SAP-Geschäftsanwendungs- und SAP HANA-Datenbanklösungen

NetApp solutions for SAP

NetApp
August 19, 2025

This PDF was generated from https://docs.netapp.com/de-de/netapp-solutions-sap/index.html on August 19, 2025. Always check docs.netapp.com for the latest.

Inhalt

SAP-Geschäftsanwendungs- und SAP HANA-Datenbanklösungen . . . 1
Was gibt es Neues bei NetApp Virtualisierungslösungen? . . . 2
18. August 2025 . . . 2
Best Practices In Sich Vereint . . . 3
Technischer Bericht: SAP HANA on NetApp AFF Systems with FCP Configuration Guide . . . 3
Technischer Bericht: SAP HANA on NetApp AFF Systems with Fibre Channel Protocol . . . 3
SAP HANA mit VMware vSphere . . . 4
Der Netapp Architektur Sind . . . 5
Storage-Dimensionierung . . . 9
Einrichtung und Konfiguration der Infrastruktur . . . 15
Wo Sie weitere Informationen finden . . . 52
Aktualisierungsverlauf . . . 53
Konfigurationsleitfaden für SAP HANA auf NetApp AFF-Systemen mit NFS . . . 54
SAP HANA on NetApp AFF Systems with NFS - Konfigurationsleitfaden . . . 54
Der Netapp Architektur Sind . . . 56
Storage-Dimensionierung . . . 61
Einrichtung und Konfiguration der Infrastruktur . . . 67
Wo Sie weitere Informationen finden . . . 97
Aktualisierungsverlauf . . . 98
Technischer Bericht: SAP HANA on NetApp ASA Systems with FCP Configuration Guide . . . 99
Technischer Bericht: SAP HANA on NetApp ASA Systems with Fibre Channel Protocol . . . 99
SAP HANA mit VMware vSphere . . . 100
Der Netapp Architektur Sind . . . 100
Storage-Dimensionierung . . . 104
Einrichtung und Konfiguration der Infrastruktur . . . 109
Wo Sie weitere Informationen finden . . . 144
Aktualisierungsverlauf . . . 145
Konfigurationsleitfaden für SAP HANA auf NetApp FAS-Systemen mit NFS . . . 145
Leitfaden für SAP HANA auf NetApp FAS-Systemen mit NFS-Konfiguration . . . 145
Der Netapp Architektur Sind . . . 148
Storage-Dimensionierung . . . 153
Einrichtung und Konfiguration der Infrastruktur . . . 159
Wo Sie weitere Informationen finden . . . 190
Aktualisierungsverlauf . . . 191
Konfigurationsleitfaden für SAP HANA auf FAS-Systemen mit FCP . . . 192
Konfigurationsleitfaden: SAP HANA auf NetApp FAS Systemen mit Fibre Channel Protocol . . . 192
Der Netapp Architektur Sind . . . 194
Storage-Dimensionierung . . . 199
Einrichtung und Konfiguration der Infrastruktur . . . 204
Wo Sie weitere Informationen finden . . . 244
Aktualisierungsverlauf . . . 245
Backup, Restore und Disaster Recovery . . . 246
SAP HANA auf Amazon FSX für NetApp ONTAP – Backup und Recovery mit SnapCenter . . . 246

TR-4926: SAP HANA auf Amazon FSX für NetApp ONTAP – Backup und Recovery mit SnapCenter . 246
Backup und Recovery mit Amazon FSX für ONTAP . 246
Architektur von SnapCenter . 251
SnapCenter-Konfiguration . 257
SnapCenter-Backup-Vorgänge . 273
Backup nicht datenmengen . 283
Restore und Recovery . 290
Backup-Replizierung mit SnapVault . 298
Wo Sie weitere Informationen finden . 312
Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter . 313
TR-4614: SAP HANA Backup und Recovery mit SnapCenter . 313
Architektur von SnapCenter . 318
SnapCenter SAP HANA Backup-Lösung . 319
SnapCenter-Konzepte und Best Practices . 323
Lab-Einrichtung für diesen Bericht . 342
SnapCenter-Konfiguration . 344
Erstkonfiguration von SnapCenter . 345
Ressourcenspezifische SnapCenter Konfiguration für SAP HANA Datenbank-Backups . 358
Ressourcenspezifische SnapCenter Konfiguration für Backups außerhalb von Datenvolumen . 377
Datenbank-Backups . 382
Block-Integritätsprüfung . 391
Restore und Recovery . 395
Erweiterte Konfiguration und Optimierung . 450
Wo finden Sie weitere Informationen und Versionsverlauf . 458
SAP HANA Datensicherung und Hochverfügbarkeit mit SnapCenter, SnapMirror Active Sync und VMware Metro Storage Cluster . 460
SAP HANA Datensicherung und Hochverfügbarkeit mit SnapCenter, SnapMirror Active Sync und VMware Metro Storage Cluster . 460
Überblick über die Hochverfügbarkeit mit SAP HANA . 461
Beispiel für eine Konfigurationsübersicht . 464
HANA-Systembereitstellung und -Installation . 465
Konfiguration der aktiven SnapMirror-Synchronisierung . 473
SnapCenter-Konfiguration . 479
SnapCenter-Backup-Vorgänge . 484
SnapCenter Restore und Recovery . 487
Aktualisierung des SAP-Systems . 489
Nicht datenbasierte SnapCenter-Volumes . 489
Failover-Szenarien . 491
Zusätzliche Informationen und Versionsverlauf . 495
SAP HANA-Datenschutz mit SnapCenter mit VMware VMFS und NetApp ASA -Systemen . 496
SAP HANA-Datenschutz mit SnapCenter mit VMware VMFS und NetApp ASA -Systemen . 496
Für dieses Dokument verwendeter Laboraufbau . 496
HANA-Systembereitstellung und -Installation . 497
HANA-Konfiguration . 504
SnapCenter-Konfiguration . 505

Backup-Vorgänge . . . 512
Restore- und Recovery-Vorgänge . . . 515
SAP-Systemaktualisierung . . . 519
Zusätzliche Informationen und Versionsverlauf . . . 529
BlueXP Backup and Recovery for SAP HANA – Cloud-Objekt-Storage als Backup-Ziel . . . 530
BlueXP Backup and Recovery for SAP HANA – Cloud-Objekt-Storage als Backup-Ziel . . . 530
Konfigurieren von BlueXP Backup und Recovery für SAP HANA . . . 532
Wiederherstellung von SAP HANA BlueXP Backup . . . 549
Zusätzliche Informationen und Versionsverlauf . . . 552
SAP HANA System Replication Backup und Recovery mit SnapCenter . . . 553
TR-4719: SAP HANA System Replication – Backup und Recovery mit SnapCenter . . . 553
Storage Snapshot Backups und SAP System Replication . . . 554
SnapCenter Konfigurationsoptionen für SAP System Replication . . . 555
Konfiguration von SnapCenter 4.6 unter Verwendung einer Ressourcengruppe . . . 557
SnapCenter Konfiguration mit einer einzigen Ressource . . . 568
Wiederherstellung und Recovery von einem auf dem anderen Host erstellten Backup . . . 582
Wo Sie weitere Informationen finden . . . 586
Versionsverlauf . . . 586
Technischer Bericht: SAP HANA Disaster Recovery with Azure NetApp Files . . . 587
TR-4891: SAP HANA Disaster Recovery mit Azure NetApp Files . . . 587
Disaster-Recovery-Lösungsvergleich . . . 589
ANF: Regionale Replizierung mit SAP HANA . . . 593
Disaster Recovery-Tests . . . 606
Disaster-Recovery-Failover . . . 619
Aktualisierungsverlauf . . . 631
TR-4646: SAP HANA Disaster Recovery with Storage Replication . . . 631
TR-4711: SAP HANA Backup and Recovery Using NetApp Storage Systems and CommVault Software . . . 632
SnapCenter Integration für SAP ASE Database . . . 632
Einführung . . . 632
Zusätzliche Informationen und Versionsverlauf . . . 645
SnapCenter Integration für IBM DB2 Database . . . 646
Einführung . . . 646
Beispiel für eine Konfigurationsübersicht . . . 647
Demo-Umgebung . . . 647
Zusätzliche Informationen und Versionsverlauf . . . 654
SnapCenter Integration für SAP MaxDB Datenbank . . . 655
Einführung . . . 655
Beispiel für eine Konfigurationsübersicht . . . 655
Demo-Umgebung . . . 656
Softwareversionen . . . 656
MaxDB Volume-Design . . . 656
Schritte zum Schutz von Datenbank M02 . . . 657
Voraussetzungen auf Host . . . 657
Voraussetzungen für die Datenbank – Backup-Vorlagen erstellen, Logbackup aktivieren . . . 658
Bereitstellung von SnapCenter-Agent für das Hosting von sap-lnx25 . . . 658

Erstellen Sie eine SnapCenter-Ressourcenkonfiguration für Datenbank M02 . . . 659
Sequenz zum Wiederherstellen von System M02 . . . 666
Instanz M02 wiederherstellen . . . 666
Zusätzliche Informationen und Versionsverlauf . . . 672
Lifecycle Management . . . 673
NetApp Integration des SAP Landscape Managements mit Ansible . . . 673
TR-4953: NetApp SAP Landscape Management Integration Using Ansible . . . 673
SAP Szenarien für Klonen, Kopieren und Aktualisieren von Systemen . . . 673
Anwendungsfälle für Systemaktualisierung, Kopie und Klonen . . . 674
Integration von NetApp SAP Lama mithilfe von Ansible . . . 677
Beispiel für eine Implementierung . . . 678
Workflow zur Bereitstellung von SAP Lama – Klon-System . . . 683
Workflow zur Deprovisionierung von SAP Lama – Systemzerstöre . . . 691
Workflow zur Bereitstellung von SAP Lama – Kopiersystem . . . 694
SAP Lama-Bereitstellungs-Workflow – Systemaktualisierung . . . 698
Provider-Skriptkonfiguration und Ansible Playbooks . . . 700
Schlussfolgerung . . . 713
Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter . . . 714
TR-4667: Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter . . . 714
SAP Szenarien für Systemkopie, Aktualisierung und Klonen . . . 716
Anwendungsfälle für Systemaktualisierung und Klonen . . . 717
Unterstützte Infrastruktur und Szenarien . . . 720
Überblick über den Workflow zur SAP Systemaktualisierung mit SnapCenter . . . 721
Überblick über den SAP Systemklonen-Workflow mit SnapCenter . . . 723
Überlegungen zu Systemaktualisierungen für SAP HANA mit Storage-Snapshot-Backups . . . 724
Beispielskripte zur Automatisierung . . . 729
Systemaktualisierung für SAP HANA mit SnapCenter . . . 732
SAP Systemklon mit SnapCenter . . . 758
Wo finden Sie weitere Informationen und Versionsverlauf . . . 772
Automatisierung von SAP-Systemkopievorgängen mit Libelle SystemCopy . . . 772
TR-4929: Automatisierung von Kopiervorgängen für SAP-Systeme mit Libelle SystemCopy . . . 772
Systemaktualisierung für SAP HANA mit LSC und SnapCenter . . . 775
Systemaktualisierung für SAP HANA mit LSC, AzACSnap und Azure NetApp Files . . . 789
Wo finden Sie weitere Informationen und Versionsverlauf . . . 802
Lösungen Im Überblick . . . 804
SB-3978: Lifecycle Management für SAP HANA . . . 804
SB-3965: Backup und Wiederherstellung für SAP HANA . . . 804
Die Herausforderung . . . 804
Die Lösung . . . 804
SB-3968: Disaster Recovery für SAP HANA . . . 804
Die Herausforderung . . . 804
Die Lösung . . . 805
SB-4292: SAP-Automatisierung mit Ansible . . . 805
Lösungsüberblick . . . 805
Schlussfolgerung . . . 808

Wo Sie weitere Informationen finden . . . 809
Versionsverlauf . . . 809
SB-4293: Automatisieren von SAP-Systemkopien, -Aktualisierungen und -Klonworkflows mit ALPACA und NetApp SnapCenter . . . 809
Lösungsüberblick . . . 809
Schlussfolgerung . . . 814
Wo Sie weitere Informationen finden . . . 814
Versionsverlauf . . . 814
SB-4294: Automatisieren von Kopieren, Aktualisieren und Klonen von SAP Systemen mit Avantra und NetApp SnapCenter . . . 814
Lösungsüberblick . . . 814
Schlussfolgerung . . . 818
Wo Sie weitere Informationen finden . . . 819
Versionsverlauf . . . 819
Rechtliche Hinweise . . . 820
Urheberrecht . . . 820
Marken . . . 820
Patente . . . 820
Datenschutzrichtlinie . . . 820

SAP-Geschäftsanwendungs- und SAP HANA-Datenbanklösungen

Was gibt es Neues bei NetApp Virtualisierungslösungen?

Informieren Sie sich über Neuigkeiten zu Lösungen für SAP.

18. August 2025

Die NetApp Solutions-Site ist jetzt die"NetApp Lösungsfamilie" , das die folgenden Websites umfasst:

- "NetApp Lösungen für künstliche Intelligenz"
- "NetApp Container-Lösungen"
- "NetApp Datenmanagementlösungen"
- "NetApp Datenbanklösungen"
- "NetApp Public- und Hybrid-Cloud-Lösungen"
- NetApp Lösungen für SAP
- "NetApp Virtualisierungslösungen"

Best Practices In Sich Vereint

Technischer Bericht: SAP HANA on NetApp AFF Systems with FCP Configuration Guide

Technischer Bericht: SAP HANA on NetApp AFF Systems with Fibre Channel Protocol

Die NetApp AFF Produktfamilie ist für die Verwendung mit SAP HANA in TDI Projekten zertifiziert. Dieser Leitfaden enthält Best Practices für SAP HANA auf dieser Plattform für FCP.

Marco Schoen, NetApp

Einführung

Die NetApp AFF/ ASA A-Series-Produktfamilie wurde für den Einsatz mit SAP HANA in maßgeschneiderten Data Center Integration (TDI)-Projekten zertifiziert.

Diese Zertifizierung gilt für folgende Modelle:

- AFF A20, AFF A30, AFF A50, AFF A70, AFF A90, AFF A1K

Eine vollständige Liste der zertifizierten NetApp Storage-Lösungen für SAP HANA finden Sie unter "Zertifiziertes und unterstütztes SAP HANA-Hardwaresverzeichnis".

In diesem Dokument werden die AFF-Konfigurationen beschrieben, die das Fibre Channel Protocol (FCP) verwenden.

> Die in diesem Dokument beschriebene Konfiguration ist erforderlich, um die erforderlichen SAP HANA KPIs und die beste Performance für SAP HANA zu erreichen. Wenn Sie Einstellungen oder Funktionen ändern, die nicht in diesem Dokument aufgeführt sind, kann dies zu einer Performance-Verschlechterung oder zu einem unerwarteten Verhalten führen. Diese Einstellungen sollten nur vorgenommen werden, wenn dies durch den NetApp Support empfohlen wird.

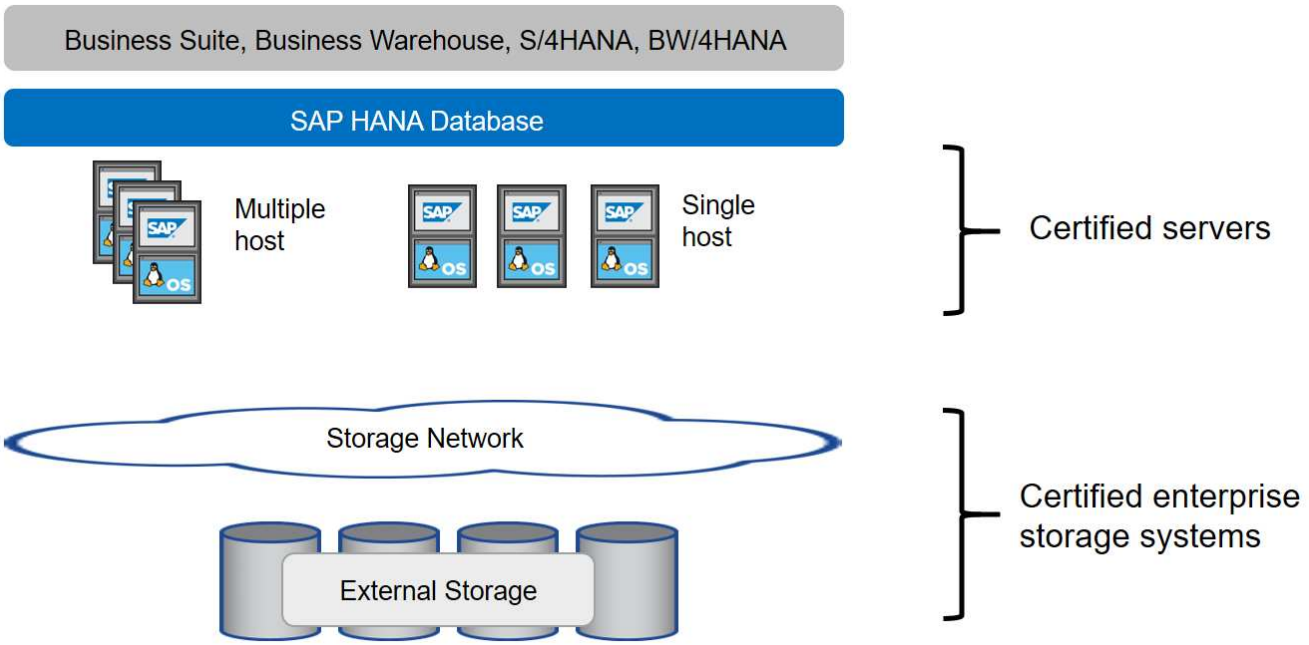
Die Konfigurationsleitfäden für AFF Systeme mit NFS und NetApp FAS Systemen können über die folgenden Links gefunden werden:

- "Technischer Bericht: SAP HANA on NetApp FAS Systems with FCP"
- "Technischer Bericht: SAP HANA on NetApp ASA Systems with FCP"
- "Technischer Bericht: SAP HANA on NetApp FAS Systems with NFS"
- "Technischer Bericht: SAP HANA on NetApp AFF Systems with NFS"

In einer SAP HANA Umgebung mit mehreren Hosts wird der standardmäßige SAP HANA-Storage-Connector verwendet, um im Falle eines Failover des SAP HANA-Hosts zu Fechten. Beachten Sie immer die relevanten SAP-Hinweise für Konfigurationsrichtlinien für Betriebssysteme und HANA-spezifische Linux-Kernel-Abhängigkeiten. Weitere Informationen finden Sie unter "SAP Note 2235581 – von SAP HANA unterstützte Betriebssysteme".

SAP HANA Tailored Datacenter Integration

NetApp AFF Storage-Systeme sind im SAP HANA TDI Programm mit NFS- (NAS) und FC (SAN) Protokollen zertifiziert. Sie können in allen aktuellen SAP HANA-Szenarien, wie SAP Business Suite on HANA, S/4HANA, BW/4HANA oder SAP Business Warehouse on HANA, entweder in Konfigurationen mit einem Host oder mehreren Hosts implementiert werden. Alle Server, die für den Einsatz mit SAP HANA zertifiziert sind, können mit von NetApp zertifizierten Storage-Lösungen kombiniert werden. Die folgende Abbildung bietet einen Überblick über die Architektur.



Weitere Informationen zu den Voraussetzungen und Empfehlungen für produktive SAP HANA-Systeme finden Sie in der folgenden Ressource:

- "SAP HANA Tailored Data Center Integration Häufig gestellte Fragen"

SAP HANA mit VMware vSphere

Es stehen verschiedene Optionen zur Verbindung von Storage mit Virtual Machines (VMs) zur Verfügung. Der bevorzugte Modus ist die direkte Verbindung der Storage Volumes mit NFS vom Gastbetriebssystem. Diese Option ist in beschrieben"Technischer Bericht: SAP HANA on NetApp AFF Systems with NFS".

Auch Raw Device Mapping (RDM), FCP Datastores oder VVOL Datastores mit FCP werden unterstützt. Bei beiden Datastore-Optionen muss für produktive Anwendungsfälle nur eine SAP HANA Daten oder ein Protokoll-Volume im Datastore gespeichert werden.

Weitere Informationen zur Verwendung von vSphere mit SAP HANA finden Sie unter den folgenden Links:

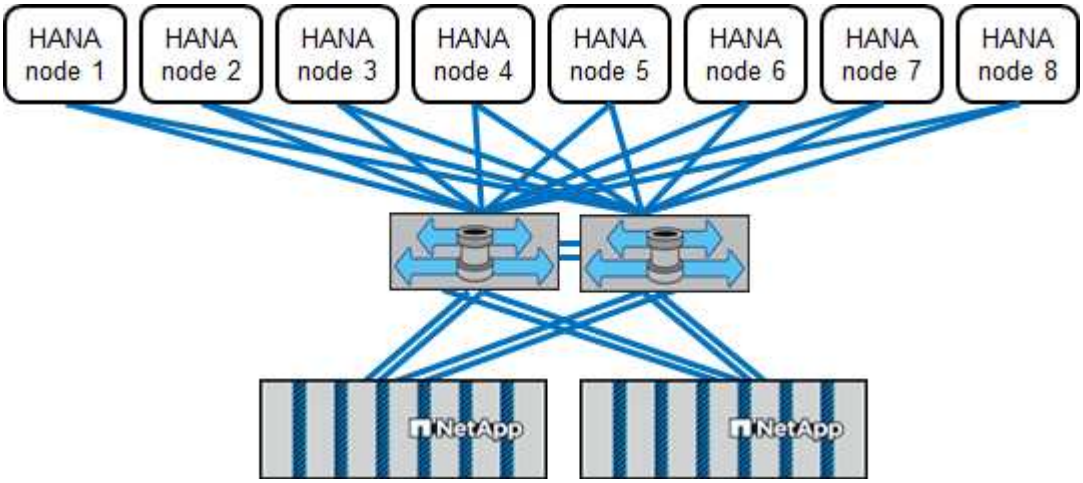
- "SAP HANA on VMware vSphere - Virtualization - Community Wiki"
- "Best Practices Guide für SAP HANA auf VMware vSphere"
- "2161991 - Konfigurationsrichtlinien für VMware vSphere - SAP ONE Support Launchpad (Anmeldung erforderlich)"

Der Netapp Architektur Sind

SAP HANA Hosts sind über eine redundante FCP-Infrastruktur und Multipathing-Software mit Storage Controllern verbunden. Eine redundante FCP Switch-Infrastruktur ist erforderlich, um eine fehlertolerante SAP HANA Host-zu-Storage-Konnektivität bei Ausfall von Switch oder Host Bus Adapter (HBA) bereitzustellen. Ein entsprechendes Zoning muss am Switch konfiguriert werden, damit alle HANA Hosts die erforderlichen LUNs auf den Storage Controllern erreichen können.

Verschiedene Modelle der AFF Produktfamilie können auf der Storage-Ebene miteinander kombiniert werden, um Wachstum und unterschiedliche Anforderungen an Performance und Kapazität zu ermöglichen. Die maximale Anzahl an SAP HANA-Hosts, die an das Storage-System angeschlossen werden können, sind durch die SAP HANA-Performance-Anforderungen und das Modell des verwendeten NetApp Controllers definiert. Die Anzahl der benötigten Festplatten-Shelfs wird nur von den Kapazitäts- und Performance-Anforderungen der SAP HANA Systeme bestimmt.

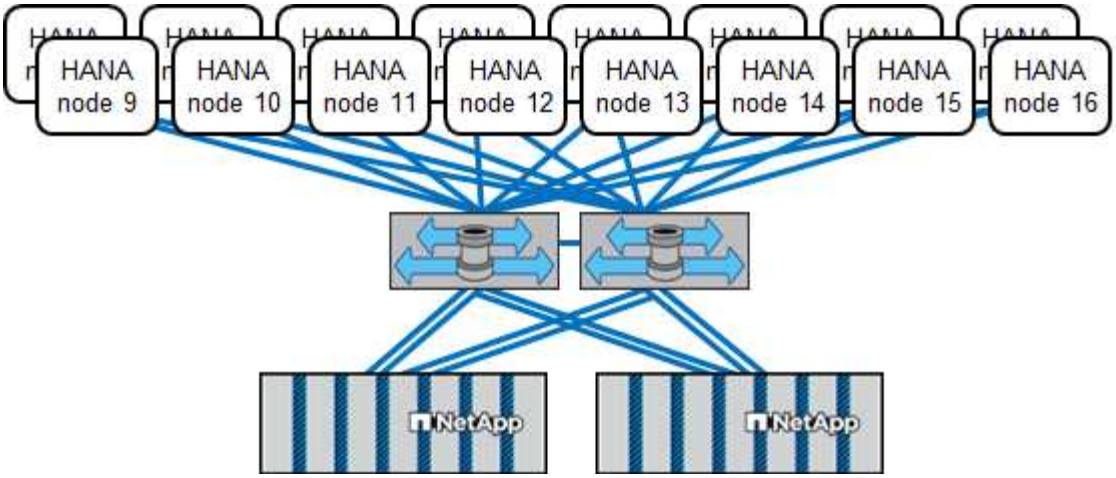
Die folgende Abbildung zeigt eine Beispielkonfiguration mit acht SAP HANA-Hosts, die an ein Storage HA-Paar angeschlossen sind.



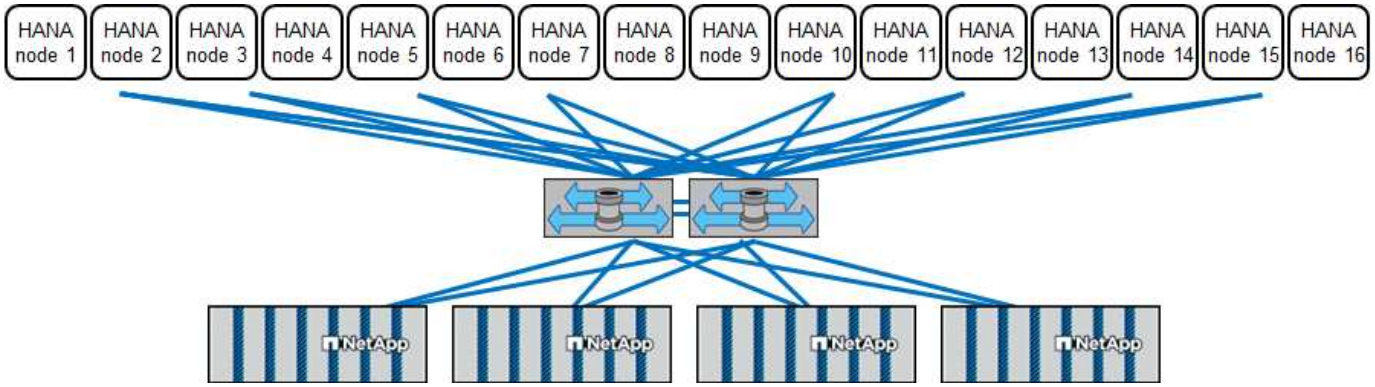
Diese Architektur lässt sich in zwei Dimensionen skalieren:

- Indem zusätzliche SAP HANA-Hosts und Storage-Kapazität an den vorhandenen Storage angeschlossen werden, können die Storage-Controller genügend Performance bieten, um die aktuellen SAP HANA-KPIs zu erfüllen
- Durch Hinzufügen weiterer Storage-Systeme mit zusätzlicher Storage-Kapazität für die zusätzlichen SAP HANA-Hosts

Die folgende Abbildung zeigt ein Konfigurationsbeispiel, in dem mehr SAP HANA-Hosts mit den Storage-Controllern verbunden sind. In diesem Beispiel sind mehr Platten-Shelves erforderlich, um die Kapazitäts- und Performance-Anforderungen der 16 SAP HANA-Hosts zu erfüllen. Abhängig von den Anforderungen an den Gesamtdurchsatz müssen die Storage Controller um zusätzliche FC-Verbindungen erweitert werden.



Unabhängig vom implementierten AFF System lässt sich die SAP HANA Landschaft auch skalieren, indem beliebige zertifizierte Storage-Controller hinzugefügt werden, um die gewünschte Node-Dichte zu erfüllen, wie in der folgenden Abbildung dargestellt.



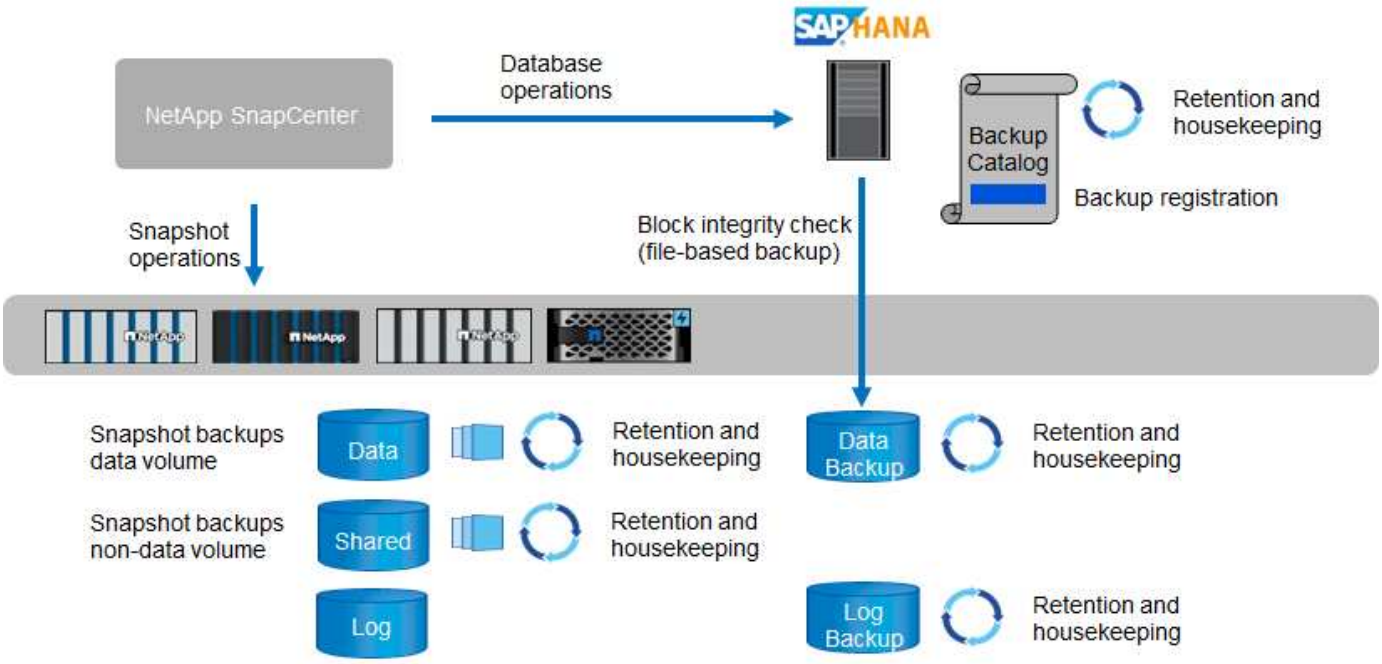
SAP HANA Backup

Die auf allen NetApp Storage-Controllern vorhandene ONTAP Software bietet einen integrierten Mechanismus zur Sicherung von SAP HANA Datenbanken, ohne die Performance zu beeinträchtigen. Storage-basierte NetApp Snapshot-Backups sind eine vollständig unterstützte und integrierte Backup-Lösung, die für einzelne SAP HANA Container sowie für SAP HANA MDC-Systeme mit einem einzelnen Mandanten oder mehreren Mandanten verfügbar ist.

Storage-basierte Snapshot Backups werden über das NetApp SnapCenter Plug-in für SAP HANA implementiert. Benutzer können auf diese Weise konsistente Storage-basierte Snapshot Backups mithilfe der Schnittstellen erstellen, die nativ von SAP HANA Datenbanken bereitgestellt werden. SnapCenter registriert jedes der Snapshot-Backups im SAP HANA-Backup-Katalog. Backups von SnapCenter sind somit innerhalb von SAP HANA Studio oder im Cockpit sichtbar, wo sie direkt für Restore- und Recovery-Vorgänge selektiert werden können.

Mit der NetApp SnapMirror Technologie können Snapshot Kopien, die auf einem Storage-System erstellt wurden, in ein sekundäres Backup-Storage-System repliziert werden, das über SnapCenter gesteuert wird. Für jedes der Backup-Sätze auf dem primären Storage und auch für die Backup-Sets auf den sekundären Storage-Systemen können somit unterschiedliche Backup-Aufbewahrungsrichtlinien definiert werden. Das SnapCenter Plug-in für SAP HANA managt automatisch die Aufbewahrung von auf Snapshot Kopien basierenden Daten-Backups und Log-Backups, einschließlich der allgemeinen Ordnung des Backup-Katalogs. Das SnapCenter Plug-in für SAP HANA ermöglicht darüber hinaus die Ausführung einer Blockintegritätsprüfung der SAP HANA-Datenbank durch Ausführen eines dateibasierten Backups.

Die Datenbankprotokolle können mithilfe eines NFS-Mount-Speichers direkt auf dem sekundären Storage gesichert werden, wie in der folgenden Abbildung dargestellt.



Storage-basierte Snapshot Backups bieten im Vergleich zu herkömmlichen dateibasierten Backups deutliche Vorteile. Zu diesen Vorteilen zählen unter anderem:

- Schnelleres Backup (einige Minuten)
- Reduzierte RTO aufgrund einer wesentlich schnelleren Restore-Zeit auf der Storage-Ebene (wenige Minuten) und häufigerer Backups
- Kein Performance-Abfall des SAP HANA-Datenbankhosts, -Netzwerks oder -Storage während Backup- und Recovery-Vorgängen
- Platzsparende und bandbreiteneffiziente Replizierung auf Basis von Blockänderungen auf sekundärem Storage

Weitere Informationen zur Backup- und Recovery-Lösung von SAP HANA finden Sie unter "TR-4614: SAP HANA Backup and Recovery with SnapCenter".

Disaster Recovery für SAP HANA

Das Disaster Recovery für SAP HANA ist entweder auf der Datenbankebene mithilfe von SAP HANA-Systemreplizierung oder auf der Storage-Ebene mithilfe von Storage-Replizierungstechnologien möglich. Der folgende Abschnitt bietet einen Überblick über Disaster-Recovery-Lösungen basierend auf der Storage-Replizierung.

Weitere Informationen zu den Disaster-Recovery-Lösungen für SAP HANA finden Sie unter "TR-4646: SAP HANA Disaster Recovery with Storage Replication".

Storage-Replizierung basierend auf SnapMirror

Die folgende Abbildung zeigt eine Disaster-Recovery-Lösung für drei Standorte mit synchroner SnapMirror Active Sync zum lokalen DR-Rechenzentrum und asynchroner SnapMirror zur Replikation der Daten in das Remote-DR-Rechenzentrum. SnapMirror Active Sync ermöglicht die Weiterführung von Geschäftsdiensten auch bei einem kompletten Standortausfall und unterstützt ein transparentes Failover von Anwendungen

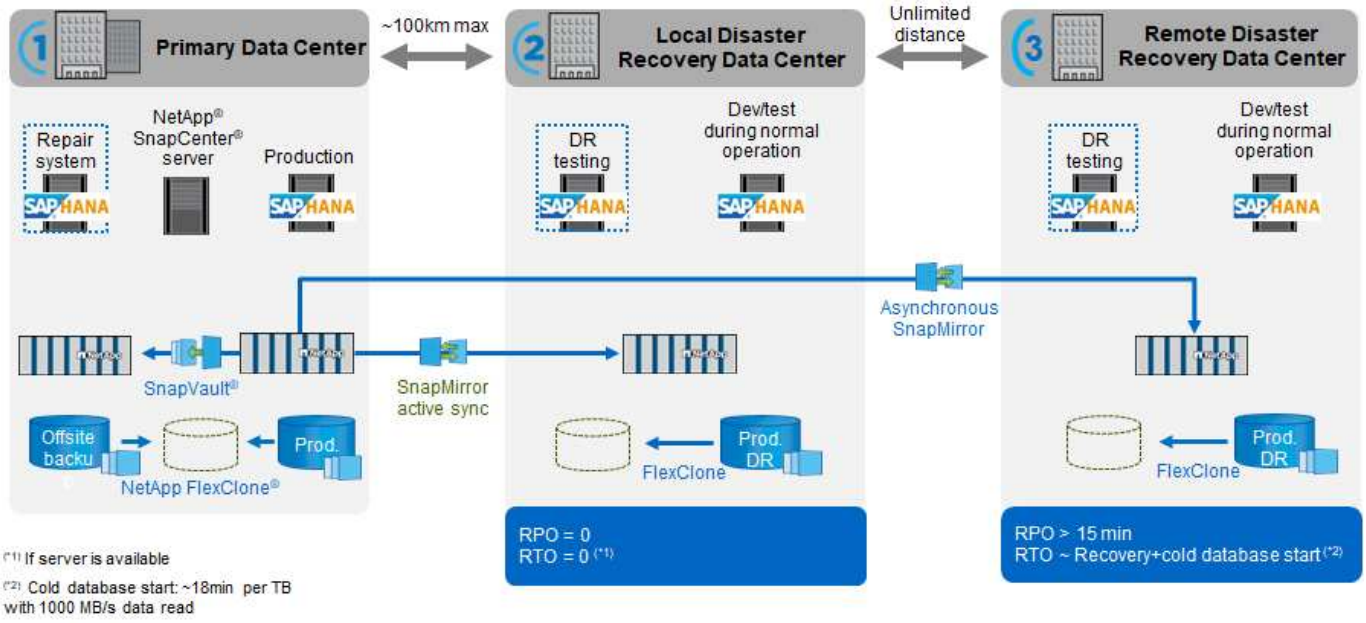
mithilfe einer sekundären Kopie (RPO=0 und RTO=0). Für die Auslösung eines Failover mit SnapMirror Active Sync sind keine manuellen Eingriffe oder benutzerdefinierten Skripts erforderlich. Ab ONTAP 9.15.1 unterstützt die SnapMirror Active Sync symmetrische aktiv/aktiv-Funktion. Symmetrische aktiv/aktiv-Konfiguration ermöglicht I/O-Vorgänge für Lese- und Schreibvorgänge von beiden Kopien einer geschützten LUN mit bidirektionaler synchroner Replizierung, sodass beide LUN-Kopien lokal für I/O-Vorgänge sorgen können.

Weitere Details finden Sie unter "Übersicht über die aktive SnapMirror-Synchronisierung in ONTAP".

Die RTO für die asynchrone SnapMirror-Replikation hängt in erster Linie von der Zeit ab, die zum Starten der HANA-Datenbank am DR-Standort und zum Laden der Daten in den Speicher benötigt wird. Mit der Annahme, dass die Daten mit einem Durchsatz von 1000 MBit/s gelesen werden, dass das Laden von 1 TB Daten ungefähr 18 Minuten dauert.

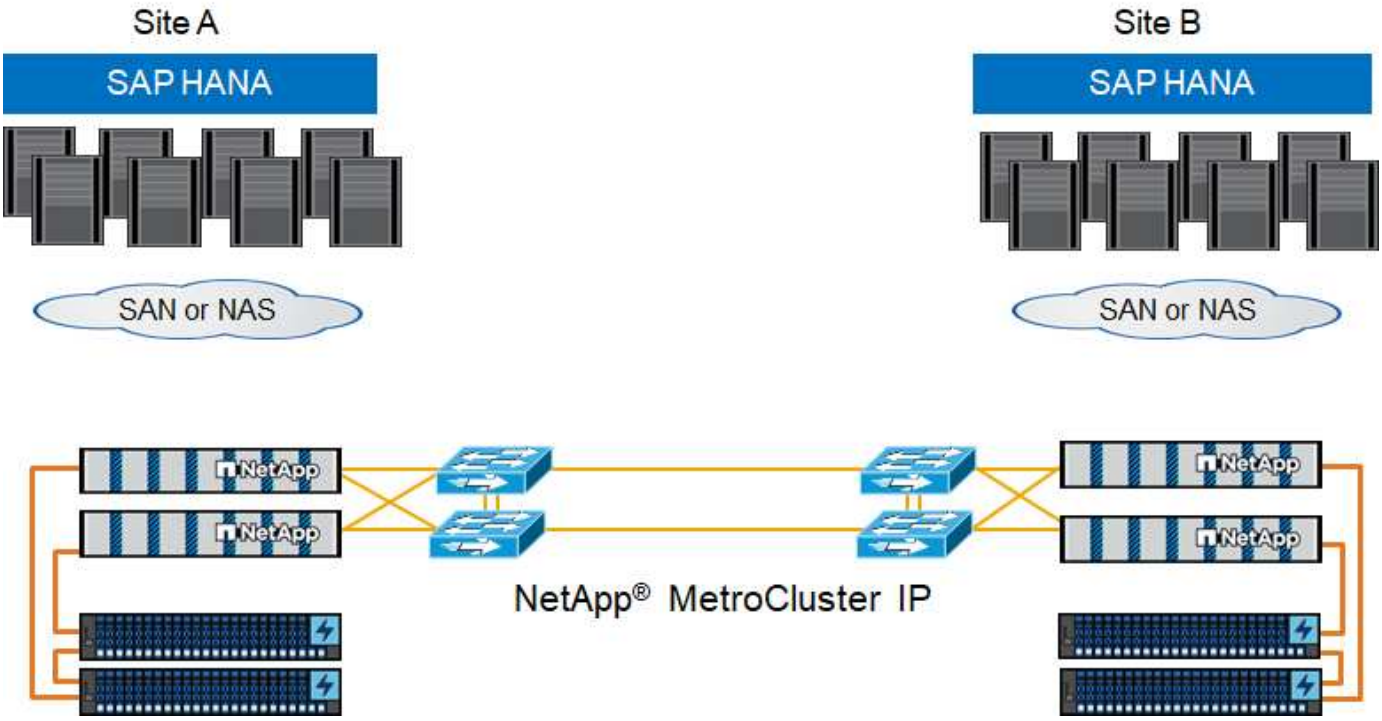
Die Server an den DR-Standorten können im normalen Betrieb als Entwicklungs- und Testsysteme genutzt werden. Bei einem Ausfall müssten die Entwicklungs- und Testsysteme heruntergefahren und als DR-Produktionsserver gestartet werden.

Beide Replizierungsmethoden ermöglichen die Durchführung von DR-Workflow-Tests ohne Auswirkungen auf RPO und RTO. FlexClone Volumes werden auf dem Storage erstellt und an die DR-Testserver angeschlossen.



Storage-Replizierung basierend auf NetApp MetroCluster

Die folgende Abbildung bietet einen allgemeinen Überblick über die Lösung. Das Storage-Cluster an jedem Standort bietet lokale Hochverfügbarkeit und wird für den Produktions-Workload verwendet. Die Daten aller Standorte werden synchron zum anderen Standort repliziert und sind im Fall eines Disaster Failovers verfügbar.



Storage-Dimensionierung

Der folgende Abschnitt bietet einen Überblick über die Performance- und Kapazitätsüberlegungen, die für die Dimensionierung eines Storage-Systems für SAP HANA erforderlich sind.

> Wenden Sie sich an Ihren Vertriebsmitarbeiter von NetApp oder einen NetApp Partner, um den Prozess der Storage-Größenbemessung zu unterstützen und Ihnen beim Aufbau einer optimal dimensionierten Storage-Umgebung zu helfen.

Überlegungen zur Performance

SAP hat einen statischen Satz von Storage Key Performance-Indikatoren definiert. Diese KPIs sind für alle produktiven SAP HANA-Umgebungen gültig, unabhängig von der Speichergröße der Datenbank-Hosts und der Anwendungen, die die SAP HANA-Datenbank nutzen. Diese KPIs gelten für Single-Host-, mehrere Hosts-, Business Suite on HANA-, Business Warehouse on HANA-, S/4HANA- und BW/4HANA-Umgebungen. Daher hängt der aktuelle Ansatz zur Performance-Dimensionierung nur von der Anzahl aktiver SAP HANA-Hosts ab, die an das Storage-System angeschlossen sind.

> Storage-Performance-KPIs sind nur für SAP HANA Produktionssysteme erforderlich, können aber in allen HANA-Systemen implementiert werden.

SAP liefert ein Performance-Testtool, das zur Validierung der Storage-Systemperformance der am Storage angeschlossenen aktiven SAP HANA Hosts verwendet werden muss.

NetApp hat die maximale Anzahl an SAP HANA Hosts getestet und vordefiniert, die an ein bestimmtes Storage-Modell angeschlossen werden können, während gleichzeitig die erforderlichen Storage-KPIs von SAP für produktionsbasierte SAP HANA Systeme erfüllt werden.

Mit dem SAP Performance-Testtool wurde die maximale Anzahl an SAP HANA Hosts ermittelt, die in einem

Platten-Shelf ausgeführt werden können und die Mindestanzahl der pro SAP HANA Host benötigten SSDs erforderlich ist. Dieser Test berücksichtigt nicht die tatsächlichen Storage-Kapazitätsanforderungen der Hosts. Außerdem müssen die Kapazitätsanforderungen berechnet werden, um die tatsächlich benötigte Storage-Konfiguration zu bestimmen.

SAS-Festplatten-Shelf

Das 12-GB-SAS-Festplatten-Shelf (DS224C) sorgt für das Performance-Sizing mit festen Festplatten-Shelf-Konfigurationen:

- Halb beladene Festplatten-Shelfs mit 12 SSDs
- Voll beladene Festplatten-Shelfs mit 24 SSDs

Beide Konfigurationen verwenden die erweiterte Laufwerkpartitionierung (Advanced Drive Partitioning, ADPv2). Ein halb beladenes Platten-Shelf unterstützt bis zu 9 SAP HANA-Hosts. Ein voll beladenes Shelf unterstützt bis zu 14 Hosts in einem einzigen Platten-Shelf. Die SAP HANA-Hosts müssen auf beide Storage Controller verteilt sein.

Das DS224C Festplatten-Shelf muss über 12 GB SAS verbunden werden, um die Anzahl von SAP HANA Hosts zu unterstützen.

Das 6-Gbit-SAS-Platten-Shelf (DS2246) unterstützt maximal 4 SAP HANA Hosts. Die SSDs und SAP HANA-Hosts müssen auf beide Storage-Controller verteilt sein. In der folgenden Abbildung ist die unterstützte Anzahl von SAP HANA-Hosts pro Festplatten-Shelf zusammengefasst.

	6-Gbit-SAS-Shelfs (DS2246) mit voller Betriebslast 24 SSDs	**12-GB-SAS-Shelfs (DS224C) mit 12 SSDs und ADPv2; halber beladen**	**12-GB-SAS-Shelfs (DS224C) mit 24 SSDs und ADPv2 voll beladen**
Maximale Anzahl von SAP HANA-Hosts pro Festplatten-Shelf	4	9	14

Diese Berechnung erfolgt unabhängig vom eingesetzten Storage Controller. Durch das Hinzufügen weiterer Platten-Shelves wird nicht die maximale Anzahl von SAP HANA-Hosts erhöht, die ein Storage-Controller unterstützen kann.

NS224 NVMe-Shelf

Eine NVMe-SSD (Daten) unterstützt bis zu 2/5 SAP HANA-Hosts, je nachdem, welche NVMe-Festplatte verwendet wird. Die SSDs und SAP HANA-Hosts müssen auf beide Storage-Controller verteilt sein. Gleiches gilt für die internen NVMe-Festplatten von AFF und ASA Systemen.

Durch das Hinzufügen weiterer Platten-Shelves wird nicht die maximale Anzahl von SAP HANA-Hosts erhöht, die ein Storage-Controller unterstützen kann.

Heterogenen Workloads

SAP HANA und andere Applikations-Workloads werden auf demselben Storage Controller oder im selben Storage-Aggregat unterstützt. Es ist jedoch eine NetApp Best Practice, SAP HANA-Workloads von allen anderen Applikations-Workloads zu trennen.

SAP HANA-Workloads und andere Applikations-Workloads können entweder auf demselben Storage-Controller oder demselben Aggregat implementiert werden. Falls ja, müssen Sie sicherstellen, dass in der Umgebung mit heterogenen Workloads für SAP HANA eine ausreichende Performance verfügbar ist. NetApp empfiehlt außerdem, Parameter für Quality of Service (QoS) zu verwenden, um die Auswirkungen anderer Applikationen auf SAP HANA Applikationen zu regulieren und den Durchsatz für SAP HANA Applikationen zu garantieren.

Das SAP HCMT-Testtool muss verwendet werden, um zu prüfen, ob zusätzliche SAP HANA Hosts auf einem vorhandenen Storage Controller ausgeführt werden können, der bereits für andere Workloads verwendet wird. SAP Applikations-Server können wie die SAP HANA Datenbanken sicher auf demselben Storage Controller und/oder Aggregat platziert werden.

Überlegungen zur Kapazität

Eine detaillierte Beschreibung der Kapazitätsanforderungen für SAP HANA ist im "SAP-Hinweis 1900823" Whitepaper:

> Das Kapazitätsdimensionieren der gesamten SAP Landschaft mit mehreren SAP HANA Systemen muss mithilfe von SAP HANA Storage-Größenanpassungs-Tools von NetApp ermittelt werden. Wenden Sie sich an NetApp oder Ihren Ansprechpartner bei NetApp Partnern, um den Prozess der Storage-Größenbemessung für eine ausreichend dimensionierte Storage-Umgebung zu validieren.

Konfiguration des Performance-Testtool

Ab SAP HANA 1.0 SPS10 führte SAP Parameter ein, um das I/O-Verhalten anzupassen und die Datenbank für das verwendete Datei- und Speichersystem zu optimieren. Diese Parameter müssen auch für das Performance-Test-Tool von SAP eingestellt werden, wenn die Storage-Performance mit dem SAP-Testtool getestet wird.

NetApp führte Performance-Tests durch, um die optimalen Werte zu ermitteln. In der folgenden Tabelle sind die Parameter aufgeführt, die in der Konfigurationsdatei des SAP-Testwerkzeugs festgelegt werden müssen.

Parameter	Wert
max_parallel_io_Requests	128
Async_read_Submit	Ein
Async_write_submit_Active	Ein
Async_Write_Submit_Blocks	Alle

Weitere Informationen zur Konfiguration von SAP-Testtool finden Sie unter "SAP-Hinweis 1943937" Für HWCCT (SAP HANA 1.0) und "SAP-Hinweis 2493172" FÜR HCMT/HCOT (SAP HANA 2.0).

Das folgende Beispiel zeigt, wie Variablen für den HCMT/HCOT-Ausführungsplan festgelegt werden können.

```
…
{
          "Comment": "Log Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "LogAsyncReadSubmit",
          "Value": "on",
```

```
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
         "Name": "DataAsyncReadSubmit",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "LogAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "DataAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "LogAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "DataAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "LogExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      },
```

```
      {
         "Comment": "Data Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "DataExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      }, …
```

Diese Variablen müssen für die Testkonfiguration verwendet werden. Dies ist in der Regel bei den vordefinierten Testsuiten der Fall, die SAP mit dem HCMT/HCOT-Tool liefert. Das folgende Beispiel für einen 4k-Protokollschreibtest stammt aus einer Testsuite.

```
…
      {
         "ID": "D664D001-933D-41DE-A904F304AEB67906",
         "Note": "File System Write Test",
         "ExecutionVariants": [
            {
               "ScaleOut": {
                  "Port": "${RemotePort}",
                  "Hosts": "${Hosts}",
                  "ConcurrentExecution": "${FSConcurrentExecution}"
               },
               "RepeatCount": "${TestRepeatCount}",
               "Description": "4K Block, Log Volume 5GB, Overwrite",
               "Hint": "Log",
               "InputVector": {
                  "BlockSize": 4096,
                  "DirectoryName": "${LogVolume}",
                  "FileOverwrite": true,
                  "FileSize": 5368709120,
                  "RandomAccess": false,
                  "RandomData": true,
                  "AsyncReadSubmit": "${LogAsyncReadSubmit}",
                  "AsyncWriteSubmitActive":
"${LogAsyncWriteSubmitActive}",
                  "AsyncWriteSubmitBlocks":
"${LogAsyncWriteSubmitBlocks}",
                  "ExtMaxParallelIoRequests":
"${LogExtMaxParallelIoRequests}",
                  "ExtMaxSubmitBatchSize": "${LogExtMaxSubmitBatchSize}",
                  "ExtMinSubmitBatchSize": "${LogExtMinSubmitBatchSize}",
                  "ExtNumCompletionQueues":
"${LogExtNumCompletionQueues}",
                  "ExtNumSubmitQueues": "${LogExtNumSubmitQueues}",
                  "ExtSizeKernelIoQueue": "${ExtSizeKernelIoQueue}"
               }
            },
…
```

Übersicht über den Prozess zur Storage-Größenbemessung

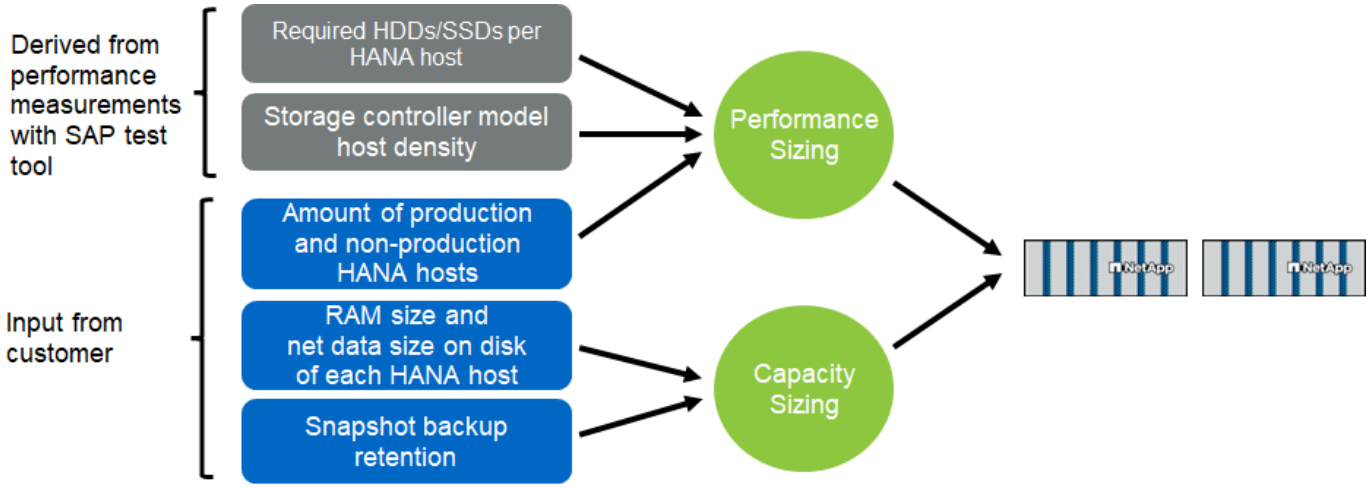
Die Anzahl der Festplatten pro HANA Host und die Host-Dichte für jedes Storage-Modell von SAP HANA wurden mithilfe des Test-Tools ermittelt.

Der Dimensionierungsprozess erfordert Einzelheiten, z. B. die Anzahl der SAP HANA-Hosts in der Produktion und für die Produktion nichtproduktive Umgebung, die RAM-Größe jedes Hosts und die Backup-Aufbewahrung der Storage-basierten Snapshot Kopien. Die Anzahl der SAP HANA-Hosts bestimmt den Storage Controller

und die Anzahl der benötigten Festplatten.

Die Größe des RAM, die Netto-Datengröße auf der Festplatte jedes SAP HANA-Hosts und der Aufbewahrungszeitraum für das Snapshot-Backup werden als Inputs bei der Kapazitätsdimensionierung verwendet.

Die folgende Abbildung fasst den Dimensionierungsprozess zusammen.



Einrichtung und Konfiguration der Infrastruktur

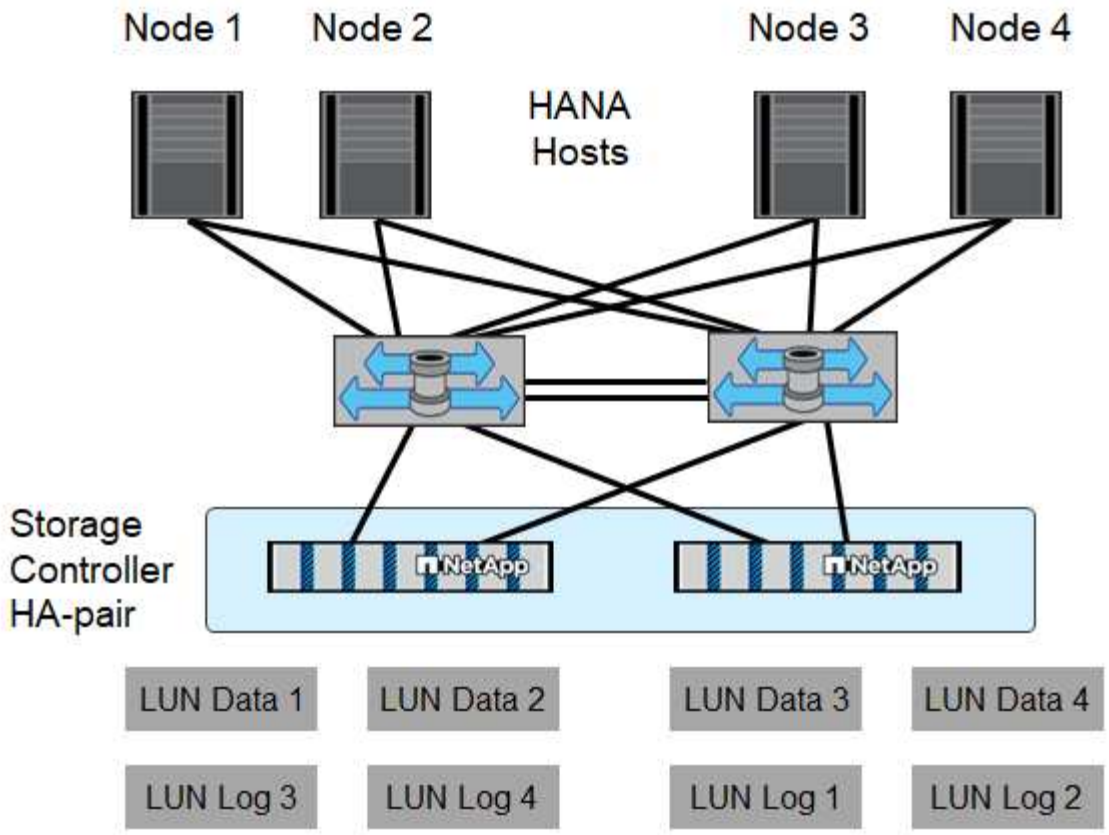
In den folgenden Abschnitten finden Sie Richtlinien zur Einrichtung und Konfiguration der SAP HANA-Infrastruktur sowie alle Schritte zur Einrichtung eines SAP HANA-Systems. In diesen Abschnitten werden die folgenden Beispielkonfigurationen verwendet:

- HANA-System mit SID=FC5
  - SAP HANA Einzel- und Mehrfachhost mit Linux Logical Volume Manager (LVM)
  - SAP HANA Einzelhost mit SAP HANA mehrere Partitionen

EINRICHTUNG VON SAN Fabric

Jeder SAP HANA-Server muss über eine redundante FCP-SAN-Verbindung mit einer Bandbreite von mindestens 8 Gbit/s. Für jeden an einen Storage Controller angeschlossenen SAP HANA-Host muss am Storage Controller mindestens eine Bandbreite von 8 GB/s konfiguriert sein.

Die folgende Abbildung zeigt ein Beispiel mit vier SAP HANA-Hosts, die mit zwei Storage-Controllern verbunden sind. Jeder SAP HANA-Host verfügt über zwei FCP-Ports, die mit der redundanten Fabric verbunden sind. Auf der Storage-Ebene sind vier FCP-Ports so konfiguriert, dass sie den erforderlichen Durchsatz für jeden SAP HANA Host liefern.



Zusätzlich zum Zoning auf der Switch-Ebene müssen Sie jede LUN auf dem Storage-System den Hosts zuordnen, die mit dieser LUN verbunden sind. Einfachheit beim Zoning auf dem Switch; das heißt, Festlegung eines Zoneneinteils, in dem alle Host-HBAs alle Controller-HBAs sehen können.

Zeitsynchronisierung

Sie müssen die Zeit zwischen den Storage-Controllern und den SAP HANA Datenbank-Hosts synchronisieren. Legen Sie dazu denselben Zeitserver für alle Storage Controller und alle SAP HANA-Hosts fest.

Einrichtung von Storage Controllern

In diesem Abschnitt wird die Konfiguration des NetApp Storage-Systems beschrieben. Sie müssen die primäre Installation und Einrichtung gemäß den entsprechenden Data ONTAP Setup- und Konfigurationsleitfäden abschließen.

Storage-Effizienz

In einer SSD-Konfiguration werden Inline-Deduplizierung, Inline-Deduplizierung, Inline-Komprimierung und Inline-Data-Compaction unterstützt.

NetApp FlexGroup Volumes

Die Verwendung von NetApp FlexGroup Volumes wird für SAP HANA nicht unterstützt. Aufgrund der Architektur von SAP HANA bietet die Verwendung von FlexGroup Volumes keinen Vorteil und kann zu Performance-Problemen führen.

NetApp Volume- und Aggregatverschlüsselung

Die Verwendung von NetApp Volume Encryption (NVE) und NetApp Aggregate Encryption (NAE) wird bei SAP HANA unterstützt.

Quality of Service

QoS kann verwendet werden, um den Storage-Durchsatz für bestimmte SAP HANA Systeme oder nicht-SAP Applikationen auf einem Shared Controller zu begrenzen.

Produktion und Entwicklung/Test

Ein Anwendungsfall wäre, den Durchsatz von Entwicklungs- und Testsystemen zu begrenzen, damit sie bei einem gemischten Setup keinen Einfluss auf die Produktionssysteme haben. Während des Dimensionierungsprozesses sollten Sie die Performance-Anforderungen eines nicht für die Produktion verwendeten Systems ermitteln. Entwicklungs- und Testsysteme können mit niedrigeren Leistungswerten dimensioniert werden, typischerweise im Bereich von 20 % bis 50 % eines von SAP definierten Produktionssystems-KPI. Ein großer I/O-Schreibvorgang wirkt sich am stärksten auf die Performance des Storage-Systems aus. Daher sollte die QoS-Durchsatzbegrenzung auf einen Prozentsatz der entsprechenden KPI-Werte für die SAP HANA-Speicherleistung in den Daten- und Protokoll-Volumes gesetzt werden.

Shared-Umgebungen

Ein weiterer Anwendungsfall ist die Einschränkung des Durchsatzes bei umfangreichen Schreib-Workloads, insbesondere um zu vermeiden, dass diese Workloads Auswirkungen auf andere latenzempfindliche Schreib-Workloads haben. In solchen Umgebungen empfiehlt es sich, eine QoS-Gruppenrichtlinie ohne gemeinsam genutzten Durchsatz auf jede LUN innerhalb jeder SVM (Storage Virtual Machine) anzuwenden, um den maximalen Durchsatz jedes einzelnen Storage-Objekts auf den angegebenen Wert zu beschränken. So besteht weniger Gefahr, dass ein einzelner Workload andere Workloads negativ beeinflussen kann.

Dazu muss über die CLI des ONTAP-Clusters für jede SVM eine Gruppenrichtlinie erstellt werden:

```
qos policy-group create -policy-group <policy-name> -vserver <vserver
name> -max-throughput 1000MB/s -is-shared false
```

Und auf jede LUN in der SVM angewendet. Nachfolgend sehen Sie ein Beispiel, um die Richtliniengruppe auf alle vorhandenen LUNs innerhalb einer SVM anzuwenden:

```
lun modify -vserver <vserver name>  -path * -qos-policy-group  <policy-
name>
```

Dies muss für jede SVM geschehen. Der Name der QoS-Polizeigruppe für jede SVM muss unterschiedlich sein. Für neue LUNs kann die Richtlinie direkt angewendet werden:

```
lun create -vserver <vserver_name> -path  /vol/<volume_name>/<lun_name>
-size <size> -ostype <e.g. linux>  -qos-policy-group <policy-name>
```

Es wird empfohlen, 1000 MB/s als maximalen Durchsatz für eine bestimmte LUN zu verwenden. Wenn eine Applikation einen höheren Durchsatz erfordert, müssen mehrere LUNs mit LUN-Striping verwendet werden,

um die erforderliche Bandbreite bereitzustellen. Dieser Leitfaden enthält ein Beispiel für SAP HANA auf Basis von Linux LVM in Abschnitt "Host-Setup".

> Das Limit gilt auch für Lesevorgänge. Daher genügend LUNs verwenden, um die erforderlichen SLAs für die Startzeit der SAP HANA-Datenbank und für Backups zu erfüllen.

NetApp FabricPool

NetApp FabricPool darf nicht für aktive primäre Filesysteme in SAP HANA Systemen verwendet werden. Dazu gehören die Dateisysteme für den Daten- und Protokollbereich sowie die `/hana/shared` File-System. Dies führt zu unvorhersehbarer Performance, insbesondere beim Start eines SAP HANA Systems.

Sie können die reine Snapshot-Tiering-Richtlinie zusammen mit FabricPool an einem Backup-Ziel wie SnapVault oder SnapMirror Ziel verwenden.

> Durch die Verwendung von FabricPool für das Tiering von Snapshot Kopien im Primärspeicher oder die Verwendung von FabricPool zu einem Backup-Ziel werden die für die Wiederherstellung und das Recovery einer Datenbank oder anderer Aufgaben benötigte Zeit, beispielsweise das Erstellen von Systemklonen oder Korrektursystemen, geändert. Nehmen Sie dies bei der Planung Ihrer gesamten Lifecycle-Management-Strategie in Betracht und prüfen Sie, ob Ihre SLAs weiterhin über diese Funktion erfüllt werden.

FabricPool ist eine gute Option, um Log-Backups auf eine andere Storage Tier zu verschieben. Das Verschieben von Backups beeinträchtigt die für das Recovery einer SAP HANA Datenbank erforderliche Zeit. Daher die Option `tiering-minimum-cooling-days` Sollte auf einen Wert gesetzt werden, der Log-Backups auflegt, die routinemäßig für die Wiederherstellung nötig sind, auf der lokalen fast Storage Tier.

Speicher konfigurieren

In der folgenden Übersicht sind die erforderlichen Schritte zur Storage-Konfiguration zusammengefasst. Jeder Schritt wird in den nachfolgenden Abschnitten näher beschrieben. In diesem Abschnitt wird die Storage-Hardware eingerichtet und die ONTAP Software bereits installiert. Außerdem muss die Verbindung der Storage FCP-Ports zur SAN-Fabric bereits vorhanden sein.

1. Überprüfen Sie die richtige Festplatten-Shelf-Konfiguration, wie in beschriebenFestplatten-Shelf-Verbindung.
2. Erstellen und konfigurieren Sie die erforderlichen Aggregate, wie in beschrieben.Konfiguration von Aggregaten
3. Erstellen Sie eine Storage Virtual Machine (SVM), wie in beschrieben.Konfiguration von Storage Virtual Machines
4. Erstellung logischer Schnittstellen (LIFs), wie in beschrieben.Konfiguration der logischen Schnittstelle
5. Erstellen Sie Initiatorgruppen (igroups) mit weltweiten Namen (WWNs) von HANA-Servern, wie im Abschnitt beschrieben Initiatorgruppen .
6. Erstellen und konfigurieren Sie Volumes und LUNs innerhalb der Aggregate wie im Abschnitt beschrieben "Einzelhost-Setup" für einzelne Hosts oder im Abschnitt "Einrichtung mehrerer Hosts"

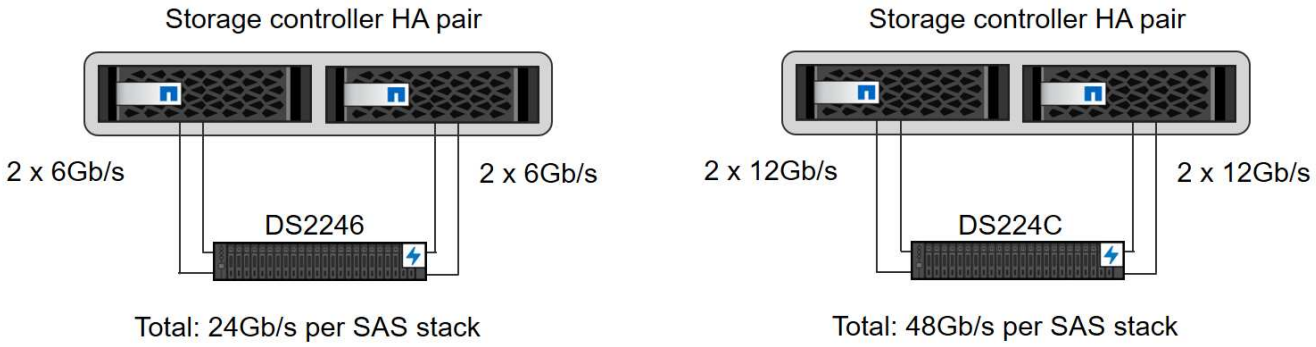
Festplatten-Shelf-Verbindungen

SAS-basierte Platten-Shelves

Es kann maximal ein Platten-Shelf mit einem SAS-Stack verbunden werden, um die erforderliche Performance

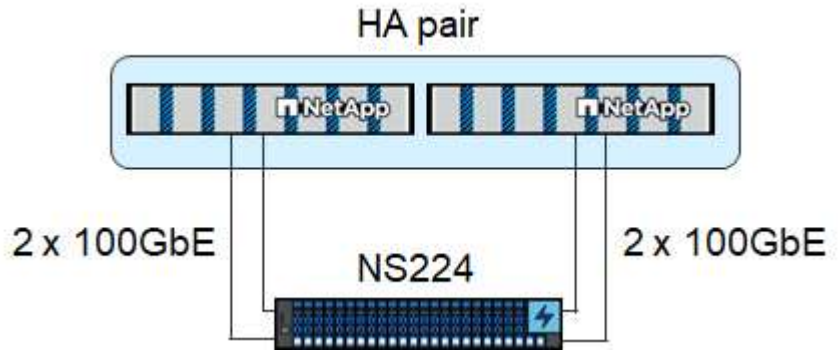
für die SAP HANA-Hosts zu liefern, wie in der folgenden Abbildung dargestellt. Die Festplatten in jedem Shelf müssen gleichmäßig zwischen beiden Controllern des HA-Paars verteilt werden. ADPv2 wird mit ONTAP 9 und DS224C Festplatten-Shelfs verwendet.

Mit dem DS224C Festplatten-Shelf können auch Quad-Path-SAS-Kabel verwendet werden, ist aber nicht erforderlich.



NVMe-basierte Festplattenregale

Jedes NS224 NVMe-Festplatten-Shelf ist, wie in der folgenden Abbildung dargestellt, mit zwei 100-GbE-Ports pro Controller verbunden. Die Festplatten in jedem Shelf müssen gleichmäßig auf beide Controller des HA-Paars verteilt werden. ADPv2 ist auch für das NS224 Festplatten-Shelf genutzt.

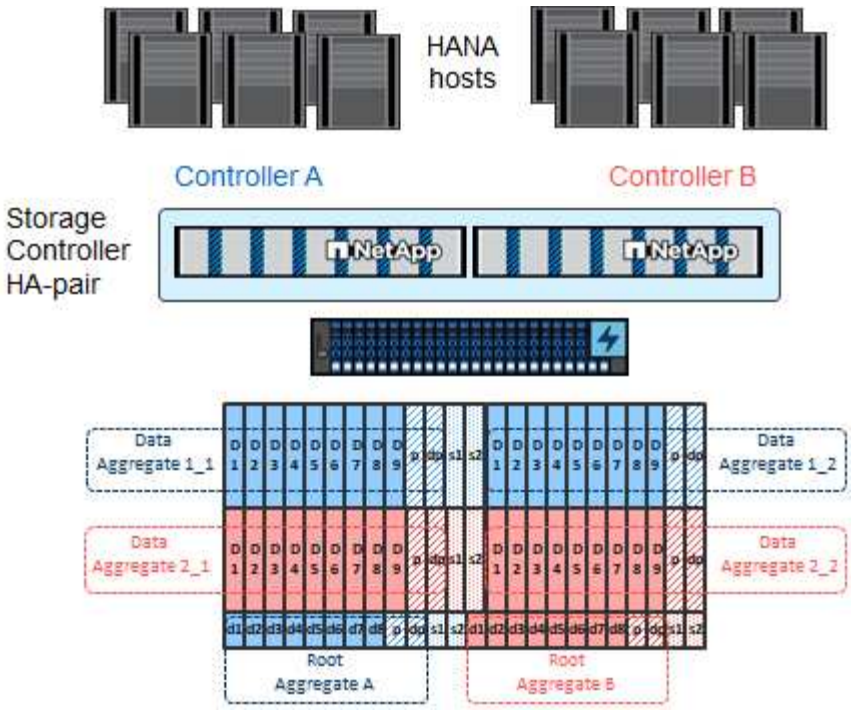


Konfiguration von Aggregaten

Im Allgemeinen müssen zwei Aggregate pro Controller konfiguriert werden, unabhängig davon, welches Platten-Shelf oder Festplattentechnologie (SSD oder HDD) zum Einsatz kommt. Dieser Schritt ist notwendig, damit Sie alle verfügbaren Controller-Ressourcen nutzen können.

ASA-Systeme, die nach dem 2024. August eingeführt wurden, erfordern diesen Schritt nicht wie automatisch

Die folgende Abbildung zeigt eine Konfiguration mit 12 SAP HANA Hosts, die auf einem 12-GB-SAS-Shelf ausgeführt werden und mit ADPv2 konfiguriert sind. Sechs SAP-HANA-Hosts sind mit jedem Storage-Controller verbunden. Vier separate Aggregate, zwei an jedem Storage Controller, sind konfiguriert. Jedes Aggregat ist mit 11 Festplatten mit neun Daten und zwei Parity-Festplatten-Partitionen konfiguriert. Für jeden Controller stehen zwei Ersatzpartitionen zur Verfügung.



Konfiguration von Storage Virtual Machines

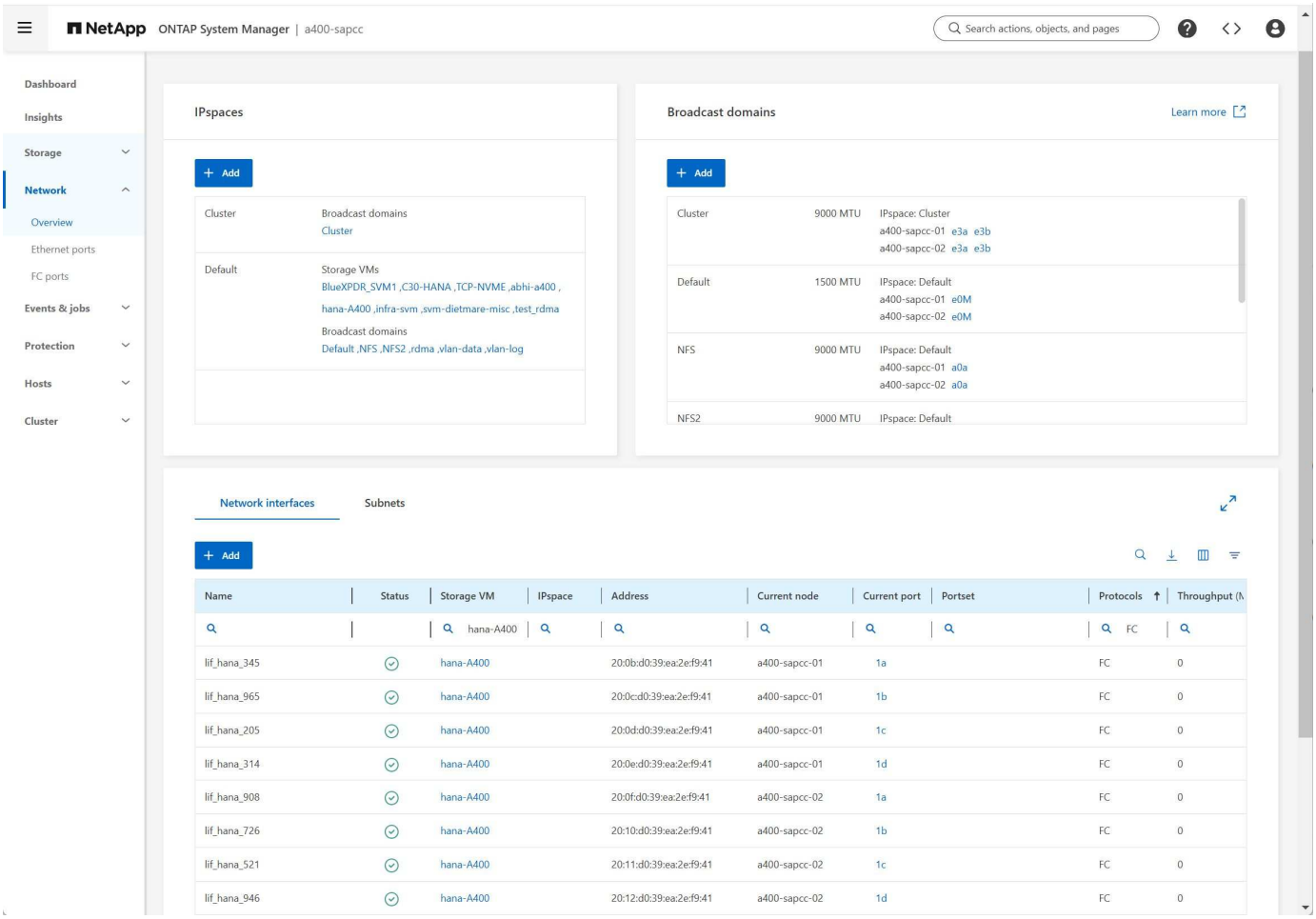
Mehrere SAP Landschaften mit SAP HANA Datenbanken können eine einzige SVM nutzen. Darüber hinaus kann jeder SAP-Landschaft bei Bedarf eine SVM zugewiesen werden, falls diese von verschiedenen Teams innerhalb eines Unternehmens gemanagt werden.

Wenn beim Erstellen einer neuen SVM ein QoS-Profil automatisch erstellt und zugewiesen wird, entfernen Sie dieses automatisch erstellte Profil aus der SVM, um die erforderliche Performance für SAP HANA zu gewährleisten:

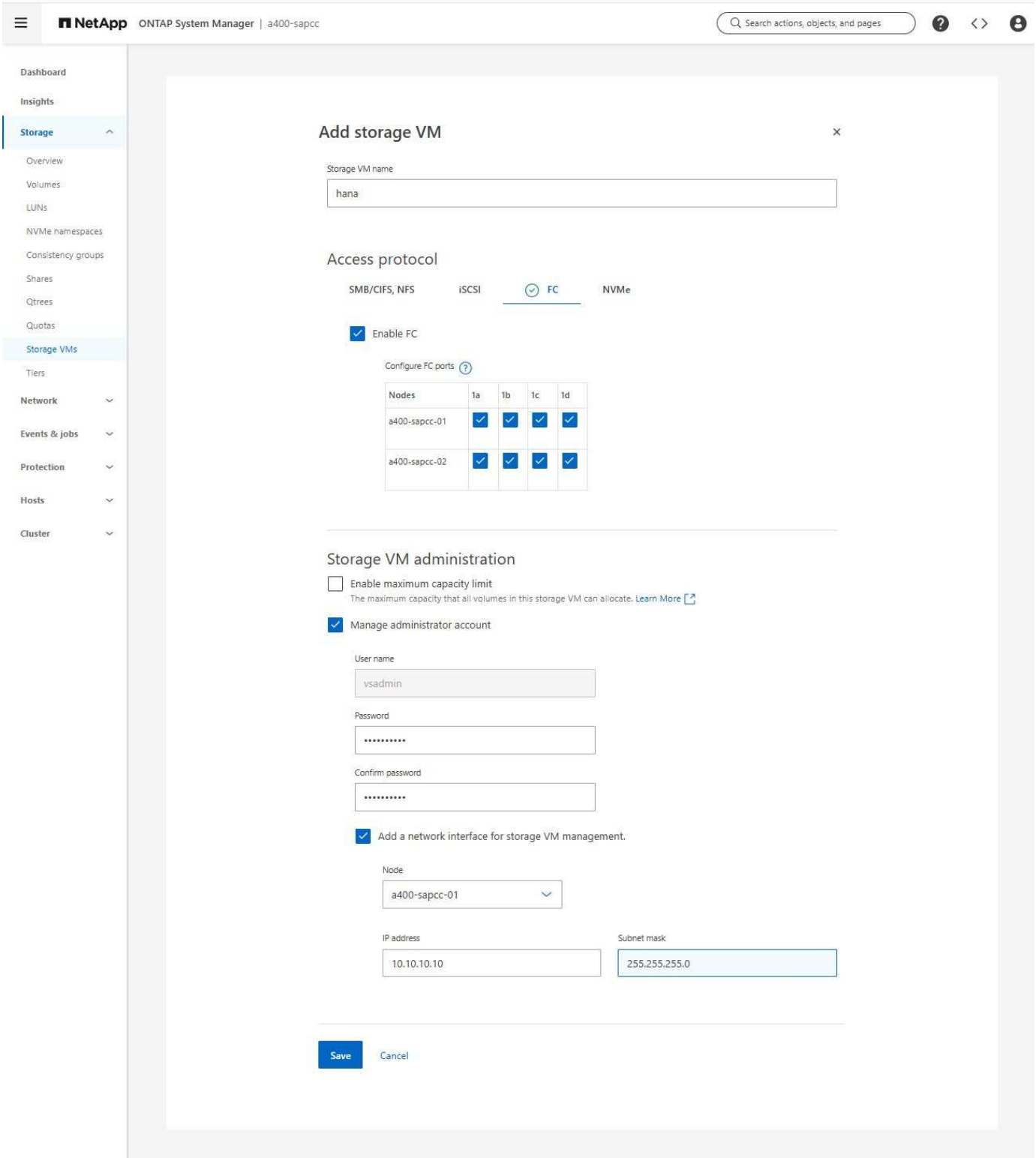
```
vserver modify -vserver <svm-name> -qos-policy-group none
```

Konfiguration der logischen Schnittstelle

Innerhalb der Storage-Cluster-Konfiguration muss eine Netzwerkschnittstelle (LIF) erstellt und einem dedizierten FCP-Port zugewiesen werden. Wenn beispielsweise vier FCP-Ports aus Performance-Gründen erforderlich sind, müssen vier LIFs erstellt werden. Die folgende Abbildung zeigt einen Screenshot der acht LIFs, die auf der SVM konfiguriert wurden.



Während der SVM-Erstellung mit ONTAP System Manager können Sie alle erforderlichen physischen FCP-Ports auswählen und es wird automatisch eine logische Schnittstelle pro physischem Port erstellt.



Initiatorgruppen

Eine Initiatorgruppe kann für jeden Server oder für eine Gruppe von Servern konfiguriert werden, die Zugriff auf eine LUN benötigen. Für die iGroup Konfiguration sind die weltweiten Port-Namen (WWPNs) der Server erforderlich.

Verwenden der `sanlun` Führen Sie den folgenden Befehl aus, um die WWPNs jedes SAP HANA-Hosts abzurufen:

```
stlrx300s8-6:~ # sanlun fcp show adapter
/sbin/udevadm
/sbin/udevadm

host0 ..... WWPN:2100000e1e163700
host1 ..... WWPN:2100000e1e163701
```

Das `sanlun` Tool ist Teil der NetApp Host Utilities und muss auf jedem SAP HANA-Host installiert sein. Weitere Details finden Sie in Abschnitt "Hosteinrichtung:"

Die Initiatorgruppen können über die CLI des ONTAP-Clusters erstellt werden.

```
lun igroup create -igroup <igroup name> -protocol fcp -ostype linux
-initiator <list of initiators> -vserver <SVM name>
```

Einzelner Host

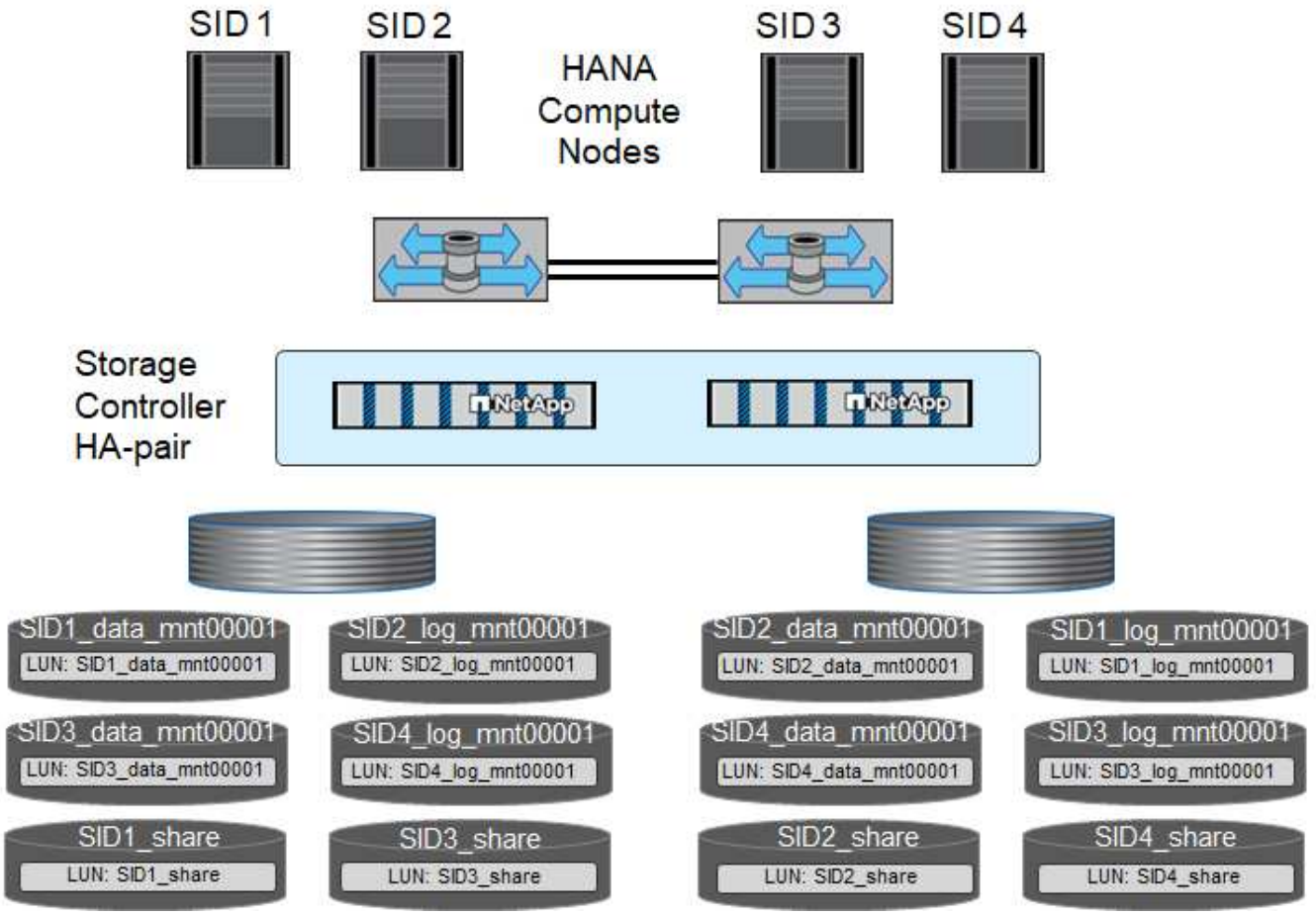
Einzelner Host

Dieser Abschnitt beschreibt die Konfiguration des NetApp-Speichersystems speziell für SAP HANA-Einzelhostsysteme

Volume- und LUN-Konfiguration für SAP HANA Single-Host-Systeme

Die folgende Abbildung zeigt die Volume-Konfiguration von vier SAP HANA-Systemen mit einem Host. Die Daten- und Protokoll-Volumes jedes SAP HANA Systems werden auf verschiedene Storage Controller verteilt. Beispiel: Volume `SID1_data_mnt00001` Wird auf Controller A und Volume konfiguriert `SID1_log_mnt00001` Ist auf Controller B konfiguriert Für jedes Volume wird eine einzelne LUN konfiguriert.

Wenn für die SAP HANA Systeme nur ein Storage-Controller eines HA-Paars verwendet wird, können Daten-Volumes und Protokoll-Volumes auch auf demselben Storage Controller gespeichert werden.



Für jeden SAP HANA-Host, ein Daten-Volume, ein Protokoll-Volume und ein Volume für `/hana/shared` Werden konfiguriert. Die folgende Tabelle zeigt eine Beispielkonfiguration mit vier SAP HANA Single-Host-Systemen.

Zweck	Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregieren 2 bei Controller B
Daten-, Protokoll- und freigegebene Volumes für System SID1	Datenvolumen: SID1_Data_mnt00001	Freigegebenes Volume: SID1_Shared	–	Protokollvolumen: SID1_log_mnt00001
Daten-, Protokoll- und freigegebene Volumes für System SID2	–	Protokollvolumen: SID2_log_mnt00001	Datenvolumen: SID2_Data_mnt00001	Freigegebenes Volume: SID2_Shared
Daten-, Protokoll- und gemeinsam genutzte Volumes für System SID3	Gemeinsam genutztes Volume: SID3_shared	Datenvolumen: SID3_Data_mnt00001	Protokollvolumen: SID3_log_mnt00001	–
Daten-, Protokoll- und gemeinsam genutzte Volumes für System SID4	Protokollvolumen: SID4_log_mnt00001	–	Gemeinsam genutztes Volume: SID4_shared	Datenvolumen: SID4_Data_mnt00001

Die folgende Tabelle zeigt ein Beispiel für die Mount-Point-Konfiguration für ein System mit einem einzelnen

Host.

LUN	Bereitstellungspunkt beim SAP HANA-Host	Hinweis
SID1_Data_mnt00001	/hana/Data/SID1/mnt00001	Mit /etc/fstab-Eintrag montiert
SID1_log_mnt00001	/hana/log/SID1/mnt00001	Mit /etc/fstab-Eintrag montiert
SID1_Shared	/hana/Shared/SID1	Mit /etc/fstab-Eintrag montiert

Mit der beschriebenen Konfiguration wird der verwendet `/usr/sap/SID1` Verzeichnis, in dem das Standard-Home-Verzeichnis des Benutzers SID1adm gespeichert ist, befindet sich auf der lokalen Festplatte. Für ein Disaster Recovery mit festplattenbasierter Replizierung empfiehlt NetApp die Erstellung einer zusätzlichen LUN innerhalb von `SID1_shared` Volume für das `/usr/sap/SID1` Verzeichnis so dass alle Dateisysteme auf dem zentralen Speicher sind.

Volume- und LUN-Konfiguration für SAP HANA Single-Host-Systeme mit Linux LVM

Der Linux LVM kann verwendet werden, um die Leistung zu steigern und um LUN-Größenbeschränkungen zu beheben. Die verschiedenen LUNs einer LVM Volume-Gruppe sollten in einem anderen Aggregat und einem anderen Controller gespeichert werden. Die folgende Tabelle enthält ein Beispiel für zwei LUNs pro Volume-Gruppe.

Es ist nicht notwendig, LVM mit mehreren LUNs zu verwenden, um die SAP HANA-KPIs zu erfüllen, es wird jedoch empfohlen.

Zweck	Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregieren 2 bei Controller B
Daten-, Protokoll- und gemeinsam genutzte Volumes für LVM-basierte Systeme	Datenvolumen: SID1_Data_mnt00001	Gemeinsames Volume: SID1_Shared Log2 Volume: SID1_log2_mnt00001	Daten2 Volumen: SID1_data2_mnt00001	Protokollvolumen: SID1_log_mnt00001

Volume-Optionen

Die in der folgenden Tabelle aufgeführten Volume-Optionen müssen auf allen für SAP HANA verwendeten Volumes überprüft und festgelegt werden.

Aktion	ONTAP 9
Deaktivieren Sie automatische Snapshot Kopien	vol modify –vserver <vserver-Name> -Volume <volname> -Snapshot-Policy keine
Deaktivieren Sie die Sichtbarkeit des Snapshot Verzeichnisses	vol modify -vserver <vserver-Name> -Volume <volname> -Snapdir-Access false

Erstellen von LUNs und Zuordnen von LUNs zu Initiatorgruppen mithilfe der CLI

Dieser Abschnitt zeigt eine Beispielkonfiguration unter Verwendung der Befehlszeile mit ONTAP 9 für ein SAP HANA-Einzelhostsystem mit SID FC5 unter Verwendung von LVM und zwei LUNs pro LVM-Volume-Gruppe:

1. Erstellung aller erforderlichen Volumes

```
vol create -volume FC5_data_mnt00001 -aggregate aggr1_1 -size 1200g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_log_mnt00001  -aggregate aggr1_2 -size 280g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_data2_mnt00001 -aggregate aggr1_2 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_log2_mnt00001  -aggregate aggr1_1 -size 280g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_shared -aggregate aggr1_1 -size 512g -state
online -policy default -snapshot-policy none -junction-path /FC5_shared
-encrypt false  -space-guarantee none
```

2. Erstellen Sie alle LUNs.

```
lun create -path  /vol/FC5_data_mnt00001/FC5_data_mnt00001   -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log_mnt00001/FC5_log_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
```

3. Erstellen Sie die Initiatorgruppe für alle Ports, die zu den Sythe-Hosts von FC5 gehören.

```
lun igroup create -igroup HANA-FC5 -protocol fcp -ostype linux
-initiator 10000090fadcc5fa,10000090fadcc5fb -vserver hana
```

4. Ordnen Sie alle LUNs der erstellten Initiatorgruppe zu.

```
lun map -path /vol/FC5_data_mnt00001/FC5_data_mnt00001    -igroup HANA-
FC5
lun map -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001  -igroup HANA-
FC5
lun map -path /vol/FC5_log_mnt00001/FC5_log_mnt00001  -igroup HANA-FC5
lun map -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001  -igroup HANA-FC5
```


Mehrere Hosts

Dieser Abschnitt beschreibt die Konfiguration des NetApp-Speichersystems speziell für SAP HANA-Mehrfachhostsysteme

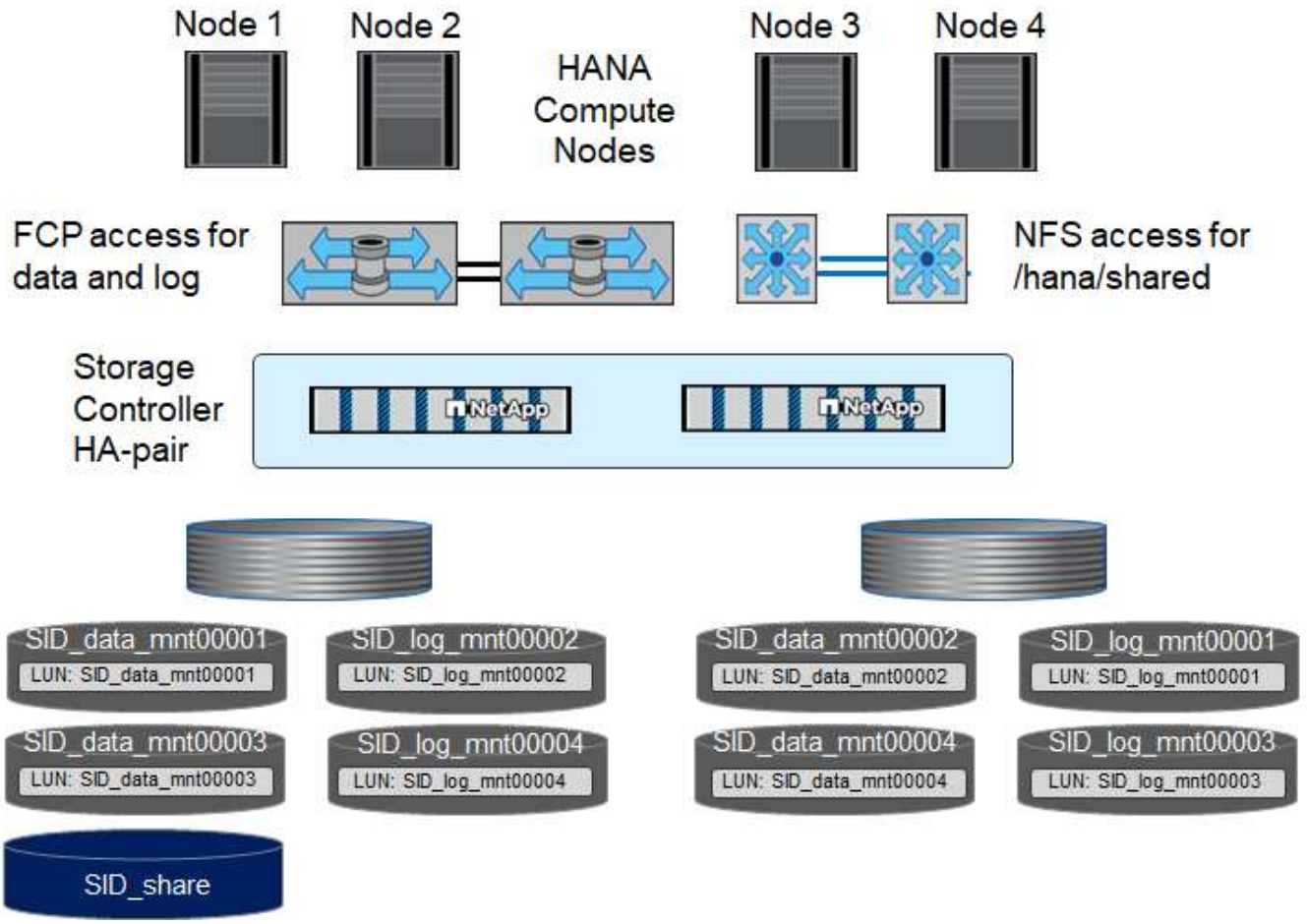
Volume- und LUN-Konfiguration für SAP HANA Multiple-Host-Systeme

Die folgende Abbildung zeigt die Volume-Konfiguration eines SAP HANA Systems mit 4+1 und mehreren Hosts. Die Daten-Volumes und Protokoll-Volumes jedes SAP HANA-Hosts werden auf verschiedene Storage-Controller verteilt. Beispiel: Das Volume `SID_data_mnt00001` Wird für Controller A und Volume konfiguriert `SID_log_mnt00001` Ist auf Controller B konfiguriert Eine LUN ist innerhalb jedes Volumes konfiguriert.

Der `/hana/shared` Das Volume muss von allen HANA-Hosts zugänglich sein und wird daher mithilfe von NFS exportiert. Obwohl es für die keine spezifischen Performance-KPIs gibt `/hana/shared` NetApp empfiehlt die Verwendung einer 10-Gbit-Ethernet-Verbindung.

Wenn für das SAP HANA System nur ein Storage-Controller eines HA-Paars verwendet wird, können Daten- und Protokoll-Volumes auch auf demselben Storage Controller gespeichert werden.

NetApp ASA -Systeme unterstützen NFS nicht als Protokoll. NetApp empfiehlt den Einsatz eines zusätzlichen AFF oder FAS -Systems für die `/hana/shared` Dateisystem.



Für jeden SAP HANA-Host werden ein Daten-Volume und ein Protokoll-Volume erstellt. Der `/hana/shared` Das Volume wird von allen Hosts des SAP HANA-Systems verwendet. Die folgende Tabelle zeigt eine Beispielkonfiguration für ein SAP HANA System mit 4+1 mehreren Hosts.

Zweck	Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregieren 2 bei Controller B
Daten- und Protokoll-Volumes für Node 1	Datenvolumen: SID_Data_mnt00001	–	Protokollvolumen: SID_log_mnt00001	–
Daten- und Protokoll-Volumes für Node 2	Protokollvolumen: SID_log_mnt002	–	Datenvolumen: SID_Data_mnt002	–
Daten- und Protokoll-Volumes für Node 3	–	Datenvolumen: SID_Data_mnt00003	–	Protokollvolumen: SID_log_mnt00003
Daten- und Protokoll-Volumes für Node 4	–	Protokollvolumen: SID_log_mnt004	–	Datenvolumen: SID_Data_mnt00004
Gemeinsames Volume für alle Hosts	Gemeinsam genutztes Volume: SID_shared	–	–	–

Die folgende Tabelle zeigt die Konfiguration und die Bereitstellungspunkte eines Systems mit mehreren Hosts mit vier aktiven SAP HANA Hosts.

LUN oder Volume	Bereitstellungspunkt beim SAP HANA-Host	Hinweis
LUN: SID_Data_mnt00001	/hana/Data/SID/mnt00001	Montiert mit Speicheranschluss
LUN: SID_log_mnt00001	/hana/log/SID/mnt00001	Montiert mit Speicheranschluss
LUN: SID_Data_mnt002	/hana/Data/SID/mnt002	Montiert mit Speicheranschluss
LUN: SID_log_mnt002	/hana/log/SID/mnt002	Montiert mit Speicheranschluss
LUN: SID_Data_mnt003	/hana/Data/SID/mnt003	Montiert mit Speicheranschluss
LUN: SID_log_mnt003	/hana/log/SID/mnt003	Montiert mit Speicheranschluss
LUN: SID_Data_mnt004	/hana/Data/SID/mnt004	Montiert mit Speicheranschluss
LUN: SID_log_mnt004	/hana/log/SID/mnt004	Montiert mit Speicheranschluss
Volume: SID_Shared	/hana/Shared	Gemountet auf allen Hosts mit NFS und /etc/fstab Eintrag

Mit der beschriebenen Konfiguration wird der verwendet `/usr/sap/SID` Verzeichnis, in dem das Standard-Home-Verzeichnis des Benutzers SIDadm gespeichert ist, befindet sich auf der lokalen Festplatte für jeden HANA-Host. Bei einem Disaster Recovery Setup mit festplattenbasierter Replizierung empfiehlt NetApp das Erstellen von vier zusätzlichen Unterverzeichnissen in `SID_shared` Volume für das `/usr/sap/SID` Dateisystem so, dass jeder Datenbank-Host alle seine Dateisysteme auf dem zentralen Speicher hat.

Volume- und LUN-Konfiguration für SAP HANA Systeme mit mehreren Hosts unter Verwendung von Linux LVM

Der Linux LVM kann verwendet werden, um die Leistung zu steigern und um LUN-Größenbeschränkungen zu beheben. Die verschiedenen LUNs einer LVM Volume-Gruppe sollten in einem anderen Aggregat und einem anderen Controller gespeichert werden.

Es ist nicht notwendig, LVM zu verwenden, um mehrere LUNs zu kombinieren, um die SAP HANA KPIs zu erfüllen, aber es wird empfohlen

Die folgende Tabelle zeigt ein Beispiel für zwei LUNs pro Volume-Gruppe für ein 2+1 SAP HANA System mit mehreren Hosts.

Zweck	Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregieren 2 bei Controller B
Daten- und Protokoll-Volumes für Node 1	Datenvolumen: SID_Data_mnt00001	Log2-Volumen: SID_log2_mnt00001	Protokollvolumen: SID_log_mnt00001	Daten2 Volumen: SID_data2_mnt00001
Daten- und Protokoll-Volumes für Node 2	Log2-Volumen: SID_log2_mnt002	Datenvolumen: SID_Data_mnt002	Daten2 Volumen: SID_data2_mnt002	Protokollvolumen: SID_log_mnt002

Zweck	Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregieren 2 bei Controller B
Gemeinsames Volume für alle Hosts	Gemeinsam genutztes Volume: SID_shared	–	–	–

Volume-Optionen

Die in der folgenden Tabelle aufgeführten Volume-Optionen müssen geprüft und auf allen SVMs eingestellt werden.

Aktion	
Deaktivieren Sie automatische Snapshot Kopien	vol modify –vserver <vserver-Name> -Volume <volname> -Snapshot-Policy keine
Deaktivieren Sie die Sichtbarkeit des Snapshot Verzeichnisses	vol modify -vserver <vserver-Name> -Volume <volname> -Snapdir-Access false

Erstellen von LUNs, Volumes und Zuordnen von LUNs zu Initiatorgruppen

Sie können NetApp ONTAP System Manager verwenden, um Storage Volumes und LUNs zu erstellen und sie Initiatorgruppen der Server und der ONTAP CLI zuzuordnen. In diesem Leitfaden wird die Verwendung der CLI beschrieben.

Erstellen von LUNs, Volumes und Zuordnen von LUNs zu Initiatorgruppen über die CLI

Dieser Abschnitt zeigt eine Beispielkonfiguration mit der Befehlszeile mit ONTAP 9 für ein 2+1 SAP HANA mehrere Hostsysteme mit SID FC5 unter Verwendung von LVM und zwei LUNs pro LVM Volume-Gruppe:

1. Erstellung aller erforderlichen Volumes

```
vol create -volume FC5_data_mnt00001 -aggregate aggr1_1 -size 1200g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_log_mnt00002  -aggregate aggr2_1 -size 280g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_log_mnt00001  -aggregate aggr1_2 -size 280g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_data_mnt00002  -aggregate aggr2_2 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_data2_mnt00001 -aggregate aggr1_2 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_log2_mnt00002  -aggregate aggr2_2 -size 280g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_log2_mnt00001  -aggregate aggr1_1 -size 280g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_data2_mnt00002  -aggregate aggr2_1 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_shared -aggregate aggr1_1 -size 512g -state
online -policy default -snapshot-policy none -junction-path /FC5_shared
-encrypt false  -space-guarantee none
```

2. Erstellen Sie alle LUNs.

```
lun create -path  /vol/FC5_data_mnt00001/FC5_data_mnt00001   -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data_mnt00002/FC5_data_mnt00002 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data2_mnt00002/FC5_data2_mnt00002 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log_mnt00001/FC5_log_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log_mnt00002/FC5_log_mnt00002 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log2_mnt00002/FC5_log2_mnt00002 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
```

3. Erstellen Sie die Initiatorgruppe für alle Server, die zu System FC5 gehören.

```
lun igroup create -igroup HANA-FC5 -protocol fcp -ostype linux
-initiator
10000090fadcc5fa,10000090fadcc5fb,10000090fadcc5c1,10000090fadcc5c2,1000
0090fadcc5c3,10000090fadcc5c4 -vserver hana
```

4. Ordnen Sie alle LUNs der erstellten Initiatorgruppe zu.

```
lun map -path /vol/FC5_data_mnt00001/FC5_data_mnt00001    -igroup HANA-
FC5
lun map -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001  -igroup HANA-
FC5
lun map -path /vol/FC5_data_mnt00002/FC5_data_mnt00002  -igroup HANA-FC5
lun map -path /vol/FC5_data2_mnt00002/FC5_data2_mnt00002  -igroup HANA-
FC5
lun map -path /vol/FC5_log_mnt00001/FC5_log_mnt00001  -igroup HANA-FC5
lun map -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001  -igroup HANA-FC5
lun map -path /vol/FC5_log_mnt00002/FC5_log_mnt00002  -igroup HANA-FC5
lun map -path /vol/FC5_log2_mnt00002/FC5_log2_mnt00002  -igroup HANA-FC5
```

SAP HANA Storage-Connector-API

Ein Storage Connector ist nur in Umgebungen mit mehreren Hosts mit Failover-Funktionen erforderlich. SAP HANA bietet bei der Einrichtung mehrerer Hosts eine Hochverfügbarkeitsfunktionen, mit der ein Failover eines SAP HANA-Datenbankhosts auf einen Standby-Host möglich ist.

In diesem Fall wird auf die LUNs des ausgefallenen Hosts zugegriffen und vom Standby-Host verwendet. Der Speicher-Connector wird verwendet, um sicherzustellen, dass eine Speicherpartition von jeweils nur einem Datenbank-Host aktiv zugegriffen werden kann.

In SAP HANA Konfigurationen mit mehreren Hosts und NetApp Storage kommt der von SAP bereitgestellte Standard-Storage Connector zum Einsatz. Der „SAP HANA Fibre Channel Storage Connector Admin Guide“ kann als Anhang zu gefunden werden "SAP-Hinweis 1900823".

Hosteinrichtung

Bevor Sie den Host einrichten, müssen die NetApp SAN Host Utilities von heruntergeladen werden "NetApp Support" Standort und auf den HANA-Servern installiert. Die Dokumentation des Host Utility enthält Informationen zu zusätzlicher Software, die abhängig vom verwendeten FCP HBA installiert werden muss.

Die Dokumentation enthält auch Informationen zu Multipath-Konfigurationen, die spezifisch für die verwendete Linux-Version sind. In diesem Dokument werden die erforderlichen Konfigurationsschritte für SLES 12 SP1 oder höher und RHEL 7 beschrieben. 2 oder höher, wie im beschrieben "Linux Host Utilities 7.1 Installations- und Setup-Leitfaden".

Konfigurieren Sie Multipathing

> Die Schritte 1 bis 6 müssen auf allen Worker- und Standby-Hosts in einer SAP HANA Konfiguration mit mehreren Hosts ausgeführt werden.

Um Multipathing zu konfigurieren, gehen Sie wie folgt vor:

1. Führen Sie Linux aus `rescan-scsi-bus.sh -a` Befehl auf jedem Server, um neue LUNs zu ermitteln.

2. Führen Sie den `sanlun lun show` und überprüfen Sie, ob alle erforderlichen LUNs sichtbar sind. Das folgende Beispiel zeigt die `sanlun lun show` Befehlsausgabe für ein 2+1-HANA-System mit mehreren Hosts, zwei Daten-LUNs und zwei Protokoll-LUNs. Die Ausgabe zeigt die LUNs und die zugehörigen Gerätedateien, z. B. LUN `FC5_data_mnt00001` und die Gerätedatei `/dev/sdag` Jede LUN verfügt über acht FC-Pfade vom Host zu den Speichercontrollern.

```
sapcc-hana-tst:~ # sanlun lun show
controller(7mode/E-Series)/                                    device
host                  lun
vserver(cDOT/FlashRay)        lun-pathname                     filename
adapter    protocol   size    product
------------------------------------------------------------------------
---------------------------------------
svm1                          FC5_log2_mnt00002                /dev/sdbb
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00002                 /dev/sdba
host21     FCP        500g    cDOT
svm1                          FC5_log2_mnt00001                /dev/sdaz
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001                 /dev/sday
host21     FCP        500g    cDOT
svm1                          FC5_data2_mnt00002               /dev/sdax
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00002                /dev/sdaw
host21     FCP        1t      cDOT
svm1                          FC5_data2_mnt00001               /dev/sdav
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001                /dev/sdau
host21     FCP        1t      cDOT
svm1                          FC5_log2_mnt00002                /dev/sdat
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00002                 /dev/sdas
host21     FCP        500g    cDOT
svm1                          FC5_log2_mnt00001                /dev/sdar
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001                 /dev/sdaq
host21     FCP        500g    cDOT
svm1                          FC5_data2_mnt00002               /dev/sdap
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00002                /dev/sdao
host21     FCP        1t      cDOT
svm1                          FC5_data2_mnt00001               /dev/sdan
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001                /dev/sdam
host21     FCP        1t      cDOT
svm1                          FC5_log2_mnt00002                /dev/sdal
```

```
host20     FCP         500g    cDOT
svm1                           FC5_log_mnt00002              /dev/sdak
host20     FCP         500g    cDOT
svm1                           FC5_log2_mnt00001             /dev/sdaj
host20     FCP         500g    cDOT
svm1                           FC5_log_mnt00001              /dev/sdai
host20     FCP         500g    cDOT
svm1                           FC5_data2_mnt00002            /dev/sdah
host20     FCP         1t      cDOT
svm1                           FC5_data_mnt00002             /dev/sdag
host20     FCP         1t      cDOT
svm1                           FC5_data2_mnt00001            /dev/sdaf
host20     FCP         1t      cDOT
svm1                           FC5_data_mnt00001             /dev/sdae
host20     FCP         1t      cDOT
svm1                           FC5_log2_mnt00002             /dev/sdad
host20     FCP         500g    cDOT
svm1                           FC5_log_mnt00002              /dev/sdac
host20     FCP         500g    cDOT
svm1                           FC5_log2_mnt00001             /dev/sdab
host20     FCP         500g    cDOT
svm1                           FC5_log_mnt00001              /dev/sdaa
host20     FCP         500g    cDOT
svm1                           FC5_data2_mnt00002            /dev/sdz
host20     FCP         1t      cDOT
svm1                           FC5_data_mnt00002             /dev/sdy
host20     FCP         1t      cDOT
svm1                           FC5_data2_mnt00001            /dev/sdx
host20     FCP         1t      cDOT
svm1                           FC5_data_mnt00001             /dev/sdw
host20     FCP         1t      cDOT
```

3. Führen Sie den `multipath -r` Und `multipath -ll` Befehl zum Abrufen der weltweiten Kennungen (WWIDs) für die Gerätedateinamen.

   In diesem Beispiel gibt es acht LUNs.

```
sapcc-hana-tst:~ # multipath -r
sapcc-hana-tst:~ # multipath -ll
3600a098038314e63492b59326b4b786d dm-7 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:2 sdaf 65:240 active ready running
  |- 20:0:5:2 sdx  65:112 active ready running
```

```
  |- 21:0:4:2 sdav 66:240 active ready running
  `- 21:0:6:2 sdan 66:112 active ready running
3600a098038314e63492b59326b4b786e dm-9 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:4 sdah 66:16  active ready running
  |- 20:0:5:4 sdz  65:144 active ready running
  |- 21:0:4:4 sdax 67:16  active ready running
  `- 21:0:6:4 sdap 66:144 active ready running
3600a098038314e63492b59326b4b786f dm-11 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:6 sdaj 66:48  active ready running
  |- 20:0:5:6 sdab 65:176 active ready running
  |- 21:0:4:6 sdaz 67:48  active ready running
  `- 21:0:6:6 sdar 66:176 active ready running
3600a098038314e63492b59326b4b7870 dm-13 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:8 sdal 66:80  active ready running
  |- 20:0:5:8 sdad 65:208 active ready running
  |- 21:0:4:8 sdbb 67:80  active ready running
  `- 21:0:6:8 sdat 66:208 active ready running
3600a098038314e63532459326d495a64 dm-6 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:1 sdae 65:224 active ready running
  |- 20:0:5:1 sdw  65:96  active ready running
  |- 21:0:4:1 sdau 66:224 active ready running
  `- 21:0:6:1 sdam 66:96  active ready running
3600a098038314e63532459326d495a65 dm-8 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:3 sdag 66:0   active ready running
  |- 20:0:5:3 sdy  65:128 active ready running
  |- 21:0:4:3 sdaw 67:0   active ready running
  `- 21:0:6:3 sdao 66:128 active ready running
3600a098038314e63532459326d495a66 dm-10 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
```

```
  |- 20:0:4:5 sdai 66:32  active ready running
  |- 20:0:5:5 sdaa 65:160 active ready running
  |- 21:0:4:5 sday 67:32  active ready running
  `- 21:0:6:5 sdaq 66:160 active ready running
3600a098038314e63532459326d495a67 dm-12 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:7 sdak 66:64  active ready running
  |- 20:0:5:7 sdac 65:192 active ready running
  |- 21:0:4:7 sdba 67:64  active ready running
  `- 21:0:6:7 sdas 66:192 active ready running
```

4. Bearbeiten Sie das `/etc/multipath.conf` Datei und fügen Sie die WWIDs und Aliasnamen hinzu.

Die Beispielausgabe zeigt den Inhalt des `/etc/multipath.conf` Datei, die Alias-Namen für die vier LUNs eines 2+1-Systems mit mehreren Hosts enthält. Wenn keine Multipath.conf-Datei verfügbar ist, können Sie eine erstellen, indem Sie den folgenden Befehl ausführen: `multipath -T > /etc/multipath.conf`.

```
sapcc-hana-tst:/ # cat /etc/multipath.conf
multipaths {
                multipath {
                wwid    3600a098038314e63492b59326b4b786d
                alias   svm1-FC5_data2_mnt00001
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b786e
                alias   svm1-FC5_data2_mnt00002
        }
        multipath {
                wwid    3600a098038314e63532459326d495a64
                alias   svm1-FC5_data_mnt00001
        }
        multipath {
                wwid    3600a098038314e63532459326d495a65
                alias   svm1-FC5_data_mnt00002
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b786f
                alias   svm1-FC5_log2_mnt00001
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b7870
                alias   svm1-FC5_log2_mnt00002
        }
        multipath {
                wwid    3600a098038314e63532459326d495a66
                alias   svm1-FC5_log_mnt00001
        }
        multipath {
                wwid    3600a098038314e63532459326d495a67
                alias   svm1-FC5_log_mnt00002
        }


}
```

5. Führen Sie die aus `multipath -r` Befehl zum Neuladen der Gerätezuordnung.
6. Überprüfen Sie die Konfiguration, indem Sie den ausführen `multipath -ll` Befehl zum Auflisten aller LUNs, Alias-Namen sowie aktiver und Standby-Pfade.

> Die folgende Beispielausgabe zeigt die Ausgabe eines 2+1-HANA-Systems mit mehreren Hosts mit zwei Daten und zwei Log-LUNs.

```
sapcc-hana-tst:~ # multipath -ll
hsvm1-FC5_data2_mnt00001 (3600a098038314e63492b59326b4b786d) dm-7
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:2 sdaf 65:240 active ready running
  |- 20:0:5:2 sdx  65:112 active ready running
  |- 21:0:4:2 sdav 66:240 active ready running
  `- 21:0:6:2 sdan 66:112 active ready running
svm1-FC5_data2_mnt00002 (3600a098038314e63492b59326b4b786e) dm-9
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:4 sdah 66:16  active ready running
  |- 20:0:5:4 sdz  65:144 active ready running
  |- 21:0:4:4 sdax 67:16  active ready running
  `- 21:0:6:4 sdap 66:144 active ready running
svm1-FC5_data_mnt00001 (3600a098038314e63532459326d495a64) dm-6
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:1 sdae 65:224 active ready running
  |- 20:0:5:1 sdw  65:96  active ready running
  |- 21:0:4:1 sdau 66:224 active ready running
  `- 21:0:6:1 sdam 66:96  active ready running
svm1-FC5_data_mnt00002 (3600a098038314e63532459326d495a65) dm-8
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:3 sdag 66:0   active ready running
  |- 20:0:5:3 sdy  65:128 active ready running
  |- 21:0:4:3 sdaw 67:0   active ready running
  `- 21:0:6:3 sdao 66:128 active ready running
svm1-FC5_log2_mnt00001 (3600a098038314e63492b59326b4b786f) dm-11
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:6 sdaj 66:48  active ready running
  |- 20:0:5:6 sdab 65:176 active ready running
  |- 21:0:4:6 sdaz 67:48  active ready running
  `- 21:0:6:6 sdar 66:176 active ready running
```

```
svm1-FC5_log2_mnt00002 (3600a098038314e63492b59326b4b7870) dm-13
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:8 sdal 66:80  active ready running
  |- 20:0:5:8 sdad 65:208 active ready running
  |- 21:0:4:8 sdbb 67:80  active ready running
  `- 21:0:6:8 sdat 66:208 active ready running
svm1-FC5_log_mnt00001 (3600a098038314e63532459326d495a66) dm-10
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:5 sdai 66:32  active ready running
  |- 20:0:5:5 sdaa 65:160 active ready running
  |- 21:0:4:5 sday 67:32  active ready running
  `- 21:0:6:5 sdaq 66:160 active ready running
svm1-FC5_log_mnt00002 (3600a098038314e63532459326d495a67) dm-12
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:7 sdak 66:64  active ready running
  |- 20:0:5:7 sdac 65:192 active ready running
  |- 21:0:4:7 sdba 67:64  active ready running
  `- 21:0:6:7 sdas 66:192 active ready running
```

Einzelhost-Setup

Einzelhost-Setup

In diesem Kapitel wird die Einrichtung eines einzelnen SAP HANA-Hosts unter Verwendung von LINUX LVM beschrieben.

LUN-Konfiguration für SAP HANA Single-Host-Systeme

Beim SAP HANA-Host müssen Volume-Gruppen und logische Volumes erstellt und eingebunden werden, wie in der folgenden Tabelle angegeben.

Logisches Volume/LUN	Bereitstellungspunkt beim SAP HANA-Host	Hinweis
LV: FC5_data_mnt0000-vol	/hana/data/FC51/mnt00001	Mit /etc/fstab-Eintrag montiert
LV: FC5_log_mnt00001-vol	/hana/log/FC5/mnt00001	Mit /etc/fstab-Eintrag montiert
LUN: FC5_shared	/hana/Shared/FC5	Mit /etc/fstab-Eintrag montiert

Mit der beschriebenen Konfiguration wird die `/usr/sap/FC5` Das Verzeichnis, in dem das Standard-Home-Verzeichnis des Benutzers FC5adm gespeichert ist, befindet sich auf der lokalen Festplatte. In einem Disaster Recovery-Setup mit festplattenbasierter Replikation empfiehlt NetApp die Erstellung einer zusätzlichen LUN innerhalb der `FC5_shared` Volumen für die `/usr/sap/FC5` Verzeichnis, sodass sich alle Dateisysteme auf dem zentralen Speicher befinden.

Erstellen von LVM-Volume-Gruppen und logischen Volumes

1. Initialisieren Sie alle LUNs als ein physisches Volume.

```
pvcreate /dev/mapper/hana-FC5_data_mnt00001
pvcreate /dev/mapper/hana-FC5_data2_mnt00001
pvcreate /dev/mapper/hana-FC5_log_mnt00001
pvcreate /dev/mapper/hana-FC5_log2_mnt00001
```

2. Erstellen Sie die Volume-Gruppen für jede Daten- und Protokollpartition.

```
vgcreate FC5_data_mnt00001 /dev/mapper/hana-FC5_data_mnt00001
/dev/mapper/hana-FC5_data2_mnt00001
vgcreate FC5_log_mnt00001 /dev/mapper/hana-FC5_log_mnt00001
/dev/mapper/hana-FC5_log2_mnt00001
```

3. Erstellen Sie für jede Daten- und Protokollpartition ein logisches Volume. Verwenden Sie eine Stripe-Größe, die der Anzahl der LUNs pro Volume-Gruppe entspricht (in diesem Beispiel sind es zwei), eine Stripe-Größe von 256 KB für Daten und 64.000 für das Protokoll. SAP unterstützt nur ein logisches Volume pro Volume-Gruppe.

```
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00001
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00001
```

4. Scannen Sie bei allen anderen Hosts die physischen Volumes, Volume-Gruppen und Volume-Gruppen.

```
modprobe dm_mod
pvscan
vgscan
lvscan
```

Wenn diese Befehle die Volumes nicht finden, ist ein Neustart erforderlich.

Zum Mounten der logischen Volumes müssen die logischen Volumes aktiviert sein. Um die Volumes zu aktivieren, führen Sie den folgenden Befehl aus:

```
vgchange -a y
```

Erstellen von Dateisystemen

Erstellen Sie das XFS-Dateisystem auf allen logischen Daten- und Protokollvolumes und der gemeinsam genutzten Hana-LUN.

```
mkfs.xfs FC5_data_mnt00001-vol
mkfs.xfs FC5_log_mnt00001-vol
mkfs.xfs /dev/mapper/svm1-FC5_shared
```

Erstellen von Bereitstellungspunkten

Erstellen Sie die erforderlichen Mount-Point-Verzeichnisse und legen Sie die Berechtigungen auf dem Datenbankhost fest:

```
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/shared
sapcc-hana-tst:/ # chmod –R 777 /hana/log/FC5
sapcc-hana-tst:/ # chmod –R 777 /hana/data/FC5
sapcc-hana-tst:/ # chmod 777 /hana/shared
```

Mounten Sie File-Systeme

Um Dateisysteme während des Systemstarts mit dem `/etc/fstab` Konfigurationsdatei, fügen Sie die erforderlichen Dateisysteme zum `/etc/fstab` Konfigurationsdatei:

```
# cat /etc/fstab
/dev/mapper/hana-FC5_shared /hana/shared xfs defaults 0 0
/dev/mapper/FC5_log_mnt00001-vol /hana/log/FC5/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/FC5_data_mnt00001-vol /hana/data/FC5/mnt00001 xfs
relatime,inode64 0 0
```

Die XFS-Dateisysteme für die Daten- und Protokoll-LUNs müssen mit dem gemountet werden `relatime` Und `inode64` Mount-Optionen:

Um die Dateisysteme zu mounten, führen Sie den `mount –a` Befehl beim Host.

Einrichtung mehrerer Hosts

Einrichtung mehrerer Hosts

In diesem Kapitel wird beispielhaft die Einrichtung eines 2+1 SAP HANA-Mehrhostsystems beschrieben.

LUN-Konfiguration für SAP HANA-Mehrhostsysteme

Beim SAP HANA-Host müssen Volume-Gruppen und logische Volumes erstellt und eingebunden werden, wie in der folgenden Tabelle angegeben.

Logisches Volumen (LV) oder Volumen	Bereitstellungspunkt beim SAP HANA-Host	Hinweis
LV: FC5_data_mnt00001-vol	/hana/Data/FC5/mnt00001	Montiert mit Speicheranschluss
LV: FC5_log_mnt00001-vol	/hana/log/FC5/mnt00001	Montiert mit Speicheranschluss
LV: FC5_data_mnt00002-vol	/hana/Data/FC5/mnt00002	Montiert mit Speicheranschluss
LV: FC5_log_mnt00002-vol	/hana/log/FC5/mnt00002	Montiert mit Speicheranschluss
Volume: FC5_shared	/hana/Shared	Gemountet auf allen Hosts mit NFS und /etc/fstab Eintrag

Mit der beschriebenen Konfiguration wird die `/usr/sap/FC5` Das Verzeichnis, in dem das Standard-Home-Verzeichnis des Benutzers FC5adm gespeichert ist, befindet sich auf der lokalen Festplatte jedes HANA-Hosts. In einem Disaster Recovery-Setup mit festplattenbasierter Replikation empfiehlt NetApp die Erstellung von vier zusätzlichen Unterverzeichnissen im `FC5_shared` Volumen für die `/usr/sap/FC5` Dateisystem, sodass jeder Datenbankhost alle seine Dateisysteme auf dem zentralen Speicher hat.

Erstellen von LVM-Volume-Gruppen und logischen Volumes

1. Initialisieren Sie alle LUNs als ein physisches Volume.

```
pvcreate /dev/mapper/hana-FC5_data_mnt00001
pvcreate /dev/mapper/hana-FC5_data2_mnt00001
pvcreate /dev/mapper/hana-FC5_data_mnt00002
pvcreate /dev/mapper/hana-FC5_data2_mnt00002
pvcreate /dev/mapper/hana-FC5_log_mnt00001
pvcreate /dev/mapper/hana-FC5_log2_mnt00001
pvcreate /dev/mapper/hana-FC5_log_mnt00002
pvcreate /dev/mapper/hana-FC5_log2_mnt00002
```

2. Erstellen Sie die Volume-Gruppen für jede Daten- und Protokollpartition.

```
vgcreate FC5_data_mnt00001 /dev/mapper/hana-FC5_data_mnt00001
/dev/mapper/hana-FC5_data2_mnt00001
vgcreate FC5_data_mnt00002 /dev/mapper/hana-FC5_data_mnt00002
/dev/mapper/hana-FC5_data2_mnt00002
vgcreate FC5_log_mnt00001 /dev/mapper/hana-FC5_log_mnt00001
/dev/mapper/hana-FC5_log2_mnt00001
vgcreate FC5_log_mnt00002 /dev/mapper/hana-FC5_log_mnt00002
/dev/mapper/hana-FC5_log2_mnt00002
```

3. Erstellen Sie für jede Daten- und Protokollpartition ein logisches Volume. Verwenden Sie eine Stripe-Größe, die der Anzahl der LUNs pro Volume-Gruppe entspricht (in diesem Beispiel sind es zwei), eine Stripe-Größe von 256 KB für Daten und 64.000 für das Protokoll. SAP unterstützt nur ein logisches Volume pro Volume-Gruppe.

```
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00001
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00002
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00002
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00001
```

4. Scannen Sie bei allen anderen Hosts die physischen Volumes, Volume-Gruppen und Volume-Gruppen.

```
modprobe dm_mod
pvscan
vgscan
lvscan
```

Wenn diese Befehle die Volumes nicht finden, ist ein Neustart erforderlich.

Zum Mounten der logischen Volumes müssen die logischen Volumes aktiviert sein. Um die Volumes zu aktivieren, führen Sie den folgenden Befehl aus:

```
vgchange -a y
```

Erstellen von Dateisystemen

Erstellen Sie das XFS-Dateisystem auf allen logischen Daten- und Protokollvolumes.

```
mkfs.xfs FC5_data_mnt00001-vol
mkfs.xfs FC5_data_mnt00002-vol
mkfs.xfs FC5_log_mnt00001-vol
mkfs.xfs FC5_log_mnt00002-vol
```

Erstellen von Bereitstellungspunkten

Erstellen Sie die erforderlichen Mount-Point-Verzeichnisse und legen Sie die Berechtigungen auf allen Worker- und Standby-Hosts fest:

```
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00002
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00002
sapcc-hana-tst:/ # mkdir -p /hana/shared
sapcc-hana-tst:/ # chmod -R 777 /hana/log/FC5
sapcc-hana-tst:/ # chmod -R 777 /hana/data/FC5
sapcc-hana-tst:/ # chmod 777 /hana/shared
```

Mounten Sie File-Systeme

Zur Montage des `/hana/shared` Dateisysteme während des Systemstarts mithilfe der `/etc/fstab` Konfigurationsdatei, fügen Sie die `/hana/shared` Dateisystem in die `/etc/fstab` Konfigurationsdatei jedes Hosts.

```
sapcc-hana-tst:/ # cat /etc/fstab
<storage-ip>:/hana_shared /hana/shared nfs rw,vers=3,hard,timeo=600,
intr,noatime,nolock 0 0
```

Alle Daten- und Protokolldateisysteme sind über den SAP HANA Storage Connector gemountet.

Führen Sie zum Mounten der Dateisysteme den aus `mount -a` Befehl an jedem Host.

I/O-Stack-Konfiguration für SAP HANA

Ab SAP HANA 1.0 SPS10 führte SAP Parameter ein, um das I/O-Verhalten anzupassen und die Datenbank für das verwendete Datei- und Speichersystem zu optimieren.

NetApp hat Performance-Tests durchgeführt, um die idealen Werte zu definieren. In der folgenden Tabelle sind die optimalen Werte aufgeführt, die aus den Leistungstests abgeleitet wurden.

Parameter	Wert
max_parallel_io_Requests	128
Async_read_Submit	Ein
Async_write_submit_Active	Ein
Async_Write_Submit_Blocks	Alle

Für SAP HANA 1.0 bis SPS12 können diese Parameter während der Installation der SAP HANA-Datenbank eingestellt werden, wie in SAP Note beschrieben "2267798 – Konfiguration der SAP HANA Datenbank während der Installation mit hdbparam".

Alternativ können die Parameter nach der SAP HANA-Datenbankinstallation über die eingestellt werden `hdbparam` Framework:

```
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.max_parallel_io_requests=128
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_write_submit_active=on
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_read_submit=on
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_write_submit_blocks=all
```

Ab SAP HANA 2.0 `hdbparam` Ist veraltet und die Parameter werden in die verschoben `global.ini` Datei: Die Parameter können über SQL-Befehle oder SAP HANA Studio eingestellt werden. Weitere Informationen finden Sie im SAP-Hinweis "2399079: Beseitigung von hdbparam in HANA 2". Die Parameter können auch im festgelegt werden `global.ini` Datei:

```
SS3adm@stlrx300s8-6: /usr/sap/SS3/SYS/global/hdb/custom/config> cat
global.ini
…
[fileio]
async_read_submit = on
async_write_submit_active = on
max_parallel_io_requests = 128
async_write_submit_blocks = all
…
```

Verwenden Sie für SAP HANA 2.0 SPS5 und höher den `setParameter.py` Skript zum Festlegen der richtigen Parameter.

```
fc5adm@sapcc-hana-tst-03:/usr/sap/FC5/HDB00/exe/python_support>
python setParameter.py
-set=SYSTEM/global.ini/fileio/max_parallel_io_requests=128
python setParameter.py -set=SYSTEM/global.ini/fileio/async_read_submit=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_active=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_blocks=all
```

SAP HANA Softwareinstallation

In diesem Abschnitt wird die Vorbereitung für die Installation von SAP HANA auf Single-Host- und Multiple-Host-Systemen beschrieben.

Installation auf Single-Host-System

Die Installation der SAP HANA-Software erfordert keine zusätzliche Vorbereitung auf ein Single-Host-System.

Installation auf Systemen mit mehreren Hosts

Erstellen Sie vor Beginn der Installation einen `global.ini` Datei, um die Verwendung des SAP-Speicheranschlusses während des Installationsprozesses zu ermöglichen. Der SAP-Speicheranschluss montiert die erforderlichen Dateisysteme während des Installationsprozesses an den Worker-Hosts. Der `global.ini` Die Datei muss in einem Dateisystem verfügbar sein, auf das über alle Hosts zugegriffen werden kann, z. B. die `/hana/shared` File-System.

Vor der Installation der SAP HANA-Software auf einem System mit mehreren Hosts müssen die folgenden Schritte durchgeführt werden:

1. Fügen Sie die folgenden Mount-Optionen für die Daten-LUNs und die Protokoll-LUNs auf dem hinzu `global.ini` Datei:
   - `relatime` Und `inode64` Für das Daten- und Protokolldateisystem
2. Fügen Sie die WWIDs der Daten- und Log-Partitionen hinzu. Die WWIDs müssen mit den im konfigurierten Aliasnamen übereinstimmen `/etc/multipath.conf` Datei:

   Die folgende Ausgabe zeigt ein Beispiel für ein 2+1-Setup mit mehreren Hosts unter Verwendung von LVM mit SID=FC5.

```
sapcc-hana-tst-03:/hana/shared # cat global.ini
[communication]
listeninterface = .global
[persistence]
basepath_datavolumes = /hana/data/FC5
basepath_logvolumes = /hana/log/FC5
[storage]
ha_provider = hdb_ha.fcClientLVM
partition_*_*__prtype = 5
partition_*_data__mountOptions = -o relatime,inode64
partition_*_log__mountOptions = -o relatime,inode64
partition_1_data__lvmname = FC5_data_mnt00001-vol
partition_1_log__lvmname = FC5_log_mnt00001-vol
partition_2_data__lvmname = FC5_data_mnt00002-vol
partition_2_log__lvmname = FC5_log_mnt00002-vol
sapcc-hana-tst-03:/hana/shared #
```

   Starten Sie die Installation mithilfe des SAP hdblcm-Installationstools, indem Sie den folgenden Befehl auf einem der Worker-Hosts ausführen. Verwenden Sie die `addhosts` Option, um den zweiten Worker (sapcc-hana-tst-06) und den Standby-Host (sapcc-hana-tst-07) hinzuzufügen.

> Das Verzeichnis, in dem die vorbereitete `global.ini` Datei gespeichert wird(`--storage_cfg=/hana/shared`, ist mit der CLI-Option) enthalten `storage_cfg`.

Je nach verwendeter Betriebssystemversion kann es erforderlich sein, Python 2.7 zu installieren, bevor die SAP HANA-Datenbank installiert wird.

```
./hdblcm --action=install --addhosts=sapcc-hana-tst
-06:role=worker:storage_partition=2,sapcc-hana-tst-07:role=standby
--storage_cfg=/hana/shared/

AP HANA Lifecycle Management - SAP HANA Database 2.00.073.00.1695288802
************************************************************************


Scanning software locations...
Detected components:
    SAP HANA AFL (incl.PAL,BFL,OFL) (2.00.073.0000.1695321500) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_AFL_LINUX_X86_64/packages
    SAP HANA Database (2.00.073.00.1695288802) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
    SAP HANA Database Client (2.18.24.1695756995) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/SAP_HANA_CLIENT/client
    SAP HANA Studio (2.3.75.000000) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_STUDIO_LINUX_X86_64/studio
    SAP HANA Local Secure Store (2.11.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HANA_LSS_24_LINUX_X86_64/packages
    SAP HANA XS Advanced Runtime (1.1.3.230717145654) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_RT_10_LINUX_X86_64/packages
    SAP HANA EML AFL (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_EML_AFL_10_LINUX_X86_64/packages
    SAP HANA EPM-MDS (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/SAP_HANA_EPM-MDS_10/packages
    Automated Predictive Library (4.203.2321.0.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/PAAPL4_H20_LINUX_X86_64/apl-
4.203.2321.0-hana2sp03-linux_x64/installer/packages
    GUI for HALM for XSA (including product installer) Version 1
(1.015.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACALMPIUI15_0.zip
    XSAC FILEPROCESSOR 1.0 (1.000.102) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACFILEPROC00_102.zip
    SAP HANA tools for accessing catalog content, data preview, SQL
```

```
console, etc. (2.015.230503) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_HRTT_20/XSACHRTT15_230503.zip
    Develop and run portal services for customer applications on XSA
(2.007.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACPORTALSERV07_0.zip
    The SAP Web IDE for HANA 2.0 (4.007.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_SAP_WEB_IDE_20/XSACSAPWEBIDE07_0.zip
    XS JOB SCHEDULER 1.0 (1.007.22) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACSERVICES07_22.zip
    SAPUI5 FESV6 XSA 1 - SAPUI5 1.71 (1.071.52) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV671_52.zip
    SAPUI5 FESV9 XSA 1 - SAPUI5 1.108 (1.108.5) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV9108_5.zip
    SAPUI5 SERVICE BROKER XSA 1 - SAPUI5 Service Broker 1.0 (1.000.4) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5SB00_4.zip
    XSA Cockpit 1 (1.001.37) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACXSACOCKPIT01_37.zip


SAP HANA Database version '2.00.073.00.1695288802' will be installed.

Select additional components for installation:

  Index | Components      | Description

-------------------------------------------------------------------------
--------------------------
  1     | all             | All components
  2     | server          | No additional components
  3     | client          | Install SAP HANA Database Client version
2.18.24.1695756995
  4     | lss             | Install SAP HANA Local Secure Store version
2.11.0
  5     | studio          | Install SAP HANA Studio version
2.3.75.000000
  6     | xs              | Install SAP HANA XS Advanced Runtime version
1.1.3.230717145654
  7     | afl             | Install SAP HANA AFL (incl.PAL,BFL,OFL)
version 2.00.073.0000.1695321500
  8     | eml             | Install SAP HANA EML AFL version
2.00.073.0000.1695321500
```

```
  9     | epmmds           | Install SAP HANA EPM-MDS version
2.00.073.0000.1695321500
  10    | sap_afl_sdk_apl | Install Automated Predictive Library version
4.203.2321.0.0

Enter comma-separated list of the selected indices [3,4]: 2,3
```

3. Vergewissern Sie sich, dass das Installationstool alle ausgewählten Komponenten bei allen Worker- und Standby-Hosts installiert hat.

Hinzufügen von zusätzlichen Daten-Volume-Partitionen für SAP HANA Single-Host-Systeme

Ab SAP HANA 2.0 SPS4 können weitere Daten-Volume-Partitionen konfiguriert werden. Mit dieser Funktion können Sie zwei oder mehr LUNs für das Daten-Volume einer SAP HANA-Mandantendatenbank konfigurieren und eine Skalierung über die Größe und Performance-Grenzen einer einzelnen LUN hinaus vornehmen.

> Es ist nicht nötig, mehrere Partitionen zu verwenden, um die SAP HANA-KPIs zu erfüllen. Eine einzelne LUN mit einer einzigen Partition erfüllt die erforderlichen KPIs.

> Die Nutzung von zwei oder mehr einzelnen LUNs für das Daten-Volume ist nur für SAP HANA Single-Host-Systeme verfügbar. Der für SAP HANA mehrere-Host-Systeme erforderliche SAP-Storage-Connector unterstützt nur ein Gerät für das Daten-Volume.

Das Hinzufügen weiterer Partitionen für Datenvolumen kann jederzeit erfolgen, erfordert aber unter Umständen einen Neustart der SAP HANA Datenbank.

Aktivieren von zusätzlichen Partitionen für Volumes

Führen Sie folgende Schritte aus, um zusätzliche Datenträger-Partitionen zu aktivieren:

1. Fügen Sie den folgenden Eintrag in das hinzu `global.ini` Datei:

```
[customizable_functionalities]
persistence_datavolume_partition_multipath = true
```

2. Starten Sie die Datenbank neu, um die Funktion zu aktivieren. Hinzufügen des Parameters über SAP HANA Studio zum `global.ini` Die Datei unter Verwendung der Systemdb-Konfiguration verhindert den Neustart der Datenbank.

Konfiguration von Volume und LUN

Das Layout der Volumes und LUNs ist wie das Layout eines einzelnen Hosts mit einer Daten-Volume-Partition, aber mit einem zusätzlichen Daten-Volume und LUN auf einem anderen Aggregat als dem Protokoll-Volume und dem anderen Daten-Volume gespeichert. Die folgende Tabelle zeigt eine Beispielkonfiguration eines SAP HANA Einzelhost-Systems mit zwei Daten-Volume-Partitionen.

Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregieren 2 bei Controller B
Datenvolumen: SID_Data_mnt00001	Gemeinsam genutztes Volume: SID_shared	Datenvolumen: SID_data2_mnt00001	Protokollvolumen: SID_log_mnt00001

Die folgende Tabelle zeigt ein Beispiel für die Mount-Punkt-Konfiguration für ein System mit einem einzelnen Host mit zwei Daten-Volume-Partitionen.

LUN	Bereitstellungspunkt beim HANA-Host	Hinweis
SID_Data_mnt00001	/hana/Data/SID/mnt00001	Mit /etc/fstab-Eintrag montiert
SID_data2_mnt00001	/hana/data2/SID/mnt00001	Mit /etc/fstab-Eintrag montiert
SID_Log_mnt00001	/hana/log/SID/mnt00001	Mit /etc/fstab-Eintrag montiert
SID_freigegeben	/hana/Shared/SID	Mit /etc/fstab-Eintrag montiert

Erstellen Sie die neuen Daten-LUNs entweder mit ONTAP System Manager oder mit der ONTAP CLI.

Host-Konfiguration

Gehen Sie wie folgt vor, um einen Host zu konfigurieren:

1. Konfigurieren Sie Multipathing für die zusätzlichen LUNs, wie im Kapitel "Host-Setup" .
2. Erstellen Sie das XFS-Dateisystem auf jeder zusätzlichen LUN, die zum HANA-System gehört:

```
stlrx300s8-6:/ # mkfs.xfs /dev/mapper/hana-FC5_data2_mnt00001
```

3. Fügen Sie die zusätzlichen Dateisysteme dem hinzu `/etc/fstab` Konfigurationsdatei

> Die XFS-Dateisysteme für die Daten- und Protokoll-LUN müssen mit dem gemountet werden `relatime` Und `inode64` Mount-Optionen:

```
stlrx300s8-6:/ # cat /etc/fstab
/dev/mapper/hana-FC5_shared /hana/shared xfs defaults 0 0
/dev/mapper/hana-FC5_log_mnt00001 /hana/log/FC5/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/hana-FC5_data_mnt00001 /hana/data/FC5/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/hana-FC5_data2_mnt00001 /hana/data2/FC5/mnt00001 xfs
relatime,inode64 0 0
```

4. Erstellen Sie Mount-Punkte und legen Sie Berechtigungen auf dem Datenbank-Host fest.

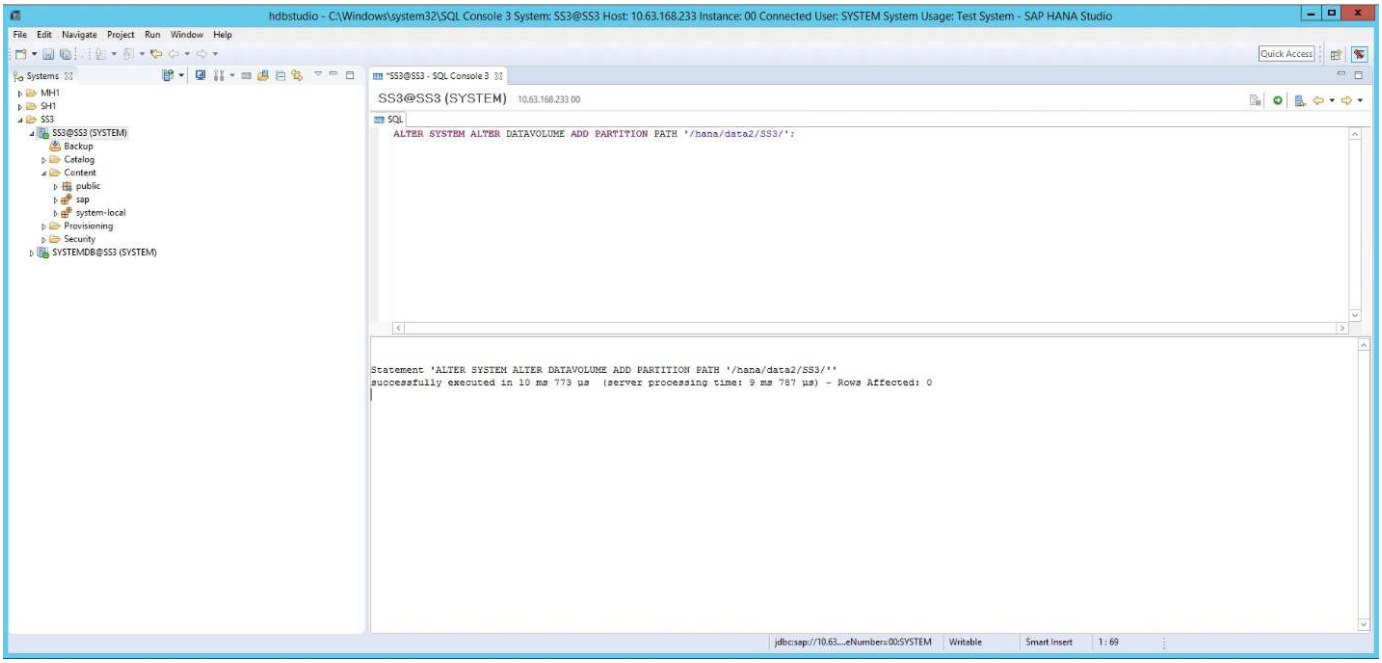
```
stlrx300s8-6:/ # mkdir -p /hana/data2/FC5/mnt00001
stlrx300s8-6:/ # chmod -R 777 /hana/data2/FC5
```

5. Mounten Sie die Dateisysteme, führen Sie den aus `mount -a` Befehl.

Hinzufügen einer zusätzlichen datavolume-Partition

Um Ihrer Mandanten-Datenbank eine zusätzliche Datavolume-Partition hinzuzufügen, führen Sie die folgende SQL-Anweisung mit der Mandanten-Datenbank aus. Jede weitere LUN kann einen anderen Pfad haben:

```
ALTER SYSTEM ALTER DATAVOLUME ADD PARTITION PATH '/hana/data2/SID/';
```



Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten bzw. auf den folgenden Websites:

- "SAP HANA Softwarelösungen"
- "TR-4646: SAP HANA Disaster Recovery with Storage Replication"
- "TR-4614: SAP HANA Backup and Recovery with SnapCenter"
- "TR-4667: Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter"
- NetApp Dokumentationszentren

  "https://www.netapp.com/support-and-training/documentation/"

- SAP Certified Enterprise Storage Hardware for SAP HANA

  "https://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/"

- SAP HANA Storage-Anforderungen

  "https://www.sap.com/documents/2024/03/146274d3-ae7e-0010-bca6-c68f7e60039b.html"

- SAP HANA Tailored Data Center Integration Häufig gestellte Fragen

  "https://www.sap.com/documents/2016/05/e8705aae-717c-0010-82c7-eda71af511fa.html"

- SAP HANA auf VMware vSphere Wiki

  "https://help.sap.com/docs/SUPPORT_CONTENT/virtualization/3362185751.html"

- Best Practices Guide für SAP HANA auf VMware vSphere

  "https://www.vmware.com/docs/sap_hana_on_vmware_vsphere_best_practices_guide-white-paper"

Aktualisierungsverlauf

An dieser Lösung wurden seit ihrer ersten Veröffentlichung folgende technische Änderungen vorgenommen:

Datum	Zusammenfassung aktualisieren
Oktober 2015	Ausgangsversion
März 2016	Aktualisierte Kapazitätsdimensionierung
Februar 2017	Neue NetApp Storage-Systeme und Festplatten-Shelfs Neue Funktionen von ONTAP 9 neuen Betriebssystemversionen (SLES12 SP1 und RHEL 7.2) Neue SAP HANA-Version
Juli 2017	Kleine Updates
September 2018	Neue NetApp Storage-Systeme Neue Betriebssystemversionen (SLES12 SP3 und RHEL 7.4) zusätzliche kleinere Updates für SAP HANA 2.0 SPS3
November 2019	Neue NetApp Storage-Systeme und NVMe Shelf Neue Betriebssystemversionen (SLES12 SP4, SLES 15 und RHEL 7.6) zusätzliche kleinere Updates
April 2020	Neue Speichersysteme der AFF ASA-Serie führen seit SAP HANA 2.0 SPS4 eine Funktion für mehrere Datenpartitionen ein
Juni 2020	Zusätzliche Informationen über optionale Funktionalitäten kleine Updates
Februar 2021	Linux LVM unterstützt neue NetApp Storage-Systeme Neue Betriebssystemversionen (SLES15SP2, RHEL 8)
April 2021	VMware vSphere-spezifische Informationen hinzugefügt
September 2022	Neue Betriebssystemversionen
August 2023	Neue Storage-Systeme (AFF C-Serie)
Mai 2024	Neue Storage-Systeme (AFF A-Series)
September 2024	Neue Storage-Systeme (ASA A-Series)

Datum	Zusammenfassung aktualisieren
November 2024	Neue Storage-Systeme
Februar 2025	Neue Storage-Systeme
Juli 2025	Kleine Updates

Konfigurationsleitfaden für SAP HANA auf NetApp AFF-Systemen mit NFS

SAP HANA on NetApp AFF Systems with NFS - Konfigurationsleitfaden

Die NetApp AFF A-Series-Produktfamilie wurde für den Einsatz mit SAP HANA in maßgeschneiderten Rechenzentrumsintegrationsprojekten (TDI) zertifiziert. Dieses Handbuch enthält Best Practices für SAP HANA auf dieser Plattform für NFS.

Marco Schoen, NetApp

Diese Zertifizierung gilt für folgende Modelle:

- AFF A20, AFF A30, AFF A50, AFF A70, AFF A90, AFF A1K

Eine vollständige Liste der zertifizierten NetApp Storage-Lösungen für SAP HANA finden Sie unter "Zertifiziertes und unterstütztes SAP HANA-Hardwaresverzeichnis".

Dieses Dokument beschreibt die ONTAP-Konfigurationsanforderungen für das NFS-Protokoll, Version 3 (NFSv3) oder NFS-Protokoll, Version 4 (NFSv4.1).

Es werden nur NFS-Versionen 3 oder 4.1 unterstützt. NFS-Versionen 1, 2, 4.0 und 4.2 werden nicht unterstützt.

Die in diesem Dokument beschriebene Konfiguration ist erforderlich, um die erforderlichen SAP HANA KPIs und die beste Performance für SAP HANA zu erreichen. Wenn Sie Einstellungen oder Funktionen ändern, die nicht in diesem Dokument aufgeführt sind, kann dies zu einer Performance-Verschlechterung oder zu einem unerwarteten Verhalten führen. Diese Einstellungen sollten nur vorgenommen werden, wenn dies durch den NetApp Support empfohlen wird.

Die Konfigurationsleitfäden für NetApp AFF Systeme mit FCP und für FAS Systeme mit NFS oder FCP sind unter folgenden Links verfügbar:

- "Technischer Bericht: SAP HANA on NetApp FAS Systems with FCP"
- "Technischer Bericht: SAP HANA on NetApp FAS Systems with NFS"
- "Technischer Bericht: SAP HANA on NetApp AFF Systems with FCP"
- "Technischer Bericht: SAP HANA on NetApp ASA Systems with FCP"

In der folgenden Tabelle sind die unterstützten Kombinationen aus der NFS-Version, der NFS-Sperre und den erforderlichen Isolierungs-Implementierungen in Abhängigkeit von der Konfiguration der SAP HANA Datenbank aufgeführt.

Für SAP HANA Einzel-Host-Systeme oder mehrere Hosts, die kein Host Auto-Failover verwenden, werden NFSv3 und NFSv4 unterstützt.

Für SAP HANA unterstützen mehrere Host-Systeme mit Host Auto-Failover nur NetApp NFSv4, während die NFSv4-Sperrung als Alternative zu einer serverspezifischen STONITH-Implementierung (SAP HANA HA/DR-Provider) dient.

SAP HANA	NFS-Version	NFS-Sperrung	SAP HANA HA-/DR-PROVIDER
SAP HANA ein Host, mehrere Hosts ohne Host Auto-Failover	NFSv3	Aus	k. A.
	NFSv4	Ein	k. A.
SAP HANA mehrere Hosts mit Host Auto-Failover	NFSv3	Aus	Serverspezifische STONITH-Implementierung erforderlich
	NFSv4	Ein	Nicht erforderlich

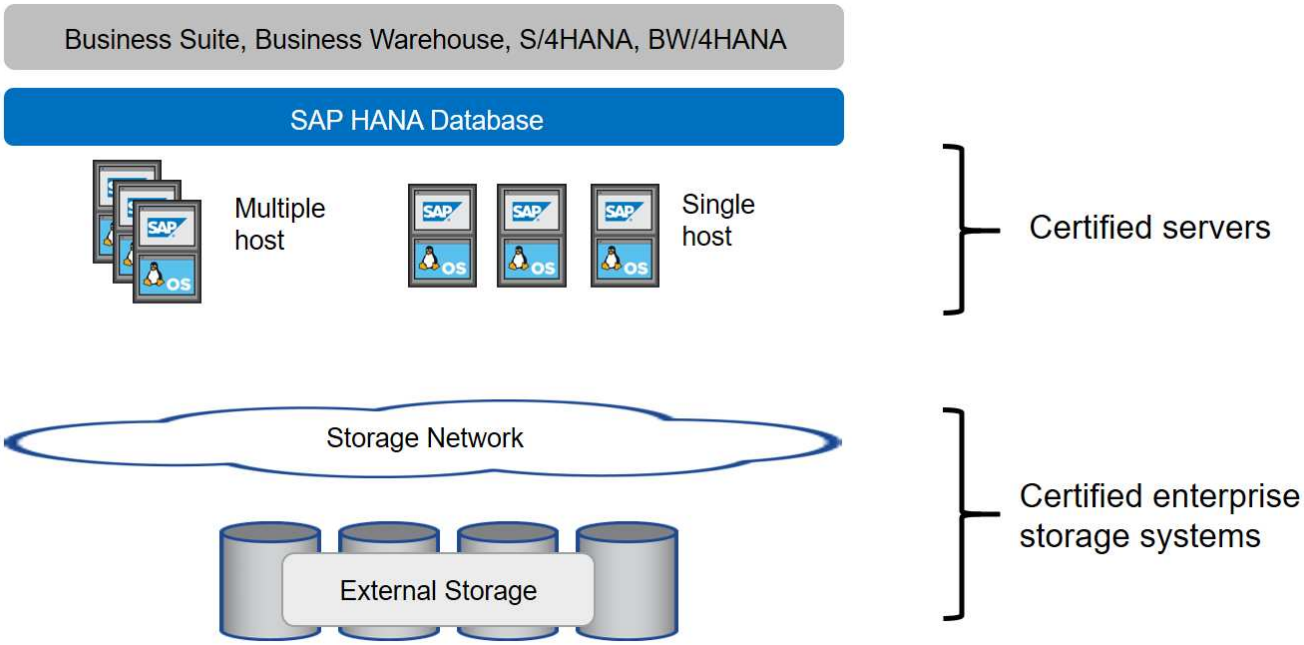
Eine serverspezifische STONITH-Implementierung ist nicht Teil dieses Leitfadens. Wenden Sie sich für eine solche Implementierung an Ihren Server-Anbieter.

Dieses Dokument enthält Konfigurationsempfehlungen für SAP HANA, die auf physischen Servern und virtuellen Servern ausgeführt werden, die VMware vSphere verwenden.

In den entsprechenden SAP-Hinweisen finden Sie die Konfigurationsrichtlinien für das Betriebssystem und die HANA-spezifischen Linux-Kernel-Abhängigkeiten. Weitere Informationen finden Sie im SAP-Hinweis 2235581: Unterstützte SAP HANA-Betriebssysteme.

SAP HANA Tailored Datacenter Integration

NetApp AFF Storage Controller sind im SAP HANA TDI Programm unter Verwendung von NFS- (NAS) und FC (SAN) Protokollen zertifiziert. Sie können in allen aktuellen SAP HANA-Szenarien, wie SAP Business Suite on HANA, S/4HANA, BW/4HANA oder SAP Business Warehouse on HANA, entweder in Konfigurationen mit einem Host oder mehreren Hosts implementiert werden. Alle Server, die für den Einsatz mit SAP HANA zertifiziert sind, können mit von NetApp zertifizierten Storage-Lösungen kombiniert werden. In der folgenden Abbildung finden Sie einen Überblick über die Architektur von SAP HANA TDI.



Weitere Informationen zu den Voraussetzungen und Empfehlungen für die produsti SAP HANA Systeme finden Sie in der folgenden Ressource:

- "SAP HANA Tailored Data Center Integration Häufig gestellte Fragen"

SAP HANA mit VMware vSphere

Für die Verbindung von Storage mit Virtual Machines (VMs) gibt es verschiedene Optionen. Die bevorzugte Option ist, die Storage Volumes mit NFS direkt aus dem Gastbetriebssystem zu verbinden. Bei Verwendung dieser Option unterscheidet sich die Konfiguration von Hosts und Storage nicht zwischen physischen Hosts und VMs.

NFS Datastores und VVOL Datastores mit NFS werden ebenfalls unterstützt. Bei beiden Optionen muss nur ein SAP HANA Daten- oder Protokoll-Volume im Datastore für Produktionsanwendungsfälle gespeichert werden.

In diesem Dokument wird das empfohlene Setup mit direkten NFS-Mounts vom Gastbetriebssystem beschrieben.

