Verwalten von SnapCenter Server und Plug-Ins

SnapCenter software

NetApp
November 06, 2025

Inhalt

Verwalten von SnapCenter Server und Plug-Ins

Dashboard anzeigen

Übersicht über das Dashboard

Über das Dashboard im linken Navigationsbereich von SnapCenter erhalten Sie einen ersten Überblick über den Zustand Ihres Systems, einschließlich der letzten Jobaktivität, Warnungen, Schutzzusammenfassung, Speichereffizienz und -nutzung, Status von SnapCenter -Jobs (Sichern, Klonen, Wiederherstellen), Konfigurationsstatus für eigenständige und Windows-Cluster-Hosts, Anzahl der von SnapCenter verwalteten Storage Virtual Machines (SVMs) und Lizenzkapazität.

Die in der Dashboard-Ansicht angezeigten Informationen hängen von der Rolle ab, die dem Benutzer zugewiesen ist, der derzeit bei SnapCenter angemeldet ist. Einige Inhalte werden möglicherweise nicht angezeigt, wenn der Benutzer nicht über die Berechtigung zum Anzeigen dieser Informationen verfügt.

In vielen Fällen können Sie weitere Informationen zu einer Anzeige anzeigen, indem Sie mit der Maus über **i** fahren. In einigen Fällen sind Informationen in Dashboard-Anzeigen mit detaillierten Quellinformationen auf SnapCenter GUI-Seiten wie Ressourcen, Monitor und Berichten verknüpft.

Aktuelle Arbeitsaktivitäten

Die Kachel „Letzte Jobaktivitäten“ zeigt die neuesten Jobaktivitäten aller Sicherungs-, Wiederherstellungs- und Klonjobs an, auf die Sie Zugriff haben. Jobs in dieser Anzeige haben einen der folgenden Status: Abgeschlossen, Warnung, Fehlgeschlagen, Wird ausgeführt, In der Warteschlange und Abgebrochen.

Wenn Sie mit der Maus über einen Job fahren, werden weitere Informationen angezeigt. Sie können zusätzliche Auftragsinformationen anzeigen, indem Sie auf eine bestimmte Auftragsnummer klicken. Dadurch werden Sie zur Monitorseite weitergeleitet. Von dort aus können Sie Auftragsdetails oder Protokollinformationen abrufen und einen spezifischen Bericht für diesen Auftrag erstellen.

Klicken Sie auf **Alle anzeigen**, um einen Verlauf aller SnapCenter -Jobs anzuzeigen.

Warnungen

Die Kachel „Warnungen“ zeigt die neuesten ungelösten kritischen und Warnmeldungen für die Hosts und den SnapCenter -Server an.

Die Gesamtzahl der Warnungen der Kategorien „Kritisch“ und „Warnung“ wird oben im Display angezeigt. Wenn Sie auf die Gesamtsummen „Kritisch“ oder „Warnung“ klicken, werden Sie auf die Seite „Warnungen“ weitergeleitet, auf der der jeweilige Filter angewendet wird.

Wenn Sie auf eine bestimmte Warnung klicken, werden Sie auf die Seite „Warnungen“ weitergeleitet, auf der Sie Einzelheiten zu dieser Warnung finden. Wenn Sie unten in der Anzeige auf **Alle anzeigen** klicken, werden Sie auf die Seite „Warnungen“ weitergeleitet, wo Sie eine Liste aller Warnungen sehen.

Neueste Schutzzusammenfassung

Die Kachel „Neueste Schutzzusammenfassung“ zeigt Ihnen den Schutzstatus für alle Entitäten an, auf die Sie Zugriff haben. Standardmäßig ist die Anzeige so eingestellt, dass der Status aller Plug-Ins angezeigt wird. Statusinformationen werden für Ressourcen bereitgestellt, die als Snapshots auf dem Primärspeicher und

mithilfe der Technologien SnapMirror und SnapVault auf dem Sekundärspeicher gesichert werden. Die Verfügbarkeit von Schutzstatusinformationen für den Sekundärspeicher hängt vom ausgewählten Plug-In-Typ ab.

Wenn Sie eine Mirror-Vault-Schutzrichtlinie verwenden, werden die Zähler für die Schutzzusammenfassung im SnapVault Zusammenfassungsdiagramm und nicht im SnapMirror Diagramm angezeigt.

Der Schutzstatus für einzelne Plug-Ins ist verfügbar, indem Sie ein Plug-In aus dem Dropdown-Menü auswählen. Ein Ringdiagramm zeigt den Prozentsatz der geschützten Ressourcen für das ausgewählte Plug-in. Durch Klicken auf ein Ringdiagramm gelangen Sie zur Seite **Berichte** > **Plug-in**, die einen detaillierten Bericht aller primären und sekundären Speicheraktivitäten für das angegebene Plug-in enthält.

Berichte zum Sekundärspeicher gelten nur für SnapVault ; SnapMirror -Berichte werden nicht unterstützt.

SAP HANA bietet Informationen zum Schutzstatus für den primären und sekundären Speicher für Snapshots. Für dateibasierte Sicherungen ist nur der Schutzstatus des primären Speichers verfügbar.

Schutzstatus	Primärspeicher	Sekundärspeicher
Fehlgeschlagen	Anzahl der Entitäten, die Teil einer Ressourcengruppe sind, wobei die Ressourcengruppe eine Sicherung ausgeführt hat, die Sicherung jedoch fehlgeschlagen ist.	Anzahl der Entitäten mit Sicherungen, deren Übertragung an ein sekundäres Ziel fehlgeschlagen ist.
Erfolgreich	Anzahl der Entitäten in einer Ressourcengruppe, wobei die Ressourcengruppe erfolgreich gesichert wurde.	Anzahl der Entitäten mit Sicherungen, die erfolgreich an ein sekundäres Ziel übertragen wurden.
Nicht konfiguriert	Anzahl der Entitäten, die nicht Teil einer Ressourcengruppe sind und nicht gesichert wurden.	Anzahl der Entitäten, die Teil einer oder mehrerer Ressourcengruppen sind, die nicht für die Übertragung von Sicherungen an ein sekundäres Ziel konfiguriert sind.
Nicht initiiert	Anzahl der Entitäten, die Teil einer Ressourcengruppe sind, für die aber keine Sicherung ausgeführt wurde.	Nicht zutreffend.

Wenn Sie SnapCenter Server 4.2 und eine frühere Version des Plug-Ins (älter als 4.2) zum Erstellen von Sicherungen verwenden, wird auf der Kachel „Neueste Schutzzusammenfassung“ der SnapMirror Schutzstatus dieser Sicherungen nicht angezeigt.

Jobs

Die Kachel „Jobs“ bietet Ihnen eine Zusammenfassung der Sicherungs-, Wiederherstellungs- und Klonjobs, auf die Sie Zugriff haben. Sie können den Zeitrahmen für jeden Bericht mithilfe des Dropdown-Menüs anpassen. Die Zeitrahmenoptionen sind auf die letzten 24 Stunden, die letzten 7 Tage und die letzten 30 Tage festgelegt. Der Standardbericht zeigt die Datenschutzjobs, die in den letzten 7 Tagen ausgeführt wurden.

Informationen zu Sicherungs-, Wiederherstellungs- und Klonaufträgen werden in Ringdiagrammen angezeigt. Wenn Sie auf ein Donut-Segment klicken, werden Sie zur Monitorseite weitergeleitet, auf deren Auswahl bereits Jobfilter angewendet sind.

Auftragsstatus	Beschreibung
Fehlgeschlagen	Anzahl der fehlgeschlagenen Jobs.
Warnung	Anzahl der Jobs, bei denen ein Fehler aufgetreten ist.
Erfolgreich	Anzahl der erfolgreich abgeschlossenen Jobs.
Wird ausgeführt	Anzahl der Jobs, die derzeit ausgeführt werden.

Storage

Die Kachel „Speicher“ zeigt den von Schutzaufträgen über einen Zeitraum von 90 Tagen verbrauchten Primär- und Sekundärspeicher an, stellt Verbrauchstrends grafisch dar und berechnet die Einsparungen beim Primärspeicher. Die Speicherinformationen werden alle 24 Stunden um 0 Uhr aktualisiert.

Der Gesamtverbrauch des Tages, der sich aus der Gesamtzahl der in SnapCenter verfügbaren Backups und der von diesen Backups belegten Größe zusammensetzt, wird oben auf dem Display angezeigt. Einem Backup können mehrere Snapshots zugeordnet sein und die Anzahl spiegelt dies wider. Dies gilt sowohl für primäre als auch für sekundäre Snapshots. Beispiel: Sie haben 10 Sicherungen erstellt, von denen 2 aufgrund der richtlinienbasierten Sicherungsaufbewahrung gelöscht werden und 1 Sicherung ausdrücklich von Ihnen gelöscht wird. Daher wird die Anzahl von 7 Sicherungen zusammen mit der von diesen 7 Sicherungen belegten Größe angezeigt.

Der Speichereinsparungsfaktor für den Primärspeicher ist das Verhältnis der logischen Kapazität (Einsparungen durch Klone und Snapshots plus verbrauchter Speicher) zur physischen Kapazität des Primärspeichers. Ein Balkendiagramm veranschaulicht die Speichereinsparungen.

Das Liniendiagramm stellt den Primär- und Sekundärspeicherverbrauch über einen rollierenden 90-Tage-Zeitraum hinweg getrennt auf Tagesbasis dar. Wenn Sie mit der Maus über die Diagramme fahren, werden detaillierte Tagesergebnisse angezeigt.

Wenn Sie SnapCenter Server 4.2 und eine frühere Version des Plug-Ins (älter als 4.2) zum Erstellen von Sicherungen verwenden, werden auf der Kachel „Speicher“ weder die Anzahl der Sicherungen, der von diesen Sicherungen belegte Speicher noch die Snapshot-Einsparungen, die Klon-Einsparungen und die Snapshot-Größe angezeigt.

Konfiguration

Die Kachel „Konfiguration“ bietet konsolidierte Statusinformationen für alle aktiven eigenständigen und Windows-Cluster-Hosts, die von SnapCenter verwaltet werden und auf die Sie Zugriff haben. Dazu gehören

die mit diesen Hosts verknüpften Plug-In-Statusinformationen.

Wenn Sie auf die Zahl neben „Hosts“ klicken, werden Sie zum Abschnitt „Verwaltete Hosts“ auf der Seite „Hosts“ weitergeleitet. Von dort aus können Sie detaillierte Informationen zu einem ausgewählten Host erhalten.

