Erstellen und Beheben von Sicherungsbeziehungen

Active IQ Unified Manager 9.13

NetApp
December 18, 2023

Inhalt

Erstellen, Überwachen und Beheben von Sicherungsbeziehungen 1
Arten der SnapMirror Sicherung 1
Einrichten von Sicherungsbeziehungen in Unified Manager 3
Durchführen eines Failover und Failback einer Sicherungsbeziehung 5
Behebung eines Schutzauftrags 9
Behebung von lag-Problemen 13

Erstellen, Überwachen und Beheben von Sicherungsbeziehungen

Unified Manager ermöglicht die Erstellung von Sicherungsbeziehungen, um den Spiegelschutz zu überwachen und Fehler zu beheben sowie die Sicherung von Daten, die in gemanagten Clustern gespeichert sind, zu sichern und Daten wiederherzustellen, wenn sie überschrieben oder verloren gehen.

Arten der SnapMirror Sicherung

Je nach Implementierung Ihrer Topologie des Storage können Sie mit Unified Manager mehrere Arten von SnapMirror Sicherungsbeziehungen konfigurieren. Alle Varianten des SnapMirror Schutzes bieten Failover Disaster Recovery-Schutz, bieten jedoch unterschiedliche Funktionen in Bezug auf Performance, Versionsflexibilität und Sicherung mehrerer Backup-Kopien.

Herkömmliche asynchrone Datensicherungsbeziehungen von SnapMirror

Herkömmlicher SnapMirror asynchroner Schutz bietet Sicherung der Blockreplizierung zwischen Quell- und Ziel-Volumes.

In herkömmlichen SnapMirror Beziehungen werden Spiegelvorgänge schneller ausgeführt als in alternativen SnapMirror Beziehungen, da der Spiegelvorgang auf der Blockreplizierung basiert. Beim herkömmlichen SnapMirror Schutz muss das Ziel-Volume jedoch unter derselben oder einer höheren kleineren Version der ONTAP Software wie das Quell-Volume innerhalb derselben größeren Version (z. B. Version 8.x zu 8.x oder 9.x zu 9.x) ausgeführt werden. Die Replizierung von einer 9.1 Quelle auf ein 9.0 Ziel wird nicht unterstützt, da auf dem Ziel eine frühere Hauptversion ausgeführt wird.

SnapMirror Asynchronous Protection mit versionsflexibler Replizierung

SnapMirror Asynchronous Schutz mit versionsflexibler Replizierung bietet einen logischen Spiegelschutz zwischen Quell- und Ziel-Volumes, auch wenn diese Volumes unter verschiedenen Versionen von ONTAP 8.3 oder höher ausgeführt werden (z. B. Version 8.3 auf 8.3.1, 8.3 zu 9.1 oder 9.2.2 zu 9.2).

In SnapMirror Beziehungen mit versionsflexibler Replizierung werden Spiegelvorgänge nicht so schnell ausgeführt wie in herkömmlichen SnapMirror Beziehungen.

Aufgrund der langsameren Ausführung eignet sich SnapMirror mit versionsflexibler Replizierungssicherung nicht für den Einsatz unter folgenden Umständen:

- Das Quellobjekt enthält mehr als 10 Millionen Dateien, die gesichert werden müssen.
- Die Recovery-Zeitvorgabe für die geschützten Daten beträgt maximal zwei Stunden. (Das heißt, das Ziel muss immer gespiegelte, wiederherstellbare Daten enthalten, die nicht mehr als zwei Stunden älter sind als die Daten der Quelle.)

In einem der aufgeführten Situationen ist die schnellere blockbasierte Ausführung der SnapMirror Standardsicherung erforderlich.

SnapMirror Asynchronous Protection mit versionsflexibler Replizierung und Option für Backups

SnapMirror Asynchronous Protection mit der versionsflexiblen Replizierungs- und Backup-Option bietet Spiegelschutz zwischen Quell- und Ziel-Volumes und die Möglichkeit, mehrere Kopien der gespiegelten Daten am Zielspeicherort zu speichern.

Der Storage-Administrator kann festlegen, welche Snapshot Kopien vom Quell- zum Zielsystem gespiegelt werden, und er kann auch angeben, wie lange diese Kopien am Ziel aufbewahrt werden sollen, selbst wenn sie an der Quelle gelöscht werden.

In SnapMirror Beziehungen mit versionsflexibler Replizierung und Backup-Option werden Spiegelvorgänge nicht so schnell ausgeführt wie in herkömmlichen SnapMirror Beziehungen.

SnapMirror Unified Replication (Spiegelung und Vault)

Dank der einheitlichen Replizierung mit SnapMirror können Disaster Recovery und Archivierung auf demselben Ziel-Volume konfiguriert werden. Wie bei SnapMirror führt die einheitliche Datensicherung beim ersten Aufruf einen Basistransfer durch. Ein Basistransfer unter der standardmäßigen, einheitlichen Datenschutzrichtlinie von „`MirrorAndVault`“ erstellt eine Snapshot Kopie des Quell-Volume, dann werden diese Kopie und die Datenblöcke übertragen, auf die sie auf das Ziel-Volume verweist. Wie bei SnapVault umfasst auch die Unified Datensicherung keine älteren Snapshot Kopien in der Basiskonfiguration.

