von AFF oder FAS Systemen (auf denen die Unified ONTAP Persönlichkeit ausgeführt wird) zu AFX ist mithilfe der folgenden Technologien verfügbar:

- SnapMirror
- SVM-Migration
- SVM DR

Darüber hinaus können FlexCache Volumes in beide Richtungen zwischen AFX- und AFF oder FAS Systemen angeschlossen werden.

Migrieren von Daten aus einer Nicht- ONTAP -Quelle

Die Datenmigration von Nicht- ONTAP -Systemen kann mithilfe von Kopiervorgängen auf Dateiebene durchgeführt werden. Schnelle Kopierprogramme wie z.B. ["XCP"](#) oder ["Kopieren und Synchronisieren"](#) Kann ebenso wie Standardprogramme wie RoboCopy (für SMB) und rsync (für NFS) sowie Drittanbieter-Tools wie DataDobi verwendet werden.

Migrationseinschränkungen

Sie können Daten von AFF oder FAS Systemen auf AFX replizieren, wenn das Quelldatenvolume keine LUNs oder NVMe-Namespaces enthält. Beim Replizieren von AFX- auf AFF oder FAS Systeme ist die minimal unterstützte ONTAP Version für das AFF oder FAS System 9.16.1. Dies ist die erste ONTAP Version, die Advanced Capacity Balancing unterstützt.

Zeigen Sie eine Übersicht Ihres Speichers an

Um mit der Verwaltung Ihrer AFX-Daten zu beginnen, sollten Sie eine Übersicht über den Speicher anzeigen.

Informationen zu diesem Vorgang

Sie können auf alle für den AFX-Cluster definierten Volumes und Buckets zugreifen. Jeder dieser Container wird als Datencontainer betrachtet.

Schritte

1. Wählen Sie im Systemmanager **Speicher** und dann **Übersicht**
2. Wählen Sie neben *Volumes* → , um eine Liste der Datenträger anzuzeigen.
3. Wählen Sie neben *Buckets* → um eine Liste der Buckets anzuzeigen.
4. Aktualisieren oder erstellen Sie nach Bedarf einen Datencontainer.

Ähnliche Informationen

- ["Erfahren Sie mehr über ONTAP File System Analytics"](#)
- ["Zusätzliche AFX SVM-Verwaltung"](#)
- ["Bereiten Sie sich auf die Verwaltung Ihres AFX-Systems vor"](#)
- ["Migrieren einer AFX-System-SVM"](#)
- ["NetApp Interoperabilitätsmatrix-Tool"](#)

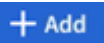
Erstellen und Konfigurieren eines Volumes auf einem AFX-Speichersystem

Sie können ein Volume erstellen und es an eine SVM anhängen. Jedes Volume kann Clients mithilfe eines der von AFX unterstützten Zugriffsprotokolle zugänglich gemacht werden.

Informationen zu diesem Vorgang

Beim Erstellen eines Volumes müssen Sie eine Mindestmenge an Konfigurationsdetails angeben. Zusätzliche Details können während der Erstellung oder nachträglich durch Bearbeiten des Datenträgers angegeben werden. Sie müssen die SVM für das Volume auswählen, wenn Sie zusätzliche SVMs erstellt haben.

Schritte

1. Wählen Sie im System-Manager **Speicher** und dann **Volumes**.
2. Wählen  **Add** und geben Sie die grundlegende Konfiguration einschließlich Name, Kapazität und Optimierung an.
3. Wählen Sie optional **Weitere Optionen** für zusätzliche Konfigurationen in Bezug auf Datenschutz, SnapLock und NFS-Zugriff.
4. Wählen Sie **Speichern**, um das Volumen hinzuzufügen.

Verwalten der AFX-Speichersystemvolumes

Es gibt mehrere Verwaltungsaufgaben, die Sie im Rahmen der Verwaltung der in Ihrem AFX-Cluster definierten Volumes ausführen können.

Erstellen Sie einen Qtree

Ein Qtree ist eine logische Unterteilung innerhalb eines Datenträgers, die Sie zum Organisieren und Verwalten von Daten erstellen können.

Schritte

1. Wählen Sie im System Manager **Speicher** und dann **Qtrees**.
2. Wählen  **Add** und geben Sie die grundlegende Konfiguration an, einschließlich Name, Volume und Sicherheitsstil. Konfigurieren Sie optional ein Kontingent.
3. Wählen Sie **Speichern**, um den Qtree hinzuzufügen.

Erstellen Sie ein Kontingent

Ein Kontingent ist eine Begrenzung der Speicherplatzmenge oder der Anzahl der Dateien, die von einem Benutzer, einer Gruppe oder einem Qtree verwendet werden können. Kontingente werden verwendet, um die Ressourcennutzung innerhalb eines AFX-Systems zu verwalten und zu steuern.

Schritte

1. Wählen Sie im System-Manager **Speicher** und dann **Kontingente**.
2. Wählen Sie die Registerkarte **Nutzung** aus, um eine Liste der aktiven Kontingente aller Volumes anzuzeigen.
3. Wählen Sie die Registerkarte **Volumes** aus, um eine Liste der im AFX-Cluster definierten Volumes anzuzeigen. Wählen Sie ein bestimmtes Volume aus, um zusätzliche Informationen anzuzeigen.
4. Um ein Kontingent festzulegen, wählen Sie die Registerkarte **Regeln**.
5. Geben Sie die Konfigurationsdetails an, einschließlich Kontingentziel, Typ und Grenzwerte.
6. Wählen Sie **Speichern**, um das Kontingent hinzuzufügen.

Erstellen und Konfigurieren eines S3-Buckets auf einem AFX-Speichersystem

Sie können einen Bucket erstellen und ihn an eine SVM anhängen. Jeder Bucket kann Clients mithilfe des von AFX unterstützten S3-Zugriffsprotokolls zugänglich gemacht werden.

Informationen zu diesem Vorgang

Beim Erstellen eines Buckets müssen Sie eine Mindestmenge an Konfigurationsdetails angeben. Zusätzliche Details können während der Erstellung oder später durch Bearbeiten des Buckets angegeben werden. Sie müssen das SVM für den Bucket auswählen, wenn Sie zusätzliche SVMs erstellt haben.

Bevor Sie beginnen

Sie müssen den S3-Dienst für die SVM konfigurieren, damit Clients auf den Bucket zugreifen können.

