Schützen Sie Windows-Dateisysteme

SnapCenter software

NetApp
November 06, 2025

Inhalt

Schützen Sie Windows-Dateisysteme

SnapCenter Plug-in für Microsoft Windows-Konzepte

Übersicht über das SnapCenter -Plug-in für Microsoft Windows

Das SnapCenter -Plug-in für Microsoft Windows ist eine hostseitige Komponente der NetApp SnapCenter -Software, die eine anwendungsbewusste Datenschutzverwaltung von Microsoft-Dateisystemressourcen ermöglicht. Darüber hinaus bietet es Speicherbereitstellung, Snapshot-Konsistenz und Speicherplatzrückgewinnung für Windows-Dateisysteme. Das Plug-in für Windows automatisiert Sicherungs-, Wiederherstellungs- und Klonvorgänge des Dateisystems in Ihrer SnapCenter -Umgebung.

Wenn das Plug-in für Windows installiert ist, können Sie SnapCenter mit der NetApp SnapMirror -Technologie verwenden, um Spiegelkopien von Sicherungssätzen auf einem anderen Volume zu erstellen, und mit der NetApp SnapVault -Technologie eine Disk-to-Disk-Sicherungsreplikation zur Archivierung oder Standardkonformität durchführen.

- Ermöglicht anwendungsbezogenen Datenschutz für andere Plug-Ins, die auf Windows-Hosts in Ihrer SnapCenter -Umgebung ausgeführt werden
- Automatisiert anwendungsorientierte Sicherungs-, Wiederherstellungs- und Klonvorgänge für Microsoft-Dateisysteme in Ihrer SnapCenter Umgebung
- Unterstützt Speicherbereitstellung, Snapshot-Konsistenz und Speicherplatzrückgewinnung für Windows-Hosts

Das Plug-in für Windows stellt SMB-Freigaben und Windows-Dateisysteme auf physischen und RDM-LUNs bereit, unterstützt jedoch keine Sicherungsvorgänge für Windows-Dateisysteme auf SMB-Freigaben.

Was Sie mit dem SnapCenter Plug-in für Microsoft Windows tun können

Wenn das Plug-in für Windows in Ihrer Umgebung installiert ist, können Sie SnapCenter zum Sichern, Wiederherstellen und Klonen von Windows-Dateisystemen verwenden. Sie können auch Aufgaben ausführen, die diese Vorgänge unterstützen.

- Ressourcen entdecken
- Sichern Sie Windows-Dateisysteme
- Planen von Sicherungsvorgängen
- Wiederherstellen von Dateisystemsicherungen
- Klonen von Dateisystemsicherungen
- Überwachen von Sicherungs-, Wiederherstellungs- und Klonvorgängen

Das Plug-in für Windows unterstützt keine Sicherung und Wiederherstellung von Dateisystemen auf SMB-Freigaben.

Funktionen des SnapCenter -Plug-ins für Windows

Das Plug-in für Windows lässt sich in die NetApp Snapshot-Technologie auf dem Speichersystem integrieren. Um mit dem Plug-in für Windows zu arbeiten, verwenden Sie die SnapCenter -Schnittstelle.

Das Plug-in für Windows umfasst die folgenden Hauptfunktionen:

- **Einheitliche grafische Benutzeroberfläche mit SnapCenter**

  Die SnapCenter Schnittstelle bietet Ihnen Standardisierung und Konsistenz über Plug-Ins und Umgebungen hinweg. Über die SnapCenter Schnittstelle können Sie konsistente Sicherungs- und Wiederherstellungsprozesse über alle Plug-Ins hinweg durchführen, zentralisierte Berichte verwenden, übersichtliche Dashboard-Ansichten nutzen, eine rollenbasierte Zugriffskontrolle (RBAC) einrichten und Jobs über alle Plug-Ins hinweg überwachen. SnapCenter bietet außerdem eine zentrale Planung und Richtlinienverwaltung zur Unterstützung von Sicherungs- und Klonvorgängen.

- **Automatisierte zentrale Verwaltung**

  Sie können routinemäßige Dateisystemsicherungen planen, eine richtlinienbasierte Sicherungsaufbewahrung konfigurieren und Wiederherstellungsvorgänge einrichten. Sie können Ihre Dateisystemumgebung auch proaktiv überwachen, indem Sie SnapCenter so konfigurieren, dass E-Mail-Benachrichtigungen gesendet werden.

- **Unterbrechungsfreie NetApp Snapshot-Technologie**

  Das Plug-in für Windows verwendet die NetApp Snapshot-Technologie. Auf diese Weise können Sie Dateisysteme in Sekundenschnelle sichern und schnell wiederherstellen, ohne den Host offline zu nehmen. Snapshots verbrauchen nur minimalen Speicherplatz.

Zusätzlich zu diesen Hauptfunktionen bietet das Plug-in für Windows die folgenden Vorteile:

- Unterstützung für Sicherungs-, Wiederherstellungs- und Klon-Workflows
- RBAC-gestützte Sicherheit und zentralisierte Rollendelegierung
- Erstellung platzsparender Kopien von Produktionsdateisystemen zum Testen oder zur Datenextraktion mithilfe der NetApp FlexClone -Technologie

  Informationen zur FlexClone -Lizenzierung finden Sie unter"SnapCenter -Lizenzen" .

- Möglichkeit, mehrere Backups gleichzeitig auf mehreren Servern auszuführen
- PowerShell-Cmdlets zum Skripting von Sicherungs-, Wiederherstellungs- und Klonvorgängen
- Unterstützung für die Sicherung von Dateisystemen und virtuellen Maschinendatenträgern (VMDKs)
- Unterstützung für physische und virtualisierte Infrastrukturen
- Unterstützung für iSCSI, Fibre Channel, FCoE, Raw Device Mapping (RDM), Asymmetric LUN Mapping (ALM), VMDK über NFS und VMFS sowie virtuelles FC
- Unterstützung für Non-Volatile Memory Express (NVMe) auf Windows Server 2022
  - Sicherungs-, Wiederherstellungs-, Klon- und Überprüfungs-Workflows auf VMDK-Layout, das auf NVMe über TCP/IP erstellt wurde.
  - Unterstützt NVMe-Firmwareversion 1.3 ab ESX 8.0 Update 2 und erfordert virtuelle Hardwareversion 21.

    - Windows Server Failover Clustering (WSFC) wird für Anwendungen über VMDK auf NVMe über TCP/IP nicht unterstützt.
- Unterstützt SnapMirror Active Sync (ursprünglich veröffentlicht als SnapMirror Business Continuity [SM-BC]), wodurch Geschäftsdienste auch bei einem vollständigen Site-Ausfall weiter ausgeführt werden können und Anwendungen mithilfe einer sekundären Kopie transparent ausfallen können. Um mit SnapMirror Active Sync ein Failover auszulösen, sind weder manuelle Eingriffe noch zusätzliche Skripts erforderlich.

So sichert SnapCenter Windows-Dateisysteme

SnapCenter verwendet Snapshot-Technologie zum Sichern von Windows-Dateisystemressourcen, die sich auf LUNs, CSVs (Cluster Shared Volumes), RDM-Volumes (Raw Device Mapping), ALM (asymmetric LUN Mapping) in Windows-Clustern und VMDKs basierend auf VMFS/NFS (VMware Virtual Machine File System using NFS) befinden.

SnapCenter erstellt Backups, indem es Snapshots der Dateisysteme erstellt. Föderierte Backups, bei denen ein Volume LUNs von mehreren Hosts enthält, sind schneller und effizienter als Backups jeder einzelnen LUN, da nur ein Snapshot des Volumes erstellt wird, im Gegensatz zu einzelnen Snapshots jedes Dateisystems.

Wenn SnapCenter einen Snapshot erstellt, wird das gesamte Speichersystemvolume im Snapshot erfasst. Allerdings ist die Sicherung nur für den Hostserver gültig, für den die Sicherung erstellt wurde.

Wenn sich Daten von anderen Hostservern auf demselben Volume befinden, können diese Daten nicht aus dem Snapshot wiederhergestellt werden.

Wenn ein Windows-Dateisystem eine Datenbank enthält, ist das Sichern des Dateisystems nicht dasselbe wie das Sichern der Datenbank. Um eine Datenbank zu sichern, müssen Sie eines der Datenbank-Plug-ins verwenden.

Vom SnapCenter Plug-in für Microsoft Windows unterstützte Speichertypen

SnapCenter unterstützt eine breite Palette von Speichertypen sowohl auf physischen als auch auf virtuellen Maschinen. Sie müssen überprüfen, ob für Ihren Speichertyp Unterstützung verfügbar ist, bevor Sie das Paket für Ihren Host installieren.

SnapCenter -Bereitstellungs- und Datenschutzunterstützung ist auf Windows Server verfügbar. Die neuesten Informationen zu unterstützten Versionen finden Sie imhttps://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT["NetApp Interoperabilitätsmatrix-Tool"^] .

Maschine	Speichertyp	Bereitstellung mittels	Support-Hinweise
Physischer Server	FC-verbundene LUNs	Grafische Benutzeroberfläche (GUI) von SnapCenter oder PowerShell-Cmdlets	
Physischer Server	Über iSCSI verbundene LUNs	SnapCenter -GUI oder PowerShell-Cmdlets	

Maschine	Speichertyp	Bereitstellung mittels	Support-Hinweise
Physischer Server	SMB3 (CIFS)-Freigaben auf einer Storage Virtual Machine (SVM)	SnapCenter -GUI oder PowerShell-Cmdlets	Support nur für die Bereitstellung.
VMware VM	Über einen FC- oder iSCSI-HBA verbundene RDM-LUNs	PowerShell-Cmdlets	
VMware VM	iSCSI-LUNs, die vom iSCSI-Initiator direkt mit dem Gastsystem verbunden sind	SnapCenter -GUI oder PowerShell-Cmdlets	
VMware VM	Virtual Machine File Systems (VMFS) oder NFS-Datenspeicher	VMware vSphere	
VMware VM	Ein Gastsystem, das mit SMB3-Freigaben verbunden ist, die sich auf einer SVM befinden	SnapCenter -GUI oder PowerShell-Cmdlets	Support nur für die Bereitstellung.
VMware VM	vVol-Datenspeicher auf NFS und SAN	ONTAP Tools für VMware vSphere	

Maschine	Speichertyp	Bereitstellung mittels	Support-Hinweise
Hyper-V-VM	Virtuelle FC (vFC) LUNs, die durch einen virtuellen Fibre Channel Switch verbunden sind	SnapCenter -GUI oder PowerShell-Cmdlets	Sie müssen Hyper-V Manager verwenden, um Virtual FC (vFC)-LUNs bereitzustellen, die über einen virtuellen Fibre Channel-Switch verbunden sind. Hyper-V-Passthrough-Festplatten und das Sichern von Datenbanken auf VHD(x), die auf NetApp -Speicher bereitgestellt werden, werden nicht unterstützt.
Hyper-V-VM	iSCSI-LUNs, die vom iSCSI-Initiator direkt mit dem Gastsystem verbunden sind	SnapCenter -GUI oder PowerShell-Cmdlets	Hyper-V-Passthrough-Festplatten und das Sichern von Datenbanken auf VHD(x), die auf NetApp -Speicher bereitgestellt werden, werden nicht unterstützt.

Maschine	Speichertyp	Bereitstellung mittels	Support-Hinweise
Hyper-V-VM	Ein Gastsystem, das mit SMB3-Freigaben verbunden ist, die sich auf einer SVM befinden	SnapCenter -GUI oder PowerShell-Cmdlets	Support nur für die Bereitstellung. Hyper-V-Passthrough-Festplatten und das Sichern von Datenbanken auf VHD(x), die auf NetApp -Speicher bereitgestellt werden, werden nicht unterstützt.

Für das Windows-Plug-In sind mindestens ONTAP -Berechtigungen erforderlich

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach den SnapCenter Plug-Ins, die Sie für den Datenschutz verwenden.

- All-Access-Befehle: Mindestberechtigungen für ONTAP 9.12.1 und höher
  - Ereignis generieren-Autosupport-Protokoll
  - Jobverlauf anzeigen
  - Jobstopp
  - Montag
  - LUN erstellen
  - LUN löschen
  - lun igroup hinzufügen
  - lun igroup erstellen
  - LUN-Igroup löschen
  - LUN-Igroup umbenennen
  - lun igroup show
  - LUN-Zuordnung Add-Reporting-Nodes
  - LUN-Zuordnung erstellen
  - LUN-Zuordnung löschen
  - LUN-Zuordnung zum Entfernen von Berichtsknoten

- LUN-Mapping-Show
- LUN ändern
- LUN-Einzugsvolumen
- lun offline
- lun online
- LUN-Größe ändern
- LUN-Seriennummer
- Lun-Show
- Snapmirror-Richtlinie Add-Rule
- Snapmirror-Richtlinienänderungsregel
- Snapmirror-Richtlinie zum Entfernen der Regel
- Snapmirror-Richtlinien-Show
- Snapmirror-Wiederherstellung
- Snapmirror-Show
- Snapmirror-Showverlauf
- Snapmirror-Update
- Snapmirror-Update-LS-Set
- Snapmirror-Listenziele
- Version
- Volume-Klon erstellen
- Lautstärke Klon Show
- Volume klonen, Aufteilen, Start
- Volumen klonen, teilen, stoppen
- Volume erstellen
- Lautstärke zerstören
- Volume-Datei klonen erstellen
- Volume-Datei Show-Disk-Usage
- Volume offline
- Volumen online
- Lautstärke ändern
- Volume-Qtree erstellen
- Volume-Qtree löschen
- Volume-Qtree ändern
- Volumen Qtree zeigen
- Lautstärkebegrenzung
- Lautstärke anzeigen
- Volume-Snapshot erstellen

- Volume-Snapshot löschen
- Volume-Snapshot ändern
- Volume-Snapshot umbenennen
- Volume-Snapshot wiederherstellen
- Volume-Snapshot-Wiederherstellungsdatei
- Volume-Snapshot anzeigen
- Volume aushängen
- VServer-CIFS
- vServer CIFS-Freigabe erstellen
- VServer CIFS-Freigabe löschen
- vServer CIFS Shadowcopy anzeigen
- VServer CIFS-Freigabe anzeigen
- VServer CIFS anzeigen
- VServer-Exportrichtlinie
- vServer-Exportrichtlinie erstellen
- VServer-Exportrichtlinie löschen
- VServer-Exportrichtlinienregel erstellen
- VServer-Exportrichtlinienregel anzeigen
- VServer-Exportrichtlinie anzeigen
- VServer-ISCSI
- VServer-ISCSI-Verbindung anzeigen
- vServer anzeigen

- Schreibgeschützte Befehle: Mindestberechtigungen für ONTAP 8.3.0 und höher
  - Netzwerkschnittstelle
  - Netzwerkschnittstelle anzeigen
  - vServer

Vorbereiten von Speichersystemen für die SnapMirror und SnapVault -Replikation

Sie können ein SnapCenter -Plug-in mit der ONTAP SnapMirror -Technologie verwenden, um Spiegelkopien von Backup-Sätzen auf einem anderen Volume zu erstellen, und mit der ONTAP SnapVault -Technologie, um eine Backup-Replikation von Festplatte zu Festplatte zur Einhaltung von Standards und für andere Governance-Zwecke durchzuführen. Bevor Sie diese Aufgaben ausführen, müssen Sie eine Datenschutzbeziehung zwischen den Quell- und Zielvolumes konfigurieren und die Beziehung initialisieren.

SnapCenter führt die Aktualisierungen für SnapMirror und SnapVault durch, nachdem der Snapshot-Vorgang abgeschlossen ist. SnapMirror und SnapVault Updates werden als Teil des SnapCenter -Jobs durchgeführt. Wenn Sie SnapMirror Active Sync verwenden, verwenden Sie die Standardzeitpläne von SnapMirror oder SnapVault sowohl für SnapMirror Active Sync als auch für asynchrone Beziehungen.

Wenn Sie von einem NetApp SnapManager -Produkt zu SnapCenter kommen und mit den von Ihnen konfigurierten Datenschutzbeziehungen zufrieden sind, können Sie diesen Abschnitt überspringen.