SnapMirror synchroner Schutz mit strenger Synchronisierung

SnapMirror Synchronous Schutz mit „`strict`“-Synchronisierung sorgt dafür, dass das primäre und sekundäre Volume immer eine echte Kopie voneinander sind. Falls beim Versuch, Daten auf das sekundäre Volume zu schreiben, ein Replizierungsfehler auftritt, wird der Client-I/O auf das primäre Volume unterbrochen.

SnapMirror synchroner Schutz mit regelmäßiger Synchronisierung

SnapMirror Synchronous Schutz mit „`regular`“-Synchronisierung erfordert nicht, dass das primäre und sekundäre Volume immer eine echte Kopie voneinander sind, wodurch die Verfügbarkeit des primären Volumes gewährleistet wird. Wenn beim Versuch, Daten auf das sekundäre Volume zu schreiben, ein Replizierungsfehler auftritt, werden die primären und sekundären Volumes nicht mehr synchronisiert und die Client-I/O-Vorgänge werden weiter zum primären Volume fortgesetzt.

> Die Schaltfläche „Wiederherstellen“ und die Schaltflächen zum Beziehungsvorgang sind nicht verfügbar, wenn synchrone Schutzbeziehungen von der Ansicht „Zustand: Alle Volumes“ oder der Seite „Volume / Health Details“ überwacht werden.

SnapMirror Synchronous Business Continuity

Die SnapMirror Business Continuity Funktion (SM-BC) ist ab ONTAP 9.8 verfügbar und kann damit für die Sicherung von Applikationen mit LUNs eingesetzt werden. Auf diese Weise können Applikationen transparent ausfallen, sodass im Notfall Business Continuity gewährleistet ist.

Damit können Sie die synchronen SnapMirror Beziehungen für Konsistenzgruppen (CGS) erkennen und überwachen, die auf Clustern und Storage Virtual Machines von Unified Manager verfügbar sind. SM-BC wird auf AFF Clustern oder All SAN Array (ASA) Clustern unterstützt, bei denen die primären und sekundären Cluster entweder AFF oder ASA sein können. SM-BC sichert Applikationen mit iSCSI oder FCP LUNs.

Wenn Sie die durch die SM-BC-Beziehung geschützten Volumes und LUNs anzeigen, erhalten Sie eine

einheitliche Ansicht für Sicherungsbeziehungen, Konsistenzgruppen im Volume-Bestand, Anzeigen der Schutztopologie für Consistency Group-Beziehungen, Anzeigen historischer Daten für Consistency Group-Beziehungen bis zu einem Jahr. Sie können den Bericht auch herunterladen. Sie können auch die Zusammenfassung der Konsistenzgruppenbeziehungen anzeigen, die Unterstützung von Konsistenzgruppenbeziehungen suchen und Informationen zu Volumes erhalten, die von der Konsistenzgruppe geschützt sind.

Auf der Seite „Beziehungen“ können Sie auch den Schutz der Quell- und Ziel-Storage-Objekte und ihre Beziehung, die durch die Konsistenzgruppe geschützt sind, sortieren, filtern und erweitern.

Weitere Informationen über SnapMirror Synchronous Business Continuity finden Sie unter "ONTAP 9 Dokumentation für SM-BC".

Einrichten von Sicherungsbeziehungen in Unified Manager

Sie müssen verschiedene Schritte durchführen, um Unified Manager und OnCommand Workflow Automation zu verwenden, um SnapMirror- und SnapVault-Beziehungen zum Schutz Ihrer Daten einzurichten.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Es müssen Peer-Beziehungen zwischen zwei Clustern oder zwei Storage Virtual Machines (SVMs) hergestellt werden.
- OnCommand Workflow Automation muss in Unified Manager integriert werden:
  - "OnCommand Workflow Automation einrichten".
  - "Überprüfen des Quellcaches von Unified Manager in Workflow Automation".

Schritte

1. Führen Sie je nach Art der Schutzbeziehung einen der folgenden Schritte aus:
   - "SnapMirror Sicherungsbeziehung erstellen".
   - "SnapVault Sicherungsbeziehung erstellen".
2. Wenn Sie je nach Art der Beziehung eine Richtlinie für die Beziehung erstellen möchten, führen Sie einen der folgenden Schritte aus:
   - "Erstellen einer SnapVault-Richtlinie".
   - "SnapMirror-Richtlinie erstellen".
3. "Erstellen eines SnapMirror oder SnapVault Zeitplans".

Konfigurieren einer Verbindung zwischen Workflow Automation und Unified Manager

Es besteht die Möglichkeit, eine sichere Verbindung zwischen OnCommand Workflow Automation (WFA) und Unified Manager zu konfigurieren. Durch die Verbindung zur Workflow-Automatisierung können Unternehmen Sicherungsfunktionen wie SnapMirror und SnapVault Konfigurations-Workflows sowie Befehle zum Management von SnapMirror Beziehungen nutzen.

Was Sie brauchen

- Die installierte Version von Workflow Automation muss 5.1 oder höher sein.

