Sichern Sie Windows Filesysteme

SnapCenter Software 4.8

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/de-de/snapcenter-48/protect-scw/concept_snapcenter_plug_in_for_microsoft_windows_overview.html on September 26, 2025. Always check docs.netapp.com for the latest.

Inhalt

Sichern Sie Windows Filesysteme . . . 1
SnapCenter Plug-in für Microsoft Windows-Konzepte . . . 1
SnapCenter Plug-in für Microsoft Windows – Übersicht . . . 1
Was Sie mit dem SnapCenter Plug-in für Microsoft Windows tun können . . . 1
SnapCenter Plug-in für Windows Funktionen . . . 1
Wie SnapCenter Windows File-Systeme sichert . . . 2
Storage-Typen unterstützt von SnapCenter Plug-ins für Microsoft Windows . . . 3
Minimale ONTAP-Berechtigungen für Windows Plug-in erforderlich . . . 5
Storage-Systeme für SnapMirror und SnapVault Replizierung vorbereiten . . . 9
Definieren einer Backup-Strategie für Windows File-Systeme . . . 10
Quellen und Ziele von Klonen für Windows Filesysteme . . . 12
Installieren Sie das SnapCenter Plug-in für Microsoft Windows . . . 12
Installationsworkflow des SnapCenter Plug-ins für Microsoft Windows . . . 12
Installationsanforderungen für das SnapCenter Plug-in für Microsoft Windows . . . 13
Fügen Sie Hosts hinzu und installieren Sie das SnapCenter Plug-in für Microsoft Windows . . . 17
Installieren Sie das SnapCenter Plug-in für Microsoft Windows auf mehreren Remote Hosts mithilfe von PowerShell cmdlets . . . 21
Installieren Sie das SnapCenter-Plug-in für Microsoft Windows im Hintergrund über die Befehlszeile . . . 21
Überwachen Sie den Installationsstatus des SnapCenter Plug-in-Pakets . . . 23
Konfigurieren Sie das CA-Zertifikat . . . 24
Installieren Sie das SnapCenter Plug-in für VMware vSphere . . . 27
Bereitstellen eines CA-Zertifikats . . . 27
Konfigurieren Sie die CRL-Datei . . . 27
Sichern Sie Windows File-Systeme . . . 28
Sichern Sie Windows File-Systeme . . . 28
Bestimmen Sie die Verfügbarkeit von Ressourcen für Windows File-Systeme . . . 28
Erstellen von Backup-Richtlinien für Windows Filesysteme . . . 29
Erstellen von Ressourcengruppen für Windows-Dateisysteme . . . 32
Bedarfsgerechtes Backup für eine einzelne Ressource für Windows File-Systeme . . . 34
Sichern Sie Ressourcengruppen für Windows File-Systeme . . . 36
Erstellen Sie eine Storage-Systemverbindung und eine Zugangsdaten mit PowerShell Cmdlets . . . 38
Sichern Sie Ressourcen mit PowerShell cmdlets . . . 39
Monitoring von Backup-Vorgängen . . . 41
Abbrechen von Backup-Vorgängen . . . 42
Sehen Sie sich zugehörige Backups und Klone auf der Seite Topologie an . . . 43
Entfernen Sie Backups mithilfe von PowerShell Cmdlets . . . 45
Reinigen Sie die Anzahl der sekundären Backups mit PowerShell cmdlets . . . 45
Stellen Sie Windows-Dateisysteme wieder her . . . 46
Windows Dateisystemsicherungen wiederherstellen . . . 46
Stellen Sie Ressourcen mithilfe von PowerShell Cmdlets wieder her . . . 48
Überwachen von Restore-Vorgängen . . . 50
Wiederherstellungsvorgänge abbrechen . . . 51
Klonen von Windows Filesystemen . . . 52

Klonen aus einem Windows File-System-Backup . . . 52
Klonen von Backups mit PowerShell Cmdlets . . . 54
Monitoring von Klonvorgängen . . . 58
Klonvorgänge abbrechen . . . 59
Teilen Sie einen Klon auf . . . 60

Sichern Sie Windows Filesysteme

SnapCenter Plug-in für Microsoft Windows-Konzepte

SnapCenter Plug-in für Microsoft Windows – Übersicht

Das SnapCenter Plug-in für Microsoft Windows ist eine Host-seitige Komponente der NetApp SnapCenter Software, die das applikationsgerechte Datensicherungsmanagement von Microsoft Filesystem-Ressourcen ermöglicht. Darüber hinaus bietet die Software Storage-Bereitstellung, Konsistenz von Snapshot Kopien und die Speicherplatzrückgewinnung für Windows File-Systeme. Das Plug-in für Windows automatisiert Backup, Wiederherstellung und Klonvorgänge in File-Systemen in Ihrer SnapCenter Umgebung.

Wenn das Plug-in für Windows installiert ist, können Sie SnapCenter mit NetApp SnapMirror Technologie verwenden, um Spiegelkopien von Backup-Sets auf einem anderen Volume zu erstellen. Zusammen mit der NetApp SnapVault Technologie können Sie eine Disk-to-Disk-Backup-Replizierung für Archivierung oder Standards durchführen.

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 mithilfe von SnapCenter Windows File-Systeme sichern, wiederherstellen und klonen. Sie können auch Aufgaben zur Unterstützung dieser Operationen ausführen.

- Und entdecken Sie Ressourcen
- Sichern Sie Windows File-Systeme
- Planen von Backup-Vorgängen
- Wiederherstellung von Dateisystemsicherungen
- Backups von Dateisystemen klonen
- Monitoring von Backup-, Restore- und Klonvorgängen

Das Plug-in für Windows unterstützt keine Backups und Restores von Filesystemen auf SMB-Freigaben.

SnapCenter Plug-in für Windows Funktionen

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

Das Plug-in für Windows umfasst folgende Hauptfunktionen:

- **Einheitliche grafische Benutzeroberfläche powered by SnapCenter**

  Die SnapCenter-Schnittstelle bietet Standardisierung und Konsistenz über Plug-ins und Umgebungen hinweg. Die Schnittstelle von SnapCenter ermöglicht die vollständige konsistente Backup- und Restore-

Prozesse über Plug-ins hinweg, die zentrale Berichterstellung, die auf einen Blick basierende Dashboard-Ansichten verwenden, die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) einrichten und Jobs in allen Plug-ins überwachen. SnapCenter bietet außerdem eine zentralisierte Planung und ein Richtlinienmanagement zur Unterstützung von Backup- und Klonvorgängen.

- **Automatisierte zentrale Verwaltung**

  Sie können routinemäßige File-System-Backups planen, die Backup-Aufbewahrung richtlinienbasiert konfigurieren und Restore-Vorgänge einrichten. Zudem lässt sich die File-System-Umgebung proaktiv überwachen, indem SnapCenter so konfiguriert wird, dass E-Mail-Warnmeldungen gesendet werden.

- **Unterbrechungsfreie NetApp Snapshot Kopie-Technologie**

  Das Plug-in für Windows verwendet die NetApp Snapshot Kopiertechnologie. So können Sie File-Systeme in Sekundenschnelle sichern und schnell wiederherstellen, ohne das Host offline zu schalten. Snapshot Kopien belegen nur minimalen Speicherplatz.

Zusätzlich zu diesen wichtigen Funktionen bietet das Plug-in für Windows folgende Vorteile:

- Unterstützung für Backup-, Restore- und Klon-Workflows
- RBAC-unterstützte Sicherheit und zentralisierte Rollendelegation
- Erstellung platzsparender Kopien von Produktionsdateisystemen für Tests oder Datenextraktion mit der NetApp FlexClone Technologie

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

- Die Möglichkeit, mehrere Backups gleichzeitig über mehrere Server hinweg auszuführen
- PowerShell cmdlets zur Skripte von Backup-, Wiederherstellungs- und Klonvorgängen
- Unterstützung von Backups von Dateisystemen und Virtual Machine Disks (VMDKs)
- Unterstützung physischer und virtualisierter Infrastrukturen
- Unterstützung für iSCSI, Fibre Channel, FCoE, Raw Device Mapping (RDM), Asymmetric LUN Mapping (ALM), VMDK über NFS und VMFS und Virtual FC

Wie SnapCenter Windows File-Systeme sichert

SnapCenter verwendet die Snapshot Technologie zum Backup von Windows File-System-Ressourcen auf LUNs, CSVs (Cluster Shared Volumes), RDM (Raw Device Mapping) Volumes, ALM (asymmetrische LUN-Zuordnung) in Windows Clustern und VMDKs basierend auf VMFS/NFS (VMware Virtual Machine File System mit NFS).

SnapCenter erstellt Backups, indem Snapshot Kopien der Filesysteme erstellt werden. Gebündelte Backups, bei denen ein Volume LUNs mehrerer Hosts enthält, sind schneller und effizienter als Backups jeder einzelnen LUN, da nur eine Snapshot Kopie des Volumes erstellt wird, im Vergleich mit den einzelnen Snapshots jedes Filesystems.

Wenn SnapCenter eine Snapshot Kopie erstellt, wird das gesamte Storage-System-Volume in der Snapshot Kopie erfasst. Die Sicherung ist jedoch nur für den Host-Server gültig, für den das Backup erstellt wurde.

Wenn sich Daten von anderen Host-Servern auf demselben Volume befinden, können diese Daten nicht aus der Snapshot Kopie 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.

Storage-Typen unterstützt von SnapCenter Plug-ins für Microsoft Windows

SnapCenter unterstützt eine Vielzahl von Storage-Typen sowohl auf physischen Computern als auch auf Virtual Machines. Sie müssen überprüfen, ob Ihr Speichertyp unterstützt wird, bevor Sie das Paket für Ihren Host installieren.

SnapCenter Provisioning und Datensicherung werden unter Windows Server unterstützt. Aktuelle Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

Maschine	Storage-Typ	Bereitstellung mit	Support-Hinweise
Physischer Server	FC-verbundene LUNs	Grafische SnapCenter Benutzeroberfläche (GUI) oder PowerShell Commandlets	
Physischer Server	ISCSI-verbundene LUNs	SnapCenter GUI oder PowerShell Commandlets	
Physischer Server	SMB3 (CIFS) Shares auf einer Storage Virtual Machine (SVM)	SnapCenter GUI oder PowerShell Commandlets	Support nur für die Bereitstellung. SnapCenter kann kein Backup von Daten und Freigaben über das SMB-Protokoll verwenden.
VMware VM	RDM-LUNs, die über einen FC- oder iSCSI-HBA verbunden sind	PowerShell Commandlets	
VMware VM	ISCSI-LUNs, die direkt über den iSCSI-Initiator mit dem Gastsystem verbunden sind	SnapCenter GUI oder PowerShell Commandlets	
VMware VM	Virtual Machine File Systems (VMFS) oder NFS-Datastores	VMware vSphere	

Maschine	Storage-Typ	Bereitstellung mit	Support-Hinweise
VMware VM	Ein mit SMB3 verbundenes Gastbetriebssystem teilt sich auf einer SVM	SnapCenter GUI oder PowerShell Commandlets	Support nur für die Bereitstellung. SnapCenter kann kein Backup von Daten und Freigaben über das SMB-Protokoll verwenden.
Hyper-V VM	Virtuelle FC-LUNs (VFC), die über einen virtuellen Fibre Channel Switch verbunden sind	SnapCenter GUI oder PowerShell Commandlets	Sie müssen Hyper-V Manager verwenden, um virtuelle FC (VFC) LUNs bereitzustellen, die über einen virtuellen Fibre Channel Switch verbunden sind. Hyper-V Pass-Through-Festplatten und Backup von Datenbanken auf VHD(x), die auf NetApp Storage bereitgestellt werden, werden nicht unterstützt.
Hyper-V VM	ISCSI-LUNs, die direkt über den iSCSI-Initiator mit dem Gastsystem verbunden sind	SnapCenter GUI oder PowerShell Commandlets	Hyper-V Pass-Through-Festplatten und Backup von Datenbanken auf VHD(x), die auf NetApp Storage bereitgestellt werden, werden nicht unterstützt.