Eine Datenschutzbeziehung repliziert Daten vom Primärspeicher (dem Quellvolume) auf den Sekundärspeicher (das Zielvolume). Wenn Sie die Beziehung initialisieren, überträgt ONTAP die auf dem Quellvolume referenzierten Datenblöcke auf das Zielvolume.

SnapCenter unterstützt keine Kaskadenbeziehungen zwischen SnapMirror und SnapVault Volumes (**Primär** > **Spiegel** > **Vault**). Sie sollten Fanout-Beziehungen verwenden.

SnapCenter unterstützt die Verwaltung versionsflexibler SnapMirror -Beziehungen. Weitere Informationen zu versionsflexiblen SnapMirror -Beziehungen und deren Einrichtung finden Sie im "ONTAP-Dokumentation" .

Definieren Sie eine Sicherungsstrategie für Windows-Dateisysteme

Durch die Definition einer Sicherungsstrategie vor der Erstellung Ihrer Sicherungen erhalten Sie die Sicherungen, die Sie zum erfolgreichen Wiederherstellen oder Klonen Ihrer Dateisysteme benötigen. Ihre Sicherungsstrategie wird weitgehend durch Ihr Service-Level-Agreement (SLA), Ihr Recovery Time Objective (RTO) und Ihr Recovery Point Objective (RPO) bestimmt.

Ein SLA definiert das erwartete Serviceniveau und behandelt viele servicebezogene Probleme, einschließlich der Verfügbarkeit und Leistung des Dienstes. RTO ist die Zeit, innerhalb derer ein Geschäftsprozess nach einer Dienstunterbrechung wiederhergestellt werden muss. RPO definiert die Strategie für das Alter der Dateien, die aus dem Sicherungsspeicher wiederhergestellt werden müssen, damit der reguläre Betrieb nach einem Fehler wieder aufgenommen werden kann. SLA, RTO und RPO tragen zur Datenschutzstrategie bei.

Sicherungszeitpläne für Windows-Dateisysteme

Die Sicherungshäufigkeit wird in Richtlinien angegeben; ein Sicherungszeitplan wird in der Ressourcengruppenkonfiguration angegeben. Der wichtigste Faktor bei der Festlegung einer Sicherungshäufigkeit oder eines Sicherungsplans ist die Änderungsrate der Ressource und die Wichtigkeit der Daten. Sie können eine häufig genutzte Ressource stündlich sichern, während Sie eine selten genutzte Ressource einmal täglich sichern. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, Ihr Service Level Agreement (SLA) und Ihr Recover Point Objective (RPO).

Ein SLA definiert das erwartete Serviceniveau und behandelt viele servicebezogene Probleme, einschließlich der Verfügbarkeit und Leistung des Dienstes. Ein RPO definiert die Strategie für das Alter der Dateien, die aus dem Sicherungsspeicher wiederhergestellt werden müssen, damit der reguläre Betrieb nach einem Fehler wieder aufgenommen werden kann. SLA und RPO tragen zur Datenschutzstrategie bei.

Selbst bei stark genutzten Ressourcen ist es nicht erforderlich, öfter als ein- oder zweimal täglich eine vollständige Sicherung durchzuführen.

Sicherungszeitpläne bestehen aus den folgenden zwei Teilen:

- Sicherungshäufigkeit

  Die Sicherungshäufigkeit (wie oft Sicherungen durchgeführt werden sollen), bei einigen Plug-Ins als *Zeitplantyp* bezeichnet, ist Teil einer Richtlinienkonfiguration. Sie können beispielsweise die Sicherungshäufigkeit auf stündlich, täglich, wöchentlich oder monatlich konfigurieren oder „Keine“

angeben, wodurch die Richtlinie zu einer Nur-On-Demand-Richtlinie wird. Sie können auf die Richtlinien zugreifen, indem Sie auf **Einstellungen** > **Richtlinien** klicken.

- Sicherungszeitpläne

  Sicherungszeitpläne (genauer Zeitpunkt der Durchführung von Sicherungen) sind Teil einer Ressourcengruppenkonfiguration. Wenn Sie beispielsweise über eine Ressourcengruppe verfügen, für die eine Richtlinie für wöchentliche Sicherungen konfiguriert ist, können Sie den Zeitplan so konfigurieren, dass jeden Donnerstag um 22:00 Uhr eine Sicherung durchgeführt wird. Sie können auf Ressourcengruppenpläne zugreifen, indem Sie auf **Ressourcen** > **Ressourcengruppen** klicken.

Anzahl der für Windows-Dateisysteme benötigten Sicherungen

Zu den Faktoren, die die Anzahl der benötigten Sicherungen bestimmen, gehören die Größe des Windows-Dateisystems, die Anzahl der verwendeten Volumes, die Änderungsrate des Dateisystems und Ihr Service Level Agreement (SLA).

Sicherungsnamenskonvention für Windows-Dateisysteme

Für die Sicherung von Windows-Dateisystemen wird die standardmäßige Snapshot-Benennungskonvention verwendet. Die standardmäßige Namenskonvention für Backups fügt den Snapshot-Namen einen Zeitstempel hinzu, der Ihnen hilft, den Zeitpunkt der Erstellung der Kopien zu identifizieren.

Der Snapshot verwendet die folgende Standard-Namenskonvention:
Ressourcengruppenname_Hostname_Zeitstempel

Sie sollten Ihre Backup-Ressourcengruppen logisch benennen, wie im folgenden Beispiel:

```
dts1_mach1x88_03-12-2015_23.17.26
```

In diesem Beispiel haben die Syntaxelemente folgende Bedeutung:

- `dts1`ist der Name der Ressourcengruppe.
- `mach1x88`ist der Hostname.
- `03-12-2016_23.17.26`ist das Datum und der Zeitstempel.

Beim Erstellen einer Sicherung können Sie auch ein beschreibendes Tag hinzufügen, um die Identifizierung der Sicherung zu erleichtern. Wenn Sie dagegen eine benutzerdefinierte Namenskonvention für die Sicherung verwenden möchten, müssen Sie die Sicherung nach Abschluss des Sicherungsvorgangs umbenennen.

Optionen zur Backup-Aufbewahrung

Sie können entweder die Anzahl der Tage auswählen, für die Sicherungskopien aufbewahrt werden sollen, oder die Anzahl der Sicherungskopien angeben, die Sie aufbewahren möchten, bis zu einem ONTAP Maximum von 255 Kopien. Beispielsweise kann es in Ihrer Organisation erforderlich sein, dass Sie Sicherungskopien für 10 Tage oder 130 Sicherungskopien aufbewahren.

Beim Erstellen einer Richtlinie können Sie die Aufbewahrungsoptionen für den Sicherungstyp und den Zeitplantyp angeben.

Wenn Sie die SnapMirror Replikation einrichten, wird die Aufbewahrungsrichtlinie auf dem Zielvolume gespiegelt.

SnapCenter löscht die aufbewahrten Sicherungen, deren Aufbewahrungsbezeichnungen dem Zeitplantyp entsprechen. Wenn der Zeitplantyp für die Ressource oder Ressourcengruppe geändert wurde, verbleiben möglicherweise noch Sicherungen mit der alten Zeitplantypbezeichnung auf dem System.

Für die langfristige Aufbewahrung von Sicherungskopien sollten Sie SnapVault Backup verwenden.

Quellen und Ziele von Klonen für Windows-Dateisysteme

Sie können eine Dateisystemsicherung vom Primär- oder Sekundärspeicher klonen. Sie können auch das Ziel auswählen, das Ihren Anforderungen entspricht: entweder den ursprünglichen Sicherungsspeicherort oder ein anderes Ziel auf demselben oder einem anderen Host. Das Ziel muss sich auf demselben Datenträger wie die Klon-Quellsicherung befinden.

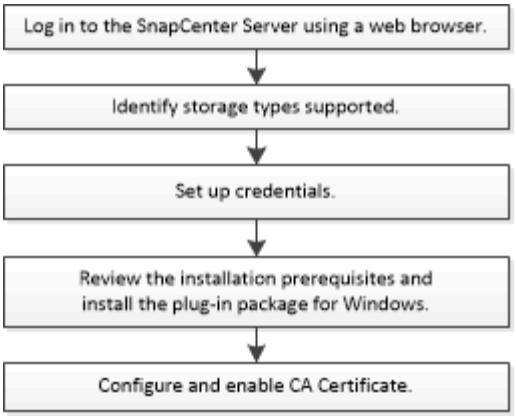
Klonziel	Beschreibung
Original, Quelle, Standort	Standardmäßig speichert SnapCenter den Klon am selben Ort und auf demselben Host wie das zu klonende Backup.
Anderer Standort	Sie können den Klon an einem anderen Ort auf demselben Host oder auf einem anderen Host speichern. Der Host muss über eine konfigurierte Verbindung zur Storage Virtual Machine (SVM) verfügen.

Sie können den Klon umbenennen, nachdem der Klonvorgang abgeschlossen ist.

Installieren Sie das SnapCenter -Plug-in für Microsoft Windows

Installationsablauf des SnapCenter Plug-ins für Microsoft Windows

Sie müssen das SnapCenter Plug-in für Microsoft Windows installieren und einrichten, wenn Sie Windows-Dateien schützen möchten, bei denen es sich nicht um Datenbankdateien handelt.



Installationsanforderungen für das SnapCenter -Plug-in für Microsoft Windows

Sie sollten sich bestimmter Installationsanforderungen bewusst sein, bevor Sie das Plug-in für Windows installieren.

Bevor Sie mit der Verwendung des Plug-ins für Windows beginnen, muss der SnapCenter Administrator den SnapCenter -Server installieren und konfigurieren und die erforderlichen Aufgaben ausführen.

- Sie müssen über SnapCenter Administratorrechte verfügen, um das Plug-in für Windows zu installieren.

  Die SnapCenter Administratorrolle muss über Administratorrechte verfügen.

- Sie müssen den SnapCenter -Server installiert und konfiguriert haben.
- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren.
- Sie müssen SnapMirror und SnapVault einrichten, wenn Sie eine Backup-Replikation wünschen.

Hostanforderungen zur Installation des SnapCenter Plug-Ins-Pakets für Windows

Bevor Sie das SnapCenter Plug-Ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatz- und Größenanforderungen des Hostsystems vertraut sein.

Artikel	Anforderungen
Betriebssysteme	Microsoft Windows Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" . Wenn Sie ein Windows-Cluster-Setup verwenden, sollten Sie auch die Windows-Remoteverwaltung (WinRM) installieren und konfigurieren.
Mindest-RAM für das SnapCenter -Plug-In auf dem Host	1 GB

Artikel	Anforderungen
Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host	5 GB Sie sollten ausreichend Speicherplatz zuweisen und den Speicherverbrauch des Protokollordners überwachen. Der erforderliche Protokollspeicherplatz variiert je nach Anzahl der zu schützenden Entitäten und der Häufigkeit der Datenschutzvorgänge. Wenn nicht genügend Speicherplatz vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	• ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting-Paket • PowerShell Core 7.4.2 Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .

Richten Sie Ihre Anmeldeinformationen für das Plug-in für Windows ein

SnapCenter verwendet Anmeldeinformationen, um Benutzer für SnapCenter -Vorgänge zu authentifizieren. Sie sollten Anmeldeinformationen für die Installation von SnapCenter -Plug-Ins und zusätzliche Anmeldeinformationen für die Durchführung von Datenschutzvorgängen auf Windows-Dateisystemen erstellen.

Was Sie brauchen

- Sie müssen Windows-Anmeldeinformationen einrichten, bevor Sie Plug-Ins installieren.
- Sie müssen die Anmeldeinformationen mit Administratorrechten, einschließlich Administratorrechten, auf dem Remote-Host einrichten.
- Wenn Sie Anmeldeinformationen für einzelne Ressourcengruppen einrichten und der Benutzer nicht über vollständige Administratorrechte verfügt, müssen Sie dem Benutzer mindestens die Ressourcengruppen- und Sicherungsrechte zuweisen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Anmeldeinformationen**.
3. Klicken Sie auf **Neu**.
4. Gehen Sie auf der Seite „Anmeldeinformationen“ wie folgt vor:

Für dieses Feld…	Machen Sie Folgendes…
Anmeldeinformationsname	Geben Sie einen Namen für die Anmeldeinformationen ein.
Benutzername/Passwort	Geben Sie den Benutzernamen und das Kennwort ein, die für die Authentifizierung verwendet werden. • Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe Geben Sie den Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter -Plug-In installieren. Gültige Formate für das Feld „Benutzername“ sind: ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` ◦ `UserName@upn` • Lokaler Administrator (nur für Arbeitsgruppen) Geben Sie für Systeme, die zu einer Arbeitsgruppe gehören, den integrierten lokalen Administrator auf dem System an, auf dem Sie das SnapCenter -Plug-In installieren. Sie können ein lokales Benutzerkonto angeben, das zur lokalen Administratorgruppe gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist. Das gültige Format für das Feld „Benutzername“ lautet wie folgt: `UserName` Verwenden Sie in den Passwörtern keine doppelten Anführungszeichen (") oder Backticks (`). Sie sollten die Zeichen „Kleiner als“ (<) und „Ausrufezeichen“ (!) nicht zusammen in Passwörtern verwenden. Zum Beispiel kleiner als <!10, kleiner als 10 <!, Backtick `12.
Passwort	Geben Sie das zur Authentifizierung verwendete Passwort ein.

5. Klicken Sie auf **OK**.

   Nachdem Sie die Anmeldeinformationen eingerichtet haben, möchten Sie möglicherweise einem Benutzer oder einer Benutzergruppe auf der Seite „Benutzer und Zugriff“ die Anmeldeinformationsverwaltung zuweisen.

Konfigurieren von gMSA unter Windows Server 2016 oder höher

Mit Windows Server 2016 oder höher können Sie ein gruppenverwaltetes Dienstkonto (gMSA) erstellen, das eine automatisierte Kennwortverwaltung für Dienstkonten von einem verwalteten Domänenkonto aus ermöglicht.

Bevor Sie beginnen

- Sie sollten über einen Domänencontroller mit Windows Server 2016 oder höher verfügen.
- Sie sollten über einen Host mit Windows Server 2016 oder höher verfügen, der Mitglied der Domäne ist.

