# Management von SnapCenter Server und Plug-ins

SnapCenter Software 4.7

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/de-de/snapcenter-47/admin/concept_overview_of_dashboard.html on September 26, 2025. Always check docs.netapp.com for the latest.

# Inhalt


Management von SnapCenter Server und Plug-ins . . . 1
- Dashboard anzeigen . . . 1
  - Überblick über das Dashboard . . . 1
  - So zeigen Sie Informationen auf dem Dashboard an . . . 6
  - Statusberichte der Jobs über das Dashboard anfordern . . . 6
  - Berichte zum Sicherungsstatus können über das Dashboard angefordert werden . . . 7
- RBAC managen . . . 7
  - Ändern Sie eine Rolle . . . 7
  - Benutzer und Gruppen ändern . . . 8
- Management von Hosts . . . 8
  - Informationen zu Virtual Machines aktualisieren . . . 10
  - Ändern Sie die Plug-in-Hosts . . . 10
  - Plug-in-Dienste starten oder neu starten . . . 11
  - Unterbrechen Sie die Zeitpläne für die Hostwartung . . . 11
- Von der Seite Ressourcen unterstützte Vorgänge . . . 12
- Management von Richtlinien . . . 13
  - Richtlinien ändern . . . 14
  - Richtlinien trennen . . . 14
  - Richtlinien löschen . . . 15
- Verwalten von Ressourcengruppen . . . 15
  - Stoppen und fortsetzen Sie den Betrieb in Ressourcengruppen . . . 16
  - Löschen von Ressourcengruppen . . . 16
- Backup-Management . . . 17
  - Backups umbenennen . . . 17
  - Backups löschen . . . 17
- Klone löschen . . . 18
- Überwachen von Jobs, Zeitplänen, Ereignissen und Protokollen . . . 19
  - Überwachen von Jobs . . . 19
  - Überwachung von Zeitplänen . . . 19
  - Monitoring von Ereignissen . . . 20
  - Monitoring von Protokollen . . . 20
  - Entfernen Sie Jobs und Protokolle aus SnapCenter . . . 21
- Überblick über die Berichterstellungsfunktionen von SnapCenter . . . 22
  - Aufrufen von Berichten . . . 23
  - Filtern Sie Ihren Bericht . . . 24
  - Berichte exportieren oder drucken . . . 24
  - Stellen Sie den SMTP-Server für E-Mail-Benachrichtigungen ein . . . 24
  - Konfigurieren Sie die Option zum E-Mail-Versenden von Berichten . . . 25
- Verwalten des SnapCenter-Server-Repositorys . . . 25
  - Voraussetzungen für den Schutz des SnapCenter-Repositorys . . . 25
  - Sichern des SnapCenter Repositorys . . . 26
  - Anzeigen von Backups des SnapCenter Repositorys . . . 26
  - Wiederherstellung des SnapCenter Datenbank-Repositorys . . . 27

SnapCenter-Repository migrieren . . . 27
Setzen Sie das SnapCenter Repository-Kennwort zurück . . . 28
Management von Ressourcen von nicht vertrauenswürdigen Domänen . . . 29
Ändern Sie nicht vertrauenswürdige Domains . . . 29
Nicht vertrauenswürdige Active Directory-Domänen werden nicht registriert . . . 30
Management des Storage-Systems . . . 30
Konfiguration des Storage-Systems ändern . . . 30
Löschen Sie das Speichersystem . . . 32
EMS-Datenerfassung managen . . . 33
EMS-Datenerfassung stoppen . . . 33
Starten Sie die EMS-Datensammlung . . . 33
EMS-Datenerfassungsplan und Ziel-SVM ändern . . . 33
Den EMS-Datenerfassungsstatus überwachen . . . 34

# Management von SnapCenter Server und Plug-ins

## Dashboard anzeigen

### Überblick über das Dashboard

Im Navigationsbereich auf der linken Seite von SnapCenter erhalten Sie einen ersten Überblick über den Systemzustand Ihres Systems. Dazu gehören die letzten Jobaktivitäten, Warnmeldungen, Sicherungsübersicht, Storage-Effizienz und -Auslastung, der Status von SnapCenter Jobs (Backup, Klonen, Wiederherstellung), der Konfigurationsstatus für Standalone- und Windows-Cluster-Hosts. Anzahl von von SnapCenter gemanagten Storage Virtual Machines (SVMs) und Lizenzkapazität.

Die in der Dashboard-Ansicht angezeigten Informationen hängen von der Rolle ab, die dem Benutzer zugewiesen ist, der aktuell 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 mehr Informationen über ein Display anzeigen, indem Sie den Mauszeiger auf **i** bewegen. In manchen Fällen sind die Informationen in den Dashboard-Anzeigen mit detaillierten Quellinformationen auf SnapCenter-GUI-Seiten wie Ressourcen, Überwachung und Berichte verknüpft.

#### Zuletzt Verwendete Job-Aktivitäten

In der Kachel „Letzte Job-Aktivitäten“ werden die letzten Job-Aktivitäten von allen Backup-, Restore- und Clone-Jobs angezeigt, auf die Sie Zugriff haben. Jobs in dieser Anzeige haben einen der folgenden Status: Abgeschlossen, Warnung, Fehlgeschlagen, wird ausgeführt, Warteschlange, Und storniert.

Wenn Sie über einen Job fahren, erhalten Sie weitere Informationen. Sie können zusätzliche Jobinformationen anzeigen, indem Sie auf eine bestimmte Jobnummer klicken, die Sie zur Seite Überwachung umleitet. Dort können Sie Job-Details oder Protokollinformationen abrufen und einen für diese Aufgabe spezifischen Bericht erstellen.

Klicken Sie auf **Alle anzeigen**, um eine Historie aller SnapCenter-Jobs anzuzeigen.

#### Meldungen

Im Feld „Meldungen“ werden die neuesten nicht behobenen kritischen Warnmeldungen und Warnmeldungen für die Hosts und den SnapCenter-Server angezeigt.

Die Gesamtzahl der Warnmeldungen für kritische und Warnungskategorien wird oben auf dem Display angezeigt. Wenn Sie auf die Summen „kritisch“ oder „Warnung“ klicken, werden Sie zur Seite „Warnungen“ weitergeleitet, auf der der Seite „Meldungen“ der spezifische Filter angewendet wird.

Wenn Sie auf eine bestimmte Warnmeldung klicken, werden Sie zur Seite „Meldungen“ weitergeleitet, die Ihnen Details zu dieser Warnmeldung enthält. Wenn Sie unten auf der Anzeige auf **Alle anzeigen** klicken, werden Sie zur Seite Warnungen weitergeleitet, um eine Liste aller Warnmeldungen anzuzeigen.

### Aktuelle Zusammenfassung Des Schutzes

Die Kachel Letzte Protection Summary gibt Ihnen den Schutzstatus für alle Einheiten an, auf die Sie Zugriff haben. Standardmäßig wird die Anzeige so eingestellt, dass der Status aller Plug-ins angezeigt wird. Statusinformationen werden für Ressourcen bestimmt, die im Primärspeicher als Snapshot-Kopien und auf sekundären Storage mithilfe von SnapMirror und SnapVault Technologien gesichert werden. Die Verfügbarkeit von Schutzstatusinformationen für den sekundären Speicher basiert auf dem ausgewählten Plug-in-Typ.

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

Der Schutzstatus für einzelne Plug-ins wird durch Auswahl eines Plug-ins im Dropdown-Menü angezeigt. Ein Donut-Diagramm zeigt den Prozentsatz der geschützten Ressourcen für das ausgewählte Plug-in an. Durch Klicken auf eine Donut-Schicht wird die Seite **Reports** > **Plug-in** umgeleitet, die einen detaillierten Bericht über alle primären und sekundären Speicheraktivitäten für das angegebene Plug-in liefert.

Berichte über sekundären Storage gelten nur für SnapVault. SnapMirror Berichte werden nicht unterstützt.