Maschine	Storage-Typ	Bereitstellung mit	Support-Hinweise
Hyper-V VM	Ein mit SMB3 verbundenes Gastbetriebssystem teilt sich auf einer SVM	SnapCenter GUI oder PowerShell Commandlets	Support nur für die Bereitstellung. SnapCenter kann kein Backup von Daten und Freigaben über das SMB-Protokoll verwenden. Hyper-V Pass-Through-Festplatten und Backup von Datenbanken auf VHD(x), die auf NetApp Storage bereitgestellt werden, werden nicht unterstützt.

Minimale ONTAP-Berechtigungen für Windows Plug-in erforderlich

Die erforderlichen Mindestberechtigungen für ONTAP variieren je nach SnapCenter Plug-ins, die Sie zur Datensicherung verwenden.

Befehle für All-Access: Mindestberechtigungen erforderlich für ONTAP 8.3.0 und höher
Event Generate-AutoSupport-log
Job-Verlauf wird angezeigt Job beenden

Befehle für All-Access: Mindestberechtigungen erforderlich für ONTAP 8.3.0 und höher
lun
lun erstellen
lun löschen
lun Initiatorgruppe hinzufügen
lun-Initiatorgruppe wird erstellt
lun-Initiatorgruppe löschen
lun igroup umbenennen
lun-Initiatorgruppe wird angezeigt
lun Mapping Add-Reporting-Nodes
lun-Zuordnung erstellen
lun-Zuordnung löschen
lun Mapping remove-Reporting-Nodes
lun-Zuordnung wird angezeigt
lun ändern
lun-Verschiebung in Volume
lun ist offline
lun ist online
die lun-Größe wird geändert
lun seriell
lun anzeigen

Befehle für All-Access: Mindestberechtigungen erforderlich für ONTAP 8.3.0 und höher
SnapMirror Richtlinie Add-Rule änderungsregel für snapmirror Remove-Rule für snapmirror-Richtlinie snapmirror-Richtlinie anzeigen snapmirror Wiederherstellung snapmirror zeigen snapmirror Vorgeschichte snapmirror Update snapmirror Update-ls-Set snapmirror Listenziele
Version

Befehle für All-Access: Mindestberechtigungen erforderlich für ONTAP 8.3.0 und höher
Erstellung von Volume-Klonen
Klon von Volume anzeigen
Split-Start des Volume-Klons
Split-Stopp für Volume-Klon
Volume erstellen
Volume destroy
Erstellen eines Volume-Dateiklonen
Show-Disk-Nutzung für Volume-Dateien
Volume ist offline
Das Volume ist online
Volume-Änderung
Erstellen von Volume-qtree
Volume qtree löschen
Änderung des Volume-qtree
Volume-qtree anzeigen
Volume-Einschränkung
Volumen anzeigen
Erstellen von Volume-Snapshots
Volume Snapshot löschen
Ändern des Volume-Snapshots
Umbenennung von Volume-Snapshots
Wiederherstellung von Volume Snapshots
Restore-Datei für Volume Snapshots
Volume-Snapshot werden angezeigt
Volume-Aufhängung nicht verfügbar

Befehle für All-Access: Mindestberechtigungen erforderlich für ONTAP 8.3.0 und höher
cifs von vserver
erstellung von cifs-Freigaben von vserver
cifs-Freigabe von vserver: Löschen
vserver cifs shadowcopy anzeigen
cifs-Freigabe von vserver wird angezeigt
vserver cifs zeigen
vserver Exportrichtlinie
Erstellung von vserver Exportrichtlinien
vserver: Löschen der Exportrichtlinie
Erstellung von vserver Export-Policy-Regel
vserver: Export-Policy-Regel anzeigen
vserver Export-Policy wird angezeigt
vserver iscsi
vserver iscsi-Verbindung wird angezeigt
vserver zeigen

Schreibgeschützter Befehl: Mindestberechtigungen für ONTAP 8.3.0 und höher erforderlich
Netzwerkschnittstelle
Netzwerkschnittstelle wird angezeigt
vserver

Storage-Systeme für SnapMirror und SnapVault Replizierung vorbereiten

Mithilfe eines SnapCenter Plug-ins mit ONTAP SnapMirror Technologie lassen sich Spiegelkopien von Backup-Sets auf einem anderen Volume erstellen. Dank der ONTAP SnapVault Technologie kann eine Disk-to-Disk-Backup-Replizierung zwecks Standards Compliance und anderen Governance-Zwecken durchgeführt werden. Bevor Sie diese Aufgaben durchführen, müssen Sie eine Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes konfigurieren und die Beziehung initialisieren.

SnapCenter führt die Updates an SnapMirror und SnapVault durch, nachdem der Vorgang der Snapshot Kopie abgeschlossen wurde. SnapMirror und SnapVault Updates werden als Teil des SnapCenter Jobs ausgeführt. Erstellen Sie keinen separaten ONTAP Zeitplan.

Wenn Sie von einem NetApp SnapManager Produkt zu SnapCenter kommen und mit Ihren konfigurierten Datensicherungsbeziehungen zufrieden sind, können Sie diesen Abschnitt überspringen.

Eine Datensicherungsbeziehung repliziert Daten auf dem Primärspeicher (das Quell-Volume) auf den sekundären Storage (das Ziel-Volume). Bei der Initialisierung der Beziehung überträgt ONTAP die Datenblöcke, auf die auf dem Quell-Volume verwiesen wird, auf das Ziel-Volume.

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

SnapCenter unterstützt das Management von versionsflexiblen SnapMirror Beziehungen. Informationen zu Beziehungen zwischen Versionen und SnapMirror sowie deren Einrichtung finden Sie im "ONTAP-Dokumentation".

SnapCenter unterstützt keine **Sync_mirror** Replikation.

Definieren einer Backup-Strategie für Windows File-Systeme

Wenn Sie eine Backup-Strategie definieren, bevor Sie Ihre Backups erstellen, erhalten Sie die Backups, die Sie benötigen, um Ihre File-Systeme erfolgreich wiederherzustellen oder zu klonen. Ihr Service Level Agreement (SLA), Recovery Time Objective (RTO) und Recovery Point Objective (RPO) bestimmen Ihre Backup-Strategie weitestgehend.

Ein SLA definiert das erwartete Service-Level und behandelt viele Service-bezogene Probleme, einschließlich Verfügbarkeit und Performance des Service. Bei der RTO handelt es sich um die Zeit, die ein Geschäftsprozess nach einer Serviceunterbrechung wiederhergestellt werden muss. Der Recovery-Zeitpunkt definiert die Strategie für das Alter der Dateien, die aus dem Backup-Storage wiederhergestellt werden müssen, damit regelmäßige Betriebsabläufe nach einem Ausfall fortgesetzt werden können. SLA, RTO und RPO tragen zur Datensicherungsstrategie bei.

Backup-Pläne für Windows File-Systeme

Die Sicherungshäufigkeit wird in den Richtlinien angegeben. Ein Backup-Zeitplan wird in der Konfiguration der Ressourcengruppe angegeben. Der wichtigste Faktor bei der Ermittlung der Backup-Häufigkeit oder des Zeitplans ist die Änderungsrate für die Ressource und die Bedeutung der Daten. Sie können eine stark genutzte Ressource unter Umständen jede Stunde sichern, während Sie selten genutzte Ressourcen einmal am Tag sichern können. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, das Service Level Agreement (SLA) und das Recovery Point Objective (RPO).

Ein SLA definiert das erwartete Service-Level und löst zahlreiche Service-bezogene Probleme, einschließlich Verfügbarkeit und Performance des Service. Ein RPO definiert die Strategie für das Alter der Dateien, die aus dem Backup-Storage wiederhergestellt werden müssen, damit die normalen Vorgänge nach einem Ausfall fortgesetzt werden können. SLA und RPO tragen zur Datensicherungsstrategie bei.

Selbst bei einer stark ausgelasteten Ressource ist es nicht mehr als ein oder zwei Mal pro Tag erforderlich, ein komplettes Backup auszuführen.

Backup-Zeitpläne haben zwei Teile:

- Sicherungshäufigkeit

Die Backup-Häufigkeit (wie oft Backups durchgeführt werden sollen), die für einige Plug-ins als *Schedule Type* bezeichnet wird, ist Teil einer Richtlinienkonfiguration. Sie können beispielsweise die Sicherungshäufigkeit als stündlich, täglich, wöchentlich oder monatlich konfigurieren oder Sie können **Keine** angeben, wodurch die Richtlinie eine reine On-Demand-Richtlinie darstellt. Sie können auf Richtlinien zugreifen, indem Sie auf **Einstellungen** > **Richtlinien** klicken.

- Backup-Pläne

  Backup-Zeitpläne (genau, wann Backups durchgeführt werden sollen) sind Teil der Konfiguration einer Ressourcengruppe. Wenn Sie beispielsweise eine Ressourcengruppe haben, die eine Richtlinie für wöchentliche Backups konfiguriert hat, können Sie den Zeitplan so konfigurieren, dass er jeden Donnerstag um 10:00 Uhr gesichert wird. Sie können auf Ressourcengruppenpläne zugreifen, indem Sie auf **Ressourcen** > **Ressourcengruppen** klicken.

Anzahl der für Windows File-Systeme benötigten Backups

Faktoren, die die Anzahl der erforderlichen Backups bestimmen, umfassen die Größe des Windows-Dateisystems, die Anzahl der verwendeten Volumes, die Änderungsrate des Dateisystems und die Service Level Agreement (SLA).

Backup Namenskonvention für Windows File-Systeme

Backups von Windows Dateisystemen verwenden die standardmäßige Namenskonvention für Snapshot Kopien. Die standardmäßige Backup-Namenskonvention fügt einen Zeitstempel zu den Namen von Snapshot Kopien hinzu, der Ihnen hilft, zu identifizieren, wann die Kopien erstellt wurden.

Die Snapshot Kopie verwendet die folgende standardmäßige Namenskonvention: Resourcegrovname_hostname_timestamp

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 Bedeutungen:

- `dts1` Ist der Name der Ressourcengruppe.
- `mach1x88` Ist der Host-Name.
- `03-12-2016_23.17.26` Sind das Datum und der Zeitstempel.

Beim Erstellen eines Backups können Sie auch ein beschreibende Tag hinzufügen, um das Backup zu identifizieren. Wenn Sie hingegen eine angepasste Backup-Namenskonvention verwenden möchten, müssen Sie das Backup umbenennen, nachdem der Backup-Vorgang abgeschlossen ist.

Optionen zur Backup-Aufbewahrung

Sie können entweder die Anzahl der Tage festlegen, für die Backup-Kopien aufbewahrt werden sollen, oder die Anzahl der Backup-Kopien angeben, die aufbewahrt werden sollen, bis zu einem ONTAP von maximal 255 Kopien. Beispielsweise muss Ihr Unternehmen unter Umständen Backup-Kopien von 10 Tagen oder 130 Backup-Kopien aufbewahren.

Beim Erstellen einer Richtlinie können Sie die Aufbewahrungsoptionen für den Backup-Typ und den

Zeitplantyp angeben.

Wenn Sie die SnapMirror Replizierung einrichten, wird die Aufbewahrungsrichtlinie auf dem Ziel-Volume gespiegelt.

SnapCenter löscht die zurückbehaltenen Backups mit Beschriftungen, die dem Zeitplantyp entsprechen. Wenn der Zeitplantyp für die Ressource oder Ressourcengruppe geändert wurde, verbleiben Backups mit dem alten Etikett des Zeitplantyps möglicherweise weiterhin im System.

Für die langfristige Aufbewahrung von Backup-Kopien sollten Sie SnapVault-Backup verwenden.

Quellen und Ziele von Klonen für Windows Filesysteme

Sie können ein File-System-Backup vom primären oder sekundären Storage klonen. Sie können auch das Ziel wählen, das Ihre Anforderungen unterstützt: Entweder den ursprünglichen Backup-Standort oder ein anderes Ziel auf demselben Host oder auf einem anderen Host. Das Ziel muss sich auf demselben Volume befinden wie das Quellbackup des Klons.