Weitere Informationen zur Verwendung von vSphere mit SAP HANA finden Sie unter den folgenden Links:

- "SAP HANA on VMware vSphere - Virtualization - Community Wiki"
- "Best Practices Guide für SAP HANA auf VMware vSphere"
- "2161991 - Konfigurationsrichtlinien für VMware vSphere - SAP ONE Support Launchpad (Anmeldung erforderlich)"

Der Netapp Architektur Sind

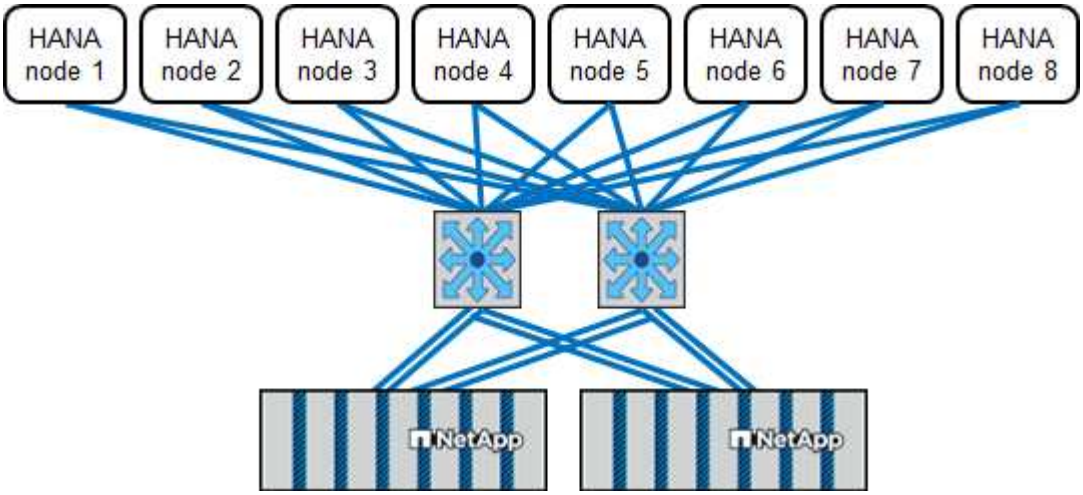
SAP HANA-Hosts sind über eine redundante 10-GbE- oder schnellere Netzwerkinfrastruktur mit Storage Controllern verbunden. Die Kommunikation zwischen SAP HANA-Hosts und Storage-Controllern basiert auf dem NFS-Protokoll. Für eine fehlertolerante SAP HANA Host-to-Storage-Konnektivität ist eine redundante Switching-

Infrastruktur erforderlich, die bei Switch- oder NIC-Ausfällen (Network Interface Card) eingesetzt werden kann.

Die Switches können die Leistung einzelner Ports mit Port-Kanälen aggregieren, um als einzelne logische Einheit auf Hostebene angezeigt zu werden.

Verschiedene Modelle der AFF Produktfamilie können auf der Storage-Ebene miteinander kombiniert werden, um Wachstum und unterschiedliche Anforderungen an Performance und Kapazität zu ermöglichen. Die maximale Anzahl an SAP HANA-Hosts, die an das Storage-System angeschlossen werden können, sind durch die SAP HANA-Performance-Anforderungen und das Modell des verwendeten NetApp Controllers definiert. Die Anzahl der benötigten Festplatten-Shelfs wird nur von den Kapazitäts- und Performance-Anforderungen der SAP HANA Systeme bestimmt.

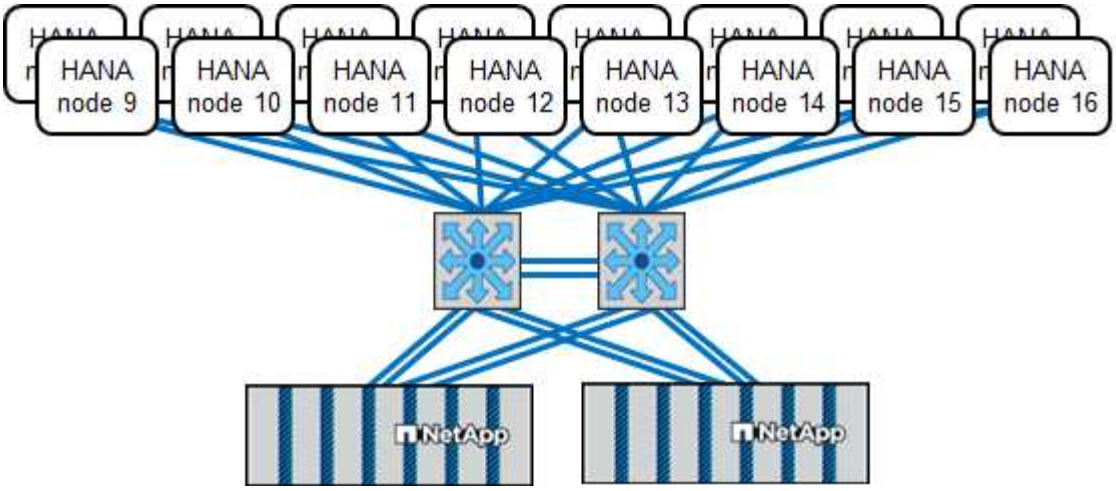
Die folgende Abbildung zeigt eine Beispielkonfiguration mit acht SAP HANA-Hosts, die an ein Storage-HA-Paar angeschlossen sind.



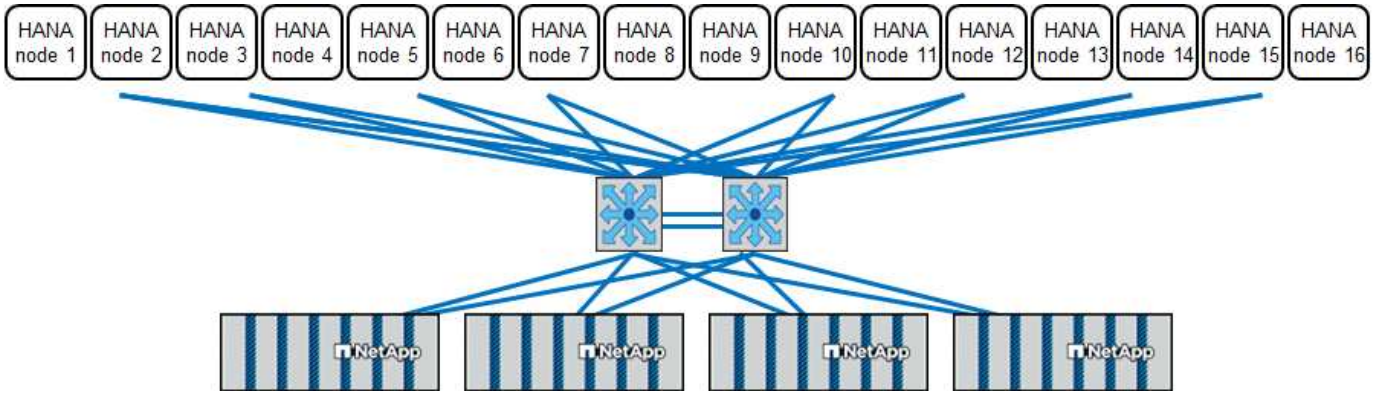
Die Architektur lässt sich in zwei Dimensionen skalieren:

- Durch Anbindung zusätzlicher SAP HANA-Hosts und Storage-Kapazität an den vorhandenen Storage, falls die Storage-Controller genügend Performance bieten, um die aktuellen Performance-Kennzahlen (KPIs) von SAP HANA zu erfüllen.
- Durch Hinzufügen weiterer Storage-Systeme mit zusätzlicher Storage-Kapazität für die zusätzlichen SAP HANA-Hosts

Die folgende Abbildung zeigt eine Beispielkonfiguration, in der mehr SAP HANA-Hosts mit den Storage-Controllern verbunden sind. In diesem Beispiel sind mehr Platten-Shelves erforderlich, um die Kapazitäts- und Performance-Anforderungen der 16 SAP HANA-Hosts zu erfüllen. Abhängig vom Gesamtdurchsatz müssen Sie den Storage Controllern weitere 10-GbE- oder schnellere Verbindungen hinzufügen.



Unabhängig vom implementierten AFF System lässt sich die SAP HANA-Landschaft auch durch Hinzufügen eines beliebigen zertifizierten Storage-Controllers skalieren, um die gewünschte Node-Dichte zu erfüllen, wie in der folgenden Abbildung dargestellt.



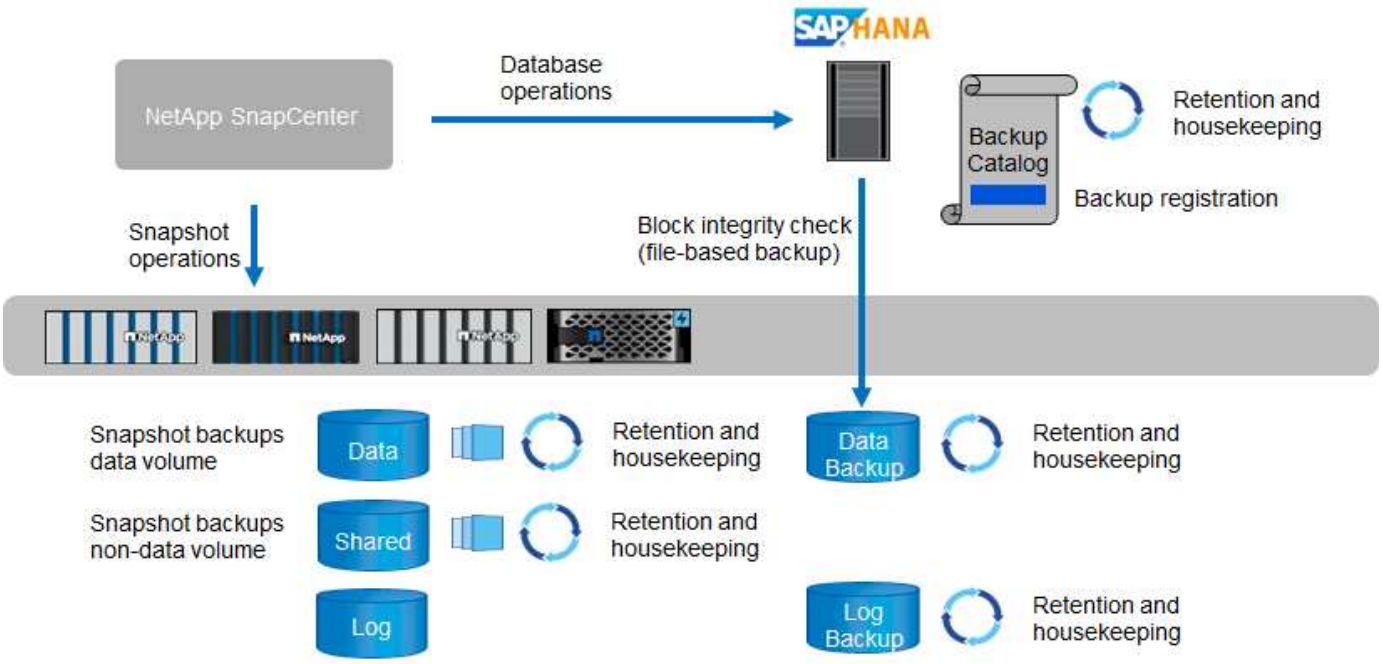
SAP HANA Backup

Die auf allen NetApp Storage-Controllern vorhandene ONTAP Software bietet einen integrierten Mechanismus zur Sicherung von SAP HANA Datenbanken, ohne die Performance zu beeinträchtigen. Storage-basierte NetApp Snapshot-Backups sind eine vollständig unterstützte und integrierte Backup-Lösung, die für einzelne SAP HANA Container sowie für SAP HANA Multitenant Database Container (MDC) Systeme mit einem einzelnen Mandanten oder mehreren Mandanten verfügbar ist.

Storage-basierte Snapshot Backups werden über das NetApp SnapCenter Plug-in für SAP HANA implementiert. Benutzer können auf diese Weise konsistente Storage-basierte Snapshot Backups mithilfe der Schnittstellen erstellen, die nativ von SAP HANA Datenbanken bereitgestellt werden. SnapCenter registriert jedes der Snapshot-Backups im SAP HANA-Backup-Katalog. Die Backups von SnapCenter sind somit innerhalb von SAP HANA Studio und Cockpit sichtbar, wo sie direkt für Restore- und Recovery-Vorgänge selektiert werden können.

Mit der NetApp SnapMirror Technologie können auf einem Storage-System erstellte Snapshot Kopien in ein sekundäres Backup-Storage-System repliziert werden, das über SnapCenter gesteuert wird. Für jedes der Backup-Sätze auf dem primären Storage und für die Backup-Sätze auf den sekundären Storage-Systemen können somit unterschiedliche Backup-Aufbewahrungsrichtlinien definiert werden. Das SnapCenter Plug-in für SAP HANA managt automatisch die Aufbewahrung von auf Snapshot Kopien basierenden Daten-Backups und Log-Backups, einschließlich der allgemeinen Ordnung des Backup-Katalogs. Das SnapCenter Plug-in für SAP HANA ermöglicht darüber hinaus die Durchführung einer Block-Integritätsprüfung der SAP HANA Datenbank durch Ausführen eines dateibasierten Backups.

Die Datenbankprotokolle können mithilfe eines NFS-Mount-Speichers direkt auf dem sekundären Storage gesichert werden, wie in der folgenden Abbildung dargestellt.



Storage-basierte Snapshot Backups bieten im Vergleich zu herkömmlichen dateibasierten Backups deutliche Vorteile. Zu diesen Vorteilen zählen unter anderem die folgenden:

- Schnelleres Backup (einige Minuten)
- Reduzierte Recovery-Zeitvorgabe (Recovery Time Objective, RTO) aufgrund einer wesentlich schnelleren Restore-Zeit auf der Storage-Ebene (wenige Minuten) und häufigerer Backups
- Kein Performance-Abfall des SAP HANA-Datenbankhosts, -Netzwerks oder -Storage während Backup- und Recovery-Vorgängen
- Platzsparende und bandbreiteneffiziente Replizierung auf Basis von Blockänderungen auf sekundärem Storage

Detaillierte Informationen zur Backup- und Recovery-Lösung von SAP HANA finden Sie unter "TR-4614: SAP HANA Backup and Recovery with SnapCenter".

Disaster Recovery für SAP HANA

SAP HANA Disaster-Recovery (DR) kann mithilfe von SAP HANA-Systemreplizierung auf der Datenbankebene oder auf der Storage-Ebene mithilfe von Storage-Replizierungstechnologien durchgeführt werden. Der folgende Abschnitt bietet einen Überblick über Disaster-Recovery-Lösungen basierend auf der Storage-Replizierung.

Weitere Informationen zu Disaster-Recovery-Lösungen für SAP HANA finden Sie unter "TR-4646: SAP HANA Disaster Recovery with Storage Replication".

Storage-Replizierung basierend auf SnapMirror

Die folgende Abbildung zeigt eine Disaster Recovery-Lösung für drei Standorte mit synchroner SnapMirror Replizierung am lokalen DR-Datacenter und asynchroner SnapMirror Replizierung der Daten in das Remote-DR-Datacenter.

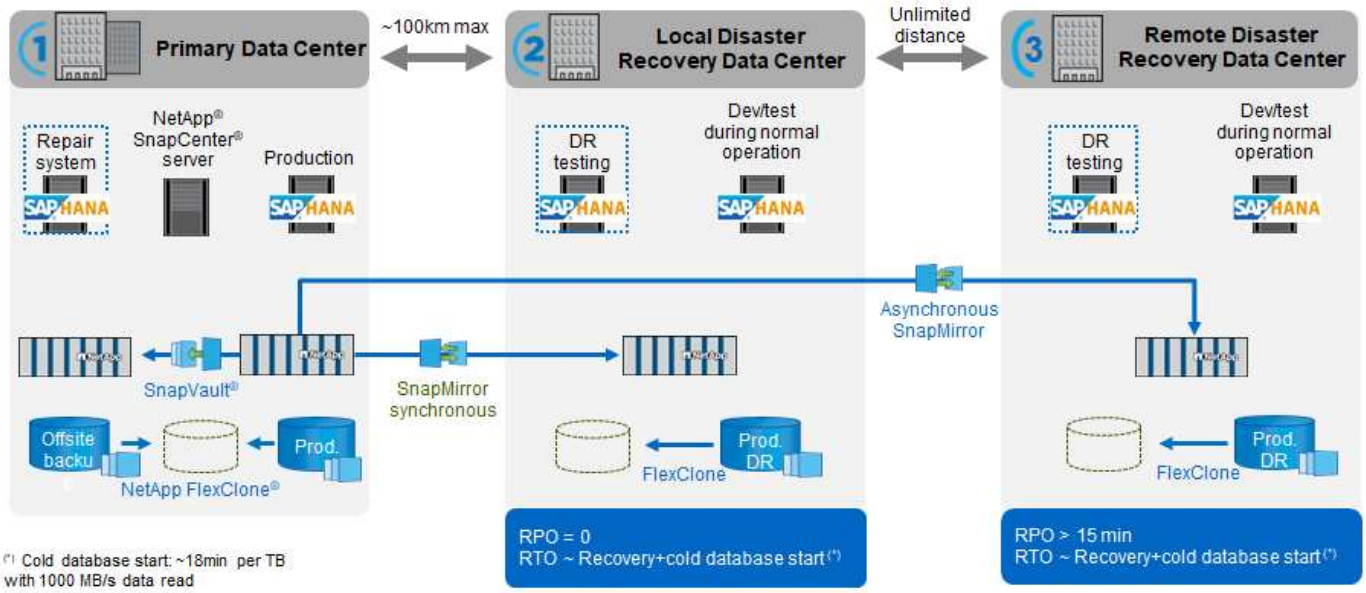
Die Datenreplizierung mit synchronem SnapMirror sorgt für einen RPO von null. Die Entfernung zwischen dem primären und dem lokalen DR-Datacenter ist auf etwa 100 km beschränkt.

Der Schutz vor Ausfällen des primären und lokalen DR-Standorts wird durch Replizieren der Daten zu einem dritten Remote-DR-Datacenter mithilfe von asynchronem SnapMirror durchgeführt. Der RPO hängt von der Häufigkeit der Replizierungs-Updates und der Übertragungsgeschwindigkeit ab. Theoretisch ist die Entfernung unbegrenzt, aber die Obergrenze hängt von der zu übertragenden Datenmenge und der zwischen den Rechenzentren verfügbaren Verbindung ab. Typische RPO-Werte liegen im Bereich von 30 Minuten bis mehreren Stunden.

Das RTO für beide Replizierungsmethoden hängt in erster Linie von der Zeit ab, die zum Starten der HANA-Datenbank am DR-Standort und zum Laden der Daten in den Speicher erforderlich ist. Mit der Annahme, dass die Daten mit einem Durchsatz von 1000 MBit/s gelesen werden, dass das Laden von 1 TB Daten ungefähr 18 Minuten dauert.

Die Server an den DR-Standorten können im normalen Betrieb als Entwicklungs- und Testsysteme genutzt werden. Bei einem Ausfall müssten die Entwicklungs- und Testsysteme heruntergefahren und als DR-Produktionsserver gestartet werden.

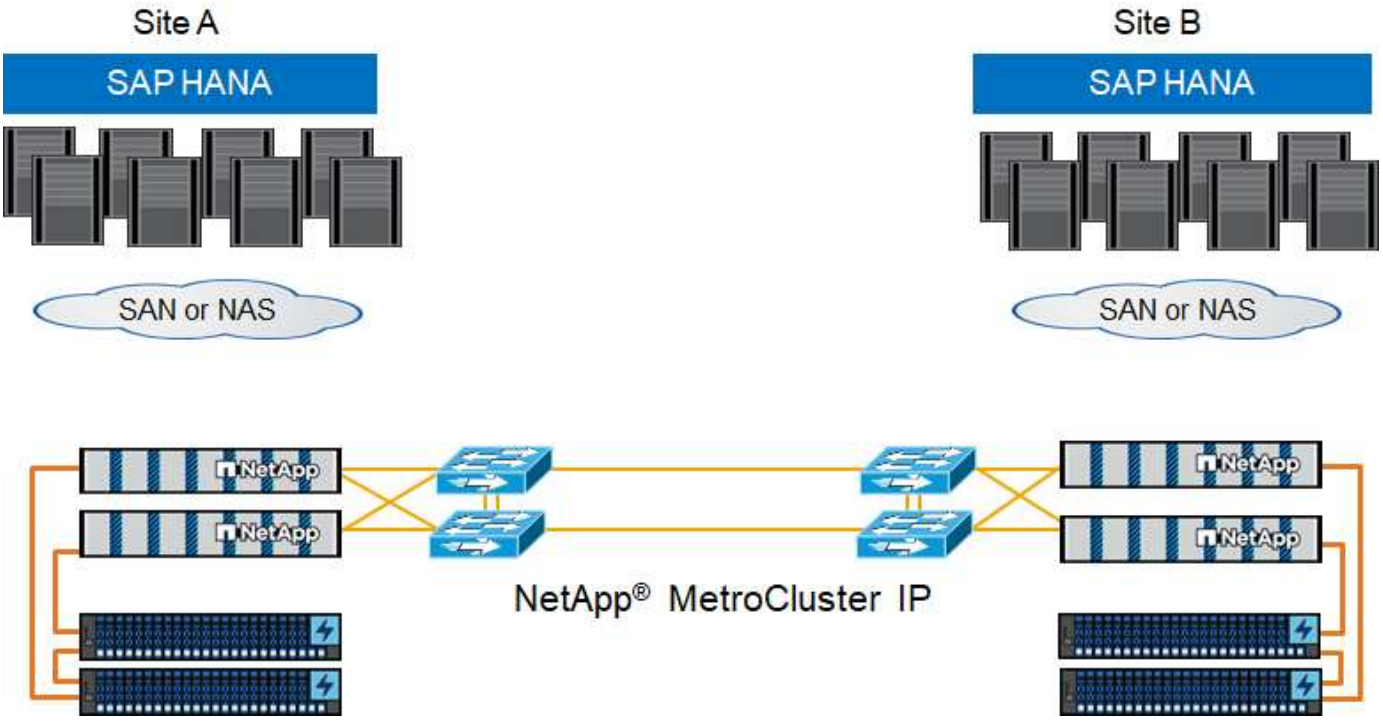
Beide Replizierungsmethoden ermöglichen die Durchführung von DR-Workflow-Tests ohne Auswirkungen auf RPO und RTO. FlexClone Volumes werden auf dem Storage erstellt und an die DR-Testserver angeschlossen.



Die synchrone Replizierung bietet den StrictSync-Modus. Wenn der Schreibvorgang auf den sekundären Storage aus irgendeinem Grund nicht abgeschlossen wird, fällt der Applikations-I/O aus. Dadurch wird sichergestellt, dass die primären und sekundären Storage-Systeme identisch sind. Der Applikations-I/O zum primären Volume wird erst wieder fortgesetzt, nachdem die SnapMirror-Beziehung zum InSync-Status zurückkehrt. Falls der Primär-Storage ausfällt, kann der Applikations-I/O nach dem Failover ohne Datenverlust auf dem sekundären Storage fortgesetzt werden. Im StrictSync-Modus ist der RPO immer Null.

Storage-Replizierung basierend auf MetroCluster

Die folgende Abbildung bietet einen allgemeinen Überblick über die Lösung. Das Storage-Cluster an jedem Standort bietet lokale Hochverfügbarkeit und wird für den Produktions-Workload verwendet. Die Daten aller Standorte werden synchron zum anderen Standort repliziert und sind im Fall eines Disaster Failovers verfügbar.



Storage-Dimensionierung

Der folgende Abschnitt bietet einen Überblick über die erforderlichen Performance- und Kapazitätsüberlegungen, die für die Dimensionierung eines Storage-Systems für SAP HANA erforderlich sind.

Wenden Sie sich an NetApp oder Ihren Vertriebsmitarbeiter von NetApp Partner, um Sie beim Aufbau einer Storage-Umgebung in einer passenden Größe zu unterstützen.

Überlegungen zur Performance

SAP hat eine statische Reihe von Storage-KPIs definiert. Diese KPIs sind für alle produktiven SAP HANA-Umgebungen gültig, unabhängig von der Speichergröße der Datenbank-Hosts und der Anwendungen, die die SAP HANA-Datenbank nutzen. Diese KPIs gelten für Single-Host-, mehrere Hosts-, Business Suite on HANA-, Business Warehouse on HANA-, S/4HANA- und BW/4HANA-Umgebungen. Daher hängt der aktuelle Ansatz zur Performance-Dimensionierung nur von der Anzahl aktiver SAP HANA-Hosts ab, die an das Storage-System angeschlossen sind.

Storage-Performance-KPIs sind nur für SAP HANA Produktionssysteme erforderlich, können aber in allen HANA-Systemen implementiert werden.

SAP liefert ein Performance-Testtool, das zur Validierung der Performance des Storage-Systems für aktive an den Storage angeschlossene SAP HANA-Hosts verwendet werden muss.

NetApp hat die maximale Anzahl an SAP HANA Hosts getestet und vordefiniert, die an ein bestimmtes Storage-Modell angeschlossen werden können, ohne dabei die erforderlichen Storage-KPIs von SAP für produktionsbasierte SAP HANA Systeme zu erfüllen.

Mit dem SAP Performance-Testtool wurde die maximale Anzahl an SAP HANA Hosts ermittelt, die in einem Platten-Shelf ausgeführt werden können und die Mindestanzahl der pro SAP HANA Host benötigten SSDs

erforderlich ist. Dieser Test berücksichtigt nicht die tatsächlichen Storage-Kapazitätsanforderungen der Hosts. Außerdem müssen die Kapazitätsanforderungen berechnet werden, um die tatsächlich benötigte Storage-Konfiguration zu bestimmen.

SAS-Festplatten-Shelf

Bei dem 12-GB-SAS-Festplatten-Shelf (Serial-Attached SCSI) (DS224C) wird die Performance-Dimensionierung mithilfe der folgenden festen Festplatten-Shelf-Konfigurationen durchgeführt:

- Halb beladene Festplatten-Shelfs mit 12 SSDs
- Voll beladene Festplatten-Shelfs mit 24 SSDs

> Beide Konfigurationen verwenden Advanced Disk Partitioning (ADPv2). Ein halb beladenes Platten-Shelf unterstützt bis zu neun SAP HANA-Hosts, während ein voll beladenes Shelf bis zu 14 Hosts in einem einzigen Platten-Shelf unterstützt. Die SAP HANA-Hosts müssen auf beide Storage Controller verteilt sein. Das gleiche gilt für die internen Festplatten eines AFF A700s Systems. Das DS224C Festplatten-Shelf muss über 12 GB SAS verbunden werden, um die Anzahl von SAP HANA-Hosts zu unterstützen.

Das 6-Gbit-SAS-Platten-Shelf (DS2246) unterstützt maximal vier SAP HANA-Hosts. Die SSDs und SAP HANA-Hosts müssen auf beide Storage-Controller verteilt sein.

In der folgenden Tabelle ist die unterstützte Anzahl von SAP HANA-Hosts pro Festplatten-Shelf zusammengefasst.

	6-Gbit-SAS-Shelfs (DS2246) mit voller Betriebslast 24 SSDs	**12-GB-SAS-Shelfs (DS224C) mit 12 SSDs und ADPv2; halb beladen**	**12-GB-SAS-Shelfs (DS224C) mit 24 SSDs und ADPv2 voll beladen**
Maximale Anzahl von SAP HANA-Hosts pro Festplatten-Shelf	4	9	14

> Diese Berechnung erfolgt unabhängig vom eingesetzten Storage Controller. Das Hinzufügen weiterer Platten-Shelves erhöhen nicht die maximale Anzahl von SAP HANA Hosts, die ein Storage-Controller unterstützen kann.

NS224 NVMe-Shelf

Eine NVMe SSD (Daten) unterstützt je nach verwendeten NVMe-Festplatten bis zu 2/5 SAP HANA-Hosts. Die SSDs und SAP HANA-Hosts müssen auf beide Storage-Controller verteilt sein. Gleiches gilt für die internen NVMe-Festplatten von AFF Systemen.

> Das Hinzufügen weiterer Festplatten-Shelfs erhöht nicht die maximale Anzahl von SAP HANA-Hosts, die ein Storage-Controller unterstützen kann.

Heterogenen Workloads

SAP HANA und andere Applikations-Workloads werden auf demselben Storage Controller oder im selben Storage-Aggregat unterstützt. Es ist jedoch eine NetApp Best Practice, SAP HANA-Workloads von allen anderen Applikations-Workloads zu trennen.

SAP HANA-Workloads und andere Applikations-Workloads können entweder auf demselben Storage-Controller oder demselben Aggregat implementiert werden. Falls ja, müssen Sie sicherstellen, dass in der Umgebung mit heterogenen Workloads für SAP HANA eine ausreichende Performance verfügbar ist. NetApp empfiehlt außerdem, Parameter für Quality of Service (QoS) zu verwenden, um die Auswirkungen anderer Applikationen auf SAP HANA Applikationen zu regulieren und den Durchsatz für SAP HANA Applikationen zu garantieren.

Das Performance-Testtool von SAP muss verwendet werden, um zu prüfen, ob zusätzliche SAP HANA Hosts auf einem vorhandenen Storage Controller ausgeführt werden können, der bereits für andere Workloads verwendet wird. SAP Applikations-Server können wie die SAP HANA Datenbanken sicher auf demselben Storage Controller und/oder Aggregat platziert werden.

Überlegungen zur Kapazität

Eine detaillierte Beschreibung der Kapazitätsanforderungen für SAP HANA ist im "SAP-Hinweis 1900823" Whitepaper:

> Das Kapazitätsdimensionieren der gesamten SAP Landschaft mit mehreren SAP HANA Systemen muss mithilfe von SAP HANA Storage-Größenanpassungs-Tools von NetApp ermittelt werden. Wenden Sie sich an NetApp oder Ihren Ansprechpartner bei NetApp Partnern, um den Prozess der Storage-Größenbemessung für eine ausreichend dimensionierte Storage-Umgebung zu validieren.

Konfigurieren des Performance-Testtool

Ab SAP HANA 1.0 SPS10 führte SAP Parameter ein, um das I/O-Verhalten anzupassen und die Datenbank für das verwendete Datei- und Speichersystem zu optimieren. Diese Parameter müssen außerdem für das Performance-Testtool von SAP festgelegt werden, wenn die Storage-Performance mit dem Performance-Testtool von SAP getestet wird.

NetApp führte Performance-Tests durch, um die optimalen Werte zu ermitteln. In der folgenden Tabelle sind die Parameter aufgeführt, die in der Konfigurationsdatei des SAP-Performance-Testwerkzeugs festgelegt werden müssen.

Parameter	Wert
max_parallel_io_Requests	128
Async_read_Submit	Ein
Async_write_submit_Active	Ein
Async_Write_Submit_Blocks	Alle

Weitere Informationen zur Konfiguration der verschiedenen SAP-Testwerkzeuge finden Sie unter "SAP-Hinweis 1943937" Für HWCCT (SAP HANA 1.0) und "SAP-Hinweis 2493172" FÜR HCMT/HCOT (SAP HANA 2.0).

Das folgende Beispiel zeigt, wie Variablen für den HCMT/HCOT-Ausführungsplan festgelegt werden können.

```
…{
          "Comment": "Log Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "LogAsyncReadSubmit",
```

```
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
         "Name": "DataAsyncReadSubmit",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "LogAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "DataAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "LogAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "DataAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "LogExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
```

```
      },
      {
         "Comment": "Data Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "DataExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      }, …
```

Diese Variablen müssen für die Testkonfiguration verwendet werden. Dies ist in der Regel bei den vordefinierten Testsuiten der Fall, die SAP mit dem HCMT/HCOT-Tool liefert. Das folgende Beispiel für einen 4k-Protokollschreibtest stammt aus einer Testsuite.

```
…
      {
         "ID": "D664D001-933D-41DE-A904F304AEB67906",
         "Note": "File System Write Test",
         "ExecutionVariants": [
            {
               "ScaleOut": {
                  "Port": "${RemotePort}",
                  "Hosts": "${Hosts}",
                  "ConcurrentExecution": "${FSConcurrentExecution}"
               },
               "RepeatCount": "${TestRepeatCount}",
               "Description": "4K Block, Log Volume 5GB, Overwrite",
               "Hint": "Log",
               "InputVector": {
                  "BlockSize": 4096,
                  "DirectoryName": "${LogVolume}",
                  "FileOverwrite": true,
                  "FileSize": 5368709120,
                  "RandomAccess": false,
                  "RandomData": true,
                  "AsyncReadSubmit": "${LogAsyncReadSubmit}",
                  "AsyncWriteSubmitActive":
"${LogAsyncWriteSubmitActive}",
                  "AsyncWriteSubmitBlocks":
"${LogAsyncWriteSubmitBlocks}",
                  "ExtMaxParallelIoRequests":
"${LogExtMaxParallelIoRequests}",
                  "ExtMaxSubmitBatchSize": "${LogExtMaxSubmitBatchSize}",
                  "ExtMinSubmitBatchSize": "${LogExtMinSubmitBatchSize}",
                  "ExtNumCompletionQueues":
"${LogExtNumCompletionQueues}",
                  "ExtNumSubmitQueues": "${LogExtNumSubmitQueues}",
                  "ExtSizeKernelIoQueue": "${ExtSizeKernelIoQueue}"
               }
            }, …
```

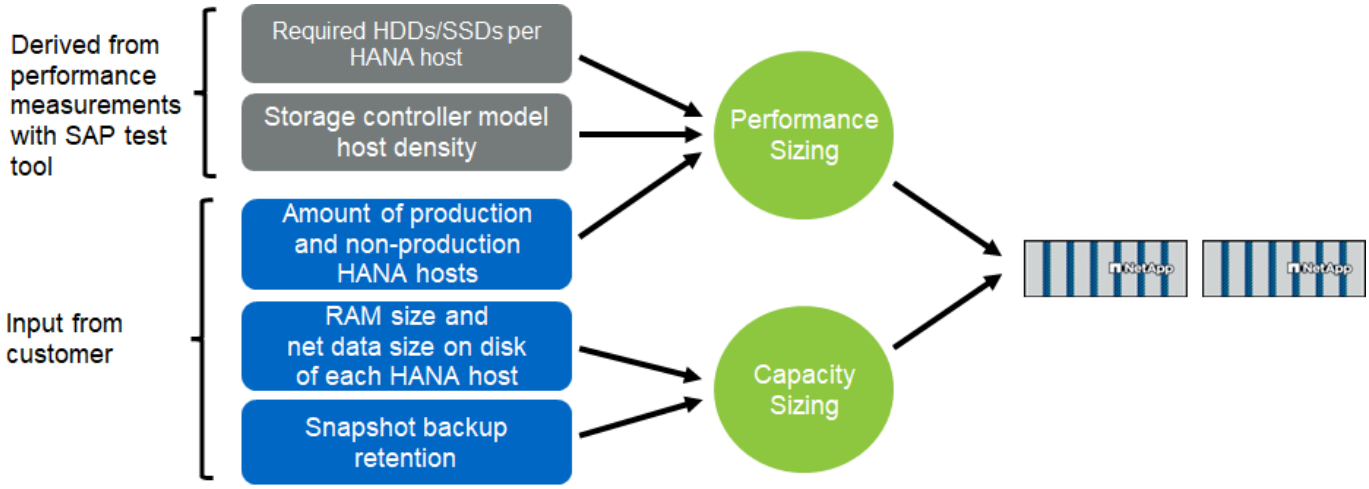
Übersicht über den Prozess zur Storage-Größenbemessung

Die Anzahl der Festplatten pro HANA Host und die SAP HANA Host-Dichte für jedes Storage-Modell wurden mit dem Performance-Testtool ermittelt.

Der Dimensionierungsprozess erfordert Einzelheiten, z. B. die Anzahl der SAP HANA-Hosts in der Produktion und für die Produktion nichtproduktive Umgebung, die RAM-Größe jedes Hosts und die Backup-Aufbewahrung der Storage-basierten Snapshot Kopien. Die Anzahl der SAP HANA-Hosts bestimmt den Storage Controller und die Anzahl der benötigten Festplatten.

Die Größe des RAM, die Netto-Datengröße auf der Festplatte jedes SAP HANA-Hosts und der Aufbewahrungszeitraum für das Snapshot-Backup werden als Inputs bei der Kapazitätsdimensionierung verwendet.

Die folgende Abbildung fasst den Dimensionierungsprozess zusammen.



Einrichtung und Konfiguration der Infrastruktur

Netzwerkeinrichtung

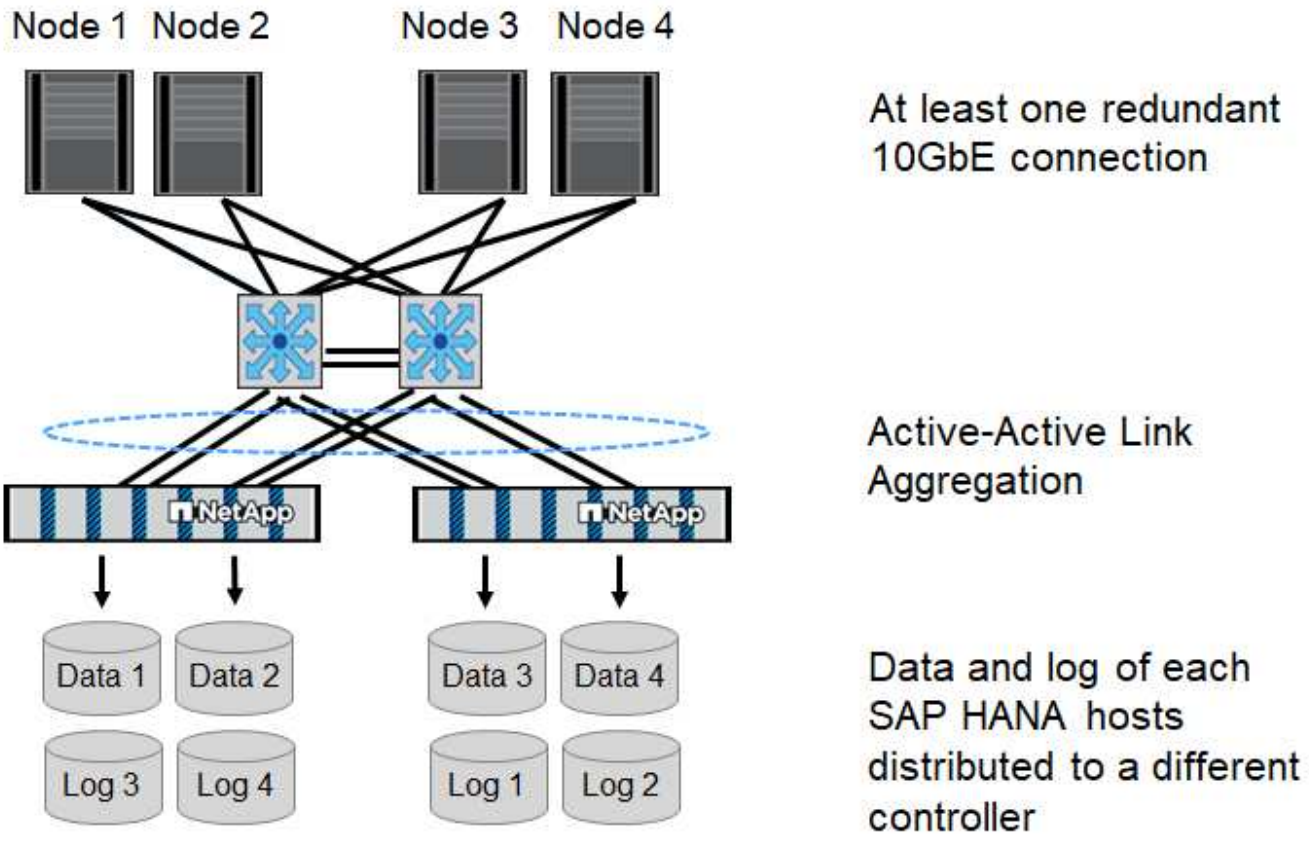
In diesem Abschnitt wird das dedizierte Setup des Storage-Netzwerks für SAP HANA-Hosts beschrieben.

Beachten Sie bei der Konfiguration des Netzwerks die folgenden Richtlinien:

- Um die SAP HANA-Hosts mit den Storage-Controllern über ein 10-GbE- oder schnelleres Netzwerk zu verbinden, muss ein dediziertes Storage-Netzwerk verwendet werden.
- Verwenden Sie dieselbe Verbindungsgeschwindigkeit für Storage Controller und SAP HANA Hosts. Ist dies nicht möglich, stellen Sie sicher, dass die Netzwerkkomponenten zwischen den Storage Controllern und den SAP HANA Hosts unterschiedliche Geschwindigkeiten verarbeiten können. Beispielsweise müssen Sie genügend Puffer bereitstellen, um eine Geschwindigkeitsverhandlung auf NFS-Ebene zwischen Storage und Hosts zu ermöglichen. Netzwerkkomponenten sind normalerweise Switches, aber andere Komponenten innerhalb des Blade-Chassis, wie z. B. die Rückebene, müssen ebenfalls in Betracht gezogen werden.
- Deaktivieren Sie die Flusssteuerung bei allen physischen Ports, die für den Storage-Verkehr auf dem Storage-Netzwerk-Switch und der Host-Ebene verwendet werden.
- Jeder SAP HANA-Host muss über eine redundante Netzwerkverbindung mit mindestens 10 GB Bandbreite verfügen.
- Jumbo-Frames mit einer Maximum Transmission Unit (MTU) von 9,000 müssen auf allen Netzwerkkomponenten zwischen den SAP HANA-Hosts und den Storage Controllern aktiviert werden.
- In einer VMware Einrichtung müssen jeder laufenden virtuellen Maschine dedizierte VMXNET3 Netzwerkadapter zugewiesen werden. Prüfen Sie die in „Einführung“ genannten Unterlagen für weitere Anforderungen.
- Verwenden Sie für den Protokoll- und Datenbereich separate Netzwerk-/E/A-Pfade, um Interferenzen zwischen den beiden zu vermeiden.

Die folgende Abbildung zeigt ein Beispiel mit vier SAP HANA-Hosts, die über ein 10-GbE-Netzwerk an ein HA-Paar des Storage-Controllers angeschlossen sind. Jeder SAP HANA-Host verfügt über eine aktiv/aktiv-Verbindung zur redundanten Fabric.

Auf der Storage-Ebene sind vier aktive Verbindungen so konfiguriert, dass sie für jeden SAP HANA Host einen 10-GB-Durchsatz bereitstellen. Auf Storage-Ebene wird eine Broadcast-Domäne mit einer MTU-Größe von 9000 konfiguriert und dieser Broadcast-Domäne werden alle erforderlichen physischen Schnittstellen hinzugefügt. Bei diesem Ansatz werden diese physischen Schnittstellen automatisch derselben Failover-Gruppe zugewiesen. Alle logischen Schnittstellen (LIFs), die diesen physischen Schnittstellen zugewiesen sind, werden dieser Failover-Gruppe hinzugefügt.



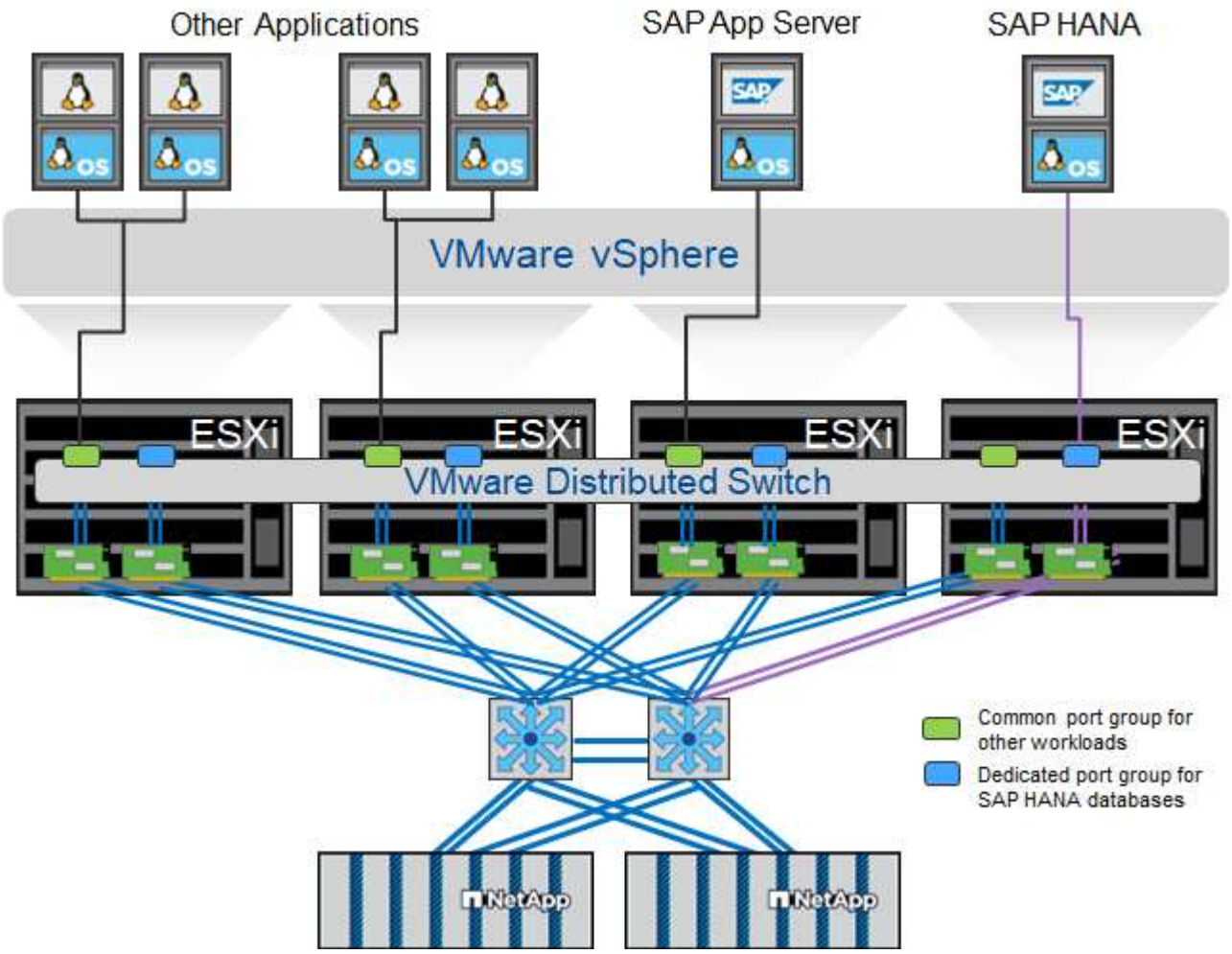
Im Allgemeinen wird empfohlen, HA-Schnittstellengruppen auf den Servern (Bonds) und den Speichersystemen zu verwenden (z. B. Link Aggregation Control Protocol [LACP] und ifgroups). Vergewissern Sie sich bei HA-Schnittstellengruppen, dass die Last gleichmäßig auf alle Schnittstellen innerhalb der Gruppe verteilt ist. Die Lastverteilung hängt von der Funktionalität der Netzwerk-Switch-Infrastruktur ab.

> Abhängig von der Anzahl der SAP HANA-Hosts und der verwendeten Verbindungsgeschwindigkeit sind unterschiedliche Anzahl aktiver physischer Ports erforderlich. Weitere Informationen finden Sie im Abschnitt "LIF-Konfiguration".

VMware-spezifische Netzwerk-Einrichtung

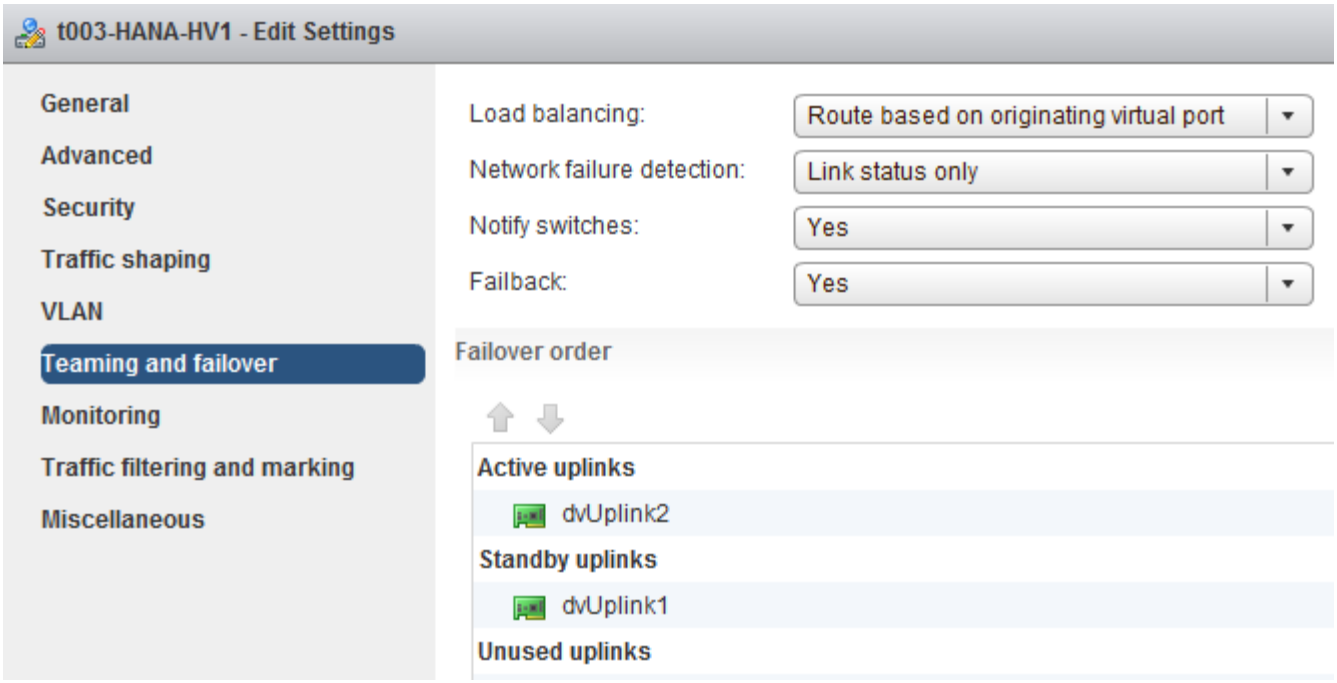
Richtiges Netzwerkdesign und richtige Konfiguration sind entscheidend, da alle Daten für SAP HANA Instanzen, einschließlich Performance-kritischer Daten und Protokoll-Volumes für die Datenbank, in dieser Lösung über NFS bereitgestellt werden. Über ein dediziertes Storage-Netzwerk wird der NFS-Traffic von der Kommunikation und der Datenverkehr mit Benutzerzugriffsrechten zwischen SAP HANA-Knoten getrennt. Jeder SAP HANA Node benötigt eine redundante, dedizierte Netzwerkverbindung mit mindestens 10 GB Bandbreite. Es wird auch eine höhere Bandbreite unterstützt. Dieses Netzwerk muss sich End-to-End von der

Storage-Ebene über Netzwerk-Switching und Computing bis hin zum auf VMware vSphere gehosteten Gastbetriebssystem erstrecken. Neben der physischen Switching-Infrastruktur wird ein VMware Distributed Switch (VdS) eingesetzt, um eine ausreichende Performance und Managebarkeit des Netzwerkverkehrs auf der Hypervisor-Ebene zu gewährleisten.



Wie in der obigen Abbildung gezeigt, verwendet jeder SAP HANA Node auf dem VMware Distributed Switch eine dedizierte Portgruppe. Diese Port-Gruppe ermöglicht eine verbesserte Servicequalität (QoS) und eine dedizierte Zuweisung von physischen Netzwerkkarten (NICs) auf den ESX Hosts. Um dedizierte physische NICs zu verwenden und gleichzeitig HA-Funktionen bei einem NIC-Ausfall zu erhalten, wird die dedizierte physische NIC als aktiver Uplink konfiguriert. Zusätzliche NICs werden in den Teaming- und Failover-Einstellungen der SAP HANA-Portgruppe als Standby-Uplinks konfiguriert. Darüber hinaus müssen Jumbo Frames (MTU 9,000) End-to-End-aktiviert sein, auf physischen und virtuellen Switches. Deaktivieren Sie darüber hinaus die Flusskontrolle bei allen ethernet-Ports, die für den Storage-Datenverkehr bei Servern, Switches und Storage-Systemen verwendet werden. Die folgende Abbildung zeigt ein Beispiel für eine solche Konfiguration.

LRO (Large Receive Offload) muss für Schnittstellen deaktiviert werden, die für NFS Traffic verwendet werden. Alle anderen Richtlinien zur Netzwerkkonfiguration finden Sie im entsprechenden VMware Best Practices Guide für SAP HANA.



Zeitsynchronisierung

Sie müssen die Zeit zwischen den Storage-Controllern und den SAP HANA Datenbank-Hosts synchronisieren. Legen Sie dazu denselben Zeitserver für alle Storage Controller und alle SAP HANA-Hosts fest.

Einrichtung von Storage Controllern

In diesem Abschnitt wird die Konfiguration des NetApp Storage-Systems beschrieben. Sie müssen die primäre Installation und Einrichtung gemäß den entsprechenden ONTAP Setup- und Konfigurationsleitfäden abschließen.

Storage-Effizienz

In einer SSD-Konfiguration werden Inline-Deduplizierung, Inline-Deduplizierung, Inline-Komprimierung und Inline-Data-Compaction unterstützt.

NetApp FlexGroup Volumes

Die Verwendung von NetApp FlexGroup Volumes wird für SAP HANA nicht unterstützt. Aufgrund der Architektur von SAP HANA bietet die Verwendung von FlexGroup Volumes keinen Vorteil und kann zu Performance-Problemen führen.

NetApp Volume- und Aggregatverschlüsselung

Die Verwendung von NetApp Volume Encryption (NVE) und NetApp Aggregate Encryption (NAE) wird bei SAP HANA unterstützt.

Quality of Service

Mit QoS lässt sich der Storage-Durchsatz für bestimmte SAP HANA Systeme oder andere Applikationen auf einem gemeinsam genutzten Controller begrenzen. Ein Anwendungsfall wäre, den Durchsatz von Entwicklungs- und Testsystemen zu begrenzen, damit sie bei einem gemischten Setup keinen Einfluss auf die

Produktionssysteme haben.

Während des Dimensionierungsprozesses sollten Sie die Performance-Anforderungen eines nicht für die Produktion verwendeten Systems ermitteln. Entwicklungs- und Testsysteme können mit niedrigeren Leistungswerten dimensioniert werden, typischerweise im Bereich von 20 % bis 50 % eines von SAP definierten Produktionssystems-KPI.

Ab ONTAP 9 wird QoS auf Storage-Volume-Ebene konfiguriert und verwendet maximale Werte für Durchsatz (MB/s) und I/O-Menge (IOPS).

Ein großer I/O-Schreibvorgang wirkt sich am stärksten auf die Performance des Storage-Systems aus. Daher sollte die QoS-Durchsatzbegrenzung auf einen Prozentsatz der entsprechenden KPI-Werte für die SAP HANA-Speicherleistung in den Daten- und Protokoll-Volumes gesetzt werden.

NetApp FabricPool

NetApp FabricPool darf nicht für aktive primäre Filesysteme in SAP HANA Systemen verwendet werden. Dazu gehören die Dateisysteme für den Daten- und Protokollbereich sowie die `/hana/shared` File-System. Dies führt zu unvorhersehbarer Performance, insbesondere beim Start eines SAP HANA Systems.

Die Verwendung der „nur-Snapshots“ Tiering-Politik ist möglich sowie auch die Nutzung von FabricPool im Allgemeinen an einem Backup-Ziel wie einem NetApp SnapVault oder SnapMirror Ziel.

> Durch die Verwendung von FabricPool für das Tiering von Snapshot Kopien im Primärspeicher oder die Verwendung von FabricPool zu einem Backup-Ziel werden die für die Wiederherstellung und das Recovery einer Datenbank oder anderer Aufgaben benötigte Zeit, beispielsweise das Erstellen von Systemklonen oder Korrektursystemen, geändert. Berücksichtigen Sie diese Überlegungen bei der Planung Ihrer gesamten Lifecycle-Management-Strategie und prüfen Sie, ob Ihre SLAs unter Verwendung dieser Funktion noch erfüllt werden.

FabricPool ist eine gute Option, um Log-Backups auf eine andere Storage Tier zu verschieben. Das Verschieben von Backups beeinträchtigt die für das Recovery einer SAP HANA Datenbank erforderliche Zeit. Daher sollte die Option „Tiering-minimum-cooling-days“ auf einen Wert gesetzt werden, der Log-Backups, die routinemäßig für die Wiederherstellung benötigt werden, auf der lokalen fast Storage Tier platziert.

Storage-Konfiguration

In der folgenden Übersicht sind die erforderlichen Schritte zur Storage-Konfiguration zusammengefasst. Jeder Schritt wird in den nachfolgenden Abschnitten näher beschrieben. In diesem Abschnitt wird die Storage-Hardware eingerichtet und die ONTAP Software bereits installiert. Außerdem müssen bereits die Verbindungen zwischen den Storage-Ports (10 GbE oder schneller) und dem Netzwerk vorhanden sein.

1. Überprüfen Sie die richtige Festplatten-Shelf-Konfiguration, wie unter „ “ beschrieben.Festplatten-Shelf-Verbindung.“
2. Erstellen und Konfigurieren der erforderlichen Aggregate wie unter „ “ beschriebenKonfiguration von Aggregaten.“
3. Erstellen einer Storage Virtual Machine (SVM) wie unter „SVM-Konfiguration.“
4. Erstellen Sie LIFs wie in „ “ beschrieben.LIF-Konfiguration.“
5. Erstellen Sie Volumes innerhalb der Aggregate, wie in „“ und „ “Volume-Konfiguration für SAP HANA Multiple-Host-Systeme beschriebenVolume-Konfiguration für SAP HANA Single-Host-Systeme.
6. Legen Sie die erforderlichen Volume-Optionen fest, wie unter „ “ beschrieben.Volume-Optionen.“

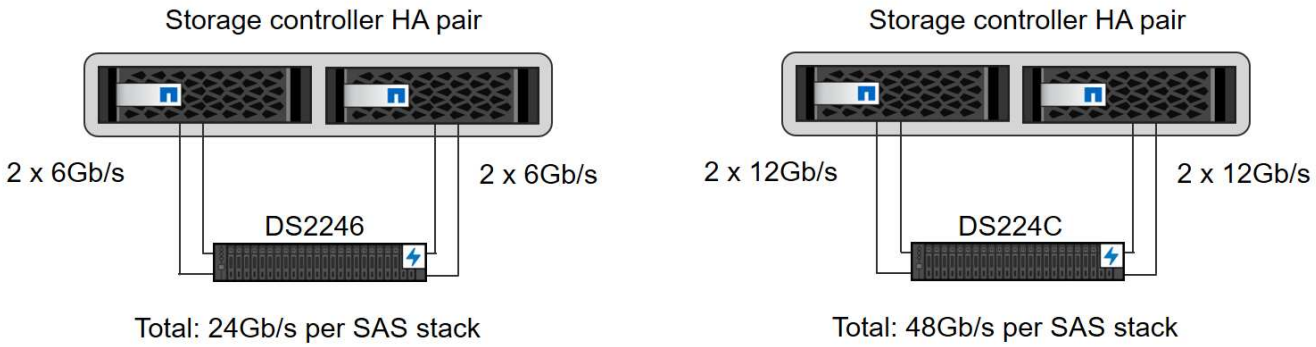
7. Legen Sie die erforderlichen Optionen für NFSv3 fest, wie in „ “ beschrieben.NFS-Konfiguration für NFSv3„ Oder für NFSv4 wie in „ “ beschriebenNFS-Konfiguration für NFSv4.“
8. Mounten Sie die Volumes in Namespace und legen Sie die Richtlinien für den Export wie in „ “ beschrieben fest.Volumes werden in Namespace mounten und Richtlinien für den Export festlegen.“

Festplatten-Shelf-Verbindung

SAS-Platten-Shelves

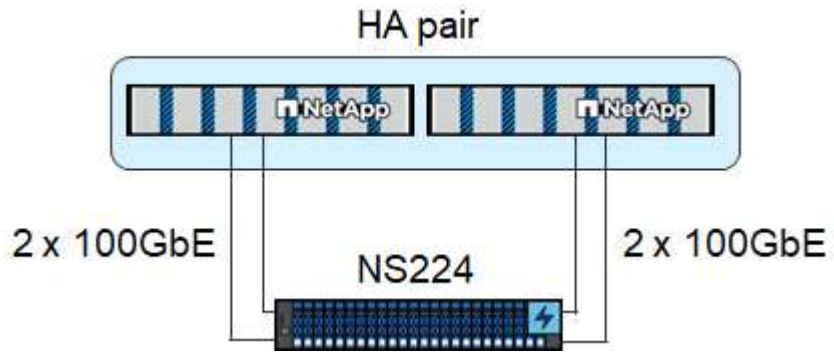
Es kann maximal ein Platten-Shelf mit einem SAS-Stack verbunden werden, um die erforderliche Performance für die SAP HANA-Hosts zu liefern, wie in der folgenden Abbildung dargestellt. Die Festplatten in jedem Shelf müssen gleichmäßig auf beide Controller des HA-Paars verteilt werden. ADPv2 wird mit ONTAP 9 und DS224C Festplatten-Shelfs verwendet.

Mit dem DS224C Festplatten-Shelf können auch Quad-Path-SAS-Kabel verwendet werden, ist aber nicht erforderlich.



NVMe (100 GbE) Festplatten-Shelfs

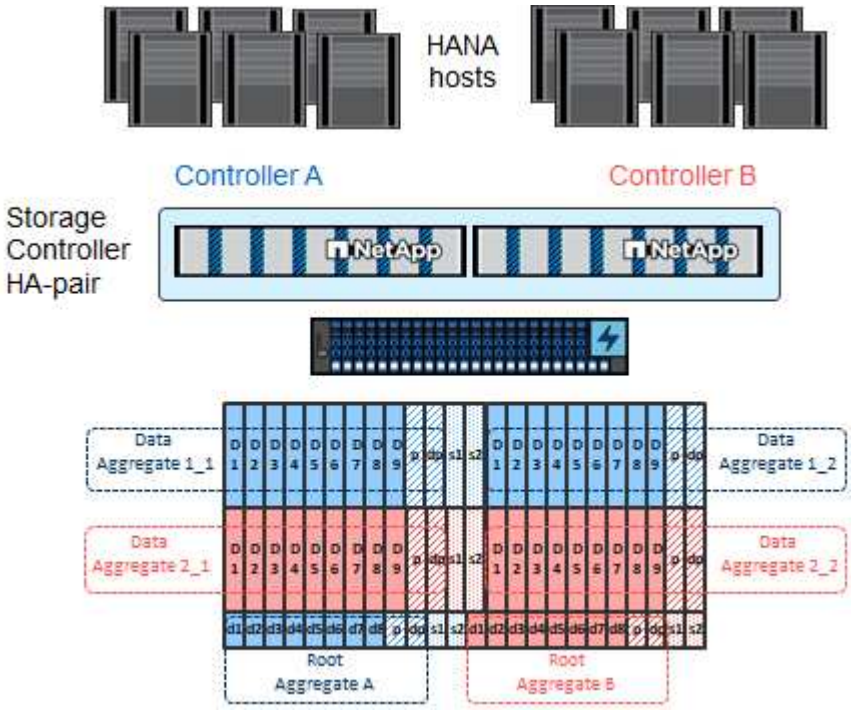
Jedes NS224 NVMe-Festplatten-Shelf ist, wie in der folgenden Abbildung dargestellt, mit zwei 100-GbE-Ports pro Controller verbunden. Die Festplatten in jedem Shelf müssen gleichmäßig auf beide Controller des HA-Paars verteilt werden. ADPv2, wie im Kapitel für die Aggregatkonfiguration beschrieben, wird auch für das NS224 Festplatten-Shelf verwendet.



Konfiguration von Aggregaten

Im Allgemeinen müssen Sie zwei Aggregate pro Controller konfigurieren, unabhängig vom verwendeten Festplatten-Shelf oder der Festplattentechnologie (SAS-SSDs oder NVMe-SSDs).

Die folgende Abbildung zeigt eine Konfiguration mit 12 SAP HANA Hosts, die auf einem 12-GB-SAS-Shelf ausgeführt werden und mit ADPv2 konfiguriert sind. Sechs SAP-HANA-Hosts sind mit jedem Storage-Controller verbunden. Vier separate Aggregate, zwei an jedem Storage Controller, sind konfiguriert. Jedes Aggregat ist mit 11 Festplatten mit neun Daten und zwei Parity-Festplatten-Partitionen konfiguriert. Für jeden Controller stehen zwei Ersatzpartitionen zur Verfügung.



SVM-Konfiguration

Mehrere SAP Landschaften mit SAP HANA Datenbanken können eine einzige SVM nutzen. Darüber hinaus kann jeder SAP-Landschaft bei Bedarf eine SVM zugewiesen werden, falls diese von verschiedenen Teams innerhalb eines Unternehmens gemanagt werden.

Wenn beim Erstellen einer neuen SVM ein QoS-Profil automatisch erstellt und zugewiesen wird, entfernen Sie dieses automatisch erstellte Profil aus der SVM, um die erforderliche Performance für SAP HANA zu aktivieren:

```
vserver modify -vserver <svm-name> -qos-policy-group none
```

LIF-Konfiguration

Für SAP HANA Produktionssysteme müssen unterschiedliche LIFs verwendet werden, um das Daten-Volume und das Protokoll-Volume vom SAP HANA-Host zu mounten. Daher sind mindestens zwei LIFs erforderlich.

Die Daten- und Protokoll-Volume-Mounts verschiedener SAP HANA Hosts können einen physischen Storage-Netzwerk-Port entweder über dieselben LIFs oder mithilfe individueller LIFs für jeden Mount gemeinsam nutzen.

Die folgende Tabelle zeigt die maximale Menge an Daten- und Protokoll-Volume-Mounts pro physischer Schnittstelle.

Ethernet-Port-Geschwindigkeit	10 GbE	25 GbE	40 GbE	100 GeE
Maximale Anzahl an Protokoll- oder Daten-Volume-Mounts pro physischem Port	3	8	12	30

Die gemeinsame Nutzung einer logischen Schnittstelle zwischen verschiedenen SAP HANA Hosts erfordert möglicherweise eine Neuaufbindung von Daten- oder Protokoll-Volumes an eine andere logische Schnittstelle. Durch diese Änderung werden Performance-Einbußen vermieden, wenn ein Volume auf einen anderen Storage Controller verschoben wird.

Entwicklungs- und Testsysteme können mehr Daten und Volume-Mounts oder LIFs auf einer physischen Netzwerkschnittstelle verwenden.

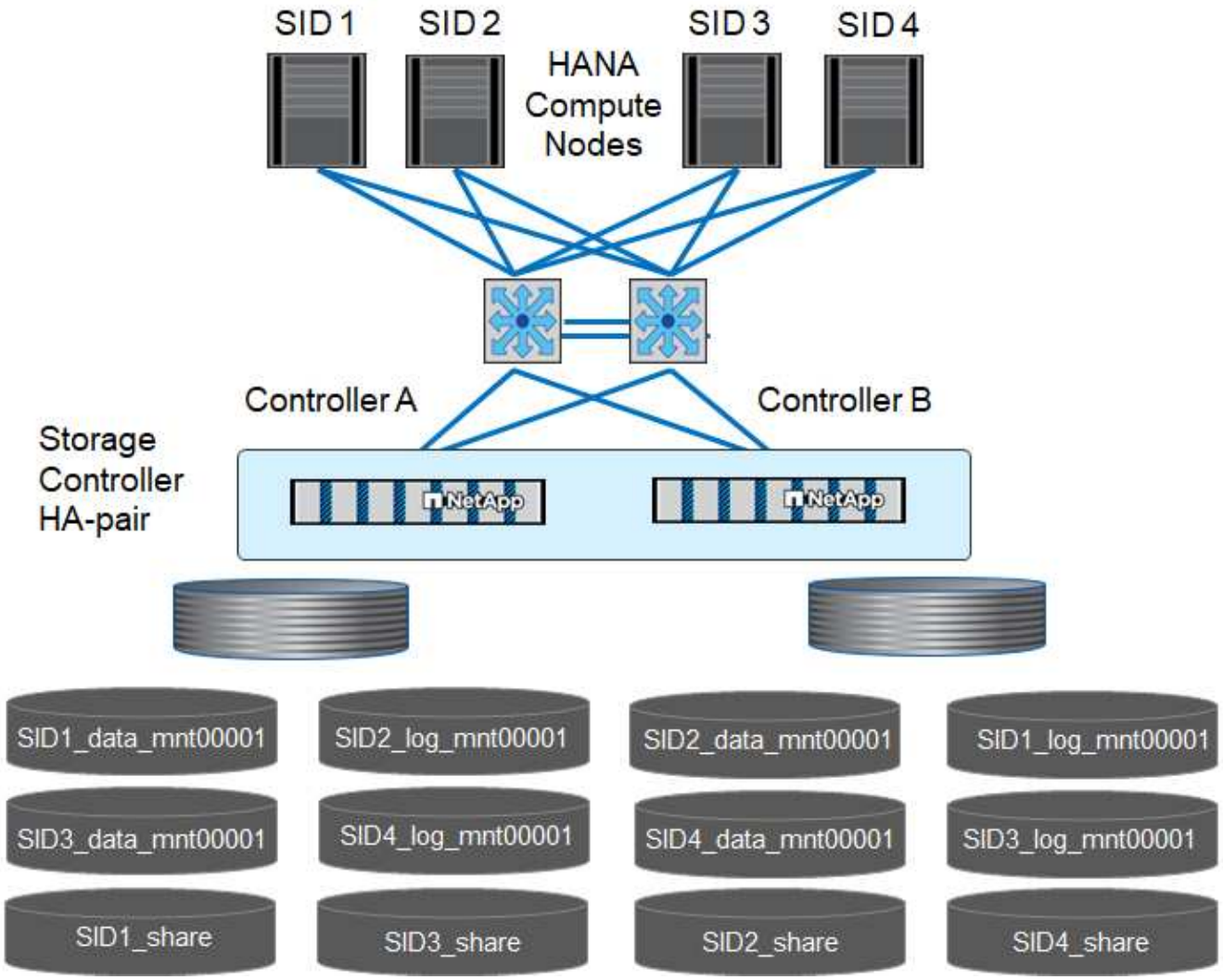
Für Produktions-, Entwicklungs- und Testsysteme liefert `/hana/shared` Das Filesystem kann dieselbe LIF wie das Daten- oder Protokoll-Volume verwenden.

Volume-Konfiguration für SAP HANA Single-Host-Systeme

Die folgende Abbildung zeigt die Volume-Konfiguration von vier SAP HANA-Systemen mit einem Host. Die Daten- und Protokoll-Volumes jedes SAP HANA Systems werden auf verschiedene Storage Controller verteilt. Beispiel: Volume `SID1_data_mnt00001` Wird auf Controller A und Volume konfiguriert `SID1_log_mnt00001` Ist auf Controller B konfiguriert

Wenn für die SAP HANA Systeme nur ein Storage-Controller eines HA-Paars verwendet wird, können Daten- und Protokoll-Volumes auch auf demselben Storage Controller gespeichert werden.

Wenn die Daten- und Protokoll-Volumes auf demselben Controller gespeichert sind, muss der Zugriff des Servers auf den Storage mit zwei unterschiedlichen LIFs durchgeführt werden: Einer logischen Schnittstelle für den Zugriff auf das Daten-Volume und der andere für den Zugriff auf das Protokoll-Volume.



Für jeden SAP HANA-Host, ein Daten-Volume, ein Protokoll-Volume und ein Volume für `/hana/shared` Werden konfiguriert. Die folgende Tabelle zeigt eine Beispielkonfiguration für SAP HANA-Systeme mit einem Host.

Zweck	Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregat 2 bei Controller b
Daten-, Protokoll- und freigegebene Volumes für System SID1	Datenvolumen: SID1_Data_mnt00001	Freigegebenes Volume: SID1_Shared	–	Protokollvolumen: SID1_log_mnt00001
Daten-, Protokoll- und freigegebene Volumes für System SID2	–	Protokollvolumen: SID2_log_mnt00001	Datenvolumen: SID2_Data_mnt00001	Freigegebenes Volume: SID2_Shared
Daten-, Protokoll- und gemeinsam genutzte Volumes für System SID3	Gemeinsam genutztes Volume: SID3_shared	Datenvolumen: SID3_Data_mnt00001	Protokollvolumen: SID3_log_mnt00001	–

Zweck	Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregat 2 bei Controller b
Daten-, Protokoll- und gemeinsam genutzte Volumes für System SID4	Protokollvolumen: SID4_log_mnt00001	–	Gemeinsam genutztes Volume: SID4_shared	Datenvolumen: SID4_Data_mnt00001

Die folgende Tabelle zeigt ein Beispiel für die Mount-Point-Konfiguration für ein System mit einem einzelnen Host. Um das Home-Verzeichnis des zu platzieren `sidadm` Benutzer auf dem zentralen Speicher, der `/usr/sap/SID` Dateisystem sollte vom gemountet werden `SID_shared` Datenmenge:

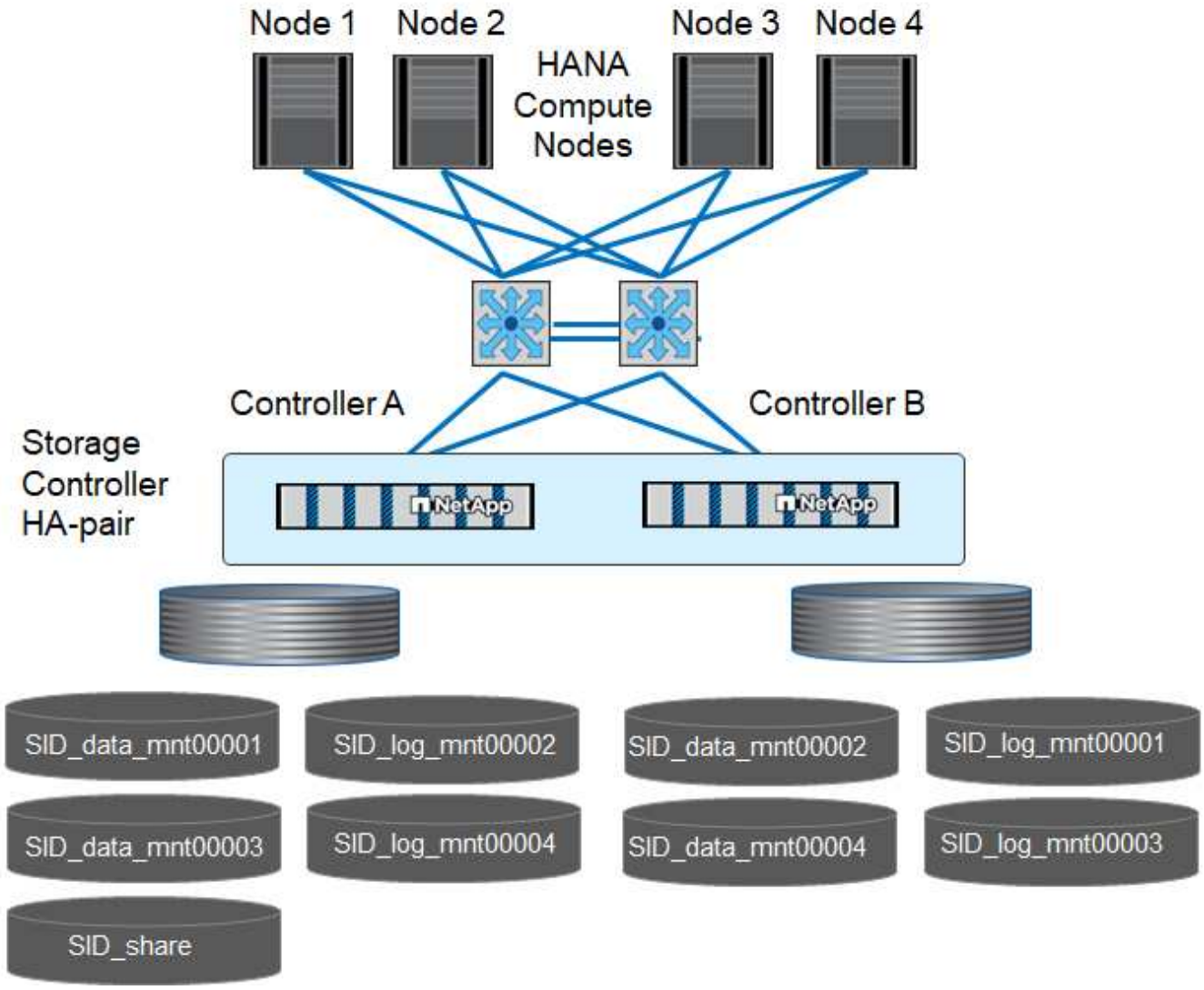
Verbindungspfad	Verzeichnis	Bereitstellungspunkt beim HANA-Host
SID_Data_mnt00001		/hana/Data/SID/mnt00001
SID_Log_mnt00001		/hana/log/SID/mnt00001
SID_freigegeben	Usr-sap freigegeben	/Usr/sap/SID /hana/shared/

Volume-Konfiguration für SAP HANA Multiple-Host-Systeme

Die folgende Abbildung zeigt die Volume-Konfiguration eines 4+1 SAP HANA-Systems. Die Daten- und Protokoll-Volumes jedes SAP HANA-Hosts werden auf verschiedene Storage-Controller verteilt. Beispiel: Volume `SID1_data1_mnt00001` Wird auf Controller A und Volume konfiguriert `SID1_log1_mnt00001` Ist auf Controller B konfiguriert

Wenn für das SAP HANA System nur ein Storage-Controller eines HA-Paars verwendet wird, können die Daten- und Protokoll-Volumes auch auf demselben Storage Controller gespeichert werden.

Wenn die Daten- und Protokoll-Volumes auf demselben Controller gespeichert sind, muss der Zugriff des Servers auf den Storage mit zwei unterschiedlichen LIFs durchgeführt werden: Einer logischen Schnittstelle für den Zugriff auf das Daten-Volume und einem für den Zugriff auf das Protokoll-Volume.



Für jeden SAP HANA-Host werden ein Daten-Volume und ein Protokoll-Volume erstellt. Der `/hana/shared` Das Volume wird von allen Hosts des SAP HANA-Systems verwendet. Die folgende Tabelle zeigt eine Beispielkonfiguration für ein SAP HANA-System mit mehreren Hosts und vier aktiven Hosts.

Zweck	Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregieren 2 bei Controller B
Daten- und Protokoll-Volumes für Node 1	Datenvolumen: SID_Data_mnt00001	–	Protokollvolumen: SID_log_mnt00001	–
Daten- und Protokoll-Volumes für Node 2	Protokollvolumen: SID_log_mnt002	–	Datenvolumen: SID_Data_mnt002	–
Daten- und Protokoll-Volumes für Node 3	–	Datenvolumen: SID_Data_mnt00003	–	Protokollvolumen: SID_log_mnt00003
Daten- und Protokoll-Volumes für Node 4	–	Protokollvolumen: SID_log_mnt004	–	Datenvolumen: SID_Data_mnt00004

Zweck	Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregieren 2 bei Controller B
Gemeinsames Volume für alle Hosts	Gemeinsam genutztes Volume: SID_shared			

Die folgende Tabelle zeigt die Konfiguration und die Bereitstellungspunkte eines Systems mit mehreren Hosts mit vier aktiven SAP HANA Hosts. Um die Home-Verzeichnisse des zu platzieren `sidadm` Benutzer jedes Hosts im zentralen Speicher, der `/usr/sap/SID` Dateisysteme werden über eingebunden `SID_shared` Datenmenge:

Verbindungspfad	Verzeichnis	Bereitstellungspunkt beim SAP HANA-Host	Hinweis
SID_Data_mnt00001	–	/hana/Data/SID/mnt00001	Auf allen Hosts montiert
SID_Log_mnt00001	–	/hana/log/SID/mnt00001	Auf allen Hosts montiert
SID_Data_mnt00002	–	/hana/Data/SID/mnt002	Auf allen Hosts montiert
SID_Log_mnt00002	–	/hana/log/SID/mnt002	Auf allen Hosts montiert
SID_Data_mnt00003	–	/hana/Data/SID/mnt003	Auf allen Hosts montiert
SID_log_mnt00003	–	/hana/log/SID/mnt003	Auf allen Hosts montiert
SID_Data_mnt00004	–	/hana/Data/SID/mnt004	Auf allen Hosts montiert
SID_log_mnt00004	–	/hana/log/SID/mnt004	Auf allen Hosts montiert
SID_freigegeben	Freigegeben	/hana/Shared/SID	Auf allen Hosts montiert
SID_freigegeben	Usr-sap-host1	/Usr/sap/SID	Angehängt auf Host 1
SID_freigegeben	Usr-sap-host2	/Usr/sap/SID	Angehängt auf Host 2
SID_freigegeben	Usr-sap-host3	/Usr/sap/SID	Angehängt auf Host 3
SID_freigegeben	Usr-sap-host4	/Usr/sap/SID	Angehängt auf Host 4
SID_freigegeben	Usr-sap-host5	/Usr/sap/SID	Angehängt auf Host 5

Volume-Optionen

Sie müssen die in der folgenden Tabelle aufgeführten Volume-Optionen auf allen SVMs überprüfen und festlegen. Bei einigen Befehlen müssen Sie in den erweiterten Berechtigungsebene in ONTAP wechseln.

Aktion	Befehl
Deaktivieren Sie die Sichtbarkeit des Snapshot Verzeichnisses	vol modify -vserver <vserver-Name> -Volume <volname> -Snapdir-Access false
Deaktivieren Sie automatische Snapshot Kopien	vol modify –vserver <vserver-Name> -Volume <volname> -Snapshot-Policy keine
Deaktivieren Sie Updates der Zugriffszeit außer dem SID_Shared-Volume	Setzen Sie Advanced vol modify -vserver <vserver-Name> -Volume <volname> -atime-Update false Administrator

NFS-Konfiguration für NFSv3

Die in der folgenden Tabelle aufgeführten NFS-Optionen müssen verifiziert und auf allen Storage Controllern eingestellt werden. Für einige der Befehle, die in dieser Tabelle aufgeführt sind, müssen Sie in den erweiterten Berechtigungsmodus wechseln.

Aktion	Befehl
Aktivieren Sie NFSv3	nfs modify -vserver <vserver-Name> v3.0 aktiviert
Legen Sie die maximale NFS-TCP-Übertragungsgröße auf 1 MB fest	Erweitertes nfs modify -vserver <vserver_Name> -tcp -max-xfer-size 1048576 set admin

In gemeinsam genutzten Umgebungen mit unterschiedlichen Workloads wird die maximale NFS-TCP-Übertragungsgröße auf 262144 festgelegt

NFS-Konfiguration für NFSv4

Die in der folgenden Tabelle aufgeführten NFS-Optionen müssen verifiziert und auf allen SVMs eingestellt werden.

Für einige Befehle in dieser Tabelle müssen Sie in den erweiterten Berechtigungsmodus wechseln.

Aktion	Befehl
Aktivieren Sie NFSv4	nfs modify -vserver <vserver-Name> -v4.1 aktiviert
Legen Sie die maximale NFS-TCP-Übertragungsgröße auf 1 MB fest	Erweitertes nfs modify -vserver <vserver_Name> -tcp -max-xfer-size 1048576 set admin
NFSv4-Zugriffssteuerungslisten (ACLs) deaktivieren	nfs modify -vserver <vServer_Name> -v4.1-acl deaktiviert
Legen Sie die NFSv4-Domain-ID fest	nfs modify -vServer <vServer_Name> -v4-id-Domain <Domain-Name>
Deaktivieren der NFSv4-Lesedelegierung	nfs modify -vServer <vServer_Name> -v4.1-read -Delegation deaktiviert
Deaktivieren der NFSv4-Schreibdelegation	nfs modify -vServer <vServer_Name> -v4.1-write -Delegation deaktiviert
Deaktivieren Sie die numerischen nfsv4-ids	nfs modify -vServer <vServer_Name> -v4-numeric-ids deaktiviert
Ändern Sie die Anzahl der NFSv4.x-Sitzungsplätze Optional	Erweiterte Einstellungen nfs modify -vserver hana -v4.x-Session-num-slots <value> Legen Sie „Admin“ fest

In gemeinsam genutzten Umgebungen mit unterschiedlichen Workloads wird die maximale NFS-TCP-Übertragungsgröße auf 262144 festgelegt

Bitte beachten Sie, dass die Deaktivierung numerischer ids eine Benutzerverwaltung erfordert, wie im Abschnitt beschrieben "„SAP HANA Installationsvorbereitungen für NFSv4“."

Die NFSv4-Domain-ID muss auf allen Linux-Servern (`/etc/idmapd.conf`) und SVMs auf denselben Wert gesetzt werden, wie im Abschnitt beschrieben "„SAP HANA Installationsvorbereitungen für NFSv4“."

PNFS kann aktiviert und verwendet werden.

Bei Einsatz von SAP HANA Systemen mit mehreren Hosts und automatischem Host-Failover müssen die Failover-Parameter innerhalb angepasst werden `nameserver.ini` Wie in der folgenden Tabelle dargestellt. Behalten Sie das standardmäßige Wiederholungsintervall von 10 Sekunden in diesen Abschnitten bei.

Abschnitt in nameserver.ini	Parameter	Wert
Failover	Normal_Wiederholungen	9
Distributed_Watchdog	Deaktivierung_Wiederholungen	11
Distributed_Watchdog	Takeover_Wiederholungen	9

Volumes werden in Namespace mounten und Richtlinien für den Export festlegen

Wenn ein Volume erstellt wird, muss das Volume im Namespace gemountet werden. In diesem Dokument gehen wir davon aus, dass der Name des Verbindungspfads dem Namen des Volumes entspricht. Standardmäßig wird das Volume mit der Standardrichtlinie exportiert. Die Exportpolitik kann bei Bedarf angepasst werden.

Hosteinrichtung

Alle in diesem Abschnitt beschriebenen Schritte zur Hosteinrichtung gelten sowohl für SAP HANA Umgebungen auf physischen Servern als auch für SAP HANA, die auf VMware vSphere ausgeführt werden.

Konfigurationsparameter für SUSE Linux Enterprise Server

Zusätzliche Kernel- und Konfigurationsparameter müssen bei jedem SAP HANA-Host an den von SAP HANA generierten Workload angepasst werden.

SUSE Linux Enterprise Server 12 und 15

Ab SUSE Linux Enterprise Server 12 SP1 muss der Kernel-Parameter in einer Konfigurationsdatei im festgelegt werden `/etc/sysctl.d` Verzeichnis. Beispielsweise müssen Sie eine Konfigurationsdatei mit dem Namen erstellen `91-NetApp-HANA.conf`.

```
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.ipv4.tcp_rmem = 4096 131072 16777216
net.ipv4.tcp_wmem = 4096 16384  16777216
net.core.netdev_max_backlog = 300000
net.ipv4.tcp_slow_start_after_idle=0
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
sunrpc.tcp_max_slot_table_entries = 128
```

Saptune, der in SLES für SAP OS-Versionen enthalten ist, kann zur Festlegung dieser Werte verwendet werden. Weitere Informationen finden Sie unter "SAP-Hinweis 3024346" (SAP-Login erforderlich).

```
```

Konfigurationsparameter für Red hat Enterprise Linux 7.2 oder höher

Für den von SAP HANA generierten Workload müssen an jedem SAP HANA-Host zusätzliche Kernel- und Konfigurationsparameter angepasst werden.

Ab Red hat Enterprise Linux 7.2 müssen Sie die Kernel-Parameter in einer Konfigurationsdatei im festlegen `/etc/sysctl.d` Verzeichnis. Beispielsweise müssen Sie eine Konfigurationsdatei mit dem Namen erstellen `91-NetApp-HANA.conf`.

```
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.ipv4.tcp_rmem = 4096 131072 16777216
net.ipv4.tcp_wmem = 4096 16384  16777216
net.core.netdev_max_backlog = 300000
net.ipv4.tcp_slow_start_after_idle = 0
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
sunrpc.tcp_max_slot_table_entries = 128
```

Seit RedHat Enterprise Linux Version 8.6 können die Einstellungen auch mithilfe der RHEL System Roles for SAP (Ansible) angewendet werden. Siehe "SAP-Hinweis 3024346" (SAP-Login erforderlich).

Unterverzeichnisse in /hana/Shared-Volume erstellen

Die folgenden Beispiele zeigen eine SAP HANA-Datenbank mit SID=NF2.

Um die erforderlichen Unterverzeichnisse zu erstellen, führen Sie eine der folgenden Aktionen durch:

- Mounten Sie für ein Single-Host-System die `/hana/shared` Volume erstellen und die `shared` Und `usr-sap` Unterverzeichnisse

```
sapcc-hana-tst-06:/mnt # mount <storage-hostname>:/NF2_shared /mnt/tmp
sapcc-hana-tst-06:/mnt # cd /mnt/tmp
sapcc-hana-tst-06:/mnt/tmp # mkdir shared
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap
sapcc-hana-tst-06:/mnt/tmp # cd ..
sapcc-hana-tst-06:/mnt # umount /mnt/tmp
```

- Mounten Sie für ein System mit mehreren Hosts die `/hana/shared` Volume erstellen und die `shared` Und das `usr-sap` Unterverzeichnisse für jeden Host.

  Die Beispielbefehle zeigen ein 2+1-HANA-System mit mehreren Hosts.

```
sapcc-hana-tst-06:/mnt # mount <storage-hostname>:/NF2_shared /mnt/tmp
sapcc-hana-tst-06:/mnt # cd /mnt/tmp
sapcc-hana-tst-06:/mnt/tmp # mkdir shared
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host1
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host2
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host3
sapcc-hana-tst-06:/mnt/tmp # cd ..
sapcc-hana-tst-06:/mnt # umount /mnt/tmp
```

Erstellen von Bereitstellungspunkten

Die folgenden Beispiele zeigen eine SAP HANA-Datenbank mit SID=NF2.

Um die erforderlichen Mount-Point-Verzeichnisse zu erstellen, führen Sie eine der folgenden Aktionen durch:

- Erstellen Sie für ein System mit einem einzelnen Host Mount Points und legen Sie die Berechtigungen für den Datenbank-Host fest.

```
sapcc-hana-tst-06:/ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-06:/ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-06:/ # mkdir -p /hana/shared
sapcc-hana-tst-06:/ # mkdir -p /usr/sap/NF2

sapcc-hana-tst-06:/ # chmod –R 777 /hana/log/NF2
sapcc-hana-tst-06:/ # chmod –R 777 /hana/data/NF2
sapcc-hana-tst-06:/ # chmod -R 777 /hana/shared
sapcc-hana-tst-06:/ # chmod -R 777 /usr/sap/NF2
```

- Erstellen Sie für ein System mit mehreren Hosts Mount-Punkte und legen Sie die Berechtigungen für alle Worker und Standby-Hosts fest. Die folgenden Beispielbefehle gelten für ein 2+1-HANA-System mit mehreren Hosts.
  - Erster Worker-Host:

```
sapcc-hana-tst-06:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-06:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-06:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-06:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-06:~ # mkdir -p /hana/shared
sapcc-hana-tst-06:~ # mkdir -p /usr/sap/NF2

sapcc-hana-tst-06:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-06:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-06:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-06:~ # chmod -R 777 /usr/sap/NF2
```

- Host zweiter Arbeiter:

```
sapcc-hana-tst-07:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-07:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-07:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-07:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-07:~ # mkdir -p /hana/shared
sapcc-hana-tst-07:~ # mkdir -p /usr/sap/NF2

sapcc-hana-tst-07:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-07:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-07:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-07:~ # chmod -R 777 /usr/sap/NF2
```

- Standby-Host:

```
sapcc-hana-tst-08:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-08:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-08:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-08:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-08:~ # mkdir -p /hana/shared
sapcc-hana-tst-08:~ # mkdir -p /usr/sap/NF2

sapcc-hana-tst-08:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-08:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-08:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-08:~ # chmod -R 777 /usr/sap/NF2
```

Mounten Sie File-Systeme

Abhängig von der NFS-Version und der ONTAP-Version müssen verschiedene Mount-Optionen verwendet werden. Die folgenden Filesysteme müssen an die Hosts angehängt werden:

- `/hana/data/SID/mnt0000*`
- `/hana/log/SID/mnt0000*`
- `/hana/shared`
- `/usr/sap/SID`

Die folgende Tabelle zeigt die NFS-Versionen, die Sie für die verschiedenen Dateisysteme für SAP HANA-Datenbanken mit einem oder mehreren Hosts verwenden müssen.

File-Systeme	SAP HANA einzelner Host	SAP HANA mehrere Hosts
/hana/Data/SID/mnt0000*	NFSv3 oder NFSv4	NFSv4
/hana/log/SID/mnt0000*	NFSv3 oder NFSv4	NFSv4
/hana/Shared	NFSv3 oder NFSv4	NFSv3 oder NFSv4
/Usr/sap/SID	NFSv3 oder NFSv4	NFSv3 oder NFSv4

Die folgende Tabelle zeigt die Mount-Optionen für die verschiedenen NFS-Versionen und ONTAP-Versionen. Die gängigen Parameter sind unabhängig von den Versionen NFS und ONTAP.

> Für SAP Lama muss das Verzeichnis /usr/sap/SID lokal sein. Mounten Sie daher kein NFS-Volume für /usr/sap/SID, wenn Sie SAP Lama verwenden.

Bei NFSv3 müssen Sie die NFS-Sperre deaktivieren, um NFS-Sperrungen im Falle eines Software- oder Serverausfalls zu vermeiden.

Mit ONTAP 9 kann die NFS-Übertragungsgröße bis zu 1 MB konfiguriert werden. Insbesondere bei 40-GbE- oder schnelleren Verbindungen zum Storage-System muss die Übertragungsgröße auf 1 MB gesetzt werden, um die erwarteten Durchsatzwerte zu erzielen.

Allgemeiner Parameter	NFSv3	NFSv4	NFS-Übertragungsgröße mit ONTAP 9	NFS-Übertragungsgröße mit ONTAP 8
rw, bg, Hard, timeso=600, noatim	Nfsvers=3,nolock	Nfsvers=4.1,sperren	Rsize=1048576,wsize=262144	Rsize=65536,wsize=65536

Um die Lese-Performance mit NFSv3 zu verbessern, empfiehlt NetApp, den zu verwenden `nconnect=n` Mount-Option, die mit SUSE Linux Enterprise Server 12 SP4 oder höher und RedHat Enterprise Linux (RHEL) 8.3 oder höher verfügbar ist.

Performance-Tests haben das gezeigt `nconnect=4` Liefert gute Leseergebnisse für die Datenvolumen. Protokollschreibvorgänge können von einer geringeren Anzahl von Sitzungen profitieren, z. B. `nconnect=2`. Für gemeinsam genutzte Volumes kann die Option 'Nconnect' auch von Vorteil sein. Beachten Sie, dass der erste Mount von einem NFS-Server (IP-Adresse) die Anzahl der verwendeten Sitzungen definiert. Weitere Halterungen an dieselbe IP-Adresse ändern dies nicht, auch wenn für nconnect ein anderer Wert verwendet wird.

Ab ONTAP 9.8 und SUSE SLES15SP2 oder RedHat RHEL 8.4 oder höher unterstützt NetApp die nconnect Option auch für NFSv4.1. Weitere Informationen finden Sie in der Dokumentation des Linux-Anbieters.

Wenn nconnect mit NFSV4.x verwendet wird, sollte die Anzahl der NFSv4.x-Sitzungsplätze gemäß der folgenden Regel angepasst werden: Anzahl der Sitzungsplätze entspricht <nconnect value> x 64. Auf dem Host wird dies durch einen Neustart adjuseted `echo options nfs max_session_slots=<calculated value> > /etc/modprobe.d/nfsclient.conf`. Der serverseitige Wert muss ebenfalls angepasst werden. Legen Sie die Anzahl der Sitzungsplätze fest, wie unter beschrieben "NFS-Konfiguration für NFSv4:"

Das folgende Beispiel zeigt eine SAP HANA-Datenbank mit einem einzelnen Host mit SID=NF2 und NFSv3 sowie eine NFS-Übertragungsgröße von 1 MB für Lesevorgänge und 256 KB für Schreibvorgänge. So mounten Sie die Dateisysteme während des Systemstarts mit dem `/etc/fstab` Konfigurationsdatei, führen Sie die folgenden Schritte aus:

1. Fügen Sie die erforderlichen Dateisysteme zum hinzu `/etc/fstab` Konfigurationsdatei

```
sapcc-hana-tst-06:/ # cat /etc/fstab
<storage-vif-data01>:/NF2_data_mnt00001 /hana/data/NF2/mnt00001 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-log01>:/NF2_log_mnt00001 /hana/log/NF2/mnt00001 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=2,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-data01>:/NF2_shared/usr-sap /usr/sap/NF2 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-data01>:/NF2_shared/shared /hana/shared nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
```

2. Laufen `mount -a` Um die Dateisysteme auf allen Hosts einzubinden.

Das nächste Beispiel zeigt eine SAP HANA Datenbank mit mehreren Hosts und SID=NF2 unter Verwendung von NFSv4.1 für Daten- und Log-Filesysteme und NFSv3 für die `/hana/shared` Und `/usr/sap/NF2` File-Systeme. Es wird eine NFS-Transfergröße von 1 MB für Lesevorgänge und 256 KB für Schreibvorgänge verwendet.

1. Fügen Sie die erforderlichen Dateisysteme zum hinzu `/etc/fstab` Konfigurationsdatei auf allen Hosts.

> Der `/usr/sap/NF2` Dateisystem ist für jeden Datenbank-Host unterschiedlich. Das folgende Beispiel zeigt `/NF2_shared/usr-sap-host1`.

```
stlrx300s8-5:/ # cat /etc/fstab
<storage-vif-data01>:/NF2_data_mnt00001 /hana/data/NF2/mnt00001 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-data02>:/NF2_data_mnt00002 /hana/data/NF2/mnt00002 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-log01>:/NF2_log_mnt00001 /hana/log/NF2/mnt00001 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=2,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-log02>:/NF2_log_mnt00002 /hana/log/NF2/mnt00002 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=2,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-data02>:/NF2_shared/usr-sap-host1 /usr/sap/NF2 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-data02>:/NF2_shared/shared /hana/shared nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
```

2. Laufen `mount -a` Um die Dateisysteme auf allen Hosts einzubinden.

Vorbereitung der Installation von SAP HANA auf NFSv4

Für NFS Version 4 und höher ist Benutzerauthentifizierung erforderlich. Diese Authentifizierung kann über ein zentrales Benutzerverwaltungstool wie z. B. einen LDAP-Server (Lightweight Directory Access Protocol) oder lokale Benutzerkonten erfolgen. In den folgenden Abschnitten wird die Konfiguration lokaler Benutzerkonten beschrieben.

Die Administrationsteilnehmer `<sid>adm`,`<sid>crypt` und die `sapsys` Gruppe müssen vor Beginn der Installation der SAP HANA-Software manuell auf den SAP HANA-Hosts und den Speicher-Controllern erstellt werden.

SAP HANA-Hosts

Wenn es nicht existiert, die `sapsys` Die Gruppe muss auf dem SAP HANA-Host erstellt werden. Es muss eine eindeutige Gruppen-ID ausgewählt werden, die keinen Konflikt mit den vorhandenen Gruppen-IDs auf den Speicher-Controllern hat.

Die Benutzer `<sid>adm` und `<sid>crypt` werden auf dem SAP HANA-Host erstellt. Es müssen eindeutige IDs ausgewählt werden, die nicht mit bestehenden Benutzer-IDs auf den Storage Controllern in Konflikt stehen.

Bei einem SAP HANA-System mit mehreren Hosts müssen die Benutzer- und Gruppen-IDs auf allen SAP HANA-Hosts identisch sein. Die Gruppe und der Benutzer werden auf den anderen SAP HANA Hosts erstellt, indem die betroffenen Zeilen in und `/etc/passwd` vom Quellsystem auf alle anderen SAP HANA Hosts kopiert `/etc/group` werden.

Bei einem SAP HANA-System mit mehreren Hosts muss die Benutzer- und Gruppen-ID auf allen SAP HANA-Hosts gleich sein. Die Gruppe und der Benutzer werden auf den anderen SAP HANA-Hosts durch Kopieren der betroffenen Zeilen in erstellt `/etc/group` Und `/etc/passwd` Vom Quellsystem zu allen anderen SAP HANA-Hosts.

> Die NFSv4-Domäne muss auf allen Linux Servern und SVMs auf den gleichen Wert gesetzt werden. Legen Sie den Domain-Parameter fest "`Domain = <domain_name>`„ In Datei" `/etc/idmapd.conf` Für die Linux-Hosts.

NFS idmapd-Service aktivieren und starten:

```
systemctl enable nfs-idmapd.service
systemctl start nfs-idmapd.service
```

> Die neuesten Linux-Kernel benötigen diesen Schritt nicht. Sie können Warnmeldungen ohne Bedenken ignorieren.

Storage Controller

Die Benutzer-ID und die Gruppen-ID müssen auf den SAP HANA-Hosts und den Storage Controllern identisch sein. Die Gruppe und der Benutzer werden durch Eingabe der folgenden Befehle auf dem Storage-Cluster erstellt:

```
vserver services unix-group create -vserver <vserver> -name <group name>
-id <group id>
vserver services unix-user create -vserver <vserver> -user <user name> -id
<user-id> -primary-gid <group id>
```

Legen Sie außerdem die Gruppen-ID des UNIX-Benutzerstamms der SVM auf 0 fest.

```
vserver services unix-user modify -vserver <vserver> -user root -primary
-gid 0
```

I/O-Stack-Konfiguration für SAP HANA

Ab SAP HANA 1.0 SPS10 führte SAP Parameter ein, um das I/O-Verhalten anzupassen und die Datenbank für die verwendeten Datei- und Speichersysteme zu optimieren.

NetApp hat Performance-Tests durchgeführt, um die idealen Werte zu definieren. In der folgenden Tabelle sind die optimalen Werte aufgeführt, die aus den Leistungstests abgeleitet wurden.

Parameter	Wert
max_parallel_io_Requests	128
Async_read_Submit	Ein

Parameter	Wert
Async_write_submit_Active	Ein
Async_Write_Submit_Blocks	Alle

Bei SAP HANA 1.0 Versionen bis SPS12 können diese Parameter während der Installation der SAP HANA Datenbank eingestellt werden, wie in SAP Note beschrieben "2267798: Konfiguration der SAP HANA Datenbank während der Installation mit hdbparam".

Alternativ können die Parameter nach der SAP HANA-Datenbankinstallation über das festgelegt werden `hdbparam` Framework:

```
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.max_parallel_io_requests=128
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_write_submit_active=on
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_read_submit=on
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_write_submit_blocks=all
```

Ab SAP HANA 2.0 `hdbparam` Wurde veraltet und die Parameter wurden in verschoben `global.ini`. Die Parameter können mit SQL-Befehlen oder SAP HANA Studio eingestellt werden. Weitere Informationen finden Sie im SAP-Hinweis "2399079: Beseitigung von hdbparam in HANA 2". Die Parameter können wie unten gezeigt auch innerhalb der global.ini eingestellt werden:

```
nf2adm@stlrx300s8-6: /usr/sap/NF2/SYS/global/hdb/custom/config> cat
global.ini
…
[fileio]
async_read_submit = on
async_write_submit_active = on
max_parallel_io_requests = 128
async_write_submit_blocks = all
…
```

Ab SAP HANA 2.0 SPS5 können Sie den nutzen `setParameter.py` Skript zum Festlegen der richtigen Parameter:

```
nf2adm@sapcc-hana-tst-03:/usr/sap/NF2/HDB00/exe/python_support>
python setParameter.py
-set=SYSTEM/global.ini/fileio/max_parallel_io_requests=128
python setParameter.py -set=SYSTEM/global.ini/fileio/async_read_submit=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_active=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_blocks=all
```

Größe des SAP HANA Daten-Volumes

Standardmäßig verwendet SAP HANA nur ein Daten-Volume pro SAP HANA Service. Aufgrund der maximalen Dateigröße des Filesystems empfiehlt NetApp die Begrenzung der maximalen Größe des Daten-Volume.

Um dies automatisch zu tun, setzen Sie den folgenden Parameter in ein `global.ini` Im Abschnitt `[persistence]`:

```
datavolume_striping = true
datavolume_striping_size_gb = 8000
```

Dadurch wird ein neues Daten-Volume erstellt, nachdem das Limit von 8.000 GB erreicht wurde. "SAP Note 240005 Frage 15" Bietet weitere Informationen.

SAP HANA Softwareinstallation

In diesem Abschnitt wird die Konfiguration eines Systems für die Installation der SAP HANA-Software auf Systemen mit einem oder mehreren Hosts beschrieben.

Installation auf einem Single-Host-System

Die Installation der SAP HANA-Software erfordert keine zusätzliche Vorbereitung auf ein Single-Host-System.

Installation auf einem System mit mehreren Hosts

Gehen Sie wie folgt vor, um SAP HANA auf einem System mit mehreren Hosts zu installieren:

1. mithilfe des SAP- `hdbclm`Starten Sie die InstallationInstallationstools, indem Sie den folgenden Befehl an einem der Arbeitshosts ausführen. Verwenden Sie die `addhosts` Option, um den zweiten Worker (`sapcc-hana-tst-03`und den Standby-Host hinzuzufügen(`sapcc-hana-tst-04`.

   ```
   apcc-hana-tst-02:/mnt/sapcc-share/software/SAP/HANA2SPS7-
   73/DATA_UNITS/HDB_LCM_LINUX_X86_64 #
   ./hdblcm --action=install --addhosts=sapcc-hana-tst-03:role=worker,sapcc
   -hana-tst-04:role=standby
   ```

```
SAP HANA Lifecycle Management - SAP HANA Database 2.00.073.00.1695288802
************************************************************************


Scanning software locations...
Detected components:
    SAP HANA AFL (incl.PAL,BFL,OFL) (2.00.073.0000.1695321500) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_AFL_LINUX_X86_64/packages
    SAP HANA Database (2.00.073.00.1695288802) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
    SAP HANA Database Client (2.18.24.1695756995) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/SAP_HANA_CLIENT/client
    SAP HANA Studio (2.3.75.000000) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_STUDIO_LINUX_X86_64/studio
    SAP HANA Local Secure Store (2.11.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HANA_LSS_24_LINUX_X86_64/packages
    SAP HANA XS Advanced Runtime (1.1.3.230717145654) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_RT_10_LINUX_X86_64/packages
    SAP HANA EML AFL (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_EML_AFL_10_LINUX_X86_64/packages
    SAP HANA EPM-MDS (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/SAP_HANA_EPM-MDS_10/packages
    Automated Predictive Library (4.203.2321.0.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/PAAPL4_H20_LINUX_X86_64/apl-
4.203.2321.0-hana2sp03-linux_x64/installer/packages
    GUI for HALM for XSA (including product installer) Version 1
(1.015.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACALMPIUI15_0.zip
    XSAC FILEPROCESSOR 1.0 (1.000.102) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACFILEPROC00_102.zip
    SAP HANA tools for accessing catalog content, data preview, SQL
console, etc. (2.015.230503) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_HRTT_20/XSACHRTT15_230503.zip
    Develop and run portal services for customer applications on XSA
(2.007.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACPORTALSERV07_0.zip
    The SAP Web IDE for HANA 2.0 (4.007.0) in /mnt/sapcc-
```

```
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_SAP_WEB_IDE_20/XSACSAPWEBIDE07_0.zip
    XS JOB SCHEDULER 1.0 (1.007.22) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACSERVICES07_22.zip
    SAPUI5 FESV6 XSA 1 - SAPUI5 1.71 (1.071.52) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV671_52.zip
    SAPUI5 FESV9 XSA 1 - SAPUI5 1.108 (1.108.5) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV9108_5.zip
    SAPUI5 SERVICE BROKER XSA 1 - SAPUI5 Service Broker 1.0 (1.000.4) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5SB00_4.zip
    XSA Cockpit 1 (1.001.37) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACXSACOCKPIT01_37.zip


SAP HANA Database version '2.00.073.00.1695288802' will be installed.

Select additional components for installation:

  Index | Components      | Description

-------------------------------------------------------------------------
--------------------------
  1     | all             | All components
  2     | server          | No additional components
  3     | client          | Install SAP HANA Database Client version
2.18.24.1695756995
  4     | lss             | Install SAP HANA Local Secure Store version
2.11.0
  5     | studio          | Install SAP HANA Studio version
2.3.75.000000
  6     | xs              | Install SAP HANA XS Advanced Runtime version
1.1.3.230717145654
  7     | afl             | Install SAP HANA AFL (incl.PAL,BFL,OFL)
version 2.00.073.0000.1695321500
  8     | eml             | Install SAP HANA EML AFL version
2.00.073.0000.1695321500
  9     | epmmds          | Install SAP HANA EPM-MDS version
2.00.073.0000.1695321500
  10    | sap_afl_sdk_apl | Install Automated Predictive Library version
4.203.2321.0.0
```

```
Enter comma-separated list of the selected indices [3,4]: 2,3
```

2. Vergewissern Sie sich, dass das Installationstool alle ausgewählten Komponenten bei allen Worker- und Standby-Hosts installiert hat.

Zusätzliche Partitionen für Datenvolumen werden hinzugefügt

Ab SAP HANA 2.0 SPS4 können weitere Daten-Volume-Partitionen konfiguriert werden. Damit können Sie zwei oder mehr Volumes für das Daten-Volume einer SAP HANA-Mandantendatenbank konfigurieren und eine Skalierung über die Größe und Performance-Grenzen eines einzelnen Volumes hinaus vornehmen.

Für SAP HANA ist ein Single-Host und SAP HANA Multiple-Host-Systeme mit zwei oder mehr einzelnen Volumes für das Daten-Volume verfügbar. Sie können jederzeit weitere Partitionen für Datenvolumen hinzufügen.

Aktivieren von zusätzlichen Partitionen für Volumes

Um zusätzliche Datenträgers Partitionen zu aktivieren, fügen Sie den folgenden Eintrag in hinzu `global.ini` Mit SAP HANA Studio oder Cockpit in der SYSTEMDB Konfiguration.

```
[customizable_functionalities]
persistence_datavolume_partition_multipath = true
```

Manuelles Hinzufügen des Parameters zum `global.ini` Datei erfordert den Neustart der Datenbank.

Volume-Konfiguration für SAP HANA Systeme mit einem Host

Das Layout der Volumes für ein SAP HANA System mit mehreren Partitionen mit nur einem Host ist wie das Layout eines Systems mit einer Datenträgers, aber mit einem zusätzlichen Datenvolumen, das auf einem anderen Aggregat als das Protokoll-Volume und das andere Datenvolumen gespeichert ist. Die folgende Tabelle zeigt eine Beispielkonfiguration eines SAP HANA Einzelhostsystems mit zwei Daten-Volume-Partitionen.

Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregat 2 bei Controller b
Datenvolumen: SID_Data_mnt00001	Gemeinsam genutztes Volume: SID_shared	Datenvolumen: SID_data2_mnt00001	Protokollvolumen: SID_log_mnt00001

Die folgende Tabelle zeigt ein Beispiel für die Mount-Punkt-Konfiguration für ein System mit einem einzelnen Host mit zwei Daten-Volume-Partitionen.

Verbindungspfad	Verzeichnis	Bereitstellungspunkt beim HANA-Host
SID_Data_mnt00001	–	/hana/Data/SID/mnt00001
SID_data2_mnt00001	–	/hana/data2/SID/mnt00001
SID_Log_mnt00001	–	/hana/log/SID/mnt00001

Verbindungspfad	Verzeichnis	Bereitstellungspunkt beim HANA-Host
SID_freigegeben	Usr-sap freigegeben	/Usr/sap/SID /hana/Shared

Sie können das neue Daten-Volume erstellen und es entweder mithilfe von NetApp ONTAP System Manager oder der ONTAP CLI in den Namespace mounten.

Volume-Konfiguration für SAP HANA Systeme mit mehreren Hosts

Das Layout der Volumes ist wie das Layout eines SAP HANA Systems mit mehreren Hosts mit einer Daten-Volume-Partition aber mit einem zusätzlichen Daten-Volume gespeichert auf einem anderen Aggregat als Log-Volume und dem anderen Daten-Volume. Die folgende Tabelle zeigt eine Beispielkonfiguration eines SAP HANA Multihost-Systems mit zwei Daten-Volume-Partitionen.

Zweck	Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregieren 2 bei Controller B
Daten- und Protokoll-Volumes für Node 1	Datenvolumen: SID_Data_mnt00001	–	Protokollvolumen: SID_log_mnt00001	Daten2 Volumen: SID_data2_mnt00001
Daten- und Protokoll-Volumes für Node 2	Protokollvolumen: SID_log_mnt002	Daten2 Volumen: SID_data2_mnt002	Datenvolumen: SID_Data_mnt002	–
Daten- und Protokoll-Volumes für Node 3	–	Datenvolumen: SID_Data_mnt00003	Daten2 Volumen: SID_data2_mnt003	Protokollvolumen: SID_log_mnt00003
Daten- und Protokoll-Volumes für Node 4	Daten2 Volumen: SID_data2_mnt004	Protokollvolumen: SID_log_mnt004	–	Datenvolumen: SID_Data_mnt00004
Gemeinsames Volume für alle Hosts	Gemeinsam genutztes Volume: SID_shared	–	–	–

Die folgende Tabelle zeigt ein Beispiel für die Mount-Punkt-Konfiguration für ein System mit einem einzelnen Host mit zwei Daten-Volume-Partitionen.

Verbindungspfad	Verzeichnis	Bereitstellungspunkt beim SAP HANA-Host	Hinweis
SID_Data_mnt00001	–	/hana/Data/SID/mnt00001	Auf allen Hosts montiert
SID_data2_mnt00001	–	/hana/data2/SID/mnt00001	Auf allen Hosts montiert
SID_Log_mnt00001	–	/hana/log/SID/mnt00001	Auf allen Hosts montiert
SID_Data_mnt00002	–	/hana/Data/SID/mnt002	Auf allen Hosts montiert
SID_data2_mnt00002	–	/hana/data2/SID/mnt002	Auf allen Hosts montiert
SID_Log_mnt00002	–	/hana/log/SID/mnt002	Auf allen Hosts montiert
SID_Data_mnt00003	–	/hana/Data/SID/mnt003	Auf allen Hosts montiert

Verbindungspfad	Verzeichnis	Bereitstellungspunkt beim SAP HANA-Host	Hinweis
SID_data2_mnt00003		/hana/data2/SID/mnt003	Auf allen Hosts montiert
SID_log_mnt00003		/hana/log/SID/mnt003	Auf allen Hosts montiert
SID_Data_mnt00004		/hana/Data/SID/mnt004	Auf allen Hosts montiert
SID_data2_mnt00004	–	/hana/data2/SID/mnt004	Auf allen Hosts montiert
SID_log_mnt00004	–	/hana/log/SID/mnt004	Auf allen Hosts montiert
SID_freigegeben	Freigegeben	/hana/Shared/SID	Auf allen Hosts montiert
SID_freigegeben	Usr-sap-host1	/Usr/sap/SID	Angehängt auf Host 1
SID_freigegeben	Usr-sap-host2	/Usr/sap/SID	Angehängt auf Host 2
SID_freigegeben	Usr-sap-host3	/Usr/sap/SID	Angehängt auf Host 3
SID_freigegeben	Usr-sap-host4	/Usr/sap/SID	Angehängt auf Host 4
SID_freigegeben	Usr-sap-host5	/Usr/sap/SID	Angehängt auf Host 5

Sie können das neue Daten-Volume erstellen und es entweder mithilfe von ONTAP System Manager oder der ONTAP CLI in den Namespace mounten.

Host-Konfiguration

Zusätzlich zu den im Abschnitt beschriebenen Aufgaben "Host-Einrichtung"müssen die zusätzlichen Mount-Punkte und `fstab` Einträge für die neuen zusätzlichen Daten-Volumes erstellt und die neuen Volumes gemountet werden.

1. Erstellen Sie zusätzliche Bereitstellungspunkte.
   - Erstellen Sie für ein System mit einem einzelnen Host Mount Points und legen Sie die Berechtigungen für den Datenbank-Host fest:

     ```
     sapcc-hana-tst-06:/ # mkdir -p /hana/data2/SID/mnt00001
     sapcc-hana-tst-06:/ # chmod –R 777 /hana/data2/SID
     ```

   - Erstellen Sie für ein System mit mehreren Hosts Mount-Punkte und legen Sie die Berechtigungen für alle Worker und Standby-Hosts fest.

     Die folgenden Beispielbefehle gelten für ein HANA-System mit mehreren Hosts und zwei plus 1.

     - Erster Worker-Host:

       ```
       sapcc-hana-tst-06:~ # mkdir -p /hana/data2/SID/mnt00001
       sapcc-hana-tst-06:~ # mkdir -p /hana/data2/SID/mnt00002
       sapcc-hana-tst-06:~ # chmod -R 777 /hana/data2/SID
       ```

     - Host zweiter Arbeiter:

```
sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00001
sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00002
sapcc-hana-tst-07:~ # chmod -R 777 /hana/data2/SID
```

- Standby-Host:

```
sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00001
sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00002
sapcc-hana-tst-07:~ # chmod -R 777 /hana/data2/SID
```

2. Fügen Sie die zusätzlichen Dateisysteme zum hinzu `/etc/fstab` Konfigurationsdatei auf allen Hosts.

   Im folgenden Beispiel ist ein System mit Single-Host unter Verwendung von NFSv4.1 enthalten:

```
<storage-vif-data02>:/SID_data2_mnt00001 /hana/data2/SID/mnt00001 nfs
rw, vers=4
minorversion=1,hard,timeo=600,rsize=1048576,wsize=262144,bg,noatime,lock
0 0
```

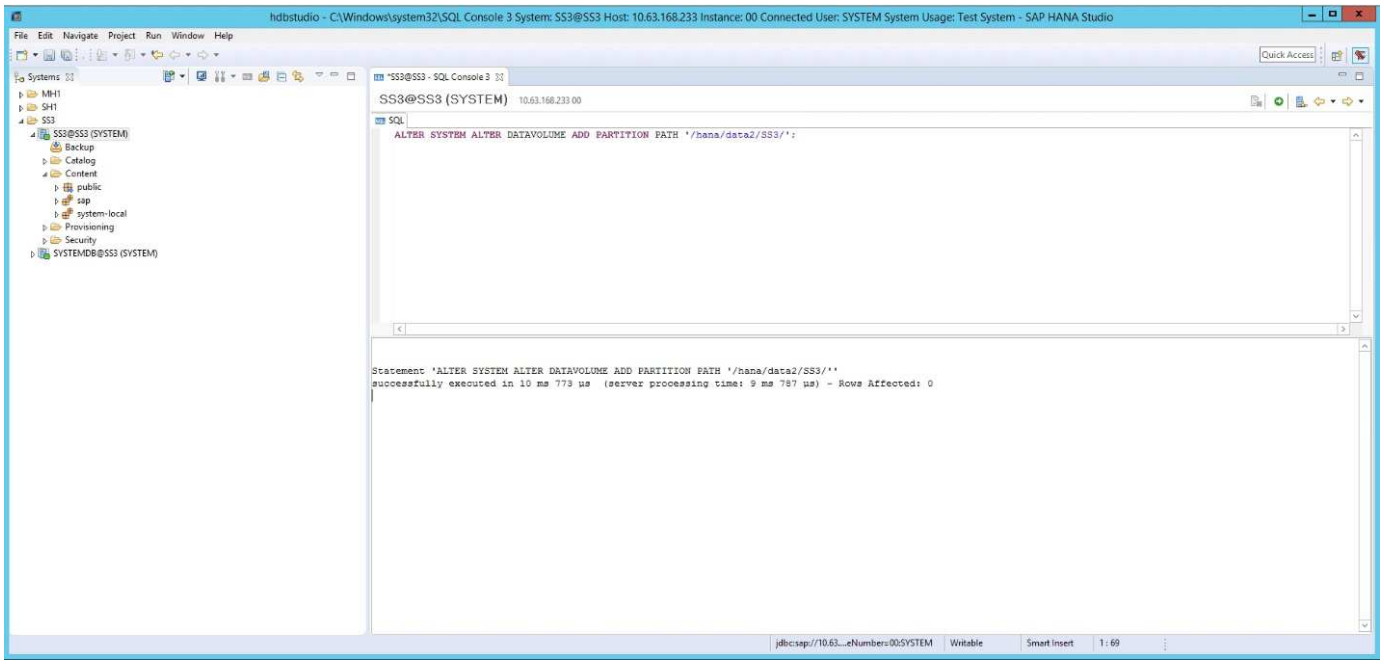
   Verwenden Sie eine andere virtuelle Speicherschnittstelle zum Verbinden der einzelnen Datenträger, um sicherzustellen, dass Sie unterschiedliche TCP-Sitzungen für jedes Volume verwenden oder die Option nconnect Mount verwenden, falls verfügbar für Ihr Betriebssystem.

3. Mounten Sie die Dateisysteme, indem Sie den ausführen `mount -a` Befehl.

Hinzufügen einer zusätzlichen Daten-Volume-Partition

Führen Sie die folgende SQL-Anweisung für die Mandantendatenbank aus, um Ihrer Mandantendatenbank eine zusätzliche Partition für das Datenvolumen hinzuzufügen. Verwenden Sie den Pfad zu zusätzlichen Volumes:

```
ALTER SYSTEM ALTER DATAVOLUME ADD PARTITION PATH '/hana/data2/SID/';
```



Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten bzw. auf den folgenden Websites:

- "SAP HANA Softwarelösungen"
- "TR-4646: SAP HANA Disaster Recovery with Storage Replication"
- "TR-4614: SAP HANA Backup and Recovery with SnapCenter"
- "TR-4667: Automatisierung von SAP Systemkopien mit dem SnapCenter SAP HANA Plug-in"
- NetApp Dokumentationszentren

  "https://www.netapp.com/support-and-training/documentation/"
- SAP Certified Enterprise Storage Hardware for SAP HANA

  "https://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/"
- SAP HANA Storage-Anforderungen

  "https://www.sap.com/documents/2024/03/146274d3-ae7e-0010-bca6-c68f7e60039b.html"
- SAP HANA Tailored Data Center Integration Häufig gestellte Fragen

  "https://www.sap.com/documents/2016/05/e8705aae-717c-0010-82c7-eda71af511fa.html"
- SAP HANA auf VMware vSphere Wiki

  "https://help.sap.com/docs/SUPPORT_CONTENT/virtualization/3362185751.html"
- Best Practices Guide für SAP HANA auf VMware vSphere

  "https://www.vmware.com/docs/sap_hana_on_vmware_vsphere_best_practices_guide-white-paper"

Aktualisierungsverlauf

An dieser Lösung wurden seit ihrer ersten Veröffentlichung folgende technische Änderungen vorgenommen:

Datum	Zusammenfassung aktualisieren
Oktober 2015	Ausgangsversion
März 2016	Aktualisierte Angaben zur Kapazitätsdimensionierung Mount-Optionen für aktualisiert `/hana/shared`Sysctl-Parameter aktualisiert
Februar 2017	Neue NetApp Storage-Systeme und Platten-Shelves Neue Funktionen von ONTAP 9 Unterstützung für 40 GbE Neue Betriebssystemversionen (SUSE Linux Enterprise Server 12 SP1 und Red hat Enterprise Linux 7.2) die neue SAP HANA-Version
Juli 2017	Kleine Updates
September 2018	Neue NetApp Storage-Systeme Unterstützung neuer Betriebssystemversionen mit 100 GbE (SUSE Linux Enterprise Server 12 SP3 und Red hat Enterprise Linux 7.4) zusätzliche kleinere Änderungen SAP HANA 2.0 SPS3
Oktober 2019	Neue NetApp Storage-Systeme und NVMe Shelf Neue Betriebssystemversionen (SUSE Linux Enterprise Server 12 SP4, SUSE Linux Enterprise Server 15 und Red hat Enterprise Linux 7.6) MAX Data Volumes klein – Änderungen
Dezember 2019	Neue NetApp Storage-Systeme Neues Betriebssystem SUSE Linux Enterprise Server 15 SP1
März 2020	Unterstützung von nconnect für NFSv3 New OS Release Red hat Enterprise Linux 8
Mai 2020	Unterstützung für mehrere Partitionen von Datenvolumen, verfügbar mit SAP HANA 2.0 SPS4
Juni 2020	Zusätzliche Informationen über optionale Funktionalitäten kleine Updates
Dezember 2020	Unterstützung von nconnect für NFSv4.1 ab ONTAP 9.8 Neue Betriebssystemversionen Neue SAP HANA Versionen
Februar 2021	Änderungen an den Host-Netzwerkeinstellungen durch neue NetApp Storage-Systeme – kleinere Änderungen
April 2021	VMware vSphere-spezifische Informationen hinzugefügt
September 2022	Neue Betriebssystemversionen
August 2023	Neue Storage-Systeme (AFF C-Serie)
Dezember 2023	Aktualisierung des Host-Setups überarbeitete nconnect-Einstellungen Informationen zu NFSv4.1-Sitzungen hinzugefügt
Mai 2024	Neue Storage-Systeme (AFF A-Series)
September 2024	Kleinere Updates
November 2024	Neue Storage-Systeme

Datum	Zusammenfassung aktualisieren
Juli 2025	Kleine Updates

Technischer Bericht: SAP HANA on NetApp ASA Systems with FCP Configuration Guide

Technischer Bericht: SAP HANA on NetApp ASA Systems with Fibre Channel Protocol

Die NetApp ASA Produktfamilie ist für die Verwendung mit SAP HANA in TDI Projekten zertifiziert. Dieser Leitfaden enthält Best Practices für SAP HANA auf dieser Plattform.

Marco Schoen, NetApp

Einführung

Die Produktfamilien NetApp ASA A-Series und ASA C-Series wurden für den Einsatz mit SAP HANA in Tailored Datacenter Integration-Projekten (TDI) zertifiziert. In diesem Handbuch werden die Best Practices für die folgenden zertifizierten Modelle beschrieben:

- ASA A20, ASA A30, ASA A50, ASA A70, ASA A90, ASA A1K
- ASA C30

Eine vollständige Liste der zertifizierten NetApp Storage-Lösungen für SAP HANA finden Sie unter "Zertifiziertes und unterstütztes SAP HANA-Hardwaresverzeichnis".

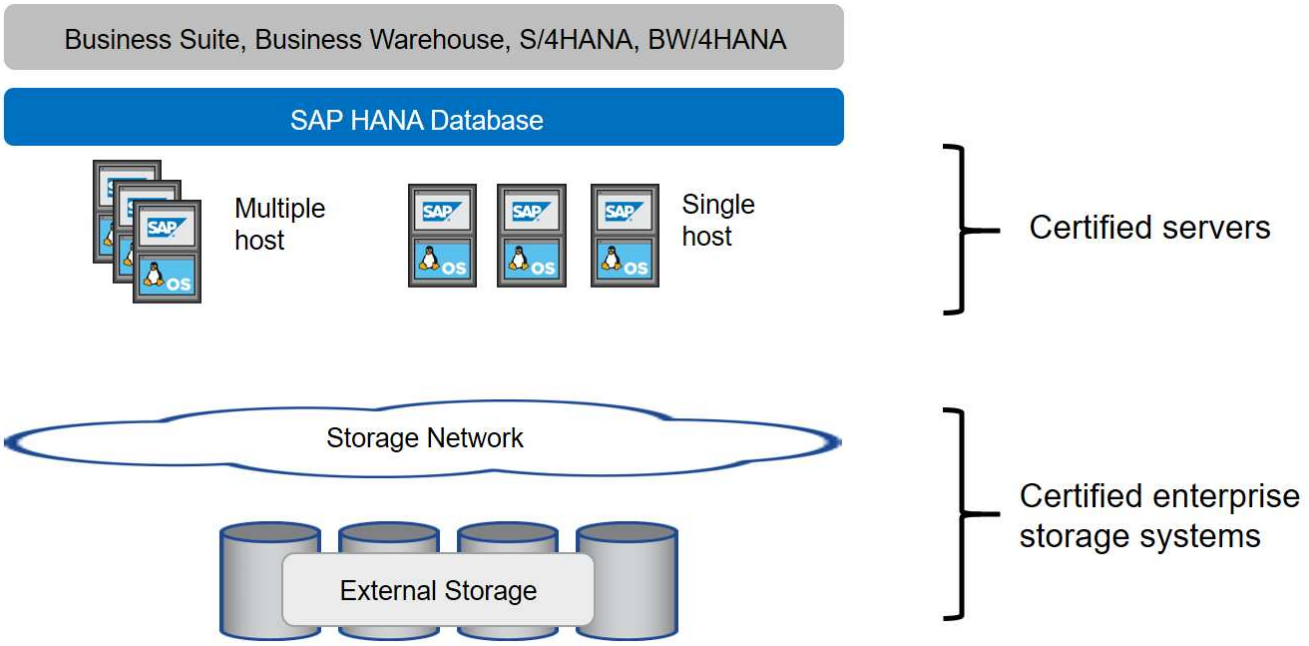
In diesem Dokument werden die ASA-Konfigurationen beschrieben, die das Fibre Channel Protocol (FCP) verwenden.

> Die in diesem Dokument beschriebene Konfiguration ist erforderlich, um die erforderlichen SAP HANA KPIs und die beste Performance für SAP HANA zu erreichen. Wenn Sie Einstellungen oder Funktionen ändern, die nicht in diesem Dokument aufgeführt sind, kann dies zu einer Performance-Verschlechterung oder zu einem unerwarteten Verhalten führen. Diese Einstellungen sollten nur vorgenommen werden, wenn dies durch den NetApp Support empfohlen wird.

In einer SAP HANA Umgebung mit mehreren Hosts wird der standardmäßige SAP HANA-Storage-Connector verwendet, um im Falle eines Failover des SAP HANA-Hosts zu Fechten. Beachten Sie immer die relevanten SAP-Hinweise für Konfigurationsrichtlinien für Betriebssysteme und HANA-spezifische Linux-Kernel-Abhängigkeiten. Weitere Informationen finden Sie unter "SAP Note 2235581 – von SAP HANA unterstützte Betriebssysteme".

SAP HANA Tailored Datacenter Integration

NetApp ASA-Speichersysteme sind im SAP HANA TDI-Programm unter Verwendung von FC (SAN)-Protokollen zertifiziert. Sie können in allen aktuellen SAP HANA-Szenarien eingesetzt werden, beispielsweise in SAP Business Suite auf HANA, S/4HANA, BW/4HANA oder SAP Business Warehouse auf HANA, entweder in Einzelhost- oder Mehrhostkonfigurationen. Alle Server, die für den Einsatz mit SAP HANA zertifiziert sind, können mit von NetApp zertifizierten Storage-Lösungen kombiniert werden. Die folgende Abbildung bietet einen Überblick über die Architektur.



Weitere Informationen zu den Voraussetzungen und Empfehlungen für produktive SAP HANA-Systeme finden Sie in der folgenden Ressource:

- "SAP HANA Tailored Data Center Integration Häufig gestellte Fragen"

SAP HANA mit VMware vSphere

Es stehen verschiedene Optionen zur Verbindung von Storage mit Virtual Machines (VMs) zur Verfügung. Raw Device Mappings (RDM), FCP-Datenspeicher oder VVOL-Datenspeicher mit FCP werden unterstützt. Bei beiden Datastore-Optionen muss für produktive Anwendungsfälle nur eine SAP HANA Daten oder ein Protokoll-Volume im Datastore gespeichert werden.

Weitere Informationen zur Verwendung von vSphere mit SAP HANA finden Sie unter den folgenden Links:

- "SAP HANA on VMware vSphere - Virtualization - Community Wiki"
- "Best Practices Guide für SAP HANA auf VMware vSphere"
- "2161991 - Konfigurationsrichtlinien für VMware vSphere - SAP ONE Support Launchpad (Anmeldung erforderlich)"

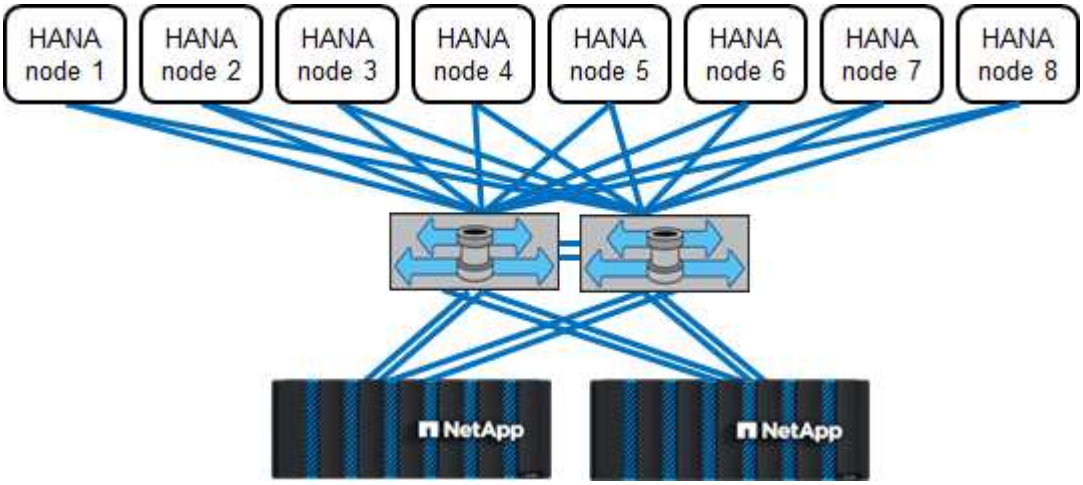
Der Netapp Architektur Sind

SAP HANA Hosts sind über eine redundante FCP-Infrastruktur und Multipathing-Software mit Storage Controllern verbunden. Eine redundante FCP Switch-Infrastruktur ist erforderlich, um eine fehlertolerante SAP HANA Host-zu-Storage-Konnektivität bei Ausfall von Switch oder Host Bus Adapter (HBA) bereitzustellen. Ein entsprechendes Zoning muss am Switch konfiguriert werden, damit alle HANA Hosts die erforderlichen LUNs auf den Storage Controllern erreichen können.

Verschiedene Modelle der ASA Produktfamilie können auf der Storage-Ebene miteinander kombiniert werden, um Wachstum und unterschiedliche Anforderungen an Performance und Kapazität zu ermöglichen. Die maximale Anzahl an SAP HANA-Hosts, die an das Storage-System angeschlossen werden können, sind durch die SAP HANA-Performance-Anforderungen und das Modell des verwendeten NetApp Controllers definiert. Die Anzahl der benötigten Festplatten-Shelfs wird nur von den Kapazitäts- und Performance-Anforderungen

der SAP HANA Systeme bestimmt.

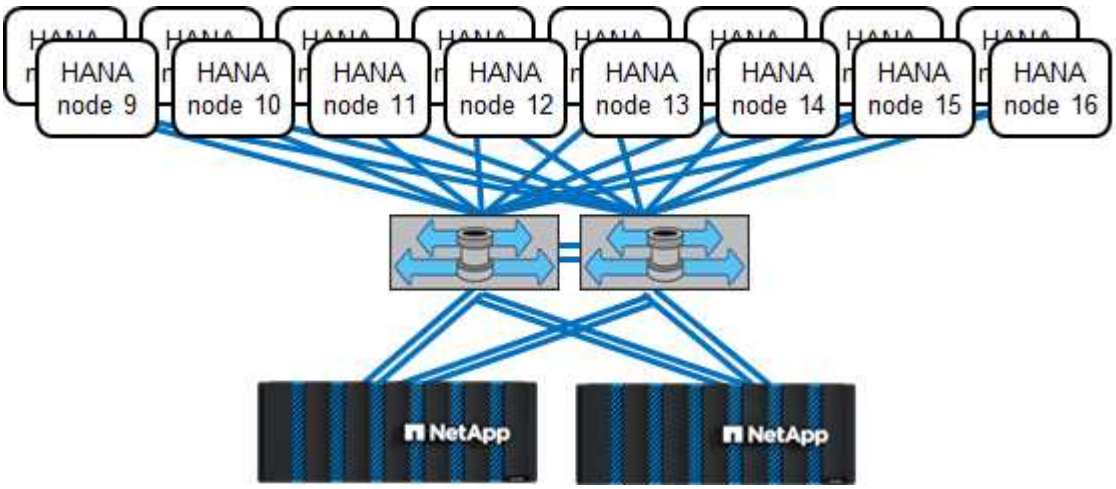
Die folgende Abbildung zeigt eine Beispielkonfiguration mit acht SAP HANA-Hosts, die an ein Storage HA-Paar angeschlossen sind.



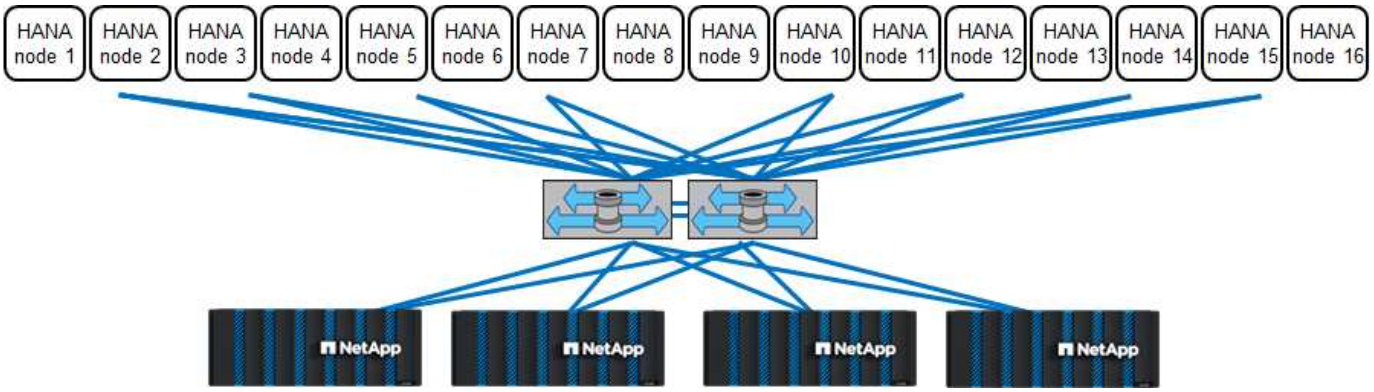
Diese Architektur lässt sich in zwei Dimensionen skalieren:

- Indem zusätzliche SAP HANA-Hosts und Storage-Kapazität an den vorhandenen Storage angeschlossen werden, können die Storage-Controller genügend Performance bieten, um die aktuellen SAP HANA-KPIs zu erfüllen
- Durch Hinzufügen weiterer Storage-Systeme mit zusätzlicher Storage-Kapazität für die zusätzlichen SAP HANA-Hosts

Die folgende Abbildung zeigt ein Konfigurationsbeispiel, in dem mehr SAP HANA-Hosts mit den Storage-Controllern verbunden sind. In diesem Beispiel sind mehr Platten-Shelves erforderlich, um die Kapazitäts- und Performance-Anforderungen der 16 SAP HANA-Hosts zu erfüllen. Abhängig von den Anforderungen an den Gesamtdurchsatz müssen die Storage Controller um zusätzliche FC-Verbindungen erweitert werden.



Unabhängig vom implementierten ASA System lässt sich die SAP HANA Landschaft auch skalieren, indem beliebige zertifizierte Storage-Controller hinzugefügt werden, um die gewünschte Node-Dichte zu erfüllen, wie in der folgenden Abbildung dargestellt.

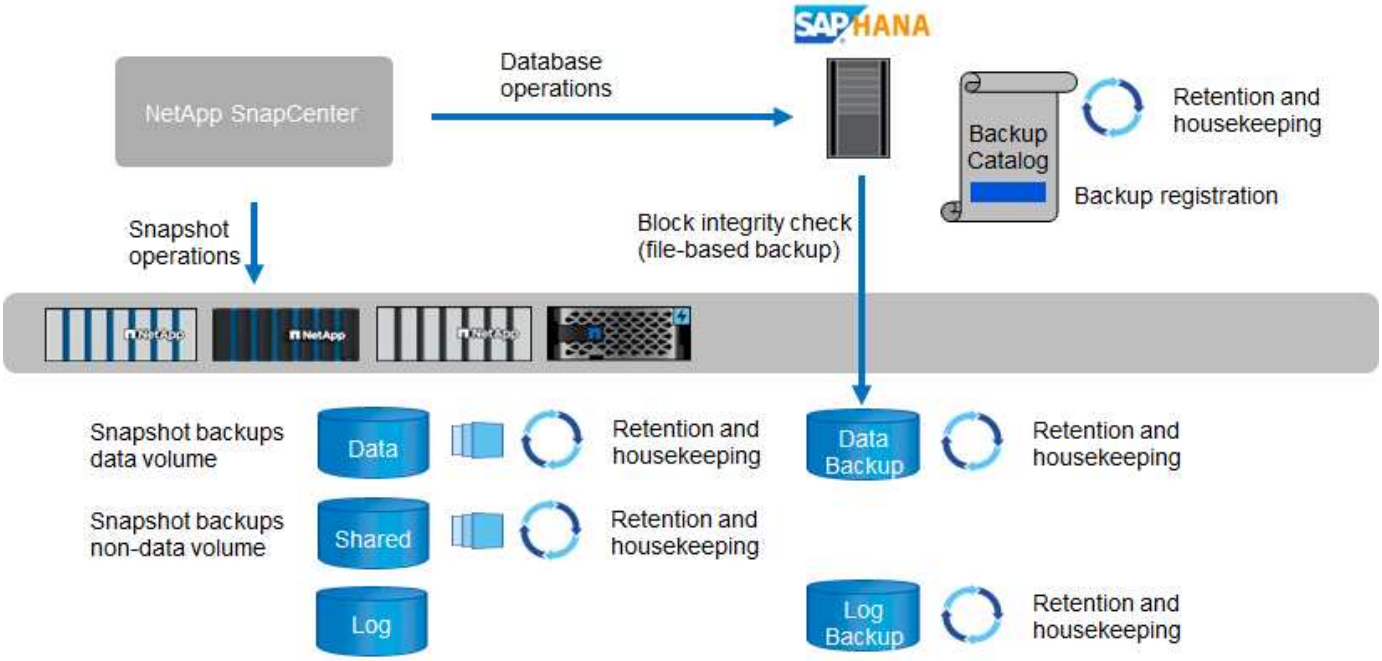


SAP HANA Backup

Die auf allen NetApp Storage-Controllern vorhandene ONTAP Software bietet einen integrierten Mechanismus zur Sicherung von SAP HANA Datenbanken, ohne die Performance zu beeinträchtigen. Storage-basierte NetApp Snapshot-Backups sind eine vollständig unterstützte und integrierte Backup-Lösung, die für einzelne SAP HANA Container sowie für SAP HANA MDC-Systeme mit einem einzelnen Mandanten oder mehreren Mandanten verfügbar ist.

Storage-basierte Snapshot Backups werden über das NetApp SnapCenter Plug-in für SAP HANA implementiert. Benutzer können auf diese Weise konsistente Storage-basierte Snapshot Backups mithilfe der Schnittstellen erstellen, die nativ von SAP HANA Datenbanken bereitgestellt werden. SnapCenter registriert jedes der Snapshot-Backups im SAP HANA-Backup-Katalog. Backups von SnapCenter sind somit innerhalb von SAP HANA Studio oder im Cockpit sichtbar, wo sie direkt für Restore- und Recovery-Vorgänge selektiert werden können.

Mit der NetApp SnapMirror Technologie können Snapshot Kopien, die auf einem Storage-System erstellt wurden, in ein sekundäres Backup-Storage-System repliziert werden, das über SnapCenter gesteuert wird. Für jedes der Backup-Sätze auf dem primären Storage und auch für die Backup-Sets auf den sekundären Storage-Systemen können somit unterschiedliche Backup-Aufbewahrungsrichtlinien definiert werden. Das SnapCenter Plug-in für SAP HANA managt automatisch die Aufbewahrung von auf Snapshot Kopien basierenden Daten-Backups und Log-Backups, einschließlich der allgemeinen Ordnung des Backup-Katalogs. Das SnapCenter Plug-in für SAP HANA ermöglicht darüber hinaus die Ausführung einer Blockintegritätsprüfung der SAP HANA-Datenbank durch Ausführen eines dateibasierten Backups.



Storage-basierte Snapshot Backups bieten im Vergleich zu herkömmlichen dateibasierten Backups deutliche Vorteile. Zu diesen Vorteilen zählen unter anderem:

- Schnelleres Backup (einige Minuten)
- Reduzierte RTO aufgrund einer wesentlich schnelleren Restore-Zeit auf der Storage-Ebene (wenige Minuten) und häufigerer Backups
- Kein Performance-Abfall des SAP HANA-Datenbankhosts, -Netzwerks oder -Storage während Backup- und Recovery-Vorgängen
- Platzsparende und bandbreiteneffiziente Replizierung auf Basis von Blockänderungen auf sekundärem Storage

Weitere Informationen zur Backup- und Recovery-Lösung von SAP HANA finden Sie unter "SAP HANA Datensicherung und Hochverfügbarkeit mit SnapCenter, SnapMirror Active Sync und VMware Metro Storage Cluster".

Zum Zeitpunkt der Erstellung dieses Dokuments werden von SnapCenter für ASA nur VMware-basierte VMs unterstützt, die VMDKs als Speicher verwenden.

Disaster Recovery für SAP HANA

Das Disaster Recovery für SAP HANA ist entweder auf der Datenbankebene mithilfe von SAP HANA-Systemreplizierung oder auf der Storage-Ebene mithilfe von Storage-Replizierungstechnologien möglich. Der folgende Abschnitt bietet einen Überblick über Disaster-Recovery-Lösungen basierend auf der Storage-Replizierung.

Weitere Informationen zu den Disaster-Recovery-Lösungen für SAP HANA finden Sie unter "TR-4646: SAP HANA Disaster Recovery with Storage Replication".

Storage-Replizierung basierend auf SnapMirror

Die folgende Abbildung zeigt eine Disaster-Recovery-Lösung für drei Standorte mit synchroner SnapMirror Active Sync zum lokalen DR-Rechenzentrum und asynchroner SnapMirror zur Replikation der Daten in das

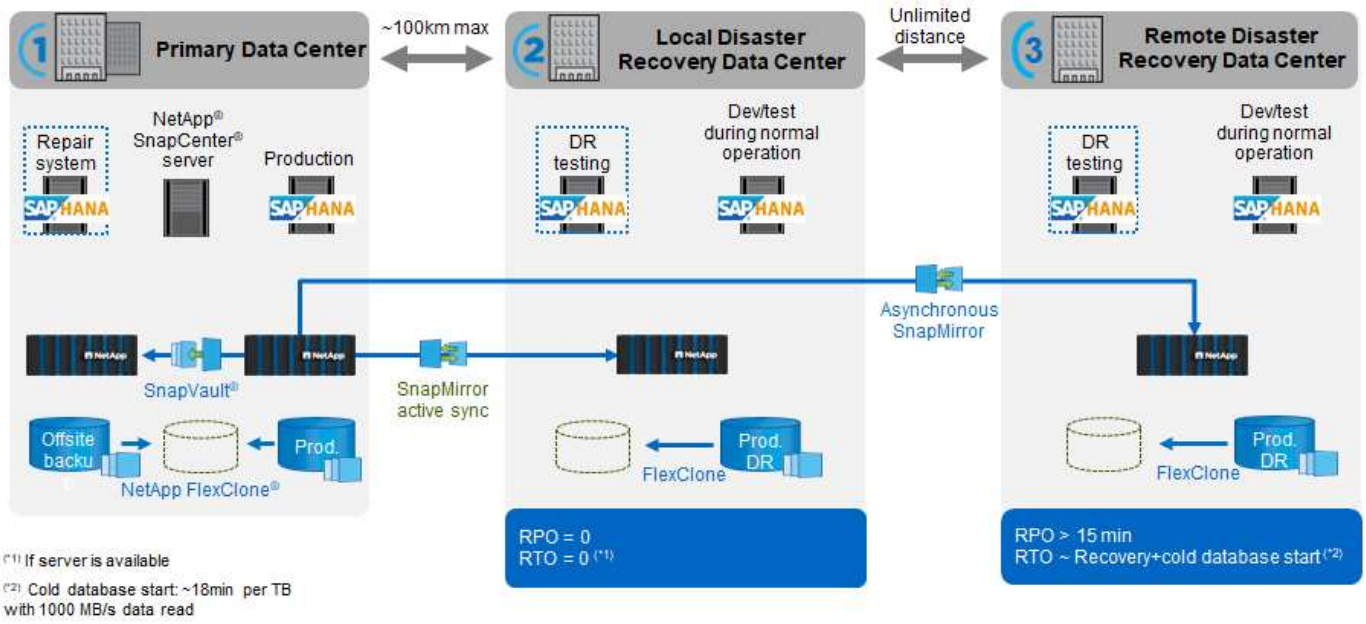
Remote-DR-Rechenzentrum. SnapMirror Active Sync ermöglicht die Weiterführung von Geschäftsdiensten auch bei einem kompletten Standortausfall und unterstützt ein transparentes Failover von Anwendungen mithilfe einer sekundären Kopie (RPO=0 und RTO=0). Für die Auslösung eines Failover mit SnapMirror Active Sync sind keine manuellen Eingriffe oder benutzerdefinierten Skripts erforderlich. Ab ONTAP 9.15.1 unterstützt die SnapMirror Active Sync symmetrische aktiv/aktiv-Funktion. Symmetrische aktiv/aktiv-Konfiguration ermöglicht I/O-Vorgänge für Lese- und Schreibvorgänge von beiden Kopien einer geschützten LUN mit bidirektionaler synchroner Replizierung, sodass beide LUN-Kopien lokal für I/O-Vorgänge sorgen können.

Weitere Details finden Sie unter "Übersicht über die aktive SnapMirror-Synchronisierung in ONTAP" ..

Die RTO für die asynchrone SnapMirror-Replikation hängt in erster Linie von der Zeit ab, die zum Starten der HANA-Datenbank am DR-Standort und zum Laden der Daten in den Speicher benötigt wird. Mit der Annahme, dass die Daten mit einem Durchsatz von 1000 MBit/s gelesen werden, dass das Laden von 1 TB Daten ungefähr 18 Minuten dauert.

Die Server an den DR-Standorten können im normalen Betrieb als Entwicklungs- und Testsysteme genutzt werden. Bei einem Ausfall müssten die Entwicklungs- und Testsysteme heruntergefahren und als DR-Produktionsserver gestartet werden.

Beide Replizierungsmethoden ermöglichen die Durchführung von DR-Workflow-Tests ohne Auswirkungen auf RPO und RTO. FlexClone Volumes werden auf dem Storage erstellt und an die DR-Testserver angeschlossen.



Storage-Dimensionierung

Der folgende Abschnitt bietet einen Überblick über die Performance- und Kapazitätsüberlegungen, die für die Dimensionierung eines Storage-Systems für SAP HANA erforderlich sind.

Wenden Sie sich an Ihren Vertriebsmitarbeiter von NetApp oder einen NetApp Partner, um den Prozess der Storage-Größenbemessung zu unterstützen und Ihnen beim Aufbau einer optimal dimensionierten Storage-Umgebung zu helfen.

Überlegungen zur Performance

SAP hat einen statischen Satz von Storage Key Performance-Indikatoren definiert. Diese KPIs sind für alle produktiven SAP HANA-Umgebungen gültig, unabhängig von der Speichergröße der Datenbank-Hosts und der Anwendungen, die die SAP HANA-Datenbank nutzen. Diese KPIs gelten für Single-Host-, mehrere Hosts-, Business Suite on HANA-, Business Warehouse on HANA-, S/4HANA- und BW/4HANA-Umgebungen. Daher hängt der aktuelle Ansatz zur Performance-Dimensionierung nur von der Anzahl aktiver SAP HANA-Hosts ab, die an das Storage-System angeschlossen sind.

> Storage-Performance-KPIs sind nur für SAP HANA Produktionssysteme erforderlich, können aber in allen HANA-Systemen implementiert werden.

SAP liefert ein Performance-Testtool, das zur Validierung der Storage-Systemperformance der am Storage angeschlossenen aktiven SAP HANA Hosts verwendet werden muss.

NetApp hat die maximale Anzahl an SAP HANA Hosts getestet und vordefiniert, die an ein bestimmtes Storage-Modell angeschlossen werden können, während gleichzeitig die erforderlichen Storage-KPIs von SAP für produktionsbasierte SAP HANA Systeme erfüllt werden.

Mit dem SAP Performance-Testtool wurde die maximale Anzahl an SAP HANA Hosts ermittelt, die in einem Platten-Shelf ausgeführt werden können und die Mindestanzahl der pro SAP HANA Host benötigten SSDs erforderlich ist. Dieser Test berücksichtigt nicht die tatsächlichen Storage-Kapazitätsanforderungen der Hosts. Außerdem müssen die Kapazitätsanforderungen berechnet werden, um die tatsächlich benötigte Storage-Konfiguration zu bestimmen.

NS224 NVMe-Shelf

Eine NVMe-SSD (Daten) unterstützt bis zu 2/5 SAP HANA-Hosts, je nachdem, welche NVMe-Festplatte verwendet wird.

> Durch das Hinzufügen weiterer Platten-Shelves wird nicht die maximale Anzahl von SAP HANA-Hosts erhöht, die ein Storage-Controller unterstützen kann.

Heterogenen Workloads

SAP HANA und andere Applikations-Workloads werden auf demselben Storage Controller oder im selben Storage-Aggregat unterstützt. Es ist jedoch eine NetApp Best Practice, SAP HANA-Workloads von allen anderen Applikations-Workloads zu trennen.

SAP HANA-Workloads und andere Applikations-Workloads können entweder auf demselben Storage-Controller oder demselben Aggregat implementiert werden. Falls ja, müssen Sie sicherstellen, dass in der Umgebung mit heterogenen Workloads für SAP HANA eine ausreichende Performance verfügbar ist. NetApp empfiehlt außerdem, Parameter für Quality of Service (QoS) zu verwenden, um die Auswirkungen anderer Applikationen auf SAP HANA Applikationen zu regulieren und den Durchsatz für SAP HANA Applikationen zu garantieren.

Das SAP HCMT-Testtool muss verwendet werden, um zu prüfen, ob zusätzliche SAP HANA Hosts auf einem vorhandenen Storage Controller ausgeführt werden können, der bereits für andere Workloads verwendet wird. SAP Applikations-Server können wie die SAP HANA Datenbanken sicher auf demselben Storage Controller und/oder Aggregat platziert werden.

Überlegungen zur Kapazität

Eine detaillierte Beschreibung der Kapazitätsanforderungen für SAP HANA ist im "SAP-Hinweis 1900823"

Whitepaper:

> Das Kapazitätsdimensionieren der gesamten SAP Landschaft mit mehreren SAP HANA Systemen muss mithilfe von SAP HANA Storage-Größenanpassungs-Tools von NetApp ermittelt werden. Wenden Sie sich an NetApp oder Ihren Ansprechpartner bei NetApp Partnern, um den Prozess der Storage-Größenbemessung für eine ausreichend dimensionierte Storage-Umgebung zu validieren.

Konfiguration des Performance-Testtool

Ab SAP HANA 1.0 SPS10 führte SAP Parameter ein, um das I/O-Verhalten anzupassen und die Datenbank für das verwendete Datei- und Speichersystem zu optimieren. Diese Parameter müssen auch für das Performance-Test-Tool von SAP eingestellt werden, wenn die Storage-Performance mit dem SAP-Testtool getestet wird.

NetApp führte Performance-Tests durch, um die optimalen Werte zu ermitteln. In der folgenden Tabelle sind die Parameter aufgeführt, die in der Konfigurationsdatei des SAP-Testwerkzeugs festgelegt werden müssen.

Parameter	Wert
max_parallel_io_Requests	128
Async_read_Submit	Ein
Async_write_submit_Active	Ein
Async_Write_Submit_Blocks	Alle

Weitere Informationen zur Konfiguration von SAP-Testtool finden Sie unter "SAP-Hinweis 1943937" Für HWCCT (SAP HANA 1.0) und "SAP-Hinweis 2493172" FÜR HCMT/HCOT (SAP HANA 2.0).

Das folgende Beispiel zeigt, wie Variablen für den HCMT/HCOT-Ausführungsplan festgelegt werden können.

```
…
{
          "Comment": "Log Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "LogAsyncReadSubmit",
          "Value": "on",
          "Request": "false"
      },
      {
          "Comment": "Data Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "DataAsyncReadSubmit",
          "Value": "on",
          "Request": "false"
      },
      {
          "Comment": "Log Volume: Controls whether write requests can be
submitted asynchronously",
```

```
         "Name": "LogAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "DataAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "LogAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "DataAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "LogExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "DataExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      }, …
```

Diese Variablen müssen für die Testkonfiguration verwendet werden. Dies ist in der Regel bei den vordefinierten Testsuiten der Fall, die SAP mit dem HCMT/HCOT-Tool liefert. Das folgende Beispiel für einen 4k-Protokollschreibtest stammt aus einer Testsuite.

```
…
      {
         "ID": "D664D001-933D-41DE-A904F304AEB67906",
         "Note": "File System Write Test",
         "ExecutionVariants": [
            {
               "ScaleOut": {
                  "Port": "${RemotePort}",
                  "Hosts": "${Hosts}",
                  "ConcurrentExecution": "${FSConcurrentExecution}"
               },
               "RepeatCount": "${TestRepeatCount}",
               "Description": "4K Block, Log Volume 5GB, Overwrite",
               "Hint": "Log",
               "InputVector": {
                  "BlockSize": 4096,
                  "DirectoryName": "${LogVolume}",
                  "FileOverwrite": true,
                  "FileSize": 5368709120,
                  "RandomAccess": false,
                  "RandomData": true,
                  "AsyncReadSubmit": "${LogAsyncReadSubmit}",
                  "AsyncWriteSubmitActive":
"${LogAsyncWriteSubmitActive}",
                  "AsyncWriteSubmitBlocks":
"${LogAsyncWriteSubmitBlocks}",
                  "ExtMaxParallelIoRequests":
"${LogExtMaxParallelIoRequests}",
                  "ExtMaxSubmitBatchSize": "${LogExtMaxSubmitBatchSize}",
                  "ExtMinSubmitBatchSize": "${LogExtMinSubmitBatchSize}",
                  "ExtNumCompletionQueues":
"${LogExtNumCompletionQueues}",
                  "ExtNumSubmitQueues": "${LogExtNumSubmitQueues}",
                  "ExtSizeKernelIoQueue": "${ExtSizeKernelIoQueue}"
               }
            },
…
```

Übersicht über den Prozess zur Storage-Größenbemessung

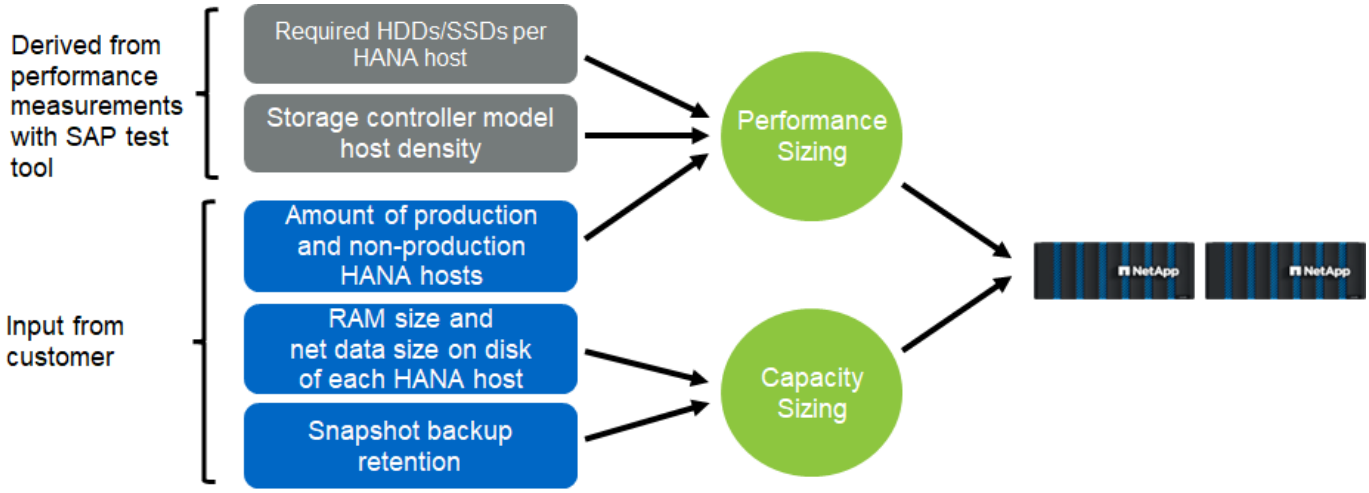
Die Anzahl der Festplatten pro HANA Host und die Host-Dichte für jedes Storage-Modell von SAP HANA wurden mithilfe des Test-Tools ermittelt.