SAP HANA bietet Sicherungsstatusinformationen für primären und sekundären Storage für Snapshot Kopien. Für dateibasierte Backups steht nur der Schutzstatus des primären Storage zur Verfügung.

| Sicherungsstatus | Primärspeicher | Sekundär-Storage |
|---|---|---|
| Fehlgeschlagen | Anzahl der Einheiten, die Teil einer Ressourcengruppe sind, in der die Ressourcengruppe ein Backup ausgeführt hat, das Backup jedoch fehlgeschlagen ist. | Anzahl der Einheiten mit Backups, die nicht an ein sekundäres Ziel übertragen wurden. |
| Erfolgreich | Anzahl der Einheiten in einer Ressourcengruppe, in der die Ressourcengruppe erfolgreich gesichert wurde. | Anzahl der Einheiten mit Backups, die erfolgreich an ein sekundäres Ziel übertragen wurden. |
| Nicht konfiguriert | Anzahl der Einheiten, die nicht zu einer Ressourcengruppe gehören und noch nicht gesichert wurden. | Anzahl der Einheiten, die Teil einer oder mehrerer Ressourcengruppen sind, die nicht für Backups konfiguriert sind, die an ein sekundäres Ziel übertragen werden sollen. |
| Nicht initiiert | Anzahl der Einheiten, die Teil einer Ressourcengruppe sind, aber kein Backup ausgeführt wurde. | Keine Angabe. |

Wenn Sie zum Erstellen von Backups SnapCenter Server 4.2 und eine frühere Version des Plug-ins (früher als 4.2) verwenden, wird der SnapMirror Sicherungsstatus dieser Backups im Kachel **Neueste Schutzzusammenfassung** nicht angezeigt.

**Jobs**

Die Kachel Jobs bietet Ihnen eine Zusammenfassung der Backup-, Wiederherstellungs- und Klonaufgaben, auf die Sie Zugriff haben. Sie können den Zeitrahmen für jeden Bericht über das Dropdown-Menü anpassen. Die Optionen für den Zeitrahmen werden in den letzten 24 Stunden, den letzten 7 Tagen und den letzten 30 Tagen festgelegt. Der Standardbericht zeigt die in den letzten 7 Tagen ausgeführten Datensicherungsaufträge an.

Jobinformationen zum Sichern, Wiederherstellen und Klonen werden in Donut-Diagrammen angezeigt. Wenn Sie auf eine Donut-Schicht klicken, werden Sie zur Seite „Monitor“ umgeleitet, auf der die Jobfilter bereits für die Auswahl angewendet werden.

| Aufgabenstatus | 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 aktuell ausgeführten Jobs. |

**Storage**

Im Bereich Storage wird der primäre und sekundäre Storage, der von Sicherungsaufgaben über einen Zeitraum von 90 Tagen verbraucht wird, grafisch dargestellt und zeigt Verbrauchstrends berechnet. Die Speicherinformationen werden alle 24 Stunden um 12 Uhr aktualisiert

Der Tagesverbrauch, der die Gesamtzahl der in SnapCenter verfügbaren Backups und die durch diese Backups belegte Größe umfasst, wird oben auf dem Display angezeigt. Einem Backup können mehrere Snapshot Kopien zugeordnet sein, und die Anzahl entspricht dem gleichen. Dies gilt sowohl für primäre als auch für sekundäre Snapshot Kopien. Sie haben z. B. 10 Backups erstellt, von denen 2 aufgrund der richtlinienbasierten Backup-Aufbewahrung gelöscht werden und 1 Backup von Ihnen explizit gelöscht wird. Somit wird eine Anzahl von 7 Backups zusammen mit der Größe angezeigt, die von diesen 7 Backups belegt wird.

Der Storage-Einsparungsfaktor für primären Storage ist das Verhältnis der logischen Kapazität (Klon- und Snapshot-Einsparungen plus verbrauchter Storage) zur physischen Kapazität des primären Storage. Ein Balkendiagramm zeigt die Storage-Einsparungen.

Das Liniendiagramm stellt den primären und sekundären Speicherverbrauch über einen laufenden Zeitraum von 90 Tagen täglich separat dar. Wenn Sie über die Diagramme fahren, erhalten Sie detaillierte tägliche Ergebnisse.

Wenn Sie zum Erstellen von Backups SnapCenter Server 4.2 und eine frühere Version des Plug-ins (früher als 4.2) verwenden, werden im Kachel **Storage** nicht die Anzahl der Backups, der von diesen Backups benötigte Storage, die Snapshot-Einsparungen, die Kloneinsparungen und die Snapshot-Größe angezeigt.

### Konfiguration

Die Konfigurationtile bietet konsolidierte Statusinformationen für alle aktiven eigenständigen und Windows Cluster Hosts, die SnapCenter verwaltet, und auf die Sie Zugriff haben. Dazu gehören auch die mit diesen Hosts verknüpften Plug-in-Statusinformationen.

Wenn Sie auf die Zahl neben Hosts klicken, werden Sie auf der Seite Hosts zum Abschnitt Managed Hosts umgeleitet. Von dort erhalten Sie detaillierte Informationen zu einem ausgewählten Host.

Zusätzlich zeigt dieses Display die Summe der eigenständigen ONTAP SVMs und Cluster ONTAP SVMs, die SnapCenter verwaltet und auf die Sie Zugriff haben. Wenn Sie auf die neben SVM angrenzende Zahl klicken, werden Sie zur Seite Storage-Systeme umgeleitet. Von dort erhalten Sie ausführliche Informationen zu einer ausgewählten SVM.

Der Status der Host-Konfiguration wird als rot (kritisch), gelb (Warnung) und grün (aktiv) angezeigt. Zudem wird die Anzahl der Hosts im jeweiligen Status angegeben. Für jeden Status werden Statusmeldungen bereitgestellt.

| Konfigurationsstatus | Beschreibung |
|---|---|
| Upgrade erforderlich | Anzahl der Hosts, auf denen nicht unterstützte Plug-ins ausgeführt werden und ein Upgrade erforderlich ist Ein nicht unterstütztes Plug-in ist mit dieser SnapCenter-Version nicht kompatibel. |
| Migration erforderlich | Anzahl der Hosts, auf denen nicht unterstützte Plug-ins ausgeführt werden und Migration erforderlich ist Ein nicht unterstütztes Plug-in ist mit dieser SnapCenter-Version nicht kompatibel. |
| Es sind keine Plug-ins installiert | Anzahl der Hosts, die erfolgreich hinzugefügt, aber die Plug-ins müssen installiert werden, oder die Installation der Plug-ins ist fehlgeschlagen. |
| Ausgesetzt | Anzahl der Hosts, deren Zeitpläne ausgesetzt und gewartet werden. |
| Angehalten | Anzahl der Hosts, die in Betrieb sind, die Plug-in-Services jedoch nicht ausgeführt werden. |
| Host ausgefallen | Anzahl der Hosts, die ausgefallen sind oder nicht erreichbar sind. |
| Upgrade verfügbar (optional) | Anzahl der Hosts, auf denen eine neuere Version des Plug-in-Pakets zur Aktualisierung verfügbar ist. |

| Konfigurationsstatus | Beschreibung |
| --- | --- |
| Migration verfügbar (optional) | Anzahl der Hosts, auf denen eine neuere Version des Plug-ins für die Migration verfügbar ist |
| Protokollverzeichnis konfigurieren | Anzahl der Hosts, für die SCSQL das Protokollverzeichnis konfiguriert werden muss, um die Sicherung des Transaktionsprotokolls zu erstellen. |
| Konfiguration von VMware Plug-ins | Anzahl der Hosts, die das SnapCenter Plug-in für VMware vSphere hinzufügen müssen |
| Unbekannt | Anzahl der Hosts, die registriert wurden, aber die Installation noch nicht ausgelöst wurde. |
| Wird Ausgeführt | Anzahl der Hosts, die vorhanden sind und Plug-ins werden ausgeführt. Und bei SCSLL-Plug-ins werden Logverzeichnis und Hypervisor konfiguriert. |
| Installieren\Deinstallieren von Plug-ins | Anzahl der Hosts, auf denen Plug-in-Installation oder Deinstallation ausgeführt wird. |

**Lizenzierte Kapazität**

Die Kachel „lizenzierte Kapazität“ zeigt Informationen über die gesamte lizenzierte Kapazität, die genutzte Kapazität, Warnmeldungen zu Kapazitätsschwellenwerten und Benachrichtigungen zum Ablauf von Lizenzen für kapazitätsbasierte SnapCenter Lizenzen an.

Diese Anzeige wird nur angezeigt, wenn Sie kapazitätsbasierte SnapCenter-Lizenzen auf Cloud Volumes ONTAP- oder ONTAP Select-Plattformen verwenden. Bei FAS oder AFF Plattformen ist die SnapCenter Lizenz Controller-basiert und für unbegrenzte Kapazität lizenziert. Es ist keine Kapazitätslizenz erforderlich.

| Lizenzstatus | Beschreibung |
| --- | --- |
| Wird verwendet | Menge der derzeit genutzten Kapazität |
| Benachrichtigen | Kapazitätsschwellenwert, bei dem Benachrichtigungen im Dashboard angezeigt werden und bei Konfiguration beim Senden von E-Mail-Benachrichtigungen. |
| Lizenziert | Menge der lizenzierten Kapazität. |
| Ein Ende | Die Menge an Kapazität, die die lizenzierte Kapazität überschritten hat. |

## So zeigen Sie Informationen auf dem Dashboard an

Im linken Navigationsbereich der 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. Die in den einzelnen Displays bereitgestellten Inhalte hängen von der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) ab.