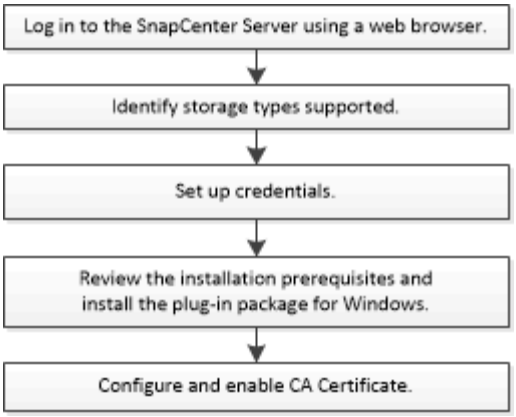
Klonziel	Beschreibung
Original, Quelle, Standort	Standardmäßig speichert SnapCenter den Klon am selben Standort und auf demselben Host wie das zu klonendes Backup.
Andere Position	Sie können den Klon an einem anderen Ort auf demselben Host oder auf einem anderen Host speichern. Der Host muss über eine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

Sie können den Klon nach Abschluss des Klonvorgangs umbenennen.

Installieren Sie das SnapCenter Plug-in für Microsoft Windows

Installationsworkflow des SnapCenter Plug-ins für Microsoft Windows

Sie müssen SnapCenter-Plug-in für Microsoft Windows installieren und einrichten, wenn Sie Windows-Dateien, die keine Datenbankdateien sind, schützen möchten.



Installationsanforderungen für das SnapCenter Plug-in für Microsoft Windows

Vor der Installation des Plug-ins für Windows sollten Sie sich über bestimmte Installationsanforderungen im Klaren sein.

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

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

  Die SnapCenter-Administratorrolle muss über Administratorrechte verfügen.

- Sie müssen den SnapCenter-Server installiert und konfiguriert haben.
- Wenn Sie ein Plug-in auf einem Windows-Host installieren, müssen Sie UAC auf dem Host deaktivieren, wenn Sie keine Anmeldedaten angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Workgroup-Benutzer gehört.
- Sie müssen SnapMirror und SnapVault einrichten, wenn Sie eine Backup-Replizierung möchten.

Hostanforderungen für die Installation des SnapCenter Plug-ins Pakets für Windows

Bevor Sie das SnapCenter Plug-ins-Paket für Windows installieren, sollten Sie mit einigen grundlegenden Speicherplatzanforderungen und Größenanforderungen für das Host-System vertraut sein.

Element	Anforderungen
Betriebssysteme	Microsoft Windows Aktuelle Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".
MindestRAM für das SnapCenter Plug-in auf dem Host	1 GB

Element	Anforderungen
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	5 GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	• Microsoft .NET Framework 4.7.2 oder höher • Windows Management Framework (WMF) 4.0 oder höher • PowerShell 4.0 oder höher Aktuelle Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool". Informationen zur .NET-spezifischen Fehlerbehebung finden Sie unter "Das Upgrade oder die Installation von SnapCenter schlägt bei älteren Systemen, die keine Internetverbindung haben, fehl."

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

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

Was Sie brauchen

- Sie müssen Windows-Anmeldeinformationen einrichten, bevor Sie Plug-ins installieren.
- Sie müssen die Anmeldedaten auf dem Remote-Host mit Administratorrechten, einschließlich Administratorrechten, einrichten.
- Wenn Sie Anmeldedaten für einzelne Ressourcengruppen einrichten und der Benutzer keine vollständigen Administratorberechtigungen hat, müssen Sie dem Benutzer mindestens die Gruppen- und Sicherungsrechte zuweisen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Credential**.

3. Klicken Sie Auf **Neu**.
4. Gehen Sie auf der Seite Credential wie folgt vor:

Für dieses Feld…	Tun Sie das…
Name der Anmeldeinformationen	Geben Sie einen Namen für die Anmeldedaten 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 Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Gültige Formate für das Feld Benutzername sind wie folgt: ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` ◦ `UserName@upn` • Lokaler Administrator (nur für Arbeitsgruppen) Geben Sie bei Systemen, 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 Administratorengruppe gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerungsfunktion auf dem Hostsystem deaktiviert ist. Das zulässige Format für das Feld Benutzername lautet wie folgt: `UserName` Verwenden Sie keine Doppelzitate (") oder Rückkreuzzeichen (`) in den Kennwörtern. Sie sollten nicht das weniger als (<) und Ausrufezeichen (!) verwenden. Symbole in Kennwörtern. Zum Beispiel lessthan<!10, lessthan10<!, backtick`12.
Passwort	Geben Sie das für die Authentifizierung verwendete Passwort ein.

5. Klicken Sie auf **OK**.

Nachdem Sie die Einrichtung von Anmeldeinformationen abgeschlossen haben, möchten Sie einem

Benutzer oder einer Gruppe von Benutzern auf der Seite Benutzer und Zugriff die Wartung von Anmeldeinformationen zuweisen.

Konfigurieren Sie gMSA unter Windows Server 2012 oder höher

Mit Windows Server 2012 oder höher können Sie ein Group Managed Service Account (gMSA) erstellen, das über ein verwaltetes Domain-Konto eine automatisierte Verwaltung von Service-Konten ermöglicht.

Was Sie brauchen

- Sie sollten einen Windows Server 2012 oder höher Domänencontroller haben.
- Sie sollten einen Windows Server 2012 oder höher-Host haben, der Mitglied der Domain 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 Domain Controller aus: Add-KDSRootKey -EffectiveImmediately
3. Erstellen und Konfigurieren des gMSA:
   a. Erstellen Sie ein Benutzerkonto in folgendem Format:

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

   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.

   Um dies zu tun, führen Sie den folgenden Befehl aus PowerShell:

```
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 den Host neu.

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

c. Überprüfen Sie Ihr gMSA-Konto, indem Sie 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 Service-Login-Konto verwendet.

Fügen Sie Hosts hinzu und installieren Sie das SnapCenter Plug-in für Microsoft Windows

Sie können die Seite SnapCenter Add Host 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 ein Cluster installieren.

Was Sie brauchen

- Sie müssen ein Benutzer sein, der einer Rolle zugewiesen ist, die über die Berechtigungen für die Plug-in-Installation und -Deinstallation verfügt, wie z. B. die Rolle „SnapCenter-Administrator“.
- Wenn Sie ein Plug-in auf einem Windows-Host installieren, müssen Sie UAC auf dem Host deaktivieren, wenn Sie keine Anmeldedaten angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Workgroup-Benutzer gehört.

- Der SnapCenter-Benutzer sollte der Rolle „`Anmelden als Dienst`“ des Windows-Servers hinzugefügt werden.
- Stellen Sie sicher, dass der Nachrichtenwarteschlange in Betrieb ist.
- Wenn Sie Group Managed Service Account (gMSA) verwenden, sollten Sie gMSA mit Administratorrechten konfigurieren.

  "Konfigurieren Sie das Gruppenkonto für Managed Services unter Windows Server 2012 oder höher für Windows File System"

Über diese Aufgabe

- 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
  - Benutzerdefinierte Plug-ins
- Installieren von Plug-ins auf einem Cluster

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

- E-Series Storage

  Sie können das Plug-in für Windows nicht auf einem mit E-Series Storage verbundenen Windows-Host installieren.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Vergewissern Sie sich, dass **verwaltete Hosts** oben ausgewählt ist.
3. Klicken Sie Auf **Hinzufügen**.
4. Gehen Sie auf der Seite Hosts wie folgt vor:

Für dieses Feld…	Tun Sie das…
Host-Typ	Wählen Sie den Host-Typ **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.

Für dieses Feld…	Tun Sie das…
Host-Name	Geben Sie den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter hängt von der richtigen Konfiguration des DNS ab. Daher empfiehlt es sich, den vollständig qualifizierten Domänennamen (FQDN) einzugeben. Sie können die IP-Adressen oder FQDN einer der folgenden Adressen eingeben: • Eigenständiger Host • Windows Server-Failover-Clustering (WSFC) Wenn Sie einen Host mit SnapCenter hinzufügen und dieser Teil einer Unterdomäne ist, müssen Sie den FQDN angeben.
Anmeldedaten	Wählen Sie den Anmeldeinformationsnamen aus, den Sie erstellt haben, oder erstellen Sie die neuen Anmeldeinformationen. Die Anmeldeinformationen müssen über Administratorrechte auf dem Remote-Host verfügen. Weitere Informationen finden Sie unter Informationen zum Erstellen von Anmeldeinformationen. Details zu Anmeldeinformationen, einschließlich Benutzername, Domäne und Hosttyp, werden angezeigt, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen platzieren. Der Authentifizierungsmodus wird durch den Hosttyp bestimmt, den Sie im Assistenten zum Hinzufügen von Hosts angeben.

5. Wählen Sie im Abschnitt Plug-ins zum Installieren auswählen die zu installierenden Plug-ins aus.

   Bei neuen Implementierungen werden keine Plug-in-Pakete aufgeführt.

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

Für dieses Feld…	Tun Sie das…
Port	Behalten Sie die Standard-Port-Nummer bei oder geben Sie die Port-Nummer an. Die Standardanschlussnummer 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:\Programmdateien\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.
Fügen Sie alle Hosts im Cluster hinzu	Aktivieren Sie dieses Kontrollkästchen, um alle Cluster-Nodes in einem WSFC hinzuzufügen.
Überspringen Sie die Prüfungen vor der Installation	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 Group Managed Service Account (gMSA), um die Plug-in-Dienste auszuführen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-in-Dienste über das Group Managed Service Account (gMSA) ausführen möchten. Geben Sie den gMSA-Namen in folgendem Format an: *Domainname\AccountName€*. GSSA wird nur für den SnapCenter-Plug-in für Windows-Dienst als Anmelde-Dienstkonto verwendet.

7. Klicken Sie Auf **Absenden**.

   Wenn Sie das Kontrollkästchen **Vorabprüfungen** nicht aktiviert haben, wird der Host überprüft, ob er die Voraussetzungen für die Installation des Plug-ins erfüllt. Der Festplattenspeicher, der RAM, die PowerShell-Version, die .NET-Version und der Speicherort werden anhand der Mindestanforderungen

validiert. Wenn die Mindestanforderungen nicht erfüllt werden, werden entsprechende Fehler- oder Warnmeldungen angezeigt.

Wenn der Fehler mit dem Festplattenspeicher oder RAM zusammenhängt, können Sie die Datei Web.config unter aktualisieren `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 auf mehreren Remote Hosts mithilfe von PowerShell cmdlets

Wenn Sie das SnapCenter Plug-in für Microsoft Windows auf mehreren Hosts gleichzeitig installieren möchten, verwenden Sie die `Install-SmHostPackage` PowerShell Cmdlet:

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

Schritte

1. Starten Sie PowerShell.
2. Richten Sie auf dem SnapCenter-Server-Host eine Sitzung mit ein `Open-SmConnection` Cmdlet und geben Sie dann Ihre Zugangsdaten ein.
3. Fügen Sie den Standalone-Host oder das Cluster mit dem zu SnapCenter hinzu `Add-SmHost` Cmdlet und die erforderlichen Parameter.

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

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

   Sie können das verwenden `-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-Benutzeroberfläche installieren können. Sie können das SnapCenter-Plug-in für Microsoft Windows-Installationsprogramm unbeaufsichtigt, im Silent-Modus, über die Windows-Befehlszeile ausführen.

Was Sie brauchen

- Sie müssen Microsoft .Net 4.7.2 oder höher installiert haben.
- Sie müssen PowerShell 4.0 oder höher installiert haben.
- Sie müssen die Windows-Nachrichtenwarteschlange aktiviert 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.

   Beispielsweise lautet der Standardinstallationspfad C:\ProgramData\NetApp\SnapCenter\Package Repository.

   Auf diesen Pfad kann von dem Host 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 zum Verzeichnis, in dem Sie die Installationsdatei heruntergeladen haben.
4. Geben Sie den folgenden Befehl ein und ersetzen Sie 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`
   ```

   Alle Parameter, die während der Installation von Plug-in für Windows übergeben wurden, sind Groß- und Kleinschreibung.