Der Dimensionierungsprozess erfordert Einzelheiten, z. B. die Anzahl der SAP HANA-Hosts in der Produktion und für die Produktion nichtproduktive Umgebung, die RAM-Größe jedes Hosts und die Backup-Aufbewahrung der Storage-basierten Snapshot Kopien. Die Anzahl der SAP HANA-Hosts bestimmt den Storage Controller

und die Anzahl der benötigten Festplatten.

Die Größe des RAM, die Netto-Datengröße auf der Festplatte jedes SAP HANA-Hosts und der Aufbewahrungszeitraum für das Snapshot-Backup werden als Inputs bei der Kapazitätsdimensionierung verwendet.

Die folgende Abbildung fasst den Dimensionierungsprozess zusammen.



Einrichtung und Konfiguration der Infrastruktur

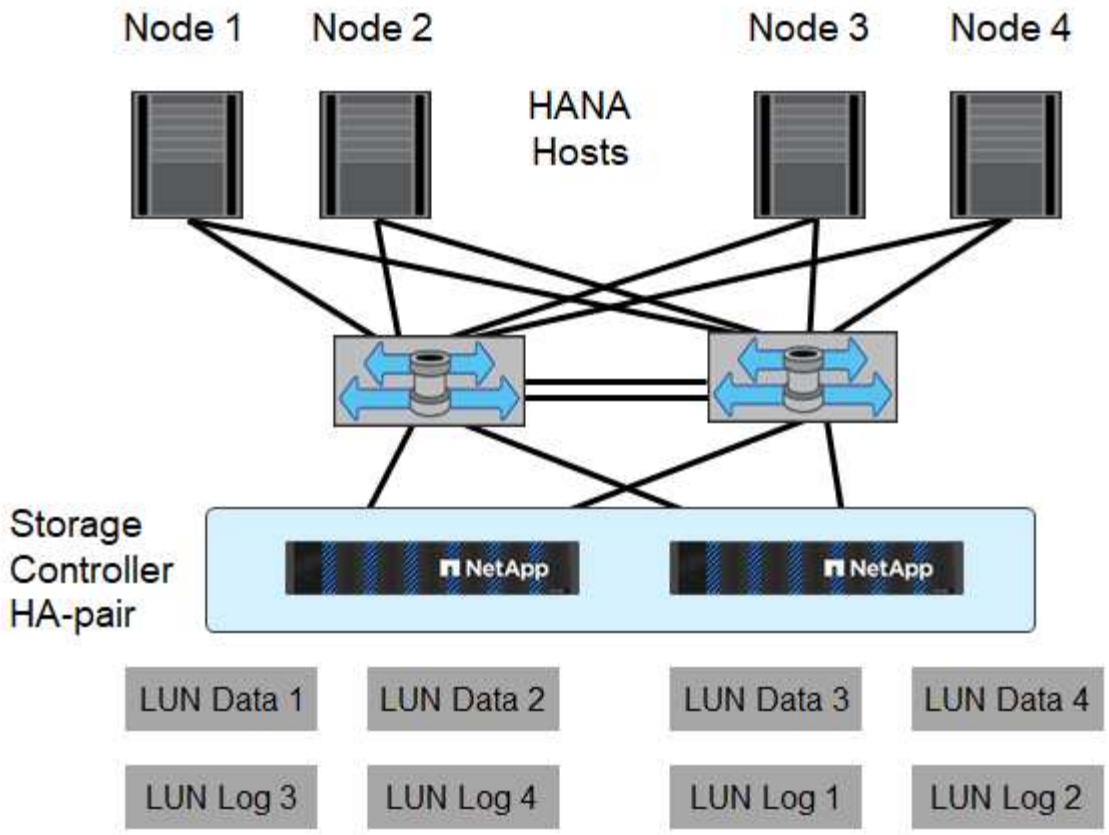
In den folgenden Abschnitten finden Sie Richtlinien zur Einrichtung und Konfiguration der SAP HANA-Infrastruktur sowie alle Schritte zur Einrichtung eines SAP HANA-Systems. In diesen Abschnitten werden die folgenden Beispielkonfigurationen verwendet:

- HANA-System mit SID=FC5
  - SAP HANA mit einem oder mehreren Hosts

EINRICHTUNG VON SAN Fabric

Jeder SAP HANA-Server muss über eine redundante FCP-SAN-Verbindung mit einer Bandbreite von mindestens 8 Gbit/s. Für jeden an einen Storage Controller angeschlossenen SAP HANA-Host muss am Storage Controller mindestens eine Bandbreite von 8 GB/s konfiguriert sein.

Die folgende Abbildung zeigt ein Beispiel mit vier SAP HANA-Hosts, die mit zwei Storage-Controllern verbunden sind. Jeder SAP HANA-Host verfügt über zwei FCP-Ports, die mit der redundanten Fabric verbunden sind. Auf der Storage-Ebene sind vier FCP-Ports so konfiguriert, dass sie den erforderlichen Durchsatz für jeden SAP HANA Host liefern.



Zusätzlich zum Zoning auf der Switch-Ebene müssen Sie jede LUN auf dem Storage-System den Hosts zuordnen, die mit dieser LUN verbunden sind. Einfachheit beim Zoning auf dem Switch; das heißt, Festlegung eines Zoneneinteils, in dem alle Host-HBAs alle Controller-HBAs sehen können.

Zeitsynchronisierung

Sie müssen die Zeit zwischen den Storage-Controllern und den SAP HANA Datenbank-Hosts synchronisieren. Legen Sie dazu denselben Zeitserver für alle Storage Controller und alle SAP HANA-Hosts fest.

Einrichtung von Storage Controllern

In diesem Abschnitt wird die Konfiguration des NetApp Storage-Systems beschrieben. Sie müssen die primäre Installation und Einrichtung gemäß den entsprechenden Data ONTAP Setup- und Konfigurationsleitfäden abschließen.

Storage-Effizienz

In einer SSD-Konfiguration werden Inline-Deduplizierung, Inline-Deduplizierung, Inline-Komprimierung und Inline-Data-Compaction unterstützt.

Quality of Service

QoS kann verwendet werden, um den Storage-Durchsatz für bestimmte SAP HANA Systeme oder nicht-SAP Applikationen auf einem Shared Controller zu begrenzen.

Produktion und Entwicklung/Test

Ein Anwendungsfall wäre, den Durchsatz von Entwicklungs- und Testsystemen zu begrenzen, damit sie bei einem gemischten Setup keinen Einfluss auf die Produktionssysteme haben. Während des Dimensionierungsprozesses sollten Sie die Performance-Anforderungen eines nicht für die Produktion verwendeten Systems ermitteln. Entwicklungs- und Testsysteme können mit niedrigeren Leistungswerten dimensioniert werden, typischerweise im Bereich von 20 % bis 50 % eines von SAP definierten Produktionssystems-KPI. Ein großer I/O-Schreibvorgang wirkt sich am stärksten auf die Performance des Storage-Systems aus. Daher sollte die QoS-Durchsatzbegrenzung auf einen Prozentsatz der entsprechenden KPI-Werte für die SAP HANA-Speicherleistung in den Daten- und Protokoll-Volumes gesetzt werden.

Shared-Umgebungen

Ein weiterer Anwendungsfall ist die Einschränkung des Durchsatzes bei umfangreichen Schreib-Workloads, insbesondere um zu vermeiden, dass diese Workloads Auswirkungen auf andere latenzempfindliche Schreib-Workloads haben. In solchen Umgebungen empfiehlt es sich, eine QoS-Gruppenrichtlinie ohne gemeinsam genutzten Durchsatz auf jede LUN innerhalb jeder SVM (Storage Virtual Machine) anzuwenden, um den maximalen Durchsatz jedes einzelnen Storage-Objekts auf den angegebenen Wert zu beschränken. So besteht weniger Gefahr, dass ein einzelner Workload andere Workloads negativ beeinflussen kann.

Dazu muss über die CLI des ONTAP-Clusters für jede SVM eine Gruppenrichtlinie erstellt werden:

```
qos policy-group create -policy-group <policy-name> -vserver <vserver
name> -max-throughput 1000MB/s -is-shared false
```

Und auf jede LUN in der SVM angewendet. Nachfolgend sehen Sie ein Beispiel, um die Richtliniengruppe auf alle vorhandenen LUNs innerhalb einer SVM anzuwenden:

```
lun modify -vserver <vserver name>  -path * -qos-policy-group  <policy-
name>
```

Dies muss für jede SVM geschehen. Der Name der QoS-Polizeigruppe für jede SVM muss unterschiedlich sein. Für neue LUNs kann die Richtlinie direkt angewendet werden:

```
lun create -vserver <vserver_name> -path  /vol/<volume_name>/<lun_name>
-size <size> -ostype <e.g. linux>  -qos-policy-group <policy-name>
```

Es wird empfohlen, 1000 MB/s als maximalen Durchsatz für eine bestimmte LUN zu verwenden. Wenn eine Applikation einen höheren Durchsatz erfordert, müssen mehrere LUNs mit LUN-Striping verwendet werden, um die erforderliche Bandbreite bereitzustellen. Dieser Leitfaden enthält ein Beispiel für SAP HANA auf Basis von Linux LVM in Abschnitt "Host-Setup".

Das Limit gilt auch für Lesevorgänge. Daher genügend LUNs verwenden, um die erforderlichen SLAs für die Startzeit der SAP HANA-Datenbank und für Backups zu erfüllen.

Speicher konfigurieren

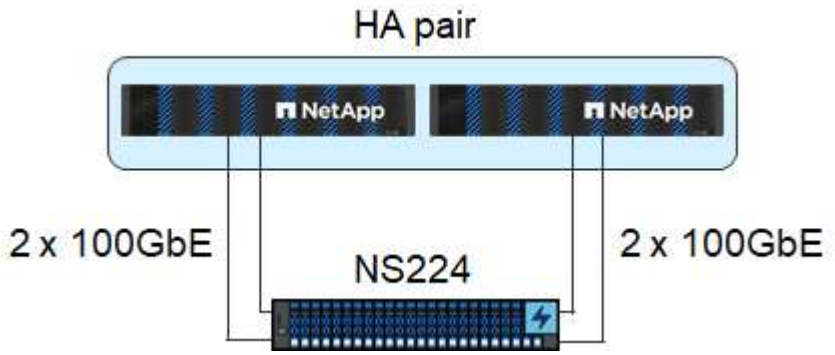
In der folgenden Übersicht sind die erforderlichen Schritte zur Storage-Konfiguration zusammengefasst. Jeder Schritt wird in den nachfolgenden Abschnitten näher beschrieben. In diesem Abschnitt wird die Storage-

Hardware eingerichtet und die ONTAP Software bereits installiert. Außerdem muss die Verbindung der Storage FCP-Ports zur SAN-Fabric bereits vorhanden sein.

1. Überprüfen Sie die richtige Festplatten-Shelf-Konfiguration, wie in beschriebenNVMe-basierte Festplattenregale.
2. Erstellen Sie Initiatorgruppen (igroups) mit weltweiten Namen (WWNs) von HANA-Servern, wie im Abschnitt xref:./bp/saphana-asa-fc-storage-controller-setup.html#initiator-groups beschrieben. Initiatorgruppen .
3. Erstellen Sie LUNs und ordnen Sie sie den im Abschnitt beschriebenen Servern zu "LUN-Konfiguration für SAP HANA Single-Host-Systeme" Und "LUN-Konfiguration für SAP HANA-Mehrhostsysteme"

NVMe-basierte Festplattenregale

Jedes NS224 NVMe-Festplatten-Shelf ist, wie in der folgenden Abbildung dargestellt, mit zwei 100-GbE-Ports pro Controller verbunden. Die Platten werden automatisch auf die beiden Controller des HA-Paares verteilt.



Initiatorgruppen

Eine Initiatorgruppe kann für jeden Server oder für eine Gruppe von Servern konfiguriert werden, die Zugriff auf eine LUN benötigen. Für die iGroup Konfiguration sind die weltweiten Port-Namen (WWPNs) der Server erforderlich.

Verwenden der `sanlun` Führen Sie den folgenden Befehl aus, um die WWPNs jedes SAP HANA-Hosts abzurufen:

```
sapcc-hana-tst:~ # sanlun fcp show adapter
/sbin/udevadm
/sbin/udevadm

host0 ..... WWPN:2100000e1e163700
host1 ..... WWPN:2100000e1e163701
```

Das `sanlun` Tool ist Teil der NetApp Host Utilities und muss auf jedem SAP HANA-Host installiert sein. Weitere Details finden Sie in Abschnitt "Hosteinrichtung:"

Einzelner Host

Einzelner Host

Dieser Abschnitt beschreibt die Konfiguration des NetApp-Speichersystems speziell für SAP HANA-Einzelhostsysteme

Erstellen von LUNs und Zuordnen von LUNs zu Initiatorgruppen

Mit NetApp ONTAP System Manager können Sie Speichervolumes und LUNs erstellen und sie den igroups der Server und der ONTAP CLI zuordnen.

Erstellen von LUNs und Zuordnen von LUNs zu Initiatorgruppen mithilfe der CLI

Dieser Abschnitt zeigt eine Beispielkonfiguration unter Verwendung der Befehlszeile mit ONTAP 9 für ein SAP HANA-Einzelhostsystem mit SID FC5 unter Verwendung von LVM und zwei LUNs pro LVM-Volume-Gruppe:

1. Erstellen Sie alle LUNs.

```
lun create -path  FC5_data_mnt00001_1 -size 1t -ostype linux  -class
regular
lun create -path FC5_data_mnt00001_2 -size 1t -ostype linux  -class
regular
lun create -path FC5_log_mnt00001_1 -size 260g -ostype linux  -class
regular
lun create -path FC5_log_mnt00001_2 -size 260g -ostype linux  -class
regular
lun create -path FC5_shared -size 260g -ostype linux  -class regular
```

2. Erstellen Sie die Initiatorgruppe für alle Server, die zu System FC5 gehören.

```
lun igroup create -igroup HANA-FC5 -protocol fcp -ostype linux
-initiator 10000090fadcc5fa,10000090fadcc5fb -vserver svm1
```

3. Ordnen Sie alle LUNs der erstellten Initiatorgruppe zu.

```
lun map -path FC5_data_mnt00001_1 -igroup HANA-FC5
lun map -path FC5_data_mnt00001_2 -igroup HANA-FC5
lun map -path FC5_log_mnt00001_1 -igroup HANA-FC5
lun map -path FC5_log_mnt00001_2 -igroup HANA-FC5
lun map -path FC5_shared -igroup HANA-FC5
```

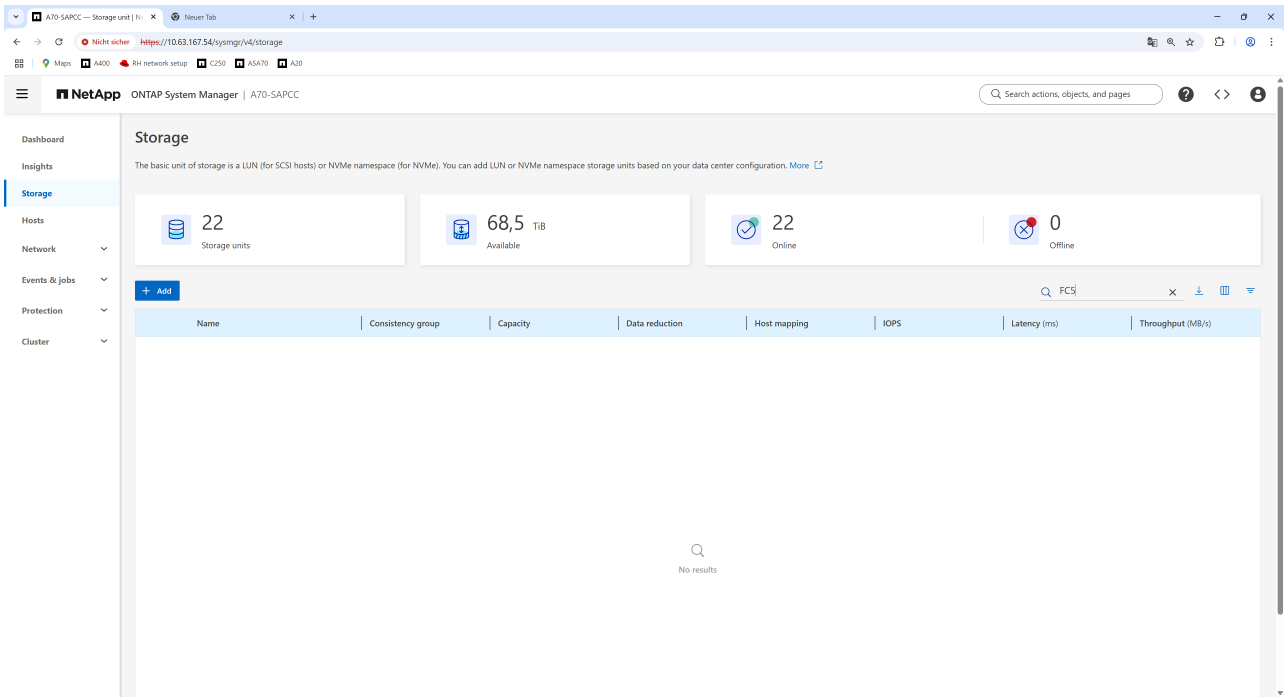
Erstellen von LUNs und Zuordnen von LUNs zu Initiatorgruppen mithilfe der GUI

Dieser Abschnitt zeigt eine Beispielkonfiguration mit `ONTAP System Manager` für ein SAP HANA-Einzelhostsystem mit SID FC5 unter Verwendung von LVM und zwei LUNs pro LVM-Volume-Gruppe:

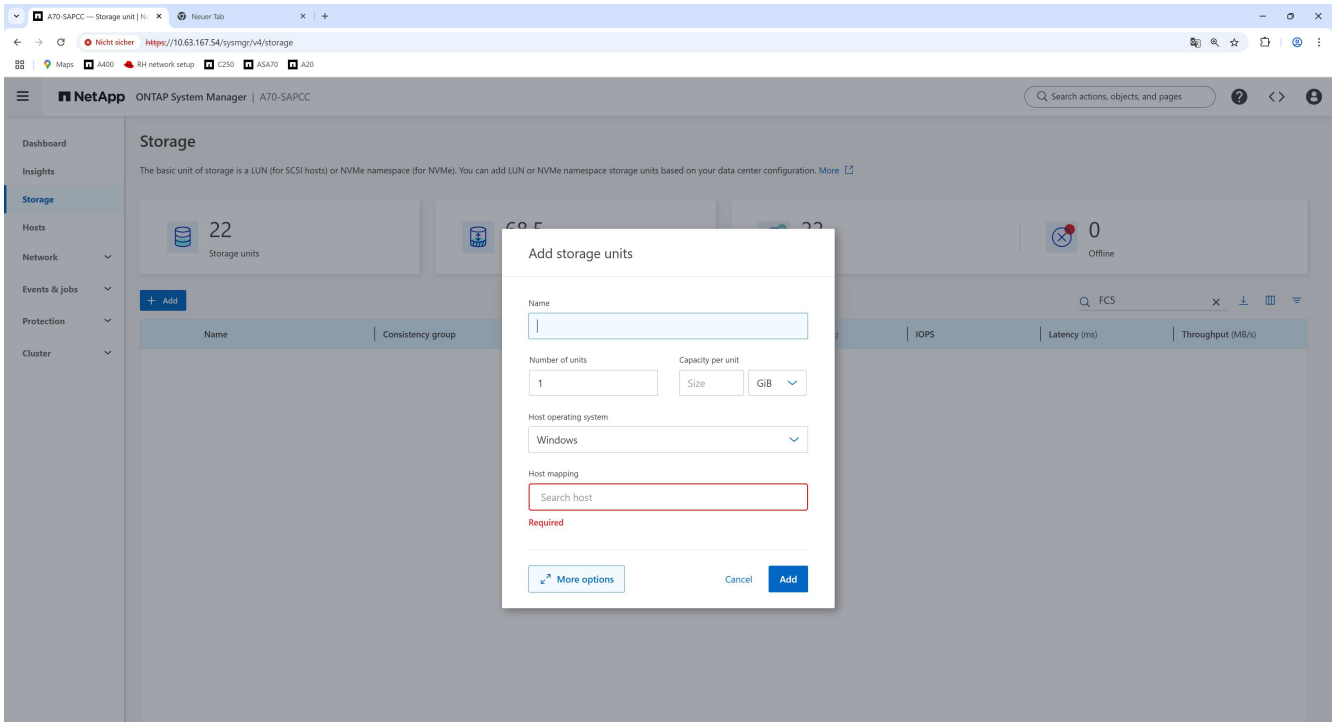
1. Melden Sie sich an bei `ONTAP System Manager` Ihres ONTAP Clusters und wählen Sie `Storage` aus

dem linken Menü.

a. Drücken `Add`



2. Wählen `More options`



3. Geben Sie die erforderlichen Informationen ein:

a. der Name der Daten-LUNs, zB.`FC5_data_mnt00001`

b. die Anzahl der mit LVM zu kombinierenden LUNs, zB 2

c. die Größe jeder LUN, zB 1000 GB

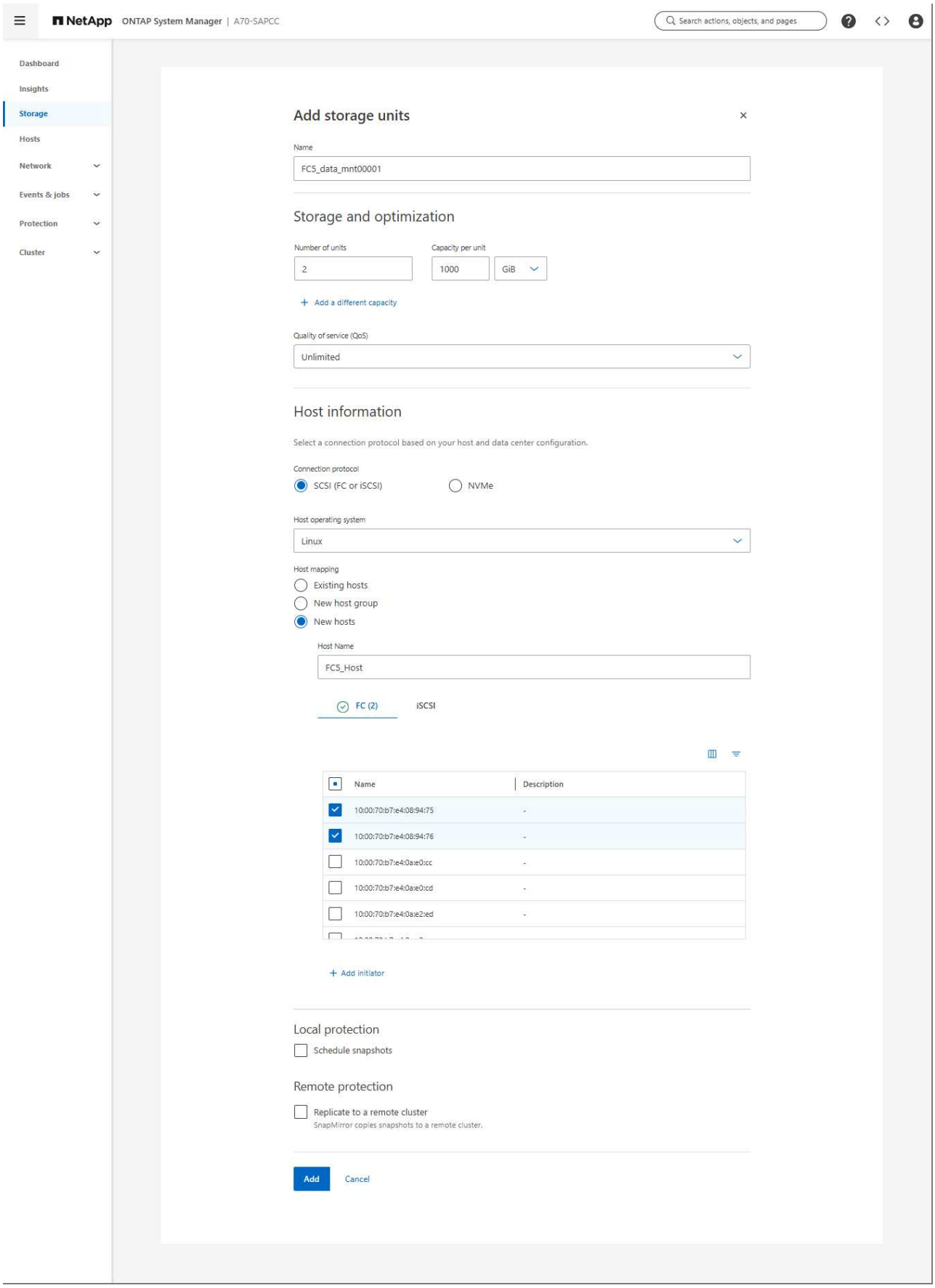
d. wählen `SCSI (FC or iSCSI)`

e. wählen `Linux` als `Host Operating system`

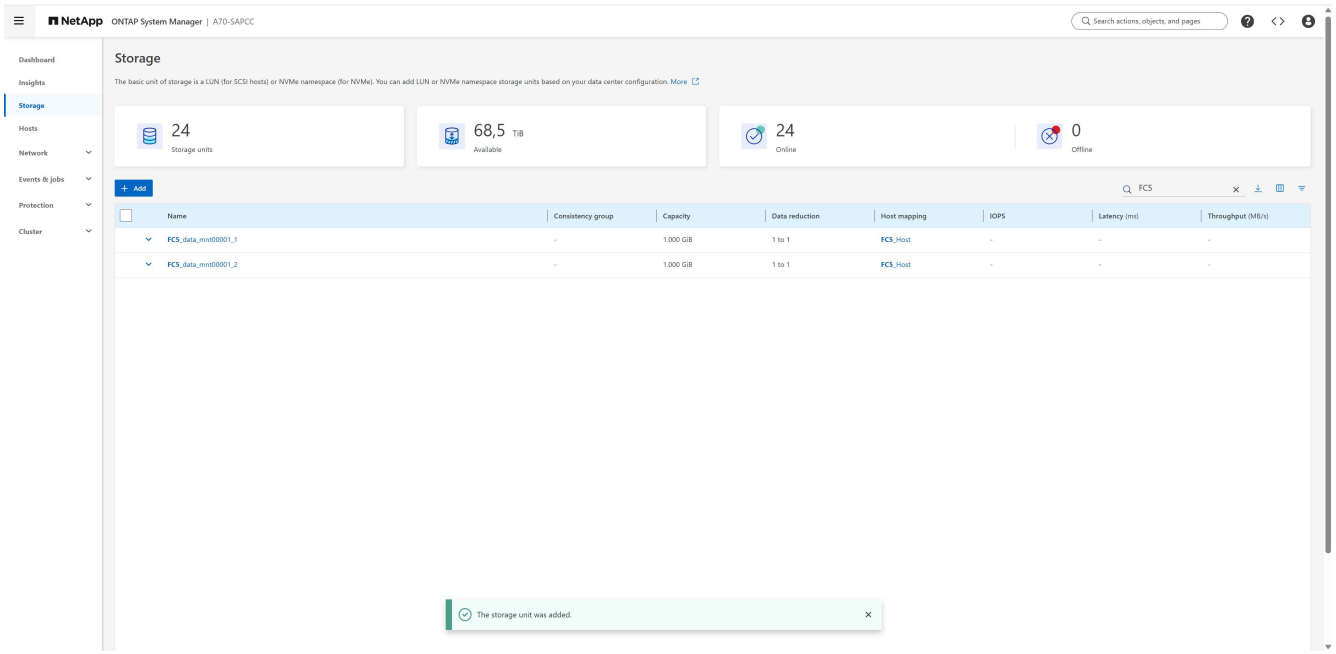
f. wählen `New host` für die `Host mapping` Option, geben Sie einen Namen an, zB `FC5_host` , wählen oder fügen Sie die gewünschten Initiatoren hinzu

g. Halten `Schedule snapshots` deaktiviert

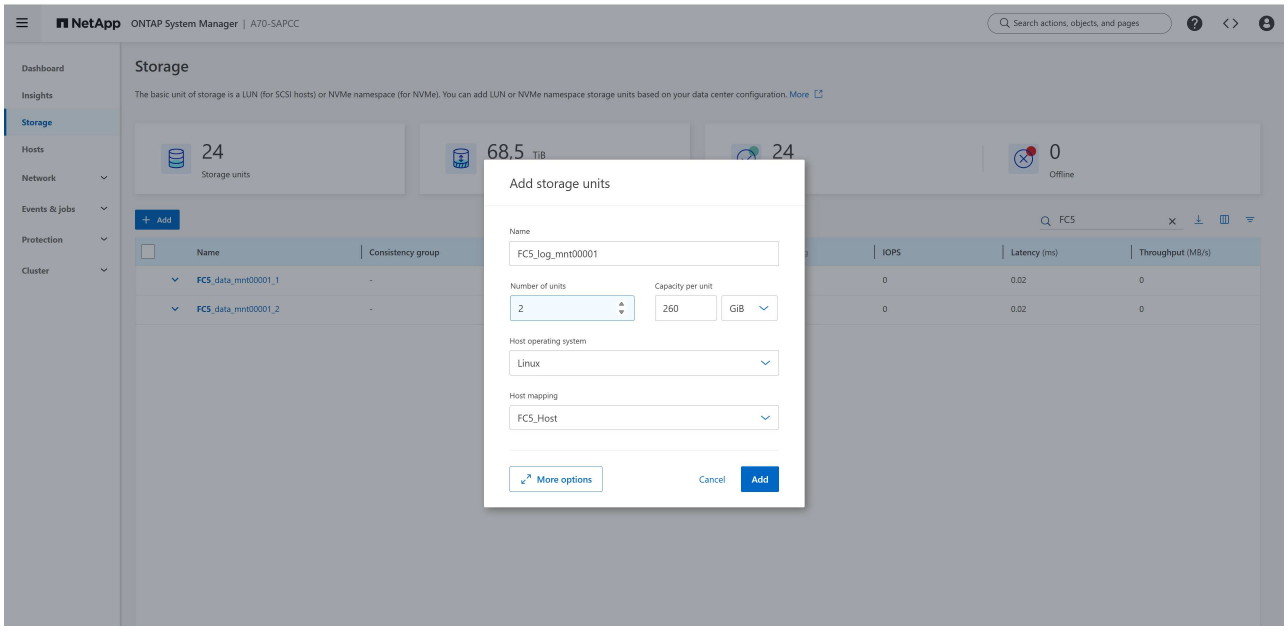
h. drücken `Add`



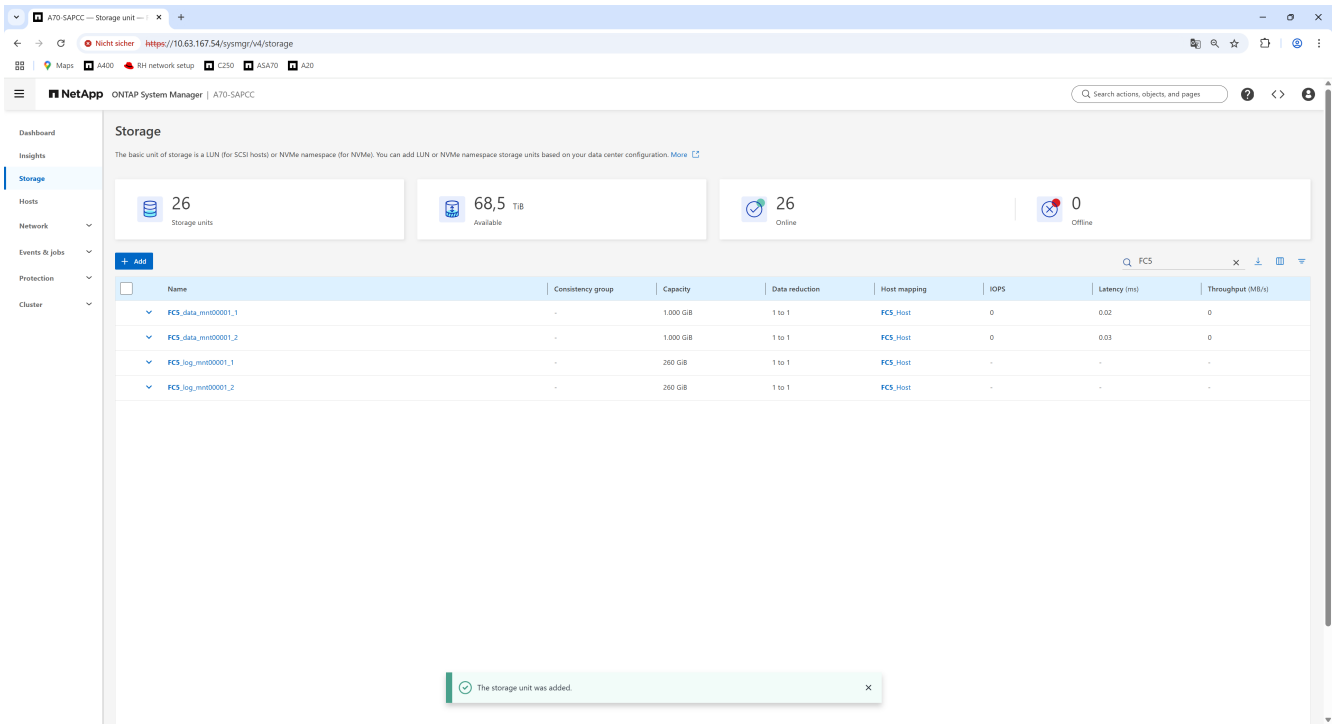
4. Nach erfolgreicher Erstellung der Daten-LUNs erstellen Sie die Log-LUNs durch Drücken von `Add`



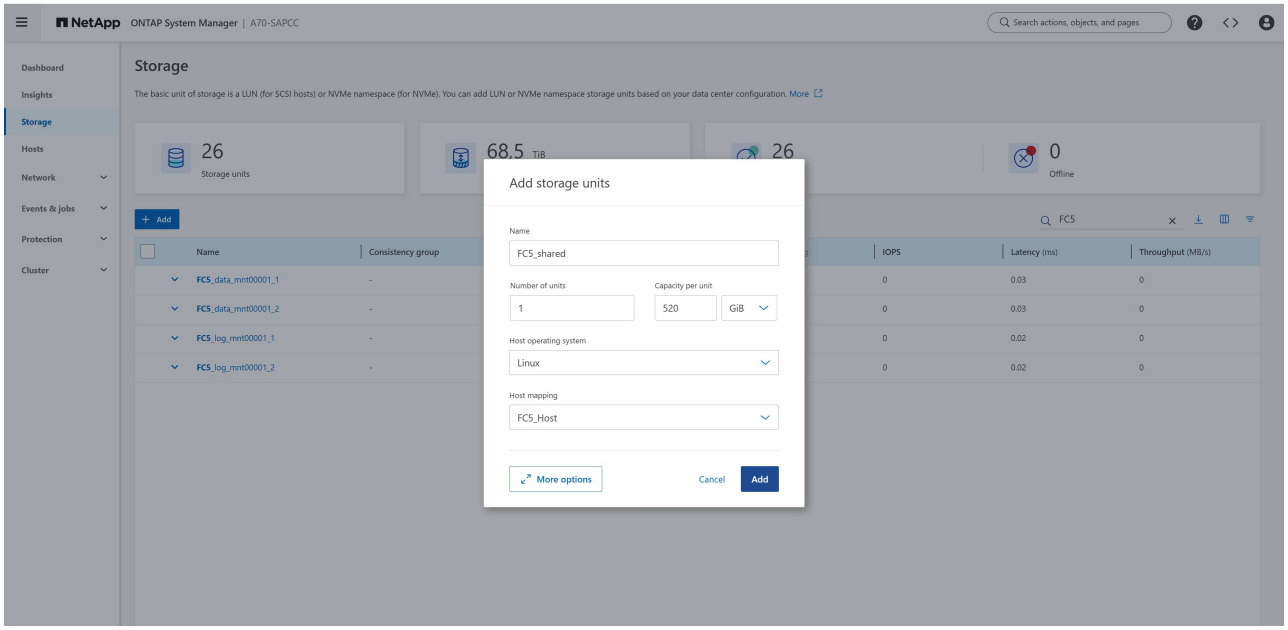
5. Geben Sie die erforderlichen Informationen ein:
   a. der Name der Log-LUNs, zB `FC5_log_mnt00001`
   b. die Anzahl der mit LVM zu kombinierenden LUNs, zB 2
   c. die Größe jeder LUN, zB 260 GB
   d. wählen `Linux` als `Host Operating system`
   e. Wählen Sie die zuvor erstellte Zuordnung `FC5_host` für die `Host mapping` Option
   f. drücken `Add`



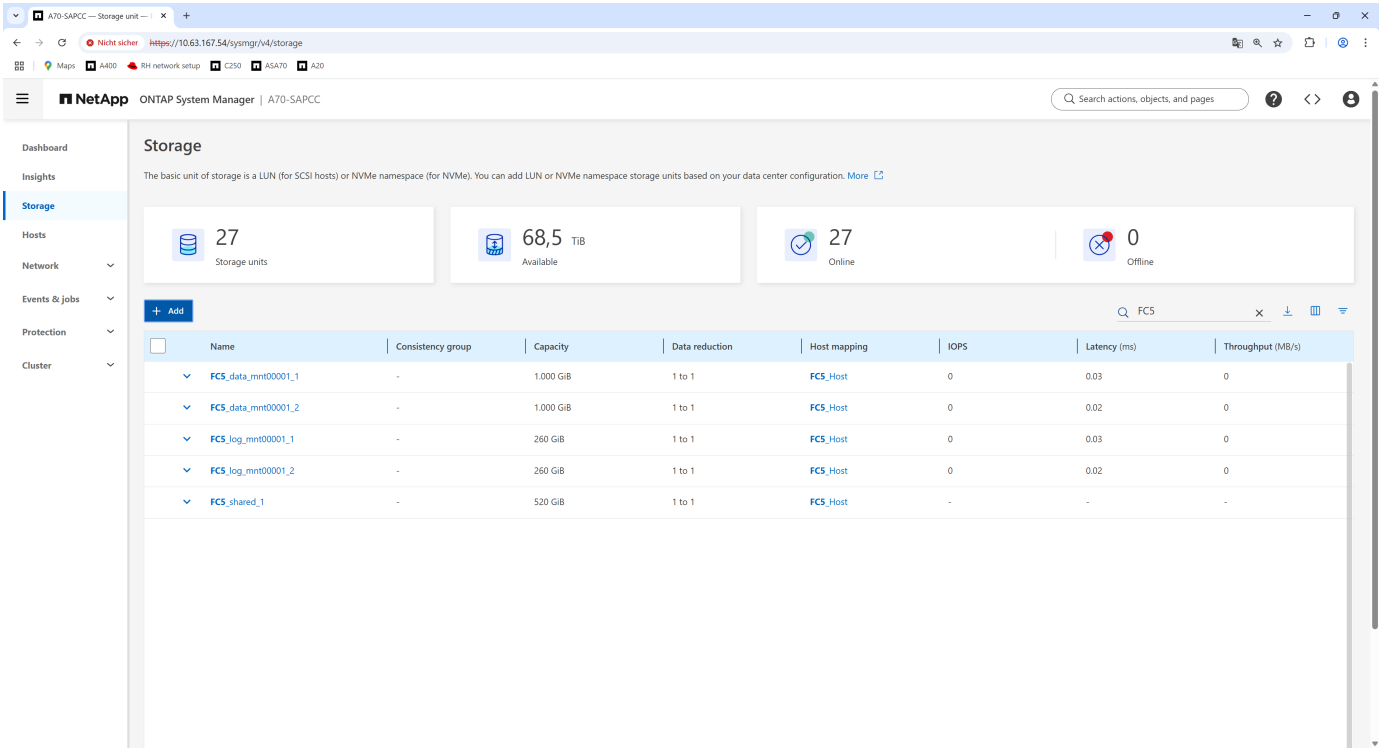
6. Nach erfolgreicher Erstellung der Log-LUNs erstellen Sie die freigegebene LUN durch Drücken von `Add`



7. Geben Sie die erforderlichen Informationen ein:
   a. der Name der freigegebenen LUN, zB.`FC5_shared`
   b. die Anzahl der LUNs, zB 1
   c. die Größe der LUN, zB 520 GB
   d. wählen `Linux` als `Host Operating system`
   e. Wählen Sie die zuvor erstellte Zuordnung `FC5_host` für die `Host mapping` Option
   f. drücken `Add`



Alle erforderlichen LUNs für ein SAP HANA-Einzelhostsystem wurden erstellt.



Mehrere Hosts

Mehrere Hosts

Dieser Abschnitt beschreibt die Konfiguration des NetApp-Speichersystems speziell für SAP HANA-Mehrfachhostsysteme

Erstellen von LUNs und Zuordnen von LUNs zu Initiatorgruppen

Mit NetApp ONTAP System Manager können Sie Speichervolumes und LUNs erstellen und sie den igroups der Server und der ONTAP CLI zuordnen.

Erstellen von LUNs und Zuordnen von LUNs zu Initiatorgruppen mithilfe der CLI

Dieser Abschnitt zeigt eine Beispielkonfiguration mit der Befehlszeile mit ONTAP 9 für ein 2+1 SAP HANA mehrere Hostsysteme mit SID FC5 unter Verwendung von LVM und zwei LUNs pro LVM Volume-Gruppe:

1. Erstellen Sie alle LUNs.

```
lun create -path FC5_data_mnt00001_1 -size 1t -ostype linux  -class
regular
lun create -path FC5_data_mnt00001_2 -size 1t -ostype linux  -class
regular
lun create -path FC5_data_mnt00002_1 -size 1t -ostype linux  -class
regular
lun create -path FC5_data_mnt00002_2 -size 1t -ostype linux  -class
regular
lun create -path FC5_log_mnt00001_1 -size 260g -ostype linux  -class
regular
lun create -path FC5_log_mnt00001_2 -size 260g -ostype linux  -class
regular
lun create -path FC5_log_mnt00002_1 -size 260g -ostype linux  -class
regular
lun create -path FC5_log_mnt00002_2 -size 260g -ostype linux  -class
regular
```

2. Erstellen Sie die Initiatorgruppe für alle Server, die zu System FC5 gehören.

```
lun igroup create -igroup HANA-FC5 -protocol fcp -ostype linux
-initiator
10000090fadcc5fa,10000090fadcc5fb,10000090fadcc5c1,10000090fadcc5c2,1000
0090fadcc5c3,10000090fadcc5c4 -vserver svm1
```

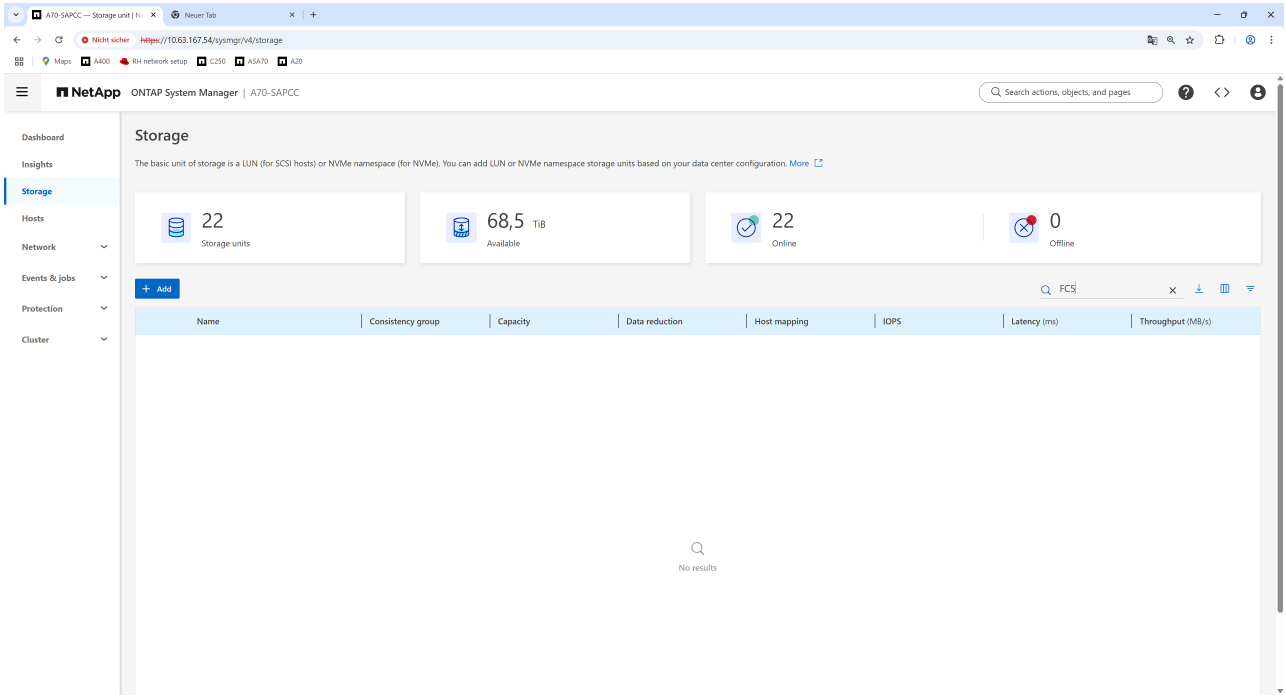
3. Ordnen Sie alle LUNs der erstellten Initiatorgruppe zu.

```
lun map -path FC5_data_mnt00001_1 -igroup HANA-FC5
lun map -path FC5_data_mnt00001_2 -igroup HANA-FC5
lun map -path FC5_data_mnt00002_1 -igroup HANA-FC5
lun map -path FC5_data_mnt00002_2 -igroup HANA-FC5
lun map -path FC5_log_mnt00001_1 -igroup HANA-FC5
lun map -path FC5_log_mnt00001_2 -igroup HANA-FC5
lun map -path FC5_log_mnt00002_1 -igroup HANA-FC5
lun map -path FC5_log_mnt00002_2 -igroup HANA-FC5
```

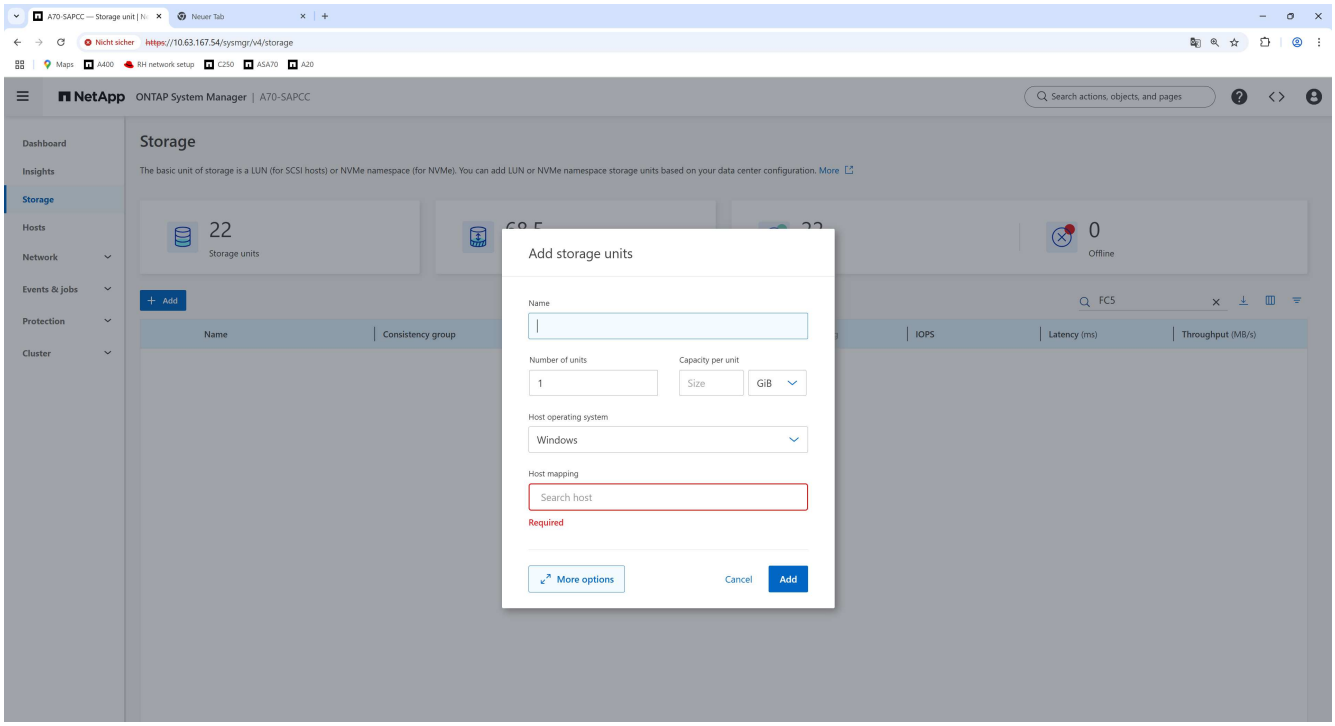
Erstellen von LUNs und Zuordnen von LUNs zu Initiatorgruppen mithilfe der GUI

Dieser Abschnitt zeigt eine Beispielkonfiguration mit `ONTAP System Manager` für ein 2+1 SAP HANA-Mehrhostsystem mit SID FC5 unter Verwendung von LVM und zwei LUNs pro LVM-Volume-Gruppe:

1. Melden Sie sich an bei `ONTAP System Manager` Ihres ONTAP Clusters und wählen Sie `Storage` aus dem linken Menü.
   a. Drücken `Add`



2. Wählen `More options`

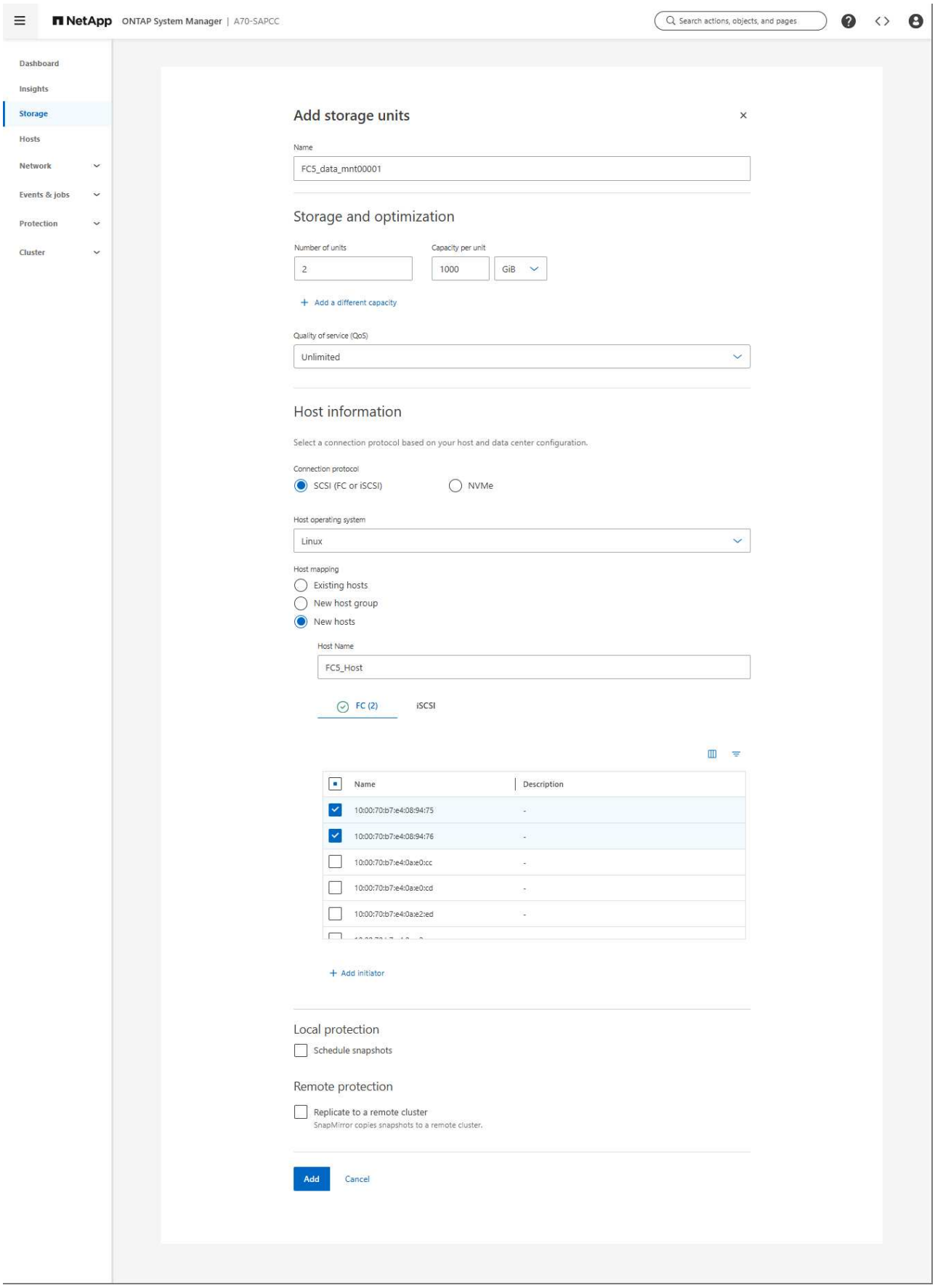


3. Geben Sie die erforderlichen Informationen ein:
   a. Name der Daten-LUNs, zB.`FC5_data_mnt00001`
   b. die Anzahl der mit LVM zu kombinierenden LUNs, zB 2
   c. die Größe jeder LUN, zB 1000 GB
   d. wählen `SCSI (FC or iSCSI)`
   e. wählen `Linux` als `Host Operating system`

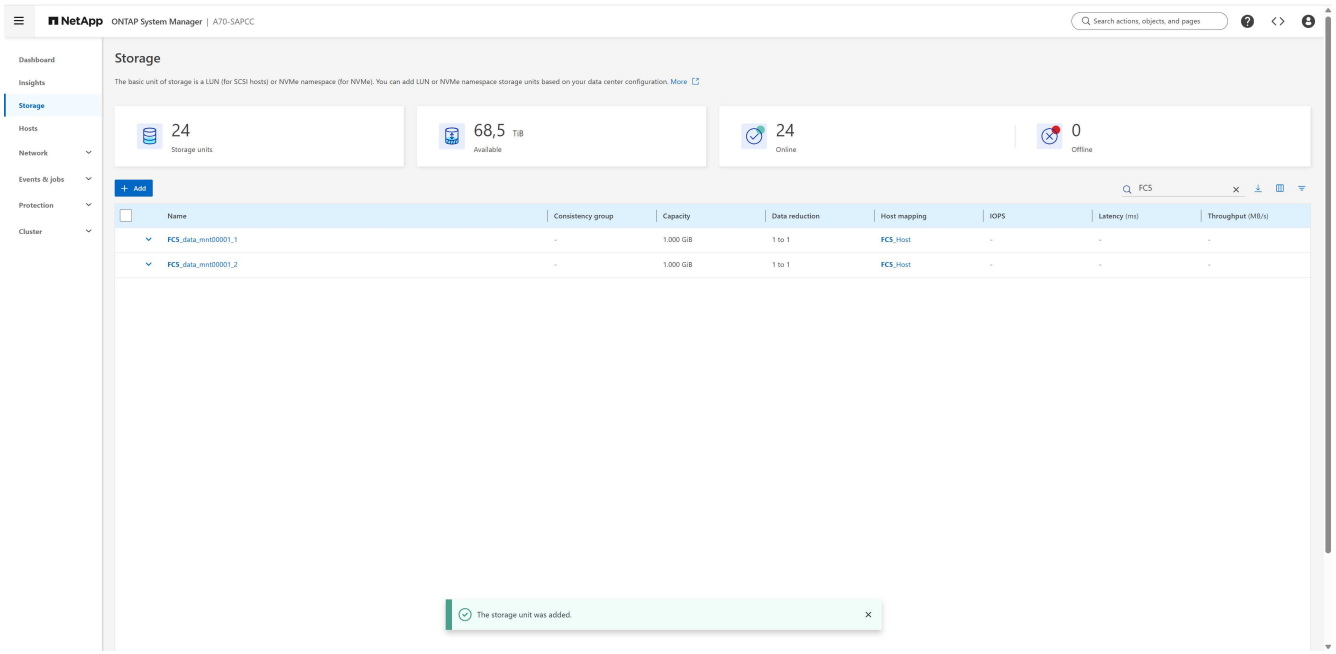
f. wählen `New host` für die `Host mapping` Option, geben Sie einen Namen an, zB `FC5_host` , wählen oder fügen Sie die gewünschten Initiatoren hinzu

g. Halten `Schedule snapshots` deaktiviert

h. drücken `Add`



4. Erstellen Sie die Daten-LUNs für den nächsten Worker-Host, indem Sie `Add`



5. Geben Sie die erforderlichen Informationen ein:

   a. der Name der zusätzlichen Daten-LUNs, zB `FC5_data_mnt00002`

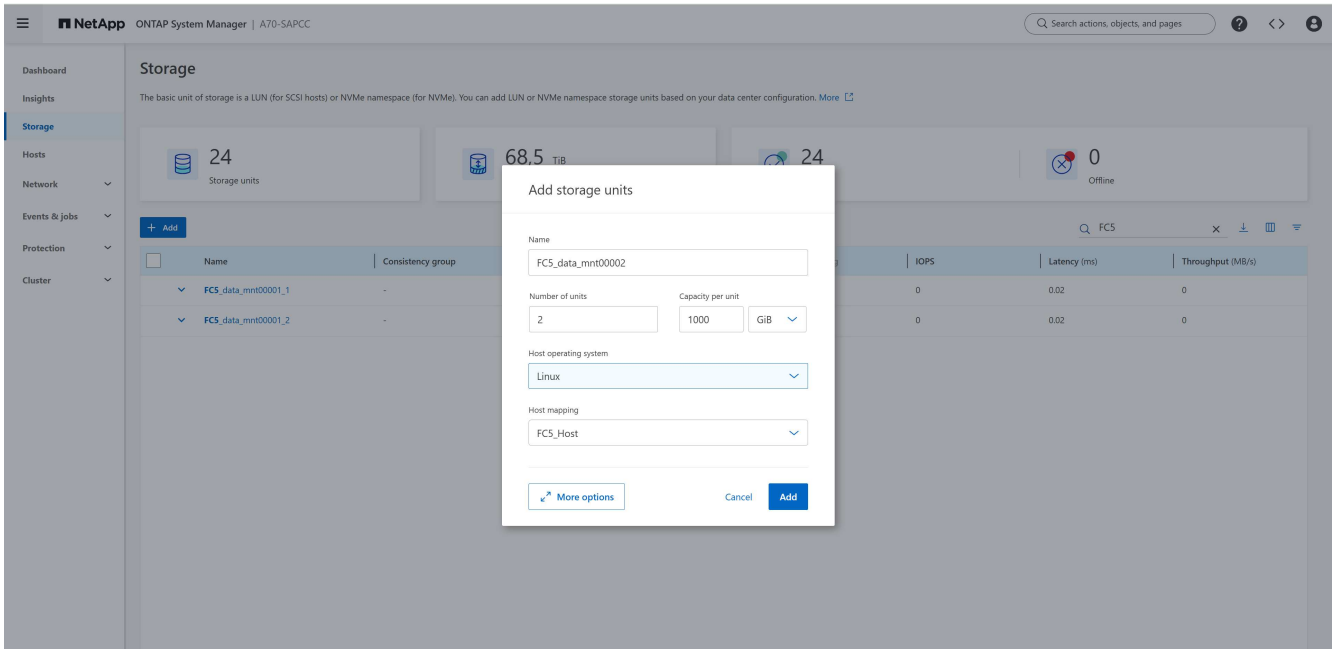
   b. die Anzahl der mit LVM zu kombinierenden LUNs, zB 2

   c. die Größe jeder LUN, zB 1000 GB

   d. wählen `Linux` als `Host Operating system`

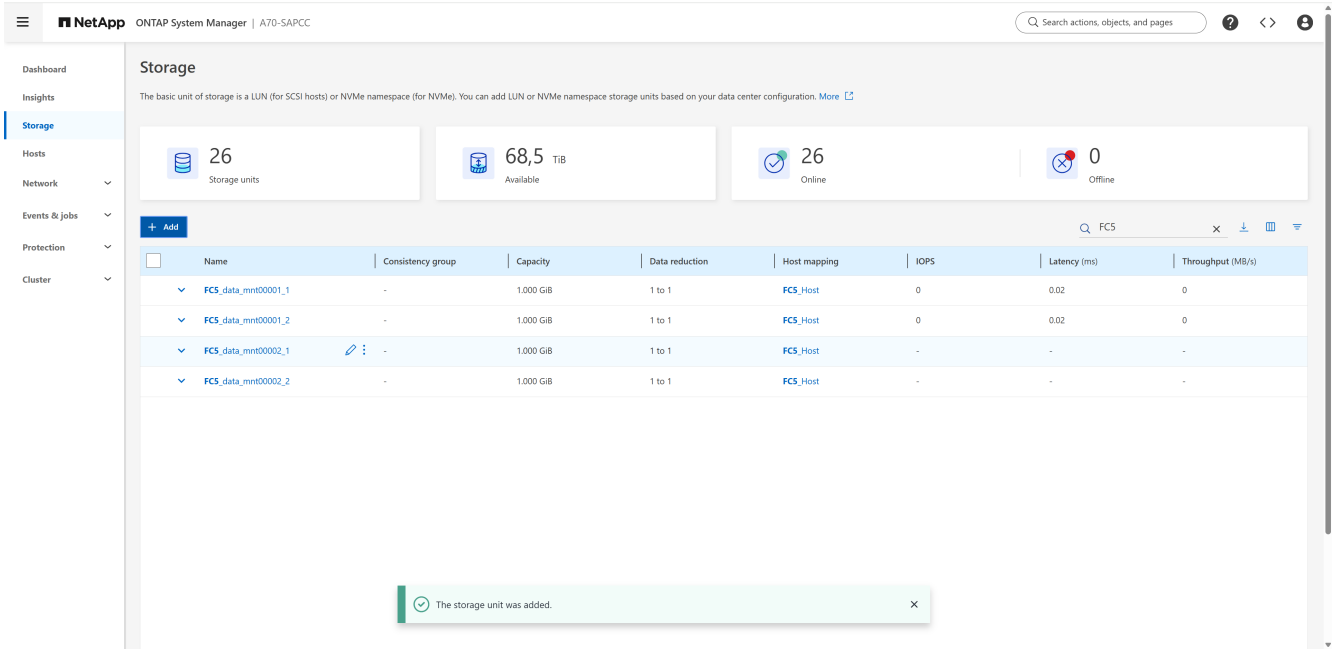
   e. Wählen Sie die zuvor erstellte Zuordnung `FC5_host` für die `Host mapping` Option

   f. drücken `Add`

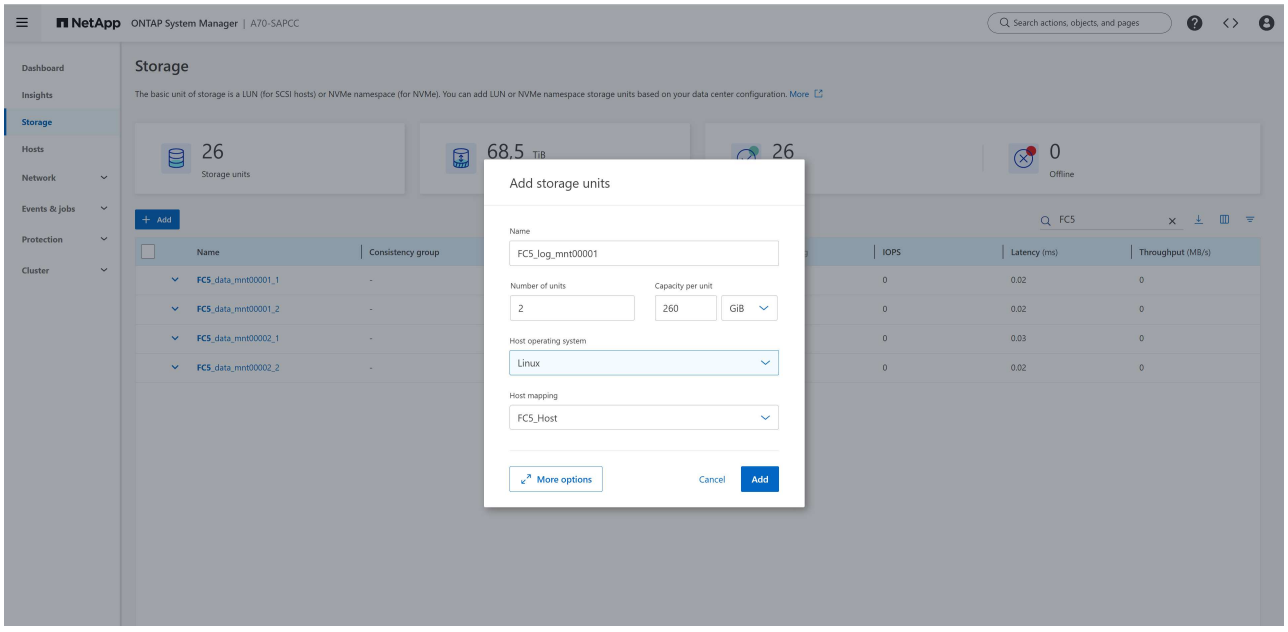


6. Wiederholen Sie die Schritte 4 und 5 für jeden weiteren Worker-Host

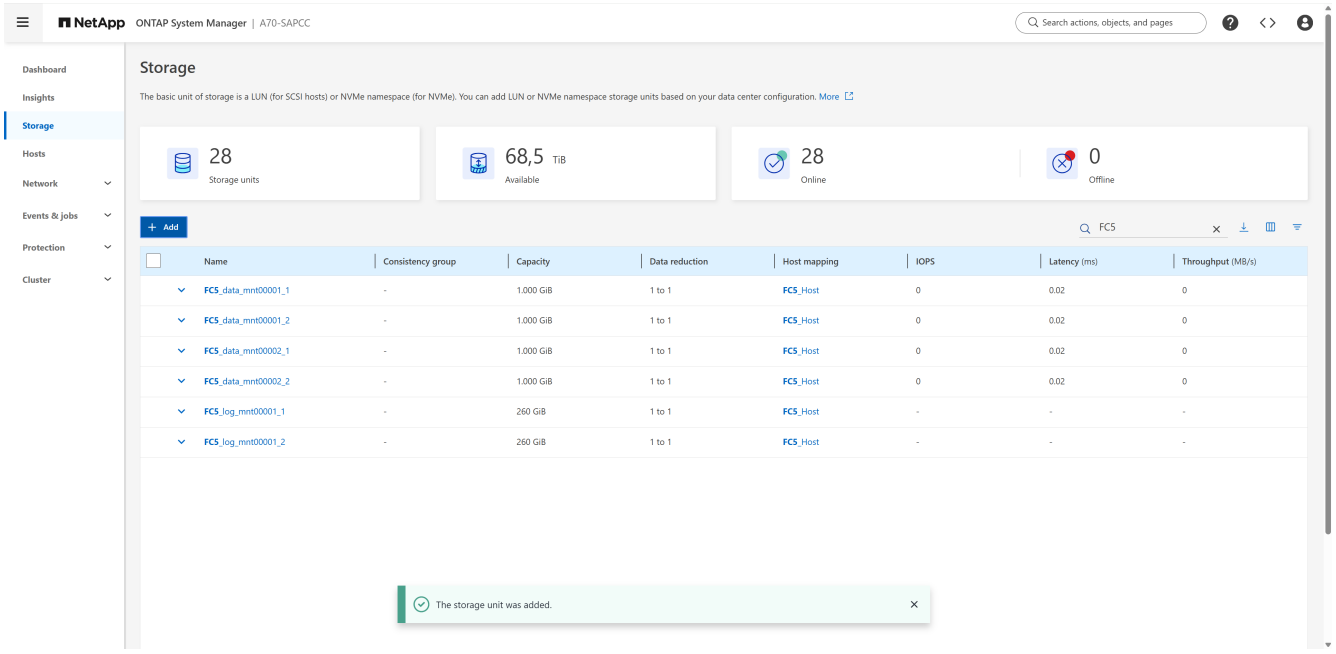
7. Nach erfolgreicher Erstellung der Daten-LUNs erstellen Sie die Log-LUNs durch Drücken von `Add`



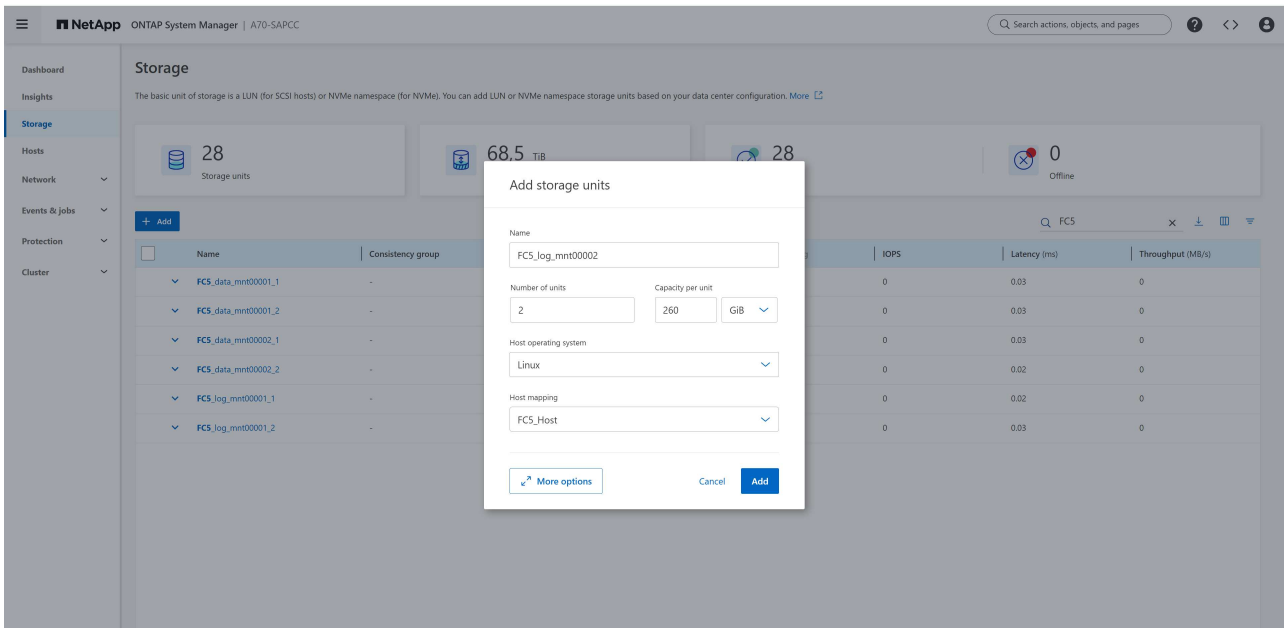
8. Geben Sie die erforderlichen Informationen ein:
   a. der Name der Log-LUNs, die mit LVM kombiniert werden sollen, zB `FC5_log_mnt00001`
   b. die Anzahl der mit LVM zu kombinierenden LUNs, zB 2
   c. die Größe jeder LUN, zB 260 GB
   d. wählen `Linux` als `Host Operating system`
   e. Wählen Sie die zuvor erstellte Zuordnung `FC5_host` für die `Host mapping` Option
   f. drücken `Add`



9. Erstellen Sie die Protokoll-LUNs für den nächsten Worker-Host, indem Sie `Add`

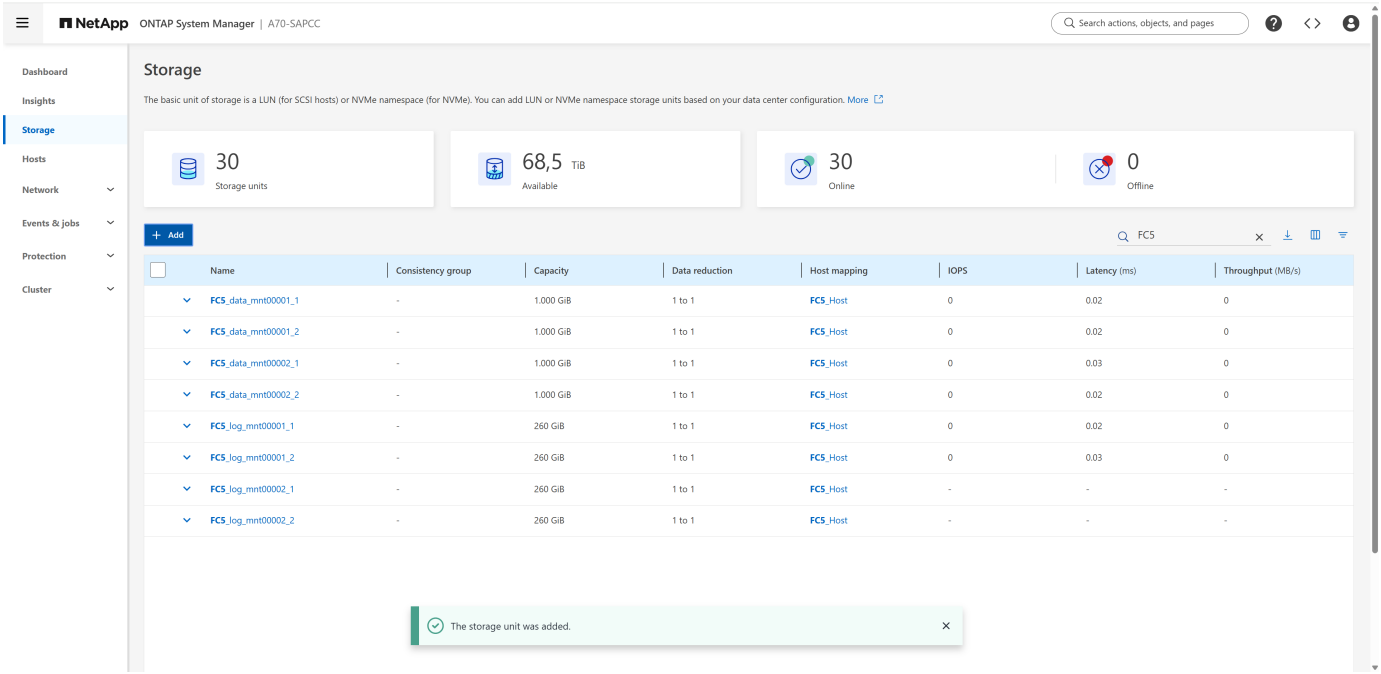


10. Geben Sie die erforderlichen Informationen ein:
    a. der Name der zusätzlichen Log-LUNs, zB `FC5_log_mnt00002`
    b. die Anzahl der mit LVM zu kombinierenden LUNs, zB 2
    c. die Größe jeder LUN, zB 260 GB
    d. wählen `Linux` als `Host Operating system`
    e. Wählen Sie die zuvor erstellte Zuordnung `FC5_host` für die `Host mapping` Option
    f. drücken `Add`



11. Wiederholen Sie die Schritte 9 und 10 für jeden weiteren Worker-Host

Alle erforderlichen LUNs für ein SAP HANA-Mehrhostsystem wurden erstellt.



SAP HANA Storage-Connector-API

Ein Storage Connector ist nur in Umgebungen mit mehreren Hosts mit Failover-Funktionen erforderlich. SAP HANA bietet bei der Einrichtung mehrerer Hosts eine Hochverfügbarkeitsfunktionen, mit der ein Failover eines SAP HANA-Datenbankhosts auf einen Standby-Host möglich ist.

In diesem Fall wird auf die LUNs des ausgefallenen Hosts zugegriffen und vom Standby-Host verwendet. Der Speicher-Connector wird verwendet, um sicherzustellen, dass eine Speicherpartition von jeweils nur einem Datenbank-Host aktiv zugegriffen werden kann.

In SAP HANA Konfigurationen mit mehreren Hosts und NetApp Storage kommt der von SAP bereitgestellte Standard-Storage Connector zum Einsatz. Der „SAP HANA Fibre Channel Storage Connector Admin Guide“ kann als Anhang zu gefunden werden "SAP-Hinweis 1900823".

Hosteinrichtung

Bevor Sie den Host einrichten, müssen die NetApp SAN Host Utilities von heruntergeladen werden "NetApp Support" Standort und auf den HANA-Servern installiert. Die Dokumentation des Host Utility enthält Informationen zu zusätzlicher Software, die abhängig vom verwendeten FCP HBA installiert werden muss.

Die Dokumentation enthält auch Informationen zu Multipath-Konfigurationen, die spezifisch für die verwendete Linux-Version sind. In diesem Dokument werden die erforderlichen Konfigurationsschritte für SLES 12 SP1 oder höher und RHEL 7 beschrieben. 2 oder höher, wie im beschrieben "Linux Host Utilities 7.1 Installations- und Setup-Leitfaden".

Konfigurieren Sie Multipathing

Die Schritte 1 bis 6 müssen auf allen Worker- und Standby-Hosts in einer SAP HANA Konfiguration mit mehreren Hosts ausgeführt werden.

Um Multipathing zu konfigurieren, gehen Sie wie folgt vor:

1. Führen Sie Linux aus `rescan-scsi-bus.sh -a` Befehl auf jedem Server, um neue LUNs zu ermitteln.
2. Führen Sie den `sanlun lun show` und überprüfen Sie, ob alle erforderlichen LUNs sichtbar sind. Das folgende Beispiel zeigt die `sanlun lun show` Befehlsausgabe für ein 2+1-HANA-System mit mehreren Hosts, zwei Daten-LUNs und zwei Protokoll-LUNs. Die Ausgabe zeigt die LUNs und die zugehörigen Gerätedateien, z. B. LUN `FC5_data_mnt00001` und die Gerätedatei `/dev/sdag` Jede LUN verfügt über acht FC-Pfade vom Host zu den Speichercontrollern.

```
sapcc-hana-tst:~ # sanlun lun show
controller(7mode/E-Series)/                                    device
host                  lun
vserver(cDOT/FlashRay)        lun-pathname                     filename
adapter    protocol   size    product
------------------------------------------------------------------------
---------------------------------------
svm1                          FC5_log_mnt00002_2               /dev/sdbb
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00002_1               /dev/sdba
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001_2               /dev/sdaz
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001_1               /dev/sday
host21     FCP        500g    cDOT
svm1                          FC5_data_mnt00002_2              /dev/sdax
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00002_1              /dev/sdaw
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001_2              /dev/sdav
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001_1              /dev/sdau
host21     FCP        1t      cDOT
svm1                          FC5_log_mnt00002_2               /dev/sdat
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00002_1               /dev/sdas
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001_2               /dev/sdar
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001_1               /dev/sdaq
host21     FCP        500g    cDOT
svm1                          FC5_data_mnt00002_2              /dev/sdap
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00002_1              /dev/sdao
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001_2              /dev/sdan
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001_1              /dev/sdam
host21     FCP        1t      cDOT
```

```
svm1                            FC5_log_mnt00002_2            /dev/sdal
host20     FCP         500g     cDOT
svm1                            FC5_log_mnt00002_1            /dev/sdak
host20     FCP         500g     cDOT
svm1                            FC5_log_mnt00001_2            /dev/sdaj
host20     FCP         500g     cDOT
svm1                            FC5_log_mnt00001_1            /dev/sdai
host20     FCP         500g     cDOT
svm1                            FC5_data_mnt00002_2           /dev/sdah
host20     FCP         1t       cDOT
svm1                            FC5_data_mnt00002_1           /dev/sdag
host20     FCP         1t       cDOT
svm1                            FC5_data_mnt00001_2           /dev/sdaf
host20     FCP         1t       cDOT
svm1                            FC5_data_mnt00001_1           /dev/sdae
host20     FCP         1t       cDOT
svm1                            FC5_log_mnt00002_2            /dev/sdad
host20     FCP         500g     cDOT
svm1                            FC5_log_mnt00002_1            /dev/sdac
host20     FCP         500g     cDOT
svm1                            FC5_log_mnt00001_2            /dev/sdab
host20     FCP         500g     cDOT
svm1                            FC5_log_mnt00001_1            /dev/sdaa
host20     FCP         500g     cDOT
svm1                            FC5_data_mnt00002_2           /dev/sdz
host20     FCP         1t       cDOT
svm1                            FC5_data_mnt00002_1           /dev/sdy
host20     FCP         1t       cDOT
svm1                            FC5_data_mnt00001_2           /dev/sdx
host20     FCP         1t       cDOT
svm1                            FC5_data_mnt00001_1           /dev/sdw
host20     FCP         1t       cDOT
```

3. Führen Sie den `multipath -r` Und `multipath -ll` Befehl zum Abrufen der weltweiten Kennungen (WWIDs) für die Gerätedateinamen.

   In diesem Beispiel gibt es acht LUNs.

```
sapcc-hana-tst:~ # multipath -r
sapcc-hana-tst:~ # multipath -ll
3600a098038314e63492b59326b4b786d dm-7 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:2 sdaf 65:240 active ready running
```

```
  |- 20:0:5:2 sdx  65:112 active ready running
  |- 21:0:4:2 sdav 66:240 active ready running
  `- 21:0:6:2 sdan 66:112 active ready running
3600a098038314e63492b59326b4b786e dm-9 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:4 sdah 66:16  active ready running
  |- 20:0:5:4 sdz  65:144 active ready running
  |- 21:0:4:4 sdax 67:16  active ready running
  `- 21:0:6:4 sdap 66:144 active ready running
3600a098038314e63492b59326b4b786f dm-11 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:6 sdaj 66:48  active ready running
  |- 20:0:5:6 sdab 65:176 active ready running
  |- 21:0:4:6 sdaz 67:48  active ready running
  `- 21:0:6:6 sdar 66:176 active ready running
3600a098038314e63492b59326b4b7870 dm-13 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:8 sdal 66:80  active ready running
  |- 20:0:5:8 sdad 65:208 active ready running
  |- 21:0:4:8 sdbb 67:80  active ready running
  `- 21:0:6:8 sdat 66:208 active ready running
3600a098038314e63532459326d495a64 dm-6 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:1 sdae 65:224 active ready running
  |- 20:0:5:1 sdw  65:96  active ready running
  |- 21:0:4:1 sdau 66:224 active ready running
  `- 21:0:6:1 sdam 66:96  active ready running
3600a098038314e63532459326d495a65 dm-8 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:3 sdag 66:0   active ready running
  |- 20:0:5:3 sdy  65:128 active ready running
  |- 21:0:4:3 sdaw 67:0   active ready running
  `- 21:0:6:3 sdao 66:128 active ready running
3600a098038314e63532459326d495a66 dm-10 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
```

```
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:5 sdai 66:32  active ready running
  |- 20:0:5:5 sdaa 65:160 active ready running
  |- 21:0:4:5 sday 67:32  active ready running
  `- 21:0:6:5 sdaq 66:160 active ready running
3600a098038314e63532459326d495a67 dm-12 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:7 sdak 66:64  active ready running
  |- 20:0:5:7 sdac 65:192 active ready running
  |- 21:0:4:7 sdba 67:64  active ready running
  `- 21:0:6:7 sdas 66:192 active ready running
```

4. Bearbeiten Sie das `/etc/multipath.conf` Datei und fügen Sie die WWIDs und Aliasnamen hinzu.

> Die Beispielausgabe zeigt den Inhalt des `/etc/multipath.conf` Datei, die Alias-Namen für die vier LUNs eines 2+1-Systems mit mehreren Hosts enthält. Wenn keine Multipath.conf-Datei verfügbar ist, können Sie eine erstellen, indem Sie den folgenden Befehl ausführen: `multipath -T > /etc/multipath.conf`.

```
sapcc-hana-tst:/ # cat /etc/multipath.conf
multipaths {
                multipath {
                wwid    3600a098038314e63492b59326b4b786d
                alias   svm1-FC5_data_mnt00001_2
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b786e
                alias   svm1-FC5_data_mnt00002_2
        }
        multipath {
                wwid    3600a098038314e63532459326d495a64
                alias   svm1-FC5_data_mnt00001_1
        }
        multipath {
                wwid    3600a098038314e63532459326d495a65
                alias   svm1-FC5_data_mnt00002_1
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b786f
                alias   svm1-FC5_log_mnt00001_2
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b7870
                alias   svm1-FC5_log_mnt00002_2
        }
        multipath {
                wwid    3600a098038314e63532459326d495a66
                alias   svm1-FC5_log_mnt00001_1
        }
        multipath {
                wwid    3600a098038314e63532459326d495a67
                alias   svm1-FC5_log_mnt00002_1
        }


}
```

5. Führen Sie die aus `multipath -r` Befehl zum Neuladen der Gerätezuordnung.
6. Überprüfen Sie die Konfiguration, indem Sie den ausführen `multipath -ll` Befehl zum Auflisten aller LUNs, Alias-Namen sowie aktiver und Standby-Pfade.

> Die folgende Beispielausgabe zeigt die Ausgabe eines 2+1-HANA-Systems mit mehreren Hosts mit zwei Daten und zwei Log-LUNs.

```
sapcc-hana-tst:~ # multipath -ll
svm1-FC5_data_mnt00001_2 (3600a098038314e63492b59326b4b786d) dm-7
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:2 sdaf 65:240 active ready running
  |- 20:0:5:2 sdx  65:112 active ready running
  |- 21:0:4:2 sdav 66:240 active ready running
  `- 21:0:6:2 sdan 66:112 active ready running
svm1-FC5_data_mnt00002_2 (3600a098038314e63492b59326b4b786e) dm-9
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:4 sdah 66:16  active ready running
  |- 20:0:5:4 sdz  65:144 active ready running
  |- 21:0:4:4 sdax 67:16  active ready running
  `- 21:0:6:4 sdap 66:144 active ready running
svm1-FC5_data_mnt00001_1 (3600a098038314e63532459326d495a64) dm-6
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:1 sdae 65:224 active ready running
  |- 20:0:5:1 sdw  65:96  active ready running
  |- 21:0:4:1 sdau 66:224 active ready running
  `- 21:0:6:1 sdam 66:96  active ready running
svm1-FC5_data_mnt00002_1 (3600a098038314e63532459326d495a65) dm-8
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:3 sdag 66:0   active ready running
  |- 20:0:5:3 sdy  65:128 active ready running
  |- 21:0:4:3 sdaw 67:0   active ready running
  `- 21:0:6:3 sdao 66:128 active ready running
svm1-FC5_log_mnt00001_2 (3600a098038314e63492b59326b4b786f) dm-11
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:6 sdaj 66:48  active ready running
  |- 20:0:5:6 sdab 65:176 active ready running
  |- 21:0:4:6 sdaz 67:48  active ready running
  `- 21:0:6:6 sdar 66:176 active ready running
```

```
svm1-FC5_log_mnt00002_2 (3600a098038314e63492b59326b4b7870) dm-13
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:8 sdal 66:80  active ready running
  |- 20:0:5:8 sdad 65:208 active ready running
  |- 21:0:4:8 sdbb 67:80  active ready running
  `- 21:0:6:8 sdat 66:208 active ready running
svm1-FC5_log_mnt00001_1 (3600a098038314e63532459326d495a66) dm-10
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:5 sdai 66:32  active ready running
  |- 20:0:5:5 sdaa 65:160 active ready running
  |- 21:0:4:5 sday 67:32  active ready running
  `- 21:0:6:5 sdaq 66:160 active ready running
svm1-FC5_log_mnt00002_1 (3600a098038314e63532459326d495a67) dm-12
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:7 sdak 66:64  active ready running
  |- 20:0:5:7 sdac 65:192 active ready running
  |- 21:0:4:7 sdba 67:64  active ready running
  `- 21:0:6:7 sdas 66:192 active ready running
```


Einzelhost-Setup

In diesem Kapitel wird die Einrichtung eines einzelnen SAP HANA-Hosts beschrieben.

LUN-Konfiguration für SAP HANA Single-Host-Systeme

Das Linux LVM wird verwendet, um die Leistung zu steigern und LUN-Größenbeschränkungen zu beheben. Beim SAP HANA-Host müssen Volume-Gruppen und logische Volumes erstellt und eingebunden werden, wie in der folgenden Tabelle angegeben.

Logisches Volume/LUN	Bereitstellungspunkt beim SAP HANA-Host	Hinweis
LV: FC5_data_mnt00001-vol	/hana/Data/FC5/mnt00001	Mit /etc/fstab-Eintrag montiert
LV: FC5_log_mnt00001-vol	/hana/log/FC5/mnt00001	Mit /etc/fstab-Eintrag montiert
LUN: FC5_shared	/hana/Shared/FC5	Mit /etc/fstab-Eintrag montiert

Mit der beschriebenen Konfiguration wird die `/usr/sap/FC5` Das Verzeichnis, in dem das Standard-Home-Verzeichnis des Benutzers FC5adm gespeichert ist, befindet sich auf der lokalen Festplatte. In einem Disaster Recovery-Setup mit festplattenbasierter Replikation empfiehlt NetApp die Erstellung einer zusätzlichen LUN für die `/usr/sap/FC5` Verzeichnis, sodass sich alle Dateisysteme auf dem zentralen Speicher befinden.

Erstellen von LVM-Volume-Gruppen und logischen Volumes

1. Initialisieren Sie alle LUNs als ein physisches Volume.

```
pvcreate /dev/mapper/svm1-FC5_data_mnt00001_1
pvcreate /dev/mapper/svm1-FC5_data_mnt00001_2
pvcreate /dev/mapper/svm1-FC5_log_mnt00001_1
pvcreate /dev/mapper/svm1-FC5_log_mnt00001_2
```

2. Erstellen Sie die Volume-Gruppen für jede Daten- und Protokollpartition.

```
vgcreate FC5_data_mnt00001 /dev/mapper/svm1-FC5_data_mnt00001_1
/dev/mapper/svm1-FC5_data_mnt00001_2
vgcreate FC5_log_mnt00001 /dev/mapper/svm1-FC5_log_mnt00001_1
/dev/mapper/svm1-FC5_log_mnt00001_2
```

3. Erstellen Sie für jede Daten- und Protokollpartition ein logisches Volume. Verwenden Sie eine Stripe-Größe, die der Anzahl der LUNs pro Volume-Gruppe entspricht (in diesem Beispiel sind es zwei), eine Stripe-Größe von 256 KB für Daten und 64.000 für das Protokoll. SAP unterstützt nur ein logisches Volume pro Volume-Gruppe.

```
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00001
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00001
```

4. Scannen Sie bei allen anderen Hosts die physischen Volumes, Volume-Gruppen und Volume-Gruppen.

```
modprobe dm_mod
pvscan
vgscan
lvscan
```

Wenn diese Befehle die Volumes nicht finden, ist ein Neustart erforderlich.

Zum Mounten der logischen Volumes müssen die logischen Volumes aktiviert sein. Um die Volumes zu aktivieren, führen Sie den folgenden Befehl aus:

```
vgchange -a y
```

Erstellen von Dateisystemen

Erstellen Sie das XFS-Dateisystem auf allen logischen Daten- und Protokollvolumes und der gemeinsam genutzten Hana-LUN.

```
mkfs.xfs FC5_data_mnt00001-vol
mkfs.xfs FC5_log_mnt00001-vol
mkfs.xfs /dev/mapper/svm1-FC5_shared
```

Die Beispielbefehle für mehrere Hosts zeigen ein 2+1-HANA-System mit mehreren Hosts.

Erstellen von Bereitstellungspunkten

Erstellen Sie die erforderlichen Mount-Point-Verzeichnisse und legen Sie die Berechtigungen auf dem Datenbankhost fest:

```
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/shared
sapcc-hana-tst:/ # chmod –R 777 /hana/log/FC5
sapcc-hana-tst:/ # chmod –R 777 /hana/data/FC5
sapcc-hana-tst:/ # chmod 777 /hana/shared
```

Mounten Sie File-Systeme

Um Dateisysteme während des Systemstarts mit dem `/etc/fstab` Konfigurationsdatei, fügen Sie die erforderlichen Dateisysteme zum `/etc/fstab` Konfigurationsdatei:

```
# cat /etc/fstab
/dev/mapper/hana-FC5_shared /hana/shared xfs defaults 0 0
/dev/mapper/FC5_log_mnt00001-vol /hana/log/FC5/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/FC5_data_mnt00001-vol /hana/data/FC5/mnt00001 xfs
relatime,inode64 0 0
```

Die XFS-Dateisysteme für die Daten- und Protokoll-LUNs müssen mit dem gemountet werden `relatime` Und `inode64` Mount-Optionen:

Um die Dateisysteme zu mounten, führen Sie den `mount –a` Befehl beim Host.

Einrichtung mehrerer Hosts

In diesem Kapitel wird beispielhaft die Einrichtung eines 2+1 SAP HANA-Mehrhostsystems beschrieben.

LUN-Konfiguration für SAP HANA-Mehrhostsysteme

Das Linux LVM wird verwendet, um die Leistung zu steigern und LUN-Größenbeschränkungen zu beheben.

Beim SAP HANA-Host müssen Volume-Gruppen und logische Volumes erstellt und eingebunden werden, wie in der folgenden Tabelle angegeben.

Logisches Volume (LV)	Bereitstellungspunkt beim SAP HANA-Host	Hinweis
LV: FC5_data_mnt00001-vol	/hana/Data/FC5/mnt00001	Montiert mit Speicheranschluss
LV: FC5_log_mnt00001-vol	/hana/log/FC5/mnt00001	Montiert mit Speicheranschluss
LV: FC5_data_mnt00002-vol	/hana/Data/FC5/mnt00002	Montiert mit Speicheranschluss
LV: FC5_log_mnt00002-vol	/hana/log/FC5/mnt00002	Montiert mit Speicheranschluss
Externe NFS-Freigabe: FC5_shared	/hana/Shared	Gemountet auf allen Hosts mit NFS und /etc/fstab Eintrag

SAP HANA-Multi-Host-Systeme erfordern die `/hana/shared` Dateisystem, das mit allen Hosts eines Systems verbunden ist. In der Regel handelt es sich dabei um eine NFS-Freigabe, die von einem NFS-Server bereitgestellt wird. Es wird empfohlen, einen hochverfügbaren NFS-Server zu verwenden, z. B. ein NetApp FAS- oder AFF-System. Alternativ kann der integrierte NFS-Server eines Linux-Hosts verwendet werden.

Mit der beschriebenen Konfiguration wird die `/usr/sap/FC5` Das Verzeichnis, in dem das Standard-Home-Verzeichnis des Benutzers FC5adm gespeichert ist, befindet sich auf der lokalen Festplatte jedes HANA-Hosts. In einem Disaster Recovery-Setup mit festplattenbasierter Replikation empfiehlt NetApp die Verwendung von vier zusätzlichen LUNs für `/usr/sap/FC5` Dateisystem jedes Hosts, sodass jeder Datenbankhost alle seine Dateisysteme auf dem zentralen Speicher hat.

Erstellen von LVM-Volume-Gruppen und logischen Volumes

1. Initialisieren Sie alle LUNs als ein physisches Volume.

```
pvcreate /dev/mapper/svm1-FC5_data_mnt00001_1
pvcreate /dev/mapper/svm1-FC5_data_mnt00001_2
pvcreate /dev/mapper/svm1-FC5_data_mnt00002_1
pvcreate /dev/mapper/svm1-FC5_data_mnt00002_2
pvcreate /dev/mapper/svm1-FC5_log_mnt00001_1
pvcreate /dev/mapper/svm1-FC5_log_mnt00001_2
pvcreate /dev/mapper/svm1-FC5_log_mnt00002_1
pvcreate /dev/mapper/svm1-FC5_log_mnt00002_2
```

2. Erstellen Sie die Volume-Gruppen für jede Daten- und Protokollpartition.

```
vgcreate FC5_data_mnt00001 /dev/mapper/svm1-FC5_data_mnt00001_1
/dev/mapper/svm1-FC5_data_mnt00001_2
vgcreate FC5_data_mnt00002 /dev/mapper/svm1-FC5_data_mnt00002_1
/dev/mapper/svm1-FC5_data_mnt00002_2
vgcreate FC5_log_mnt00001 /dev/mapper/svm1-FC5_log_mnt00001_1
/dev/mapper/svm1-FC5_log_mnt00001_2
vgcreate FC5_log_mnt00002 /dev/mapper/svm1-FC5_log_mnt00002_1
/dev/mapper/svm1-FC5_log_mnt00002_2
```

3. Erstellen Sie für jede Daten- und Protokollpartition ein logisches Volume. Verwenden Sie eine Stripe-Größe, die der Anzahl der LUNs pro Volume-Gruppe entspricht (in diesem Beispiel sind es zwei), eine Stripe-Größe von 256 KB für Daten und 64.000 für das Protokoll. SAP unterstützt nur ein logisches Volume pro Volume-Gruppe.

```
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00001
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00002
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00002
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00001
```

4. Scannen Sie bei allen anderen Hosts die physischen Volumes, Volume-Gruppen und Volume-Gruppen.

```
modprobe dm_mod
pvscan
vgscan
lvscan
```

Wenn diese Befehle die Volumes nicht finden, ist ein Neustart erforderlich.

Zum Mounten der logischen Volumes müssen die logischen Volumes aktiviert sein. Um die Volumes zu aktivieren, führen Sie den folgenden Befehl aus:

```
vgchange -a y
```

Erstellen von Dateisystemen

Erstellen Sie das XFS-Dateisystem auf allen logischen Daten- und Protokollvolumes.

```
mkfs.xfs FC5_data_mnt00001-vol
mkfs.xfs FC5_data_mnt00002-vol
mkfs.xfs FC5_log_mnt00001-vol
mkfs.xfs FC5_log_mnt00002-vol
```

Erstellen von Bereitstellungspunkten

Erstellen Sie die erforderlichen Mount-Point-Verzeichnisse und legen Sie die Berechtigungen auf allen Worker- und Standby-Hosts fest:

```
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00002
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00002
sapcc-hana-tst:/ # mkdir -p /hana/shared
sapcc-hana-tst:/ # chmod –R 777 /hana/log/FC5
sapcc-hana-tst:/ # chmod –R 777 /hana/data/FC5
sapcc-hana-tst:/ # chmod 777 /hana/shared
```

Mounten Sie File-Systeme

Zur Montage des `/hana/shared` Dateisysteme während des Systemstarts mithilfe der `/etc/fstab` Konfigurationsdatei, fügen Sie die `/hana/shared` Dateisystem in die `/etc/fstab` Konfigurationsdatei jedes Hosts.

```
sapcc-hana-tst:/ # cat /etc/fstab
<storage-ip>:/hana_shared /hana/shared nfs rw,vers=3,hard,timeo=600,
intr,noatime,nolock 0 0
```

Alle Daten- und Protokolldateisysteme sind über den SAP HANA Storage Connector gemountet.

Führen Sie zum Mounten der Dateisysteme den aus `mount –a` Befehl an jedem Host.

I/O-Stack-Konfiguration für SAP HANA

I/O-Stack-Konfiguration für SAP HANA

Ab SAP HANA 1.0 SPS10 führte SAP Parameter ein, um das I/O-Verhalten anzupassen und die Datenbank für

das verwendete Datei- und Speichersystem zu optimieren.

NetApp hat Performance-Tests durchgeführt, um die idealen Werte zu definieren. In der folgenden Tabelle sind die optimalen Werte aufgeführt, die aus den Leistungstests abgeleitet wurden.

Parameter	Wert
max_parallel_io_Requests	128
Async_read_Submit	Ein
Async_write_submit_Active	Ein
Async_Write_Submit_Blocks	Alle

Für SAP HANA 1.0 bis SPS12 können diese Parameter während der Installation der SAP HANA-Datenbank eingestellt werden, wie in SAP Note beschrieben "2267798 – Konfiguration der SAP HANA Datenbank während der Installation mit hdbparam".

Alternativ können die Parameter nach der SAP HANA-Datenbankinstallation über die eingestellt werden `hdbparam` Framework:

```
FC5adm@sapcc-hana-tst:/usr/sap/FC5/HDB00> hdbparam --paramset
fileio.max_parallel_io_requests=128
FC5adm@sapcc-hana-tst:/usr/sap/FC5/HDB00> hdbparam --paramset
fileio.async_write_submit_active=on
FC5adm@sapcc-hana-tst:/usr/sap/FC5/HDB00> hdbparam --paramset
fileio.async_read_submit=on
FC5adm@sapcc-hana-tst:/usr/sap/FC5/HDB00> hdbparam --paramset
fileio.async_write_submit_blocks=all
```

Ab SAP HANA 2.0 `hdbparam` Ist veraltet und die Parameter werden in die verschoben `global.ini` Datei: Die Parameter können über SQL-Befehle oder SAP HANA Studio eingestellt werden. Weitere Informationen finden Sie im SAP-Hinweis "2399079: Beseitigung von hdbparam in HANA 2". Die Parameter können auch im festgelegt werden `global.ini` Datei:

```
FC5adm@sapcc-hana-tst: /usr/sap/FC5/SYS/global/hdb/custom/config> cat
global.ini
…
[fileio]
async_read_submit = on
async_write_submit_active = on
max_parallel_io_requests = 128
async_write_submit_blocks = all
…
```

Verwenden Sie für SAP HANA 2.0 SPS5 und höher den `setParameter.py` Skript zum Festlegen der richtigen Parameter.

```
fc5adm@sapcc-hana-tst-03:/usr/sap/FC5/HDB00/exe/python_support>
python setParameter.py
-set=SYSTEM/global.ini/fileio/max_parallel_io_requests=128
python setParameter.py -set=SYSTEM/global.ini/fileio/async_read_submit=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_active=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_blocks=all
```

SAP HANA Softwareinstallation

In diesem Abschnitt wird die Vorbereitung für die Installation von SAP HANA auf Single-Host- und Multiple-Host-Systemen beschrieben.

Installation auf Single-Host-System

Die Installation der SAP HANA-Software erfordert keine zusätzliche Vorbereitung auf ein Single-Host-System.

Installation auf Systemen mit mehreren Hosts

Erstellen Sie vor Beginn der Installation einen `global.ini` Datei, um die Verwendung des SAP-Speicheranschlusses während des Installationsprozesses zu ermöglichen. Der SAP-Speicheranschluss montiert die erforderlichen Dateisysteme während des Installationsprozesses an den Worker-Hosts. Der `global.ini` Die Datei muss in einem Dateisystem verfügbar sein, auf das über alle Hosts zugegriffen werden kann, z. B. die `/hana/shared` File-System.

Vor der Installation der SAP HANA-Software auf einem System mit mehreren Hosts müssen die folgenden Schritte durchgeführt werden:

1. Fügen Sie die folgenden Mount-Optionen für die Daten-LUNs und die Protokoll-LUNs auf dem hinzu `global.ini` Datei:
   - `relatime` Und `inode64` Für das Daten- und Protokolldateisystem
2. Fügen Sie die WWIDs der Daten- und Log-Partitionen hinzu. Die WWIDs müssen mit den im konfigurierten Aliasnamen übereinstimmen `/etc/multipath.conf` Datei:

   Das folgende Beispiel zeigt eine 2+1 Konfiguration mehrerer Hosts mit SID=FC5.

```
sapcc-hana-tst-03:/hana/shared # cat global.ini
[communication]
listeninterface = .global
[persistence]
basepath_datavolumes = /hana/data/FC5
basepath_logvolumes = /hana/log/FC5
[storage]
ha_provider = hdb_ha.fcClientLVM
partition_*_*__prtype = 5
partition_*_data__mountOptions = -o relatime,inode64
partition_*_log__mountOptions = -o relatime,inode64
partition_1_data__lvmname = FC5_data_mnt00001-vol
partition_1_log__lvmname = FC5_log_mnt00001-vol
partition_2_data__lvmname = FC5_data_mnt00002-vol
partition_2_log__lvmname = FC5_log_mnt00002-vol
sapcc-hana-tst-03:/hana/shared #
```

Starten Sie die Installation mithilfe des SAP hdblcm-Installationstools, indem Sie den folgenden Befehl auf einem der Worker-Hosts ausführen. Verwenden Sie die `addhosts` Option, um den zweiten Worker (sapcc-hana-tst-06) und den Standby-Host (sapcc-hana-tst-07) hinzuzufügen.

+

Das Verzeichnis, in dem die vorbereitete `global.ini` Datei gespeichert wird(`--storage_cfg=/hana/shared`, ist mit der CLI-Option) enthalten `storage_cfg`.

+

Je nach verwendeter Betriebssystemversion kann es erforderlich sein, Python 2.7 zu installieren, bevor die SAP HANA-Datenbank installiert wird.

+

```
./hdblcm --action=install --addhosts=sapcc-hana-tst
-06:role=worker:storage_partition=2,sapcc-hana-tst-07:role=standby
--storage_cfg=/hana/shared/

AP HANA Lifecycle Management - SAP HANA Database 2.00.073.00.1695288802
************************************************************************


Scanning software locations...
Detected components:
    SAP HANA AFL (incl.PAL,BFL,OFL) (2.00.073.0000.1695321500) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
```

```
73/DATA_UNITS/HDB_AFL_LINUX_X86_64/packages
    SAP HANA Database (2.00.073.00.1695288802) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
    SAP HANA Database Client (2.18.24.1695756995) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/SAP_HANA_CLIENT/client
    SAP HANA Studio (2.3.75.000000) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/HDB_STUDIO_LINUX_X86_64/studio
    SAP HANA Local Secure Store (2.11.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HANA_LSS_24_LINUX_X86_64/packages
    SAP HANA XS Advanced Runtime (1.1.3.230717145654) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/XSA_RT_10_LINUX_X86_64/packages
    SAP HANA EML AFL (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_EML_AFL_10_LINUX_X86_64/packages
    SAP HANA EPM-MDS (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/SAP_HANA_EPM-MDS_10/packages
    Automated Predictive Library (4.203.2321.0.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/PAAPL4_H20_LINUX_X86_64/apl-
4.203.2321.0-hana2sp03-linux_x64/installer/packages
    GUI for HALM for XSA (including product installer) Version 1 (1.015.0)
in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACALMPIUI15_0.zip
    XSAC FILEPROCESSOR 1.0 (1.000.102) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACFILEPROC00_102.zip
    SAP HANA tools for accessing catalog content, data preview, SQL
console, etc. (2.015.230503) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_HRTT_20/XSACHRTT15_230503.zip
    Develop and run portal services for customer applications on XSA
(2.007.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACPORTALSERV07_0.zip
    The SAP Web IDE for HANA 2.0 (4.007.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_SAP_WEB_IDE_20/XSACSAPWEBIDE07_0.zip
    XS JOB SCHEDULER 1.0 (1.007.22) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACSERVICES07_22.zip
    SAPUI5 FESV6 XSA 1 - SAPUI5 1.71 (1.071.52) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV671_52.zip
    SAPUI5 FESV9 XSA 1 - SAPUI5 1.108 (1.108.5) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV9108_5.zip
    SAPUI5 SERVICE BROKER XSA 1 - SAPUI5 Service Broker 1.0 (1.000.4) in
```

```
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5SB00_4.zip
    XSA Cockpit 1 (1.001.37) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACXSACOCKPIT01_37.zip


SAP HANA Database version '2.00.073.00.1695288802' will be installed.

Select additional components for installation:

  Index | Components      | Description

-------------------------------------------------------------------------------
------------------------
  1     | all             | All components
  2     | server          | No additional components
  3     | client          | Install SAP HANA Database Client version
2.18.24.1695756995
  4     | lss             | Install SAP HANA Local Secure Store version
2.11.0
  5     | studio          | Install SAP HANA Studio version 2.3.75.000000
  6     | xs              | Install SAP HANA XS Advanced Runtime version
1.1.3.230717145654
  7     | afl             | Install SAP HANA AFL (incl.PAL,BFL,OFL)
version 2.00.073.0000.1695321500
  8     | eml             | Install SAP HANA EML AFL version
2.00.073.0000.1695321500
  9     | epmmds          | Install SAP HANA EPM-MDS version
2.00.073.0000.1695321500
  10    | sap_afl_sdk_apl | Install Automated Predictive Library version
4.203.2321.0.0

Enter comma-separated list of the selected indices [3,4]: 2,3
```

1. Vergewissern Sie sich, dass das Installationstool alle ausgewählten Komponenten bei allen Worker- und Standby-Hosts installiert hat.

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten bzw. auf den folgenden Websites:

- "SAP HANA Softwarelösungen"
- "TR-4646: SAP HANA Disaster Recovery with Storage Replication"
- "SAP HANA Datensicherung und Hochverfügbarkeit mit SnapCenter, SnapMirror Active Sync und VMware Metro Storage Cluster"

- "TR-4614: SAP HANA Backup and Recovery with SnapCenter"
- "TR-4667: Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter"
- NetApp Dokumentationszentren

  "https://www.netapp.com/support-and-training/documentation/"
- SAP Certified Enterprise Storage Hardware for SAP HANA

  "https://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/"
- SAP HANA Storage-Anforderungen

  "https://www.sap.com/documents/2024/03/146274d3-ae7e-0010-bca6-c68f7e60039b.html"
- SAP HANA Tailored Data Center Integration Häufig gestellte Fragen

  "https://www.sap.com/documents/2016/05/e8705aae-717c-0010-82c7-eda71af511fa.html"
- SAP HANA auf VMware vSphere Wiki

  "https://help.sap.com/docs/SUPPORT_CONTENT/virtualization/3362185751.html"
- Best Practices Guide für SAP HANA auf VMware vSphere

  "https://www.vmware.com/docs/sap_hana_on_vmware_vsphere_best_practices_guide-white-paper"

Aktualisierungsverlauf

An dieser Lösung wurden seit ihrer ersten Veröffentlichung folgende technische Änderungen vorgenommen:

Datum	Zusammenfassung aktualisieren
Juli 2025	Ausgangsversion

Konfigurationsleitfaden für SAP HANA auf NetApp FAS-Systemen mit NFS

Leitfaden für SAP HANA auf NetApp FAS-Systemen mit NFS-Konfiguration

Die NetApp FAS Produktfamilie wurde für die Verwendung mit SAP HANA für Tailored Datacenter Integration-Projekte (TDI) zertifiziert. Dieser Leitfaden enthält Best Practices für SAP HANA auf dieser Plattform mit NFS.

Marco Schoen, NetApp

Diese Zertifizierung gilt derzeit nur für die folgenden Modelle:

- FAS2750, FAS2820, FAS8300, FAS50, FAS8700, FAS70, FAS9500, FAS90 Eine vollständige Liste der von NetApp zertifizierten Storage-Lösungen für SAP HANA finden Sie unter "Zertifiziertes und unterstütztes SAP HANA Hardware Directory" .

In diesem Dokument werden die ONTAP-Konfigurationsanforderungen für das NFS-Protokoll, Version 3 (NFSv3) oder das NFS Version 4 (NFSv4.1)-Protokoll beschrieben.

Es werden nur NFS-Versionen 3 oder 4.1 unterstützt. NFS-Versionen 1, 2, 4.0 und 4.2 werden nicht unterstützt.

Die in diesem Dokument beschriebene Konfiguration ist erforderlich, um die erforderlichen SAP HANA KPIs und die beste Performance für SAP HANA zu erreichen. Wenn Sie Einstellungen oder Funktionen ändern, die nicht in diesem Dokument aufgeführt sind, kann dies zu einer Performance-Verschlechterung oder zu einem unerwarteten Verhalten führen. Diese Einstellungen sollten nur durchgeführt werden, wenn sie vom NetApp Support empfohlen werden.

Die Konfigurationsleitfäden für NetApp FAS Systeme mit FCP und für AFF Systeme mit NFS oder FC sind unter folgenden Links verfügbar:

- "Technischer Bericht: SAP HANA on NetApp FAS Systems with FCP"
- "Technischer Bericht: SAP HANA on NetApp AFF Systems with NFS"
- "Technischer Bericht: SAP HANA on NetApp AFF Systems with FCP"
- "Technischer Bericht: SAP HANA on NetApp ASA Systems with FCP"

In der folgenden Tabelle sind die unterstützten Kombinationen aus der NFS-Version, der NFS-Sperre und den erforderlichen Isolierungs-Implementierungen in Abhängigkeit von der Konfiguration der SAP HANA Datenbank aufgeführt.

Für SAP HANA Single-Host-Systeme oder mehrere Hosts ohne Host Auto-Failover werden NFSv3 und NFSv4 unterstützt.

Für SAP HANA unterstützen mehrere Host-Systeme mit Host Auto-Failover nur NetApp NFSv4, während die NFSv4-Sperrung als Alternative zu einer serverspezifischen STONITH-Implementierung (SAP HANA HA/DR-Provider) dient.

SAP HANA	NFS-Version	NFS-Sperre	SAP HANA HA-/DR-PROVIDER
SAP HANA ein Host, mehrere Hosts ohne Host Auto-Failover	NFSv3	Aus	k. A.
	NFSv4	Ein	k. A.
SAP HANA mehrere Hosts mit Host Auto-Failover	NFSv3	Aus	Serverspezifische STONITH-Implementierung erforderlich
	NFSv4	Ein	Nicht erforderlich

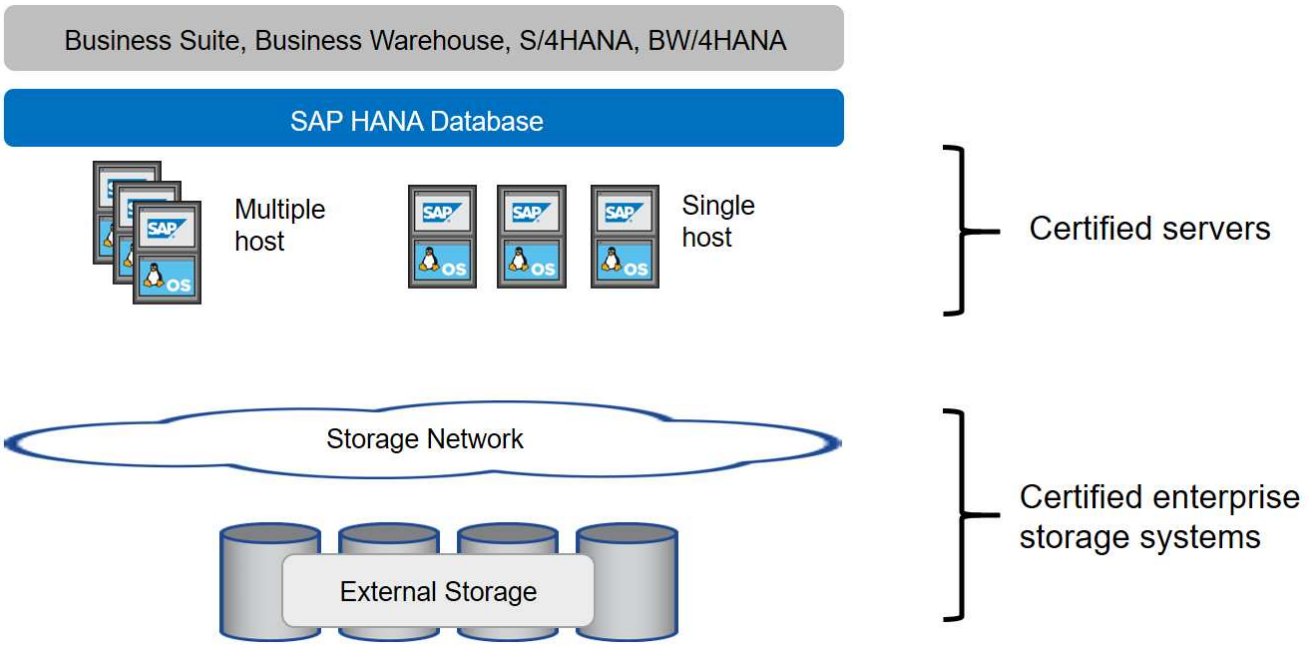
Eine serverspezifische STONITH-Implementierung ist nicht Teil dieses Leitfadens. Wenden Sie sich für eine solche Implementierung an Ihren Server-Anbieter.

Dieses Dokument enthält Konfigurationsempfehlungen für SAP HANA, die auf physischen Servern und virtuellen Servern ausgeführt werden, die VMware vSphere verwenden.

Beachten Sie immer die relevanten SAP-Hinweise für Konfigurationsrichtlinien für Betriebssysteme und HANA-spezifische Linux-Kernel-Abhängigkeiten. Weitere Informationen finden Sie unter "SAP-Hinweis 2235581: Von SAP HANA unterstützte Betriebssysteme".

SAP HANA Tailored Datacenter Integration

NetApp FAS Storage Controller sind im SAP HANA TDI Programm unter Verwendung von NFS- (NAS) und FC (SAN) Protokollen zertifiziert. Sie können in allen aktuellen SAP HANA-Szenarien wie SAP Business Suite on HANA, S/4HANA, BW/4HANA oder SAP Business Warehouse on HANA in Konfigurationen mit einem Host oder mehreren Hosts implementiert werden. Alle Server, die für den Einsatz mit SAP HANA zertifiziert sind, können mit von NetApp zertifizierten Storage-Lösungen kombiniert werden. In der folgenden Abbildung finden Sie eine Übersicht über die Architektur.



Weitere Informationen zu den Voraussetzungen und Empfehlungen für SAP HANA-Systeme in der Produktion finden Sie in der folgenden SAP-Ressource:

- "SAP HANA Tailored Data Center Integration Häufig gestellte Fragen"

SAP HANA mit VMware vSphere

Es gibt verschiedene Optionen, um den Storage mit Virtual Machines (VMs) zu verbinden. Der bevorzugte Modus ist die direkte Verbindung der Storage Volumes mit NFS vom Gastbetriebssystem. Bei Verwendung dieser Option unterscheidet sich die Konfiguration der Hosts und Storages nicht zwischen physischen Hosts und VMs.

NFS Datastores oder VVOL Datastores mit NFS werden ebenfalls unterstützt. Bei beiden Optionen muss nur ein SAP HANA Daten- oder Protokoll-Volume im Datastore für Produktionsanwendungsfälle gespeichert werden.

In diesem Dokument wird das empfohlene Setup mit direkten NFS-Mounts vom Gastbetriebssystem beschrieben.

Weitere Informationen zur Verwendung von vSphere mit SAP HANA finden Sie unter den folgenden Links:

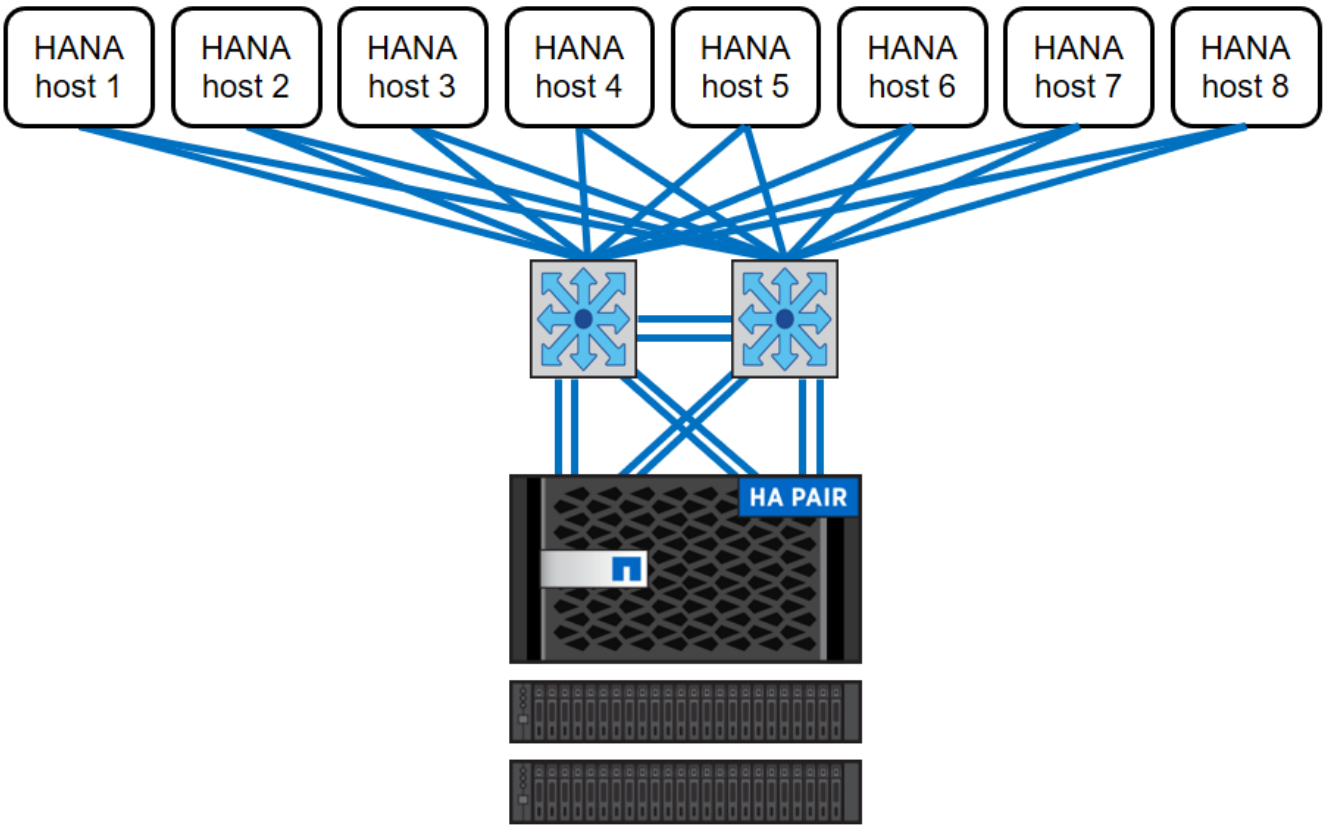
- "SAP HANA on VMware vSphere - Virtualization - Community Wiki"
- "Best Practices Guide für SAP HANA auf VMware vSphere"
- "2161991 - Konfigurationsrichtlinien für VMware vSphere - SAP ONE Support Launchpad (Anmeldung erforderlich)"

Der Netapp Architektur Sind

SAP HANA-Hosts sind über eine redundante 10-GbE- oder schnellere Netzwerkinfrastruktur mit Storage Controllern verbunden. Die Kommunikation zwischen SAP HANA-Hosts und Storage-Controllern basiert auf dem NFS-Protokoll.

Eine redundante Switching-Infrastruktur wird empfohlen, um eine fehlertolerante SAP HANA Host-zu-Storage-Konnektivität bei Switch- oder NIC-Ausfall (Network Interface Card) bereitzustellen. Die Switches können die Leistung einzelner Ports mit Port-Kanälen aggregieren, um als einzelne logische Einheit auf Hostebene angezeigt zu werden.

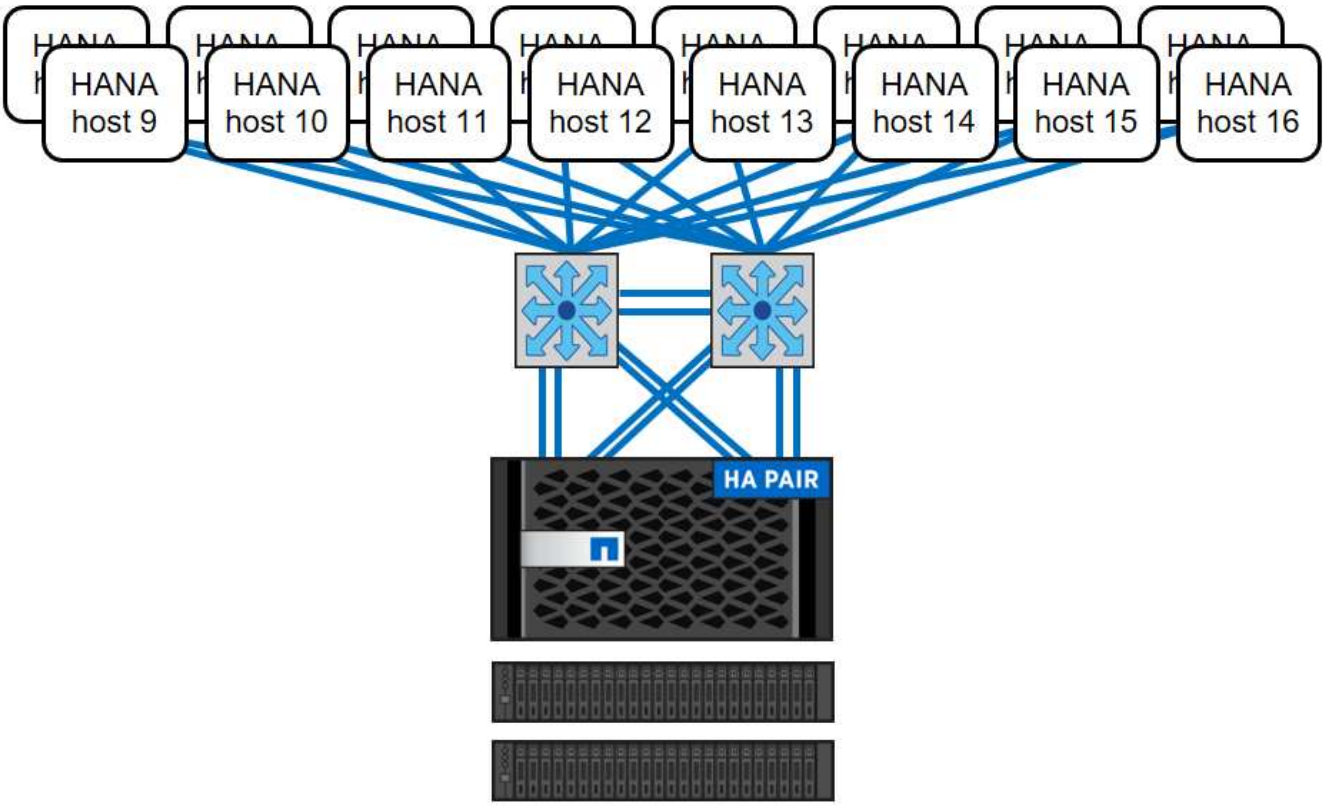
Verschiedene Modelle der FAS Produktfamilie können auf der Storage-Ebene miteinander kombiniert werden, um Wachstum und unterschiedliche Anforderungen an Performance und Kapazität zu ermöglichen. Die maximale Anzahl an SAP HANA-Hosts, die an das Storage-System angeschlossen werden können, sind durch die SAP HANA-Performance-Anforderungen und das Modell des verwendeten NetApp Controllers definiert. Die Anzahl der benötigten Festplatten-Shelfs wird nur von den Kapazitäts- und Performance-Anforderungen der SAP HANA Systeme bestimmt. Die folgende Abbildung zeigt eine Beispielkonfiguration mit acht SAP HANA-Hosts, die an ein Storage-HA-Paar angeschlossen sind.



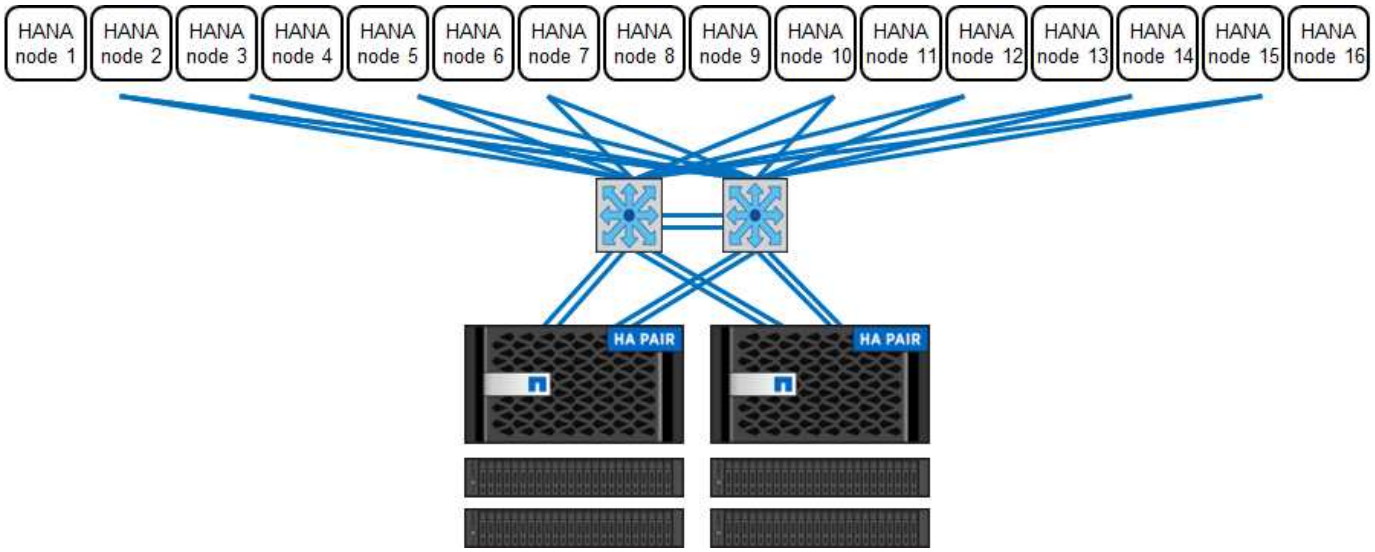
Die Architektur lässt sich in zwei Dimensionen skalieren:

- Durch Anbindung zusätzlicher SAP HANA-Hosts und/oder Speicherkapazität an den vorhandenen Storage, falls die Storage-Controller genügend Performance bieten, um die aktuellen Performance-Kennzahlen (KPIs) von SAP zu erfüllen
- Durch Hinzufügen weiterer Storage-Systeme mit zusätzlicher Storage-Kapazität für die zusätzlichen SAP HANA-Hosts

Die folgende Abbildung zeigt eine Beispielkonfiguration, in der mehr SAP HANA-Hosts mit den Storage-Controllern verbunden sind. In diesem Beispiel sind mehr Platten-Shelves erforderlich, um sowohl die Kapazitäts- als auch die Performance-Anforderungen von 16 SAP HANA-Hosts zu erfüllen. Je nach Gesamtdurchsatz müssen zusätzliche 10-GbE-Verbindungen (oder schneller) zu den Storage Controllern hinzugefügt werden.



Unabhängig vom implementierten FAS System lässt sich die SAP HANA Landschaft auch skalieren, indem beliebige der zertifizierten Storage-Controller hinzugefügt werden, um die gewünschte Node-Dichte zu erfüllen (siehe folgende Abbildung).



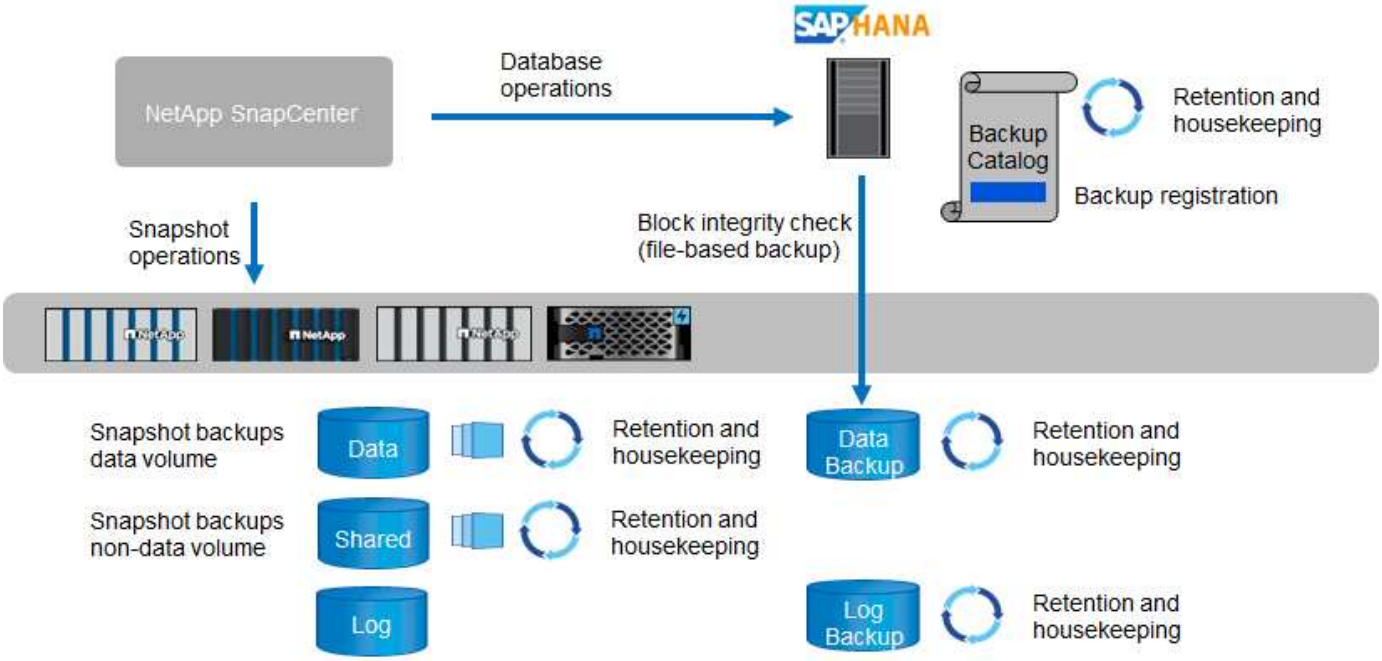
SAP HANA Backup

Die auf allen NetApp Storage-Controllern vorhandene ONTAP Software bietet einen integrierten Mechanismus zur Sicherung von SAP HANA Datenbanken, ohne die Performance zu beeinträchtigen. Storage-basierte NetApp Snapshot-Backups sind eine vollständig unterstützte und integrierte Backup-Lösung, die für einzelne SAP HANA Container sowie für SAP HANA MDC-Systeme (Multitenant Database Container) mit einem einzelnen Mandanten oder mehreren Mandanten verfügbar ist.

Storage-basierte Snapshot Backups werden über das NetApp SnapCenter Plug-in für SAP HANA implementiert. Benutzer können auf diese Weise konsistente Storage-basierte Snapshot Backups mithilfe der Schnittstellen erstellen, die nativ von SAP HANA Datenbanken bereitgestellt werden. SnapCenter registriert jedes der Snapshot-Backups im SAP HANA-Backup-Katalog. Die Backups von SnapCenter sind somit innerhalb von SAP HANA Studio und Cockpit sichtbar, wo sie direkt für Restore- und Recovery-Vorgänge selektiert werden können.

Mit der NetApp SnapMirror Technologie können Snapshot Kopien, die auf einem Storage-System erstellt wurden, in ein sekundäres Backup-Storage-System repliziert werden, das über SnapCenter gesteuert wird. Für jedes der Backup-Sätze auf dem primären Storage und für die Backup-Sätze auf den sekundären Storage-Systemen können somit unterschiedliche Backup-Aufbewahrungsrichtlinien definiert werden. Das SnapCenter Plug-in für SAP HANA managt automatisch die Aufbewahrung von auf Snapshot Kopien basierenden Daten-Backups und Log-Backups, einschließlich der allgemeinen Ordnung des Backup-Katalogs. Das SnapCenter Plug-in für SAP HANA ermöglicht darüber hinaus die Durchführung einer Block-Integritätsprüfung der SAP HANA Datenbank durch Ausführen eines dateibasierten Backups.

Die Datenbankprotokolle können mithilfe eines NFS-Mount-Speichers direkt auf dem sekundären Storage gesichert werden, wie in der folgenden Abbildung dargestellt.



Storage-basierte Snapshot Backups bieten im Vergleich zu herkömmlichen dateibasierten Backups deutliche Vorteile. Zu diesen Vorteilen zählen unter anderem die folgenden:

- Schnelleres Backup (einige Minuten)
- Reduzierte Recovery-Zeitvorgabe (Recovery Time Objective, RTO) aufgrund einer wesentlich schnelleren Restore-Zeit auf der Storage-Ebene (wenige Minuten) und häufigerer Backups
- Kein Performance-Abfall des SAP HANA-Datenbankhosts, -Netzwerks oder -Storage während Backup- und Recovery-Vorgängen
- Platzsparende und bandbreiteneffiziente Replizierung auf Basis von Blockänderungen auf sekundärem Storage

Weitere Informationen zur Backup- und Recovery-Lösung SAP HANA mit SnapCenter finden Sie unter "TR-4614: SAP HANA Backup and Recovery with SnapCenter".

Disaster Recovery für SAP HANA

SAP HANA Disaster Recovery kann mithilfe von SAP HANA-Systemreplizierung auf der Datenbankebene oder über Storage-Replizierungstechnologien auf der Storage-Ebene durchgeführt werden. Der folgende Abschnitt bietet einen Überblick über Disaster-Recovery-Lösungen basierend auf der Storage-Replizierung.

Weitere Informationen zu den Disaster-Recovery-Lösungen für SAP HANA finden Sie unter "TR-4646: SAP HANA Disaster Recovery with Storage Replication".

Storage-Replizierung basierend auf SnapMirror

Die folgende Abbildung zeigt eine Disaster-Recovery-Lösung für drei Standorte, die synchrone SnapMirror Replizierung in das lokale Disaster-Recovery-Datacenter und asynchrone SnapMirror zur Replizierung von Daten in das Remote Disaster Recovery-Datacenter verwendet.

Die Datenreplizierung mit synchronem SnapMirror sorgt für einen RPO von null. Die Entfernung zwischen dem primären und dem lokalen Disaster Recovery-Datacenter beträgt zirka 100 km.

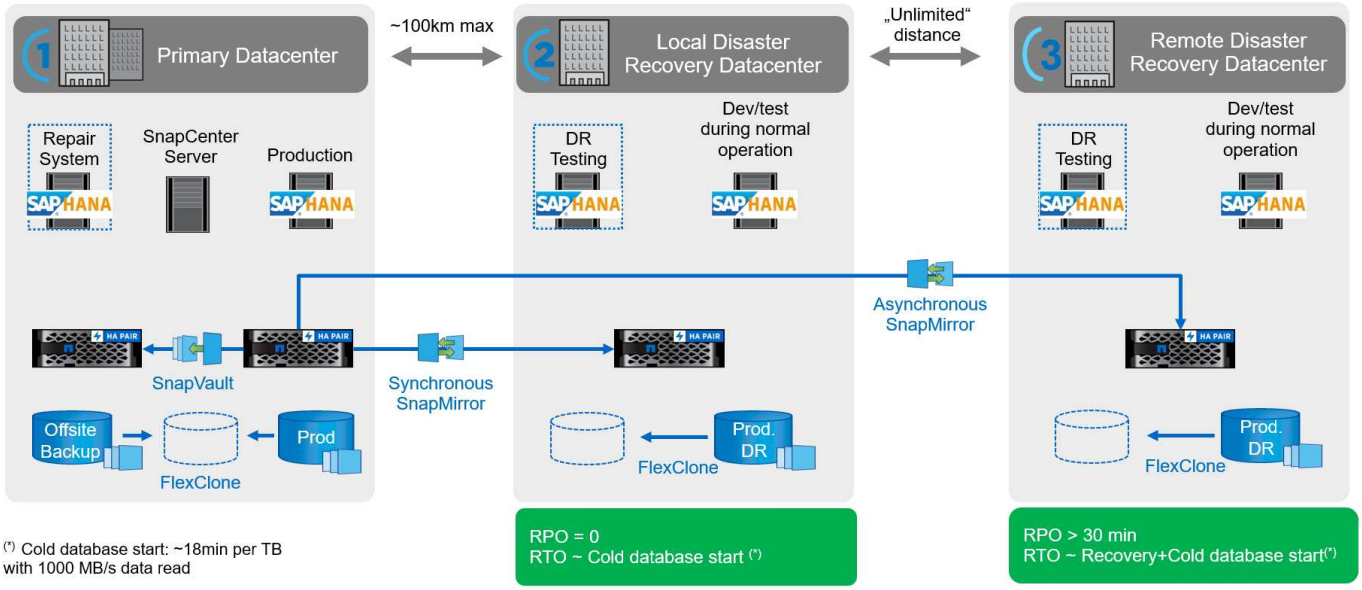
Der Schutz vor Ausfällen des primären und lokalen Disaster-Recovery-Standorts wird durch Replizieren der

Daten mithilfe von asynchronem SnapMirror zu einem dritten Disaster Recovery Datacenter durchgeführt. Der RPO hängt von der Häufigkeit der Replizierungs-Updates und der Übertragungsgeschwindigkeit ab. Theoretisch ist die Entfernung unbegrenzt, aber die Obergrenze hängt von der zu übertragenden Datenmenge und der zwischen den Rechenzentren verfügbaren Verbindung ab. Typische RPO-Werte liegen im Bereich von 30 Minuten bis mehreren Stunden.

Das RTO für beide Replizierungsmethoden hängt in erster Linie von der Zeit ab, die zum Starten der HANA-Datenbank am Disaster-Recovery-Standort und zum Laden der Daten in den Arbeitsspeicher benötigt wird. Mit der Annahme, dass die Daten mit einem Durchsatz von 1000 MBit/s gelesen werden, dass das Laden von 1 TB Daten ungefähr 18 Minuten dauert.

Die Server an den Disaster-Recovery-Standorten können als Entwicklungs-/Testsysteme im normalen Betrieb eingesetzt werden. Bei einem Ausfall müssten die Entwicklungs- und Testsysteme heruntergefahren und als Disaster Recovery-Produktionsserver gestartet werden.

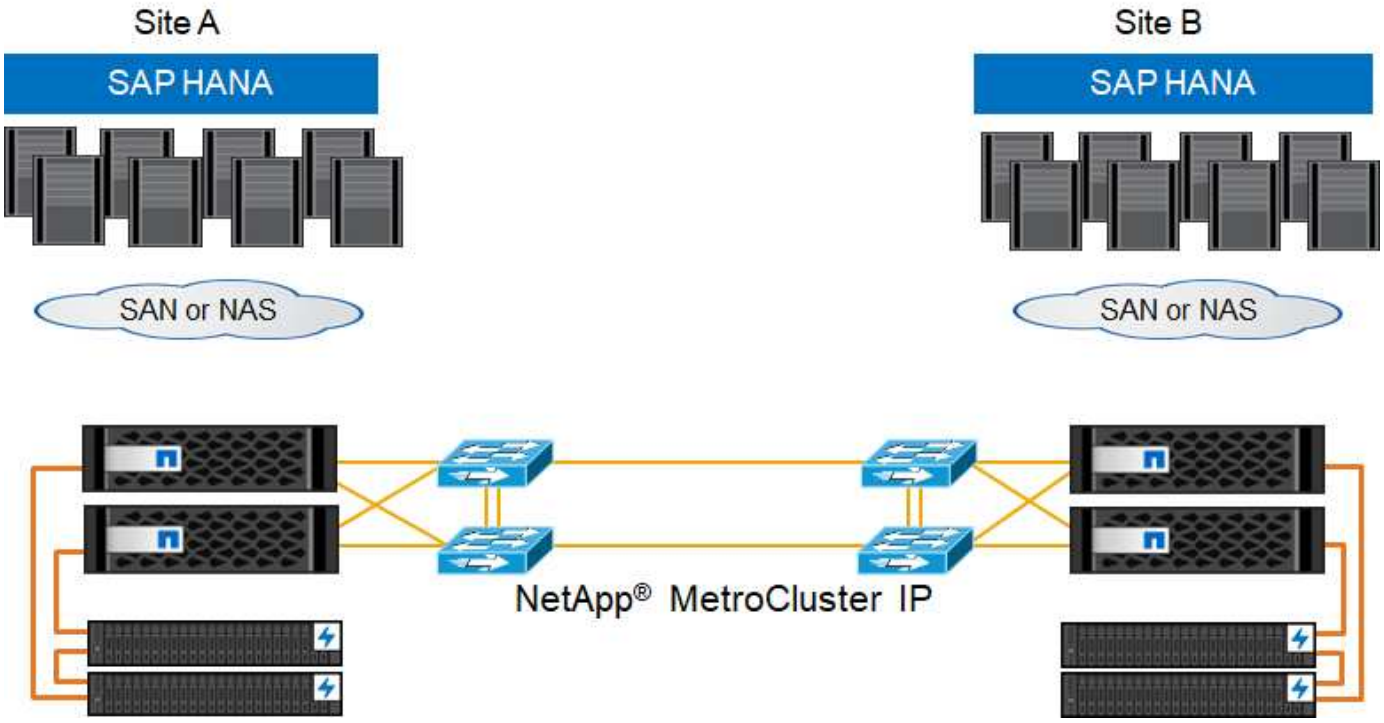
Beide Replizierungsmethoden ermöglichen die Durchführung von Disaster-Recovery-Workflow-Tests ohne Auswirkungen auf RPO und RTO. FlexClone Volumes werden auf dem Storage erstellt und an die Testserver von Disaster Recovery angeschlossen.



Die synchrone Replizierung bietet den StrictSync-Modus. Wenn der Schreibvorgang auf den sekundären Storage aus irgendeinem Grund nicht abgeschlossen wird, fällt der Applikations-I/O aus. Dadurch wird sichergestellt, dass die primären und sekundären Storage-Systeme identisch sind. Der Applikations-I/O zum primären Volume wird erst wieder fortgesetzt, nachdem die SnapMirror-Beziehung zum InSync-Status zurückkehrt. Falls der primäre Storage ausfällt, kann der Applikations-I/O nach dem Failover auf dem sekundären Storage fortgesetzt werden, ohne dass die Daten verloren gehen. Im StrictSync-Modus ist der RPO immer Null.

Storage-Replizierung basierend auf MetroCluster

Die folgende Abbildung bietet einen allgemeinen Überblick über die Lösung. Das Storage-Cluster an jedem Standort bietet lokale Hochverfügbarkeit und wird für den Produktions-Workload verwendet. Die Daten aller Standorte werden synchron zum anderen Standort repliziert und sind bei einem Disaster Failover verfügbar.



Storage-Dimensionierung

Der folgende Abschnitt bietet einen Überblick über die erforderlichen Performance- und Kapazitätsüberlegungen, die für die Dimensionierung eines Storage-Systems für SAP HANA erforderlich sind.

Wenden Sie sich an NetApp oder Ihren Vertriebsmitarbeiter von NetApp Partner, um Sie beim Aufbau einer Storage-Umgebung in einer passenden Größe zu unterstützen.

Überlegungen zur Performance

SAP hat einen statischen Satz von Storage-KPIs definiert, die für alle produktiven SAP HANA-Umgebungen gültig sind, unabhängig von der Speichergröße der Datenbank-Hosts und der Applikationen, die die SAP HANA-Datenbank nutzen. Diese KPIs gelten für Single-Host-, mehrere Hosts-, Business Suite on HANA-, Business Warehouse on HANA-, S/4HANA- und BW/4HANA-Umgebungen. Daher hängt der aktuelle Ansatz zur Performance-Dimensionierung nur von der Anzahl aktiver SAP HANA-Hosts ab, die an das Storage-System angeschlossen sind.

Storage-Performance-KPIs sind nur für SAP HANA Produktionssysteme erforderlich, können aber in allen HANA-Systemen implementiert werden.

SAP liefert ein Performance-Testtool, mit dem die Performance des Storage-Systems für aktive an den Storage angeschlossene SAP HANA Hosts validiert werden.

NetApp hat die maximale Anzahl an SAP HANA Hosts getestet und vordefiniert, die an ein bestimmtes Storage-Modell angeschlossen werden können, ohne dabei die erforderlichen Storage-KPIs von SAP für produktionsbasierte SAP HANA Systeme zu erfüllen.

Die Storage-Controller der zertifizierten FAS Produktfamilie können auch für SAP HANA mit anderen Festplattentypen oder Disk Back-End-Lösungen verwendet werden. Sie müssen jedoch von NetApp unterstützt werden und die Performance-KPIs von SAP HANA TDI erfüllen. Beispiele dafür sind NetApp Storage Encryption (NSE) und NetApp FlexArray Technologien.

In diesem Dokument wird die Festplattengröße für SAS-HDDs und Solid-State-Laufwerke (SSDs) beschrieben.

HDDs

Um die Storage-Performance-KPIs von SAP zu erfüllen, sind mindestens 10 Datenfestplatten (SAS mit 10.000 U/min) pro SAP HANA-Node erforderlich.

Diese Berechnung ist unabhängig vom verwendeten Storage Controller und Platten-Shelf sowie den Kapazitätsanforderungen der Datenbank. Das Hinzufügen weiterer Platten-Shelves erhöht nicht die maximale Anzahl von SAP HANA Hosts, die ein Storage-Controller unterstützen kann.

Solid State Drives

Bei SSDs wird die Anzahl an Datenfestplatten durch den Durchsatz der SAS-Verbindung von den Storage-Controllern zum SSD-Shelf bestimmt.

Mit dem SAP Performance-Test-Tool wurde die maximale Anzahl an SAP HANA-Hosts ermittelt, die in einem einzelnen Platten-Shelf ausgeführt werden können und die Mindestanzahl der pro SAP HANA-Host benötigten SSDs erforderlich ist. Dieser Test berücksichtigt nicht die tatsächlichen Storage-Kapazitätsanforderungen der Hosts. Zusätzlich müssen die Kapazitätsanforderungen berechnet werden, um die tatsächlich benötigte Storage-Konfiguration zu bestimmen.

- Das 12-GB-SAS-Festplatten-Shelf (DS224C) mit 24 SSDs unterstützt bis zu 14 SAP HANA-Hosts, wenn das Festplatten-Shelf mit 12 GB verbunden ist.
- Das 6 Gbit SAS-Platten-Shelf (DS2246) mit 24 SSDs unterstützt bis zu 4 SAP HANA Hosts.

Die SSDs und SAP HANA-Hosts müssen auf beide Storage-Controller verteilt sein.

In der folgenden Tabelle ist die unterstützte Anzahl von SAP HANA-Hosts pro Festplatten-Shelf zusammengefasst.

	6-Gbit-SAS-Shelfs (DS2246) mit voller Betriebslast 24 SSDs	12-GB-SAS-Shelfs (DS224C) mit 24 SSDs
Maximale Anzahl von SAP HANA-Hosts pro Festplatten-Shelf	4	14

Diese Berechnung erfolgt unabhängig vom eingesetzten Storage Controller. Das Hinzufügen weiterer Platten-Shelves erhöhen nicht die maximale Anzahl von SAP HANA Hosts, die ein Storage-Controller unterstützen kann.

Heterogenen Workloads

SAP HANA und andere Applikations-Workloads werden auf demselben Storage Controller oder im selben Storage-Aggregat unterstützt. Es ist jedoch eine NetApp Best Practice, SAP HANA-Workloads von allen anderen Applikations-Workloads zu trennen.

SAP HANA-Workloads und andere Applikations-Workloads können entweder auf demselben Storage-

Controller oder demselben Aggregat implementiert werden. Falls ja, müssen Sie sicherstellen, dass in der Umgebung mit heterogenen Workloads für SAP HANA eine ausreichende Performance verfügbar ist. NetApp empfiehlt außerdem, Parameter der Quality of Service (QoS) zu verwenden, um die Auswirkungen anderer Applikationen zu regulieren und einen Durchsatz für SAP HANA-Applikationen zu garantieren.

Das Performance-Testtool von SAP muss verwendet werden, um zu prüfen, ob zusätzliche SAP HANA Hosts auf einem vorhandenen Storage Controller ausgeführt werden können, der bereits für andere Workloads verwendet wird. SAP Applikations-Server können wie die SAP HANA Datenbanken sicher auf demselben Storage Controller und/oder Aggregat platziert werden.

Überlegungen zur Kapazität

Eine detaillierte Beschreibung der Kapazitätsanforderungen für SAP HANA ist im "SAP-Hinweis 1900823" Beigefügtes Whitepaper.

> ⓘ Das Kapazitätsdimensionieren der gesamten SAP Landschaft mit mehreren SAP HANA Systemen muss mithilfe von SAP HANA Storage-Größenanpassungs-Tools von NetApp ermittelt werden. Wenden Sie sich an NetApp oder Ihren Ansprechpartner bei NetApp Partnern, um den Prozess der Storage-Größenbemessung für eine ausreichend dimensionierte Storage-Umgebung zu validieren.

Konfiguration des Performance-Testtool

Ab SAP HANA 1.0 SPS10 führte SAP Parameter ein, um das I/O-Verhalten anzupassen und die Datenbank für das verwendete Datei- und Speichersystem zu optimieren. Diese Parameter müssen auch dann eingestellt werden, wenn die Speicherleistung mit dem SAP-Performance-Testtool getestet wird.

NetApp führte Performance-Tests durch, um die optimalen Werte zu ermitteln. In der folgenden Tabelle sind die Parameter aufgeführt, die in der Konfigurationsdatei des SAP-Performance-Testwerkzeugs festgelegt werden müssen.

Parameter	Wert
max_parallel_io_Requests	128
Async_read_Submit	Ein
Async_write_submit_Active	Ein
Async_Write_Submit_Blocks	Alle

Weitere Informationen zur Konfiguration des SAP-Testwerkzeugs finden Sie unter "SAP-Hinweis 1943937" Für HWCCT (SAP HANA 1.0) und "SAP-Hinweis 2493172" FÜR HCMT/HCOT (SAP HANA 2.0).

Das folgende Beispiel zeigt, wie Variablen für den HCMT/HCOT-Ausführungsplan festgelegt werden können.

```
…{
          "Comment": "Log Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "LogAsyncReadSubmit",
          "Value": "on",
          "Request": "false"
      },
```

```
      {
         "Comment": "Data Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
         "Name": "DataAsyncReadSubmit",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "LogAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "DataAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "LogAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "DataAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "LogExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Maximum number of parallel I/O requests
```

```
per completion queue",
          "Name": "DataExtMaxParallelIoRequests",
          "Value": "128",
          "Request": "false"
       }, …
```

Diese Variablen müssen für die Testkonfiguration verwendet werden. Dies ist in der Regel bei den vordefinierten Testsuiten der Fall, die SAP mit dem HCMT/HCOT-Tool liefert. Das folgende Beispiel für einen 4k-Protokollschreibtest stammt aus einer Testsuite.

```
…
      {
         "ID": "D664D001-933D-41DE-A904F304AEB67906",
         "Note": "File System Write Test",
         "ExecutionVariants": [
            {
               "ScaleOut": {
                  "Port": "${RemotePort}",
                  "Hosts": "${Hosts}",
                  "ConcurrentExecution": "${FSConcurrentExecution}"
               },
               "RepeatCount": "${TestRepeatCount}",
               "Description": "4K Block, Log Volume 5GB, Overwrite",
               "Hint": "Log",
               "InputVector": {
                  "BlockSize": 4096,
                  "DirectoryName": "${LogVolume}",
                  "FileOverwrite": true,
                  "FileSize": 5368709120,
                  "RandomAccess": false,
                  "RandomData": true,
                  "AsyncReadSubmit": "${LogAsyncReadSubmit}",
                  "AsyncWriteSubmitActive":
"${LogAsyncWriteSubmitActive}",
                  "AsyncWriteSubmitBlocks":
"${LogAsyncWriteSubmitBlocks}",
                  "ExtMaxParallelIoRequests":
"${LogExtMaxParallelIoRequests}",
                  "ExtMaxSubmitBatchSize": "${LogExtMaxSubmitBatchSize}",
                  "ExtMinSubmitBatchSize": "${LogExtMinSubmitBatchSize}",
                  "ExtNumCompletionQueues":
"${LogExtNumCompletionQueues}",
                  "ExtNumSubmitQueues": "${LogExtNumSubmitQueues}",
                  "ExtSizeKernelIoQueue": "${ExtSizeKernelIoQueue}"
               }
            }, …
```

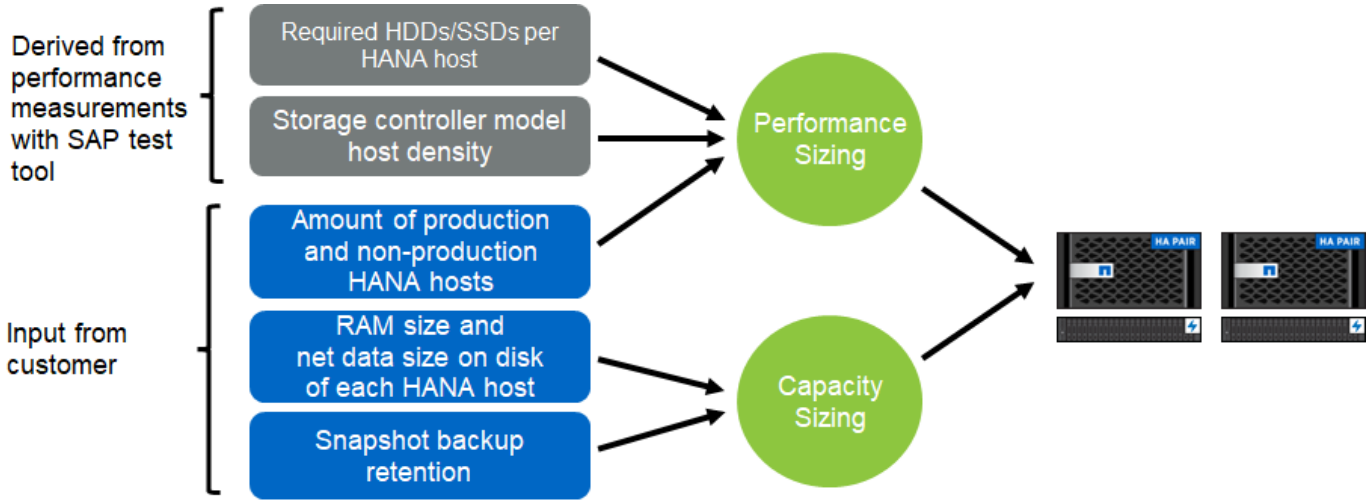
Übersicht über den Prozess zur Storage-Größenbemessung

Die Anzahl der Festplatten pro HANA Host und die SAP HANA Host-Dichte für jedes Storage-Modell wurden mit dem Performance-Testtool von SAP ermittelt.