> Das „`WFA Paket zum Management von Clustered Data ONTAP`“ ist in WFA 5.1 enthalten. Sie müssen dieses Paket also nicht mehr aus dem NetAppStorage Automation Store herunterladen und es je nach Bedarf separat auf Ihrem WFA Server installieren. "WFA Pack zum Management von ONTAP"

- Sie müssen den Namen des in Unified Manager erstellten Datenbankbenutzers haben, um WFA- und Unified Manager-Verbindungen zu unterstützen.

  Diesem Datenbankbenutzer muss die Rolle „Integration Schema“ zugewiesen worden sein.

- In Workflow Automation müssen Sie entweder die Administratorrolle oder die Rolle „Architekt“ zuweisen.
- Sie müssen über die Host-Adresse, die Portnummer 443, den Benutzernamen und das Passwort für die Workflow Automation-Einrichtung verfügen.
- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Workflow Automation**.
2. Wählen Sie im Bereich **Datenbankbenutzer** der Seite **Workflow Automation** den Namen aus und geben Sie das Kennwort für den Datenbankbenutzer ein, den Sie erstellt haben, um Unified Manager- und Workflow-Automatisierungsverbindungen zu unterstützen.
3. Geben Sie im Bereich **Workflow Automation Credentials** der Seite den Hostnamen oder die IP-Adresse (IPv4 oder IPv6) sowie den Benutzernamen und das Passwort für das Workflow Automation Setup ein.

   Sie müssen den Unified Manager-Serverport verwenden (Port 443).

4. Klicken Sie Auf **Speichern**.
5. Wenn Sie ein selbstsigniertes Zertifikat verwenden, klicken Sie auf **Ja**, um das Sicherheitszertifikat zu autorisieren.

   Die Seite Workflow Automation wird angezeigt.

6. Klicken Sie auf **Ja**, um die Web-Benutzeroberfläche neu zu laden, und fügen Sie die Workflow-Automation-Funktionen hinzu.

Verwandte Informationen

"NetApp Dokumentation: OnCommand Workflow Automation (aktuelle Versionen)"

Überprüfen des Quellcaches von Unified Manager in Workflow Automation

Sie können feststellen, ob das Caching der Datenquelle von Unified Manager ordnungsgemäß funktioniert, indem Sie prüfen, ob die Datenerfassung in Workflow Automation erfolgreich ist. Dies kann Sie erreichen, wenn Sie Workflow Automation in Unified Manager integrieren, um sicherzustellen, dass Workflow-Automatisierung nach der Integration verfügbar ist.

Was Sie brauchen

Um diese Aufgabe ausführen zu können, müssen Sie in Workflow Automation entweder die Administratorrolle oder die Rolle „Architekt“ zuweisen.

Schritte

1. Wählen Sie in der Workflow Automation UI **Ausführung** > **Datenquellen** aus.
2. Klicken Sie mit der rechten Maustaste auf den Namen der Datenquelle von Unified Manager und wählen Sie dann **Jetzt erwerben** aus.
3. Vergewissern Sie sich, dass die Akquisition fehlerfrei erfolgreich ist.

   Um die Workflow-Automatisierung in Unified Manager erfolgreich zu integrieren, müssen Konfigurationsfehler behoben werden.

Was passiert, wenn OnCommand Workflow Automation neu installiert oder aktualisiert wird

Bevor Sie OnCommand Workflow Automation neu installieren oder aktualisieren OnCommand Workflow Automation, müssen Sie zuerst die Verbindung zwischen OnCommand Workflow Automation und Unified Manager entfernen und sicherstellen, dass alle aktuell ausgeführten oder geplanten Jobs angehalten werden.

Sie müssen Unified Manager auch manuell aus OnCommand Workflow Automation löschen.

Nachdem Sie OnCommand Workflow Automation neu installiert oder aktualisiert haben, müssen Sie die Verbindung zu Unified Manager erneut einrichten.

Entfernen des OnCommand Workflow Automation Setup aus Unified Manager

Sie können das OnCommand Workflow Automation Setup aus Unified Manager entfernen, wenn Sie Workflow-Automatisierung nicht mehr verwenden möchten.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsfenster im linken Einrichtungsmenü auf **Allgemein** > **Workflow-Automatisierung**.
2. Klicken Sie auf der Seite **Workflow Automation** auf **Setup entfernen**.

Durchführen eines Failover und Failback einer Sicherungsbeziehung

Wenn ein Quell-Volume in Ihrer Sicherungsbeziehung aufgrund eines Hardware-Ausfalls oder eines Notfalls deaktiviert wird, können Sie die Sicherungsfunktionen in Unified Manager verwenden, um den Zugriff auf Lese-/Schreibzugriff auf das Schutzziel zu ermöglichen und ein Failover auf dieses Volume durchzuführen, bis die Quelle wieder online ist; Anschließend können Sie ein Failback zur ursprünglichen Quelle erstellen, sobald Daten zur Verfügung stehen.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen OnCommand Workflow Automation einrichten, um diesen Vorgang auszuführen.

Schritte

1. "SnapMirror Beziehung unterbrechen".

   Sie müssen die Beziehung unterbrechen, bevor Sie das Ziel von einem Datensicherungs-Volume in ein Lese-/Schreib-Volume konvertieren können, und bevor Sie die Beziehung rückgängig machen können.