   Geben Sie die Werte für die folgenden Variablen ein:

Variabel	Wert
/Debuglog“<Debug_Log_Path>	Geben Sie den Namen und den Speicherort der Protokolldatei für das Installationsprogramm der Suite an, wie im folgenden Beispiel: Setup.exe /debuglog"C:\PathToLog\setupexe.log".
BI_SNAPCENTER_PORT	Geben Sie den Port an, auf dem SnapCenter mit SMCore kommuniziert.

Variabel	Wert
SUITE_INSTALLDIR	Geben Sie das Installationsverzeichnis für das Host-Plug-in-Paket an.
BI_SERVICEACCOUNT	Geben Sie das SnapCenter-Plug-in für das Web-Service-Konto von Microsoft Windows an.
BI_SERVICEPWD	Geben Sie das Passwort für das SnapCenter-Plug-in für das Microsoft Windows-Webservice-Konto an.
ISFeatureInstall	Geben Sie die Lösung an, die von SnapCenter auf dem Remote-Host implementiert werden soll.

Der Parameter *debuglog* enthält den Pfad der Protokolldatei für SnapCenter. Das Schreiben in diese Protokolldatei ist die bevorzugte Methode, um Informationen zur Fehlerbehebung zu erhalten, da die Datei die Ergebnisse von Prüfungen enthält, die die Installation für Plug-in-Voraussetzungen ausführt.

Weitere Informationen zur Fehlerbehebung finden Sie bei Bedarf in der Protokolldatei für das Paket SnapCenter für Windows. Die Protokolldateien für das Paket werden (älteste zuerst) im Ordner *%Temp%* aufgeführt, z. B. *C:\temp*\.

Die Installation des Plug-ins für Windows registriert das Plug-in auf dem Host und nicht auf dem SnapCenter-Server. Sie können das Plug-in auf dem SnapCenter Server registrieren, indem Sie den Host mithilfe der SnapCenter GUI oder PowerShell Cmdlet hinzufügen. Nach dem Hinzufügen des Hosts wird das Plug-in automatisch erkannt.

Überwachen Sie den Installationsstatus des SnapCenter Plug-in-Pakets

Sie können den Fortschritt der Installation des SnapCenter-Plug-in-Pakets über die Seite Jobs überwachen. Möglicherweise möchten Sie den Installationsfortschritt prüfen, um festzustellen, wann die Installation abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Abgeschlossen mit Warnungen oder konnte aufgrund von Warnungen nicht gestartet werden
- Warteschlange

Schritte

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

3. Gehen Sie auf der Seite Jobs folgendermaßen vor, um die Liste so zu filtern, dass nur Plug-in-Installationsvorgänge aufgeführt werden:
   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**.
   d. Wählen Sie im Dropdown-Menü Status den Installationsstatus aus.
   e. Klicken Sie Auf **Anwenden**.
4. Wählen Sie den Installationsauftrag aus und klicken Sie auf **Details**, um die Jobdetails anzuzeigen.
5. Klicken Sie auf der Seite Jobdetails auf **Protokolle anzeigen**.

Konfigurieren Sie das CA-Zertifikat

ZertifikatCSR-Datei erstellen

Sie können eine Zertifikatsignierungsanforderung (CSR) generieren und das Zertifikat importieren, das von einer Zertifizierungsstelle (CA) mit dem generierten CSR abgerufen werden kann. Dem Zertifikat ist ein privater Schlüssel zugeordnet.

CSR ist ein Block von codiertem Text, der einem autorisierten Zertifikatanbieter zur Beschaffung des signierten CA-Zertifikats übergeben wird.

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

> Wenn Sie das CA-Zertifikat für Ihre Domain (*.domain.company.com) oder Ihr System (machine1.domain.company.com) besitzen, können Sie die Erstellung der CA-Zertifikat-CSR-Datei überspringen. Sie können das vorhandene CA-Zertifikat mit SnapCenter bereitstellen.

Bei Clusterkonfigurationen sollten der Clustername (virtueller Cluster-FQDN) und die entsprechenden Hostnamen im CA-Zertifikat aufgeführt werden. Das Zertifikat kann aktualisiert werden, indem Sie vor dem Erwerb des Zertifikats das Feld alternativer Antragstellername (SAN) ausfüllen. Bei einem Platzhalter-Zertifikat (*.domain.company.com) enthält das Zertifikat implizit alle Hostnamen der Domäne.

Importieren von CA-Zertifikaten

Sie müssen die CA-Zertifikate mithilfe der Microsoft-Verwaltungskonsole (MMC) auf den SnapCenter-Server und die Windows-Host-Plug-ins importieren.

Schritte

1. Gehen Sie zur Microsoft Management Console (MMC) und klicken Sie dann auf **Datei** > **Snapin hinzufügen/entfernen**.
2. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
3. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
4. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate – Lokaler Computer** > **Vertrauenswürdige Stammzertifizierungsbehörden** > **Zertifikate**.

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

In diesem Fenster des Assistenten…	Gehen Sie wie folgt vor…
Privaten Schlüssel Importieren	Wählen Sie die Option **Ja**, importieren Sie den privaten Schlüssel und klicken Sie dann auf **Weiter**.
Dateiformat Importieren	Keine Änderungen vornehmen; klicken Sie auf **Weiter**.
Sicherheit	Geben Sie das neue Passwort an, das für das exportierte Zertifikat verwendet werden soll, und klicken Sie dann auf **Weiter**.
Abschließen des Assistenten zum Importieren von Zertifikaten	Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**, um den Import zu starten.

Der Import des Zertifikats 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 Daumenabdrucks für das CA-Zertifikat

Ein ZertifikatDaumendruck ist eine hexadezimale Zeichenfolge, die ein Zertifikat identifiziert. Ein Daumendruck wird aus dem Inhalt des Zertifikats mithilfe eines Daumendruckalgorithmus berechnet.

Schritte

1. Führen Sie auf der GUI folgende Schritte durch:
   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 **Miniaturdruck**.
   d. Kopieren Sie die hexadezimalen Zeichen aus dem Feld.
   e. Entfernen Sie die Leerzeichen zwischen den hexadezimalen Zahlen.

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

2. Führen Sie Folgendes aus PowerShell aus:
   a. Führen Sie den folgenden Befehl aus, um den Daumendruck des installierten Zertifikats aufzulisten und das kürzlich installierte Zertifikat anhand des Betreff-Namens zu identifizieren.

Get-ChildItem -Path Cert:\LocalMachine\My

b. Kopieren Sie den Daumendruck.

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 durch, auf denen CA-Zertifikate bereits bereitgestellt wurden.