Schritte

1. Erstellen Sie einen KDS-Stammschlüssel, um eindeutige Passwörter für jedes Objekt in Ihrem gMSA zu generieren.
2. Führen Sie für jede Domäne den folgenden Befehl vom Windows-Domänencontroller aus: Add-KDSRootKey -EffectiveImmediately
3. Erstellen und konfigurieren Sie Ihr gMSA:
   a. Erstellen Sie ein Benutzergruppenkonto im folgenden Format:

```
 domainName\accountName$
.. Fügen Sie der Gruppe Computerobjekte hinzu.
.. Verwenden Sie die gerade erstellte Benutzergruppe, um das gMSA zu
erstellen.
```

   Zum Beispiel,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Laufen `Get-ADServiceAccount` Befehl zum Überprüfen des
Dienstkontos.
```

4. Konfigurieren Sie das gMSA auf Ihren Hosts:
   a. Aktivieren Sie das Active Directory-Modul für Windows PowerShell auf dem Host, auf dem Sie das gMSA-Konto verwenden möchten.

   Führen Sie dazu den folgenden Befehl von PowerShell aus:

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                            Name                Install State
------------                            ----                -------------
[ ] Active Directory Domain Services    AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

a. Starten Sie Ihren Host neu.

b. Installieren Sie das gMSA auf Ihrem Host, indem Sie den folgenden Befehl in der PowerShell-Eingabeaufforderung ausführen: `Install-AdServiceAccount <gMSA>`

c. Überprüfen Sie Ihr gMSA-Konto, indem Sie den folgenden Befehl ausführen: `Test-AdServiceAccount <gMSA>`

5. Weisen Sie dem konfigurierten gMSA auf dem Host die Administratorrechte zu.
6. Fügen Sie den Windows-Host hinzu, indem Sie das konfigurierte gMSA-Konto im SnapCenter -Server angeben.

   SnapCenter Server installiert die ausgewählten Plug-Ins auf dem Host und das angegebene gMSA wird während der Plug-In-Installation als Dienstanmeldekonto verwendet.

Hosts hinzufügen und SnapCenter Plug-in für Microsoft Windows installieren

Sie können die SnapCenter -Seite „Host hinzufügen“ verwenden, um Windows-Hosts hinzuzufügen. Das SnapCenter -Plug-in für Microsoft Windows wird automatisch auf dem angegebenen Host installiert. Dies ist die empfohlene Methode zum Installieren von Plug-Ins. Sie können einen Host hinzufügen und ein Plug-In entweder für einen einzelnen Host oder einen Cluster installieren.

Bevor Sie beginnen

- Wenn das Betriebssystem des SnapCenter Server-Hosts Windows 2019 und das Betriebssystem des Plug-in-Hosts Windows 2022 ist, sollten Sie Folgendes durchführen:
  - Upgrade auf Windows Server 2019 (OS Build 17763.5936) oder höher
  - Upgrade auf Windows Server 2022 (OS Build 20348.2402) oder höher
- Sie müssen ein Benutzer sein, dem eine Rolle mit den Berechtigungen zum Installieren und Deinstallieren von Plug-Ins zugewiesen ist, beispielsweise die SnapCenter Administratorrolle.

- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren.
- Der SnapCenter -Benutzer sollte der Rolle „Als Dienst anmelden“ des Windows-Servers hinzugefügt werden.
- Sie sollten sicherstellen, dass der Nachrichtenwarteschlangendienst ausgeführt wird.
- Wenn Sie ein gruppenverwaltetes Dienstkonto (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren.

  "Konfigurieren Sie das gruppenverwaltete Dienstkonto auf Windows Server 2016 oder höher für das Windows-Dateisystem"

Informationen zu diesem Vorgang

- Sie können einen SnapCenter -Server nicht als Plug-In-Host zu einem anderen SnapCenter -Server hinzufügen.
- Windows-Plug-Ins
  - Microsoft Windows
  - Microsoft Exchange Server
  - Microsoft SQL Server
  - SAP HANA
- Installieren von Plug-ins auf einem Cluster

  Wenn Sie Plug-Ins auf einem Cluster (WSFC, Oracle RAC oder Exchange DAG) installieren, werden sie auf allen Knoten des Clusters installiert.

- Speicher der E-Serie

  Sie können das Plug-in für Windows nicht auf einem Windows-Host installieren, der mit einem Speicher der E-Serie verbunden ist.

> SnapCenter unterstützt nicht das Hinzufügen desselben Hosts (Plug-In-Hosts) zu SnapCenter , wenn der Host bereits Teil einer Arbeitsgruppe ist und in eine andere Domäne geändert wurde oder umgekehrt. Wenn Sie denselben Host hinzufügen möchten, sollten Sie den Host aus SnapCenter entfernen und erneut hinzufügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Stellen Sie sicher, dass oben **Managed Hosts** ausgewählt ist.
3. Klicken Sie auf **Hinzufügen**.
4. Gehen Sie auf der Seite „Hosts“ wie folgt vor:

Für dieses Feld…	Machen Sie Folgendes…
Hosttyp	Wählen Sie den Hosttyp **Windows** aus. SnapCenter Server fügt den Host hinzu und installiert dann das Plug-in für Windows, falls es nicht bereits auf dem Host installiert ist.
Hostname	Geben Sie den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter ist auf die richtige Konfiguration des DNS angewiesen. Daher empfiehlt es sich, den vollqualifizierten Domänennamen (FQDN) einzugeben. Sie können die IP-Adressen oder den FQDN eines der folgenden Elemente eingeben: • Eigenständiger Host • Windows Server-Failoverclustering (WSFC) Wenn Sie mit SnapCenter einen Host hinzufügen und dieser Teil einer Subdomäne ist, müssen Sie den FQDN angeben.
Anmeldeinformationen	Wählen Sie den von Ihnen erstellten Anmeldeinformationsnamen aus oder erstellen Sie die neuen Anmeldeinformationen. Die Anmeldeinformationen müssen über Administratorrechte auf dem Remote-Host verfügen. Einzelheiten finden Sie in den Informationen zum Erstellen einer Anmeldeinformation. Details zu den Anmeldeinformationen, einschließlich Benutzername, Domäne und Hosttyp, werden angezeigt, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen bewegen. Der Authentifizierungsmodus wird durch den Hosttyp bestimmt, den Sie im Assistenten „Host hinzufügen“ angeben.

5. Wählen Sie im Abschnitt „Zu installierende Plug-ins auswählen“ die zu installierenden Plug-ins aus.

   Für neue Bereitstellungen werden keine Plug-In-Pakete aufgelistet.

6. (Optional) Klicken Sie auf **Weitere Optionen**.

Für dieses Feld…	Machen Sie Folgendes…
Hafen	Behalten Sie entweder die Standard-Portnummer bei oder geben Sie die Portnummer an. Die Standard-Portnummer ist 8145. Wenn der SnapCenter -Server auf einem benutzerdefinierten Port installiert wurde, wird diese Portnummer als Standardport angezeigt. Wenn Sie die Plug-Ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.
Installationspfad	Der Standardpfad ist C:\Programme\ NetApp\ SnapCenter. Optional können Sie den Pfad anpassen. Für das SnapCenter Plug-ins-Paket für Windows lautet der Standardpfad C:\Programme\ NetApp\ SnapCenter. Wenn Sie möchten, können Sie den Standardpfad jedoch anpassen.
Alle Hosts im Cluster hinzufügen	Aktivieren Sie dieses Kontrollkästchen, um alle Clusterknoten in einem WSFC hinzuzufügen.
Vorinstallationsprüfungen überspringen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-ins bereits manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt.
Verwenden Sie ein gruppenverwaltetes Dienstkonto (gMSA), um die Plug-In-Dienste auszuführen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie zum Ausführen der Plug-In-Dienste ein gruppenverwaltetes Dienstkonto (gMSA) verwenden möchten. Geben Sie den gMSA-Namen im folgenden Format an: *Domänenname\Kontoname$*. gMSA wird nur als Anmeldedienstkonto für das SnapCenter -Plug-in für den Windows-Dienst verwendet.

7. Klicken Sie auf **Senden**.

Wenn Sie das Kontrollkästchen **Vorabprüfungen überspringen** nicht aktiviert haben, wird überprüft, ob

der Host die Anforderungen für die Installation des Plug-Ins erfüllt. Speicherplatz, RAM, PowerShell-Version, .NET-Version und Speicherort werden anhand der Mindestanforderungen überprüft. Werden die Mindestanforderungen nicht erfüllt, werden entsprechende Fehler- bzw. Warnmeldungen angezeigt.

Wenn der Fehler mit dem Speicherplatz oder RAM zusammenhängt, können Sie die Datei web.config aktualisieren, die sich unter `C:\Program Files\NetApp\SnapCenter` WebApp zum Ändern der Standardwerte. Wenn der Fehler mit anderen Parametern zusammenhängt, müssen Sie das Problem beheben.

Wenn Sie in einem HA-Setup die Datei web.config aktualisieren, müssen Sie die Datei auf beiden Knoten aktualisieren.

8. Überwachen Sie den Installationsfortschritt.

Installieren Sie das SnapCenter -Plug-in für Microsoft Windows mithilfe von PowerShell-Cmdlets auf mehreren Remotehosts

Wenn Sie das SnapCenter Plug-in für Microsoft Windows auf mehreren Hosts gleichzeitig installieren möchten, können Sie dies mithilfe des `Install-SmHostPackage` PowerShell-Cmdlet.

Sie müssen sich auf jedem Host, auf dem Sie Plug-Ins installieren möchten, als Domänenbenutzer mit lokalen Administratorrechten bei SnapCenter angemeldet haben.

Schritte

1. Starten Sie PowerShell.
2. Richten Sie auf dem SnapCenter Server-Host eine Sitzung ein, indem Sie `Open-SmConnection` Cmdlet und geben Sie dann Ihre Anmeldeinformationen ein.
3. Fügen Sie den eigenständigen Host oder den Cluster mithilfe des `Add-SmHost` Cmdlet und die erforderlichen Parameter.

   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" .

4. Installieren Sie das Plug-in auf mehreren Hosts mithilfe der `Install-SmHostPackage` Cmdlet und die erforderlichen Parameter.

   Sie können die `-skipprecheck` Option, wenn Sie die Plug-Ins manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-Ins erfüllt.

Installieren Sie das SnapCenter -Plug-in für Microsoft Windows im Hintergrund über die Befehlszeile

Sie können das SnapCenter -Plug-in für Microsoft Windows lokal auf einem Windows-Host installieren, wenn Sie das Plug-in nicht remote über die SnapCenter -GUI installieren können. Sie können das Installationsprogramm des SnapCenter -Plug-ins für Microsoft Windows unbeaufsichtigt im stillen Modus über die Windows-Befehlszeile ausführen.

Bevor Sie beginnen

- Sie müssen das Hosting-Paket ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) installiert haben.
- Sie müssen PowerShell 7.4.2 oder höher installiert haben.
- Sie müssen ein lokaler Administrator auf dem Host sein.

Schritte

1. Laden Sie das SnapCenter -Plug-in für Microsoft Windows von Ihrem Installationsort herunter.

   Der Standardinstallationspfad ist beispielsweise C:\ProgramData\ NetApp\ SnapCenter\Package Repository.

   Auf diesen Pfad kann vom Host aus zugegriffen werden, auf dem der SnapCenter -Server installiert ist.

2. Kopieren Sie die Installationsdatei auf den Host, auf dem Sie das Plug-In installieren möchten.
3. Navigieren Sie in der Eingabeaufforderung zu dem Verzeichnis, in das Sie die Installationsdatei heruntergeladen haben.
4. Geben Sie den folgenden Befehl ein und ersetzen Sie die Variablen durch Ihre Daten:

   ```
   "snapcenter_windows_host_plugin.exe"/silent / debuglog"" /log""
   BI_SNAPCENTER_PORT= SUITE_INSTALLDIR="" BI_SERVICEACCOUNT= BI_SERVICEPWD=
   ISFeatureInstall=SCW
   ```

   Beispiel:

   ```
   `"C:\ProgramData\NetApp\SnapCenter\Package Repository
   \snapcenter_windows_host_plugin.exe"/silent /debuglog"C:
   \HPPW_SCW_Install.log" /log"C:\" BI_SNAPCENTER_PORT=8145
   SUITE_INSTALLDIR="C: \Program Files\NetApp\SnapCenter"
   BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
   ISFeatureInstall=SCW`
   ```

   Bei allen während der Installation des Plug-ins für Windows übergebenen Parametern wird zwischen Groß- und Kleinschreibung unterschieden.

   Geben Sie die Werte für die folgenden Variablen ein:

Variable	Wert
/debuglog"<Debug_Log_Pfad>	Geben Sie den Namen und den Speicherort der Protokolldatei des Suite-Installationsprogramms an, wie im folgenden Beispiel: Setup.exe /debuglog"C:\PathToLog\setupexe.log".
BI_SNAPCENTER_PORT	Geben Sie den Port an, über den SnapCenter mit SMCore kommuniziert.

Variable	Wert
SUITE_INSTALLDIR	Geben Sie das Installationsverzeichnis des Host-Plug-In-Pakets an.
BI_SERVICEACCOUNT	Geben Sie das SnapCenter Plug-in für das Microsoft Windows-Webdienstkonto an.
BI_SERVICEPWD	Geben Sie das Kennwort für das SnapCenter Plug-in für das Microsoft Windows-Webdienstkonto an.
ISFeatureInstall	Geben Sie die Lösung an, die von SnapCenter auf dem Remote-Host bereitgestellt werden soll.

Der Parameter *debuglog* enthält den Pfad der Protokolldatei für SnapCenter. Das Schreiben in diese Protokolldatei ist die bevorzugte Methode zum Abrufen von Informationen zur Fehlerbehebung, da die Datei die Ergebnisse der Prüfungen enthält, die die Installation hinsichtlich der Plug-In-Voraussetzungen durchführt.

Bei Bedarf finden Sie zusätzliche Informationen zur Fehlerbehebung in der Protokolldatei für das SnapCenter für Windows-Paket. Die Protokolldateien für das Paket werden (die ältesten zuerst) im Ordner *%Temp%* aufgelistet, beispielsweise *C:\temp*.

Bei der Installation des Plug-ins für Windows wird das Plug-in auf dem Host und nicht auf dem SnapCenter -Server registriert. Sie können das Plug-In auf dem SnapCenter -Server registrieren, indem Sie den Host mithilfe der SnapCenter GUI oder des PowerShell-Cmdlets hinzufügen. Nachdem der Host hinzugefügt wurde, wird das Plug-In automatisch erkannt.

Überwachen des Installationsstatus des SnapCenter -Plug-In-Pakets

Sie können den Fortschritt der Installation des SnapCenter -Plug-In-Pakets auf der Seite „Jobs“ überwachen. Möglicherweise möchten Sie den Installationsfortschritt überprüfen, um festzustellen, wann die Installation abgeschlossen ist oder ob ein Problem vorliegt.

Informationen zu diesem Vorgang

Die folgenden Symbole werden auf der Seite „Jobs“ angezeigt und geben den Status des Vorgangs an:

- Im Gange
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In der Warteschlange

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Überwachen** auf **Jobs**.

3. Um auf der Seite **Jobs** die Liste so zu filtern, dass nur Plug-In-Installationsvorgänge aufgeführt werden, gehen Sie wie folgt vor:
   a. Klicken Sie auf **Filter**.
   b. Optional: Geben Sie das Start- und Enddatum an.
   c. Wählen Sie im Dropdown-Menü „Typ“ die Option „Plug-in-Installation“ aus.
   d. Wählen Sie im Dropdown-Menü „Status“ den Installationsstatus aus.
   e. Klicken Sie auf **Übernehmen**.
4. Wählen Sie den Installationsauftrag aus und klicken Sie auf **Details**, um die Auftragsdetails anzuzeigen.
5. Klicken Sie auf der Seite **Auftragsdetails** auf **Protokolle anzeigen**.

Konfigurieren des CA-Zertifikats

CA-Zertifikat-CSR-Datei generieren

Sie können eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) generieren und das Zertifikat importieren, das Sie mithilfe der generierten CSR von einer Zertifizierungsstelle (Certificate Authority, CA) erhalten können. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block verschlüsselten Textes, der einem autorisierten Zertifikatsanbieter übergeben wird, um das signierte CA-Zertifikat zu beschaffen.

Die RSA-Schlüssellänge des CA-Zertifikats muss mindestens 3072 Bit betragen.

Informationen zum Generieren einer CSR finden Sie unter "So generieren Sie eine CA-Zertifikat-CSR-Datei" .

Wenn Sie das CA-Zertifikat für Ihre Domäne (*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie das Generieren der CSR-Datei des CA-Zertifikats überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die jeweiligen Hostnamen im CA-Zertifikat erwähnt werden. Das Zertifikat kann aktualisiert werden, indem vor dem Erwerb des Zertifikats das Feld „Subject Alternative Name (SAN)“ ausgefüllt wird. Bei einem Wildcard-Zertifikat (*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

CA-Zertifikate importieren

Sie müssen die CA-Zertifikate mithilfe der Microsoft Management Console (MMC) in den SnapCenter -Server und die Windows-Host-Plug-Ins importieren.

Schritte

1. Gehen Sie zur Microsoft-Verwaltungskonsole (MMC) und klicken Sie dann auf **Datei** > **Snap-In hinzufügen/entfernen**.
2. Wählen Sie im Fenster „Snap-Ins hinzufügen oder entfernen“ **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Zertifikat-Snap-In-Fenster die Option **Computerkonto** und klicken Sie dann auf **Fertig**.
4. Klicken Sie auf **Konsolenstamm** > **Zertifikate – Lokaler Computer** > **Vertrauenswürdige**

Stammzertifizierungsstellen > **Zertifikate**.

5. Klicken Sie mit der rechten Maustaste auf den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ und wählen Sie dann **Alle Aufgaben** > **Importieren**, um den Importassistenten zu starten.
6. Schließen Sie den Assistenten wie folgt ab:

In diesem Assistentenfenster …	Gehen Sie wie folgt vor…
Privaten Schlüssel importieren	Wählen Sie die Option **Ja**, importieren Sie den privaten Schlüssel und klicken Sie anschließend auf **Weiter**.
Importdateiformat	Nehmen Sie keine Änderungen vor; klicken Sie auf **Weiter**.
Sicherheit	Geben Sie das neue Kennwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf **Weiter**.
Abschließen des Zertifikatimport-Assistenten	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**, um den Import zu starten.

Das zu importierende Zertifikat sollte mit dem privaten Schlüssel gebündelt werden (unterstützte Formate sind: *.pfx, *.p12 und *.p7b).

7. Wiederholen Sie Schritt 5 für den Ordner „Persönlich“.

Abrufen des CA-Zertifikatfingerabdrucks

Ein Zertifikatfingerabdruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Aus dem Inhalt des Zertifikats wird mithilfe eines Fingerabdruckalgorithmus ein Fingerabdruck berechnet.

Schritte

1. Führen Sie auf der GUI Folgendes aus:
   a. Doppelklicken Sie auf das Zertifikat.
   b. Klicken Sie im Dialogfeld „Zertifikat“ auf die Registerkarte „Details“.
   c. Blättern Sie durch die Liste der Felder und klicken Sie auf **Fingerabdruck**.
   d. Kopieren Sie die Hexadezimalzeichen aus dem Feld.
   e. Entfernen Sie die Leerzeichen zwischen den Hexadezimalzahlen.

      Wenn der Fingerabdruck beispielsweise lautet: „a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b“, lautet er nach dem Entfernen der Leerzeichen: „a909502dd82ae41433e6f83886b00d4277a32a7b“.

2. Führen Sie in PowerShell Folgendes aus:
   a. Führen Sie den folgenden Befehl aus, um den Fingerabdruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreffnamens zu identifizieren.

Get-ChildItem -Pfad Zertifikat:\LocalMachine\My

b. Kopieren Sie den Fingerabdruck.

Konfigurieren Sie das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten

Sie sollten das CA-Zertifikat mit den Windows-Host-Plug-In-Diensten konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

Führen Sie die folgenden Schritte auf dem SnapCenter -Server und allen Plug-In-Hosts aus, auf denen bereits CA-Zertifikate bereitgestellt sind.

Schritte

1. Entfernen Sie die vorhandene Zertifikatsbindung mit dem SMCore-Standardport 8145, indem Sie den folgenden Befehl ausführen:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Beispiel:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Binden Sie das neu installierte Zertifikat an die Windows-Host-Plug-in-Dienste, indem Sie die folgenden Befehle ausführen:
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert appid="$guid"
   ```