Schritte

1. Wählen Sie im System Manager **Speicher** und dann **Buckets** aus.

2. Wählen **+ Add** und geben Sie die Basiskonfiguration einschließlich Name und Kapazität an.
3. Wählen Sie optional **Weitere Optionen** für zusätzliche Konfigurationen in Bezug auf Datenschutz, Sperren und Berechtigungen.
4. Wählen Sie **Speichern**, um den Bucket hinzuzufügen.

Verwalten der AFX-Speichersystem-Buckets

Im Rahmen der Verwaltung von AFX S3-Buckets und Clientzugriff können Sie verschiedene Verwaltungsaufgaben ausführen. Die S3-Konfiguration und -Unterstützung in AFX ist dieselbe wie bei Unified ONTAP. Weitere Informationen finden Sie in der Unified ONTAP -Dokumentation.

Ähnliche Informationen

["Erfahren Sie mehr über die ONTAP S3-Konfiguration"](#)

Überwachen und Fehlerbeheben eines AFX-Speichersystems

Das AFX-System umfasst mehrere Optionen zur Überwachung des von jedem Cluster verwalteten Speichers.

NAS-Clients anzeigen

Sie können eine Liste der NFS- und SMB/CIFS-Clients anzeigen, die derzeit mit dem AFX-Cluster verbunden sind.

Schritte

1. Wählen Sie im System-Manager im Navigationsbereich **Clients** aus.
2. Wählen Sie je nach Wunsch den Reiter **NFS** oder **SMB/CIFS**.
3. Passen Sie die Anzeige an und suchen und laden Sie die Kundeninformationen nach Bedarf herunter.

Ähnliche Informationen

- ["Bereiten Sie sich auf die Verwaltung Ihrer AFX-Daten vor"](#)

Daten schützen

Bereiten Sie sich auf den Schutz Ihrer AFX-Speichersystemdaten vor

Bevor Sie Ihre AFX-Daten schützen, sollten Sie mit einigen der wichtigsten Konzepte und Funktionen vertraut sein.



Da viele der Konzepte und Administrationsverfahren, die auf AFF und FAS -Systemen verfügbar sind, mit denen auf AFX-Speichersystemen identisch sind, sollten Sie die Unified ONTAP Dokumentation für ["Datenschutz und Notfallwiederherstellung"](#) kann hilfreich sein.

Terminologie und Optionen

Es gibt mehrere Begriffe im Zusammenhang mit dem AFX-Datenschutz, mit denen Sie vertraut sein sollten.

Schnappschuss

Ein Snapshot ist ein schreibgeschütztes, zeitpunktbezogenes Abbild eines Datenträgers. Es handelt sich um eine grundlegende Technologie für die Replikations- und Datenschutzdienste von ONTAP.

Konsistenzgruppe

Eine Konsistenzgruppe ist eine Sammlung von Volumes, die als eine Einheit verwaltet werden. Sie können Konsistenzgruppen erstellen, um die Speicherverwaltung und den Datenschutz für Anwendungs-Workloads zu vereinfachen. Sie können beispielsweise in einem Vorgang einen Snapshot mehrerer Volumes erstellen, indem Sie die Konsistenzgruppe anstelle der einzelnen Volumes verwenden.

Hierarchische Konsistenzgruppe

Hierarchische Konsistenzgruppen wurden mit ONTAP 9.16.1 eingeführt und sind mit AFX verfügbar. Bei einer hierarchischen Struktur können eine oder mehrere Konsistenzgruppen als untergeordnete Elemente unter einem übergeordneten Element konfiguriert werden. Mit diesen hierarchischen Gruppen können Sie individuelle Snapshot-Richtlinien auf untergeordnete Konsistenzgruppen anwenden und die Snapshots aller untergeordneten Elemente durch Replikation des übergeordneten Elements als einzelne Einheit auf einem Remote-Cluster replizieren.

SnapLock

SnapLock ist eine ONTAP Funktion, mit der Sie Ihre Dateien schützen können, indem Sie sie in einen WORM-Zustand (Write Once Read Many) versetzen. Dadurch wird eine Änderung oder Löschung für einen festgelegten Aufbewahrungszeitraum verhindert. SnapLock -Volumes können nach der Erstellung basierend auf der Aufbewahrung nicht aus Nicht- SnapLock -Volumes konvertiert werden.

Einschränkungen des AFX-Datenschutzes

Sie sollten sich der ONTAP Datenschutzgrenzen und -beschränkungen bewusst sein, die durch das AFX-Speichersystem erzwungen werden.

SnapMirror synchron (SM-S)

Bei der Verwendung von SM-S gibt es eine Skalierungsbeschränkung. Sie können maximal 400 Beziehungen in einem einzelnen AFX-Systemcluster haben.

Ähnliche Informationen

- ["Zusätzliche AFX SVM-Verwaltung"](#)
- ["Bereiten Sie sich auf die Verwaltung Ihres AFX-Systems vor"](#)

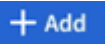
Erstellen einer Konsistenzgruppe auf einem AFX-Speichersystem

Sie können Konsistenzgruppen erstellen, um die Speicherverwaltung und den Datenschutz für Anwendungs-Workloads zu vereinfachen. Eine Konsistenzgruppe kann auf vorhandenen oder neuen Volumes basieren.

Bevor Sie beginnen

Wenn Sie planen, ein oder mehrere neue Volumes zu erstellen, sollten Sie sich mit den Konfigurationsoptionen beim Erstellen eines neuen Volumes vertraut machen.

Schritte

1. Wählen Sie im System Manager **Schutz** und dann **Konsistenzgruppen** aus.
2. Wählen  **Add** und wählen Sie eine der folgenden Optionen:

- Vorhandene Volumes verwenden
- Neue NAS-Volumes verwenden

3. Geben Sie die Konfigurationsdetails an, einschließlich Name, Volumes, Anwendungstyp und Schutz.
4. Wählen Sie **Hinzufügen**.

Ähnliche Informationen

- ["Verwalten von Konsistenzgruppen"](#)
- ["Erstellen und Konfigurieren eines AFX-Volumes"](#)

Verwalten von Konsistenzgruppen auf einem AFX-Speichersystem

Sie können die Konsistenzgruppen auf einem AFX-System verwalten. Dies kann Ihre Speicherverwaltung rationalisieren.

Hinzufügen des Snapshot-Datenschutzes zu einer Konsistenzgruppe

Wenn Sie einer Konsistenzgruppe Snapshot-Datenschutz hinzufügen, können lokale Snapshots der Konsistenzgruppe in regelmäßigen Abständen basierend auf einem vordefinierten Zeitplan erstellt werden.