**Schritte**

1. Klicken Sie im linken Navigationsbereich auf **Dashboard**.
2. Klicken Sie auf die aktiven Bereiche der Anzeige, um weitere Informationen zu erhalten.

   Wenn Sie beispielsweise in **Jobs** auf ein Donut-Diagramm klicken, werden Sie zur Seite Überwachen umgeleitet, um weitere Informationen zu Ihrer Auswahl zu erhalten. Durch Klicken auf ein Donut-Diagramm in **Schutz-Übersicht** werden Sie zur Seite Berichte weitergeleitet, die Ihnen weitere Informationen zu Ihrer Auswahl geben kann.

## Statusberichte der Jobs über das Dashboard anfordern

Sie können Berichte über Backup-, Wiederherstellungs- und Klonaufträge über die Dashboard-Seite 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 die Kachel Jobs und wählen Sie dann **Backup**, **Restore** oder **Clone** aus.
3. Wählen Sie im Pulldown-Menü den Zeitrahmen aus, für den Sie Jobinformationen wünschen: 24 Stunden, 7 Tage oder 30 Tage.

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

4. Klicken Sie auf die Donut-Schicht, die die Jobinformationen enthält, für die Sie einen Bericht erstellen möchten.

   Wenn Sie auf das Donut-Diagramm klicken, werden Sie von der Dashboard-Seite zur Monitor-Seite umgeleitet. Auf der Seite „Überwachen“ werden die Jobs angezeigt, die den Status aufweisen, den Sie im Donut-Diagramm ausgewählt haben.

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

**Ergebnisse**

Der Bericht zeigt nur Informationen für den ausgewählten Job an. Sie können den Bericht prüfen oder auf Ihr lokales System herunterladen.

### Berichte zum Sicherungsstatus können über das Dashboard angefordert werden

Sie können Sicherungsdetails für Ressourcen anfordern, die von bestimmten Plug-ins gemanagt werden, über das Dashboard. Nur Daten-Backups werden als Zusammenfassung zu Datensicherung in Betracht gezogen.

**Schritte**

1. Klicken Sie im linken Navigationsbereich auf **Dashboard**.
2. Suchen Sie im Dashboard die Kachel Letzte Schutzübersicht, und wählen Sie über das Pulldown-Menü ein Plug-in aus.

   Das Dashboard zeigt ein Donut-Diagramm für Ressourcen an, die im primären Speicher gesichert sind und, falls zutreffend, für das Plug-in, ein Donut-Diagramm für Ressourcen, die auf dem sekundären Speicher gesichert sind.

   Datensicherungsberichte sind nur für bestimmte Plug-ins-Typen verfügbar. Das Festlegen von **Alle Plug-ins** wird nicht unterstützt.

3. Klicken Sie auf die Donut-Schicht, die den Status darstellt, für den ein Bericht erstellt werden soll.

   Wenn Sie auf das Donut-Diagramm klicken, werden Sie von der Dashboard-Seite zu den Berichten und dann zur Plug-in-Seite umgeleitet. Der Bericht zeigt nur den Status des ausgewählten Plug-ins an. Sie können den Bericht prüfen oder auf Ihr lokales System herunterladen.

   Umleitung zur Seite Berichte für SnapMirror-Donut-Diagramm und dateibasiertes SAP HANA-Backup wird nicht unterstützt.

# RBAC managen

SnapCenter ermöglicht Ihnen, Rollen, Benutzer und Gruppen zu ändern.

## Ändern Sie eine Rolle

Sie können eine SnapCenter-Rolle ändern, um Benutzer oder Gruppen zu entfernen und die mit der Rolle verknüpften Berechtigungen zu ändern. Es ist besonders nützlich, Rollen zu ändern, wenn Sie die Berechtigungen einer ganzen Rolle ändern oder löschen möchten.

**Was Sie brauchen**

Sie müssen sich als „SnapCenterAdmin“-Rolle angemeldet haben.

Sie können die Berechtigungen für die SnapCenterAdmin-Rolle nicht ändern oder 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. Ändern Sie auf der Seite Rollendetails die Berechtigungen, oder heben Sie die Zuweisung der Mitglieder nach Bedarf ab.
5. Wählen Sie **Alle Mitglieder dieser Rolle können Objekte anderer Mitglieder** sehen, damit andere Mitglieder der Rolle nach der Aktualisierung der Ressourcenliste Ressourcen wie Volumes und Hosts sehen können.

   Deaktivieren Sie diese Option, wenn Mitglieder dieser Rolle keine Objekte anzeigen möchten, denen andere Mitglieder zugewiesen sind.

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

6. Klicken Sie Auf **Absenden**.

### Benutzer und Gruppen ändern

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

#### Was Sie brauchen

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 Sie ändern möchten.
4. Ändern Sie auf der Seite Benutzer- oder Gruppendetails die Rollen und Assets.
5. Klicken Sie Auf **Absenden**.

# Management von Hosts

Sie können Hosts hinzufügen und SnapCenter-Plug-in-Pakete installieren, einen Verifizierungsserver hinzufügen, Hosts entfernen, Backup-Jobs migrieren und den Host aktualisieren, um Plug-in-Pakete zu aktualisieren oder neue Plug-in-Pakete hinzuzufügen. Abhängig vom verwendeten Plug-in können Sie auch Festplatten bereitstellen, SMB-Freigaben managen, Initiatorgruppen managen, iSCSI-Sessions managen und Daten migrieren.

| Sie können diese Aufgaben ausführen… | Für Microsoft Exchange Server | Für Microsoft SQL Server | Für Microsoft Windows | Für Oracle Database | Für SAP HANA Database | Für benutzerdefinierte Plug-ins |
|---|---|---|---|---|---|---|
| Fügen Sie Hosts hinzu und installieren Sie das Plug-in-Paket | Ja. | Ja. | Ja. | Ja. | Ja. | Ja. |
| Aktualisieren Sie ESXi-Informationen für einen Host | Nein | Ja. | Nein | Nein | Nein | Nein |
| Unterbrechen Sie die Zeitpläne und versetzen Sie Hosts in den Wartungsmodus | Ja. | Ja. | Ja. | Ja. | Ja. | Ja. |
| Ändern Sie Hosts durch Hinzufügen, Aktualisieren oder Entfernen von Plug-ins | Ja. | Ja. | Ja. | Ja. | Ja. | Ja. |
| Entfernen Sie Hosts aus SnapCenter | Ja. | Ja. | Ja. | Ja. | Ja. | Ja. |
| Starten Sie Plug-in-Services | Ja. | Ja. | Ja. | Ja. | Ja. | Ja. |
| Bereitstellung von Festplatten | Nein | Nein | Ja. | Nein | Nein | Nein |
| SMB-Freigaben managen | Nein | Nein | Ja. | Nein | Nein | Nein |

| Sie können diese Aufgaben ausführen… | Für Microsoft Exchange Server | Für Microsoft SQL Server | Für Microsoft Windows | Für Oracle Database | Für SAP HANA Database | Für benutzerdefinierte Plug-ins |
|---|---|---|---|---|---|---|
| IGroups managen | Nein | Nein | Ja. | Nein | Nein | Nein |
| Verwalten von iSCSI-Sitzungen | Nein | Nein | Ja. | Nein | Nein | |

## Informationen zu Virtual Machines aktualisieren

Sie sollten Ihre Virtual Machine-Informationen aktualisieren, wenn sich die VMware vCenter-Anmeldedaten ändern oder der Datenbank- oder Dateisystem-Host neu startet. Durch die Aktualisierung der Informationen Ihrer Virtual Machine in SnapCenter wird die Kommunikation mit dem VMware vSphere vCenter initiiert und die Anmeldedaten für vCenter abgerufen.

RDM-basierte Festplatten werden vom SnapCenter-Plug-in für Microsoft Windows verwaltet, das auf dem Datenbank-Host installiert ist. Um RDMs zu managen, kommuniziert das SnapCenter Plug-in für Microsoft Windows mit dem vCenter Server, der den Datenbank-Host managt.

**Schritte**

1. Klicken Sie im linken Navigationsbereich des SnapCenter auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **verwaltete Hosts**.
3. Wählen Sie auf der Seite verwaltete Hosts den Host aus, den Sie aktualisieren möchten.
4. Klicken Sie auf **VM aktualisieren**.