Darüber hinaus zeigt diese Anzeige die Summe der Standalone ONTAP SVMs und Cluster ONTAP SVMs, die von SnapCenter verwaltet werden und auf die Sie Zugriff haben. Wenn Sie auf die Zahl neben SVM klicken, werden Sie auf die Seite „Speichersysteme“ weitergeleitet. Von dort aus können Sie detaillierte Informationen zu einem ausgewählten SVM erhalten.

Der Hostkonfigurationsstatus wird zusammen mit der Anzahl der Hosts in jedem Status als Rot (kritisch), Gelb (Warnung) und Grün (aktiv) angezeigt. Für jeden Zustand werden Statusmeldungen bereitgestellt.

Konfigurationsstatus	**Beschreibung**
Upgrade obligatorisch	Anzahl der Hosts, die nicht unterstützte Plug-Ins ausführen und ein Upgrade benötigen. Ein nicht unterstütztes Plug-In ist mit dieser Version von SnapCenter nicht kompatibel.
Migration obligatorisch	Anzahl der Hosts, die nicht unterstützte Plug-Ins ausführen und migriert werden müssen. Ein nicht unterstütztes Plug-In ist mit dieser Version von SnapCenter nicht kompatibel.
Keine Plug-Ins installiert	Anzahl der Hosts, die erfolgreich hinzugefügt wurden, bei denen aber die Plug-Ins installiert werden müssen oder bei denen die Plug-In-Installation fehlgeschlagen ist.
Ausgesetzt	Anzahl der Hosts, deren Zeitpläne ausgesetzt sind und gewartet werden.
Gestoppt	Anzahl der Hosts, die aktiv sind, deren Plug-In-Dienste jedoch nicht ausgeführt werden.
Host ausgefallen	Anzahl der Hosts, die ausgefallen oder nicht erreichbar sind.
Upgrade verfügbar (optional)	Anzahl der Hosts, für die eine neuere Version des Plug-In-Pakets zum Upgrade verfügbar ist.
Migration verfügbar (optional)	Anzahl der Hosts, für die eine neuere Version des Plug-Ins zur Migration verfügbar ist.
Konfigurieren des Protokollverzeichnisses	Anzahl der Hosts, bei denen das Protokollverzeichnis für SCSQL konfiguriert werden muss, um eine Transaktionsprotokollsicherung durchzuführen.

Konfigurationsstatus	Beschreibung
Konfigurieren von VMware-Plug-Ins	Anzahl der Hosts, denen das SnapCenter Plug-in for VMware vSphere hinzugefügt werden muss.
Unbekannt	Anzahl der Hosts, die registriert wurden, deren Installation jedoch noch nicht ausgelöst wurde.
Wird ausgeführt	Anzahl der aktiven Hosts und ausgeführten Plug-Ins. Und im Fall von SCSQL-Plugins werden Log-Verzeichnis und Hypervisor konfiguriert.
Installieren/Deinstallieren von Plug-Ins	Anzahl der Hosts, auf denen die Plug-In-Installation oder -Deinstallation läuft.

So zeigen Sie Informationen auf dem Dashboard an

Im linken Navigationsbereich von SnapCenter können Sie verschiedene Dashboard-Kacheln oder Anzeigen zusammen mit den zugehörigen Systemdetails anzeigen. Die Anzahl der im Dashboard verfügbaren Anzeigen ist festgelegt und kann nicht geändert werden. Der in jeder Anzeige bereitgestellte Inhalt hängt von der rollenbasierten Zugriffskontrolle (RBAC) ab.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Dashboard**.
2. Klicken Sie auf die aktiven Bereiche auf jedem Display, um zusätzliche Informationen zu erhalten.

   Wenn Sie beispielsweise in **Jobs** auf ein Ringdiagramm klicken, werden Sie auf die Monitorseite weitergeleitet, wo Sie weitere Informationen zu Ihrer Auswahl erhalten. Wenn Sie in der **Schutzzusammenfassung** auf ein Ringdiagramm klicken, werden Sie auf die Seite „Berichte“ weitergeleitet, auf der Sie weitere Informationen zu Ihrer Auswahl erhalten.

Fordern Sie Statusberichte der Jobs vom Dashboard an

Sie können auf der Dashboard-Seite Berichte zu Sicherungs-, Wiederherstellungs- und Klonaufträgen anfordern. Dies ist nützlich, wenn Sie die Gesamtzahl der erfolgreichen oder fehlgeschlagenen Jobs in Ihrer SnapCenter -Umgebung ermitteln möchten.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Dashboard**
2. Suchen Sie im Dashboard nach der Kachel „Jobs“ und wählen Sie dann **Backup**, **Wiederherstellen** oder **Klonen**.
3. Wählen Sie mithilfe des Pulldown-Menüs den Zeitraum aus, für den Sie Jobinformationen wünschen: 24 Stunden, 7 Tage oder 30 Tage.

   Die Systeme zeigen ein Donut-Diagramm an, das die Daten abdeckt.

4. Klicken Sie auf das Donut-Segment, das die Auftragsinformationen darstellt, für die Sie einen Bericht wünschen.

   Wenn Sie auf das Ringdiagramm klicken, werden Sie von der Dashboard-Seite zur Monitor-Seite weitergeleitet. Auf der Seite „Überwachen“ werden die Jobs mit dem Status angezeigt, den Sie im Ringdiagramm ausgewählt haben.

5. Klicken Sie in der Liste der Monitorseite auf einen bestimmten Job, um ihn auszuwählen.
6. Klicken Sie oben auf der Monitorseite auf **Berichte**.

Ergebnis

Der Bericht zeigt nur Informationen zu dem von Ihnen ausgewählten Job an. Sie können den Bericht überprüfen oder auf Ihr lokales System herunterladen.

Fordern Sie Berichte zum Schutzstatus vom Dashboard an

Sie können über das Dashboard Schutzdetails für Ressourcen anfordern, die von bestimmten Plug-ins verwaltet werden. Für die Datenschutzzusammenfassung werden ausschließlich Datensicherungen berücksichtigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Dashboard**.
2. Suchen Sie im Dashboard nach der Kachel „Neueste Schutzzusammenfassung“ und wählen Sie über das Pulldown-Menü ein Plug-In aus.

   Das Dashboard zeigt ein Ringdiagramm für im primären Speicher gesicherte Ressourcen und, falls für das Plug-In zutreffend, ein Ringdiagramm für im sekundären Speicher gesicherte Ressourcen an.

   Datenschutzberichte sind nur für bestimmte Plug-In-Typen verfügbar. Die Angabe von **Alle Plug-ins** wird nicht unterstützt.

3. Klicken Sie auf das Donut-Segment, das den Status darstellt, für den Sie einen Bericht wünschen.

   Wenn Sie auf das Ringdiagramm klicken, werden Sie von der Dashboard-Seite zu den Berichten und dann zur Plug-in-Seite weitergeleitet. Der Bericht zeigt nur den Status für das von Ihnen ausgewählte Plug-In an. Sie können den Bericht überprüfen oder auf Ihr lokales System herunterladen.

   Die Umleitung zur Berichtsseite für SnapMirror -Ringdiagramme und dateibasierte SAP HANA-Sicherungen wird nicht unterstützt.

RBAC verwalten

Mit SnapCenter können Sie Rollen, Benutzer und Gruppen ändern.

Ändern einer Rolle

Sie können eine SnapCenter -Rolle ändern, um Benutzer oder Gruppen zu entfernen und die mit der Rolle verknüpften Berechtigungen zu ändern. Das Ändern von Rollen ist besonders dann sinnvoll, wenn Sie die von

einer ganzen Rolle verwendeten Berechtigungen ändern oder entfernen möchten.

Bevor Sie beginnen

Sie müssen sich mit der Rolle „SnapCenterAdmin“ angemeldet haben.

Sie können die Berechtigungen für die Rolle „SnapCenterAdmin“ weder ändern noch entfernen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Rollen**.
3. Klicken Sie im Feld „Rollenname“ auf die Rolle, die Sie ändern möchten.
4. Wählen Sie **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen** aus, um anderen Mitgliedern der Rolle das Anzeigen von Ressourcen wie Volumes und Hosts zu ermöglichen, nachdem sie die Ressourcenliste aktualisiert haben.

   Deaktivieren Sie diese Option, wenn Sie nicht möchten, dass Mitglieder dieser Rolle Objekte sehen, denen andere Mitglieder zugewiesen sind.

   Wenn diese Option aktiviert ist, ist es nicht erforderlich, Benutzern Zugriff auf Objekte oder Ressourcen zuzuweisen, wenn die Benutzer derselben Rolle angehören wie der Benutzer, der die Objekte oder Ressourcen erstellt hat.

5. Ändern Sie auf der Seite „Rollendetails“ die Berechtigungen oder heben Sie die Zuweisung der Mitglieder nach Bedarf auf.
6. Klicken Sie auf **Senden**.

Benutzer und Gruppen ändern

Sie können SnapCenter Benutzer oder -Gruppen ändern, um ihre Rollen und Ressourcen zu verändern.

Bevor Sie beginnen

Sie müssen als SnapCenter Administrator angemeldet sein.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Benutzer und Zugriff**.
3. Klicken Sie in der Liste „Benutzer- oder Gruppenname“ auf den Benutzer oder die Gruppe, den/die Sie ändern möchten.
4. Ändern Sie auf der Benutzer- oder Gruppendetailseite Rollen und Assets.
5. Klicken Sie auf **Senden**.

Hosts verwalten

Sie können Hosts hinzufügen und SnapCenter Plug-In-Pakete installieren, einen Verifizierungsserver hinzufügen, Hosts entfernen, Sicherungsaufträge migrieren und Hosts aktualisieren, um Plug-In-Pakete zu aktualisieren oder neue Plug-In-Pakete

hinzuzufügen. Je nach verwendetem Plug-In können Sie auch Datenträger bereitstellen, SMB-Freigaben verwalten, Initiatorgruppen (igroups) verwalten, iSCSI-Sitzungen verwalten und Daten migrieren.