2. "Die Sicherungsbeziehung wird umkehren".

   Wenn das ursprüngliche Quell-Volume wieder verfügbar ist, können Sie vielleicht entscheiden, die ursprüngliche Schutzbeziehung wiederherzustellen, indem Sie das Quell-Volume wiederherstellen. Bevor Sie die Quelle wiederherstellen können, müssen Sie sie mit den Daten synchronisieren, die auf das frühere Ziel geschrieben wurden. Sie verwenden die umgekehrte Resynchronisierung, um eine neue Schutzbeziehung zu erstellen, indem Sie die Rollen der ursprünglichen Beziehung rückgängig machen und das Quell-Volume mit dem vorherigen Ziel synchronisieren. Für die neue Beziehung wird eine neue Basis-Snapshot Kopie erstellt.

   Die umgekehrte Beziehung sieht ähnlich aus wie eine kaskadierte Beziehung:

3. "Die umgekehrte SnapMirror Beziehung unterbrechen".

   Wenn das ursprüngliche Quell-Volume neu synchronisiert wird und erneut Daten bereitstellen kann, unterbrechen Sie die umgekehrte Beziehung.

4. "Entfernen Sie die Beziehung".

   Wenn die umgekehrte Beziehung nicht mehr erforderlich ist, sollten Sie diese Beziehung entfernen, bevor Sie die ursprüngliche Beziehung wieder herstellen.

5. "Beziehung neu synchronisieren".

   Verwenden Sie den Vorgang zur erneuten Synchronisierung, um Daten von der Quelle zum Ziel zu synchronisieren und die ursprüngliche Beziehung wiederherzustellen.

Eine SnapMirror Beziehung von der Seite „Volume/Health Details“ abbrechen

Sie können eine Sicherungsbeziehung von der Seite Volume / Health Details brechen und die Datentransfers zwischen einem Quell- und Ziel-Volume in einer SnapMirror Beziehung stoppen. Wenn Sie Daten migrieren, für Disaster Recovery-Zwecke oder zum Testen von Applikationen nutzen möchten, können Sie eine Beziehung unterbrechen. Das Zielvolume wird in ein Lese- und Schreib-Volume geändert. Man kann keine SnapVault Beziehung durchbrechen.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Schritte

1. Wählen Sie auf der Registerkarte **Schutz** der Seite **Volumen / Gesundheit** Details aus der Topologie die SnapMirror Beziehung aus, die Sie brechen möchten.
2. Klicken Sie mit der rechten Maustaste auf das Ziel und wählen Sie im Menü die Option **Pause** aus.

   Das Dialogfeld Beziehung unterbrechen wird angezeigt.
3. Klicken Sie auf **Weiter**, um die Beziehung zu brechen.
4. Stellen Sie in der Topologie sicher, dass die Beziehung unterbrochen ist.

Rückkehrschutzbeziehungen auf der Seite Volume/Health Details

Wenn ein Notfall das Quellvolume in Ihrer Schutzbeziehung deaktiviert, können Sie das Zielvolume für die Bereitstellung von Daten verwenden, indem Sie es in Lese-/Schreibzugriff konvertieren, während Sie die Quelle reparieren oder ersetzen. Wenn die Quelle für den Empfang von Daten erneut verfügbar ist, können Sie mithilfe der Resynchronisierung auf umgekehrter Richtung die Beziehung herstellen und die Daten auf der Quelle mit den Daten auf dem Ziel für Lesen/Schreiben synchronisieren.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.
- Die Beziehung darf keine SnapVault Beziehung sein.
- Eine Schutzbeziehung muss bereits vorhanden sein.
- Die Schutzbeziehung muss gebrochen werden.
- Sowohl die Quelle als auch das Ziel müssen online sein.
- Die Quelle darf nicht Ziel eines anderen Datensicherungs-Volumes sein.
- Wenn Sie diese Aufgabe ausführen, werden Daten in der Quelle, die neuer als die Daten in der gemeinsamen Snapshot Kopie ist, gelöscht.
- Die für die umgekehrte Resynchronisierung erstellten Richtlinien und Zeitpläne sind mit denen in der ursprünglichen Schutzbeziehung identisch.

  Wenn Richtlinien und Zeitpläne nicht vorhanden sind, werden sie erstellt.

Schritte

1. Suchen Sie auf der **Protection**-Registerkarte der **Volume / Health**-Detailseite in der Topologie die SnapMirror-Beziehung, auf der Sie Quelle und Ziel umkehren möchten, und klicken Sie mit der rechten Maustaste darauf.
2. Wählen Sie aus dem Menü die Option **Resync rückwärts**.

   Das Dialogfeld Resync umkehren wird angezeigt.
3. Stellen Sie sicher, dass die Beziehung, die im Dialogfeld **Resync** umkehren angezeigt wird, die Beziehung ist, für die Sie die Neusynchronisierung rückgängig machen möchten, und klicken Sie dann auf **Absenden**.

   Das Dialogfeld „Resync umkehren“ wird geschlossen und oben auf der Seite „Volume/Health Details“ wird

ein Job-Link angezeigt.

4. **Optional:** Klicken Sie auf **Jobs anzeigen** auf der Seite **Volumen / Gesundheit** Details, um den Status jedes umgekehrten Neusynchronisierung zu verfolgen.