## Ändern Sie die Plug-in-Hosts

Nach der Installation eines Plug-ins können Sie ggf. die Details der Plug-in Hosts ändern. Sie können Anmeldeinformationen, Installationspfad, Plug-ins, Logverzeichnis-Details für das SnapCenter-Plug-in für Microsoft SQL Server, das Group Managed Service Account (gMSA) und den Plug-in-Port ändern.

Stellen Sie sicher, dass die Plug-in-Version mit der Version des SnapCenter-Servers identisch ist.

**Über diese Aufgabe**

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

  Sie können den Plug-in-Port nicht ändern, während Upgrade-Vorgänge ausgeführt werden.

- Beim Ändern eines Plug-in-Ports sollten Sie die folgenden Port-Rollback-Szenarien beachten:
  - Wenn SnapCenter in einem eigenständigen Setup den Port einer der Komponenten nicht ändert, schlägt der Vorgang fehl und der alte Port wird für alle Komponenten beibehalten.

Wenn der Port für alle Komponenten geändert wurde, aber eine der Komponenten nicht mit dem neuen Port startet, wird der alte Port für alle Komponenten beibehalten. Wenn Sie beispielsweise den Port für zwei Plug-ins auf dem Standalone-Host ändern möchten und SnapCenter den neuen Port nicht auf eines der Plug-ins anwenden kann, schlägt der Vorgang fehl (mit entsprechender Fehlermeldung) und der alte Port wird für beide Plug-ins beibehalten.

- Wenn SnapCenter in einer geclusterten Einrichtung den Port des auf einem Node installierten Plug-ins nicht ändert, schlägt der Vorgang fehl und der alte Port wird für alle Nodes beibehalten.

  Wenn beispielsweise das Plug-in auf vier Nodes in einem Cluster-Setup installiert ist und wenn der Port nicht für einen der Nodes geändert wird, wird der alte Port für alle Nodes beibehalten.

Wenn Plug-ins mit gMSA installiert sind, können Sie im Fenster **More Options** ändern. Wenn Plug-ins ohne gMSA installiert sind, können Sie das gMSA-Konto angeben, um es als Plug-in-Dienstkonto zu verwenden.

**Schritte**

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Vergewissern Sie sich, dass **verwaltete Hosts** oben ausgewählt ist.
3. Wählen Sie den Host aus, für den Sie ein Feld ändern und ändern möchten.

   Es kann jeweils nur ein Feld geändert werden.

4. Klicken Sie Auf **Absenden**.

**Ergebnisse**

Der Host wurde validiert und zum SnapCenter-Server hinzugefügt.

## Plug-in-Dienste starten oder neu starten

Wenn Sie die SnapCenter Plug-in-Dienste starten, können Sie Dienste starten, wenn sie nicht ausgeführt werden, oder wenn sie ausgeführt werden. Sie möchten die Dienste möglicherweise neu starten, nachdem die Wartung durchgeführt wurde.

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 Host-Seite auf **verwaltete Hosts**.
3. Wählen Sie auf der Seite verwaltete Hosts den Host aus, den Sie starten möchten.
4. Klicken Sie auf das Symbol und dann auf **Dienst starten** oder **Dienst neu starten**.

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

## Unterbrechen Sie die Zeitpläne für die Hostwartung

Wenn Sie verhindern möchten, dass der Host geplante SnapCenter-Jobs ausführt, können Sie Ihren Host in den Wartungsmodus versetzen. Führen Sie dies vor dem Upgrade der Plug-ins durch oder führen Sie Wartungsaufgaben auf Hosts durch.

Sie können die Zeitpläne auf einem Host nicht unterbrechen, der ausgefallen ist, da SnapCenter nicht mit diesem Host kommunizieren kann.

**Schritte**

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **verwaltete Hosts**.
3. Wählen Sie auf der Seite verwaltete Hosts den Host aus, den Sie aussetzen möchten.
4. Klicken Sie auf das Symbol und dann auf **Zeitplan unterbrechen**, um den Host für dieses Plug-in in den Wartungsmodus zu versetzen.

   Sie können den Zeitplan mehrerer Hosts gleichzeitig unterbrechen.

   Sie müssen den Plug-in-Dienst nicht zuerst beenden. Der Plug-in-Dienst kann sich im Status „ausgeführt“ oder „angehalten“ befinden.

**Ergebnisse**

Nachdem Sie die Zeitpläne auf dem Host unterbrochen haben, wird auf der Seite Managed Hosts **suspended** im Feld Gesamtstatus des Hosts angezeigt.

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

# Von der Seite Ressourcen unterstützte Vorgänge

Sie können auf der Seite Ressourcen Ressourcen Ressourcen Ressourcen Ressourcen erkennen und Datensicherungsvorgänge durchführen. Die Operationen, die Sie durchführen können, unterscheiden sich je nach dem Plug-in, das Sie für das Management 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 Database | Für SAP HANA Database | Für benutzerdefinierte Plug-ins |
|---|---|---|---|---|---|---|
| Bestimmen Sie, ob Ressourcen für ein Backup verfügbar sind | Ja. | Ja. | Ja. | Ja. | Ja. | Ja. |

| Sie können diese Aufgaben ausführen… | Für Microsoft Exchange Server | Für Microsoft SQL Server | Für Microsoft Windows | Für Oracle Database | Für SAP HANA Database | Für benutzerdefinierte Plug-ins |
|---|---|---|---|---|---|---|
| On-Demand Backup einer Ressource durchführen | Ja. | Ja. | Ja. | Ja. | Ja. | Ja. |
| Restore aus Backups | Ja. | Ja. | Ja. | Ja. | Ja. | Ja. |
| Backups klonen | Nein | Ja. | Ja. | Ja. | Ja. | Ja. |
| Backup-Management | Ja. | Ja. | Ja. | Ja. | Ja. | Ja. |
| Management von Klonen | Nein | Ja. | Ja. | Ja. | Ja. | Ja. |
| Management von Richtlinien | Ja. | Ja. | Ja. | Ja. | Ja. | Ja. |
| Storage-Verbindungen managen | Ja. | Ja. | Ja. | Ja. | Ja. | Ja. |
| Mount-Backups | Nein | Nein | Nein | Ja. | Nein | Nein |
| Deaktivieren Sie das Mounten von Backups | Nein | Nein | Nein | Ja. | Nein | Nein |
| Details anzeigen | Ja. | Ja. | Ja. | Ja. | Ja. | Ja. |

# Management von Richtlinien

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

## Richtlinien ändern

Sie können die Replizierungsoptionen, die Aufbewahrungseinstellungen für Snapshot Kopien, die Anzahl der Wiederholversuche oder die Informationen über Skripte ändern, während eine Richtlinie an eine Ressource oder Ressourcengruppe angehängt ist. Sie können den Terminplantyp (Häufigkeit) nur ändern, wenn Sie eine Richtlinie trennen.

**Über diese Aufgabe**

Das Ändern des Zeitplantyps in einer Richtlinie erfordert zusätzliche Schritte, da der SnapCenter-Server den Zeitplantyp nur dann registriert, wenn die Richtlinie an eine Ressource oder Ressourcengruppe angeschlossen ist.

| Ihr Ziel ist | Dann… |
|---|---|
| Fügen Sie einen zusätzlichen Terminplantyp hinzu | Erstellen Sie eine neue Richtlinie, und fügen Sie sie an die erforderlichen Ressourcen oder Ressourcengruppen an.<br><br>Wenn z. B. eine Ressourcengruppenrichtlinie nur stündliche Backups angibt und Sie auch tägliche Backups 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. |
| Entfernen oder ändern Sie einen Planungstyp | Führen Sie Folgendes aus:<br><br>1. Trennen Sie die Richtlinie von allen Ressourcen- und Ressourcengruppen, die diese Richtlinie verwenden.<br>2. Ändern Sie den Terminplantyp.<br>3. Hängen Sie die Richtlinie erneut an alle Ressourcen und Ressourcengruppen an.<br><br>Wenn z. B. eine Richtlinie stündliche Backups angibt und Sie diese in tägliche Backups ändern möchten, müssen Sie zuerst die Richtlinie 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 stellen**.

## Richtlinien trennen

Sie können Richtlinien jederzeit von einer Ressource oder Ressourcengruppe trennen, wenn diese Richtlinien nicht mehr den Datenschutz für die Ressourcen regeln sollen. Sie müssen eine Richtlinie trennen, bevor Sie

sie löschen können oder bevor Sie den Terminplantyp ändern.