   Beispiel:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert appid="$guid"
   ```

CA-Zertifikate für Plug-Ins aktivieren

Sie sollten die CA-Zertifikate konfigurieren und die CA-Zertifikate im SnapCenter -Server und den entsprechenden Plug-In-Hosts bereitstellen. Sie sollten die CA-Zertifikatvalidierung für die Plug-Ins aktivieren.

Bevor Sie beginnen

- Sie können die CA-Zertifikate mit dem Cmdlet „*Set-SmCertificateSettings*“ aktivieren oder deaktivieren.
- Den Zertifikatsstatus der Plug-ins können Sie sich mit *Get-SmCertificateSettings* anzeigen lassen.

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" .

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Verwaltete Hosts**.
3. Wählen Sie einzelne oder mehrere Plug-In-Hosts aus.
4. Klicken Sie auf **Weitere Optionen**.
5. Wählen Sie **Zertifikatvalidierung aktivieren**.

Nach Abschluss

Auf der Registerkarte „Managed Hosts“ wird ein Vorhängeschloss angezeigt und die Farbe des Vorhängeschlosses zeigt den Status der Verbindung zwischen SnapCenter Server und dem Plug-in-Host an.

- * * zeigt an, dass das CA-Zertifikat weder aktiviert noch dem Plug-In-Host zugewiesen ist.
- * * zeigt an, dass das CA-Zertifikat erfolgreich validiert wurde.
- * * zeigt an, dass das CA-Zertifikat nicht validiert werden konnte.
- * * zeigt an, dass die Verbindungsinformationen nicht abgerufen werden konnten.

Wenn der Status gelb oder grün ist, wurden die Datenschutzvorgänge erfolgreich abgeschlossen.

Installieren Sie das SnapCenter Plug-in for VMware vSphere

Wenn Ihre Datenbank oder Ihr Dateisystem auf virtuellen Maschinen (VMs) gespeichert ist oder Sie VMs und Datenspeicher schützen möchten, müssen Sie das SnapCenter Plug-in for VMware vSphere Appliance bereitstellen.

Informationen zur Bereitstellung finden Sie unter "Bereitstellungsübersicht" .

CA-Zertifikat bereitstellen

Informationen zum Konfigurieren des CA-Zertifikats mit dem SnapCenter Plug-in for VMware vSphere finden Sie unter "SSL-Zertifikat erstellen oder importieren" .

Konfigurieren der CRL-Datei

Das SnapCenter Plug-in for VMware vSphere sucht in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien. Das Standardverzeichnis der CRL-Dateien für das SnapCenter Plug-in for VMware vSphere ist */opt/netapp/config/crl*.

Sie können mehr als eine CRL-Datei in diesem Verzeichnis ablegen. Die eingehenden Zertifikate werden anhand der einzelnen CRLs überprüft.

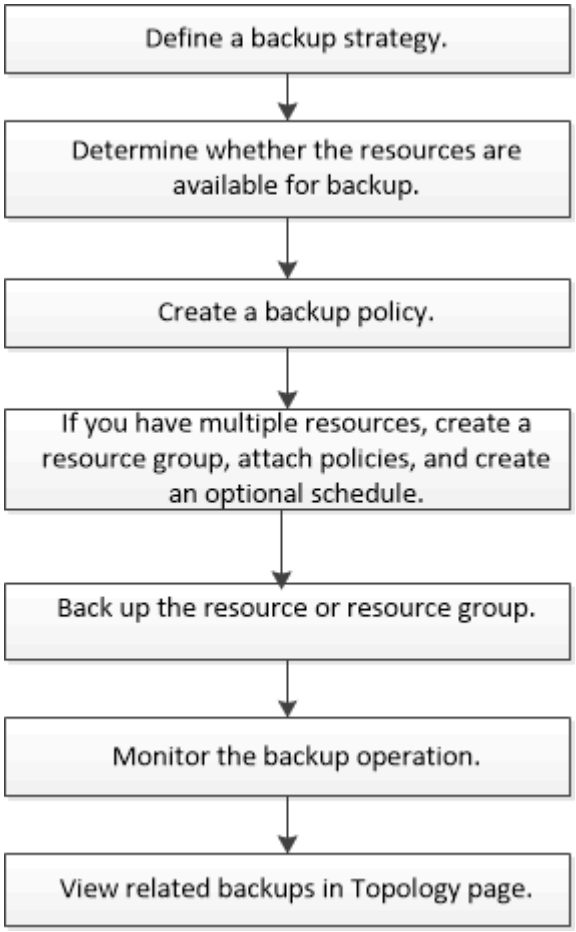
Sichern Sie Windows-Dateisysteme

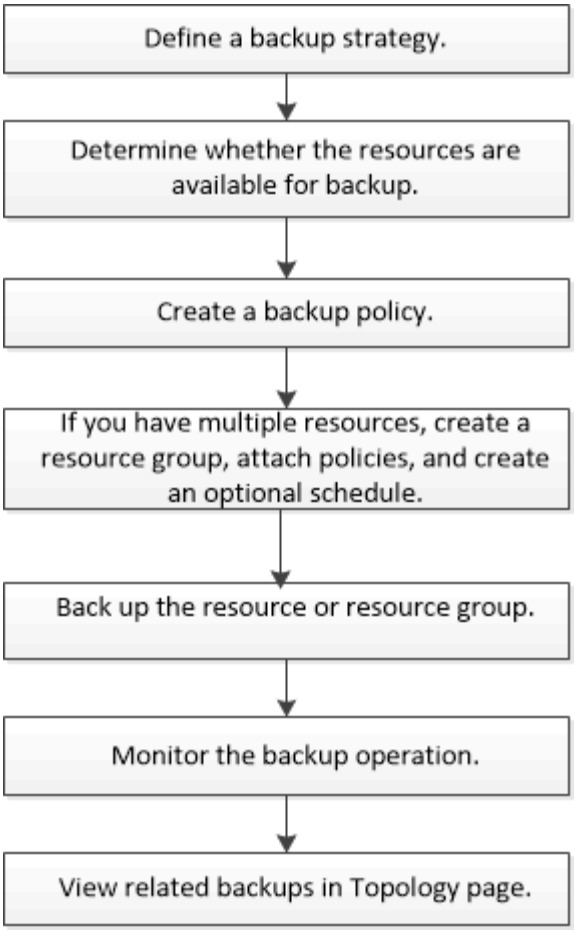
Sichern Sie Windows-Dateisysteme

Wenn Sie das SnapCenter -Plug-in für Microsoft Windows in Ihrer Umgebung installieren, können Sie SnapCenter zum Sichern von Windows-Dateisystemen verwenden. Sie können ein einzelnes Dateisystem oder eine Ressourcengruppe sichern, die mehrere Dateisysteme enthält. Sie können Backups nach Bedarf oder gemäß einem festgelegten Schutzzeitplan durchführen.

Sie können mehrere Sicherungen so planen, dass sie gleichzeitig auf mehreren Servern ausgeführt werden. Sicherungs- und Wiederherstellungsvorgänge können nicht gleichzeitig auf derselben Ressource ausgeführt werden.

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie die Sicherungsvorgänge durchführen müssen:





Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter -Cmdlet-Hilfe oder die "Referenzhandbuch für SnapCenter -Software-Cmdlets" enthält ausführliche Informationen zu PowerShell-Cmdlets.

Ermitteln der Ressourcenverfügbarkeit für Windows-Dateisysteme

Ressourcen sind die LUNs und ähnliche Komponenten in Ihrem Dateisystem, die von den von Ihnen installierten Plug-Ins verwaltet werden. Sie können diese Ressourcen zu Ressourcengruppen hinzufügen, sodass Sie Datenschutzjobs auf mehreren Ressourcen ausführen können. Zunächst müssen Sie jedoch ermitteln, welche Ressourcen Ihnen zur Verfügung stehen. Durch die Ermittlung verfügbarer Ressourcen wird auch überprüft, ob die Plug-In-Installation erfolgreich abgeschlossen wurde.

Bevor Sie beginnen

- Sie müssen bereits Aufgaben wie die Installation von SnapCenter Server, das Hinzufügen von Hosts, das Erstellen von Verbindungen für virtuelle Speichermaschinen (SVM) und das Hinzufügen von Anmeldeinformationen abgeschlossen haben.
- Wenn sich Dateien auf VMware RDM LUNs oder VMDKs befinden, müssen Sie das SnapCenter Plug-in for VMware vSphere bereitstellen und das Plug-in bei SnapCenter registrieren. Weitere Informationen finden Sie unter "SnapCenter Plug-in for VMware vSphere Dokumentation" .

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“ **Dateisysteme** aus der Liste aus.
3. Wählen Sie den Host aus, um die Liste der Ressourcen zu filtern, und klicken Sie dann auf **Ressourcen aktualisieren**.

   Die neu hinzugefügten, umbenannten oder gelöschten Dateisysteme werden im SnapCenter Server-Inventar aktualisiert.

   Sie müssen die Ressourcen aktualisieren, wenn die Datenbanken außerhalb von SnapCenter umbenannt werden.

Erstellen von Sicherungsrichtlinien für Windows-Dateisysteme

Sie können eine neue Sicherungsrichtlinie für Ressourcen erstellen, bevor Sie SnapCenter zum Sichern von Windows-Dateisystemen verwenden, oder Sie können eine neue Sicherungsrichtlinie erstellen, wenn Sie eine Ressourcengruppe erstellen oder eine Ressource sichern.

Bevor Sie beginnen

- Sie müssen Ihre Sicherungsstrategie definiert haben."Mehr erfahren"
- Sie müssen sich auf den Datenschutz vorbereitet haben.

  Zur Vorbereitung des Datenschutzes müssen Sie Aufgaben wie die Installation von SnapCenter, das Hinzufügen von Hosts, das Erkennen von Ressourcen und das Erstellen von Verbindungen zu virtuellen Speichermaschinen (SVM) erledigen.

- Wenn Sie Snapshots auf einen Spiegel- oder Tresor-Sekundärspeicher replizieren, muss der SnapCenter Administrator Ihnen die SVMs sowohl für das Quell- als auch für das Zielvolume zugewiesen haben.
- Wenn Sie die PowerShell-Skripte in Prescripts und Postscripts ausführen möchten, sollten Sie den Wert des Parameters usePowershellProcessforScripts in der Datei web.config auf true setzen.

  Der Standardwert ist „false“

- Überprüfen Sie die spezifischen Voraussetzungen und Einschränkungen der SnapMirror Active Sync. Weitere Informationen finden Sie unter "Objektlimits für SnapMirror Active Sync" .

Informationen zu diesem Vorgang

- Der SCRIPTS_PATH wird mithilfe des Schlüssels „PredefinedWindowsScriptsDirectory“ definiert, der sich in der Datei „SMCoreServiceHost.exe.Config“ des Plug-In-Hosts befindet.

  Bei Bedarf können Sie diesen Pfad ändern und den SMcore-Dienst neu starten. Aus Sicherheitsgründen wird empfohlen, den Standardpfad zu verwenden.

  Der Wert des Schlüssels kann von Swagger über die API angezeigt werden: API /4.7/configsettings

  Sie können die GET-API verwenden, um den Wert des Schlüssels anzuzeigen. SET-API wird nicht unterstützt.

- SnapLock
  - Wenn die Option „Sicherungskopien für eine bestimmte Anzahl von Tagen aufbewahren“ ausgewählt

ist, muss die SnapLock -Aufbewahrungsdauer kleiner oder gleich der angegebenen Aufbewahrungsdauer in Tagen sein.

- Durch die Angabe einer Snapshot-Sperrfrist wird das Löschen der Snapshots verhindert, bis die Aufbewahrungsfrist abgelaufen ist. Dies kann dazu führen, dass mehr Snapshots aufbewahrt werden als in der Richtlinie angegeben.
- Bei ONTAP 9.12.1 und niedrigeren Versionen erben die im Rahmen der Wiederherstellung aus den SnapLock Vault-Snapshots erstellten Klone die Ablaufzeit von SnapLock Vault. Der Speicheradministrator sollte die Klone nach Ablauf des SnapLock manuell bereinigen.

Schritte

1. Wählen Sie im linken Navigationsbereich **Einstellungen** aus.
2. Wählen Sie auf der Seite „Einstellungen“ **Richtlinien** aus.
3. Wählen Sie **Neu**.
4. Geben Sie auf der Seite „Name“ den Richtliniennamen und die Details ein.
5. Führen Sie auf der Seite „Sicherung und Replikation“ die folgenden Aufgaben aus:

   a. Wählen Sie eine Sicherungseinstellung aus.

Option	Beschreibung
Dateisystemkonsistente Sicherung	Wählen Sie diese Option, wenn SnapCenter das Festplattenlaufwerk, auf dem sich das Dateisystem befindet, vor Beginn des Sicherungsvorgangs stilllegen und das Festplattenlaufwerk nach Abschluss des Sicherungsvorgangs wieder aktivieren soll.
Dateisystem-Absturzkonsistente Sicherung	Wählen Sie diese Option, wenn SnapCenter das Festplattenlaufwerk, auf dem sich das Dateisystem befindet, nicht stilllegen soll.

   b. Wählen Sie eine Zeitplanhäufigkeit (auch Richtlinientyp genannt) aus.

   Die Richtlinie gibt nur die Sicherungshäufigkeit an. Der spezifische Schutzzeitplan für die Sicherung wird in der Ressourcengruppe definiert. Daher können zwei oder mehr Ressourcengruppen dieselbe Richtlinie und Sicherungshäufigkeit verwenden, jedoch unterschiedliche Sicherungspläne haben.

   Wenn Sie 2:00 Uhr morgens geplant haben, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.

   c. Wählen Sie eine Richtlinienbezeichnung aus.

   Abhängig von der von Ihnen ausgewählten Snapshot-Bezeichnung wendet ONTAP die sekundäre Snapshot-Aufbewahrungsrichtlinie an, die der Bezeichnung entspricht.

Wenn Sie * SnapMirror nach dem Erstellen einer lokalen Snapshot-Kopie aktualisieren* ausgewählt haben, können Sie optional die sekundäre Richtlinienbezeichnung angeben. Wenn Sie jedoch * SnapVault nach dem Erstellen einer lokalen Snapshot-Kopie aktualisieren* ausgewählt haben, sollten Sie die sekundäre Richtlinienbezeichnung angeben.

6. Wählen Sie im Abschnitt „Sekundäre Replikationsoptionen auswählen“ eine oder beide der folgenden sekundären Replikationsoptionen aus:

Für dieses Feld…	Machen Sie Folgendes…
Aktualisieren Sie SnapMirror , nachdem Sie eine lokale Snapshot-Kopie erstellt haben	Wählen Sie diese Option, um Spiegelkopien von Sicherungssätzen auf einem anderen Volume (SnapMirror) zu erstellen. Diese Option sollte für die aktive Synchronisierung von SnapSnapMirror aktiviert werden. Während der sekundären Replikation lädt die Ablaufzeit des SnapLock die Ablaufzeit des primären SnapLock . Durch Klicken auf die Schaltfläche **Aktualisieren** auf der Seite „Topologie“ werden die Ablaufzeiten des sekundären und primären SnapLock aktualisiert, die von ONTAP abgerufen werden. Sehen "Anzeigen zugehöriger Sicherungen und Klone auf der Seite „Topologie““ .
Aktualisieren Sie SnapVault nach dem Erstellen einer Snapshot-Kopie	Wählen Sie diese Option, um eine Backup-Replikation von Festplatte zu Festplatte durchzuführen. Während der sekundären Replikation lädt die Ablaufzeit des SnapLock die Ablaufzeit des primären SnapLock . Durch Klicken auf die Schaltfläche „Aktualisieren“ auf der Seite „Topologie“ werden die Ablaufzeiten des sekundären und primären SnapLock aktualisiert, die von ONTAP abgerufen werden. Wenn SnapLock nur auf dem sekundären Server von ONTAP , bekannt als SnapLock Vault, konfiguriert ist, wird durch Klicken auf die Schaltfläche „Aktualisieren“ auf der Seite „Topologie“ die Sperrdauer auf dem sekundären Server aktualisiert, die von ONTAP abgerufen wird. Weitere Informationen zu SnapLock Vault finden Sie unter "Übertragen Sie Snapshot-Kopien in WORM auf einem Tresorziel"

Für dieses Feld…	Machen Sie Folgendes…
Fehleranzahl der Wiederholungsversuche	Geben Sie die Anzahl der Replikationsversuche ein, die durchgeführt werden sollen, bevor der Prozess angehalten wird.

Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Speicher konfigurieren, um zu vermeiden, dass das maximale Limit für Snapshots auf dem sekundären Speicher erreicht wird.

7. Geben Sie auf der Seite „Aufbewahrungseinstellungen“ die Aufbewahrungseinstellungen für On-Demand-Backups und für jede von Ihnen ausgewählte Zeitplanhäufigkeit an.

Option	Beschreibung
Gesamtzahl der aufzubewahrenden Snapshot-Kopien	Wählen Sie diese Option, wenn Sie die Anzahl der Snapshots angeben möchten, die SnapCenter speichert, bevor sie automatisch gelöscht werden.
Bewahren Sie Snapshot-Kopien für	Wählen Sie diese Option, wenn Sie die Anzahl der Tage angeben möchten, die SnapCenter eine Sicherungskopie aufbewahrt, bevor sie gelöscht wird.
Sperrzeitraum für Snapshot-Kopien	Wählen Sie den Snapshot-Sperrzeitraum aus und geben Sie die Dauer in Tagen, Monaten oder Jahren an. Die Aufbewahrungsdauer von SnapLock sollte weniger als 100 Jahre betragen.

Sie sollten die Aufbewahrungsanzahl auf 2 oder höher einstellen. Der Mindestwert für die Aufbewahrungsanzahl beträgt 2.

Der maximale Aufbewahrungswert beträgt 1018. Sicherungen schlagen fehl, wenn die Aufbewahrung auf einen höheren Wert eingestellt ist, als von der ONTAP Version unterstützt wird.

8. Geben Sie auf der Seite „Skript“ den Pfad des Präskripts oder Postskripts ein, das der SnapCenter -Server vor bzw. nach dem Sicherungsvorgang ausführen soll, sowie ein Zeitlimit, das SnapCenter auf die Ausführung des Skripts wartet, bevor es zu einer Zeitüberschreitung kommt.

   Sie können beispielsweise ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnungen zu automatisieren und Protokolle zu senden.

Der Prescripts- oder Postscripts-Pfad sollte keine Laufwerke oder Freigaben enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

Erstellen von Ressourcengruppen für Windows-Dateisysteme

Eine Ressourcengruppe ist der Container, zu dem Sie mehrere Dateisysteme hinzufügen können, die Sie schützen möchten. Sie müssen der Ressourcengruppe außerdem eine oder mehrere Richtlinien zuordnen, um den Typ des Datenschutzauftrags zu definieren, den Sie ausführen möchten, und dann den Sicherungszeitplan angeben.

Informationen zu diesem Vorgang

- Bei ONTAP 9.12.1 und niedrigeren Versionen erben die im Rahmen der Wiederherstellung aus den SnapLock Vault-Snapshots erstellten Klone die Ablaufzeit von SnapLock Vault. Der Speicheradministrator sollte die Klone nach Ablauf des SnapLock manuell bereinigen.
- Das Hinzufügen neuer Dateisysteme ohne SnapMirror Active Sync zu einer vorhandenen Ressourcengruppe, die Ressourcen mit SnapMirror Active Sync enthält, wird nicht unterstützt.
- Das Hinzufügen neuer Dateisysteme zu einer vorhandenen Ressourcengruppe im Failover-Modus von SnapMirror Active Sync wird nicht unterstützt. Sie können der Ressourcengruppe nur im regulären oder Failback-Zustand Ressourcen hinzufügen.

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“ **Dateisysteme** aus der Liste aus.

   Wenn Sie SnapCenter kürzlich ein Dateisystem hinzugefügt haben, klicken Sie auf **Ressourcen aktualisieren**, um die neu hinzugefügte Ressource anzuzeigen.

3. Klicken Sie auf **Neue Ressourcengruppe**.
4. Führen Sie auf der Seite „Name“ des Assistenten die folgenden Schritte aus:

Für dieses Feld…	Machen Sie Folgendes…
Name	Geben Sie den Namen der Ressourcengruppe ein. Der Name der Ressourcengruppe sollte nicht länger als 250 Zeichen sein.
Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden	Optional: Geben Sie einen benutzerdefinierten Snapshot-Namen und ein benutzerdefiniertes Format ein. Beispiel: customtext_resourcegroup_policy_hostname oder resourcegroup_hostname. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.
Etikett	Geben Sie ein beschreibendes Tag ein, um die Suche nach einer Ressourcengruppe zu erleichtern.

5. Führen Sie auf der Seite „Ressourcen“ die folgenden Aufgaben aus:

   a. Wählen Sie den Host aus, um die Liste der Ressourcen zu filtern.

      Wenn Sie kürzlich Ressourcen hinzugefügt haben, werden diese erst in der Liste der verfügbaren Ressourcen angezeigt, nachdem Sie Ihre Ressourcenliste aktualisiert haben.

   b. Klicken Sie im Abschnitt „Verfügbare Ressourcen“ auf die Dateisysteme, die Sie sichern möchten, und klicken Sie dann auf den Rechtspfeil, um sie in den Abschnitt „Hinzugefügt“ zu verschieben.

      Wenn Sie die Option **Alle Ressourcen auf demselben Speichervolume automatisch auswählen** auswählen, werden alle Ressourcen auf demselben Volume ausgewählt. Wenn Sie sie in den Abschnitt „Hinzugefügt“ verschieben, werden alle Ressourcen auf diesem Volume zusammen verschoben.