Schritte

1. Wählen Sie im System Manager **Schutz** und dann **Konsistenzgruppen** aus.
2. Bewegen Sie den Mauszeiger über die Konsistenzgruppe, die Sie schützen möchten.
3. Wählen  ; wählen Sie dann **Bearbeiten**.
4. Wählen Sie unter **Lokaler Schutz** die Option **Schnappschüsse planen**.
5. Wählen Sie eine Snapshot-Richtlinie aus.

Akzeptieren Sie die Standard-Snapshot-Richtlinie, wählen Sie eine vorhandene Richtlinie aus oder erstellen Sie eine neue Richtlinie.

Option	Schritte
Auswählen einer vorhandenen Snapshot-Richtlinie	Wählen  neben der Standardrichtlinie; wählen Sie dann die vorhandene Richtlinie aus, die Sie verwenden möchten.

Option	Schritte
Erstellen einer neuen Snapshot-Richtlinie	- Wählen + Add ; geben Sie dann den neuen Richtliniennamen ein. - Wählen Sie den Richtlinienbereich aus. - Wählen Sie unter *Zeitpläne* + Add . - Wählen Sie den Namen aus, der unter Zeitplanname angezeigt wird. dann ✓ . - Wählen Sie den Richtlinienzeitplan aus. - Geben Sie unter Maximale Snapshots die maximale Anzahl von Snapshots ein, die Sie von der Konsistenzgruppe behalten möchten. - Optional können Sie unter * SnapMirror -Bezeichnung* eine SnapMirror -Bezeichnung eingeben. - Wählen Sie Speichern.

6. Wählen Sie **Bearbeiten**.

Ähnliche Informationen

- ["Erfahren Sie mehr über ONTAP Consistency Groups"](#)

Erstellen eines Snapshots auf einem AFX-Speichersystem

Um Daten auf Ihrem AFX-System zu sichern, müssen Sie einen Snapshot erstellen. Sie können einen Snapshot manuell erstellen oder die automatische Erstellung mithilfe einer Konsistenzgruppe planen.

Bevor Sie beginnen

Ein Snapshot ist eine lokale, schreibgeschützte Kopie Ihrer Daten, mit der Sie Volumes zu bestimmten Zeitpunkten wiederherstellen können. Snapshots können manuell bei Bedarf oder automatisch in regelmäßigen Abständen basierend auf einem ["Snapshot-Richtlinie und -Zeitplan"](#) .

Die Snapshot-Richtlinie und der Snapshot-Zeitplan geben die Details an, einschließlich des Zeitpunkts der Snapshot-Erstellung, der Anzahl der aufzubewahrenden Kopien, der Benennung und der Kennzeichnung für die Replikation. Beispielsweise könnte ein System jeden Tag um 0:10 Uhr einen Snapshot erstellen, die beiden aktuellsten Kopien behalten, sie „täglich“ nennen (mit einem angehängten Zeitstempel versehen) und sie für die Replikation mit „täglich“ kennzeichnen.

Arten von Snapshots

Sie können einen On-Demand-Snapshot eines einzelnen Volumes oder einer Konsistenzgruppe erstellen. Sie können auch automatisierte Snapshots einer Konsistenzgruppe erstellen, die mehrere Volumes enthält. Sie können jedoch keine automatisierten Snapshots eines einzelnen Volumes erstellen.

- On-Demand-Schnappschüsse

Sie können jederzeit einen On-Demand-Snapshot eines Volumes erstellen. Das Volume muss kein Mitglied einer Konsistenzgruppe sein, um durch einen On-Demand-Snapshot geschützt zu werden. Wenn Sie einen Snapshot eines Volumes erstellen, das Mitglied einer Konsistenzgruppe ist, werden die anderen Volumes

in der Konsistenzgruppe nicht in den Snapshot aufgenommen. Wenn Sie einen On-Demand-Snapshot einer Konsistenzgruppe erstellen, werden alle Volumes in der Konsistenzgruppe einbezogen.

- **Automatisierte Snapshots**

Basierend auf den Snapshot-Richtliniendefinitionen werden automatisierte Snapshots erstellt. Um eine Snapshot-Richtlinie auf ein Volume zur automatischen Snapshot-Erstellung anzuwenden, müssen die Volumes Mitglied derselben Konsistenzgruppe sein. Wenn Sie eine Snapshot-Richtlinie auf eine Konsistenzgruppe anwenden, sind alle Volumes in der Konsistenzgruppe geschützt.

Erstellen eines Snapshots

Erstellen Sie einen Snapshot eines Volumes oder einer Konsistenzgruppe.

Snapshot einer Konsistenzgruppe

Schritte

1. Wählen Sie im System Manager **Schutz** und dann **Konsistenzgruppen** aus.
2. Bewegen Sie den Mauszeiger über den Namen der Konsistenzgruppe, die Sie schützen möchten.
3. Wählen  ; wählen Sie dann **Schützen**.
4. Wenn Sie bei Bedarf sofort einen Snapshot erstellen möchten, wählen Sie unter **Lokaler Schutz** die Option **Jetzt einen Snapshot hinzufügen**.

Der lokale Schutz erstellt den Snapshot auf demselben Cluster, der das Volume enthält.

- a. Geben Sie einen Namen für den Snapshot ein oder akzeptieren Sie den Standardnamen. Geben Sie anschließend optional eine SnapMirror -Bezeichnung ein.

Das SnapMirror -Label wird vom Remote-Ziel verwendet.

5. Wenn Sie mithilfe einer Snapshot-Richtlinie automatisierte Snapshots erstellen möchten, wählen Sie **Snapshots planen**.

- a. Wählen Sie eine Snapshot-Richtlinie aus.

Akzeptieren Sie die Standard-Snapshot-Richtlinie, wählen Sie eine vorhandene Richtlinie aus oder erstellen Sie eine neue Richtlinie.

Option	Schritte
Auswählen einer vorhandenen Snapshot-Richtlinie	Wählen  neben der Standardrichtlinie; wählen Sie dann die vorhandene Richtlinie aus, die Sie verwenden möchten.
Erstellen einer neuen Snapshot-Richtlinie	i. Wählen  Add ; geben Sie dann die Parameter der Snapshot-Richtlinie ein. ii. Wählen Sie Richtlinie hinzufügen.

6. Wenn Sie Ihre Snapshots auf einen Remote-Cluster replizieren möchten, wählen Sie unter **Remote-Schutz** die Option **Auf einen Remote-Cluster replizieren**.

- a. Wählen Sie den Quellcluster und die Speicher-VM aus und wählen Sie dann die Replikationsrichtlinie aus.

Die anfängliche Datenübertragung für die Replikation beginnt standardmäßig sofort.