Der Dimensionierungsprozess erfordert Einzelheiten, z. B. die Anzahl der SAP HANA-Hosts in der Produktion und für die Produktion nichtproduktive Umgebung, die RAM-Größe jedes Hosts und die Backup-Aufbewahrung der Storage-basierten Snapshot Kopien. Die Anzahl der SAP HANA-Hosts bestimmt den Storage Controller und die Anzahl der benötigten Festplatten.

Die Größe des RAM, die Netto-Datengröße auf der Festplatte jedes SAP HANA-Hosts und der Aufbewahrungszeitraum für das Snapshot-Backup werden als Inputs bei der Kapazitätsdimensionierung verwendet.

Die folgende Abbildung fasst den Dimensionierungsprozess zusammen.



Einrichtung und Konfiguration der Infrastruktur

Netzwerkeinrichtung

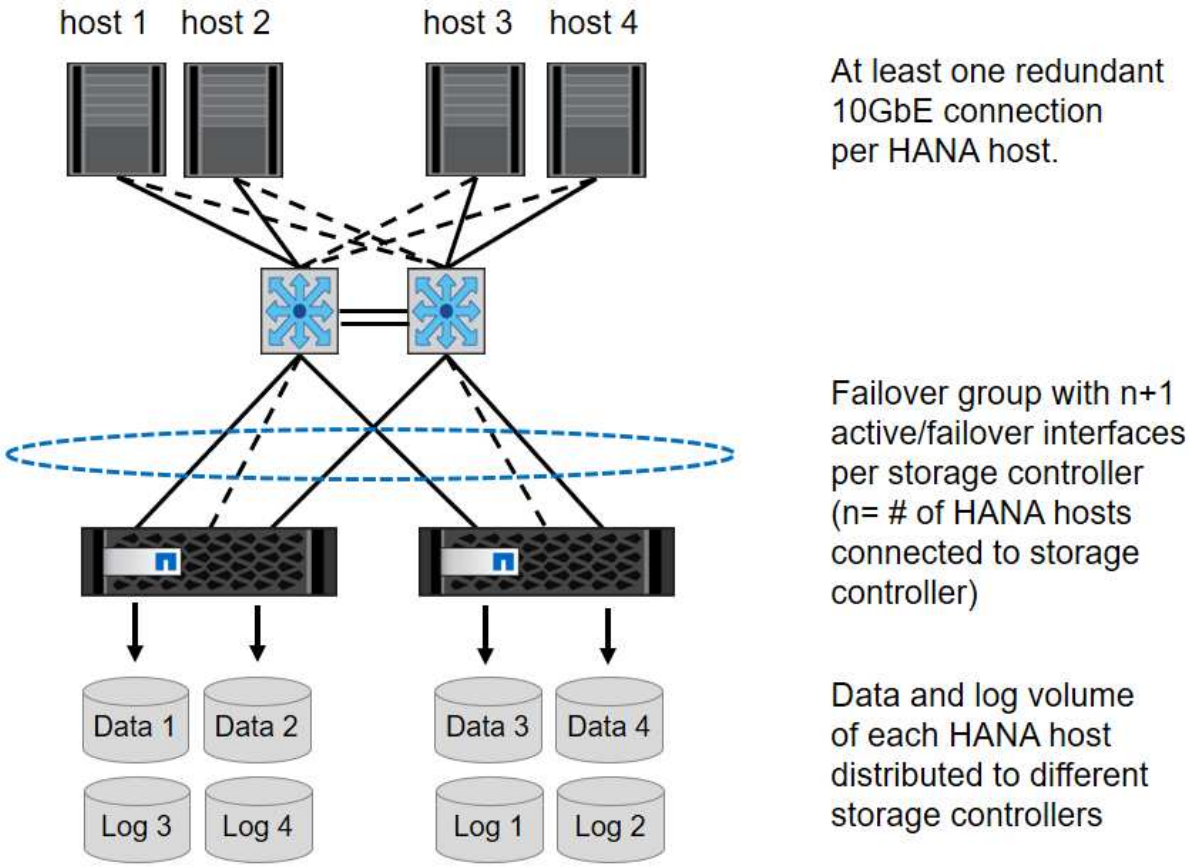
Beachten Sie bei der Konfiguration des Netzwerks die folgenden Richtlinien:

- Um die SAP HANA-Hosts mit den Storage-Controllern über ein 10-GbE- oder schnelleres Netzwerk zu verbinden, muss ein dediziertes Storage-Netzwerk verwendet werden.
- Verwenden Sie dieselbe Verbindungsgeschwindigkeit für Storage Controller und SAP HANA Hosts. Ist dies nicht möglich, stellen Sie sicher, dass die Netzwerkkomponenten zwischen den Storage Controllern und den SAP HANA Hosts unterschiedliche Geschwindigkeiten verarbeiten können. Beispielsweise müssen Sie genügend Puffer bereitstellen, um eine Geschwindigkeitsverhandlung auf NFS-Ebene zwischen Storage und Hosts zu ermöglichen. Netzwerkkomponenten sind normalerweise Switches, aber andere Komponenten innerhalb des Blade-Chassis, wie z. B. die Rückebene, müssen ebenfalls in Betracht gezogen werden.
- Deaktivieren Sie die Flusssteuerung bei allen physischen Ports, die für den Storage-Verkehr auf dem Storage-Netzwerk-Switch und der Host-Ebene verwendet werden.
- Jeder SAP HANA-Host muss über eine redundante Netzwerkverbindung mit mindestens 10 GB Bandbreite verfügen.
- Jumbo-Frames mit einer Maximum Transmission Unit (MTU) von 9,000 müssen auf allen Netzwerkkomponenten zwischen den SAP HANA-Hosts und den Storage Controllern aktiviert werden.
- In einer VMware Einrichtung müssen jeder laufenden virtuellen Maschine dedizierte VMXNET3 Netzwerkadapter zugewiesen werden. Weitere Anforderungen finden Sie in den entsprechenden Papieren, die im aufgeführt "Einführung"sind.
- Verwenden Sie für den Protokoll- und Datenbereich separate Netzwerk-/E/A-Pfade, um Interferenzen zwischen den beiden zu vermeiden.

Die folgende Abbildung zeigt ein Beispiel mit vier SAP HANA-Hosts, die über ein 10-GbE-Netzwerk an ein HA-Paar des Storage-Controllers angeschlossen sind. Jeder SAP HANA-Host besitzt eine aktiv/Passiv-Verbindung zur redundanten Fabric.

Auf der Storage-Ebene sind vier aktive Verbindungen so konfiguriert, dass sie für jeden SAP HANA Host einen 10-GB-Durchsatz bereitstellen. Zudem ist auf jedem Storage Controller eine Spare-Schnittstelle konfiguriert.

Auf Storage-Ebene wird eine Broadcast-Domäne mit einer MTU-Größe von 9000 konfiguriert und dieser Broadcast-Domäne werden alle erforderlichen physischen Schnittstellen hinzugefügt. Bei diesem Ansatz werden diese physischen Schnittstellen automatisch derselben Failover-Gruppe zugewiesen. Alle logischen Schnittstellen (LIFs), die diesen physischen Schnittstellen zugewiesen sind, werden dieser Failover-Gruppe hinzugefügt.



Im Allgemeinen ist es auch möglich, HA-Interface-Gruppen auf den Servern (Bonds) und den Storage-Systemen zu verwenden (z. B. Link Aggregation Control Protocol [LACP] und ifgroups). Vergewissern Sie sich bei HA-Schnittstellengruppen, dass die Last gleichmäßig auf alle Schnittstellen innerhalb der Gruppe verteilt ist. Die Lastverteilung hängt von der Funktionalität der Netzwerk-Switch-Infrastruktur ab.

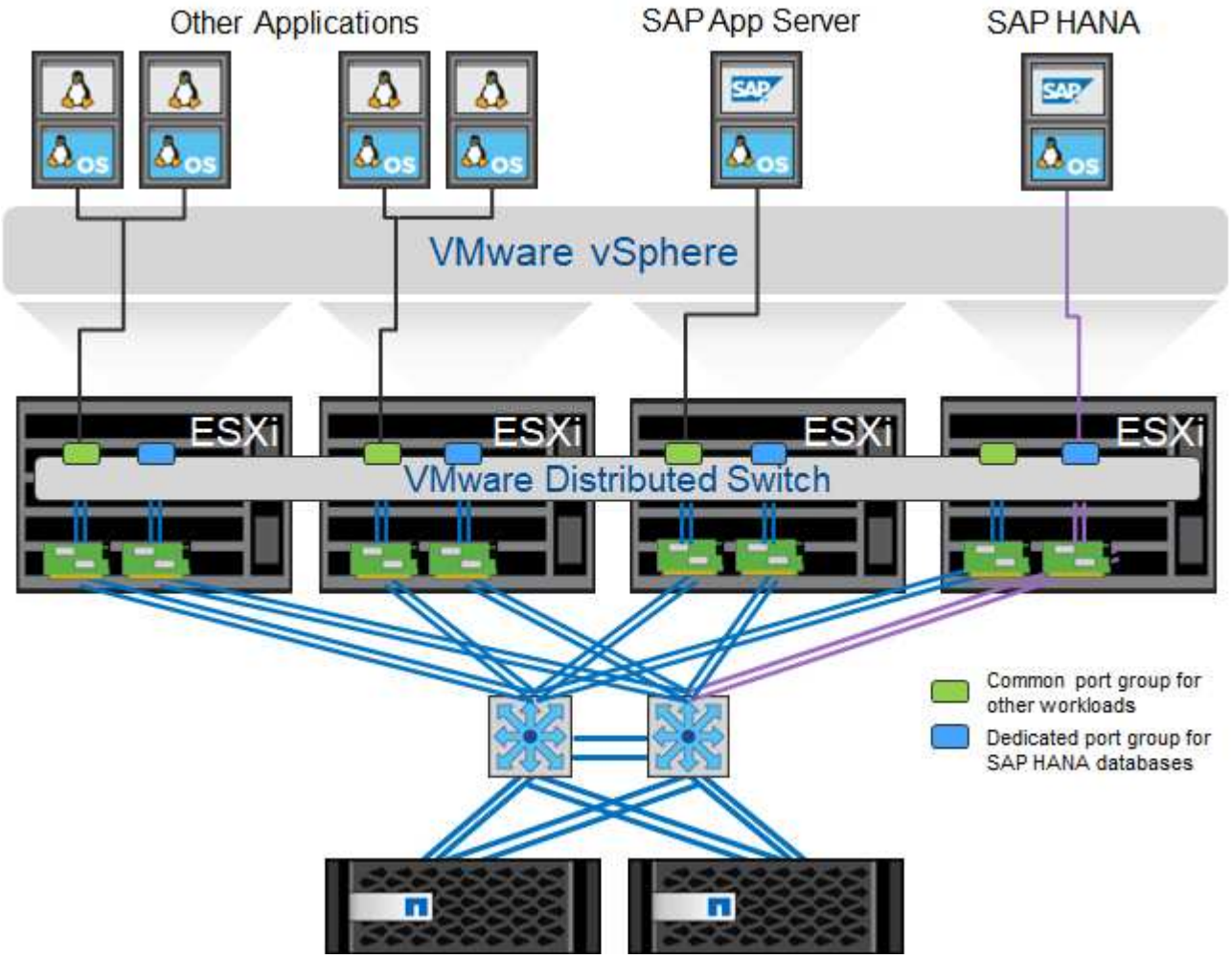
Abhängig von der Anzahl der SAP HANA-Hosts und der verwendeten Verbindungsgeschwindigkeit sind unterschiedliche Anzahl aktiver physischer Ports erforderlich.

VMware-spezifische Netzwerk-Einrichtung

Da in dieser Lösung alle Daten für SAP HANA Instanzen, einschließlich Performance-kritischer Daten und Protokoll-Volumes für die Datenbank, über NFS bereitgestellt werden, ist ein angemessenes Netzwerkdesign und entsprechende Konfiguration von entscheidender Bedeutung. Über ein dediziertes Storage-Netzwerk wird der NFS-Traffic von der Kommunikation und der Datenverkehr mit Benutzerzugriffsrechten zwischen SAP HANA-Knoten getrennt. Jeder SAP HANA Node benötigt eine redundante, dedizierte Netzwerkverbindung mit mindestens 10 GB Bandbreite. Es wird auch eine höhere Bandbreite unterstützt. Dieses Netzwerk muss sich End-to-End von der Storage-Ebene über Netzwerk-Switching und Computing bis hin zum auf VMware vSphere

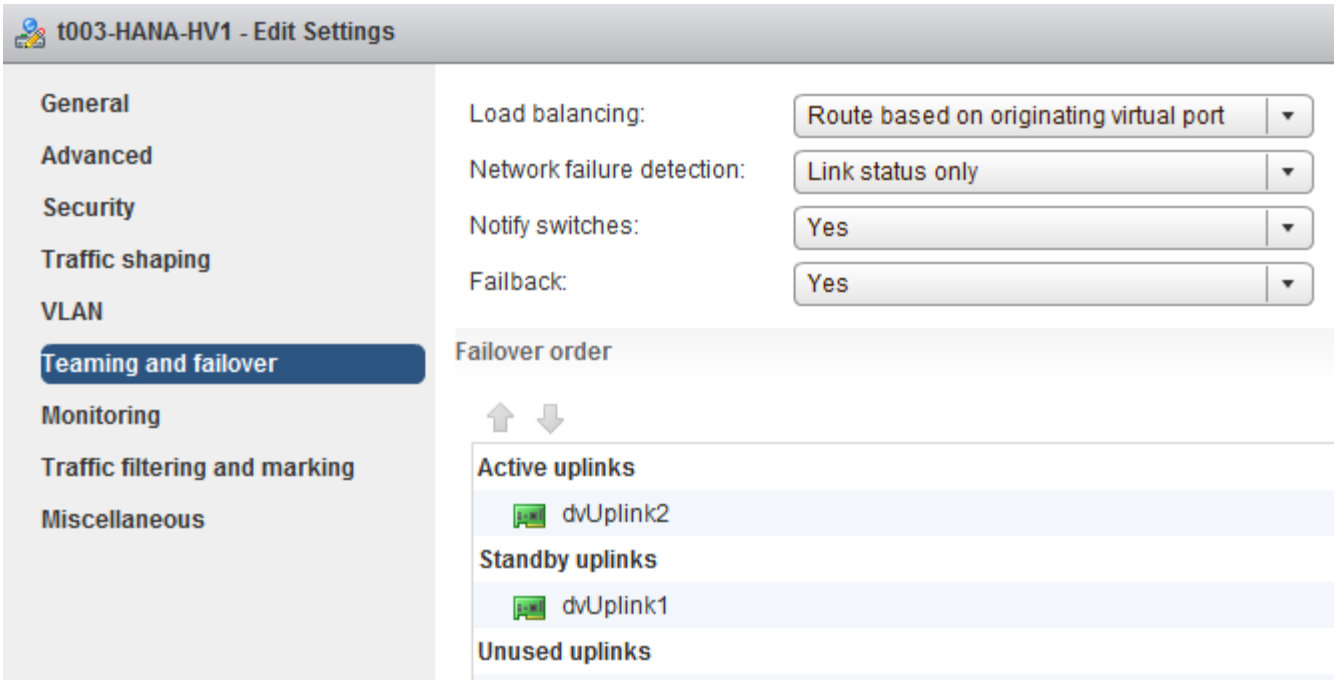
gehosteten Gastbetriebssystem erstrecken. Neben der physischen Switching-Infrastruktur wird ein VMware Distributed Switch (VdS) eingesetzt, um eine ausreichende Performance und Managebarkeit des Netzwerkverkehrs auf der Hypervisor-Ebene zu gewährleisten.

Die folgende Abbildung bietet einen Netzwerküberblick.



Jeder SAP HANA Node verwendet eine dedizierte Portgruppe auf dem VMware Distributed Switch. Diese Port-Gruppe ermöglicht eine verbesserte Servicequalität (QoS) und eine dedizierte Zuweisung von physischen Netzwerkkarten (NICs) auf den ESX Hosts. Um dedizierte physische NICs zu verwenden und gleichzeitig HA-Funktionen bei einem NIC-Ausfall zu erhalten, wird die dedizierte physische NIC als aktiver Uplink konfiguriert. Zusätzliche NICs werden in den Teaming- und Failover-Einstellungen der SAP HANA-Portgruppe als Standby-Uplinks konfiguriert. Darüber hinaus müssen Jumbo Frames (MTU 9,000) End-to-End-aktiviert sein, auf physischen und virtuellen Switches. Deaktivieren Sie darüber hinaus die Flusskontrolle bei allen ethernet-Ports, die für den Storage-Datenverkehr bei Servern, Switches und Storage-Systemen verwendet werden. Die folgende Abbildung zeigt ein Beispiel für eine solche Konfiguration.

LRO (Large Receive Offload) muss für Schnittstellen deaktiviert werden, die für NFS Traffic verwendet werden. Alle anderen Richtlinien zur Netzwerkkonfiguration finden Sie im entsprechenden VMware Best Practices Guide für SAP HANA.



Zeitsynchronisierung

Sie müssen die Zeit zwischen den Storage-Controllern und den SAP HANA Datenbank-Hosts synchronisieren. Legen Sie dazu denselben Zeitserver für alle Storage Controller und alle SAP HANA-Hosts fest.

Einrichtung von Storage Controllern

In diesem Abschnitt wird die Konfiguration des NetApp Storage-Systems beschrieben. Sie müssen die primäre Installation und Einrichtung gemäß den entsprechenden ONTAP Setup- und Konfigurationsleitfäden abschließen.

Storage-Effizienz

Inline-Deduplizierung, Inline-Deduplizierung, Inline-Komprimierung und Inline-Data-Compaction werden von SAP HANA in einer SSD-Konfiguration unterstützt.

Die Aktivierung von Storage-Effizienzfunktionen in einer HDD-basierten Konfiguration wird nicht unterstützt.

NetApp FlexGroup Volumes

Die Verwendung von NetApp FlexGroup Volumes wird für SAP HANA nicht unterstützt. Aufgrund der Architektur von SAP HANA bietet die Verwendung von FlexGroup Volumes keinen Vorteil und kann zu Performance-Problemen führen.

NetApp Volume- und Aggregatverschlüsselung

Die Verwendung von NetApp Volume Encryption (NVE) und NetApp Aggregate Encryption (NAE) wird bei SAP HANA unterstützt.

Um Servicequalität bieten zu können

Mit QoS lässt sich der Storage-Durchsatz für bestimmte SAP HANA Systeme oder andere Applikationen auf einem gemeinsam genutzten Controller begrenzen. Ein Anwendungsfall wäre, den Durchsatz von Entwicklungs- und Testsystemen zu begrenzen, damit sie bei einem gemischten Setup keinen Einfluss auf die Produktionssysteme haben.

Während des Dimensionierungsprozesses sollten Sie die Performance-Anforderungen eines nicht für die Produktion verwendeten Systems ermitteln. Entwicklungs- und Testsysteme können mit niedrigeren Leistungswerten dimensioniert werden, typischerweise im Bereich von 20 % bis 50 % eines von SAP definierten Produktionssystems-KPI.

Ab ONTAP 9 wird QoS auf Storage-Volume-Ebene konfiguriert und verwendet maximale Werte für Durchsatz (MB/s) und I/O-Menge (IOPS).

Ein großer I/O-Schreibvorgang wirkt sich am stärksten auf die Performance des Storage-Systems aus. Daher sollte die QoS-Durchsatzbegrenzung auf einen Prozentsatz der entsprechenden KPI-Werte für die SAP HANA-Speicherleistung in den Daten- und Protokoll-Volumes gesetzt werden.

NetApp FabricPool

NetApp FabricPool darf nicht für aktive primäre Filesysteme in SAP HANA Systemen verwendet werden. Dazu gehören die Dateisysteme für den Daten- und Protokollbereich sowie die `/hana/shared` File-System. Dies führt zu unvorhersehbarer Performance, insbesondere beim Start eines SAP HANA Systems.

Die Verwendung der „nur-Snapshots“ Tiering-Politik ist möglich sowie generell die Verwendung von FabricPool an einem Backup-Ziel wie einem SnapVault oder SnapMirror Ziel.

> ⓘ Durch die Verwendung von FabricPool für das Tiering von Snapshot Kopien im Primärspeicher oder die Verwendung von FabricPool zu einem Backup-Ziel werden die für die Wiederherstellung und das Recovery einer Datenbank oder anderer Aufgaben benötigte Zeit, beispielsweise das Erstellen von Systemklonen oder Korrektursystemen, geändert. Nehmen Sie dies bei der Planung Ihrer gesamten Lifecycle- Management-Strategie in Betracht und prüfen Sie, ob Ihre SLAs unter Verwendung dieser Funktion weiterhin erfüllt werden.

FabricPool ist eine gute Option, um Log-Backups auf eine andere Storage Tier zu verschieben. Das Verschieben von Backups beeinträchtigt die für das Recovery einer SAP HANA Datenbank erforderliche Zeit. Daher sollte die Option „Tiering-minimum-cooling-days“ auf einen Wert gesetzt werden, der Log-Backups, die routinemäßig für die Wiederherstellung benötigt werden, auf der lokalen fast Storage Tier platziert.

Storage-Konfiguration

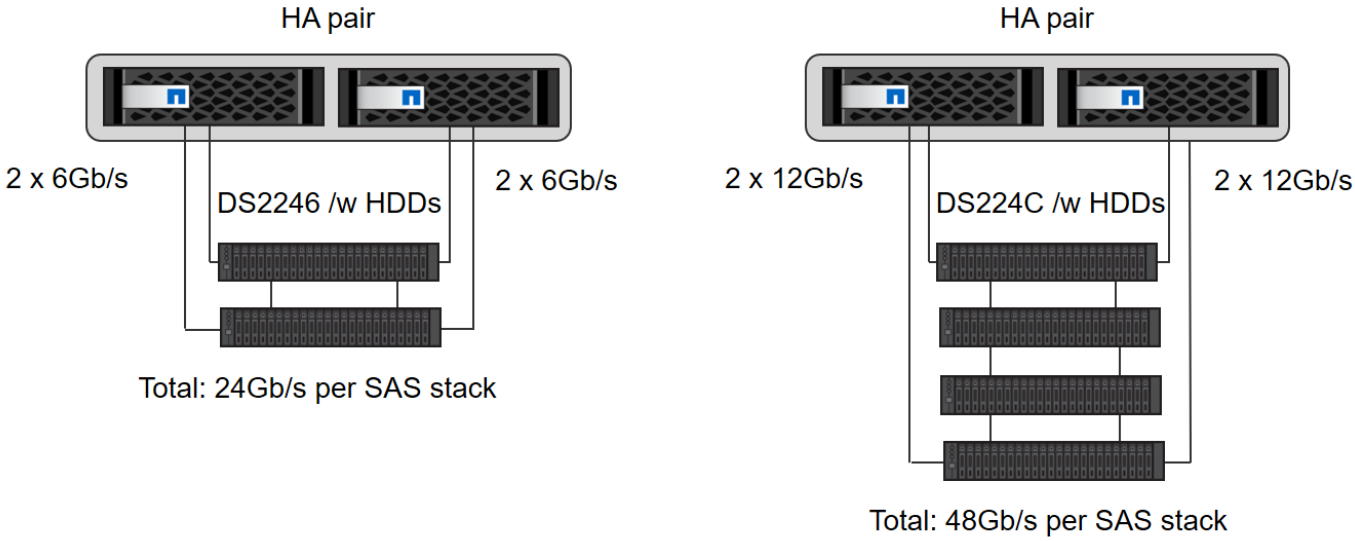
In der folgenden Übersicht sind die erforderlichen Schritte zur Storage-Konfiguration zusammengefasst. Jeder Schritt wird in den nachfolgenden Abschnitten näher beschrieben. In diesem Abschnitt wird die Storage-Hardware eingerichtet und die ONTAP Software bereits installiert. Außerdem müssen bereits die Verbindungen zwischen den Storage-Ports (10 GbE oder schneller) und dem Netzwerk vorhanden sein.

1. Überprüfen Sie die richtige SAS-Stack-Konfiguration, wie in beschrieben "Festplatten-Shelf-Verbindung."
2. Erstellen und konfigurieren Sie die erforderlichen Aggregate wie in beschrieben "Konfiguration von Aggregaten"
3. Erstellen Sie eine Storage Virtual Machine (SVM) wie in beschrieben "Konfiguration von Storage Virtual Machines"
4. Erstellen Sie LIFs wie in beschrieben "Konfiguration der logischen Schnittstelle:"

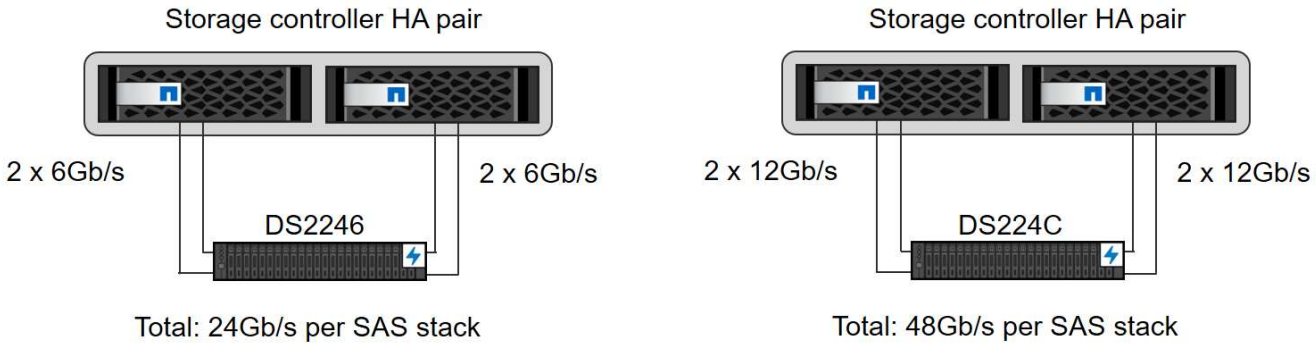
5. Erstellen Sie Volumes innerhalb der Aggregate, wie in und beschrieben "Volume-Konfiguration für SAP HANA Single-Host-Systeme""Volume-Konfiguration für SAP HANA Multiple-Host-Systeme."
6. Legen Sie die erforderlichen Volume-Optionen wie unter beschrieben fest "Volume-Optionen:"
7. Legen Sie die erforderlichen Optionen für NFSv3 fest, wie unter oder für NFSv4 beschrieben, wie unter beschrieben "NFS-Konfiguration für NFSv3""NFS-Konfiguration für NFSv4:"
8. Mounten Sie die Volumes im Namespace und legen Sie Exportrichtlinien fest, wie unter beschrieben "Volumes werden in Namespace mounten und Richtlinien für den Export festlegen."

Festplatten-Shelf-Verbindung

Mit HDDs können maximal zwei DS2246 Festplatten-Shelfs oder vier DS224C Festplatten-Shelfs mit einem SAS-Stack verbunden werden, um die erforderliche Performance für die SAP HANA-Hosts zu liefern, wie in der folgenden Abbildung dargestellt. Die Festplatten in jedem Shelf müssen gleichmäßig auf beide Controller des HA-Paars verteilt werden.

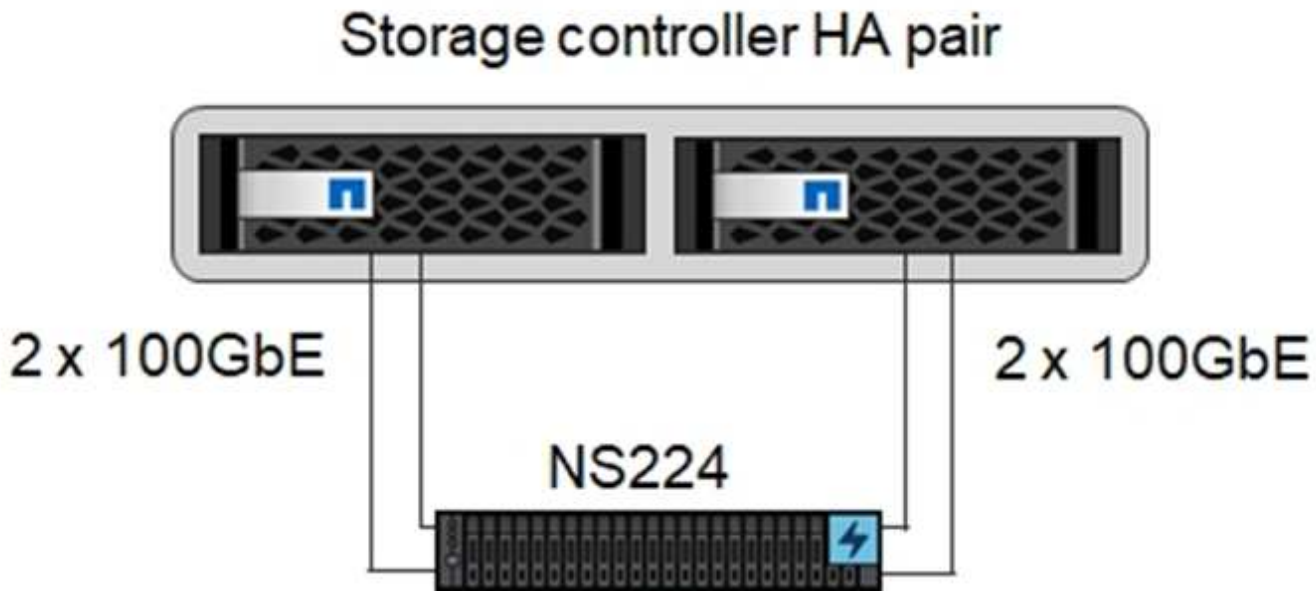


Bei SSDs kann maximal ein Platten-Shelf mit einem SAS-Stack verbunden werden, um die erforderliche Performance für die SAP HANA-Hosts zu liefern, wie in der folgenden Abbildung dargestellt. Die Festplatten in jedem Shelf müssen gleichmäßig auf beide Controller des HA-Paars verteilt werden. Mit dem DS224C Festplatten-Shelf können auch Quad-Path-SAS-Verkabelung verwendet werden, ist aber nicht erforderlich.



NVMe (100 GbE) Festplatten-Shelfs

Jedes NS224 NVMe-Festplatten-Shelf ist, wie in der folgenden Abbildung dargestellt, mit zwei 100-GbE-Ports pro Controller verbunden. Die Festplatten in jedem Shelf müssen gleichmäßig auf beide Controller des HA-Paars verteilt werden.

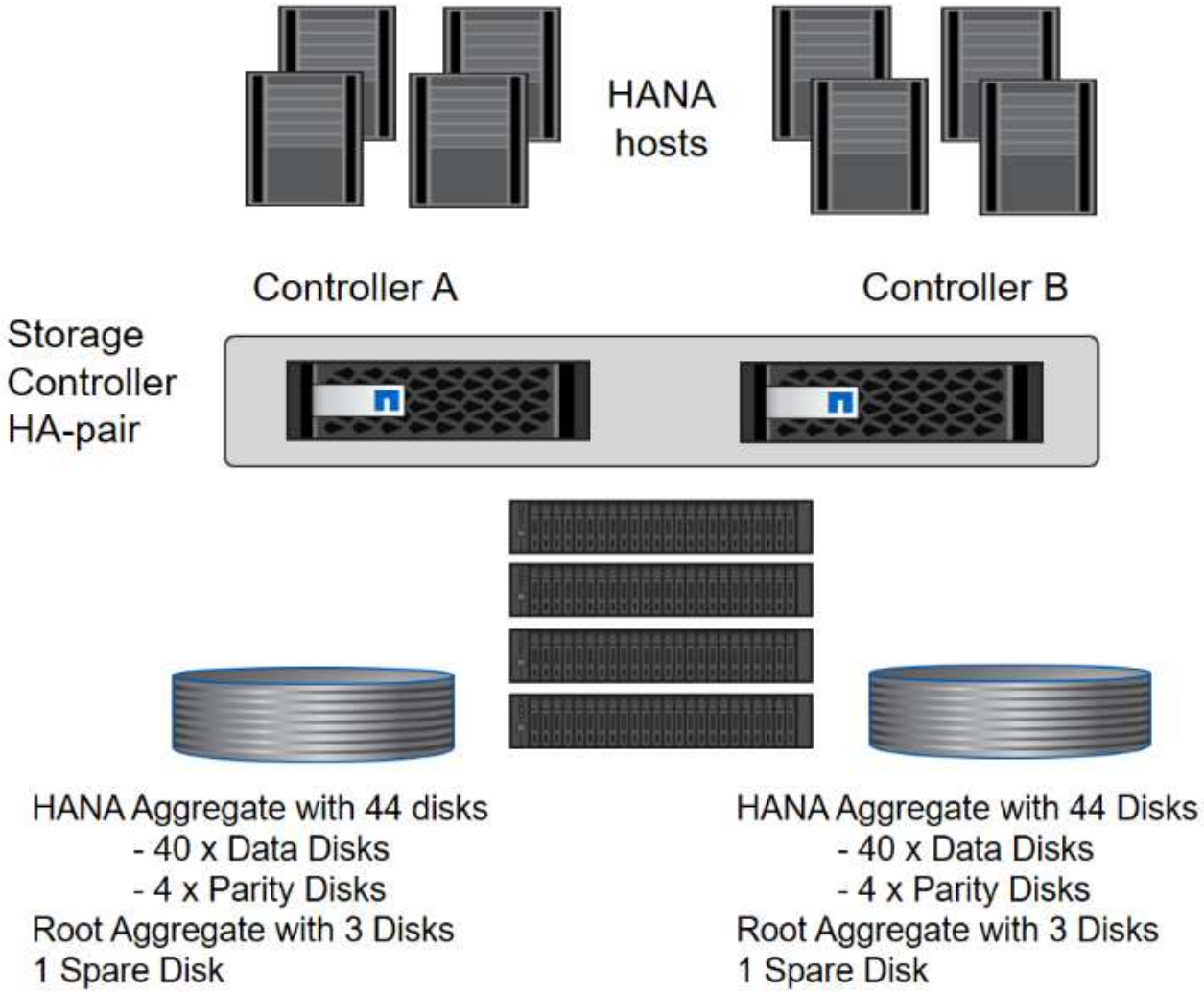


Konfiguration von Aggregaten

Im Allgemeinen müssen zwei Aggregate pro Controller konfiguriert werden, unabhängig vom verwendeten Festplatten-Shelf oder der Festplattentechnologie (SSD oder HDD). Für Systeme der FAS2000 Serie genügt ein Datenaggregat.

Aggregatkonfiguration mit HDDs

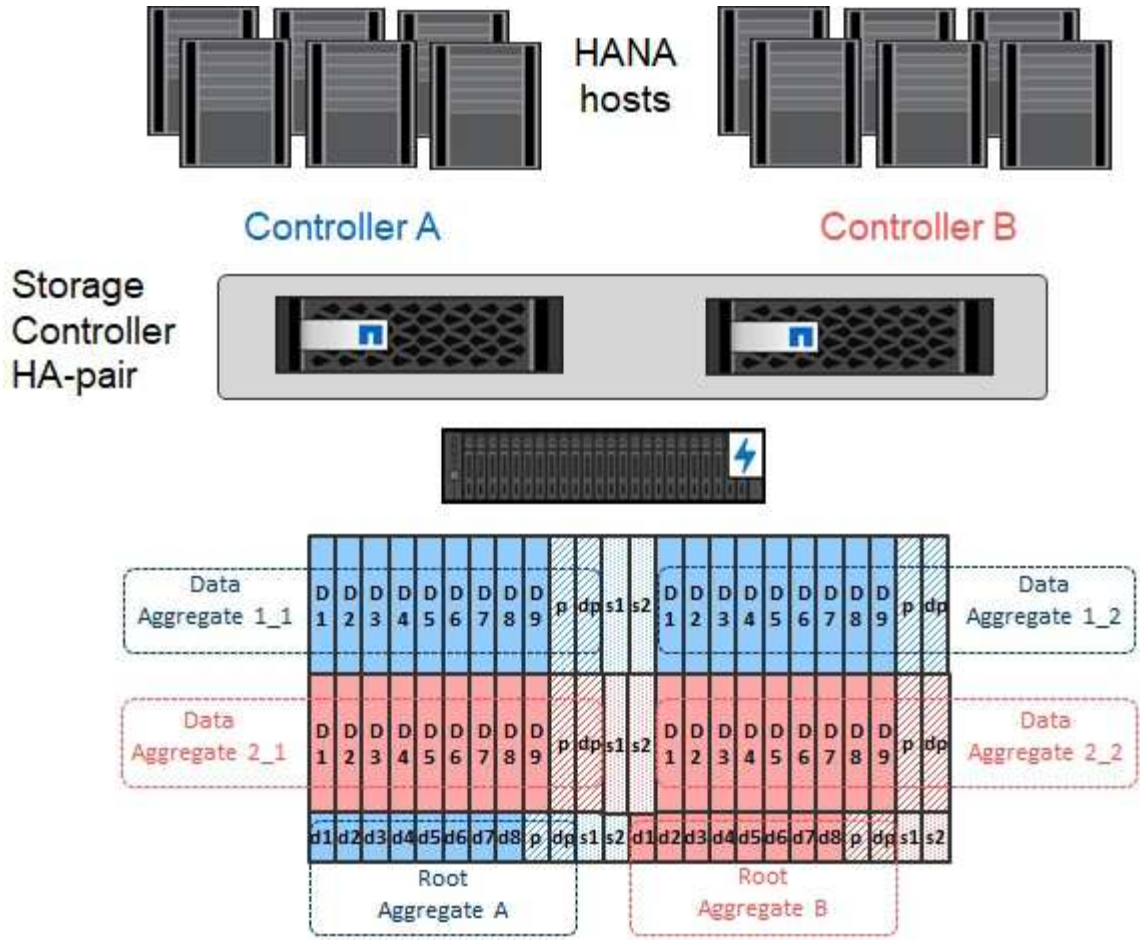
Die folgende Abbildung zeigt eine Konfiguration für acht SAP HANA-Hosts. Vier SAP HANA-Hosts sind mit jedem Storage-Controller verbunden. Zwei separate Aggregate, eines an jedem Storage Controller, sind konfiguriert. Jedes Aggregat ist mit 4 × 10 = 40 Datenfestplatten (HDDs) konfiguriert.



Aggregat-Konfiguration mit nur SDD-Systemen

Im Allgemeinen müssen zwei Aggregate pro Controller konfiguriert werden, unabhängig davon, welches Platten-Shelf oder Festplattentechnologie (SSDs oder HDDs) zum Einsatz kommt. Für Systeme der FAS2000 Serie genügt ein Datenaggregat.

Die folgende Abbildung zeigt eine Konfiguration mit 12 SAP HANA Hosts, die auf einem 12-GB-SAS-Shelf ausgeführt werden und mit ADPv2 konfiguriert sind. Sechs SAP-HANA-Hosts sind mit jedem Storage-Controller verbunden. Vier separate Aggregate, zwei an jedem Storage Controller, sind konfiguriert. Jedes Aggregat ist mit 11 Festplatten mit neun Daten und zwei Parity-Festplatten-Partitionen konfiguriert. Für jeden Controller stehen zwei Ersatzpartitionen zur Verfügung.



Konfiguration von Storage Virtual Machines

Mehrere SAP Landschaften mit SAP HANA Datenbanken können eine einzige SVM nutzen. Darüber hinaus kann jeder SAP-Landschaft bei Bedarf eine SVM zugewiesen werden, falls diese von verschiedenen Teams innerhalb eines Unternehmens gemanagt werden.

Wenn bei der Erstellung einer neuen SVM automatisch ein QoS-Profil erstellt und zugewiesen wurde, entfernen Sie das automatisch erstellte Profil aus der SVM, um die erforderliche Performance für SAP HANA bereitzustellen:

```
vserver modify -vserver <svm-name> -qos-policy-group none
```

Konfiguration der logischen Schnittstelle

Für SAP HANA Produktionssysteme müssen unterschiedliche LIFs zum Mounten des Daten-Volumes und des Protokoll-Volumes vom SAP HANA-Host verwendet werden. Daher sind mindestens zwei LIFs erforderlich.

Die Daten- und Protokoll-Volume-Mounts verschiedener SAP HANA Hosts können einen physischen Storage-Netzwerk-Port mithilfe derselben LIFs oder mithilfe individueller LIFs für jeden Mount gemeinsam nutzen.

Die maximale Anzahl an Daten- und Protokoll-Volume-Mounts pro physische Schnittstelle sind in der folgenden Tabelle aufgeführt.

Ethernet-Port-Geschwindigkeit	10 GbE	25 GbE	40 GbE	100 GeE
Maximale Anzahl an Protokoll- oder Daten-Volume-Mounts pro physischem Port	3	8	12	30

Die gemeinsame Nutzung einer logischen Schnittstelle zwischen verschiedenen SAP HANA Hosts erfordert möglicherweise eine Neuaufbindung von Daten- oder Protokoll-Volumes an eine andere logische Schnittstelle. Durch diese Änderung werden Performance-Einbußen vermieden, wenn ein Volume auf einen anderen Storage Controller verschoben wird.

Entwicklungs- und Testsysteme können mehr Daten und Volume-Mounts oder LIFs auf einer physischen Netzwerkschnittstelle verwenden.

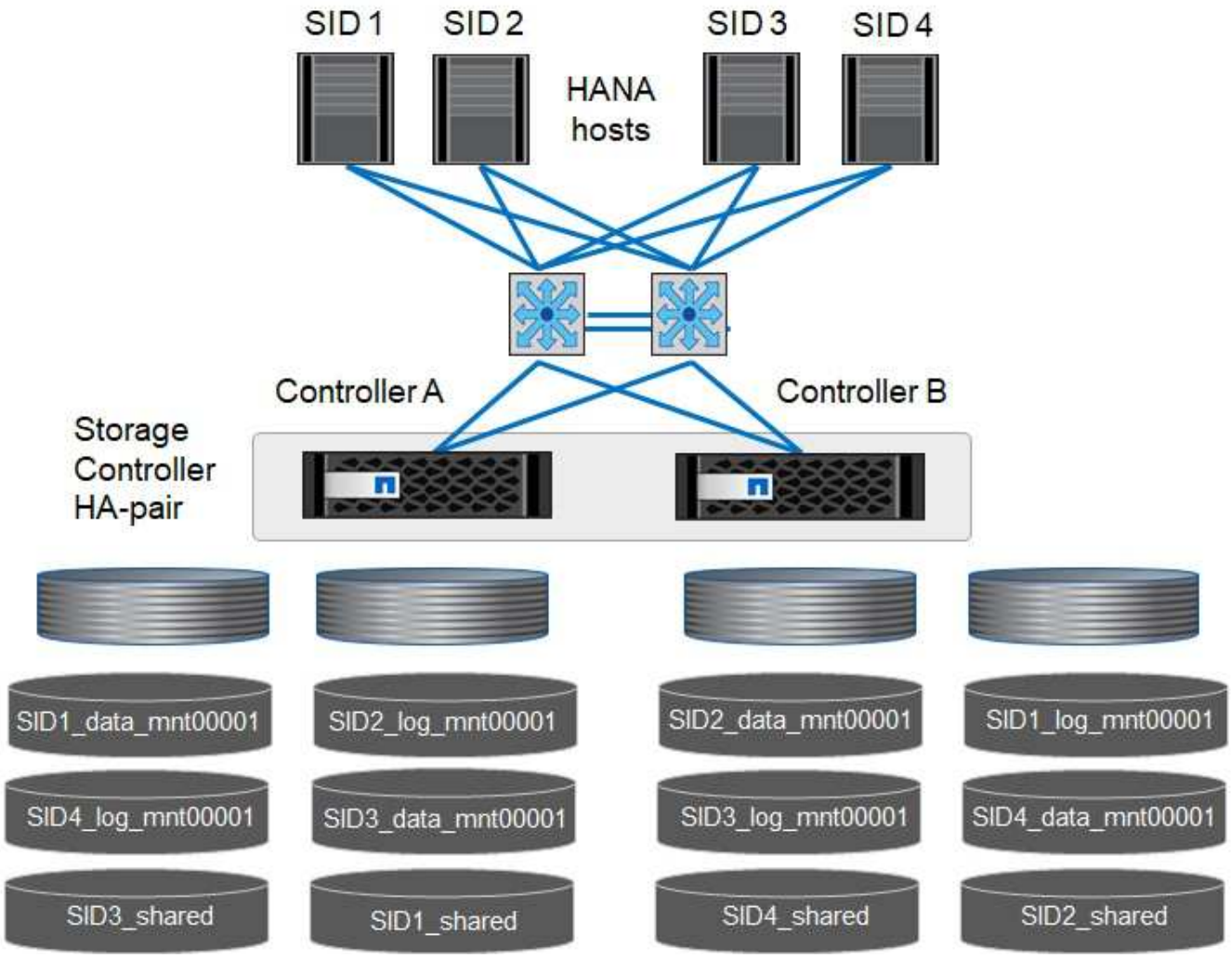
Für Produktions-, Entwicklungs- und Testsysteme liefert `/hana/shared` Das Filesystem kann dieselbe LIF wie das Daten- oder Protokoll-Volume verwenden.

Volume-Konfiguration für SAP HANA Single-Host-Systeme

Die folgende Abbildung zeigt die Volume-Konfiguration von vier SAP HANA-Systemen mit einem Host. Die Daten- und Protokoll-Volumes jedes SAP HANA Systems werden auf verschiedene Storage Controller verteilt. Beispiel: Volume `SID1_data_mnt00001` Wird auf Controller A und Volume konfiguriert `SID1_log_mnt00001` Ist auf Controller B konfiguriert

Wenn für die SAP HANA Systeme nur ein Storage-Controller eines HA-Paars verwendet wird, können Daten- und Protokoll-Volumes auch auf demselben Storage Controller gespeichert werden.

Wenn die Daten- und Protokoll-Volumes auf demselben Controller gespeichert sind, muss der Zugriff des Servers auf den Storage mit zwei unterschiedlichen LIFs durchgeführt werden: Einer logischen Schnittstelle für den Zugriff auf das Daten-Volume und einem für den Zugriff auf das Protokoll-Volume.



Für jeden SAP HANA DB-Host, ein Daten-Volume, ein Protokoll-Volume und ein Volume für `/hana/shared` Werden konfiguriert. Die folgende Tabelle zeigt eine Beispielkonfiguration für SAP HANA-Systeme mit einem Host.

Zweck	Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregat 2 bei Controller b
Daten-, Protokoll- und freigegebene Volumes für System SID1	Datenvolumen: SID1_Data_mnt00001	Freigegebenes Volume: SID1_Shared	–	Protokollvolumen: SID1_log_mnt00001
Daten-, Protokoll- und freigegebene Volumes für System SID2	–	Protokollvolumen: SID2_log_mnt00001	Datenvolumen: SID2_Data_mnt00001	Freigegebenes Volume: SID2_Shared
Daten-, Protokoll- und gemeinsam genutzte Volumes für System SID3	Gemeinsam genutztes Volume: SID3_shared	Datenvolumen: SID3_Data_mnt00001	Protokollvolumen: SID3_log_mnt00001	–

Zweck	Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregat 2 bei Controller b
Daten-, Protokoll- und gemeinsam genutzte Volumes für System SID4	Protokollvolumen: SID4_log_mnt00001	–	Gemeinsam genutztes Volume: SID4_shared	Datenvolumen: SID4_Data_mnt00001

Die folgende Tabelle zeigt ein Beispiel für die Mount-Point-Konfiguration für ein System mit einem einzelnen Host. Um das Home-Verzeichnis des zu platzieren `sidadm` Benutzer auf dem zentralen Speicher, der `/usr/sap/SID` Dateisystem sollte vom gemountet werden `SID_shared` Datenmenge:

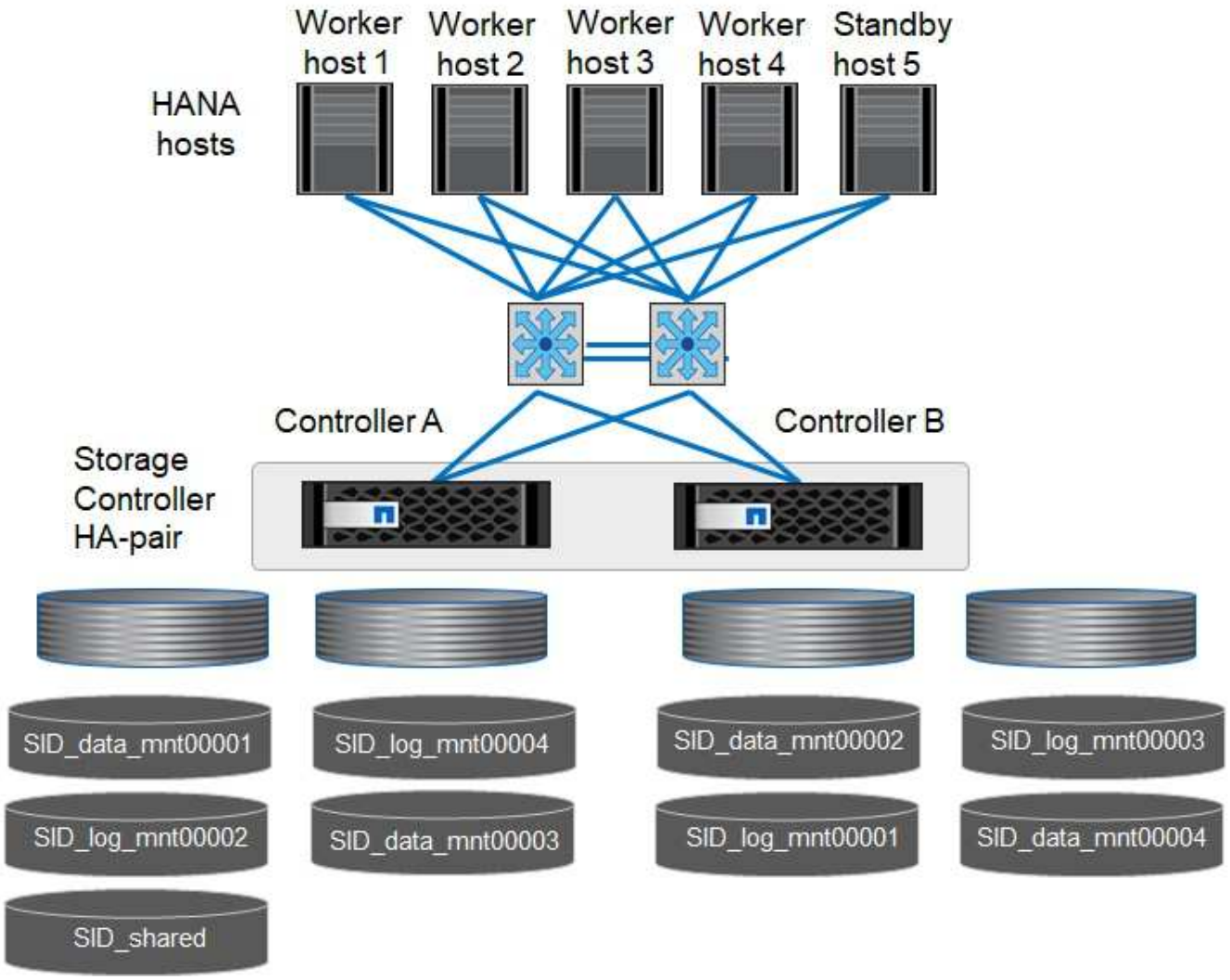
Verbindungspfad	Verzeichnis	Bereitstellungspunkt beim HANA-Host
SID_Data_mnt00001	–	/hana/Data/SID/mnt00001
SID_Log_mnt00001	–	/hana/log/SID/mnt00001
SID_freigegeben	Usr-sap freigegeben	/Usr/sap/SID /hana/Shared

Volume-Konfiguration für SAP HANA Multiple-Host-Systeme

Die folgende Abbildung zeigt die Volume-Konfiguration eines 4+1 SAP HANA-Systems. Die Daten- und Protokoll-Volumes jedes SAP HANA-Hosts werden auf verschiedene Storage-Controller verteilt. Beispiel: Volume `SID1_data1_mnt00001` Wird auf Controller A und Volume konfiguriert `SID1_log1_mnt00001` Ist auf Controller B konfiguriert

Wenn für das SAP HANA System nur ein Storage-Controller eines HA-Paars verwendet wird, können die Daten- und Protokoll-Volumes auch auf demselben Storage Controller gespeichert werden.

Wenn die Daten- und Protokoll-Volumes auf demselben Controller gespeichert sind, muss der Zugriff des Servers auf den Storage mit zwei verschiedenen LIFs durchgeführt werden: Einem für den Zugriff auf das Daten-Volume und einem für den Zugriff auf das Protokoll-Volume.



Für jeden SAP HANA-Host werden ein Daten-Volume und ein Protokoll-Volume erstellt. Der `/hana/shared` Das Volume wird von allen Hosts des SAP HANA-Systems verwendet. Die folgende Tabelle zeigt eine Beispielkonfiguration für ein SAP HANA-System mit mehreren Hosts und vier aktiven Hosts.

Zweck	Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregieren 2 bei Controller B
Daten- und Protokoll-Volumes für Node 1	Datenvolumen: SID_Data_mnt00001	–	Protokollvolumen: SID_log_mnt00001	–
Daten- und Protokoll-Volumes für Node 2	Protokollvolumen: SID_log_mnt002	–	Datenvolumen: SID_Data_mnt002	–
Daten- und Protokoll-Volumes für Node 3	–	Datenvolumen: SID_Data_mnt00003	–	Protokollvolumen: SID_log_mnt00003
Daten- und Protokoll-Volumes für Node 4	–	Protokollvolumen: SID_log_mnt004	–	Datenvolumen: SID_Data_mnt00004

Zweck	Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregieren 2 bei Controller B
Gemeinsames Volume für alle Hosts	Gemeinsam genutztes Volume: SID_shared	–	–	–

Die folgende Tabelle zeigt die Konfiguration und die Bereitstellungspunkte eines Systems mit mehreren Hosts mit vier aktiven SAP HANA Hosts. Um die Home-Verzeichnisse des zu platzieren `sidadm` Benutzer jedes Hosts im zentralen Speicher, der `/usr/sap/SID` Dateisysteme werden über eingebunden `SID_shared` Datenmenge:

Verbindungspfad	Verzeichnis	Bereitstellungspunkt beim SAP HANA-Host	Hinweis
SID_Data_mnt00001	–	/hana/Data/SID/mnt00001	Auf allen Hosts montiert
SID_Log_mnt00001	–	/hana/log/SID/mnt00001	Auf allen Hosts montiert
SID_Data_mnt00002	–	/hana/Data/SID/mnt002	Auf allen Hosts montiert
SID_Log_mnt00002	–	/hana/log/SID/mnt002	Auf allen Hosts montiert
SID_Data_mnt00003	–	/hana/Data/SID/mnt003	Auf allen Hosts montiert
SID_log_mnt00003	–	/hana/log/SID/mnt003	Auf allen Hosts montiert
SID_Data_mnt00004	–	/hana/Data/SID/mnt004	Auf allen Hosts montiert
SID_log_mnt00004	–	/hana/log/SID/mnt004	Auf allen Hosts montiert
SID_freigegeben	Freigegeben	/hana/Shared/	Auf allen Hosts montiert
SID_freigegeben	Usr-sap-host1	/Usr/sap/SID	Angehängt auf Host 1
SID_freigegeben	Usr-sap-host2	/Usr/sap/SID	Angehängt auf Host 2
SID_freigegeben	Usr-sap-host3	/Usr/sap/SID	Angehängt auf Host 3
SID_freigegeben	Usr-sap-host4	/Usr/sap/SID	Angehängt auf Host 4
SID_freigegeben	Usr-sap-host5	/Usr/sap/SID	Angehängt auf Host 5

Volume-Optionen

Sie müssen die in der folgenden Tabelle aufgeführten Volume-Optionen auf allen SVMs überprüfen und festlegen. Bei einigen Befehlen müssen Sie in den erweiterten Berechtigungsebene in ONTAP wechseln.

Aktion	Befehl
Deaktivieren Sie die Sichtbarkeit des Snapshot Verzeichnisses	vol modify -vserver <vserver-Name> -Volume <volname> -Snapdir-Access false
Deaktivieren Sie automatische Snapshot Kopien	vol modify –vserver <vserver-Name> -Volume <volname> -Snapshot-Policy keine
Deaktivieren Sie Updates der Zugriffszeit außer dem SID_Shared Volume	Setzen Sie Advanced vol modify -vserver <vserver-Name> -Volume <volname> -atime-Update false Administrator

NFS-Konfiguration für NFSv3

Die in der folgenden Tabelle aufgeführten NFS-Optionen müssen verifiziert und auf allen Storage Controllern eingestellt werden.

Für einige der angezeigten Befehle müssen Sie in den erweiterten Berechtigungsebene in ONTAP wechseln.

Aktion	Befehl
Aktivieren Sie NFSv3	nfs modify -vserver <vserver-Name> v3.0 aktiviert
Legen Sie die maximale NFS-TCP-Übertragungsgröße auf 1 MB fest	Erweitertes nfs modify -vserver <vserver_Name> -tcp -max-xfer-size 1048576 set admin

In gemeinsam genutzten Umgebungen mit unterschiedlichen Workloads wird die maximale NFS-TCP-Übertragungsgröße auf 262144 festgelegt

NFS-Konfiguration für NFSv4

Die in der folgenden Tabelle aufgeführten NFS-Optionen müssen verifiziert und auf allen SVMs eingestellt werden.

Bei einigen Befehlen müssen Sie in den erweiterten Berechtigungsebene in ONTAP wechseln.

Aktion	Befehl
Aktivieren Sie NFSv4	nfs modify -vserver <vserver-Name> -v4.1 aktiviert
Legen Sie die maximale NFS-TCP-Übertragungsgröße auf 1 MB fest	Erweitertes nfs modify -vserver <vserver_Name> -tcp -max-xfer-size 1048576 set admin
NFSv4-Zugriffssteuerungslisten (ACLs) deaktivieren	nfs modify -vserver <vServer_Name> -v4.1-acl deaktiviert
Legen Sie die NFSv4-Domain-ID fest	nfs modify -vServer <vServer_Name> -v4-id-Domain <Domain-Name>
Deaktivieren der NFSv4-Lesedelegierung	nfs modify -vServer <vServer_Name> -v4.1-read -Delegation deaktiviert
Deaktivieren der NFSv4-Schreibdelegation	nfs modify -vServer <vServer_Name> -v4.1-write -Delegation deaktiviert
Deaktivieren Sie die numerischen nfsv4-ids	nfs modify -vServer <vServer_Name> -v4-numeric-ids deaktiviert
Ändern Sie die Anzahl der NFSv4.x-Sitzungsplätze optional	Erweiterte Einstellungen nfs modify -vserver hana -v4.x-Session-num-slots <value> Legen Sie „Admin“ fest

In gemeinsam genutzten Umgebungen mit unterschiedlichen Workloads wird die maximale NFS-TCP-Übertragungsgröße auf 262144 festgelegt

Bitte beachten Sie, dass zur Deaktivierung von Nummerierung-ids eine Benutzerverwaltung erforderlich ist, wie unter beschrieben "Vorbereitung der Installation von SAP HANA auf NFSv4:"

Die NFSv4-Domänen-ID muss auf allen Linux-Servern () und SVMs, wie unter beschrieben, auf denselben Wert gesetzt werden /`etc/idmapd.conf`"Vorbereitung der Installation von SAP HANA auf NFSv4:"

PNFS kann aktiviert und verwendet werden.

Bei Einsatz von SAP HANA Systemen mit mehreren Hosts und automatischem Host-Failover müssen die Failover-Parameter innerhalb angepasst werden `nameserver.ini` Wie in der folgenden Tabelle dargestellt. Halten Sie das Standard-Wiederholungsintervall von 10 Sekunden in diesen Abschnitten ein.

Abschnitt in nameserver.ini	Parameter	Wert
Failover	Normal_Wiederholungen	9
Distributed_Watchdog	Deaktivierung_Wiederholungen	11
Distributed_Watchdog	Takeover_Wiederholungen	9

Volumes werden in Namespace mounten und Richtlinien für den Export festlegen

Wenn ein Volume erstellt wird, muss das Volume im Namespace gemountet werden. In diesem Dokument gehen wir davon aus, dass der Name des Verbindungspfads dem Namen des Volumes entspricht. Standardmäßig wird das Volume mit der Standardrichtlinie exportiert. Die Exportpolitik kann bei Bedarf angepasst werden.

Hosteinrichtung

Alle in diesem Abschnitt beschriebenen Schritte gelten sowohl für SAP HANA Umgebungen auf physischen Servern als auch für SAP HANA, die auf VMware vSphere ausgeführt werden.

Konfigurationsparameter für SUSE Linux Enterprise Server

Zusätzliche Kernel- und Konfigurationsparameter müssen bei jedem SAP HANA-Host an den von SAP HANA generierten Workload angepasst werden.

SUSE Linux Enterprise Server 12 und 15

Mit SUSE Linux Enterprise Server (SLES) 12 SP1 muss der Kernel-Parameter in einer Konfigurationsdatei im festgelegt werden `/etc/sysctl.d` Verzeichnis. Beispiel: Eine Konfigurationsdatei mit dem Namen `91-NetApp-HANA.conf` Muss erstellt werden.

```
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.ipv4.tcp_rmem = 4096 131072 16777216
net.ipv4.tcp_wmem = 4096 16384 16777216
net.core.netdev_max_backlog = 300000
net.ipv4.tcp_slow_start_after_idle = 0
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
sunrpc.tcp_max_slot_table_entries = 128
```

Saptune, das in SLES für SAP OS-Versionen enthalten ist, kann verwendet werden, um diese Werte festzulegen. Siehe "SAP-Hinweis 3024346" (SAP-Login erforderlich).

Konfigurationsparameter für Red hat Enterprise Linux 7.2 oder höher

Für den von SAP HANA generierten Workload müssen an jedem SAP HANA-Host zusätzliche Kernel- und Konfigurationsparameter angepasst werden.

Ab Red hat Enterprise Linux 7.2 müssen Sie die Kernel-Parameter in einer Konfigurationsdatei im festlegen `/etc/sysctl.d` Verzeichnis. Beispiel: Eine Konfigurationsdatei mit dem Namen `91-NetApp-HANA.conf` Muss erstellt werden.

```
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.ipv4.tcp_rmem = 4096 131072 16777216
net.ipv4.tcp_wmem = 4096 16384  16777216
net.core.netdev_max_backlog = 300000
net.ipv4.tcp_slow_start_after_idle = 0
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
sunrpc.tcp_max_slot_table_entries = 128
```

Seit RedHat Enterprise Linux Version 8.6 können diese Einstellungen auch mithilfe von RHEL System Roles for SAP (Ansible) angewendet werden. Siehe "SAP-Hinweis 3024346" (SAP-Login erforderlich).

Unterverzeichnisse in /hana/Shared-Volume erstellen

Die Beispiele zeigen eine SAP HANA-Datenbank mit SID=NF2.

Um die erforderlichen Unterverzeichnisse zu erstellen, führen Sie eine der folgenden Aktionen durch:

- Mounten Sie für ein Single-Host-System die `/hana/shared` Volume erstellen und die `shared` Und `usr-sap` Unterverzeichnisse

```
sapcc-hana-tst-06:/mnt # mount <storage-hostname>:/NF2_shared /mnt/tmp
sapcc-hana-tst-06:/mnt # cd /mnt/tmp
sapcc-hana-tst-06:/mnt/tmp # mkdir shared
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap
sapcc-hana-tst-06:mnt/tmp # cd ..
sapcc-hana-tst-06:/mnt # umount /mnt/tmp
```

- Mounten Sie für ein System mit mehreren Hosts die `/hana/shared` Volume erstellen und die `shared` Und das `usr-sap` Unterverzeichnisse für jeden Host.

  Die Beispielbefehle zeigen ein 2+1-HANA-System mit mehreren Hosts.

```
sapcc-hana-tst-06:/mnt # mount <storage-hostname>:/NF2_shared /mnt/tmp
sapcc-hana-tst-06:/mnt # cd /mnt/tmp
sapcc-hana-tst-06:/mnt/tmp # mkdir shared
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host1
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host2
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host3
sapcc-hana-tst-06:/mnt/tmp # cd ..
sapcc-hana-tst-06:/mnt # umount /mnt/tmp
```

Erstellen von Bereitstellungspunkten

Die Beispiele zeigen eine SAP HANA-Datenbank mit SID=NF2.

Um die erforderlichen Mount-Point-Verzeichnisse zu erstellen, führen Sie eine der folgenden Aktionen durch:

- Erstellen Sie für ein System mit einem einzelnen Host Mount Points und legen Sie die Berechtigungen für den Datenbank-Host fest.

```
sapcc-hana-tst-06:/ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-06:/ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-06:/ # mkdir -p /hana/shared
sapcc-hana-tst-06:/ # mkdir -p /usr/sap/NF2
sapcc-hana-tst-06:/ # chmod –R 777 /hana/log/NF2
sapcc-hana-tst-06:/ # chmod –R 777 /hana/data/NF2
sapcc-hana-tst-06:/ # chmod -R 777 /hana/shared
sapcc-hana-tst-06:/ # chmod -R 777 /usr/sap/NF2
```

- Erstellen Sie für ein System mit mehreren Hosts Mount-Punkte und legen Sie die Berechtigungen für alle Worker und Standby-Hosts fest.

  Die folgenden Beispielbefehle gelten für ein 2+1-HANA-System mit mehreren Hosts.

  - Erster Worker-Host:

```
sapcc-hana-tst-06:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-06:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-06:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-06:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-06:~ # mkdir -p /hana/shared
sapcc-hana-tst-06:~ # mkdir -p /usr/sap/NF2
sapcc-hana-tst-06:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-06:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-06:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-06:~ # chmod -R 777 /usr/sap/NF2
```

- Host zweiter Arbeiter:

```
sapcc-hana-tst-07:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-07:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-07:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-07:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-07:~ # mkdir -p /hana/shared
sapcc-hana-tst-07:~ # mkdir -p /usr/sap/NF2
sapcc-hana-tst-07:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-07:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-07:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-07:~ # chmod -R 777 /usr/sap/NF2
```

- Standby-Host:

```
sapcc-hana-tst-08:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-08:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-08:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-08:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-08:~ # mkdir -p /hana/shared
sapcc-hana-tst-08:~ # mkdir -p /usr/sap/NF2
sapcc-hana-tst-08:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-08:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-08:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-08:~ # chmod -R 777 /usr/sap/NF2
```

Mounten Sie File-Systeme

Abhängig von der NFS Version und der ONTAP Version werden verschiedene Mount-Optionen verwendet. Die folgenden Filesysteme müssen an die Hosts angehängt werden:

- `/hana/data/SID/mnt0000*`
- `/hana/log/SID/mnt0000*`
- `/hana/shared`
- `/usr/sap/SID`

In der folgenden Tabelle werden die NFS-Versionen aufgeführt, die für die verschiedenen Filesysteme für SAP HANA Datenbanken mit einem oder mehreren Hosts verwendet werden müssen.

File-Systeme	SAP HANA einzelner Host	SAP HANA mehrere Hosts
/hana/Data/SID/mnt0000*	NFSv3 oder NFSv4	NFSv4
/hana/log/SID/mnt0000*	NFSv3 oder NFSv4	NFSv4
/hana/Shared	NFSv3 oder NFSv4	NFSv3 oder NFSv4
/Usr/sap/SID	NFSv3 oder NFSv4	NFSv3 oder NFSv4

Die folgende Tabelle zeigt die Mount-Optionen für die verschiedenen NFS-Versionen und ONTAP-Versionen. Die gängigen Parameter sind unabhängig von den Versionen NFS und ONTAP.

Für SAP Lama muss das Verzeichnis /usr/sap/SID lokal sein. Mounten Sie daher kein NFS Volume für /usr/sap/SID, wenn Sie SAP Lama verwenden.

Bei NFSv3 müssen Sie die NFS-Sperre deaktivieren, um NFS-Sperrungsvorgänge bei einem Software- oder Serverausfall zu vermeiden.

Mit ONTAP 9 kann die NFS-Übertragungsgröße bis zu 1 MB konfiguriert werden. Insbesondere bei 40-GbE- oder schnelleren Verbindungen zum Storage-System muss die Übertragungsgröße auf 1 MB gesetzt werden, um die erwarteten Durchsatzwerte zu erzielen.

Allgemeiner Parameter	NFSv3	NFSv4	NFS-Übertragungsgröße mit ONTAP 9	NFS-Übertragungsgröße mit ONTAP 8
rw, bg, hart, timeso=600, noatim,	Nfsvers=3,nolock,	Nfsvers=4.1,sperren	Rsize=1048576,wsize=262144,	Rsize=65536,wsize=65536,

Um die Lese-Performance mit NFSv3 zu verbessern, empfiehlt NetApp, den zu verwenden `nconnect=n` Mount-Option, die mit SUSE Linux Enterprise Server 12 SP4 oder höher und RedHat Enterprise Linux (RHEL) 8.3 oder höher verfügbar ist.

Performance-Tests zeigen das `nconnect=4` Bietet gute Leseergebnisse speziell für das Datenvolumen. Protokollschreibvorgänge können von einer geringeren Anzahl von Sitzungen profitieren, z. B. `nconnect=2`. Für gemeinsam genutzte Volumes bietet sich die Option „nconnect“ möglicherweise ebenfalls an. Beachten Sie, dass der erste Mount von einem NFS-Server (IP-Adresse) die Anzahl der verwendeten Sitzungen definiert. Weitere Halterungen an dieselbe IP-Adresse ändern dies nicht, auch wenn für nconnect ein anderer Wert verwendet wird.

Ab ONTAP 9.8 und SUSE SLES15SP2 oder RedHat RHEL 8.4 oder höher unterstützt NetApp die nconnect Option auch für NFSv4.1.

Wenn nconnect mit NFSV4.x verwendet wird, sollte die Anzahl der NFSv4.x-Sitzungsplätze gemäß der folgenden Regel angepasst werden: Anzahl der Sitzungsplätze entspricht <nconnect value> x 64. Auf dem Host wird dies durch einen Neustart adjuseted `echo options nfs max_session_slots=<calculated value> > /etc/modprobe.d/nfsclient.conf`. Der serverseitige Wert muss ebenfalls angepasst werden. Legen Sie die Anzahl der Sitzungsplätze fest, wie unter beschrieben "NFS-Konfiguration für NFSv4:"

So mounten Sie die Dateisysteme während des Systemstarts mit dem `/etc/fstab` Konfigurationsdatei, führen Sie die folgenden Schritte aus:

Das folgende Beispiel zeigt eine SAP HANA-Datenbank mit einem einzelnen Host mit SID=NF2 und NFSv3 sowie eine NFS-Übertragungsgröße von 1 MB für Lesevorgänge und 256 KB für Schreibvorgänge.

1. Fügen Sie die erforderlichen Dateisysteme zum hinzu `/etc/fstab` Konfigurationsdatei

```
sapcc-hana-tst-06:/ # cat /etc/fstab
<storage-vif-data01>:/NF2_data_mnt00001 /hana/data/NF2/mnt00001 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-log01>:/NF2_log_mnt00001 /hana/log/NF2/mnt00001 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=2,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-data01>:/NF2_shared/usr-sap /usr/sap/NF2 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-data01>:/NF2_shared/shared /hana/shared nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
```

2. Laufen `mount -a` Um die Dateisysteme auf allen Hosts einzubinden.

Das nächste Beispiel zeigt eine SAP HANA Datenbank mit mehreren Hosts und SID=NF2 unter Verwendung von NFSv4.1 für Daten- und Log-Filesysteme und NFSv3 für die `/hana/shared` Und `/usr/sap/NF2` File-Systeme. Es wird eine NFS-Transfergröße von 1 MB für Lesevorgänge und 256 KB für Schreibvorgänge verwendet.

1. Fügen Sie die erforderlichen Dateisysteme zum hinzu `/etc/fstab` Konfigurationsdatei auf allen Hosts.

   Der `/usr/sap/NF2` Dateisystem ist für jeden Datenbank-Host unterschiedlich. Das folgende Beispiel zeigt `/NF2_shared/usr-sap-host1`.

```
sapcc-hana-tst-06:/ # cat /etc/fstab
<storage-vif-data01>:/NF2_data_mnt00001 /hana/data/NF2/mnt00001 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-data02>:/NF2_data_mnt00002 /hana/data/NF2/mnt00002 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-log01>:/NF2_log_mnt00001 /hana/log/NF2/mnt00001 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=2,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-log02>:/NF2_log_mnt00002 /hana/log/NF2/mnt00002 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=2,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-data02>:/NF2_shared/usr-sap-host1 /usr/sap/NF2 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-data02>:/NF2_shared/shared /hana/shared nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
```

2. Laufen `mount -a` Um die Dateisysteme auf allen Hosts einzubinden.

Vorbereitung der Installation von SAP HANA auf NFSv4

Für NFS Version 4 und höher ist Benutzerauthentifizierung erforderlich. Diese Authentifizierung kann über ein zentrales Benutzerverwaltungstool wie z. B. einen LDAP-Server (Lightweight Directory Access Protocol) oder lokale Benutzerkonten erfolgen. In den folgenden Abschnitten wird die Konfiguration lokaler Benutzerkonten beschrieben.

Die Administrationsteilnehmer `<sid>adm`,`<sid>crypt` und die `sapsys` Gruppe müssen vor Beginn der Installation der SAP HANA-Software manuell auf den SAP HANA-Hosts und den Speicher-Controllern erstellt werden.

SAP HANA-Hosts

Wenn es nicht existiert, die `sapsys` Die Gruppe muss auf dem SAP HANA-Host erstellt werden. Es muss eine eindeutige Gruppen-ID ausgewählt werden, die keinen Konflikt mit den vorhandenen Gruppen-IDs auf den Speicher-Controllern hat.

Die Benutzer `<sid>adm` und `<sid>crypt` werden auf dem SAP HANA-Host erstellt. Es müssen eindeutige IDs ausgewählt werden, die nicht mit bestehenden Benutzer-IDs auf den Storage Controllern in Konflikt stehen.

Bei einem SAP HANA-System mit mehreren Hosts müssen die Benutzer- und Gruppen-IDs auf allen SAP HANA-Hosts identisch sein. Die Gruppe und der Benutzer werden auf den anderen SAP HANA Hosts erstellt, indem die betroffenen Zeilen in und `/etc/passwd` vom Quellsystem auf alle anderen SAP HANA Hosts kopiert `/etc/group` werden.

Die NFSv4-Domäne muss auf allen Linux Servern auf den gleichen Wert gesetzt werden `/etc/idmapd.conf`) Und SVMs. Legen Sie in der Datei den Domain-Parameter „Domain = <Domain-Name>“ fest `/etc/idmapd.conf` Für die Linux-Hosts.

Aktivieren und starten Sie den NFS-IDMAPD-Service.

```
systemctl enable nfs-idmapd.service
systemctl start nfs-idmapd.service
```

Die neuesten Linux-Kernel benötigen diesen Schritt nicht. Warnmeldungen können sicher ignoriert werden.

Storage Controller

Die Benutzer-IDs und Gruppen-IDs müssen auf den SAP HANA-Hosts und den Speicher-Controllern identisch sein. Die Gruppe und der Benutzer werden durch Eingabe der folgenden Befehle auf dem Storage-Cluster erstellt:

```
vserver services unix-group create -vserver <vserver> -name <group name>
-id <group id>
vserver services unix-user create -vserver <vserver> -user <user name> -id
<user-id> -primary-gid <group id>
```

Legen Sie außerdem die Gruppen-ID des UNIX-Benutzerstamms der SVM auf 0 fest.

```
vserver services unix-user modify -vserver <vserver> -user root -primary
-gid 0
```

I/O-Stack-Konfiguration für SAP HANA

Ab SAP HANA 1.0 SPS10 führte SAP Parameter ein, um das I/O-Verhalten anzupassen und die Datenbank für die verwendeten Datei- und Speichersysteme zu optimieren.

NetApp hat Performance-Tests durchgeführt, um die idealen Werte zu definieren. In der folgenden Tabelle sind die optimalen Werte aufgeführt, die aus den Leistungstests abgeleitet wurden.

Parameter	Wert
max_parallel_io_Requests	128
Async_read_Submit	Ein

Parameter	Wert
Async_write_submit_Active	Ein
Async_Write_Submit_Blocks	Alle

Bei SAP HANA 1.0 Versionen bis SPS12 können diese Parameter während der Installation der SAP HANA Datenbank eingestellt werden, wie in SAP Note beschrieben "2267798: Konfiguration der SAP HANA Datenbank während der Installation mit hdbparam".

Alternativ können die Parameter nach der SAP HANA-Datenbankinstallation über die eingestellt werden `hdbparam` Framework:

```
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.max_parallel_io_requests=128
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_write_submit_active=on
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_read_submit=on
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_write_submit_blocks=all
```

Ab SAP HANA 2.0 `hdbparam` Wurde veraltet und die Parameter wurden in verschoben `global.ini`. Die Parameter können mit SQL-Befehlen oder SAP HANA Studio eingestellt werden. Weitere Informationen finden Sie im SAP-Hinweis "2399079: Beseitigung von hdbparam in HANA 2". Sie können die Parameter auch in global.ini einstellen, wie im folgenden Text dargestellt:

```
nf2adm@stlrx300s8-6: /usr/sap/NF2/SYS/global/hdb/custom/config> cat
global.ini
…
[fileio]
async_read_submit = on
async_write_submit_active = on
max_parallel_io_requests = 128
async_write_submit_blocks = all
…
```

Seit SAP HANA 2.0 SPS5, dem `setParameter.py` Skript kann verwendet werden der Satz die richtigen Parameter:

```
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00/exe/python_support>
python setParameter.py
-set=SYSTEM/global.ini/fileio/max_parallel_io_requests=128
python setParameter.py -set=SYSTEM/global.ini/fileio/async_read_submit=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_active=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_blocks=all
```

Größe des SAP HANA Daten-Volumes

Standardmäßig verwendet SAP HANA nur ein Daten-Volume pro SAP HANA Service. Aufgrund der maximalen Dateigröße des Dateisystems empfehlen wir, die maximale Größe des Datenträgers zu begrenzen.

Um dies automatisch zu tun, setzen Sie den folgenden Parameter in ein `global.ini` Im Abschnitt `[persistence]`:

```
datavolume_striping = true
datavolume_striping_size_gb = 8000
```

Dadurch wird ein neues Daten-Volume erstellt, nachdem das Limit von 8 GB erreicht wurde. "SAP Note 240005 Frage 15" Bietet weitere Informationen.

SAP HANA Softwareinstallation

Im Folgenden sind Anforderungen für die Softwareinstallation für SAP HANA aufgeführt.

Installation auf Single-Host-System

Die Installation der SAP HANA-Software erfordert keine zusätzliche Vorbereitung auf ein Single-Host-System.

Installation auf Systemen mit mehreren Hosts

Gehen Sie wie folgt vor, um SAP HANA auf einem System mit mehreren Hosts zu installieren:

1. mithilfe des SAP- `hdbclm`Starten Sie die InstallationInstallationstools, indem Sie den folgenden Befehl an einem der Arbeitshosts ausführen. Verwenden Sie die `addhosts` Option, um den zweiten Worker (`sapcc-hana-tst-03`und den Standby-Host hinzuzufügen(`sapcc-hana-tst-04`.

   ```
   apcc-hana-tst-02:/mnt/sapcc-share/software/SAP/HANA2SPS7-
   73/DATA_UNITS/HDB_LCM_LINUX_X86_64 #
   ./hdblcm --action=install --addhosts=sapcc-hana-tst-03:role=worker,sapcc
   -hana-tst-04:role=standby
   ```

```
SAP HANA Lifecycle Management - SAP HANA Database 2.00.073.00.1695288802
************************************************************************


Scanning software locations...
Detected components:
    SAP HANA AFL (incl.PAL,BFL,OFL) (2.00.073.0000.1695321500) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_AFL_LINUX_X86_64/packages
    SAP HANA Database (2.00.073.00.1695288802) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
    SAP HANA Database Client (2.18.24.1695756995) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/SAP_HANA_CLIENT/client
    SAP HANA Studio (2.3.75.000000) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_STUDIO_LINUX_X86_64/studio
    SAP HANA Local Secure Store (2.11.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HANA_LSS_24_LINUX_X86_64/packages
    SAP HANA XS Advanced Runtime (1.1.3.230717145654) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_RT_10_LINUX_X86_64/packages
    SAP HANA EML AFL (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_EML_AFL_10_LINUX_X86_64/packages
    SAP HANA EPM-MDS (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/SAP_HANA_EPM-MDS_10/packages
    Automated Predictive Library (4.203.2321.0.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/PAAPL4_H20_LINUX_X86_64/apl-
4.203.2321.0-hana2sp03-linux_x64/installer/packages
    GUI for HALM for XSA (including product installer) Version 1
(1.015.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACALMPIUI15_0.zip
    XSAC FILEPROCESSOR 1.0 (1.000.102) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACFILEPROC00_102.zip
    SAP HANA tools for accessing catalog content, data preview, SQL
console, etc. (2.015.230503) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_HRTT_20/XSACHRTT15_230503.zip
    Develop and run portal services for customer applications on XSA
(2.007.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACPORTALSERV07_0.zip
    The SAP Web IDE for HANA 2.0 (4.007.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
```

```
73/DATA_UNITS/XSAC_SAP_WEB_IDE_20/XSACSAPWEBIDE07_0.zip
    XS JOB SCHEDULER 1.0 (1.007.22) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACSERVICES07_22.zip
    SAPUI5 FESV6 XSA 1 - SAPUI5 1.71 (1.071.52) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV671_52.zip
    SAPUI5 FESV9 XSA 1 - SAPUI5 1.108 (1.108.5) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV9108_5.zip
    SAPUI5 SERVICE BROKER XSA 1 - SAPUI5 Service Broker 1.0 (1.000.4) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5SB00_4.zip
    XSA Cockpit 1 (1.001.37) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACXSACOCKPIT01_37.zip


SAP HANA Database version '2.00.073.00.1695288802' will be installed.

Select additional components for installation:

  Index | Components      | Description

-------------------------------------------------------------------------
--------------------------
  1     | all             | All components
  2     | server          | No additional components
  3     | client          | Install SAP HANA Database Client version
2.18.24.1695756995
  4     | lss             | Install SAP HANA Local Secure Store version
2.11.0
  5     | studio          | Install SAP HANA Studio version
2.3.75.000000
  6     | xs              | Install SAP HANA XS Advanced Runtime version
1.1.3.230717145654
  7     | afl             | Install SAP HANA AFL (incl.PAL,BFL,OFL)
version 2.00.073.0000.1695321500
  8     | eml             | Install SAP HANA EML AFL version
2.00.073.0000.1695321500
  9     | epmmds          | Install SAP HANA EPM-MDS version
2.00.073.0000.1695321500
  10    | sap_afl_sdk_apl | Install Automated Predictive Library version
4.203.2321.0.0
```

```
Enter comma-separated list of the selected indices [3,4]: 2,3
```

2. Vergewissern Sie sich, dass das Installationstool alle ausgewählten Komponenten bei allen Worker- und Standby-Hosts installiert hat.

Zusätzliche Partitionen für Datenvolumen werden hinzugefügt

Ab SAP HANA 2.0 SPS4 können Sie zusätzliche Daten-Volume-Partitionen konfigurieren, mit denen Sie zwei oder mehr Volumes für das Datenvolumen einer SAP HANA-Mandantendatenbank konfigurieren können. Ein einzelnes Volume kann auch jenseits der Größe und Performance-Grenzen skaliert werden.

Für SAP HANA sind zwei oder mehr einzelne Volumes für das Daten-Volume verfügbar, ein- und mehrere Host-Systeme. Sie können jederzeit weitere Volume-Partitionen hinzufügen, jedoch ist hierfür möglicherweise ein Neustart der SAP HANA Datenbank erforderlich.

Aktivieren von zusätzlichen Partitionen für Volumes

1. Um zusätzliche Datenträgers Partitionen zu aktivieren, fügen Sie den folgenden Eintrag in hinzu `global.ini` Verwendung von SAP HANA Studio oder Cockpit in der SYSTEMDB Konfiguration.

```
[customizable_functionalities]
persistence_datavolume_partition_multipath = true
```

Manuelles Hinzufügen des Parameters zum `global.ini` Datei erfordert den Neustart der Datenbank.

Volume-Konfiguration für ein SAP HANA System mit einem Host

Das Layout von Volumes für ein SAP HANA System mit mehreren Partitionen mit nur einem Host ist ähnlich wie das Layout eines Systems mit einer Datenträgers, aber mit einem zusätzlichen Datenvolumen gespeichert auf einem anderen Aggregat als das Protokoll-Volume und das andere Datenvolumen. Die folgende Tabelle zeigt eine Beispielkonfiguration eines SAP HANA Einzelhostsystems mit zwei Daten-Volume-Partitionen.

Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregat 2 bei Controller b
Datenvolumen: SID_Data_mnt00001	Gemeinsam genutztes Volume: SID_shared	Datenvolumen: SID_data2_mnt00001	Protokollvolumen: SID_log_mnt00001

Die folgende Tabelle zeigt ein Beispiel für die Mount-Punkt-Konfiguration für ein System mit einem einzelnen Host mit zwei Daten-Volume-Partitionen.

Verbindungspfad	Verzeichnis	Bereitstellungspunkt beim HANA-Host
SID_Data_mnt00001	–	/hana/Data/SID/mnt00001
SID_data2_mnt00001	–	/hana/data2/SID/mnt00001
SID_Log_mnt00001	–	/hana/log/SID/mnt00001
SID_freigegeben	Usr-sap freigegeben	/Usr/sap/SID /hana/Shared

Erstellen Sie das neue Daten-Volume und mounten Sie es mit ONTAP System Manager oder der ONTAP Cluster-Befehlszeilenschnittstelle am Namespace.

Volume-Konfiguration für SAP HANA System mit mehreren Hosts

Das Layout von Volumes für ein SAP HANA System mit mehreren Hosts mit mehreren Partitionen ist wie das Layout eines Systems mit einer Daten-Volume-Partition, aber mit einem zusätzlichen Datenvolumen gespeichert auf einem anderen Aggregat als das Protokoll-Volume und das andere Datenvolumen. Die folgende Tabelle zeigt eine Beispielkonfiguration eines SAP HANA Multihost-Systems mit zwei Daten-Volume-Partitionen.

Zweck	Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregieren 2 bei Controller B
Daten- und Protokoll-Volumes für Node 1	Datenvolumen: SID_Data_mnt00001	–	Protokollvolumen: SID_log_mnt00001	Daten2 Volumen: SID_data2_mnt00001
Daten- und Protokoll-Volumes für Node 2	Protokollvolumen: SID_log_mnt002	Daten2 Volumen: SID_data2_mnt002	Datenvolumen: SID_Data_mnt002	–
Daten- und Protokoll-Volumes für Node 3	–	Datenvolumen: SID_Data_mnt00003	Daten2 Volumen: SID_data2_mnt003	Protokollvolumen: SID_log_mnt00003
Daten- und Protokoll-Volumes für Node 4	Daten2 Volumen: SID_data2_mnt004	Protokollvolumen: SID_log_mnt004	–	Datenvolumen: SID_Data_mnt00004
Gemeinsames Volume für alle Hosts	Gemeinsam genutztes Volume: SID_shared	–	–	–

Die folgende Tabelle zeigt ein Beispiel für die Mount-Punkt-Konfiguration für ein System mit einem einzelnen Host mit zwei Daten-Volume-Partitionen.

Verbindungspfad	Verzeichnis	Bereitstellungspunkt beim SAP HANA-Host	Hinweis
SID_Data_mnt00001	–	/hana/Data/SID/mnt00001	Auf allen Hosts montiert
SID_data2_mnt00001	–	/hana/data2/SID/mnt00001	Auf allen Hosts montiert
SID_Log_mnt00001	–	/hana/log/SID/mnt00001	Auf allen Hosts montiert
SID_Data_mnt00002	–	/hana/Data/SID/mnt002	Auf allen Hosts montiert
SID_data2_mnt00002	–	/hana/data2/SID/mnt002	Auf allen Hosts montiert
SID_Log_mnt00002	–	/hana/log/SID/mnt002	Auf allen Hosts montiert
SID_Data_mnt00003	–	/hana/Data/SID/mnt003	Auf allen Hosts montiert
SID_data2_mnt00003	–	/hana/data2/SID/mnt003	Auf allen Hosts montiert
SID_log_mnt00003	–	/hana/log/SID/mnt003	Auf allen Hosts montiert
SID_Data_mnt00004	–	/hana/Data/SID/mnt004	Auf allen Hosts montiert

Verbindungspfad	Verzeichnis	Bereitstellungspunkt beim SAP HANA-Host	Hinweis
SID_data2_mnt00004	–	/hana/data2/SID/mnt004	Auf allen Hosts montiert
SID_log_mnt00004	–	/hana/log/SID/mnt004	Auf allen Hosts montiert
SID_freigegeben	Freigegeben	/hana/Shared/SID	Auf allen Hosts montiert
SID_freigegeben	Usr-sap-host1	/Usr/sap/SID	Angehängt auf Host 1
SID_freigegeben	Usr-sap-host2	/Usr/sap/SID	Angehängt auf Host 2
SID_freigegeben	Usr-sap-host3	/Usr/sap/SID	Angehängt auf Host 3
SID_freigegeben	Usr-sap-host4	/Usr/sap/SID	Angehängt auf Host 4
SID_freigegeben	Usr-sap-host5	/Usr/sap/SID	Angehängt auf Host 5

Erstellen Sie das neue Daten-Volume und mounten Sie es mit ONTAP System Manager oder der ONTAP Cluster-Befehlszeilenschnittstelle am Namespace.

Host-Konfiguration

Zusätzlich zu den im Abschnitt beschriebenen Aufgaben "„Host-Einrichtung“,"müssen Sie die zusätzlichen Mount-Punkte und fstab-Einträge für die neuen zusätzlichen Daten-Volumes erstellen und die neuen Volumes mounten.

1. Zusätzliche Bereitstellungspunkte erstellen:
   - Erstellen Sie für ein System mit einem einzelnen Host Mount Points und legen Sie die Berechtigungen für den Datenbank-Host fest.

     ```
     sapcc-hana-tst-06:/ # mkdir -p /hana/data2/SID/mnt00001
     sapcc-hana-tst-06:/ # chmod –R 777 /hana/data2/SID
     ```

   - Erstellen Sie für ein System mit mehreren Hosts Mount-Punkte und legen Sie die Berechtigungen für alle Worker und Standby-Hosts fest. Die folgenden Beispielbefehle gelten für ein 2+1-HANA-System mit mehreren Hosts.
     - Erster Worker-Host:

       ```
       sapcc-hana-tst-06:~ # mkdir -p /hana/data2/SID/mnt00001
       sapcc-hana-tst-06:~ # mkdir -p /hana/data2/SID/mnt00002
       sapcc-hana-tst-06:~ # chmod -R 777 /hana/data2/SID
       ```

     - Host zweiter Arbeiter:

       ```
       sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00001
       sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00002
       sapcc-hana-tst-07:~ # chmod -R 777 /hana/data2/SID
       ```

- Standby-Host:

```
sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00001
sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00002
sapcc-hana-tst-07:~ # chmod -R 777 /hana/data2/SID
```

2. Fügen Sie die zusätzlichen Dateisysteme zum hinzu `/etc/fstab` Konfigurationsdatei auf allen Hosts. Ein Beispiel für ein Single-Host-System mit NFSv4.1 ist:

```
<storage-vif-data02>:/SID_data2_mnt00001 /hana/data2/SID/mnt00001 nfs
rw,vers=4,
minorversion=1,hard,timeo=600,rsize=1048576,wsize=262144,bg,noatime,lock
0 0
```

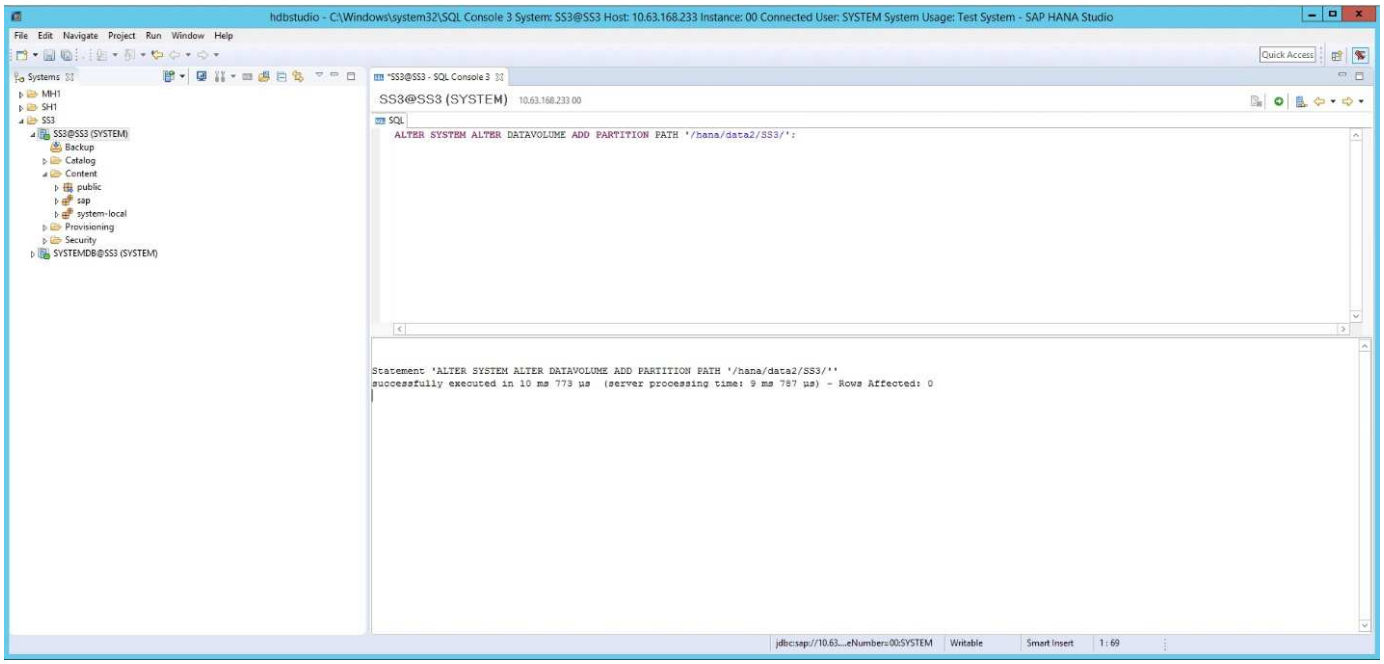
> Verwenden Sie eine andere virtuelle Storage-Schnittstelle für die Verbindung zu den einzelnen Daten-Volumes, um sicherzustellen, dass für jedes Volume unterschiedliche TCP-Sitzungen verwendet werden. Sie können auch die Option nconnect Mount verwenden, wenn sie für Ihr Betriebssystem verfügbar ist.

3. Führen Sie zum Mounten der Dateisysteme den aus `mount -a` Befehl.

Hinzufügen einer zusätzlichen Daten-Volume-Partition

Führen Sie die folgende SQL-Anweisung für die Mandantendatenbank aus, um Ihrer Mandantendatenbank eine zusätzliche Partition für das Datenvolumen hinzuzufügen. Verwenden Sie den Pfad zu zusätzlichen Volumes:

```
ALTER SYSTEM ALTER DATAVOLUME ADD PARTITION PATH '/hana/data2/SID/';
```



Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten bzw. auf den folgenden Websites:

- "SAP HANA Softwarelösungen"
- "TR-4646: SAP HANA Disaster Recovery with Storage Replication"
- "TR-4614: SAP HANA Backup and Recovery with SnapCenter"
- "TR-4667: Automatisierung von SAP Systemkopien mit dem SnapCenter SAP HANA Plug-in"
- NetApp Dokumentationszentren

  "https://www.netapp.com/support-and-training/documentation/"
- SAP Certified Enterprise Storage Hardware for SAP HANA

  "https://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/"
- SAP HANA Storage-Anforderungen

  "https://www.sap.com/documents/2024/03/146274d3-ae7e-0010-bca6-c68f7e60039b.html"
- SAP HANA Tailored Data Center Integration Häufig gestellte Fragen

  "https://www.sap.com/documents/2016/05/e8705aae-717c-0010-82c7-eda71af511fa.html"
- SAP HANA auf VMware vSphere Wiki

  "https://help.sap.com/docs/SUPPORT_CONTENT/virtualization/3362185751.html"
- Best Practices Guide für SAP HANA auf VMware vSphere

  "https://www.vmware.com/docs/sap_hana_on_vmware_vsphere_best_practices_guide-white-paper"

Aktualisierungsverlauf

An dieser Lösung wurden seit ihrer ersten Veröffentlichung folgende technische Änderungen vorgenommen:

Datum	Zusammenfassung aktualisieren
April 2014	Ausgangsversion
August 2014	Aktualisierte Auswahl der Festplattengröße und zusätzliche SSD-Konfiguration Hinzugefügt Konfiguration von Red hat Enterprise Linux OS zusätzliche Informationen zum SAP HANA Storage Connector zusätzliche Informationen zur VMware Konfiguration
November 2014	Abschnitt zur Storage-Größenbemessung aktualisiert
Januar 2015	Aktualisierter Abschnitt über die API des Storage-Konnektors Aktualisierung der Aggregat- und Volume-Konfiguration
März 2015	Neue STONITH-Implementierung für SAP HANA SPS9 zusätzlicher Abschnitt zur Einrichtung von Computing-Nodes und HANA-Installation hinzugefügt
Oktober 2015	NFSv4-Unterstützung für cDOT wurde mit dem aktualisierten sysctl-Parameter I/O-Parameter für SAP HANA und HWVAL > SPS10 hinzugefügt
März 2016	Aktualisierte Kapazitätsdimensionierung aktualisierte Mount-Optionen für den aktualisierten sysctl-Parameter /hana/shared
Februar 2017	Neue NetApp Storage-Systeme und Platten-Shelfs Neue Funktionen von ONTAP 9 Unterstützung für 40 GbE Neue Betriebssystemversionen (SUSE Linux Enterprise Server12 SP1 und Red hat Enterprise Linux 7.2) die neue SAP HANA-Version
Juli 2017	Kleine Updates
September 2018	Neue NetApp Storage-Systeme Neue Betriebssystemversionen (SUSE Linux Enterprise Server 12 SP3 und Red hat Enterprise Linux 7.4) zusätzliche kleinere Änderungen SAP HANA 2.0 SPS3
September 2019	Neue Betriebssystemversionen (SUSE Linux Enterprise Server 12 SP4, SUSE Linux Enterprise Server 15 und Red hat Enterprise Linux 7.6) kleinere Änderungen an der MAX Data-Volume-Größe
Dezember 2019	Neue NetApp Storage-Systeme Neues Betriebssystem SUSE Linux Enterprise Server 15 SP1
März 2020	Unterstützung von nconnect für NFSv3 New OS Release Red hat Enterprise Linux 8
Mai 2020	Einführung mehrerer Funktionen für die Datenpartition, die seit SAP HANA 2.0 SPS4 verfügbar sind
Juni 2020	Zusätzliche Informationen über optionale Funktionalitäten kleine Updates
Dezember 2020	Unterstützung von nconnect für NFSv4.1 ab ONTAP 9.8 Neue Betriebssystemversionen Neue SAP HANA-Version

Datum	Zusammenfassung aktualisieren
Februar 2021	Änderungen an den Hostnetzwerkeinstellungen und anderen geringfügigen Änderungen
April 2021	VMware vSphere-spezifische Informationen hinzugefügt
September 2022	Neue Betriebssystemversionen
Dezember 2023	Aktualisierung des Host-Setups überarbeitete nconnect-Einstellungen Informationen zu NFSv4.1-Sitzungen hinzugefügt
September 2024	Neue Storage-Systeme und kleinere Updates
Februar 2025	Neues Storage-System
Juli 2025	Kleine Updates

Konfigurationsleitfaden für SAP HANA auf FAS-Systemen mit FCP

Konfigurationsleitfaden: SAP HANA auf NetApp FAS Systemen mit Fibre Channel Protocol

Die NetApp FAS-Produktfamilie wurde für die Verwendung mit SAP HANA in TDI-Projekten zertifiziert. Dieser Leitfaden enthält Best Practices für SAP HANA auf dieser Plattform für FCP.

Marco Schoen, NetApp

Die Zertifizierung gilt für folgende Modelle:

- FAS2750, FAS2820, FAS8300, FAS50, FAS8700 FAS70, FAS9500, FAS90

Eine vollständige Liste der zertifizierten NetApp Storage-Lösungen für SAP HANA finden Sie unter "Zertifiziertes und unterstütztes SAP HANA-Hardwaresverzeichnis".

In diesem Dokument werden die FAS-Konfigurationen beschrieben, die das Fibre Channel Protocol (FCP) verwenden.

> Die in diesem Dokument beschriebene Konfiguration ist erforderlich, um die erforderlichen SAP HANA KPIs und die beste Performance für SAP HANA zu erreichen. Wenn Sie Einstellungen oder Funktionen ändern, die nicht in diesem Dokument aufgeführt sind, kann dies zu einer Performance-Verschlechterung oder zu einem unerwarteten Verhalten führen. Diese Einstellungen sollten nur nach Rat des NetApp Supports vorgenommen werden.

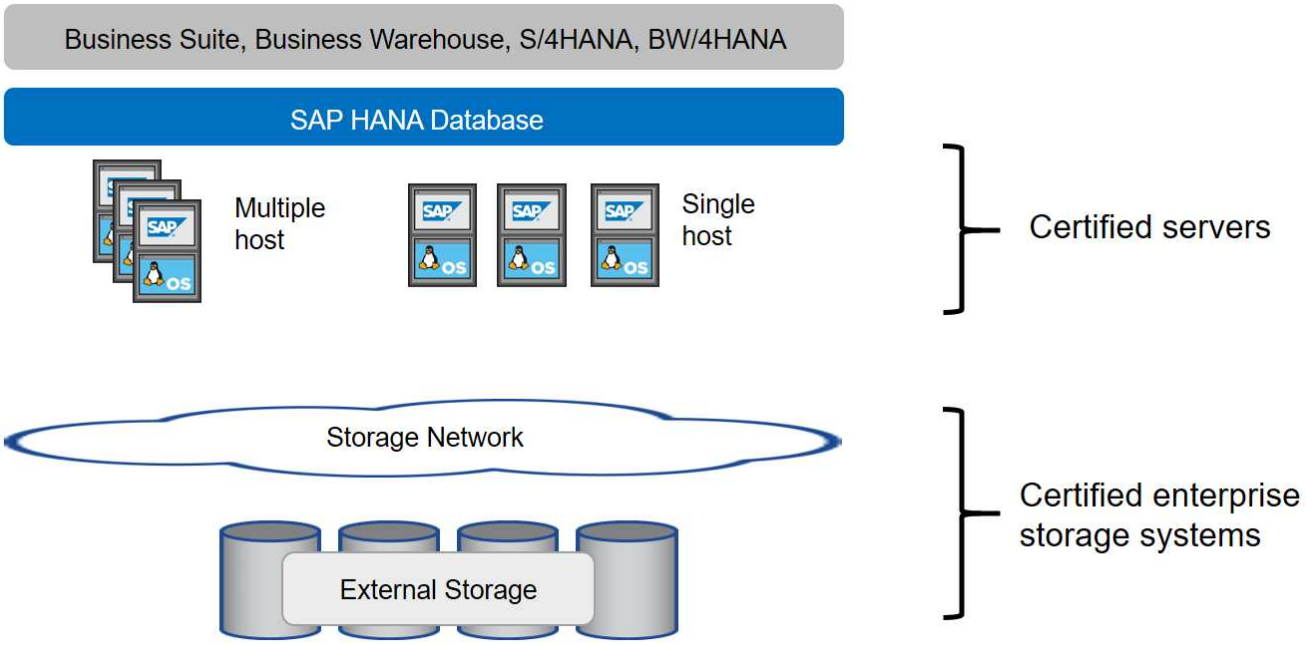
Die Konfigurationsleitfäden für FAS Systeme mit NFS und NetApp AFF Systemen können über die folgenden Links gefunden werden:

- "Technischer Bericht: SAP HANA on NetApp AFF Systems with FCP"
- "Technischer Bericht: SAP HANA on NetApp ASA Systems with FCP"
- "Technischer Bericht: SAP HANA on NetApp FAS Systems with NFS"
- "Technischer Bericht: SAP HANA on NetApp AFF Systems with NFS"

In einer SAP HANA Umgebung mit mehreren Hosts wird der standardmäßige SAP HANA-Storage-Connector verwendet, um im Falle eines Failover des SAP HANA-Hosts zu Fechten. In den entsprechenden SAP-Hinweisen finden Sie die Konfigurationsrichtlinien für das Betriebssystem und die HANA-spezifischen Linux-Kernel-Abhängigkeiten. Weitere Informationen finden Sie unter "SAP Note 2235581 – von SAP HANA unterstützte Betriebssysteme".

SAP HANA Tailored Datacenter Integration

NetApp FAS Storage Controller sind im SAP HANA Tailored Datacenter Integration-Programm (TDI) unter Verwendung der NFS-Protokolle (NAS) und Fibre Channel (SAN) zertifiziert. Sie können in beliebigen SAP HANA-Szenarien wie SAP Business Suite on HANA, S/4HANA, BW/4HANA oder SAP Business Warehouse on HANA in Konfigurationen mit einem Host oder mehreren Hosts implementiert werden. Alle Server, die für den Einsatz mit SAP HANA zertifiziert sind, können mit der zertifizierten Storage-Lösung kombiniert werden. In der folgenden Abbildung finden Sie eine Übersicht über die Architektur.



Weitere Informationen zu den Voraussetzungen und Empfehlungen für produktive SAP HANA-Systeme finden Sie in der folgenden Ressource:

- "SAP HANA Tailored Data Center Integration Häufig gestellte Fragen"

SAP HANA mit VMware vSphere

Für die Verbindung von Storage mit Virtual Machines (VMs) gibt es verschiedene Optionen. Der bevorzugte Modus ist die direkte Verbindung der Storage Volumes mit NFS vom Gastbetriebssystem. Diese Option ist in beschrieben"Technischer Bericht: SAP HANA on NetApp AFF Systems with NFS".

Auch Raw Device Mapping (RDM), FCP Datastores oder VVOL Datastores mit FCP werden unterstützt. Bei beiden Datastore-Optionen muss für produktive Anwendungsfälle nur eine SAP HANA Daten oder ein Protokoll-Volume im Datastore gespeichert werden.

Weitere Informationen zur Verwendung von vSphere mit SAP HANA finden Sie unter den folgenden Links:

- "SAP HANA on VMware vSphere - Virtualization - Community Wiki"

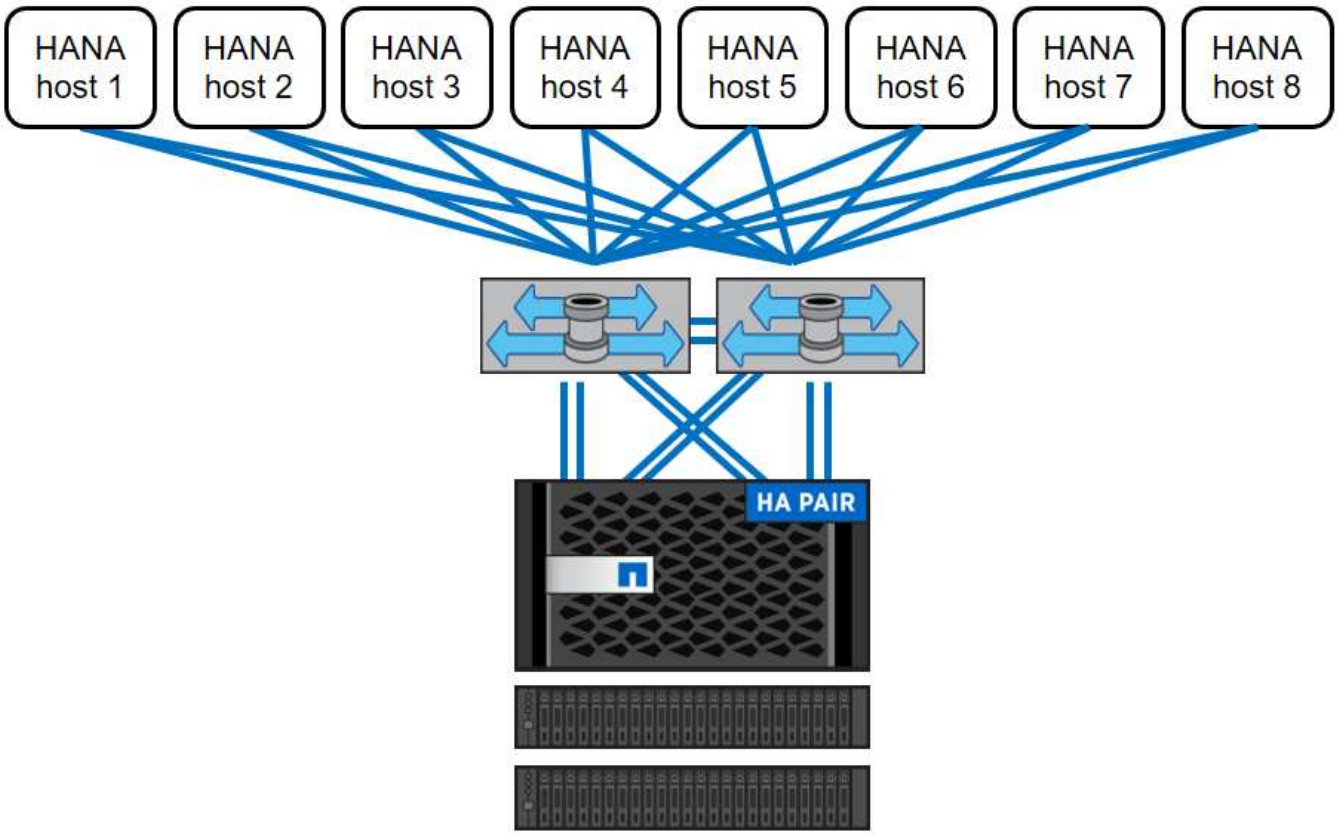
- "Best Practices Guide für SAP HANA auf VMware vSphere"
- "2161991 - Konfigurationsrichtlinien für VMware vSphere - SAP ONE Support Launchpad (Anmeldung erforderlich)"

Der Netapp Architektur Sind

SAP HANA-Hosts sind über eine redundante FCP-Infrastruktur und Multipathing-Software mit den Storage Controllern verbunden. Eine redundante FCP Switch-Infrastruktur ist erforderlich, um eine fehlertolerante SAP HANA Host-zu-Storage-Konnektivität bei Ausfall von Switch oder Host Bus Adapter (HBA) bereitzustellen. Ein entsprechendes Zoning muss am Switch konfiguriert werden, damit alle HANA Hosts die erforderlichen LUNs auf den Storage Controllern erreichen können.

Auf der Storage-Ebene können verschiedene Modelle der FAS Produktfamilie verwendet werden. Die maximale Anzahl an an mit dem Storage verbundenen SAP HANA-Hosts wird durch die Performance-Anforderungen von SAP HANA definiert. Die Anzahl der benötigten Platten-Shelves richtet sich nach den Kapazitäts- und Performance-Anforderungen der SAP HANA-Systeme.

Die folgende Abbildung zeigt eine Beispielkonfiguration mit acht SAP HANA-Hosts, die an ein Storage HA-Paar angeschlossen sind.



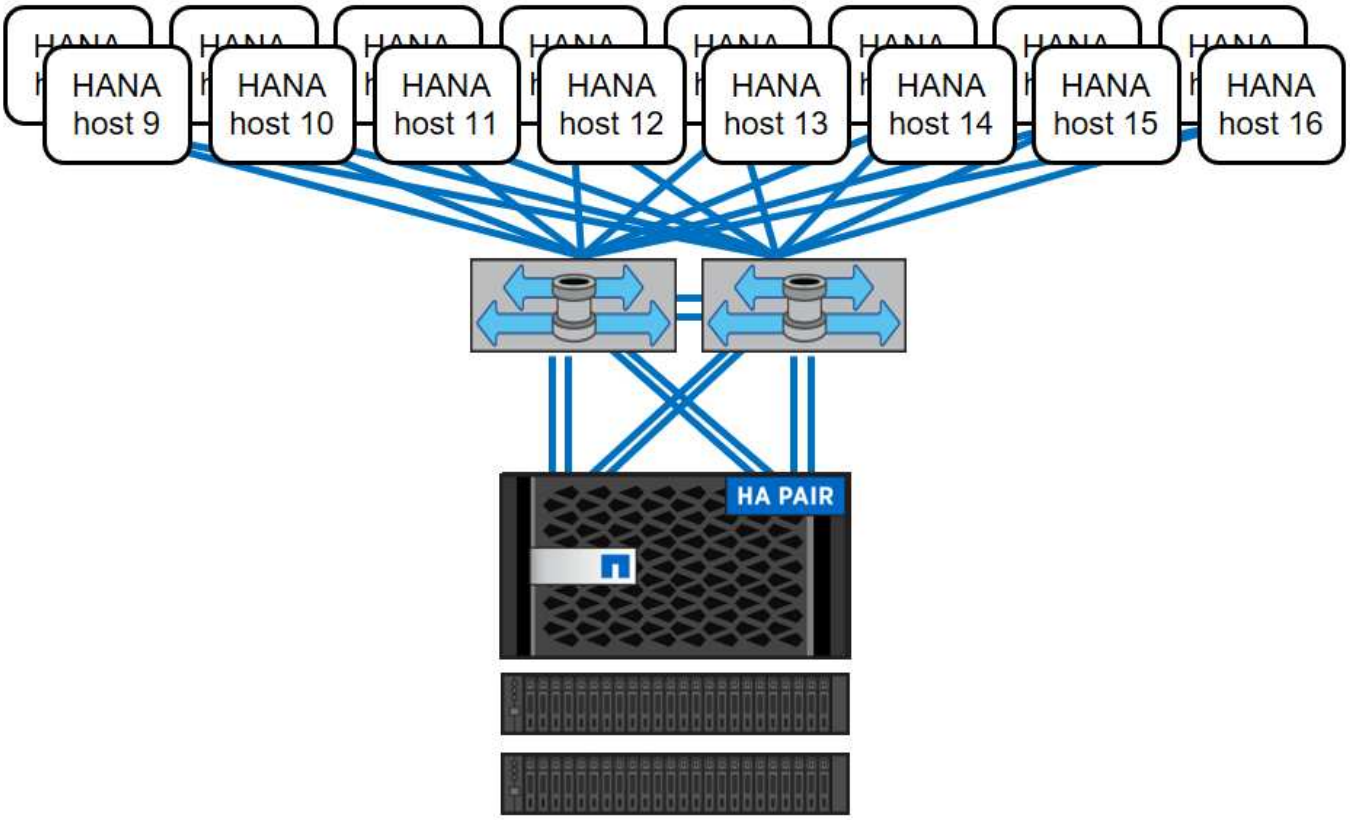
Diese Architektur lässt sich in zwei Dimensionen skalieren:

- Durch das Anschließen zusätzlicher SAP HANA-Hosts und Festplattenkapazität an den Storage, sofern die Storage-Controller bei der neuen Last genügend Performance bieten können, um wichtige Performance-

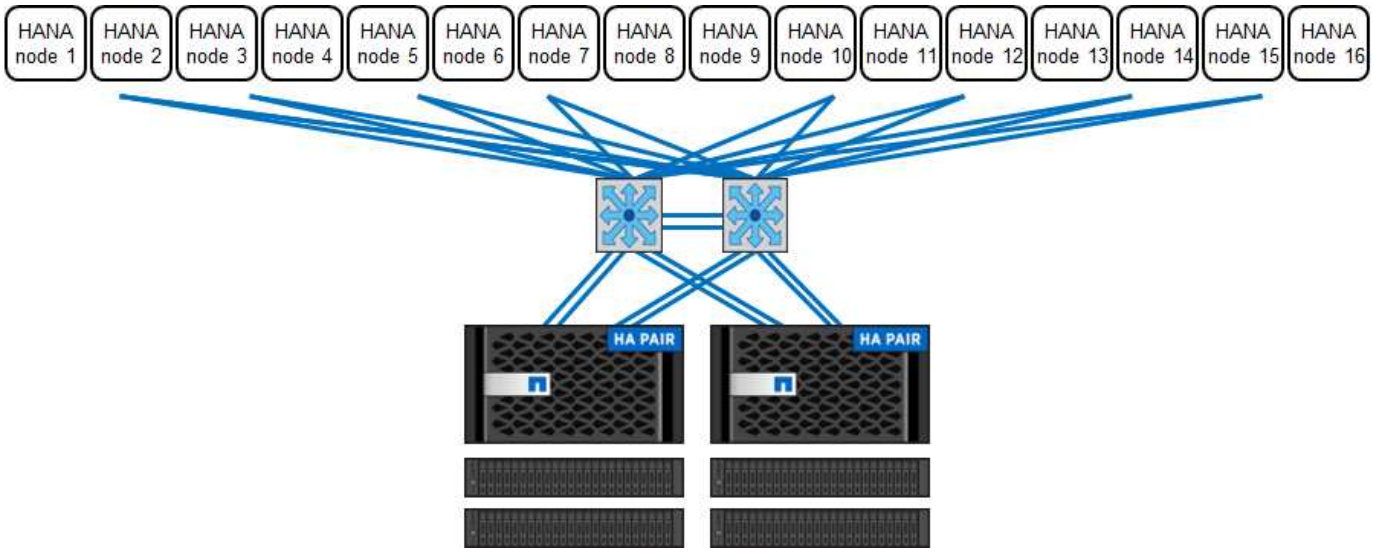
Kennzahlen (KPIs) zu erfüllen.

- Durch Hinzufügen weiterer Storage-Systeme und Festplattenkapazität für die zusätzlichen SAP HANA-Hosts

Die folgende Abbildung zeigt ein Konfigurationsbeispiel, in dem mehr SAP HANA-Hosts mit den Storage-Controllern verbunden sind. In diesem Beispiel sind mehr Platten-Shelves erforderlich, um die Kapazitäts- und Performance-Anforderungen der 16 SAP HANA-Hosts zu erfüllen. Abhängig von den Anforderungen an den Gesamtdurchsatz müssen die Storage Controller um zusätzliche FC-Verbindungen erweitert werden.



Unabhängig vom implementierten FAS Storage-Modell lässt sich die SAP HANA Landschaft auch durch Hinzufügen weiterer Storage-Controller skalieren, wie in der folgenden Abbildung dargestellt.



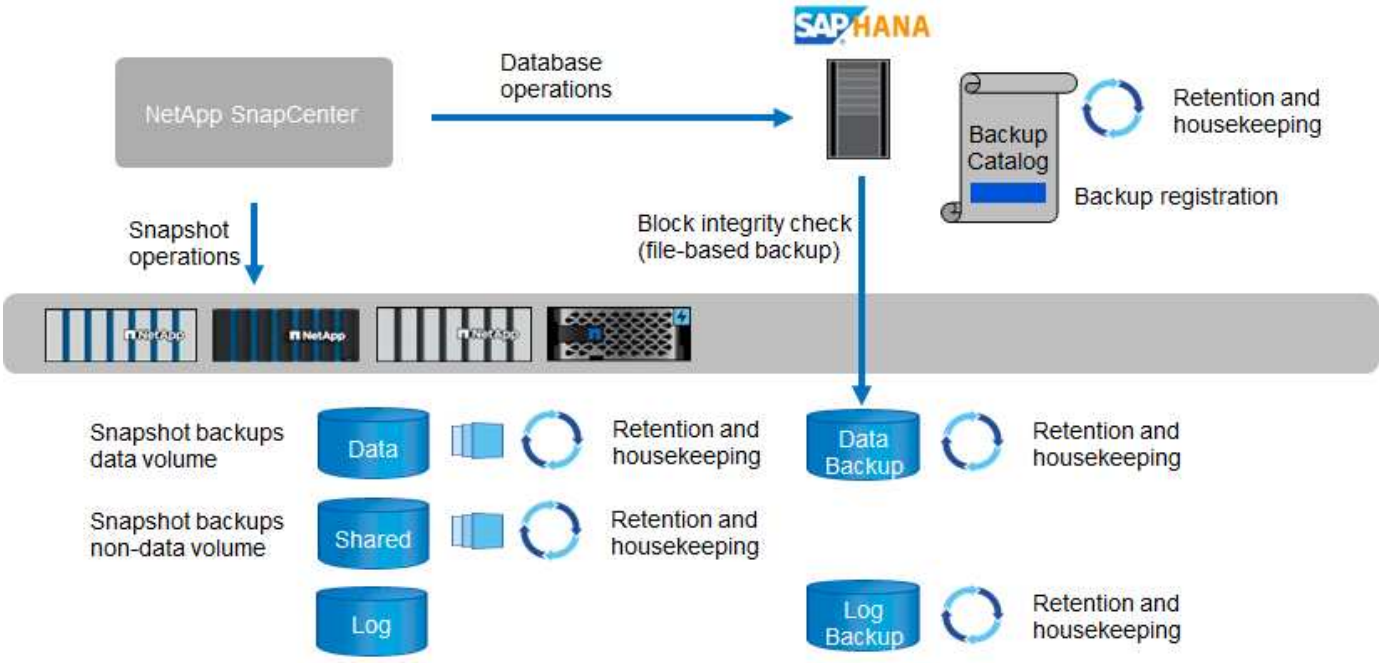
SAP HANA Backup

Die NetApp ONTAP Software bietet einen integrierten Mechanismus für das Backup von SAP HANA Datenbanken. Storage-basiertes Snapshot Backup ist eine vollständig unterstützte und integrierte Backup-Lösung, die für SAP HANA Single-Container-Systeme und SAP HANA MDC-Einzelmandanten-Systeme verfügbar ist.

Storage-basierte Snapshot Backups werden mithilfe des NetApp SnapCenter Plug-ins für SAP HANA implementiert, das über die von der SAP HANA Datenbank bereitgestellten Schnittstellen konsistente Storage-basierte Snapshot Backups ermöglicht. SnapCenter registriert die Snapshot-Backups im SAP HANA Backup-Katalog, damit die Backups im SAP HANA Studio sichtbar sind und für Restore- und Recovery-Vorgänge ausgewählt werden können.

Mit der NetApp SnapVault Software können die auf dem Primärspeicher erstellten Snapshot Kopien auf dem sekundären Backup-Storage repliziert werden, der von SnapCenter gesteuert wird. Für Backups auf dem primären Storage und für Backups auf dem sekundären Storage können unterschiedliche Richtlinien zur Backup-Aufbewahrung definiert werden. Das SnapCenter Plug-in für SAP HANA Database managt die Aufbewahrung von auf Snapshot Kopien basierenden Daten-Backups und Log-Backups, einschließlich der allgemeinen Ordnung des Backup-Katalogs. Das SnapCenter Plug-in für SAP HANA Database ermöglicht darüber hinaus die Überprüfung der Blockintegrität der SAP HANA Datenbank durch ein dateibasiertes Backup.

Die Datenbankprotokolle können mithilfe eines NFS-Mount-Speichers direkt auf dem sekundären Storage gesichert werden, wie in der folgenden Abbildung dargestellt.



Storage-basierte Snapshot Backups bieten im Vergleich zu dateibasierten Backups entscheidende Vorteile. Zu diesen Vorteilen zählen unter anderem:

- Schnelleres Backup (wenige Minuten)
- Schnellere Restores auf Storage-Ebene (wenige Minuten)
- Keine Auswirkungen auf die Performance des SAP HANA Datenbank-Hosts, Netzwerks oder Storage während des Backups
- Platzsparende und bandbreiteneffiziente Replizierung auf Basis von Blockänderungen auf sekundärem

Storage

Weitere Informationen zur Backup- und Recovery-Lösung SAP HANA mit SnapCenter finden Sie unter "TR-4614: SAP HANA Backup and Recovery with SnapCenter".

Disaster Recovery für SAP HANA

SAP HANA Disaster Recovery kann mithilfe von SAP-Systemreplizierung oder auf der Storage-Ebene mithilfe von Storage-Replizierungstechnologien auf der Datenbankebene durchgeführt werden. Der folgende Abschnitt bietet einen Überblick über Disaster-Recovery-Lösungen basierend auf der Storage-Replizierung.

Weitere Informationen zur Disaster-Recovery-Lösung SAP HANA mit SnapCenter finden Sie unter "TR-4646: SAP HANA Disaster Recovery with Storage Replication".

Storage-Replizierung basierend auf SnapMirror

Die folgende Abbildung zeigt eine Disaster-Recovery-Lösung für drei Standorte, die synchrone SnapMirror Replizierung zum lokalen DR-Datacenter und asynchrone SnapMirror zur Replizierung von Daten an das Remote-DR-Datacenter verwendet.

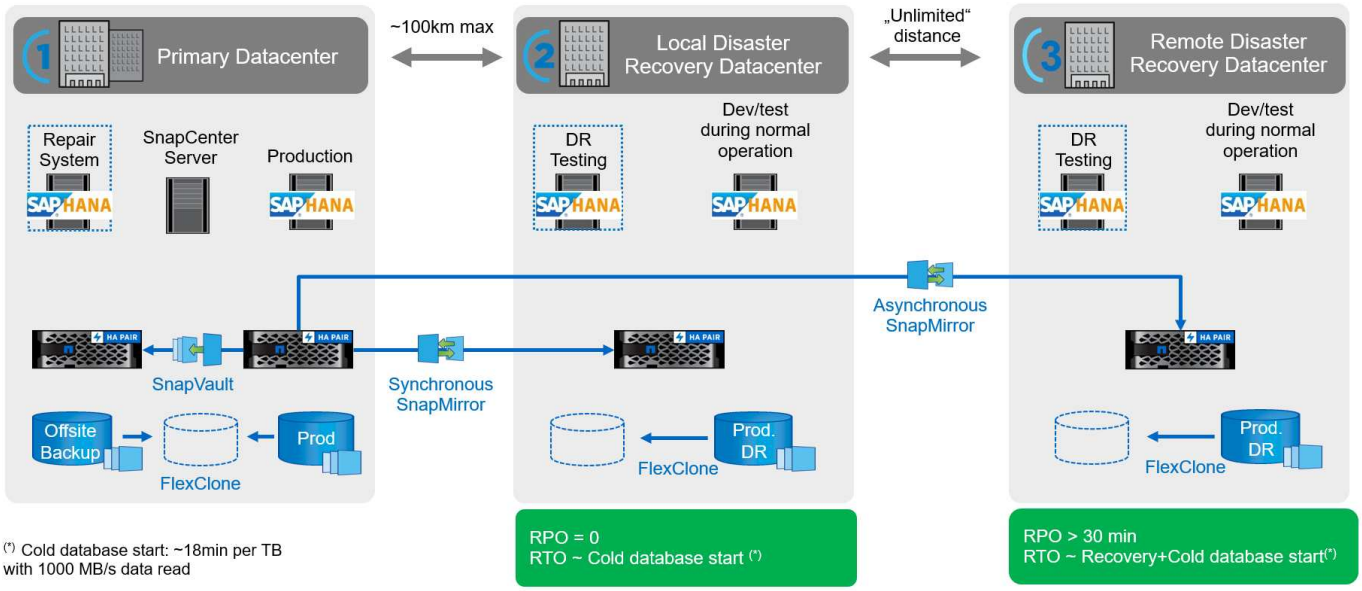
Die Datenreplizierung mit synchronem SnapMirror sorgt für einen RPO von null. Die Entfernung zwischen dem primären und dem lokalen DR-Datacenter ist auf etwa 100 km beschränkt.

Der Schutz vor Ausfällen des primären und lokalen DR-Standorts wird durch Replizieren der Daten zu einem dritten Remote-DR-Datacenter mithilfe von asynchronem SnapMirror durchgeführt. Der RPO hängt von der Häufigkeit der Replizierungs-Updates und der Übertragungsgeschwindigkeit ab. Theoretisch ist die Entfernung unbegrenzt, aber die Obergrenze hängt von der zu übertragenden Datenmenge und der zwischen den Rechenzentren verfügbaren Verbindung ab. Typische RPO-Werte liegen im Bereich von 30 Minuten bis mehreren Stunden.

Das RTO für beide Replizierungsmethoden hängt in erster Linie von der Zeit ab, die zum Starten der HANA-Datenbank am DR-Standort und zum Laden der Daten in den Speicher erforderlich ist. Mit der Annahme, dass die Daten mit einem Durchsatz von 1000 MBit/s gelesen werden, dass das Laden von 1 TB Daten ungefähr 18 Minuten dauert.

Die Server an den DR-Standorten können im normalen Betrieb als Entwicklungs- und Testsysteme genutzt werden. Bei einem Ausfall müssten die Entwicklungs- und Testsysteme heruntergefahren und als DR-Produktionsserver gestartet werden.

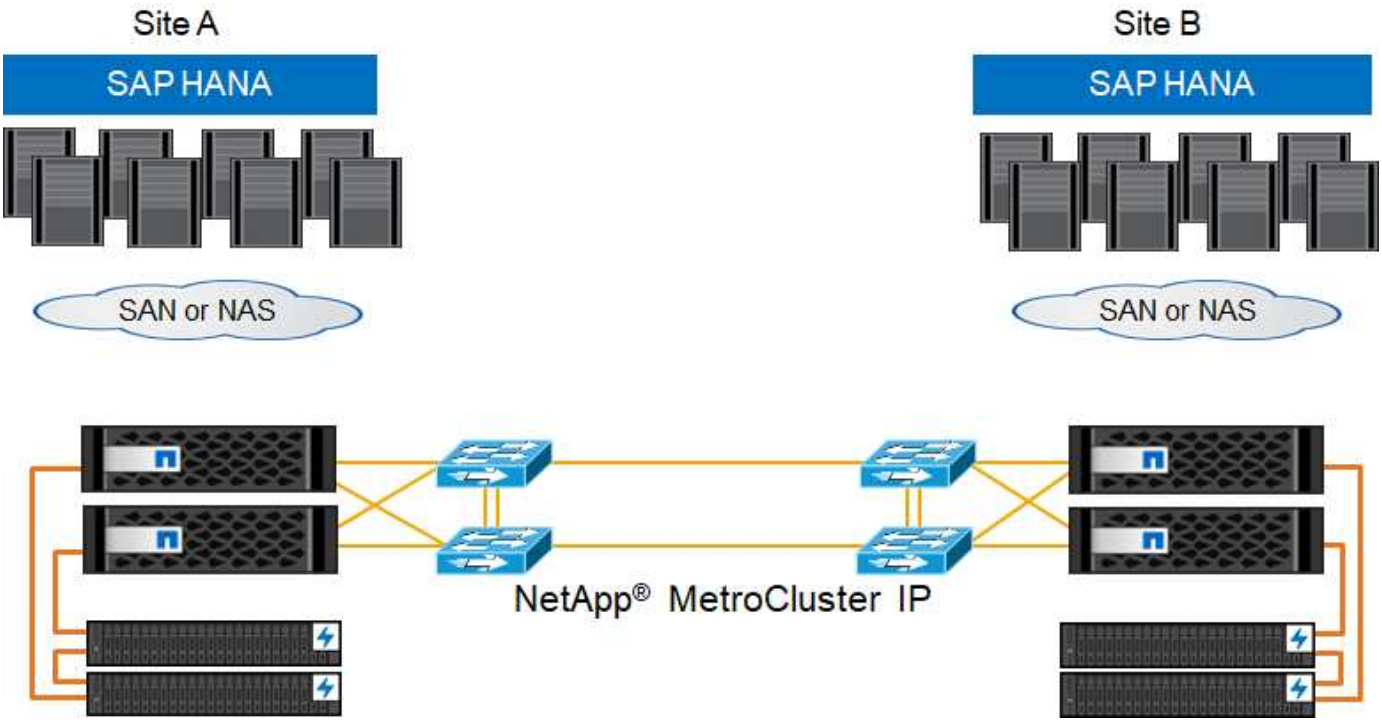
Beide Replizierungsmethoden ermöglichen die Durchführung von DR-Workflow-Tests ohne Auswirkungen auf RPO und RTO. FlexClone Volumes werden auf dem Storage erstellt und an die DR-Testserver angeschlossen.



Die synchrone Replizierung bietet den StrictSync-Modus. Wenn der Schreibvorgang auf den sekundären Storage aus irgendeinem Grund nicht abgeschlossen wird, fällt der Applikations-I/O aus. Dadurch wird sichergestellt, dass die primären und sekundären Storage-Systeme identisch sind. Der Applikations-I/O zum primären Volume wird erst wieder fortgesetzt, nachdem die SnapMirror-Beziehung zum InSync-Status zurückkehrt. Falls der Primär-Storage ausfällt, kann der Applikations-I/O nach dem Failover ohne Datenverlust auf dem sekundären Storage fortgesetzt werden. Im StrictSync-Modus ist der RPO immer Null.

Storage-Replizierung basierend auf NetApp MetroCluster

Die folgende Abbildung bietet einen allgemeinen Überblick über die Lösung. Der Storage Cluster an jedem Standort sorgt für lokale Hochverfügbarkeit und wird für Produktions-Workloads verwendet. Die Daten an jedem Standort werden synchron zum anderen Standort repliziert und sind im Fall eines Disaster Failovers verfügbar.



Storage-Dimensionierung

Der folgende Abschnitt bietet einen Überblick über die Performance- und Kapazitätsüberlegungen für die Dimensionierung eines Storage-Systems für SAP HANA.

> Wenden Sie sich an Ihren Vertriebsmitarbeiter von NetApp oder einen NetApp Partner, um den Prozess der Storage-Größenbemessung zu unterstützen und eine passende Storage-Umgebung zu erstellen.

Überlegungen zur Performance

SAP hat eine statische Reihe von Storage-KPIs definiert. Diese KPIs sind für alle produktiven SAP HANA-Umgebungen gültig, unabhängig von der Speichergröße der Datenbank-Hosts und der Anwendungen, die die SAP HANA-Datenbank nutzen. Diese KPIs gelten für Single-Host-, mehrere Hosts-, Business Suite on HANA-, Business Warehouse on HANA-, S/4HANA- und BW/4HANA-Umgebungen. Daher hängt der aktuelle Ansatz zur Performance-Dimensionierung nur von der Anzahl aktiver SAP HANA-Hosts ab, die an das Storage-System angeschlossen sind.

> Storage-Performance-KPIs sind nur für produktive SAP HANA Systeme erforderlich.

SAP liefert ein Performance-Testtool, das zur Validierung der Storage-Performance für an den Storage angeschlossene aktive SAP HANA Hosts verwendet werden muss.

NetApp hat die maximale Anzahl an SAP HANA Hosts getestet und vordefiniert, die an ein bestimmtes Storage-Modell angeschlossen werden können, während gleichzeitig die erforderlichen Storage-KPIs von SAP für produktionsbasierte SAP HANA Systeme erfüllt werden.

> Die Storage Controller der zertifizierten FAS Produktfamilie können auch für SAP HANA mit anderen Festplattentypen oder Back-End-Lösungen verwendet werden, sofern sie von NetApp unterstützt werden und die Performance-KPIs von SAP HANA TDI erfüllen. Beispiele dafür sind NetApp Storage Encryption (NSE) und NetApp FlexArray Technologien.

In diesem Dokument wird die Festplattengröße für SAS-Festplatten und Solid-State-Laufwerke beschrieben.

Festplatten

Um die Storage-Performance-KPIs von SAP zu erfüllen, sind mindestens 10 Datenfestplatten (SAS mit 10.000 U/min) pro SAP HANA-Node erforderlich.

> Diese Berechnung erfolgt unabhängig vom verwendeten Storage Controller und Platten-Shelf.

Solid State Drives

Bei Solid State-Laufwerken (SSDs) wird die Anzahl der Datenfestplatten durch den Durchsatz der SAS-Verbindung von den Storage-Controllern zum SSD-Shelf bestimmt.

Mit dem SAP Performance-Testtool wurde die maximale Anzahl an SAP HANA Hosts ermittelt, die in einem Platten-Shelf ausgeführt werden können und die Mindestanzahl der pro SAP HANA Host benötigten SSDs erforderlich ist.

- Das 12-GB-SAS-Festplatten-Shelf (DS224C) mit 24 SSDs unterstützt bis zu 14 SAP HANA-Hosts, wenn das Festplatten-Shelf mit 12 GB verbunden ist.

- Das 6 Gbit SAS-Platten-Shelf (DS2246) mit 24 SSDs unterstützt bis zu 4 SAP HANA Hosts.

Die SSDs und SAP HANA-Hosts müssen auf beide Storage-Controller verteilt sein.

In der folgenden Tabelle ist die unterstützte Anzahl von SAP HANA-Hosts pro Festplatten-Shelf zusammengefasst.

	6-Gbit-SAS-Shelfs (DS2246) mit voller Betriebslast 24 SSDs	**12-GB-SAS-Shelfs (DS224C) mit 24 SSDs sind voll beladen**
Maximale Anzahl von SAP HANA-Hosts pro Festplatten-Shelf	4	14

Diese Berechnung erfolgt unabhängig vom eingesetzten Storage Controller. Durch das Hinzufügen weiterer Platten-Shelves wird nicht die maximale Anzahl von SAP HANA-Hosts erhöht, die ein Storage-Controller unterstützen kann.

NS224 NVMe-Shelf

Eine NVMe-SSD (Daten) unterstützt bis zu 2 SAP HANA-Hosts. Die SSDs und SAP HANA-Hosts müssen auf beide Storage-Controller verteilt sein.

Heterogenen Workloads

SAP HANA und andere Applikations-Workloads werden auf demselben Storage Controller oder im selben Storage-Aggregat unterstützt. Es ist jedoch eine NetApp Best Practice, SAP HANA-Workloads von allen anderen Applikations-Workloads zu trennen.

SAP HANA-Workloads und andere Applikations-Workloads können entweder auf demselben Storage-Controller oder demselben Aggregat implementiert werden. Ist dies der Fall, müssen Sie sicherstellen, dass für SAP HANA in der Umgebung mit heterogenen Workloads immer genug Performance verfügbar ist. NetApp empfiehlt zudem, Parameter der Quality of Service (QoS) zu verwenden, um die Auswirkungen anderer Applikationen auf SAP HANA Applikationen zu regulieren.

Mit dem SAP HCMT-Testtool muss überprüft werden, ob weitere SAP HANA Hosts auf einem Storage Controller ausgeführt werden können, der bereits für andere Workloads verwendet wird. SAP Applikations-Server können jedoch sicher auf demselben Storage-Controller platziert und aggregiert werden wie die SAP HANA Datenbanken.

Überlegungen zur Kapazität

Eine detaillierte Beschreibung der Kapazitätsanforderungen für SAP HANA ist im "SAP-Hinweis 1900823" Whitepaper:

Das Kapazitätsdimensionieren der gesamten SAP Landschaft mit mehreren SAP HANA Systemen muss mithilfe von SAP HANA Storage-Größenanpassungs-Tools von NetApp ermittelt werden. Wenden Sie sich an NetApp oder Ihren Ansprechpartner bei NetApp Partnern, um den Prozess der Storage-Größenbemessung für eine ausreichend dimensionierte Storage-Umgebung zu validieren.

Konfiguration des Performance-Testtool

Ab SAP HANA 1.0 SPS10 führte SAP Parameter ein, um das I/O-Verhalten anzupassen und die Datenbank für

das verwendete Datei- und Speichersystem zu optimieren. Diese Parameter müssen auch für das Performance-Test-Tool aus SAP (fsperf) gesetzt werden, wenn die Speicherleistung mit dem SAP-Testwerkzeug getestet wird.

Die Performance-Tests wurden von NetApp durchgeführt, um die optimalen Werte zu definieren. In der folgenden Tabelle sind die Parameter aufgeführt, die in der Konfigurationsdatei des SAP-Testwerkzeugs festgelegt werden müssen.

Parameter	Wert
max_parallel_io_Requests	128
Async_read_Submit	Ein
Async_write_submit_Active	Ein
Async_Write_Submit_Blocks	Alle

Weitere Informationen zur Konfiguration von SAP-Testtool finden Sie unter "SAP-Hinweis 1943937" Für HWCCT (SAP HANA 1.0) und "SAP-Hinweis 2493172" FÜR HCMT/HCOT (SAP HANA 2.0).

Das folgende Beispiel zeigt, wie Variablen für den HCMT/HCOT-Ausführungsplan festgelegt werden können.

```
…{
          "Comment": "Log Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "LogAsyncReadSubmit",
          "Value": "on",
          "Request": "false"
       },
       {
          "Comment": "Data Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "DataAsyncReadSubmit",
          "Value": "on",
          "Request": "false"
       },
       {
          "Comment": "Log Volume: Controls whether write requests can be
submitted asynchronously",
          "Name": "LogAsyncWriteSubmitActive",
          "Value": "on",
          "Request": "false"
       },
       {
          "Comment": "Data Volume: Controls whether write requests can be
submitted asynchronously",
          "Name": "DataAsyncWriteSubmitActive",
          "Value": "on",
          "Request": "false"
```

```
      },
      {
         "Comment": "Log Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "LogAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "DataAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "LogExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "DataExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      }, …
```

Diese Variablen müssen für die Testkonfiguration verwendet werden. Dies ist in der Regel bei den vordefinierten Testsuiten der Fall, die SAP mit dem HCMT/HCOT-Tool liefert. Das folgende Beispiel für einen 4k-Protokollschreibtest stammt aus einer Testsuite.

```
…
      {
         "ID": "D664D001-933D-41DE-A904F304AEB67906",
         "Note": "File System Write Test",
         "ExecutionVariants": [
            {
               "ScaleOut": {
                  "Port": "${RemotePort}",
                  "Hosts": "${Hosts}",
                  "ConcurrentExecution": "${FSConcurrentExecution}"
               },
               "RepeatCount": "${TestRepeatCount}",
               "Description": "4K Block, Log Volume 5GB, Overwrite",
               "Hint": "Log",
               "InputVector": {
                  "BlockSize": 4096,
                  "DirectoryName": "${LogVolume}",
                  "FileOverwrite": true,
                  "FileSize": 5368709120,
                  "RandomAccess": false,
                  "RandomData": true,
                  "AsyncReadSubmit": "${LogAsyncReadSubmit}",
                  "AsyncWriteSubmitActive":
"${LogAsyncWriteSubmitActive}",
                  "AsyncWriteSubmitBlocks":
"${LogAsyncWriteSubmitBlocks}",
                  "ExtMaxParallelIoRequests":
"${LogExtMaxParallelIoRequests}",
                  "ExtMaxSubmitBatchSize": "${LogExtMaxSubmitBatchSize}",
                  "ExtMinSubmitBatchSize": "${LogExtMinSubmitBatchSize}",
                  "ExtNumCompletionQueues":
"${LogExtNumCompletionQueues}",
                  "ExtNumSubmitQueues": "${LogExtNumSubmitQueues}",
                  "ExtSizeKernelIoQueue": "${ExtSizeKernelIoQueue}"
               }
            }, …
```

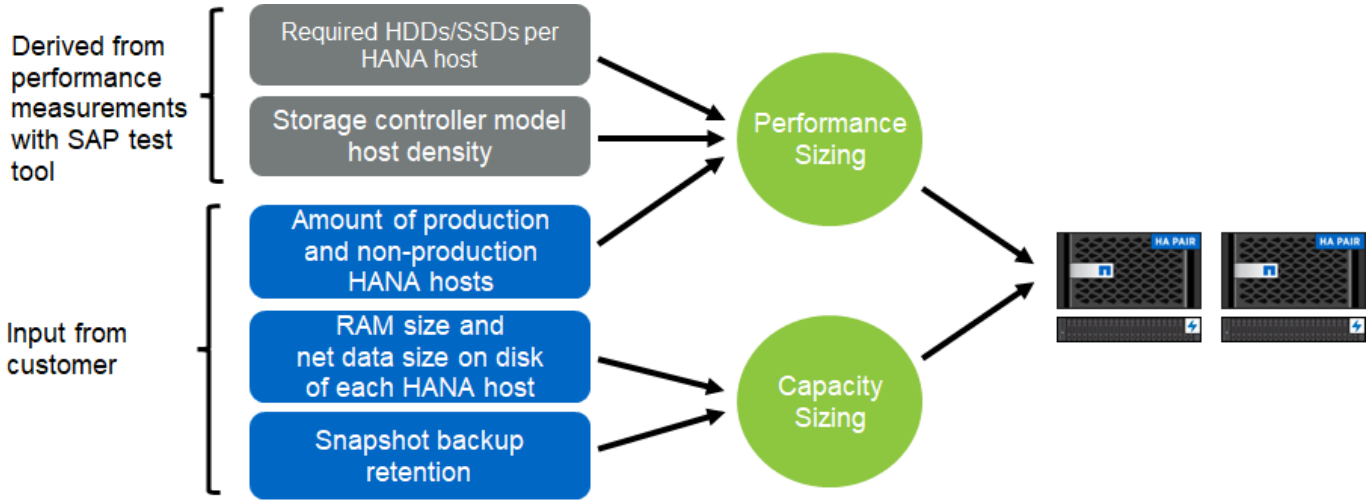
Übersicht über den Prozess zur Storage-Größenbemessung

Die Anzahl der Festplatten pro HANA Host und die Host-Dichte von SAP HANA für jedes Storage-Modell wurden mit dem Test-Tool SAP HANA ermittelt.

Der Dimensionierungsprozess erfordert Einzelheiten, z. B. die Anzahl der SAP HANA-Hosts in der Produktion und für die Produktion nichtproduktive Umgebung, die RAM-Größe jedes Hosts und die Aufbewahrungsdauer von Storage-basierten Snapshot Kopien für Backups. Die Anzahl der SAP HANA-Hosts bestimmt den Storage Controller und die Anzahl der benötigten Festplatten.

Die Größe des RAM, die Netto-Datengröße auf der Festplatte jedes SAP HANA-Hosts und der Aufbewahrungszeitraum für Snapshot-Backups werden als Inputs bei der Kapazitätsdimensionierung verwendet.

Die folgende Abbildung fasst den Dimensionierungsprozess zusammen.



Einrichtung und Konfiguration der Infrastruktur

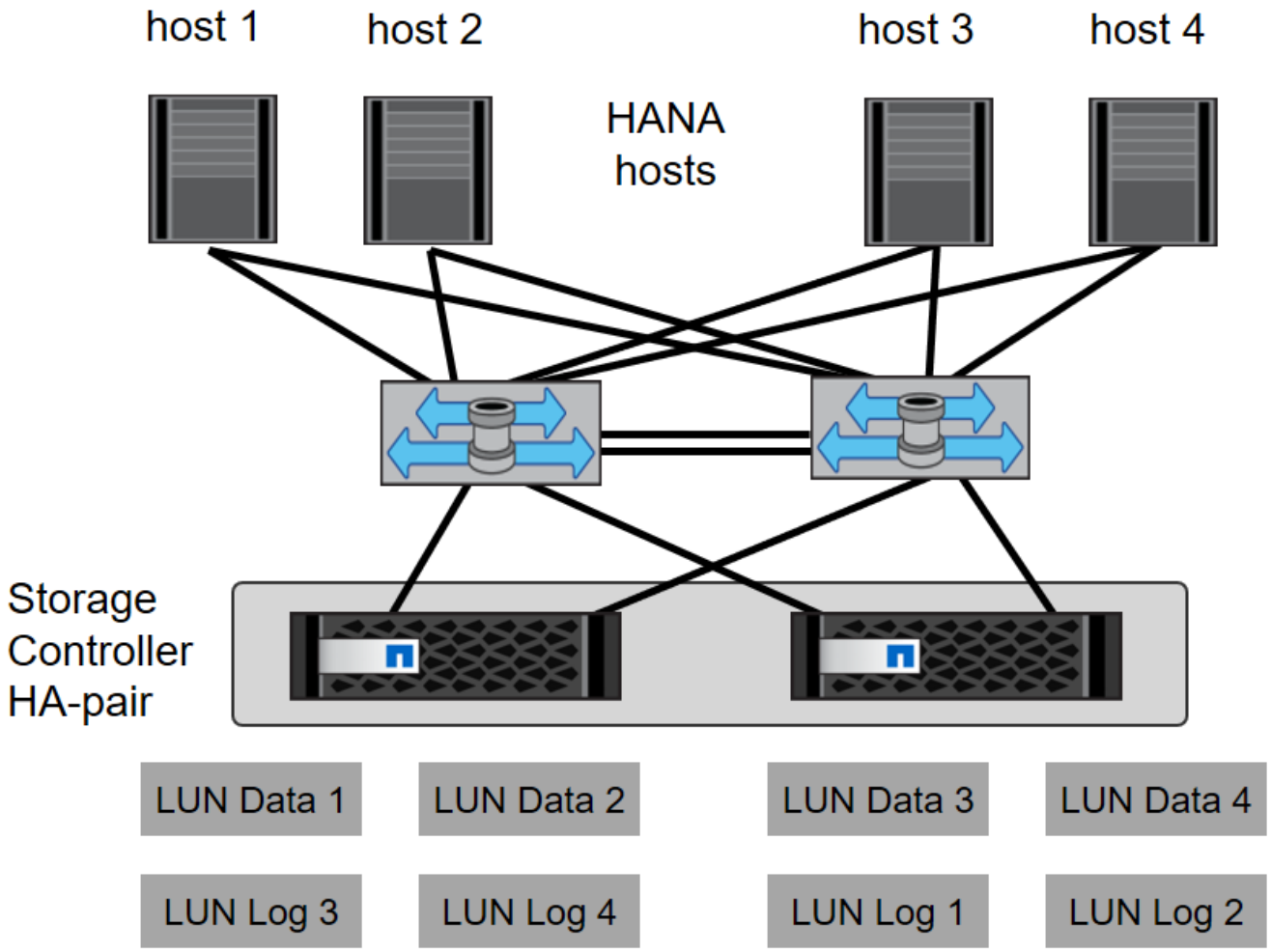
In den folgenden Abschnitten finden Sie Richtlinien zur Einrichtung und Konfiguration der SAP HANA-Infrastruktur sowie alle Schritte zur Einrichtung eines SAP HANA-Systems. In diesen Abschnitten werden die folgenden Beispielkonfigurationen verwendet:

- HANA-System mit SID=FC5
  - SAP HANA Einzel- und Mehrfachhost mit Linux Logical Volume Manager (LVM)
  - SAP HANA Einzelhost mit SAP HANA mehrere Partitionen

EINRICHTUNG VON SAN Fabric

Jeder SAP HANA-Server muss über eine redundante FCP-SAN-Verbindung mit einer Bandbreite von mindestens 8 Gbit/s. Für jeden an einen Storage Controller angeschlossenen SAP HANA-Host muss am Storage Controller mindestens 8 GBit/s Bandbreite konfiguriert sein.

Die folgende Abbildung zeigt ein Beispiel mit vier SAP HANA-Hosts, die mit zwei Storage-Controllern verbunden sind. Jeder SAP HANA-Host verfügt über zwei FCP-Ports, die mit der redundanten Fabric verbunden sind. Auf der Storage-Ebene sind vier FCP-Ports so konfiguriert, dass sie den erforderlichen Durchsatz für jeden SAP HANA Host liefern.



Zusätzlich zum Zoning auf der Switch-Ebene müssen Sie jede LUN auf dem Storage-System den Hosts zuordnen, die mit dieser LUN verbunden sind. Einfachheit beim Zoning auf dem Switch; das heißt, Festlegung eines Zoneneinteils, in dem alle Host-HBAs alle Controller-HBAs sehen können.

Zeitsynchronisierung

Sie müssen die Zeit zwischen den Storage-Controllern und den SAP HANA Datenbank-Hosts synchronisieren. Es muss der gleiche Zeitserver für alle Storage Controller und alle SAP HANA-Hosts festgelegt sein.

Einrichtung von Storage Controllern

In diesem Abschnitt wird die Konfiguration des NetApp Storage-Systems beschrieben. Sie müssen die primäre Installation und Einrichtung gemäß den entsprechenden ONTAP Setup- und Konfigurationsleitfäden abschließen.

Storage-Effizienz

Inline-Deduplizierung, Inline-Deduplizierung, Inline-Komprimierung und Inline-Data-Compaction werden von SAP HANA in einer SSD-Konfiguration unterstützt.

Die Aktivierung von Storage-Effizienzfunktionen in einer HDD-Konfiguration wird nicht unterstützt.

NetApp FlexGroup Volumes

Die Verwendung von NetApp FlexGroup Volumes wird für SAP HANA nicht unterstützt. Aufgrund der Architektur von SAP HANA bietet die Verwendung von FlexGroup Volumes keinen Vorteil und kann zu Performance-Problemen führen.

NetApp Volume- und Aggregatverschlüsselung

Die Verwendung von NetApp Volume Encryption (NVE) und NetApp Aggregate Encryption (NAE) wird bei SAP HANA unterstützt.

Quality of Service

QoS kann verwendet werden, um den Storage-Durchsatz für bestimmte SAP HANA Systeme oder nicht-SAP Applikationen auf einem Shared Controller zu begrenzen.

Produktion und Entwicklung/Test

Ein Anwendungsfall wäre, den Durchsatz von Entwicklungs- und Testsystemen zu begrenzen, damit sie bei einem gemischten Setup keinen Einfluss auf die Produktionssysteme haben. Während des Dimensionierungsprozesses sollten Sie die Performance-Anforderungen eines nicht für die Produktion verwendeten Systems ermitteln. Entwicklungs- und Testsysteme können mit niedrigeren Leistungswerten dimensioniert werden, typischerweise im Bereich von 20 % bis 50 % eines von SAP definierten Produktionssystems-KPI. Ein großer I/O-Schreibvorgang wirkt sich am stärksten auf die Performance des Storage-Systems aus. Daher sollte die QoS-Durchsatzbegrenzung auf einen Prozentsatz der entsprechenden KPI-Werte für die SAP HANA-Speicherleistung in den Daten- und Protokoll-Volumes gesetzt werden.

Shared-Umgebungen

Ein weiterer Anwendungsfall ist die Einschränkung des Durchsatzes bei umfangreichen Schreib-Workloads, insbesondere um zu vermeiden, dass diese Workloads Auswirkungen auf andere latenzempfindliche Schreib-Workloads haben. In solchen Umgebungen empfiehlt es sich, eine QoS-Gruppenrichtlinie ohne gemeinsam genutzten Durchsatz auf jede LUN innerhalb jeder SVM (Storage Virtual Machine) anzuwenden, um den maximalen Durchsatz jedes einzelnen Storage-Objekts auf den angegebenen Wert zu beschränken. So besteht weniger Gefahr, dass ein einzelner Workload andere Workloads negativ beeinflussen kann.

Dazu muss über die CLI des ONTAP-Clusters für jede SVM eine Gruppenrichtlinie erstellt werden:

```
qos policy-group create -policy-group <policy-name> -vserver <vserver
name> -max-throughput 1000MB/s -is-shared false
```

Und auf jede LUN in der SVM angewendet. Nachfolgend sehen Sie ein Beispiel, um die Richtliniengruppe auf alle vorhandenen LUNs innerhalb einer SVM anzuwenden:

```
lun modify -vserver <vserver name>  -path * -qos-policy-group  <policy-
name>
```

Dies muss für jede SVM geschehen. Der Name der QoS-Polizeigruppe für jede SVM muss unterschiedlich sein. Für neue LUNs kann die Richtlinie direkt angewendet werden:

```
lun create -vserver <vserver_name> -path  /vol/<volume_name>/<lun_name>
-size <size> -ostype <e.g. linux>  -qos-policy-group <policy-name>
```

Es wird empfohlen, 1000 MB/s als maximalen Durchsatz für eine bestimmte LUN zu verwenden. Wenn eine Applikation einen höheren Durchsatz erfordert, müssen mehrere LUNs mit LUN-Striping verwendet werden, um die erforderliche Bandbreite bereitzustellen. Dieser Leitfaden enthält ein Beispiel für SAP HANA auf Basis von Linux LVM in Abschnitt "Host-Setup".

Das Limit gilt auch für Lesevorgänge. Daher genügend LUNs verwenden, um die erforderlichen SLAs für die Startzeit der SAP HANA-Datenbank und für Backups zu erfüllen.

NetApp FabricPool

NetApp FabricPool darf nicht für aktive primäre Filesysteme in SAP HANA Systemen verwendet werden. Dazu gehören die Dateisysteme für den Daten- und Protokollbereich sowie die `/hana/shared` File-System. Dies führt zu unvorhersehbarer Performance, insbesondere beim Start eines SAP HANA Systems.

Die Verwendung der „nur-Snapshots“ Tiering-Politik ist möglich sowie auch die Nutzung von FabricPool im Allgemeinen an einem Backup-Ziel wie SnapVault oder SnapMirror Ziel.

Durch die Verwendung von FabricPool für das Tiering von Snapshot Kopien im Primärspeicher oder die Verwendung von FabricPool zu einem Backup-Ziel werden die für die Wiederherstellung und das Recovery einer Datenbank oder anderer Aufgaben benötigte Zeit, beispielsweise das Erstellen von Systemklonen oder Korrektursystemen, geändert. Nehmen Sie dies bei der Planung Ihrer gesamten Lifecycle- Management-Strategie in Betracht und prüfen Sie, ob Ihre SLAs unter Verwendung dieser Funktion noch erfüllt werden.