Schritte

1. Entfernen Sie die vorhandene Zertifikatbindung mit 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"
   ```

Aktivieren Sie CA-Zertifikate für Plug-ins

Sie sollten die CA-Zertifikate konfigurieren und die CA-Zertifikate im SnapCenter-Server und den entsprechenden Plug-in-Hosts bereitstellen. Sie sollten die CA-Zertifikatsvalidierung für die Plug-ins aktivieren.

Was Sie brauchen

- Sie können die CA-Zertifikate mit dem Cmdlet "Run_set-SmCertificateSettings_" aktivieren oder

deaktivieren.

- Sie können den Zertifikatsstatus für die Plug-ins mithilfe der *get-SmCertificateSettings* anzeigen.

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **verwaltete Hosts**.
3. Wählen Sie ein- oder mehrere Plug-in-Hosts aus.
4. Klicken Sie auf **Weitere Optionen**.
5. Wählen Sie **Zertifikatvalidierung Aktivieren**.

Nach Ihrer Beendigung

Auf dem Reiter Managed Hosts wird ein Schloss 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 lautet, werden die Datensicherungsvorgänge erfolgreich abgeschlossen.

Installieren Sie das SnapCenter Plug-in für VMware vSphere

Wenn Ihre Datenbanken auf Virtual Machines (VMs) gespeichert sind oder VMs und Datastores geschützt werden sollen, müssen Sie das SnapCenter Plug-in für die virtuelle Appliance VMware vSphere implementieren.

Informationen zur Bereitstellung finden Sie unter "Implementierungsübersicht".

Bereitstellen eines CA-Zertifikats

Informationen zur Konfiguration des CA-Zertifikats mit dem SnapCenter-Plug-in für VMware vSphere finden Sie unter "Erstellen oder importieren Sie ein SSL-Zertifikat".

Konfigurieren Sie die CRL-Datei

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

Sie können mehrere CRL-Dateien in diesem Verzeichnis platzieren. Die eingehenden Zertifikate werden gegen jede CRL überprüft.

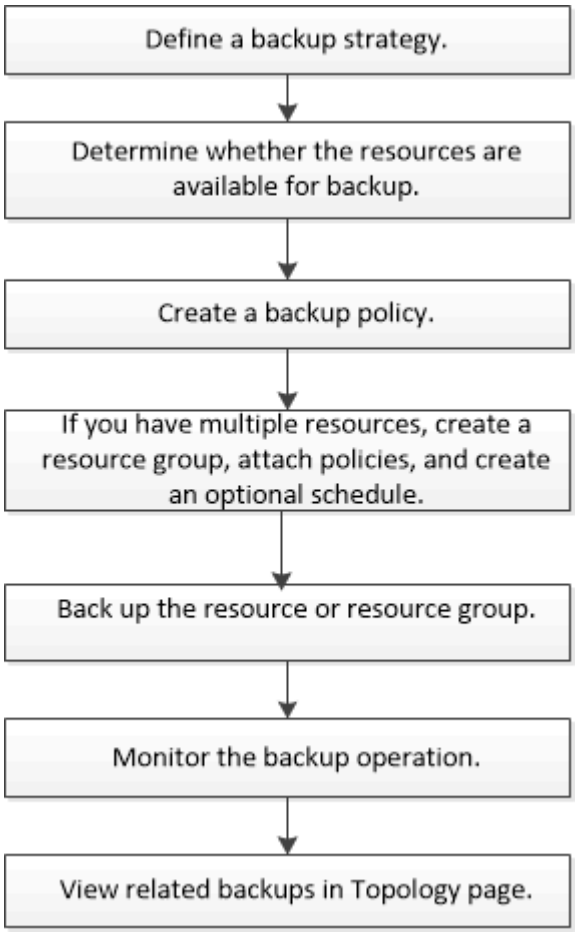
Sichern Sie Windows File-Systeme

Sichern Sie Windows File-Systeme

Wenn das SnapCenter-Plug-in für Microsoft Windows in Ihrer Umgebung installiert wird, können Sie mit SnapCenter Backups der Windows Filesysteme erstellen. Sie können ein einzelnes Dateisystem oder eine Ressourcengruppe sichern, die mehrere Dateisysteme enthält. Sie können Backups nach Bedarf oder gemäß einem definierten Schutzzeitplan erstellen.

Sie können mehrere Backups so planen, dass sie gleichzeitig über mehrere Server ausgeführt werden. Backup- und Restore-Vorgänge können nicht gleichzeitig auf derselben Ressource durchgeführt werden.

Der folgende Workflow zeigt die Reihenfolge, in der Sie die Backup-Vorgänge durchführen müssen:



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter Cmdlet-Hilfe oder das "SnapCenter Software Cmdlet Referenzhandbuch" enthält detaillierte Informationen zu PowerShell Cmdlets.

Bestimmen Sie die Verfügbarkeit von Ressourcen für Windows File-Systeme

Ressourcen sind die LUNs und ähnliche Komponenten in Ihrem Dateisystem, die von Ihren installierten Plug-ins verwaltet werden. Sie können diese Ressourcen zu Ressourcengruppen hinzufügen, sodass Sie Datensicherungsaufträge auf mehreren

Ressourcen ausführen können. Zunächst müssen Sie jedoch ermitteln, welche Ressourcen Sie verfügbar haben. Die Ermittlung verfügbarer Ressourcen überprüft außerdem, ob die Plug-in-Installation erfolgreich abgeschlossen wurde.

Was Sie brauchen

- Sie müssen bereits Aufgaben abgeschlossen haben, z. B. das Installieren von SnapCenter-Servern, das Hinzufügen von Hosts, das Erstellen von SVM-Verbindungen (Storage Virtual Machine) und das Hinzufügen von Anmeldeinformationen.
- Wenn Dateien auf VMware RDM-LUNs oder VMDKs vorhanden sind, müssen Sie das SnapCenter Plug-in für VMware vSphere implementieren und das Plug-in mit SnapCenter registrieren. Weitere Informationen finden Sie unter "Dokumentation zum SnapCenter Plug-in für VMware vSphere".

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 Option **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 in den SnapCenter-Serverbestand aktualisiert.

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

Erstellen von Backup-Richtlinien für Windows Filesysteme

Sie können eine neue Sicherungsrichtlinie für Ressourcen erstellen, bevor Sie SnapCenter zum Sichern von Windows-Dateisystemen verwenden, oder Sie können eine neue Backup-Richtlinie zum Zeitpunkt der Erstellung einer Ressourcengruppen oder beim Backup einer Ressource erstellen.

Was Sie brauchen

- Sie müssen Ihre Backup-Strategie definiert haben. "Weitere Informationen ."
- Sie müssen auf die Datensicherung vorbereitet sein.

  Zur Vorbereitung auf die Datensicherung müssen Aufgaben wie das Installieren von SnapCenter, das Hinzufügen von Hosts, die Erkennung von Ressourcen und das Erstellen von SVM-Verbindungen (Storage Virtual Machine) durchgeführt werden.

- Wenn Sie Snapshot Kopien in einen gespiegelten oder sekundären Vault-Storage replizieren, muss der SnapCenter Administrator Ihnen die SVMs sowohl für die Quell- als auch die Ziel-Volumes 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

Über diese Aufgabe

- DER SCRIPTS_PATH wird mit dem PredefinedWindowsScriptDirectory-Schlüssel definiert, der sich in der SMCoreServiceHost.exe.Config-Datei des Plug-in-Hosts befindet.

  Bei Bedarf können Sie diesen Pfad ändern und den SMCore Service neu starten. Es wird empfohlen, den Standardpfad für die Sicherheit 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 der Taste anzuzeigen. SET-API wird nicht unterstützt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Richtlinien**.
3. Um zu bestimmen, ob Sie eine vorhandene Richtlinie verwenden können, wählen Sie den Richtliniennamen aus und klicken Sie dann auf **Details**.

   Nach Überprüfung der vorhandenen Richtlinien können Sie eine der folgenden Aktionen durchführen:

   - Vorhandene Richtlinie verwenden
   - Kopieren Sie eine vorhandene Richtlinie, und ändern Sie die Richtlinienkonfiguration.
   - Erstellen Sie eine neue Richtlinie.
4. Um eine neue Richtlinie zu erstellen, klicken Sie auf **Neu**.
5. Geben Sie auf der Seite Name den Richtliniennamen und eine Beschreibung ein.
6. Führen Sie auf der Seite Backup-Optionen die folgenden Aufgaben aus:

   a. Wählen Sie eine Sicherungseinstellung aus.

Option	Beschreibung
Konsistentes File-System-Backup	Wählen Sie diese Option, wenn SnapCenter das Festplattenlaufwerk stilllegen soll, auf dem sich das Dateisystem befindet, bevor der Sicherungsvorgang beginnt, und setzen Sie das Laufwerk nach Abschluss des Sicherungsvorgangs wieder ein.
Crash-konsistentes Backup des File-Systems	Wählen Sie diese Option, wenn Sie nicht möchten, dass SnapCenter das Festplattenlaufwerk stilllegt, auf dem sich das Dateisystem befindet.

   b. Wählen Sie eine Zeitplanfrequenz (auch als Richtlinientyp bezeichnet) aus.

      Die Richtlinie gibt nur die Backup-Häufigkeit an. Der spezifische Schutzzeitplan für das Sichern ist in der Ressourcengruppe festgelegt. Daher können zwei oder mehr Ressourcengruppen dieselbe Richtlinien- und Backup-Häufigkeit teilen, jedoch unterschiedliche Backup-Pläne haben.

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

7. Legen Sie auf der Seite Aufbewahrung die Aufbewahrungseinstellungen für On-Demand-Backups und für jede ausgewählte Zeitplanfrequenz fest.

Option	Beschreibung
Gesamtzahl der zu behaltenden Snapshot-Kopien	Wählen Sie diese Option, wenn Sie die Anzahl der Snapshot Kopien SnapCenter-Speicher angeben möchten, bevor Sie sie automatisch löschen.
Snapshot Kopien löschen, die älter als sind	Wählen Sie diese Option, wenn Sie die Anzahl der Tage angeben möchten, die SnapCenter eine Backup-Kopie behält, bevor Sie sie löschen.

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

Der maximale Aufbewahrungswert ist 1018 für Ressourcen auf ONTAP 9.4 oder höher und 254 für Ressourcen unter ONTAP 9.3 oder einer früheren Version. Backups schlagen fehl, wenn die Aufbewahrung auf einen Wert festgelegt ist, der höher ist, als die zugrunde liegende ONTAP Version unterstützt.

8. Geben Sie auf der Seite „Replikation“ die Replikation auf das sekundäre Speichersystem an:

Für dieses Feld…	Tun Sie das…
Aktualisieren Sie SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie	Wählen Sie diese Option aus, um Spiegelkopien von Backup-Sets auf einem anderen Volume (SnapMirror) zu erstellen.
Aktualisieren Sie die SnapVault nach dem Erstellen einer Snapshot Kopie	Wählen Sie diese Option aus, um die Disk-to-Disk-Backup-Replikation durchzuführen.

Für dieses Feld…	Tun Sie das…
Sekundäres Policy-Label	Wählen Sie eine Snapshot-Bezeichnung aus. Abhängig von dem ausgewählten Etikett der Snapshot Kopie wendet ONTAP die Aufbewahrungsrichtlinie für sekundäre Snapshot Kopien an, die mit dem Etikett übereinstimmt. Wenn Sie **Update SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, können Sie optional das Label für die sekundäre Richtlinie angeben. Wenn Sie jedoch **Update SnapVault nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, sollten Sie das sekundäre Policy Label angeben.
Fehler bei Wiederholungszählung	Geben Sie die Anzahl der Replikationsversuche ein, die vor dem Anhalten des Prozesses auftreten sollen.

Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Storage konfigurieren, um zu vermeiden, dass die maximale Anzahl an Snapshot Kopien auf dem sekundären Storage erreicht wird.

9. Geben Sie auf der Seite Skript den Pfad des Prescript oder Postscript ein, den der SnapCenter-Server vor oder nach dem Backup ausführen soll, bzw. ein Zeitlimit, das SnapCenter wartet, bis das Skript ausgeführt wird, bevor das Timing out abgeschlossen wird.

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

   Der Pfad für Prescripts oder Postscripts darf keine Laufwerke oder Shares enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Erstellen von Ressourcengruppen für Windows-Dateisysteme

Eine Ressourcengruppe ist der Container, zu dem Sie mehrere Dateisysteme hinzufügen können, die Sie schützen möchten. Sie müssen auch eine oder mehrere Richtlinien an die Ressourcengruppe anhängen, um den Typ des Datensicherungsauftrags zu definieren, den Sie ausführen möchten, und dann den Backup-Zeitplan festlegen.

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 Option **Dateisysteme** aus der Liste aus.

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

3. Klicken Sie Auf **Neue Ressourcengruppe**.
4. Gehen Sie auf der Seite Name im Assistenten wie folgt vor:

Für dieses Feld…	Tun Sie das…
Name	Geben Sie den Namen der Ressourcengruppe ein. Der Name der Ressourcengruppe darf 250 Zeichen nicht überschreiten.
Verwenden Sie für Snapshot-Kopie das benutzerdefinierte Namensformat	Optional: Geben Sie einen Namen und ein Format für die benutzerdefinierte Snapshot Kopie ein. Beispiel: Custtext_resourcegruppe_Policy_hostname oder resourcegruppe_hostname. Standardmäßig wird ein Zeitstempel an den Namen der Snapshot Kopie angehängt.
Tag	Geben Sie ein beschreibende Tag ein, um beim Suchen einer Ressourcengruppe zu helfen.

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 vor Kurzem Ressourcen hinzugefügt haben, werden diese erst nach einer Aktualisierung der Ressourcenliste in der Liste der verfügbaren Ressourcen angezeigt.

   b. Klicken Sie im Abschnitt Verfügbare Ressourcen auf die Dateisysteme, die Sie sichern möchten, und klicken Sie dann auf den rechten Pfeil, um sie in den Abschnitt Hinzufügen zu verschieben.

      Wenn Sie die Option **Autoselect alle Ressourcen auf demselben Speichervolumen** 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 **Autoselect alle Ressourcen auf demselben Speichervolumen**, und wählen Sie dann die Dateisysteme aus, die Sie in den Abschnitt Hinzufügen verschieben möchten.

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

   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdown-Liste aus.