**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 **Ansicht** 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 aus der Dropdown-Liste das Häkchen neben den Richtlinien, die Sie entfernen möchten.
5. Nehmen Sie zusätzliche Änderungen an der Ressourcengruppe im Rest des Assistenten vor, und klicken Sie dann auf **Fertig stellen**.

## Richtlinien löschen

Wenn Sie keine Richtlinien mehr benötigen, können Sie sie löschen.

**Was Sie brauchen**

Sie sollten die Richtlinie von Ressourcen- oder Ressourcengruppen trennen, wenn die Richtlinie mit einer Ressource oder Ressourcengruppe 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 ausführen.

Sie können die folgenden Aufgaben bezüglich 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 während der Änderung der Ressourcengruppe ändern. Wenn Sie jedoch den Terminplantyp ändern möchten, müssen Sie die Richtlinie ändern.

  Wenn Sie Ressourcen aus einer Ressourcengruppe entfernen, werden die in den Richtlinien, die derzeit der Ressourcengruppe zugeordnet sind, definierten Backup-Aufbewahrungseinstellungen weiterhin auf die entfernten Ressourcen angewendet.

- Erstellen Sie ein Backup einer Ressourcengruppe.
- Erstellen Sie einen Klon eines Backups.

Sie können die Backups von SQL, Oracle, Windows Filesystemen, benutzerdefinierten Applikationen und SAP HANA Datenbankressourcen oder Ressourcengruppen klonen.

- Erstellen Sie einen Klon einer Ressourcengruppe.

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

- Verhindern Sie, dass geplante Vorgänge in Ressourcengruppen gestartet werden.
- Löschen einer Ressourcengruppe.

## Stoppen und fortsetzen Sie den Betrieb in Ressourcengruppen

Sie können geplante Vorgänge vorübergehend vom Starten einer Ressourcengruppe deaktivieren. Später können Sie diese Vorgänge 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 **Ansicht** die Option **Ressourcengruppe** aus.
3. Wählen Sie die Ressourcengruppe aus und klicken Sie auf **Wartung**.
4. Klicken Sie auf **OK**.

Wenn Sie die Vorgänge der Ressourcengruppe, die Sie im Wartungsmodus ausgeführt haben, wieder aufnehmen möchten, wählen Sie die Ressourcengruppe aus und klicken Sie auf **Produktion**.

## Löschen von Ressourcengruppen

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 manuell alle Klone löschen, die für eine der Ressourcen der Ressourcengruppe erstellt wurden. Optional können Sie das Löschen aller Backups, Metadaten, Richtlinien und Snapshot Kopien, die der Ressourcengruppe zugeordnet sind, 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 **Ansicht** die Option **Ressourcengruppe** aus.
3. Wählen Sie die Ressourcengruppe aus, und klicken Sie dann auf **Löschen**.
4. Optional: Aktivieren Sie das Kontrollkästchen **Backups löschen und Richtlinien trennen, die mit dieser Ressourcengruppe** verknüpft sind, um alle Backups, Metadaten, Richtlinien und Snapshot-Kopien zu entfernen, die der Ressourcengruppe zugeordnet sind.
5. Klicken Sie auf **OK**.

# Backup-Management

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

## Backups umbenennen

Sie können Backups umbenennen, wenn Sie einen besseren Namen angeben möchten, um die Suchfähigkeit 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 Ressourcengruppe aus der Dropdown-Liste **Ansicht** aus.
3. Wählen Sie die Ressource oder Ressourcengruppe aus der Liste aus.

   Die Seite „Topologie der Ressourcen- oder Ressourcengruppe“ wird angezeigt. Wenn die Ressourcen- oder Ressourcengruppe nicht für den Datenschutz konfiguriert ist, wird anstelle der Topologieseite der Schutzassistent angezeigt.

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

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

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

5. Wählen Sie das Backup aus, und klicken Sie dann auf .
6. Geben Sie im Feld **Backup unter** umbenennen einen neuen Namen ein und klicken Sie auf **OK**.

## Backups löschen

Backups können gelöscht werden, wenn das Backup für andere Datensicherungsvorgänge nicht mehr benötigt wird.

### Was Sie brauchen

Sie müssen die zugehörigen Klone gelöscht haben, bevor Sie ein Backup löschen.

Wenn ein Backup einer geklonten Ressource zugeordnet ist, können Sie das Backup 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 Ressourcengruppe aus der Dropdown-Liste **Ansicht** aus.

3. Wählen Sie die Ressource oder Ressourcengruppe aus der Liste aus.

   Die Seite „Topologie der Ressourcen- oder Ressourcengruppe“ wird angezeigt.

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

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

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

   Wenn Sie ein SAP HANA-Datenbankbackup löschen, werden auch die zugehörigen SAP HANA-Kataloge des Backups gelöscht.

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

6. Klicken Sie auf **OK**.

   Wenn Sie einige veraltete Datenbank-Backups in SnapCenter haben, die keine entsprechenden Backups auf dem Speichersystem haben, müssen Sie den Befehl remove-smbackup verwenden, um diese veralteten Backup-Einträge zu bereinigen. Wenn die veralteten Backups katalogisiert wurden, werden sie von der Datenbank des Recovery-Katalogs entkatalogisiert.

# Klone löschen

Klone können gelöscht werden, wenn Sie sie nicht mehr benötigen.

**Über diese Aufgabe**

Klone, die sich als Quelle für andere Klone fungieren, können nicht gelöscht werden.

Wenn die Produktionsdatenbank beispielsweise db1 ist, wird Datenbank-Klon1 aus Backup von db1 geklont und anschließend clone1 geschützt. Der Datenbankklone2 wird aus dem Backup von Klon1 geklont. Wenn Sie Klon1 löschen möchten, müssen Sie zuerst Klon2 löschen 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 Ressourcengruppe aus der Dropdown-Liste **Ansicht** aus.
3. Wählen Sie die Ressource oder Ressourcengruppe aus der Liste aus.

   Die Seite „Ressource“ oder „Topologie der Ressourcengruppe“ wird angezeigt.

4. Wählen Sie in der Ansicht Kopien managen die Option **Klone** aus den primären oder sekundären (gespiegelten oder replizierten) Storage-Systemen aus.
5. Wählen Sie den Klon aus, und klicken Sie dann auf .

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

a. Geben Sie im Feld **Pre Clone delete** die Befehle ein, die ausgeführt werden sollen, bevor Sie den Klon löschen.

b. Geben Sie im Feld **Unmount** den Befehl ein, um die Bereitstellung des Klons zu deaktivieren, bevor Sie den Klon löschen.

6. Klicken Sie auf **OK**.

**Nach Ihrer Beendigung**

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 Löschvorgangs von Applikationsklonen und vor dem Löschen des Dateisystems warten müssen.

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

# Überwachen von Jobs, Zeitplänen, Ereignissen und Protokollen

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

## Überwachen von Jobs

Sie können Informationen zu Backup-, Klon-, Wiederherstellungs- und Verifizierungsaufgaben von SnapCenter anzeigen. Sie können diese Ansicht nach Start- und Enddatum, Jobtyp, Ressourcengruppe, Richtlinie oder SnapCenter-Plug-in filtern. Sie können auch zusätzliche Details und Protokolldateien für bestimmte Jobs erhalten.

Sie können auch Jobs bezüglich SnapMirror und SnapVault Vorgängen überwachen.

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

Sie können die folgenden Aufgaben im Zusammenhang mit Überwachungsaufgaben ausführen:

- Überwachen Sie Backup-, Klon-, Wiederherstellungs- und Überprüfungsvorgänge.
- Job-Details und -Berichte anzeigen
- Einen geplanten Job stoppen.

## Überwachung von Zeitplänen

Sie möchten möglicherweise aktuelle Zeitpläne anzeigen, um zu bestimmen, wann der Vorgang gestartet wird, wann er zuletzt ausgeführt wurde und wann er als Nächstes ausgeführt wird. Sie können auch den Host bestimmen, auf dem der Vorgang ausgeführt wird, sowie die Ressourcengruppe und die Richtlinieninformationen des Vorgangs.

**Schritte**

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

## Monitoring 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. die Erstellung eines geplanten Backups. Möglicherweise möchten Sie Ereignisse anzeigen, um zu bestimmen, ob ein Vorgang, z. B. ein Backup- oder Wiederherstellungsvorgang, derzeit 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 das Backup abgeschlossen ist, wird ein Ereignis „`Backup Complete`“ angezeigt.

**Schritte**

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite Monitor auf **Events**.
3. (Optional) Geben Sie im Feld Filter das Start- oder Enddatum, die Ereigniskategorie (z. B. Backup, Ressourcengruppe oder Richtlinie) und den Schweregrad ein, und klicken Sie auf **Anwenden**. Alternativ können Sie auch Zeichen in das Suchfeld eingeben.
4. Zeigen Sie die Liste der Ereignisse an.