7. Wählen Sie **Speichern**.

Snapshot eines Volumes

Schritte

1. Wählen Sie im System-Manager **Speicher** und dann **Volumes**.
2. Bewegen Sie den Mauszeiger über den Namen des Volumes, das Sie schützen möchten.
3. Wählen  ; wählen Sie dann **Schützen**. Wenn Sie bei Bedarf sofort einen Snapshot erstellen möchten, wählen Sie unter **Lokaler Schutz** die Option **Jetzt einen Snapshot hinzufügen**.

Der lokale Schutz erstellt den Snapshot auf demselben Cluster, der das Volume enthält.

4. Geben Sie einen Namen für den Snapshot ein oder akzeptieren Sie den Standardnamen. Geben Sie anschließend optional eine SnapMirror -Bezeichnung ein.

Das SnapMirror -Label wird vom Remote-Ziel verwendet.

5. Wenn Sie mithilfe einer Snapshot-Richtlinie automatisierte Snapshots erstellen möchten, wählen Sie **Snapshots planen**.

- a. Wählen Sie eine Snapshot-Richtlinie aus.

Akzeptieren Sie die Standard-Snapshot-Richtlinie, wählen Sie eine vorhandene Richtlinie aus oder erstellen Sie eine neue Richtlinie.

Option	Schritte
Auswählen einer vorhandenen Snapshot-Richtlinie	Wählen  neben der Standardrichtlinie; wählen Sie dann die vorhandene Richtlinie aus, die Sie verwenden möchten.
Erstellen einer neuen Snapshot-Richtlinie	i. Wählen  Add ; geben Sie dann die Parameter der Snapshot-Richtlinie ein. ii. Wählen Sie Richtlinie hinzufügen.

6. Wenn Sie Ihre Snapshots auf einen Remote-Cluster replizieren möchten, wählen Sie unter **Remote-Schutz** die Option **Auf einen Remote-Cluster replizieren**.

- a. Wählen Sie den Quellcluster und die Speicher-VM aus und wählen Sie dann die Replikationsrichtlinie aus.

Die anfängliche Datenübertragung für die Replikation beginnt standardmäßig sofort.

7. Wählen Sie **Speichern**.

Ähnliche Informationen

- ["Erstellen einer ONTAP Snapshot-Richtlinie"](#)

Verwalten von Snapshots auf einem AFX-Speichersystem

Sie können Snapshots auf Ihrem AFX-System verwalten. Weitere Informationen finden Sie in der Unified ONTAP -Dokumentation.

Ähnliche Informationen

- ["Erstellen einer ONTAP Snapshot-Richtlinie"](#)
- ["Schützen Sie ONTAP FlexGroup -Volumes mit Snapshots"](#)

Erstellen einer Intercluster-SVM-Peer-Beziehung auf einem AFX-Speichersystem

Eine Peer-Beziehung definiert Netzwerkverbindungen, die Clustern und virtuellen Speichermaschinen (VMs) den sicheren Datenaustausch ermöglichen. Sie können eine

Peer-Beziehung zwischen Speicher-VMs auf verschiedenen Clustern erstellen, um Datenschutz und Notfallwiederherstellung mit SnapMirror zu ermöglichen.

Bevor Sie beginnen

Sie müssen eine Cluster-Peer-Beziehung zwischen dem lokalen und dem Remote-Cluster hergestellt haben, bevor Sie eine Speicher-VM-Peer-Beziehung erstellen können. ["Erstellen einer Cluster-Peer-Beziehung"](#) falls Sie dies nicht bereits getan haben.

Schritte

1. Wählen Sie im System Manager **Schutz > Übersicht**.
2. Wählen Sie unter **Storage-VM-Peers** die Option **Einen Storage-VM-Peer hinzufügen** aus.
3. Wählen Sie die Speicher-VM auf dem lokalen Cluster und dann die Speicher-VM auf dem Remote-Cluster aus.
4. Wählen Sie **Einen Speicher-VM-Peer hinzufügen**.

Ähnliche Informationen

- ["Erfahren Sie mehr über Peer-Beziehungen"](#) .

Verwalten der Snapshot-Replikation auf einem AFX-Speichersystem

Bei der Snapshot-Replikation handelt es sich um einen Prozess, bei dem Konsistenzgruppen auf Ihrem AFX-System an einen geografisch entfernten Standort kopiert werden. Nach der ersten Replikation werden Änderungen an Konsistenzgruppen basierend auf einer Replikationsrichtlinie an den Remote-Standort kopiert. Replizierte Konsistenzgruppen können zur Notfallwiederherstellung oder Datenmigration verwendet werden.

Um die Snapshot-Replikation einzurichten, müssen Sie eine Replikationsbeziehung zwischen Ihrem AFX-Speichersystem und dem Remote-Standort herstellen. Die Replikationsbeziehung wird durch eine Replikationsrichtlinie geregelt. Während der Clustereinrichtung wird eine Standardrichtlinie zum Replizieren aller Snapshots erstellt. Sie können die Standardrichtlinie verwenden oder optional eine neue Richtlinie erstellen.

Schritt 1: Erstellen einer Cluster-Peer-Beziehung

Bevor Sie Ihre Daten durch Replikation auf einen Remote-Cluster schützen können, müssen Sie eine Cluster-Peer-Beziehung zwischen dem lokalen und dem Remote-Cluster erstellen.

Bevor Sie beginnen

Die Voraussetzungen für Cluster-Peering sind für AFX-Systeme dieselben wie für andere ONTAP Systeme. ["Überprüfen der Voraussetzungen für Cluster-Peering"](#) .

Schritte

1. Wählen Sie im lokalen Cluster im System Manager **Cluster > Einstellungen**.
2. Wählen Sie unter **Intercluster-Einstellungen** neben **Cluster-Peers***  und wählen Sie dann ***Cluster-Peer hinzufügen**.
3. Wählen Sie **Remote-Cluster starten**. Dadurch wird eine Passphrase generiert, die Sie zur Authentifizierung beim Remote-Cluster verwenden.

4. Nachdem die Passphrase für den Remote-Cluster generiert wurde, fügen Sie sie unter **Passphrase** im lokalen Cluster ein.
5. Wählen **+ Add** ; geben Sie dann die IP-Adresse der Cluster-übergreifenden Netzwerkschnittstelle ein.
6. Wählen Sie **Cluster-Peering initiieren**.

Wie geht es weiter?

Sie haben mit einem Remote-Cluster eine Peering-Verbindung für einen lokalen AFX-Cluster hergestellt. Sie können jetzt eine Replikationsbeziehung erstellen.