FabricPool ist eine gute Option, um Log-Backups auf eine andere Storage Tier zu verschieben. Das Verschieben von Backups beeinträchtigt die für das Recovery einer SAP HANA Datenbank erforderliche Zeit. Daher sollte die Option „Tiering-minimum-cooling-days“ auf einen Wert gesetzt werden, der Log-Backups, die routinemäßig für die Wiederherstellung benötigt werden, auf der lokalen fast Storage Tier platziert.

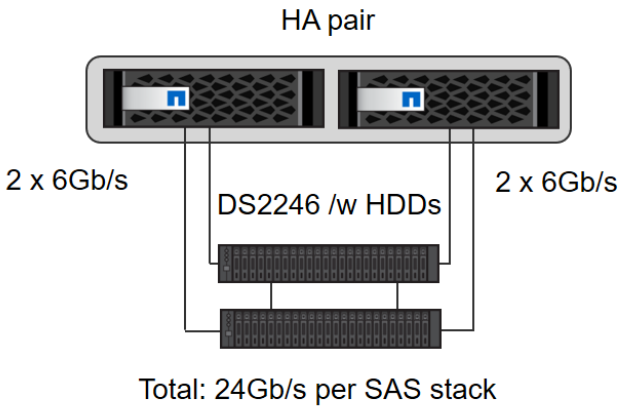
Speicher konfigurieren

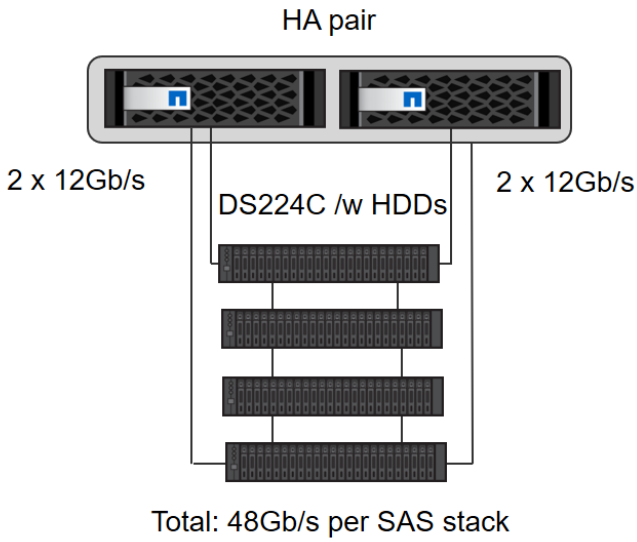
In der folgenden Übersicht sind die erforderlichen Schritte zur Storage-Konfiguration zusammengefasst. Jeder Schritt wird in den nachfolgenden Abschnitten näher beschrieben. Bevor Sie diese Schritte initiieren, sollten Sie das Setup der Storage-Hardware, die Installation der ONTAP Software und die Verbindung der Speicher-FCP-Ports mit dem SAN Fabric abschließen.

1. Überprüfen Sie die richtige Festplatten-Shelf-Konfiguration, wie in beschriebenFestplatten-Shelf-Verbindung.
2. Erstellen und konfigurieren Sie die erforderlichen Aggregate, wie in beschrieben.Konfiguration von Aggregaten
3. Erstellen Sie eine Storage Virtual Machine (SVM), wie in beschrieben.Konfiguration von Storage Virtual Machines
4. Erstellung logischer Schnittstellen (LIFs), wie in beschrieben.Konfiguration der logischen Schnittstelle
5. Erstellen Sie Initiatorgruppen mit weltweiten Namen (WWNs) von hana-Servern wie im Abschnitt Link:hana-fas-fc-Storage-Controller-Setup.HTML#Initiator-groups beschriebenInitiatorgruppen.
6. Erstellen und konfigurieren Sie Volumes und LUNs innerhalb der Aggregate wie im Abschnitt beschrieben

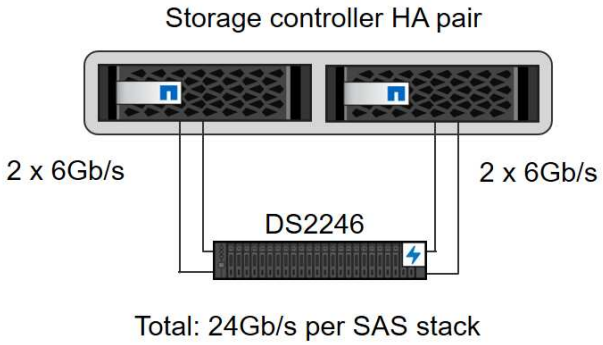
"Einzelhost-Setup" für einzelne Hosts oder im Abschnitt "Einrichtung mehrerer Hosts" für mehrere Hosts

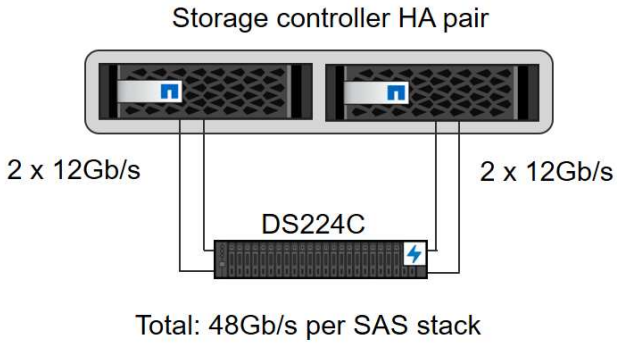
Mit HDDs können maximal zwei DS2246 Festplatten-Shelfs oder vier DS224C Festplatten-Shelfs mit einem SAS-Stack verbunden werden, um die erforderliche Performance für die SAP HANA-Hosts zu liefern, wie in der folgenden Abbildung dargestellt. Die Festplatten in jedem Shelf müssen gleichmäßig auf beide Controller des HA-Paars verteilt werden.





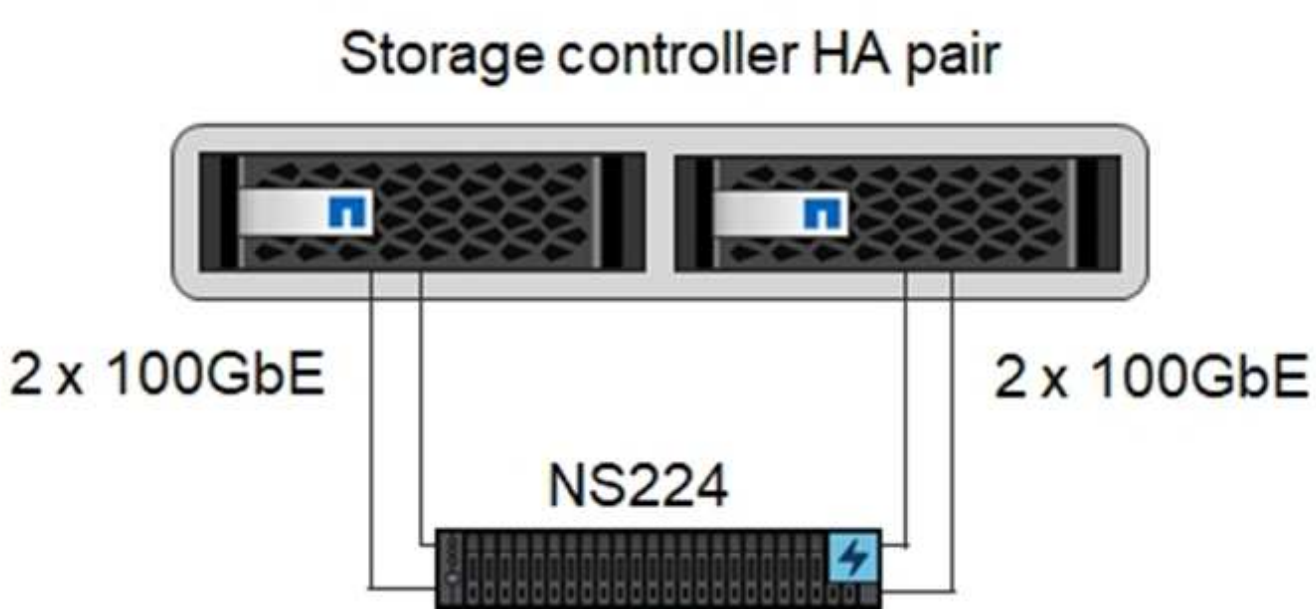
Bei SSDs kann maximal ein Platten-Shelf mit einem SAS-Stack verbunden werden, um die erforderliche Performance für die SAP HANA-Hosts zu liefern, wie in der folgenden Abbildung dargestellt. Die Festplatten in jedem Shelf müssen gleichmäßig auf beide Controller des HA-Paars verteilt werden. Mit dem DS224C Festplatten-Shelf können auch Quad-Path-SAS-Kabel verwendet werden, ist aber nicht erforderlich.





NVMe-Festplatten-Shelves

Jedes NS224 NVMe-Festplatten-Shelf ist, wie in der folgenden Abbildung dargestellt, mit zwei 100-GbE-Ports pro Controller verbunden. Die Festplatten in jedem Shelf müssen gleichmäßig auf beide Controller des HA-Paars verteilt werden.

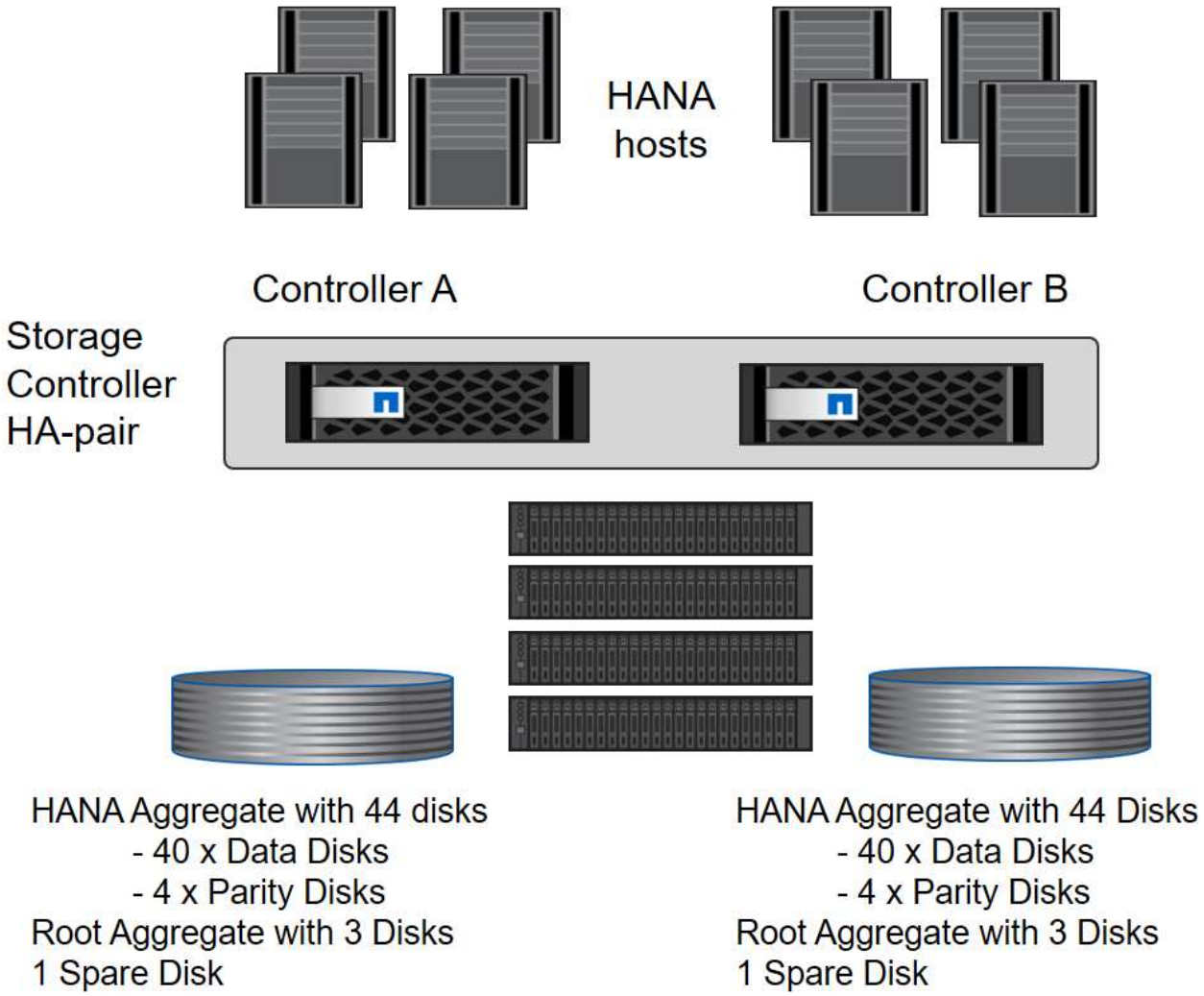


Konfiguration von Aggregaten

Im Allgemeinen müssen zwei Aggregate pro Controller konfiguriert werden, unabhängig davon, welches Platten-Shelf oder Festplattentechnologie (SSD oder HDD) zum Einsatz kommt. Dieser Schritt ist notwendig, damit Sie alle verfügbaren Controller-Ressourcen nutzen können. Für Systeme der FAS 2000 Serie genügt ein Daten-Aggregat.

Aggregatkonfiguration mit HDDs

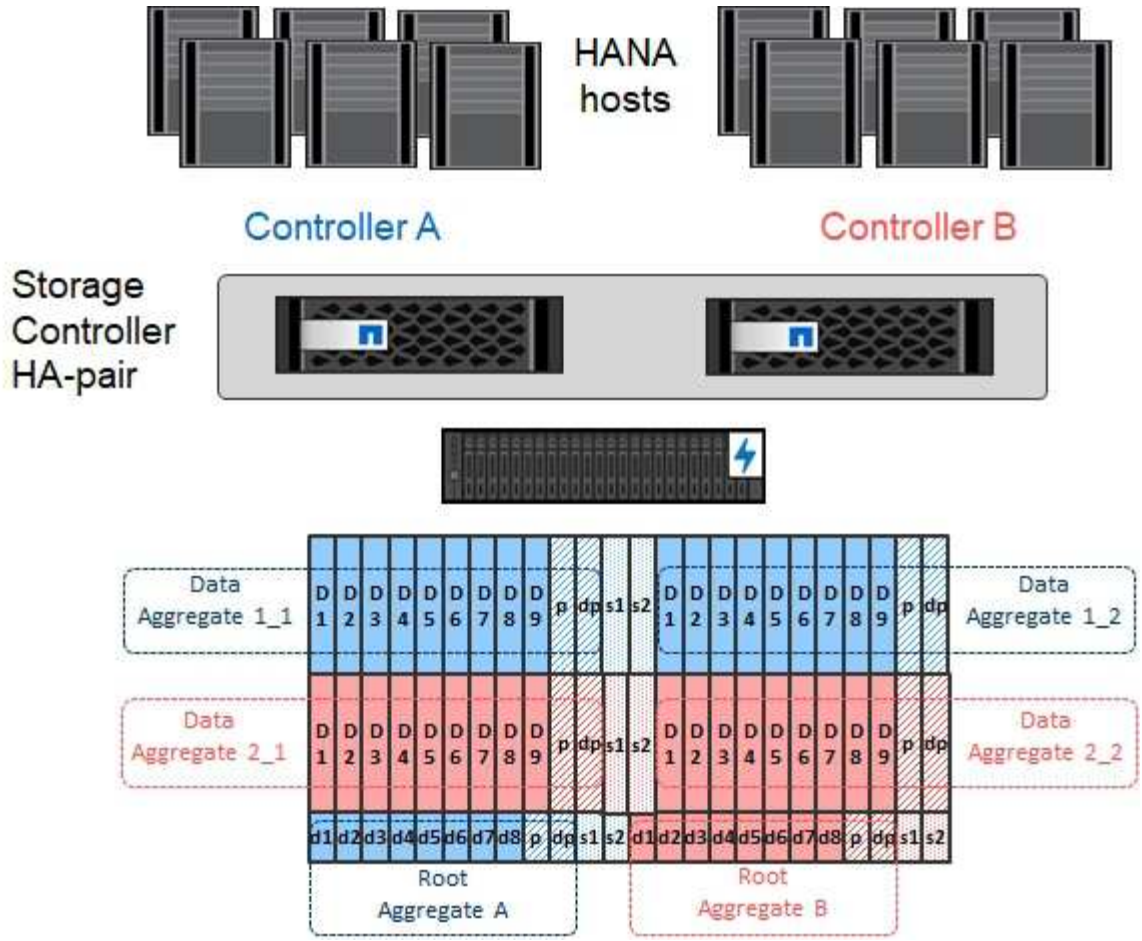
Die folgende Abbildung zeigt eine Konfiguration für acht SAP HANA-Hosts. Vier SAP HANA-Hosts sind mit jedem Storage-Controller verbunden. Zwei separate Aggregate, eines an jedem Storage Controller, sind konfiguriert. Jedes Aggregat ist mit 4 × 10 = 40 Datenfestplatten (HDDs) konfiguriert.



Aggregat-Konfiguration mit nur SDD-Systemen

Im Allgemeinen müssen zwei Aggregate pro Controller konfiguriert werden, unabhängig davon, welches Platten-Shelf oder Festplattentechnologie (SSDs oder HDDs) zum Einsatz kommt.

Die folgende Abbildung zeigt eine Konfiguration mit 12 SAP HANA Hosts, die auf einem 12-GB-SAS-Shelf ausgeführt werden und mit ADPv2 konfiguriert sind. Sechs SAP-HANA-Hosts sind mit jedem Storage-Controller verbunden. Vier separate Aggregate, zwei an jedem Storage Controller, sind konfiguriert. Jedes Aggregat ist mit 11 Festplatten mit neun Daten und zwei Parity-Festplatten-Partitionen konfiguriert. Für jeden Controller stehen zwei Ersatzpartitionen zur Verfügung.

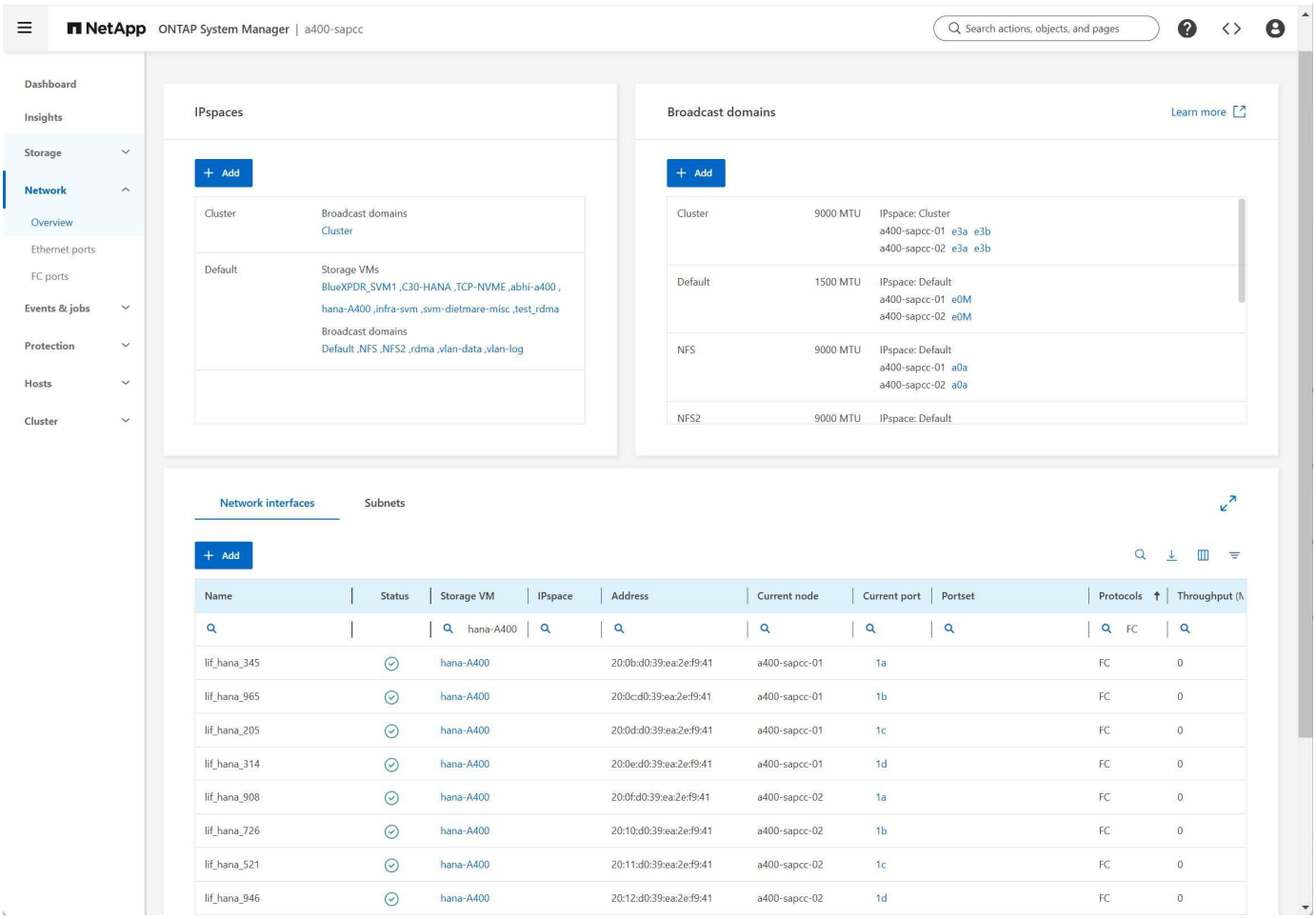


Konfiguration von Storage Virtual Machines

SAP Landschaften mit SAP HANA Datenbanken aus mehreren Hosts können eine einzige SVM verwenden. Falls erforderlich, kann jeder SAP-Landschaft auch eine SVM zugewiesen werden, falls diese von verschiedenen Teams innerhalb eines Unternehmens gemanagt werden. Die Screenshots und die Befehlsausgaben in diesem Dokument verwenden eine SVM mit dem Namen `hana`.

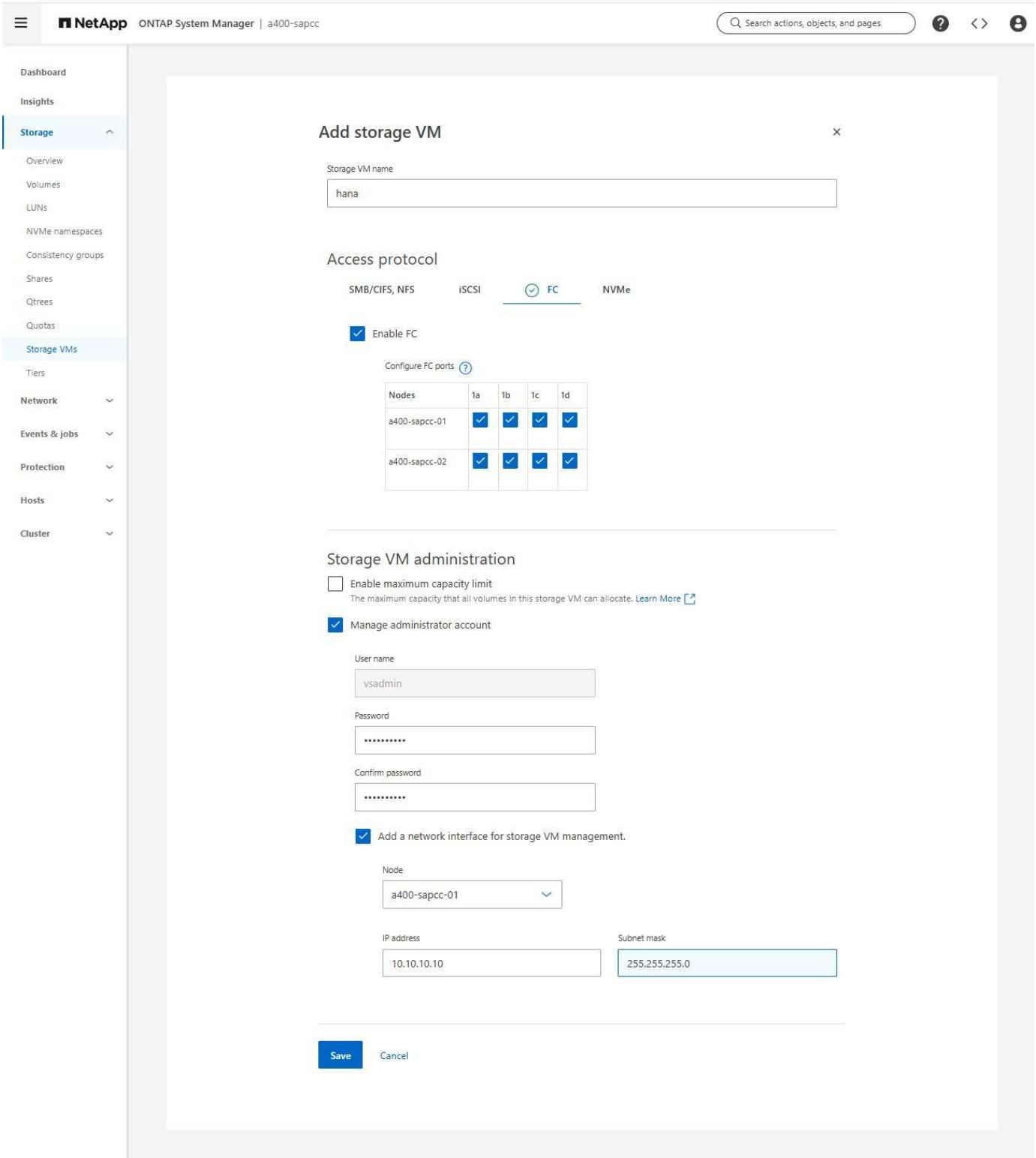
Konfiguration der logischen Schnittstelle

Innerhalb der Storage-Cluster-Konfiguration muss eine Netzwerkschnittstelle (LIF) erstellt und einem dedizierten FCP-Port zugewiesen werden. Wenn beispielsweise vier FCP-Ports aus Performance-Gründen erforderlich sind, müssen vier LIFs erstellt werden. Die folgende Abbildung zeigt einen Screenshot der acht LIFs, die auf der SVM konfiguriert wurden.



Während der SVM-Erstellung mit ONTAP 9 System Manager können alle erforderlichen physischen FCP-Ports ausgewählt und automatisch eine LIF pro physischem Port erstellt werden.

In der folgenden Abbildung ist die Erstellung von SVMs und LIFs mit ONTAP System Manager dargestellt.



Initiatorgruppen

Eine Initiatorgruppe kann für jeden Server oder für eine Gruppe von Servern konfiguriert werden, die Zugriff auf eine LUN benötigen. Für die iGroup Konfiguration sind die weltweiten Port-Namen (WWPNs) der Server erforderlich.

Verwenden der `sanlun` Führen Sie den folgenden Befehl aus, um die WWPNs jedes SAP HANA-Hosts abzurufen:

```
stlrx300s8-6:~ # sanlun fcp show adapter
/sbin/udevadm
/sbin/udevadm

host0 ..... WWPN:2100000e1e163700
host1 ..... WWPN:2100000e1e163701
```

Das `sanlun` Tool ist Teil der NetApp Host Utilities und muss auf jedem SAP HANA-Host installiert sein. Weitere Details finden Sie in Abschnitt "Hosteinrichtung:"

Die Initiatorgruppen können über die CLI des ONTAP-Clusters erstellt werden.

```
lun igroup create -igroup <igroup name> -protocol fcp -ostype linux
-initiator <list of initiators> -vserver <SVM name>
```

Einzelner Host

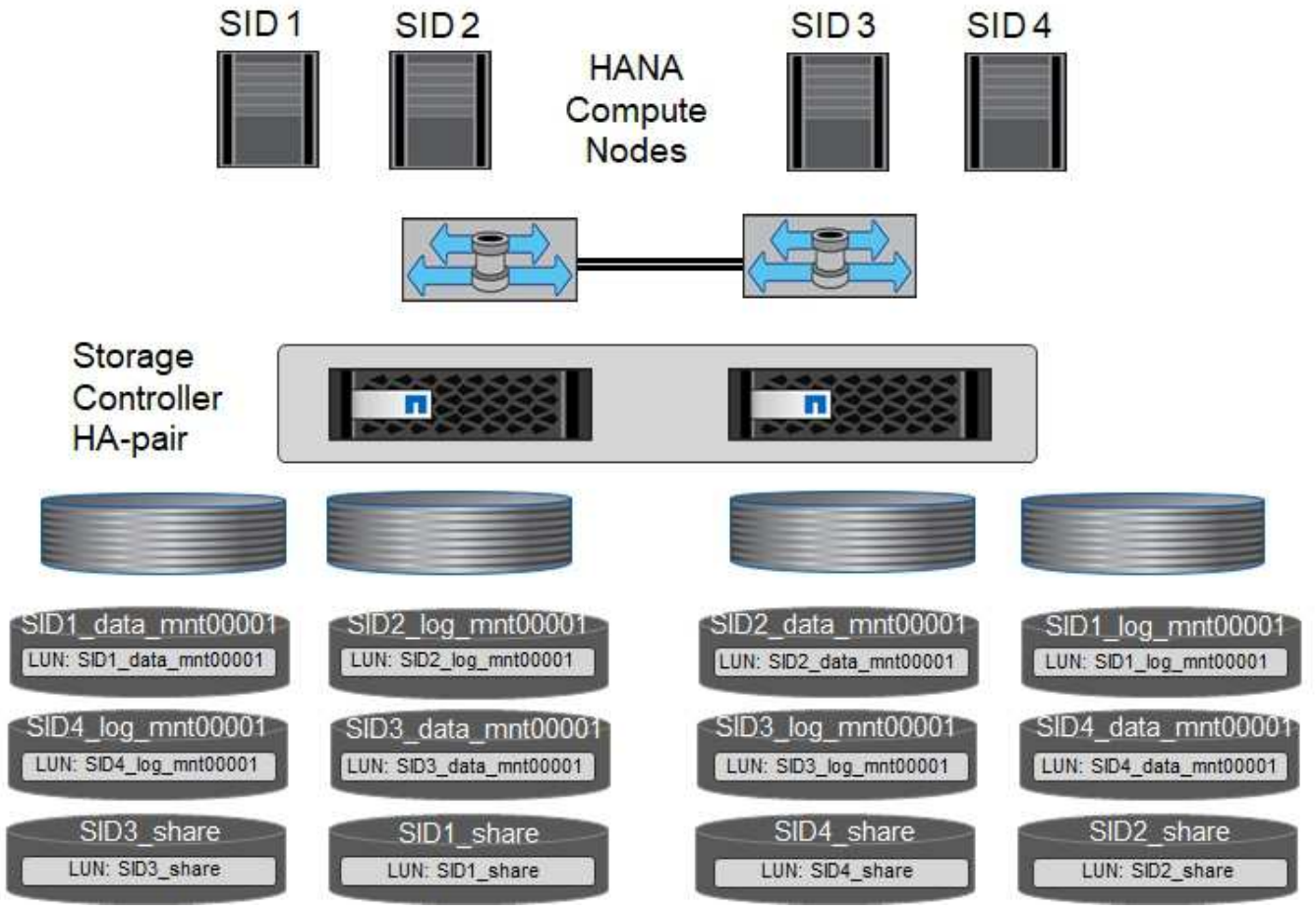
Einzelner Host

Dieser Abschnitt beschreibt die Konfiguration des NetApp-Speichersystems speziell für SAP HANA-Einzelhostsysteme

Volume- und LUN-Konfiguration für SAP HANA Single-Host-Systeme

Die folgende Abbildung zeigt die Volume-Konfiguration von vier SAP HANA-Systemen mit einem Host. Die Daten- und Protokoll-Volumes jedes SAP HANA Systems werden auf verschiedene Storage Controller verteilt. Beispielsweise ist das Volume `SID1_data_mnt00001` auf Controller A konfiguriert und das Volume `SID1_log_mnt00001` auf Controller B konfiguriert. Innerhalb jedes Volumes wird eine einzelne LUN konfiguriert.

Wird für die SAP HANA Systeme nur ein Storage-Controller eines Hochverfügbarkeitspaars (HA) verwendet, können Daten-Volumes und Protokoll-Volumes auch auf demselben Storage Controller gespeichert werden.



Für jeden SAP HANA-Host, ein Daten-Volume, ein Protokoll-Volume und ein Volume für `/hana/shared` Werden konfiguriert. Die folgende Tabelle zeigt eine Beispielkonfiguration mit vier SAP HANA Single-Host-Systemen.

Zweck	Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregieren 2 bei Controller B
Daten-, Protokoll- und freigegebene Volumes für System SID1	Datenvolumen: SID1_Data_mnt00001	Freigegebenes Volume: SID1_Shared	–	Protokollvolumen: SID1_log_mnt00001
Daten-, Protokoll- und freigegebene Volumes für System SID2	–	Protokollvolumen: SID2_log_mnt00001	Datenvolumen: SID2_Data_mnt00001	Freigegebenes Volume: SID2_Shared
Daten-, Protokoll- und gemeinsam genutzte Volumes für System SID3	Gemeinsam genutztes Volume: SID3_shared	Datenvolumen: SID3_Data_mnt00001	Protokollvolumen: SID3_log_mnt00001	–
Daten-, Protokoll- und gemeinsam genutzte Volumes für System SID4	Protokollvolumen: SID4_log_mnt00001	–	Gemeinsam genutztes Volume: SID4_shared	Datenvolumen: SID4_Data_mnt00001

Die nächste Tabelle zeigt ein Beispiel für die Mount-Point-Konfiguration für ein System mit einem einzelnen

Host.

LUN	Bereitstellungspunkt beim HANA-Host	Hinweis
SID1_Data_mnt00001	/hana/Data/SID1/mnt00001	Mit /etc/fstab-Eintrag montiert
SID1_log_mnt00001	/hana/log/SID1/mnt00001	Mit /etc/fstab-Eintrag montiert
SID1_Shared	/hana/Shared/SID1	Mit /etc/fstab-Eintrag montiert

Mit der beschriebenen Konfiguration wird der verwendet `/usr/sap/SID1` Verzeichnis, in dem das Standard-Home-Verzeichnis des Benutzers SID1adm gespeichert ist, befindet sich auf der lokalen Festplatte. Für ein Disaster Recovery mit festplattenbasierter Replizierung empfiehlt NetApp die Erstellung einer zusätzlichen LUN innerhalb von `SID1_shared` Volume für das `/usr/sap/SID1` Verzeichnis so dass alle Dateisysteme auf dem zentralen Speicher sind.

Volume- und LUN-Konfiguration für SAP HANA Single-Host-Systeme mit Linux LVM

Der Linux LVM kann verwendet werden, um die Leistung zu steigern und um LUN-Größenbeschränkungen zu beheben. Die verschiedenen LUNs einer LVM Volume-Gruppe sollten in einem anderen Aggregat und einem anderen Controller gespeichert werden. Die folgende Tabelle enthält ein Beispiel für zwei LUNs pro Volume-Gruppe.

Es ist nicht notwendig, LVM mit mehreren LUNs zu verwenden, um die SAP HANA KPIs zu erfüllen, aber es wird empfohlen

Zweck	Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregieren 2 bei Controller B
Daten-, Protokoll- und gemeinsam genutzte Volumes für LVM-basierte Systeme	Datenvolumen: SID1_Data_mnt00001	Gemeinsames Volume: SID1_Shared Log2 Volume: SID1_log2_mnt00001	Daten2 Volumen: SID1_data2_mnt00001	Protokollvolumen: SID1_log_mnt00001

Mit der beschriebenen Konfiguration wird der verwendet `/usr/sap/SID1` Verzeichnis, in dem das Standard-Home-Verzeichnis des Benutzers SID1adm gespeichert ist, befindet sich auf der lokalen Festplatte. Für ein Disaster Recovery mit festplattenbasierter Replizierung empfiehlt NetApp die Erstellung einer zusätzlichen LUN innerhalb von `SID1_shared` Volume für das `/usr/sap/SID1` Verzeichnis so dass alle Dateisysteme auf dem zentralen Speicher sind.

Volume-Optionen

Die in der folgenden Tabelle aufgeführten Volume-Optionen müssen auf allen für SAP HANA verwendeten Volumes überprüft und festgelegt werden.

Aktion	ONTAP 9
Deaktivieren Sie automatische Snapshot Kopien	vol modify –vserver <vserver-Name> -Volume <volname> -Snapshot-Policy keine

Aktion	ONTAP 9
Deaktivieren Sie die Sichtbarkeit des Snapshot Verzeichnisses	vol modify -vserver <vserver-Name> -Volume <volname> -Snapdir-Access false

Erstellen von LUNs, Volumes und Zuordnen von LUNs zu Initiatorgruppen

Sie können NetApp ONTAP System Manager verwenden, um Storage Volumes und LUNs zu erstellen und sie Initiatorgruppen der Server und der ONTAP CLI zuzuordnen. In diesem Leitfaden wird die Verwendung der CLI beschrieben.

Erstellen von LUNs, Volumes und Zuordnen von LUNs zu Initiatorgruppen über die CLI

Dieser Abschnitt zeigt eine Beispielkonfiguration unter Verwendung der Befehlszeile mit ONTAP 9 für ein SAP HANA-Einzelhostsystem mit SID FC5 unter Verwendung von LVM und zwei LUNs pro LVM-Volume-Gruppe:

1. Erstellung aller erforderlichen Volumes

```
vol create -volume FC5_data_mnt00001 -aggregate aggr1_1 -size 1200g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_log_mnt00001  -aggregate aggr1_2 -size 280g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_data2_mnt00001 -aggregate aggr1_2 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_log2_mnt00001  -aggregate aggr1_1 -size 280g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_shared -aggregate aggr1_1 -size 512g -state
online -policy default -snapshot-policy none -junction-path /FC5_shared
-encrypt false  -space-guarantee none
```

2. Erstellen Sie alle LUNs.

```
lun create -path  /vol/FC5_data_mnt00001/FC5_data_mnt00001   -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log_mnt00001/FC5_log_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
```

3. Erstellen Sie die Initiatorgruppe für alle Ports, die zu den Sythe-Hosts von FC5 gehören.

```
lun igroup create -igroup HANA-FC5 -protocol fcp -ostype linux
-initiator 10000090fadcc5fa,10000090fadcc5fb -vserver hana
```

4. Ordnen Sie alle LUNs der erstellten Initiatorgruppe zu.

```
lun map -path /vol/FC5_data_mnt00001/FC5_data_mnt00001    -igroup HANA-
FC5
lun map -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001  -igroup HANA-
FC5
lun map -path /vol/FC5_log_mnt00001/FC5_log_mnt00001  -igroup HANA-FC5
lun map -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001  -igroup HANA-FC5
```

Mehrere Hosts

Mehrere Hosts

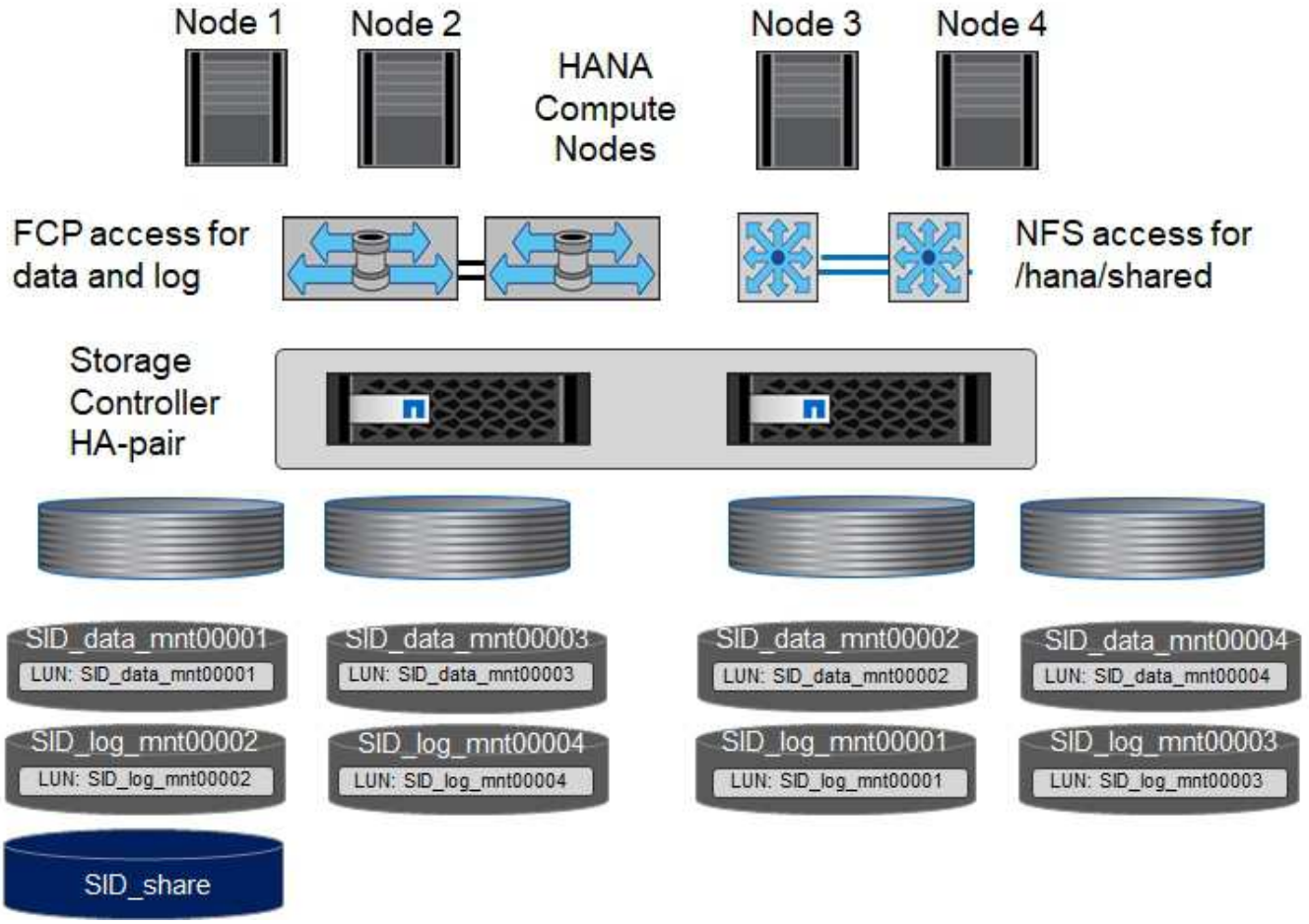
Dieser Abschnitt beschreibt die Konfiguration des NetApp-Speichersystems speziell für SAP HANA-Mehrfachhostsysteme

Volume- und LUN-Konfiguration für SAP HANA Multiple-Host-Systeme

Die folgende Abbildung zeigt die Volume-Konfiguration eines SAP HANA Systems mit 4+1 und mehreren Hosts. Die Daten-Volumes und Protokoll-Volumes jedes SAP HANA-Hosts werden auf verschiedene Storage-Controller verteilt. Beispiel: Das Volume `SID_data_mnt00001` Wird für Controller A und Volume konfiguriert `SID_log_mnt00001` Ist auf Controller B konfiguriert Eine LUN ist innerhalb jedes Volumes konfiguriert.

Der `/hana/shared` Das Volume muss von allen HANA-Hosts zugänglich sein und wird daher mithilfe von NFS exportiert. Obwohl es für die keine spezifischen Performance-KPIs gibt `/hana/shared` NetApp empfiehlt die Verwendung einer 10-Gbit-Ethernet-Verbindung.

Wenn für das SAP HANA System nur ein Storage-Controller eines HA-Paars verwendet wird, können Daten- und Protokoll-Volumes auch auf demselben Storage Controller gespeichert werden.



Für jeden SAP HANA-Host werden ein Daten-Volume und ein Protokoll-Volume erstellt. Der `/hana/shared` Das Volume wird von allen Hosts des SAP HANA-Systems verwendet. Die folgende Abbildung zeigt eine Beispielkonfiguration für ein SAP HANA System mit 4+1 mehreren Hosts.

Zweck	Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregieren 2 bei Controller B
Daten- und Protokoll-Volumes für Node 1	Datenvolumen: SID_Data_mnt00001	–	Protokollvolumen: SID_log_mnt00001	–
Daten- und Protokoll-Volumes für Node 2	Protokollvolumen: SID_log_mnt002	–	Datenvolumen: SID_Data_mnt002	–
Daten- und Protokoll-Volumes für Node 3	–	Datenvolumen: SID_Data_mnt00003	–	Protokollvolumen: SID_log_mnt00003
Daten- und Protokoll-Volumes für Node 4	–	Protokollvolumen: SID_log_mnt004	–	Datenvolumen: SID_Data_mnt00004

Zweck	Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregieren 2 bei Controller B
Gemeinsames Volume für alle Hosts	Gemeinsam genutztes Volume: SID_shared	–	–	–

Die nächste Tabelle zeigt die Konfiguration und die Mount-Punkte eines Systems mit mehreren Hosts mit vier aktiven SAP HANA-Hosts.

LUN oder Volume	Bereitstellungspunkt beim SAP HANA-Host	Hinweis
LUN: SID_Data_mnt00001	/hana/Data/SID/mnt00001	Montiert mit Speicheranschluss
LUN: SID_log_mnt00001	/hana/log/SID/mnt00001	Montiert mit Speicheranschluss
LUN: SID_Data_mnt002	/hana/Data/SID/mnt002	Montiert mit Speicheranschluss
LUN: SID_log_mnt002	/hana/log/SID/mnt002	Montiert mit Speicheranschluss
LUN: SID_Data_mnt003	/hana/Data/SID/mnt003	Montiert mit Speicheranschluss
LUN: SID_log_mnt003	/hana/log/SID/mnt003	Montiert mit Speicheranschluss
LUN: SID_Data_mnt004	/hana/Data/SID/mnt004	Montiert mit Speicheranschluss
LUN: SID_log_mnt004	/hana/log/SID/mnt004	Montiert mit Speicheranschluss
Volume: SID_Shared	/hana/Shared/SID	Gemountet auf allen Hosts mit NFS und /etc/fstab Eintrag

Bei der beschriebenen Konfiguration befindet sich das `/usr/sap/SID` Verzeichnis, in dem das Standard-Home-Verzeichnis des Benutzers SIDadm gespeichert ist, auf der lokalen Festplatte für jeden HANA-Host. Bei einer Disaster-Recovery-Einrichtung mit festplattenbasierter Replizierung empfiehlt NetApp die Erstellung von vier zusätzlichen Unterverzeichnissen im `SID_shared` Volume für das `/usr/sap/SID` Filesystem, damit jeder Datenbank-Host über alle Dateisysteme im zentralen Storage verfügt.

Volume- und LUN-Konfiguration für SAP HANA Systeme mit mehreren Hosts unter Verwendung von Linux LVM

Der Linux LVM kann verwendet werden, um die Leistung zu steigern und um LUN-Größenbeschränkungen zu beheben. Die verschiedenen LUNs einer LVM Volume-Gruppe sollten in einem anderen Aggregat und einem anderen Controller gespeichert werden. Die folgende Tabelle zeigt ein Beispiel für zwei LUNs pro Volume-Gruppe für ein 2+1 SAP HANA System mit mehreren Hosts.

Es ist nicht notwendig, LVM zu verwenden, um mehrere LUNs zu kombinieren und so die SAP HANA-KPIs zu erfüllen, es wird jedoch empfohlen.

Zweck	Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregieren 2 bei Controller B
Daten- und Protokoll-Volumes für Node 1	Datenvolumen: SID_Data_mnt00001	Log2-Volumen: SID_log2_mnt00001	Protokollvolumen: SID_log_mnt00001	Daten2 Volumen: SID_data2_mnt00001

Zweck	Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregieren 2 bei Controller B
Daten- und Protokoll-Volumes für Node 2	Log2-Volumen: SID_log2_mnt002	Datenvolumen: SID_Data_mnt002	Daten2 Volumen: SID_data2_mnt002	Protokollvolumen: SID_log_mnt002
Gemeinsames Volume für alle Hosts	Gemeinsam genutztes Volume: SID_shared	–	–	–

Volume-Optionen

Die in der folgenden Tabelle aufgeführten Volume-Optionen müssen auf allen für SAP HANA verwendeten Volumes überprüft und festgelegt werden.

Aktion	ONTAP 9
Deaktivieren Sie automatische Snapshot Kopien	vol modify –vserver <vserver-Name> -Volume <volname> -Snapshot-Policy keine
Deaktivieren Sie die Sichtbarkeit des Snapshot Verzeichnisses	vol modify -vserver <vserver-Name> -Volume <volname> -Snapdir-Access false

Erstellen von LUNs, Volumes und Zuordnen von LUNs zu Initiatorgruppen

Sie können NetApp ONTAP System Manager verwenden, um Storage Volumes und LUNs zu erstellen und sie Initiatorgruppen der Server und der ONTAP CLI zuzuordnen. In diesem Leitfaden wird die Verwendung der CLI beschrieben.

Erstellen von LUNs, Volumes und Zuordnen von LUNs zu Initiatorgruppen über die CLI

Dieser Abschnitt zeigt eine Beispielkonfiguration mit der Befehlszeile mit ONTAP 9 für ein 2+1 SAP HANA mehrere Hostsysteme mit SID FC5 unter Verwendung von LVM und zwei LUNs pro LVM Volume-Gruppe.

1. Erstellung aller erforderlichen Volumes

```
vol create -volume FC5_data_mnt00001 -aggregate aggr1_1 -size 1200g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_log_mnt00002  -aggregate aggr2_1 -size 280g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_log_mnt00001  -aggregate aggr1_2 -size 280g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_data_mnt00002  -aggregate aggr2_2 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_data2_mnt00001 -aggregate aggr1_2 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_log2_mnt00002  -aggregate aggr2_2 -size 280g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_log2_mnt00001  -aggregate aggr1_1 -size 280g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_data2_mnt00002  -aggregate aggr2_1 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_shared -aggregate aggr1_1 -size 512g -state
online -policy default -snapshot-policy none -junction-path /FC5_shared
-encrypt false  -space-guarantee none
```

2. Erstellen Sie alle LUNs.

```
lun create -path  /vol/FC5_data_mnt00001/FC5_data_mnt00001   -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data_mnt00002/FC5_data_mnt00002 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data2_mnt00002/FC5_data2_mnt00002 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log_mnt00001/FC5_log_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log_mnt00002/FC5_log_mnt00002 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log2_mnt00002/FC5_log2_mnt00002 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
```

3. Erstellen Sie die Initiatorgruppe für alle Server, die zu System FC5 gehören.

```
lun igroup create -igroup HANA-FC5 -protocol fcp -ostype linux
-initiator 10000090fadcc5fa,10000090fadcc5fb,
10000090fadcc5c1,10000090fadcc5c2,  10000090fadcc5c3,10000090fadcc5c4
-vserver hana
```

4. Ordnen Sie alle LUNs der erstellten Initiatorgruppe zu.

```
lun map -path  /vol/FC5_data_mnt00001/FC5_data_mnt00001    -igroup HANA-
FC5
lun map -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001  -igroup HANA-
FC5
lun map -path /vol/FC5_data_mnt00002/FC5_data_mnt00002  -igroup HANA-FC5
lun map -path /vol/FC5_data2_mnt00002/FC5_data2_mnt00002  -igroup HANA-
FC5
lun map -path /vol/FC5_log_mnt00001/FC5_log_mnt00001  -igroup HANA-FC5
lun map -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001  -igroup HANA-FC5
lun map -path /vol/FC5_log_mnt00002/FC5_log_mnt00002  -igroup HANA-FC5
lun map -path /vol/FC5_log2_mnt00002/FC5_log2_mnt00002  -igroup HANA-FC5
```

SAP HANA Storage-Connector-API

Ein Storage Connector ist nur in Umgebungen mit mehreren Hosts mit Failover-Funktionen erforderlich. SAP HANA bietet bei der Einrichtung mehrerer Hosts eine Hochverfügbarkeitsfunktionen, mit der ein Failover eines SAP HANA-Datenbankhosts auf einen Standby-Host möglich ist. In diesem Fall wird auf die LUNs des ausgefallenen Hosts zugegriffen und vom Standby-Host verwendet. Der Speicher-Connector wird verwendet, um sicherzustellen, dass eine Speicherpartition von jeweils nur einem Datenbank-Host aktiv zugegriffen werden kann.

In SAP HANA Konfigurationen mit mehreren Hosts und NetApp Storage kommt der von SAP bereitgestellte Standard-Storage Connector zum Einsatz. Der „SAP HANA FC Storage Connector Admin Guide“ kann als Anhang zu gefunden werden "SAP-Hinweis 1900823".

Hosteinrichtung

Bevor Sie den Host einrichten, müssen die NetApp SAN Host Utilities von heruntergeladen werden "NetApp Support" Standort und auf den HANA-Servern installiert. Die Dokumentation des Host Utility enthält Informationen zu zusätzlicher Software, die abhängig vom verwendeten FCP HBA installiert werden muss.

Die Dokumentation enthält auch Informationen zu Multipath-Konfigurationen, die spezifisch für die verwendete Linux-Version sind. In diesem Dokument werden die erforderlichen Konfigurationsschritte für SLES 15 und Red hat Enterprise Linux 7.6 oder höher beschrieben, wie in beschrieben "Linux Host Utilities 7.1 Installations- und Setup-Leitfaden".

Konfigurieren Sie Multipathing

> ⓘ Die Schritte 1 bis 6 müssen für alle Mitarbeiter- und Standby-Hosts in der SAP HANA Konfiguration mit mehreren Hosts ausgeführt werden.

Um Multipathing zu konfigurieren, gehen Sie wie folgt vor:

1. Führen Sie Linux aus `rescan-scsi-bus.sh -a` Befehl auf jedem Server, um neue LUNs zu ermitteln.

2. Führen Sie die aus `sanlun lun show` Führen Sie einen Befehl aus und vergewissern Sie sich, dass alle erforderlichen LUNs sichtbar sind. Das folgende Beispiel zeigt die `sanlun lun show` Befehlsausgabe für ein 2+1 HANA-System mit mehreren Hosts mit zwei Daten-LUNs und zwei Protokoll-LUNs. Die Ausgabe zeigt die LUNs und die entsprechenden Gerätedateien, z. B. LUN `SS3_data_mnt00001` Und die Gerätedatei `/dev/sdag`. Jede LUN verfügt über acht FC-Pfade vom Host zu den Storage Controllern.

```
sapcc-hana-tst:~ # sanlun lun show
controller(7mode/E-Series)/                                    device
host                  lun
vserver(cDOT/FlashRay)        lun-pathname                     filename
adapter    protocol   size    product
------------------------------------------------------------------------
---------------------------------------
svm1                          FC5_log2_mnt00002                /dev/sdbb
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00002                 /dev/sdba
host21     FCP        500g    cDOT
svm1                          FC5_log2_mnt00001                /dev/sdaz
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001                 /dev/sday
host21     FCP        500g    cDOT
svm1                          FC5_data2_mnt00002               /dev/sdax
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00002                /dev/sdaw
host21     FCP        1t      cDOT
svm1                          FC5_data2_mnt00001               /dev/sdav
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001                /dev/sdau
host21     FCP        1t      cDOT
svm1                          FC5_log2_mnt00002                /dev/sdat
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00002                 /dev/sdas
host21     FCP        500g    cDOT
svm1                          FC5_log2_mnt00001                /dev/sdar
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001                 /dev/sdaq
host21     FCP        500g    cDOT
svm1                          FC5_data2_mnt00002               /dev/sdap
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00002                /dev/sdao
host21     FCP        1t      cDOT
svm1                          FC5_data2_mnt00001               /dev/sdan
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001                /dev/sdam
host21     FCP        1t      cDOT
svm1                          FC5_log2_mnt00002                /dev/sdal
```

```
host20     FCP        500g    cDOT
svm1                          FC5_log_mnt00002              /dev/sdak
host20     FCP        500g    cDOT
svm1                          FC5_log2_mnt00001             /dev/sdaj
host20     FCP        500g    cDOT
svm1                          FC5_log_mnt00001              /dev/sdai
host20     FCP        500g    cDOT
svm1                          FC5_data2_mnt00002            /dev/sdah
host20     FCP        1t      cDOT
svm1                          FC5_data_mnt00002             /dev/sdag
host20     FCP        1t      cDOT
svm1                          FC5_data2_mnt00001            /dev/sdaf
host20     FCP        1t      cDOT
svm1                          FC5_data_mnt00001             /dev/sdae
host20     FCP        1t      cDOT
svm1                          FC5_log2_mnt00002             /dev/sdad
host20     FCP        500g    cDOT
svm1                          FC5_log_mnt00002              /dev/sdac
host20     FCP        500g    cDOT
svm1                          FC5_log2_mnt00001             /dev/sdab
host20     FCP        500g    cDOT
svm1                          FC5_log_mnt00001              /dev/sdaa
host20     FCP        500g    cDOT
svm1                          FC5_data2_mnt00002            /dev/sdz
host20     FCP        1t      cDOT
svm1                          FC5_data_mnt00002             /dev/sdy
host20     FCP        1t      cDOT
svm1                          FC5_data2_mnt00001            /dev/sdx
host20     FCP        1t      cDOT
svm1                          FC5_data_mnt00001             /dev/sdw
host20     FCP        1t      cDOT
```

3. Führen Sie den `multipath -r` Und `multipath -ll` Befehl zum Abrufen der weltweiten Kennungen (WWIDs) für die Gerätedateinamen.

   In diesem Beispiel gibt es acht LUNs.

```
sapcc-hana-tst:~ # multipath -r
sapcc-hana-tst:~ # multipath -ll
3600a098038314e63492b59326b4b786d dm-7 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:2 sdaf 65:240 active ready running
  |- 20:0:5:2 sdx  65:112 active ready running
```

```
  |- 21:0:4:2 sdav 66:240 active ready running
  `- 21:0:6:2 sdan 66:112 active ready running
3600a098038314e63492b59326b4b786e dm-9 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:4 sdah 66:16  active ready running
  |- 20:0:5:4 sdz  65:144 active ready running
  |- 21:0:4:4 sdax 67:16  active ready running
  `- 21:0:6:4 sdap 66:144 active ready running
3600a098038314e63492b59326b4b786f dm-11 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:6 sdaj 66:48  active ready running
  |- 20:0:5:6 sdab 65:176 active ready running
  |- 21:0:4:6 sdaz 67:48  active ready running
  `- 21:0:6:6 sdar 66:176 active ready running
3600a098038314e63492b59326b4b7870 dm-13 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:8 sdal 66:80  active ready running
  |- 20:0:5:8 sdad 65:208 active ready running
  |- 21:0:4:8 sdbb 67:80  active ready running
  `- 21:0:6:8 sdat 66:208 active ready running
3600a098038314e63532459326d495a64 dm-6 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:1 sdae 65:224 active ready running
  |- 20:0:5:1 sdw  65:96  active ready running
  |- 21:0:4:1 sdau 66:224 active ready running
  `- 21:0:6:1 sdam 66:96  active ready running
3600a098038314e63532459326d495a65 dm-8 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:3 sdag 66:0   active ready running
  |- 20:0:5:3 sdy  65:128 active ready running
  |- 21:0:4:3 sdaw 67:0   active ready running
  `- 21:0:6:3 sdao 66:128 active ready running
3600a098038314e63532459326d495a66 dm-10 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
```

```
  |- 20:0:4:5 sdai 66:32  active ready running
  |- 20:0:5:5 sdaa 65:160 active ready running
  |- 21:0:4:5 sday 67:32  active ready running
  `- 21:0:6:5 sdaq 66:160 active ready running
3600a098038314e63532459326d495a67 dm-12 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:7 sdak 66:64  active ready running
  |- 20:0:5:7 sdac 65:192 active ready running
  |- 21:0:4:7 sdba 67:64  active ready running
  `- 21:0:6:7 sdas 66:192 active ready running
```

4. Bearbeiten Sie das `/etc/multipath.conf` Datei und fügen Sie die WWIDs und Aliasnamen hinzu.

Die Beispielausgabe zeigt den Inhalt des `/etc/multipath.conf` Datei, die Alias-Namen für die vier LUNs eines 2+1-Systems mit mehreren Hosts enthält. Wenn keine Multipath.conf-Datei verfügbar ist, können Sie eine erstellen, indem Sie den folgenden Befehl ausführen: `multipath -T > /etc/multipath.conf`.

```
sapcc-hana-tst:/ # cat /etc/multipath.conf
multipaths {
                multipath {
                wwid    3600a098038314e63492b59326b4b786d
                alias   svm1-FC5_data2_mnt00001
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b786e
                alias   svm1-FC5_data2_mnt00002
        }
        multipath {
                wwid    3600a098038314e63532459326d495a64
                alias   svm1-FC5_data_mnt00001
        }
        multipath {
                wwid    3600a098038314e63532459326d495a65
                alias   svm1-FC5_data_mnt00002
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b786f
                alias   svm1-FC5_log2_mnt00001
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b7870
                alias   svm1-FC5_log2_mnt00002
        }
        multipath {
                wwid    3600a098038314e63532459326d495a66
                alias   svm1-FC5_log_mnt00001
        }
        multipath {
                wwid    3600a098038314e63532459326d495a67
                alias   svm1-FC5_log_mnt00002
        }


}
```

5. Führen Sie die aus `multipath -r` Befehl zum Neuladen der Gerätezuordnung.
6. Überprüfen Sie die Konfiguration, indem Sie den ausführen `multipath -ll` Befehl zum Auflisten aller LUNs, Alias-Namen sowie aktiver und Standby-Pfade.

Die folgende Beispielausgabe zeigt die Ausgabe eines 2+1-HANA-Systems mit mehreren Hosts mit zwei Daten und zwei Log-LUNs.

```
sapcc-hana-tst:~ # multipath -ll
hsvm1-FC5_data2_mnt00001 (3600a098038314e63492b59326b4b786d) dm-7
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:2 sdaf 65:240 active ready running
  |- 20:0:5:2 sdx  65:112 active ready running
  |- 21:0:4:2 sdav 66:240 active ready running
  `- 21:0:6:2 sdan 66:112 active ready running
svm1-FC5_data2_mnt00002 (3600a098038314e63492b59326b4b786e) dm-9
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:4 sdah 66:16  active ready running
  |- 20:0:5:4 sdz  65:144 active ready running
  |- 21:0:4:4 sdax 67:16  active ready running
  `- 21:0:6:4 sdap 66:144 active ready running
svm1-FC5_data_mnt00001 (3600a098038314e63532459326d495a64) dm-6
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:1 sdae 65:224 active ready running
  |- 20:0:5:1 sdw  65:96  active ready running
  |- 21:0:4:1 sdau 66:224 active ready running
  `- 21:0:6:1 sdam 66:96  active ready running
svm1-FC5_data_mnt00002 (3600a098038314e63532459326d495a65) dm-8
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:3 sdag 66:0   active ready running
  |- 20:0:5:3 sdy  65:128 active ready running
  |- 21:0:4:3 sdaw 67:0   active ready running
  `- 21:0:6:3 sdao 66:128 active ready running
svm1-FC5_log2_mnt00001 (3600a098038314e63492b59326b4b786f) dm-11
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:6 sdaj 66:48  active ready running
  |- 20:0:5:6 sdab 65:176 active ready running
  |- 21:0:4:6 sdaz 67:48  active ready running
  `- 21:0:6:6 sdar 66:176 active ready running
```

```
svm1-FC5_log2_mnt00002 (3600a098038314e63492b59326b4b7870) dm-13
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:8 sdal 66:80  active ready running
  |- 20:0:5:8 sdad 65:208 active ready running
  |- 21:0:4:8 sdbb 67:80  active ready running
  `- 21:0:6:8 sdat 66:208 active ready running
svm1-FC5_log_mnt00001 (3600a098038314e63532459326d495a66) dm-10
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:5 sdai 66:32  active ready running
  |- 20:0:5:5 sdaa 65:160 active ready running
  |- 21:0:4:5 sday 67:32  active ready running
  `- 21:0:6:5 sdaq 66:160 active ready running
svm1-FC5_log_mnt00002 (3600a098038314e63532459326d495a67) dm-12
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:7 sdak 66:64  active ready running
  |- 20:0:5:7 sdac 65:192 active ready running
  |- 21:0:4:7 sdba 67:64  active ready running
  `- 21:0:6:7 sdas 66:192 active ready running
```

Einzelhost-Setup

Einzelhost-Setup

In diesem Kapitel wird die Einrichtung eines einzelnen SAP HANA-Hosts unter Verwendung von Linux LVM beschrieben.

LUN-Konfiguration für SAP HANA Single-Host-Systeme

Beim SAP HANA-Host müssen Volume-Gruppen und logische Volumes erstellt und eingebunden werden, wie in der folgenden Tabelle angegeben.

Logisches Volume/LUN	Bereitstellungspunkt beim SAP HANA-Host	Hinweis
LV: FC5_data_mnt0000-vol	/hana/data/FC51/mnt00001	Mit /etc/fstab-Eintrag montiert
LV: FC5_log_mnt00001-vol	/hana/log/FC5/mnt00001	Mit /etc/fstab-Eintrag montiert
LUN: FC5_shared	/hana/Shared/FC5	Mit /etc/fstab-Eintrag montiert

Mit der beschriebenen Konfiguration wird die `/usr/sap/FC5` Das Verzeichnis, in dem das Standard-Home-Verzeichnis des Benutzers FC5adm gespeichert ist, befindet sich auf der lokalen Festplatte. In einem Disaster Recovery-Setup mit festplattenbasierter Replikation empfiehlt NetApp die Erstellung einer zusätzlichen LUN innerhalb der `FC5_shared` Volumen für die `/usr/sap/FC5` Verzeichnis, sodass sich alle Dateisysteme auf dem zentralen Speicher befinden.

Erstellen von LVM-Volume-Gruppen und logischen Volumes

1. Initialisieren Sie alle LUNs als ein physisches Volume.

```
pvcreate /dev/mapper/hana-FC5_data_mnt00001
pvcreate /dev/mapper/hana-FC5_data2_mnt00001
pvcreate /dev/mapper/hana-FC5_log_mnt00001
pvcreate /dev/mapper/hana-FC5_log2_mnt00001
```

2. Erstellen Sie die Volume-Gruppen für jede Daten- und Protokollpartition.

```
vgcreate FC5_data_mnt00001 /dev/mapper/hana-FC5_data_mnt00001
/dev/mapper/hana-FC5_data2_mnt00001
vgcreate FC5_log_mnt00001 /dev/mapper/hana-FC5_log_mnt00001
/dev/mapper/hana-FC5_log2_mnt00001
```

3. Erstellen Sie für jede Daten- und Protokollpartition ein logisches Volume. Verwenden Sie eine Stripe-Größe, die der Anzahl der LUNs pro Volume-Gruppe entspricht (in diesem Beispiel sind es zwei), eine Stripe-Größe von 256 KB für Daten und 64.000 für das Protokoll. SAP unterstützt nur ein logisches Volume pro Volume-Gruppe.

```
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00001
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00001
```

4. Scannen Sie bei allen anderen Hosts die physischen Volumes, Volume-Gruppen und Volume-Gruppen.

```
modprobe dm_mod
pvscan
vgscan
lvscan
```

Wenn diese Befehle die Volumes nicht finden, ist ein Neustart erforderlich.

Zum Mounten der logischen Volumes müssen die logischen Volumes aktiviert sein. Um die Volumes zu aktivieren, führen Sie den folgenden Befehl aus:

```
vgchange -a y
```

Erstellen von Dateisystemen

Erstellen Sie das XFS-Dateisystem auf allen logischen Daten- und Protokollvolumes und der gemeinsam genutzten Hana-LUN.

```
mkfs.xfs FC5_data_mnt00001-vol
mkfs.xfs FC5_log_mnt00001-vol
mkfs.xfs /dev/mapper/svm1-FC5_shared
```

Erstellen von Bereitstellungspunkten

Erstellen Sie die erforderlichen Mount-Point-Verzeichnisse und legen Sie die Berechtigungen auf dem Datenbankhost fest:

```
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/shared
sapcc-hana-tst:/ # chmod –R 777 /hana/log/FC5
sapcc-hana-tst:/ # chmod –R 777 /hana/data/FC5
sapcc-hana-tst:/ # chmod 777 /hana/shared
```

Mounten Sie File-Systeme

Um Dateisysteme während des Systemstarts mit dem `/etc/fstab` Konfigurationsdatei, fügen Sie die erforderlichen Dateisysteme zum `/etc/fstab` Konfigurationsdatei:

```
# cat /etc/fstab
/dev/mapper/hana-FC5_shared /hana/shared xfs defaults 0 0
/dev/mapper/FC5_log_mnt00001-vol /hana/log/FC5/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/FC5_data_mnt00001-vol /hana/data/FC5/mnt00001 xfs
relatime,inode64 0 0
```

Die XFS-Dateisysteme für die Daten- und Protokoll-LUNs müssen mit dem gemountet werden `relatime` Und `inode64` Mount-Optionen:

Um die Dateisysteme zu mounten, führen Sie den `mount –a` Befehl beim Host.

Einrichtung mehrerer Hosts

Einrichtung mehrerer Hosts

In diesem Kapitel wird beispielhaft die Einrichtung eines 2+1 SAP HANA-Mehrhostsystems beschrieben.

LUN-Konfiguration für SAP HANA-Mehrhostsysteme

Beim SAP HANA-Host müssen Volume-Gruppen und logische Volumes erstellt und eingebunden werden, wie in der folgenden Tabelle angegeben.

Logisches Volumen (LV) oder Volumen	Bereitstellungspunkt beim SAP HANA-Host	Hinweis
LV: FC5_data_mnt00001-vol	/hana/Data/FC5/mnt00001	Montiert mit Speicheranschluss
LV: FC5_log_mnt00001-vol	/hana/log/FC5/mnt00001	Montiert mit Speicheranschluss
LV: FC5_data_mnt00002-vol	/hana/Data/FC5/mnt00002	Montiert mit Speicheranschluss
LV: FC5_log_mnt00002-vol	/hana/log/FC5/mnt00002	Montiert mit Speicheranschluss
Volume: FC5_shared	/hana/Shared	Gemountet auf allen Hosts mit NFS und /etc/fstab Eintrag

Mit der beschriebenen Konfiguration wird die `/usr/sap/FC5` Das Verzeichnis, in dem das Standard-Home-Verzeichnis des Benutzers FC5adm gespeichert ist, befindet sich auf der lokalen Festplatte jedes HANA-Hosts. In einem Disaster Recovery-Setup mit festplattenbasierter Replikation empfiehlt NetApp die Erstellung von vier zusätzlichen Unterverzeichnissen im `FC5_shared` Volumen für die `/usr/sap/FC5` Dateisystem, sodass jeder Datenbankhost alle seine Dateisysteme auf dem zentralen Speicher hat.

Erstellen von LVM-Volume-Gruppen und logischen Volumes

1. Initialisieren Sie alle LUNs als ein physisches Volume.

```
pvcreate /dev/mapper/hana-FC5_data_mnt00001
pvcreate /dev/mapper/hana-FC5_data2_mnt00001
pvcreate /dev/mapper/hana-FC5_data_mnt00002
pvcreate /dev/mapper/hana-FC5_data2_mnt00002
pvcreate /dev/mapper/hana-FC5_log_mnt00001
pvcreate /dev/mapper/hana-FC5_log2_mnt00001
pvcreate /dev/mapper/hana-FC5_log_mnt00002
pvcreate /dev/mapper/hana-FC5_log2_mnt00002
```

2. Erstellen Sie die Volume-Gruppen für jede Daten- und Protokollpartition.

```
vgcreate FC5_data_mnt00001 /dev/mapper/hana-FC5_data_mnt00001
/dev/mapper/hana-FC5_data2_mnt00001
vgcreate FC5_data_mnt00002 /dev/mapper/hana-FC5_data_mnt00002
/dev/mapper/hana-FC5_data2_mnt00002
vgcreate FC5_log_mnt00001 /dev/mapper/hana-FC5_log_mnt00001
/dev/mapper/hana-FC5_log2_mnt00001
vgcreate FC5_log_mnt00002 /dev/mapper/hana-FC5_log_mnt00002
/dev/mapper/hana-FC5_log2_mnt00002
```

3. Erstellen Sie für jede Daten- und Protokollpartition ein logisches Volume. Verwenden Sie eine Stripe-Größe, die der Anzahl der LUNs pro Volume-Gruppe entspricht (in diesem Beispiel sind es zwei), eine Stripe-Größe von 256 KB für Daten und 64.000 für das Protokoll. SAP unterstützt nur ein logisches Volume pro Volume-Gruppe.

```
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00001
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00002
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00002
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00001
```

4. Scannen Sie bei allen anderen Hosts die physischen Volumes, Volume-Gruppen und Volume-Gruppen.

```
modprobe dm_mod
pvscan
vgscan
lvscan
```

Wenn diese Befehle die Volumes nicht finden, ist ein Neustart erforderlich.

Zum Mounten der logischen Volumes müssen die logischen Volumes aktiviert sein. Um die Volumes zu aktivieren, führen Sie den folgenden Befehl aus:

```
vgchange -a y
```

Erstellen von Dateisystemen

Erstellen Sie das XFS-Dateisystem auf allen logischen Daten- und Protokollvolumes.

```
mkfs.xfs FC5_data_mnt00001-vol
mkfs.xfs FC5_data_mnt00002-vol
mkfs.xfs FC5_log_mnt00001-vol
mkfs.xfs FC5_log_mnt00002-vol
```

Erstellen von Bereitstellungspunkten

Erstellen Sie die erforderlichen Mount-Point-Verzeichnisse und legen Sie die Berechtigungen auf allen Worker- und Standby-Hosts fest:

```
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00002
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00002
sapcc-hana-tst:/ # mkdir -p /hana/shared
sapcc-hana-tst:/ # chmod -R 777 /hana/log/FC5
sapcc-hana-tst:/ # chmod -R 777 /hana/data/FC5
sapcc-hana-tst:/ # chmod 777 /hana/shared
```

Mounten Sie File-Systeme

Zur Montage des `/hana/shared` Dateisysteme während des Systemstarts mithilfe der `/etc/fstab` Konfigurationsdatei, fügen Sie die `/hana/shared` Dateisystem in die `/etc/fstab` Konfigurationsdatei jedes Hosts.

```
sapcc-hana-tst:/ # cat /etc/fstab
<storage-ip>:/hana_shared /hana/shared nfs rw,vers=3,hard,timeo=600,
intr,noatime,nolock 0 0
```

Alle Daten- und Protokolldateisysteme sind über den SAP HANA Storage Connector gemountet.

Führen Sie zum Mounten der Dateisysteme den aus `mount -a` Befehl an jedem Host.

I/O-Stack-Konfiguration für SAP HANA

Ab SAP HANA 1.0 SPS10 führte SAP Parameter ein, um das I/O-Verhalten anzupassen und die Datenbank für das verwendete Datei- und Speichersystem zu optimieren.

NetApp hat Performance-Tests durchgeführt, um die idealen Werte zu definieren. In der folgenden Tabelle sind die optimalen Werte aufgeführt, die aus den Leistungstests abgeleitet wurden.

Parameter	Wert
max_parallel_io_Requests	128
Async_read_Submit	Ein
Async_write_submit_Active	Ein
Async_Write_Submit_Blocks	Alle

Für SAP HANA 1.0 bis SPS12 können diese Parameter während der Installation der SAP HANA-Datenbank wie in SAP Note beschrieben eingestellt werden "2267798 – Konfiguration der SAP HANA Datenbank während der Installation mit hdbparam".

Alternativ können die Parameter nach der SAP HANA-Datenbankinstallation mit dem eingestellt werden `hdbparam` Framework:

```
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.max_parallel_io_requests=128
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_write_submit_active=on
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_read_submit=on
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_write_submit_blocks=all
```

Ab SAP HANA 2.0 `hdbparam` Ist veraltet und die Parameter wurden in die verschoben `global.ini` Datei: Die Parameter können über SQL-Befehle oder SAP HANA Studio eingestellt werden. Weitere Informationen finden Sie unter SAP-Hinweis "2399079 - Beseitigung von hdbparam in HANA 2". Die Parameter können auch im festgelegt werden `global.ini` Datei:

```
SS3adm@stlrx300s8-6:/usr/sap/SS3/SYS/global/hdb/custom/config> cat
global.ini
…
[fileio]
async_read_submit = on
async_write_submit_active = on
max_parallel_io_requests = 128
async_write_submit_blocks = all
…
```

Mit SAP HANA 2.0 SPS5 und später können Sie die oben genannten Parameter mithilfe des `setParameter.py `s-Handkript einstellen.

```
fc5adm@sapcc-hana-tst-03:/usr/sap/FC5/HDB00/exe/python_support>
python setParameter.py
-set=SYSTEM/global.ini/fileio/max_parallel_io_requests=128
python setParameter.py -set=SYSTEM/global.ini/fileio/async_read_submit=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_active=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_blocks=all
```

SAP HANA Softwareinstallation

Im Folgenden sind die Anforderungen für die Installation der SAP HANA Software aufgeführt.

Installation auf Single-Host-System

Die Installation der SAP HANA-Software erfordert keine zusätzliche Vorbereitung auf ein Single-Host-System.

Installation auf Systemen mit mehreren Hosts

Das folgende Installationsverfahren basiert auf SAP HANA 1.0 SPS12 oder höher.

Erstellen Sie vor Beginn der Installation einen `global.ini` Datei, um die Verwendung des SAP-Speicheranschlusses während des Installationsprozesses zu ermöglichen. Der SAP-Speicheranschluss montiert die erforderlichen Dateisysteme während des Installationsprozesses an den Worker-Hosts. Der `global.ini` Die Datei muss in einem Dateisystem verfügbar sein, auf das über alle Hosts zugegriffen werden kann, z. B. die `/hana/shared/SID` File-System.

Vor der Installation der SAP HANA-Software auf einem System mit mehreren Hosts müssen die folgenden Schritte durchgeführt werden:

1. Fügen Sie die folgenden Mount-Optionen für die Daten-LUNs und die Protokoll-LUNs auf dem hinzu `global.ini` Datei:
   - `relatime` Und `inode64` Für das Daten- und Protokolldateisystem
2. Fügen Sie die WWIDs der Daten- und Log-Partitionen hinzu. Die WWIDs müssen mit den im konfigurierten Aliasnamen übereinstimmen `/etc/multipath.conf` Datei:

   Die folgende Ausgabe zeigt ein Beispiel für ein 2+1-Setup mit mehreren Hosts, bei dem die System-ID (SID) SS3 ist.

```
stlrx300s8-6:~ # cat /hana/shared/global.ini
[communication]
listeninterface = .global
[persistence]
basepath_datavolumes = /hana/data/SS3
basepath_logvolumes = /hana/log/SS3
[storage]
ha_provider = hdb_ha.fcClient
partition_*_*__prtype = 5
partition_*_data__mountoptions = -o relatime,inode64
partition_*_log__mountoptions = -o relatime,inode64,nobarrier
partition_1_data__wwid = hana-SS3_data_mnt00001
partition_1_log__wwid = hana-SS3_log_mnt00001
partition_2_data__wwid = hana-SS3_data_mnt00002
partition_2_log__wwid = hana-SS3_log_mnt00002
[system_information]
usage = custom
[trace]
ha_fcclient = info
stlrx300s8-6:~ #
```

   Wenn LVM verwendet wird, ist die erforderliche Konfiguration unterschiedlich. Das unten stehende Beispiel

zeigt eine 2+1 Konfiguration mit mehreren Hosts mit SID=FC5.

```
sapcc-hana-tst-03:/hana/shared # cat global.ini
[communication]
listeninterface = .global
[persistence]
basepath_datavolumes = /hana/data/FC5
basepath_logvolumes = /hana/log/FC5
[storage]
ha_provider = hdb_ha.fcClientLVM
partition_*_*__prtype = 5
partition_*_data__mountOptions = -o relatime,inode64
partition_*_log__mountOptions = -o relatime,inode64
partition_1_data__lvmname = FC5_data_mnt00001-vol
partition_1_log__lvmname = FC5_log_mnt00001-vol
partition_2_data__lvmname = FC5_data_mnt00002-vol
partition_2_log__lvmname = FC5_log_mnt00002-vol
sapcc-hana-tst-03:/hana/shared #
```

Starten Sie die Installation mithilfe des SAP- `hdblcm`Installationstools, indem Sie den folgenden Befehl an einem der Arbeitshosts ausführen. Verwenden Sie die `addhosts` Option, um den zweiten Worker (sapcc-hana-tst-06) und den Standby-Host (sapcc-hana-tst-07) hinzuzufügen. Das Verzeichnis, in dem die vorbereitete `global.ini` Datei gespeichert wurde(`--storage_cfg=/hana/shared`, ist in der CLI-Option enthalten `storage_cfg`. Je nach verwendeter Betriebssystemversion kann es erforderlich sein, Phyton 2.7 vor der Installation der SAP HANA-Datenbank zu installieren.

```
/hdblcm --action=install --addhosts=sapcc-hana-tst
-06:role=worker:storage_partition=2,sapcc-hana-tst-07:role=standby
--storage_cfg=/hana/shared/

AP HANA Lifecycle Management - SAP HANA Database 2.00.073.00.1695288802
************************************************************************


Scanning software locations...
Detected components:
    SAP HANA AFL (incl.PAL,BFL,OFL) (2.00.073.0000.1695321500) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_AFL_LINUX_X86_64/packages
    SAP HANA Database (2.00.073.00.1695288802) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
    SAP HANA Database Client (2.18.24.1695756995) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/SAP_HANA_CLIENT/client
```

```
    SAP HANA Studio (2.3.75.000000) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/HDB_STUDIO_LINUX_X86_64/studio
    SAP HANA Local Secure Store (2.11.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HANA_LSS_24_LINUX_X86_64/packages
    SAP HANA XS Advanced Runtime (1.1.3.230717145654) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/XSA_RT_10_LINUX_X86_64/packages
    SAP HANA EML AFL (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_EML_AFL_10_LINUX_X86_64/packages
    SAP HANA EPM-MDS (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/SAP_HANA_EPM-MDS_10/packages
    Automated Predictive Library (4.203.2321.0.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/PAAPL4_H20_LINUX_X86_64/apl-
4.203.2321.0-hana2sp03-linux_x64/installer/packages
    GUI for HALM for XSA (including product installer) Version 1 (1.015.0)
in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACALMPIUI15_0.zip
    XSAC FILEPROCESSOR 1.0 (1.000.102) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACFILEPROC00_102.zip
    SAP HANA tools for accessing catalog content, data preview, SQL
console, etc. (2.015.230503) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_HRTT_20/XSACHRTT15_230503.zip
    Develop and run portal services for customer applications on XSA
(2.007.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACPORTALSERV07_0.zip
    The SAP Web IDE for HANA 2.0 (4.007.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_SAP_WEB_IDE_20/XSACSAPWEBIDE07_0.zip
    XS JOB SCHEDULER 1.0 (1.007.22) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACSERVICES07_22.zip
    SAPUI5 FESV6 XSA 1 - SAPUI5 1.71 (1.071.52) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV671_52.zip
    SAPUI5 FESV9 XSA 1 - SAPUI5 1.108 (1.108.5) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV9108_5.zip
    SAPUI5 SERVICE BROKER XSA 1 - SAPUI5 Service Broker 1.0 (1.000.4) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5SB00_4.zip
    XSA Cockpit 1 (1.001.37) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACXSACOCKPIT01_37.zip
```

```
SAP HANA Database version '2.00.073.00.1695288802' will be installed.

Select additional components for installation:

  Index | Components      | Description

-------------------------------------------------------------------------------
------------------------
  1     | all             | All components
  2     | server          | No additional components
  3     | client          | Install SAP HANA Database Client version
2.18.24.1695756995
  4     | lss             | Install SAP HANA Local Secure Store version
2.11.0
  5     | studio          | Install SAP HANA Studio version 2.3.75.000000
  6     | xs              | Install SAP HANA XS Advanced Runtime version
1.1.3.230717145654
  7     | afl             | Install SAP HANA AFL (incl.PAL,BFL,OFL)
version 2.00.073.0000.1695321500
  8     | eml             | Install SAP HANA EML AFL version
2.00.073.0000.1695321500
  9     | epmmds          | Install SAP HANA EPM-MDS version
2.00.073.0000.1695321500
  10    | sap_afl_sdk_apl | Install Automated Predictive Library version
4.203.2321.0.0

Enter comma-separated list of the selected indices [3,4]: 2,3
```

```
Verify that the installation tool installed all selected components at all
worker and standby hosts.
```

Hinzufügen von zusätzlichen Daten-Volume-Partitionen für SAP HANA Single-Host-Systeme

Ab SAP HANA 2.0 SPS4 können weitere Daten-Volume-Partitionen konfiguriert werden. Mit dieser Funktion können Sie zwei oder mehr LUNs für das Daten-Volume einer SAP HANA-Mandantendatenbank konfigurieren und eine Skalierung über die Größe und Performance-Grenzen einer einzelnen LUN hinaus vornehmen.

Es ist nicht nötig, mehrere Partitionen zu verwenden, um die SAP HANA-KPIs zu erfüllen. Eine einzelne LUN mit einer einzigen Partition erfüllt die erforderlichen KPIs.

Die Nutzung von zwei oder mehr einzelnen LUNs für das Daten-Volume ist nur für SAP HANA Single-Host-Systeme verfügbar. Der für SAP HANA mehrere-Host-Systeme erforderliche SAP-Storage-Connector unterstützt nur ein Gerät für das Daten-Volume.

Sie können jederzeit weitere Daten-Volume-Partitionen hinzufügen, jedoch ist möglicherweise ein Neustart der SAP HANA-Datenbank erforderlich.

Aktivieren von zusätzlichen Partitionen für Volumes

Führen Sie folgende Schritte aus, um zusätzliche Datenträger-Partitionen zu aktivieren:

1. Fügen Sie den folgenden Eintrag in das hinzu `global.ini` Datei:

```
[customizable_functionalities]
persistence_datavolume_partition_multipath = true
```

2. Starten Sie die Datenbank neu, um die Funktion zu aktivieren. Hinzufügen des Parameters über SAP HANA Studio zum `global.ini` Die Datei unter Verwendung der Systemdb-Konfiguration verhindert den Neustart der Datenbank.

Konfiguration von Volume und LUN

Das Layout von Volumes und LUNs ähnelt dem Layout eines einzelnen Hosts mit einer Daten-Volume-Partition, doch mit einem zusätzlichen Daten-Volume und einer anderen LUN, die auf einem anderen Aggregat als Protokoll-Volume und dem anderen Daten-Volume gespeichert sind. Die folgende Tabelle zeigt eine Beispielkonfiguration eines SAP HANA Einzelhost-Systems mit zwei Daten-Volume-Partitionen.

Aggregat 1 bei Controller A	Aggregat 2 bei Controller A	Aggregat 1 bei Controller B	Aggregieren 2 bei Controller B
Datenvolumen: SID_Data_mnt00001	Gemeinsam genutztes Volume: SID_shared	Datenvolumen: SID_data2_mnt00001	Protokollvolumen: SID_log_mnt00001

Die nächste Tabelle zeigt ein Beispiel für die Mount-Punkt-Konfiguration für ein System mit einem einzelnen Host mit zwei Daten-Volume-Partitionen.

LUN	Bereitstellungspunkt beim HANA-Host	Hinweis
SID_Data_mnt00001	/hana/Data/SID/mnt00001	Mit /etc/fstab-Eintrag montiert
SID_data2_mnt00001	/hana/data2/SID/mnt00001	Mit /etc/fstab-Eintrag montiert
SID_Log_mnt00001	/hana/log/SID/mnt00001	Mit /etc/fstab-Eintrag montiert
SID_freigegeben	/hana/Shared/SID	Mit /etc/fstab-Eintrag montiert

Erstellen Sie die neuen Daten-LUNs entweder mit ONTAP System Manager oder mit der ONTAP CLI.

Host-Konfiguration

Gehen Sie wie folgt vor, um einen Host zu konfigurieren:

1. Konfigurieren Sie Multipathing für die zusätzlichen LUNs, wie in Abschnitt 0 beschrieben.
2. Erstellen Sie das XFS-Dateisystem auf jeder zusätzlichen LUN, die zum HANA-System gehört.

```
stlrx300s8-6:/ # mkfs.xfs /dev/mapper/hana-FC5_data2_mnt00001
```

3. Fügen Sie die zusätzlichen Dateisysteme dem hinzu `/etc/fstab` Konfigurationsdatei

> Die XFS-Dateisysteme für die Daten-LUN müssen mit dem gemountet werden `relatime` Und `inode64` Mount-Optionen: Die XFS-Dateisysteme für die Protokoll-LUN müssen mit dem gemountet werden `relatime`, `inode64`, und `nobarrier` Mount-Optionen:

```
stlrx300s8-6:/ # cat /etc/fstab
/dev/mapper/hana-FC5_shared /hana/shared xfs defaults 0 0
/dev/mapper/hana-FC5_log_mnt00001 /hana/log/FC5/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/hana-FC5_data_mnt00001 /hana/data/FC5/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/hana-FC5_data2_mnt00001 /hana/data2/FC5/mnt00001 xfs
relatime,inode64 0 0
```

4. Erstellen Sie die Bereitstellungspunkte und legen Sie die Berechtigungen auf dem Datenbank-Host fest.

```
stlrx300s8-6:/ # mkdir -p /hana/data2/FC5/mnt00001
stlrx300s8-6:/ # chmod –R 777 /hana/data2/FC5
```

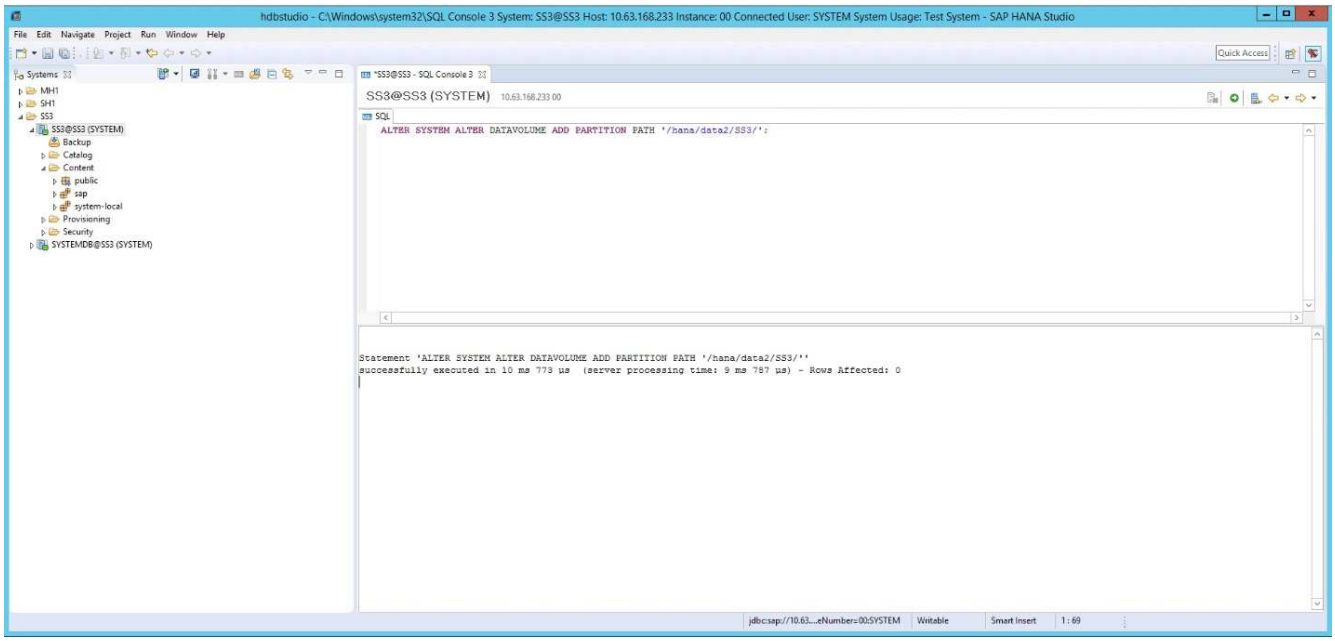
5. Führen Sie zum Mounten der Dateisysteme den aus `mount –a` Befehl.

Hinzufügen einer zusätzlichen datavolume-Partition

Gehen Sie wie folgt vor, um Ihrer Mandanten-Datenbank eine zusätzliche Datavolume-Partition hinzuzufügen:

1. Führen Sie die folgende SQL-Anweisung für die Mandantendatenbank aus. Jede zusätzliche LUN kann einen anderen Pfad haben.

```
ALTER SYSTEM ALTER DATAVOLUME ADD PARTITION PATH '/hana/data2/SID/';
```



Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten bzw. auf den folgenden Websites:

- "SAP HANA Softwarelösungen"
- "TR-4646: SAP HANA Disaster Recovery with Storage Replication"
- "TR-4614: SAP HANA Backup and Recovery with SnapCenter"
- "TR-4667: Automatisierung von SAP Systemkopien mit dem SnapCenter SAP HANA Plug-in"
- NetApp Dokumentationszentren

  "https://www.netapp.com/support-and-training/documentation/"
- SAP Certified Enterprise Storage Hardware for SAP HANA

  "https://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/"
- SAP HANA Storage-Anforderungen

  "https://www.sap.com/documents/2024/03/146274d3-ae7e-0010-bca6-c68f7e60039b.html"
- SAP HANA Tailored Data Center Integration Häufig gestellte Fragen

  "https://www.sap.com/documents/2016/05/e8705aae-717c-0010-82c7-eda71af511fa.html"
- SAP HANA auf VMware vSphere Wiki

  "https://help.sap.com/docs/SUPPORT_CONTENT/virtualization/3362185751.html"
- Best Practices Guide für SAP HANA auf VMware vSphere

  "https://www.vmware.com/docs/sap_hana_on_vmware_vsphere_best_practices_guide-white-paper"

Aktualisierungsverlauf

An dieser Lösung wurden seit ihrer ersten Veröffentlichung folgende technische Änderungen vorgenommen:

Datum	Zusammenfassung aktualisieren
Februar 2015	Ausgangsversion
Oktober 2015	Integrierte I/O-Parameter für SAP HANA und HWVAL SPS 10 und höher
Februar 2016	Aktualisierte Kapazitätsdimensionierung
Februar 2017	Neue NetApp Storage-Systeme und Festplatten-Shelfs Neue Funktionen der neuen Betriebssystemversionen von ONTAP 9 (SLES12 SP1 und Red hat Enterprise Linux 7.2)
Juli 2017	Kleine Updates
September 2018	Neue NetApp Storage-Systeme Neue Betriebssystemversionen (SLES12 SP3 und Red hat Enterprise Linux 7.4) zusätzliche kleinere Updates für SAP HANA 2.0 SPS3
September 2019	Neues Betriebssystem veröffentlicht kleine Updates
April 2020	Einführung mehrerer Funktionen für die Datenpartition, die seit SAP HANA 2.0 SPS4 verfügbar sind
Juni 2020	Zusätzliche Informationen über optionale Funktionalitäten kleine Updates
Februar 2021	Linux LVM unterstützt neue NetApp Storage-Systeme Neue Betriebssystemversionen (SLES15SP2, RHEL 8)
April 2021	VMware vSphere-spezifische Informationen hinzugefügt
September 2022	Neue Betriebssystemversionen
September 2024	Neue Storage-Systeme
Februar 2025	Neues Storage-System
Juli 2025	Kleine Updates

Backup, Restore und Disaster Recovery

SAP HANA auf Amazon FSX für NetApp ONTAP – Backup und Recovery mit SnapCenter

TR-4926: SAP HANA auf Amazon FSX für NetApp ONTAP – Backup und Recovery mit SnapCenter

Dieser technische Bericht enthält die Best Practices für die Datensicherung von SAP HANA auf Amazon FSX für NetApp ONTAP und NetApp SnapCenter. Dieses Dokument behandelt SnapCenter-Konzepte, Konfigurationsempfehlungen und Betriebs-Workflows, einschließlich Konfiguration, Backup-Vorgänge Sowie Restore- und Recovery-Vorgänge durchzuführen.

Autor: Nils Bauer, NetApp

Unternehmen benötigen heutzutage eine kontinuierliche, unterbrechungsfreie Verfügbarkeit ihrer SAP-Applikationen. Sie erwarten eine konsistente Performance, angesichts ständig wachsender Datenvolumen und bei routinemäßigen Wartungsaufgaben, wie System-Backups. Das Durchführen von Backups von SAP-Datenbanken ist eine wichtige Aufgabe, die erhebliche Auswirkungen auf die Performance des SAP-Produktionssystems haben kann.

Die Backup-Fenster verkürzen sich, während die zu sichernden Daten immer größer werden. Daher ist es schwierig, eine Zeit zu finden, in der Backups mit nur minimalen Auswirkungen auf Geschäftsprozesse durchgeführt werden können. Die Zeit, die zum Wiederherstellen und Wiederherstellen von SAP-Systemen benötigt wird, ist besorgt, da Ausfallzeiten von SAP-Produktions- und nicht produktiven Systemen minimiert werden müssen, um die Kosten für das Unternehmen zu senken.

Backup und Recovery mit Amazon FSX für ONTAP

Mit NetApp Snapshot Technologie können Datenbank-Backups innerhalb von Minuten erstellt werden.

Wie lange es dauert, eine Snapshot Kopie zu erstellen, ist unabhängig von der Größe der Datenbank, da bei Snapshot Kopien keine physischen Datenblöcke auf der Storage-Plattform verschoben werden. Darüber hinaus wirkt sich der Einsatz der Snapshot-Technologie auf das laufende SAP-System nicht auf die Performance aus. Daher können Sie die Erstellung von Snapshot Kopien so planen, dass die Zeiten für Spitzenzeiten oder Batch-Aktivitäten nicht berücksichtigt werden. SAP- und NetApp-Kunden planen in der Regel mehrere Online Snapshot Backups pro Tag, beispielsweise alle sechs Stunden ist üblich. Diese Snapshot Backups werden in der Regel drei bis fünf Tage auf dem primären Storage-System gespeichert, bevor sie entfernt oder zu einem günstigeren Storage verschoben werden, und zwar zur langfristigen Aufbewahrung.

Snapshot Kopien bieten auch wichtige Vorteile für Wiederherstellung und Recovery. Mit der NetApp SnapRestore-Technologie können auf der Grundlage der derzeit verfügbaren Snapshot Kopien eine gesamte Datenbank oder alternativ nur ein Teil einer Datenbank zu einem beliebigen Zeitpunkt wiederhergestellt werden. Solche Wiederherstellungen sind innerhalb von wenigen Sekunden abgeschlossen, unabhängig von der Größe der Datenbank. Da mehrere Online Snapshot Backups tagsüber erstellt werden können, verringert sich die für den Recovery-Prozess erforderliche Zeit erheblich im Vergleich zu einem herkömmlichen Backup-Ansatz nur einmal pro Tag. Da Sie eine Wiederherstellung mit einer Snapshot-Kopie durchführen können, die

höchstens ein paar Stunden alt ist (anstatt bis zu 24 Stunden), müssen während des Forward Recovery weniger Transaktions-Logs angewendet werden. Daher reduziert sich die RTO auf mehrere Minuten anstatt auf mehrere Stunden, die bei herkömmlichen Streaming Backups benötigt werden.

Backups von Snapshot-Kopien werden auf demselben Festplattensystem wie die aktiven Online-Daten gespeichert. Daher empfiehlt NetApp, Backups von Snapshot-Kopien als Ergänzung zu verwenden, anstatt Backups an einen sekundären Standort zu ersetzen. Die meisten Restore- und Recovery-Aktionen werden mit SnapRestore auf dem primären Storage-System gemanagt. Restores von einem Sekundärstandort sind nur nötig, wenn das primäre Storage-System, das die Snapshot-Kopien enthält, beschädigt ist. Sie können den sekundären Standort auch verwenden, wenn ein Backup wiederhergestellt werden muss, das am primären Standort nicht mehr verfügbar ist.

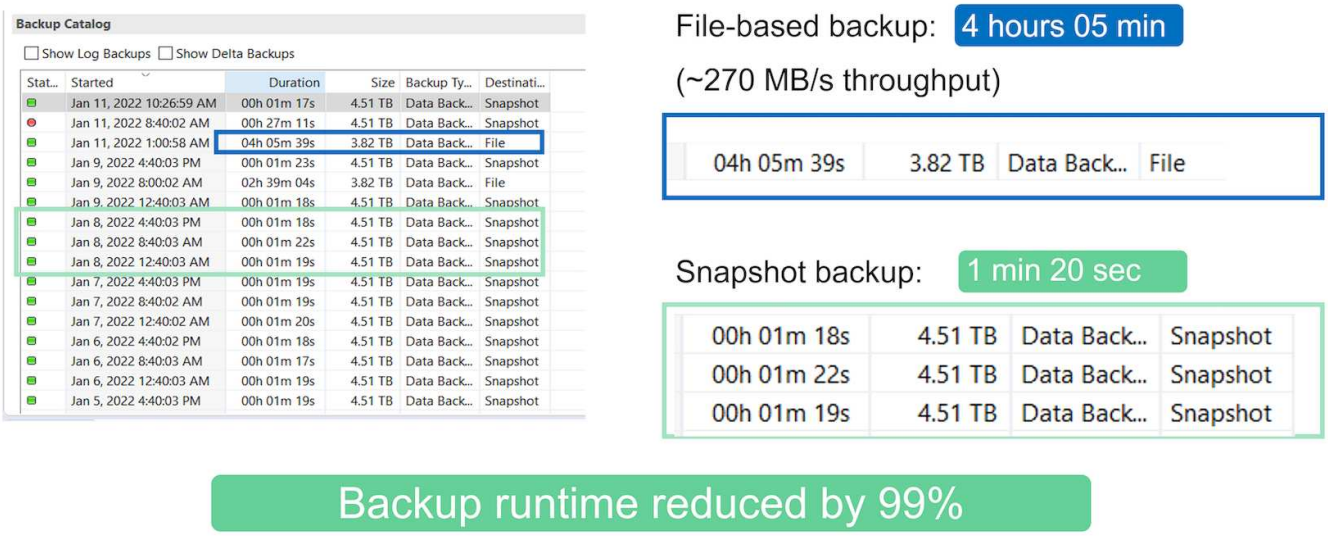
Ein Backup an einen sekundären Standort basiert auf Snapshot-Kopien, die auf dem primären Storage erstellt wurden. Somit werden die Daten direkt aus dem primären Storage-System eingelesen, ohne dass dabei der SAP Datenbankserver belastet wird. Der primäre Storage kommuniziert direkt mit dem sekundären Storage und repliziert mithilfe der NetApp SnapVault Funktion die Backup-Daten am Ziel.

SnapVault bietet im Vergleich zu herkömmlichen Backups deutliche Vorteile. Nach einem anfänglichen Datentransfer, bei dem alle Daten vom Quell- zum Ziel übertragen wurden, werden bei allen nachfolgenden Backups nur die geänderten Blöcke in den sekundären Storage verschoben. Somit werden die Last auf dem primären Storage-System und der Zeitaufwand für ein Vollbackup deutlich reduziert. Da SnapVault nur die geänderten Blöcke am Ziel speichert, belegen alle zusätzlichen vollständigen Datenbank-Backups erheblich weniger Festplattenspeicher.

Laufzeit von Snapshot-Backup- und -Restore-Vorgängen

Die folgende Abbildung zeigt HANA Studio eines Kunden, das Snapshot-Backup-Vorgänge verwendet. Das Bild zeigt, dass die HANA-Datenbank (ca. 4 TB groß) mithilfe der Snapshot Backup-Technologie in 1 Minute und 20 Sekunden und mehr als 4 Stunden bei einem dateibasierten Backup-Vorgang gesichert wird.

Der größte Teil der gesamten Laufzeit des Backup-Workflows ist die Zeit, die zur Ausführung des HANA Backup-Speicherpunktes benötigt wird. Dieser Schritt hängt von der Last der HANA-Datenbank ab. Das Snapshot Backup selbst ist in wenigen Sekunden abgeschlossen.



Vergleich der Recovery-Zeitvorgaben

Dieser Abschnitt enthält einen RTO-Vergleich (Recovery Time Objective) von Datei- und Storage-basierten Snapshot Backups. Das RTO wird durch die Summe der Zeit definiert, die für das Wiederherstellen, Wiederherstellen und Starten der Datenbank benötigt wird.

Benötigte Zeit zum Wiederherstellen der Datenbank

Bei einem dateibasierten Backup hängt die Restore-Zeit von der Größe der Datenbank und der Backup-Infrastruktur ab, die die Restore-Geschwindigkeit in Megabyte pro Sekunde festlegt. Wenn die Infrastruktur beispielsweise einen Restore-Vorgang mit einer Geschwindigkeit von 250 MB/s unterstützt, dauert es etwa 4.5 Stunden, um eine Datenbank mit einer Größe von 4 TB auf der Persistenz wiederherzustellen.

Bei den Backups der Storage Snapshot-Kopien ist die Wiederherstellungszeit unabhängig von der Größe der Datenbank und befindet sich immer im Bereich von einigen Sekunden.

Benötigte Zeit zum Starten der Datenbank

Die Startzeit der Datenbank hängt von der Größe der Datenbank und der Zeit ab, die zum Laden der Daten in den Arbeitsspeicher erforderlich ist. In den folgenden Beispielen wird davon ausgegangen, dass die Daten mit 1000 MBit/s geladen werden können. Das Laden von 4 TB in den Speicher dauert etwa 1 Stunde und 10 Minuten. Die Startzeit ist bei dateibasierten und Snapshot-basierten Restore- und Recovery-Vorgängen gleich.

Benötigte Zeit für das Recovery von Datenbanken

Die Wiederherstellungszeit hängt von der Anzahl der Protokolle ab, die nach der Wiederherstellung angewendet werden müssen. Diese Zahl hängt von der Häufigkeit ab, mit der Daten-Backups erstellt werden.

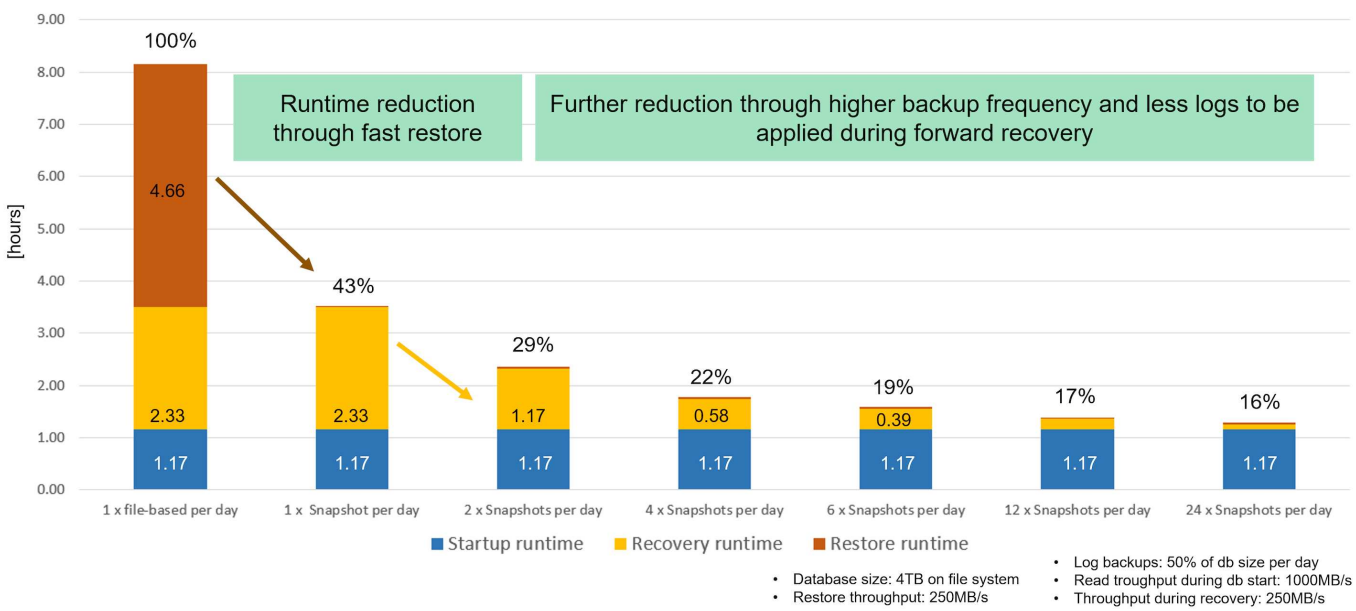
Bei dateibasierten Daten-Backups wird der Backup-Zeitplan normalerweise einmal pro Tag erstellt. Eine höhere Backup-Frequenz ist normalerweise nicht möglich, da das Backup die Produktions-Performance beeinträchtigt. Daher müssen im schlimmsten Fall alle Protokolle, die während des Tages geschrieben wurden, während der Forward Recovery angewendet werden.

Snapshot Backups werden in der Regel mit höherer Frequenz geplant, da sie nicht die Performance der SAP HANA Datenbank beeinträchtigen. Wenn Snapshot Backups beispielsweise alle sechs Stunden geplant sind, wäre die Recovery-Zeit im schlimmsten Fall ein Viertel der Recovery-Zeit für ein dateibasiertes Backup (6 Stunden / 24 Stunden = .25).

Die folgende Abbildung zeigt einen Vergleich von Restore- und Recovery-Vorgängen mit einem täglichen dateibasierten Backup und Snapshot Backups mit verschiedenen Zeitplänen.

Die ersten beiden Balken zeigen, dass sich auch bei einem einzelnen Snapshot Backup pro Tag die Wiederherstellung und Wiederherstellung dank der Geschwindigkeit des Restore-Vorgangs aus einem Snapshot Backup auf 43 % reduziert. Wenn pro Tag mehrere Snapshot Backups erstellt werden, kann die Laufzeit weiter reduziert werden, da während der Wiederherstellung weniger Protokolle angewendet werden müssen.

Die folgende Abbildung zeigt außerdem, dass vier bis sechs Snapshot Backups pro Tag am sinnvollsten sind, da eine höhere Frequenz keine großen Auswirkungen mehr auf die Gesamtlaufzeit hat.



Anwendungsfälle und Vorteile beschleunigter Backup- und Klonvorgänge

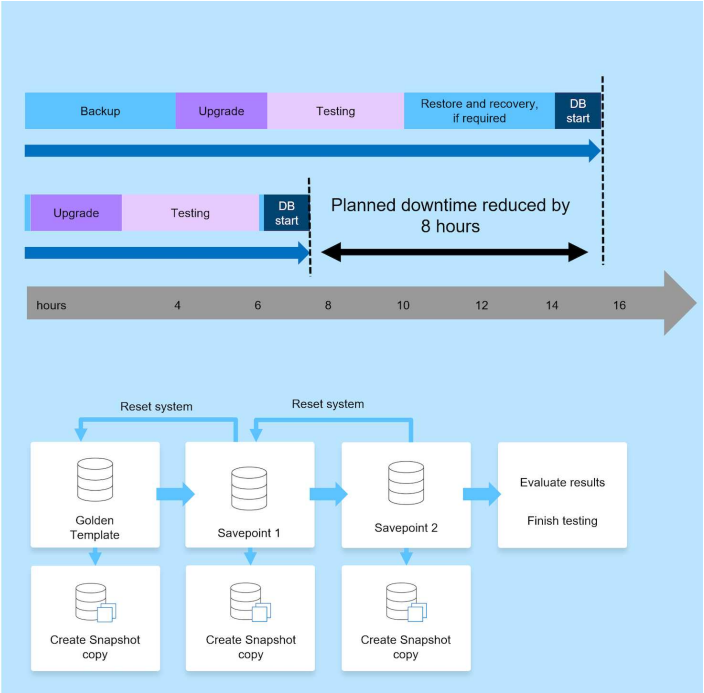
Die Ausführung von Backups ist ein wichtiger Bestandteil jeder Datensicherungsstrategie. Die Backups werden regelmäßig geplant, um sicherzustellen, dass Sie nach Systemausfällen wiederherstellen können. Dies ist der naheliegende Anwendungsfall, aber auch andere SAP Lifecycle Management-Aufgaben, von denen Beschleunigung von Backup- und Recovery-Vorgängen entscheidend ist.

Ein SAP HANA System-Upgrade ist ein Beispiel dafür, wo ein On-Demand-Backup vor dem Upgrade und ein möglicher Restore-Vorgang, wenn das Upgrade fehlschlägt, eine erhebliche Auswirkung auf die gesamte geplante Ausfallzeit hat. Wenn Sie beispielsweise eine Datenbank mit 4 TB verwenden, können Sie die geplanten Ausfallzeiten dank Snapshot-basierter Backup- und Restore-Vorgänge um 8 Stunden reduzieren.

Ein weiteres Anwendungsbeispiel wäre ein typischer Testzyklus, bei dem Tests über mehrere Iterationen mit unterschiedlichen Datensätzen oder Parametern durchgeführt werden müssen. Wenn Sie die schnellen Backup- und Restore-Vorgänge nutzen, können Sie ganz einfach Speicherpunkte innerhalb Ihres Testzyklus erstellen und das System auf jeden dieser vorherigen Speicherpunkte zurücksetzen, wenn ein Test fehlschlägt oder wiederholt werden muss. So können die Tests früher abgeschlossen werden oder es können mehr Tests gleichzeitig durchgeführt werden, und die Testergebnisse werden verbessert.

Use Cases for Backup and Recovery Operations

- Accelerate HANA system upgrade operations
  - Fast on-demand backup before HANA system upgrade
  - Fast restore operation in case of an upgrade failure
  - Reduction of planned downtime



- Acclerate test cycles
  - Fast creation of savepoints after a successful step
  - Fast reset of system to any savepoint
  - Repeat step until successful

Nachdem Snapshot Backups implementiert wurden, können sie für mehrere andere Anwendungsfälle verwendet werden, die Kopien einer HANA-Datenbank benötigen. Mit FSX für ONTAP können Sie ein neues Volume auf Basis des Inhalts jedes verfügbaren Snapshot-Backups erstellen. Die Laufzeit dieses Vorgangs beträgt unabhängig von der Größe des Volumes einige Sekunden.

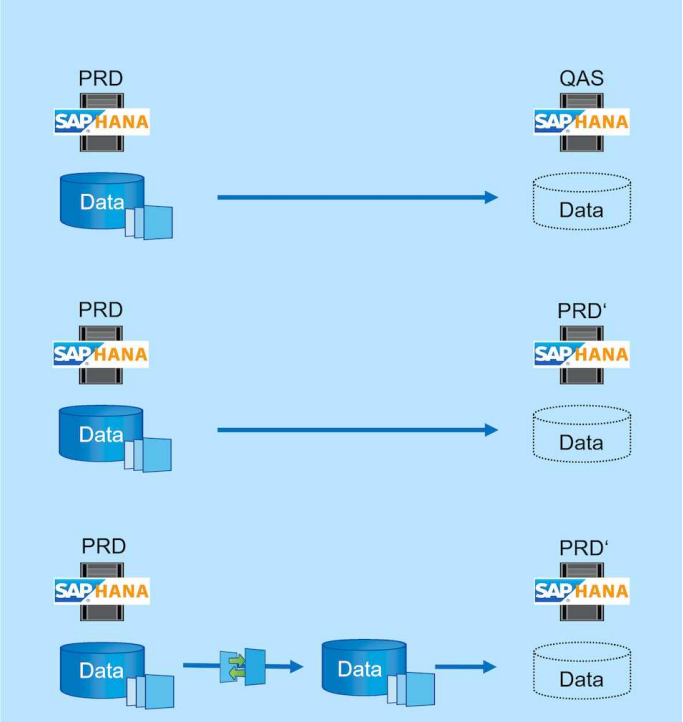
Der beliebteste Anwendungsfall ist SAP Systemaktualisierung, in dem Daten aus dem Produktionssystem in das Test- oder QA-System kopiert werden müssen. Mit der Klonfunktion von FSX für ONTAP lässt sich das Volume für das Testsystem von jeder beliebigen Snapshot Kopie des Produktionssystems in Sekundenschnelle bereitstellen. Das neue Volume muss dann an das Testsystem angeschlossen und die HANA-Datenbank wiederhergestellt werden.

Der zweite Anwendungsfall ist die Erstellung eines Reparatursystems, mit dem eine logische Beschädigung im Produktionssystem bewältigt wird. In diesem Fall wird ein älteres Snapshot Backup des Produktionssystems verwendet, um ein Reparatursystem zu starten, das ein identischer Klon des Produktionssystems mit den Daten ist, bevor die Beschädigung aufgetreten ist. Das Reparatursystem wird dann verwendet, um das Problem zu analysieren und die erforderlichen Daten zu exportieren, bevor sie beschädigt wurden.

Im letzten Anwendungsfall kann ein Disaster-Recovery-Failover-Test ausgeführt werden, ohne die Replizierung zu unterbrechen. Dies hat keinen Einfluss auf RTO und Recovery Point Objective (RPO) des Disaster-Recovery-Setups. Wenn die Daten mithilfe von FSX für ONTAP Replizierung mit NetApp SnapMirror am Disaster Recovery-Standort repliziert werden, stehen am Disaster Recovery-Standort Snapshot Backups der Produktionsumgebung zur Verfügung und können dann für Tests im Disaster Recovery ein neues Volume erstellt werden.

Use Cases for Cloning Operations

- SAP System Refresh
  - Fast creation of a new volume based on a production Snapshot backup
  - Attach volume to the test system and recover HANA database with SID change
- Repair System creation to address logical corruption
  - Fast creation of a new volume based on a production Snapshot backup
  - Attach volume to the repair system and recover HANA database w/o SID change
- Disaster Recovery testing
  - Combined with SnapMirror Replication
  - Attach storage clone from a replicated production Snapshot backup to a DR test system



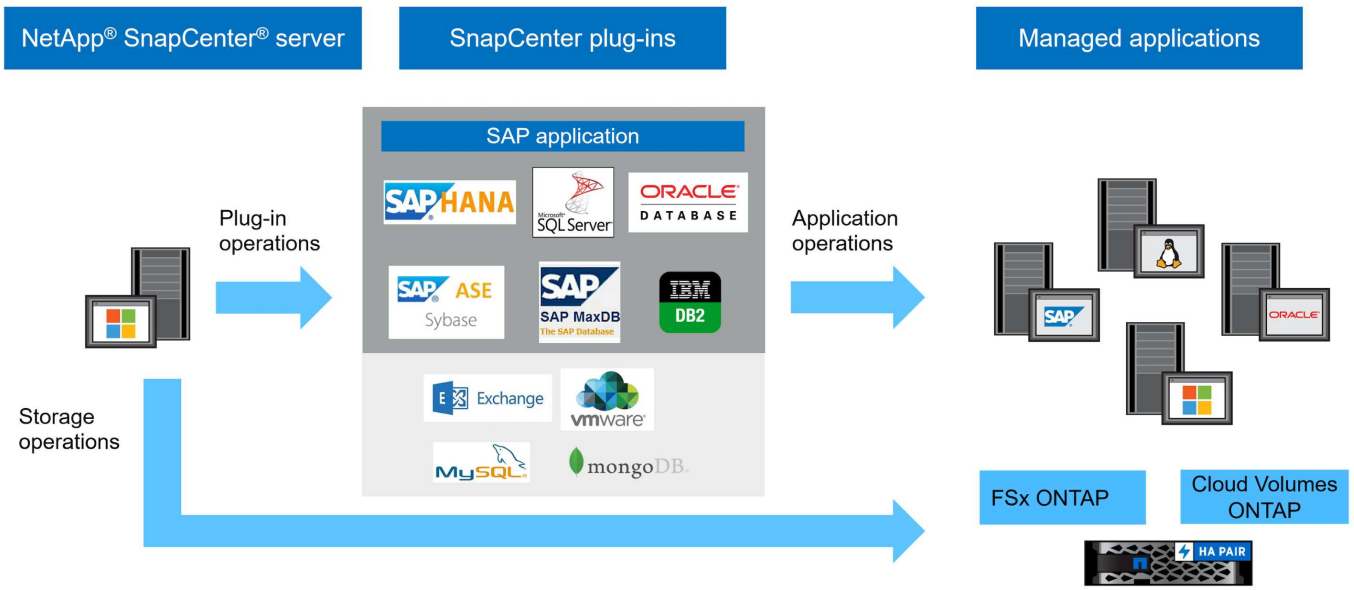
Architektur von SnapCenter

SnapCenter ist eine einheitliche, skalierbare Plattform für applikationskonsistente Datensicherung. SnapCenter bietet zentrale Kontrolle und Überwachung und delegiert die Möglichkeit, dass Benutzer applikationsspezifische Backup-, Restore- und Klonaufgaben managen können. Mit SnapCenter erhalten Datenbank- und Storage-Administratoren ein Tool, mit dem sie Backup-, Wiederherstellungs- und Klonvorgänge für verschiedene Applikationen und Datenbanken managen können.

SnapCenter managt Daten über Endpunkte in der Data-Fabric-Architektur von NetApp hinweg. Daten können mit SnapCenter zwischen lokalen Umgebungen, zwischen lokalen Umgebungen und der Cloud sowie zwischen Private, Hybrid oder Public Clouds repliziert werden.

Komponenten von SnapCenter

SnapCenter umfasst den SnapCenter-Server, das SnapCenter-Plug-in-Paket für Windows und das SnapCenter-Plug-in-Paket für Linux. Jedes Paket enthält SnapCenter-Plug-ins für diverse Applikations- und Infrastrukturkomponenten.



SnapCenter SAP HANA Backup-Lösung

Die SnapCenter Backup-Lösung für SAP HANA umfasst folgende Bereiche:

- Backup-Vorgänge, Planung und Aufbewahrungsmanagement
  - SAP HANA Daten-Backup mit Storage-basierten Snapshot Kopien
  - Backup nicht datenbasierter Volumes mit Storage-basierten Snapshot Kopien (z. B. `/hana/shared`)
  - Integritätsprüfungen der Datenbankblöcke mithilfe eines dateibasierten Backups
  - Die Replizierung an ein externes Backup oder einen Disaster-Recovery-Standort
- Allgemeine Ordnung und Sauberkeit des SAP HANA Backup-Katalogs
  - Für HANA Daten-Backups (Snapshot und dateibasiert)
  - Für HANA-Protokoll-Backups
- Restore- und Recovery-Vorgänge
  - Automatisiertes Restore und Recovery
  - Restore von einzelnen Mandanten für SAP HANA (MDC)-Systeme

Backups von Datenbankdateien werden von SnapCenter in Kombination mit dem Plug-in für SAP HANA ausgeführt. Das Plug-in löst den Speicherpunkt für das SAP HANA Datenbank-Backup aus, sodass die Snapshot Kopien, die auf dem primären Storage-System erstellt werden, auf einem konsistenten Image der SAP HANA Datenbank basieren.

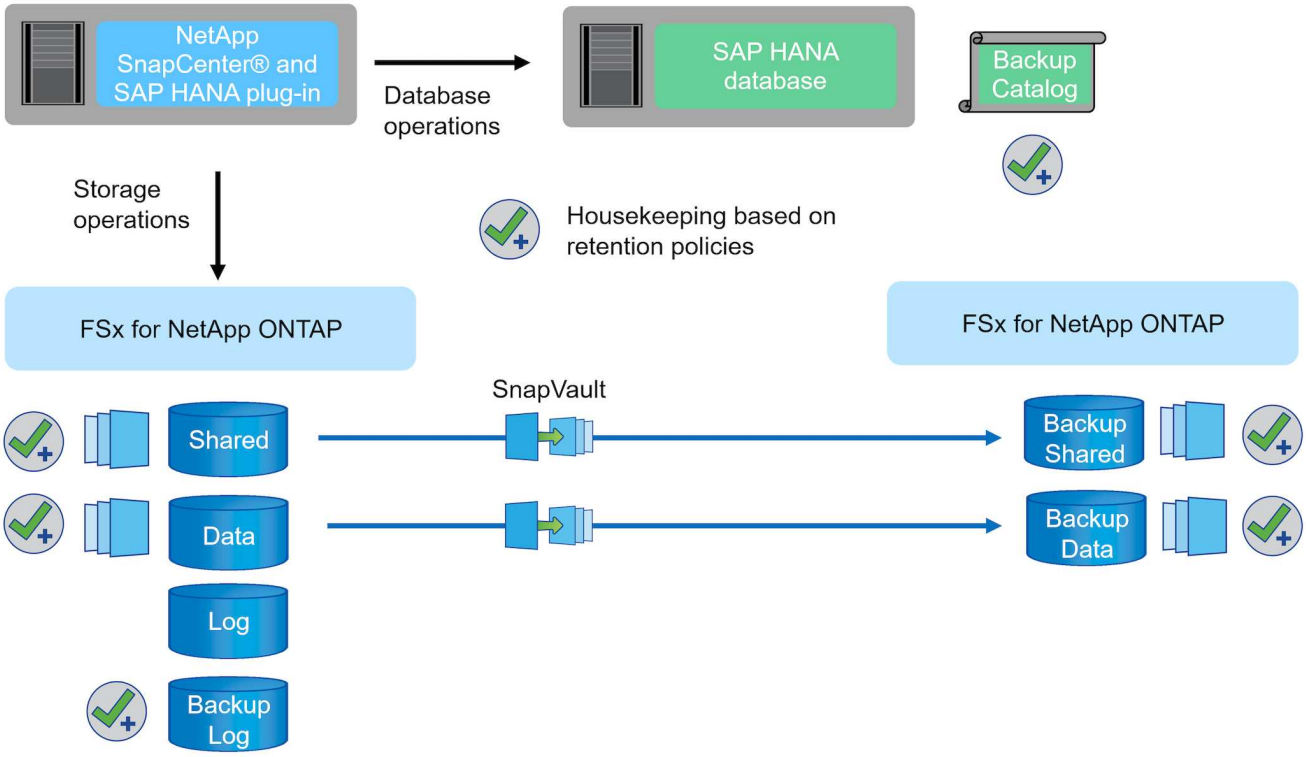
SnapCenter ermöglicht die Replizierung konsistenter Datenbank-Images auf einen externen Backup- oder Disaster-Recovery-Standort mithilfe von SnapVault oder der SnapMirror Funktion. In der Regel werden verschiedene Aufbewahrungsrichtlinien für Backups auf dem primären und externen Backup-Storage definiert. SnapCenter übernimmt die Aufbewahrung im Primärspeicher und ONTAP übernimmt die Aufbewahrung auf dem externen Backup-Storage.

Für ein vollständiges Backup aller mit SAP HANA verbundenen Ressourcen ermöglicht SnapCenter auch das Backup aller nicht datenbezogenen Volumes über das SAP HANA Plug-in mit Storage-basierten Snapshot Kopien. Sie können nicht-Daten-Volumes unabhängig vom Datenbank-Daten-Backup planen, um individuelle Aufbewahrungs- und Sicherungsrichtlinien zu aktivieren.

SAP empfiehlt, Storage-basierte Snapshot-Backups mit einem wöchentlichen dateibasierten Backup zu kombinieren, um eine Integritätsprüfung für Blöcke durchzuführen. Sie können die Integritätsprüfung der Blöcke in SnapCenter ausführen. Basierend auf Ihren konfigurierten Aufbewahrungsrichtlinien managt SnapCenter die allgemeine Ordnung und Sauberkeit der Datendatei-Backups im primären Storage, Backup von Protokolldateien und den SAP HANA Backup-Katalog.

SnapCenter übernimmt die Aufbewahrung auf dem primären Storage, während FSX für ONTAP die sekundäre Backup-Aufbewahrung managt.

Die folgende Abbildung bietet einen Überblick über die SnapCenter Backup- und Aufbewahrungsvorgänge.



Beim Ausführen eines Storage-basierten Snapshot Backups der SAP HANA Datenbank führt SnapCenter die folgenden Aufgaben durch:

1. Erstellung eines SAP HANA Backup-Speicherpunktes, um ein konsistentes Image auf der Persistenzschicht zu erstellen.
2. Erstellt eine Storage-basierte Snapshot Kopie des Daten-Volumes
3. Registrieren des Storage-basierten Snapshot-Backups im SAP HANA Backup-Katalog
4. Gibt den Speicherpunkt für SAP HANA Backup frei.
5. Führt, falls konfiguriert, ein SnapVault oder SnapMirror Update für das Daten-Volume durch
6. Löscht die Storage-Snapshot-Kopien im primären Storage auf der Grundlage der definierten Aufbewahrungsrichtlinien.
7. Löscht die Einträge des SAP HANA Backup-Katalogs, wenn die Backups nicht mehr im primären oder externen Backup-Speicher vorhanden sind.
8. Sobald ein Backup auf Basis der Aufbewahrungsrichtlinie oder manuell gelöscht wurde, löscht SnapCenter auch alle Log-Backups, die älter als das älteste Daten-Backup sind. Log-Backups werden im Dateisystem und im SAP HANA Backup-Katalog gelöscht.

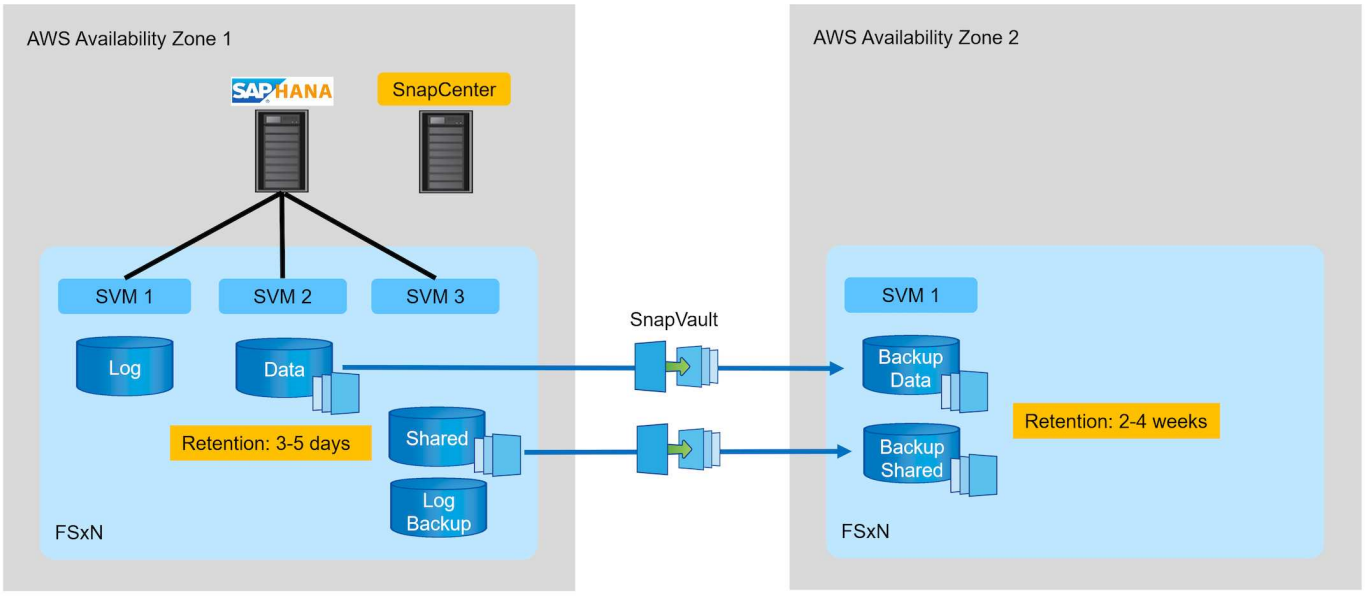
Inhalt des vorliegenden Dokuments

Dieses Dokument beschreibt die gängigste SnapCenter-Konfigurationsoption für ein einzelnes Hostsystem mit einem einzelnen SAP HANA MDC-Mandanten auf FSX für ONTAP. Es sind andere Konfigurationsoptionen möglich und in manchen Fällen auch für bestimmte SAP HANA Systeme erforderlich, beispielsweise für ein mehrere Host-Systeme. Eine ausführliche Beschreibung zu anderen Konfigurationsoptionen finden Sie unter "SnapCenter-Konzepte und Best Practices (netapp.com)".

In diesem Dokument verwenden wir die Amazon Web Services (AWS)-Konsole und die FSX für ONTAP CLI, um die erforderlichen Konfigurationsschritte auf der Storage-Ebene auszuführen. Sie können FSX für ONTAP auch mit NetApp Cloud Manager managen. Dies ist jedoch nicht im Umfang dieses Dokuments enthalten. Informationen zur Verwendung von NetApp Cloud Manager für FSX für ONTAP finden Sie unter "Weitere Informationen zu Amazon FSX für ONTAP (netapp.com)".

Datensicherung Strategie

Die folgende Abbildung zeigt eine typische Backup-Architektur für SAP HANA auf FSX für ONTAP. Das HANA-System befindet sich in der AWS-Verfügbarkeitszone 1 und verwendet ein FSX für ONTAP-Dateisystem innerhalb derselben Verfügbarkeitszone. Snapshot Backup-Vorgänge werden für die Daten und das gemeinsam genutzte Volume der HANA Datenbank ausgeführt. Neben den lokalen Snapshot Backups, die 3-5 Tage aufbewahrt werden, werden Backups auch zur längerfristigen Aufbewahrung auf einen externen Storage repliziert. Der externe Backup-Storage ist ein zweites FSX für ONTAP-Filesystem, das sich in einer anderen AWS-Verfügbarkeitszone befindet. Backups der HANA Daten und des gemeinsam genutzten Volumes werden mit SnapVault in die zweite FSX für ONTAP Filesystem repliziert und 2-3 Wochen aufbewahrt.



Vor dem Konfigurieren von SnapCenter muss die Datensicherungsstrategie auf Basis der RTO- und RPO-Anforderungen der verschiedenen SAP Systeme definiert werden.

Ein gemeinsamer Ansatz besteht in der Definition von Systemtypen wie Systemen für Produktion, Entwicklung, Test oder Sandbox. Alle SAP-Systeme des gleichen Systemtyps haben typischerweise die gleichen Datenschutzparameter.

Folgende Parameter müssen definiert werden:

- Wie oft sollte ein Snapshot Backup ausgeführt werden?
- Wie lange sollten Snapshot Kopien Backups auf dem Primärspeichersystem aufbewahrt werden?

- Wie oft sollte eine Blockintegritätsprüfung ausgeführt werden?
- Sollten die primären Backups auf einen externen Backup-Standort repliziert werden?
- Wie lange sollten die Backups auf dem externen Backup-Storage aufbewahrt werden?

Die folgende Tabelle zeigt ein Beispiel für die Datensicherungsparameter für die Systemtypen: Produktion, Entwicklung und Test. Für das Produktionssystem wurde eine hohe Backup-Frequenz definiert und die Backups werden einmal pro Tag an einen externen Backup-Standort repliziert. Die Testsysteme haben niedrigere Anforderungen und keine Replikation der Backups.

Parameter	Produktionssysteme auszuführen	Entwicklungssysteme	Testsysteme
Sicherungshäufigkeit	Alle 6 Stunden	Alle 6 Stunden	Alle 6 Stunden
Primäre Aufbewahrung	3 Tage	3 Tage	3 Tage
Block-Integritätsprüfung	Einmal in der Woche	Einmal in der Woche	Nein
Replizierung an externe Backup-Standorte	Einmal am Tag	Einmal am Tag	Nein
Externe Backup-Aufbewahrung	2 Wochen	2 Wochen	Keine Angabe

In der folgenden Tabelle werden die Richtlinien aufgeführt, die für die Datensicherheitsparameter konfiguriert werden müssen.

Parameter	RichtliniengebietsSnap	Policy LocalSnapAndSnapVault	RichtlinienblockIntegritätsprüfung
Backup-Typ	Auf Snapshot-Basis	Auf Snapshot-Basis	File-basiert
Zeitplanhäufigkeit	Stündlich	Täglich	Wöchentlich
Primäre Aufbewahrung	Anzahl = 12	Anzahl = 3	Anzahl = 1
SnapVault Replizierung	Nein	Ja.	Keine Angabe

Richtlinie `LocalSnapshot` Werden für Produktions-, Entwicklungs- und Testsysteme verwendet, um lokale Snapshot-Backups mit einer Aufbewahrung von zwei Tagen abzudecken.

In der Konfiguration für den Ressourcenschutz wird der Zeitplan für die Systemtypen unterschiedlich definiert:

- Produktion: Zeitplan alle 4 Stunden.
- Entwicklung: Alle 4 Stunden einplanen.
- Test: Alle 4 Stunden planen.

Richtlinie `LocalSnapAndSnapVault` Wird für die Produktions- und Entwicklungssysteme eingesetzt, um die tägliche Replizierung auf den externen Backup Storage zu decken.

In der Konfiguration für den Ressourcenschutz wird der Zeitplan für die Produktion und Entwicklung definiert:

- Produktion: Zeitplan jeden Tag.
- Entwicklung: Zeitplan jeden Tag.die Politik `BlockIntegrityCheck` Wird für die Produktions- und

Entwicklungssysteme eingesetzt, um die wöchentliche Blockintegritätsprüfung mithilfe eines dateibasierten Backups abzudecken.

In der Konfiguration für den Ressourcenschutz wird der Zeitplan für die Produktion und Entwicklung definiert:

- Produktion: Zeitplan jede Woche.
- Entwicklung: Zeitplan jede Woche.

Für jede einzelne SAP HANA Datenbank, die die externe Backup-Richtlinie nutzt, müssen Sie eine Sicherungsbeziehung auf der Storage-Ebene konfigurieren. Die Sicherungsbeziehung definiert, welche Volumes repliziert werden und wie die Aufbewahrung von Backups im externen Backup-Storage aufbewahrt wird.

Im folgenden Beispiel wird für jedes Produktions- und Entwicklungssystem im externen Backup-Storage eine Aufbewahrung von zwei Wochen definiert.

In diesem Beispiel unterscheiden sich die Sicherungsrichtlinien und die Aufbewahrung von SAP HANA Datenbankressourcen und Ressourcen ohne Datenvolumen.

Beispiel für die Laboreinrichtung

Das folgende Lab-Setup wurde als Beispielkonfiguration für den Rest dieses Dokuments verwendet.

HANA-System-PFX:

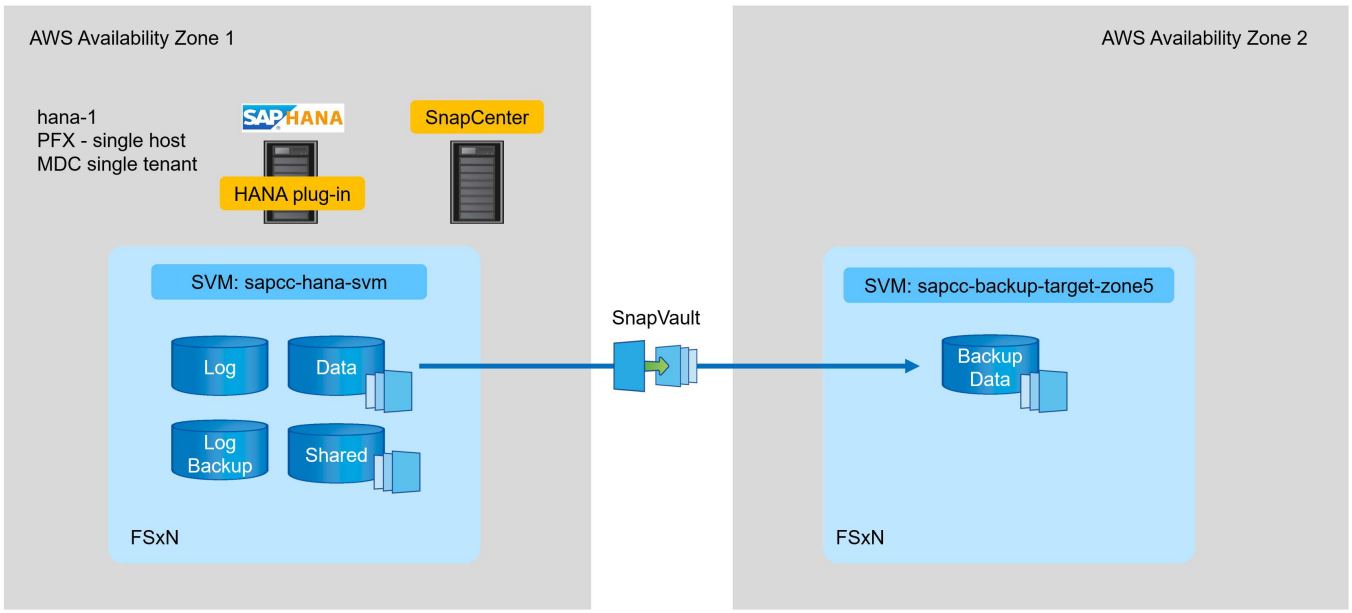
- Ein Host-MDC-System mit einem einzelnen Mandanten
- HANA 2.0 SPS 6, Version 60
- SLES FÜR SAP 15SP3

SnapCenter

- Version 4.6
- Auf einem HANA Datenbank-Host implementiertem HANA und Linux Plug-in

FSX für ONTAP-Dateisysteme:

- Zwei FSX für ONTAP Filesysteme mit einer einzigen Storage Virtual Machine (SVM)
- Jedes FSX für ONTAP-System in einer anderen AWS-Verfügbarkeitszone
- HANA Daten-Volume zur Replizierung in das zweite FSX für ONTAP Filesystem



SnapCenter-Konfiguration

Sie müssen die in diesem Abschnitt aufgeführten Schritte zur Basiskonfiguration von SnapCenter und zum Schutz der HANA-Ressource ausführen.

Übersicht über die Konfigurationsschritte

Führen Sie die folgenden Schritte für die SnapCenter Basiskonfiguration und den Schutz der HANA-Ressource durch. Jeder Schritt wird in den folgenden Kapiteln detailliert beschrieben.

1. Konfiguration des SAP HANA-Backup-Benutzers und des hdbuserstore-Schlüssels Zugriff auf die HANA-Datenbank mit dem hdbsql-Client
2. Konfigurieren Sie den Speicher in SnapCenter. Zugangsdaten für den Zugriff auf FSX für ONTAP SVMs von SnapCenter aus
3. Konfigurieren Sie Anmeldedaten für die Plug-in-Bereitstellung. Wird verwendet, um die erforderlichen SnapCenter-Plug-ins automatisch auf dem HANA-Datenbank-Host zu implementieren und zu installieren.
4. Fügen Sie HANA-Host zu SnapCenter hinzu. Implementierung und Installation der erforderlichen SnapCenter Plug-ins
5. Richtlinien konfigurieren. Definiert den Backup-Typ (Snapshot, Datei), die Aufbewahrung sowie optionale Snapshot Backup-Replizierung.
6. Konfigurieren Sie den Schutz von HANA-Ressourcen. Bereitstellung von hdbuserstore-Schlüsselrichtlinien und -Zeitplänen sowie Anhängen an die HANA-Ressource

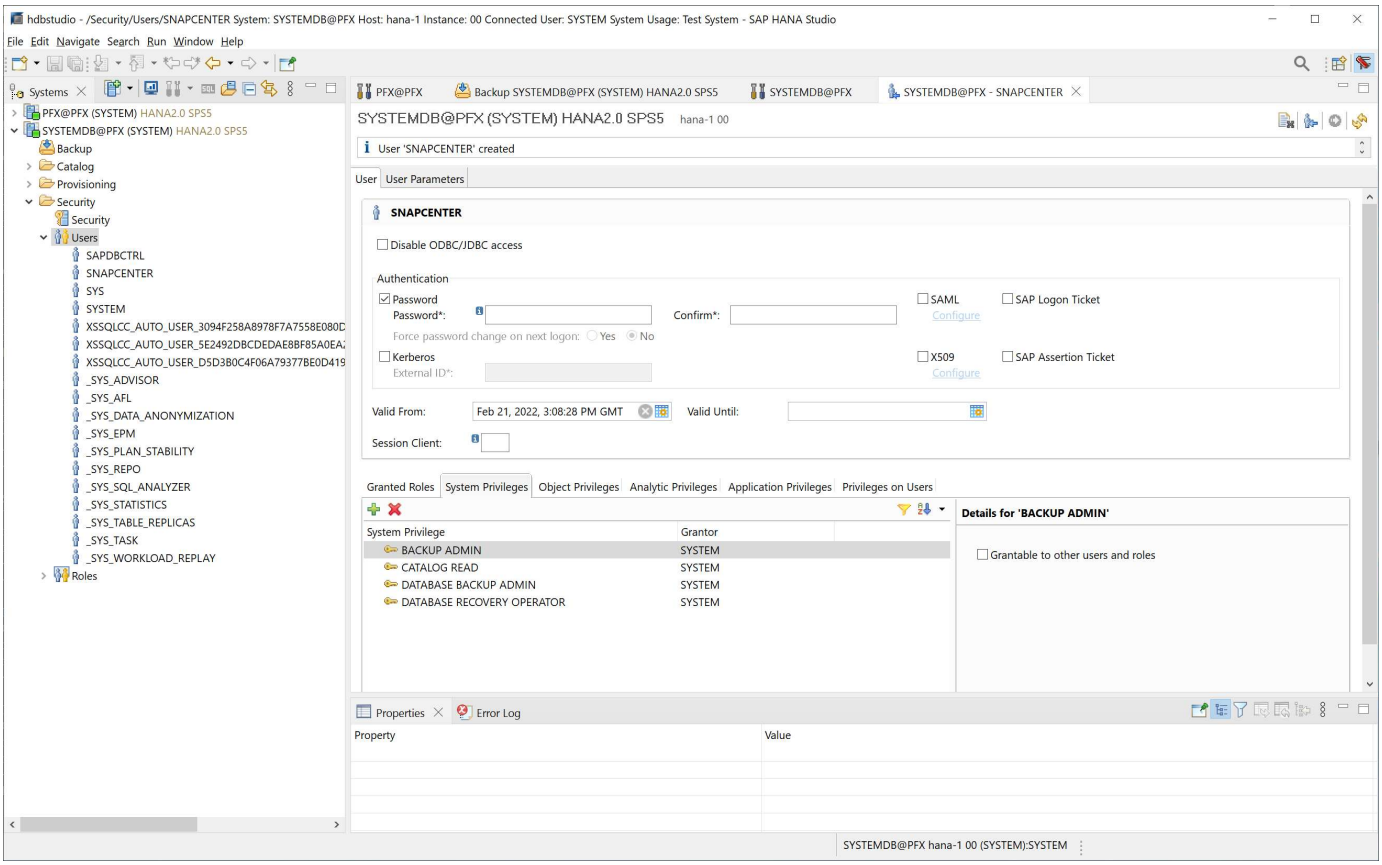
SAP HANA Backup-Benutzer und hdbuserstore-Konfiguration

NetApp empfiehlt, einen dedizierten Datenbankbenutzer in der HANA Datenbank zu konfigurieren, um Backup-Vorgänge mit SnapCenter auszuführen. Im zweiten Schritt wird für diesen Backup-Benutzer ein SAP HANA User Store Key konfiguriert und dieser User Store Key wird bei der Konfiguration des SnapCenter SAP HANA Plug-ins verwendet.

Die folgende Abbildung zeigt das SAP HANA Studio, über das Sie den Backup-Benutzer erstellen können

Die erforderlichen Berechtigungen werden mit HANA 2.0 SPS5 Version geändert: Backup-Admin, Lesevorgang im Katalog, Datenbank-Backup-Administrator und Datenbank-Recovery-Operator. Für ältere Versionen reichen der Backup-Administrator und der Lesevorgang des Katalogs aus.

Für ein SAP HANA MDC-System müssen Sie den Benutzer in der Systemdatenbank erstellen, da alle Backup-Befehle für das System und die Mandantendatenbanken über die Systemdatenbank ausgeführt werden.



Der folgende Befehl wird für die Konfiguration des Benutzerspeichers mit dem verwendet `<sid>adm` Benutzer:

```
hdbuserstore set <key> <host>:<port> <database user> <password>
```

SnapCenter verwendet das `<sid>adm` Benutzer zur Kommunikation mit der HANA-Datenbank. Daher müssen Sie den User Store Key mit dem <`sid>adm` Benutzer auf dem Datenbank-Host konfigurieren. In der Regel wird die SAP HANA hdbsql-Client-Software zusammen mit der Datenbank-Server-Installation installiert. Wenn dies nicht der Fall ist, müssen Sie zuerst den hdbclient installieren.

In einer SAP HANA MDC-Einrichtung, Port `3<instanceNo>13` Ist der Standard-Port für den SQL-Zugriff auf die Systemdatenbank und muss in der hdbuserstore-Konfiguration verwendet werden.

Für eine SAP HANA Einrichtung mit mehreren Hosts müssen Sie die Benutzerspeicherschlüssel für alle Hosts konfigurieren. SnapCenter versucht, über jeden der angegebenen Schlüssel eine Verbindung zur Datenbank herzustellen und kann somit unabhängig vom Failover eines SAP HANA Service zu einem anderen Host funktionieren. In unserem Labor-Setup haben wir einen User Store Key für den Benutzer konfiguriert `pfxadm` Für unser System PFX, ein einziges HANA MDC-Host-System mit einem einzelnen Mandanten.

```
pfxadm@hana-1:/usr/sap/PFX/home> hdbuserstore set PFXKEY hana-1:30013
SNAPCENTER <password>
Operation succeed.
```

```
pfxadm@hana-1:/usr/sap/PFX/home> hdbuserstore list
DATA FILE       : /usr/sap/PFX/home/.hdb/hana-1/SSFS_HDB.DAT
KEY FILE        : /usr/sap/PFX/home/.hdb/hana-1/SSFS_HDB.KEY
ACTIVE RECORDS  : 7
DELETED RECORDS : 0
KEY PFXKEY
  ENV : hana-1:30013
  USER: SNAPCENTER
KEY PFXSAPDBCTRL
  ENV : hana-1:30013
  USER: SAPDBCTRL
Operation succeed.
```

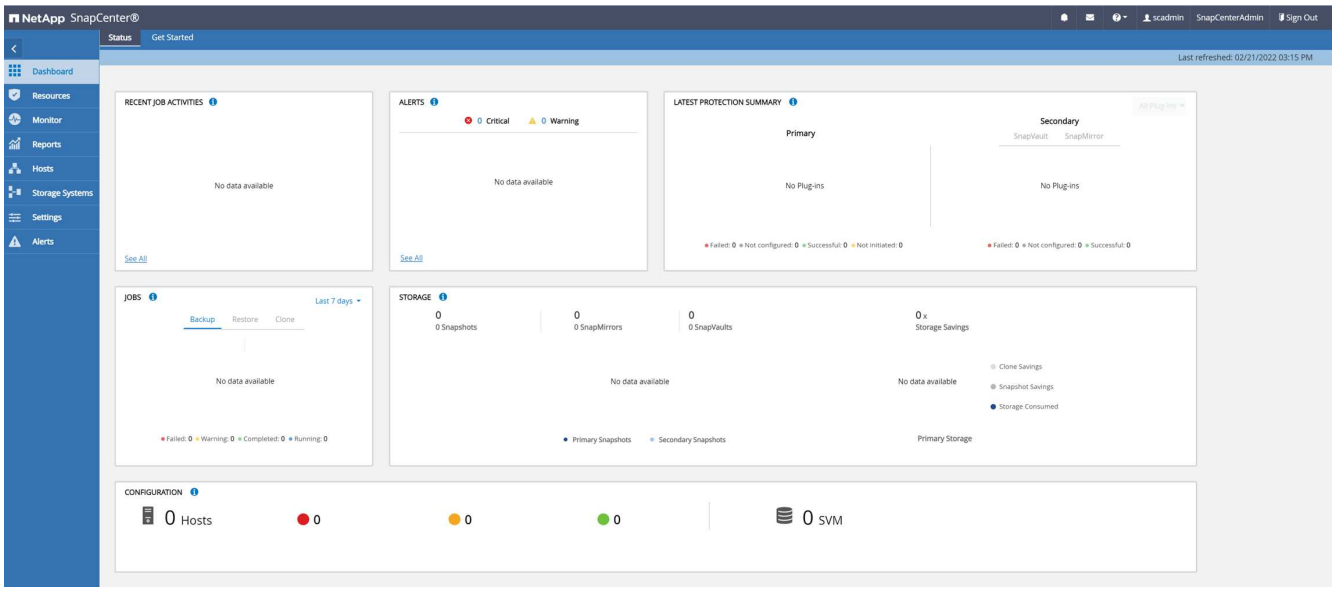
Sie können den Zugriff auf die HANA-Systemdatenbank prüfen, die den Schlüssel mit dem verwendet `hdbsql` Befehl.

```
pfxadm@hana-1:/usr/sap/PFX/home> hdbsql -U PFXKEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql SYSTEMDB=>
```

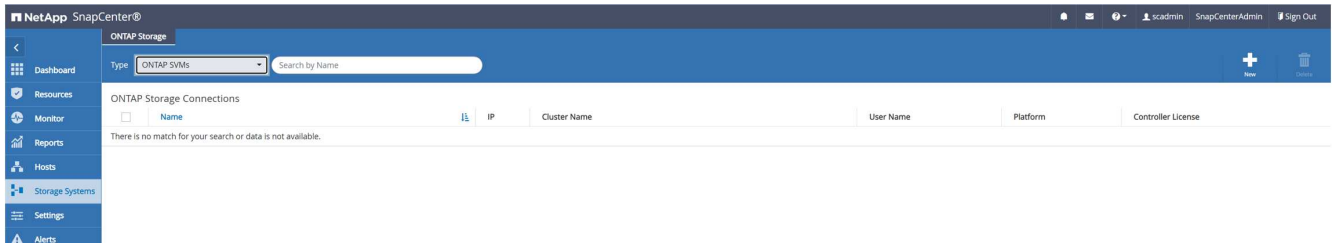
Speicher konfigurieren

Führen Sie diese Schritte aus, um Storage in SnapCenter zu konfigurieren.

1. Wählen Sie in der SnapCenter-Benutzeroberfläche Storage-Systeme aus.

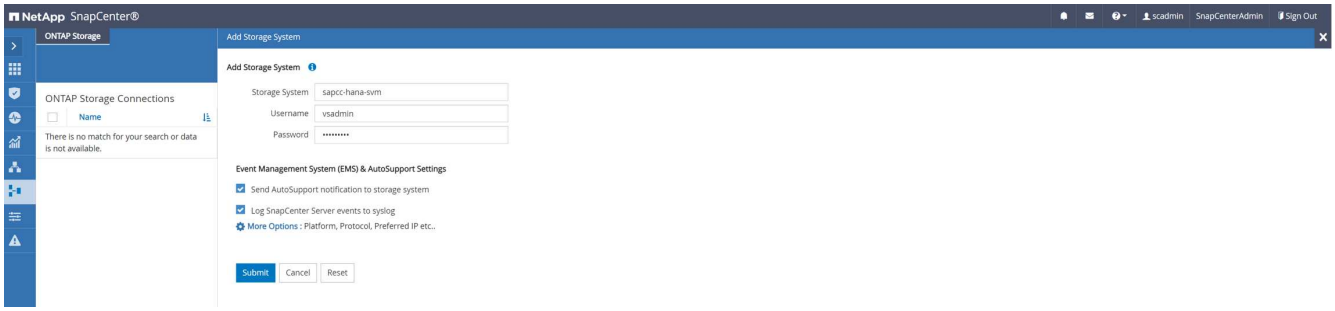


Sie können den Storage-Systemtyp auswählen, der ONTAP SVMs oder ONTAP Cluster sein kann. Im folgenden Beispiel ist das SVM-Management ausgewählt.

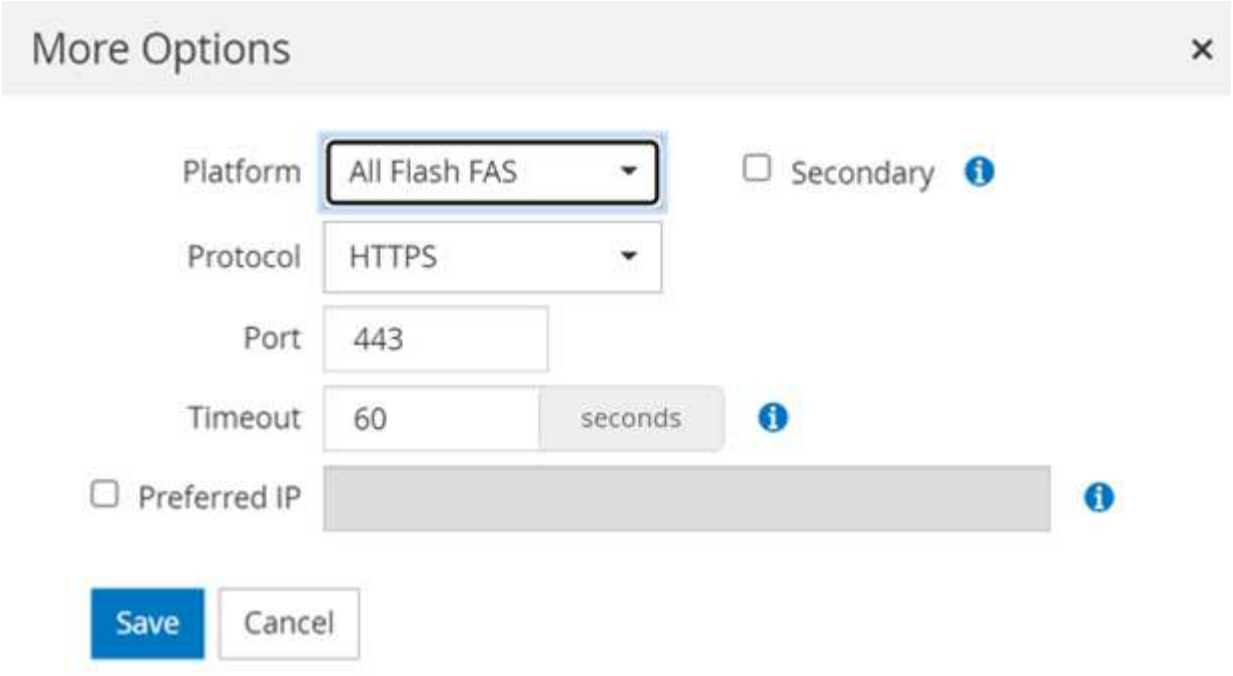


2. Klicken Sie auf Neu, um ein Speichersystem hinzuzufügen und den erforderlichen Hostnamen und die Anmeldeinformationen anzugeben.