Sie können diese Aufgaben ausführen…	Für Microsoft Exchange Server	Für Microsoft SQL Server	Für Microsoft Windows	Für Oracle-Datenbanken	Für SAP HANA-Datenbank	Für NetApp unterstützte Plug-Ins	Für Db2	Für PostgreSQL	Für MySQL
Hosts hinzufügen und Plug-In-Paket installieren	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Aktualisieren der ESXi-Informationen für einen Host	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein
Zeitpläne aussetzen und Hosts in den Wartungsmodus versetzen	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Ändern Sie Hosts, indem Sie Plug-Ins hinzufügen, aktualisieren oder entfernen	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Sie können diese Aufgaben ausführen…	Für Microsoft Exchange Server	Für Microsoft SQL Server	Für Microsoft Windows	Für Oracle-Datenbanken	Für SAP HANA-Datenbank	Für NetApp unterstützte Plug-Ins	Für Db2	Für PostgreSQL	Für MySQL
Hosts aus SnapCenter entfernen	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Plug-In-Dienste starten (gilt nur für Plug-Ins, die auf einem Windows-Host ausgeführt werden)	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja
Bereitstellen von Datenträgern	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein
Verwalten von SMB-Freigaben	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein
iGroups verwalten	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein
Verwalten von iSCSI-Sitzungen	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein

Aktualisieren der Informationen zur virtuellen Maschine

Sie sollten die Informationen Ihrer virtuellen Maschine aktualisieren, wenn sich die Anmeldeinformationen für

VMware vCenter ändern oder der Datenbank- oder Dateisystemhost neu gestartet wird. Durch das Aktualisieren Ihrer virtuellen Maschineninformationen in SnapCenter wird die Kommunikation mit dem VMware vSphere vCenter initiiert und die vCenter-Anmeldeinformationen abgerufen.

RDM-basierte Festplatten werden vom SnapCenter -Plug-in für Microsoft Windows verwaltet, das auf dem Datenbankhost installiert ist. Zur Verwaltung von RDMs kommuniziert das SnapCenter -Plug-in für Microsoft Windows mit dem vCenter-Server, der den Datenbankhost verwaltet.

Schritte

1. Klicken Sie im linken Navigationsbereich von SnapCenter auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Verwaltete Hosts**.
3. Wählen Sie auf der Seite „Verwaltete Hosts“ den Host aus, den Sie aktualisieren möchten.
4. Klicken Sie auf **VM aktualisieren**.

Plug-In-Hosts ändern

Nach der Installation eines Plug-Ins können Sie die Details des Plug-In-Hosts bei Bedarf ändern. Sie können Anmeldeinformationen, Installationspfad, Plug-Ins, Protokollverzeichnisdetails für das SnapCenter -Plug-In für Microsoft SQL Server, das gruppenverwaltete Dienstkonto (gMSA) und den Plug-In-Port ändern.

Stellen Sie sicher, dass die Plug-in-Version mit der SnapCenter Server-Version übereinstimmt.

Über diese Aufgabe

- Sie können einen Plug-In-Port erst ändern, nachdem das Plug-In installiert wurde.

  Während der Ausführung von Upgrade-Vorgängen können Sie den Plug-In-Port nicht ändern.

- Beim Ändern eines Plug-In-Ports sollten Sie sich der folgenden Port-Rollback-Szenarien bewusst sein:
  - Wenn SnapCenter in einer eigenständigen Konfiguration den Port einer der Komponenten nicht ändern kann, schlägt der Vorgang fehl und der alte Port wird für alle Komponenten beibehalten.

    Wurde der Port bei allen Komponenten geändert, eine Komponente startet jedoch nicht mit dem neuen Port, bleibt der alte Port bei allen Komponenten erhalten. Wenn Sie beispielsweise den Port für zwei Plug-Ins auf dem eigenständigen Host ändern möchten und SnapCenter den neuen Port nicht auf eines der Plug-Ins anwenden kann, schlägt der Vorgang fehl (mit einer entsprechenden Fehlermeldung) und der alte Port wird für beide Plug-Ins beibehalten.

  - Wenn SnapCenter in einer Clusterkonfiguration den Port des auf einem der Knoten installierten Plug-Ins nicht ändern kann, schlägt der Vorgang fehl und der alte Port wird für alle Knoten beibehalten.

    Wenn das Plug-In beispielsweise auf vier Knoten in einer Clusterkonfiguration installiert ist und der Port für einen der Knoten nicht geändert wird, bleibt der alte Port für alle Knoten erhalten.

Wenn Plug-Ins mit gMSA installiert werden, können Sie im Fenster **Weitere Optionen** Änderungen vornehmen. Wenn Plug-Ins ohne gMSA installiert werden, können Sie das gMSA-Konto angeben, um es als Plug-In-Dienstkonto zu verwenden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Stellen Sie sicher, dass oben **Managed Hosts** ausgewählt ist.
3. Wählen Sie den Host aus, für den Sie Änderungen vornehmen möchten, und ändern Sie ein beliebiges Feld.

   Es kann immer nur ein Feld gleichzeitig geändert werden.
4. Klicken Sie auf **Senden**.

Ergebnis

Der Host wird validiert und zum SnapCenter -Server hinzugefügt.

Starten oder Neustarten von Plug-In-Diensten

Durch das Starten der SnapCenter Plug-In-Dienste können Sie Dienste starten, wenn sie nicht ausgeführt werden, oder sie neu starten, wenn sie ausgeführt werden. Möglicherweise möchten Sie die Dienste nach der Durchführung der Wartung neu starten.

Sie sollten sicherstellen, dass beim Neustart der Dienste keine Jobs ausgeführt werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Verwaltete Hosts**.
3. Wählen Sie auf der Seite „Verwaltete Hosts“ den Host aus, den Sie starten möchten.
4. Klicken Symbol und klicken Sie auf **Dienst starten** oder **Dienst neu starten**.

   Sie können den Dienst mehrerer Hosts gleichzeitig starten oder neu starten.

Zeitpläne für Host-Wartung aussetzen

Wenn Sie verhindern möchten, dass der Host geplante SnapCenter -Jobs ausführt, können Sie Ihren Host in den Wartungsmodus versetzen. Sie sollten dies tun, bevor Sie die Plug-Ins aktualisieren oder wenn Sie Wartungsaufgaben auf Hosts durchführen.

Sie können die Zeitpläne auf einem ausgefallenen Host nicht anhalten, da SnapCenter nicht mit diesem Host kommunizieren kann.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Verwaltete Hosts**.
3. Wählen Sie auf der Seite „Verwaltete Hosts“ den Host aus, den Sie sperren möchten.
4. Klicken Sie auf das und klicken Sie dann auf **Zeitplan anhalten**, um den Host für dieses Plug-In in den Wartungsmodus zu versetzen.

   Sie können den Zeitplan mehrerer Hosts gleichzeitig aussetzen.

Sie müssen den Plug-In-Dienst nicht zuerst beenden. Der Plug-In-Dienst kann ausgeführt oder gestoppt werden.

Ergebnis

Nachdem Sie die Zeitpläne auf dem Host ausgesetzt haben, wird auf der Seite „Verwaltete Hosts“ im Feld „Gesamtstatus“ für den Host der Eintrag **Ausgesetzt** angezeigt.

Nachdem Sie die Hostwartung abgeschlossen haben, können Sie den Host aus dem Wartungsmodus holen, indem Sie auf **Zeitplan aktivieren** klicken. Sie können den Zeitplan mehrerer Hosts gleichzeitig aktivieren.

Von der Seite „Ressourcen“ unterstützte Vorgänge

Auf der Seite „Ressourcen“ können Sie Ressourcen ermitteln und Datenschutzvorgänge durchführen. Die Vorgänge, die Sie ausführen können, unterscheiden sich je nach dem Plug-In, das Sie zum Verwalten Ihrer Ressourcen verwenden.

Auf der Seite „Ressourcen“ können Sie die folgenden Aufgaben ausführen:

Sie können diese Aufgaben ausführen…	Für Microsoft Exchange Server	Für Microsoft SQL Server	Für Microsoft Windows	Für Oracle-Datenbanken	Für SAP HANA-Datenbank
Ermitteln, ob Ressourcen für die Sicherung verfügbar sind	Ja	Ja	Ja	Ja	Ja
Führen Sie bei Bedarf eine Sicherung einer Ressource durch	Ja	Ja	Ja	Ja	Ja
Wiederherstellen aus Backups	Ja	Ja	Ja	Ja	Ja
Klonen von Backups	Nein	Ja	Ja	Ja	Ja
Backups verwalten	Ja	Ja	Ja	Ja	Ja
Verwalten von Klonen	Nein	Ja	Ja	Ja	Ja
Richtlinien verwalten	Ja	Ja	Ja	Ja	Ja

Sie können diese Aufgaben ausführen…	Für Microsoft Exchange Server	Für Microsoft SQL Server	Für Microsoft Windows	Für Oracle-Datenbanken	Für SAP HANA-Datenbank
Speicherverbindungen verwalten	Ja	Ja	Ja	Ja	Ja
Mounten von Backups	Nein	Nein	Nein	Ja	Nein
Sicherungen aushängen	Nein	Nein	Nein	Ja	Nein
Details anzeigen	Ja	Ja	Ja	Ja	Ja

Richtlinien verwalten

Sie können Richtlinien von einer Ressource oder Ressourcengruppe trennen, ändern, löschen, anzeigen und kopieren.

Richtlinien ändern

Sie können die Replikationsoptionen, die Einstellungen für die Snapshot-Aufbewahrung, die Anzahl der Wiederholungsversuche bei Fehlern oder die Skriptinformationen ändern, während eine Richtlinie an eine Ressource oder Ressourcengruppe angehängt ist. Sie können den Zeitplantyp (Häufigkeit) erst ändern, nachdem Sie eine Richtlinie getrennt haben.

Über diese Aufgabe

Das Ändern des Zeitplantyps in einer Richtlinie erfordert zusätzliche Schritte, da der SnapCenter Server den Zeitplantyp nur zu dem Zeitpunkt registriert, zu dem die Richtlinie einer Ressource oder Ressourcengruppe zugeordnet wird.

Wenn Sie wollen…	Dann…
Einen zusätzlichen Zeitplantyp hinzufügen	Erstellen Sie eine neue Richtlinie und hängen Sie sie an die erforderlichen Ressourcen oder Ressourcengruppen an. Wenn beispielsweise eine Ressourcengruppenrichtlinie nur stündliche Sicherungen vorgibt und Sie auch tägliche Sicherungen hinzufügen möchten, können Sie eine Richtlinie mit einem täglichen Zeitplantyp erstellen und sie der Ressourcengruppe hinzufügen. Die Ressourcengruppe hätte dann zwei Richtlinien: stündlich und täglich.