   Um ein einzelnes Dateisystem hinzuzufügen, deaktivieren Sie die Option **Alle Ressourcen auf demselben Speichervolume automatisch auswählen** und wählen Sie dann die Dateisysteme aus, die Sie in den Abschnitt „Hinzugefügt“ verschieben möchten.

6. Führen Sie auf der Seite „Richtlinien“ die folgenden Aufgaben aus:

   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdownliste aus.

      Sie können eine beliebige vorhandene Richtlinie auswählen und auf **Details** klicken, um festzustellen, ob Sie diese Richtlinie verwenden können.

      Wenn keine vorhandene Richtlinie Ihren Anforderungen entspricht, können Sie eine neue Richtlinie erstellen, indem Sie auf * klicken.  * um den Richtlinienassistenten zu starten.

      Die ausgewählten Richtlinien werden in der Spalte „Richtlinie“ im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ aufgelistet.

   b. Klicken Sie im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ auf *  * in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie den Zeitplan konfigurieren möchten.

   c. Wenn die Richtlinie mit mehreren Zeitplantypen (Häufigkeiten) verknüpft ist, wählen Sie die Häufigkeit aus, die Sie konfigurieren möchten.

   d. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtlinienname* hinzufügen“ den Zeitplan, indem Sie das Startdatum, das Ablaufdatum und die Häufigkeit angeben, und klicken Sie dann auf **Fertig**.

      Die konfigurierten Zeitpläne werden in der Spalte „Angewandte Zeitpläne“ im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ aufgelistet.

   Sicherungspläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit den Sicherungsplänen von SnapCenter überschneiden. Sie sollten die Zeitpläne des Windows-Taskplaners und des SQL Server-Agenten nicht ändern.

7. Geben Sie auf der Seite „Benachrichtigung“ die folgenden Benachrichtigungsinformationen ein:

Für dieses Feld…	Machen Sie Folgendes…
E-Mail-Präferenz	Wählen Sie **Immer**, **Bei Fehler** oder **Bei Fehler oder Warnung** aus, um nach dem Erstellen von Sicherungsressourcengruppen, dem Anhängen von Richtlinien und dem Konfigurieren von Zeitplänen E-Mails an Empfänger zu senden. Geben Sie den SMTP-Server, die Standard-E-Mail-Betreffzeile sowie die E-Mail-Adressen „An“ und „Von“ ein.
Aus	E-Mail-Adresse
Zu	E-Mail an Adresse
Betreff	Standardmäßige E-Mail-Betreffzeile

8. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

   Sie können eine Sicherung bei Bedarf durchführen oder auf die geplante Sicherung warten.

Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für Windows-Dateisysteme auf ASA R2-Systemen

Sie sollten die Ressourcengruppe erstellen, um die Ressourcen hinzuzufügen, die sich auf ASA R2-Systemen befinden. Sie können den sekundären Schutz auch beim Erstellen der Ressourcengruppe bereitstellen.

Bevor Sie beginnen

- Sie sollten sicherstellen, dass Sie nicht sowohl ONTAP 9.x-Ressourcen als auch ASA r2-Ressourcen zur gleichen Ressourcengruppe hinzufügen.
- Sie sollten sicherstellen, dass Sie keine Datenbank mit ONTAP 9.x-Ressourcen und ASA r2-Ressourcen haben.

Informationen zu diesem Vorgang

- Der sekundäre Schutz ist nur verfügbar, wenn dem angemeldeten Benutzer die Rolle zugewiesen ist, für die die Funktion **SecondaryProtection** aktiviert ist.
- Wenn Sie den sekundären Schutz aktiviert haben, wird die Ressourcengruppe beim Erstellen der primären und sekundären Konsistenzgruppen in den Wartungsmodus versetzt. Nachdem die primäre und sekundäre Konsistenzgruppe erstellt wurden, wird der Wartungsmodus der Ressourcengruppe beendet.
- SnapCenter unterstützt keinen sekundären Schutz für eine Klonressource.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und das entsprechende Plug-In aus der Liste aus.
2. Klicken Sie auf der Seite „Ressourcen“ auf **Neue Ressourcengruppe**.
3. Führen Sie auf der Seite „Name“ die folgenden Aktionen aus:
   a. Geben Sie im Feld „Name“ einen Namen für die Ressourcengruppe ein.

Der Name der Ressourcengruppe sollte nicht länger als 250 Zeichen sein.

b. Geben Sie im Feld „Tag“ eine oder mehrere Bezeichnungen ein, um die spätere Suche nach der Ressourcengruppe zu erleichtern.

   Wenn Sie beispielsweise „HR“ als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle mit dem HR-Tag verknüpften Ressourcengruppen finden.

c. Aktivieren Sie dieses Kontrollkästchen und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

   Beispiel: benutzerdefinierter Text_Ressourcengruppenrichtlinien-Hostname oder Ressourcengruppen-Hostname. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

d. Geben Sie die Ziele der Archivprotokolldateien an, die Sie nicht sichern möchten.

   Sie sollten genau dasselbe Ziel verwenden, das in der Anwendung festgelegt wurde, gegebenenfalls einschließlich Präfix.

4. Wählen Sie auf der Seite „Ressourcen“ den Datenbank-Hostnamen aus der Dropdown-Liste **Host** aus.

   Die Ressourcen werden nur dann im Abschnitt „Verfügbare Ressourcen“ aufgeführt, wenn die Ressource erfolgreich erkannt wurde. Wenn Sie kürzlich Ressourcen hinzugefügt haben, werden diese erst in der Liste der verfügbaren Ressourcen angezeigt, nachdem Sie Ihre Ressourcenliste aktualisiert haben.

5. Wählen Sie die ASA r2-Ressourcen aus dem Abschnitt „Verfügbare Ressourcen“ aus und verschieben Sie sie in den Abschnitt „Ausgewählte Ressourcen“.
6. Wählen Sie auf der Seite „Anwendungseinstellungen“ die Sicherungsoption aus.
7. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:

   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdownliste aus.

      Sie können eine Richtlinie auch erstellen, indem Sie auf + .

      Im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ werden die ausgewählten Richtlinien aufgelistet.

   b. Klicken + in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.

   c. Konfigurieren Sie im Fenster „Zeitpläne für Richtlinie *Richtlinienname* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

      Dabei ist *Richtlinienname* der Name der von Ihnen ausgewählten Richtlinie.

      Die konfigurierten Zeitpläne werden in der Spalte „Angewandte Zeitpläne“ aufgelistet.

Sicherungspläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit den Sicherungsplänen von SnapCenter überschneiden.

8. Wenn der sekundäre Schutz für die von Ihnen ausgewählte Richtlinie aktiviert ist, wird die Seite „Sekundärer Schutz“ angezeigt und Sie müssen die folgenden Schritte ausführen:
   a. Wählen Sie den Typ der Replikationsrichtlinie aus.

      Die synchrone Replikationsrichtlinie wird nicht unterstützt.

   b. Geben Sie das Konsistenzgruppensuffix an, das Sie verwenden möchten.
   c. Wählen Sie aus den Dropdown-Menüs „Zielcluster“ und „Ziel-SVM“ den Peering-Cluster und die SVM aus, die Sie verwenden möchten.

      Das Cluster- und SVM-Peering wird von SnapCenter nicht unterstützt. Sie sollten System Manager oder ONTAP CLIs verwenden, um Cluster- und SVM-Peering durchzuführen.

Wenn die Ressourcen bereits außerhalb von SnapCenter geschützt sind, werden diese Ressourcen im Abschnitt „Sekundär geschützte Ressourcen“ angezeigt.

1. Führen Sie auf der Seite „Verifizierung“ die folgenden Schritte aus:
   a. Klicken Sie auf **Locators laden**, um die SnapMirror oder SnapVault -Volumes zu laden und die Überprüfung auf dem sekundären Speicher durchzuführen.
   b. Klicken + in der Spalte „Zeitpläne konfigurieren“, um den Überprüfungszeitplan für alle Zeitplantypen der Richtlinie zu konfigurieren.
   c. Führen Sie im Dialogfeld „Verifizierungszeitpläne hinzufügen“ (Richtlinienname) die folgenden Aktionen aus:

Wenn Sie wollen…	Machen Sie Folgendes…
Führen Sie nach der Sicherung eine Überprüfung durch	Wählen Sie **Überprüfung nach Sicherung ausführen**.
Planen Sie eine Überprüfung	Wählen Sie **Geplante Überprüfung ausführen** und wählen Sie dann den Zeitplantyp aus der Dropdownliste aus.

   d. Wählen Sie **Am sekundären Speicherort überprüfen**, um Ihre Sicherungen auf dem sekundären Speichersystem zu überprüfen.
   e. Klicken Sie auf **OK**.

      Die konfigurierten Überprüfungszeitpläne werden in der Spalte „Angewandte Zeitpläne“ aufgelistet.

2. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.

   Sie müssen außerdem die E-Mail-Adressen des Absenders und des Empfängers sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht über den an der Ressourcengruppe durchgeführten Vorgang anhängen möchten, wählen Sie **Jobbericht anhängen**.

Für die E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder über die GUI oder den PowerShell-Befehl „Set-SmSmtpServer“ angegeben haben.

3. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell-Cmdlets

Sie müssen eine Verbindung zur Storage Virtual Machine (SVM) und Anmeldeinformationen erstellen, bevor Sie PowerShell-Cmdlets zum Ausführen von Datenschutzvorgängen verwenden.

Bevor Sie beginnen

- Sie sollten die PowerShell-Umgebung für die Ausführung der PowerShell-Cmdlets vorbereitet haben.
- Sie sollten über die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ verfügen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-In-Installationen nicht im Gange sind.

  Während des Hinzufügens einer Speichersystemverbindung dürfen keine Host-Plug-In-Installationen ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbankstatus in der SnapCenter -GUI möglicherweise als „Nicht für Sicherung verfügbar“ oder „Nicht auf NetApp -Speicher“ angezeigt wird.

- Speichersystemnamen sollten eindeutig sein.

  SnapCenter unterstützt nicht mehrere Speichersysteme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Speichersystem sollte einen eindeutigen Namen und eine eindeutige Verwaltungs-LIF-IP-Adresse haben.

Schritte

1. Initiieren Sie eine PowerShell Core-Verbindungssitzung mithilfe des Cmdlets Open-SmConnection.

   Dieses Beispiel öffnet eine PowerShell-Sitzung:

   ```
   PS C:\> Open-SmConnection
   ```

2. Erstellen Sie mithilfe des Cmdlets Add-SmStorageConnection eine neue Verbindung zum Speichersystem.

   In diesem Beispiel wird eine neue Speichersystemverbindung erstellt:

   ```
   PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
   -Timeout 60
   ```

3. Erstellen Sie mithilfe des Cmdlets Add-SmCredential neue Anmeldeinformationen.

   In diesem Beispiel wird eine neue Anmeldeinformation mit dem Namen „FinanceAdmin“ mit Windows-Anmeldeinformationen erstellt:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

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" .

Sichern Sie bei Bedarf eine einzelne Ressource für Windows-Dateisysteme

Wenn sich eine Ressource nicht in einer Ressourcengruppe befindet, können Sie die Ressource bei Bedarf auf der Seite „Ressourcen“ sichern.

Informationen zu diesem Vorgang

Wenn Sie eine Ressource sichern möchten, die über eine SnapMirror -Beziehung mit einem sekundären Speicher verfügt, sollte die dem Speicherbenutzer zugewiesene Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.

Beim Sichern eines Dateisystems sichert SnapCenter keine LUNs, die auf einem Volume Mount Point (VMP) im zu sichernden Dateisystem gemountet sind.

Wenn Sie im Kontext eines Windows-Dateisystems arbeiten, sichern Sie keine Datenbankdateien. Dadurch entsteht eine inkonsistente Sicherung und es kann beim Wiederherstellen zu Datenverlust kommen. Zum Schutz von Datenbankdateien müssen Sie das entsprechende SnapCenter -Plug-in für die Datenbank verwenden (z. B. SnapCenter -Plug-in für Microsoft SQL Server oder SnapCenter -Plug-in für Microsoft Exchange Server).

SnapCenter -Benutzeroberfläche

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“ den Ressourcentyp „Dateisystem“ und dann die Ressource aus, die Sie sichern möchten.
3. Wenn der Assistent „Dateisystem – Schützen“ nicht automatisch startet, klicken Sie auf **Schützen**, um den Assistenten zu starten.

   Geben Sie die Schutzeinstellungen an, wie in den Aufgaben zum Erstellen von Ressourcengruppen beschrieben.

4. Optional: Geben Sie auf der Ressourcenseite des Assistenten ein benutzerdefiniertes Namensformat für den Snapshot ein.

   Beispiel: customtext_resourcegroup_policy_hostname oder resourcegroup_hostname. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

5. Führen Sie auf der Seite „Richtlinien“ die folgenden Aufgaben aus:

   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdownliste aus.

      Sie können eine beliebige vorhandene Richtlinie auswählen und dann auf **Details** klicken, um festzustellen, ob Sie diese Richtlinie verwenden können.

      Wenn keine vorhandene Richtlinie Ihren Anforderungen entspricht, können Sie eine vorhandene Richtlinie kopieren und ändern oder eine neue Richtlinie erstellen, indem Sie auf , um den Richtlinienassistenten zu starten. Wenn keine vorhandene Richtlinie Ihren Anforderungen entspricht, können Sie eine vorhandene Richtlinie kopieren und ändern oder eine neue Richtlinie erstellen, indem Sie auf , um den Richtlinienassistenten zu starten.

      Die ausgewählten Richtlinien werden in der Spalte „Richtlinie“ im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ aufgelistet.

   b. Klicken Sie im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ auf in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie den Zeitplan konfigurieren möchten.

   c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtlinienname* hinzufügen“ den Zeitplan, indem Sie das Startdatum, das Ablaufdatum und die Häufigkeit angeben, und klicken Sie dann auf **Fertig**.

      Die konfigurierten Zeitpläne werden in der Spalte „Angewandte Zeitpläne“ im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ aufgelistet.

   "Geplante Vorgänge können fehlschlagen"

6. Führen Sie auf der Seite „Benachrichtigung“ die folgenden Aufgaben aus:

Für dieses Feld…	Machen Sie Folgendes…
E-Mail-Präferenz	Wählen Sie **Immer**, **Bei Fehler** oder **Bei Fehler oder Warnung** aus, um nach dem Erstellen von Sicherungsressourcengruppen, dem Anhängen von Richtlinien und dem Konfigurieren von Zeitplänen E-Mails an Empfänger zu senden. Geben Sie die SMTP-Serverinformationen, die Standard-Betreffzeile der E-Mail sowie die E-Mail-Adressen „An“ und „Von“ ein.
Aus	E-Mail-Adresse
Zu	E-Mail an Adresse
Betreff	Standardmäßige E-Mail-Betreffzeile

7. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

   Die Seite „Datenbanktopologie“ wird angezeigt.

8. Klicken Sie auf **Jetzt sichern**.
9. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:
   a. Wenn Sie mehrere Richtlinien auf die Ressource angewendet haben, wählen Sie aus der Dropdownliste „Richtlinie“ die Richtlinie aus, die Sie für die Sicherung verwenden möchten.

      Wenn die für die On-Demand-Sicherung ausgewählte Richtlinie mit einem Sicherungszeitplan verknüpft ist, werden die On-Demand-Sicherungen basierend auf den für den Zeitplantyp angegebenen Aufbewahrungseinstellungen aufbewahrt.

   b. Klicken Sie auf **Sichern**.
10. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.

PowerShell-Cmdlets

Schritte

1. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

   ```
   Open-smconnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
   ```

   Die Eingabeaufforderung für Benutzername und Kennwort wird angezeigt.

2. Erstellen Sie eine Sicherungsrichtlinie mithilfe des Cmdlets Add-SmPolicy.

   In diesem Beispiel wird eine neue Sicherungsrichtlinie mit dem SQL-Sicherungstyp „FullBackup“ erstellt:

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

In diesem Beispiel wird eine neue Sicherungsrichtlinie mit dem Sicherungstyp „CrashConsistent“ für das Windows-Dateisystem erstellt:

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

3. Ermitteln Sie Hostressourcen mithilfe des Cmdlets „Get-SmResources“.

   Dieses Beispiel ermittelt die Ressourcen für das Microsoft SQL-Plug-In auf dem angegebenen Host:

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCSQL
```