      Sie können eine beliebige vorhandene Richtlinie auswählen und auf **Details** klicken, um zu bestimmen, 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“ aufgeführt.

b. Klicken Sie im Abschnitt Configure Schedules for Selected Policies auf * * in der Spalte Configure Schedules für die Richtlinie, für die Sie den Zeitplan konfigurieren möchten.

c. Wenn die Richtlinie mit mehreren Terminplantypen (Frequenzen) verknüpft ist, wählen Sie die Frequenz aus, die Sie konfigurieren möchten.

d. Konfigurieren Sie den Zeitplan im Dialogfeld Add Schedules for Policy_Name_, indem Sie das Startdatum, das Ablaufdatum und die Häufigkeit angeben und dann auf **Finish** klicken.

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

Backup-Zeitpläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit SnapCenter Backup-Zeitplänen überschneiden. Sie sollten die Zeitpläne aus dem Windows Task Scheduler und dem SQL Server Agent nicht ändern.

7. Geben Sie auf der Seite Benachrichtigung wie folgt Informationen an:

Für dieses Feld…	Tun Sie das…
E-Mail-Präferenz	Wählen Sie **immer**, **bei Ausfall** oder **bei Fehlschlag oder Warnung**, um E-Mails an Empfänger zu senden, nachdem Sie Backup-Ressourcengruppen erstellt, Richtlinien angehängt und Zeitpläne konfiguriert haben. Geben Sie den SMTP-Server, die Standard-E-Mail-Betreffzeile und die E-Mail-Adressen an und von ein.
Von	E-Mail-Adresse
Bis	E-Mail-Adresse
Betreff	Standard-E-Mail-Betreffzeile

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

Sie können ein Backup nach Bedarf durchführen oder warten, bis das geplante Backup durchgeführt wird.

Bedarfsgerechtes Backup für eine einzelne Ressource für Windows File-Systeme

Wenn sich eine Ressource nicht in einer Ressourcengruppe befindet, können Sie die Ressource On Demand auf der Seite Ressourcen sichern.

Über diese Aufgabe

Wenn Sie eine Ressource mit einer SnapMirror Beziehung zum sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.

Beim Backup eines Dateisystems sichert SnapCenter keine LUNs, die auf einem Volume Mount-Punkt (VMP) in dem gesicherten Dateisystem gemountet sind.

Wenn Sie in einem Windows-Dateisystemkontext arbeiten, sichern Sie keine Datenbankdateien. Dadurch entsteht ein inkonsistentes Backup und ein möglicher Datenverlust beim Restore. Zum Schutz von Datenbankdateien müssen Sie das entsprechende SnapCenter Plug-in für die Datenbank verwenden (z. B. SnapCenter Plug-in für Microsoft SQL Server, SnapCenter Plug-in für Microsoft Exchange Server oder ein benutzerdefiniertes Plug-in für Datenbankdateien).

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

   Legen Sie die Schutzeinstellungen fest, wie in den Aufgaben zum Erstellen von Ressourcengruppen beschrieben.

4. Optional: Geben Sie auf der Seite „Ressource“ des Assistenten ein benutzerdefiniertes Namensformat für die Snapshot Kopie ein.

   Beispiel: Custtext_resourcegruppe_Policy_hostname oder resourcegruppe_hostname. Standardmäßig wird ein Zeitstempel an den Namen der Snapshot Kopie angehängt.

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

   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdown-Liste aus.

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

      Wenn keine vorhandene Richtlinie Ihren Anforderungen entspricht, können Sie eine vorhandene Richtlinie kopieren und ändern oder Sie können 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“ aufgeführt.

   b. Klicken Sie im Abschnitt Configure Schedules for Selected Policies in der Spalte Configure Schedules für die Richtlinie, für die Sie den Zeitplan konfigurieren möchten, auf .

   c. Konfigurieren Sie den Zeitplan im Dialogfeld Add Schedules for Policy_Name_, indem Sie das Startdatum, das Ablaufdatum und die Häufigkeit angeben und dann auf **Finish** klicken.

      Die konfigurierten Zeitpläne werden in der Spalte „angewendete Zeitpläne“ im Abschnitt „Zeitpläne für

ausgewählte Richtlinien konfigurieren“ aufgeführt.

"Geplante Vorgänge können fehlschlagen"

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

Für dieses Feld…	Tun Sie das…
E-Mail-Präferenz	Wählen Sie * immer* oder **bei Ausfall** oder **bei Fehlschlag oder Warnung** aus, um E-Mails an Empfänger zu senden, nachdem Sie Backup-Ressourcengruppen erstellt, Richtlinien angehängt und Zeitpläne konfiguriert haben. Geben Sie die SMTP-Serverinformationen, die Standard-E-Mail-Betreffzeile und die E-Mail-Adressen „`bis`“ und „`von`“ ein.
Von	E-Mail-Adresse
Bis	E-Mail-Adresse
Betreff	Standard-E-Mail-Betreffzeile

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

   Die Seite der Datenbanktopologie wird angezeigt.

8. Klicken Sie auf **Jetzt sichern**.
9. Führen Sie auf der Seite Backup die folgenden Schritte aus:
   a. Wenn Sie mehrere Richtlinien auf die Ressource angewendet haben, wählen Sie aus der Dropdown-Liste Richtlinie die Richtlinie aus, die Sie für das Backup verwenden möchten.

      Wenn die für das On-Demand-Backup ausgewählte Richtlinie einem Backup-Zeitplan zugeordnet ist, werden die On-Demand-Backups auf Basis der für den Zeitplantyp festgelegten Aufbewahrungseinstellungen beibehalten.

   b. Klicken Sie Auf **Backup**.
10. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Sichern Sie Ressourcengruppen für Windows File-Systeme

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host oder Cluster. Für alle in der Ressourcengruppe definierten Ressourcen wird ein Sicherungsvorgang in der Ressourcengruppe durchgeführt. Auf der Seite „Ressourcen“ können Sie ein Backup einer Ressourcengruppe nach Bedarf erstellen. Wenn eine Ressourcengruppe über eine Richtlinie und einen konfigurierten Zeitplan verfügt, werden die Backups automatisch gemäß dem Zeitplan durchgeführt.

Was Sie brauchen

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Wenn Sie eine Ressource mit einer SnapMirror Beziehung zum sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.
- Wenn eine Ressourcengruppe mehrere Datenbanken von verschiedenen Hosts verwendet, kann der Backup-Vorgang bei einigen Hosts aufgrund von Netzwerkproblemen zu spät auslösen. Sie sollten den Wert von MaxRetryForUninitializedHosts in Web.config mit dem Cmdlet "Set-SmConfigSettings PowerShell" konfigurieren

Beim Backup eines Dateisystems sichert SnapCenter keine LUNs, die auf einem Volume Mount-Punkt (VMP) in dem gesicherten Dateisystem gemountet sind.

Wenn Sie in einem Windows-Dateisystemkontext arbeiten, sichern Sie keine Datenbankdateien. Dadurch entsteht ein inkonsistentes Backup und ein möglicher Datenverlust beim Restore. Zum Schutz von Datenbankdateien müssen Sie das entsprechende SnapCenter Plug-in für die Datenbank verwenden (z. B. SnapCenter Plug-in für Microsoft SQL Server, SnapCenter Plug-in für Microsoft Exchange Server oder ein benutzerdefiniertes Plug-in für Datenbankdateien).

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste **Ansicht** die Option **Ressourcengruppe** aus.

   Sie können die Ressourcengruppe durchsuchen, indem Sie den Namen der Ressourcengruppe in das Suchfeld eingeben, oder indem Sie auf klicken und das Tag auswählen. Sie können dann klicken , 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 für das SnapCenter Plug-in für Oracle Database eine föderierte Ressourcengruppe mit zwei Datenbanken haben und eine der Datenbanken Datendatei auf einem nicht-NetApp Storage besitzt, wird der Backup-Vorgang abgebrochen, obwohl sich die andere Datenbank auf einem NetApp Storage befindet.

4. Führen Sie auf der Seite Backup die folgenden Schritte aus:
   a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet haben, wählen Sie aus der Dropdown-Liste **Richtlinie** die Richtlinie aus, die Sie zum Sichern verwenden möchten.

      Wenn die für das On-Demand-Backup ausgewählte Richtlinie einem Backup-Zeitplan zugeordnet ist, werden die On-Demand-Backups auf Basis der für den Zeitplantyp festgelegten Aufbewahrungseinstellungen beibehalten.

   b. Klicken Sie Auf **Backup**.
5. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.
   - In MetroCluster-Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Sicherungsbeziehung 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 für VMware vSphere nicht groß genug ist, kann die Sicherung fehlschlagen. Um die Java-Heap-Größe zu erhöhen, suchen Sie die Skriptdatei `/opt/netapp/init_scripts/scvservice`. In diesem Skript, das `do_start method` Befehl startet den SnapCenter-VMware-Plug-in-Service. Aktualisieren Sie diesen Befehl auf Folgendes: `Java -jar -Xmx8192M -Xms4096M`.

Erstellen Sie eine Storage-Systemverbindung und eine Zugangsdaten mit PowerShell Cmdlets

Sie müssen eine SVM-Verbindung (Storage Virtual Machine) und Zugangsdaten erstellen, bevor Sie PowerShell cmdlets verwenden können, um Datensicherungsvorgänge durchzuführen.

Was Sie brauchen

- Sie sollten die PowerShell Umgebung auf die Ausführung der PowerShell Commandlets vorbereitet haben.
- Sie sollten die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ besitzen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-in-Installationen nicht ausgeführt werden.

  Die Host-Plug-in-Installationen dürfen beim Hinzufügen einer Speichersystemverbindung nicht ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbank-Status in der SnapCenter GUI unter „`not available for Backup`“ oder „`not on NetApp Storage`“ angezeigt werden kann.

- Speichersystemnamen sollten eindeutig sein.

  SnapCenter unterstützt nicht mehrere Storage-Systeme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Storage-System sollte über einen eindeutigen Namen und eine eindeutige Management-LIF-IP-Adresse verfügen.

Schritte

1. Initiieren Sie eine PowerShell-Verbindungssitzung mit dem Cmdlet Open-SmConnection.

   In diesem Beispiel wird eine PowerShell Sitzung geöffnet:

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

2. Erstellen Sie mit dem Cmdlet "Add-SmStorageConnection" eine neue Verbindung zum Storage-System.

   In diesem Beispiel wird eine neue Speichersystemverbindung erstellt:

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

3. Erstellen Sie mit dem Cmdlet "Add-SmCredential" eine neue Anmeldeinformation.

In diesem Beispiel werden neue Anmeldeinformationen mit dem Namen FinanceAdmin mit Windows-Anmeldeinformationen erstellt:

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

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

Sichern Sie Ressourcen mit PowerShell cmdlets

Sie können die PowerShell Commandlets zum Sichern von SQL Server-Datenbanken oder Windows-Dateisystemen verwenden. Dazu gehört die Sicherung einer SQL Server-Datenbank oder eines Windows-Dateisystems, einschließlich der Herstellung einer Verbindung mit dem SnapCenter-Server, der Ermittlung der SQL Server-Datenbankinstanzen oder Windows-Dateisysteme, das Hinzufügen einer Richtlinie, das Erstellen einer Backup-Ressourcengruppe, das Sichern und das Überprüfen des Backups.

Was Sie brauchen

- Sie müssen die PowerShell Umgebung vorbereitet haben, um die PowerShell Cmdlets auszuführen.
- Sie müssen die Speichersystemverbindung hinzugefügt und Anmeldedaten erstellt haben.
- Sie müssen Hosts hinzugefügt und Ressourcen erkannt haben.

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

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

   Die Eingabeaufforderung für Benutzername und Passwort wird angezeigt.

2. Erstellen Sie mithilfe des Cmdlet "Add-SmPolicy" eine Backup-Richtlinie.

   Dieses Beispiel erstellt eine neue Backup-Richtlinie mit einem SQL Backup-Typ von FullBackup:

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

   In diesem Beispiel wird eine neue Backup-Richtlinie mit einem Backup-Typ von CrashConsistent für Windows File-Systeme erstellt:

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

3. Ermitteln Sie Host-Ressourcen mit dem Cmdlet "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
```