Wenn Sie wollen…	Dann…
Entfernen oder Ändern eines Zeitplantyps	Führen Sie die folgenden Schritte aus: 1. Trennen Sie die Richtlinie von jeder Ressource und Ressourcengruppe, die diese Richtlinie verwendet. 2. Ändern Sie den Zeitplantyp. 3. Fügen Sie die Richtlinie erneut allen Ressourcen und Ressourcengruppen hinzu. Wenn beispielsweise eine Richtlinie stündliche Sicherungen vorsieht und Sie diese in tägliche Sicherungen ändern möchten, müssen Sie die Richtlinie zuerst trennen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Richtlinien**.
3. Wählen Sie die Richtlinie aus und klicken Sie dann auf **Ändern**.
4. Ändern Sie die Informationen und klicken Sie dann auf **Fertig**.

Richtlinien trennen

Sie können Richtlinien jederzeit von einer Ressource oder Ressourcengruppe trennen, wenn Sie nicht mehr möchten, dass diese Richtlinien den Datenschutz für die Ressourcen regeln. Sie müssen eine Richtlinie trennen, bevor Sie sie löschen oder den Zeitplantyp ändern können.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Anzeigen“ die Option „Ressourcengruppe“ aus.
3. Wählen Sie die Ressourcengruppe aus und klicken Sie dann auf **Ressourcengruppe ändern**.
4. Deaktivieren Sie auf der Seite „Richtlinien“ des Assistenten „Ressourcengruppe ändern“ in der Dropdownliste das Häkchen neben den Richtlinien, die Sie trennen möchten.
5. Nehmen Sie im Rest des Assistenten weitere Änderungen an der Ressourcengruppe vor und klicken Sie dann auf **Fertig**.

Richtlinien löschen

Wenn Sie Richtlinien nicht mehr benötigen, möchten Sie sie möglicherweise löschen.

Bevor Sie beginnen

Sie sollten die Richtlinie von Ressourcen oder Ressourcengruppen trennen, wenn die Richtlinie mit Ressourcen oder Ressourcengruppen verknüpft ist.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Richtlinien**.
3. Wählen Sie die Richtlinie aus und klicken Sie dann auf **Löschen**.
4. Klicken Sie auf **Ja**.

Verwalten von Ressourcengruppen

Sie können verschiedene Vorgänge an Ressourcengruppen durchführen.

Sie können die folgenden Aufgaben im Zusammenhang mit Ressourcengruppen ausführen:

- Ändern Sie eine Ressourcengruppe, indem Sie die Ressourcengruppe auswählen und auf **Ressourcengruppe ändern** klicken, um die Informationen zu bearbeiten, die Sie beim Erstellen der Ressourcengruppe angegeben haben.

  Sie können den Zeitplan ändern, während Sie die Ressourcengruppe ändern. Um den Zeitplantyp zu ändern, müssen Sie jedoch die Richtlinie ändern.

  Wenn Sie Ressourcen aus einer Ressourcengruppe entfernen, werden die in den aktuell mit der Ressourcengruppe verknüpften Richtlinien definierten Einstellungen zur Sicherungsaufbewahrung weiterhin auf die entfernten Ressourcen angewendet.

- Erstellen Sie eine Sicherung einer Ressourcengruppe.
- Erstellen Sie einen Klon einer Sicherung.

  Sie können aus den vorhandenen Sicherungen von SQL, Oracle, Windows-Dateisystemen, benutzerdefinierten Anwendungen und SAP HANA-Datenbankressourcen oder -Ressourcengruppen klonen.

- Erstellen Sie einen Klon einer Ressourcengruppe.

  Dieser Vorgang wird nur für SQL-Ressourcengruppen unterstützt (die nur Datenbanken enthalten). Sie können einen Zeitplan zum Klonen einer Ressourcengruppe (Klon-Lebenszyklus) konfigurieren.

- Verhindern Sie, dass geplante Vorgänge für Ressourcengruppen gestartet werden.
- Löschen Sie eine Ressourcengruppe.

Stoppen und Fortsetzen von Vorgängen für Ressourcengruppen

Sie können den Start geplanter Vorgänge für eine Ressourcengruppe vorübergehend deaktivieren. Sie können diese Vorgänge später bei Bedarf aktivieren.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Anzeigen“ die Option „Ressourcengruppe“ aus.
3. Wählen Sie die Ressourcengruppe aus und klicken Sie auf **Wartung**.
4. Klicken Sie auf **OK**.

Wenn Sie den Betrieb der Ressourcengruppe fortsetzen möchten, die Sie in den Wartungsmodus versetzt haben, wählen Sie die Ressourcengruppe aus und klicken Sie auf **Produktion**.

Ressourcengruppen löschen

Sie können eine Ressourcengruppe löschen, wenn Sie die Ressourcen in der Ressourcengruppe nicht mehr schützen müssen. Sie müssen sicherstellen, dass Ressourcengruppen gelöscht werden, bevor Sie Plug-Ins aus SnapCenter entfernen.

Über diese Aufgabe

Sie sollten alle für eine der Ressourcen in der Ressourcengruppe erstellten Klone manuell löschen. Sie können optional das Löschen aller mit der Ressourcengruppe verknüpften Sicherungen, Metadaten, Richtlinien und Snapshots erzwingen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Anzeigen“ die Option „Ressourcengruppe“ aus.
3. Wählen Sie die Ressourcengruppe aus und klicken Sie dann auf **Löschen**.
4. Optional: Aktivieren Sie das Kontrollkästchen **Mit dieser Ressourcengruppe verknüpfte Sicherungen löschen und Richtlinien trennen**, um alle mit der Ressourcengruppe verknüpften Sicherungen, Metadaten, Richtlinien und Snapshots zu entfernen.
5. Klicken Sie auf **OK**.

Backups verwalten

Sie können Backups umbenennen und löschen. Sie können auch mehrere Backups gleichzeitig löschen.

Backups umbenennen

Sie können Sicherungen umbenennen, wenn Sie einen besseren Namen angeben möchten, um die Suchbarkeit zu verbessern.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ entweder die Ressource oder die Ressourcengruppe aus der Dropdownliste **Anzeigen** aus.
3. Wählen Sie die Ressource oder Ressourcengruppe aus der Liste aus.

   Die Topologieseite der Ressource oder Ressourcengruppe wird angezeigt. Wenn die Ressource oder Ressourcengruppe nicht für den Datenschutz konfiguriert ist, wird anstelle der Topologieseite der Schutzassistent angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** aus den primären Speichersystemen aus.

   Sie können die Sicherungen, die sich auf dem sekundären Speichersystem befinden, nicht umbenennen.

Wenn Sie die Sicherungen von Oracle-Datenbanken mit Oracle Recovery Manager (RMAN) katalogisiert haben, können Sie diese katalogisierten Sicherungen nicht umbenennen.

5. Wählen Sie die Sicherung aus und klicken Sie dann auf  .
6. Geben Sie im Feld **Backup umbenennen in** einen neuen Namen ein und klicken Sie auf **OK**.

Backups löschen

Sie können Sicherungen löschen, wenn Sie die Sicherung für andere Datenschutzvorgänge nicht mehr benötigen.

Bevor Sie beginnen

Vor dem Löschen eines Backups müssen Sie die zugehörigen Klone gelöscht haben.

Wenn eine Sicherung mit einer geklonten Ressource verknüpft ist, können Sie die Sicherung nicht löschen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ entweder die Ressource oder die Ressourcengruppe aus der Dropdownliste **Anzeigen** aus.
3. Wählen Sie die Ressource oder Ressourcengruppe aus der Liste aus.

   Die Topologieseite der Ressource oder Ressourcengruppe wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** aus den primären Speichersystemen aus.

   Sie können die Sicherungen, die sich auf dem sekundären Speichersystem befinden, nicht löschen.

5. Wählen Sie die Sicherung aus und klicken Sie dann auf  .

   Wenn Sie eine SAP HANA-Datenbanksicherung löschen, werden auch die zugehörigen SAP HANA-Kataloge der Sicherung gelöscht.

   Wenn die letzte verbleibende Sicherung gelöscht wird, können die zugehörigen HANA-Katalogeinträge nicht gelöscht werden.

6. Klicken Sie auf **OK**.

   Wenn Sie in SnapCenter über veraltete Datenbanksicherungen verfügen, für die es keine entsprechenden Sicherungen auf dem Speichersystem gibt, müssen Sie den Befehl „remove-smbackup“ verwenden, um diese veralteten Sicherungseinträge zu bereinigen. Wenn die veralteten Sicherungen katalogisiert wurden, werden sie aus der Wiederherstellungskatalogdatenbank dekatalogisiert.

Schutz entfernen

Durch Entfernen des Schutzes werden alle Sicherungen gelöscht und alle Richtlinien getrennt. Bevor Sie den

Schutz entfernen, sollten Sie sicherstellen, dass die Sicherungen nicht gemountet sind und keine Klone mit der Sicherung verknüpft sind.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ entweder die Ressource oder die Ressourcengruppe aus der Dropdownliste **Anzeigen** aus.
3. Wählen Sie die Ressource oder Ressourcengruppe aus der Liste aus.

   Die Topologieseite der Ressource oder Ressourcengruppe wird angezeigt.

4. Wählen Sie die Sicherung aus und klicken Sie auf **Schutz entfernen**.

Klone löschen

Sie können Klone löschen, wenn Sie sie nicht mehr benötigen.

Über diese Aufgabe

Sie können keine Klone löschen, die als Quelle für andere Klone fungieren.

Wenn die Produktionsdatenbank beispielsweise db1 ist, wird die Datenbank clone1 aus der Sicherung von db1 geklont und anschließend clone1 geschützt. Die Datenbank „Klon2“ wird aus der Sicherung von „Klon1“ geklont. Wenn Sie Klon1 löschen möchten, müssen Sie zuerst Klon2 und dann Klon1 löschen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ entweder die Ressource oder die Ressourcengruppe aus der Dropdownliste **Anzeigen** aus.
3. Wählen Sie die Ressource oder Ressourcengruppe aus der Liste aus.

   Die Topologieseite der Ressource oder Ressourcengruppe wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Klone** entweder aus dem primären oder sekundären (gespiegelten oder replizierten) Speichersystem aus.
5. Wählen Sie den Klon aus und klicken Sie dann auf  .

   Wenn Sie SAP HANA-Datenbankklone löschen, führen Sie auf der Seite „Klone löschen“ die folgenden Aktionen aus:

   a. Geben Sie im Feld **Pre clone delete** die Befehle ein, die vor dem Löschen des Klons ausgeführt werden sollen.
   b. Geben Sie im Feld **Unmount** den Befehl zum Unmounten des Klons ein, bevor Sie ihn löschen.
6. Klicken Sie auf **OK**.