## Monitoring von Protokollen

Sie können SnapCenter-Serverprotokolle, SnapCenter-Host-Agent-Protokolle und Plug-in-Protokolle anzeigen und herunterladen. Sie sollten die Protokolle anzeigen, die Ihnen bei der Fehlerbehebung helfen.

**Über diese Aufgabe**

Sie können die Protokolle filtern, um nur einen bestimmten Schweregrad für das Protokoll anzuzeigen:

- Debuggen
- Info
- Warnen
- Fehler
- Tödlich

Sie können auch Protokolle auf Jobebene abrufen, z. B. Protokolle, die Ihnen dabei helfen, den Grund für einen fehlgeschlagbaren Backup-Job zu beheben. 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 Ordner mit gezippten Daten enthält die Jobprotokolle und die allgemeinen Protokolle. Der Name des gezippten Ordners enthält die Job-id und den ausgewählten Jobtyp.

3. Klicken Sie auf der Seite Monitor auf **Protokolle**.
4. Wählen Sie Protokolltyp, Host und Instanz aus.

   Wenn Sie Logtyp als **Plugin** auswählen, können Sie einen Host oder ein SnapCenter Plug-in auswählen. Dies ist nicht möglich, wenn der Protokolltyp **Server** lautet.

5. Um die Protokolle nach einer bestimmten Quell-, Nachrichten- oder Protokollebene zu filtern, klicken Sie oben in der Spaltenüberschrift auf das Filtersymbol.

   Um alle Protokolle anzuzeigen, wählen Sie **größer oder gleich** als die `Debug` Ebene.

6. Klicken Sie Auf **Aktualisieren**.
7. Zeigen Sie die Liste der Protokolle an.
8. Klicken Sie auf **Download**, um die Protokolle herunterzuladen.

   Der heruntergeladene Ordner mit gezippten Daten enthält die Jobprotokolle und die allgemeinen Protokolle. Der Name des gezippten Ordners enthält die Job-id und den ausgewählten Jobtyp.

In großen Konfigurationen für eine optimale Performance sollten Sie die Protokolleinstellungen für SnapCenter mit dem PowerShell Cmdlet auf ein minimales Level setzen.

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

Führen Sie das Cmdlet aus, um auf Daten zum Systemzustand oder zur Konfiguration zuzugreifen, die nach Abschluss eines Failover-Jobs abgeschlossen sind `Get-SmRepositoryConfig`.

## Entfernen Sie Jobs und Protokolle aus SnapCenter

Sie können Backup-, Restore-, Klon- und Verifizierungsaufgaben und Protokolle aus SnapCenter entfernen. SnapCenter speichert erfolgreiche und fehlgeschlagene Job-Protokolle unbeschränkt, es sei denn, Sie entfernen sie. Möglicherweise möchten Sie sie entfernen, um den Storage aufzufüllen.

### Über diese Aufgabe

Derzeit dürfen keine Jobs in Betrieb sein. Sie können einen bestimmten Job entfernen, indem Sie eine Job-ID angeben oder 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 an der Eingabeaufforderung Folgendes ein: `Open-SMConnection`

3. Geben Sie an 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.

**Weitere Informationen**

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

# Überblick über die Berichterstellungsfunktionen von SnapCenter

SnapCenter bietet eine Vielzahl von Berichtsoptionen, mit denen Sie den Systemzustand und den Betrieb überwachen und managen können.

| Berichtstyp | Beschreibung |
|---|---|
| Backup-Bericht | Der Backup-Bericht enthält allgemeine Daten zu Backup-Trends für Ihre SnapCenter-Umgebung, die Erfolgsrate des Backups und einige Informationen zu jedem während der festgelegten Zeit durchgeführten Backup. Wenn ein Backup gelöscht wird, zeigt der Bericht keine Statusinformationen für das gelöschte Backup an. Der Bericht Backup Detail enthält detaillierte Informationen zu einem bestimmten Backup-Job und listet die erfolgreich gesicherten Ressourcen und die fehlgeschlagenen Ressourcen auf. |
| Bericht Klonen | Der Klonbericht enthält allgemeine Daten zu Klon-Trends für Ihre SnapCenter Umgebung, die Erfolgsrate von Klonen und einige Informationen zu jedem Klonjob, der während des festgelegten Zeits ausgeführt wurde. Wenn ein Klon gelöscht wird, zeigt der Bericht keine Statusinformationen für den gelöschten Klon an. Der Detailbericht zum Klonen enthält Details zum angegebenen Klon-, Klon-Host- und Klon-Auftragsstatus. Wenn eine Aufgabe fehlschlägt, zeigt der Detailbericht zum Klonen Informationen über den Fehler an. |

| Berichtstyp | Beschreibung |
| --- | --- |
| Bericht Wiederherstellen | Der Wiederherstellungsbericht enthält allgemeine Informationen zu Wiederherstellungsjobs. Der Detailbericht zur Wiederherstellung enthält Details zu einem festgelegten Wiederherstellungsauftrag, einschließlich Host-Name, Backup-Name, Jobstart und -Dauer sowie Status einzelner Job-Aufgaben. Wenn eine Aufgabe fehlschlägt, zeigt der Detailbericht zur Wiederherstellung Informationen zum Fehler an. |
| Sicherungsbericht | Diese Berichte enthalten Einzelheiten zu Sicherungsmaßnahmen für Ressourcen, die von allen SnapCenter Plug-in-Instanzen gemanagt werden. Dieser Bericht enthält Sicherungsdetails für Ressourcen, die von allen Plug-in-Instanzen gemanagt werden. Sie sehen eine Übersicht, Details zu ungeschützten Ressourcen, Ressourcen, die zum Zeitpunkt der Berichterstellung nicht gesichert wurden, Ressourcen einer Ressourcengruppe, für die Backup-Vorgänge ausgefallen sind, und den SnapVault-Status. |
| Planter Bericht | Diese Berichte werden regelmäßig wie täglich, wöchentlich oder monatlich erstellt. Die Berichte werden automatisch zu dem angegebenen Datum und Uhrzeit erstellt und der Bericht wird per E-Mail an die jeweiligen Personen gesendet Sie können die Zeitpläne aktivieren, deaktivieren, ändern oder löschen. Der aktivierte Zeitplan kann auf Anforderung ausgeführt werden, indem Sie auf die Schaltfläche **Jetzt ausführen** klicken. Der Administrator kann einen beliebigen Zeitplan ausführen, der erstellte Bericht enthält jedoch Daten, die auf der Berechtigung des Benutzers basieren, der den Zeitplan erstellt hat.<br><br>Andere Benutzer als Administrator können den Zeitplan anhand ihrer Berechtigung anzeigen oder ändern. Wenn alle Mitglieder dieser Rolle die Option Objekte anderer Mitglieder auf der Seite Rolle hinzufügen ausgewählt haben, können andere Mitglieder der Rolle sehen und ändern. |

## Aufrufen von Berichten

Mit dem SnapCenter-Dashboard erhalten Sie einen schnellen Überblick über den Zustand Ihres Systems. Über das Dashboard können Sie weitere Details abrufen. Alternativ können Sie direkt auf detaillierte Berichte zugreifen.

Sie können auf Berichte über eine der folgenden Methoden zugreifen:

- Klicken Sie im linken Navigationsbereich auf **Dashboard** und dann auf **Letzte Schutzübersicht** Kreisdiagramm, um weitere Details auf der Seite Berichte anzuzeigen.
- Klicken Sie im linken Navigationsbereich auf **Berichte**.

## Filtern Sie Ihren Bericht

Sie können Ihre Berichtsdaten nach verschiedenen Parametern filtern, je nachdem, wie viel Details und Zeit Sie benötigen.

**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 Zeitbereich an, für den der Bericht ausgeführt werden soll. + Wenn Sie das Enddatum nicht angeben, werden alle verfügbaren Informationen abgerufen.
4. Filtern Sie Ihre Berichtsinformationen nach den folgenden Kriterien:
    - Ressourcengruppe
    - Host
    - Richtlinie
    - Ressource
    - Status
    - Plug-in-Name
5. Klicken Sie Auf **Anwenden**.

## Berichte exportieren oder drucken

Durch das Exportieren von SnapCenter-Berichten können Sie den Bericht in verschiedenen anderen Formaten anzeigen. Sie können auch Berichte drucken.

**Schritte**

1. Klicken Sie im linken Navigationsbereich auf **Berichte**.
2. Führen Sie in der Symbolleiste Berichte 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 **Exportieren**-Symbol 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 Berichtsübersicht anzuzeigen, blättern Sie zum entsprechenden Abschnitt des Berichts.