   In diesem Beispiel werden Ressourcen für Windows File-Systeme auf dem angegebenen Host ermittelt:

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

4. Fügen Sie mit dem Cmdlet "Add-SmResourceGroup" eine neue Ressourcengruppe zu SnapCenter hinzu.

   In diesem Beispiel wird eine neue Ressourcengruppe für die Sicherung von SQL-Datenbanken 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"
```

   Dieses Beispiel erstellt eine neue Windows Dateisystem-Backup-Ressourcengruppe mit der angegebenen Richtlinie und Ressourcen:

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

5. Initiieren Sie einen neuen Sicherungsauftrag mit dem Cmdlet "New-SmBackup".

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

6. Zeigen Sie den Status des Backup-Jobs mit dem Cmdlet "Get-SmBackupReport" an.

   In diesem Beispiel wird ein Job-Summary-Bericht aller Jobs angezeigt, die am angegebenen Datum

ausgeführt wurden:

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

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

Monitoring von Backup-Vorgängen

Sie können den Fortschritt verschiedener Backup-Vorgänge über die Seite SnapCenterJobs überwachen. Sie können den Fortschritt überprüfen, um festzustellen, wann er abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

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

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Abgeschlossen mit Warnungen oder konnte aufgrund von Warnungen nicht gestartet werden
- Warteschlange
- Storniert

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 Sie hier , um die Liste so zu filtern, dass nur Backup-Vorgänge aufgeführt werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Backup** aus.
   d. Wählen Sie im Dropdown-Menü **Status** den Sicherungsstatus aus.
   e. Klicken Sie auf **Anwenden**, um die abgeschlossenen Vorgänge anzuzeigen.
4. Wählen Sie einen Sicherungsauftrag aus, und klicken Sie dann auf **Details**, um die Jobdetails anzuzeigen.

   Der Status des Backupjobs wird zwar angezeigt Wenn Sie auf die Jobdetails klicken, wird möglicherweise angezeigt, dass einige der untergeordneten Aufgaben des Backup-Vorgangs noch ausgeführt oder mit Warnzeichen markiert sind.

5. Klicken Sie auf der Seite Jobdetails auf **Protokolle anzeigen**.

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

Überwachen Sie die Vorgänge im Teilfenster „Aktivität“

Im Aktivitätsbereich werden die fünf zuletzt durchgeführten Operationen angezeigt. Der Bereich „Aktivität“ wird auch angezeigt, wenn der Vorgang initiiert wurde und der Status des Vorgangs.

Im Fensterbereich Aktivität werden Informationen zu Backup-, Wiederherstellungs-, Klon- und geplanten Backup-Vorgängen angezeigt. Wenn Sie Plug-in für SQL Server oder Plug-in für Exchange Server verwenden, werden im Aktivitätsbereich auch Informationen über den erneuten Seeding angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Klicken Sie auf den Bereich „Aktivität“, um die fünf letzten Vorgänge anzuzeigen.

   Wenn Sie auf einen der Vorgänge klicken, werden die Arbeitsdetails auf der Seite Jobdetails aufgeführt.

Abbrechen von Backup-Vorgängen

Sie können Backup-Vorgänge in der Warteschlange abbrechen.

Was Sie brauchen

- Sie müssen als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um Vorgänge abzubrechen.
- Sie können einen Sicherungsvorgang entweder über die Seite **Monitor** oder über den Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Sicherungsvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell Commandlets oder CLI-Befehle verwenden, um die Backup-Vorgänge abzubrechen.
- Die Schaltfläche **Job abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie **Alle Mitglieder dieser Rolle sehen und auf anderen Mitgliedsobjekten** auf der Seite Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Backup-Vorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	a. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. b. Wählen Sie den Vorgang aus, und klicken Sie dann auf **Job abbrechen**.

Von der…	Aktion
Aktivitätsbereich	a. Nachdem Sie den Sicherungsvorgang gestartet haben, klicken Sie im Aktivitätsbereich auf * * , um die letzten fünf Vorgänge anzuzeigen. b. Wählen Sie den Vorgang aus. c. Klicken Sie auf der Seite Jobdetails auf **Job abbrechen**.

Der Vorgang wird abgebrochen und die Ressource wird in den vorherigen Status zurückgesetzt.

Sehen Sie sich zugehörige Backups und Klone auf der Seite Topologie an

Wenn Sie die Erstellung von Backups oder Klonen einer Ressource vorbereiten, können Sie eine grafische Darstellung aller Backups und Klone auf dem primären und sekundären Storage anzeigen. Auf der Seite Topology sehen Sie alle Backups und Klone, die für die ausgewählte Ressource oder Ressourcengruppe zur Verfügung stehen. Sie können die Details zu diesen Backups und Klonen anzeigen und diese dann zur Durchführung von Datensicherungsvorgängen auswählen.

Über diese Aufgabe

In der Ansicht Kopien managen können Sie die folgenden Symbole überprüfen, um festzustellen, ob die Backups und Klone auf dem primären oder sekundären Storage (Mirror-Kopien oder Vault-Kopien) verfügbar sind.

- 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 Storage gespiegelt werden.

  Klone eines Backups einer versionsflexiblen Spiegelung auf einem Volume vom Typ Mirror werden in der Topologieansicht angezeigt, aber die Anzahl der gespiegelten Backups in der Topologieansicht umfasst nicht das versionsflexible Backup.

- Zeigt die Anzahl der Backups und Klone an, die mithilfe der SnapVault Technologie auf dem sekundären Storage repliziert werden.
  - Die Anzahl der angezeigten Backups umfasst die Backups, die aus dem sekundären Speicher gelöscht wurden. Wenn Sie beispielsweise 6 Backups mit einer Richtlinie erstellt haben, um nur 4 Backups aufzubewahren, werden die Anzahl der angezeigten Backups 6 angezeigt.
  - Wenn Sie ein Upgrade von SnapCenter 1.1 durchgeführt haben, werden die Klone auf dem sekundären (Mirror oder Vault) nicht unter Mirror-Kopien oder Vault-Kopien in der Topologieseite angezeigt. Alle mit SnapCenter 1.1 erstellten Klone werden unter den lokalen Kopien in SnapCenter 3.0 angezeigt.

Klone eines Backups einer versionsflexiblen Spiegelung auf einem Volume vom Typ Mirror werden in der Topologieansicht angezeigt, aber die Anzahl der gespiegelten Backups in der Topologieansicht umfasst nicht das versionsflexible Backup.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen entweder die Ressource oder Ressourcengruppe aus der Dropdown-Liste **Ansicht** aus.
3. Wählen Sie die Ressource entweder in der Ansicht „Ressourcendetails“ oder in der Ansicht „Ressourcengruppendetails“ aus.

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

4. Prüfen Sie die Übersichtskarte, um eine Zusammenfassung der Anzahl der Backups und Klone anzuzeigen, die auf dem primären und sekundären Storage verfügbar sind.

   Im Abschnitt „Übersichtskarte“ wird die Gesamtanzahl der Backups und Klone angezeigt. Nur für Oracle-Datenbanken wird im Abschnitt „Übersichtskarte“ auch die Gesamtanzahl der Protokollsicherungen angezeigt.

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

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

   Die Details zu Backups und Klonen werden in einem Tabellenformat angezeigt.

6. Wählen Sie das Backup aus der Tabelle aus, und klicken Sie dann auf die Datensicherungssymbole, um Vorgänge zum Wiederherstellen, Klonen, Umbenennen und Löschen durchzuführen.

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

   Wenn Sie benutzerdefinierte SnapCenter-Plug-ins verwenden, können Sie die Backups, die sich auf dem primären Speichersystem befinden, nicht umbenennen.

   - Wenn Sie ein Backup einer Oracle-Ressource oder Ressourcengruppe auswählen, können Sie auch Mount- und Unmount-Vorgänge durchführen.
   - Wenn Sie ein Protokoll-Backup einer Oracle-Ressource oder Ressourcengruppe ausgewählt haben, können Sie Vorgänge zum Umbenennen, Mounten, Aufheben und Löschen ausführen.
   - Wenn Sie SnapCenter Plug-ins Package für Linux verwenden und das Backup mit Oracle Recovery Manager (RMAN) katalogisiert haben, können Sie diese katalogisierten Backups nicht umbenennen.

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

Beispiel für Backups und Klone auf dem primären Speicher

Entfernen Sie Backups mithilfe von PowerShell Cmdlets

Mit dem Cmdlet "Remove-SmBackup" können Sie Backups löschen, wenn Sie diese nicht mehr für andere Datenschutzvorgänge benötigen.

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

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

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

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

2. Löschen Sie ein oder mehrere Backups mit dem Cmdlet "Remove-SmBackup".

   In diesem Beispiel werden zwei Backups mithilfe der Backup-IDs gelöscht:

```
Remove-SmBackup -BackupIds 3,4
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"):
```

Reinigen Sie die Anzahl der sekundären Backups mit PowerShell cmdlets

Sie können das Cmdlet "Remove-SmBackup" verwenden, um die Anzahl der Backups für sekundäre Backups zu bereinigen, die keine Snapshot-Kopien haben. Sie möchten dieses Cmdlet vielleicht verwenden, wenn die gesamten Snapshot Kopien, die in der Topologie zum Managen von Kopien angezeigt werden, nicht mit der Einstellung zum Speichern von sekundären Storage Snapshot Kopien übereinstimmen.

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

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

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

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

2. Bereinigen Sie die Anzahl der sekundären Backups mit dem Parameter -CleanupSecondaryBackups.

   Dieses Beispiel bereinigt die Anzahl der Backups für sekundäre Backups ohne Snapshot-Kopien:

```
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"):
```

Stellen Sie Windows-Dateisysteme wieder her

Windows Dateisystemsicherungen wiederherstellen

Sie können SnapCenter verwenden, um Backups von Dateisystemen wiederherzustellen. Die Wiederherstellung des Dateisystems ist ein mehrphasiger Prozess, bei dem alle Daten von einem angegebenen Backup an den ursprünglichen Speicherort des Filesystems kopiert werden.

Was Sie brauchen

- Sie müssen das Dateisystem gesichert haben.
- Wenn ein geplanter Vorgang, z. B. ein Backup-Vorgang, derzeit für ein Dateisystem ausgeführt wird, muss dieser Vorgang abgebrochen werden, bevor Sie einen Wiederherstellungsvorgang starten können.
- Sie können ein Dateisystem-Backup nur am ursprünglichen Speicherort, nicht in einem alternativen Pfad wiederherstellen.

  Sie können keine einzelne Datei aus einem Backup wiederherstellen, da das wiederhergestellte Dateisystem alle Daten überschreibt, die sich am ursprünglichen Speicherort des Dateisystems befinden. Zum Wiederherstellen einer einzelnen Datei aus einem Dateisystem-Backup müssen Sie das Backup klonen und auf die Datei im Klon zugreifen.

- Sie können ein System oder ein Startvolume nicht wiederherstellen.
- SnapCenter kann Filesysteme in einem Windows Cluster wiederherstellen, ohne die Cluster-Gruppe offline

zu schalten.

Über diese Aufgabe

- DER SCRIPTS_PATH wird mit dem PredefinedWindowsScriptDirectory-Schlüssel definiert, der sich in der SMCoreServiceHost.exe.Config-Datei des Plug-in-Hosts befindet.

  Bei Bedarf können Sie diesen Pfad ändern und den SMCore Service neu starten. Es wird empfohlen, den Standardpfad für die Sicherheit 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 der Taste anzuzeigen. SET-API wird nicht unterstützt.

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 Ressourcengruppen aus.
3. Wählen Sie eine Ressourcengruppe aus der Liste aus, und klicken Sie dann auf **Wiederherstellen**.
4. Wählen Sie auf der Seite Backups aus, ob Sie Daten aus primären oder sekundären Speichersystemen wiederherstellen möchten, und wählen Sie dann ein Backup aus, das wiederhergestellt werden soll.
5. Wählen Sie im Assistenten Wiederherstellen Ihre Optionen aus.
6. Sie können den Pfad und die Argumente des Prescript oder Postscript eingeben, die SnapCenter vor bzw. nach der Wiederherstellung ausführen soll.

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

   Der Pfad für Prescripts oder Postscripts darf keine Laufwerke oder Shares enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

7. Wählen Sie auf der Seite Benachrichtigung eine der folgenden Optionen aus:

Für dieses Feld…	Tun Sie das…
Protokollieren der Ereignisse des SnapCenter-Servers im Syslog-Storage-System	Wählen Sie diese Option aus, um SnapCenter Serverereignisse im Syslog des Speichersystems zu protokollieren.
Senden der AutoSupport-Benachrichtigung für fehlgeschlagene Vorgänge an das Storage-System	Wählen Sie diese Option aus, um Informationen zu fehlgeschlagenen Vorgängen mithilfe von AutoSupport an NetApp zu senden.

Für dieses Feld…	Tun Sie das…
E-Mail-Präferenz	Wählen Sie **immer**, **bei Ausfall** oder **bei Fehlschlag oder Warnung** aus, um nach der Wiederherstellung von Backups E-Mail-Nachrichten an Empfänger zu senden. Geben Sie den SMTP-Server, die Standard-E-Mail-Betreffzeile und die E-Mail-Adressen an und von ein.

8. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
9. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Wenn das wiederhergestellte Dateisystem eine Datenbank enthält, müssen Sie auch die Datenbank wiederherstellen. Wenn Sie die Datenbank nicht wiederherstellen, ist Ihre Datenbank möglicherweise ungültig. Informationen zum Wiederherstellen von Datenbanken finden Sie im Data Protection Guide für diese Datenbank.

Stellen Sie Ressourcen mithilfe von PowerShell Cmdlets wieder her

Zur Wiederherstellung eines Ressourcen-Backups gehört die Initiierung einer Verbindungssitzung mit dem SnapCenter-Server, die Auflistung der Backups und das Abrufen von Backup-Informationen sowie die Wiederherstellung eines Backups.

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

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

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

2. Rufen Sie die Informationen zu einem oder mehreren Backups ab, die Sie wiederherstellen möchten, indem Sie die Cmdlets Get-SmBackup und Get-SmBackupReport verwenden.

   In diesem Beispiel werden Informationen zu allen verfügbaren Backups angezeigt:

```
 C:\PS>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 an:

```
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 dem Backup mit dem Cmdlet "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          :
```

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

Überwachen von Restore-Vorgängen

Sie können den Fortschritt der verschiedenen SnapCenter-Wiederherstellungen über die Seite Jobs überwachen. Sie können den Fortschritt eines Vorgangs überprüfen, um zu bestimmen, wann dieser abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Status nach der Wiederherstellung beschreiben die Bedingungen der Ressource nach einem Wiederherstellungsvorgang und alle weiteren Wiederherstellungsmaßnahmen, die Sie ergreifen können.