Nachdem Sie fertig sind

Manchmal werden die Dateisysteme nicht gelöscht. Sie müssen den Wert des Parameters CLONE_DELETE_DELAY erhöhen, indem Sie den folgenden Befehl ausführen: `./sccli Set-SmConfigSettings`

> Der Parameter CLONE_DELETE_DELAY gibt die Anzahl der Sekunden an, die nach Abschluss des Löschens des Anwendungsklons gewartet werden soll, bevor mit dem Löschen des Dateisystems begonnen wird.

Starten Sie den SnapCenter Plug-in Loader (SPL)-Dienst neu, nachdem Sie den Wert des Parameters geändert haben.

Überwachen Sie Jobs, Zeitpläne, Ereignisse und Protokolle

Auf der Seite „Überwachen“ können Sie den Fortschritt Ihrer Jobs überwachen, Informationen zu geplanten Jobs abrufen und Ereignisse und Protokolle überprüfen.

Überwachen von Jobs

Sie können Informationen zu SnapCenter -Sicherungs-, Klon-, Wiederherstellungs- und Überprüfungsaufträgen anzeigen. Sie können diese Ansicht nach Start- und Enddatum, Auftragstyp, Ressourcengruppe, Richtlinie oder SnapCenter -Plug-in filtern. Sie können auch zusätzliche Details und Protokolldateien für bestimmte Aufträge abrufen.

Sie können auch Jobs im Zusammenhang mit SnapMirror und SnapVault -Vorgängen überwachen.

> Sie können nur die Jobs überwachen, die Sie erstellt haben und die für Sie relevant sind, es sei denn, Ihnen wird die Rolle „SnapCenter -Administrator“ oder eine andere Superuser-Rolle zugewiesen.

Sie können die folgenden Aufgaben im Zusammenhang mit der Überwachung von Jobs ausführen:

- Überwachen Sie Sicherungs-, Klon-, Wiederherstellungs- und Überprüfungsvorgänge.
- Zeigen Sie Auftragsdetails und Berichte an.
- Stoppen Sie einen geplanten Job.

Verwalten geplanter Sicherungsaufträge

Ab der Version SnapCenter 6.0.1 wurde ein neuer Parameter **JobConcurrencyThreshold** eingeführt, der einen Schwellenwert für die Anzahl der geplanten Jobs festlegt, die zu einem bestimmten Zeitpunkt ausgeführt werden können. Auf diese Weise können Sie die Anzahl der Sicherungen, die Sie ausführen möchten, basierend auf der Hardwarekonfiguration Ihres Systems steuern.

Der **JobConcurrencyThreshold** zugewiesene Standardwert ist 0 und ist deaktiviert. Sie können die Funktion aktivieren, indem Sie einen Wert zuweisen, wenn Sie während des geplanten Sicherungsfensters eine Leistungsverschlechterung feststellen.

> Wenn Sie **JobConcurrencyThreshold** aktivieren, um gleichzeitige Jobs zu verwalten, können Sie mit SnapCenter die Reihenfolge der Sicherungen nicht steuern und die Sicherungen werden möglicherweise nicht zum im Zeitplan angegebenen Zeitpunkt ausgelöst.

Schritte

1. Legen Sie den Wert des Parameters *JobConcurrencyThreshold* fest, der sich unter _C:\Programme\ NetApp\ SnapCenter WebApp\ SnapManager befindet.
2. Starten Sie den SnapCenter -Anwendungspool neu, indem Sie auf IIS > Anwendungspools > SnapCenter > Neustart klicken.
3. Starten Sie den SnapCenter -Webdienst neu, indem Sie auf IIS > Sites > SnapCenter > Neustart klicken.

Verwalten veralteter Jobs

Veraltete Jobs entstehen durch Unterbrechungen in SnapCenter oder durch unsachgemäße Job-Updates. Ab der Version SnapCenter 6.0.1 wird ein vordefinierter Zeitplan eingeführt, um diese veralteten Jobs zu bereinigen, die länger als 72 Stunden feststecken. Sie können die Zeitplanhäufigkeit ändern, indem Sie den konfigurierbaren Parameter **CleanUpStaleJobsIntervalHours** bearbeiten.

Sie können die Bereinigung bei Bedarf auslösen, indem Sie den Zeitplan unter **Monitor** > **Zeitpläne** > **SnapCenter_StaleJobCleanUp** ausführen.

Schritte

1. Legen Sie den Wert des Parameters *CleanUpStaleJobsIntervalHours* fest, der sich unter _C:\Programme\ NetApp\ SnapCenter WebApp\ SnapManager befindet.
2. Starten Sie den SnapCenter -Anwendungspool neu, indem Sie auf IIS > Anwendungspools > SnapCenter > Neustart klicken.
3. Starten Sie den SnapCenter -Webdienst neu, indem Sie auf IIS > Sites > SnapCenter > Neustart klicken.

Zeitpläne überwachen

Möglicherweise möchten Sie aktuelle Zeitpläne anzeigen, um festzustellen, wann der Vorgang beginnt, wann er zuletzt ausgeführt wurde und wann er das nächste Mal ausgeführt wird. Sie können außerdem den Host bestimmen, auf dem der Vorgang ausgeführt wird, sowie die Ressourcengruppe und Richtlinieninformationen des Vorgangs.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite „Überwachen“ auf **Zeitpläne**.
3. Wählen Sie die Ressourcengruppe und den Zeitplantyp aus.
4. Zeigen Sie die Liste der geplanten Vorgänge an.

Überwachen von Ereignissen

Sie können eine Liste der SnapCenter -Ereignisse im System anzeigen, z. B. wenn ein Benutzer eine Ressourcengruppe erstellt oder wenn das System Aktivitäten initiiert, z. B. das Erstellen einer geplanten Sicherung. Möglicherweise möchten Sie Ereignisse anzeigen, um festzustellen, ob gerade ein Vorgang wie beispielsweise eine Sicherung oder Wiederherstellung ausgeführt wird.

Über diese Aufgabe

Alle Jobinformationen werden auf der Seite „Ereignisse“ angezeigt. Wenn beispielsweise ein Sicherungsauftrag gestartet wird, wird ein Ereignis „Sicherungsstart“ angezeigt. Wenn die Sicherung abgeschlossen ist, wird das Ereignis „Sicherung abgeschlossen“ angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite „Überwachen“ auf **Ereignisse**.
3. (Optional) Geben Sie im Feld „Filter“ das Start- oder Enddatum, die Ereigniskategorie (z. B. Sicherung, Ressourcengruppe oder Richtlinie) und den Schweregrad ein und klicken Sie auf „Übernehmen“. Alternativ können Sie Zeichen in das Suchfeld eingeben.
4. Sehen Sie sich die Liste der Ereignisse an.

Überwachen von Protokollen

Sie können SnapCenter -Serverprotokolle, SnapCenter Host-Agent-Protokolle und Plug-In-Protokolle anzeigen und herunterladen. Möglicherweise möchten Sie die Protokolle zur Unterstützung bei der Fehlerbehebung anzeigen.

Über diese Aufgabe

Sie können die Protokolle filtern, um nur einen bestimmten Protokollschweregrad anzuzeigen:

- Debuggen
- Info
- Warnen
- Fehler
- Tödlich

Sie können auch Protokolle auf Auftragsebene abrufen, beispielsweise Protokolle, die Ihnen bei der Fehlerbehebung bei einem fehlgeschlagenen Sicherungsauftrag helfen. Verwenden Sie für Protokolle auf Jobebene die Option **Monitor** > **Jobs**.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Wählen Sie auf der Seite „Jobs“ einen Job aus und klicken Sie auf „Protokolle herunterladen“.

   Der heruntergeladene ZIP-Ordner enthält die Jobprotokolle und die allgemeinen Protokolle. Der Name des komprimierten Ordners enthält die Job-ID und den ausgewählten Jobtyp.
3. Klicken Sie auf der Seite „Überwachen“ auf **Protokolle**.
4. Wählen Sie den Protokolltyp, den Host und die Instanz aus.

   Wenn Sie den Protokolltyp „Plugin“ auswählen, können Sie ein Host- oder SnapCenter -Plugin auswählen. Dies ist nicht möglich, wenn der Protokolltyp „Server“ ist.
5. Um die Protokolle nach einer bestimmten Quelle, Nachricht oder Protokollebene zu filtern, klicken Sie auf das Filtersymbol oben in der Spaltenüberschrift.

   Um alle Protokolle anzuzeigen, wählen Sie **Größer als oder gleich** als `Debug` Ebene.
6. Klicken Sie auf **Aktualisieren**.
7. Zeigen Sie die Liste der Protokolle an.
8. Klicken Sie auf **Herunterladen**, um die Protokolle herunterzuladen.

Der heruntergeladene ZIP-Ordner enthält die Jobprotokolle und die allgemeinen Protokolle. Der Name des komprimierten Ordners enthält die Job-ID und den ausgewählten Jobtyp.

In großen Konfigurationen sollten Sie für eine optimale Leistung die Protokolleinstellungen für SnapCenter mithilfe des PowerShell-Cmdlets auf ein minimales Niveau setzen.

```
Set-SmLogSettings -LogLevel All -MaxFileSize 10MB -MaxSizeRollBackups 10
-JobLogsMaxFileSize 10MB -Server
```

Um nach Abschluss eines Failover-Jobs auf Integritäts- oder Konfigurationsinformationen zuzugreifen, führen Sie das Cmdlet aus `Get-SmRepositoryConfig` .

Entfernen Sie Jobs und Protokolle aus SnapCenter

Sie können Sicherungs-, Wiederherstellungs-, Klon- und Überprüfungsaufträge sowie Protokolle aus SnapCenter entfernen. SnapCenter speichert erfolgreiche und fehlgeschlagene Jobprotokolle auf unbestimmte Zeit, sofern Sie sie nicht entfernen. Möglicherweise möchten Sie sie entfernen, um den Speicher aufzufüllen.

Über diese Aufgabe

Es dürfen derzeit keine Jobs ausgeführt werden. Sie können einen bestimmten Job entfernen, indem Sie eine Job-ID angeben, oder Sie können Jobs innerhalb eines bestimmten Zeitraums entfernen.

Sie müssen den Host nicht in den Wartungsmodus versetzen, um Jobs zu entfernen.

Schritte

1. Starten Sie PowerShell.
2. Geben Sie in der Eingabeaufforderung Folgendes ein: `Open-SMConnection`
3. Geben Sie in der Eingabeaufforderung Folgendes ein: `Remove-SmJobs`
4. Klicken Sie im linken Navigationsbereich auf **Monitor**.
5. Klicken Sie auf der Seite „Überwachen“ auf **Jobs**.
6. Überprüfen Sie auf der Seite „Jobs“ den Status des Jobs.