## Stellen Sie den SMTP-Server für E-Mail-Benachrichtigungen ein

Sie können den SMTP-Server angeben, der zum Senden von Datenschutzjobberichten an sich selbst oder 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 die E-Mail-

Benachrichtigung konfigurieren.

Mit dieser Option wird der SMTP-Server zum Senden aller Datensicherheitsjobberichte konfiguriert. Wenn Sie jedoch regelmäßige Aktualisierungen für den SnapCenter-Datenschutz für eine bestimmte Ressource an sich selbst oder andere gesendet haben möchten, damit Sie den Status dieser Updates überwachen können, können Sie die Option konfigurieren, die SnapCenter-Berichte per E-Mail zu versenden, wenn Sie eine Ressourcengruppe erstellen.

**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 aus Sie die E-Mail senden, geben Sie den Betreff ein und klicken Sie auf **Senden**.

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

Wenn Sie regelmäßige Aktualisierungen für den SnapCenter-Datenschutz an sich selbst oder andere Benutzer senden möchten, damit Sie den Status dieser Updates überwachen können, können Sie die Option konfigurieren, die SnapCenter-Berichte per E-Mail zu senden, wenn Sie eine Ressourcengruppe erstellen.

**Was Sie brauchen**

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 Bereich Benachrichtigung des Assistenten für neue Ressourcengruppe aus dem Pulldown-Menü aus, ob Sie Berichte immer, bei Ausfall, bei Ausfall oder bei Fehler oder Warnung empfangen 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-Repositorys

Informationen zu verschiedenen von SnapCenter durchgeführten 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 für den Schutz des SnapCenter-Repositorys

Ihre Umgebung sollte bestimmte Voraussetzungen zum Schutz des SnapCenter-Repositorys erfüllen.

- Managen von Storage Virtual Machine-Verbindungen (SVM

  Sie sollten die Speicher-Anmeldeinformationen konfigurieren.

- Bereitstellung von Hosts

  Auf dem SnapCenter Repository-Host sollte mindestens eine NetApp Speicherplatte vorhanden sein. Wenn auf dem SnapCenter Repository-Host kein NetApp-Laufwerk vorhanden ist, müssen Sie ein Laufwerk erstellen.

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

- Bereitstellung von iSCSI LUN oder VMDK

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

## Sichern des SnapCenter Repositorys

Wenn Sie ein Backup des SnapCenter Server Repositorys durchführen, können Sie diese vor Datenverlust schützen. Sie können das Repository durch Ausführen des Cmdlet *Protect-SmRepository* sichern.

**Über diese Aufgabe**

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

- Erstellt eine Ressourcengruppe und eine Richtlinie
- Erstellt einen Backup-Zeitplan für das SnapCenter-Repository

**Schritte**

1. Starten Sie PowerShell.
2. Erstellen Sie auf dem SnapCenter-Server-Host eine Sitzung mit dem Cmdlet *Open-SmConnection*, 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-Backups von SnapCenter Server anzeigen, indem Sie das Cmdlet *get-SmRepositoryBackups* ausführen.

Die Repository-Backups 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 Anmeldeinformationen für die Verbindung zum SnapCenter-Server an: *Open-SMConnection*
3. Listen Sie alle verfügbaren SnapCenter-Datenbank-Backups mit dem Cmdlet *get-SmoryBackups* auf.

## Wiederherstellung des SnapCenter Datenbank-Repositorys

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

Wenn Sie das SnapCenter-Repository wiederherstellen, sind andere ausgeführte SnapCenter-Vorgänge betroffen, da während des Wiederherstellungsvorgangs die Repository-Datenbank nicht zugänglich ist.

**Schritte**

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

   Mit dem folgenden Cmdlet wird das SnapCenter MySQL Datenbank-Repository aus den auf iSCSI LUN oder VMDK vorhandenen Backups wiederhergestellt:

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

   Mit dem folgenden Cmdlet wird die SnapCenter MySQL Datenbank wiederhergestellt, wenn Backup-Dateien versehentlich in der iSCSI-LUN gelöscht werden. Bei VMDK wird der Backup manuell aus ONTAP Snapshot Kopien wiederhergestellt.

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

> Das Backup, das zur Durchführung des Repository-Wiederherstellungsvorgangs verwendet wurde, wird nicht aufgeführt, wenn die Repository-Backups nach Durchführung der Wiederherstellung abgerufen werden.

## SnapCenter-Repository migrieren

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

**Schritte**

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

   Das Datenverzeichnis finden Sie in der Regel unter C:\ProgramData\MySQL\MySQL Server 5.7\Data.

3. Kopieren Sie das MySQL-Datenverzeichnis in den neuen Speicherort, z. B. E:\Data\nsm.
4. Klicken Sie mit der rechten Maustaste auf das neue Verzeichnis, und wählen Sie dann **Eigenschaften** > **Sicherheit** aus, um das lokale Network Service Server-Konto dem neuen Verzeichnis hinzuzufügen, und

weisen Sie dann die volle Kontrolle zu.

5. Benennen Sie das ursprüngliche Datenbankverzeichnis um, z. B. nsm_copy.
6. Erstellen Sie in einer Windows-Eingabeaufforderung mithilfe des Befehls *mklink* einen symbolischen Verzeichnislink.

   ```
   "mklink /d "C:\ProgramData\MySQL\MySQL Server 5.7\Data\nsm" "E:\Data\nsm" "
   ```

7. Starten Sie den MYSQL57-Dienst unter Windows.
8. Stellen Sie sicher, dass die Änderung des Datenbankstandorts erfolgreich ist, indem Sie sich bei SnapCenter anmelden und 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 SnapCenter Repository-Kennwort zurück

Das MySQL Server Repository-Datenbankkennwort wird bei der Installation des SnapCenter Servers von SnapCenter 4.2 automatisch generiert. Dieses automatisch generierte Passwort ist dem SnapCenter-Benutzer an keinem Punkt bekannt. Wenn Sie auf die Repository-Datenbank zugreifen möchten, sollten Sie das Passwort zurücksetzen.

### Was Sie brauchen

Sie sollten über die SnapCenter-Administratorrechte 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 zum SnapCenter-Server an: *Open-SMConnection*
3. Setzen Sie das Repository-Passwort zurück: *Set-SmRepositoryPassword*

   Mit dem folgenden Befehl wird das Repository-Passwort zurückgesetzt:

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

### Weitere Informationen

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

# Management von Ressourcen von nicht vertrauenswürdigen Domänen

Neben dem Management von Hosts in vertrauenswürdigen Active Directory (AD) Domänen managt SnapCenter auch Hosts in mehreren AD-Domänen, die nicht vertrauenswürdig sind. Die nicht vertrauenswürdigen AD-Domänen müssen beim SnapCenter-Server registriert werden. SnapCenter unterstützt Benutzer und Gruppen aus mehreren nicht vertrauenswürdigen 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, müssen Sie die Domänenanmeldeinformationen angeben, wenn sich der Computer in einer Domäne befindet oder sich die lokalen Administratoranmeldeinformationen befinden, wenn sich der Computer in einer Arbeitsgruppe befindet.

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

## Ändern Sie nicht vertrauenswürdige Domains

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

**Über diese Aufgabe**

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

Zum Ändern einer nicht vertrauenswürdigen Domäne können Sie entweder die SnapCenter Benutzeroberfläche oder PowerShell Commandlets 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 Sie Auf , Und geben Sie dann die folgenden Details:

| Für dieses Feld… | Tun Sie das… |
| --- | --- |
| Domain-FQDN | Geben Sie den FQDN an, und klicken Sie auf **Auflösen**. |
| IP-Adressen des Domänencontrollers | Wenn der Domain-FQDN nicht lösbar ist, geben Sie eine oder mehrere IP-Adressen des Domänencontrollers an. |

5. Klicken Sie auf **OK**.

## Nicht vertrauenswürdige Active Directory-Domänen werden nicht registriert

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

### Was Sie brauchen

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

### Über diese Aufgabe

- Nachdem die Domäne vom SnapCenter-Server nicht registriert wurde, können Benutzer dieser Domäne nicht auf den SnapCenter-Server zugreifen.
- Wenn es zugeordnete Assets (Hosts, Benutzer und Gruppen) gibt, sind die Assets nach der Registrierung der Domäne nicht mehr betriebsbereit.
- Um die Registrierung einer nicht vertrauenswürdigen Domäne zu aufheben, können Sie entweder die SnapCenter Benutzeroberfläche oder PowerShell Commandlets 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 Liste der Domänen die Domain aus, die Sie aufheben möchten.
5. Klicken Sie auf , und klicken Sie dann auf **OK**.