   Eine gefilterte Liste von Jobs wird angezeigt.

5. **Optional:** Klicken Sie auf den Pfeil **Zurück** in Ihrem Browser, um zur Detailseite **Volumen / Gesundheit** zurückzukehren.

   Nach erfolgreichem Abschluss aller Jobaufgaben ist die Neusynchronisierung bei umgekehrter Neusynchronisierung abgeschlossen.

Entfernen einer Schutzbeziehung von der Seite Volume / Health Details

Sie können eine Schutzbeziehung entfernen, um eine vorhandene Beziehung zwischen der ausgewählten Quelle und dem ausgewählten Ziel dauerhaft zu löschen, z. B. wenn Sie eine Beziehung unter Verwendung eines anderen Ziels erstellen möchten. Durch diesen Vorgang werden alle Metadaten entfernt und können nicht rückgängig gemacht werden.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation einrichten.

Schritte

1. Wählen Sie auf der Registerkarte **Protection** der Seite **Volume / Health** Details aus der Topologie die SnapMirror Beziehung aus, die Sie entfernen möchten.
2. Klicken Sie mit der rechten Maustaste auf den Namen des Ziels und wählen Sie im Menü die Option **Entfernen**.

   Das Dialogfeld Beziehung entfernen wird angezeigt.

3. Klicken Sie auf **Weiter**, um die Beziehung zu entfernen.

   Die Beziehung wird von der Seite Volume / Health Details entfernt.

Sicherungsbeziehungen von der Seite Volume / Health Details neu synchronisieren

Sie können Daten auf einer SnapMirror oder SnapVault-Beziehung neu synchronisieren, die unterbrochen wurde, und dann wurde das Ziel gelesen/geschrieben, sodass die Daten auf der Quelle mit den Daten auf dem Ziel übereinstimmen. Sie können auch neu synchronisieren, wenn eine erforderliche gemeinsame Snapshot Kopie auf dem Quell-Volume gelöscht wird, sodass SnapMirror oder SnapVault Updates fehlschlagen.

Was Sie brauchen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen OnCommand Workflow Automation eingerichtet haben.

Schritte

1. Suchen Sie auf der Registerkarte **Schutz** der Seite **Volumen / Gesundheit** Details in der Topologie die Schutzbeziehung, die Sie neu synchronisieren möchten, und klicken Sie mit der rechten Maustaste darauf.
2. Wählen Sie im Menü * resynchronisieren* aus.

   Alternativ können Sie im Menü **Aktionen** die Option **Beziehung** > **Resynchronisieren** wählen, um die Beziehung, für die Sie die Details anzeigen, neu zu synchronisieren.

   Das Dialogfeld „Resynchronisieren“ wird angezeigt.
3. Wählen Sie auf der Registerkarte **Resynchronisierung Optionen** eine Übertragungs-Priorität und die maximale Übertragungsrate aus.
4. Klicken Sie auf **Quelle Snapshot Kopien** und dann in der Spalte **Snapshot Kopie** auf **Standard**.

   Das Dialogfeld Quell-Snapshot-Kopie auswählen wird angezeigt.
5. Wenn Sie eine vorhandene Snapshot Kopie angeben möchten, anstatt die Standard-Snapshot Kopie zu übertragen, klicken Sie auf **vorhandene Snapshot Kopie** und wählen Sie eine Snapshot Kopie aus der Liste aus.
6. Klicken Sie Auf **Absenden**.

   Sie werden wieder zum Dialogfeld „erneut synchronisieren“ angezeigt.
7. Wenn Sie mehrere Quellen zum erneuten Synchronisieren ausgewählt haben, klicken Sie für die nächste Quelle, für die Sie eine vorhandene Snapshot Kopie angeben möchten, auf **Standard**.
8. Klicken Sie auf **Senden**, um die Neusynchronisierung zu beginnen.

   Der Resynchronisierung-Job wurde gestartet, Sie werden auf die Seite Volume / Health Details zurückgeschickt und oben auf der Seite wird ein Link zu Jobs angezeigt.
9. **Optional:** Klicken Sie auf **Jobs anzeigen** auf der Seite **Volume / Health Details**, um den Status jedes Resynchronisierung Jobs zu verfolgen.

   Eine gefilterte Liste von Jobs wird angezeigt.
10. **Optional:** Klicken Sie auf den Pfeil **Zurück** in Ihrem Browser, um zur Detailseite **Volumen / Gesundheit** zurückzukehren.

    Die Neusynchronisierung ist abgeschlossen, nachdem alle Aufgabenstellungen erfolgreich abgeschlossen wurden.

Behebung eines Schutzauftrags

Dieser Workflow bietet ein Beispiel dafür, wie Sie Fehler im Schutz über das Unified Manager-Dashboard identifizieren und beheben können.

Was Sie brauchen

Da für einige Aufgaben in diesem Workflow eine Anmeldung über die Administratorrolle erforderlich ist, müssen Sie mit den Rollen vertraut sein, die für die Verwendung verschiedener Funktionen erforderlich sind.