   Dieses Beispiel ermittelt die Ressourcen für Windows-Dateisysteme auf dem angegebenen Host:

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

4. Fügen Sie SnapCenter mithilfe des Cmdlets Add-SmResourceGroup eine neue Ressourcengruppe hinzu.

   In diesem Beispiel wird eine neue SQL-Datenbank-Sicherungsressourcengruppe mit der angegebenen Richtlinie und den angegebenen Ressourcen erstellt:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource
-Resources @{"Host"="visef6.org.com";
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}
-Policies "BackupPolicy"
```

   In diesem Beispiel wird eine neue Ressourcengruppe zur Sicherung des Windows-Dateisystems mit der angegebenen Richtlinie und den angegebenen Ressourcen erstellt:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

5. Starten Sie einen neuen Sicherungsauftrag mithilfe des Cmdlets New-SmBackup.

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

6. Zeigen Sie den Status des Sicherungsauftrags mithilfe des Cmdlets Get-SmBackupReport an.

   In diesem Beispiel wird ein Job-Zusammenfassungsbericht aller Jobs angezeigt, die am angegebenen Datum ausgeführt wurden:

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

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" .

Sichern von Ressourcengruppen für Windows-Dateisysteme

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host oder Cluster. Ein Sicherungsvorgang für die Ressourcengruppe wird für alle in der Ressourcengruppe definierten Ressourcen ausgeführt. Sie können eine Ressourcengruppe bei Bedarf von der Seite „Ressourcen“ aus sichern. Wenn einer Ressourcengruppe eine Richtlinie zugeordnet und ein Zeitplan konfiguriert ist, werden die Sicherungen automatisch gemäß dem Zeitplan durchgeführt.

Bevor Sie beginnen

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Wenn Sie eine Ressource mit einer SnapMirror -Beziehung zum sekundären Speicher sichern möchten, sollte die dem Speicherbenutzer zugewiesene Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.
- Wenn eine Ressourcengruppe über mehrere Datenbanken von verschiedenen Hosts verfügt, kann es sein, dass der Sicherungsvorgang auf einigen Hosts aufgrund von Netzwerkproblemen verspätet ausgelöst wird. Sie sollten den Wert von MaxRetryForUninitializedHosts in web.config mithilfe des PowerShell-Cmdlets Set-SmConfigSettings konfigurieren.

Beim Sichern eines Dateisystems sichert SnapCenter keine LUNs, die auf einem Volume Mount Point (VMP) im zu sichernden Dateisystem gemountet sind.

Wenn Sie im Kontext eines Windows-Dateisystems arbeiten, sichern Sie keine Datenbankdateien. Dadurch entsteht eine inkonsistente Sicherung und es kann beim Wiederherstellen zu Datenverlust kommen. Zum Schutz von Datenbankdateien müssen Sie das entsprechende SnapCenter -Plug-in für die Datenbank verwenden (z. B. SnapCenter -Plug-in für Microsoft SQL Server oder SnapCenter -Plug-in für Microsoft Exchange Server).

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.

   Sie können die Ressourcengruppe suchen, indem Sie entweder den Namen der Ressourcengruppe in das Suchfeld eingeben oder auf und wählen Sie das Tag aus. Sie können dann auf , um den Filterbereich zu schließen.
3. Wählen Sie auf der Seite „Ressourcengruppen“ die Ressourcengruppe aus, die Sie sichern möchten, und klicken Sie dann auf **Jetzt sichern**.

   Wenn Sie beim SnapCenter Plug-in für Oracle Database über eine föderierte Ressourcengruppe mit zwei Datenbanken verfügen und eine der Datenbanken eine Datendatei auf einem Nicht- NetApp -Speicher hat, wird der Sicherungsvorgang abgebrochen, obwohl sich die andere Datenbank auf einem NetApp -Speicher befindet.
4. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:
   a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet haben, wählen Sie aus der Dropdownliste **Richtlinie** die Richtlinie aus, die Sie für die Sicherung verwenden möchten.

      Wenn die für die On-Demand-Sicherung ausgewählte Richtlinie mit einem Sicherungszeitplan verknüpft ist, werden die On-Demand-Sicherungen basierend auf den für den Zeitplantyp angegebenen Aufbewahrungseinstellungen aufbewahrt.
   b. Klicken Sie auf **Sichern**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.
   - In MetroCluster -Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Schutzbeziehung erkennen.

     "SnapMirror oder SnapVault -Beziehung kann nach MetroCluster Failover nicht erkannt werden"
   - Wenn Sie Anwendungsdaten auf VMDKs sichern und die Java-Heap-Größe für das SnapCenter Plug-in for VMware vSphere nicht groß genug ist, schlägt die Sicherung möglicherweise fehl. Um die Größe des Java-Heaps zu erhöhen, suchen Sie die Skriptdatei `/opt/netapp/init_scripts/scvservice` . In diesem Skript `do_start method` Der Befehl startet den SnapCenter VMware-Plug-In-Dienst. Aktualisieren Sie diesen Befehl wie folgt: `Java -jar -Xmx8192M -Xms4096M` .

Überwachen von Sicherungsvorgängen

Sie können den Fortschritt verschiedener Sicherungsvorgänge mithilfe der SnapCenterJobs-Seite überwachen. Möglicherweise möchten Sie den Fortschritt überprüfen, um festzustellen, wann der Vorgang abgeschlossen ist oder ob ein Problem vorliegt.

Informationen zu diesem Vorgang

Die folgenden Symbole werden auf der Seite „Jobs“ angezeigt und zeigen den entsprechenden Status der Vorgänge an:

- Im Gange

- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In der Warteschlange
- Abgesagt

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite „Überwachen“ auf **Jobs**.
3. Führen Sie auf der Seite „Jobs“ die folgenden Schritte aus:
   a. Klicken um die Liste so zu filtern, dass nur Sicherungsvorgänge aufgelistet werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdownliste **Typ** die Option **Backup** aus.
   d. Wählen Sie aus der Dropdown-Liste **Status** den Sicherungsstatus aus.
   e. Klicken Sie auf **Übernehmen**, um die erfolgreich abgeschlossenen Vorgänge anzuzeigen.
4. Wählen Sie einen Sicherungsauftrag aus und klicken Sie dann auf **Details**, um die Auftragsdetails anzuzeigen.

   Obwohl der Status des Sicherungsauftrags angezeigt wird Wenn Sie auf die Auftragsdetails klicken, sehen Sie möglicherweise, dass einige der untergeordneten Aufgaben des Sicherungsvorgangs noch ausgeführt werden oder mit Warnzeichen markiert sind.

5. Klicken Sie auf der Seite „Auftragsdetails“ auf **Protokolle anzeigen**.

   Die Schaltfläche **Protokolle anzeigen** zeigt die detaillierten Protokolle für den ausgewählten Vorgang an.

Überwachen von Vorgängen im Aktivitätsbereich

Im Aktivitätsbereich werden die fünf zuletzt ausgeführten Vorgänge angezeigt. Im Aktivitätsbereich wird auch angezeigt, wann der Vorgang gestartet wurde und welchen Status er hat.

Im Aktivitätsbereich werden Informationen zu Sicherungs-, Wiederherstellungs-, Klon- und geplanten Sicherungsvorgängen angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Klicken im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen.

   Wenn Sie auf einen der Vorgänge klicken, werden die Vorgangsdetails auf der Seite **Auftragsdetails** aufgelistet.

Abbrechen von Sicherungsvorgängen

Sie können Sicherungsvorgänge in der Warteschlange abbrechen.

Was Sie brauchen

- Sie müssen als SnapCenter -Administrator oder Auftragseigentümer angemeldet sein, um Vorgänge abzubrechen.
- Sie können einen Sicherungsvorgang entweder auf der Seite **Überwachen** oder im Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Sicherungsvorgang nicht abbrechen.
- Sie können die Sicherungsvorgänge über die SnapCenter -GUI, PowerShell-Cmdlets oder CLI-Befehle abbrechen.
- Die Schaltfläche **Auftrag abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer\Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Sicherungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitorseite	a. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. b. Wählen Sie den Vorgang aus und klicken Sie dann auf **Auftrag abbrechen**.
Aktivitätsbereich	a. Klicken Sie nach dem Starten des Sicherungsvorgangs auf * * im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen. b. Wählen Sie den Vorgang aus. c. Klicken Sie auf der Seite „Auftragsdetails“ auf **Auftrag abbrechen**.

Der Vorgang wird abgebrochen und die Ressource in den vorherigen Zustand zurückversetzt.

Anzeigen zugehöriger Sicherungen und Klone auf der Seite „Topologie“

Wenn Sie die Sicherung oder das Klonen einer Ressource vorbereiten, können Sie eine grafische Darstellung aller Sicherungen und Klone auf dem primären und sekundären Speicher anzeigen. Auf der Seite „Topologie“ können Sie alle Sicherungen und Klone sehen, die für die ausgewählte Ressource oder Ressourcengruppe verfügbar sind. Sie können die Details dieser Sicherungen und Klone anzeigen und sie dann auswählen, um

Datenschutzvorgänge durchzuführen.

Informationen zu diesem Vorgang

Sie können die folgenden Symbole in der Ansicht „Kopien verwalten“ überprüfen, um festzustellen, ob die Sicherungen und Klone auf dem primären oder sekundären Speicher verfügbar sind (Spiegelkopien oder Tresorkopien).

-  zeigt die Anzahl der Backups und Klone an, die auf dem primären Speicher verfügbar sind.
-  zeigt die Anzahl der Backups und Klone an, die mithilfe der SnapMirror -Technologie auf dem sekundären Speicher gespiegelt werden.

  Klone einer Sicherung eines versionsflexiblen Spiegels auf einem Volume vom Typ „Mirror-Vault“ werden in der Topologieansicht angezeigt, die Anzahl der Spiegelsicherungen in der Topologieansicht umfasst jedoch nicht die versionsflexible Sicherung.

-  zeigt die Anzahl der Backups und Klone an, die mithilfe der SnapVault -Technologie auf dem sekundären Speicher repliziert werden.
  - Die angezeigte Anzahl der Backups umfasst die aus dem sekundären Speicher gelöschten Backups. Wenn Sie beispielsweise 6 Sicherungen mit einer Richtlinie zum Aufbewahren von nur 4 Sicherungen erstellt haben, wird die Anzahl der angezeigten Sicherungen mit 6 angegeben.

Klone einer Sicherung eines versionsflexiblen Spiegels auf einem Volume vom Typ „Mirror-Vault“ werden in der Topologieansicht angezeigt, die Anzahl der Spiegelsicherungen in der Topologieansicht umfasst jedoch nicht die versionsflexible Sicherung.

Wenn Sie eine sekundäre Beziehung als SnapMirror Active Sync haben (ursprünglich veröffentlicht als SnapMirror Business Continuity [SM-BC]), können Sie die folgenden zusätzlichen Symbole sehen:

-  Die Replikationssite ist aktiv.
-  Die Replikationssite ist ausgefallen.
-  Die sekundäre Spiegel- oder Tresorbeziehung wurde nicht wiederhergestellt.

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 entweder aus der Ressourcendetailansicht oder aus der Ressourcengruppendetailansicht aus.

   Wenn die Ressource geschützt ist, wird die Topologieseite der ausgewählten Ressource angezeigt.

4. Überprüfen Sie die Karte „Zusammenfassung“, um eine Übersicht über die Anzahl der auf dem primären und sekundären Speicher verfügbaren Sicherungen und Klone anzuzeigen.

   Im Abschnitt „Zusammenfassungskarte“ wird die Gesamtzahl der Sicherungen und Klone angezeigt. Nur für Oracle-Datenbanken wird im Abschnitt „Zusammenfassungskarte“ auch die Gesamtzahl der Protokollsicherungen angezeigt.

   Durch Klicken auf die Schaltfläche **Aktualisieren** wird eine Abfrage des Speichers gestartet, um eine genaue Anzahl anzuzeigen.