Ähnliche Informationen

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie auch auf die "Referenzhandbuch für SnapCenter -Software-Cmdlets" .

Übersicht über die Berichtsfunktionen von SnapCenter

SnapCenter bietet eine Vielzahl von Berichtsoptionen, mit denen Sie die Integrität und den Betriebserfolg Ihres Systems überwachen und verwalten können.

Berichtstyp	Beschreibung
Sicherungsbericht	Der Sicherungsbericht bietet allgemeine Daten zu Sicherungstrends für Ihre SnapCenter -Umgebung, zur Erfolgsrate der Sicherung und einige Informationen zu jeder Sicherung, die während des angegebenen Zeitraums durchgeführt wurde. Wenn ein Backup gelöscht wird, zeigt der Bericht keine Statusinformationen zum gelöschten Backup an. Der Sicherungsdetailbericht bietet ausführliche Informationen zu einem angegebenen Sicherungsauftrag und listet die erfolgreich gesicherten Ressourcen sowie alle Ressourcen auf, bei denen ein Backup fehlgeschlagen ist.
Klonbericht	Der Klonbericht bietet allgemeine Daten zu Klontrends für Ihre SnapCenter -Umgebung, zur Klonerfolgsrate und einige Informationen zu jedem Klonauftrag, der während der angegebenen Zeit ausgeführt wurde. Wenn ein Klon gelöscht wird, zeigt der Bericht keine Statusinformationen zum gelöschten Klon an. Der Klondetailbericht enthält Details zum angegebenen Klon, Klonhost und Status der Klonauftragsaufgabe. Wenn eine Aufgabe fehlschlägt, werden im Klondetailbericht Informationen zum Fehler angezeigt.
Wiederherstellungsbericht	Der Wiederherstellungsbericht bietet allgemeine Informationen zu Wiederherstellungsaufträgen. Der Wiederherstellungsdetailbericht enthält Einzelheiten zu einem angegebenen Wiederherstellungsjob, einschließlich Hostname, Sicherungsname, Jobstart und -dauer sowie den Status einzelner Jobaufgaben. Wenn eine Aufgabe fehlschlägt, werden im Wiederherstellungsdetailbericht Informationen zum Fehler angezeigt.
Schutzbericht	Diese Berichte enthalten Schutzdetails für Ressourcen, die von allen SnapCenter Plug-In-Instanzen verwaltet werden. Dieser Bericht enthält Schutzdetails für Ressourcen, die von allen Plug-in-Instanzen verwaltet werden. Sie können eine Übersicht, Details zu ungeschützten Ressourcen, Ressourcen, die zum Zeitpunkt der Berichterstellung nicht gesichert wurden, Ressourcen einer Ressourcengruppe, für die Sicherungsvorgänge fehlgeschlagen sind, und den SnapVault -Status anzeigen.

Berichtstyp	Beschreibung
Geplanter Bericht	Die Ausführung dieser Berichte ist in regelmäßigen Abständen geplant, beispielsweise täglich, wöchentlich oder monatlich. Die Berichte werden automatisch zum angegebenen Datum und zur angegebenen Uhrzeit erstellt und per E-Mail an die entsprechenden Personen gesendet. Sie können die Zeitpläne aktivieren, deaktivieren, ändern oder löschen. Der aktivierte Zeitplan kann bei Bedarf durch Klicken auf die Schaltfläche **Jetzt ausführen** ausgeführt werden. Der Administrator kann jeden Zeitplan ausführen, der generierte Bericht enthält jedoch Daten basierend auf der Berechtigung des Benutzers, der den Zeitplan erstellt hat. Jeder andere Benutzer außer dem Administrator kann den Zeitplan basierend auf seiner Berechtigung sehen oder ändern. Wenn auf der Seite „Rolle hinzufügen“ die Option „Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen“ ausgewählt ist, können andere Mitglieder dieser Rolle den Zeitplan sehen und ändern.

Zugriffsberichte

Mit dem SnapCenter -Dashboard können Sie sich schnell einen Überblick über den Zustand Ihres Systems verschaffen. Vom Dashboard aus können Sie weitere Details einsehen. Alternativ können Sie direkt auf die ausführlichen Berichte zugreifen.

Sie können auf Berichte mit einer der folgenden Methoden zugreifen:

- Klicken Sie im linken Navigationsbereich auf **Dashboard** und dann auf das Kreisdiagramm **Zusammenfassung des letzten Schutzes**, um auf der Seite „Berichte“ weitere Details anzuzeigen.
- Klicken Sie im linken Navigationsbereich auf **Berichte**.

Filtern Sie Ihren Bericht

Möglicherweise möchten Sie Ihre Berichtsdaten nach einer Reihe von Parametern filtern, je nach Detaillierungsgrad und Zeitraum der von Ihnen benötigten Informationen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Berichte**.
2. Wenn die Parameteransicht nicht angezeigt wird, klicken Sie in der Berichtssymbolleiste auf das Symbol **Parameterbereich umschalten**.
3. Geben Sie den Zeitraum an, für den Sie Ihren Bericht ausführen möchten. + Wenn Sie das Enddatum weglassen, rufen Sie alle verfügbaren Informationen ab.
4. Filtern Sie Ihre Berichtsinformationen anhand der folgenden Kriterien:
    - Ressourcengruppe

- Gastgeber
- Politik
- Ressource
- Status
- Plug-in-Name

5. Klicken Sie auf **Übernehmen**.

Berichte exportieren oder drucken

Durch das Exportieren von SnapCenter -Berichten können Sie den Bericht in einer Vielzahl alternativer Formate anzeigen. Sie können auch Berichte ausdrucken.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Berichte**.
2. Führen Sie in der Berichtssymbolleiste einen der folgenden Schritte aus:
   - Klicken Sie auf das Symbol **Druckvorschau umschalten**, um eine Vorschau eines druckbaren Berichts anzuzeigen.
   - Wählen Sie ein Format aus der Dropdown-Liste des Symbols **Exportieren** aus, um einen Bericht in ein anderes Format zu exportieren.
3. Um einen Bericht zu drucken, klicken Sie auf das Symbol **Drucken**.
4. Um eine bestimmte Berichtszusammenfassung anzuzeigen, scrollen Sie zum entsprechenden Abschnitt des Berichts.

SMTP-Server für E-Mail-Benachrichtigungen festlegen

Sie können den SMTP-Server angeben, der zum Senden von Datenschutz-Jobberichten an Sie selbst oder an andere verwendet werden soll. Sie können auch eine Test-E-Mail senden, um die Konfiguration zu überprüfen. Die Einstellungen werden global für jeden SnapCenter -Job angewendet, für den Sie eine E-Mail-Benachrichtigung konfigurieren.

Diese Option konfiguriert den SMTP-Server zum Senden aller Datenschutz-Jobberichte. Wenn Sie jedoch regelmäßige SnapCenter Datenschutzjob-Updates für eine bestimmte Ressource an sich selbst oder an andere senden möchten, damit Sie den Status dieser Updates überwachen können, können Sie beim Erstellen einer Ressourcengruppe die Option zum E-Mail-Versand der SnapCenter -Berichte konfigurieren.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Globale Einstellungen**.
3. Geben Sie den SMTP-Server ein und klicken Sie auf **Speichern**.
4. Um eine Test-E-Mail zu senden, geben Sie die E-Mail-Adresse ein, von der und an die Sie die E-Mail senden möchten, geben Sie den Betreff ein und klicken Sie auf **Senden**.

Konfigurieren Sie die Option zum Versenden von Berichten per E-Mail

Wenn Sie regelmäßige Updates zu SnapCenter -Datenschutzaufträgen an sich selbst oder andere senden lassen möchten, damit Sie den Status dieser Updates überwachen können, können Sie beim Erstellen einer

Ressourcengruppe die Option zum E-Mail-Versand der SnapCenter -Berichte konfigurieren.

Bevor Sie beginnen

Sie müssen Ihren SMTP-Server auf der Seite „Globale Einstellungen“ unter „Einstellungen“ konfiguriert haben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie den Ressourcentyp aus, den Sie anzeigen möchten, und klicken Sie auf **Neue Ressourcengruppe**, oder wählen Sie eine vorhandene Ressourcengruppe aus und klicken Sie auf **Ändern**, um E-Mail-Berichte für eine vorhandene Ressourcengruppe zu konfigurieren.
3. Wählen Sie im Benachrichtigungsbereich des Assistenten „Neue Ressourcengruppe“ aus dem Pulldown-Menü aus, ob Sie immer, bei Fehlern oder bei Fehlern oder Warnungen Berichte erhalten möchten.
4. Geben Sie die Adresse ein, von der die E-Mail gesendet wird, die Adresse, an die die E-Mail gesendet wird, und den Betreff der E-Mail.

Verwalten des SnapCenter Server-Repository

Informationen zu verschiedenen von SnapCenter ausgeführten Vorgängen werden im Datenbank-Repository des SnapCenter Servers gespeichert. Sie müssen Backups des Repositorys erstellen, um den SnapCenter -Server vor Datenverlust zu schützen.

Das SnapCenter Server-Repository wird manchmal als NSM-Datenbank bezeichnet.

Voraussetzungen zum Schutz des SnapCenter -Repositorys

Ihre Umgebung sollte bestimmte Voraussetzungen erfüllen, um das SnapCenter Repository zu schützen.

- Verwalten von Verbindungen virtueller Speichermaschinen (SVM)

  Sie sollten die Speicheranmeldeinformationen konfigurieren.

- Bereitstellen von Hosts

  Auf dem SnapCenter -Repository-Host sollte mindestens eine NetApp Speicherfestplatte vorhanden sein. Wenn auf dem SnapCenter -Repository-Host keine NetApp Festplatte vorhanden ist, müssen Sie eine erstellen.

  Einzelheiten zum Hinzufügen von Hosts, Einrichten von SVM-Verbindungen und Bereitstellen von Hosts finden Sie in den Installationsanweisungen.

- Bereitstellung von iSCSI LUN oder VMDK

  Für eine Hochverfügbarkeitskonfiguration (HA) können Sie entweder ein iSCSI-LUN oder ein VMDK auf einem der SnapCenter -Server bereitstellen.

Sichern Sie das SnapCenter Repository

Durch die Sicherung des SnapCenter Server-Repositorys können Sie es vor Datenverlust schützen. Sie können das Repository sichern, indem Sie das Cmdlet *Protect-SmRepository* ausführen.