In diesem Szenario greifen Sie auf die Dashboard-Seite zu, um festzustellen, ob es Probleme mit Ihren

Schutzaufgaben gibt. Im Bereich Schutzvorfall stellen Sie fest, dass ein Vorfall mit dem Jobabbruch vorliegt und ein Fehler beim Schutz eines Volumes angezeigt wird. Sie untersuchen diesen Fehler, um die mögliche Ursache und mögliche Lösung zu ermitteln.

Schritte

1. Klicken Sie im Bereich Schutz-Vorfälle im Bereich ungelöste Vorfälle und Risiken auf das Ereignis * Schutz Job fehlgeschlagen*.

   Der verknüpfte Text für das Ereignis wird in das Formular geschrieben `object_name:/object_name - Error Name`, Wie z. B. `cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed`.

   Die Seite Ereignisdetails für den fehlgeschlagenen Schutzauftrag wird angezeigt.

2. Prüfen Sie die Fehlermeldung im Feld Ursache im Bereich **Zusammenfassung**, um das Problem zu ermitteln und mögliche Korrekturmaßnahmen zu bewerten.

   Siehe "Identifizieren des Problems und Durchführen von Korrekturmaßnahmen für einen fehlgeschlagenen Schutzauftrag".

Identifizieren des Problems und Durchführen von Korrekturmaßnahmen für einen fehlgeschlagenen Schutzauftrag

Sie überprüfen die Fehlermeldung zum Jobfehler im Feld Ursache auf der Seite Ereignisdetails und stellen fest, dass der Job aufgrund eines Fehlers bei der Snapshot-Kopie fehlgeschlagen ist. Fahren Sie dann zur Seite Volume / Health Details, um weitere Informationen zu erhalten.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Die Fehlermeldung, die im Feld Ursache auf der Seite Ereignisdetails angezeigt wird, enthält den folgenden Text über den fehlgeschlagenen Job:

```
Protection Job Failed. Reason: (Transfer operation for
relationship 'cluster2_src_svm:cluster2_src_vol2->cluster3_dst_svm:
managed_svc2_vol3' ended unsuccessfully. Last error reported by
Data ONTAP: Failed to create Snapshot copy 0426cluster2_src_vol2snap
on volume cluster2_src_svm:cluster2_src_vol2. (CSM: An operation
failed due to an ONC RPC failure.)
Job Details
```

Diese Meldung enthält folgende Informationen:

- Ein Backup- oder Spiegelungsauftrag wurde nicht erfolgreich abgeschlossen.

  Der Job umfasste eine Sicherungsbeziehung zwischen dem Quell-Volume `cluster2_src_vol2` Auf dem virtuellen Server `cluster2_src_svm` Und dem Ziel-Volume `managed_svc2_vol3` Auf dem virtuellen

Server mit dem Namen `cluster3_dst_svm`.

- Fehler beim Erstellen eines Jobs für die Snapshot Kopie `0426cluster2_src_vol2snap` Auf dem Quell-Volume `cluster2_src_svm:/cluster2_src_vol2`.

In diesem Szenario können Sie die Ursache und mögliche Korrekturmaßnahmen für den Job-Fehler identifizieren. Zur Behebung des Fehlers müssen Sie jedoch entweder auf die Web-UI des System Managers oder auf die CLI-Befehle von ONTAP zugreifen.

Schritte

1. Sie überprüfen die Fehlermeldung und stellen fest, dass ein Snapshot-Kopierauftrag auf dem Quell-Volume fehlgeschlagen ist, was darauf hinweist, dass möglicherweise ein Problem mit Ihrem Quell-Volume vorliegt.

   Optional können Sie am Ende der Fehlermeldung auf den Link **Job Details** klicken, aber für die Zwecke dieses Szenarios wählen Sie nicht zu tun.

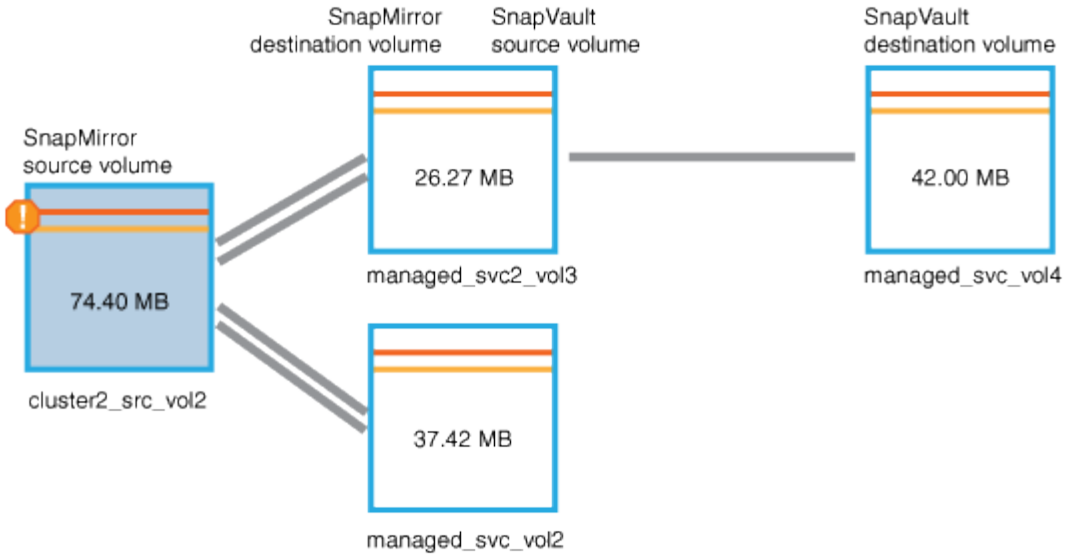
2. Sie entscheiden, dass Sie versuchen möchten, das Ereignis zu lösen, so gehen Sie wie folgt vor:
   a. Klicken Sie auf die Schaltfläche **Zuweisen zu** und wählen Sie im Menü die Option **ME** aus.
   b. Klicken Sie auf die Schaltfläche **Bestätigen**, damit Sie keine wiederholten Warnmeldungen erhalten, wenn für das Ereignis Warnmeldungen eingerichtet wurden.
   c. Optional können Sie auch Anmerkungen zum Ereignis hinzufügen.
3. Klicken Sie im Fensterbereich **Zusammenfassung** auf das Feld **Quelle**, um Details zum Quellvolumen anzuzeigen.