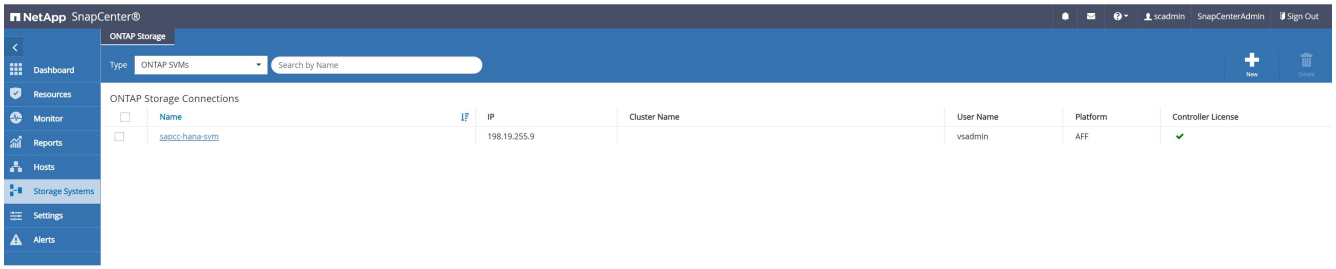
   Der SVM-Benutzer muss nicht wie in der folgenden Abbildung dargestellt vsadmin verwendet werden. In der Regel wird ein Benutzer für die SVM konfiguriert und den erforderlichen Berechtigungen zum Ausführen von Backup- und Restore-Vorgängen zugewiesen. Informationen zu erforderlichen Berechtigungen finden Sie unter "SnapCenter Installationshandbuch" Im Abschnitt „Minimale ONTAP-Berechtigungen erforderlich“.



3. Klicken Sie zum Konfigurieren der Speicherplattform auf Weitere Optionen.
4. Wählen Sie als Storage-System All-Flash FAS aus, um sicherzustellen, dass die Lizenz, die Teil des FSX für ONTAP ist, für SnapCenter verfügbar ist.



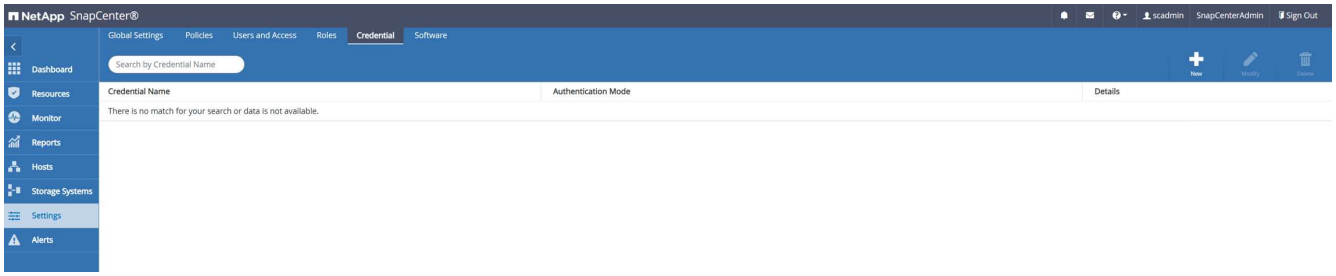
Der SVM `sapcc-hana-svm` Ist jetzt in SnapCenter konfiguriert.



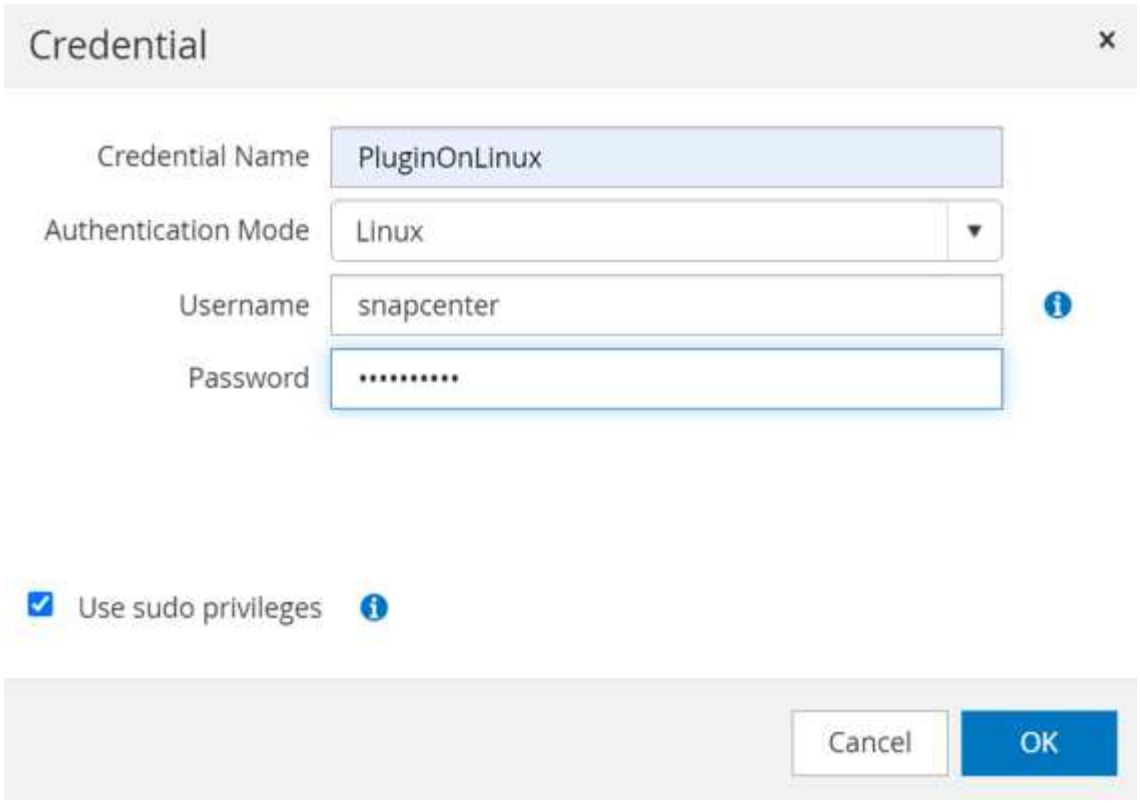
Anmeldedaten für Plug-in-Implementierung erstellen

Damit SnapCenter die erforderlichen Plug-ins auf den HANA-Hosts bereitstellen kann, müssen die Benutzeranmeldeinformationen konfiguriert werden.

1. Gehen Sie zu Einstellungen, wählen Sie Anmeldeinformationen aus, und klicken Sie auf Neu.



2. Im Lab-Setup haben wir einen neuen Benutzer, `snapcenter`, Auf dem HANA-Host, der für die Plug-in-Implementierung verwendet wird. Sie müssen sudo prvileges aktivieren, wie in der folgenden Abbildung dargestellt.




```
hana-1:/etc/sudoers.d # cat /etc/sudoers.d/90-cloud-init-users
# Created by cloud-init v. 20.2-8.48.1 on Mon, 14 Feb 2022 10:36:40 +0000
# User rules for ec2-user
ec2-user ALL=(ALL) NOPASSWD:ALL
# User rules for snapcenter user
snapcenter ALL=(ALL) NOPASSWD:ALL
hana-1:/etc/sudoers.d #
```

Hinzufügen eines SAP HANA-Hosts

Beim Hinzufügen eines SAP HANA-Hosts implementiert SnapCenter die erforderlichen Plug-ins auf dem Datenbank-Host und führt automatische Erkennungsvorgänge aus.

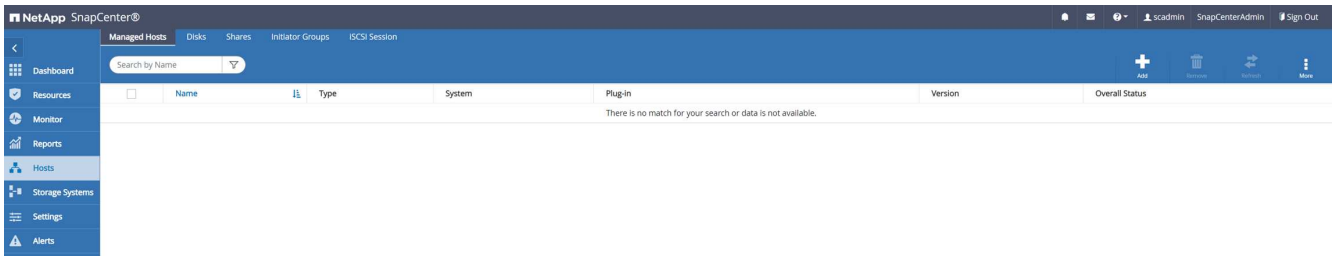
Für das SAP HANA Plug-in ist Java 64-Bit Version 1.8 erforderlich. Java muss auf dem Host installiert sein, bevor der Host zu SnapCenter hinzugefügt wird.

```
hana-1:/etc/ssh # java -version
openjdk version "1.8.0_312"
OpenJDK Runtime Environment (IcedTea 3.21.0) (build 1.8.0_312-b07 suse-
3.61.3-x86_64)
OpenJDK 64-Bit Server VM (build 25.312-b07, mixed mode)
hana-1:/etc/ssh #
```

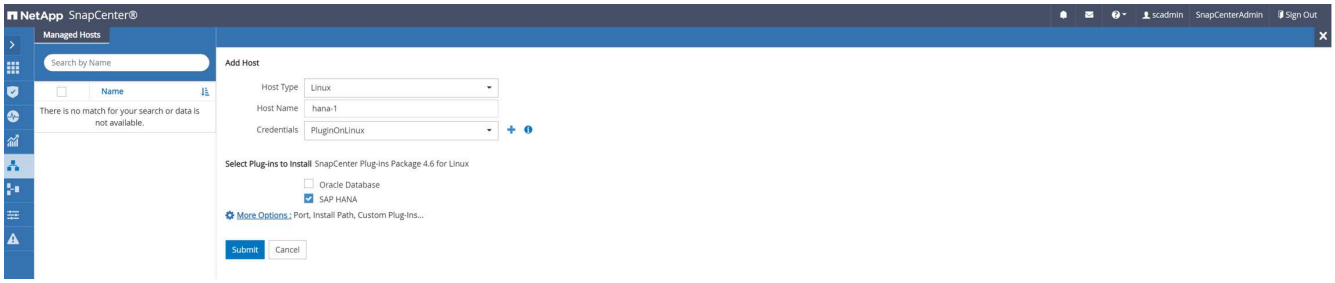
OpenJDK oder Oracle Java wird mit SnapCenter unterstützt.

Gehen Sie wie folgt vor, um den SAP HANA-Host hinzuzufügen:

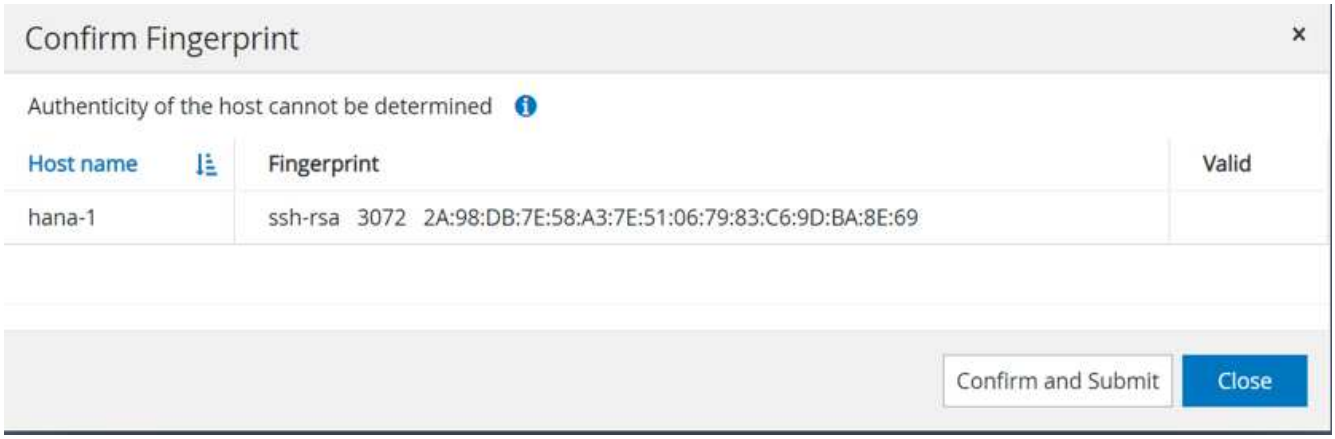
1. Klicken Sie auf der Registerkarte Host auf Hinzufügen.



2. Geben Sie Host-Informationen an, und wählen Sie das zu installierende SAP HANA-Plug-in aus. Klicken Sie Auf Senden.

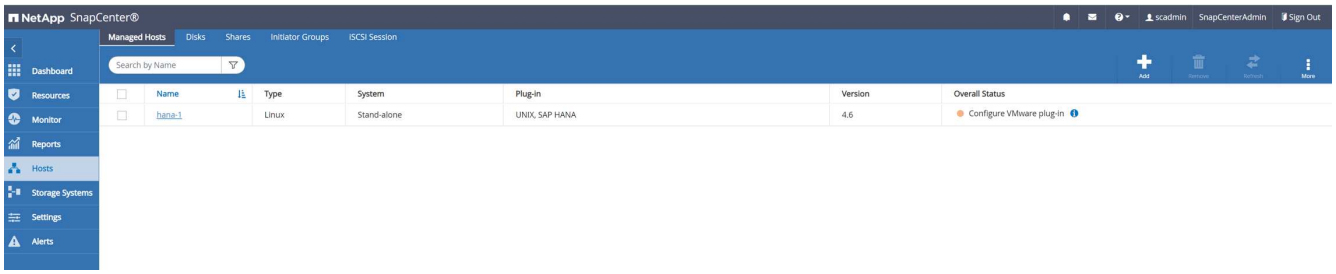


3. Bestätigen Sie den Fingerabdruck.



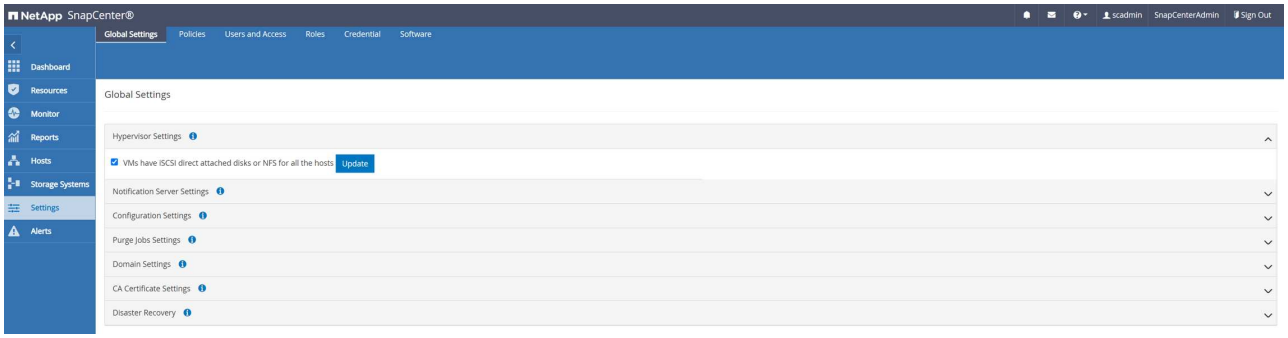
Die Installation des HANA und des Linux Plug-ins wird automatisch gestartet. Nach Abschluss der Installation wird in der Statusspalte des Hosts das VMware Plug-in konfigurieren angezeigt. SnapCenter erkennt, ob das SAP HANA Plug-in in in einer virtualisierten Umgebung installiert ist. Dabei kann es sich um eine VMware Umgebung oder eine Umgebung bei einem Public Cloud-Provider handelt. In diesem Fall zeigt SnapCenter eine Warnung an, um den Hypervisor zu konfigurieren.

Sie können die Warnmeldung mithilfe der folgenden Schritte entfernen.

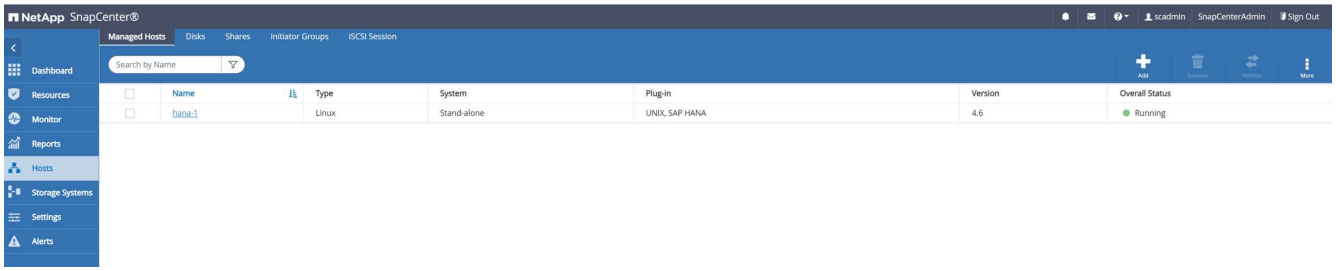


a. Wählen Sie auf der Registerkarte Einstellungen die Option Globale Einstellungen.

b. Wählen Sie für die Hypervisor-Einstellungen die Option VMs mit iSCSI Direct Attached Disks oder NFS für alle Hosts aus, und aktualisieren Sie die Einstellungen.



Der Bildschirm zeigt nun das Linux-Plug-in und das HANA-Plug-in mit dem Status läuft.



Richtlinien konfigurieren

Richtlinien werden normalerweise unabhängig von der Ressource konfiguriert und können von mehreren SAP HANA Datenbanken verwendet werden.

Eine typische Minimalkonfiguration umfasst folgende Richtlinien:

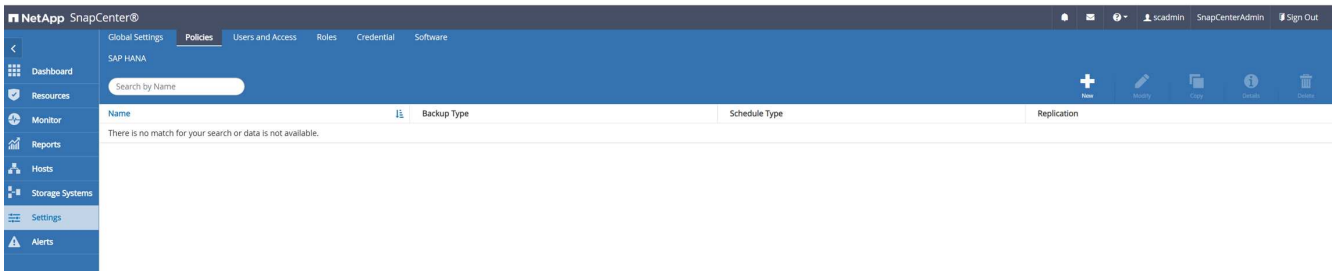
- Richtlinie für stündliche Backups ohne Replikation: `LocalSnap`.
- Richtlinie für wöchentliche Blockintegritätsprüfung über ein dateibasiertes Backup: `BlockIntegrityCheck`.

In den folgenden Abschnitten wird die Konfiguration dieser Richtlinien beschrieben.

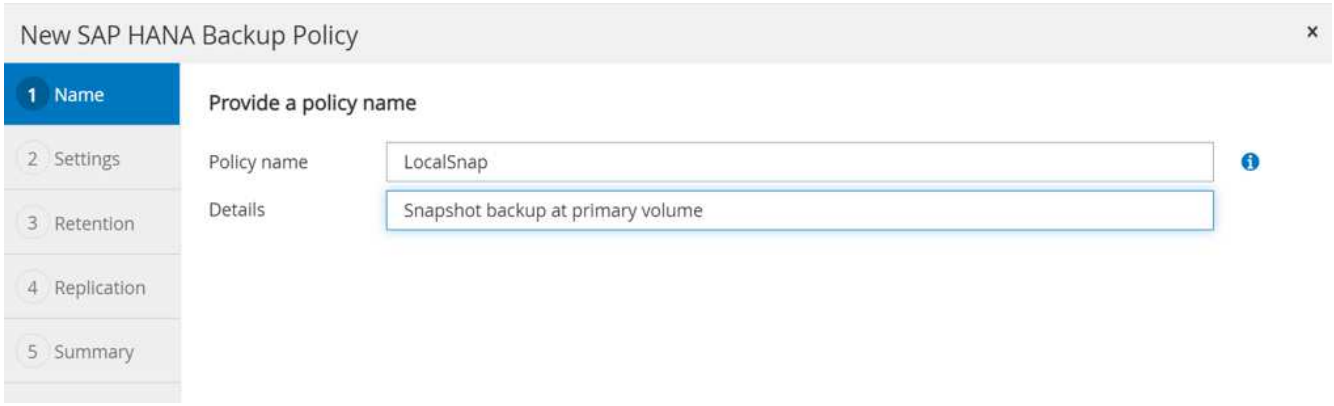
Richtlinien für Snapshot-Backups

Führen Sie diese Schritte aus, um Snapshot Backup-Richtlinien zu konfigurieren.

1. Gehen Sie zu Einstellungen > Richtlinien, und klicken Sie auf Neu.

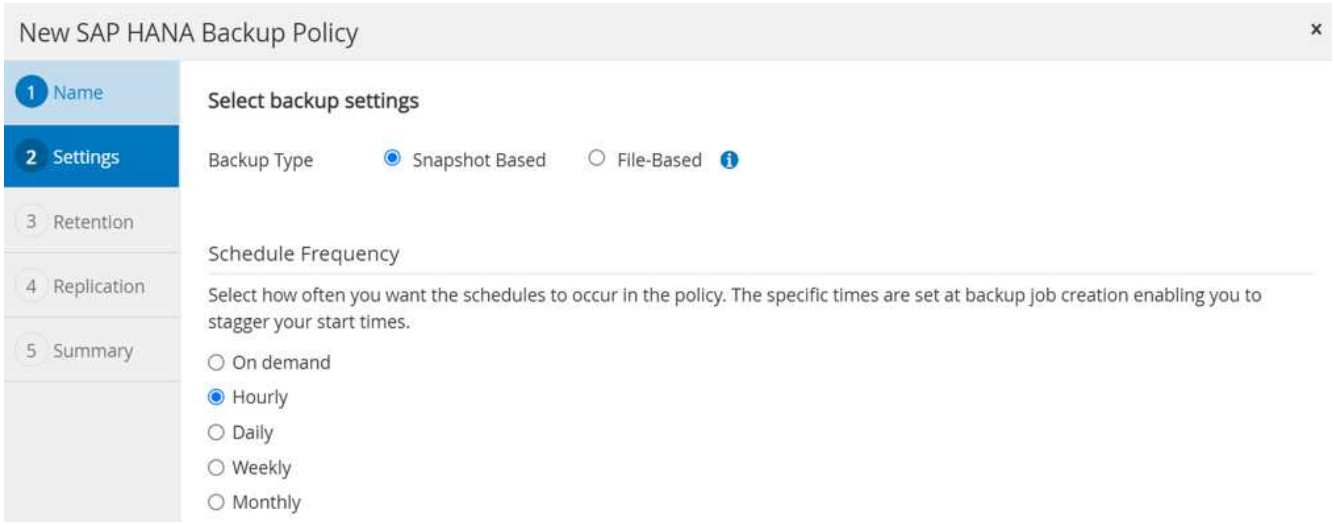


2. Geben Sie den Namen und die Beschreibung der Richtlinie ein. Klicken Sie Auf Weiter.

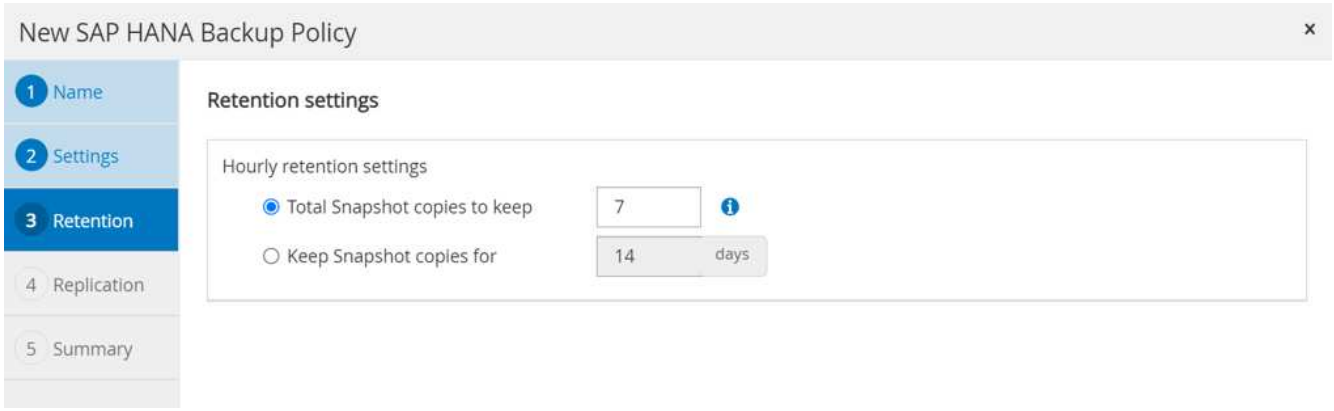


3. Wählen Sie den Backup-Typ als Snapshot-basiert aus und wählen Sie stündlich für die Zeitplanfrequenz aus.

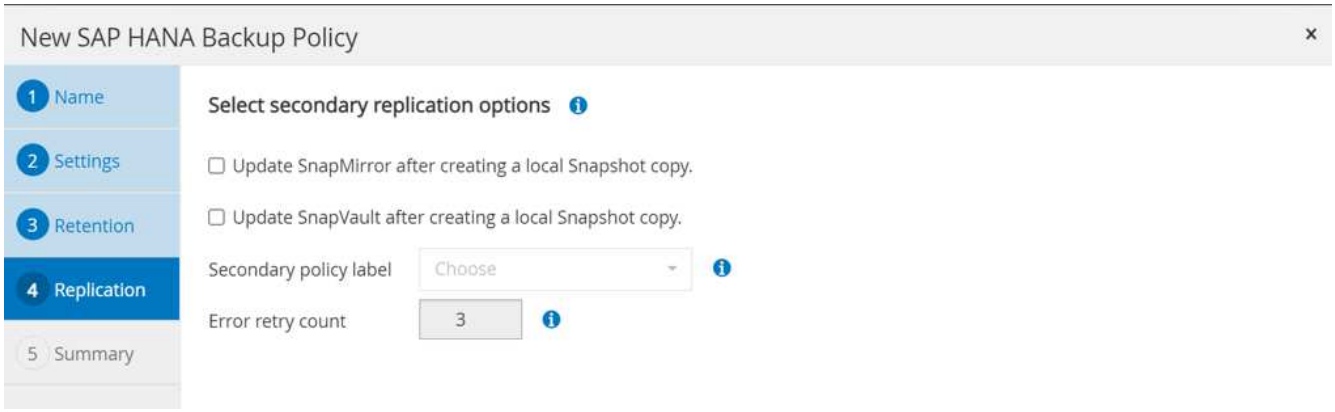
   Der Zeitplan selbst wird später mit der HANA-Ressourcenschutzkonfiguration konfiguriert.

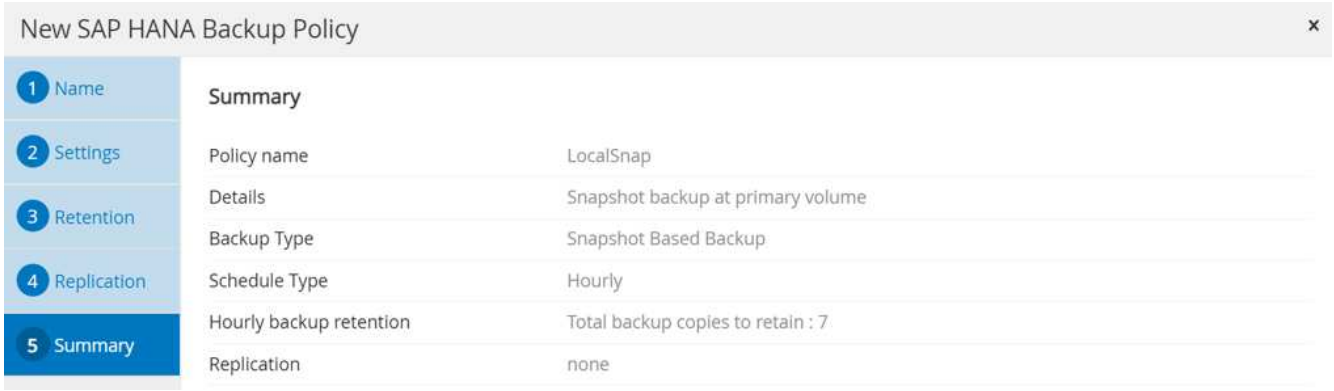


4. Konfigurieren Sie die Aufbewahrungseinstellungen für On-Demand-Backups.

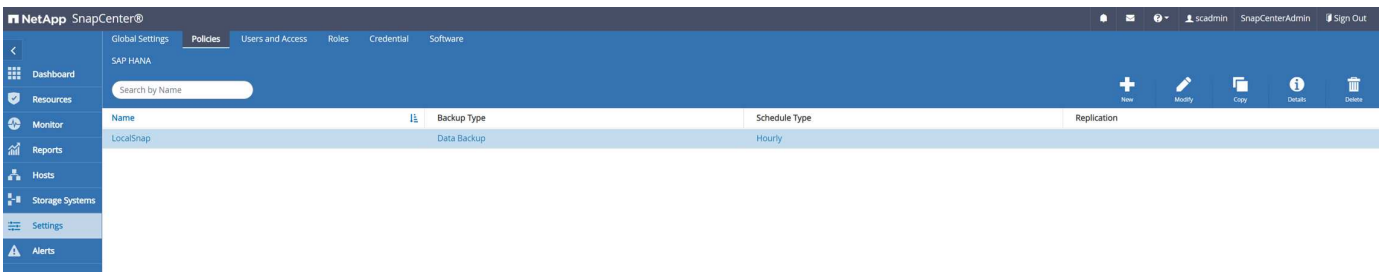


5. Konfigurieren der Replikationsoptionen. In diesem Fall ist kein SnapVault oder SnapMirror Update ausgewählt.





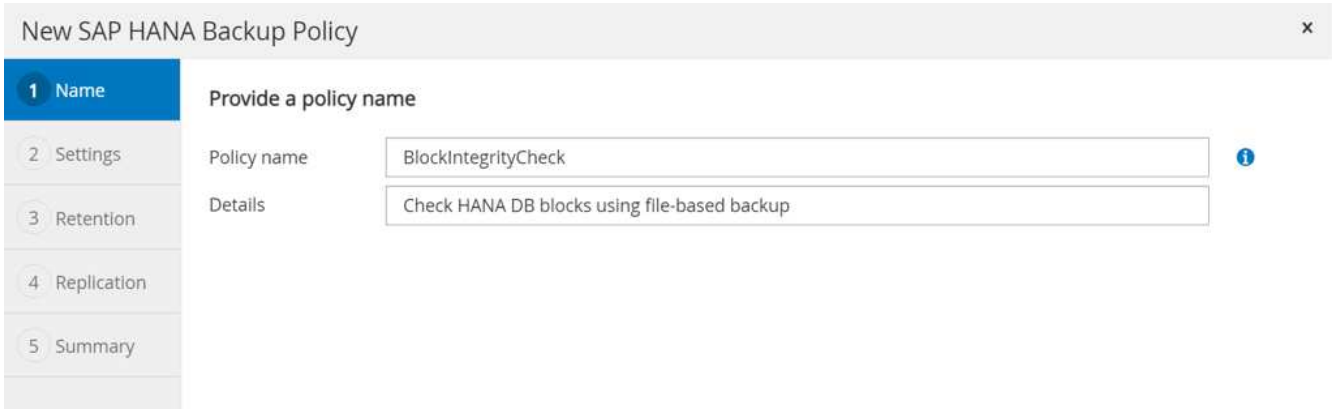
Die neue Richtlinie ist jetzt konfiguriert.



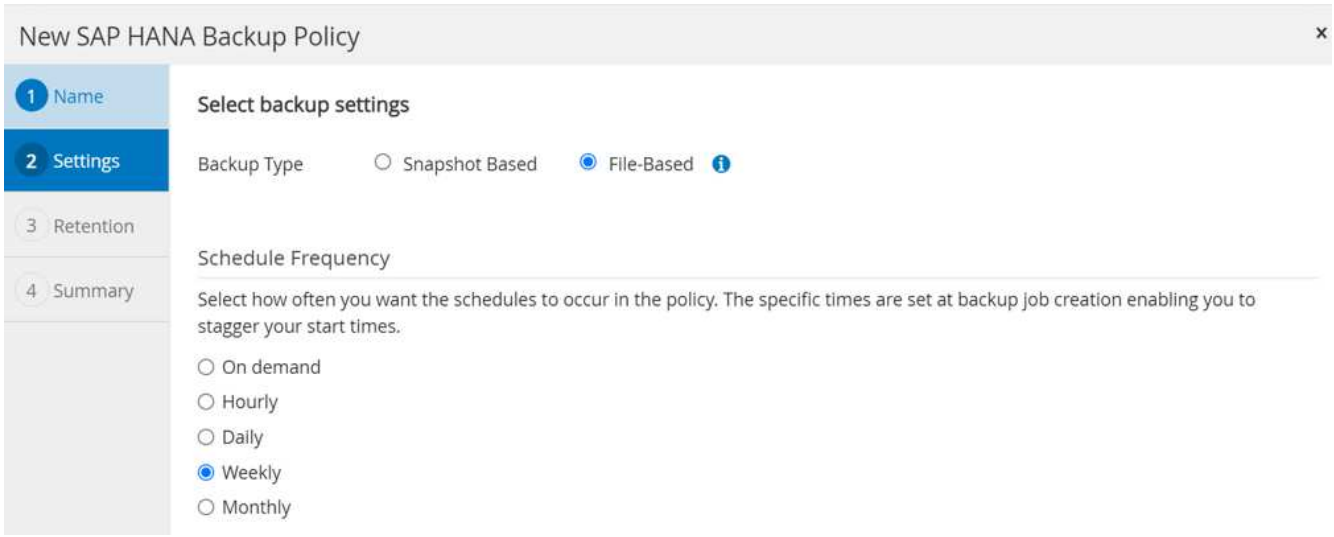
Richtlinie zur Block-Integritätsprüfung

Befolgen Sie diese Schritte, um die Richtlinie zur Integritätsprüfung von Blöcken zu konfigurieren.

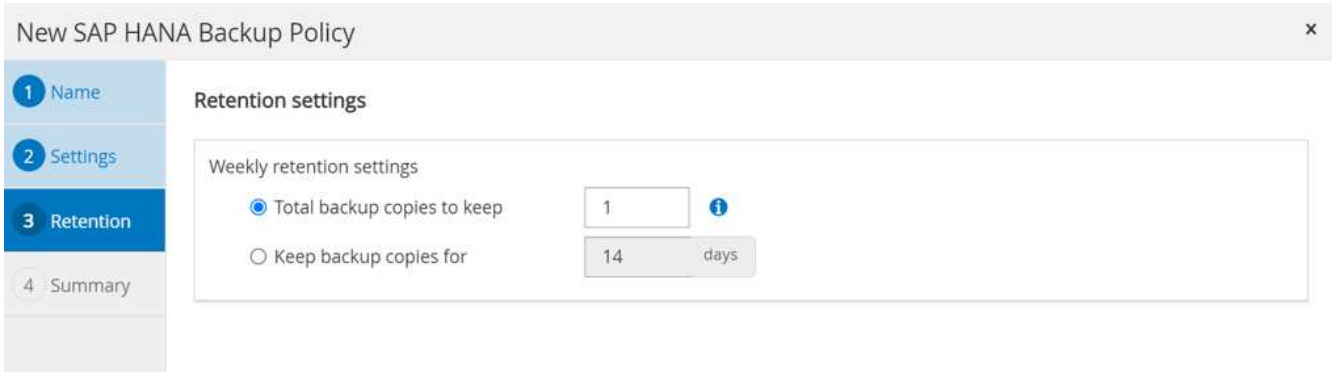
1. Gehen Sie zu Einstellungen > Richtlinien, und klicken Sie auf Neu.
2. Geben Sie den Namen und die Beschreibung der Richtlinie ein. Klicken Sie Auf Weiter.



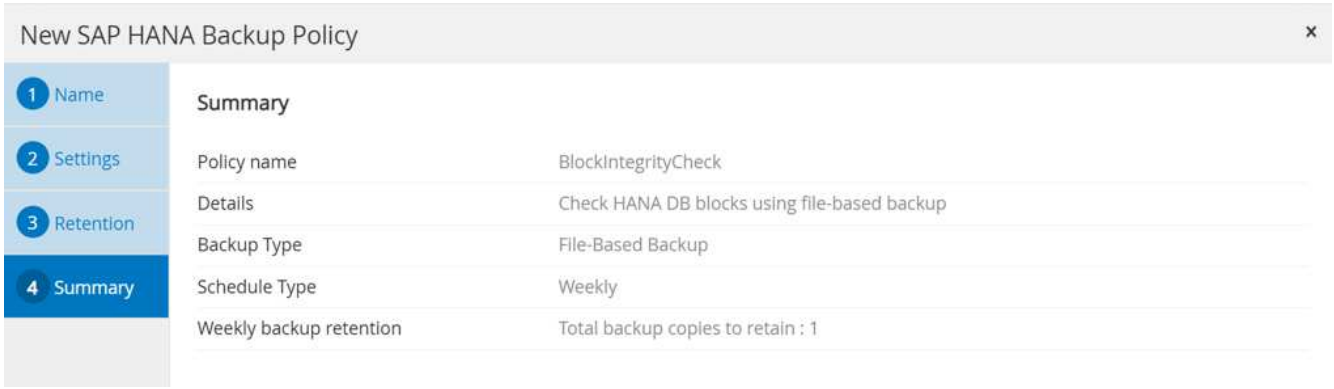
3. Legen Sie den Sicherungstyp auf „File-based“ und „Schedule Frequency“ auf „Weekly“ fest. Der Zeitplan selbst wird später mit der HANA-Ressourcenschutzkonfiguration konfiguriert.

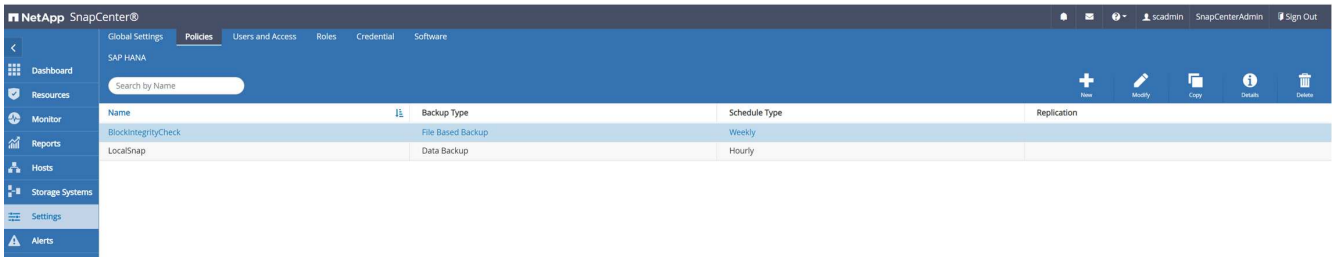


4. Konfigurieren Sie die Aufbewahrungseinstellungen für On-Demand-Backups.



5. Klicken Sie auf der Seite Zusammenfassung auf Fertig stellen.



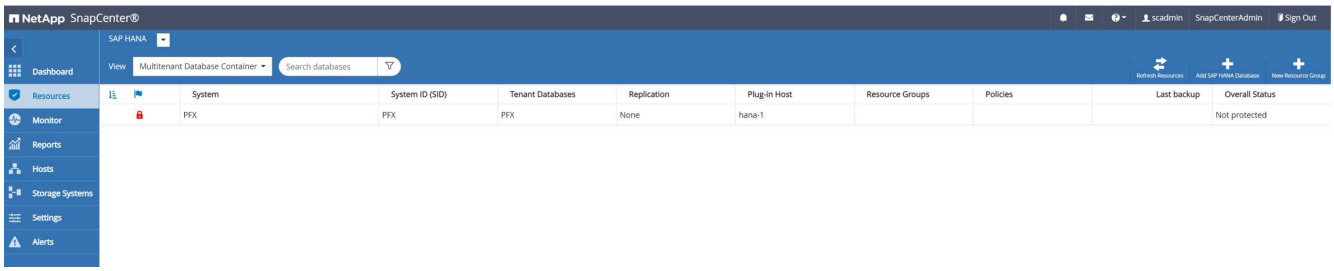


Konfiguration und Sicherung einer HANA-Ressource

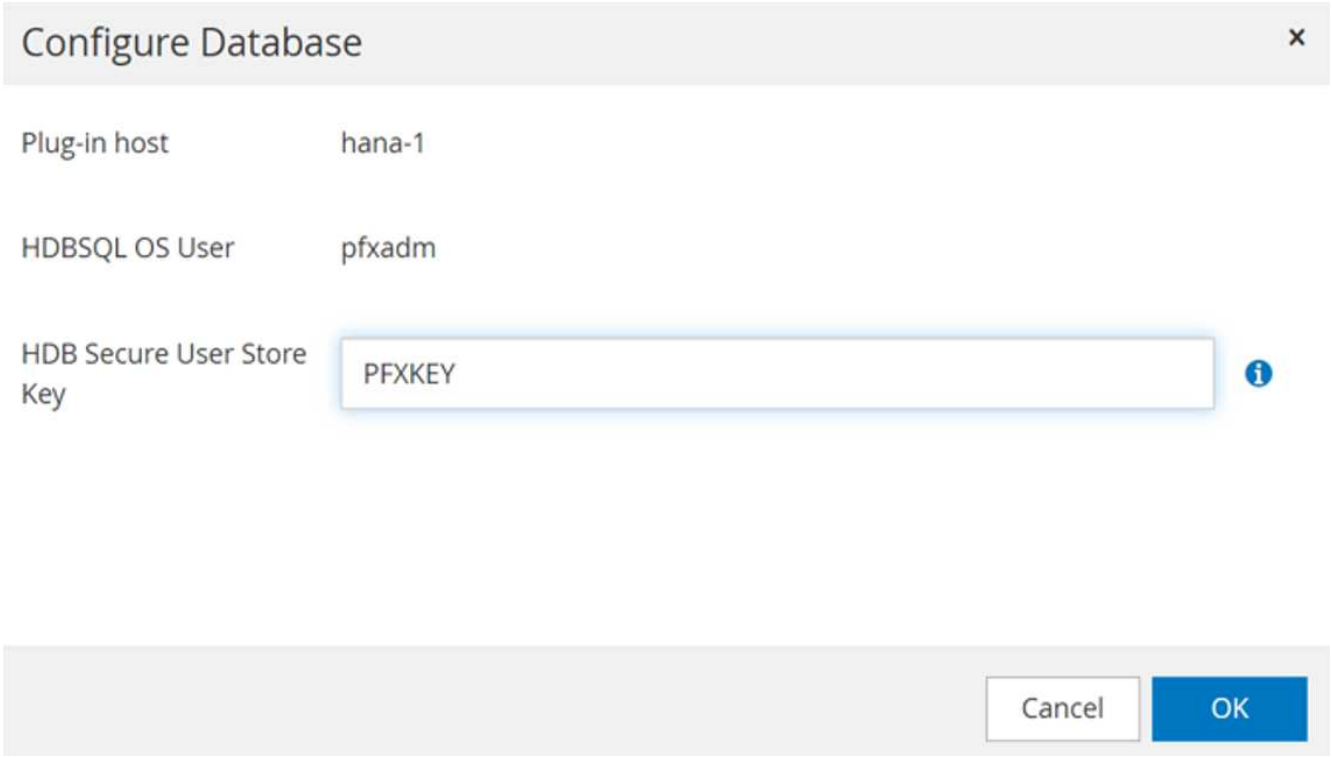
Nach der Plug-in-Installation startet der automatische Erkennungsvorgang der HANA-Ressource automatisch. Im Bildschirm Ressourcen wird eine neue Ressource erstellt, die mit dem roten Vorhängeschloss-Symbol als gesperrt markiert ist. Gehen Sie wie folgt vor, um die neue HANA-Ressource zu konfigurieren und zu schützen:

1. Wählen Sie und klicken Sie auf die Ressource, um mit der Konfiguration fortzufahren.

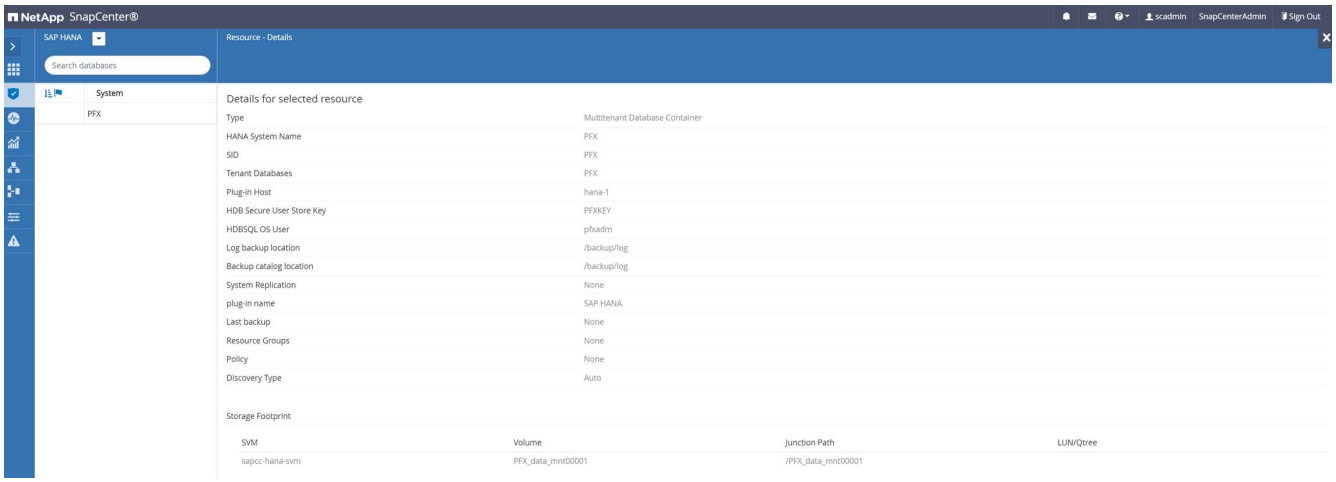
   Sie können den automatischen Erkennungsvorgang auch manuell im Bildschirm Ressourcen auslösen, indem Sie auf Ressourcen aktualisieren klicken.



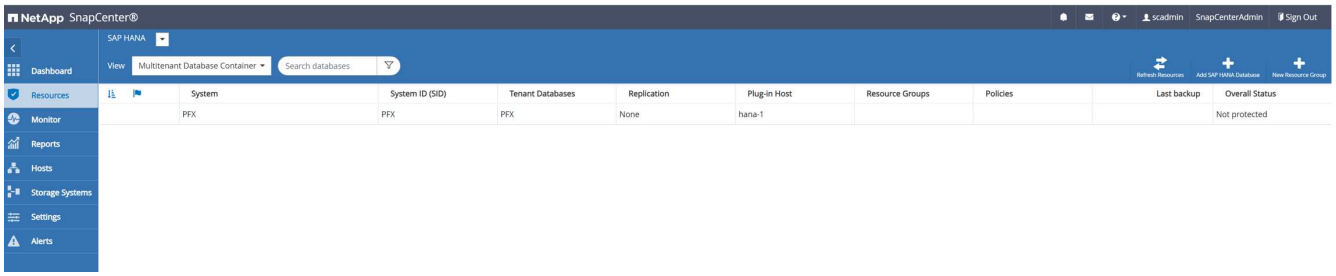
2. Geben Sie den UserStore-Schlüssel für die HANA-Datenbank an.



Der zweite Ebene-Prozess der automatischen Bestandsaufnahme beginnt, bei dem Mandantendaten und Storage-Platzbedarf erfasst werden.

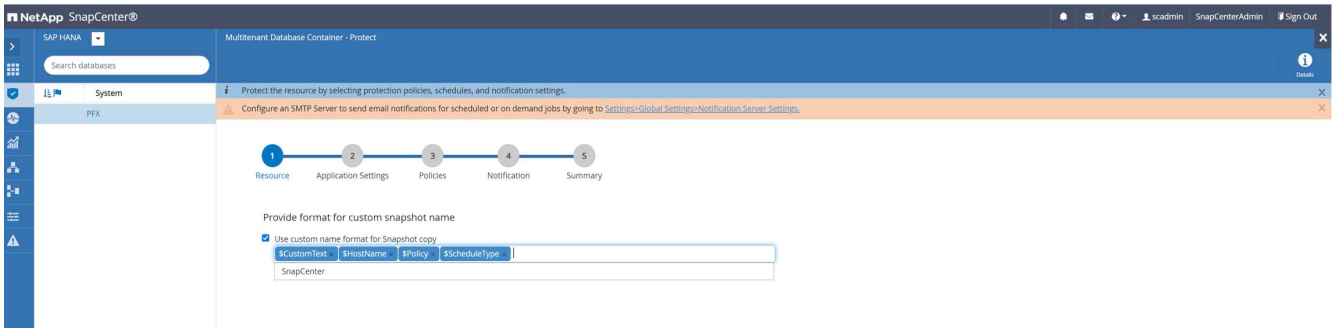


3. Doppelklicken Sie auf der Registerkarte Ressourcen auf die Ressource, um den Ressourcenschutz zu konfigurieren.

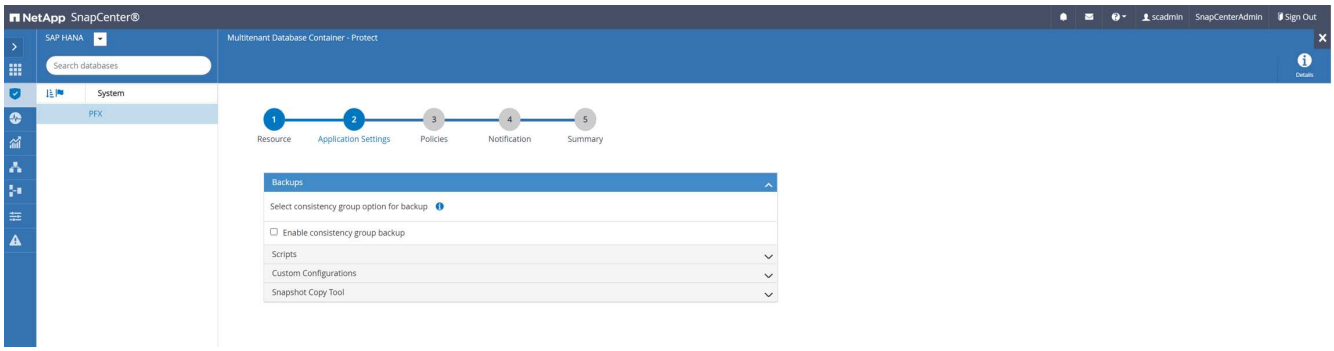


4. Konfigurieren Sie ein benutzerdefiniertes Namensformat für die Snapshot Kopie.

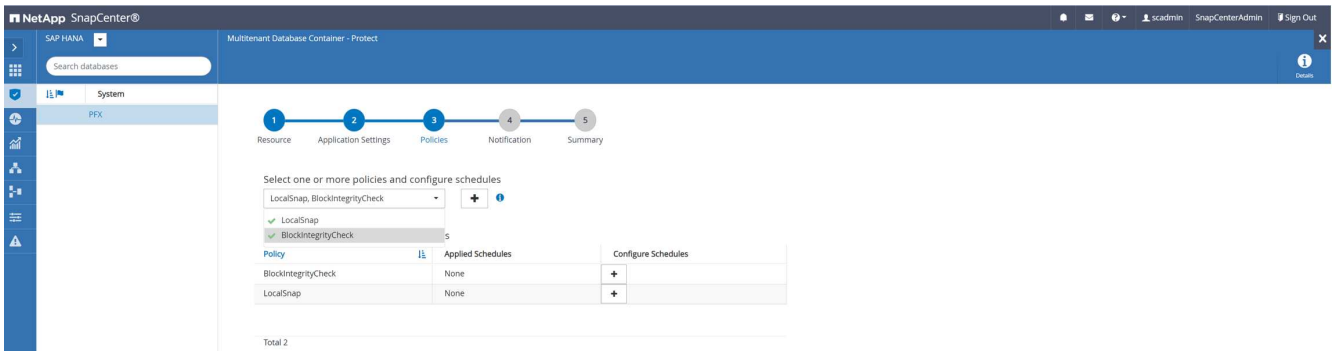
NetApp empfiehlt den Einsatz einer benutzerdefinierten Snapshot Kopie, um schnell ermitteln zu können, mit welcher Richtlinie und welche Zeitplantypen Backups erstellt wurden. Durch Hinzufügen des Zeitplantyps zum Namen der Snapshot Kopie können Sie zwischen geplanten und On-Demand-Backups unterscheiden. Der `schedule name` String für On-Demand-Backups ist leer, während geplante Backups den String enthalten `Hourly`, `Daily`, `or Weekly`.



5. Auf der Seite „Anwendungseinstellungen“ müssen keine spezifischen Einstellungen vorgenommen werden. Klicken Sie Auf Weiter.

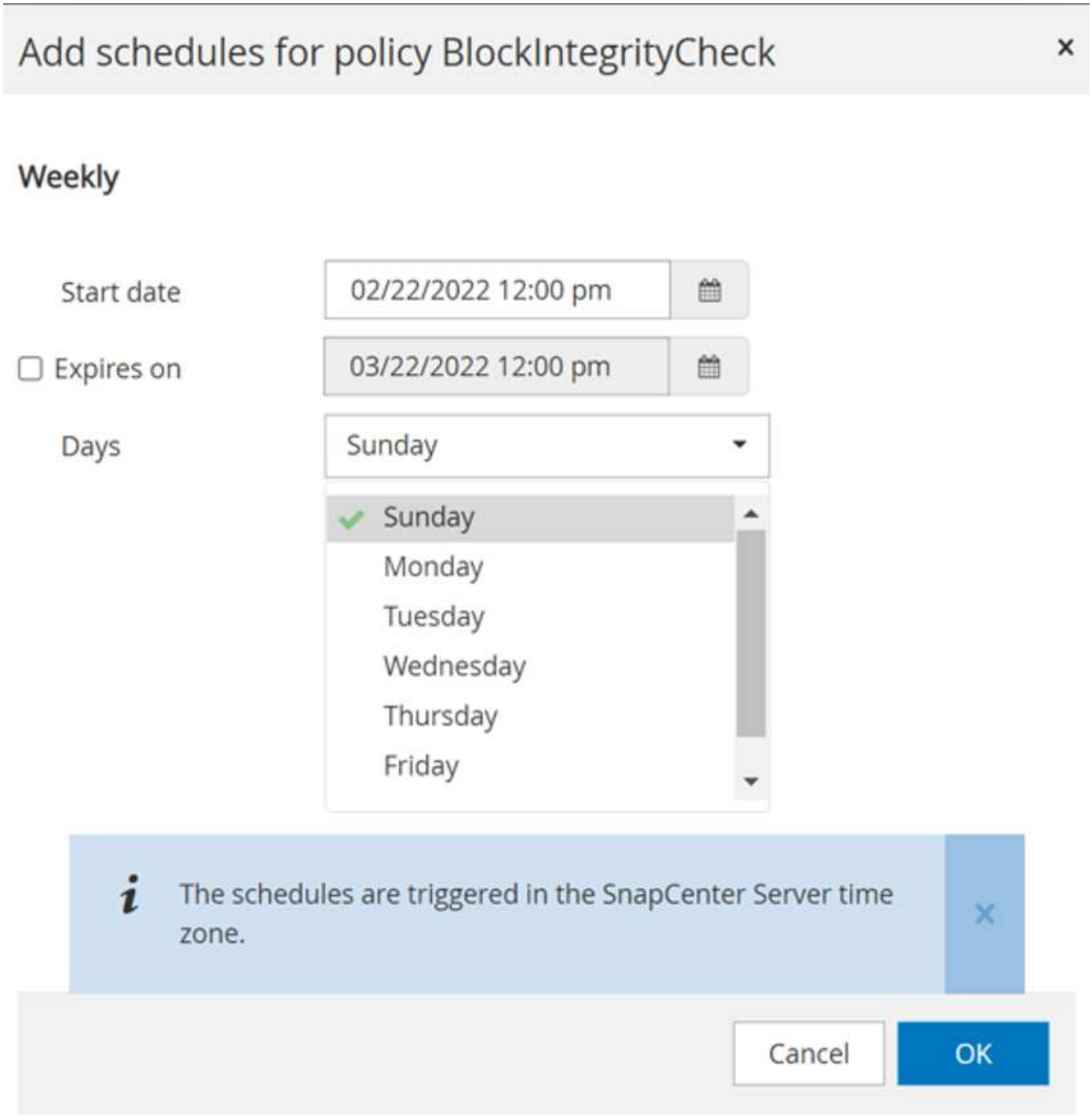


6. Wählen Sie die Richtlinien aus, die der Ressource hinzugefügt werden sollen.



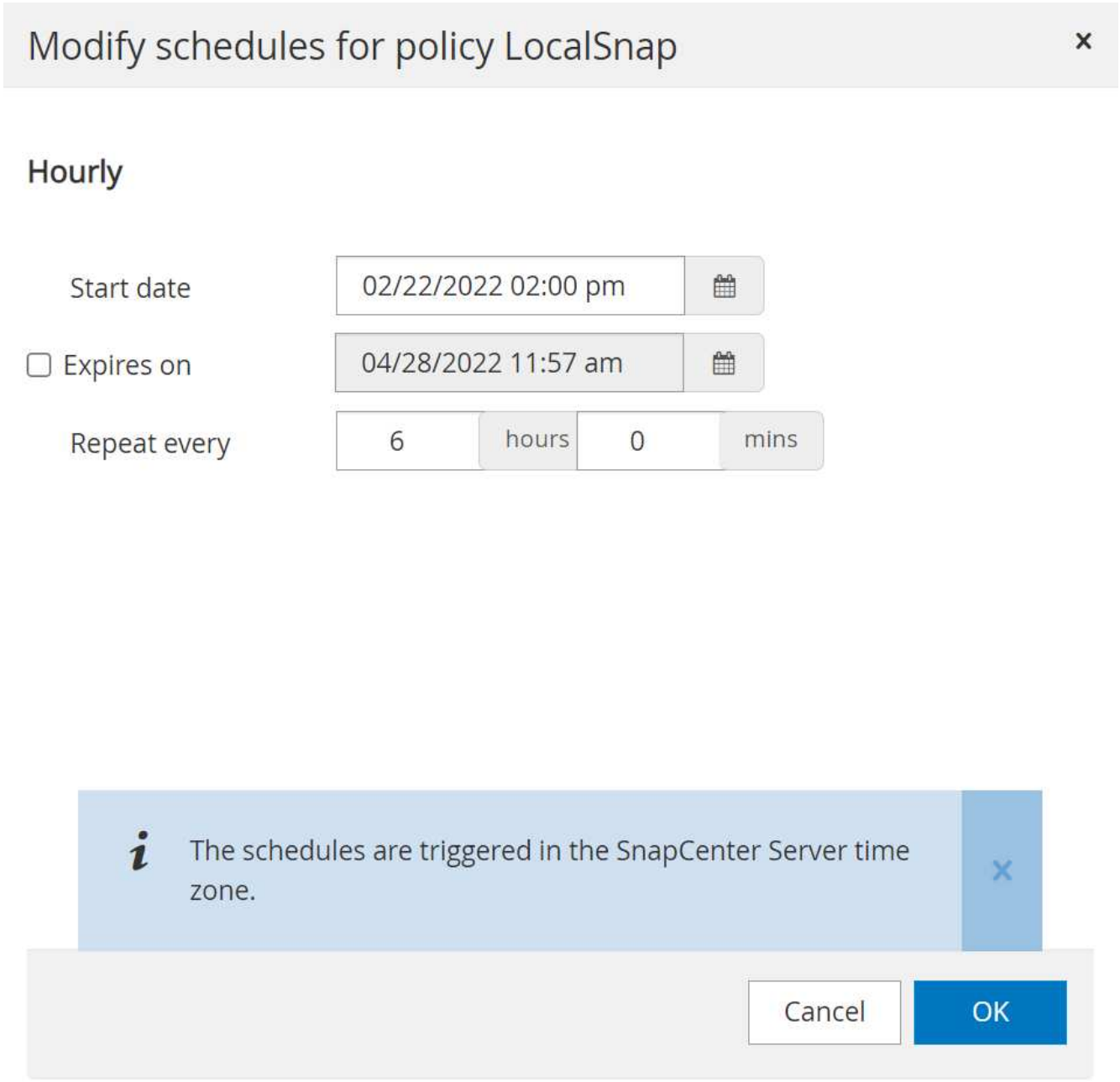
7. Legen Sie den Zeitplan für die Richtlinie zur Integritätsprüfung der Blöcke fest.

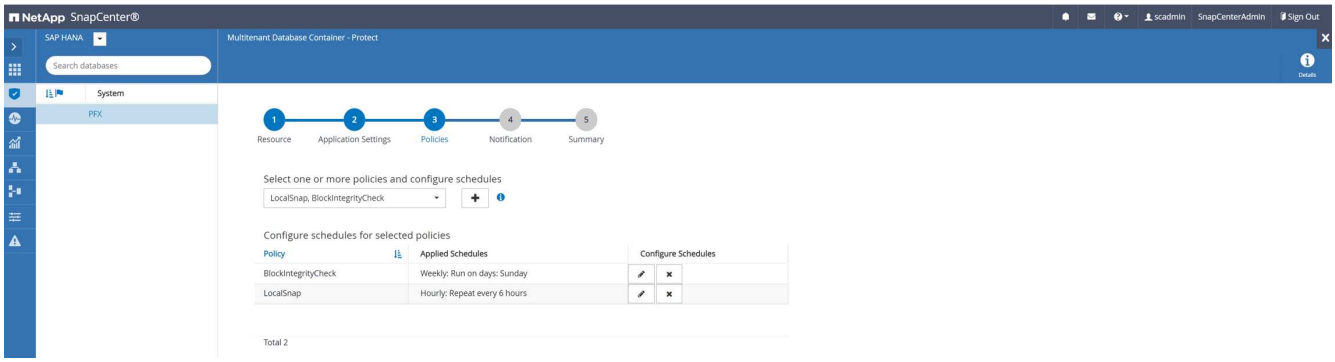
   In diesem Beispiel wird sie für einmal pro Woche festgelegt.



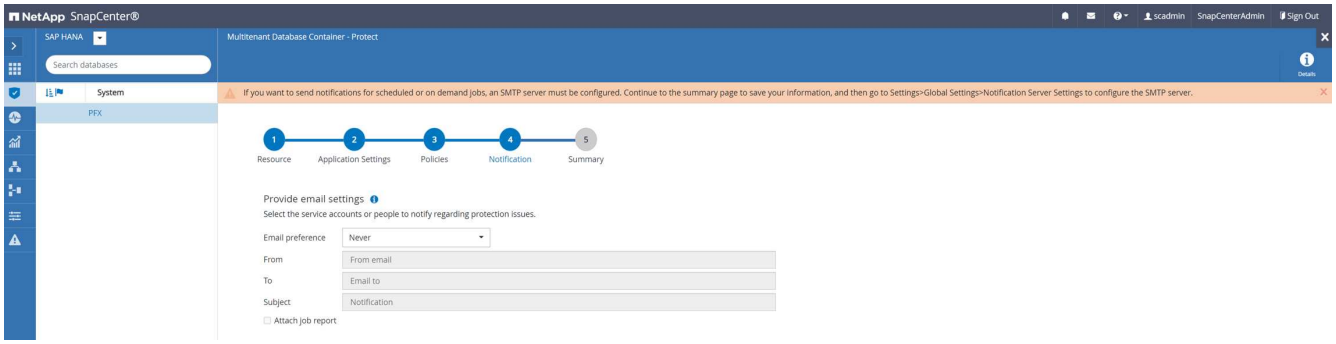
8. Legen Sie den Zeitplan für die lokale Snapshot-Richtlinie fest.

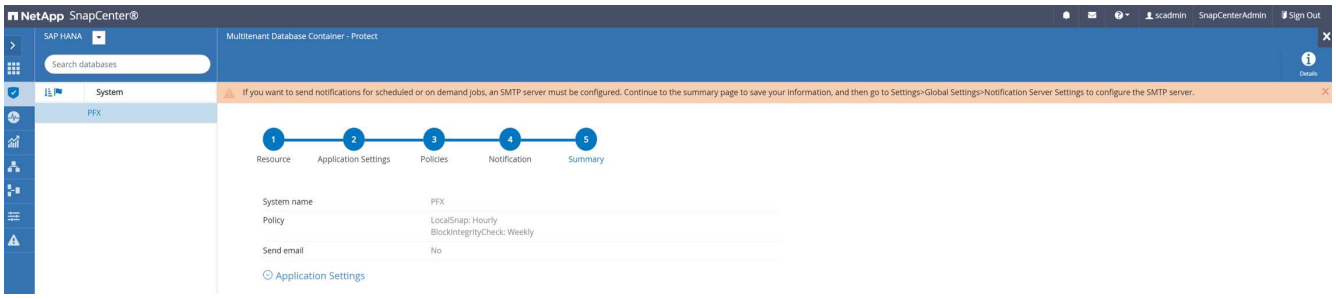
   In diesem Beispiel wird die Einstellung alle 6 Stunden durchgeführt.



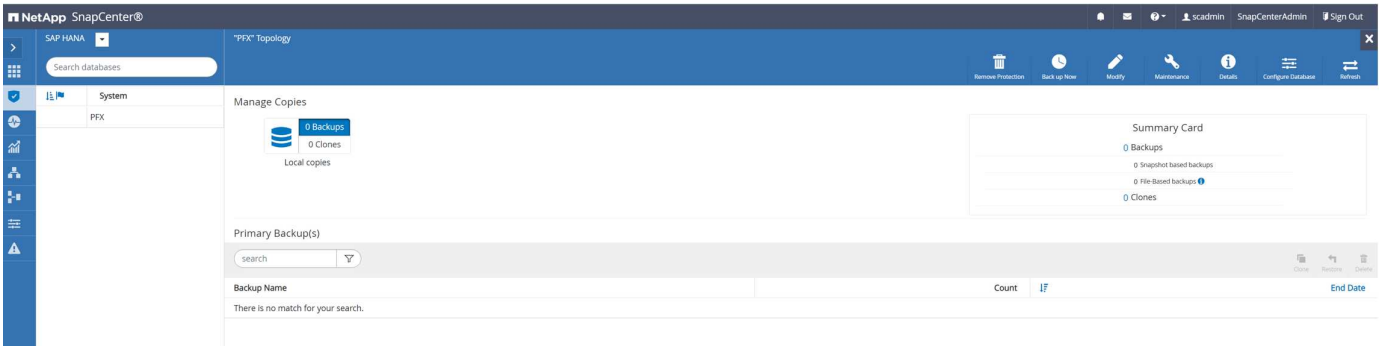


9. Geben Sie Informationen zur E-Mail-Benachrichtigung an.





Die Konfiguration der HANA-Ressourcen ist jetzt abgeschlossen, und Sie können Backups ausführen.



SnapCenter-Backup-Vorgänge

Sie können ein On-Demand-Snapshot-Backup und eine On-Demand-Blockintegritätsprüfung erstellen.

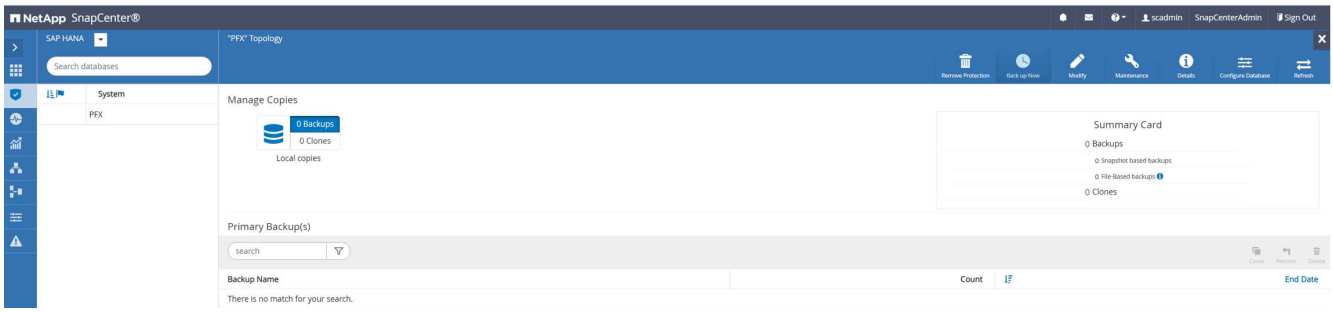
Erstellen Sie ein Snapshot Backup nach Bedarf

Führen Sie die folgenden Schritte aus, um On-Demand Snapshot Backups zu erstellen.

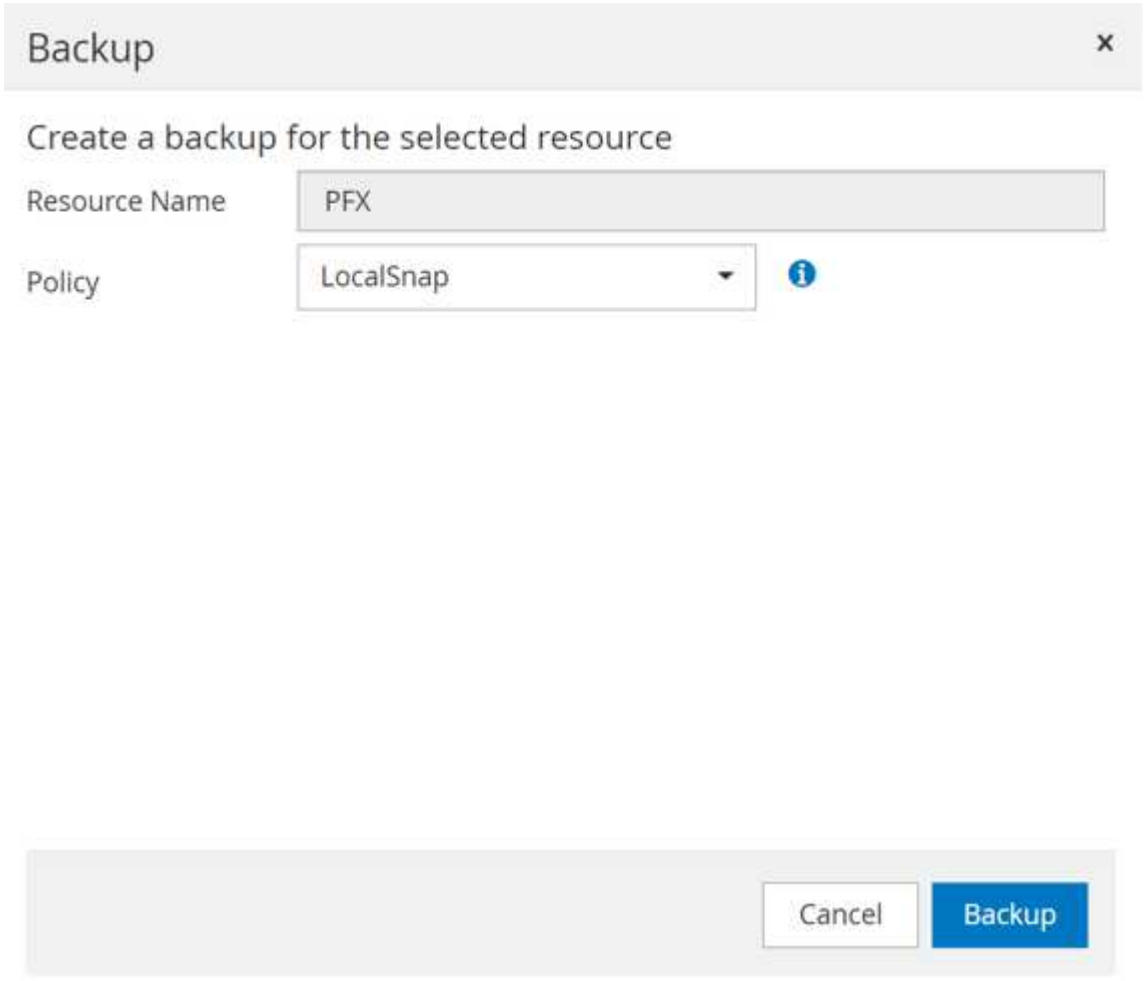
1. Wählen Sie in der Ansicht Ressource die Ressource aus und doppelklicken Sie auf die Zeile, um zur Ansicht Topologie zu wechseln.

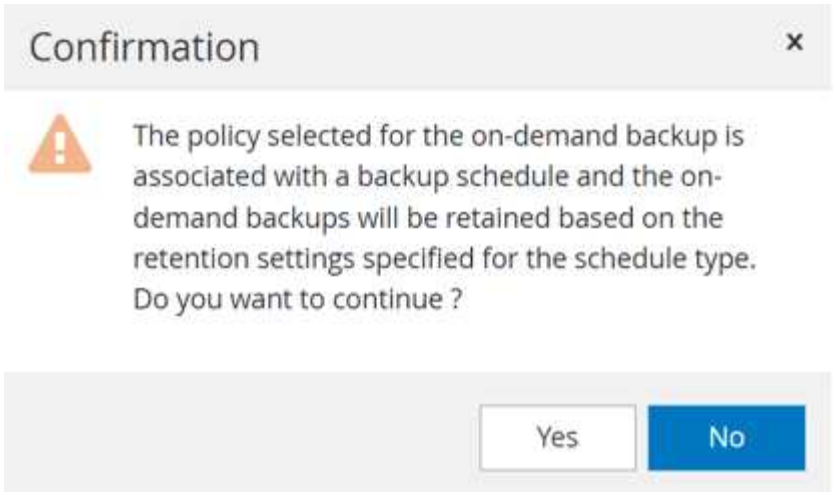
   Die Ansicht RessourcTopologie gibt einen Überblick über alle verfügbaren Backups, die mithilfe von SnapCenter erstellt wurden. Im oberen Bereich dieser Ansicht wird die Backup-Topologie angezeigt, die die Backups des primären Storage (lokale Kopien) und, falls verfügbar, auf dem externen Backup-Storage (Vault-Kopien) anzeigt.

2. Klicken Sie in der oberen Zeile auf das Symbol Jetzt sichern, um ein On-Demand-Backup zu starten.



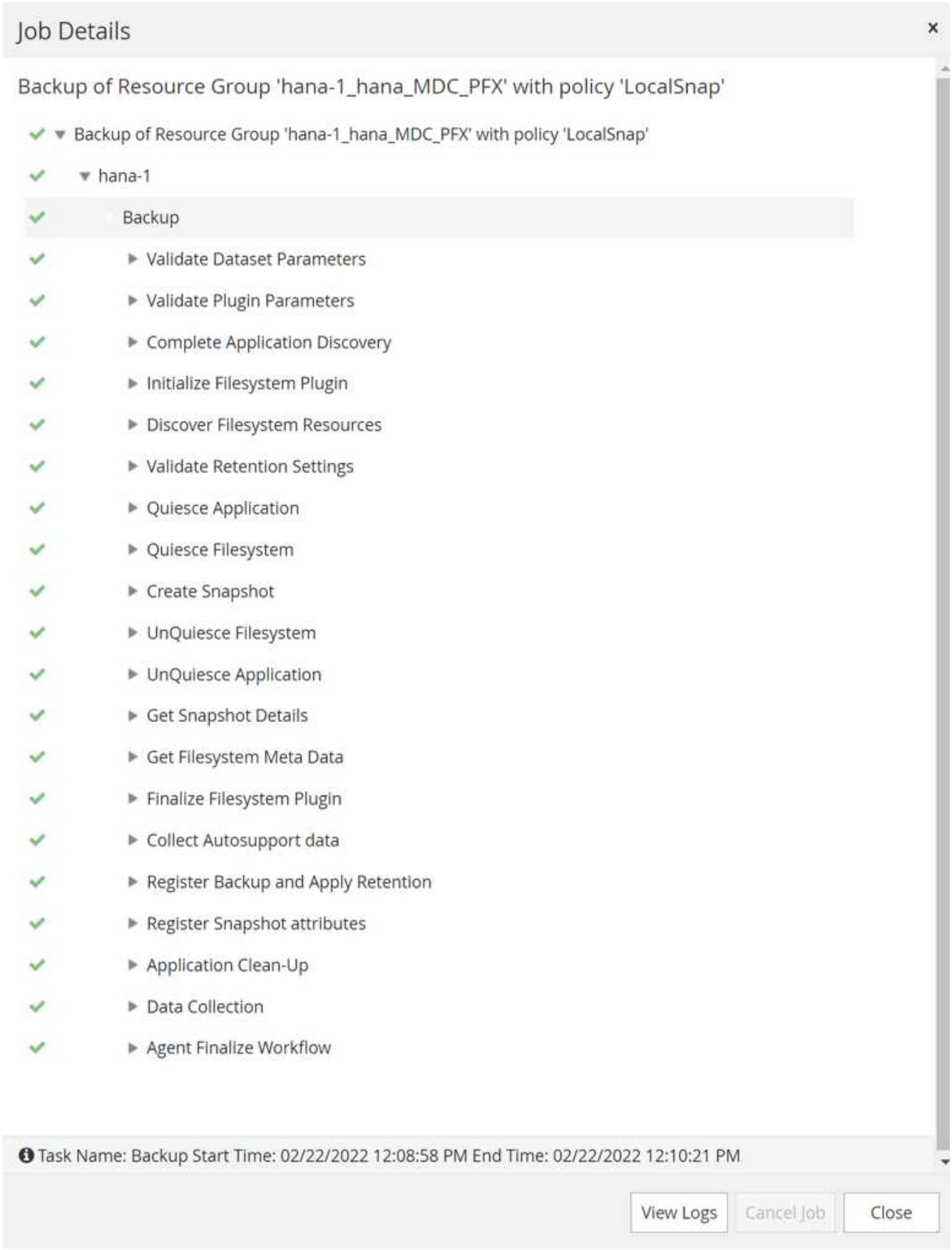
3. Wählen Sie aus der Dropdown-Liste die Backup-Richtlinie aus `LocalSnap`, Und klicken Sie dann auf Backup, um das On-Demand-Backup zu starten.





Ein Protokoll der vorherigen fünf Jobs wird im Aktivitätsbereich unten in der Topologieansicht angezeigt.

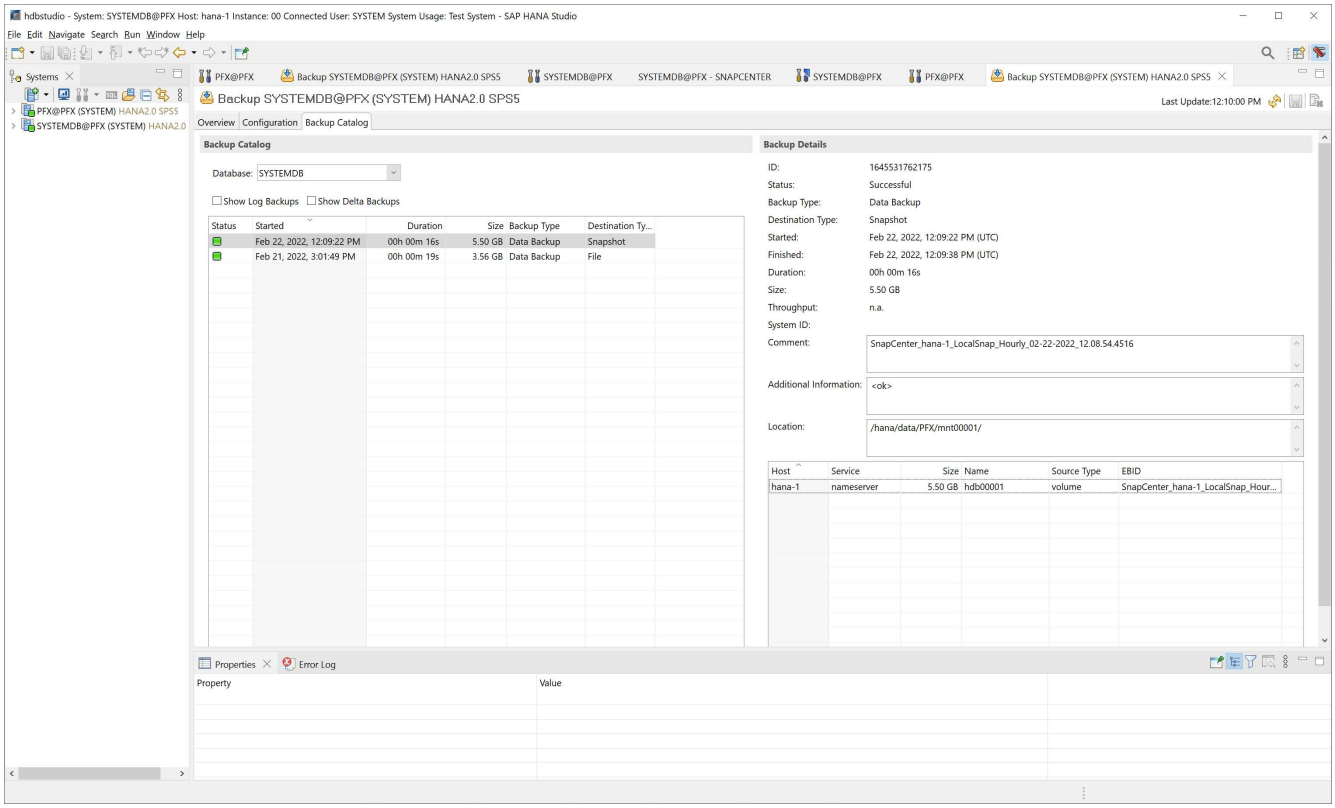
4. Die Jobdetails werden angezeigt, wenn Sie im Aktivitätsbereich auf die Vorgangszeile des Jobs klicken. Sie können ein detailliertes Jobprotokoll öffnen, indem Sie auf Protokolle anzeigen klicken

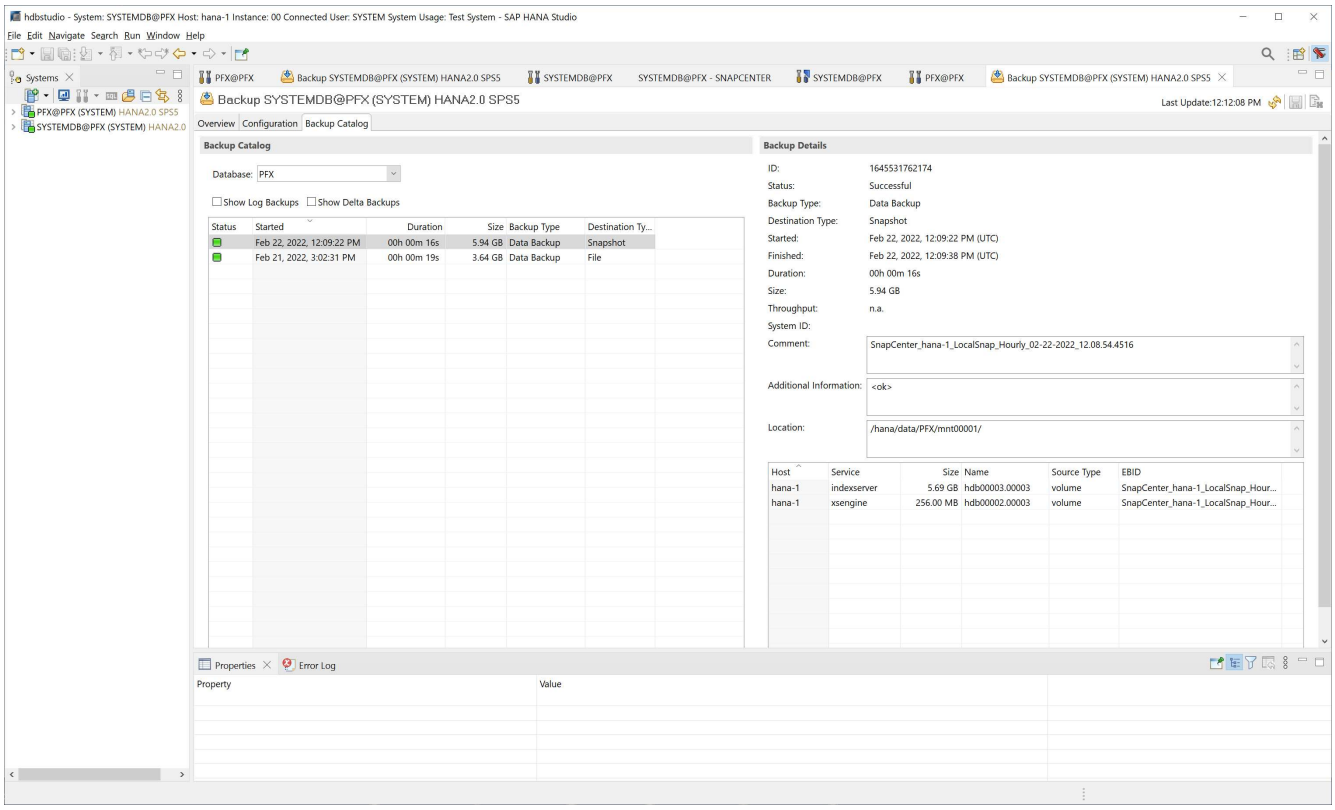


Nach Abschluss des Backups wird in der Topologieansicht ein neuer Eintrag angezeigt. Die Backup-Namen folgen derselben Namenskonvention wie der in Abschnitt definierte Snapshot Name "„Konfigurieren und Schützen einer HANA-Ressource“."

Sie müssen die Topologieansicht schließen und erneut öffnen, um die aktualisierte Backup-Liste anzuzeigen.

Im SAP HANA Backup-Katalog wird der SnapCenter-Backup-Name als A gespeichert `Comment` Außerdem Feld `External Backup ID (EBID)`. Dies ist in der folgenden Abbildung für die Systemdatenbank und in der nächsten Abbildung für die PFX der Mandanten-Datenbank dargestellt.



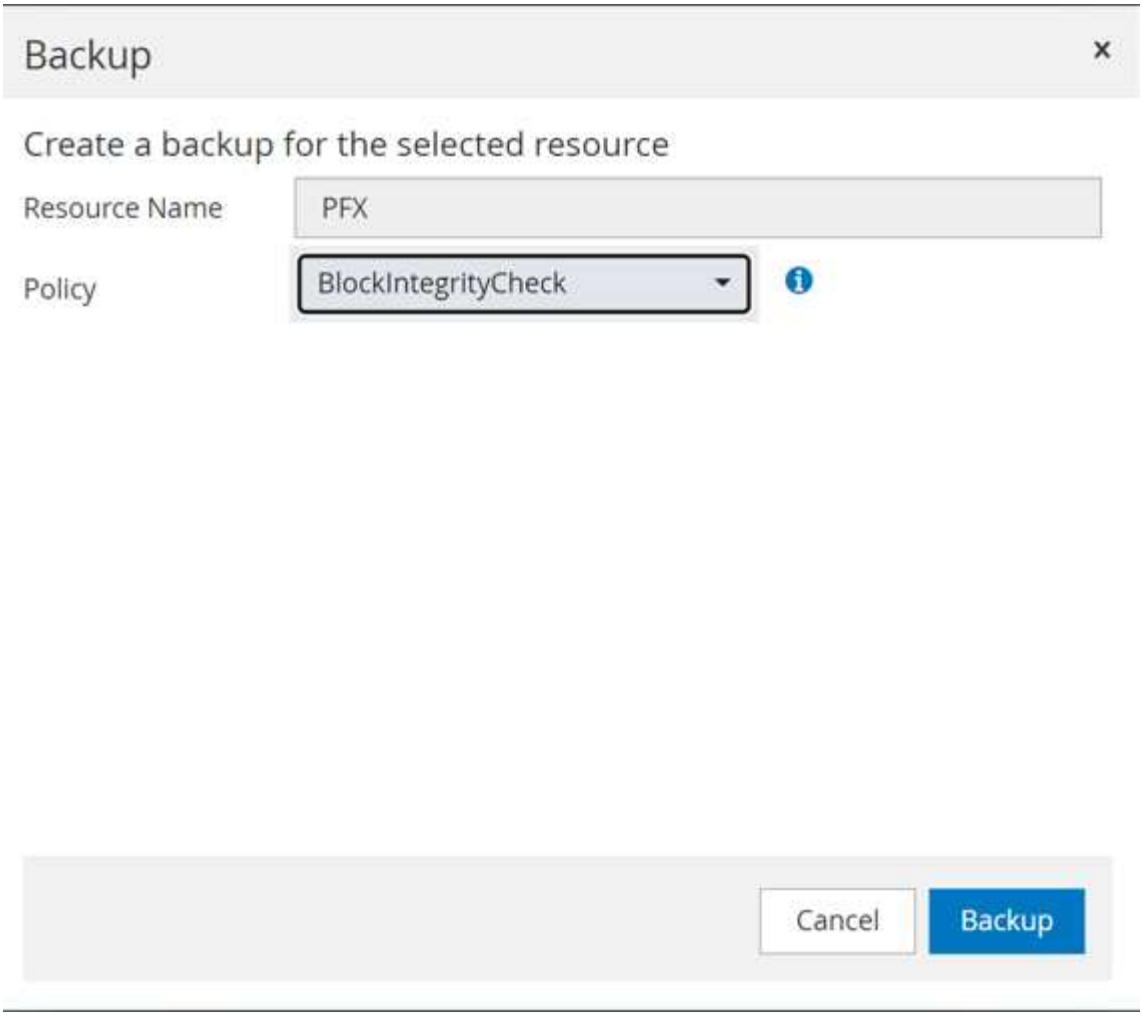


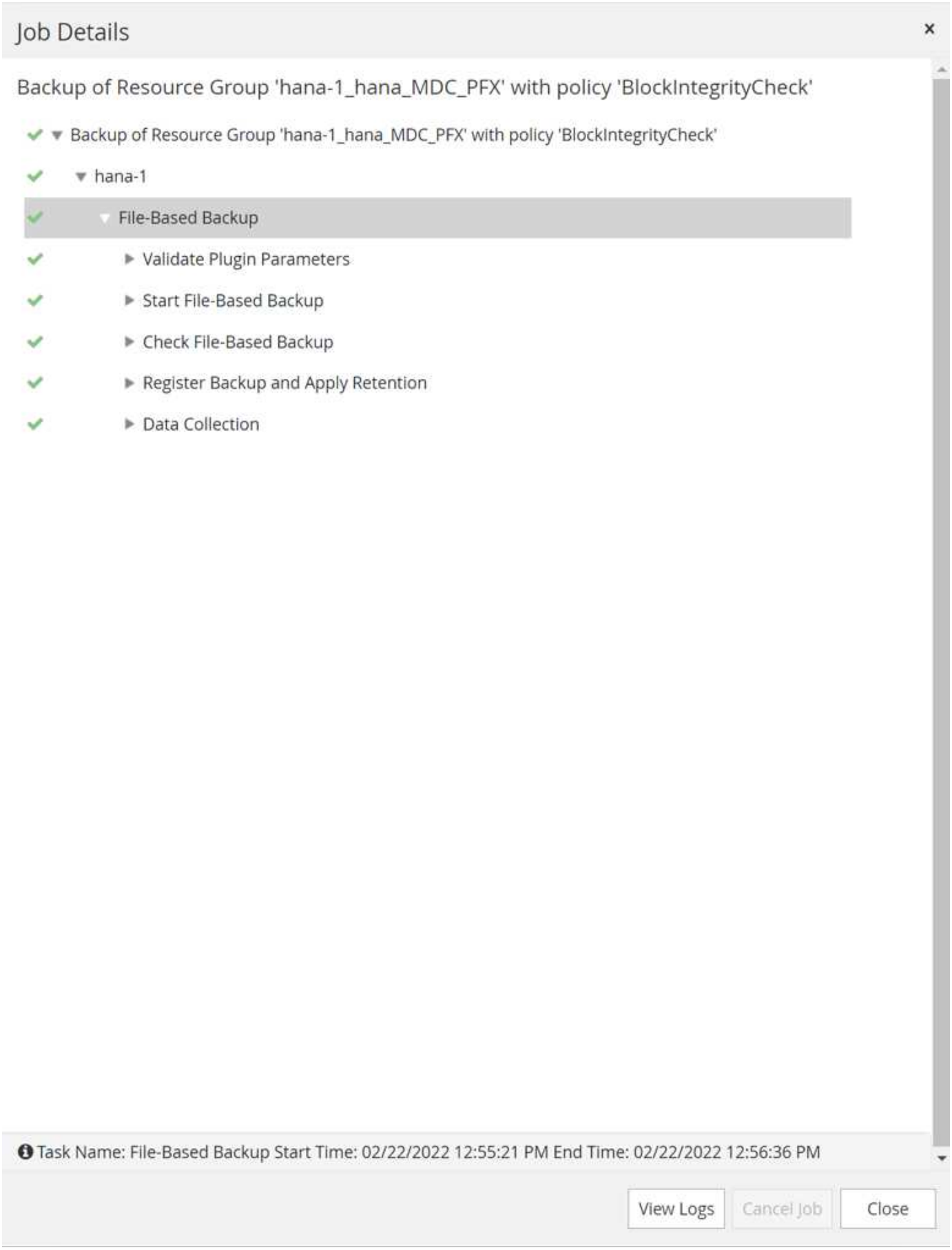
Auf dem FSX für ONTAP Filesystem können Sie die Snapshot-Backups durch eine Verbindung mit der Konsole der SVM auflisten.

```
sapcc-hana-svm::> snapshot show -volume PFX_data_mnt00001
---Blocks---
Vserver  Volume   Snapshot                                  Size Total%
Used%
-------- -------- ------------------------------------ -------- ------
-----
sapcc-hana-svm
         PFX_data_mnt00001
                  SnapCenter_hana-1_LocalSnap_Hourly_02-22-
2022_12.08.54.4516
                                                        126.6MB     0%
2%
sapcc-hana-svm::>
```

Erstellung einer bedarfsgerechten Blockintegritätsprüfung

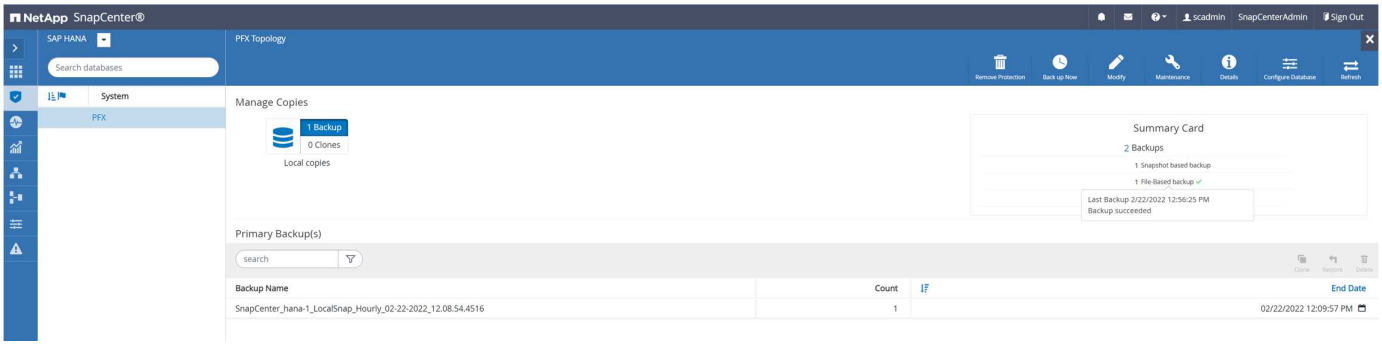
Ein on-Demand Block Integrity Check Vorgang wird auf dieselbe Weise wie ein Snapshot Backup Job ausgeführt, indem die Richtlinie BlockIntegrtyCheck ausgewählt wird. Bei der Planung von Backups mithilfe dieser Richtlinie erstellt SnapCenter eine standardmäßige SAP HANA Datei-Backup für das System und die Mandantendatenbanken.


Backup
Create a backup for the selected resource
Resource Name
PFX
Policy
BlockIntegrityCheck
Cancel
Backup

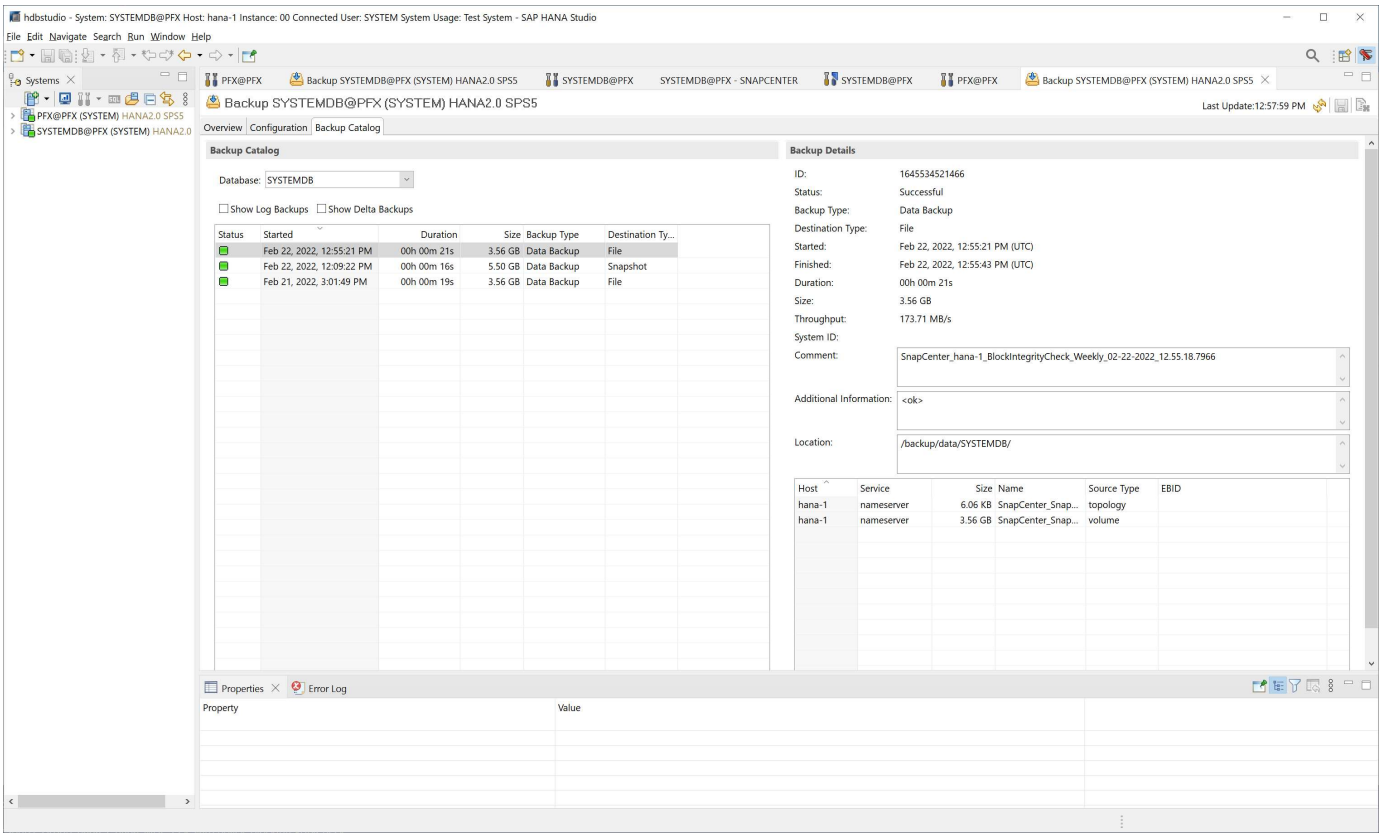


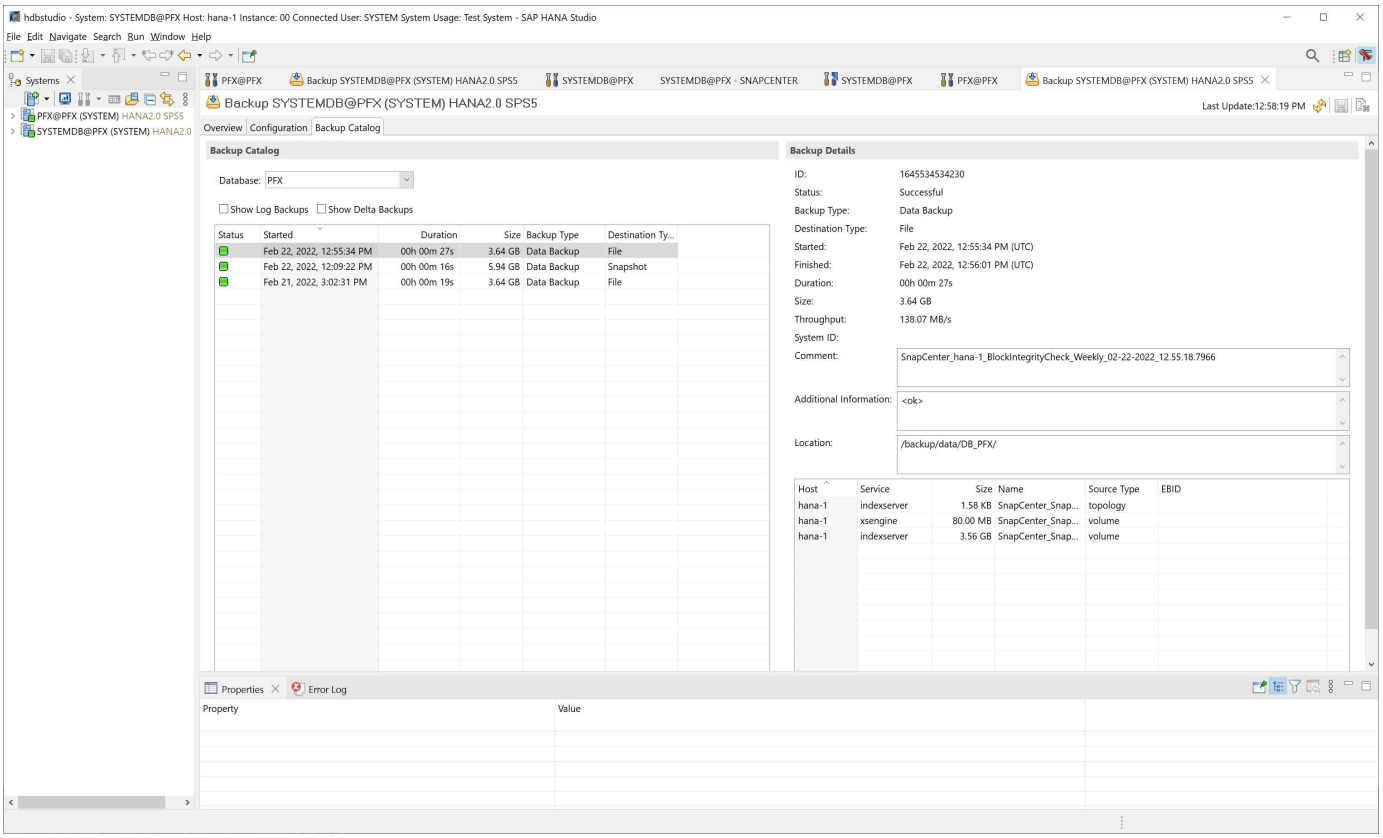
SnapCenter zeigt die Blockintegritätsprüfung nicht auf dieselbe Weise an wie Backups basierend auf

Snapshot-Kopien. Stattdessen zeigt die Übersichtskarte die Anzahl der dateibasierten Backups und den Status des vorherigen Backups an.



Der SAP HANA-Backup-Katalog zeigt Einträge sowohl für das System als auch für die Mandanten-Datenbanken an. Die folgenden Abbildungen zeigen die Integritätsprüfung der SnapCenter Blöcke im Backup-Katalog des Systems und der Mandanten-Datenbank.





Eine erfolgreiche Überprüfung der Blockintegrität erstellt standardisierte SAP HANA Daten-Backup-Dateien. SnapCenter verwendet den Backup-Pfad, der mit der HANA-Datenbank für dateibasierte Daten-Backup-Vorgänge konfiguriert wurde.

```
hana-1:~ # ls -al /backup/data/*
/backup/data/DB_PFX:
total 7665384
drwxr-xr-- 2 pfxadm sapsys       4096 Feb 22 12:56 .
drwxr-xr-x 4 pfxadm sapsys       4096 Feb 21 15:02 ..
-rw-r----- 1 pfxadm sapsys     155648 Feb 21 15:02
COMPLETE_DATA_BACKUP_databackup_0_1
-rw-r----- 1 pfxadm sapsys   83894272 Feb 21 15:02
COMPLETE_DATA_BACKUP_databackup_2_1
-rw-r----- 1 pfxadm sapsys 3825213440 Feb 21 15:02
COMPLETE_DATA_BACKUP_databackup_3_1
-rw-r----- 1 pfxadm sapsys     155648 Feb 22 12:55
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_0_1
-rw-r----- 1 pfxadm sapsys   83894272 Feb 22 12:55
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_2_1
-rw-r----- 1 pfxadm sapsys 3825213440 Feb 22 12:56
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_3_1
/backup/data/SYSTEMDB:
total 7500880
drwxr-xr-- 2 pfxadm sapsys       4096 Feb 22 12:55 .
drwxr-xr-x 4 pfxadm sapsys       4096 Feb 21 15:02 ..
-rw-r----- 1 pfxadm sapsys     159744 Feb 21 15:01
COMPLETE_DATA_BACKUP_databackup_0_1
-rw-r----- 1 pfxadm sapsys 3825213440 Feb 21 15:02
COMPLETE_DATA_BACKUP_databackup_1_1
-rw-r----- 1 pfxadm sapsys     159744 Feb 22 12:55
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_0_1
-rw-r----- 1 pfxadm sapsys 3825213440 Feb 22 12:55
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_1_1
hana-1:~ #
```

Backup nicht datenmengen

Das Backup von nicht-Daten-Volumes ist ein integrierter Teil des SnapCenter und des SAP HANA Plug-ins.

Der Schutz des Datenbank-Daten-Volumes reicht aus, um die SAP HANA Datenbank auf einen bestimmten Zeitpunkt wiederherzustellen, vorausgesetzt, die Ressourcen für die Datenbankinstallation und die erforderlichen Protokolle sind weiterhin verfügbar.

Um das Recovery von Situationen durchzuführen, in denen andere nicht-Datendateien wiederhergestellt

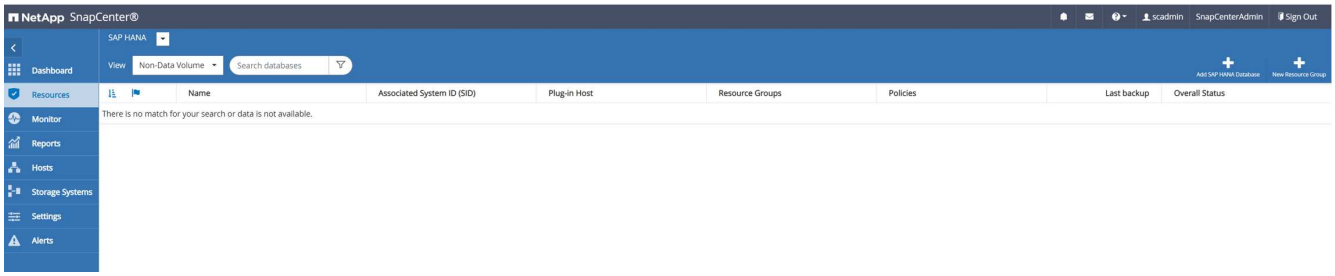
werden müssen, empfiehlt NetApp, eine zusätzliche Backup-Strategie für nicht-Daten-Volumes zu entwickeln, um das SAP HANA Datenbank-Backup zu erweitern. Je nach Ihren spezifischen Anforderungen kann sich das Backup von nicht-Daten-Volumes in den Einstellungen für die Planungsfrequenz und -Aufbewahrung unterscheiden, und Sie sollten bedenken, wie oft nicht-Datendateien geändert werden. Zum Beispiel das HANA Volume `/hana/shared` Enthält ausführbare Dateien, aber auch SAP HANA Trace-Dateien. Zwar ändern sich ausführbare Dateien nur beim Upgrade der SAP HANA Datenbank, doch benötigen die SAP HANA Trace-Dateien möglicherweise eine höhere Backup-Häufigkeit, um Problemsituationen mit SAP HANA zu analysieren.

Dank des nicht-Daten-Volume-Backups von SnapCenter können Snapshot-Kopien aller relevanten Volumes in wenigen Sekunden mit derselben Speichereffizienz erstellt werden wie bei SAP HANA-Datenbank-Backups. Der Unterschied liegt darin, dass keine SQL Kommunikation mit der SAP HANA Datenbank erforderlich ist.

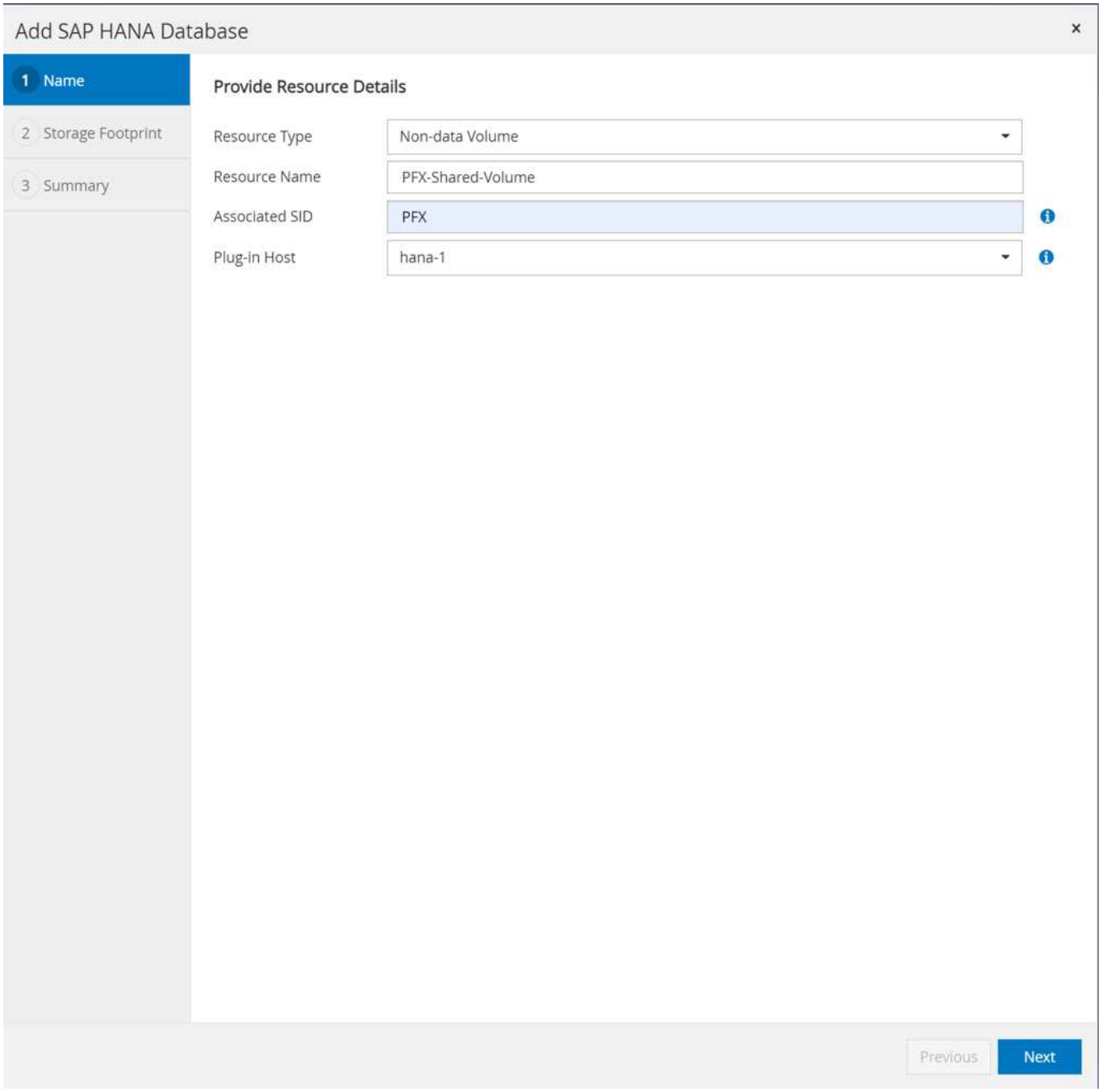
Konfiguration von Ressourcen, die nicht von Datenvolumen stammen

Führen Sie die folgenden Schritte aus, um nicht-Daten-Volume-Ressourcen zu konfigurieren:

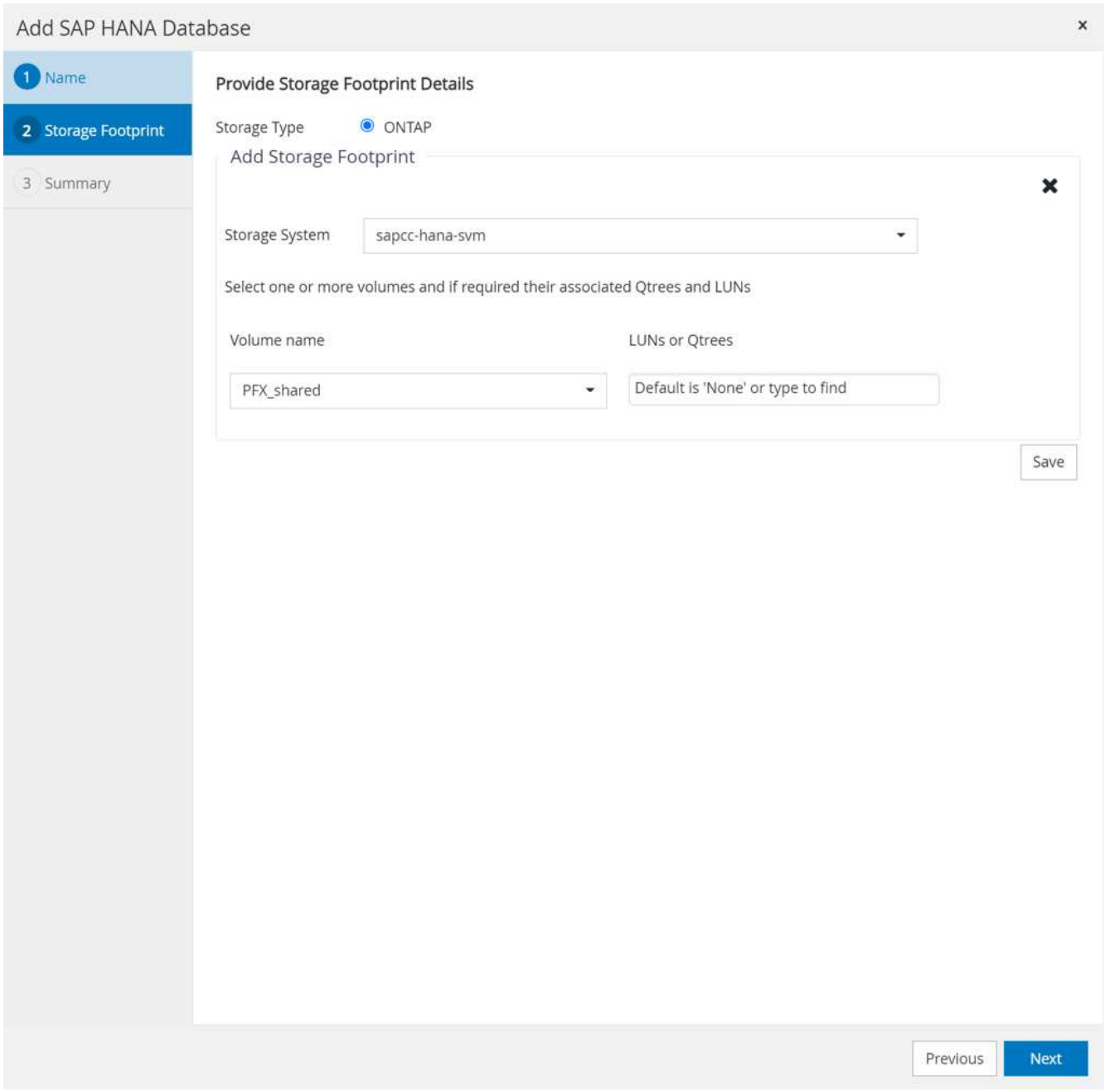
1. Wählen Sie auf der Registerkarte Ressourcen die Option Non-Data-Volume, und klicken Sie auf Add SAP HANA Database.



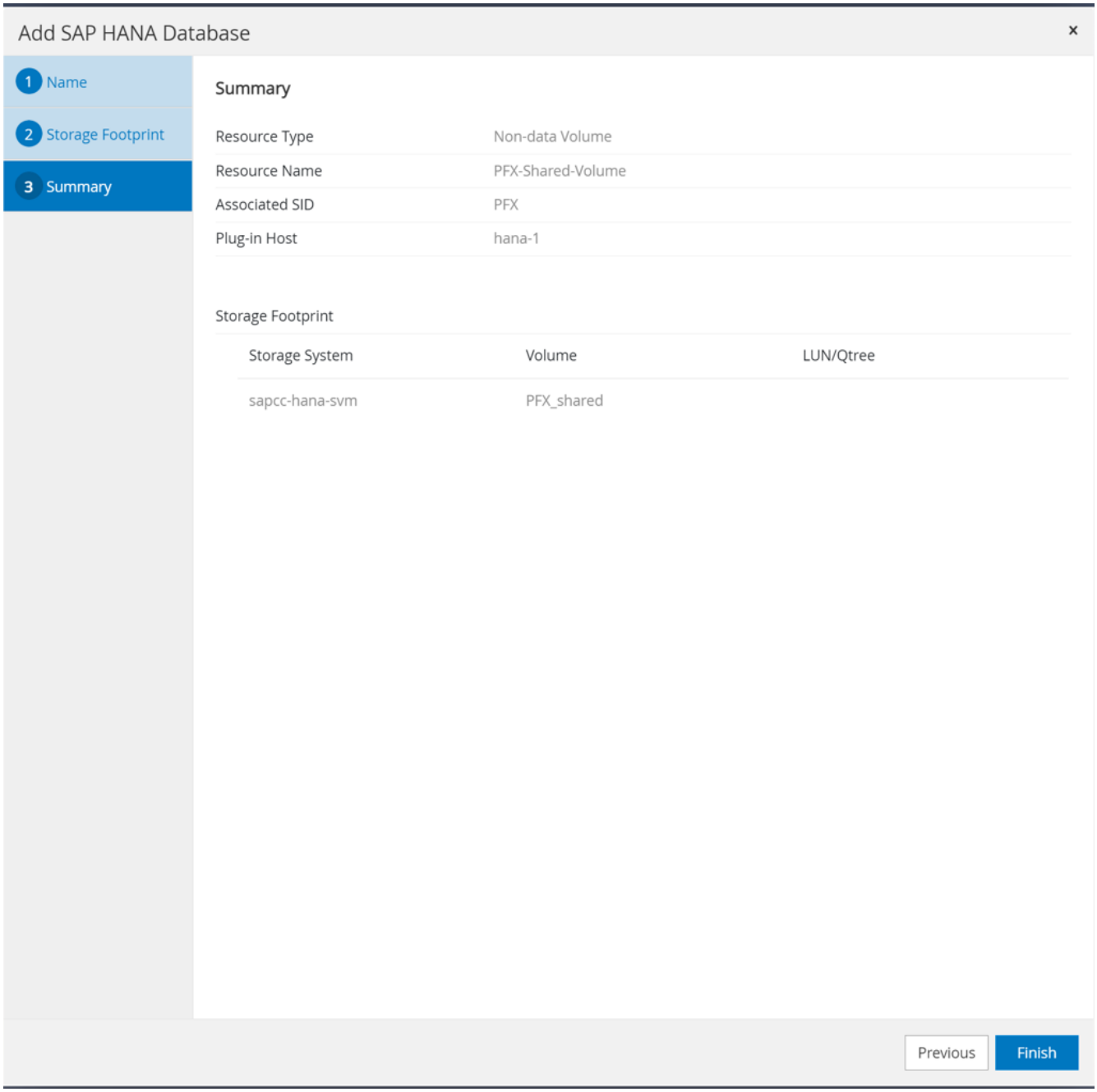
2. Wählen Sie in Schritt 1 des Dialogfelds SAP HANA-Datenbank hinzufügen in der Liste Ressourcentyp die Option nicht-Datenvolumen aus. Geben Sie einen Namen für die Ressource und den zugehörigen SID und den SAP HANA Plug-in-Host an, den Sie für die Ressource verwenden möchten, und klicken Sie dann auf Weiter.



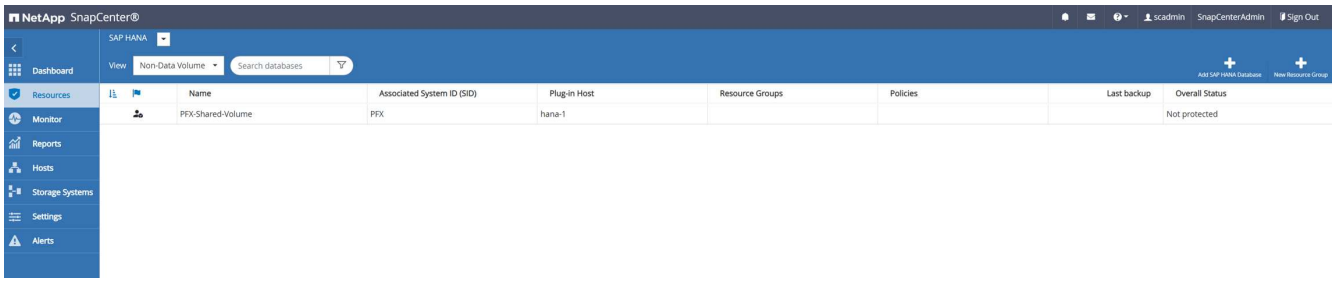
3. Fügen Sie die SVM und das Storage-Volume als Storage-Platzbedarf hinzu und klicken Sie dann auf Weiter.



4. Um die Einstellungen zu speichern, klicken Sie im Zusammenfassungsschritt auf Fertig stellen.



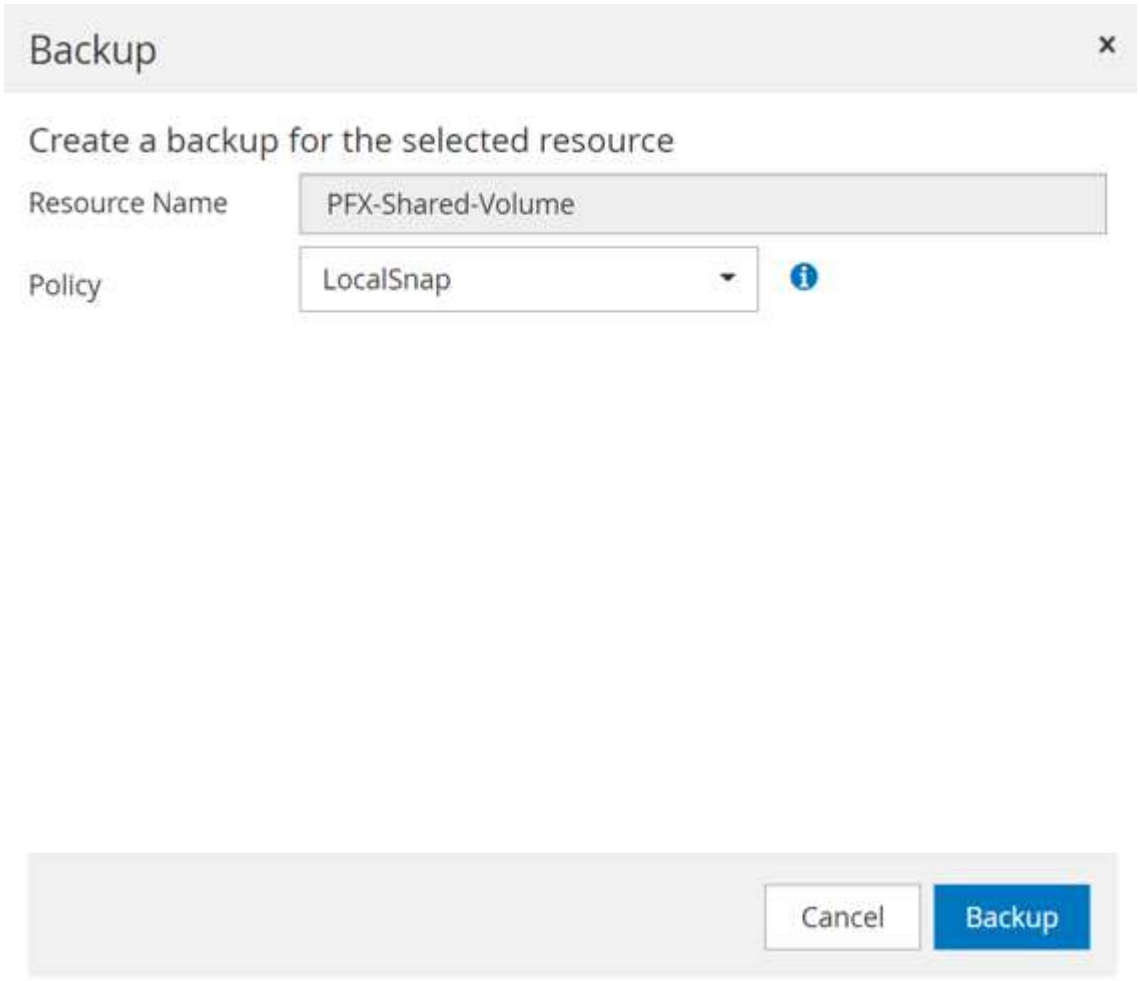
Das neue nicht-Daten-Volume wird nun SnapCenter hinzugefügt. Doppelklicken Sie auf die neue Ressource, um den Ressourcenschutz auszuführen.



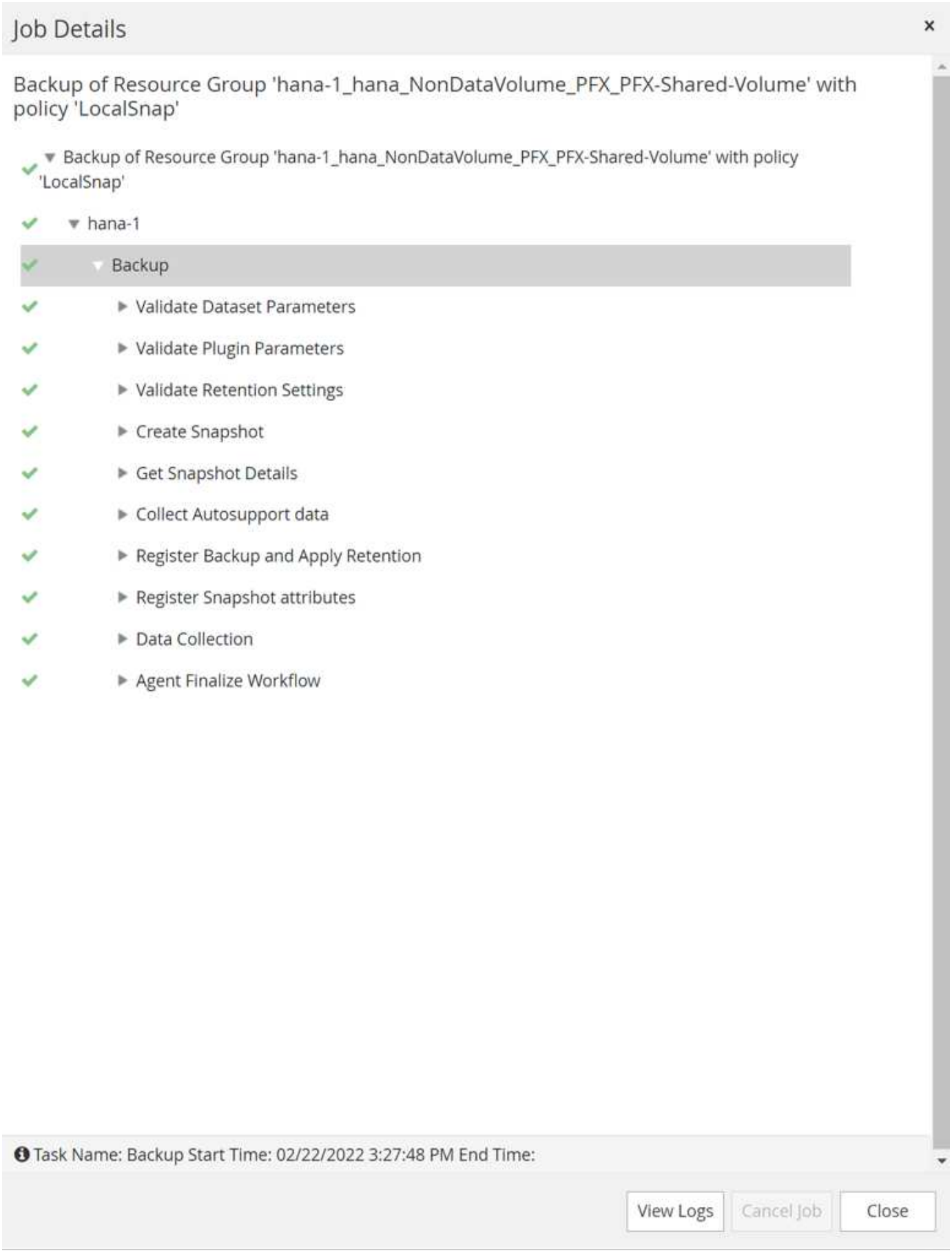
Der Ressourcenschutz erfolgt auf dieselbe Weise wie zuvor bei einer HANA-Datenbankressource.

5. Sie können jetzt ein Backup ausführen, indem Sie auf Jetzt sichern klicken.

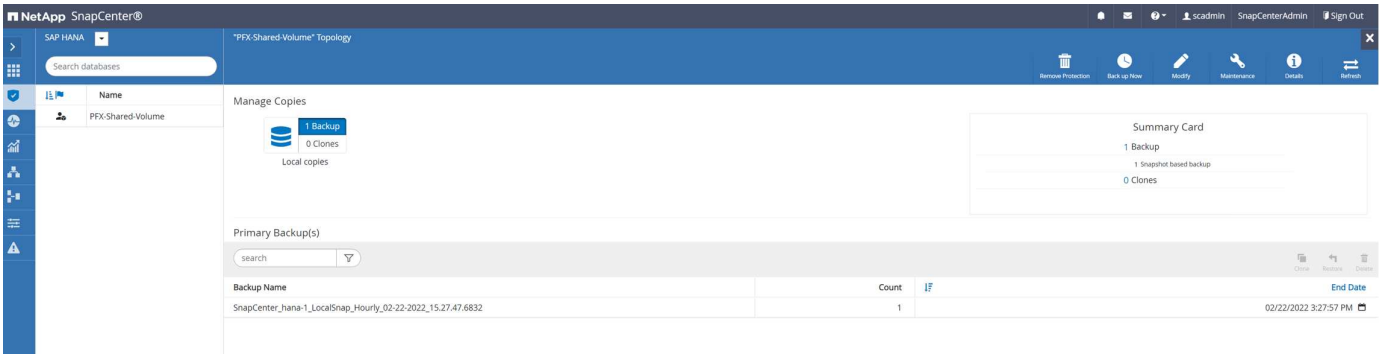
6. Wählen Sie die Richtlinie aus, und starten Sie den Backup-Vorgang.



Das Jobprotokoll von SnapCenter zeigt die einzelnen Workflow-Schritte.



Das neue Backup ist nun in der Ressourcenansicht der Ressource ohne Datenvolumen sichtbar.



Restore und Recovery

Mit SnapCenter werden für HANA-einzelne-Host-MDC-Systeme über einen einzelnen Mandanten automatisierte Restore- und Recovery-Vorgänge unterstützt. Bei Systemen mit mehreren Hosts oder MDC-Systemen mit mehreren Mandanten führt SnapCenter nur den Wiederherstellungsvorgang aus, und Sie müssen die Wiederherstellung manuell durchführen.

Sie können eine automatisierte Wiederherstellung und Operation mit den folgenden Schritten ausführen:

1. Wählen Sie das Backup aus, das für den Wiederherstellungsvorgang verwendet werden soll.
2. Wählen Sie den Wiederherstellungstyp aus. Wählen Sie mit Volume Revert oder ohne Volume Revert die Option Complete Restore.
3. Wählen Sie den Wiederherstellungstyp aus den folgenden Optionen aus:
   - Auf den letzten Stand
   - Zeitpunktgenau
   - Zu einem bestimmten Daten-Backup
   - Keine Wiederherstellung

     Der ausgewählte Wiederherstellungstyp wird für die Wiederherstellung des Systems und der Mandanten-Datenbank verwendet.

Als Nächstes führt SnapCenter die folgenden Operationen durch:

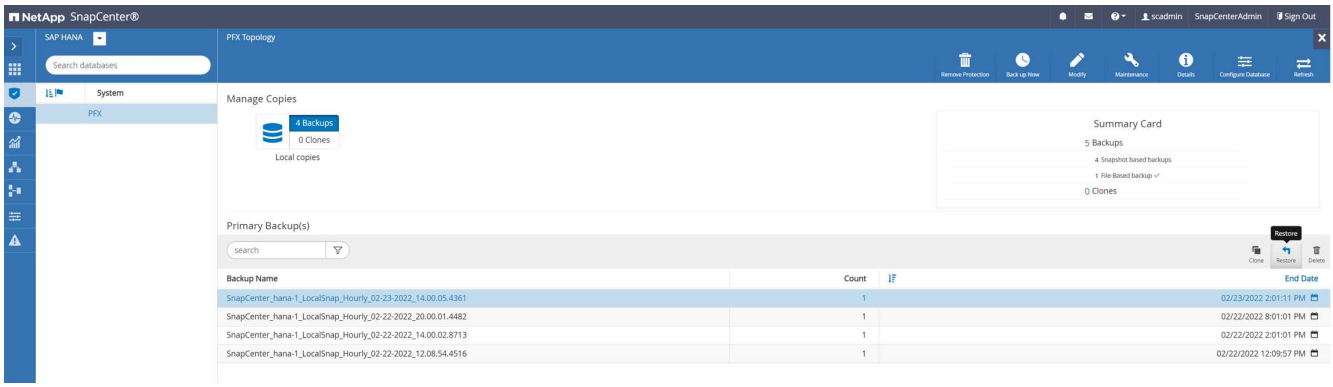
1. Die HANA-Datenbank wird gestoppt.
2. Die Datenbank wird wiederhergestellt. Je nach gewähltem Wiederherstellungstyp werden verschiedene Operationen ausgeführt.
   - Wenn das Zurücksetzen von Volumes ausgewählt wird, hängt SnapCenter das Volume ab, stellt das Volume mithilfe von Volume-basierten SnapRestore auf der Storage-Ebene wieder her und hängt das Volume an.
   - Wenn das Zurücksetzen von Volumes nicht ausgewählt wird, stellt SnapCenter alle Dateien mithilfe einzelner Datei-SnapRestore-Vorgänge auf der Storage-Ebene wieder her.
3. Es stellt die Datenbank wieder her:
   a. Durch Wiederherstellen der Systemdatenbank
   b. Wiederherstellung der Mandantendatenbank
   c. Starten der HANA-Datenbank

   Wenn keine Wiederherstellung ausgewählt ist, wird die SnapCenter beendet, und Sie müssen den

Wiederherstellungsvorgang für das System und die Mandantendatenbank manuell durchführen.

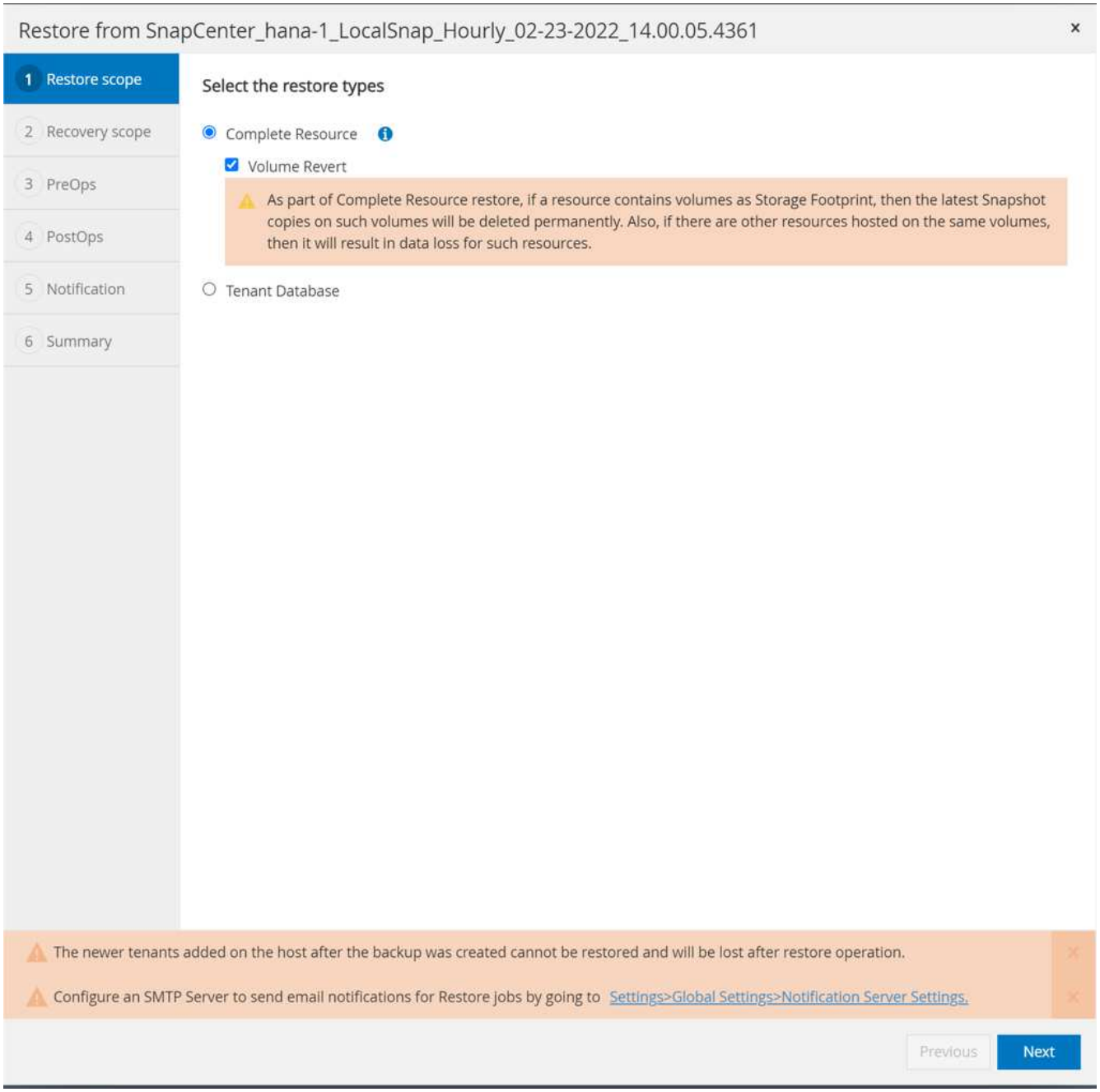
Führen Sie die folgenden Schritte aus, um einen manuellen Wiederherstellungsvorgang durchzuführen:

1. Wählen Sie ein Backup in SnapCenter aus, das für den Wiederherstellungsvorgang verwendet werden soll.



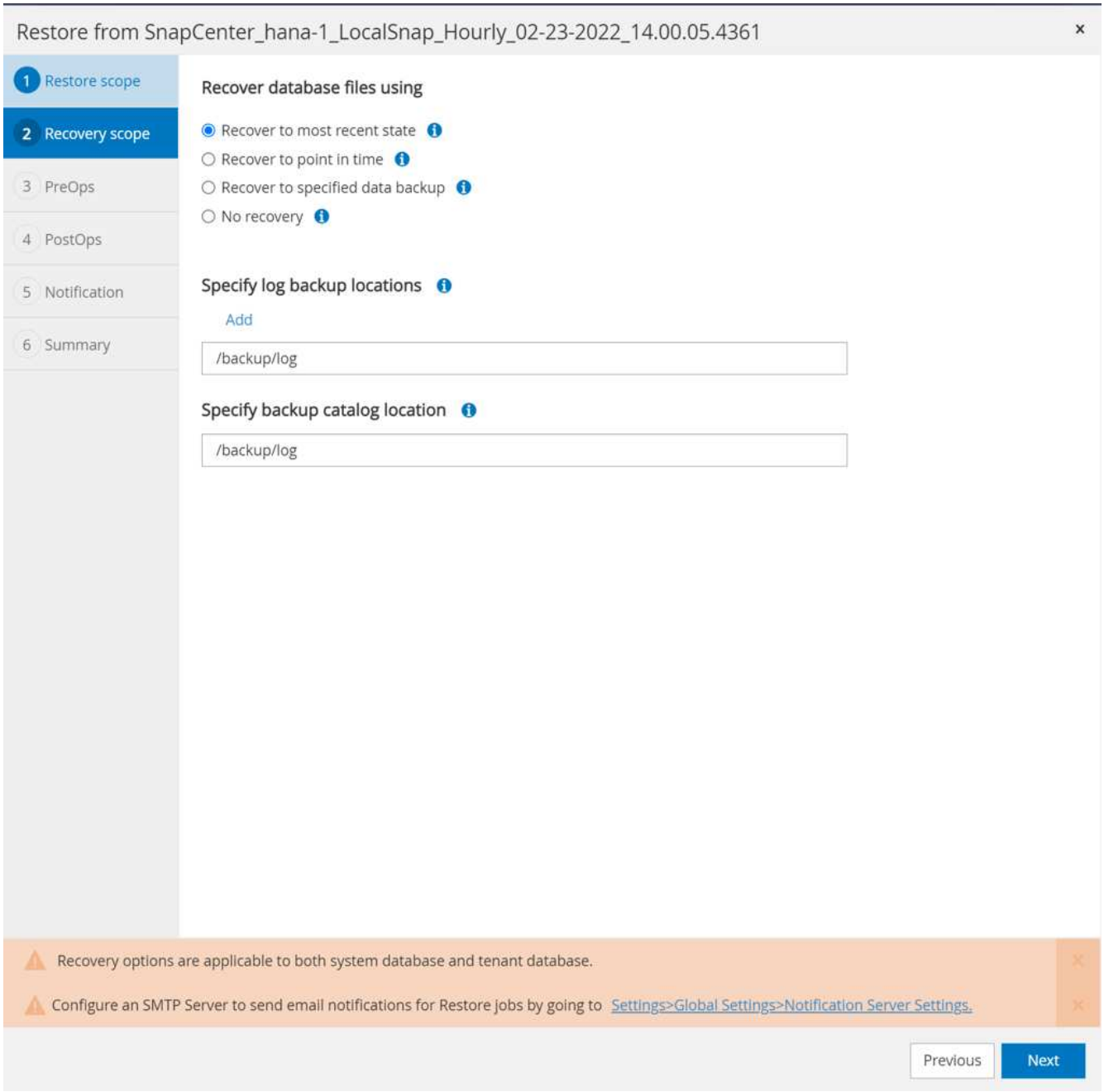
2. Wählen Sie den Umfang und den Typ der Wiederherstellung aus.

   Das Standardszenario für HANA MDC-Einzelmandant-Systeme besteht darin, komplette Ressourcen mit Zurücksetzen des Volumes zu nutzen. Bei einem HANA MDC-System mit mehreren Mandanten möchten Sie möglicherweise nur einen einzelnen Mandanten wiederherstellen. Weitere Informationen zur Wiederherstellung einzelner Mandanten finden Sie unter "Restore und Recovery (netapp.com)".

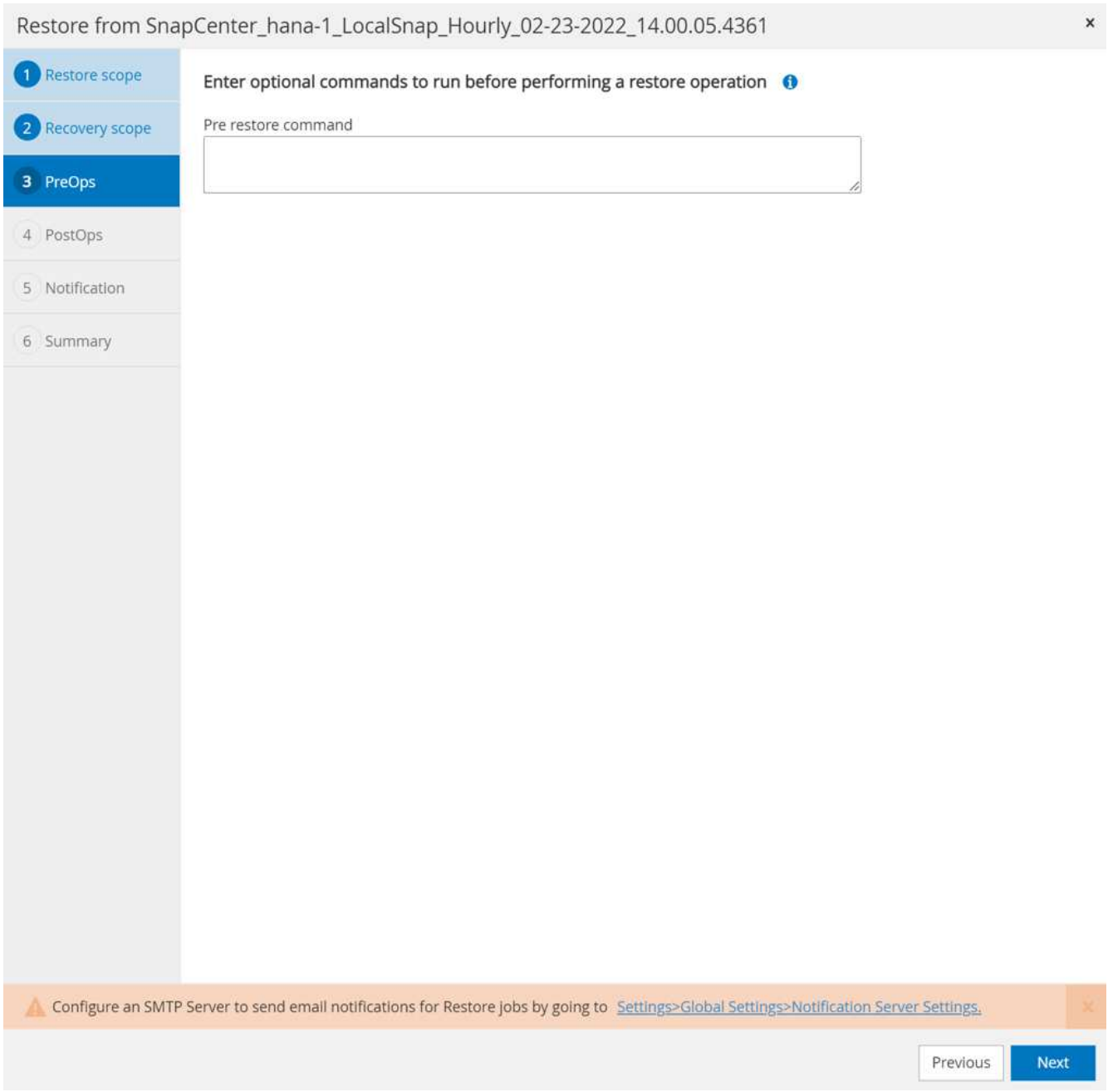


3. Wählen Sie „Recovery Scope“ aus, und stellen Sie den Speicherort für das Backup und das Katalog-Backup bereit.

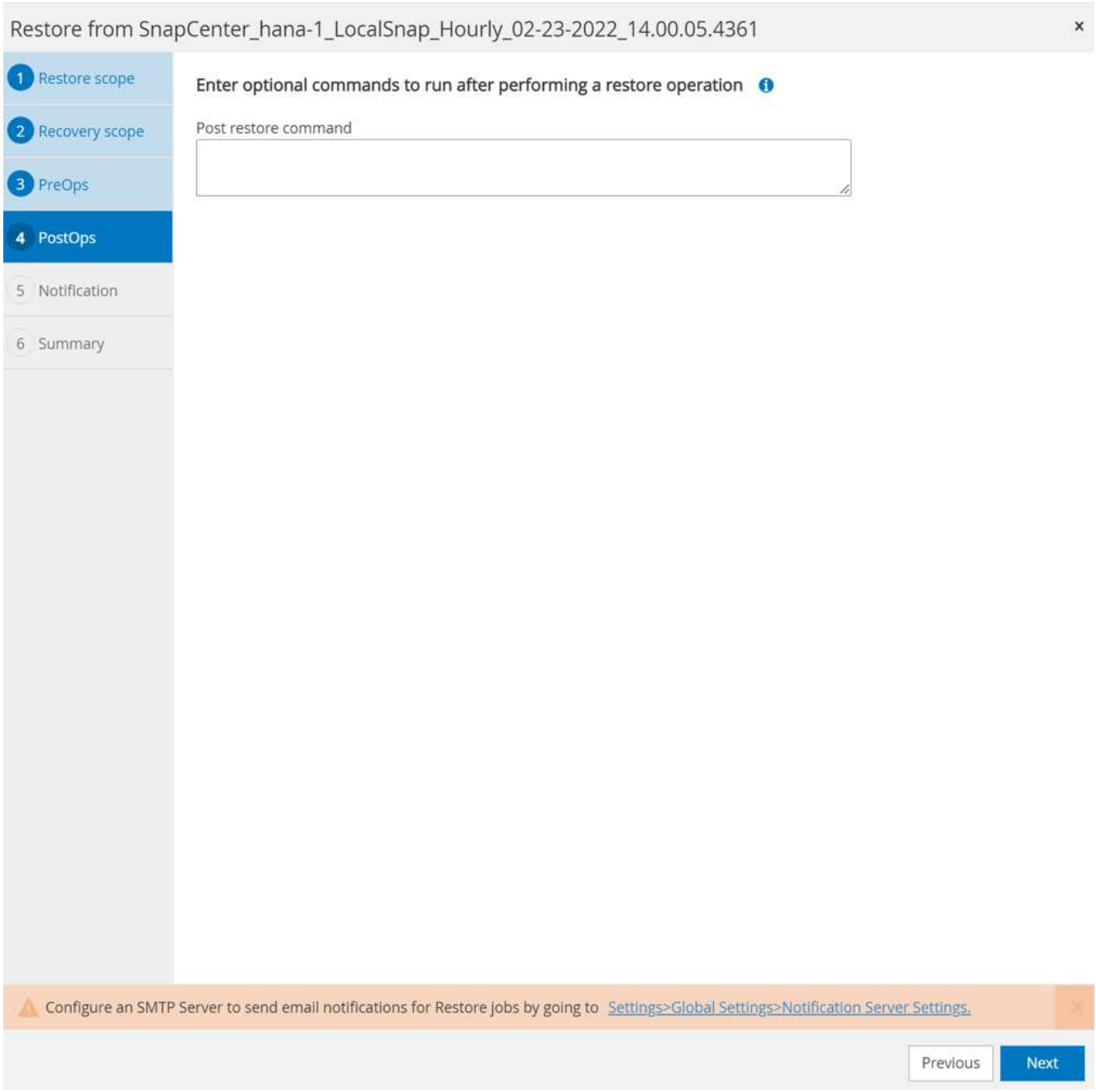
   SnapCenter verwendet den Standardpfad oder die geänderten Pfade in der HANA global.ini-Datei, um die Backup-Standorte für das Protokoll und den Katalog vorab aufzufüllen.



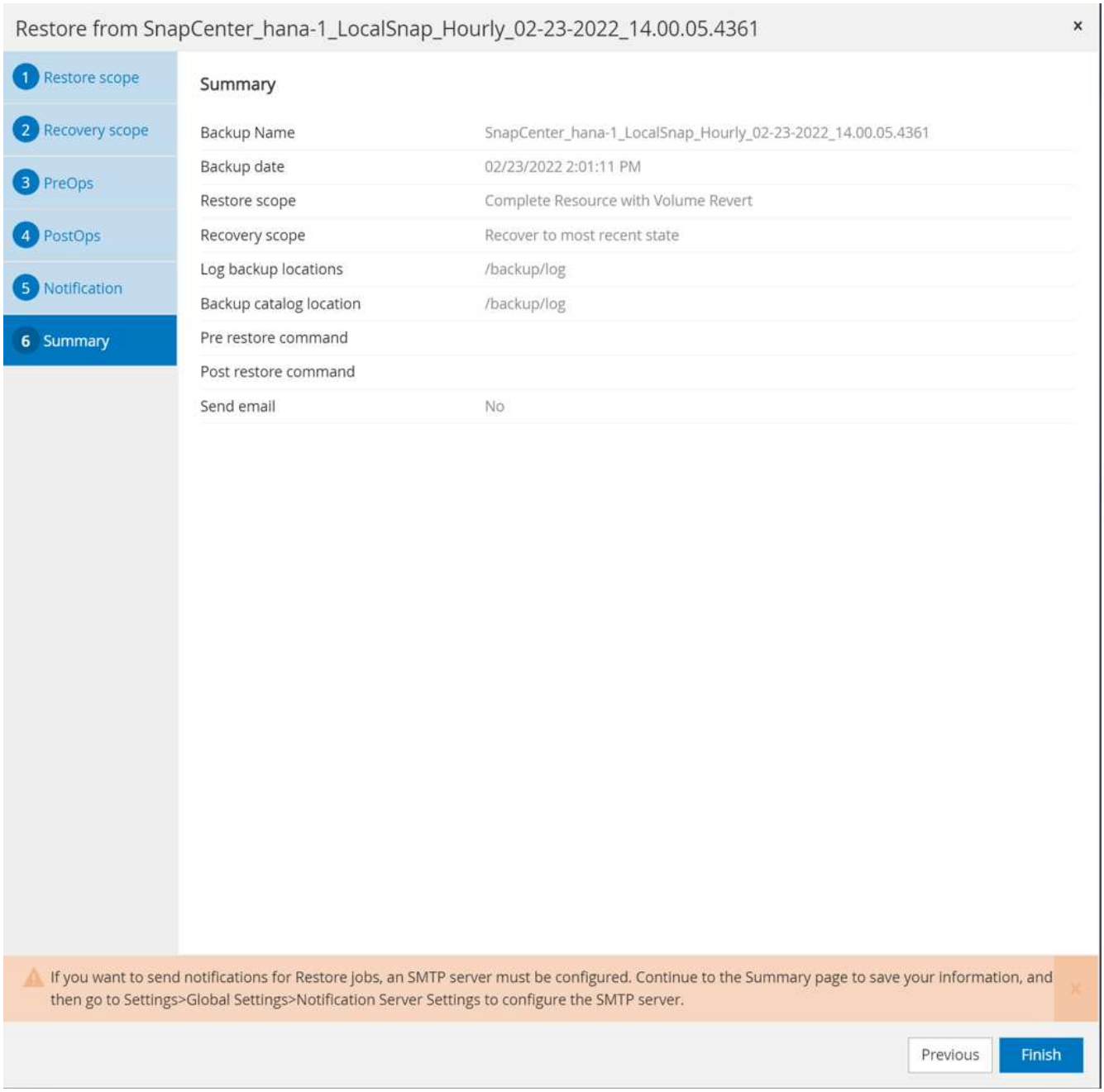
4. Geben Sie die optionalen Befehle vor der Wiederherstellung ein.



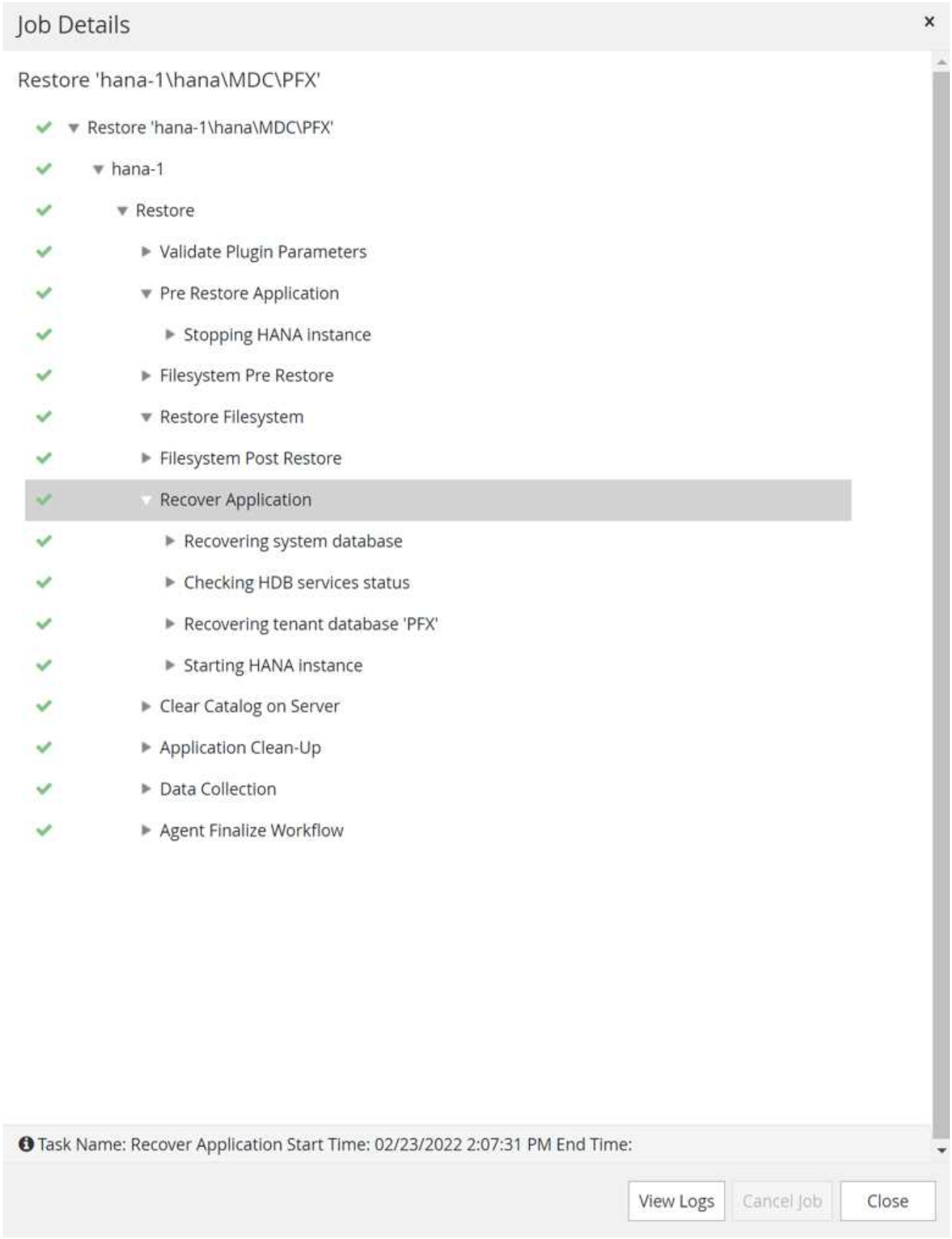
5. Geben Sie die optionalen Befehle nach der Wiederherstellung ein.