Schritt 2: Optional eine Replikationsrichtlinie erstellen

Die Snapshot-Replikationsrichtlinie definiert, wann auf dem AFX-Cluster durchgeführte Updates auf den Remote-Standort repliziert werden.

Schritte

1. Wählen Sie im System Manager **Schutz > Richtlinien** und dann **Replikationsrichtlinien**.
2. Wählen **+ Add** .
3. Geben Sie einen Namen für die Replikationsrichtlinie ein oder akzeptieren Sie den Standardnamen. Geben Sie anschließend eine Beschreibung ein.
4. Wählen Sie den **Richtlinienumfang** aus.

Wenn Sie die Replikationsrichtlinie auf den gesamten Cluster anwenden möchten, wählen Sie **Cluster** aus. Wenn die Replikationsrichtlinie nur auf das Volume in einer bestimmten Speicher-VM angewendet werden soll, wählen Sie **Speicher-VM**.

5. Wählen Sie den **Richtlinientyp** aus.

Option	Schritte
Kopieren Sie Daten an den Remote-Standort, nachdem sie in die Quelle geschrieben wurden.	a. Wählen Sie Asynchron. b. Akzeptieren Sie unter Snapshots von Quelle übertragen den Standardübertragungszeitplan oder wählen Sie einen anderen aus. c. Wählen Sie aus, ob alle Snapshots übertragen werden sollen oder ob Regeln erstellt werden sollen, um zu bestimmen, welche Snapshots übertragen werden sollen. d. Aktivieren Sie optional die Netzwerkkomprimierung.
Schreiben Sie Daten gleichzeitig auf die Quell- und Remote-Sites.	a. Wählen Sie Synchron.

6. Wählen Sie **Speichern**.

Wie geht es weiter?

Sie haben eine Replikationsrichtlinie erstellt und sind nun bereit, eine Replikationsbeziehung zwischen Ihrem AFX-System und Ihrem Remote-Standort zu erstellen.

Schritt 3: Erstellen einer Replikationsbeziehung

Eine Snapshot-Replikationsbeziehung stellt eine Verbindung zwischen Ihrem AFX-System und einem Remotestandort her, sodass Sie Konsistenzgruppen auf einen Remotecluster replizieren können. Replizierte Konsistenzgruppen können zur Notfallwiederherstellung oder zur Datenmigration verwendet werden.

Zum Schutz vor Ransomware-Angriffen können Sie beim Einrichten Ihrer Replikationsbeziehung die Ziel-Snapshots sperren. Gesperrte Snapshots können nicht versehentlich oder böswillig gelöscht werden. Sie können gesperrte Snapshots verwenden, um Daten wiederherzustellen, wenn ein Volume durch einen Ransomware-Angriff kompromittiert wurde.

Bevor Sie beginnen

Erstellen Sie eine Replikationsbeziehung mit oder ohne gesperrte Ziel-Snapshots.

Mit gesperrten Snapshots

Schritte

1. Wählen Sie im System Manager **Schutz > Konsistenzgruppen**.
2. Wählen Sie eine Konsistenzgruppe aus.
3. Wählen  ; wählen Sie dann **Schützen**.
4. Wählen Sie unter **Remote-Schutz** die Option **Auf einen Remote-Cluster replizieren** aus.
5. Wählen Sie die **Replikationsrichtlinie** aus.

Sie müssen eine *Vault*-Replikationsrichtlinie auswählen.

6. Wählen Sie **Zieleinstellungen**.
7. Wählen Sie **Ziel-Snapshots sperren, um Löschung zu verhindern**
8. Geben Sie die maximale und minimale Datenaufbewahrungsdauer ein.
9. Um den Beginn der Datenübertragung zu verzögern, deaktivieren Sie **Übertragung sofort starten**.

Die erste Datenübertragung beginnt standardmäßig sofort.

10. Um den Standardübertragungszeitplan zu überschreiben, wählen Sie optional **Zieleinstellungen** und dann **Übertragungszeitplan überschreiben**.

Ihr Transferplan muss mindestens 30 Minuten betragen, um unterstützt zu werden.

11. Wählen Sie **Speichern**.

Ohne gesperrte Snapshots

Schritte

1. Wählen Sie im System Manager **Schutz > Replikation**.
2. Wählen Sie diese Option aus, um die Replikationsbeziehung mit einem lokalen Ziel oder einer lokalen Quelle zu erstellen.

Option	Schritte
Lokale Ziele	a. Wählen Sie Lokale Ziele und dann . b. Suchen Sie nach der Quellkonsistenzgruppe und wählen Sie sie aus. Die <i>Quell</i>-Konsistenzgruppe bezieht sich auf die Konsistenzgruppe auf Ihrem lokalen Cluster, die Sie replizieren möchten.

Option	Schritte
Lokale Quellen	a. Wählen Sie Lokale Quellen und dann  . b. Suchen Sie nach der Quellkonsistenzgruppe und wählen Sie sie aus. Die <i>Quell</i>-Konsistenzgruppe bezieht sich auf die Konsistenzgruppe auf Ihrem lokalen Cluster, die Sie replizieren möchten. c. Wählen Sie unter Replikationsziel den Cluster aus, in den repliziert werden soll, und wählen Sie dann die Speicher-VM aus.

3. Wählen Sie eine Replikationsrichtlinie aus.

4. Um den Beginn der Datenübertragung zu verzögern, wählen Sie **Zieleinstellungen** und deaktivieren Sie anschließend **Übertragung sofort starten**.

Die erste Datenübertragung beginnt standardmäßig sofort.

5. Um den Standardübertragungszeitplan zu überschreiben, wählen Sie optional **Zieleinstellungen** und dann **Übertragungszeitplan überschreiben**.

Ihr Transferplan muss mindestens 30 Minuten betragen, um unterstützt zu werden.

6. Wählen Sie **Speichern**.

Wie geht es weiter?

Nachdem Sie nun eine Replikationsrichtlinie und -beziehung erstellt haben, beginnt Ihre erste Datenübertragung, wie in Ihrer Replikationsrichtlinie definiert. Sie können optional Ihr Replikations-Failover testen, um zu überprüfen, ob ein erfolgreiches Failover erfolgen kann, wenn Ihr AFX-System offline geht.

Schritt 4: Testen des Replikationsfailovers

Überprüfen Sie optional, ob Sie Daten von replizierten Volumes auf einem Remotecluster erfolgreich bereitstellen können, wenn der Quellcluster offline ist.

Schritte

1. Wählen Sie im System Manager **Schutz > Replikation**.

2. Bewegen Sie den Mauszeiger über die Replikationsbeziehung, die Sie testen möchten, und wählen Sie dann  .

3. Wählen Sie **Failover testen**.

4. Geben Sie die Failover-Informationen ein und wählen Sie dann **Failover testen**.

Wie geht es weiter?