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Abgeschlossen mit Warnungen oder konnte aufgrund von Warnungen nicht gestartet werden
- Warteschlange
- Storniert

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 Sie hier , um die Liste so zu filtern, dass nur Wiederherstellungsvorgänge aufgelistet werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Restore** aus.
   d. Wählen Sie aus der Dropdown-Liste **Status** den Wiederherstellungsstatus aus.
   e. Klicken Sie auf **Anwenden**, um die Vorgänge anzuzeigen, die erfolgreich abgeschlossen wurden.
4. Wählen Sie den Wiederherstellungsauftrag aus, und klicken Sie dann auf **Details**, um die Jobdetails anzuzeigen.
5. Klicken Sie auf der Seite Jobdetails auf **Protokolle anzeigen**.

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

Nach der Volume-basierten Wiederherstellung werden die Backup-Metadaten aus dem SnapCenter-Repository gelöscht, die Backup-Katalogeinträge bleiben aber im SAP HANA-Katalog. Der Status des Wiederherstellungsjobs wird angezeigt , Sie sollten auf Jobdetails klicken, um das Warnzeichen einiger der untergeordneten Aufgaben anzuzeigen. Klicken Sie auf das Warnschild und löschen Sie die angezeigten Backup-Katalog-Einträge.

Wiederherstellungsvorgänge abbrechen

Sie können Wiederherstellungsaufträge abbrechen, die in die Warteschlange gestellt werden.

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

Über diese Aufgabe

- Sie können einen Wiederherstellungsvorgang in der Warteschlange entweder über die Seite **Monitor** oder über den Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Wiederherstellungsvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell Commandlets oder CLI-Befehle verwenden, um die in der

Warteschlange befindlichen Wiederherstellungsvorgänge abzubrechen.

- Die Schaltfläche **Job abbrechen** ist für Wiederherstellungsvorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie **Alle Mitglieder dieser Rolle sehen und auf anderen Mitgliedsobjekten** auf der Seite Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Wiederherstellungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritt

Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	1. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. 2. Wählen Sie den Job aus und klicken Sie auf **Job abbrechen**.
Aktivitätsbereich	1. Nachdem Sie den Wiederherstellungsvorgang gestartet haben, klicken Sie auf das Aktivitätsfenster, um die fünf letzten Vorgänge anzuzeigen. 2. Wählen Sie den Vorgang aus. 3. Klicken Sie auf der Seite Jobdetails auf **Job abbrechen**.

Klonen von Windows Filesystemen

Klonen aus einem Windows File-System-Backup

Sie können SnapCenter zum Klonen eines Windows Filesystem-Backups verwenden. Wenn Sie eine Kopie einer einzelnen Datei wünschen, die versehentlich gelöscht oder geändert wurde, können Sie ein Backup klonen und auf diese Datei im Klon zugreifen.

Was Sie brauchen

- Sie sollten auf die Datensicherung vorbereitet sein, indem Sie Aufgaben wie das Hinzufügen von Hosts, die Identifizierung von Ressourcen und das Erstellen von SVM-Verbindungen (Storage Virtual Machine) abschließen.
- Sie sollten eine Sicherung des Dateisystems haben.
- Sie sollten sicherstellen, dass die Aggregate, die die Volumes hosten, sich in der Liste der zugewiesenen Aggregate der Storage Virtual Machine (SVM) befinden.
- Sie können keine Ressourcengruppe klonen. Sie können nur individuelle File-System-Backups klonen.
- Wenn sich ein Backup auf einer virtuellen Maschine mit VMDK-Laufwerk befindet, kann SnapCenter das Backup nicht auf einem physischen Server klonen.
- Wenn Sie ein Windows Cluster klonen (z. B. eine gemeinsame LUN oder ein gemeinsam genutztes

Cluster-Volume (CSV)-LUN), wird der Klon als dedizierte LUN auf dem von Ihnen angegebenen Host gespeichert.

- Für einen Klonvorgang kann das Stammverzeichnis des Volume-Bereitstellungspunkts kein freigegebenes Verzeichnis sein.
- Auf einem Node, der nicht der Home-Node für das Aggregat ist, können Sie keinen Klon erstellen.
- Sie können keine wiederkehrenden Vorgänge des Klons (Lebenszyklus von Klonen) für Windows Filesysteme planen, sondern nur Backups nach Bedarf klonen.
- Wenn Sie eine LUN verschieben, die einen Klon enthält, auf ein neues Volume, kann SnapCenter den Klon nicht mehr unterstützen. Beispielsweise können Sie diesen Klon nicht mit SnapCenter löschen.
- Sie können nicht über mehrere Umgebungen hinweg klonen. Zum Beispiel Klonen von einer physischen Festplatte auf eine virtuelle Festplatte oder umgekehrt.

Über diese Aufgabe

- DER SCRIPTS_PATH wird mit dem PredefinedWindowsScriptDirectory-Schlüssel definiert, der sich in der SMCoreServiceHost.exe.Config-Datei des Plug-in-Hosts befindet.

  Bei Bedarf können Sie diesen Pfad ändern und den SMCore Service neu starten. Es wird empfohlen, den Standardpfad für die Sicherheit 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 der Taste anzuzeigen. SET-API wird nicht unterstützt.

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

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

4. Wählen Sie in der Liste Ressourcen das zu klonenden Backup aus, und klicken Sie dann auf das Klon-Symbol.
5. Gehen Sie auf der Seite Optionen wie folgt vor:

Für dieses Feld…	Tun Sie das…
Klonserver	Wählen Sie den Host aus, auf dem der Klon erstellt werden soll.

Für dieses Feld…	Tun Sie das…
„Automatische Zuweisung von Bereitstellungspunkt“ oder „Automatische Zuweisung von Volume-Bereitstellungspunkt unter Pfad“	Legen Sie fest, ob unter einem Pfad automatisch ein Mount-Punkt oder ein Volume-Mount-Punkt zugewiesen werden soll. Automatisches Zuweisen von Volume-Mount-Punkt unter Pfad: Der Mount-Punkt unter einem Pfad ermöglicht es Ihnen, ein bestimmtes Verzeichnis bereitzustellen, in dem die Mount-Punkte erstellt werden. Bevor Sie diese Option auswählen, müssen Sie überprüfen, ob das Verzeichnis leer ist. Wenn ein Backup im Verzeichnis vorhanden ist, befindet sich das Backup nach dem Mount-Vorgang in einem ungültigen Status.
Speicherort der Archivierung	Wählen Sie einen Archivort aus, wenn Sie ein sekundäres Backup klonen.

6. Geben Sie auf der Seite Skript alle Druckschriften oder Postskripte an, die Sie ausführen möchten.

   Der Pfad für Prescripts oder Postscripts darf keine Laufwerke oder Shares enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

7. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
8. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Klonen von Backups mit PowerShell Cmdlets

Der Klon-Workflow umfasst die Planung, die Durchführung des Klonvorgangs und die Überwachung des Vorgangs.

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

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

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

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

   In diesem Beispiel werden Informationen zu allen verfügbaren Backups angezeigt:

```
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 über eine bestimmte Ressourcengruppe, ihre Ressourcen und zugehörige 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. Initiieren Sie einen Klonvorgang aus einem vorhandenen Backup mit dem Cmdlet "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 für eine angegebene 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 Clone-Jobs mit dem Cmdlet Get-SmCloneReport an.

   In diesem Beispiel wird ein Klonbericht für die angegebene Job-ID angezeigt:

```
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}
```

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

Monitoring von Klonvorgängen

Sie können den Status von SnapCenter-Klonvorgängen mithilfe der Seite Jobs überwachen. Sie können den Fortschritt eines Vorgangs überprüfen, um zu bestimmen, wann dieser abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Abgeschlossen mit Warnungen oder konnte aufgrund von Warnungen nicht gestartet werden
- Warteschlange
- Storniert

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 Sie hier , um die Liste so zu filtern, dass nur Klonvorgänge aufgelistet werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Clone** aus.
   d. Wählen Sie aus der Dropdown-Liste **Status** den Klonstatus aus.
   e. Klicken Sie auf **Anwenden**, um die Vorgänge anzuzeigen, die erfolgreich abgeschlossen wurden.
4. Wählen Sie den Klon-Job aus, und klicken Sie dann auf **Details**, um die Job-Details anzuzeigen.
5. Klicken Sie auf der Seite Jobdetails auf **Protokolle anzeigen**.

Klonvorgänge abbrechen

Sie können Klonvorgänge in die Warteschlange abbrechen.

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

Über diese Aufgabe

- Sie können einen Klonvorgang in der Warteschlange entweder über die Seite **Monitor** oder über den Bereich **Aktivität** abbrechen.
- Sie können einen ausgeführten Klonvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell Commandlets oder CLI-Befehle verwenden, um die in der Warteschlange befindlichen Klonvorgänge abzubrechen.
- Wenn Sie **Alle Mitglieder dieser Rolle sehen und auf anderen Mitgliedsobjekten** auf der Seite Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Klonvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritt

Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	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 das Teilfenster „Aktivität“, um die fünf letzten Vorgänge anzuzeigen. 2. Wählen Sie den Vorgang aus. 3. Klicken Sie auf der Seite Jobdetails auf **Job abbrechen**.

Teilen Sie einen Klon auf

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

Über diese Aufgabe

- Sie können den Clone-Split-Vorgang nicht für einen Zwischenkon ausführen.

  Wenn Sie beispielsweise Klon1 aus einem Datenbank-Backup erstellen, können Sie eine Sicherung von Klon1 erstellen und dann dieses Backup klonen (Klon2). Nach dem Erstellen von Klon2 ist Klon1 ein Zwischenkon, und Sie können den Klonteilvorgang auf Klon1 nicht ausführen. Sie können jedoch den Vorgang zum Aufteilen von Klonen auf Klon2 durchführen.

  Nach dem Aufteilen von Klon2 können Sie den Clone Split-Vorgang auf Klon1 durchführen, da Klon1 nicht mehr der Zwischenklon ist.

- Wenn Sie einen Klon aufteilen, werden die Backup-Kopien und Klonjobs des Klons gelöscht.
- Informationen zu Einschränkungen für den Klon-Split-Vorgang finden Sie unter "ONTAP 9 Leitfaden für das Management von logischem Storage".
- Stellen Sie sicher, dass das Volume oder Aggregat auf dem Storage-System 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 Ansicht aus:

Option	Beschreibung
Für Datenbankapplikationen	Wählen Sie in der Liste Ansicht die Option **Datenbank** aus.
Für File-Systeme	Wählen Sie in der Liste Ansicht **Pfad** aus.

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

   Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht Manage Copies die geklonte Ressource (z. B. die Datenbank oder die LUN) aus, und klicken Sie dann auf * * .
5. Überprüfen Sie die geschätzte Größe des zu teilenden Klons und den benötigten Speicherplatz auf dem Aggregat, und klicken Sie dann auf **Start**.
6. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

   Der Clone-Splitvorgang reagiert nicht mehr, wenn der SMCore-Dienst neu gestartet wird. Sie sollten das Cmdlet "Stop-SmJob" ausführen, um den Clone-Split-Vorgang zu beenden, und dann den Clone-Split-Vorgang wiederholen.

   Wenn Sie eine längere Abfragzeit oder kürzere Abfragzeit benötigen, um zu prüfen, ob der Klon geteilt ist

oder nicht, können Sie den Wert von *CloneSplitStatusCheckPollTime* Parameter in der Datei *SMCoreServiceHost.exe.config* ändern, um das Zeitintervall für SMCore so einzustellen, dass der Status des Clone Split-Vorgangs angezeigt wird. Der Wert liegt in Millisekunden, und der Standardwert ist 5 Minuten.

Beispiel:

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

Der Startvorgang für die Klontrennung schlägt fehl, wenn gerade Backup-, Wiederherstellungs- oder andere Klonsplitonen durchgeführt werden. Sie sollten den Clone Split-Vorgang erst nach Abschluss der laufenden Vorgänge neu starten.

Weitere Informationen

"Der SnapCenter Klon oder die Überprüfung schlägt fehl, wenn das Aggregat nicht vorhanden ist"

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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