6. Um den Wiederherstellungs- und Wiederherstellungsvorgang zu starten, klicken Sie auf Fertig stellen.



SnapCenter führt den Wiederherstellungsvorgang und die Wiederherstellung aus. Dieses Beispiel zeigt die Jobdetails des Wiederherstellungsjobs.

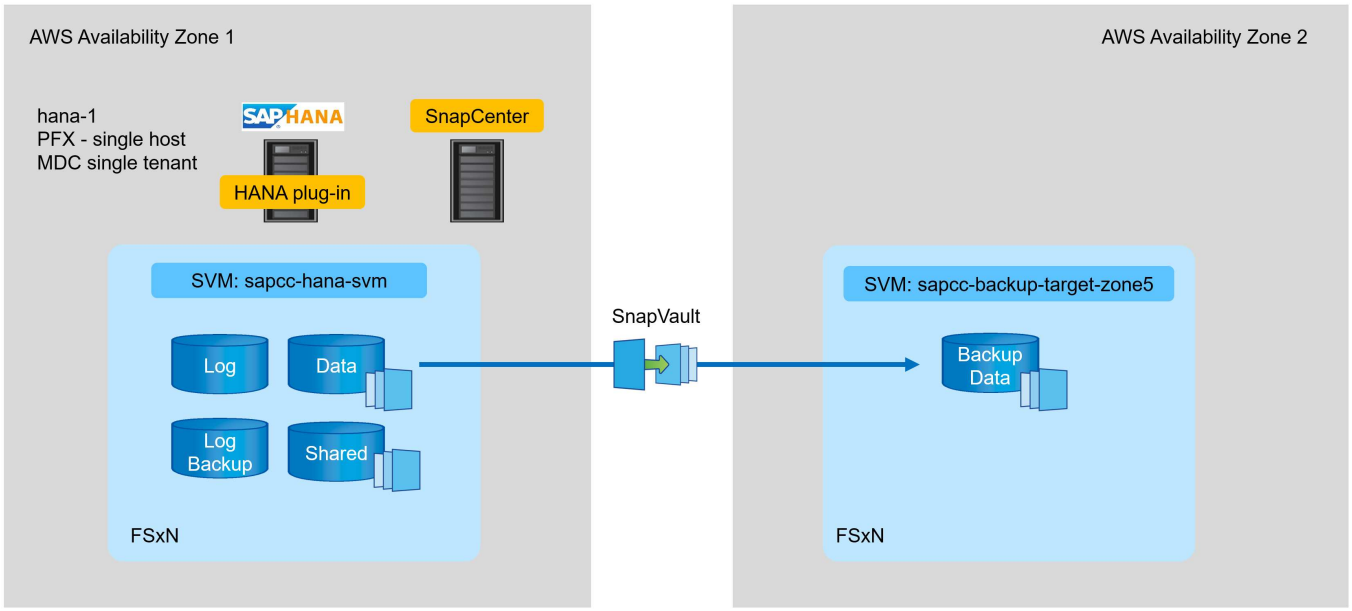

Job Details
Restore 'hana-1\hana\MDC\PFX'
Restore 'hana-1\hana\MDC\PFX'
hana-1
Restore
Validate Plugin Parameters
Pre Restore Application
Stopping HANA instance
Filesystem Pre Restore
Restore Filesystem
Filesystem Post Restore
Recover Application
Recovering system database
Checking HDB services status
Recovering tenant database 'PFX'
Starting HANA instance
Clear Catalog on Server
Application Clean-Up
Data Collection
Agent Finalize Workflow
Task Name: Recover Application Start Time: 02/23/2022 2:07:31 PM End Time:
View Logs
Cancel Job
Close

Backup-Replizierung mit SnapVault

Übersicht - Backup-Replikation mit SnapVault

Im Lab-Setup verwenden wir ein zweites FSX für ONTAP-Filesystem in einer zweiten AWS-Verfügbarkeitszone, um die Backup-Replizierung für das HANA-Datenvolumen zu präsentieren.

Wie in Kapitel erläutert"„Datensicherungsstrategie“", muss das Replikationsziel ein zweites FSX für ONTAP-Dateisystem in einer anderen Verfügbarkeitszone sein, um vor einem Ausfall des primären FSX für ONTAP-Dateisystems geschützt zu werden. Außerdem sollte das gemeinsame HANA-Volume auf das sekundäre FSX für das ONTAP-Dateisystem repliziert werden.



Übersicht über die Konfigurationsschritte

Es gibt einige Konfigurationsschritte, die auf der FSX für ONTAP-Ebene ausgeführt werden müssen. Dies lässt sich entweder mit NetApp Cloud Manager oder über die Befehlszeile des FSX für ONTAP durchführen.

1. Peer-FSX für ONTAP-Filesysteme FSX für ONTAP-Dateisysteme müssen peed werden, um eine Replizierung zwischen beiden zu ermöglichen.
2. Peer-SVMs: SVMs müssen Peering durchgeführt werden, um eine Replizierung zwischen den beiden SVMs zu ermöglichen.
3. Erstellen eines Ziel-Volumes Erstellung eines Volumes in der Ziel-SVM mit Volume-Typ `DP`. Typ `DP` Muss als Ziel-Volume für die Replikation verwendet werden.
4. SnapMirror-Richtlinie erstellen Dies wird verwendet, um eine Policy für Replikation mit Typ zu erstellen `vault`.
    a. Fügen Sie eine Regel zur Richtlinie hinzu. Die Regel enthält das SnapMirror-Etikett und die Aufbewahrung für Backups am sekundären Standort. Sie müssen dasselbe SnapMirror-Label später in der SnapCenter-Richtlinie konfigurieren, damit SnapCenter Snapshot-Backups auf dem Quell-Volume mit diesem Etikett erstellt.
5. SnapMirror Beziehung erstellen Definiert die Replikationsbeziehung zwischen dem Quell- und dem Ziel-Volume und fügt eine Richtlinie hinzu.

6. SnapMirror initialisieren. Damit wird die erste Replikation gestartet, bei der die vollständigen Quelldaten auf das Ziel-Volume übertragen werden.

Wenn die Konfiguration der Volume-Replikation abgeschlossen ist, müssen Sie die Backup-Replikation in SnapCenter wie folgt konfigurieren:

1. Fügen Sie die Ziel-SVM zu SnapCenter hinzu.
2. Erstellen einer neuen SnapCenter-Richtlinie für Snapshot Backup und SnapVault-Replizierung
3. Fügen Sie die Richtlinie zu HANA-Ressourcenschutz hinzu.
4. Sie können jetzt Backups mit der neuen Richtlinie ausführen.

In den folgenden Kapiteln werden die einzelnen Schritte detaillierter beschrieben.

Konfigurieren Sie Replikationsbeziehungen auf FSX für ONTAP-Dateisysteme

Weitere Informationen zur SnapMirror Konfigurationsoptionen finden Sie in der ONTAP-Dokumentation unter "SnapMirror Replizierungs-Workflow (netapp.com)".

- Quell-FSX für ONTAP Dateisystem: `FsxId00fa9e3c784b6abbb`
- Quell-SVM: `sapcc-hana-svm`
- Ziel-FSX für ONTAP Dateisystem: `FsxId05f7f00af49dc7a3e`
- Ziel-SVM: `sapcc-backup-target-zone5`

Peer-FSX für ONTAP-Filesysteme

```
FsxId00fa9e3c784b6abbb::> network interface show -role intercluster
            Logical    Status     Network            Current       Current
Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ ------------- -------
----
FsxId00fa9e3c784b6abbb
            inter_1      up/up    10.1.1.57/24
FsxId00fa9e3c784b6abbb-01
                                                                   e0e
true
            inter_2      up/up    10.1.2.7/24
FsxId00fa9e3c784b6abbb-02
                                                                   e0e
true
2 entries were displayed.
```

```
FsxId05f7f00af49dc7a3e::> network interface show -role intercluster
            Logical    Status     Network            Current       Current
Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ ------------- -------
----
FsxId05f7f00af49dc7a3e
            inter_1      up/up    10.1.2.144/24
FsxId05f7f00af49dc7a3e-01
                                                                   e0e
true
            inter_2      up/up    10.1.2.69/24
FsxId05f7f00af49dc7a3e-02
                                                                   e0e
true
2 entries were displayed.
```

```
FsxId05f7f00af49dc7a3e::> cluster peer create -address-family ipv4 -peer
-addrs 10.1.1.57, 10.1.2.7
Notice: Use a generated passphrase or choose a passphrase of 8 or more
characters. To ensure the authenticity of the peering relationship, use a
phrase or sequence of characters that would be hard to guess.
Enter the passphrase:
Confirm the passphrase:
Notice: Now use the same passphrase in the "cluster peer create" command
in the other cluster.
```

`peer-addrs` Sind Cluster-IPs des Ziel-Clusters.

```
FsxId00fa9e3c784b6abbb::>  cluster peer create -address-family ipv4 -peer
-addrs  10.1.2.144, 10.1.2.69
Notice: Use a generated passphrase or choose a passphrase of 8 or more
characters. To ensure the authenticity of the peering relationship, use a
        phrase or sequence of characters that would be hard to guess.
Enter the passphrase:
Confirm the passphrase:
FsxId00fa9e3c784b6abbb::>
FsxId00fa9e3c784b6abbb::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
FsxId05f7f00af49dc7a3e    1-80-000011           Available      ok
```

Peer-SVMs

```
FsxId05f7f00af49dc7a3e::> vserver peer create -vserver sapcc-backup-
target-zone5 -peer-vserver sapcc-hana-svm -peer-cluster
FsxId00fa9e3c784b6abbb -applications snapmirror
Info: [Job 41] 'vserver peer create' job queued
```

```
FsxId00fa9e3c784b6abbb::> vserver peer accept -vserver sapcc-hana-svm
-peer-vserver sapcc-backup-target-zone5
Info: [Job 960] 'vserver peer accept' job queued
```

```
FsxId05f7f00af49dc7a3e::> vserver peer show
            Peer        Peer                           Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
sapcc-backup-target-zone5
            peer-source-cluster
                        peered       FsxId00fa9e3c784b6abbb
                                                       snapmirror
sapcc-hana-svm
```

Erstellen eines Ziel-Volumes

Sie müssen das Ziel-Volume mit dem Typ erstellen `DP` So markieren Sie es als Replikationsziel.

```
FsxId05f7f00af49dc7a3e::> volume create -vserver sapcc-backup-target-zone5
-volume PFX_data_mnt00001 -aggregate aggr1 -size 100GB -state online
-policy default -type DP -autosize-mode grow_shrink -snapshot-policy none
-foreground true -tiering-policy all -anti-ransomware-state disabled
[Job 42] Job succeeded: Successful
```

SnapMirror-Richtlinie erstellen

Die SnapMirror-Richtlinie und die hinzugefügte Regel definieren die Aufbewahrung und das SnapMirror-Etikett, um die zu replizierenden Snapshots zu identifizieren. Wenn Sie die SnapCenter-Richtlinie später erstellen, müssen Sie dasselbe Etikett verwenden.

```
FsxId05f7f00af49dc7a3e::> snapmirror policy create -policy snapcenter-
policy -tries 8 -transfer-priority normal -ignore-atime false -restart
always -type vault -vserver sapcc-backup-target-zone5
```

```
FsxId05f7f00af49dc7a3e::> snapmirror policy add-rule -vserver sapcc-
backup-target-zone5  -policy snapcenter-policy -snapmirror-label
snapcenter -keep 14
```

```
FsxId00fa9e3c784b6abbb::> snapmirror policy showVserver Policy
Policy Number         Transfer
Name    Name               Type   Of Rules Tries Priority Comment
------- ------------------ ------ -------- ----- -------- ----------
FsxId00fa9e3c784b6abbb
        snapcenter-policy  vault         1     8  normal  -
  SnapMirror Label: snapcenter                          Keep:      14
                                                  Total Keep:      14
```

SnapMirror Beziehung erstellen

Jetzt wird die Beziehung zwischen dem Quell- und dem Ziel-Volume sowie der Typ XDP und der zuvor erstellten Richtlinie definiert.

```
FsxId05f7f00af49dc7a3e::> snapmirror create -source-path sapcc-hana-
svm:PFX_data_mnt00001 -destination-path sapcc-backup-target-
zone5:PFX_data_mnt00001 -vserver sapcc-backup-target-zone5 -throttle
unlimited -identity-preserve false -type XDP -policy snapcenter-policy
Operation succeeded: snapmirror create for the relationship with
destination "sapcc-backup-target-zone5:PFX_data_mnt00001".
```

SnapMirror initialisieren

Mit diesem Befehl wird die erste Replikation gestartet. Bei diesem Vorgang werden alle Daten vom Quell-Volume auf das Ziel-Volume übertragen.

```
FsxId05f7f00af49dc7a3e::> snapmirror initialize -destination-path sapcc-
backup-target-zone5:PFX_data_mnt00001 -source-path sapcc-hana-
svm:PFX_data_mnt00001
Operation is queued: snapmirror initialize of destination "sapcc-backup-
target-zone5:PFX_data_mnt00001".
```

Sie können den Status der Replikation mit überprüfen `snapmirror show` Befehl.

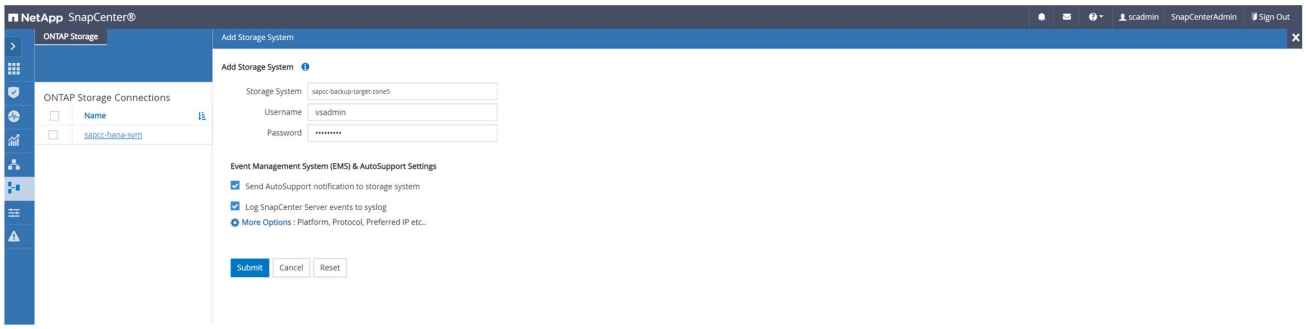
```
FsxId05f7f00af49dc7a3e::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
sapcc-hana-svm:PFX_data_mnt00001
            XDP  sapcc-backup-target-zone5:PFX_data_mnt00001
                             Uninitialized
                                     Transferring   1009MB    true
02/24 12:34:28
```

```
FsxId05f7f00af49dc7a3e::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
sapcc-hana-svm:PFX_data_mnt00001
            XDP  sapcc-backup-target-zone5:PFX_data_mnt00001
                             Snapmirrored
                                     Idle           -         true    -
```

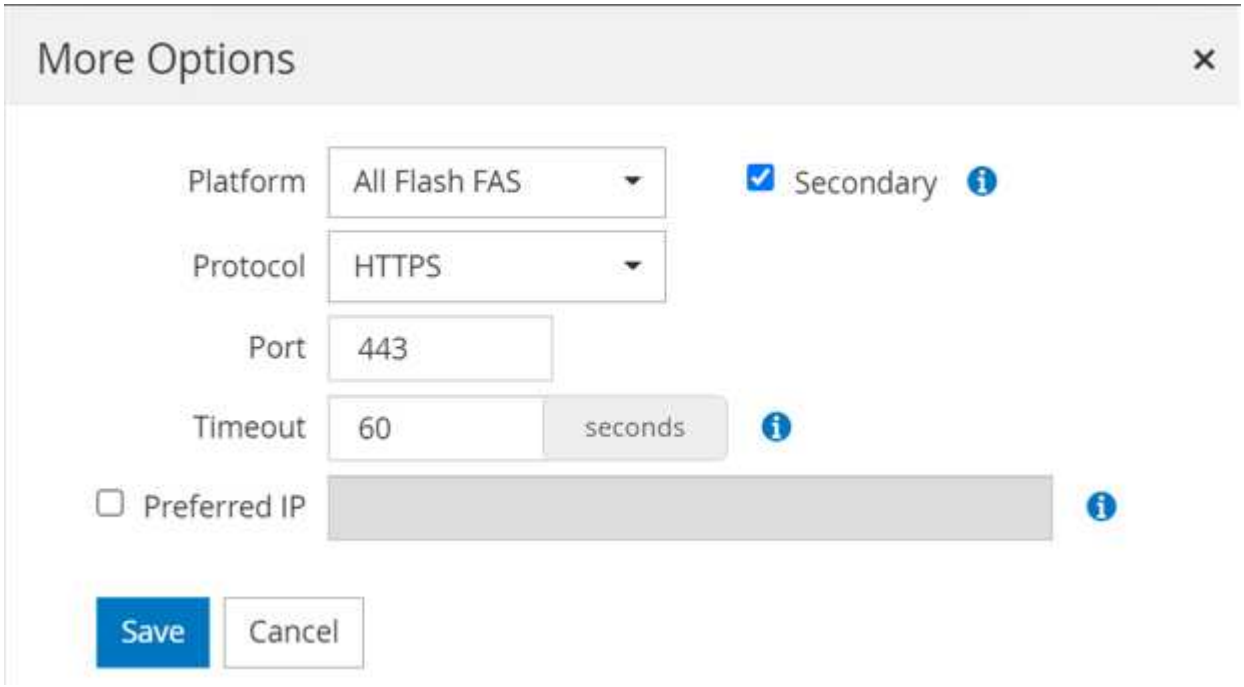
Fügen Sie eine Backup-SVM zu SnapCenter hinzu

So fügen Sie eine Backup-SVM zu SnapCenter hinzu:

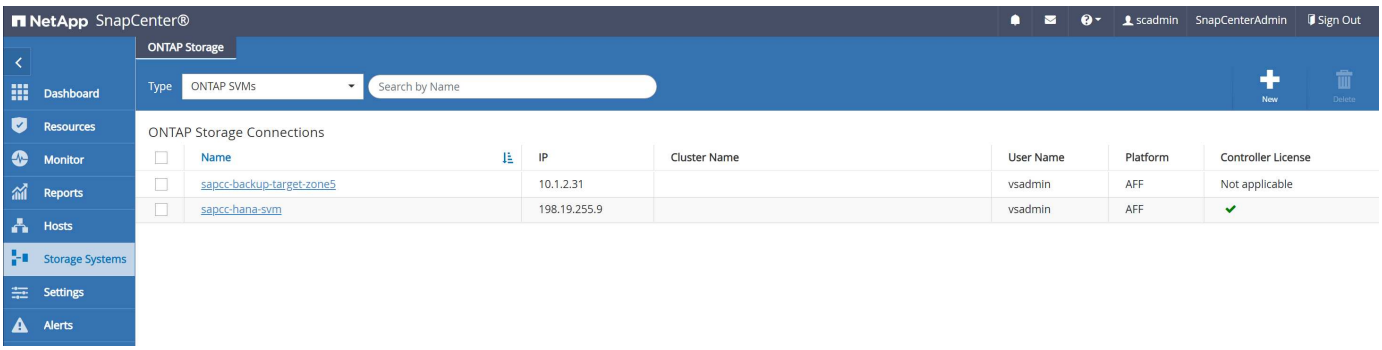
1. Konfigurieren Sie die SVM, auf der sich das SnapVault Ziel-Volume in SnapCenter befindet.



2. Wählen Sie im Fenster Weitere Optionen als Plattform All-Flash-FAS aus, und wählen Sie Sekundär aus.



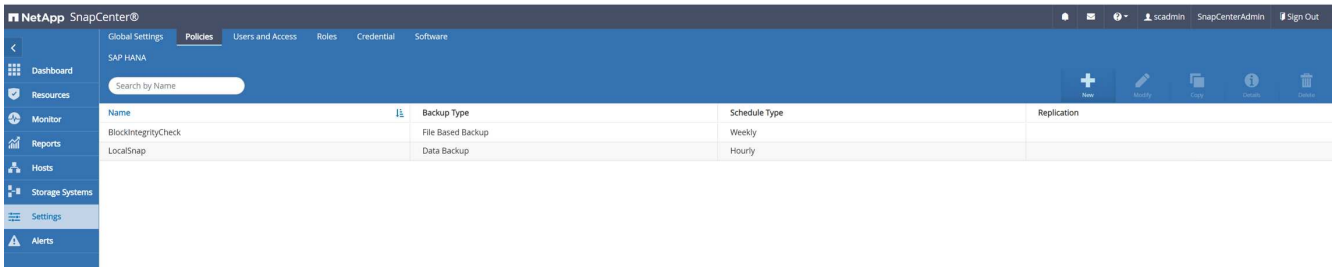
Die SVM ist jetzt in SnapCenter verfügbar.



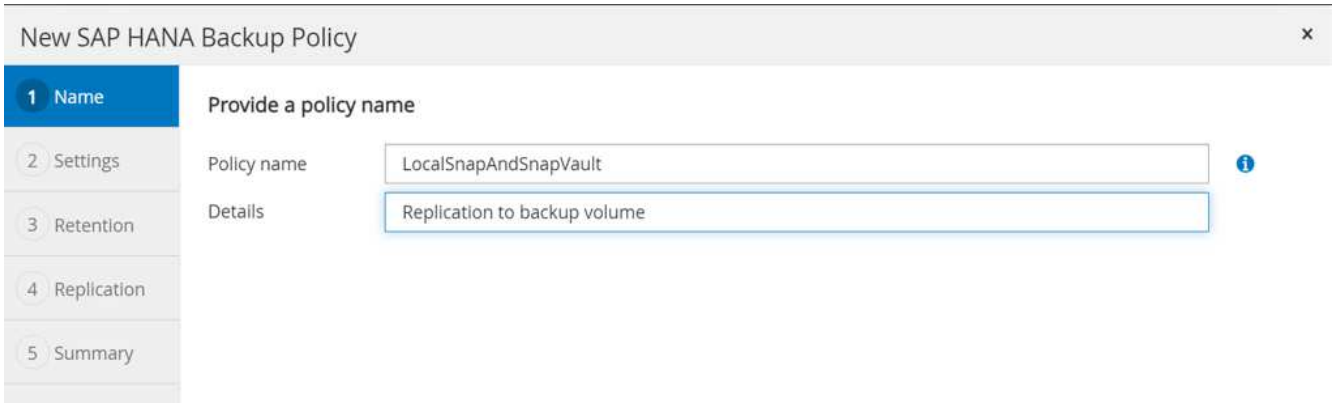
Erstellen einer neuen SnapCenter-Richtlinie für Backup-Replizierung

Sie müssen eine Richtlinie für die Backup-Replikation wie folgt konfigurieren:

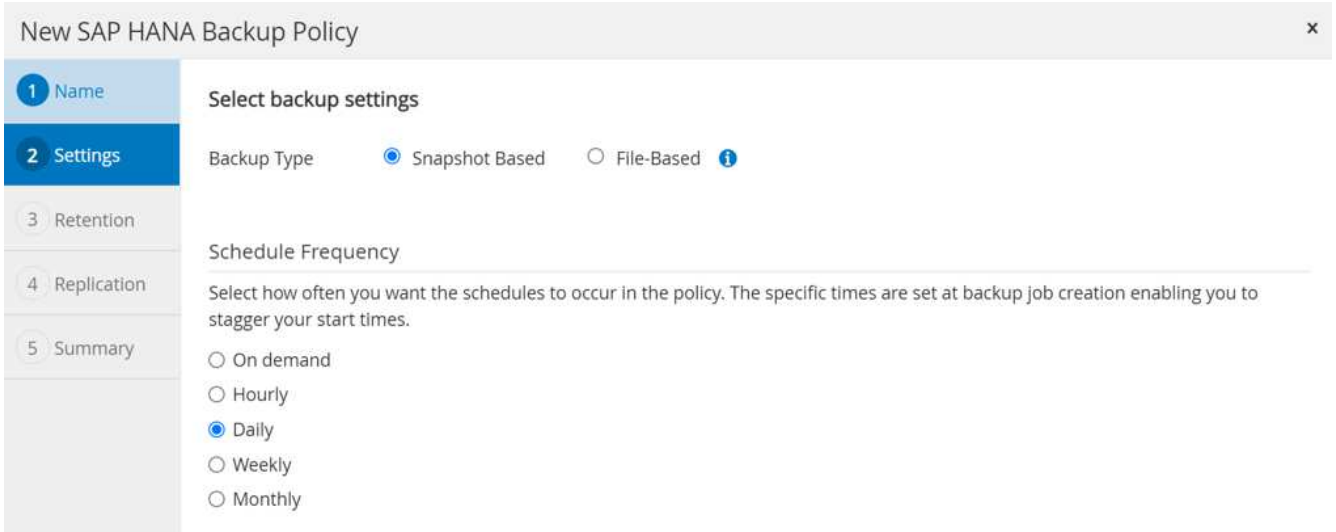
1. Geben Sie einen Namen für die Richtlinie ein.



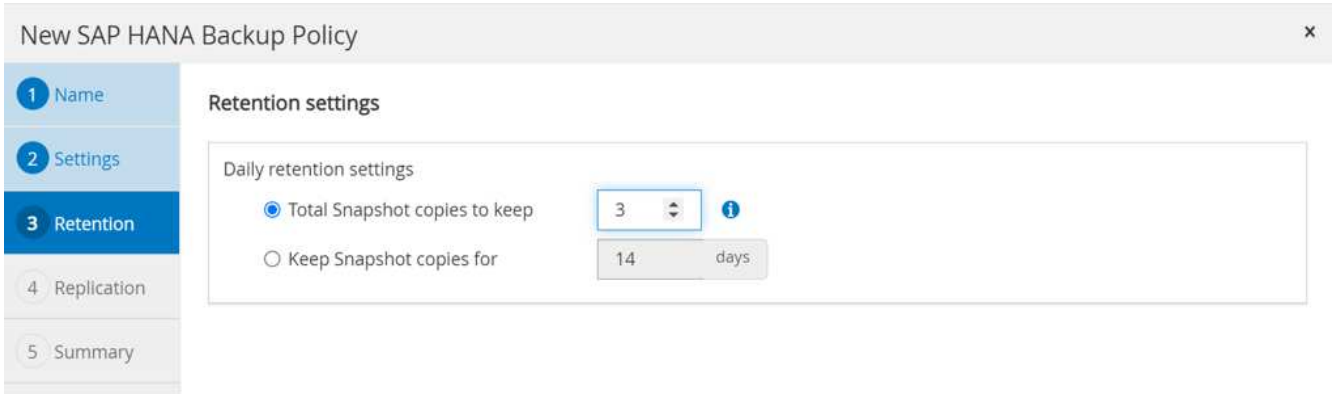
2. Wählen Sie Snapshot Backup und eine Zeitplanfrequenz aus. Für die Backup-Replizierung wird täglich verwendet.



3. Wählen Sie die Aufbewahrung für die Snapshot-Backups aus.

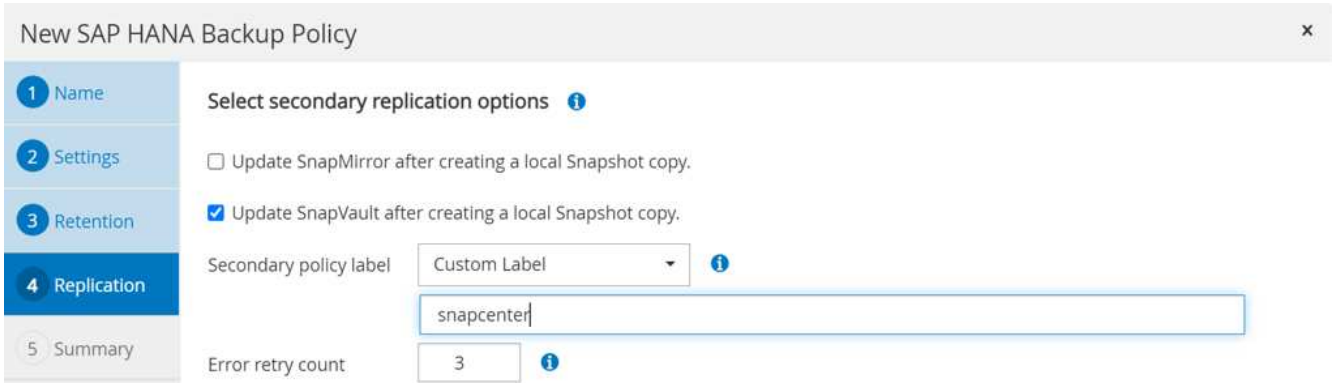


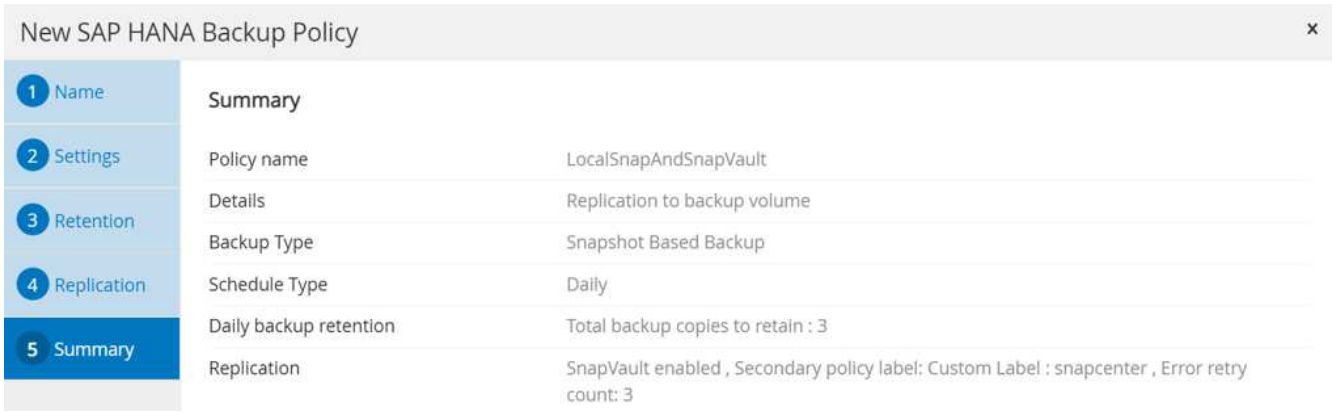
Dies ist die Aufbewahrung für die täglichen Snapshot Backups, die im primären Storage erstellt wurden. Die Aufbewahrung für sekundäre Backups auf dem SnapVault-Ziel wurde bereits mit dem Befehl „Add rule“ auf der ONTAP-Ebene konfiguriert. Siehe „Konfigurieren von Replikationsbeziehungen auf FSX für ONTAP-Dateisysteme“ (xref).



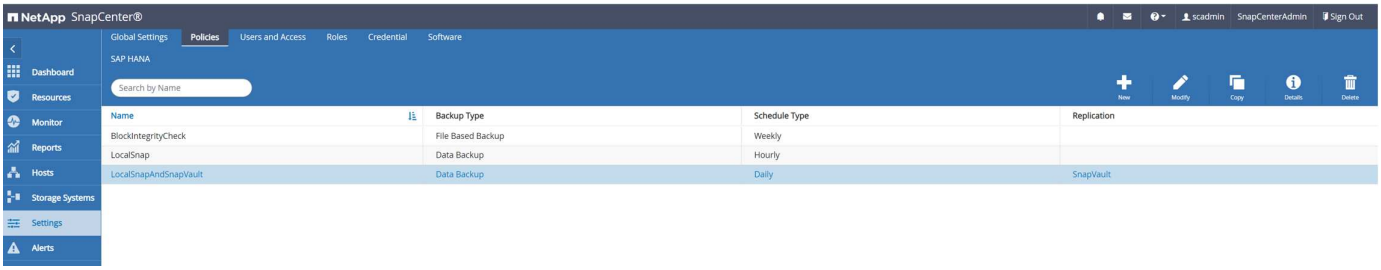
4. Wählen Sie das Feld SnapVault aktualisieren aus, und geben Sie eine benutzerdefinierte Bezeichnung an.

   Dieses Etikett muss mit der SnapMirror-Bezeichnung im übereinstimmen `add rule` Befehl auf ONTAP-Ebene.



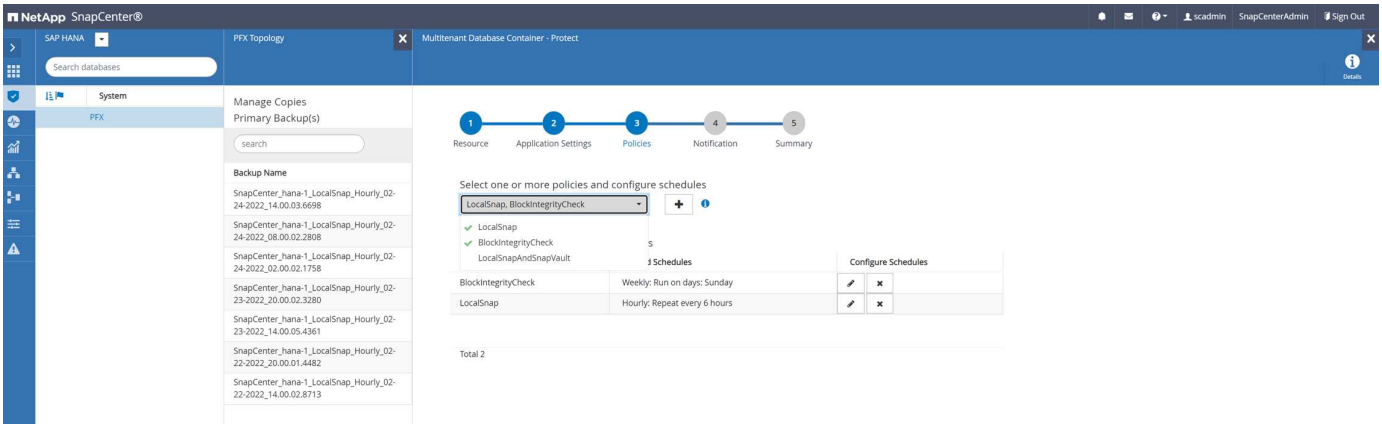


Die neue SnapCenter-Richtlinie ist jetzt konfiguriert.

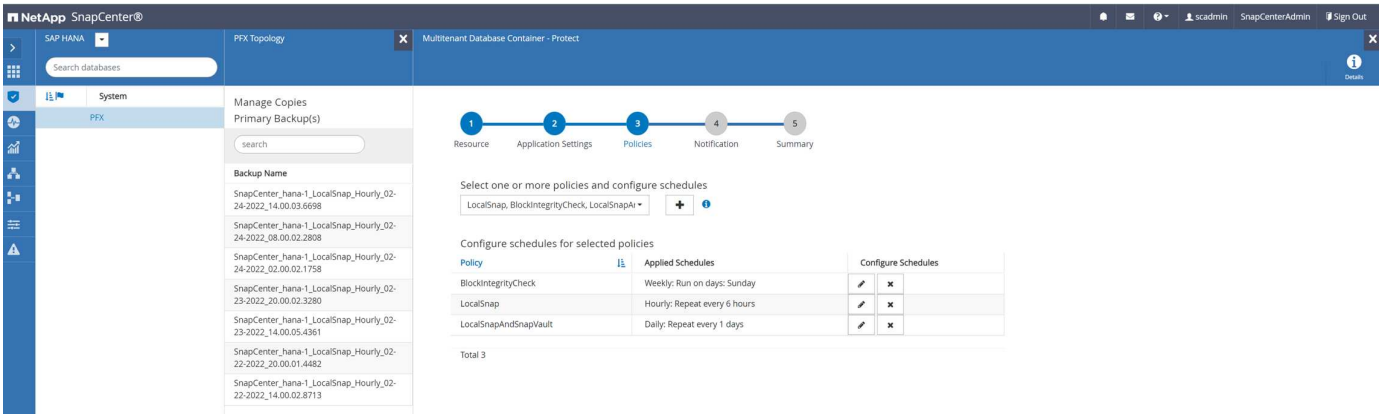


Fügen Sie eine Richtlinie zum Ressourcenschutz hinzu

Sie müssen die neue Richtlinie der HANA-Ressourcenschutzkonfiguration hinzufügen, wie in der folgenden Abbildung dargestellt.



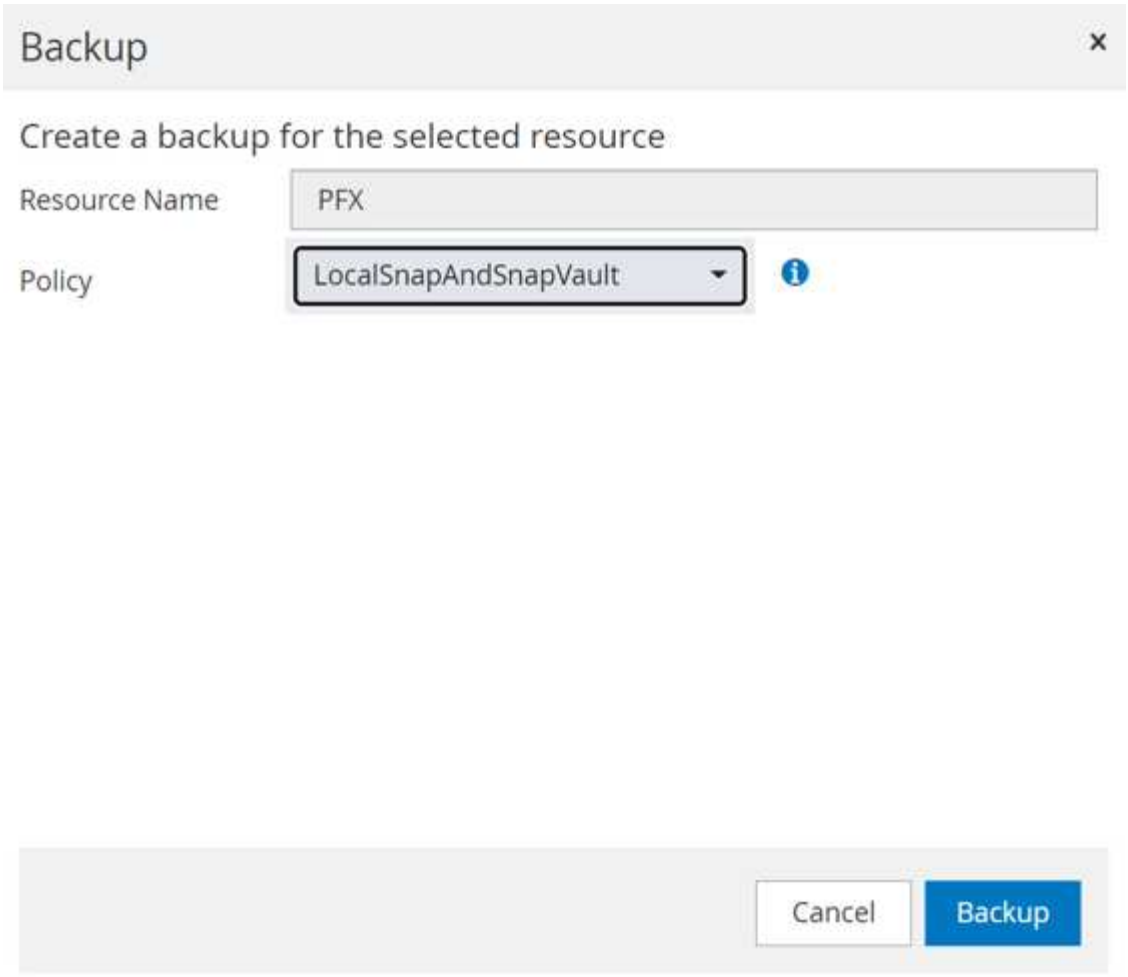
Ein täglicher Zeitplan wird in unserem Setup festgelegt.



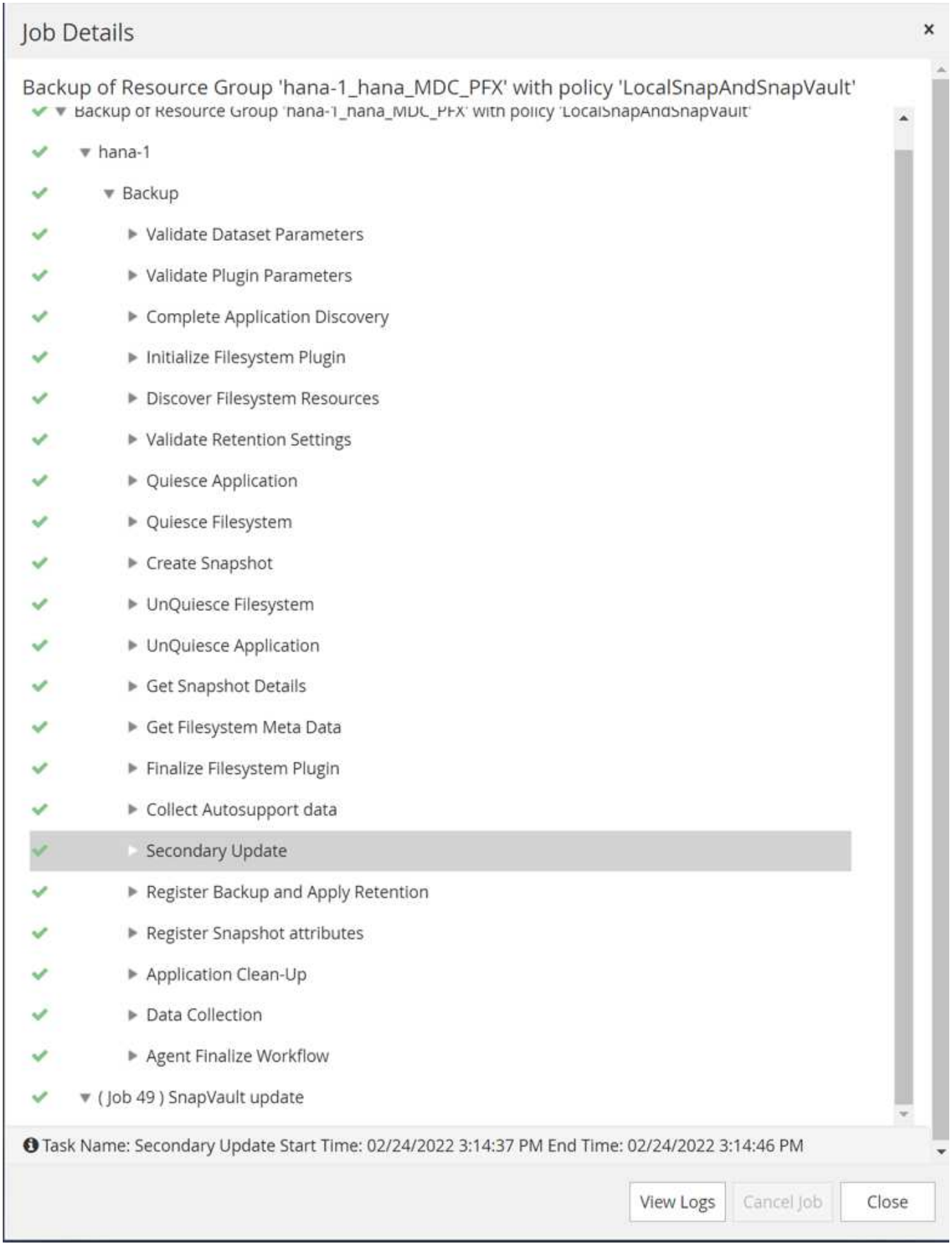
Erstellen Sie ein Backup mit Replikation

Ein Backup wird auf dieselbe Weise wie eine lokale Snapshot Kopie erstellt.

Um ein Backup mit Replikation zu erstellen, wählen Sie die Richtlinie aus, die die Backup-Replikation enthält, und klicken Sie auf Backup.



Im Jobprotokoll von SnapCenter wird der Schritt sekundäre Aktualisierung angezeigt, der einen SnapVault-Aktualisierungsvorgang initiiert. Replizierung hat geänderte Blöcke vom Quell-Volume auf das Ziel-Volume repliziert.



Auf dem FSX für ONTAP Filesystem wird ein Snapshot auf dem Quell-Volume mit dem SnapMirror Label

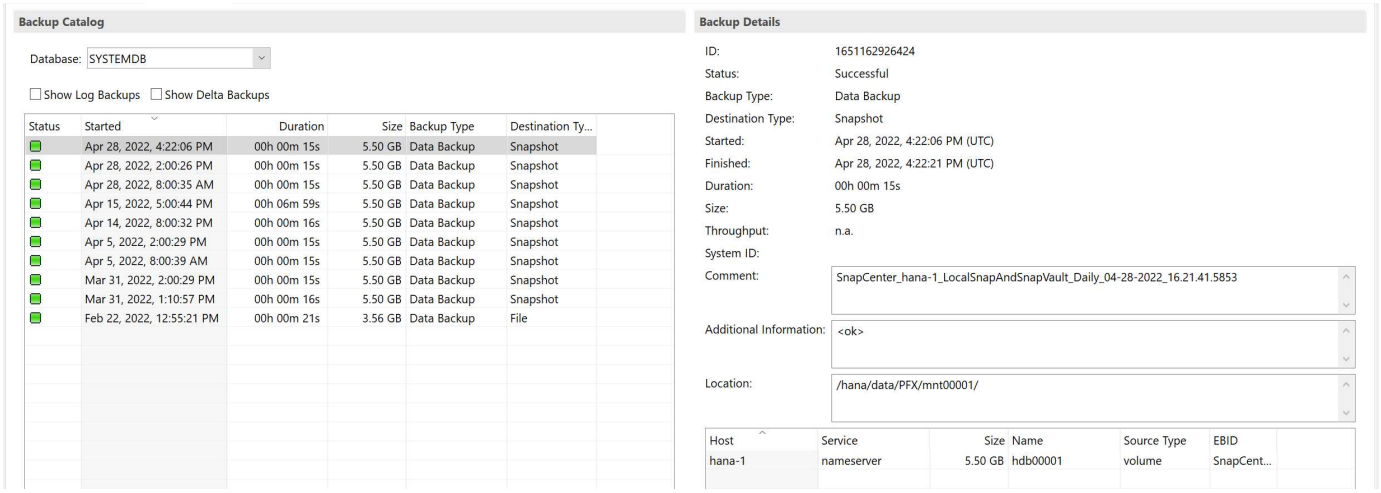
erstellt. `snapcenter`, Wie in der SnapCenter-Richtlinie konfiguriert.

```
FsxId00fa9e3c784b6abbb::> snapshot show -vserver sapcc-hana-svm -volume
PFX_data_mnt00001 -fields snapmirror-label
vserver        volume            snapshot
snapmirror-label
-------------- -----------------
-------------------------------------------------------------
----------------
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_03-31-
2022_13.10.26.5482 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_03-31-
2022_14.00.05.2023 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-05-
2022_08.00.06.3380 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-05-
2022_14.00.01.6482 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-14-
2022_20.00.05.0316 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-28-
2022_08.00.06.3629 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-28-
2022_14.00.01.7275 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-
1_LocalSnapAndSnapVault_Daily_04-28-2022_16.21.41.5853

snapcenter
8 entries were displayed.
```

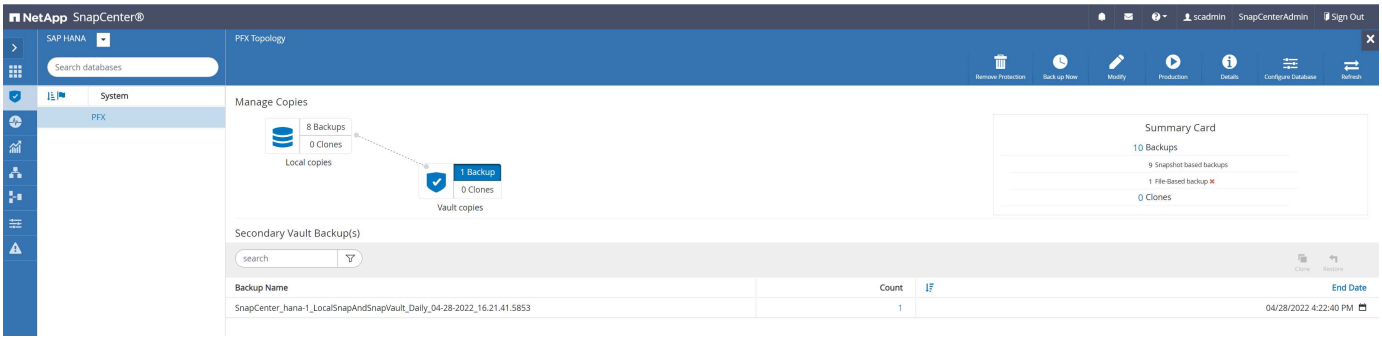
Auf dem Ziel-Volume wird eine Snapshot Kopie mit demselben Namen erstellt.

```
FsxId05f7f00af49dc7a3e::> snapshot show -vserver sapcc-backup-target-zone5
-volume PFX_data_mnt00001 -fields snapmirror-label
vserver                   volume            snapshot
snapmirror-label
------------------------- -----------------
-------------------------------------------------------------------------
----------------
sapcc-backup-target-zone5 PFX_data_mnt00001 SnapCenter_hana-
1_LocalSnapAndSnapVault_Daily_04-28-2022_16.21.41.5853 snapcenter
FsxId05f7f00af49dc7a3e::>
```

Auch das neue Snapshot-Backup ist im HANA-Backup-Katalog enthalten.



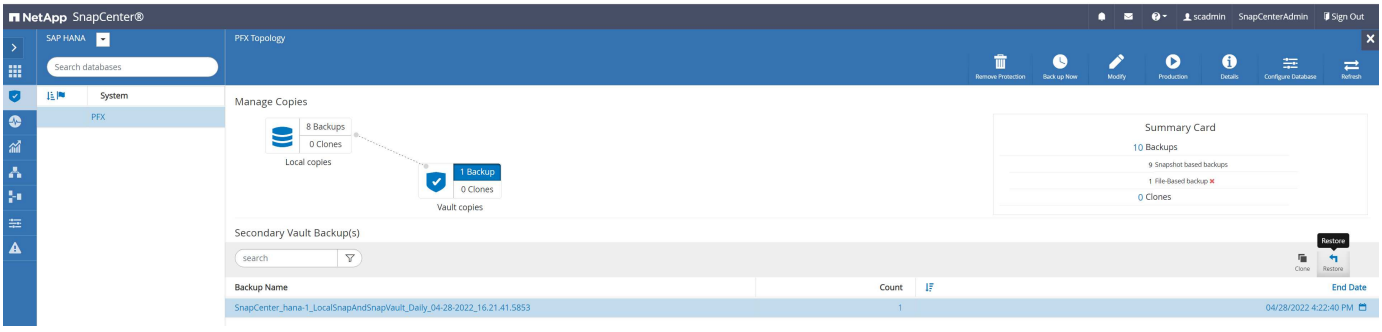
In SnapCenter können Sie die replizierten Backups auflisten, indem Sie in der Topologieansicht auf Vault Kopien klicken.



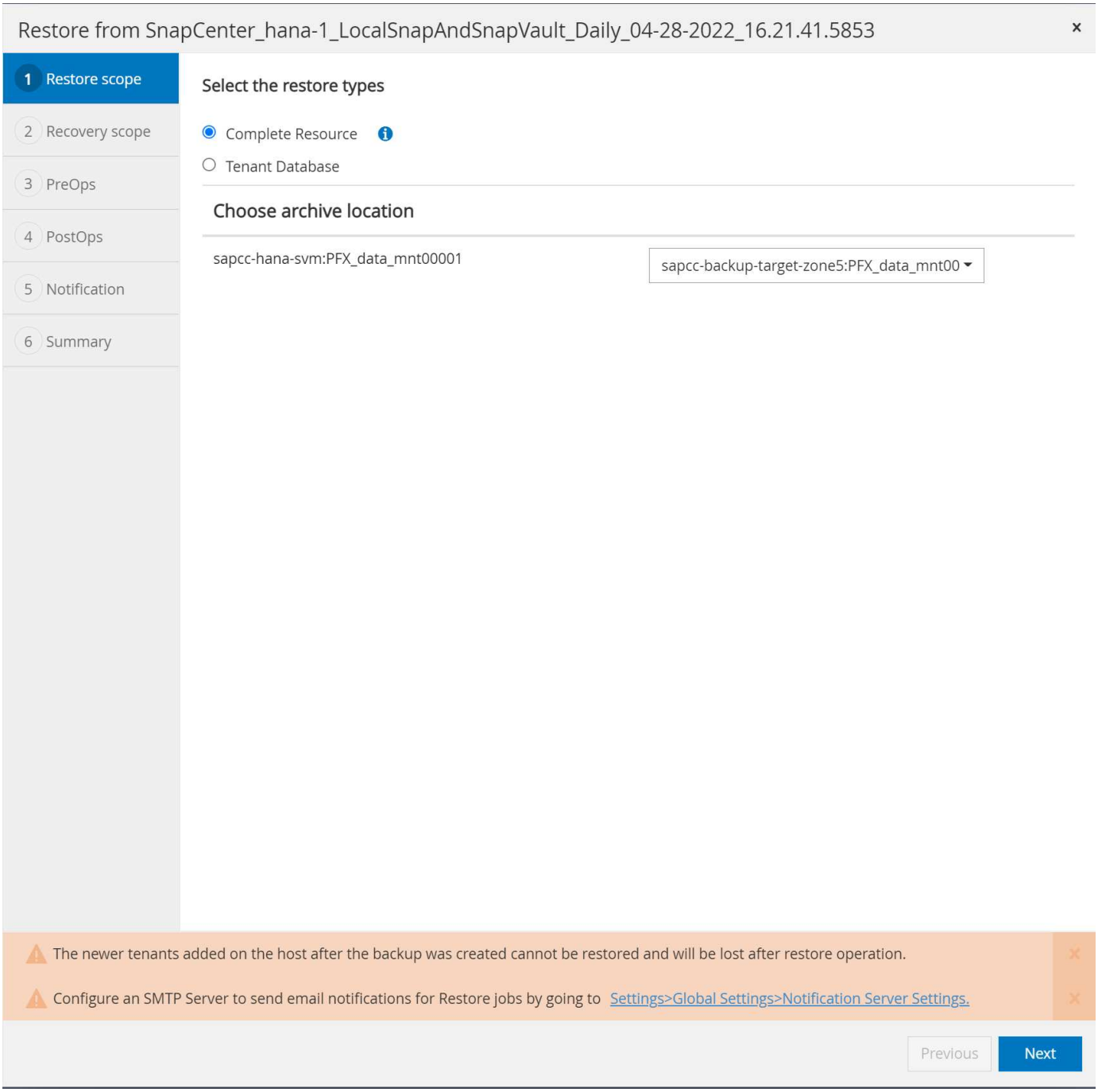
Wiederherstellung im Sekundär-Storage

Führen Sie die folgenden Schritte aus, um im Sekundärspeicher wiederherzustellen und eine Wiederherstellung durchzuführen:

Um die Liste aller Backups auf dem sekundären Storage abzurufen, klicken Sie in der Ansicht SnapCenter Topology auf Vault Kopien, wählen Sie dann ein Backup aus und klicken Sie auf Wiederherstellen.



Das Dialogfeld Wiederherstellen zeigt die sekundären Speicherorte an.



Weitere Restore- und Recovery-Schritte sind mit denen identisch, die bei einem Snapshot Backup im Primärspeicher besprochen wurden.

Wo Sie weitere Informationen finden

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- FSX für NetApp ONTAP Benutzerhandbuch – Was ist Amazon FSX für NetApp ONTAP?

  https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/what-is-fsx-ontap.html

- Ressourcen-Seite zu SnapCenter

"https://www.netapp.com/us/documentation/snapcenter-software.aspx"

- SnapCenter-Softwaredokumentation

  "https://docs.netapp.com/us-en/snapcenter/index.html"

- TR-4667: Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter

  "Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter"

- TR-4719: SAP HANA System Replication – Backup und Recovery mit SnapCenter

  "Backup und Recovery mit SnapCenter"

Versionsverlauf

Version	Datum	Versionsverlauf des Dokuments
Version 1.0	Mai 2022	Erste Version.

Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter

TR-4614: SAP HANA Backup und Recovery mit SnapCenter

Unternehmen benötigen heutzutage eine kontinuierliche, unterbrechungsfreie Verfügbarkeit ihrer SAP-Applikationen. Sie erwarten konsistente Performance angesichts stetig wachsender Datenvolumen und bei routinemäßigen Wartungsaufgaben wie System-Backups. Das Durchführen von Backups von SAP-Datenbanken ist eine wichtige Aufgabe, die erhebliche Performance-Auswirkungen auf das SAP-Produktionssystem haben kann.

Autor: Nils Bauer, NetApp

Die Backup-Fenster schrumpfen, während die zu sichernden Daten immer größer werden. Somit ist es schwierig, mit minimalen Auswirkungen auf Geschäftsprozesse einen Zeitpunkt zu finden, in dem Backups durchgeführt werden können. Die Zeit, die zum Wiederherstellen und Wiederherstellen von SAP-Systemen benötigt wird, ist besorgt, da Ausfallzeiten bei SAP-Produktions- und nicht produktiven Systemen minimiert werden müssen, um Datenverlusten und Kosten für das Unternehmen zu reduzieren.

Folgende Punkte fassen die Herausforderungen zusammen, die mit SAP-Backup und -Recovery zu tun haben:

- **Performance-Auswirkungen auf SAP-Produktionssysteme.** herkömmliche Copy-basierte Backups führen in der Regel aufgrund der hohen Belastungen auf den Datenbankserver, das Storage-System und das Speichernetzwerk zu einer erheblichen Performance-Belastung für SAP-Produktionssysteme.
- **Schrumpfende Backup-Fenster.** herkömmliche Backups können nur vorgenommen werden, wenn nur wenige Dialoge oder Batch-Aktivitäten im SAP-System ausgeführt werden. Wenn SAP Systeme rund um die Uhr im Einsatz sind, gestaltet sich die Planung von Backups schwieriger.
- **Schnelles Datenwachstum.** für ein schnelles Datenwachstum und immer kleiner werdende Backup-Fenster sind laufende Investitionen in die Backup-Infrastruktur erforderlich. Das bedeutet, dass Sie mehr Tape-Laufwerke, zusätzlichen Backup-Speicherplatz und schnellere Backup-Netzwerke beschaffen

müssen. Außerdem müssen Sie die laufenden Kosten für die Speicherung und das Management der Tape-Ressourcen tragen. Inkrementelle oder differenzielle Backups können diese Probleme beheben. Allerdings führt diese Anordnung zu einem sehr langsamen, umständlichen und komplexen Restore-Prozess, der sich schwieriger überprüfen lässt. Derartige Systeme verkürzen in der Regel die Zeiten der Recovery-Zeit (Recovery Time Objective, RTO) und des Recovery-Zeitpunkts (RPO) und sind für das Unternehmen nicht akzeptabel.

- **Steigende Kosten von Ausfallzeiten.** ungeplante Ausfallzeiten eines SAP-Systems haben typischerweise Auswirkungen auf die Geschäftsfinanzen. Die Notwendigkeit der Wiederherstellung des SAP Systems erfordert einen Großteil aller ungeplanten Ausfallzeiten. Daher bestimmt die gewünschte RTO das Design der Backup- und Recovery-Architektur.
- **Backup- und Wiederherstellungszeit für SAP-Upgrade-Projekte.** der Projektplan für ein SAP-Upgrade beinhaltet mindestens drei Backups der SAP-Datenbank. Diese Backups reduzieren die für den Upgrade-Prozess verfügbare Zeit erheblich. Die Entscheidung zum Fortfahren hängt im Allgemeinen von der Zeit ab, die zur Wiederherstellung der Datenbank aus dem zuvor erstellten Backup benötigt wird. Statt ein System in den vorherigen Zustand wiederherzustellen, bietet eine schnelle Wiederherstellung mehr Zeit zur Behebung von Problemen, die bei einem Upgrade auftreten können.

Die Lösung von NetApp

Mit der NetApp Snapshot Technologie können Datenbank-Backups innerhalb von Minuten erstellt werden. Wie lange es dauert, eine Snapshot Kopie zu erstellen, ist unabhängig von der Größe der Datenbank, da bei Snapshot Kopien keine physischen Datenblöcke auf der Storage-Plattform verschoben werden. Weil die NetApp Snapshot Technologie keine Datenblöcke verschiebt oder kopiert, wirkt sie sich nicht auf die Performance des produktiven SAP Systems aus, wenn Snapshot Kopie erstellt oder Daten im aktiven Filesystem geändert werden. Daher kann die Erstellung von Snapshot Kopien ohne die Berücksichtigung von Spitzenzeiten oder Batch-Aktivitäten geplant werden. SAP- und NetApp-Kunden planen normalerweise mehrere Online Snapshot-Backups pro Tag, so dass beispielsweise alle vier Stunden üblich sind. Diese Snapshot Backups werden in der Regel drei bis fünf Tage auf dem primären Storage-System gespeichert, bevor sie entfernt werden.

Snapshot Kopien bieten auch wichtige Vorteile für Wiederherstellung und Recovery. NetApp SnapRestore Daten-Recovery-Software ermöglicht auf der Grundlage von verfügbaren Snapshot Kopien die Wiederherstellung einer gesamten Datenbank oder eines Teils einer Datenbank zu einem beliebigen Zeitpunkt. Solche Wiederherstellungen sind innerhalb von wenigen Minuten abgeschlossen, unabhängig von der Größe der Datenbank. Da mehrere Online Snapshot Backups tagsüber erstellt werden, verringert sich die für den Recovery-Prozess erforderliche Zeit im Vergleich zu einem herkömmlichen Backup-Ansatz deutlich. Da eine Wiederherstellung mit einer Snapshot-Kopie durchgeführt werden kann, die nur wenige Stunden alt ist (und nicht bis zu 24 Stunden), müssen weniger Transaktions-Logs angewendet werden. Daher reduziert sich die RTO auf mehrere Minuten – statt auf mehrere Stunden für herkömmliche Single-Cycle Tape Backups.

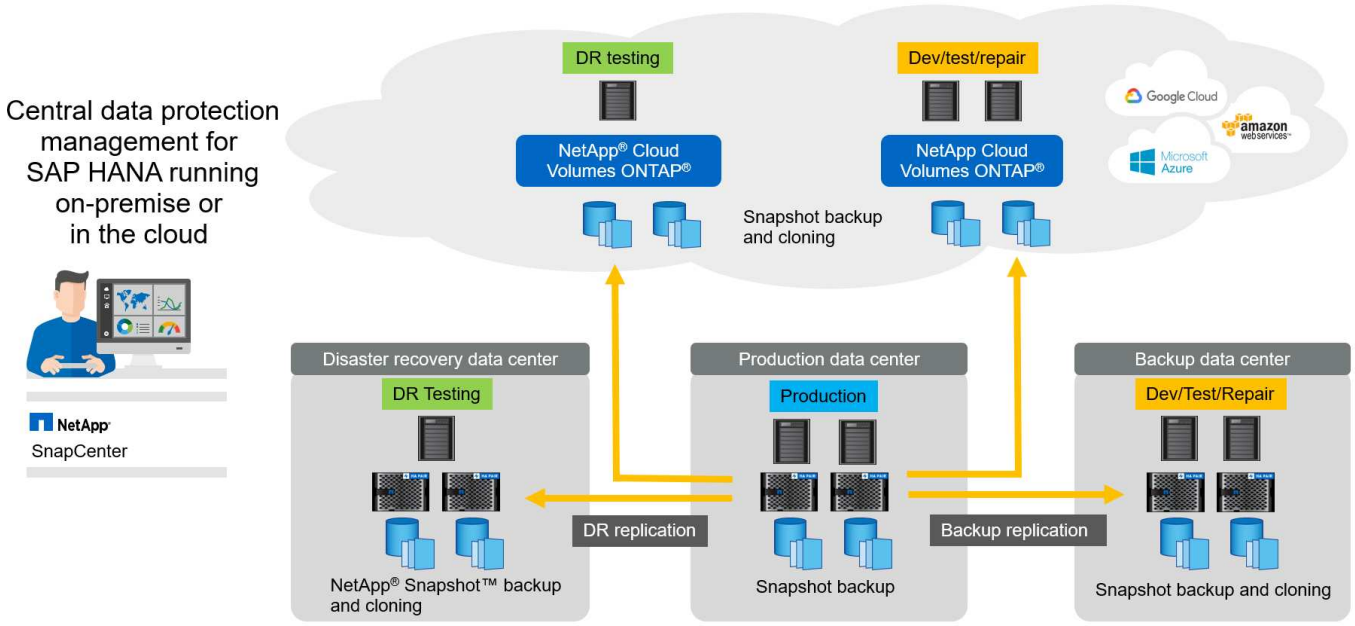
Backups von Snapshot-Kopien werden auf demselben Festplattensystem wie die aktiven Online-Daten gespeichert. Daher empfiehlt NetApp, Backups von Snapshot-Kopien als Ergänzung zu verwenden, anstatt Backups an einen sekundären Standort zu ersetzen. Die meisten Restore- und Recovery-Aktionen werden mithilfe von SnapRestore im primären Storage-System durchgeführt. Restores von einem Sekundärstandort sind nur nötig, wenn das primäre Storage-System, das die Snapshot-Kopien enthält, beschädigt ist. Der sekundäre Standort kann auch verwendet werden, wenn ein Backup, das nicht mehr in einer Snapshot Kopie verfügbar ist, wiederhergestellt werden muss: Ein monatliches Backup.

Ein Backup an einen sekundären Standort basiert auf Snapshot-Kopien, die auf dem primären Storage erstellt wurden. Somit werden die Daten direkt aus dem primären Storage-System eingelesen, ohne dass dabei der SAP Datenbankserver belastet wird. Der primäre Storage kommuniziert direkt mit dem sekundären Storage und sendet mithilfe eines NetApp SnapVault Disk-to-Disk Backups die Backup-Daten an das Ziel.

SnapVault bietet im Vergleich zu herkömmlichen Backups deutliche Vorteile. Nach einem ersten Datentransfer,

bei dem alle Daten vom Quell- zum Ziel-Volume übertragen wurden, kopieren bei allen nachfolgenden Backups nur die geänderten Blöcke in den sekundären Storage. Somit werden die Last auf dem primären Storage-System und der Zeitaufwand für ein Vollbackup deutlich reduziert. Da SnapVault nur die geänderten Blöcke am Ziel speichert, benötigt ein vollständiges Datenbank-Backup weniger Festplattenspeicher.

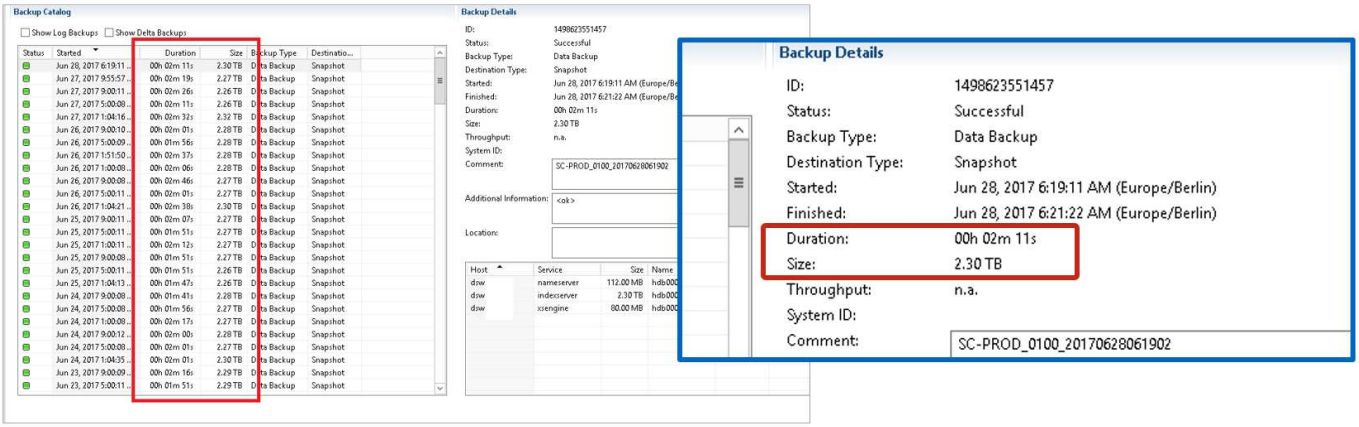
Die Lösung kann zudem nahtlos auf ein Hybrid-Cloud-Betriebsmodell erweitert werden. Die Datenreplizierung für die Disaster Recovery oder für ein externes Backup kann von lokalen NetApp ONTAP Systemen auf Cloud Volumes ONTAP Instanzen in der Cloud durchgeführt werden. SnapCenter kann als zentrales Tool für das Management der Datensicherung und der Datenreplizierung eingesetzt werden – unabhängig davon, ob das SAP HANA System lokal oder in der Cloud ausgeführt wird. Die folgende Abbildung zeigt einen Überblick über die Backup-Lösung.



Laufzeit von Snapshot-Backups

Der nächste Screenshot zeigt ein Kunde im HANA Studio, in dem SAP HANA auf NetApp Storage läuft. Der Kunde erstellt mithilfe von Snapshot Kopien ein Backup der HANA Datenbank. Das Bild zeigt, dass die HANA-Datenbank (ca. 2,3 TB groß) mithilfe der Snapshot-Backup-Technologie in 2 Minuten und 11 Sekunden gesichert wird.

Der größte Teil der gesamten Laufzeit des Backup-Workflows ist die Zeit, die zur Ausführung des HANA-Backup-Speicherpunktvorgangs benötigt wird. Dieser Schritt hängt von der Last der HANA-Datenbank ab. Das Snapshot Backup selbst ist in wenigen Sekunden abgeschlossen.



Vergleich der Recovery-Zeitvorgaben

Dieser Abschnitt enthält einen RTO-Vergleich von Datei- und Storage-basierten Snapshot-Backups. Das RTO wird durch die Summe der Zeit, die zur Wiederherstellung der Datenbank benötigt wird, und der Zeit definiert, die zum Starten und Wiederherstellen der Datenbank erforderlich ist.

Benötigte Zeit zum Wiederherstellen der Datenbank

Bei einem dateibasierten Backup hängt die Restore-Zeit von der Größe der Datenbank und der Backup-Infrastruktur ab, die die Restore-Geschwindigkeit in Megabyte pro Sekunde festlegt. Wenn die Infrastruktur beispielsweise einen Restore-Vorgang mit einer Geschwindigkeit von 250 MB/s unterstützt, dauert es etwa 1 Stunde und 10 Minuten, um eine Datenbank mit einer Größe von 1 TB wiederherzustellen.

Die Restore-Dauer ist bei Backups der Storage Snapshot Kopien unabhängig von der Größe der Datenbank und liegt im Bereich von einigen Sekunden, wenn die Wiederherstellung im Primärspeicher durchgeführt werden kann. Eine Wiederherstellung aus sekundärem Storage ist nur bei einem Notfall erforderlich, wenn der primäre Storage nicht mehr verfügbar ist.

Benötigte Zeit zum Starten der Datenbank

Die Startzeit der Datenbank hängt von der Größe der Zeile und des Spaltenspeichers ab. Für den Spaltenspeicher hängt die Startzeit auch davon ab, wie viele Daten während des Datenbankstartens vorgeladen werden. In den folgenden Beispielen gehen wir davon aus, dass die Startzeit 30 Minuten beträgt. Die Startzeit ist bei einem dateibasierten Restore und Recovery gleich, sowie bei einem Restore und Recovery auf Basis von Snapshot.

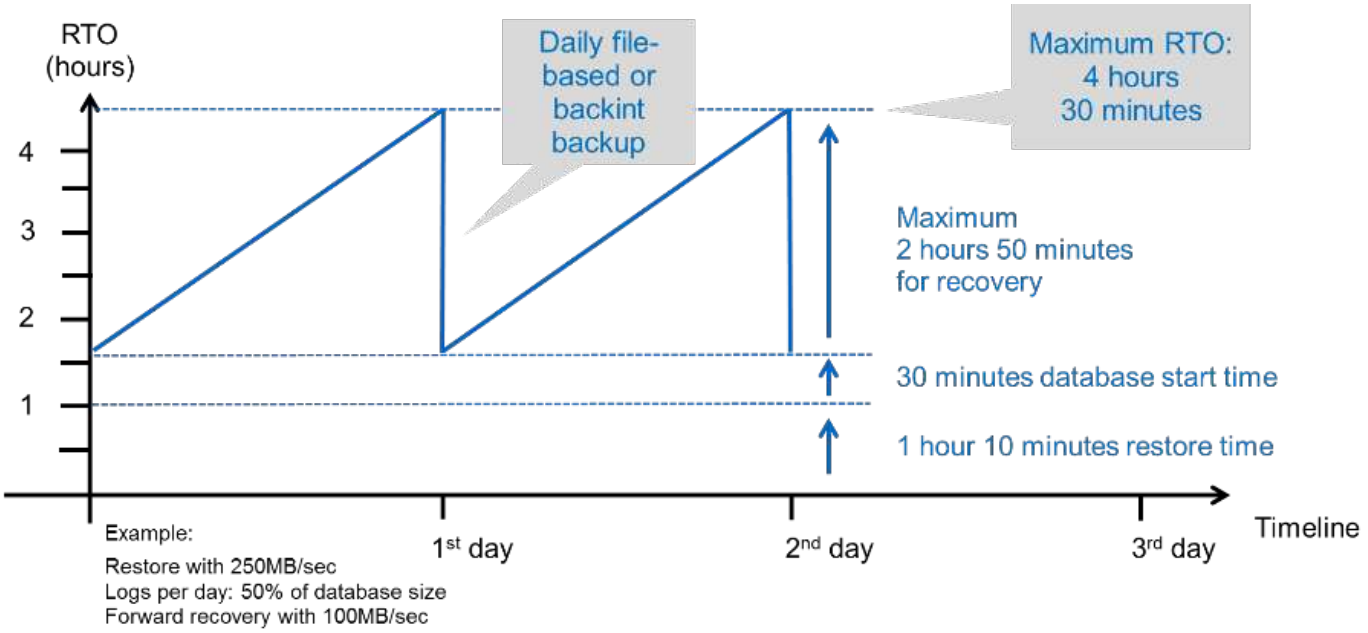
Benötigte Zeit für das Recovery von Datenbanken

Die Wiederherstellungszeit hängt von der Anzahl der Protokolle ab, die nach der Wiederherstellung angewendet werden müssen. Diese Zahl hängt von der Häufigkeit ab, mit der Daten-Backups erstellt werden.

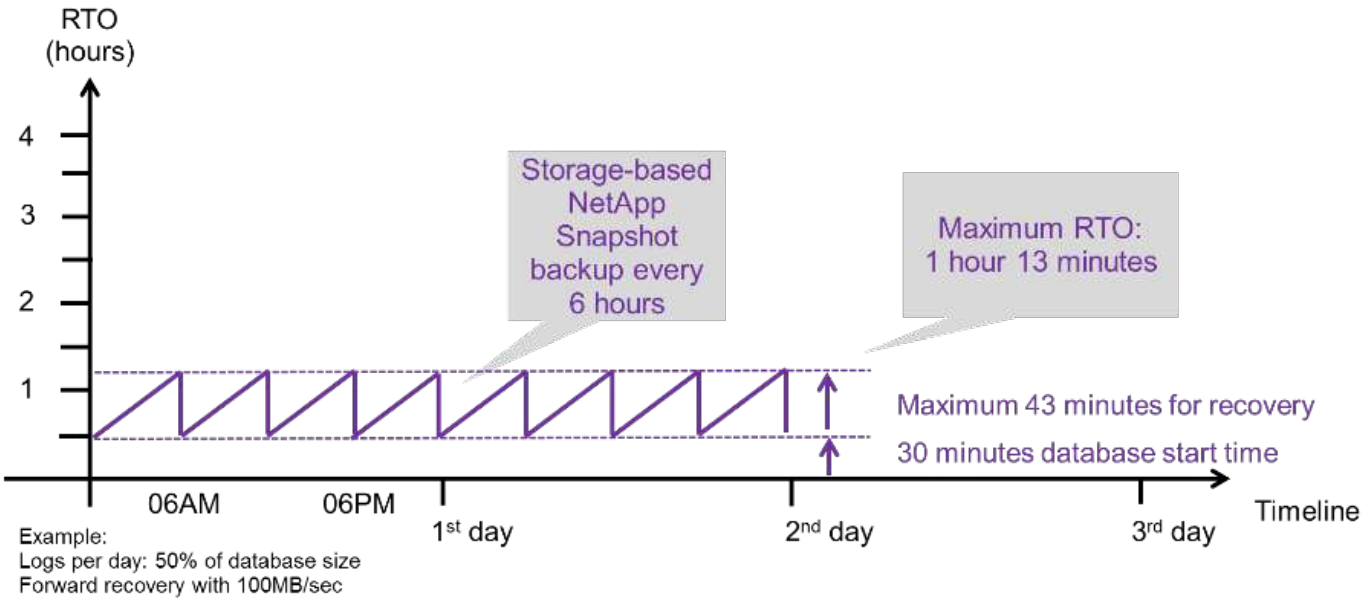
Bei dateibasierten Daten-Backups wird der Backup-Zeitplan normalerweise einmal pro Tag erstellt. Eine höhere Backup-Frequenz ist normalerweise nicht möglich, da das Backup die Produktions-Performance beeinträchtigt. Daher müssen im schlimmsten Fall alle Protokolle, die während des Tages geschrieben wurden, während der Forward Recovery angewendet werden.

Backups von Storage Snapshot Kopien werden in der Regel häufiger geplant, da sie die Performance der SAP HANA Datenbank nicht beeinträchtigen. Wenn beispielsweise alle sechs Stunden Snapshot Kopien Backups geplant werden, wäre die Recovery-Zeit im schlimmsten Fall ein Viertel der Recovery-Zeit für ein dateibasiertes Backup (6 Stunden / 24 Stunden = ¼).

Die folgende Abbildung zeigt ein RTO-Beispiel für eine 1-TB-Datenbank, wenn dateibasierte Daten-Backups verwendet werden. In diesem Beispiel wird ein Backup einmal pro Tag erstellt. Die RTO unterscheidet sich je nach dem Zeitpunkt der Wiederherstellung und des Recovery. Falls die Restore- und Recovery-Vorgänge unmittelbar nach dem Backup durchgeführt wurden, basiert die RTO in erster Linie auf der Restore-Zeit, die in dem Beispiel 1 Stunde und 10 Minuten beträgt. Die Recovery-Zeit stieg auf 2 Stunden und 50 Minuten, wenn Restore und Recovery unmittelbar vor dem nächsten Backup durchgeführt wurden und die maximale RTO 4 Stunden und 30 Minuten betrug.

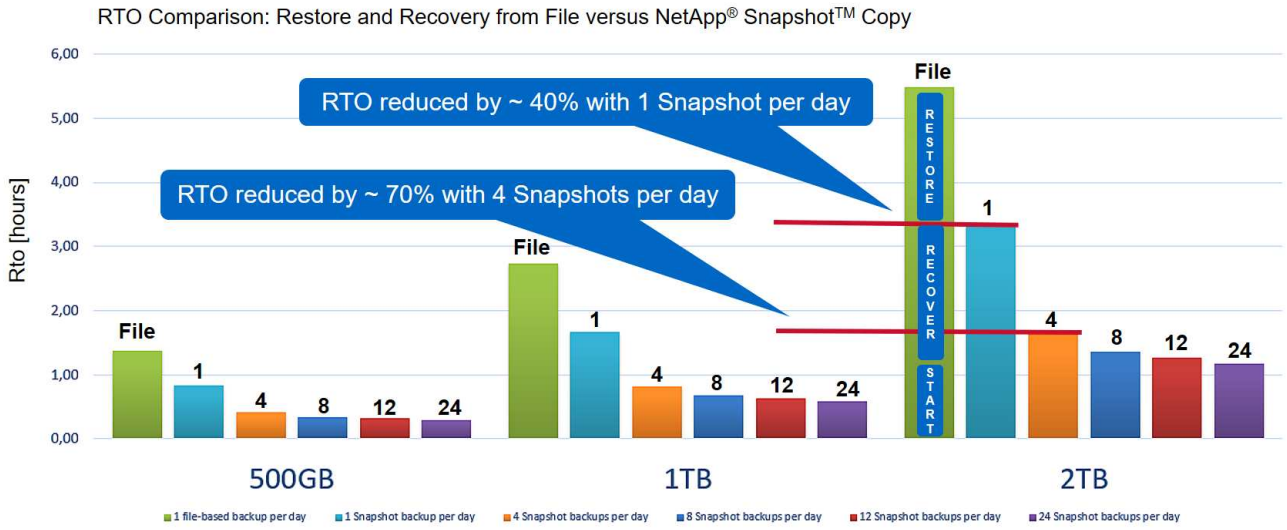


Die folgende Abbildung zeigt ein RTO-Beispiel für eine 1-TB-Datenbank, wenn Snapshot Backups verwendet werden. Bei Storage-basierten Snapshot Backups hängt die RTO nur von der Startzeit der Datenbank und der Wiederherstellungszeit ab, da die Wiederherstellung unabhängig von der Größe der Datenbank in wenigen Sekunden abgeschlossen wurde. Die Recovery-Zeit bis zur Vorwärtszeit wird auch abhängig vom Zeitpunkt der Wiederherstellung und der Wiederherstellung erhöht. Aufgrund der höheren Backup-Häufigkeit (in diesem Beispiel alle sechs Stunden) beträgt die Recovery-Zeit höchstens 43 Minuten. In diesem Beispiel beträgt die maximale RTO 1 Stunde und 13 Minuten.



Die folgende Abbildung zeigt einen RTO-Vergleich von dateibasierten und Storage-basierten Snapshot Backups für unterschiedliche Datenbankgrößen und verschiedene Häufigkeit von Snapshot-Backups. Der grüne Balken zeigt das dateibasierte Backup an. Die anderen Balken zeigen Backups von Snapshot Kopien mit unterschiedlichen Backup-Frequenzen.

Bei einem Daten-Backup pro Tag einer einzelnen Snapshot Kopie ist die RTO im Vergleich zu einem dateibasierten Daten-Backup bereits um 40 % reduziert. Die Reduzierung beträgt 70 %, wenn vier Snapshot-Backups pro Tag erstellt werden. Die Abbildung zeigt auch, dass die Kurve konstant bleibt, wenn die Snapshot-Backup-Frequenz auf mehr als vier bis sechs Snapshot-Backups pro Tag erhöht wird. Unsere Kunden konfigurieren daher typischerweise vier bis sechs Snapshot Backups pro Tag.



Assumptions: Restore from file with 250MB/sec; database start with 400MB/s; log files per day: 50% of database size; forward recovery with 250MB/sec

Das Diagramm zeigt die RAM-Größe des HANA-Servers. Die Größe der Datenbank im Arbeitsspeicher wird auf die Hälfte des Server-RAM-Größen berechnet.

Die Restore- und Recovery-Zeit wird anhand folgender Annahmen berechnet. Die Datenbank kann mit 250 MBit/s wiederhergestellt werden. Die Anzahl der Log-Dateien pro Tag beträgt 50 % der Datenbankgröße. Beispielsweise erstellt eine Datenbank mit 1 TB 500MB an Log-Dateien pro Tag. Eine Wiederherstellung kann mit 100 Mbit/s durchgeführt werden.

Architektur von SnapCenter

SnapCenter ist eine einheitliche, skalierbare Plattform für applikationskonsistente Datensicherung. SnapCenter bietet zentrale Kontrolle und Überwachung und delegiert die Möglichkeit, dass Benutzer applikationsspezifische Backup-, Restore- und Klonaufgaben managen können. Mit SnapCenter erhalten Datenbank- und Storage-Administratoren ein Tool, mit dem sie Backup-, Wiederherstellungs- und Klonvorgänge für verschiedene Applikationen und Datenbanken managen können.

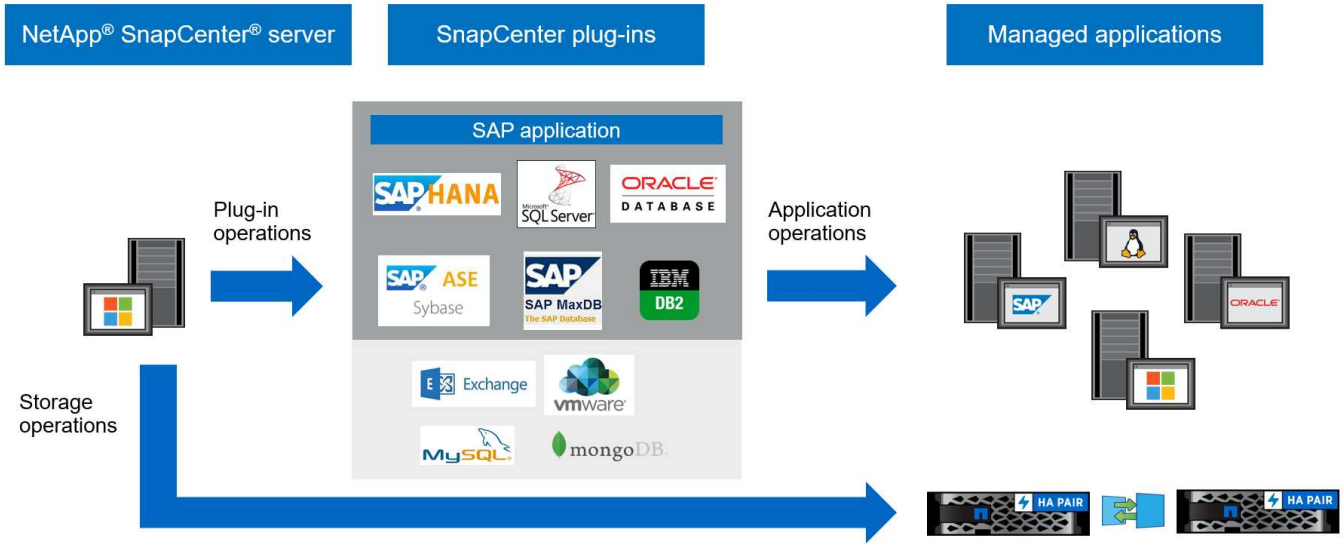
SnapCenter managt Daten über Endpunkte in der Data-Fabric-Architektur von NetApp hinweg. Daten können mit SnapCenter zwischen lokalen Umgebungen, zwischen On-Premises-Umgebungen und der Cloud sowie zwischen Private, Hybrid oder Public Clouds repliziert werden.

Komponenten von SnapCenter

SnapCenter umfasst den SnapCenter-Server, das SnapCenter-Plug-in-Paket für Windows und das SnapCenter-Plug-ins-Paket für Linux. Jedes Paket enthält SnapCenter-Plug-ins für diverse Applikations- und Infrastrukturkomponenten.

Mit den benutzerdefinierten SnapCenter Plug-ins können Sie Ihre eigenen Plug-ins erstellen und Ihre Applikation über dieselbe SnapCenter Oberfläche schützen.

In der folgenden Abbildung sind die SnapCenter Komponenten dargestellt.



SnapCenter SAP HANA Backup-Lösung

In diesem Abschnitt werden die Komponenten, unterstützte SAP HANA-Versionen und -Konfigurationen sowie in dieser Lösung verwendete Verbesserungen von SnapCenter 4.6 aufgeführt.

Lösungskomponenten

Die SnapCenter Backup-Lösung für SAP HANA umfasst folgende Bereiche:

- SAP HANA Daten-Backup mit Storage-basierten Snapshot Kopien:
  - Backup-Planung
  - Retentionmanagement
  - Allgemeine Ordnung und Sauberkeit des SAP HANA Backup-Katalogs
- Nicht-Datenvolumen (z. B. `/hana/shared`) Backup mit Storage-basierten Snapshot Kopien:
  - Backup-Planung
  - Retentionmanagement
- Replizierung an externe Backups oder Disaster-Recovery-Standorte:
  - Backup von SAP HANA Daten-Snapshots
  - Kein Datenvolumen

    - Aufbewahrungsmanagement wird auf externen Backup-Speichern konfiguriert
    - Allgemeine Ordnung und Sauberkeit des SAP HANA Backup-Katalogs
- Integritätsprüfungen der Datenbankblöcke mithilfe eines dateibasierten Backups:
    - Backup-Planung
    - Retentionmanagement
    - Allgemeine Ordnung und Sauberkeit des SAP HANA Backup-Katalogs
- Aufbewahrungsmanagement von HANA-Datenbankprotokoll-Backup:
    - Retentionmanagement basierend auf der Aufbewahrung von Daten-Backups
    - Allgemeine Ordnung und Sauberkeit des SAP HANA Backup-Katalogs
- Automatische Erkennung von HANA-Datenbanken
- Automatisiertes Restore und Recovery
- Restore einzelner Mandanten mit SAP HANA mandantenfähigen Datenbank-Containern (MDC) Systemen

Backups von Datenbankdateien werden von SnapCenter in Kombination mit dem Plug-in für SAP HANA ausgeführt. Das Plug-in löst einen Speicherpunkt für das SAP HANA Datenbank-Backup aus, sodass die Snapshot Kopien, die auf dem primären Storage-System erstellt werden, auf einem konsistenten Image der SAP HANA Datenbank basieren.

SnapCenter ermöglicht die Replizierung konsistenter Datenbank-Images an einen externen Backup- oder Disaster-Recovery-Standort mithilfe von SnapVault oder NetApp SnapMirror. Merkmal: In der Regel werden verschiedene Aufbewahrungsrichtlinien für Backups auf dem primären und externen Backup-Storage definiert. SnapCenter übernimmt die Aufbewahrung im Primärspeicher und ONTAP übernimmt die Aufbewahrung auf dem externen Backup-Storage.

Für ein vollständiges Backup aller mit SAP HANA verbundenen Ressourcen ermöglicht SnapCenter zudem das Backup aller nicht aus Daten stammenden Volumes über das SAP HANA Plug-in mit Storage-basierten Snapshot Kopien. Nicht vorhandene Datenvolumen können unabhängig vom Datenbank-Daten-Backup geplant werden, um individuelle Aufbewahrungs- und Sicherungsrichtlinien zu ermöglichen.

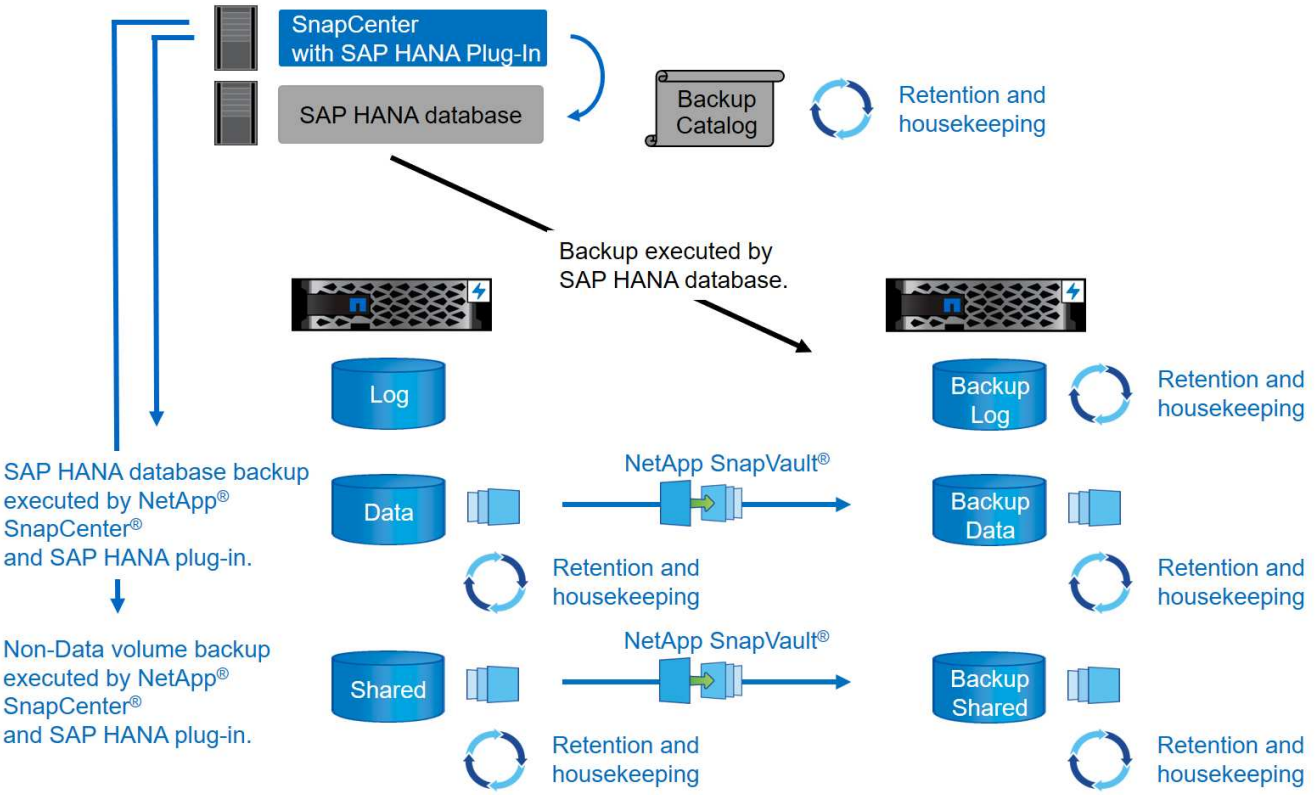
Die SAP HANA Datenbank führt automatisch Protokoll-Backups aus. Abhängig von den Vorgaben für Recovery-Zeitpunkte gibt es mehrere Optionen für den Speicherort der Log-Backups:

- Das Protokoll-Backup wird auf ein Storage-System geschrieben, das die Daten mithilfe der NetApp MetroCluster Storage-Software (HA) und Disaster Recovery synchron an einen zweiten Standort spiegelt.
- Das Protokoll-Backup-Ziel kann auf demselben primären Storage-System konfiguriert und dann mit SnapMirror synchron oder asynchron auf einen sekundären Storage repliziert werden.
- Das Backup-Ziel für das Protokoll kann auf demselben externen Backup-Storage konfiguriert werden, in dem die Datenbank-Backups mit SnapVault repliziert werden. Mit dieser Konfiguration stellt der externe Backup-Storage Verfügbarkeitsanforderungen wie den des primären Storage dar, sodass Log-Backups auf den externen Backup-Storage geschrieben werden können.

SAP empfiehlt, Storage-basierte Snapshot-Backups mit einem wöchentlichen dateibasierten Backup zu kombinieren, um eine Integritätsprüfung für Blöcke durchzuführen. Die Blockintegritätsprüfung kann innerhalb von SnapCenter ausgeführt werden. Basierend auf Ihren konfigurierbaren Aufbewahrungsrichtlinien managt SnapCenter die allgemeine Ordnung und Sauberkeit der Datendatei-Backups auf dem Primärspeicher, Backup von Protokolldateien und den SAP HANA Backup-Katalog.

SnapCenter übernimmt die Aufbewahrung im Primärspeicher, während ONTAP die sekundäre Backup-Aufbewahrung managt.

Die folgende Abbildung zeigt eine Übersicht über die Datenbank- und Backup-Protokollierungs-Konfiguration, bei der die Protokoll-Backups auf einen NFS Mount des externen Backup-Storage geschrieben werden.



Bei der Ausführung eines Storage-basierten Snapshot-Backups von Volumes ohne Daten führt SnapCenter die folgenden Aufgaben aus:

1. Erstellung einer Storage-Snapshot-Kopie des nicht-Daten-Volumes
2. Ausführung eines SnapVault- oder SnapMirror-Updates für das Daten-Volume, falls konfiguriert
3. Löschen von Storage-Snapshot-Kopien im primären Storage auf Grundlage der festgelegten Aufbewahrungsrichtlinie.

Beim Ausführen eines Storage-basierten Snapshot Backups der SAP HANA Datenbank führt SnapCenter die folgenden Aufgaben durch:

1. Erstellung eines SAP HANA-Speicherpunktes für Backups, um ein konsistentes Image auf der Persistenzschicht zu erstellen.
2. Erstellung einer Storage-Snapshot-Kopie des Daten-Volumes
3. Registrierung des Storage-Snapshot-Backups im SAP HANA-Backup-Katalog
4. Veröffentlichung des Speicherpunktes SAP HANA Backup
5. Ausführung eines SnapVault- oder SnapMirror-Updates für das Daten-Volume, falls konfiguriert
6. Löschen von Storage-Snapshot-Kopien im primären Storage auf Grundlage der festgelegten Aufbewahrungsrichtlinie.

7. Löschen der Einträge des SAP HANA Backup-Katalogs, wenn die Backups nicht mehr im primären oder externen Backup-Speicher vorhanden sind.
8. Sobald ein Backup auf Grundlage der Aufbewahrungsrichtlinie oder manuell gelöscht wurde, löscht SnapCenter alle Log-Backups, die älter als das älteste Daten-Backup sind. Log-Backups werden im Dateisystem und im SAP HANA Backup-Katalog gelöscht.

Unterstützte SAP HANA-Versionen und -Konfigurationen

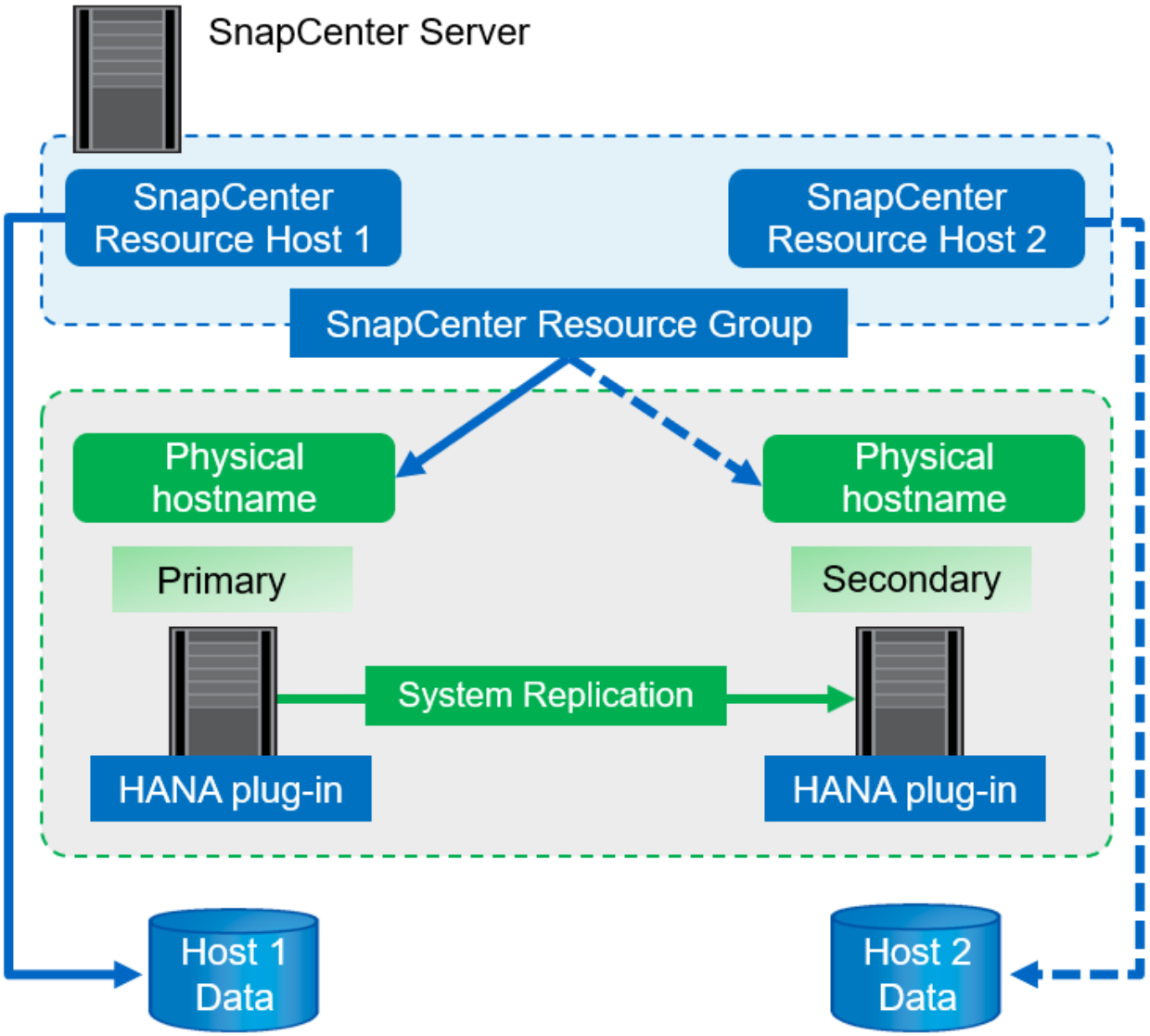
SnapCenter unterstützt SAP HANA Einzel- und Konfigurationen für mehrere Hosts über NFS- oder FC-Attached NetApp Storage-Systeme (AFF und FAS) sowie SAP HANA Systeme, die auf Cloud Volumes ONTAP bei AWS, Azure, der Google Cloud Platform und AWS FSX ONTAP über NFS ausgeführt werden.

SnapCenter unterstützt die folgenden SAP HANA-Architekturen und -Releases:

- SAP HANA Single-Container: SAP HANA 1.0 SPS12
- SAP HANA mandantenfähige Datenbank-Container (MDC) mit einem Mandanten: SAP HANA 2.0 SPS3 und höher
- SAP HANA mandantenfähige Datenbank-Container (MDC) mehrere Mandanten: SAP HANA 2.0 SPS4 und höher

Verbesserungen von SnapCenter 4.6

Ab Version 4.6 unterstützt SnapCenter die automatische Erkennung von HANA-Systemen, die in einer HANA-System-Replizierungsbeziehung konfiguriert sind. Jeder Host wird mit seiner physischen IP-Adresse (Host-Name) und seinem individuellen Daten-Volume auf der Storage-Ebene konfiguriert. Die beiden SnapCenter Ressourcen werden in einer Ressourcengruppe kombiniert, SnapCenter erkennt automatisch, welcher Host sich auf einem primären oder sekundären Server befindet, und führt dann die erforderlichen Backup-Vorgänge entsprechend aus. Das Aufbewahrungsmanagement für Snapshot und dateibasierte Backups, die mit SnapCenter erstellt wurden, erfolgt über beide Hosts hinweg, sodass sichergestellt ist, dass alte Backups auch am aktuellen sekundären Host gelöscht werden. Die folgende Abbildung bietet einen allgemeinen Überblick. Eine detaillierte Beschreibung der Konfiguration und des Betriebs von HANA-System-Replication-fähigen HANA-Systemen in SnapCenter finden Sie in "TR-4719 SAP HANA System Replication, Backup und Recovery mit SnapCenter".



SnapCenter-Konzepte und Best Practices

In diesem Abschnitt werden die SnapCenter-Konzepte und Best Practices im Zusammenhang mit der Konfiguration und Implementierung von SAP HANA-Ressourcen beschrieben.

Optionen und Konzepte für die Konfiguration von SAP HANA Ressourcen

Mit SnapCenter kann die Konfiguration von SAP HANA Datenbankressourcen mit zwei verschiedenen Ansätzen durchgeführt werden.

- **Manuelle Ressourcenkonfiguration.** HANA Ressourcen- und Speicherplatzinformationen müssen manuell bereitgestellt werden.
- **Automatische Erkennung von HANA-Ressourcen.** Automatische Erkennung vereinfacht die Konfiguration von HANA-Datenbanken in SnapCenter und ermöglicht automatisiertes Restore und Recovery.

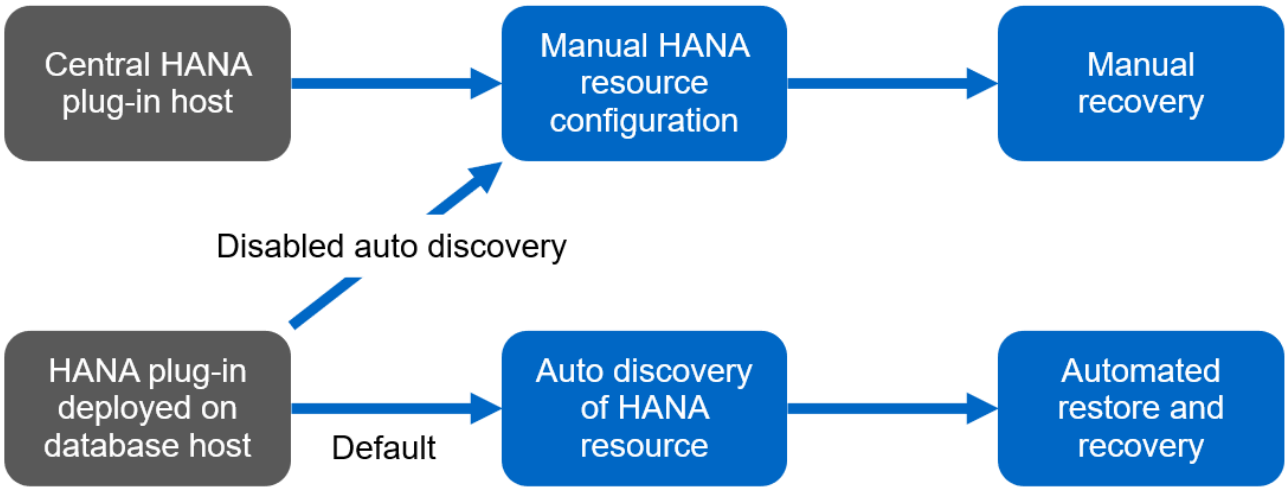
Dabei ist es wichtig zu wissen, dass nur HANA-Datenbankressourcen in SnapCenter aktiviert sind, die

automatisch erkannt wurden, für automatisierte Wiederherstellungen und Recoverys. HANA-Datenbankressourcen, die in SnapCenter manuell konfiguriert sind, müssen nach einer Wiederherstellung in SnapCenter manuell wiederhergestellt werden.

Andererseits wird die automatische Erkennung mit SnapCenter nicht für alle HANA-Architekturen und Infrastrukturkonfigurationen unterstützt. Daher erfordern HANA-Landschaften einen gemischten Ansatz, bei dem für einige HANA-Systeme (HANA mehrere Hostsysteme) eine manuelle Ressourcenkonfiguration erforderlich ist, und alle anderen Systeme können mithilfe der automatischen Erkennung konfiguriert werden.

Die automatische Erkennung und die automatisierte Wiederherstellung und Wiederherstellung hängen von der Möglichkeit ab, OS-Befehle auf dem Datenbank-Host auszuführen. Beispiele hierfür sind die Ermittlung des Platzbedarfs für Filesystem und Storage sowie die Unmount-, Mount- oder LUN-Erkennung. Diese Vorgänge werden mit dem SnapCenter Linux Plug-in ausgeführt, das gemeinsam mit dem HANA-Plug-in automatisch implementiert wird. Daher ist es Voraussetzung, das HANA-Plug-in auf dem Datenbank-Host zu implementieren, um automatische Erkennung sowie automatisiertes Restore und Recovery zu ermöglichen. Es ist auch möglich, die automatische Erkennung nach der Bereitstellung des HANA-Plug-ins auf dem Datenbank-Host zu deaktivieren. In diesem Fall handelt es sich bei der Ressource um eine manuell konfigurierte Ressource.

In der folgenden Abbildung sind die Abhängigkeiten zusammengefasst. Weitere Einzelheiten zu den HANA-Implementierungsoptionen finden Sie im Abschnitt „Bereitstellungsoptionen für das SAP HANA-Plug-in“.



Die HANA- und Linux-Plug-ins sind derzeit nur für Systeme mit Intel-Technik verfügbar. Falls die HANA-Datenbanken auf IBM Power Systems laufen, muss ein zentraler HANA-Plug-in-Host verwendet werden.

Unterstützte HANA-Architekturen für automatisches Discovery und automatisiertes Recovery

Mit SnapCenter werden automatische Erkennung und automatisierte Wiederherstellung und Recovery für die meisten HANA-Konfigurationen unterstützt, mit der Ausnahme, dass für HANA mehrere Host-Systeme eine manuelle Konfiguration erforderlich ist.

Die folgende Tabelle zeigt die unterstützten HANA-Konfigurationen für die automatische Erkennung.

HANA-Plug-in installiert auf:	HANA-Architektur	HANA-Systemkonfiguration	Infrastruktur
HANA Datenbank-Host	Einzelner Host	• HANA-einzelner Container • Mandantenfähige SAP HANA Datenbank-Container (MDC) mit einzelnen oder mehreren Mandanten • HANA System Replication	• Bare Metal mit NFS • Bare Metal mit XFS und FC mit oder ohne Linux Logical Volume Manager (LVM) • VMware mit direkt-Betriebssystem-NFS-Mounts

HANA MDC-Systeme mit mehreren Mandanten werden für automatische Erkennung unterstützt, nicht jedoch für automatisiertes Restore und Recovery mit der aktuellen SnapCenter-Version.

Unterstützte HANA-Architekturen für manuelle HANA-Ressourcenkonfiguration

Die manuelle Konfiguration von HANA-Ressourcen wird für alle HANA-Architekturen unterstützt, erfordert jedoch einen zentralen HANA-Plug-in-Host. Der zentrale Plug-in-Host kann der SnapCenter-Server selbst oder ein separater Linux- oder Windows-Host sein.

Wenn das HANA-Plug-in auf dem HANA-Datenbank-Host implementiert wird, wird die Ressource standardmäßig automatisch erkannt. Die automatische Erkennung kann für einzelne Hosts deaktiviert werden, sodass das Plug-in bereitgestellt werden kann. Beispielsweise auf einem Datenbank-Host mit aktivierter HANA-Systemreplizierung und einer SnapCenter-Version < 4.6, bei der die automatische Erkennung nicht unterstützt wird. Weitere Informationen finden Sie im Abschnitt "„Automatische Erkennung auf dem HANA-Plug-in-Host deaktivieren.“"

Die folgende Tabelle zeigt die unterstützten HANA-Konfigurationen für die manuelle HANA-Ressourcenkonfiguration.

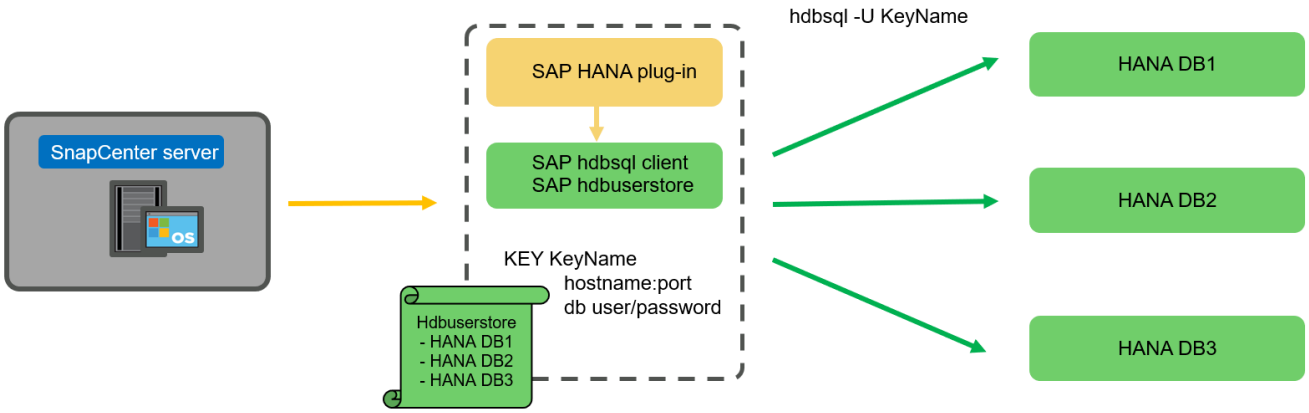
HANA-Plug-in installiert auf:	HANA-Architektur	HANA-Systemkonfiguration	Infrastruktur
Zentraler Plug-in-Host (SnapCenter-Server oder separater Linux-Host)	Single oder mehrere Hosts	• HANA-einzelner Container • HANA MDC mit einzelnen oder mehreren Mandanten • HANA System Replication	• Bare Metal mit NFS • Bare Metal mit XFS und FC mit oder ohne Linux LVM • VMware mit direkt-Betriebssystem-NFS-Mounts

Implementierungsoptionen für das SAP HANA Plug-in

Die folgende Abbildung zeigt die logische Ansicht und die Kommunikation zwischen dem SnapCenter Server und den SAP HANA Datenbanken.

Der SnapCenter-Server kommuniziert über das SAP HANA Plug-in mit den SAP HANA Datenbanken. Das

SAP HANA Plug-in nutzt die SAP HANA hdbsql-Client-Software, um SQL-Befehle an die SAP HANA-Datenbanken auszuführen. Der SAP HANA hdbuserstore wird verwendet, um die Benutzeranmeldeinformationen, den Hostnamen und die Portinformationen für den Zugriff auf die SAP HANA-Datenbanken bereitzustellen.



Das SAP HANA-Plug-in und die SAP-hdbsql-Client-Software, zu der auch das hdbuserstore-Konfigurationstool gehört, müssen auf demselben Host zusammen installiert werden.

Der Host kann entweder der SnapCenter-Server selbst, ein separater zentraler Plug-in-Host oder die einzelnen SAP HANA Datenbank-Hosts sein.

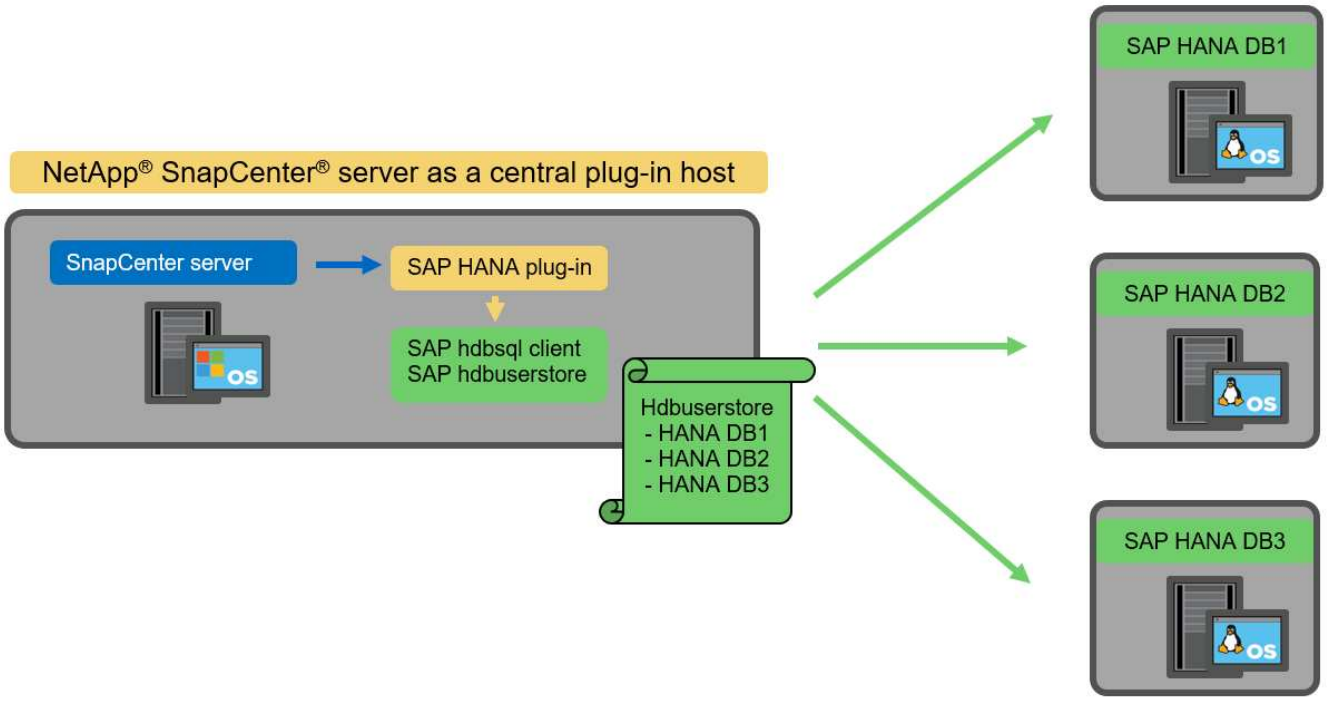
Hochverfügbarkeit mit SnapCenter Server

SnapCenter kann in einer HA-Konfiguration mit zwei Nodes eingerichtet werden. In dieser Konfiguration wird ein Load Balancer (z. B. F5) unter Verwendung einer virtuellen IP-Adresse verwendet, die auf den aktiven SnapCenter-Host verweist. Das SnapCenter-Repository (die MySQL-Datenbank) wird von SnapCenter zwischen den beiden Hosts repliziert, sodass die SnapCenter-Daten immer synchron sind.

SnapCenter Server HA wird nicht unterstützt, wenn das HANA-Plug-in auf dem SnapCenter-Server installiert ist. Wenn Sie SnapCenter in einer HA-Konfiguration einrichten möchten, installieren Sie das HANA Plug-in nicht auf dem SnapCenter Server. Weitere Informationen zur SnapCenter HA finden Sie unter diesem "NetApp Knowledge Base Seite".

SnapCenter Server als zentraler HANA Plug-in-Host

Die folgende Abbildung zeigt eine Konfiguration, in der der SnapCenter-Server als zentraler Plug-in-Host verwendet wird. Das SAP HANA Plug-in und die SAP hdbsql-Client-Software sind auf dem SnapCenter-Server installiert.



Da das HANA-Plug-in mit den gemanagten HANA-Datenbanken über den hdbclient über das Netzwerk kommunizieren kann, müssen keine SnapCenter-Komponenten auf den einzelnen HANA-Datenbank-Hosts installiert werden. SnapCenter kann die HANA-Datenbanken über einen zentralen HANA Plug-in-Host sichern, auf dem alle Benutzerspeicherschlüssel für die gemanagten Datenbanken konfiguriert sind.

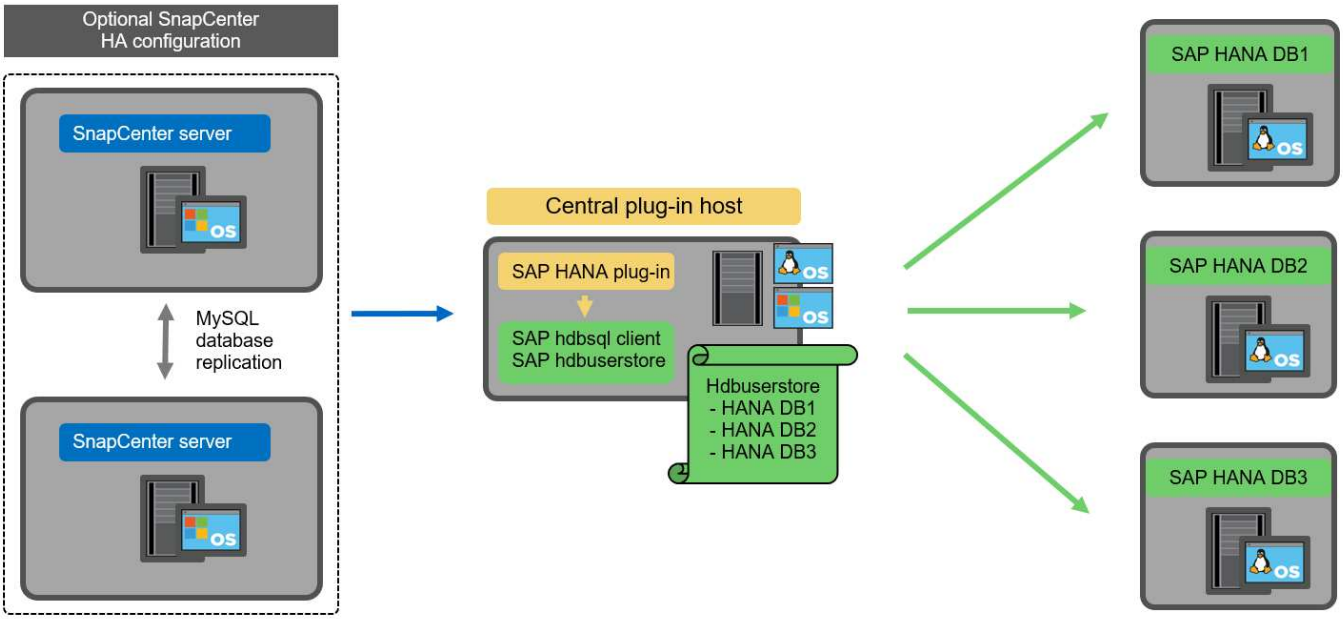
Um dagegen die Workflow-Automatisierung für die automatische Erkennung, die Automatisierung von Wiederherstellung und Wiederherstellung sowie die Aktualisierung von SAP Systemen zu verbessern, müssen auf dem Datenbank-Host SnapCenter Komponenten installiert werden. Bei Verwendung eines zentralen HANA-Plug-in-Hosts sind diese Funktionen nicht verfügbar.

Darüber hinaus kann die Hochverfügbarkeit des SnapCenter-Servers mit der in-Build-HA-Funktion nicht verwendet werden, wenn das HANA-Plug-in auf dem SnapCenter-Server installiert ist. Hochverfügbarkeit kann mit VMware HA erzielt werden, wenn der SnapCenter Server auf einer VM innerhalb eines VMware Clusters ausgeführt wird.

Separater Host als zentraler HANA Plug-in-Host

Die folgende Abbildung zeigt eine Konfiguration, in der ein separater Linux-Host als zentraler Plug-in-Host verwendet wird. In diesem Fall sind das SAP HANA Plug-in und die SAP hdbsql-Client-Software auf dem Linux-Host installiert.

Der separate zentrale Plug-in-Host kann auch ein Windows-Host sein.

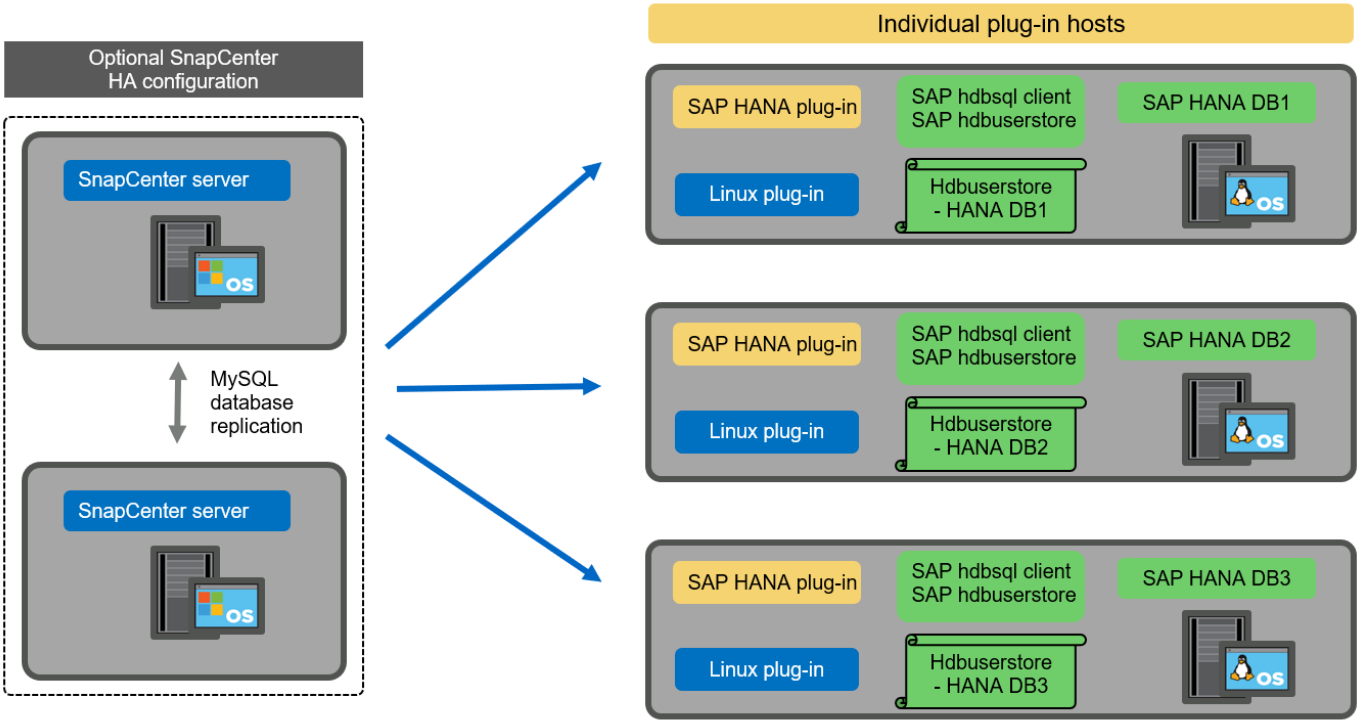


Die gleiche Einschränkung hinsichtlich der im vorherigen Abschnitt beschriebenen Funktionsverfügbarkeit gilt auch für einen separaten zentralen Plug-in Host.

Bei dieser Implementierungsoption kann der SnapCenter Server jedoch mit den in-Build-HA-Funktionen konfiguriert werden. Auch der zentrale Plug-in-Host muss HA sein, beispielsweise durch Verwendung einer Linux-Cluster-Lösung.

Auf einzelnen HANA-Datenbank-Hosts implementiertem HANA Plug-in

Die folgende Abbildung zeigt eine Konfiguration, in der das SAP HANA Plug-in auf jedem SAP HANA Datenbank-Host installiert ist.



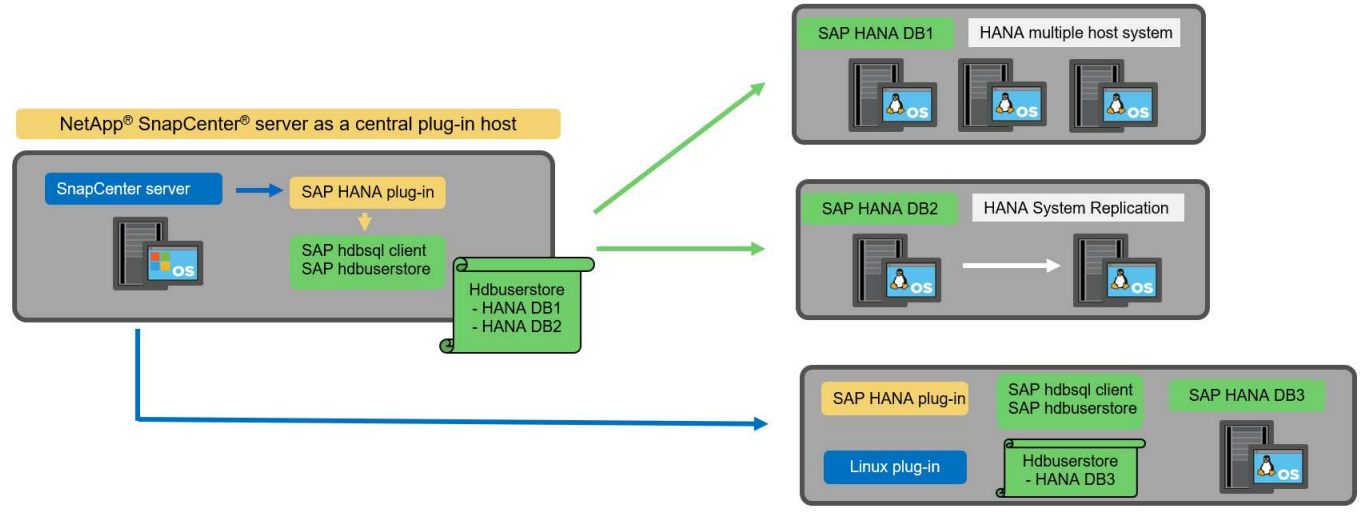
Wird das HANA-Plug-in auf jedem einzelnen HANA-Datenbank-Host installiert, sind alle Funktionen verfügbar, beispielsweise automatische Erkennung, automatisiertes Restore und Recovery. Zudem kann der SnapCenter Server in einer HA-Konfiguration eingerichtet werden.

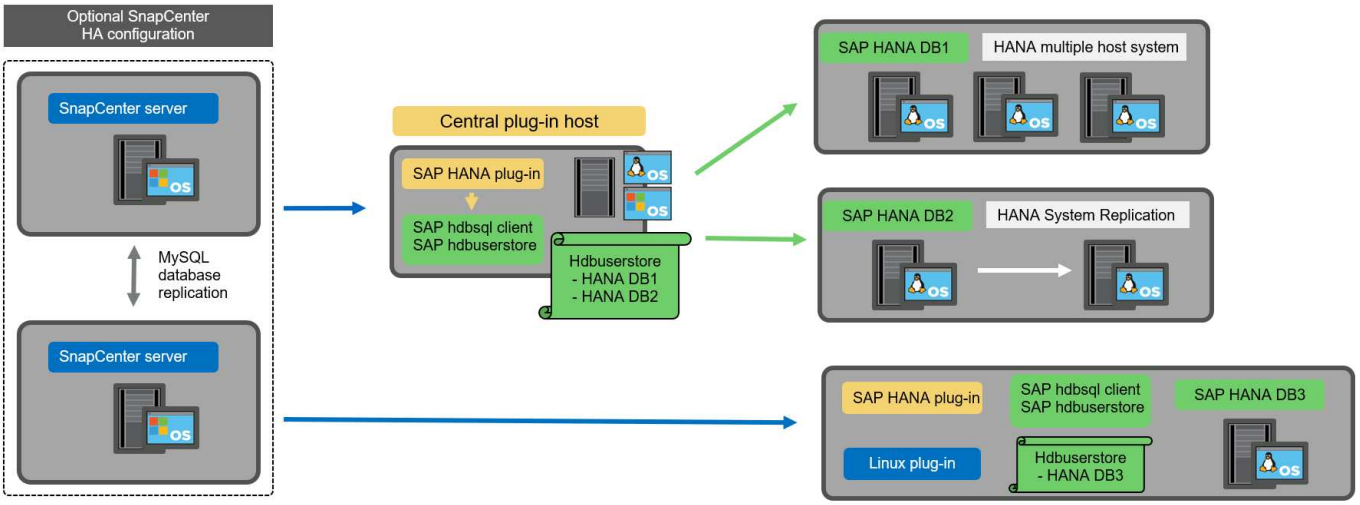
Plug-in-Implementierung für heterogene HANA

Wie zu Beginn dieses Abschnitts erläutert, erfordern einige HANA-Systemkonfigurationen, wie z. B. Systeme mit mehreren Hosts, einen zentralen Plug-in-Host. Daher erfordern die meisten SnapCenter Konfigurationen eine gemischte Implementierung des HANA Plug-ins.

NetApp empfiehlt, das HANA Plug-in auf dem HANA-Datenbank-Host für alle HANA-Systemkonfigurationen zu implementieren, die zur automatischen Erkennung unterstützt werden. Andere HANA-Systeme, wie beispielsweise Konfigurationen mit mehreren Hosts, sollten mit einem zentralen HANA Plug-in-Host gemanagt werden.

Die folgenden beiden Abbildungen zeigen gemischte Plug-in-Bereitstellungen entweder mit dem SnapCenter-Server oder einem separaten Linux-Host als zentralen Plug-in-Host. Der einzige Unterschied zwischen diesen beiden Implementierungen ist die optionale HA-Konfiguration.





Zusammenfassung und Empfehlungen

Im Allgemeinen empfiehlt NetApp die Implementierung des HANA Plug-ins auf jedem SAP HANA Host, um alle verfügbaren SnapCenter HANA Funktionen zu aktivieren und die Workflow-Automatisierung zu verbessern.

> Die HANA- und Linux-Plug-ins sind derzeit nur für Systeme mit Intel-Technik verfügbar. Falls die HANA-Datenbanken auf IBM Power Systems laufen, muss ein zentraler HANA-Plug-in-Host verwendet werden.

Für HANA-Konfigurationen, bei denen keine automatische Erkennung wie HANA-Konfigurationen mit mehreren Hosts unterstützt wird, muss ein zusätzlicher zentraler HANA-Plug-in-Host konfiguriert werden. Der zentrale Plug-in-Host kann der SnapCenter Server sein, wenn VMware HA für SnapCenter HA genutzt werden kann. Wenn Sie die im Build-HA-Funktion von SnapCenter verwenden möchten, verwenden Sie einen separaten Linux-Plug-in-Host.

In der folgenden Tabelle sind die verschiedenen Implementierungsoptionen aufgeführt.

Implementierungsoptionen	Abhängigkeiten
Zentrales HANA-Plug-in-Host-Plug-in auf SnapCenter-Server installiert	Vorteile: * Single HANA Plug-in, zentrale HDB User Store-Konfiguration * auf einzelnen HANA-Datenbank-Hosts werden keine SnapCenter-Softwarekomponenten benötigt * Unterstützung aller HANA-Architekturen Cons: * Manuelle Ressourcenkonfiguration * Manuelle Wiederherstellung * keine Unterstützung für die Wiederherstellung einzelner Mandanten * Alle Pre- und Post-Script-Schritte werden auf dem zentralen Plug-in-Host ausgeführt * in-Build SnapCenter Hochverfügbarkeit nicht unterstützt * Kombination von SID und Mandantenname muss für alle verwalteten HANA-Datenbanken eindeutig sein * Protokoll Für alle gemanagten HANA-Datenbanken ist das Backup-Aufbewahrungsmanagement aktiviert/deaktiviert
Zentrales HANA-Plug-in-Host-Plug-in auf separatem Linux- oder Windows-Server installiert	Vorteile: * Single HANA Plug-in, zentrale HDB User Store-Konfiguration * Keine SnapCenter Software-Komponenten erforderlich auf einzelnen HANA-Datenbank-Hosts * Unterstützung aller HANA-Architekturen * in-Build SnapCenter Hochverfügbarkeit unterstützt Cons: * Manuelle Ressourcenkonfiguration * Manuelle Wiederherstellung * keine Unterstützung für die Wiederherstellung einzelner Mandanten * Alle Pre- und Post-Script-Schritte werden auf dem zentralen Plug-in-Host ausgeführt * Kombination von SID und Mandantenname muss für alle verwalteten HANA-Datenbanken eindeutig sein * Protokoll Backup Aufbewahrungsmanagement aktiviert/deaktiviert für alle gemanagt HANA-Datenbanken

Implementierungsoptionen	Abhängigkeiten
Auf dem HANA-Datenbankserver wird ein individuelles HANA-Plug-in-Host-Plug-in installiert	Vorteile: * Automatische Bestandsaufnahme von HANA-Ressourcen * automatisierte Wiederherstellung und Recovery * Wiederherstellung einzelner Mandanten * vorab- und Postscript-Automatisierung für SAP Systemaktualisierung * in-Build SnapCenter Hochverfügbarkeit unterstützt * Backup-Aufbewahrungsmanagement für Protokoll kann für jede einzelne HANA-Datenbank aktiviert/deaktiviert werden Cons: * Nicht unterstützt für alle HANA-Architekturen. Zusätzlicher zentraler Plug-in-Host für HANA mehrere Host-Systeme erforderlich * HANA-Plug-in muss auf jedem HANA-Datenbank-Host implementiert werden

Datensicherung Strategie

Vor der Konfiguration von SnapCenter und dem SAP HANA Plug-in muss die Datensicherungsstrategie auf Grundlage der RTO- und RPO-Anforderungen der verschiedenen SAP Systeme definiert werden.

Ein gemeinsamer Ansatz besteht in der Definition von Systemtypen wie Systemen für Produktion, Entwicklung, Test oder Sandbox. Alle SAP-Systeme des gleichen Systemtyps haben typischerweise die gleichen Datenschutzparameter.

Folgende Parameter müssen definiert werden:

- Wie oft sollte ein Snapshot Backup ausgeführt werden?
- Wie lange sollten Snapshot Kopien Backups auf dem Primärspeichersystem aufbewahrt werden?
- Wie oft sollte eine Blockintegritätsprüfung ausgeführt werden?
- Sollten die primären Backups auf einen externen Backup-Standort repliziert werden?
- Wie lange sollten die Backups auf dem externen Backup-Storage aufbewahrt werden?

Die folgende Tabelle zeigt ein Beispiel für die Datenschutzparameter für die Produktion, Entwicklung und Prüfung des Systemtyps. Für das Produktionssystem wurde eine hohe Backup-Frequenz definiert und die Backups werden einmal pro Tag an einen externen Backup-Standort repliziert. Die Testsysteme haben niedrigere Anforderungen und keine Replikation der Backups.

Parameter	Produktionssysteme auszuführen	Entwicklungssysteme	Testsysteme
Sicherungshäufigkeit	Alle 4 Stunden	Alle 4 Stunden	Alle 4 Stunden
Primäre Aufbewahrung	2 Tage	2 Tage	2 Tage
Block-Integritätsprüfung	Einmal in der Woche	Einmal in der Woche	Nein
Replizierung an externe Backup-Standorte	Einmal am Tag	Einmal am Tag	Nein
Externe Backup-Aufbewahrung	2 Wochen	2 Wochen	Keine Angabe

In der folgenden Tabelle werden die Richtlinien aufgeführt, die für die Datensicherheitsparameter konfiguriert

werden müssen.

Parameter	RichtlinienLocalSnap	RichtlinieLocalSnapAndSnapVault	RichtlinienBlockIntegritätPrüfung
Backup-Typ	Auf Snapshot-Basis	Auf Snapshot-Basis	File-basiert
Zeitplanhäufigkeit	Stündlich	Täglich	Wöchentlich
Primäre Aufbewahrung	Anzahl = 12	Anzahl = 3	Anzahl = 1
SnapVault Replizierung	Nein	Ja.	Keine Angabe

Richtlinie `LocalSnapshot` Werden für Produktions-, Entwicklungs- und Testsysteme verwendet, um lokale Snapshot-Backups mit einer Aufbewahrung von zwei Tagen abzudecken.

In der Konfiguration für den Ressourcenschutz wird der Zeitplan für die Systemtypen unterschiedlich definiert:

- **Produktion.** Zeitplan alle 4 Stunden.
- **Entwicklung** Zeitplan alle 4 Stunden.
- **Test.** Zeitplan alle 4 Stunden.

Richtlinie `LocalSnapAndSnapVault` Wird für die Produktions- und Entwicklungssysteme eingesetzt, um die tägliche Replizierung auf den externen Backup Storage zu decken.

In der Konfiguration für den Ressourcenschutz wird der Zeitplan für die Produktion und Entwicklung definiert:

- **Produktion.** Zeitplan jeden Tag.
- **Entwicklung.** Zeitplan jeden Tag.

Richtlinie `BlockIntegrityCheck` Wird für die Produktions- und Entwicklungssysteme verwendet, um die wöchentliche Blockintegritätsprüfung mithilfe eines dateibasierten Backups abzudecken.

In der Konfiguration für den Ressourcenschutz wird der Zeitplan für die Produktion und Entwicklung definiert:

- **Produktion.** Zeitplan jede Woche.
- **Entwicklung.** Zeitplan jede Woche.

Für jede einzelne SAP HANA Datenbank, die die externe Backup-Richtlinie nutzt, muss auf der Storage-Ebene eine Sicherungsbeziehung konfiguriert werden. Die Sicherungsbeziehung definiert, welche Volumes repliziert werden und wie die Aufbewahrung von Backups im externen Backup-Storage aufbewahrt wird.

Mit unserem Beispiel wird für jedes Produktions- und Entwicklungssystem im externen Backup-Storage eine Aufbewahrung von zwei Wochen definiert.

> In unserem Beispiel sind die Sicherungsrichtlinien und die Aufbewahrung von SAP HANA-Datenbankressourcen und die nicht-Datenvolumen-Ressourcen nicht anders.

Backup-Vorgänge

SAP führte die Unterstützung von Snapshot Backups für MDC-Mehrmandantensysteme mit HANA 2.0 SPS4 ein. SnapCenter unterstützt Snapshot-Backup-Vorgänge von HANA MDC-Systemen mit mehreren Mandanten. SnapCenter unterstützt außerdem zwei verschiedene Wiederherstellungsvorgänge eines HANA MDC-Systems. Sie können entweder das komplette System, die System-DB und alle Mandanten wiederherstellen

oder nur einen einzelnen Mandanten wiederherstellen. Es gibt einige Voraussetzungen, wenn SnapCenter die Ausführung dieser Vorgänge ermöglicht.

In einem MDC-System ist die Mandantenkonfiguration nicht unbedingt statisch. Mandanten können hinzugefügt oder Mandanten gelöscht werden. SnapCenter kann sich nicht auf die Konfiguration verlassen, die beim Hinzufügen der HANA-Datenbank zu SnapCenter erkannt wird. SnapCenter muss wissen, welche Mandanten zum Zeitpunkt der Ausführung des Backup-Vorgangs verfügbar sind.

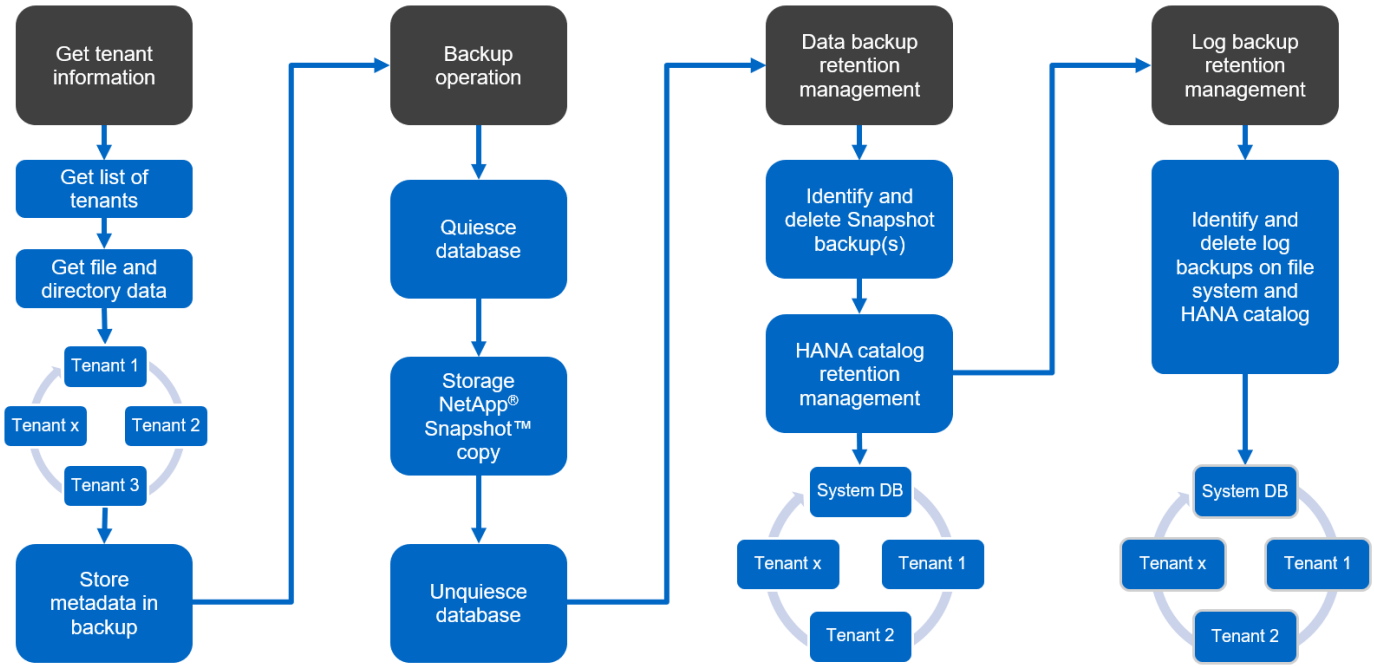
Um eine einzelne Mandanten-Wiederherstellung zu ermöglichen, muss SnapCenter wissen, welche Mandanten in jedem Snapshot-Backup enthalten sind. Zusätzlich muss die IT wissen, welche Dateien und Verzeichnisse zu den einzelnen Mandanten im Snapshot Backup gehören.

Somit müssen bei jedem Backup-Vorgang die Mandantendaten angezeigt werden. Dazu gehören die Mandantennamen und die entsprechenden Datei- und Verzeichnisinformationen. Diese Daten müssen in den Snapshot Backup-Metadaten gespeichert werden, um eine Wiederherstellung eines einzelnen Mandanten zu unterstützen. Der nächste Schritt ist der Snapshot-Backup-Vorgang selbst. Dieser Schritt umfasst den SQL-Befehl, um den HANA-Backup-Speicherpunkt auszulösen, das Storage-Snapshot-Backup und den SQL-Befehl zum Schließen des Snapshot-Vorgangs. Mit dem Befehl close aktualisiert die HANA-Datenbank den Backup-Katalog der System-DB und aller Mandanten.

SAP unterstützt keine Snapshot Backup-Vorgänge für MDC-Systeme, wenn ein oder mehrere Mandanten angehalten werden.

Für das Aufbewahrungsmanagement von Daten-Backups und das HANA-Backup-Katalogmanagement muss SnapCenter die Kataloglösch-Operationen für die Systemdatenbank und alle Mandantendatenbanken ausführen, die im ersten Schritt identifiziert wurden. Auf dieselbe Weise für die Log-Backups muss der SnapCenter-Workflow auf jedem Mandanten laufen, der Teil des Backup-Vorgangs war.

Die folgende Abbildung zeigt einen Überblick über den Backup-Workflow.



Backup-Workflow für Snapshot-Backups der HANA-Datenbank

SnapCenter sichert die SAP HANA-Datenbank in folgender Reihenfolge:

1. SnapCenter liest die Liste der Mandanten aus der HANA-Datenbank vor.
2. SnapCenter liest die Dateien und Verzeichnisse für jeden Mandanten aus der HANA-Datenbank vor.
3. Informationen zu Mandanten werden bei diesem Backup in den Metadaten von SnapCenter gespeichert.
4. SnapCenter löst einen globalen, synchronisierten Speicherpunkt für Backups von SAP HANA aus, um ein konsistentes Datenbank-Image auf der Persistenzschicht zu erstellen.

   Für ein SAP HANA MDC-System mit einem oder mehreren Mandanten wird ein synchronisierter globaler Backup-Speicherpunkt für die Systemdatenbank und für jede Mandantendatenbank erstellt.

5. SnapCenter erstellt Storage-Snapshot-Kopien für alle Daten-Volumes, die für die Ressource konfiguriert sind. In unserem Beispiel einer HANA-Datenbank mit einem einzigen Host gibt es nur ein Daten-Volume. Bei einer SAP HANA Datenbank mit mehreren Hosts sind mehrere Daten-Volumes vorhanden.
6. Das Storage Snapshot Backup wird von SnapCenter im SAP HANA Backup-Katalog registriert.
7. SnapCenter löscht den Speicherpunkt für SAP HANA-Backups.
8. SnapCenter startet ein SnapVault- oder SnapMirror-Update für alle konfigurierten Daten-Volumes in der Ressource.

   Dieser Schritt wird nur ausgeführt, wenn die ausgewählte Richtlinie eine SnapVault- oder SnapMirror-Replizierung umfasst.

9. SnapCenter löscht die Storage-Snapshot-Kopien und die Backup-Einträge in seiner Datenbank sowie im SAP HANA Backup-Katalog basierend auf der Aufbewahrungsrichtlinie, die für Backups im primären Storage definiert ist. HANA-Backup-Katalogvorgänge werden für die Systemdatenbank und alle Mandanten ausgeführt.

   Ist das Backup noch auf dem sekundären Speicher verfügbar, wird der SAP HANA-Katalogeintrag nicht gelöscht.

10. SnapCenter löscht alle Log-Backups auf dem Filesystem und im SAP HANA-Backup-Katalog, die älter als die älteste im SAP HANA-Backup-Katalog identifizierte Datensicherung sind. Diese Vorgänge werden für die Systemdatenbank und alle Mandanten durchgeführt.

    Dieser Schritt wird nur ausgeführt, wenn die allgemeine Ordnung der Protokollsicherung nicht deaktiviert ist.

Backup-Workflow für die Überprüfung der Blockintegrität

SnapCenter führt die Integritätsprüfung der Blöcke in folgender Reihenfolge aus:

1. SnapCenter liest die Liste der Mandanten aus der HANA-Datenbank vor.
2. SnapCenter löst einen dateibasierten Backup-Vorgang für die Systemdatenbank und jeden Mandanten aus.
3. SnapCenter löscht dateibasierte Backups in seiner Datenbank, im Filesystem und im SAP HANA-Backup-Katalog basierend auf der Aufbewahrungsrichtlinie, die für die Überprüfung der Blockintegrität definiert ist. Das Löschen des Backups im Filesystem und der HANA-Backup-Katalog werden für die Systemdatenbank und alle Mandanten durchgeführt.
4. SnapCenter löscht alle Log-Backups auf dem Filesystem und im SAP HANA-Backup-Katalog, die älter als

die älteste im SAP HANA-Backup-Katalog identifizierte Datensicherung sind. Diese Vorgänge werden für die Systemdatenbank und alle Mandanten durchgeführt.

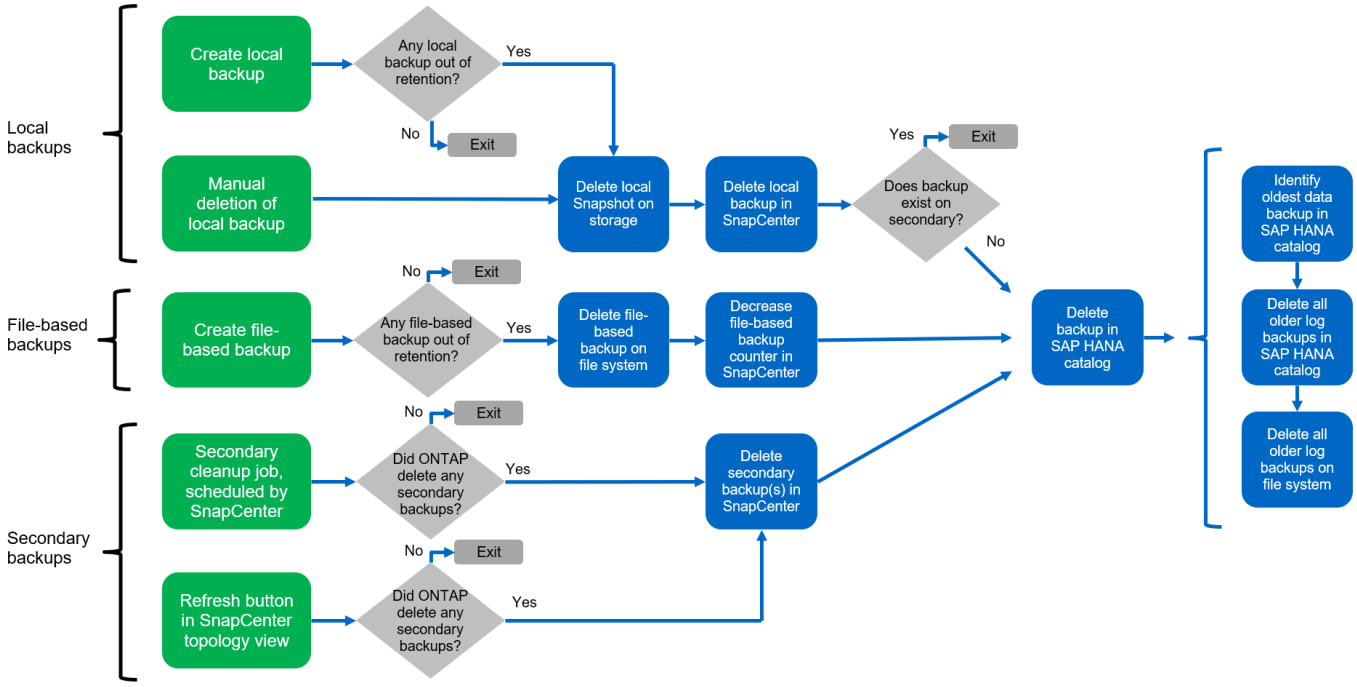
Dieser Schritt wird nur ausgeführt, wenn die allgemeine Ordnung der Protokollsicherung nicht deaktiviert ist.

Management der Backup-Aufbewahrung und allgemeine Ordnung der Daten und Backup-Protokollierung

Das Management der Daten-Backup-Aufbewahrung und die allgemeine Ordnung der Backup-Protokollierung können in fünf Hauptbereiche unterteilt werden, einschließlich Aufbewahrungsmanagement von:

- Lokale Backups im primären Storage
- Dateibasierten Backups
- Backups im sekundären Storage
- Daten-Backups im SAP HANA Backup-Katalog
- Protokollierung von Backups im SAP HANA Backup-Katalog und im Filesystem

Die folgende Abbildung bietet einen Überblick über die verschiedenen Workflows und die Abhängigkeiten jedes einzelnen Vorgangs. In den folgenden Abschnitten werden die verschiedenen Operationen im Detail beschrieben.



Aufbewahrungsmanagement von lokalen Backups auf dem Primärstorage

SnapCenter übernimmt die allgemeine Ordnung und Sauberkeit von SAP HANA Datenbank-Backups und Backups nicht-Daten-Volumes, indem Snapshot Kopien im primären Storage und im SnapCenter Repository gemäß einer in der SnapCenter Backup-Richtlinie definierten Aufbewahrung gelöscht werden.

Die Aufbewahrungsmanagement-Logik wird mit jedem Backup Workflow in SnapCenter ausgeführt.

Beachten Sie, dass SnapCenter das Aufbewahrungsmanagement für sowohl geplante als auch On-Demand-Backups individuell übernimmt.

Lokale Backups im Primärspeicher können auch manuell in SnapCenter gelöscht werden.

Aufbewahrungsmanagement von dateibasierten Backups

SnapCenter übernimmt die allgemeine Ordnung und Sauberkeit der dateibasierten Backups, indem die Backups auf dem Filesystem gemäß einer in der SnapCenter Backup Policy definierten Aufbewahrung gelöscht werden.

Die Aufbewahrungsmanagement-Logik wird mit jedem Backup Workflow in SnapCenter ausgeführt.

Beachten Sie, dass SnapCenter das Aufbewahrungsmanagement individuell für geplante oder On-Demand Backups handhabt.

Aufbewahrungsmanagement von Backups im sekundären Storage

Das Aufbewahrungsmanagement von Backups im sekundären Storage wird durch ONTAP verarbeitet, basierend auf der in der ONTAP-Sicherungsbeziehung definierten Aufbewahrung.

Zur Synchronisierung dieser Änderungen auf dem sekundären Storage im SnapCenter-Repository verwendet SnapCenter einen geplanten Bereinigungsauftrag. Dieser Bereinigungsjob synchronisiert alle sekundären Storage-Backups mit dem SnapCenter Repository für alle SnapCenter Plug-ins und alle Ressourcen.

Der Bereinigungsjob wird standardmäßig einmal pro Woche geplant. Dieser wöchentliche Zeitplan führt zu einer Verzögerung beim Löschen von Backups in SnapCenter und SAP HANA Studio im Vergleich zu den Backups, die bereits auf dem Sekundärspeicher gelöscht wurden. Um diese Inkonsistenz zu vermeiden, können Kunden den Zeitplan beispielsweise einmal pro Tag auf eine höhere Frequenz ändern.

Der Bereinigungsauftrag kann auch manuell für eine einzelne Ressource ausgelöst werden, indem Sie in der Topologieansicht der Ressource auf die Schaltfläche „Aktualisieren“ klicken.

Weitere Informationen zur Anpassung des Zeitplans des Bereinigungsjobs oder zum Auslösen einer manuellen Aktualisierung finden Sie im Abschnitt "„Change Scheduling Frequency of Backup Synchronization with off-Site Backup Storage“."

Aufbewahrungsmanagement von Daten-Backups im SAP HANA Backup-Katalog

Hat SnapCenter ein Backup, lokale Snapshots oder dateibasierte Backups gelöscht oder das Backup im sekundären Storage identifiziert, so wird dieses Daten-Backup auch im SAP HANA Backup-Katalog gelöscht.

Bevor der SAP HANA-Katalogeintrag für ein lokales Snapshot Backup im primären Storage gelöscht wird, überprüft SnapCenter, ob das Backup noch im sekundären Storage vorhanden ist.

Aufbewahrungsmanagement von Protokoll-Backups

Die SAP HANA Datenbank erstellt automatisch Protokoll-Backups. Diese Backup-Durchläufe für das Protokoll erstellen Backup-Dateien für jeden einzelnen SAP HANA Service in einem in SAP HANA konfigurierten Backup-Verzeichnis.

Log-Backups, die älter als die aktuelle Datensicherung sind, werden für die zukünftige Wiederherstellung nicht mehr benötigt und können daher gelöscht werden.

SnapCenter übernimmt die allgemeine Ordnung und Sauberkeit der Log-Datei-Backups auf Filesystem-Ebene sowie im SAP HANA Backup-Katalog, indem Sie die folgenden Schritte durchführen:

1. SnapCenter liest den SAP HANA-Backup-Katalog, um die Backup-ID des ältesten erfolgreichen dateibasierten oder Snapshot-Backups zu erhalten.
2. SnapCenter löscht alle Log-Backups im SAP HANA-Katalog und das Filesystem, die älter als diese Backup-ID sind.

> SnapCenter kümmert sich nur um die allgemeine Ordnung und Sauberkeit der Backups, die von SnapCenter erstellt wurden. Falls zusätzliche dateibasierte Backups außerhalb von SnapCenter erstellt werden, müssen Sie sicherstellen, dass die dateibasierten Backups aus dem Backup-Katalog gelöscht werden. Wird eine solche Datensicherung nicht manuell aus dem Backup-Katalog gelöscht, kann sie zur ältesten Datensicherung werden, und ältere Log-Backups werden erst gelöscht, wenn diese dateibasierte Sicherung gelöscht wird.