Nachdem Ihre Daten nun durch die Snapshot-Replikation für die Notfallwiederherstellung geschützt sind, sollten Sie **"Verschlüsseln Sie Ihre Daten im Ruhezustand"** sodass sie nicht gelesen werden kann, wenn eine Festplatte in Ihrem AFX-System zweckentfremdet, zurückgegeben, verlegt oder gestohlen wird.

Verwalten Sie Datenschutzrichtlinien und -pläne für AFX-Speichersysteme

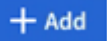
Sie können Snapshot-Richtlinien verwenden, um Daten in Ihren Konsistenzgruppen basierend auf einem automatisierten Zeitplan zu schützen. Die Richtlinienpläne innerhalb der Snapshot-Richtlinien bestimmen, wie oft Snapshots erstellt werden.

Erstellen eines neuen Schutzrichtlinienzeitplans

Ein Schutzrichtlinienplan definiert, wie oft eine Snapshot-Richtlinie ausgeführt wird. Sie können Zeitpläne erstellen, die in regelmäßigen Abständen basierend auf einer Anzahl von Tagen, Stunden oder Minuten ausgeführt werden. Sie können beispielsweise einen Zeitplan erstellen, der stündlich oder nur einmal pro Tag ausgeführt wird. Sie können auch Zeitpläne erstellen, die zu bestimmten Zeiten an bestimmten Wochen- oder Montagstagen ausgeführt werden. Sie können beispielsweise einen Zeitplan erstellen, der am 20. jedes Monats um 0:15 Uhr ausgeführt wird.

Durch die Definition verschiedener Schutzrichtlinienpläne haben Sie die Flexibilität, die Häufigkeit von Snapshots für verschiedene Anwendungen zu erhöhen oder zu verringern. Auf diese Weise können Sie für Ihre kritischen Workloads ein höheres Maß an Schutz und ein geringeres Risiko eines Datenverlusts bereitstellen, als dies bei weniger kritischen Workloads erforderlich wäre.

Schritte

1. Wählen Sie **Schutz** und dann **Richtlinien**; wählen Sie dann **Zeitplan**.
2. Wählen  **Add** .
3. Geben Sie einen Namen für den Zeitplan ein und wählen Sie dann die Zeitplanparameter aus.
4. Wählen Sie **Speichern**.

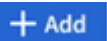
Wie geht es weiter?

Nachdem Sie nun einen neuen Richtlinienzeitplan erstellt haben, können Sie den neu erstellten Zeitplan innerhalb Ihrer Richtlinien verwenden, um zu definieren, wann Snapshots erstellt werden.

Erstellen einer Snapshot-Richtlinie

Eine Snapshot-Richtlinie definiert, wie oft Snapshots erstellt werden, wie viele Snapshots maximal zulässig sind und wie lange Snapshots aufbewahrt werden.

Schritte

1. Wählen Sie im System Manager **Schutz** und dann **Richtlinien**; wählen Sie dann **Snapshot-Richtlinien**.
2. Wählen  **Add** .
3. Geben Sie einen Namen für die Snapshot-Richtlinie ein.
4. Wählen Sie **Cluster** aus, um die Richtlinie auf den gesamten Cluster anzuwenden. Wählen Sie **Storage-VM** aus, um die Richtlinie auf eine einzelne Storage-VM anzuwenden.
5. Wählen Sie **Zeitplan hinzufügen** und geben Sie dann den Zeitplan für die Snapshot-Richtlinie ein.
6. Wählen Sie **Richtlinie hinzufügen**.

Wie geht es weiter?

Nachdem Sie nun eine Snapshot-Richtlinie erstellt haben, können Sie sie auf eine Konsistenzgruppe anwenden. Basierend auf den Parametern, die Sie in Ihrer Snapshot-Richtlinie festgelegt haben, werden Snapshots der Konsistenzgruppe erstellt.

Anwenden einer Snapshot-Richtlinie auf eine Konsistenzgruppe

Wenden Sie eine Snapshot-Richtlinie auf eine Konsistenzgruppe an, um Snapshots der Konsistenzgruppe automatisch zu erstellen, aufzubewahren und zu kennzeichnen.

Schritte

1. Wählen Sie im System Manager **Schutz** und dann **Richtlinien**; wählen Sie dann **Snapshot-Richtlinien**.
2. Bewegen Sie den Mauszeiger über den Namen der Snapshot-Richtlinie, die Sie anwenden möchten.
3. Wählen  ; wählen Sie dann **Übernehmen**.
4. Wählen Sie die Konsistenzgruppen aus, auf die Sie die Snapshot-Richtlinie anwenden möchten, und wählen Sie dann **Übernehmen**.

Wie geht es weiter?

Nachdem Ihre Daten nun mit Snapshots geschützt sind, sollten Sie ["Richten Sie eine Replikationsbeziehung ein"](#) um Ihre Konsistenzgruppen zur Sicherung und Notfallwiederherstellung an einen geografisch entfernten Standort zu kopieren.

Bearbeiten, Löschen oder Deaktivieren einer Snapshot-Richtlinie

Bearbeiten Sie eine Snapshot-Richtlinie, um den Richtliniennamen, die maximale Anzahl von Snapshots oder die SnapMirror -Bezeichnung zu ändern. Löschen Sie eine Richtlinie, um sie und die zugehörigen Sicherungsdaten aus Ihrem Cluster zu entfernen. Deaktivieren Sie eine Richtlinie, um die Erstellung oder Übertragung der in der Richtlinie angegebenen Snapshots vorübergehend zu stoppen.

Schritte

1. Wählen Sie im System Manager **Schutz** und dann **Richtlinien**; wählen Sie dann **Snapshot-Richtlinien**.
2. Bewegen Sie den Mauszeiger über den Namen der Snapshot-Richtlinie, die Sie bearbeiten möchten.
3. Wählen  ; wählen Sie dann **Bearbeiten**, **Löschen** oder **Deaktivieren**.

Ergebnis

Sie haben die Snapshot-Richtlinie geändert, gelöscht oder deaktiviert.

Bearbeiten einer Replikationsrichtlinie

Bearbeiten Sie eine Replikationsrichtlinie, um die Richtlinienbeschreibung, den Übertragungsplan und die Regeln zu ändern. Sie können die Richtlinie auch bearbeiten, um die Netzwerkkomprimierung zu aktivieren oder zu deaktivieren.