   Das Feld **Quelle** enthält den Namen des Quellobjekts: In diesem Fall das Volume, auf dem der Snapshot-Kopierauftrag geplant wurde.

   Die Seite Volume / Health Details wird für angezeigt `cluster2_src_vol2`, Zeigt den Inhalt der Registerkarte Schutz.

4. Wenn man sich das Topologiediagramm ansieht, wird ein Fehlersymbol angezeigt, das mit dem ersten Volume in der Topologie verknüpft ist, das das Quell-Volume für die SnapMirror Beziehung ist.

   Die horizontalen Balken im Quell-Volume-Symbol zeigen die für dieses Volume eingestellten Warn- und Fehlerschwellenwerte an.



5. Sie platzieren den Cursor über das Fehlersymbol, um das Popup-Dialogfeld anzuzeigen, in dem die Schwellenwerteinstellungen angezeigt werden. Es wird angezeigt, dass das Volume den Fehlerschwellenwert überschritten hat und ein Kapazitätsproblem angezeigt wird.
6. Klicken Sie auf die Registerkarte **Kapazität**.

   Kapazitätsinformationen zum Volume `cluster2_src_vol2` Anzeigen.
7. Im Fenster **Kapazität** sehen Sie, dass im Balkendiagramm ein Fehlersymbol angezeigt wird, das wiederum anzeigt, dass die Volumenkapazität den für das Volumen festgelegten Schwellenwert überschritten hat.
8. Unter dem Kapazitätsdiagramm sehen Sie, dass Autogrow von Volume deaktiviert wurde und eine Volume-Platzgarantie gesetzt wurde.

   Sie könnten sich für die Aktivierung von Autogrow entscheiden. In diesem Szenario entscheiden Sie sich jedoch, bis Sie eine Entscheidung treffen, wie das Kapazitätsproblem zu lösen ist, bevor Sie eine Entscheidung treffen.
9. Sie scrollen nach unten zur Liste **Ereignisse** und sehen, dass der Schutzauftrag fehlgeschlagen ist, Volume Days bis Full und Volume Space Full Events generiert wurden.
10. In der **Events**-Liste klicken Sie auf das Event **Volume Space Full**, um weitere Informationen zu erhalten, nachdem Sie entschieden haben, dass dieses Ereignis für Ihr Kapazitätsproblem am relevantesten erscheint.

    Auf der Seite Ereignisdetails wird das Ereignis Volume Space Full für das Quell-Volume angezeigt.
11. Im Bereich **Zusammenfassung** lesen Sie das Feld Ursache für das Ereignis: `The full threshold set at 90% is breached. 45.38 MB (95.54%) of 47.50 MB is used.`
12. Unter dem Übersichtsbereich werden vorgeschlagene Korrekturmaßnahmen angezeigt.

    Die vorgeschlagenen Korrekturmaßnahmen werden nur für bestimmte Ereignisse angezeigt, sodass dieser Bereich für alle Arten von Ereignissen nicht angezeigt wird.

    Klicken Sie durch die Liste der vorgeschlagenen Aktionen, die Sie möglicherweise durchführen können, um das Ereignis Volume Space Full aufzulösen:

    - Aktivieren Sie Autogrow auf diesem Volume.

- Die Volume-Größe ändern
- Aktivierung und Ausführung der Deduplizierung auf diesem Volume
- Aktivieren und führen Sie die Komprimierung auf diesem Volume durch.

13. Sie entscheiden sich für die Aktivierung von Autogrow auf dem Volume. Dazu müssen Sie jedoch den verfügbaren freien Speicherplatz im übergeordneten Aggregat und die aktuelle Wachstumsrate des Volume bestimmen:
    a. Sehen Sie sich das übergeordnete Aggregat an, `cluster2_src_aggr1`, Im Fenster **Verwandte Geräte**.

       Sie können auf den Namen des Aggregats klicken, um weitere Details zum Aggregat zu erhalten.

       Sie bestimmen, dass das Aggregat über ausreichend Platz verfügt, um die Autogrow von Volumes zu aktivieren.

    b. Sehen Sie sich oben auf der Seite das Symbol für einen kritischen Vorfall an, und überprüfen Sie den Text unter dem Symbol.