   Wenn eine SnapLock -fähige Sicherung durchgeführt wird, wird durch Klicken auf die Schaltfläche **Aktualisieren** die von ONTAP abgerufene Ablaufzeit des primären und sekundären SnapLock aktualisiert. Ein wöchentlicher Zeitplan aktualisiert auch die von ONTAP abgerufene Ablaufzeit des primären und sekundären SnapLock .

   Wenn die Anwendungsressource auf mehrere Volumes verteilt ist, entspricht die SnapLock -Ablaufzeit für die Sicherung der längsten SnapLock -Ablaufzeit, die für einen Snapshot in einem Volume festgelegt ist. Die längste SnapLock -Ablaufzeit wird von ONTAP abgerufen.

   Bei der aktiven Synchronisierung von SnapMirror wird durch Klicken auf die Schaltfläche **Aktualisieren** das SnapCenter -Sicherungsinventar aktualisiert, indem ONTAP sowohl nach primären als auch nach Replikationsstandorten abgefragt wird. Ein wöchentlicher Zeitplan führt diese Aktivität auch für alle Datenbanken aus, die eine aktive Synchronisierungsbeziehung mit SnapMirror enthalten.

   - Für SnapMirror Active Sync und nur für ONTAP 9.14.1 sollten Async Mirror- oder Async MirrorVault-Beziehungen zum neuen primären Ziel nach dem Failover manuell konfiguriert werden. Ab ONTAP 9.15.1 wird Async Mirror oder Async MirrorVault automatisch auf das neue primäre Ziel konfiguriert.
   - Nach dem Failover sollte ein Backup für SnapCenter erstellt werden, um über das Failover informiert zu sein. Sie können erst auf **Aktualisieren** klicken, nachdem eine Sicherung erstellt wurde.

5. Klicken Sie in der Ansicht „Kopien verwalten“ auf **Backups** oder **Klone** vom primären oder sekundären Speicher, um Details zu einem Backup oder Klon anzuzeigen.

   Die Details der Backups und Klone werden in einem Tabellenformat angezeigt.

6. Wählen Sie die Sicherung aus der Tabelle aus und klicken Sie dann auf die Datenschutzsymbole, um Wiederherstellungs-, Klon-, Umbenennungs- und Löschvorgänge durchzuführen.

   Sie können Sicherungen, die sich auf dem sekundären Speichersystem befinden, weder umbenennen noch löschen.

7. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon aus der Tabelle aus und klicken Sie auf , um den Klon zu löschen.

Beispiel für Backups und Klone auf dem Primärspeicher

Bereinigen der Anzahl sekundärer Sicherungen mithilfe von PowerShell-Cmdlets

Sie können das Cmdlet „Remove-SmBackup“ verwenden, um die Sicherungsanzahl für sekundäre Sicherungen ohne Snapshot zu bereinigen. Sie können dieses Cmdlet verwenden, wenn die Gesamtzahl der in der Topologie „Kopien verwalten“ angezeigten Snapshots nicht mit der Snapshot-Aufbewahrungseinstellung des sekundären Speichers übereinstimmt.

Sie müssen die PowerShell-Umgebung vorbereitet haben, um die PowerShell-Cmdlets auszuführen.

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" .

Schritte

1. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Bereinigen Sie die Anzahl sekundärer Sicherungen mit dem Parameter -CleanupSecondaryBackups.

   In diesem Beispiel wird die Sicherungsanzahl für sekundäre Sicherungen ohne Snapshots bereinigt:

```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

Wiederherstellen von Windows-Dateisystemen

Wiederherstellen von Windows-Dateisystemsicherungen

Sie können SnapCenter verwenden, um Dateisystemsicherungen wiederherzustellen. Die

Wiederherstellung des Dateisystems ist ein mehrphasiger Prozess, bei dem alle Daten aus einer angegebenen Sicherung an den ursprünglichen Speicherort des Dateisystems kopiert werden.

Bevor Sie beginnen

- Sie müssen das Dateisystem gesichert haben.
- Wenn für ein Dateisystem gerade ein geplanter Vorgang ausgeführt wird, beispielsweise ein Sicherungsvorgang, muss dieser Vorgang abgebrochen werden, bevor Sie einen Wiederherstellungsvorgang starten können.
- Sie können eine Dateisystemsicherung nur am ursprünglichen Speicherort wiederherstellen, nicht auf einem alternativen Pfad.

  Sie können aus einer Sicherung keine einzelne Datei wiederherstellen, da das wiederhergestellte Dateisystem alle Daten am ursprünglichen Speicherort des Dateisystems überschreibt. Um eine einzelne Datei aus einer Dateisystemsicherung wiederherzustellen, müssen Sie die Sicherung klonen und auf die Datei im Klon zugreifen.

- Sie können ein System- oder Startvolume nicht wiederherstellen.
- SnapCenter kann Dateisysteme in einem Windows-Cluster wiederherstellen, ohne die Clustergruppe offline zu nehmen.

Informationen zu diesem Vorgang

- Der SCRIPTS_PATH wird mithilfe des Schlüssels „PredefinedWindowsScriptsDirectory“ definiert, der sich in der Datei „SMCoreServiceHost.exe.Config“ des Plug-In-Hosts befindet.

  Bei Bedarf können Sie diesen Pfad ändern und den SMcore-Dienst neu starten. Aus Sicherheitsgründen wird empfohlen, den Standardpfad zu verwenden.

  Der Wert des Schlüssels kann von Swagger über die API angezeigt werden: API /4.7/configsettings

  Sie können die GET-API verwenden, um den Wert des Schlüssels anzuzeigen. SET-API wird nicht unterstützt.

- Für den Wiederherstellungsvorgang mit SnapMirror Active Sync müssen Sie die Sicherung vom primären Speicherort auswählen.
- Bei ONTAP 9.12.1 und niedrigeren Versionen erben die im Rahmen der Wiederherstellung aus den SnapLock Vault-Snapshots erstellten Klone die Ablaufzeit von SnapLock Vault. Der Speicheradministrator sollte die Klone nach Ablauf des SnapLock manuell bereinigen.

SnapCenter -Benutzeroberfläche

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Um die Liste der Ressourcen zu filtern, wählen Sie die Optionen „Dateisystem“ und „Ressourcengruppe“ aus.
3. Wählen Sie eine Ressourcengruppe aus der Liste aus und klicken Sie dann auf **Wiederherstellen**.
4. Wählen Sie auf der Seite „Sicherungen“ aus, ob Sie von primären oder sekundären Speichersystemen wiederherstellen möchten, und wählen Sie dann eine wiederherzustellende Sicherung aus.
5. Wählen Sie Ihre Optionen im Wiederherstellungsassistenten aus.
6. Sie können den Pfad und die Argumente des Präskripts oder Postskripts eingeben, das SnapCenter vor bzw. nach dem Wiederherstellungsvorgang ausführen soll.

   Sie können beispielsweise ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnungen zu automatisieren, Protokolle zu senden usw.

   Der Prescripts- oder Postscripts-Pfad sollte keine Laufwerke oder Freigaben enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

7. Wählen Sie auf der Benachrichtigungsseite eine der folgenden Optionen aus:

Für dieses Feld…	Machen Sie Folgendes…
Protokollieren Sie SnapCenter Serverereignisse im Syslog des Speichersystems	Wählen Sie diese Option, um SnapCenter Server-Ereignisse im Syslog des Speichersystems zu protokollieren.
Senden Sie eine AutoSupport -Benachrichtigung für fehlgeschlagene Vorgänge an das Speichersystem	Wählen Sie diese Option, um Informationen zu fehlgeschlagenen Vorgängen mithilfe von AutoSupport an NetApp zu senden.
E-Mail-Präferenz	Wählen Sie **Immer**, **Bei Fehler** oder **Bei Fehler oder Warnung** aus, um nach der Wiederherstellung von Sicherungen E-Mail-Nachrichten an die Empfänger zu senden. Geben Sie den SMTP-Server, die Standard-Betreffzeile der E-Mail sowie die E-Mail-Adressen „An“ und „Von“ ein.

8. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
9. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.

Wenn das wiederhergestellte Dateisystem eine Datenbank enthält, müssen Sie auch die Datenbank wiederherstellen. Wenn Sie die Datenbank nicht wiederherstellen, befindet sich Ihre Datenbank möglicherweise in einem ungültigen Zustand. Informationen zum Wiederherstellen von Datenbanken finden Sie im Datenschutzhandbuch für die jeweilige Datenbank.

PowerShell-Cmdlets

Schritte

1. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
PS C:\> Open-Smconnection
```

2. Rufen Sie die Informationen zu den Sicherungen ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets „Get-SmBackup“ und „Get-SmBackupReport“ verwenden.

   Dieses Beispiel zeigt Informationen zu allen verfügbaren Backups an:

```
PS C:\> Get-SmBackup

BackupId                      BackupName
BackupTime                    BackupType
--------                      ----------
----------                    ----------
  1               Payroll Dataset_vise-f6_08... 8/4/2015    11:02:32
AM                 Full Backup
  2               Payroll Dataset_vise-f6_08... 8/4/2015    11:23:17
AM
```

   Dieses Beispiel zeigt detaillierte Informationen zum Backup vom 29. Januar 2015 bis 3. Februar 2015:

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"2/3/2015"

   SmBackupId           : 113
   SmJobId              : 2032
   StartDateTime        : 2/2/2015 6:57:03 AM
   EndDateTime          : 2/2/2015 6:57:11 AM
   Duration             : 00:00:07.3060000
   CreatedDateTime      : 2/2/2015 6:57:23 AM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_06.57.08
   VerificationStatus   : NotVerified

   SmBackupId           : 114
   SmJobId              : 2183
   StartDateTime        : 2/2/2015 1:02:41 PM
   EndDateTime          : 2/2/2015 1:02:38 PM
   Duration             : -00:00:03.2300000
   CreatedDateTime      : 2/2/2015 1:02:53 PM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_13.02.45
   VerificationStatus   : NotVerified
```

3. Stellen Sie Daten aus der Sicherung mithilfe des Cmdlets Restore-SmBackup wieder her.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

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" .

Wiederherstellen von Ressourcen mithilfe von PowerShell-Cmdlets

Das Wiederherstellen einer Ressourcensicherung umfasst das Einleiten einer Verbindungssitzung mit dem SnapCenter -Server, das Auflisten der Sicherungen und Abrufen von Sicherungsinformationen sowie das Wiederherstellen einer Sicherung.

Sie müssen die PowerShell-Umgebung vorbereitet haben, um die PowerShell-Cmdlets auszuführen.

Schritte

1. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
PS C:\> Open-Smconnection
```

2. Rufen Sie die Informationen zu den Sicherungen ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets „Get-SmBackup“ und „Get-SmBackupReport“ verwenden.

   Dieses Beispiel zeigt Informationen zu allen verfügbaren Backups an:

```
PS C:\> Get-SmBackup

BackupId                      BackupName                    BackupTime
BackupType
--------                      ----------                    ----------
----------
  1               Payroll Dataset_vise-f6_08... 8/4/2015    11:02:32 AM
Full Backup
  2               Payroll Dataset_vise-f6_08... 8/4/2015    11:23:17 AM
```

   Dieses Beispiel zeigt detaillierte Informationen zum Backup vom 29. Januar 2015 bis 3. Februar 2015:

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"2/3/2015"

   SmBackupId           : 113
   SmJobId              : 2032
   StartDateTime        : 2/2/2015 6:57:03 AM
   EndDateTime          : 2/2/2015 6:57:11 AM
   Duration             : 00:00:07.3060000
   CreatedDateTime      : 2/2/2015 6:57:23 AM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_06.57.08
   VerificationStatus   : NotVerified

   SmBackupId           : 114
   SmJobId              : 2183
   StartDateTime        : 2/2/2015 1:02:41 PM
   EndDateTime          : 2/2/2015 1:02:38 PM
   Duration             : -00:00:03.2300000
   CreatedDateTime      : 2/2/2015 1:02:53 PM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_13.02.45
   VerificationStatus   : NotVerified
```

3. Stellen Sie Daten aus der Sicherung mithilfe des Cmdlets Restore-SmBackup wieder her.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

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" .