# Management des Storage-Systems

Nach dem Hinzufügen des Speichersystems können Sie die Konfiguration und Verbindungen des Speichersystems ändern oder das Speichersystem löschen.

## Konfiguration des Storage-Systems ändern

Sie können mit SnapCenter die Konfiguration Ihres Storage-Systems ändern, wenn Sie den Benutzernamen, das Passwort, die Plattform, Port, das Protokoll, ändern möchten. Timeout-Zeitraum, bevorzugte IP-Adresse oder Messaging-Optionen.

### Über diese Aufgabe

Sie können Speicherverbindungen für einen einzelnen Benutzer oder für eine Gruppe ändern. Wenn Sie einer oder mehreren Gruppen mit Berechtigung zum selben Speichersystem angehören, wird der Name der Speicherverbindung mehrfach in der Liste der Speicherverbindungen 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 Storage Systems aus dem Dropdown-Menü **Typ** eine der folgenden Aktionen aus:

| **Auswählen…** | **Schritte…** |
| --- | --- |
| ONTAP SVMs | So können alle hinzugefügten Storage Virtual Machines (SVMs) und die erforderliche SVM-Konfiguration angezeigt werden.<br><br>a. Klicken Sie auf der Seite Storage Connections auf den entsprechenden SVM-Namen.<br><br>b. Führen Sie eine der folgenden Aktionen aus:<br><br>◦ Wenn die SVM nicht Teil eines Clusters ist, ändern Sie auf der Seite „Speichersystem ändern“ die Konfigurationen wie Benutzername, Passwort, EMS- und AutoSupport-Einstellungen, Plattform, Protokoll, Port, Timeout Und bevorzugte IP-Adresse.<br><br>◦ Wenn die SVM Teil eines Clusters ist, wählen Sie auf der Seite Speichersystem ändern die Option **SVM unabhängig managen** aus und ändern Sie die Konfigurationen wie Benutzername, Passwort, EMS- und AutoSupport-Einstellungen, Plattform, Protokoll, Port, Timeout, Und bevorzugte IP-Adresse.<br><br>Nachdem Sie die SVM für das unabhängige Management geändert haben und sich für das Management über den Cluster entscheiden, sollten Sie die SVM löschen und dann auf **neu entdeckt** klicken. Die SVM wird dem ONTAP-Cluster hinzugefügt.<br><br>ⓘ Wenn ein Speichersystemkennwort auf der SnapCenter-GUI aktualisiert wird, sollten Sie die SMCore-Dienste des jeweiligen Plug-ins oder des Server-Hosts neu starten, da das aktualisierte Passwort nicht in SMCore reflektiert wird, und die Backupjobs mit einem falschen Anmeldeinformationsfehler fehlschlagen. |

| Auswählen… | Schritte… |
| --- | --- |
| ONTAP Cluster | Anzeige aller hinzugefügten Cluster und Änderung der erforderlichen Cluster-Konfiguration<br>a. Klicken Sie auf der Seite Storage Connections auf den Cluster-Namen.<br>b. Klicken Sie auf der Seite Speichersystem ändern auf das Bearbeiten-Symbol neben Benutzername und ändern Sie den Benutzernamen und das Kennwort.<br>c. Wählen Sie die EMS- und AutoSupport-Einstellungen aus oder löschen Sie diese.<br>d. Klicken Sie auf **Weitere Optionen** und ändern Sie andere Konfigurationen wie Plattform, Protokoll, Port, Timeout und bevorzugte IP. |

3. Klicken Sie Auf **Absenden**.

## Löschen Sie das Speichersystem

Sie können SnapCenter verwenden, um alle nicht verwendeten Speichersysteme zu löschen.

### Über diese Aufgabe

Sie können Speicherverbindungen für einen einzelnen Benutzer oder für eine Gruppe löschen. Wenn Sie einer oder mehreren Gruppen mit Berechtigung zum selben Speichersystem angehören, wird der Name des Speichersystems mehrfach in der Liste der Speicherverbindungen angezeigt, einmal für jede Gruppe mit Berechtigung für das Speichersystem.

Wenn Sie ein Storage-System löschen, fallen alle Vorgänge aus, die auf diesem Storage-System ausgeführt werden, aus.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speichersysteme**.
2. Wählen Sie auf der Seite Speichersysteme im Dropdown-Menü **Typ** entweder **ONTAP-SVMs** oder **ONTAP-Cluster** aus.
3. Aktivieren Sie auf der Seite Storage Connections das Kontrollkästchen neben der SVM oder das Cluster, das Sie löschen möchten.

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

4. Klicken Sie Auf **Löschen**.
5. Klicken Sie auf der Seite Einstellungen für die Speichersystemverbindung löschen auf **OK**.

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

# EMS-Datenerfassung managen

Sie können die Datenerfassung im Event Management System (EMS) mithilfe von PowerShell Cmdlets planen und verwalten. Die EMS-Datenerfassung umfasst die Sammlung von Details zum SnapCenter-Server, den installierten SnapCenter-Plug-in-Paketen, den Hosts und ähnlichen Informationen und sendet sie dann an eine bestimmte ONTAP Storage Virtual Machine (SVM).

Die CPU-Auslastung des Systems ist hoch, wenn gerade die Datenerfassung läuft. Die CPU-Auslastung bleibt hoch, solange der Betrieb unabhängig von der Datengröße fortschreitet.

## EMS-Datenerfassung stoppen

Die EMS-Datenerfassung ist standardmäßig aktiviert und wird alle sieben Tage nach dem Installationsdatum ausgeführt. Sie können die Datenerfassung jederzeit mit dem PowerShell Cmdlet *Disable-SmDataCollectionEMS* deaktivieren.

**Schritte**

1. Erstellen Sie in einer PowerShell-Befehlszeile eine Sitzung mit SnapCenter, indem Sie *Open-SmConnection* eingeben.
2. Deaktivieren Sie die EMS-Datensammlung, indem Sie *Disable-SmDataCollectionEms* eingeben.

## Starten Sie die EMS-Datensammlung

Die EMS-Datenerfassung ist standardmäßig aktiviert und wird voraussichtlich alle sieben Tage ab dem Installationsdatum ausgeführt. Wenn Sie die EMS-Datensammlung deaktiviert haben, können Sie die EMS-Datensammlung erneut mit dem Cmdlet *enable-SmDataCollectionEMS* starten.

Die Berechtigung zum Generieren des Data ONTAP-Events „Generate-AutoSupport-log“ wurde dem SVM-Benutzer (Storage Virtual Machine) zugewiesen.

**Schritte**

1. Erstellen Sie in einer PowerShell-Befehlszeile eine Sitzung mit SnapCenter, indem Sie *Open-SmConnection* eingeben.
2. Aktivieren Sie die EMS-Datensammlung, indem Sie *enable-SmDataCollectionEMS* eingeben.

## EMS-Datenerfassungsplan und Ziel-SVM ändern

Mit PowerShell cmdlets können Sie den EMS-Zeitplan zur Datenerfassung oder die Ziel-Storage Virtual Machine (SVM) ändern.

**Schritte**

1. Geben Sie in einer PowerShell-Befehlszeile zum Erstellen einer Sitzung mit SnapCenter das Cmdlet *Open-SmConnection* ein.
2. Um das EMS-Datenerfassungsziel zu ändern, geben Sie das Cmdlet *set-SmDataCollectionEmsTarget* ein.
3. Um den EMS-Datenerfassungsplan zu ändern, geben Sie das Cmdlet *set-SmDataCollectionEmsSchedule* ein.

## Den EMS-Datenerfassungsstatus überwachen

Sie können den Status Ihrer EMS-Datensammlung mithilfe mehrerer PowerShell Commandlets überwachen. Sie erhalten Informationen zum Zeitplan, zum Storage Virtual Machine-Ziel (SVM) und zum Status.

### Schritte

1. Erstellen Sie in einer PowerShell-Befehlszeile eine Sitzung mit SnapCenter, indem Sie *Open-SmConnection* eingeben.
2. Rufen Sie Informationen zum EMS-Datenerfassungsplan ab, indem Sie *get-SmDataCollectionEmsSchedule* eingeben.
3. Rufen Sie Informationen zum EMS-Datenerfassungsstatus ab, indem Sie *get-SmDataCollectionEmsStatus* eingeben.
4. Rufen Sie Informationen zum EMS-Datenerfassungsziel ab, indem Sie *get-SmDataCollectionEmsTarget* eingeben.

### Weitere Informationen

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

**Copyright-Informationen**

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

**Markeninformationen**

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