Schritte

1. Wählen Sie im System-Manager **Schutz** und dann **Richtlinien**.
2. Wählen Sie **Replikationsrichtlinien** aus.
3. Bewegen Sie den Mauszeiger über die Replikationsrichtlinie, die Sie bearbeiten möchten. Wählen Sie dann  .
4. Wählen Sie **Bearbeiten**.
5. Aktualisieren Sie die Richtlinie und wählen Sie dann **Speichern**.

Sichere Daten

Bereiten Sie sich auf die Sicherung Ihrer AFX-Speichersystemdaten vor

Bevor Sie Ihre AFX-Daten verwalten, sollten Sie mit den wichtigsten Konzepten und Funktionen vertraut sein.

Terminologie und Optionen

Es gibt mehrere Begriffe im Zusammenhang mit der AFX-Datensicherheit, mit denen Sie vertraut sein sollten.

Ransomware

Ransomware ist Schadsoftware, die Dateien verschlüsselt und sie für den Benutzer unzugänglich macht. In der Regel wird eine Art Zahlung verlangt, um die Daten zu entschlüsseln. ONTAP bietet Lösungen zum Schutz vor Ransomware durch Funktionen wie den autonomen Ransomware-Schutz (ARP).

Verschlüsselung

Bei der Verschlüsselung handelt es sich um den Prozess der Konvertierung von Daten in ein sicheres Format, das ohne entsprechende Autorisierung nicht einfach gelesen werden kann. ONTAP bietet sowohl software- als auch hardwarebasierte Verschlüsselungstechnologien zum Schutz ruhender Daten. Dadurch wird sichergestellt, dass es nicht gelesen werden kann, wenn das Speichermedium zweckentfremdet, zurückgegeben, verlegt oder gestohlen wird. Diese Verschlüsselungslösungen können entweder mit einem externen Schlüsselverwaltungsserver oder dem von ONTAP bereitgestellten Onboard Key Manager verwaltet werden. Siehe ["Verschlüsseln Sie ruhende Daten auf einem AFX-Speichersystem"](#) für weitere Informationen.

Digitale Zertifikate und PKI

Ein digitales Zertifikat ist ein elektronisches Dokument, mit dem der Besitz eines öffentlichen Schlüssels nachgewiesen wird. Der öffentliche Schlüssel und der zugehörige private Schlüssel können auf verschiedene Weise verwendet werden, unter anderem zur Feststellung der Identität, typischerweise als Teil eines größeren Sicherheitsrahmens wie TLS und IPsec. Diese Schlüssel sowie die unterstützenden Protokolle und Formatierungsstandards bilden die Grundlage für die Public Key Infrastructure (PKI). Siehe ["Verwalten von Zertifikaten auf einem AFX-Speichersystem"](#) für weitere Informationen.

Internetprotokollsicherheit

IPsec ist ein Internetstandard, der die Verschlüsselung, Integrität und Authentifizierung von Daten während der Übertragung zwischen Netzwerkendpunkten auf IP-Ebene gewährleistet. Es sichert den gesamten IP-Verkehr zwischen ONTAP und Clients, einschließlich höherer Protokolle wie NFS und SMB. IPsec bietet Schutz vor böswilligen Replay- und Man-in-the-Middle-Angriffen auf Ihre Daten. Siehe ["Sichere IP-Verbindungen auf Ihren AFX-Speichersystemen"](#) für weitere Informationen.

Ähnliche Informationen

- ["Zusätzliche AFX SVM-Verwaltung"](#)
- ["Bereiten Sie sich auf die Verwaltung Ihres AFX-Systems vor"](#)

Verschlüsseln Sie ruhende Daten auf einem AFX-Speichersystem

Sie können Ihre Daten auf Hardware- und Softwareebene verschlüsseln, um einen zweischichtigen Schutz zu gewährleisten. Wenn Sie ruhende Daten verschlüsseln, können diese nicht gelesen werden, wenn das Speichermedium zweckentfremdet,

zurückgegeben, verlegt oder gestohlen wird.

NetApp Storage Encryption (NSE) unterstützt die Hardwareverschlüsselung mithilfe von selbstverschlüsselnden Laufwerken (SEDs). SEDs verschlüsseln Daten beim Schreiben. Jedes SED enthält einen einzigartigen Verschlüsselungsschlüssel. Auf dem SED gespeicherte verschlüsselte Daten können ohne den Verschlüsselungsschlüssel des SED nicht gelesen werden. Knoten, die versuchen, von einem SED zu lesen, müssen authentifiziert werden, um auf den Verschlüsselungsschlüssel des SED zugreifen zu können. Knoten werden authentifiziert, indem sie einen Authentifizierungsschlüssel von einem Schlüsselmanager erhalten und diesen dann dem SED vorlegen. Wenn der Authentifizierungsschlüssel gültig ist, gibt das SED dem Knoten seinen Verschlüsselungsschlüssel, um auf die darin enthaltenen Daten zuzugreifen.

Bevor Sie beginnen

Verwenden Sie den integrierten AFX-Schlüsselmanager oder einen externen Schlüsselmanager, um Ihren Knoten Authentifizierungsschlüssel bereitzustellen. Zusätzlich zu NSE können Sie auch die Softwareverschlüsselung aktivieren, um Ihren Daten eine weitere Sicherheitsebene hinzuzufügen.

Schritte

1. Wählen Sie im Systemmanager **Cluster** und dann **Einstellungen**.
2. Wählen Sie im Abschnitt **Sicherheit** unter **Verschlüsselung** die Option **Konfigurieren** aus.
3. Konfigurieren Sie den Schlüsselmanager.

Option	Schritte
Konfigurieren des Onboard-Schlüsselmanagers	a. Wählen Sie Onboard Key Manager, um die Schlüsselserver hinzuzufügen. b. Geben Sie eine Passphrase ein.
Konfigurieren eines externen Schlüsselmanagers	a. Wählen Sie Externer Schlüsselmanager aus, um die Schlüsselserver hinzuzufügen. b. Wählen + Add um die Schlüsselserver hinzuzufügen. c. Fügen Sie die CA-Zertifikate des KMIP-Servers hinzu. d. Fügen Sie die KMIP-Client-Zertifikate hinzu.

4. Wählen Sie **Dual-Layer-Verschlüsselung**, um die Softwareverschlüsselung zu aktivieren.
5. Wählen Sie **Speichern**.

Ähnliche Informationen

- ["Verschlüsselung"](#)

Sichere IP-Verbindungen auf Ihren AFX-Speichersystemen

IP Security (IPsec) ist ein Internetprotokollstandard, der Datenverschlüsselung, -integrität und -authentifizierung für den Datenverkehr zwischen Netzwerkendpunkten auf IP-Ebene bietet. Mit IPsec lässt sich die Sicherheit des Front-End-Netzwerks zwischen einem AFX-Cluster und den Clients verbessern.