Über diese Aufgabe

Das Cmdlet *Protect-SmRepository* führt die folgenden Aufgaben aus:

- Erstellt eine Ressourcengruppe und eine Richtlinie
- Erstellt einen Sicherungszeitplan für das SnapCenter -Repository

Schritte

1. Starten Sie PowerShell.
2. Richten Sie auf dem SnapCenter Server-Host eine Sitzung mit dem Cmdlet *Open-SmConnection* ein und geben Sie dann Ihre Anmeldeinformationen ein.
3. Sichern Sie das Repository mit dem Cmdlet *Protect-SmRepository* und den erforderlichen Parametern.

Anzeigen von Backups des SnapCenter -Repositorys

Sie können eine Liste der Datenbank-Repository-Sicherungen des SnapCenter Servers anzeigen, indem Sie das Cmdlet *Get-SmRepositoryBackups* ausführen.

Die Repository-Sicherungen werden gemäß dem im Cmdlet *Protect-SmRepository* angegebenen Zeitplan erstellt.

Schritte

1. Starten Sie PowerShell.
2. Geben Sie in der Eingabeaufforderung das folgende Cmdlet ein und geben Sie dann die Anmeldeinformationen für die Verbindung mit dem SnapCenter -Server ein: *Open-SMConnection*
3. Listen Sie alle verfügbaren SnapCenter -Datenbanksicherungen mit dem Cmdlet *Get-SmRepositoryBackups* auf.

Wiederherstellen des SnapCenter -Datenbankrepositorys

Sie können das SnapCenter Repository wiederherstellen, indem Sie das Cmdlet *Restore-SmRepositoryBackup* ausführen.

Wenn Sie das SnapCenter -Repository wiederherstellen, werden andere laufende SnapCenter Vorgänge beeinträchtigt, da während des Wiederherstellungsvorgangs nicht auf die Repository-Datenbank zugegriffen werden kann.

Schritte

1. Starten Sie PowerShell.
2. Geben Sie in der Eingabeaufforderung das folgende Cmdlet ein und geben Sie dann die Anmeldeinformationen für die Verbindung mit dem SnapCenter -Server ein: *Open-SMConnection*
3. Stellen Sie die Repository-Sicherung mit dem Cmdlet *Restore-SmRepositoryBackup* wieder her.

   Das folgende Cmdlet stellt das SnapCenter MySQL-Datenbank-Repository aus den auf iSCSI LUN oder VMDK vorhandenen Sicherungen wieder her:

```
C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mva-
x3550-s09_09-15-2016_10.32.00.4445
```

Das folgende Cmdlet stellt die SnapCenter MySQL-Datenbank wieder her, wenn Sicherungsdateien versehentlich im iSCSI-LUN gelöscht werden. Stellen Sie für VMDK das Backup manuell aus ONTAP -Snapshots wieder her.

```
C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mva-
x3550-s09_09-15-2016_10.32.00.4445 -RestoreFileSystem
```

Die Sicherung, die zum Ausführen des Repository-Wiederherstellungsvorgangs verwendet wurde, wird nicht aufgelistet, wenn die Repository-Sicherungen nach dem Ausführen des Wiederherstellungsvorgangs abgerufen werden.

Migrieren des SnapCenter -Repositorys

Sie können das Datenbank-Repository des SnapCenter Servers vom Standardspeicherort auf eine andere Festplatte migrieren. Sie können das Repository migrieren, wenn Sie es auf eine Festplatte mit mehr Speicherplatz verschieben möchten.

Schritte

1. Stoppen Sie den MYSQL57-Dienst in Windows.
2. Suchen Sie das MySQL-Datenverzeichnis.

   Normalerweise finden Sie das Datenverzeichnis unter C:\ProgramData\MySQL\MySQL Server 5.7\Data.
3. Kopieren Sie das MySQL-Datenverzeichnis an den neuen Speicherort, beispielsweise E:\Data\nsm.
4. Klicken Sie mit der rechten Maustaste auf das neue Verzeichnis und wählen Sie dann **Eigenschaften** > **Sicherheit**, um das lokale Serverkonto des Netzwerkdienstes zum neuen Verzeichnis hinzuzufügen und dem Konto dann Vollzugriff zuzuweisen.
5. Benennen Sie das ursprüngliche Datenbankverzeichnis um, beispielsweise in nsm_copy.
6. Erstellen Sie in einer Windows-Eingabeaufforderung mit dem Befehl *mklink* einen symbolischen Verzeichnislink.

   ```
   "mklink /d "C:\ProgramData\MySQL\MySQL Server 5.7\Data\nsm" "E:\Data\nsm" "
   ```
7. Starten Sie den MYSQL57-Dienst in Windows.
8. Überprüfen Sie, ob die Änderung des Datenbankspeicherorts erfolgreich war, indem Sie sich bei SnapCenter anmelden und die Repository-Einträge überprüfen oder indem Sie sich beim MySQL-Dienstprogramm anmelden und eine Verbindung zum neuen Repository herstellen.
9. Löschen Sie das ursprüngliche, umbenannte Datenbank-Repository-Verzeichnis (nsm_copy).

Setzen Sie das Kennwort für das SnapCenter -Repository zurück

Das Datenbankkennwort für das MySQL-Server-Repository wird während der SnapCenter -Serverinstallation

von SnapCenter 4.2 automatisch generiert. Dieses automatisch generierte Passwort ist dem SnapCenter -Benutzer zu keinem Zeitpunkt bekannt. Wenn Sie auf die Repository-Datenbank zugreifen möchten, sollten Sie das Passwort zurücksetzen.

Bevor Sie beginnen

Sie sollten über die Administratorrechte von SnapCenter verfügen, um das Kennwort zurückzusetzen.

Schritte

1. Starten Sie PowerShell.
2. Geben Sie in der Eingabeaufforderung den folgenden Befehl ein und geben Sie dann die Anmeldeinformationen für die Verbindung mit dem SnapCenter -Server ein: *Open-SMConnection*
3. Setzen Sie das Repository-Passwort zurück: *Set-SmRepositoryPassword*

   Der folgende Befehl setzt das Repository-Passwort zurück:

```
Set-SmRepositoryPassword at command pipeline position 1
Supply values for the following parameters:
NewPassword: ********
ConfirmPassword: ********
Successfully updated the MySQL server password.
```

Ähnliche Informationen

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie auch auf die "Referenzhandbuch für SnapCenter -Software-Cmdlets" .

Verwalten von Ressourcen nicht vertrauenswürdiger Domänen

SnapCenter verwaltet nicht nur Hosts in vertrauenswürdigen Active Directory-Domänen (AD), sondern auch Hosts in mehreren nicht vertrauenswürdigen AD-Domänen. Die nicht vertrauenswürdigen AD-Domänen müssen beim SnapCenter -Server registriert werden. SnapCenter unterstützt Benutzer und Gruppen mehrerer nicht vertrauenswürdiger AD-Domänen.

Sie können den SnapCenter -Server auf einem Computer installieren, der sich entweder in einer Domäne oder einer Arbeitsgruppe befindet. Um den SnapCenter -Server zu installieren, sollten Sie die Domänenanmeldeinformationen angeben, wenn sich der Computer in einer Domäne befindet, oder die lokalen Administratoranmeldeinformationen, wenn sich der Computer in einer Arbeitsgruppe befindet.

Active Directory (AD)-Gruppen, die zu Domänen gehören, die nicht beim SnapCenter -Server registriert sind, werden nicht unterstützt. Obwohl Sie mit diesen AD-Gruppen SnapCenter -Rollen erstellen können, schlägt die Anmeldung beim SnapCenter Server mit der folgenden Fehlermeldung fehl: Der Benutzer, bei dem Sie sich anmelden möchten, gehört keiner Rolle an. Bitte wenden Sie sich an den Administrator.

Ändern nicht vertrauenswürdiger Domänen

Sie können eine nicht vertrauenswürdige Domäne ändern, wenn Sie die IP-Adressen des Domänencontrollers oder den vollqualifizierten Domänennamen (FQDN) aktualisieren möchten.

Über diese Aufgabe

Nachdem Sie den FQDN geändert haben, funktionieren die zugehörigen Assets (Hosts, Benutzer und Gruppen) möglicherweise nicht wie erwartet.

Um eine nicht vertrauenswürdige Domäne zu ändern, können Sie entweder die SnapCenter Benutzeroberfläche oder PowerShell-Cmdlets verwenden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Globale Einstellungen**.
3. Klicken Sie auf der Seite „Globale Einstellungen“ auf **Domäneneinstellungen**.
4. Klicken  und geben Sie dann die folgenden Details an:

Für dieses Feld…	Machen Sie Folgendes…
Domänen-FQDN	Geben Sie den FQDN an und klicken Sie auf **Auflösen**.
IP-Adressen des Domänencontrollers	Wenn der Domänen-FQDN nicht aufgelöst werden kann, geben Sie eine oder mehrere IP-Adressen des Domänencontrollers an.

5. Klicken Sie auf **OK**.

Aufheben der Registrierung nicht vertrauenswürdiger Active Directory-Domänen

Sie können die Registrierung einer nicht vertrauenswürdigen Active Directory-Domäne aufheben, wenn Sie die mit dieser Domäne verknüpften Assets nicht verwenden möchten.

Bevor Sie beginnen

Sie sollten die Hosts, Benutzer, Gruppen und Anmeldeinformationen entfernt haben, die mit der nicht vertrauenswürdigen Domäne verknüpft sind.

Über diese Aufgabe

- Nachdem die Domäne vom SnapCenter -Server abgemeldet wurde, können Benutzer dieser Domäne nicht mehr auf den SnapCenter -Server zugreifen.
- Wenn zugehörige Assets (Hosts, Benutzer und Gruppen) vorhanden sind, sind diese Assets nach der Abmeldung der Domäne nicht mehr betriebsbereit.
- Um die Registrierung einer nicht vertrauenswürdigen Domäne aufzuheben, können Sie entweder die SnapCenter Benutzeroberfläche oder PowerShell-Cmdlets verwenden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Globale Einstellungen**.
3. Klicken Sie auf der Seite „Globale Einstellungen“ auf **Domäneneinstellungen**.
4. Wählen Sie aus der Domänenliste die Domäne aus, deren Registrierung Sie aufheben möchten.
5. Klicken und klicken Sie dann auf **OK**.

Verwalten des Speichersystems

Nachdem Sie das Speichersystem hinzugefügt haben, können Sie die Konfiguration und Verbindungen des Speichersystems ändern oder das Speichersystem löschen.