       Sie bestimmen, dass „Tage voll: Weniger als ein Tag“- Wachstumsrate: 5.4%.

14. Wechseln Sie zu System Manager oder rufen Sie die ONTAP-CLI auf, um die zu aktivieren `volume autogrow` Option.

    Notieren Sie sich die Namen des Volumes und des Aggregats, sodass Sie sie bei der Aktivierung von Autogrow zur Verfügung haben.

15. Kehren Sie nach der Behebung des Kapazitätsproblem zur Detailseite für Unified Manager **Event** zurück, und markieren Sie das Ereignis als erledigt.

Behebung von lag-Problemen

Dieser Workflow bietet ein Beispiel dafür, wie Sie ein lag-Problem lösen können. In diesem Szenario greifen Sie als Administrator oder Operator auf die Seite Unified ManagerDashboard zu, um zu sehen, ob Probleme mit Ihren Schutzbeziehungen auftreten und, falls sie vorhanden sind, Lösungen zu finden.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Auf der Dashboard-Seite sehen Sie sich den Bereich „ungelöste Vorfälle und Risiken“ an und Sie sehen einen SnapMirror lag-Fehler im Teilfenster „Sicherung“ unter „Sicherungsrisiken“.

Schritte

1. Suchen Sie im Fensterbereich **Protection** auf der Seite **Dashboard** den Fehler bezüglich SnapMirror Beziehung lag und klicken Sie darauf.

   Es wird die Seite Ereignisdetails für das Ereignis lag-Fehler angezeigt.

2. Auf der Seite **Event** Details können Sie eine oder mehrere der folgenden Aufgaben ausführen:

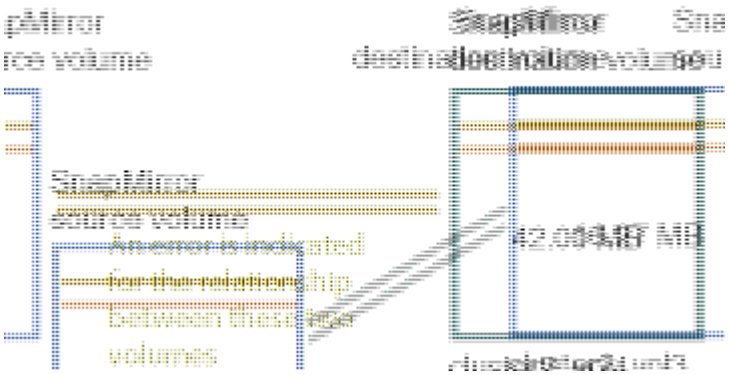
- Prüfen Sie die Fehlermeldung im Feld Ursache im Übersichtsbereich, um festzustellen, ob Korrekturmaßnahmen vorgeschlagen werden.
- Klicken Sie im Feld Quelle des Übersichtsbereichs auf den Objektnamen, in diesem Fall ein Volume, um Details zum Volume anzuzeigen.
- Suchen Sie nach Notizen, die zu diesem Event hinzugefügt wurden.
- Fügen Sie dem Ereignis eine Notiz hinzu.
- Weisen Sie das Ereignis einem bestimmten Benutzer zu.
- Bestätigen oder beheben Sie das Ereignis.

3. In diesem Szenario klicken Sie im Feld Quelle des Bereichs **Zusammenfassung** auf den Objektnamen (in diesem Fall ein Volume), um Details zum Volume zu erhalten.

   Die Registerkarte Schutz der Seite Volume / Health Details wird angezeigt.

4. Auf der Registerkarte **Schutz** sehen Sie sich das Topologiediagramm an.

   Die Tatsache, dass das Volume mit dem lag-Fehler das letzte Volume einer SnapMirror Kaskadierung mit drei Volumes ist, ist zu beachten. Das ausgewählte Volume wird in Dunkelgrau dargestellt, und eine doppelte orangefarbene Linie des Quell-Volume weist auf einen SnapMirror Beziehungsfehler hin.



5. Klicken Sie auf jedes der Volumes in der SnapMirror-Kaskadierung.

   Bei der Auswahl der einzelnen Volumes sind die Schutzinformationen in der Zusammenfassung, Topologie, Verlauf, Ereignisse, Verwandte Geräte, Die Bereiche „Verwandte Warnungen“ ändern sich, um die für das ausgewählte Volume relevanten Details anzuzeigen.

6. Sie sehen den Bereich **Zusammenfassung** und positionieren den Cursor über dem Informationssymbol im Feld **Zeitplan aktualisieren** für jedes Volumen.

   In diesem Szenario beachten Sie, dass die SnapMirror-Richtlinie DPStandard ist und dass die SnapMirror-Zeitpläne stündlich innerhalb von fünf Minuten nach der Stunde aktualisiert werden. Sie wissen, dass alle Volumes in der Beziehung versuchen, einen SnapMirror Transfer gleichzeitig abzuschließen.

7. Um das lag-Problem zu beheben, ändern Sie die Zeitpläne für zwei der kaskadierten Volumes, sodass jedes Ziel nach Abschluss des Transfers einen SnapMirror Transfer beginnt.