Konfigurieren von IPsec auf einem AFX-System

Die IPsec-Konfigurationsverfahren für AFX-Speichersysteme sind die gleichen wie für AFF und FAS -Systeme, mit Ausnahme der unterstützten Netzwerkschnittstellenkarten (NIC), die mit der Hardware-Offload-Funktion verwendet werden. Siehe ["Bereiten Sie die Konfiguration der IP-Sicherheit für das ONTAP Netzwerk vor."](#) für weitere Informationen.

Hardware-Entlastungsfunktion

Mehrere IPsec-Kryptografieoperationen, wie Verschlüsselung und Integritätsprüfungen, können auf eine unterstützte Netzwerkkarte Ihres AFX-Systems ausgelagert werden. Dies kann die Leistung und den Durchsatz des durch IPsec geschützten Netzwerkverkehrs erheblich verbessern.



Ab ONTAP 9.18.1 wurde die IPsec-Hardware-Offload-Funktion erweitert, um IPv6-Datenverkehr zu unterstützen.

Die folgenden Netzwerkkarten werden für die IPsec-Hardware-Offload-Funktion auf AFX-Speichersystemen ab ONTAP 9.17.1 unterstützt:

- X50130B (2p, 40G/100G Ethernet-Controller)
- X50131B (2p, 40G/100G/200G/400G Ethernet-Controller)

Siehe die ["NetApp Hardware Universe"](#) Weitere Informationen zu den unterstützten Grafikkarten für die ONTAP Version auf Ihrem AFX-System finden Sie hier.

Ähnliche Informationen

- ["Bereiten Sie die Konfiguration der IP-Sicherheit für das ONTAP Netzwerk vor."](#)
- ["NetApp Hardware Universe"](#)

Zusätzliche Verwaltung für eine AFX-Speichersystem-SVM

Zusätzlich zur typischen AFX SVM-Administration müssen Sie je nach Ihrer Umgebung möglicherweise noch weitere Aufgaben ausführen. Die meisten zusätzlichen Aufgaben können mit System Manager ausgeführt werden, in einigen Fällen müssen Sie jedoch möglicherweise die CLI verwenden.



Die beschriebenen ONTAP -Funktionen und -Verwaltung gelten für AFX-Speichersysteme und AFF oder FAS -Systeme mit Unified ONTAP. Links zur entsprechenden Unified ONTAP Dokumentation sind gegebenenfalls enthalten.

Speicherverwaltung und Leistung

Es gibt mehrere optionale Speicherverwaltungs- und Leistungsfunktionen, die Sie konfigurieren und mit Ihrer AFX-Bereitstellung verwenden können.

ONTAP NAS-Speicherverwaltung

Network Attached Storage (NAS) bietet dedizierten Dateispeicher, auf den mehrere Clients im Netzwerk zugreifen können. ONTAP unterstützt mehrere NAS-Protokolle. Siehe ["NAS-Speicherverwaltung"](#) für weitere Informationen.

ONTAP FlexCache -Volumes

FlexCache ist eine Remote-Caching-Funktion von ONTAP . Es bringt Daten näher an die Kunden, was die Zugriffsleistung verbessert und die Kosten senkt. Das Erstellen eines FlexCache -Volumes, das zunächst nur die Metadaten aus dem ursprünglichen Dateisystem kopiert, vereinfacht die Dateiverteilung und reduziert den WAN-Verkehr. Siehe ["Erfahren Sie mehr über ONTAP FlexCache -Volumes"](#) für weitere Informationen.

ONTAP FlexGroup Volumes

Ein FlexGroup -Volume besteht aus mehreren Mitgliedsvolumes, die den Datenverkehr automatisch und transparent teilen. FlexGroup -Volumes bieten mehrere Vorteile, darunter hohe Leistung und vereinfachte Verwaltung. Siehe ["FlexGroup -Volumeneinrichtung"](#) für weitere Informationen.

Datenschutz

Es gibt mehrere optionale Datenschutzfunktionen, die Sie konfigurieren und mit Ihrer AFX-Bereitstellung verwenden können.

Konsistenzgruppen

Eine Konsistenzgruppe ist eine Sammlung von Volumes, die als eine Einheit verwaltet werden. Siehe ["Erfahren Sie mehr über ONTAP Consistency Groups"](#) für weitere Informationen.

SnapLock

Sie können Ihre Dateien schützen, indem Sie sie auf Volumeebene in einen WORM-Zustand (Write Once Read Many) konvertieren. SnapLock unterstützt zwei Modi. Der Compliance-Modus stellt sicher, dass die Dateien erst gelöscht werden können, wenn ihre Aufbewahrungsfrist abgelaufen ist, was behördlichen oder branchenspezifischen Vorschriften entspricht. Im Enterprise-Modus können privilegierte Benutzer Dateien löschen, bevor ihre Aufbewahrungsfrist abläuft. Siehe ["Erfahren Sie mehr über ONTAP SnapLock"](#) für weitere Informationen.

Sicherheit

Es gibt mehrere optionale Sicherheitsfunktionen, die Sie konfigurieren und mit Ihrer AFX-Bereitstellung verwenden können.

Fpolicy

FPolicy ist ein Framework zur Benachrichtigung über Dateizugriffe, das zur Überwachung und Verwaltung von Dateizugriffsereignissen auf Storage Virtual Machines (SVMs) verwendet wird. Mit FPolicy können Sie Richtlinien erstellen, die festlegen, welche Dateivorgänge überwacht und optional blockiert werden sollen, basierend auf von Ihnen definierten Kriterien. FPolicy wird häufig für Sicherheitsaudits, Compliance und Daten-Governance eingesetzt. Siehe ["Erfahren Sie mehr über die ONTAP FPolicy-Lösungen"](#) für weitere Informationen.

ONTAP Ereignis- und Leistungsüberwachung

Sie können den Zustand und die Leistung eines Clusters überwachen. Hierzu gehört das Einrichten von Alarmen für Ereignisse und das Verwalten von Benachrichtigungen für Systemzustandsalarme. Siehe ["Ereignis-, Leistungs- und Integritätsüberwachung"](#) für weitere Informationen.

Ähnliche Informationen

- ["FAQ zu AFX-Speichersystemen"](#)
- ["Zusätzliche Administration für AFX-Cluster"](#)

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

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

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

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

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

Markeninformationen

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