Überwachen von Wiederherstellungsvorgängen

Sie können den Fortschritt verschiedener SnapCenter -Wiederherstellungsvorgänge mithilfe der Seite „Jobs“ überwachen. Möglicherweise möchten Sie den Fortschritt eines Vorgangs überprüfen, um festzustellen, wann er abgeschlossen ist oder ob ein Problem vorliegt.

Informationen zu diesem Vorgang

Zustände nach der Wiederherstellung beschreiben den Zustand der Ressource nach einem Wiederherstellungsvorgang und alle weiteren Wiederherstellungsaktionen, die Sie durchführen können.

Die folgenden Symbole werden auf der Seite „Jobs“ angezeigt und geben den Status des Vorgangs an:

- Im Gange
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In der Warteschlange
- Abgesagt

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Überwachen** auf **Jobs**.
3. Führen Sie auf der Seite **Jobs** die folgenden Schritte aus:
   a. Klicken um die Liste so zu filtern, dass nur Wiederherstellungsvorgänge aufgelistet werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdownliste **Typ** die Option **Wiederherstellen** aus.
   d. Wählen Sie aus der Dropdown-Liste **Status** den Wiederherstellungsstatus aus.
   e. Klicken Sie auf **Übernehmen**, um die erfolgreich abgeschlossenen Vorgänge anzuzeigen.
4. Wählen Sie den Wiederherstellungsauftrag aus und klicken Sie dann auf **Details**, um die Auftragsdetails anzuzeigen.
5. Klicken Sie auf der Seite **Auftragsdetails** auf **Protokolle anzeigen**.

   Die Schaltfläche **Protokolle anzeigen** zeigt die detaillierten Protokolle für den ausgewählten Vorgang an.

Abbrechen von Wiederherstellungsvorgängen

Sie können in der Warteschlange befindliche Wiederherstellungsaufträge abbrechen.

Sie sollten als SnapCenter -Administrator oder Auftragseigentümer angemeldet sein, um Wiederherstellungsvorgänge abzubrechen.

Informationen zu diesem Vorgang

- Sie können einen in die Warteschlange gestellten Wiederherstellungsvorgang entweder auf der Seite **Überwachen** oder im Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Wiederherstellungsvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell-Cmdlets oder CLI-Befehle verwenden, um die in die Warteschlange gestellten Wiederherstellungsvorgänge abzubrechen.
- Die Schaltfläche **Auftrag abbrechen** ist für Wiederherstellungsvorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer\Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Wiederherstellungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritt

Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitorseite	1. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. 2. Wählen Sie den Auftrag aus und klicken Sie auf **Auftrag abbrechen**.
Aktivitätsbereich	1. Klicken Sie nach dem Starten des Wiederherstellungsvorgangs auf im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen. 2. Wählen Sie den Vorgang aus. 3. Klicken Sie auf der Seite „Auftragsdetails“ auf **Auftrag abbrechen**.

Klonen Sie Windows-Dateisysteme

Klonen aus einer Windows-Dateisystemsicherung

Sie können SnapCenter verwenden, um eine Windows-Dateisystemsicherung zu klonen. Wenn Sie eine Kopie einer einzelnen Datei wünschen, die versehentlich gelöscht oder geändert wurde, können Sie eine Sicherungskopie klonen und im Klon auf diese Datei zugreifen.

Bevor Sie beginnen

- Sie sollten sich auf den Datenschutz vorbereitet haben, indem Sie Aufgaben wie das Hinzufügen von Hosts, das Identifizieren von Ressourcen und das Erstellen von Verbindungen zu virtuellen Speichermaschinen (SVM) erledigt haben.
- Sie sollten über eine Sicherungskopie des Dateisystems verfügen.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) enthalten sind.
- Sie können eine Ressourcengruppe nicht klonen. Sie können nur einzelne Dateisystemsicherungen klonen.
- Wenn sich eine Sicherung auf einer virtuellen Maschine mit einer VMDK-Festplatte befindet, kann SnapCenter die Sicherung nicht auf einen physischen Server klonen.
- Wenn Sie einen Windows-Cluster klonen (z. B. eine freigegebene LUN oder eine Cluster Shared Volume (CSV)-LUN), wird der Klon als dedizierte LUN auf dem von Ihnen angegebenen Host gespeichert.
- Bei einem Klonvorgang darf das Stammverzeichnis des Volume-Mount-Punkts kein freigegebenes Verzeichnis sein.
- Sie können keinen Klon auf einem Knoten erstellen, der nicht der Home-Knoten für das Aggregat ist.
- Sie können für Windows-Dateisysteme keine wiederkehrenden Klonvorgänge (Klon-Lebenszyklus) planen. Sie können eine Sicherung nur bei Bedarf klonen.
- Wenn Sie eine LUN, die einen Klon enthält, auf ein neues Volume verschieben, kann SnapCenter den Klon nicht mehr unterstützen. Beispielsweise können Sie SnapCenter nicht zum Löschen dieses Klons

verwenden.

- Sie können nicht über Umgebungen hinweg klonen. Beispielsweise das Klonen von einer physischen Festplatte auf eine virtuelle Festplatte oder umgekehrt.

Informationen zu diesem Vorgang

- Der SCRIPTS_PATH wird mithilfe des Schlüssels „PredefinedWindowsScriptsDirectory“ definiert, der sich in der Datei „SMCoreServiceHost.exe.Config“ des Plug-In-Hosts befindet.

  Bei Bedarf können Sie diesen Pfad ändern und den SMcore-Dienst neu starten. Aus Sicherheitsgründen wird empfohlen, den Standardpfad zu verwenden.

  Der Wert des Schlüssels kann von Swagger über die API angezeigt werden: API /4.7/configsettings

  Sie können die GET-API verwenden, um den Wert des Schlüssels anzuzeigen. SET-API wird nicht unterstützt.

- Bei ONTAP 9.12.1 und niedrigeren Versionen erben die im Rahmen der Wiederherstellung aus den SnapLock Vault-Snapshots erstellten Klone die Ablaufzeit von SnapLock Vault. Der Speicheradministrator sollte die Klone nach Ablauf des SnapLock manuell bereinigen.

SnapCenter -Benutzeroberfläche

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“ **Dateisysteme** aus der Liste aus.
3. Wählen Sie den Host aus.

   Die Topologieansicht wird automatisch angezeigt, wenn die Ressource geschützt ist.

4. Wählen Sie aus der Ressourcenliste das Backup aus, das Sie klonen möchten, und klicken Sie dann auf das Klonsymbol.
5. Gehen Sie auf der Seite „Optionen“ wie folgt vor:

Für dieses Feld…	Machen Sie Folgendes…
Server klonen	Wählen Sie den Host aus, auf dem der Klon erstellt werden soll.
„`Mountpunkt automatisch zuweisen`“ oder „`Volume-Mountpunkt automatisch unter Pfad zuweisen`“	Wählen Sie, ob automatisch ein Bereitstellungspunkt oder ein Volume-Bereitstellungspunkt unter einem Pfad zugewiesen werden soll. Automatische Zuweisung des Volume-Mount-Punkts unter Pfad: Der Mount-Punkt unter einem Pfad ermöglicht Ihnen, ein bestimmtes Verzeichnis anzugeben, in dem die Mount-Punkte erstellt werden. Bevor Sie diese Option wählen, müssen Sie sicherstellen, dass das Verzeichnis leer ist. Wenn sich im Verzeichnis eine Sicherung befindet, befindet sich die Sicherung nach dem Mount-Vorgang in einem ungültigen Zustand.
Archivspeicherort	Wählen Sie einen Archivspeicherort, wenn Sie eine sekundäre Sicherung klonen.

6. Geben Sie auf der Skriptseite alle Präskripte oder Postskripte an, die Sie ausführen möchten.

   Der Prescripts- oder Postscripts-Pfad sollte keine Laufwerke oder Freigaben enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

7. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
8. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.

PowerShell-Cmdlets

Schritte

1. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
Open-SmConnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

2. Listen Sie die Sicherungen auf, die mit dem Cmdlet Get-SmBackup oder Get-SmResourceGroup geklont werden können.

   Dieses Beispiel zeigt Informationen zu allen verfügbaren Backups an:

```
C:\PS>PS C:\> Get-SmBackup

BackupId   BackupName                    BackupTime   BackupType
--------   ----------                    ----------   ----------
1          Payroll Dataset_vise-f6_08...  8/4/2015     Full Backup
                                          11:02:32 AM

2          Payroll Dataset_vise-f6_08...  8/4/2015
                                          11:23:17 AM
```

   In diesem Beispiel werden Informationen zu einer angegebenen Ressourcengruppe, ihren Ressourcen und zugehörigen Richtlinien angezeigt:

```
PS C:\> Get-SmResourceGroup -ListResources –ListPolicies

Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMaping : {}
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
```

```
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
ApplySnapvaultUpdate : False
ApplyRetention : False
RetentionCount : 0
RetentionDays : 0
ApplySnapMirrorUpdate : False
SnapVaultLabel :
MirrorVaultUpdateRetryCount : 7
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :
PreScriptArguments :
PostScriptPath :
PostScriptArguments :
ScriptTimeOut : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCoreContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
Type :
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :
```

```
SQLInstance : clab-a13-13
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
SqlDbFileGroups : {}
SqlDbLogFiles : {}
AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
```

3. Starten Sie einen Klonvorgang aus einer vorhandenen Sicherung mithilfe des Cmdlets New-SmClone.

   Dieses Beispiel erstellt einen Klon aus einem angegebenen Backup mit allen Protokollen:

```
PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\sqlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

   In diesem Beispiel wird ein Klon einer angegebenen Microsoft SQL Server-Instanz erstellt:

```
PS C:\> New-SmClone
-BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"
```

4. Zeigen Sie den Status des Klonauftrags mithilfe des Cmdlets Get-SmCloneReport an.

   Dieses Beispiel zeigt einen Klonbericht für die angegebene Job-ID an:

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
                   Sally_DRAPER}
```

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" .

Überwachen von Klonvorgängen

Sie können den Fortschritt der SnapCenter -Klonvorgänge auf der Seite „Jobs“ überwachen. Möglicherweise möchten Sie den Fortschritt eines Vorgangs überprüfen, um festzustellen, wann er abgeschlossen ist oder ob ein Problem vorliegt.

Informationen zu diesem Vorgang

Die folgenden Symbole werden auf der Seite „Jobs“ angezeigt und geben den Status des Vorgangs an:

- Im Gange
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In der Warteschlange
- Abgesagt

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Überwachen** auf **Jobs**.
3. Führen Sie auf der Seite **Jobs** die folgenden Schritte aus:
   a. Klicken um die Liste so zu filtern, dass nur Klonvorgänge aufgelistet werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdownliste **Typ** die Option **Klon** aus.
   d. Wählen Sie aus der Dropdown-Liste **Status** den Klonstatus aus.
   e. Klicken Sie auf **Übernehmen**, um die erfolgreich abgeschlossenen Vorgänge anzuzeigen.
4. Wählen Sie den Klonauftrag aus und klicken Sie dann auf **Details**, um die Auftragsdetails anzuzeigen.
5. Klicken Sie auf der Seite „Auftragsdetails“ auf **Protokolle anzeigen**.

Abbrechen von Klonvorgängen

Sie können in der Warteschlange befindliche Klonvorgänge abbrechen.

Sie sollten als SnapCenter Administrator oder Auftragseigentümer angemeldet sein, um Klonvorgänge abzubrechen.

Informationen zu diesem Vorgang

- Sie können einen in die Warteschlange gestellten Klonvorgang entweder auf der Seite **Monitor** oder im Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Klonvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell-Cmdlets oder CLI-Befehle verwenden, um die in die Warteschlange gestellten Klonvorgänge abzubrechen.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer\Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Klonvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritt

Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitorseite	1. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. 2. Wählen Sie den Vorgang aus und klicken Sie auf **Auftrag abbrechen**.
Aktivitätsbereich	1. Klicken Sie nach dem Starten des Klonvorgangs auf im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen. 2. Wählen Sie den Vorgang aus. 3. Klicken Sie auf der Seite **Auftragsdetails** auf **Auftrag abbrechen**.

Einen Klon teilen

Sie können SnapCenter verwenden, um eine geklonte Ressource von der übergeordneten Ressource zu trennen. Der geteilte Klon wird unabhängig von der übergeordneten Ressource.

Informationen zu diesem Vorgang

- Sie können den Klon-Split-Vorgang nicht auf einem Zwischenklon durchführen.

  Nachdem Sie beispielsweise Klon1 aus einer Datenbanksicherung erstellt haben, können Sie eine Sicherung von Klon1 erstellen und diese Sicherung dann klonen (Klon2). Nachdem Sie Klon2 erstellt haben, ist Klon1 ein Zwischenklon und Sie können den Klonaufteilungsvorgang nicht auf Klon1 durchführen. Sie können den Klon-Split-Vorgang jedoch auf Klon2 durchführen.

  Nachdem Sie Klon2 geteilt haben, können Sie den Klon-Teilungsvorgang für Klon1 durchführen, da Klon1 nicht mehr der Zwischenklon ist.

- Wenn Sie einen Klon aufteilen, werden die Sicherungskopien und Klonaufträge des Klons gelöscht.
- Informationen zu FlexClone -Volume-Split-Vorgängen finden Sie unter "Teilen Sie ein FlexClone -Volume von seinem übergeordneten Volume" .
- Stellen Sie sicher, dass das Volume oder Aggregat auf dem Speichersystem online ist.

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** die entsprechende Option aus der Liste „Anzeigen“ aus:

Option	Beschreibung
Für Datenbankanwendungen	Wählen Sie **Datenbank** aus der Ansichtsliste.
Für Dateisysteme	Wählen Sie **Pfad** aus der Ansichtsliste.

3. Wählen Sie die entsprechende Ressource aus der Liste aus.

Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht **Kopien verwalten** die geklonte Ressource (z. B. die Datenbank oder LUN) aus und klicken Sie dann auf *  *.
5. Überprüfen Sie die geschätzte Größe des aufzuteilenden Klons und den erforderlichen verfügbaren Speicherplatz auf dem Aggregat und klicken Sie dann auf **Start**.
6. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.

   Der Klon-Split-Vorgang reagiert nicht mehr, wenn der SMCore-Dienst neu gestartet wird. Sie sollten das Cmdlet „Stop-SmJob“ ausführen, um den Klon-Split-Vorgang zu stoppen, und ihn dann erneut versuchen.

   Wenn Sie eine längere oder kürzere Abfragezeit wünschen, um zu überprüfen, ob der Klon aufgeteilt ist oder nicht, können Sie den Wert des Parameters *CloneSplitStatusCheckPollTime* in der Datei *SMCoreServiceHost.exe.config* ändern, um das Zeitintervall festzulegen, in dem SMCore den Status des Klonaufteilungsvorgangs abfragt. Der Wert wird in Millisekunden angegeben und der Standardwert beträgt 5 Minuten.

   Beispiel:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   Der Startvorgang für die Klonaufteilung schlägt fehl, wenn eine Sicherung, Wiederherstellung oder eine andere Klonaufteilung ausgeführt wird. Sie sollten den Klon-Split-Vorgang erst neu starten, nachdem die laufenden Vorgänge abgeschlossen sind.

Ähnliche Informationen

"SnapCenter -Klon oder -Verifizierung schlägt fehl, da Aggregat nicht vorhanden ist"