Ändern der Speichersystemkonfiguration

Sie können SnapCenter verwenden, um die Konfiguration Ihres Speichersystems zu ändern, wenn Sie den Benutzernamen, das Kennwort, die Plattform, den Port, das Protokoll, die Zeitüberschreitungsdauer, die bevorzugte IP-Adresse oder die Nachrichtenoptionen ändern möchten.

Über diese Aufgabe

Sie können Speicherverbindungen für einen einzelnen Benutzer oder für eine Gruppe ändern. Wenn Sie zu einer oder mehreren Gruppen mit Berechtigung für dasselbe Speichersystem gehören, wird der Name der Speicherverbindung in der Speicherverbindungsliste mehrmals angezeigt, einmal für jede Gruppe mit Berechtigung für das Speichersystem.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speichersysteme**.
2. Führen Sie auf der Seite „Speichersysteme“ im Dropdown-Menü **Typ** eine der folgenden Aktionen aus:

Wählen…	Schritte…
ONTAP SVMs	Um alle hinzugefügten virtuellen Speichermaschinen (SVMs) anzuzeigen und die erforderliche SVM-Konfiguration zu ändern. a. Klicken Sie auf der Seite „Speicherverbindungen“ auf den entsprechenden SVM-Namen. b. Führen Sie eine der folgenden Aktionen aus: ◦ Wenn die SVM nicht Teil eines Clusters ist, ändern Sie auf der Seite „Speichersystem ändern“ die Konfigurationen wie Benutzername, Kennwort, EMS- und AutoSupport -Einstellungen, Plattform, Protokoll, Port, Timeout und bevorzugte IP. ◦ Wenn die SVM Teil eines Clusters ist, wählen Sie auf der Seite „Speichersystem ändern“ die Option „SVM unabhängig verwalten“ und ändern Sie die Konfigurationen wie Benutzername, Kennwort, EMS- und AutoSupport -Einstellungen, Plattform, Protokoll, Port, Timeout und bevorzugte IP. Wenn Sie sich nach der Änderung der SVM für eine unabhängige Verwaltung für die Verwaltung über einen Cluster entscheiden, sollten Sie die SVM löschen und dann auf „Neu erkennen“ klicken. Die SVM wird dem ONTAP Cluster hinzugefügt. Wenn ein Speichersystemkennwort auf der SnapCenter -GUI aktualisiert wird, sollten Sie die SMCore-Dienste des jeweiligen Plug-Ins oder des Serverhosts neu starten, da das aktualisierte Kennwort nicht in SMCore angezeigt wird und die Sicherungsaufträge mit einem Fehler bezüglich falscher Anmeldeinformationen fehlschlagen.

Wählen…	Schritte…
ONTAP Cluster	Um alle hinzugefügten Cluster anzuzeigen und die erforderliche Clusterkonfiguration zu ändern. a. Klicken Sie auf der Seite „Speicherverbindungen“ auf den Clusternamen. b. Klicken Sie auf der Seite „Speichersystem ändern“ auf das Bearbeitungssymbol neben „Benutzername“ und ändern Sie den Benutzernamen und das Kennwort. c. Wählen oder löschen Sie die EMS- und AutoSupport -Einstellungen. d. Klicken Sie auf **Weitere Optionen** und ändern Sie andere Konfigurationen wie Plattform, Protokoll, Port, Timeout und bevorzugte IP.

3. Klicken Sie auf **Senden**.

Löschen Sie das Speichersystem

Mit SnapCenter können Sie alle nicht verwendeten Speichersysteme löschen.

Über diese Aufgabe

Sie können Speicherverbindungen für einen einzelnen Benutzer oder für eine Gruppe löschen. Wenn Sie zu einer oder mehreren Gruppen mit Berechtigung für dasselbe Speichersystem gehören, wird der Name des Speichersystems in der Speicherverbindungsliste mehrmals angezeigt, einmal für jede Gruppe mit Berechtigung für das Speichersystem.

Wenn Sie ein Speichersystem löschen, schlagen alle auf diesem Speichersystem ausgeführten Vorgänge fehl.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speichersysteme**.
2. Wählen Sie auf der Seite „Speichersysteme“ aus der Dropdown-Liste **Typ** entweder * ONTAP SVMs* oder * ONTAP Clusters* aus.
3. Aktivieren Sie auf der Seite „Speicherverbindungen“ entweder das Kontrollkästchen neben der SVM oder dem Cluster, den Sie löschen möchten.

   Sie können die SVM, die Teil eines Clusters ist, nicht auswählen.

4. Klicken Sie auf **Löschen**.
5. Klicken Sie auf der Seite „Verbindungseinstellungen des Speichersystems löschen“ auf **OK**.

   Wenn ein SVM mithilfe der ONTAP -GUI aus dem ONTAP Cluster gelöscht wird, klicken Sie in der SnapCenter -GUI auf **Neu erkennen**, um die SVM-Liste zu aktualisieren.

REST-API-Unterstützung

Alle ASA, AFF oder FAS -Systemverbindungen zu ONTAP erfolgen standardmäßig über ZAPI. REST API kann für bestimmte ONTAP Versionen aktiviert werden.

SnapCenter nutzt REST-APIs, um alle Vorgänge auf ASA r2-Systemen auszuführen, die ZAPIs nicht unterstützen.

Sie können die Konfigurationsschlüssel in den folgenden Konfigurationsdateien ändern:

- IsRestEnabledForStorageConnection

  Der Standardwert ist „false“.

- MinOntapVersionToUseREST

  Der Standardwert ist 9.13.1.

Verbindung über REST-API aktivieren

1. Setzen Sie IsRestEnabledForStorageConnection auf „true“.
2. Fügen Sie den Schlüssel in SMCoreServiceHost.dll.config und SnapDriveService.dll.config sowohl auf dem Server als auch auf den Windows-Plug-In-Hosts hinzu.

   <add key="IsRestEnabledForStorageConnection" value="true" />

Beschränken Sie die Verbindung über die REST-API auf eine bestimmte ONTAP Version.

1. Setzen Sie den Konfigurationsparameter MinOntapVersionToUseREST auf „true“.
2. Fügen Sie den Schlüssel in SMCoreServiceHost.dll.config und SnapDriveService.dll.config sowohl auf dem Server als auch auf den Windows-Plug-In-Hosts hinzu.

   <add key="MinOntapVersionToUseREST" value="9.13.1" />

3. Starten Sie den Dienst für SmCore auf dem Server und den Plug-In- und SnapDrive -Dienst auf der Plug-In-Maschine neu.

Verwalten der EMS-Datenerfassung

Sie können die Datenerfassung des Event Management System (EMS) mithilfe von PowerShell-Cmdlets planen und verwalten. Bei der EMS-Datenerfassung werden Details zum SnapCenter -Server, den installierten SnapCenter Plug-In-Paketen, den Hosts und ähnlichen Informationen gesammelt und anschließend an eine angegebene ONTAP Storage Virtual Machine (SVM) gesendet.

Die CPU-Auslastung des Systems ist hoch, wenn eine Datenerfassungsaufgabe ausgeführt wird. Die CPU-Auslastung bleibt hoch, solange der Vorgang ausgeführt wird, unabhängig von der Datengröße.

Stoppen Sie die EMS-Datenerfassung

Die EMS-Datenerfassung ist standardmäßig aktiviert und wird alle sieben Tage nach Ihrem Installationsdatum

ausgeführt. Sie können die Datenerfassung jederzeit mithilfe des PowerShell-Cmdlets *Disable-SmDataCollectionEMS* deaktivieren.

Schritte

1. Stellen Sie über eine PowerShell-Befehlszeile eine Sitzung mit SnapCenter her, indem Sie *Open-SmConnection* eingeben.
2. Deaktivieren Sie die EMS-Datenerfassung, indem Sie *Disable-SmDataCollectionEms* eingeben.

Starten Sie die EMS-Datenerfassung

Die EMS-Datenerfassung ist standardmäßig aktiviert und wird ab dem Installationsdatum alle sieben Tage ausgeführt. Wenn Sie es deaktiviert haben, können Sie die EMS-Datenerfassung mithilfe des Cmdlets *Enable-SmDataCollectionEMS* erneut starten.

Dem Benutzer der Storage Virtual Machine (SVM) wurde die Berechtigung „Generate-Autosupport-Log“ für das NetApp ONTAP Ereignis erteilt.

Schritte

1. Stellen Sie über eine PowerShell-Befehlszeile eine Sitzung mit SnapCenter her, indem Sie *Open-SmConnection* eingeben.
2. Aktivieren Sie die EMS-Datenerfassung, indem Sie *Enable-SmDataCollectionEMS* eingeben.

Ändern Sie den Zeitplan für die EMS-Datenerfassung und das Ziel-SVM

Sie können PowerShell-Cmdlets verwenden, um den Zeitplan für die EMS-Datenerfassung oder die Ziel-Storage-Virtual-Machine (SVM) zu ändern.

Schritte

1. Um eine Sitzung mit SnapCenter herzustellen, geben Sie in einer PowerShell-Befehlszeile das Cmdlet *Open-SmConnection* ein.
2. Um das EMS-Datenerfassungsziel zu ändern, geben Sie das Cmdlet *Set-SmDataCollectionEmsTarget* ein.
3. Um den Zeitplan für die EMS-Datenerfassung zu ändern, geben Sie das Cmdlet *Set-SmDataCollectionEmsSchedule* ein.

Überwachen Sie den Status der EMS-Datenerfassung

Sie können den Status Ihrer EMS-Datenerfassung mithilfe mehrerer PowerShell-Cmdlets überwachen. Sie können Informationen zum Zeitplan, zum Ziel der Storage Virtual Machine (SVM) und zum Status abrufen.

Schritte

1. Stellen Sie über eine PowerShell-Befehlszeile eine Sitzung mit SnapCenter her, indem Sie *Open-SmConnection* eingeben.
2. Rufen Sie Informationen zum EMS-Datenerfassungszeitplan ab, indem Sie *Get-SmDataCollectionEmsSchedule* eingeben.
3. Rufen Sie Informationen zum Status der EMS-Datenerfassung ab, indem Sie *Get-SmDataCollectionEmsStatus* eingeben.
4. Rufen Sie Informationen zum EMS-Datenerfassungsziel ab, indem Sie *Get-SmDataCollectionEmsTarget* eingeben.

Ähnliche Informationen

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie auch auf die "Referenzhandbuch für SnapCenter -Software-Cmdlets" .