> Obwohl eine Aufbewahrung für On-Demand-Backups in der Richtlinienkonfiguration definiert wird, wird die allgemeine Ordnung und Sauberkeit nur dann ausgeführt, wenn ein weiteres On-Demand-Backup ausgeführt wird. Daher müssen On-Demand-Backups in der Regel manuell in SnapCenter gelöscht werden, um sicherzustellen, dass diese Backups auch im SAP HANA Backup-Katalog gelöscht werden und die allgemeine Ordnung der Protokollbackups nicht auf einem alten On-Demand-Backup basiert.

Das Backup-Aufbewahrungsmanagement für Protokolle ist standardmäßig aktiviert. Bei Bedarf kann er wie im Abschnitt beschrieben deaktiviert werden "„Automatische Erkennung auf dem HANA-Plug-in-Host deaktivieren.“"

Kapazitätsanforderungen für Snapshot Backups

Dabei müssen Sie die höhere Blockänderungsrate auf Storage-Ebene in Relation zur Änderungsrate bei herkömmlichen Datenbanken berücksichtigen. Aufgrund des HANA-Tabellen-Zusammenführungsprozesses des Spaltenspeichers wird die komplette Tabelle auf die Festplatte geschrieben, nicht nur die geänderten Blöcke.

Die Daten unseres Kundenstamms zeigen eine tägliche Änderungsrate zwischen 20 % und 50 %, wenn mehrere Snapshot-Backups während des Tages erstellt werden. Wenn beim SnapVault-Ziel die Replizierung nur einmal pro Tag durchgeführt wird, ist die tägliche Änderungsrate in der Regel kleiner.

Restore- und Recovery-Vorgänge

Wiederherstellung von Vorgängen mit SnapCenter

Aus Sicht der HANA-Datenbank unterstützt SnapCenter zwei verschiedene Restore-Vorgänge.

- **Wiederherstellung der gesamten Ressource.** Alle Daten des HANA-Systems sind wiederhergestellt. Enthält das HANA-System einen oder mehrere Mandanten, werden die Daten der Systemdatenbank und die Daten aller Mandanten wiederhergestellt.
- **Restore eines einzelnen Mieters.** nur die Daten des ausgewählten Mieters werden wiederhergestellt.

In Bezug auf Storage müssen die oben genannten Restore-Vorgänge unterschiedlich durchgeführt werden, abhängig vom verwendeten Storage-Protokoll (NFS oder Fibre Channel SAN), der konfigurierten Datensicherung (Primärstorage mit oder ohne externen Backup-Storage). Und das ausgewählte Backup, das für den Wiederherstellungsvorgang verwendet werden soll (Wiederherstellung vom primären oder externen Backup-Storage).

Wiederherstellung vollständiger Ressourcen aus dem primären Storage

Beim Wiederherstellen der gesamten Ressource aus dem primären Speicher unterstützt SnapCenter zwei verschiedene ONTAP Funktionen zum Ausführen des Wiederherstellungsvorgangs. Sie können zwischen den folgenden beiden Funktionen wählen:

- **Volume-basierte SnapRestore.** Ein Volume-basierter SnapRestore setzt den Inhalt des Speichervolumens in den Status des ausgewählten Snapshot Backups zurück.
  - Das Kontrollkästchen zur Zurücksetzen von Volumes ist verfügbar für automatisch erkannte Ressourcen mithilfe von NFS.
  - Aktivieren Sie das Optionsfeld „Ressource“ für manuell konfigurierte Ressourcen.
- **File-Based SnapRestore.** ein dateibasierter SnapRestore, auch als Single File SnapRestore bekannt, stellt alle einzelnen Dateien (NFS) oder alle LUNs (SAN) wieder her.
  - Standardwiederherstellungsmethode für automatisch erkannte Ressourcen. Kann mit dem Kontrollkästchen Volume zurücksetzen für NFS geändert werden.
  - Optionsfeld auf Dateiebene für manuell konfigurierte Ressourcen.

Die folgende Tabelle enthält einen Vergleich der verschiedenen Wiederherstellungsmethoden.

	Volume-basierte SnapRestore	File-basiertes SnapRestore
Geschwindigkeit der Wiederherstellung	Sehr schnell, unabhängig von der Volume-Größe	Sehr schnelle Restore-Prozesse, nutzt aber Hintergrundkopiejobs für das Storage-System, wodurch die Erstellung neuer Snapshot Backups blockiert wird
Snapshot Backup-Verlauf	Wiederherstellung auf ein älteres Snapshot-Backup, entfernt alle neueren Snapshot-Backups.	Kein Einfluss
Wiederherstellung der Verzeichnisstruktur	Verzeichnisstruktur wird ebenfalls wiederhergestellt	NFS: Stellt nur die einzelnen Dateien wieder her, nicht die Verzeichnisstruktur. Wenn auch die Verzeichnisstruktur verloren geht, muss sie manuell erstellt werden, bevor der Wiederherstellungsvorgang ausgeführt wird.auch die Verzeichnisstruktur wird wiederhergestellt
Für die Konfiguration der Ressource ist die Replizierung auf einen externen Backup-Storage eingerichtet	Eine Wiederherstellung auf Volume-Basis kann nicht an einem Backup der Snapshot Kopie durchgeführt werden, das älter als die Snapshot Kopie ist, die für die SnapVault-Synchronisierung verwendet wird	Ein beliebiges Snapshot Backup kann ausgewählt werden

Wiederherstellung kompletter Ressourcen von externen Backup-Speichern

Eine Wiederherstellung über den externen Backup-Speicher wird immer mithilfe einer SnapVault-Wiederherstellung durchgeführt, bei der alle Dateien oder alle LUNs des Storage-Volumes mit dem Inhalt des

Snapshot-Backups überschrieben werden.

Wiederherstellung eines einzelnen Mandanten

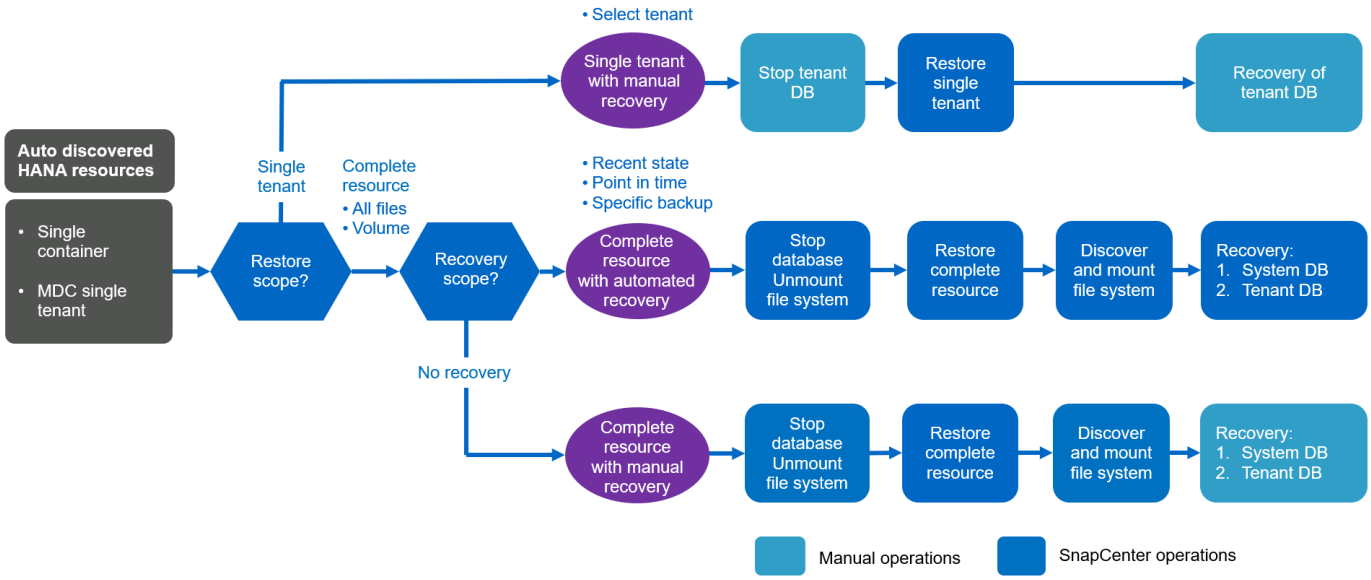
Die Wiederherstellung eines einzelnen Mandanten erfordert eine dateibasierte Wiederherstellung. Je nach verwendetem Storage-Protokoll werden verschiedene Restore-Workflows von SnapCenter ausgeführt.

- NFS
  - Primärspeicher. Dateibasierte SnapRestore-Vorgänge werden für alle Dateien der Mandanten-Datenbank ausgeführt.
  - Externer Backup-Storage: Für alle Dateien der Mandanten-Datenbank werden SnapVault Restore-Vorgänge durchgeführt.
- SAN
  - Primärspeicher. Klonen und Verbinden der LUN mit dem Datenbank-Host und Kopieren aller Dateien der Mandanten-Datenbank.
  - Externer Backup-Storage: Klonen und Verbinden der LUN mit dem Datenbank-Host und Kopieren aller Dateien der Mandanten-Datenbank.

Wiederherstellung und Recovery von automatisch erkannten HANA-Einzelcontainern und MDC-Einzelmandanten-Systemen

HANA-einzelner Container und HANA MDC-Einzelmandanten-Systeme, die automatisch erkannt wurden, sind für die automatisierte Wiederherstellung und das automatisierte Recovery mit SnapCenter aktiviert. Für diese HANA-Systeme unterstützt SnapCenter drei verschiedene Restore- und Recovery-Workflows, wie in der folgenden Abbildung dargestellt:

- **Einzelner Mandant mit manueller Wiederherstellung.** bei Auswahl eines einzelnen Mandanten führt SnapCenter alle Mandanten auf, die im ausgewählten Snapshot-Backup enthalten sind. Sie müssen die Mandantendatenbank manuell anhalten und wiederherstellen. Der Restore-Vorgang mit SnapCenter wird mit einzelnen Datei-SnapRestore-Vorgängen für NFS oder Klon-, Mount- und Kopiervorgängen in SAN-Umgebungen durchgeführt.
- **Komplette Ressource mit automatisierter Wiederherstellung.** Wenn Sie einen kompletten Ressourcenwiederherstellungsvorgang und eine automatisierte Wiederherstellung auswählen, wird der gesamte Workflow mit SnapCenter automatisiert. SnapCenter unterstützt den aktuellen Zustand, zeitpunktgenaue oder bestimmte Backup Recovery-Vorgänge. Der ausgewählte Wiederherstellungsvorgang wird für das System und die Mandantendatenbank verwendet.
- **Vollständige Ressource mit manueller Wiederherstellung.** Wenn Sie No Recovery wählen, stoppt SnapCenter die HANA-Datenbank und führt das erforderliche Dateisystem (unmount, Mount) und Restore Operationen aus. Sie müssen die System- und die Mandantendatenbank manuell wiederherstellen.

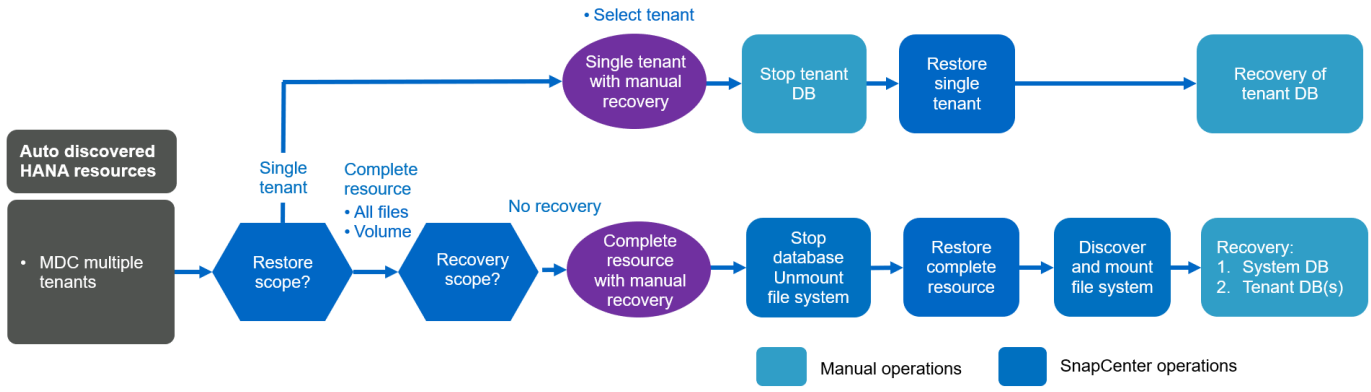


Wiederherstellung und Wiederherstellung von automatisch erkannten HANA MDC-Systemen mit mehreren Mandanten

Obwohl HANA MDC-Systeme mit mehreren Mandanten automatisch erkannt werden können, wird die automatisierte Wiederherstellung und Wiederherstellung mit der aktuellen SnapCenter-Version nicht unterstützt. Bei MDC-Systemen mit mehreren Mandanten unterstützt SnapCenter zwei verschiedene Wiederherstellungs- und Recovery-Workflows, wie in der folgenden Abbildung dargestellt:

- Ein einzelner Mandant mit manueller Recovery
- Ressource mit manueller Wiederherstellung abschließen

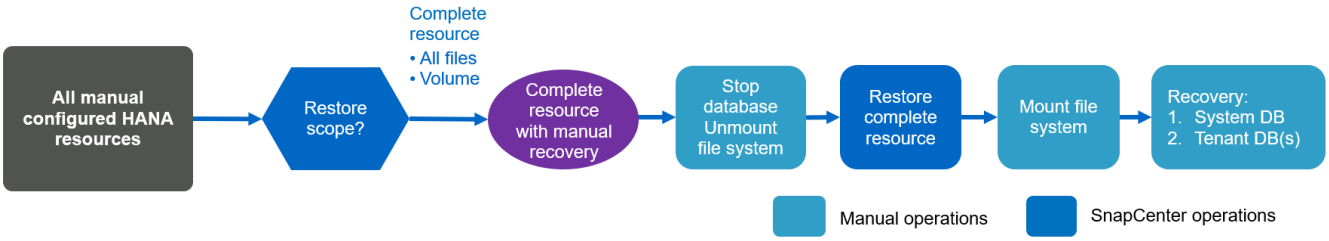
Die Workflows sind die gleichen wie im vorherigen Abschnitt beschrieben.



Wiederherstellung und Recovery von manuellen konfigurierten HANA-Ressourcen

Manuelle konfigurierte HANA-Ressourcen sind für automatisiertes Restore und Recovery nicht aktiviert. Zudem wird bei MDC-Systemen mit einzelnen oder mehreren Mandanten kein Restore-Vorgang eines einzelnen Mandanten unterstützt.

Bei manuell konfigurierten HANA-Ressourcen unterstützt SnapCenter nur eine manuelle Recovery, wie in der folgenden Abbildung dargestellt. Der Workflow für die manuelle Wiederherstellung ist der gleiche wie in den vorherigen Abschnitten beschrieben.



Zusammenfassung von Restore- und Recovery-Vorgängen

In der folgenden Tabelle sind die Restore- und Recovery-Vorgänge abhängig von der Konfiguration der HANA-Ressourcen in SnapCenter zusammengefasst.

Konfiguration von SnapCenter-Ressourcen	Wiederherstellungs- und Recovery-Optionen	Stoppen Sie die HANA Datenbank	Vorher unmounten, nach Wiederherstellungsvorgang mounten	Recovery-Vorgang
Automatisch erkannte Einzelcontainer MDC Einzelmandant	• Füllen Sie die Ressource mit entweder aus • Standard (alle Dateien) • Volume-Zurücksetzen (NFS nur aus Primärspeicher) • Automatische Wiederherstellung ausgewählt	Automatisiert mit SnapCenter	Automatisiert mit SnapCenter	Automatisiert mit SnapCenter
	• Füllen Sie die Ressource mit entweder aus • Standard (alle Dateien) • Volume-Zurücksetzen (NFS nur aus Primärspeicher) • Keine Wiederherstellung ausgewählt	Automatisiert mit SnapCenter	Automatisiert mit SnapCenter	Manuell
	• Wiederherstellung von Mandanten	Manuell	Nicht erforderlich	Manuell

Konfiguration von SnapCenter-Ressourcen	Wiederherstellungs- und Recovery-Optionen	Stoppen Sie die HANA Datenbank	Vorher unmounten, nach Wiederherstellungsvorgang mounten	Recovery-Vorgang
Automatisch erkannte MDC mehrere Mandanten	• Füllen Sie die Ressource mit entweder aus • Standard (alle Dateien) • Volume-Zurücksetzen (NFS nur aus Primärspeicher) • Automatisierte Wiederherstellung wird nicht unterstützt	Automatisiert mit SnapCenter	Automatisiert mit SnapCenter	Manuell
	• Wiederherstellung von Mandanten	Manuell	Nicht erforderlich	Manuell
Alle manuell konfigurierten Ressourcen	• Komplette Ressource (= Volume revert, verfügbar für NFS und SAN nur auf Basis des Primärspeichers) • Dateiebene (alle Dateien) • Automatisierte Wiederherstellung wird nicht unterstützt	Manuell	Manuell	Manuell

Lab-Einrichtung für diesen Bericht

Die für diesen technischen Bericht verwendete Lab-Einrichtung umfasst fünf verschiedene SAP HANA-Konfigurationen:

- **MS1.**
  - SAP HANA MDC-Einzelmandant-System mit mehreren Hosts
  - Management über einen zentralen Plug-in-Host (SnapCenter Server)

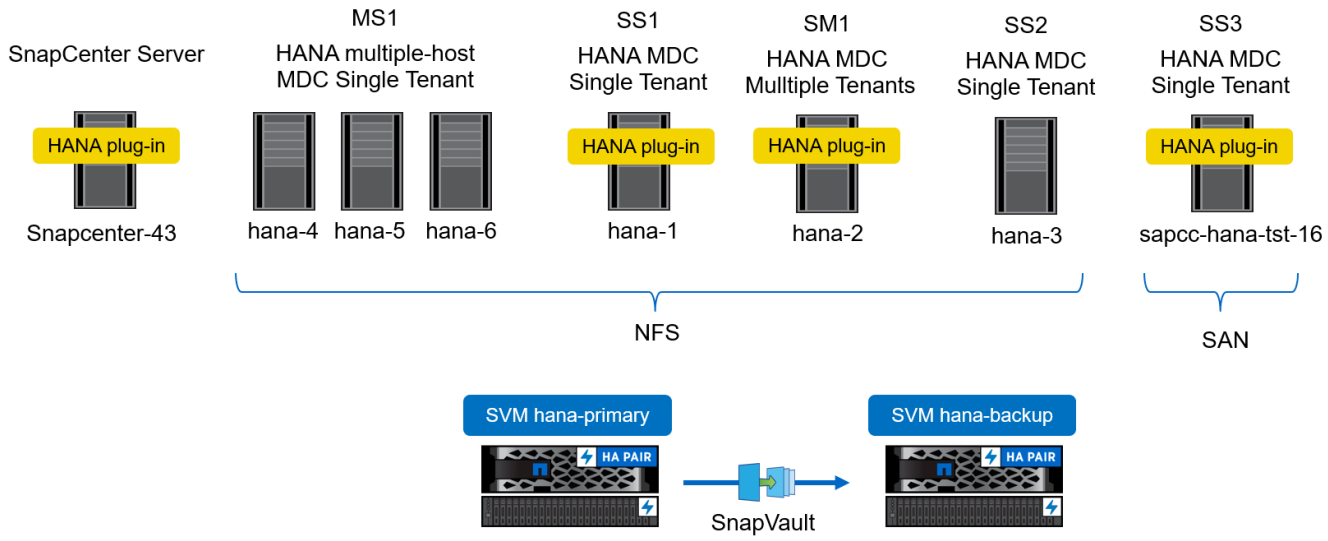
- Verwendet NFS als Storage-Protokoll

- **SS1.**
  - SAP HANA Single-Host-MDC-Einzelmandant-System
  - Automatisch erkannt mit installiertem HANA-Plug-in auf HANA-Datenbank-Host
  - Verwendet NFS als Storage-Protokoll
- **SM1.**
  - SAP HANA MDC-Mandantensystem mit einem Host
  - Automatisch erkannt mit installiertem HANA-Plug-in auf HANA-Datenbank-Host
  - Verwendet NFS als Storage-Protokoll
- **SS2.**
  - SAP HANA Single-Host-MDC-Einzelmandant-System
  - Management über einen zentralen Plug-in-Host (SnapCenter-Server)
  - Verwendet NFS als Storage-Protokoll
- **SS3.**
  - SAP HANA Single-Host-MDC-Einzelmandant-System
  - Automatisch erkannt mit installiertem HANA-Plug-in auf HANA-Datenbank-Host
  - Verwendet Fibre Channel SAN als Storage-Protokoll

In den folgenden Abschnitten werden die vollständige Konfiguration sowie die Workflows für Backup, Wiederherstellung und Recovery beschrieben. Die Beschreibung behandelt lokale Snapshot Backups sowie die Replizierung auf Backup Storage mit SnapVault. Die Storage Virtual Machines (SVMs) sind `hana-primary` Für den primären Storage und `hana-backup` Für die externe Backup-Speicherung.

Der SnapCenter-Server wird als zentraler HANA-Plug-in-Host für die HANA-Systeme MS1 und SS2 verwendet.

Die folgende Abbildung zeigt die Laboreinrichtung.

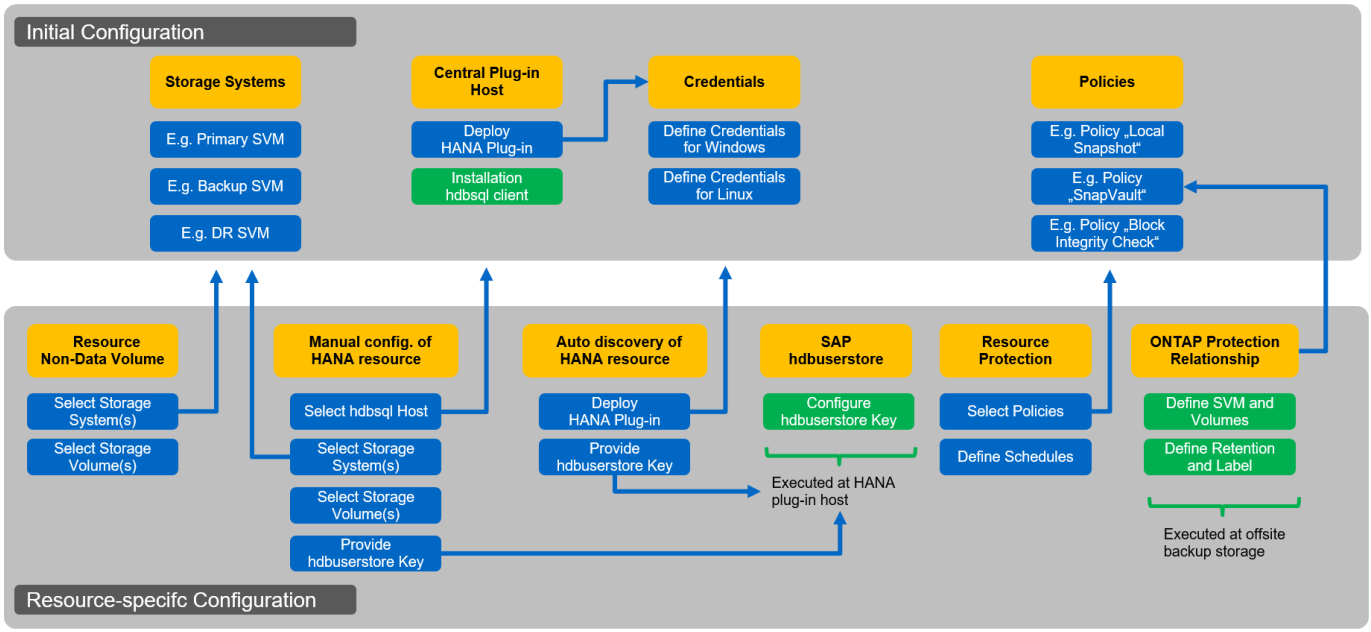


SnapCenter-Konfiguration

Die SnapCenter Konfiguration lässt sich in zwei Hauptbereiche trennen:

- **Erstkonfiguration.** umfasst allgemeine Konfigurationen, unabhängig von einer einzelnen SAP HANA Datenbank. Konfigurationen wie Storage-Systeme, zentrale HANA-Plug-in-Hosts und Richtlinien, die bei Ausführung der ressourcenspezifischen Konfigurationen ausgewählt werden.
- **Ressourcenspezifische Konfiguration.** umfasst SAP HANA systemspezifische Konfigurationen und muss für jede SAP HANA Datenbank durchgeführt werden.

Die folgende Abbildung bietet einen Überblick über die Konfigurationskomponenten und ihre Abhängigkeiten. Die grünen Felder zeigen Konfigurationsschritte, die außerhalb von SnapCenter ausgeführt werden müssen. Die blauen Felder zeigen die Schritte auf, die über die SnapCenter-Benutzeroberfläche ausgeführt werden.



Bei der Erstkonfiguration werden die folgenden Komponenten installiert und konfiguriert:

- **Storage-System.** Credential-Konfiguration für alle SVMs, die von den SAP HANA Systemen verwendet werden: In der Regel primärer Storage, externer Backup- und Disaster Recovery-Storage.

> Die auch Storage-Cluster-Anmeldedaten können anstelle einzelner SVM-Anmeldedaten konfiguriert werden.

- **Anmeldeinformationen** Konfiguration von Anmeldeinformationen, die zur Bereitstellung des SAP HANA-Plug-ins auf den Hosts verwendet werden.
- **Hosts (für zentrale HANA-Plug-in-Hosts).** Bereitstellung von SAP HANA-Plug-in. Installation der SAP HANA hdbclient-Software auf dem Host. Die SAP hdbclient-Software muss manuell installiert werden.
- **Richtlinien.** Konfiguration von Backup-Typ, Aufbewahrung und Replikation. In der Regel sind mindestens eine Richtlinie für lokale Snapshot-Kopien, eine für SnapVault-Replizierung und eine für dateibasiertes Backup erforderlich.

Die ressourcenspezifische Konfiguration muss für jede SAP HANA Datenbank durchgeführt werden und umfasst die folgenden Konfigurationen:

- Konfiguration der nicht datenvolumenlosen SAP HANA-Ressource:
  - Storage-Systeme und Volumes
- SAP hdbuserstore Schlüsselkonfiguration:
  - Die SAP hdbuserstore Schlüsselkonfiguration für die spezifische SAP HANA Datenbank muss entweder auf dem zentralen Plug-in-Host oder auf dem HANA-Datenbank-Host erfolgen, je nachdem, wo das HANA-Plug-in bereitgestellt wird.
- Automatisch erkannte SAP HANA Datenbankressourcen:
  - Implementierung des SAP HANA Plug-ins auf dem Datenbank-Host
  - Geben Sie den hdbuserstore-Schlüssel an
- Manuelle Konfiguration der SAP HANA-Datenbankressourcen:
  - SAP HANA Datenbank-SID, Plug-in-Host, hdbuserstore-Schlüssel, Storage-Systeme und Volumes
- Konfiguration für Ressourcenschutz:
  - Auswahl der erforderlichen Richtlinien
  - Definition von Zeitplänen für die einzelnen Richtlinien
- Konfiguration der ONTAP Datensicherung:
  - Nur erforderlich, wenn die Backups in einen externen Backup-Storage repliziert werden sollen.
  - Definition von Beziehung und Aufbewahrung

Erstkonfiguration von SnapCenter

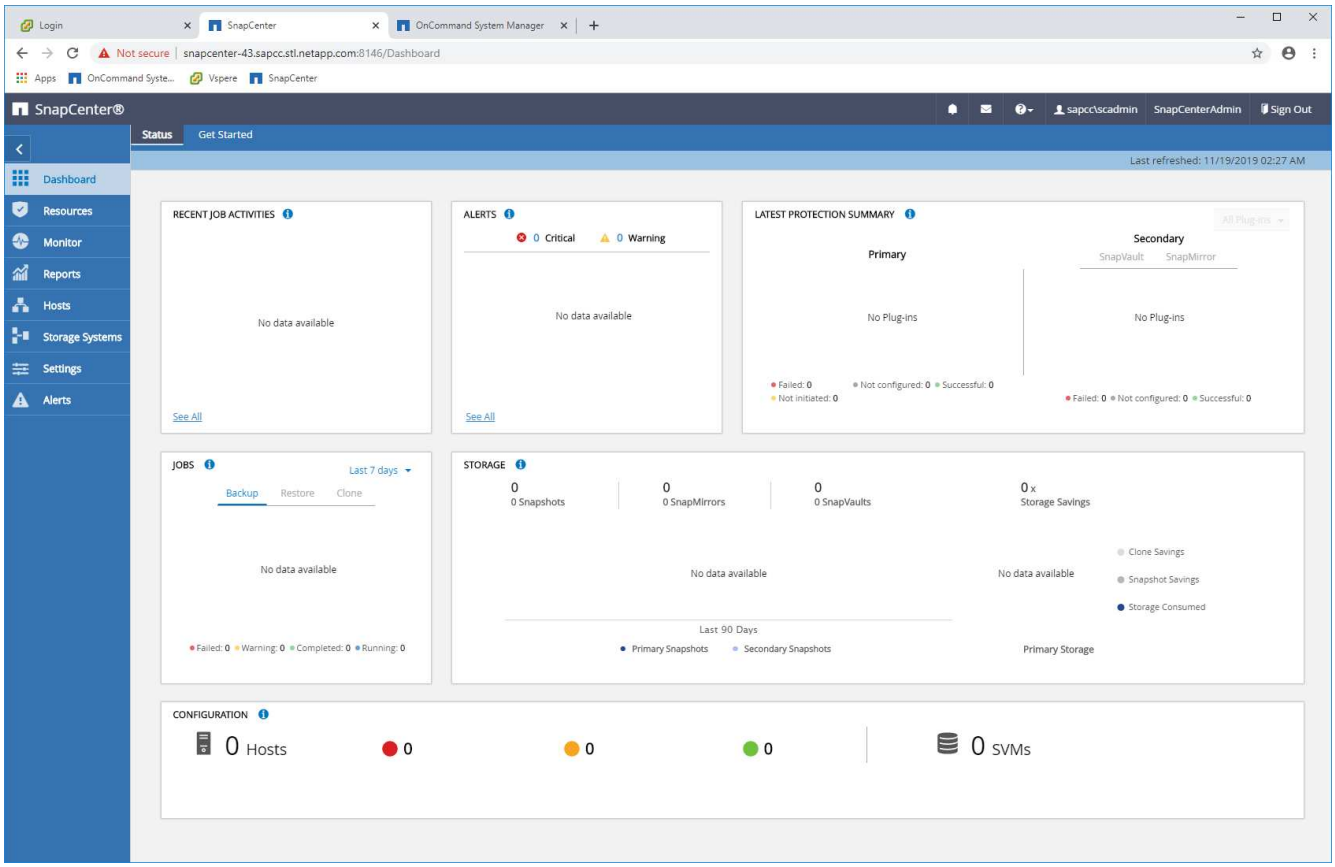
Die Erstkonfiguration umfasst die folgenden Schritte:

1. Konfiguration des Storage-Systems
2. Konfiguration von Anmeldeinformationen für die Plug-in-Installation
3. Für einen zentralen HANA-Plug-in-Host:
   a. Host-Konfiguration und SAP HANA Plug-in-Implementierung
   b. Installation und Konfiguration der SAP HANA hdbsql Client-Software
4. Konfiguration von Richtlinien

In den folgenden Abschnitten werden die ersten Konfigurationsschritte beschrieben.

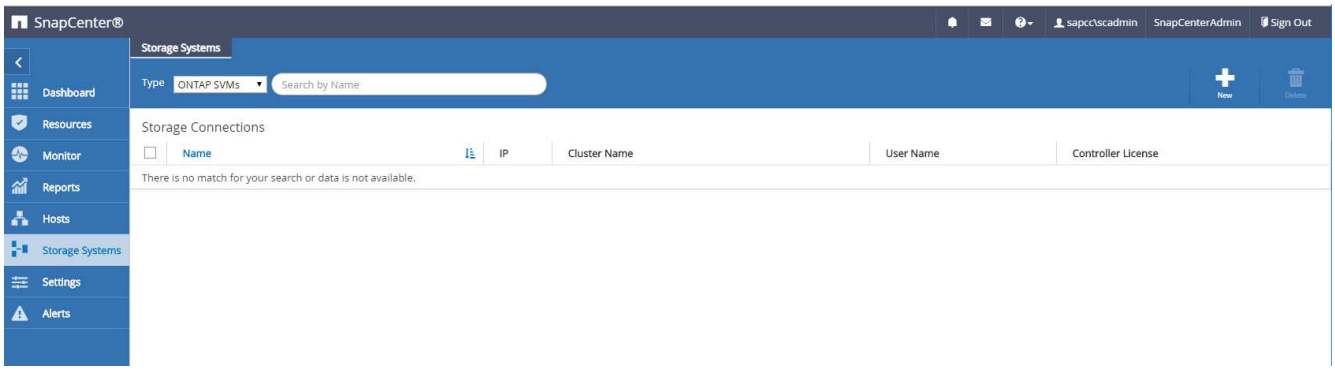
Konfiguration des Storage-Systems

1. Melden Sie sich bei der SnapCenter-ServerGUI an.



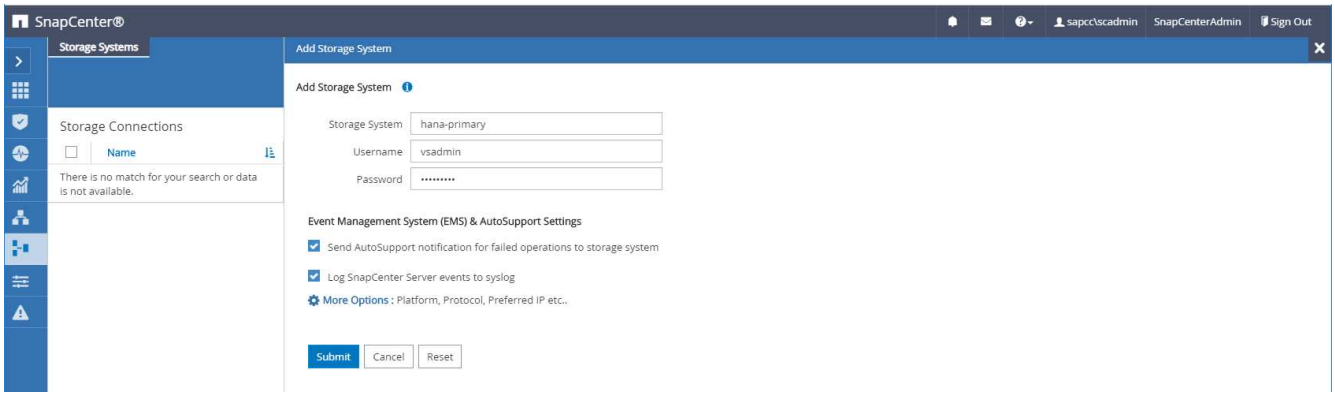
2. Wählen Sie Storage Systems Aus.

Im Bildschirm können Sie den Storage-System-Typ auswählen, der ONTAP SVMs oder ONTAP Cluster sein kann. Wenn Sie die Storage-Systeme auf SVM-Ebene konfigurieren, müssen Sie für jede SVM eine Management-LIF konfiguriert haben. Alternativ können Sie einen SnapCenter-Managementzugriff auf Cluster-Ebene verwenden. Das SVM-Management wird im folgenden Beispiel verwendet.



3. Klicken Sie auf Neu, um ein Speichersystem hinzuzufügen und den erforderlichen Hostnamen und die erforderlichen Anmeldeinformationen anzugeben.

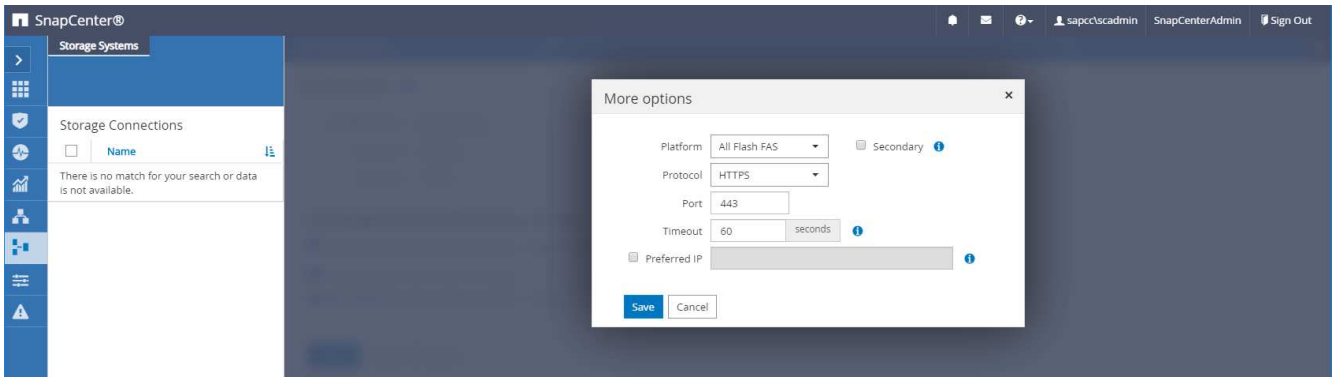
Der SVM-Benutzer muss nicht der vsadmin-Benutzer sein, wie in dem Screenshot dargestellt. In der Regel wird ein Benutzer für die SVM konfiguriert und den erforderlichen Berechtigungen zum Ausführen von Backup- und Restore-Vorgängen zugewiesen. Einzelheiten zu den erforderlichen Berechtigungen finden Sie im "SnapCenter Installationshandbuch" Im Abschnitt „Minimale ONTAP-Berechtigungen erforderlich“.



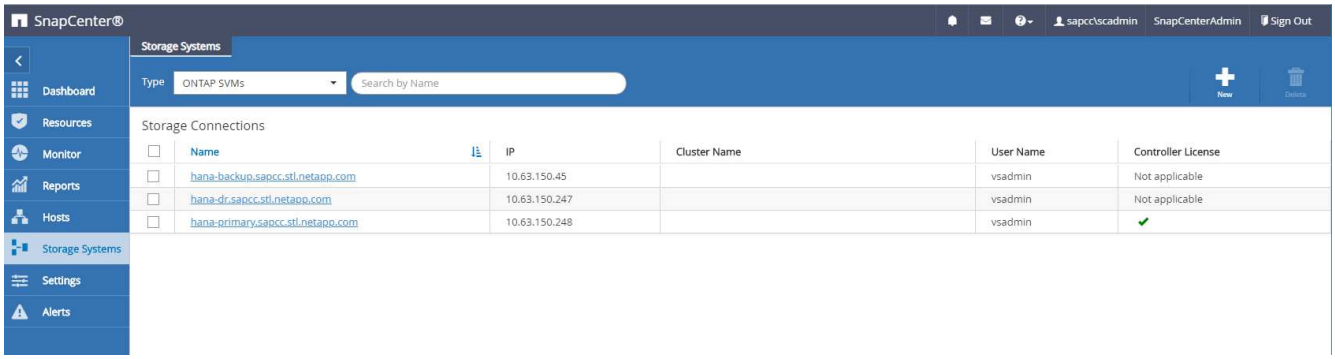
4. Klicken Sie auf Mehr Optionen, um die Storage-Plattform zu konfigurieren.

   Als Storage-Plattform können FAS, AFF, ONTAP Select oder Cloud Volumes ONTAP verwendet werden.

   Wählen Sie bei einem System, das als SnapVault- oder SnapMirror-Ziel verwendet wird, das sekundäre Symbol aus.

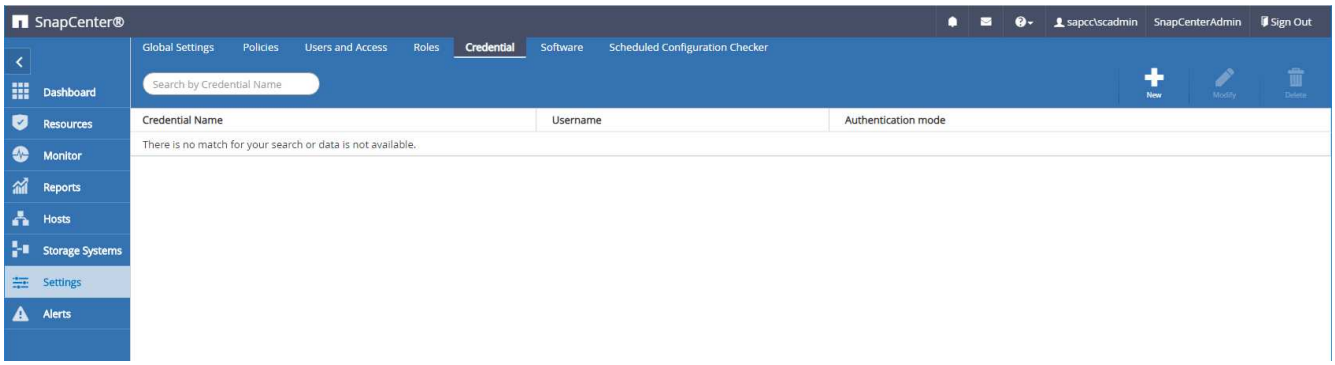


5. Fügen Sie bei Bedarf zusätzliche Storage-Systeme hinzu. Beispielsweise wurde ein zusätzlicher externer Backup-Storage und eine Disaster Recovery-Storage hinzugefügt.

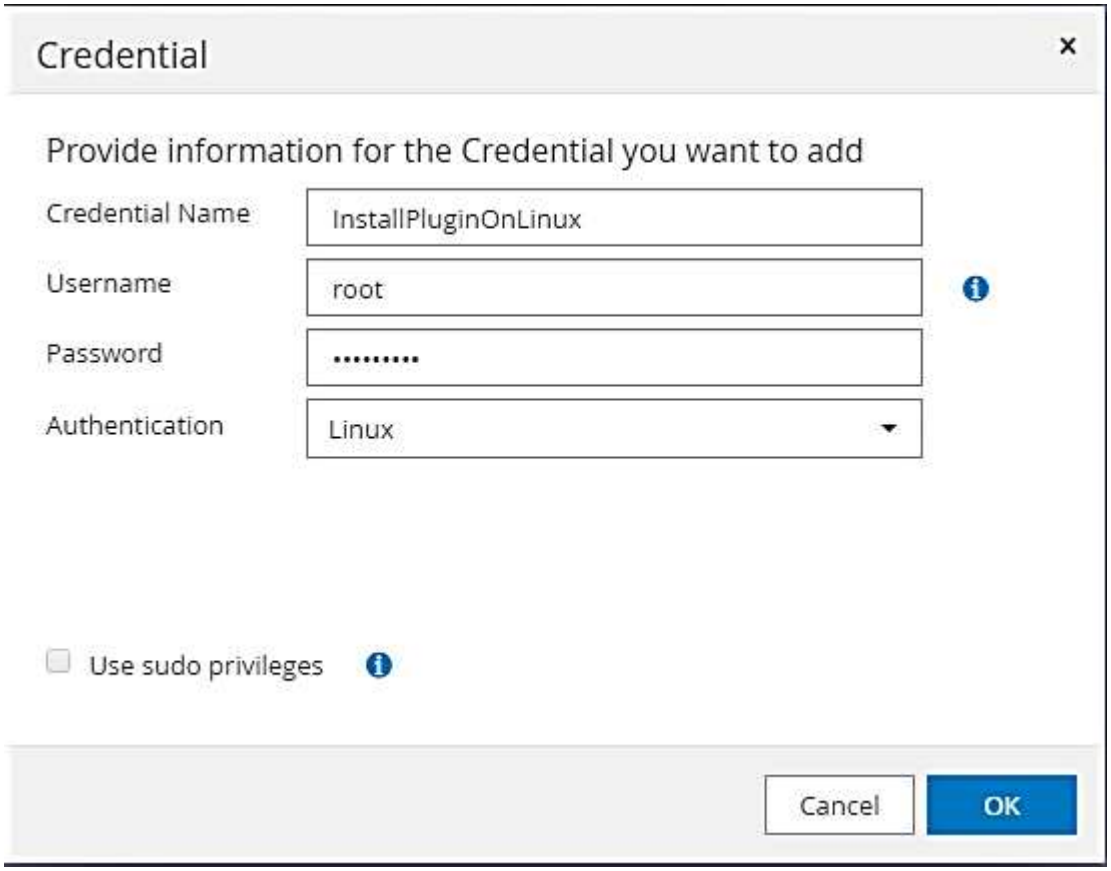


Konfiguration von Anmeldeinformationen

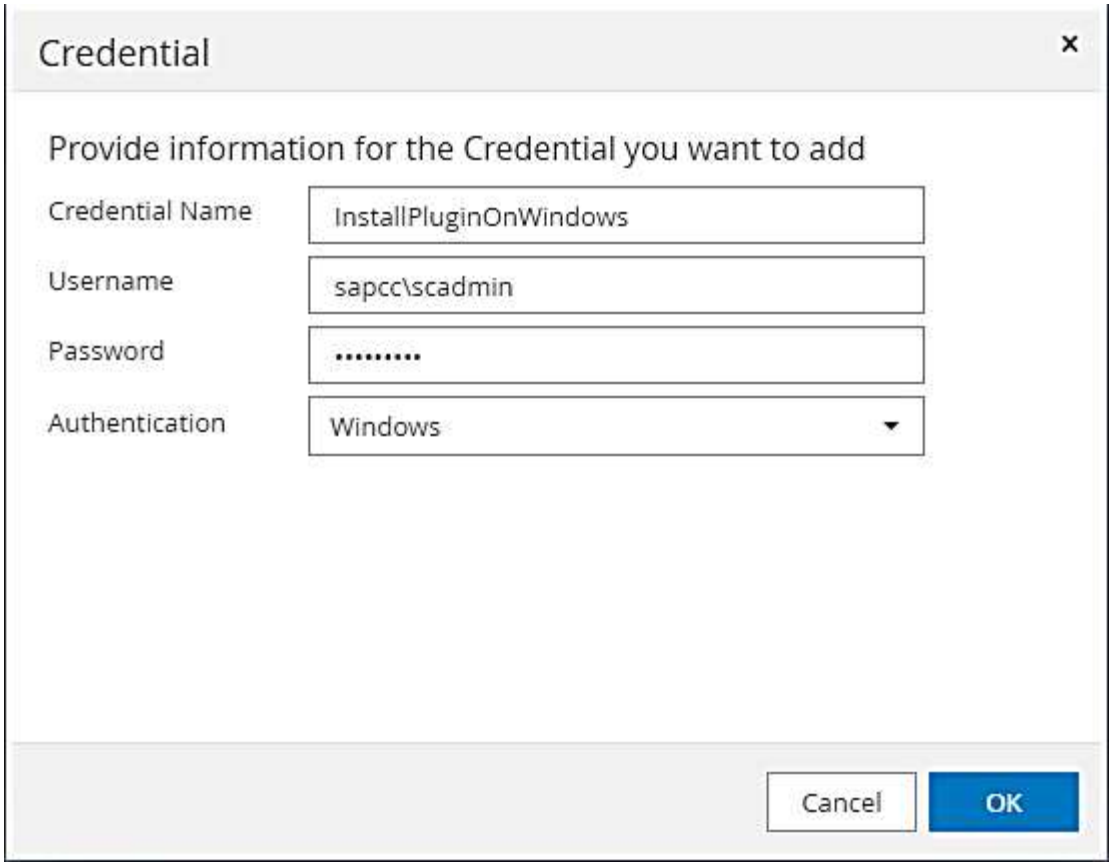
1. Gehen Sie zu Einstellungen, wählen Sie Anmeldeinformationen aus, und klicken Sie auf Neu.



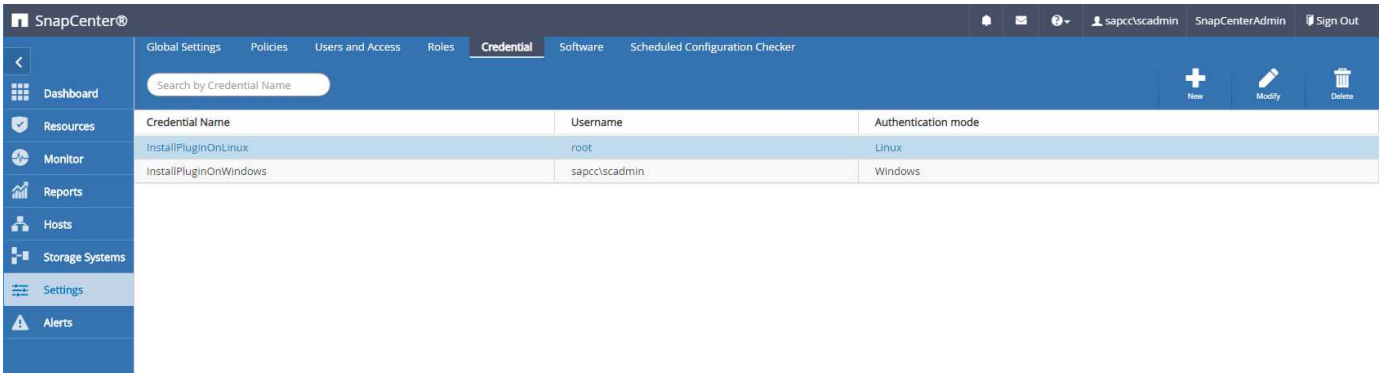
2. Geben Sie die Anmeldeinformationen für den Benutzer an, der für Plug-in-Installationen auf Linux-Systemen verwendet wird.



3. Geben Sie die Anmeldeinformationen für den Benutzer an, der für Plug-in-Installationen auf Windows-Systemen verwendet wird.



Die folgende Abbildung zeigt die konfigurierten Anmeldedaten.

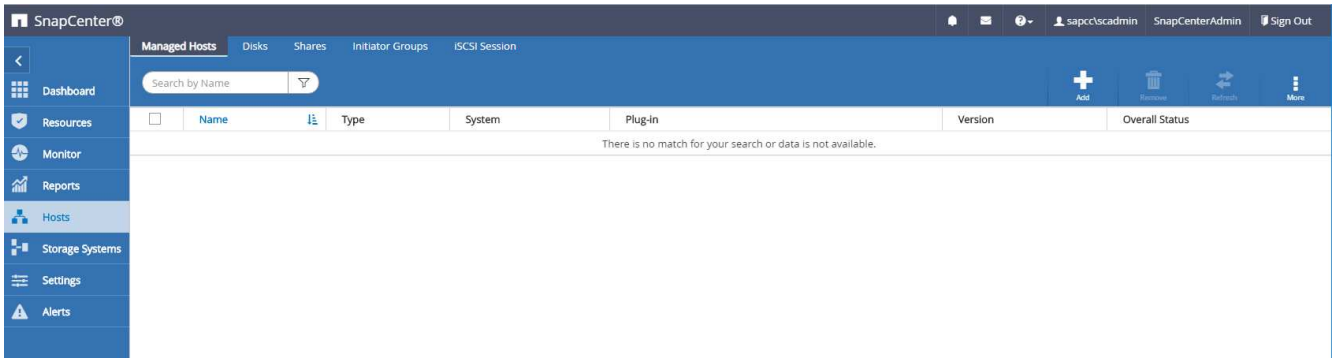


SAP HANA Plug-in-Installation auf einem zentralen Plug-in-Host

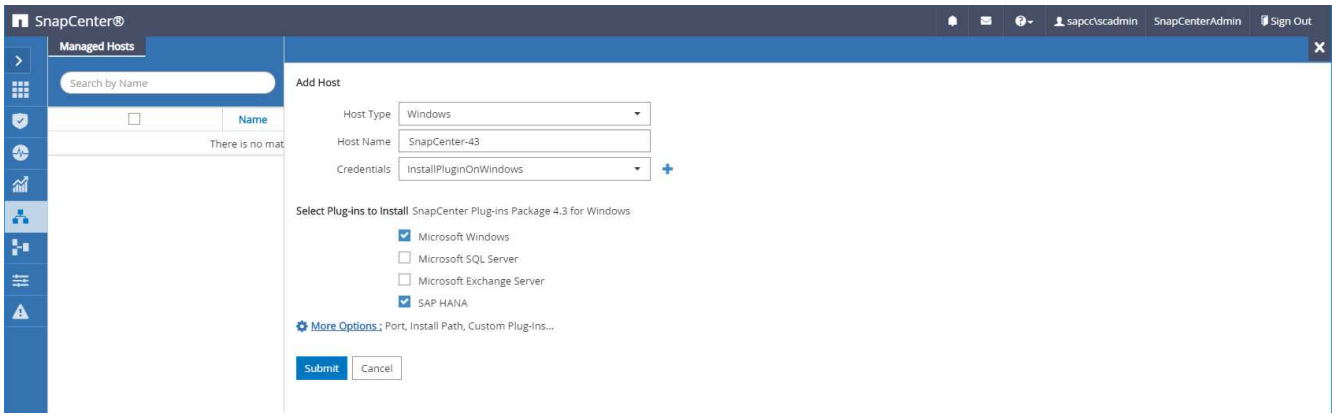
Bei der Lab-Einrichtung wird der SnapCenter-Server auch als zentraler HANA-Plug-in-Host verwendet. Der Windows-Host, auf dem SnapCenter Server ausgeführt wird, wird als Host hinzugefügt, und das SAP HANA-Plug-in ist auf dem Windows-Host installiert.

Für das SAP HANA Plug-in ist Java 64-Bit Version 1.8 erforderlich. Vor der Bereitstellung des SAP HANA Plug-ins muss Java auf dem Host installiert sein.

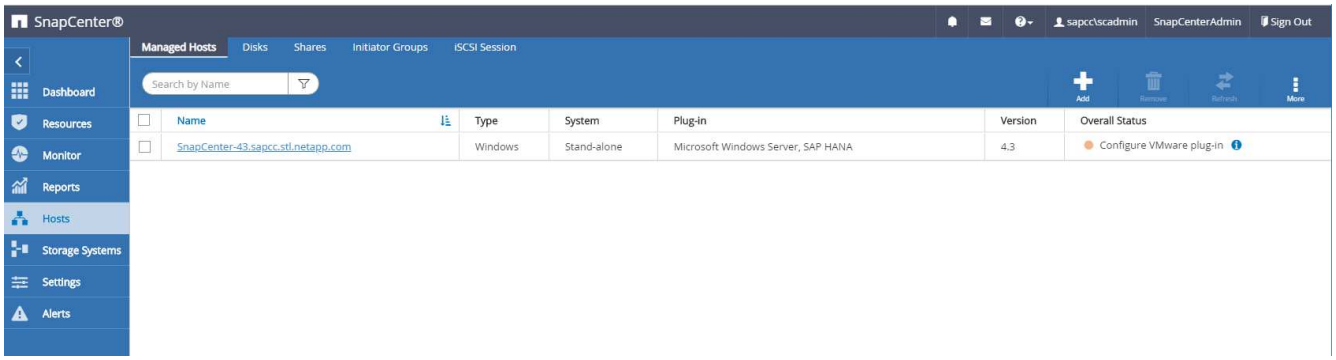
1. Gehen Sie zu Hosts und klicken Sie auf Hinzufügen.



2. Geben Sie die erforderlichen Hostinformationen ein. Klicken Sie Auf Senden.



Die folgende Abbildung zeigt alle konfigurierten Hosts, die nach der Implementierung des HANA-Plug-ins konfiguriert wurden.



Installation und Konfiguration der SAP HANA hdbsql Client-Software

Die SAP HANA hdbsql-Client-Software muss auf dem gleichen Host installiert sein, auf dem das SAP HANA-Plug-in installiert ist. Die Software kann von heruntergeladen werden "SAP-Supportportal".

Der während der Ressourcenkonfiguration konfigurierte HDBSQL OS-Benutzer muss in der Lage sein, die ausführbare Datei hdbsql auszuführen. Der Pfad zur ausführbaren Datei hdbsql muss im konfiguriert werden `hana.properties` Datei:

- Windows:

```
C:\More C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in
Creator\etc\hana.properties
HANA_HDBSQL_CMD=C:\\Program Files\\sap\\hdbclient\\hdbsql.exe
```

- Linux

```
cat /opt/NetApp/snapcenter/scc/etc/hana.properties
HANA_HDBSQL_CMD=/usr/sap/hdbclient/hdbsql
```

Konfiguration von Richtlinien

Wie im Abschnitt erläutert, "„Datensicherungsstrategie“,"werden Richtlinien in der Regel unabhängig von der Ressource konfiguriert und können von mehreren SAP HANA-Datenbanken verwendet werden.

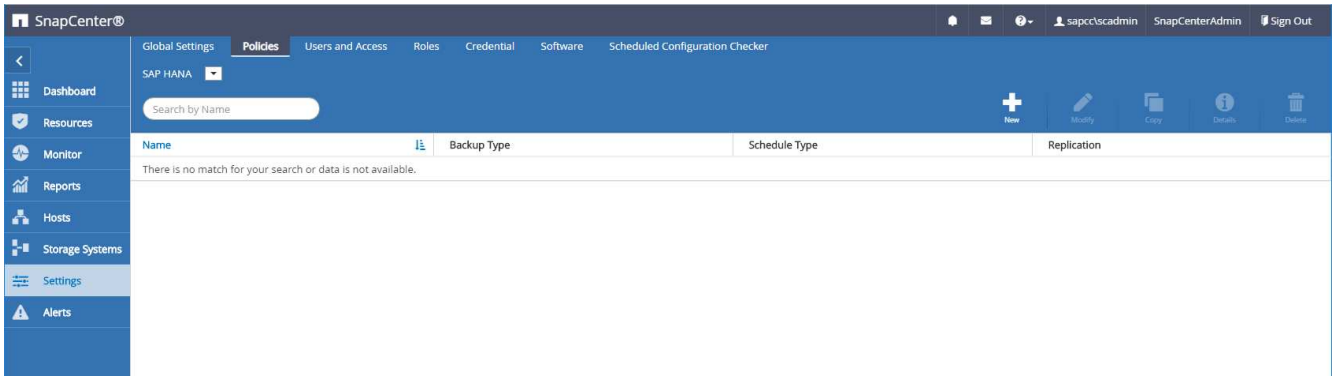
Eine typische Minimalkonfiguration umfasst folgende Richtlinien:

- Richtlinie für stündliche Backups ohne Replikation: `LocalSnap`
- Richtlinie für tägliche Backups mit SnapVault-Replikation: `LocalSnapAndSnapVault`
- Richtlinie für wöchentliche Blockintegritätsprüfung über ein dateibasiertes Backup: `BlockIntegrityCheck`

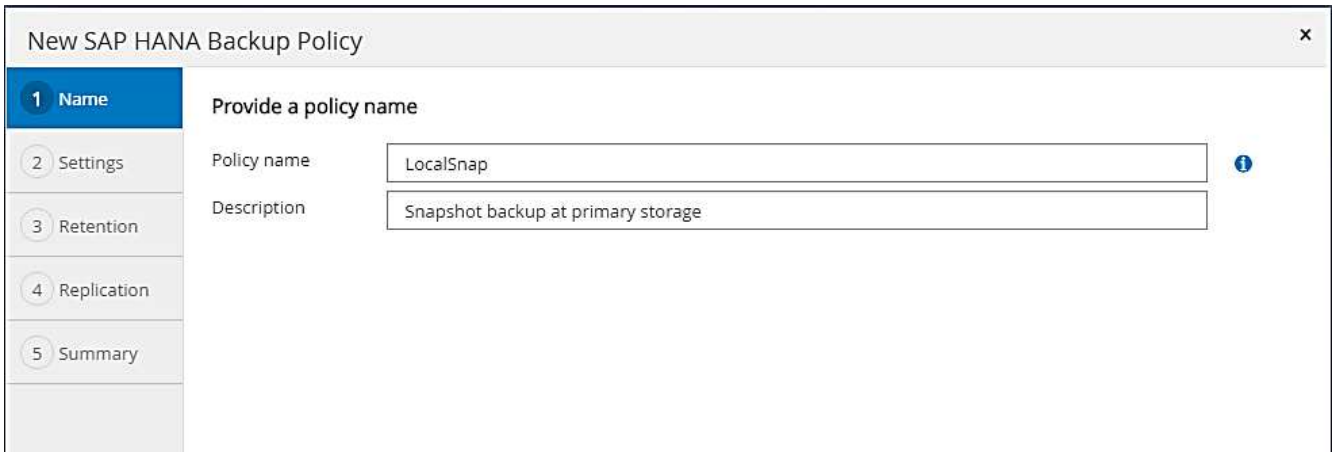
In den folgenden Abschnitten wird die Konfiguration dieser drei Richtlinien beschrieben.

Richtlinie für stündliche Snapshot Backups

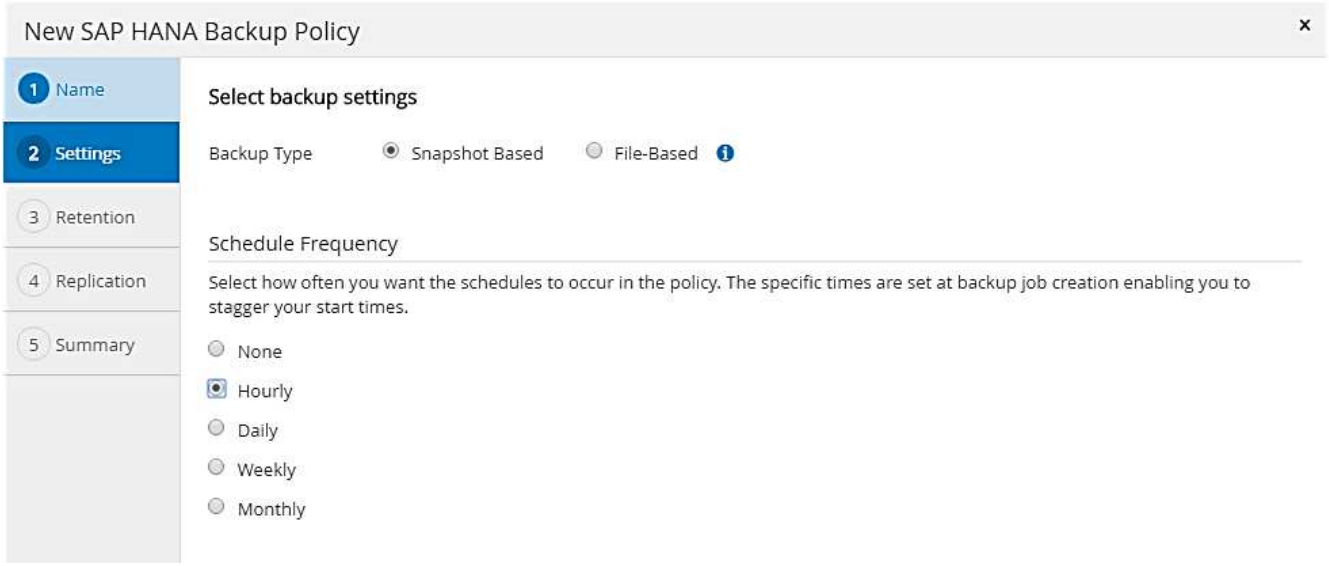
1. Gehen Sie zu Einstellungen > Richtlinien, und klicken Sie auf Neu.



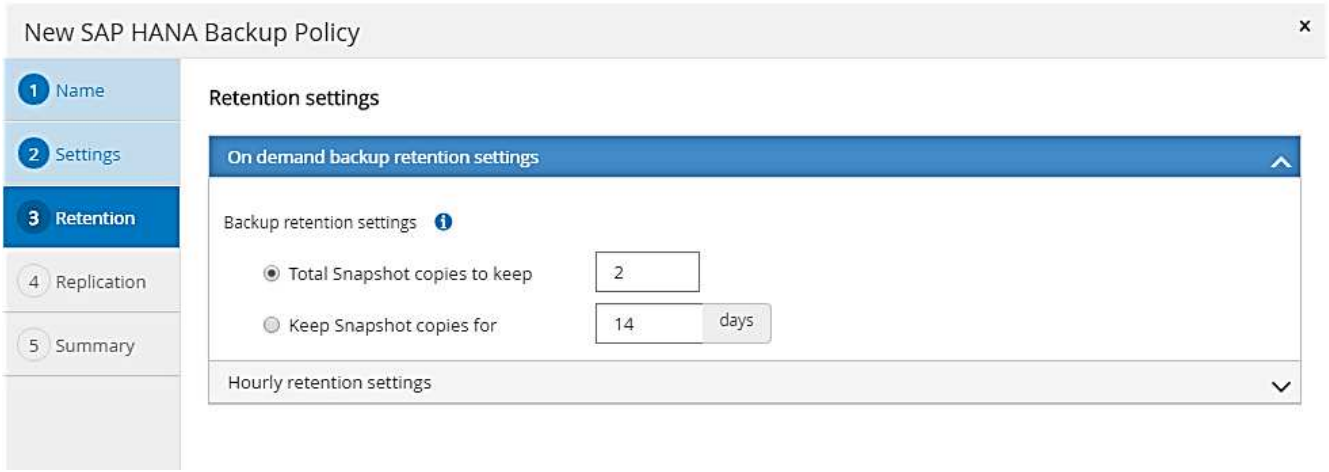
2. Geben Sie den Namen und die Beschreibung der Richtlinie ein. Klicken Sie Auf Weiter.



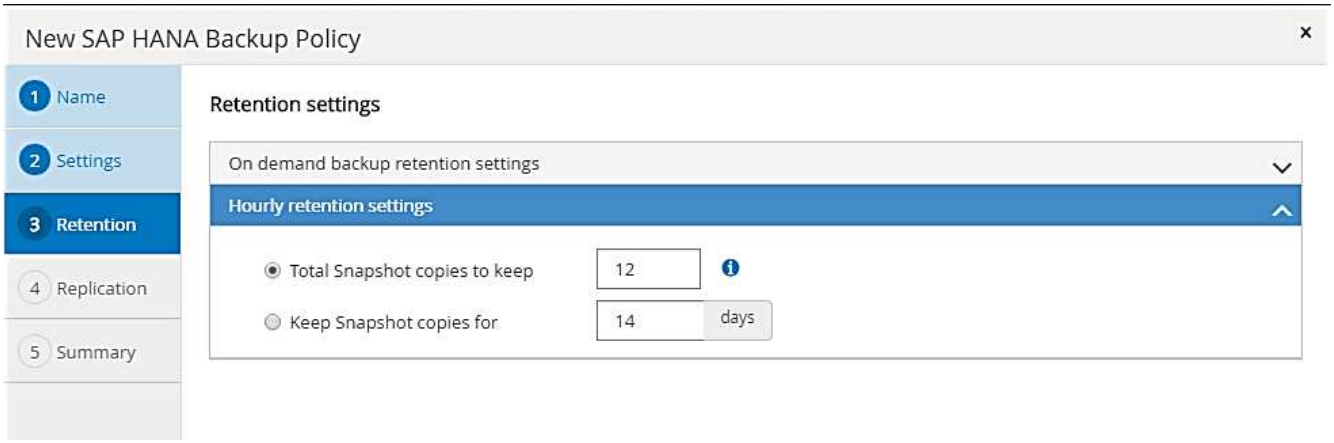
3. Wählen Sie den Backup-Typ als Snapshot-basiert aus und wählen Sie stündlich für die Zeitplanfrequenz aus.



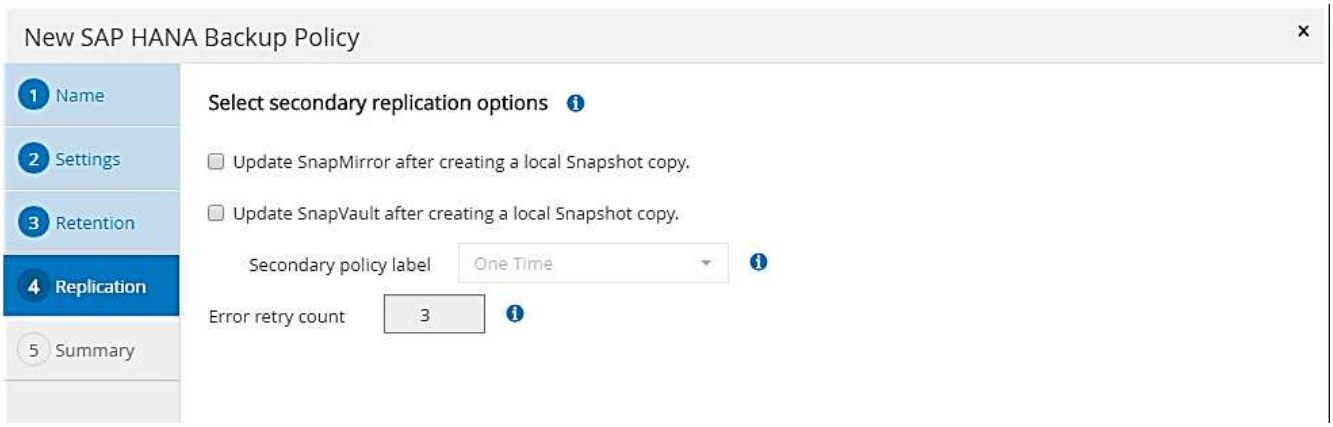
4. Konfigurieren Sie die Aufbewahrungseinstellungen für On-Demand-Backups.



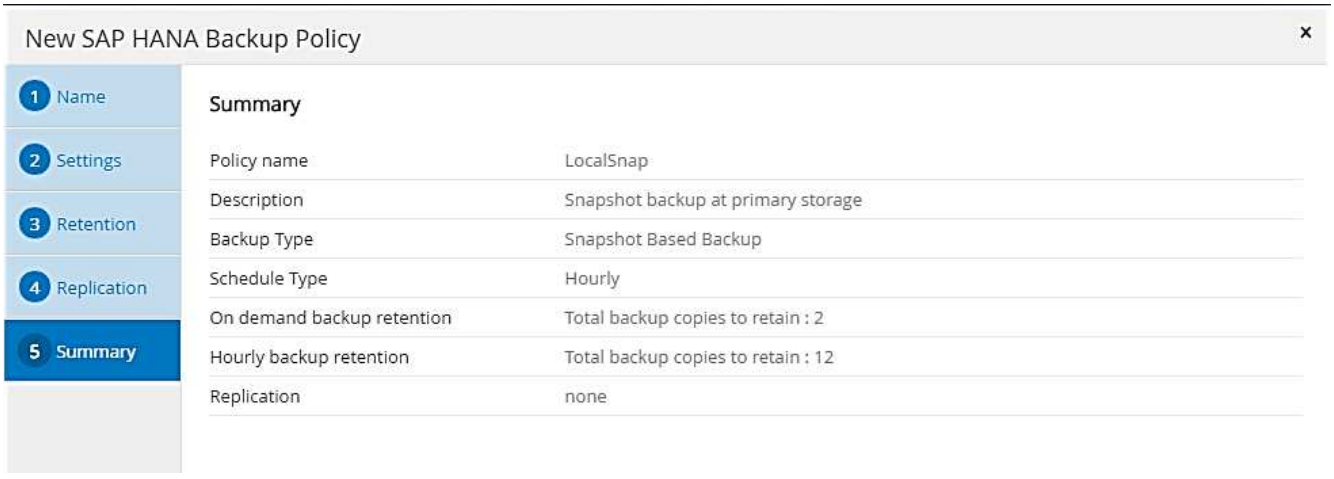
5. Konfigurieren Sie die Aufbewahrungseinstellungen für geplante Backups.



6. Konfigurieren der Replikationsoptionen. In diesem Fall ist kein SnapVault oder SnapMirror Update ausgewählt.

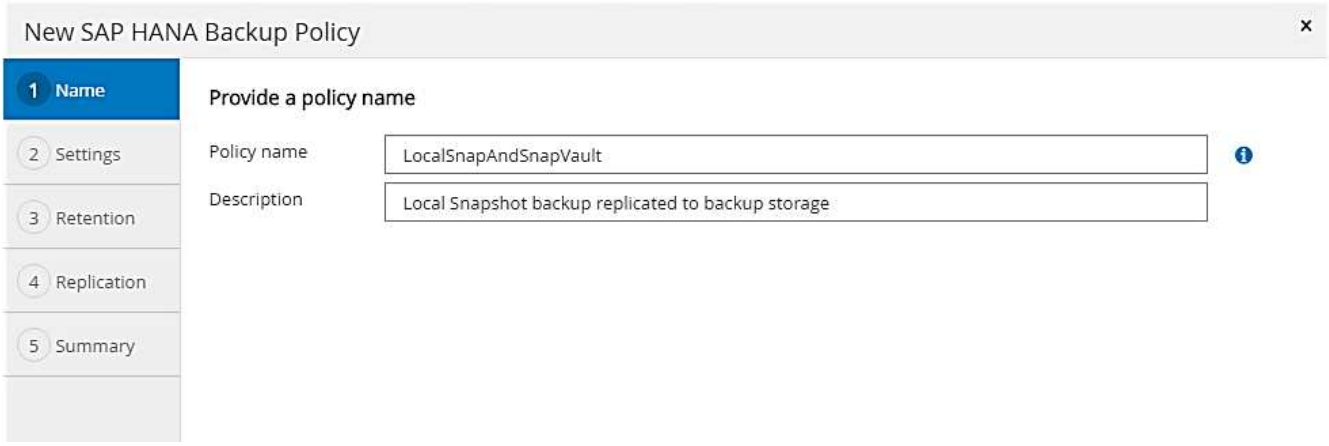


7. Klicken Sie auf der Seite Zusammenfassung auf Fertig stellen.

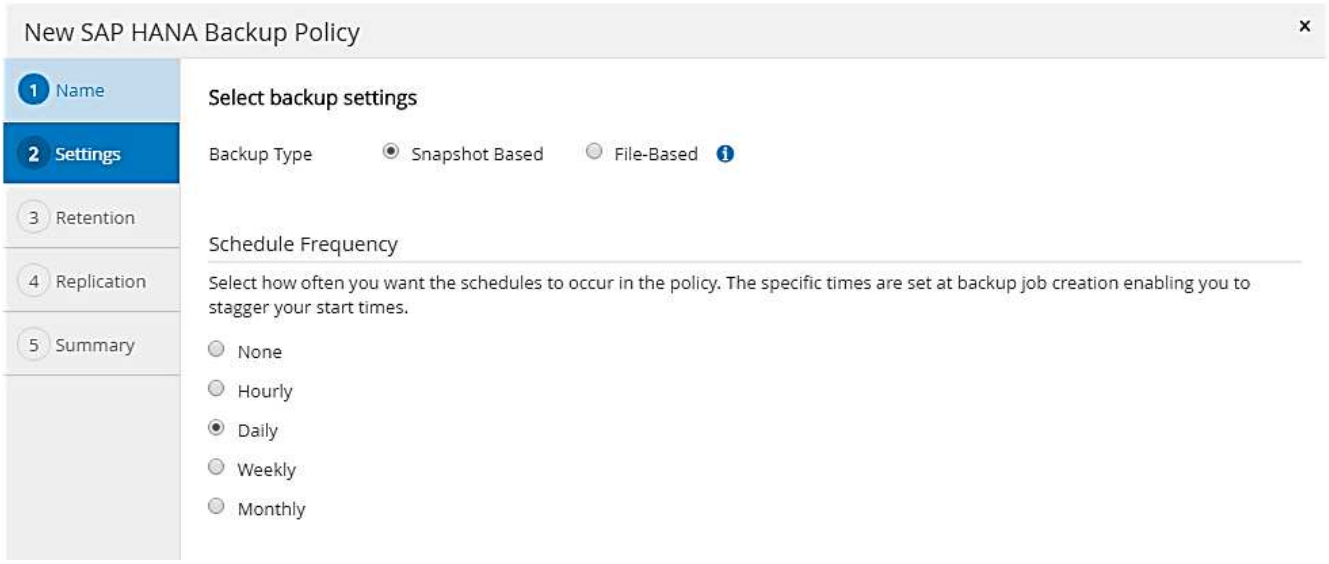


Richtlinie für tägliche Snapshot Backups mit SnapVault Replizierung

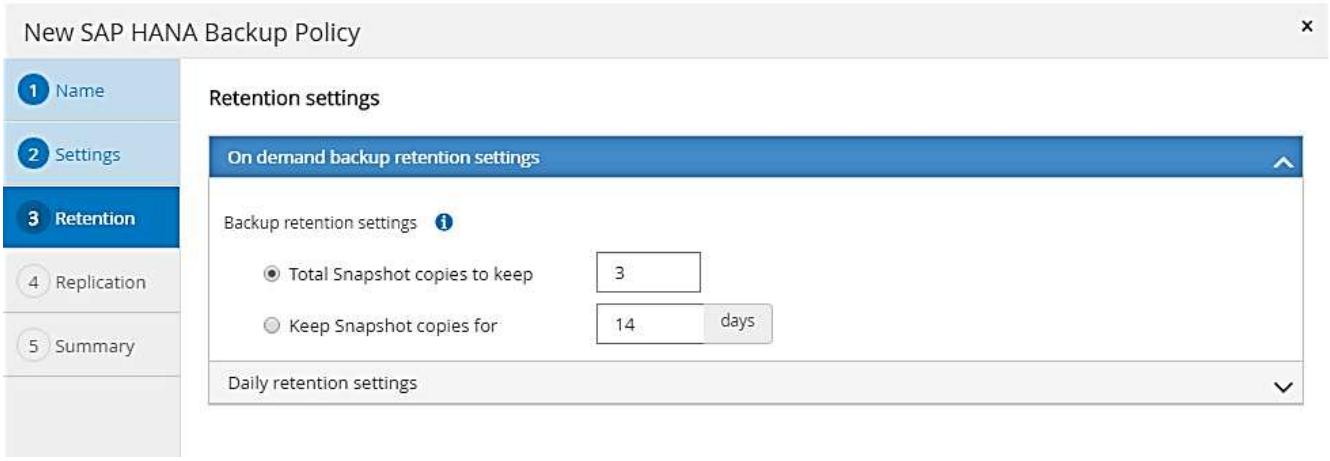
1. Gehen Sie zu Einstellungen > Richtlinien, und klicken Sie auf Neu.
2. Geben Sie den Namen und die Beschreibung der Richtlinie ein. Klicken Sie Auf Weiter.



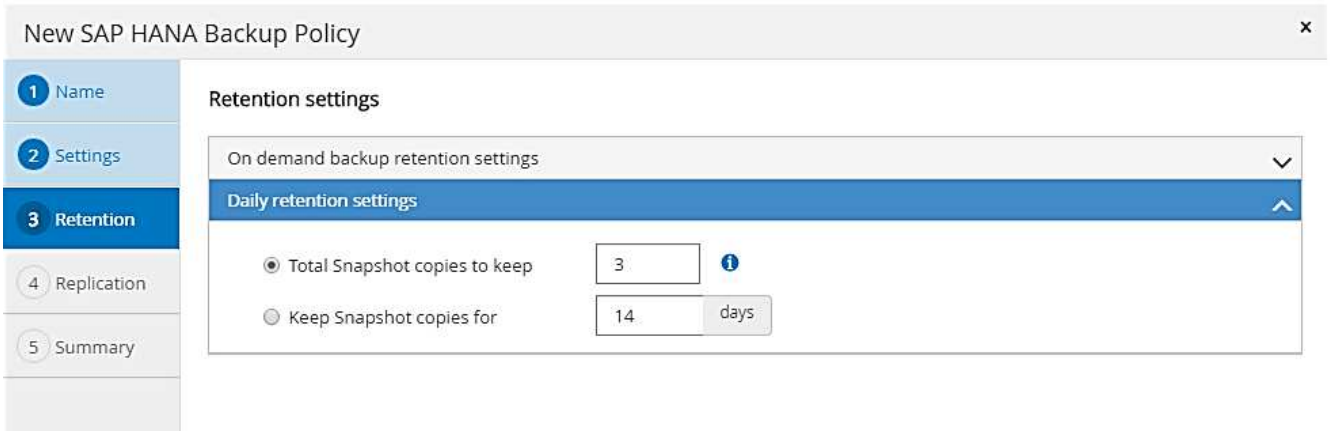
3. Legen Sie den Backup-Typ auf Snapshot-basiert und die Zeitplanfrequenz auf täglich fest.



4. Konfigurieren Sie die Aufbewahrungseinstellungen für On-Demand-Backups.

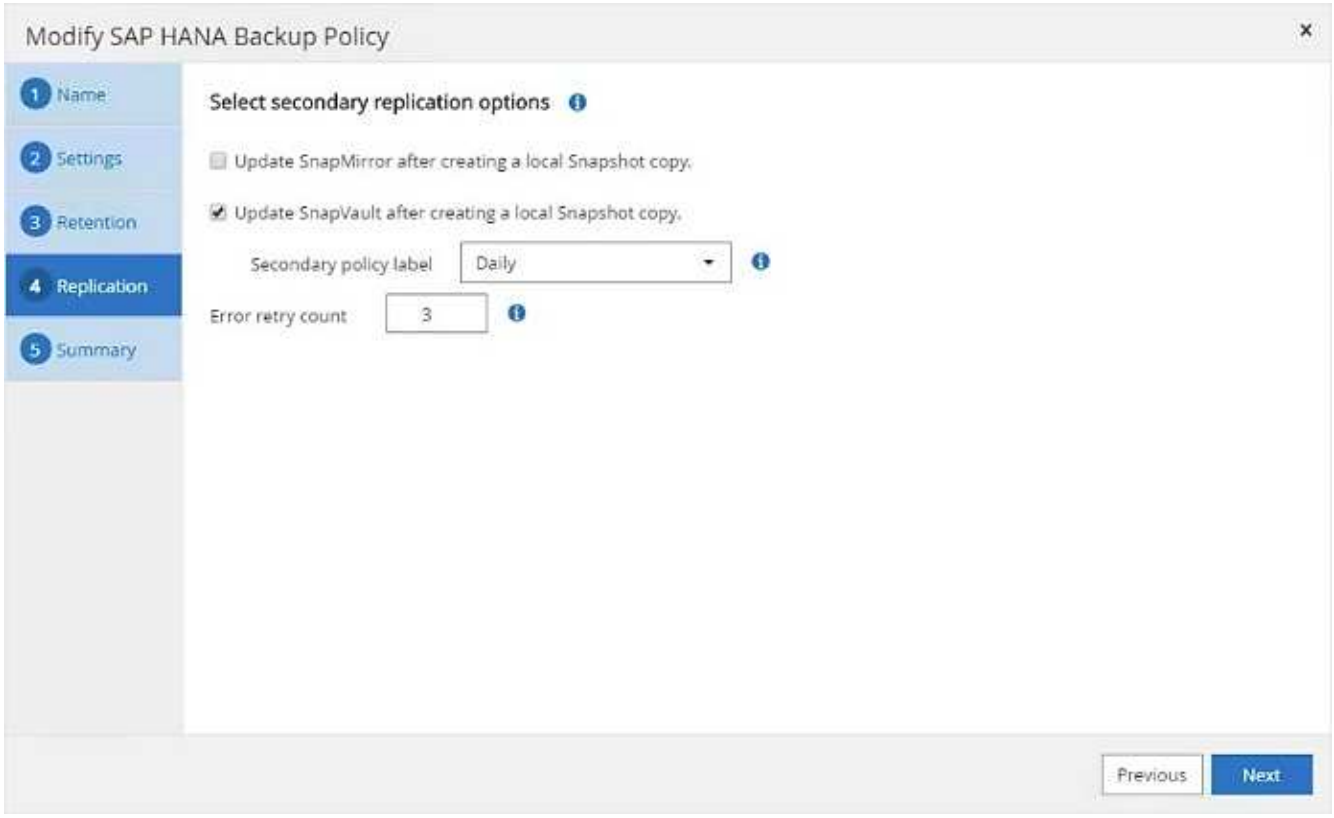


5. Konfigurieren Sie die Aufbewahrungseinstellungen für geplante Backups.

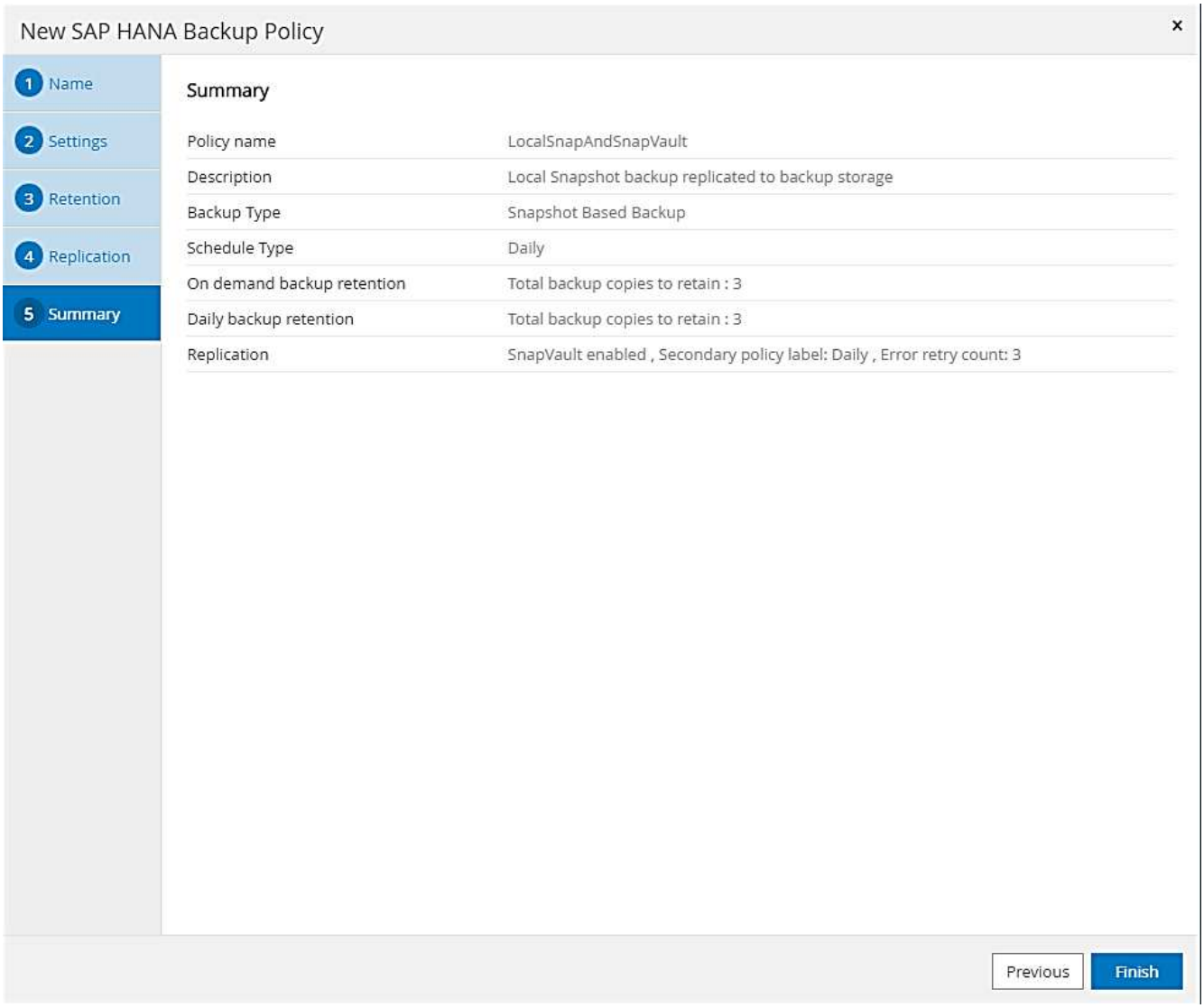


6. Wählen Sie SnapVault aktualisieren aus, nachdem Sie eine lokale Snapshot-Kopie erstellt haben.

Das sekundäre Richtlinienetikett muss mit dem SnapMirror Etikett in der Datensicherungskonfiguration auf der Storage-Ebene identisch sein. Siehe Abschnitt "„Konfiguration von Datenschutz auf externen Backup-Speicher“."

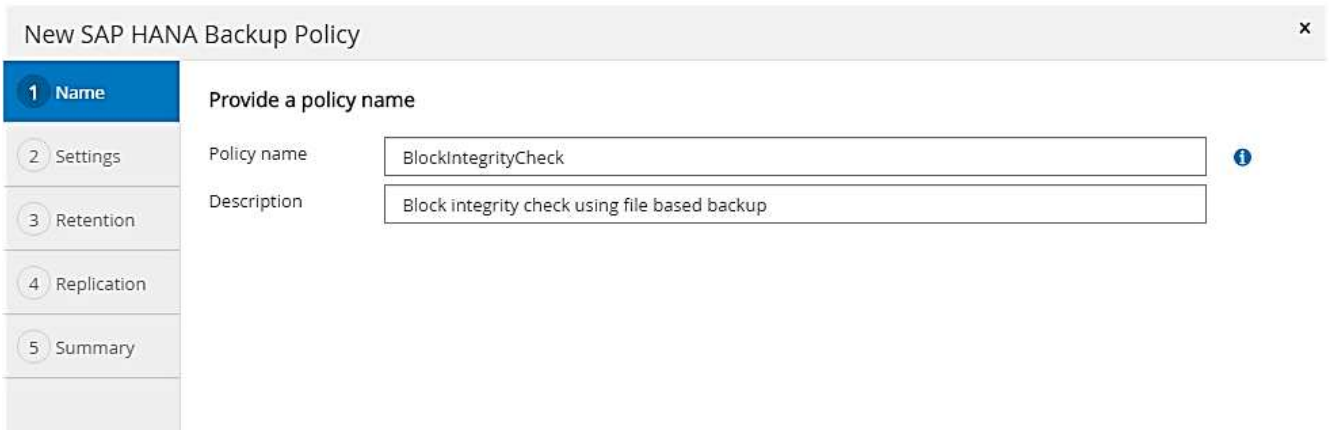


7. Klicken Sie auf der Seite Zusammenfassung auf Fertig stellen.

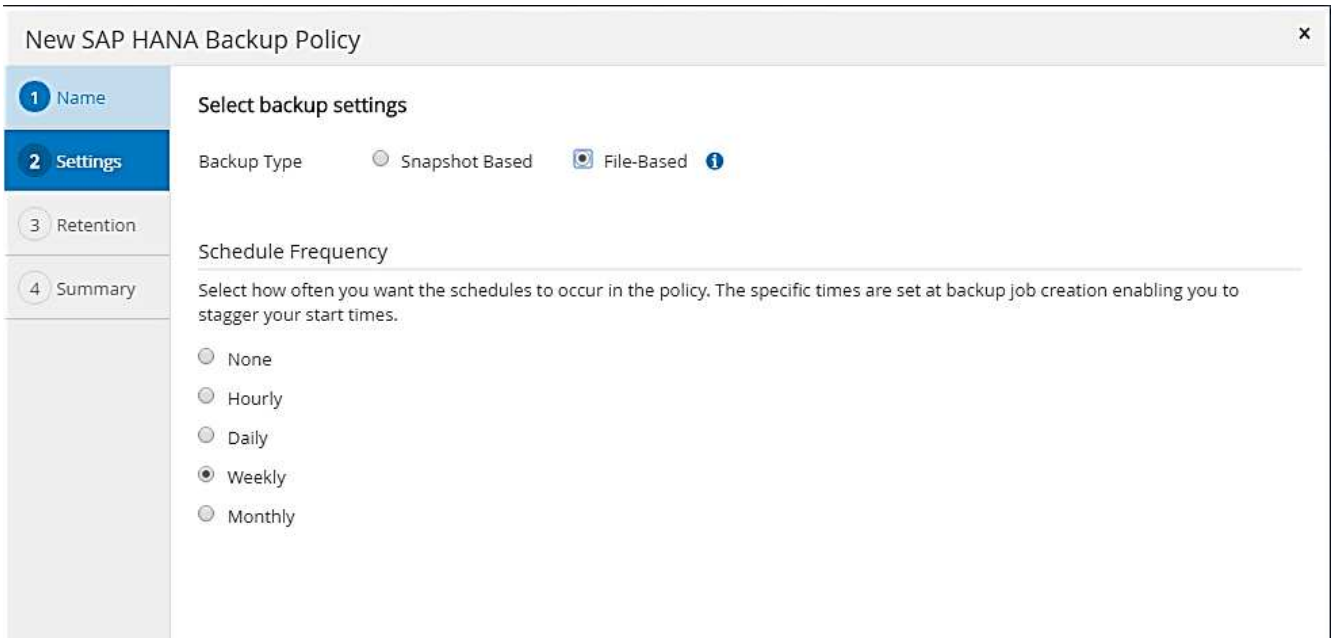


Richtlinie für die wöchentliche Blockintegritätsprüfung

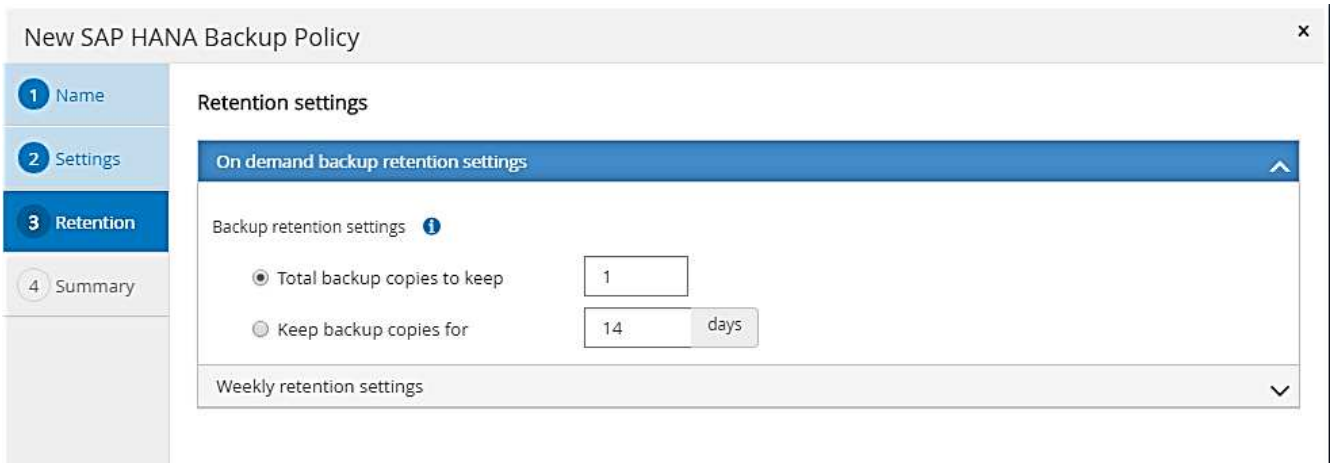
1. Gehen Sie zu Einstellungen > Richtlinien, und klicken Sie auf Neu.
2. Geben Sie den Namen und die Beschreibung der Richtlinie ein. Klicken Sie Auf Weiter.



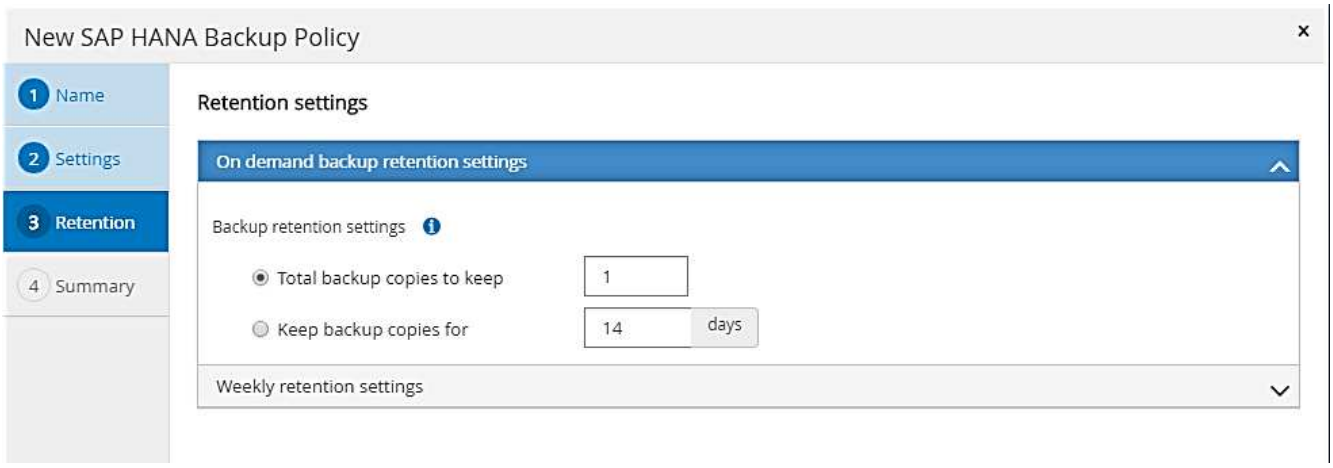
3. Legen Sie den Sicherungstyp auf „File-based“ und „Schedule Frequency“ auf „Weekly“ fest.



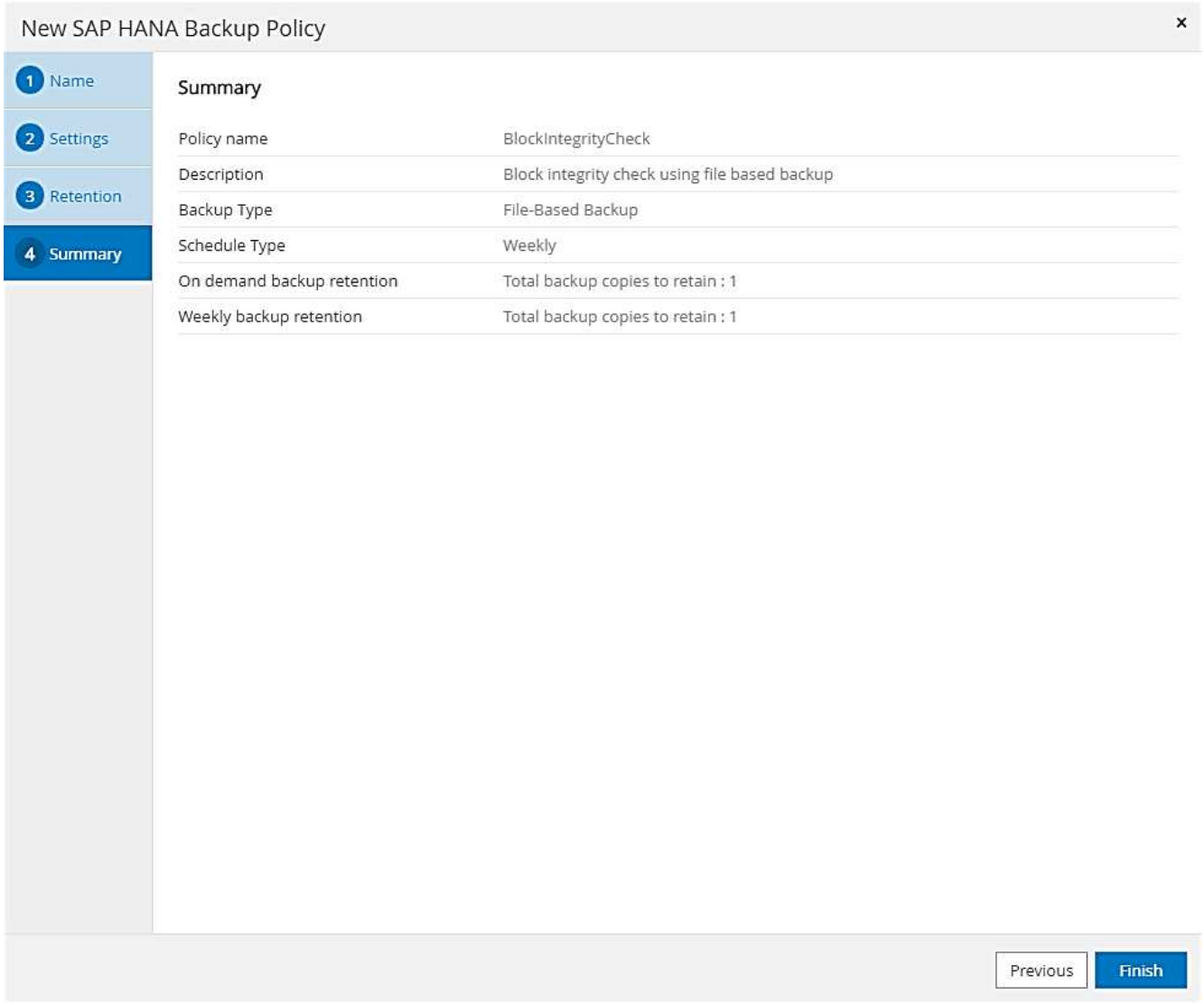
4. Konfigurieren Sie die Aufbewahrungseinstellungen für On-Demand-Backups.



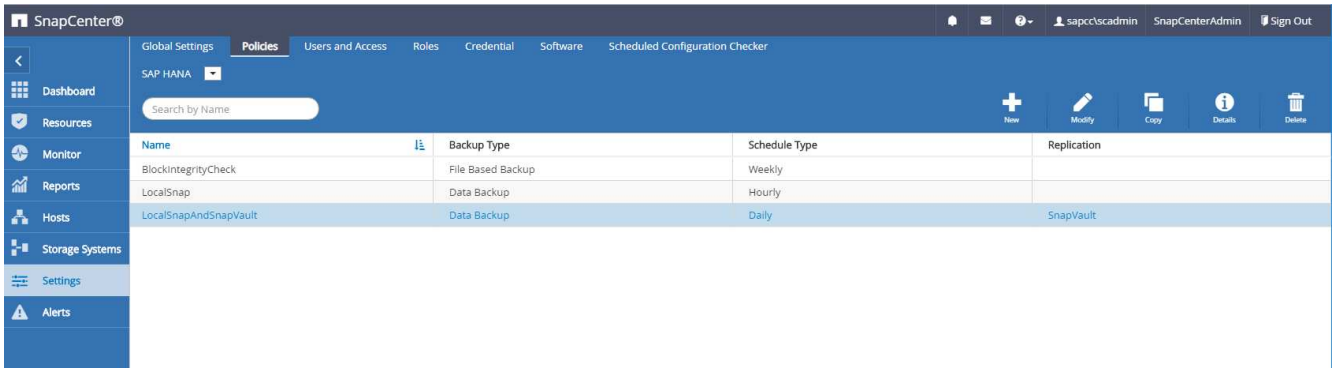
5. Konfigurieren Sie die Aufbewahrungseinstellungen für geplante Backups.



6. Klicken Sie auf der Seite Zusammenfassung auf Fertig stellen.



Die folgende Abbildung zeigt eine Zusammenfassung der konfigurierten Richtlinien.



Ressourcenspezifische SnapCenter Konfiguration für SAP HANA Datenbank-Backups

In diesem Abschnitt werden die Konfigurationsschritte für zwei Beispielkonfigurationen beschrieben.

- **SS2.**
  - SAP HANA MDC, ein mandantenfähiges Single-Host-System mit NFS für Storage-Zugriff
  - Die Ressource wird manuell in SnapCenter konfiguriert.
  - Die Ressource ist so konfiguriert, lokale Snapshot Backups zu erstellen und mithilfe eines wöchentlichen dateibasierten Backups die Blockintegritätsprüfungen für die SAP HANA Datenbank durchzuführen.
- **SS1.**
  - SAP HANA MDC, ein mandantenfähiges Single-Host-System mit NFS für Storage-Zugriff
  - Die Ressource wird mit SnapCenter automatisch erkannt.
  - Die Ressource ist so konfiguriert, dass sie lokale Snapshot Backups erstellt, mithilfe von SnapVault auf einen externen Backup-Storage repliziert und mithilfe eines wöchentlichen dateibasierten Backups die Blockintegritätsprüfungen für die SAP HANA Datenbank durchführt.

Die Unterschiede zwischen einem SAN-Attached Storage, einem Single-Container oder einem System mit mehreren Hosts werden in den entsprechenden Konfigurations- oder Workflow-Schritten wiedergegeben.

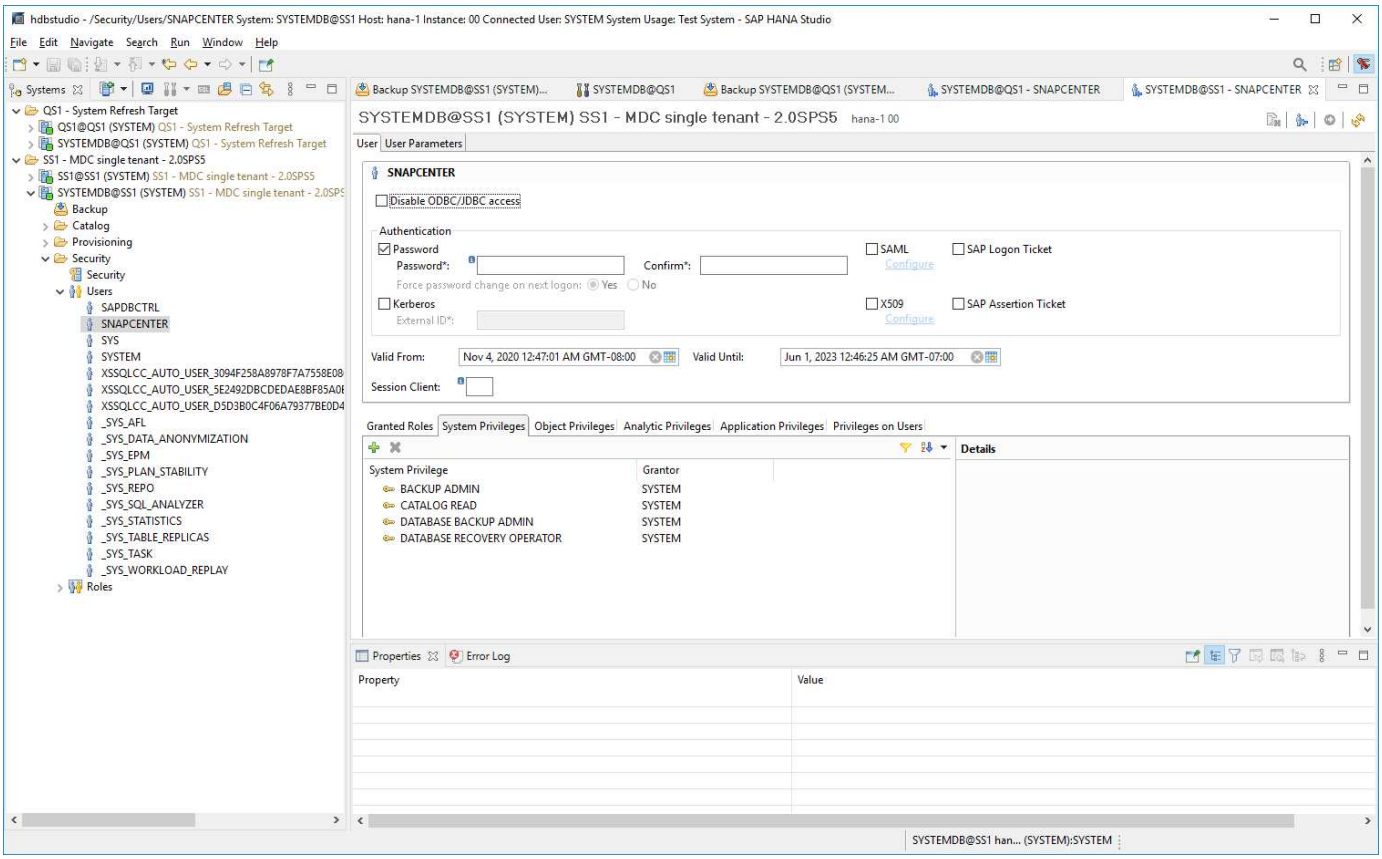
SAP HANA Backup-Benutzer und hdbuserstore-Konfiguration

NetApp empfiehlt, einen dedizierten Datenbankbenutzer in der HANA Datenbank zu konfigurieren, um Backup-Vorgänge mit SnapCenter auszuführen. Im zweiten Schritt wird für diesen Backup-Benutzer ein SAP HANA User Store Key konfiguriert und dieser User Store Key wird bei der Konfiguration des SnapCenter SAP HANA Plug-ins verwendet.

Die folgende Abbildung zeigt das SAP HANA Studio, über das der Backup-Benutzer erstellt werden kann.

> Die erforderlichen Berechtigungen wurden mit HANA 2.0 SPS5 Version geändert: Backup-Admin, Lesevorgang für den Katalog, Datenbank-Backup-Administrator und Datenbank-Recovery-Operator. Für ältere Versionen reichen der Backup-Administrator und der Lesevorgang des Katalogs aus.

> Bei einem SAP HANA MDC-System muss der Benutzer in der Systemdatenbank erstellt werden, da alle Backup-Befehle für das System und die Mandantendatenbanken über die Systemdatenbank ausgeführt werden.



Beim HANA-Plug-in-Host, auf dem das SAP HANA-Plug-in und der SAP-hdbsql-Client installiert sind, muss ein Benutzerspeicherschlüssel konfiguriert werden.

Userstore-Konfiguration auf dem SnapCenter-Server, der als zentraler HANA-Plug-in-Host verwendet wird

Wenn das SAP HANA-Plug-in und der SAP-hdbsql-Client unter Windows installiert sind, führt der lokale Systembenutzer die hdbsql-Befehle aus und wird standardmäßig in der Ressourcenkonfiguration konfiguriert. Da es sich bei dem Systembenutzer nicht um einen Anmeldesbenutzer handelt, muss die Konfiguration des Benutzerspeichers mit einem anderen Benutzer und mit der ausgeführt werden `-u <User>` Option.

```
hdbuserstore.exe -u SYSTEM set <key> <host>:<port> <database user>
<password>
```

Die SAP HANA hdbclient-Software muss zuerst auf dem Windows-Host installiert sein.

Konfiguration des Benutzerspeichers auf einem separaten Linux-Host, der als zentraler HANA-Plug-in-Host verwendet wird

Wenn das SAP HANA-Plug-in und der SAP-hdbsql-Client auf einem separaten Linux-Host installiert sind, wird der folgende Befehl für die User-Store-Konfiguration verwendet, wobei der Benutzer in der Ressourcenkonfiguration definiert ist:

```
hdbuserstore set <key> <host>:<port> <database user> <password>
```

Die SAP HANA hdbclient-Software muss zuerst auf dem Linux-Host installiert sein.

UserStore-Konfiguration auf dem HANA-Datenbank-Host

Wenn das SAP HANA-Plug-in auf dem HANA-Datenbank-Host bereitgestellt wird, wird der folgende Befehl für die User Store-Konfiguration mit dem verwendet `<sid>adm` Benutzer:

```
hdbuserstore set <key> <host>:<port> <database user> <password>
```

SnapCenter verwendet das `<sid>adm` Benutzer zur Kommunikation mit der HANA-Datenbank. Daher muss der User Store Key mit dem <`sid>adm` Benutzer auf dem Datenbank-Host konfiguriert werden.

In der Regel wird die SAP HANA hdbsql-Client-Software zusammen mit der Datenbank-Server-Installation installiert. Wenn dies nicht der Fall ist, muss der hdbclient zuerst installiert werden.

Konfiguration des Benutzerspeichers abhängig von der HANA Systemarchitektur

In einer SAP HANA MDC-Einzelmandant-Einrichtung, Port `3<instanceNo>13` Ist der Standard-Port für den SQL-Zugriff auf die Systemdatenbank und muss in der hdbuserstore-Konfiguration verwendet werden.

Für eine SAP HANA-Installation mit einem Container ist Port erforderlich `3<instanceNo>15` Ist der Standard-Port für den SQL-Zugriff auf den Indexserver und muss in der hdbuserstore-Konfiguration verwendet werden.

Für eine SAP HANA Einrichtung mit mehreren Hosts müssen die Benutzerspeicherschlüssel für alle Hosts konfiguriert werden. SnapCenter versucht mit jedem der angegebenen Schlüssel eine Verbindung zur Datenbank herzustellen und kann somit unabhängig vom Failover eines SAP HANA Service zu einem anderen Host funktionieren.

Anwendungskonfigurationsbeispiele

Im Lab-Setup wird eine gemischte SAP HANA Plug-in-Implementierung verwendet. Das HANA-Plug-in wird für einige HANA-Systeme auf dem SnapCenter-Server installiert und für andere Systeme auf den einzelnen HANA-Datenbankservern implementiert.

SAP HANA System SS1, MDC Einzelmieter, Instanz 00

Das HANA-Plug-in wurde auf dem Datenbank-Host implementiert. Daher muss der Schlüssel auf dem Datenbank-Host mit dem Benutzer ss1adm konfiguriert werden.

```
hana-1:/ # su - ss1adm
ss1adm@hana-1:/usr/sap/SS1/HDB00>
ss1adm@hana-1:/usr/sap/SS1/HDB00>
ss1adm@hana-1:/usr/sap/SS1/HDB00> hdbuserstore set SS1KEY hana-1:30013
SnapCenter password
ss1adm@hana-1:/usr/sap/SS1/HDB00> hdbuserstore list
DATA FILE       : /usr/sap/SS1/home/.hdb/hana-1/SSFS_HDB.DAT
KEY FILE        : /usr/sap/SS1/home/.hdb/hana-1/SSFS_HDB.KEY
KEY SS1KEY
  ENV : hana-1:30013
  USER: SnapCenter
KEY SS1SAPDBCTRLSS1
  ENV : hana-1:30015
  USER: SAPDBCTRL
ss1adm@hana-1:/usr/sap/SS1/HDB00>
```

- SAP HANA System MS1, Multihost MDC Einzelmandant, Instanz 00*

Für HANA sind mehrere Hostsysteme ein zentraler Plug-in-Host erforderlich, in unserem Setup haben wir den SnapCenter Server verwendet. Daher muss die Konfiguration des Benutzerspeichers auf dem SnapCenter-Server ausgeführt werden.

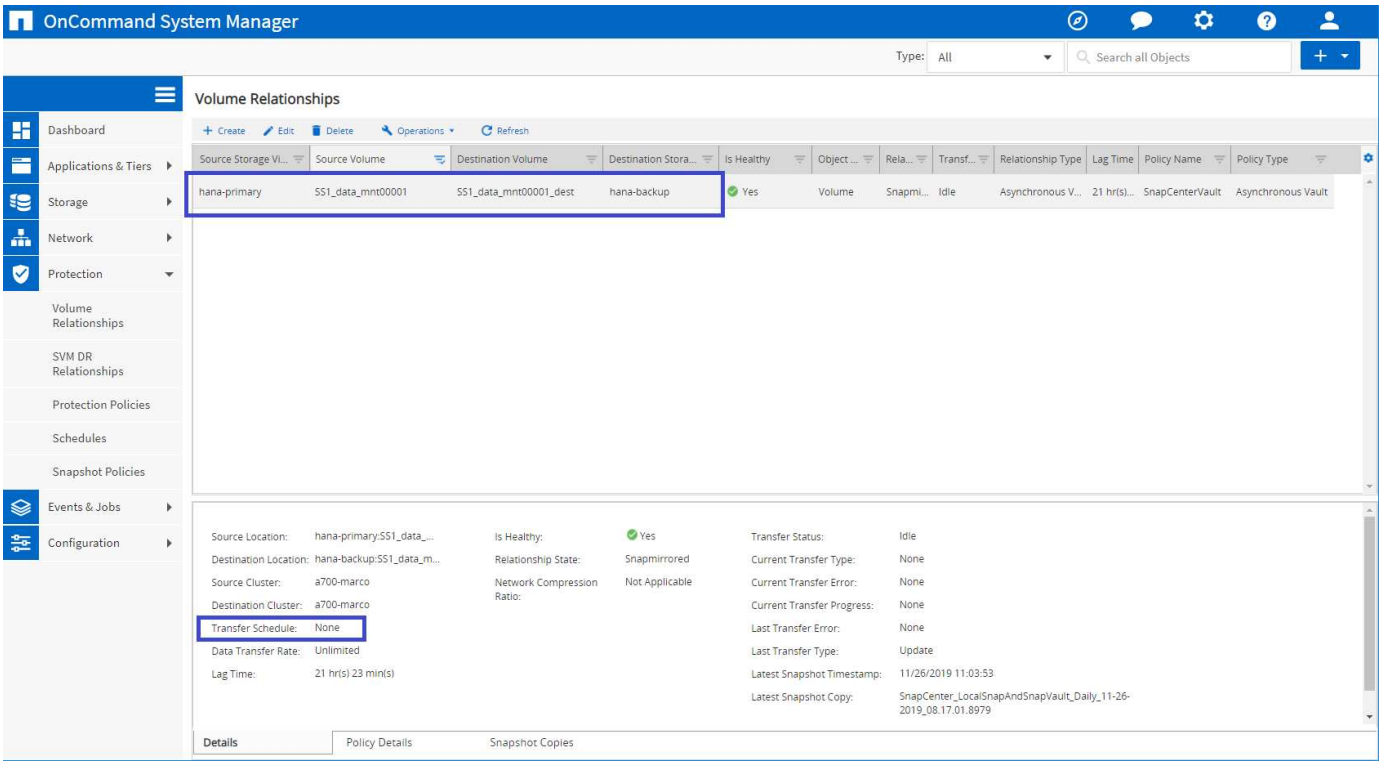
```
hdbuserstore.exe -u SYSTEM set MS1KEYHOST1 hana-4:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST2 hana-5:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST3 hana-6:30013 SNAPCENTER
password
C:\Program Files\sap\hdbclient>hdbuserstore.exe -u SYSTEM list
DATA FILE       : C:\ProgramData\.hdb\SNAPCENTER-43\S-1-5-18\SSFS_HDB.DAT
KEY FILE        : C:\ProgramData\.hdb\SNAPCENTER-43\S-1-5-18\SSFS_HDB.KEY
KEY MS1KEYHOST1
  ENV : hana-4:30013
  USER: SNAPCENTER
KEY MS1KEYHOST2
  ENV : hana-5:30013
  USER: SNAPCENTER
KEY MS1KEYHOST3
  ENV : hana-6:30013
  USER: SNAPCENTER
KEY SS2KEY
  ENV : hana-3:30013
  USER: SNAPCENTER
C:\Program Files\sap\hdbclient>
```

Konfiguration der Datensicherung auf externen Backup-Storage

Die Konfiguration der Datensicherungsbeziehung sowie der anfängliche Datentransfer müssen ausgeführt werden, bevor Replizierungs-Updates von SnapCenter gemanagt werden können.

Die folgende Abbildung zeigt die konfigurierte Sicherungsbeziehung für das SAP HANA-System SS1. Mit unserem Beispiel das Quellvolumen `SS1_data_mnt00001` Bei der SVM `hana-primary` Wird auf die SVM repliziert `hana-backup` Und das Ziel-Volume `SS1_data_mnt00001_dest`.

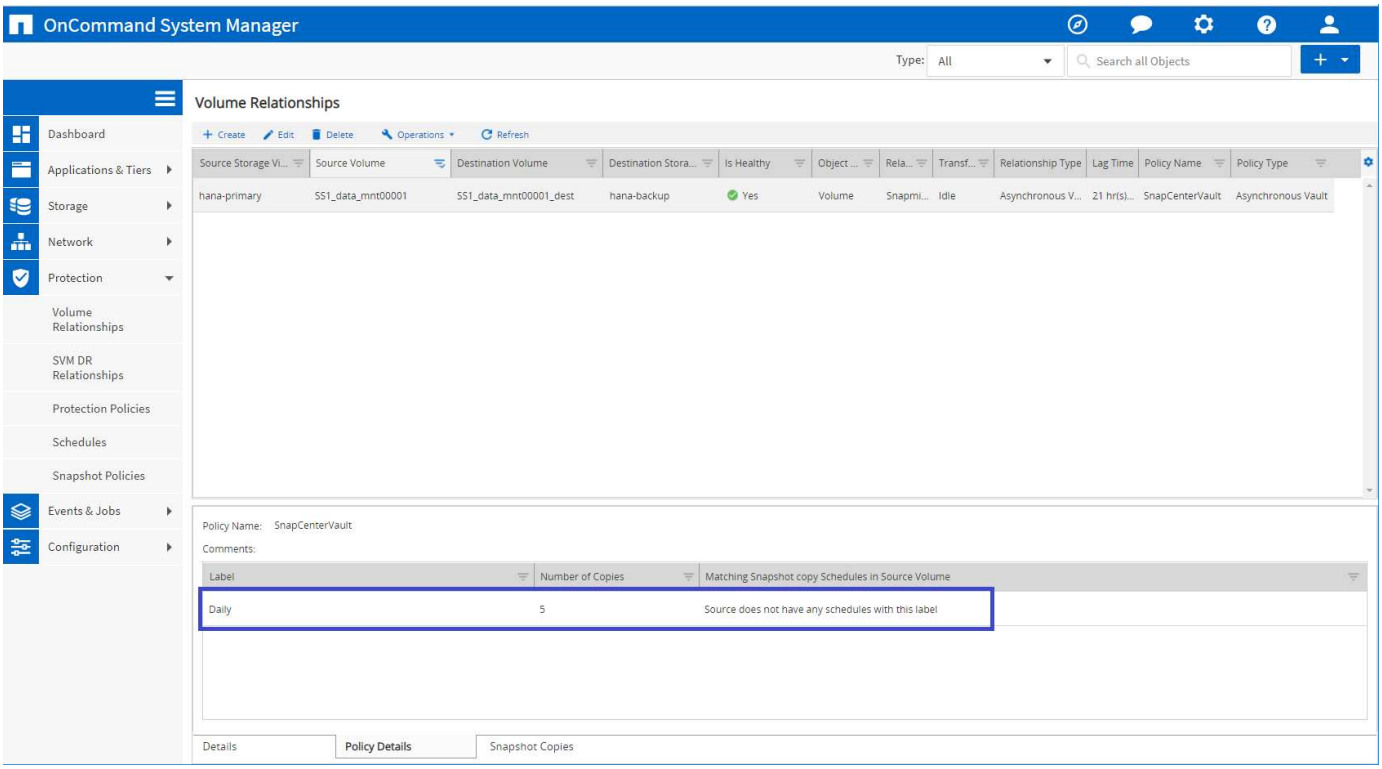
Der Zeitplan für die Beziehung muss auf „Keine“ gesetzt werden, da SnapCenter das SnapVault Update auslöst.



Die folgende Abbildung zeigt die Sicherungsrichtlinie. Die Sicherungsrichtlinie, die für die Schutzbeziehung verwendet wird, definiert das SnapMirror-Label und die Aufbewahrung von Backups im sekundären Storage. In unserem Beispiel ist das verwendete Etikett `Daily`, Und die Aufbewahrung ist auf 5 eingestellt.

Das SnapMirror-Label in der erstellten Richtlinie muss mit der in der Konfiguration der SnapCenter-Richtlinie definierten Beschriftung übereinstimmen. Weitere Informationen finden Sie unter "Richtlinie für tägliche Snapshot Backups mit SnapVault Replizierung".

Die Aufbewahrung für Backups im externen Backup-Storage wird in der Richtlinie definiert und durch ONTAP gesteuert.



Manuelle Konfiguration der HANA-Ressourcen

In diesem Abschnitt wird die manuelle Konfiguration der SAP HANA-Ressourcen SS2 und MS1 beschrieben.

- SS2 ist ein MDC-Einzelmandant-System mit einem Host
- MS1 ist ein MDC-Einzelmandant-System mit mehreren Hosts.

a. Wählen Sie auf der Registerkarte Ressourcen SAP HANA aus, und klicken Sie auf Add SAP HANA Database.

b. Geben Sie die Informationen zum Konfigurieren der SAP HANA-Datenbank ein, und klicken Sie auf Weiter.

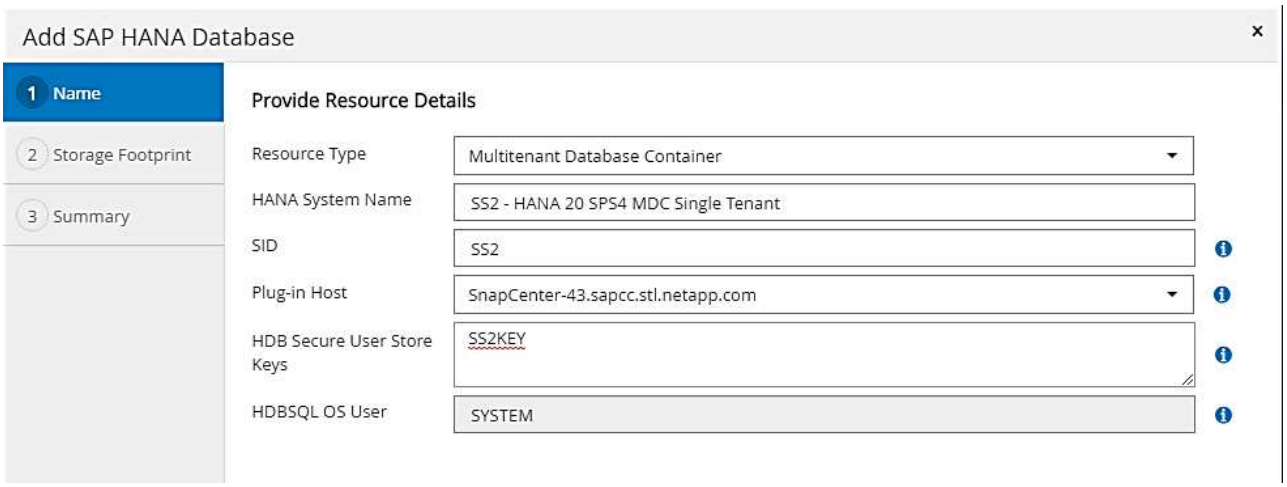
Wählen Sie in unserem Beispiel den Ressourcentyp Multitenant Database Container aus.

> Für ein HANA-System mit einem einzelnen Container muss der Ressourcentyp Single Container ausgewählt werden. Alle anderen Konfigurationsschritte sind identisch.

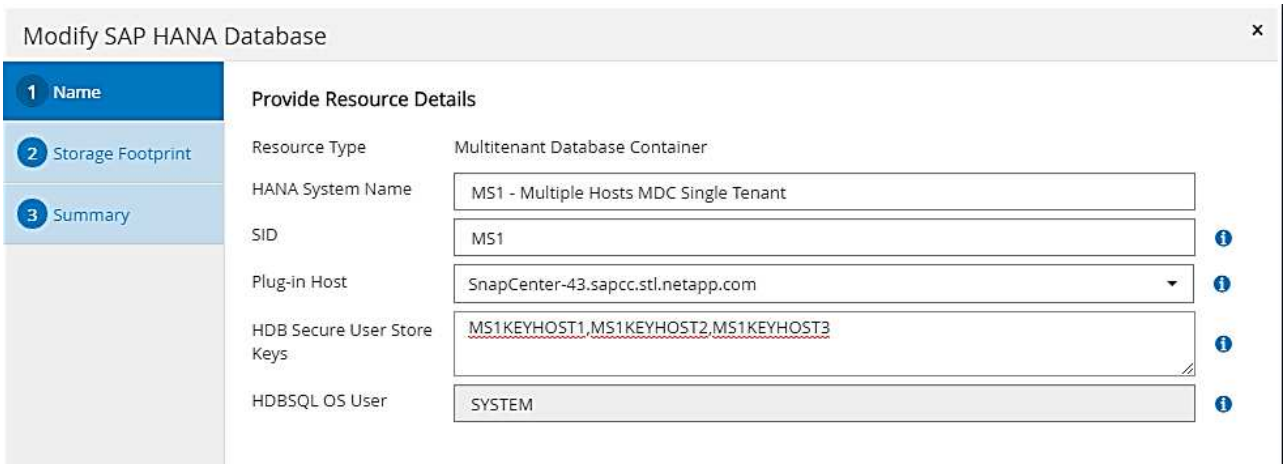
Für unser SAP HANA System ist SID SS2.

Der HANA-Plug-in-Host in unserem Beispiel ist der SnapCenter-Server.

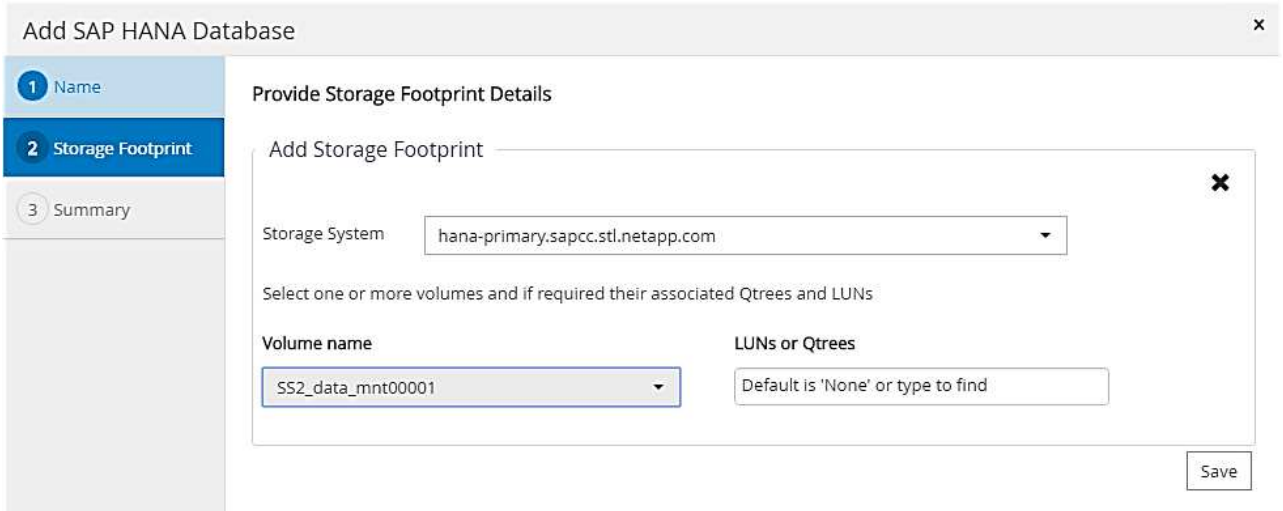
Der hdbuserstore-Schlüssel muss mit dem Schlüssel übereinstimmen, der für die HANA-Datenbank SS2 konfiguriert wurde. In unserem Beispiel ist es SS2KEY.



Bei einem SAP HANA-System mit mehreren Hosts müssen die hdbuserstore-Schlüssel für alle Hosts enthalten sein, wie in der folgenden Abbildung dargestellt. SnapCenter versucht, eine Verbindung mit der ersten Taste in der Liste herzustellen, und setzt den anderen Fall fort, falls der erste Schlüssel nicht funktioniert. Dies ist zur Unterstützung von HANA Failover in einem System mit mehreren Hosts mit Worker und Standby-Hosts erforderlich.

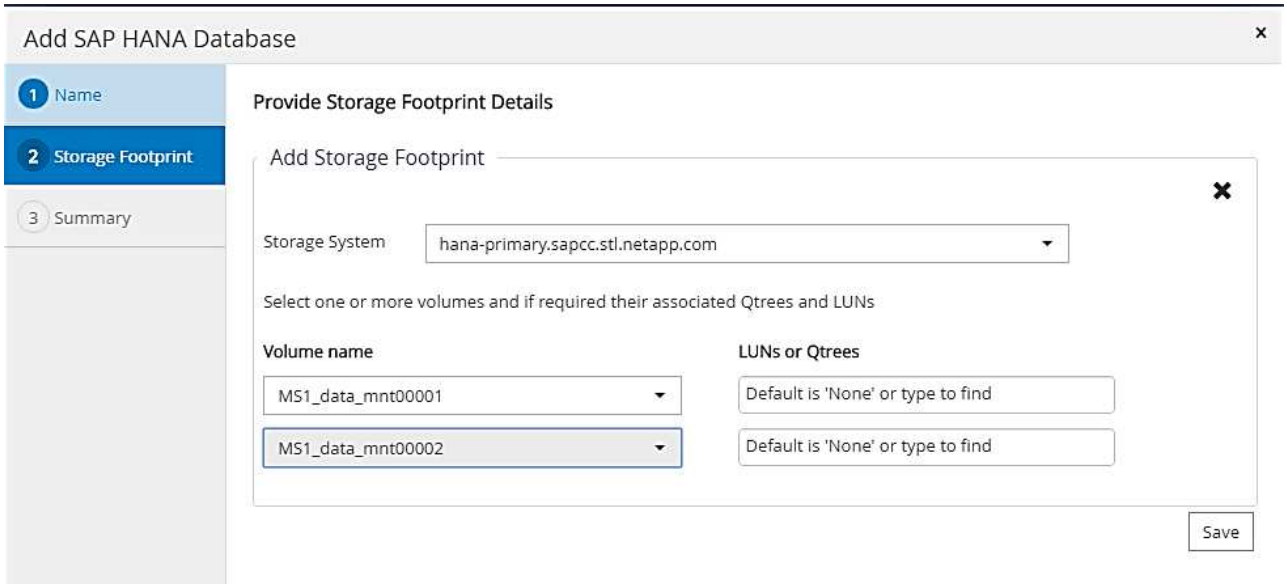


c. Wählen Sie die erforderlichen Daten für das Storage-System (SVM) und den Volume-Namen aus.



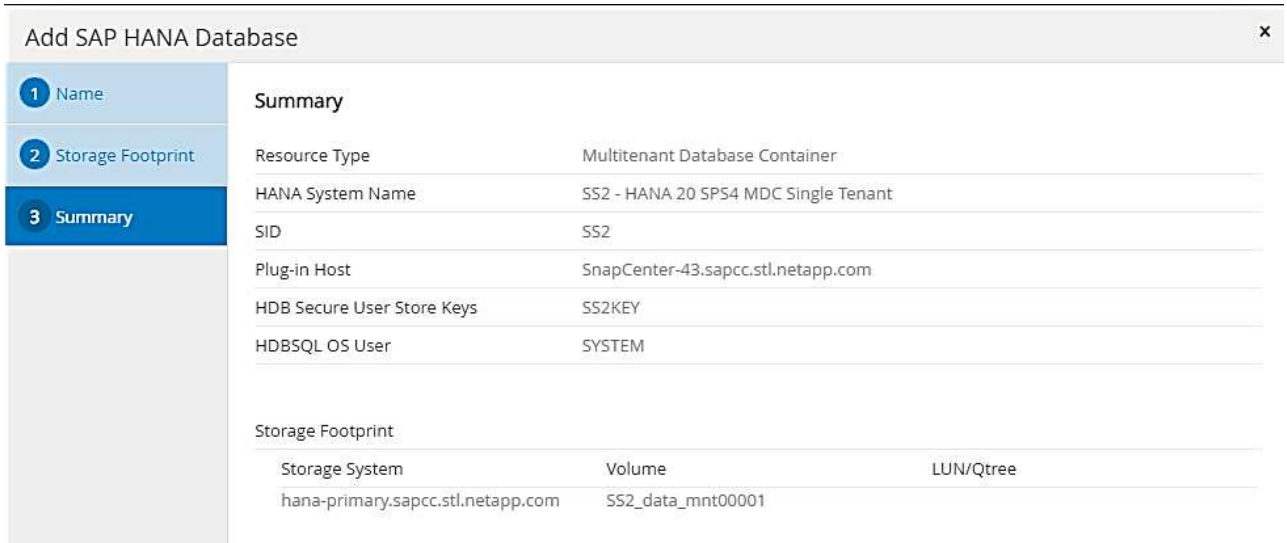
Für eine Fibre-Channel-SAN-Konfiguration muss auch die LUN ausgewählt werden.

Bei einem SAP HANA-System mit mehreren Hosts müssen alle Datenvolumen des SAP HANA Systems ausgewählt werden, wie in der folgenden Abbildung dargestellt.



Der Übersichtsbildschirm der Ressourcenkonfiguration wird angezeigt.

a. Klicken Sie auf Fertig stellen, um die SAP HANA-Datenbank hinzuzufügen.



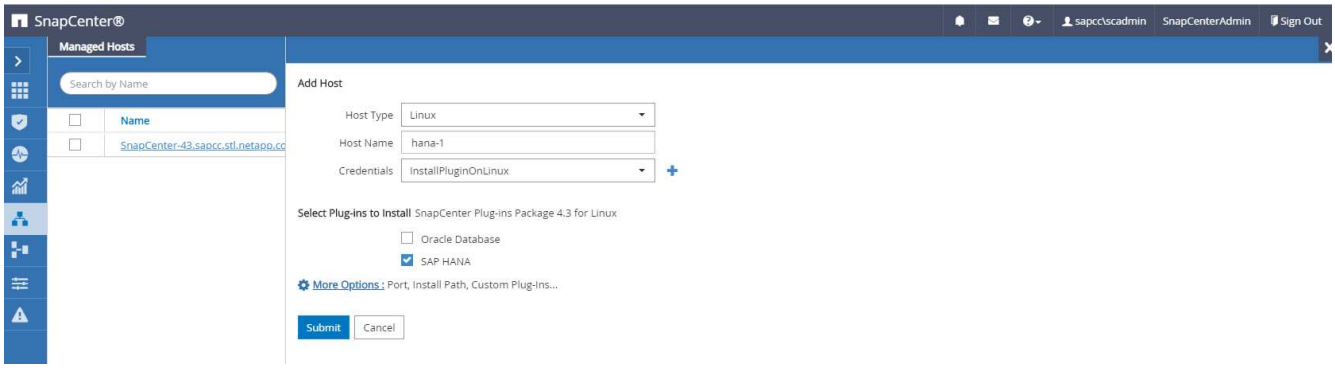
b. Wenn die Ressourcenkonfiguration abgeschlossen ist, führen Sie die Konfiguration des Ressourcenschutzes aus, wie im Abschnitt beschrieben"Konfiguration für Ressourcenschutz".

Automatische Erkennung von HANA-Datenbanken

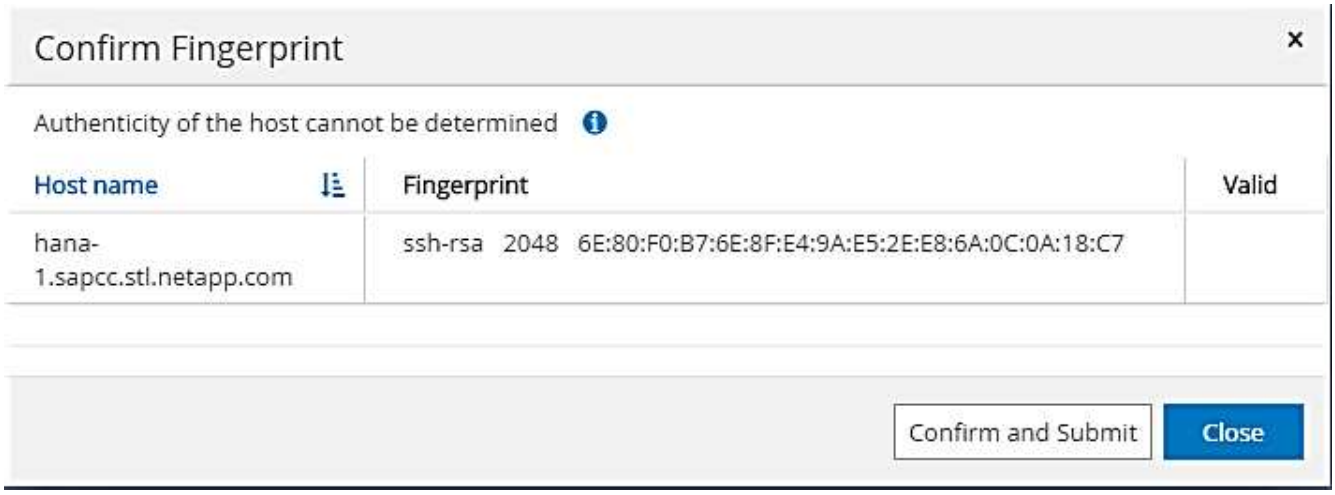
In diesem Abschnitt wird die automatische Erkennung der SAP HANA-Ressource SS1 (Single-Host-MDC-Einzelmandant-System mit NFS) beschrieben. Alle beschriebenen Schritte sind identisch mit einem HANA-Einzelcontainer, HANA-MDC-Systemen mehrerer Mandanten und einem HANA-System, das Fibre Channel-SAN verwendet.

Für das SAP HANA Plug-in ist Java 64-Bit Version 1.8 erforderlich. Java muss auf dem Host installiert sein, bevor das SAP HANA Plug-in bereitgestellt wird.

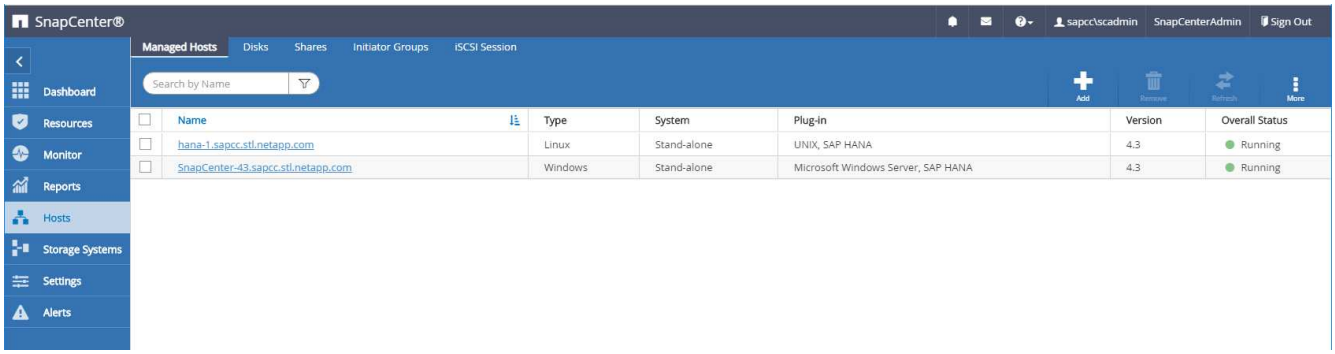
1. Klicken Sie auf der Registerkarte Host auf Hinzufügen.
2. Geben Sie Host-Informationen an, und wählen Sie das zu installierende SAP HANA-Plug-in aus. Klicken Sie Auf Senden.



3. Bestätigen Sie den Fingerabdruck.



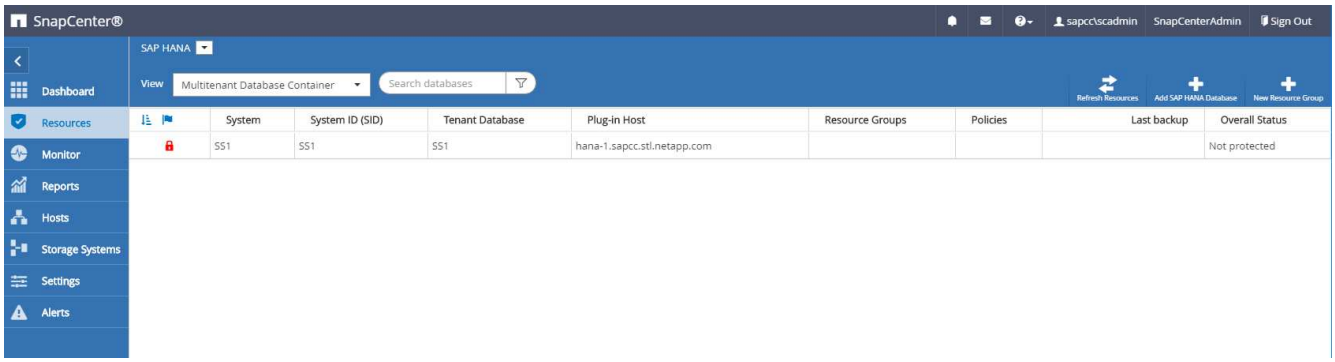
Die Installation des HANA-Plug-ins und des Linux-Plug-ins wird automatisch gestartet. Nach Abschluss der Installation wird in der Statusspalte des Hosts die Ausführung angezeigt. Der Bildschirm zeigt auch, dass das Linux-Plug-in zusammen mit dem HANA-Plug-in installiert wird.



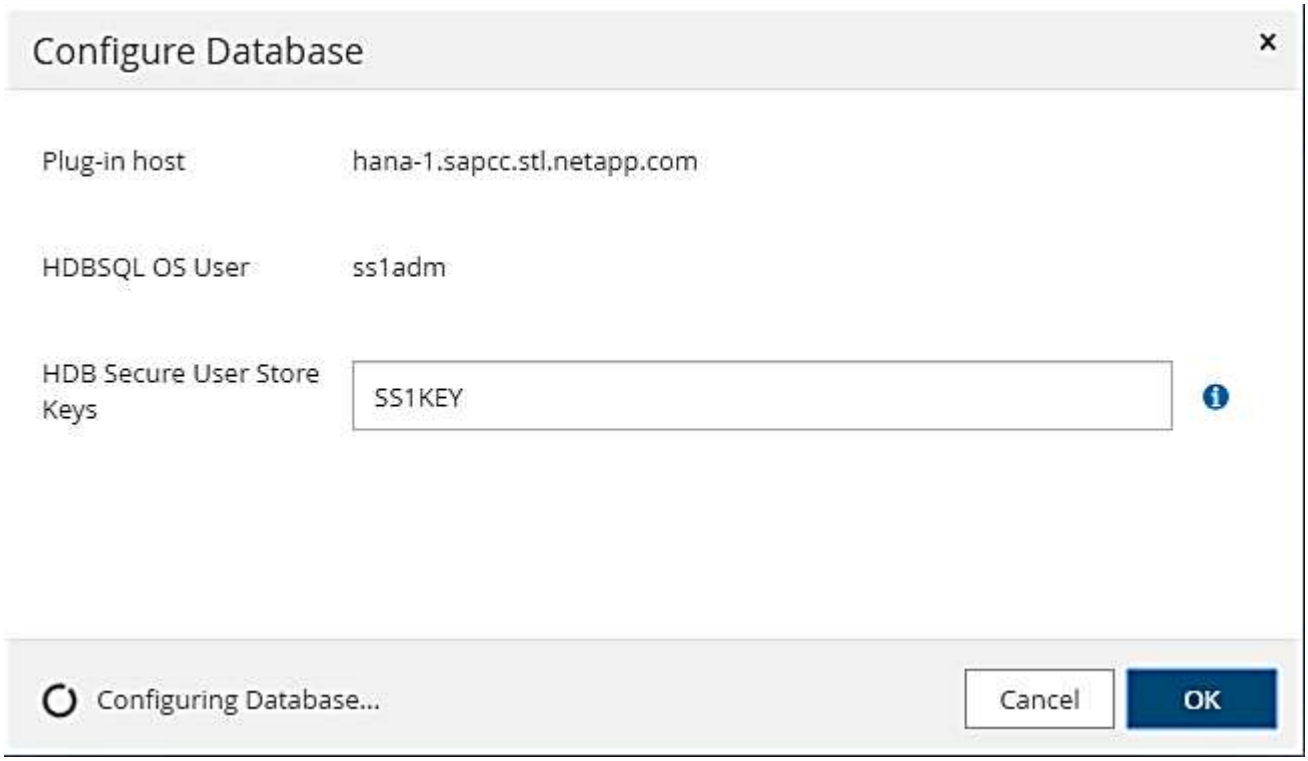
Nach der Plug-in-Installation startet der automatische Erkennungsvorgang der HANA-Ressource automatisch. Im Bildschirm Ressourcen wird eine neue Ressource erstellt, die mit dem roten Vorhängeschloss-Symbol als gesperrt markiert ist.

4. Wählen Sie und klicken Sie auf die Ressource, um mit der Konfiguration fortzufahren.

Sie können den automatischen Erkennungsvorgang auch manuell im Bildschirm Ressourcen auslösen, indem Sie auf Ressourcen aktualisieren klicken.

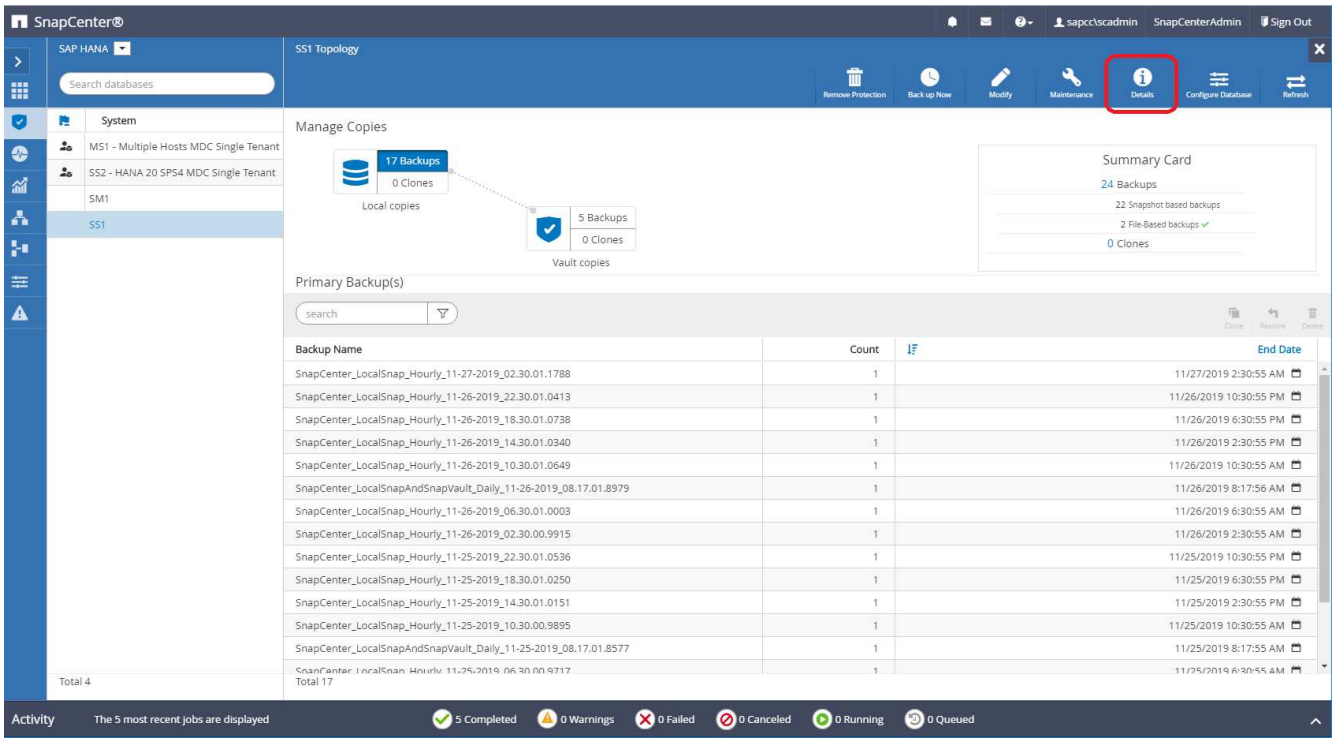


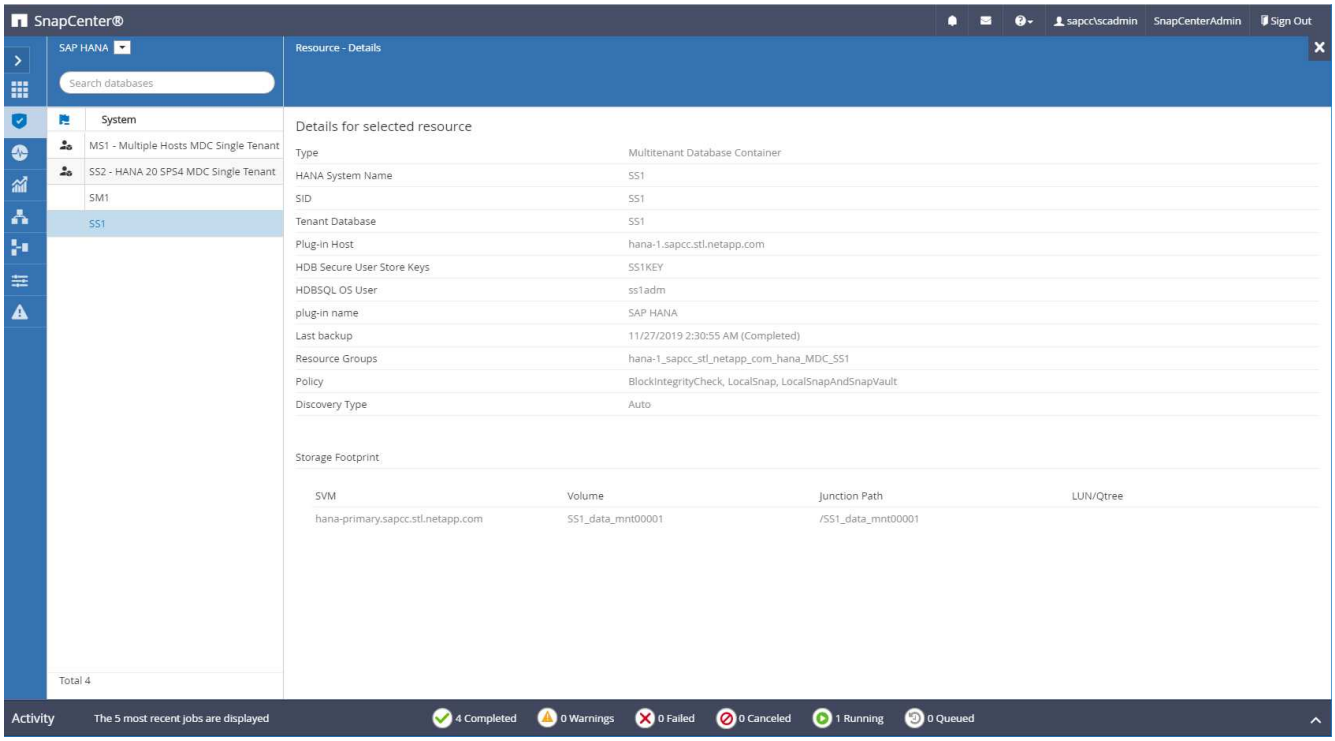
5. Geben Sie den UserStore-Schlüssel für die HANA-Datenbank an.



Der zweite Ebene-Prozess der automatischen Bestandsaufnahme beginnt, bei dem Mandantendaten und Storage-Platzbedarf erfasst werden.

6. Klicken Sie auf Details, um die Konfigurationsinformationen der HANA-Ressource in der Ansicht der Ressourcentopologie anzuzeigen.





Wenn die Ressourcenkonfiguration abgeschlossen ist, muss die Konfiguration des Ressourcenschutzes wie im folgenden Abschnitt beschrieben ausgeführt werden.

Konfiguration für Ressourcenschutz

In diesem Abschnitt wird die Konfiguration für den Ressourcenschutz beschrieben. Die Ressourcenschutzkonfiguration ist dieselbe, unabhängig davon, ob die Ressource automatisch erkannt oder manuell konfiguriert wurde. Und ist für alle HANA-Architekturen, einzelne oder mehrere Hosts, einzelnen Container oder MDC-Systeme identisch.

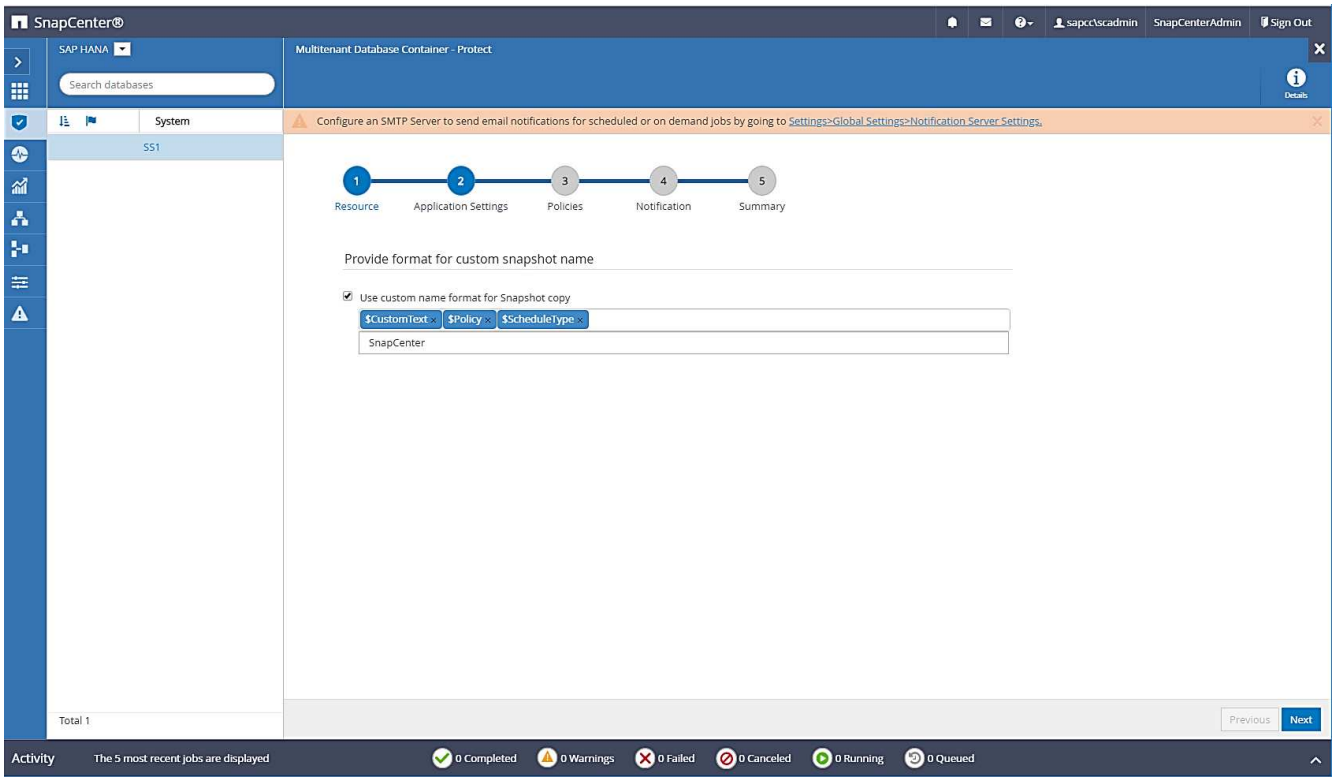
1. Doppelklicken Sie auf der Registerkarte Ressourcen auf die Ressource.
2. Konfigurieren Sie ein benutzerdefiniertes Namensformat für die Snapshot Kopie.

> NetApp empfiehlt den Einsatz einer benutzerdefinierten Snapshot Kopie, um schnell ermitteln zu können, mit welcher Richtlinie und welche Zeitplantypen Backups erstellt wurden. Durch Hinzufügen des Zeitplantyps zum Namen der Snapshot Kopie können Sie zwischen geplanten und On-Demand-Backups unterscheiden. Der `schedule name` String für On-Demand-Backups ist leer, während geplante Backups den String enthalten `Hourly`, `Daily`, `or Weekly`.

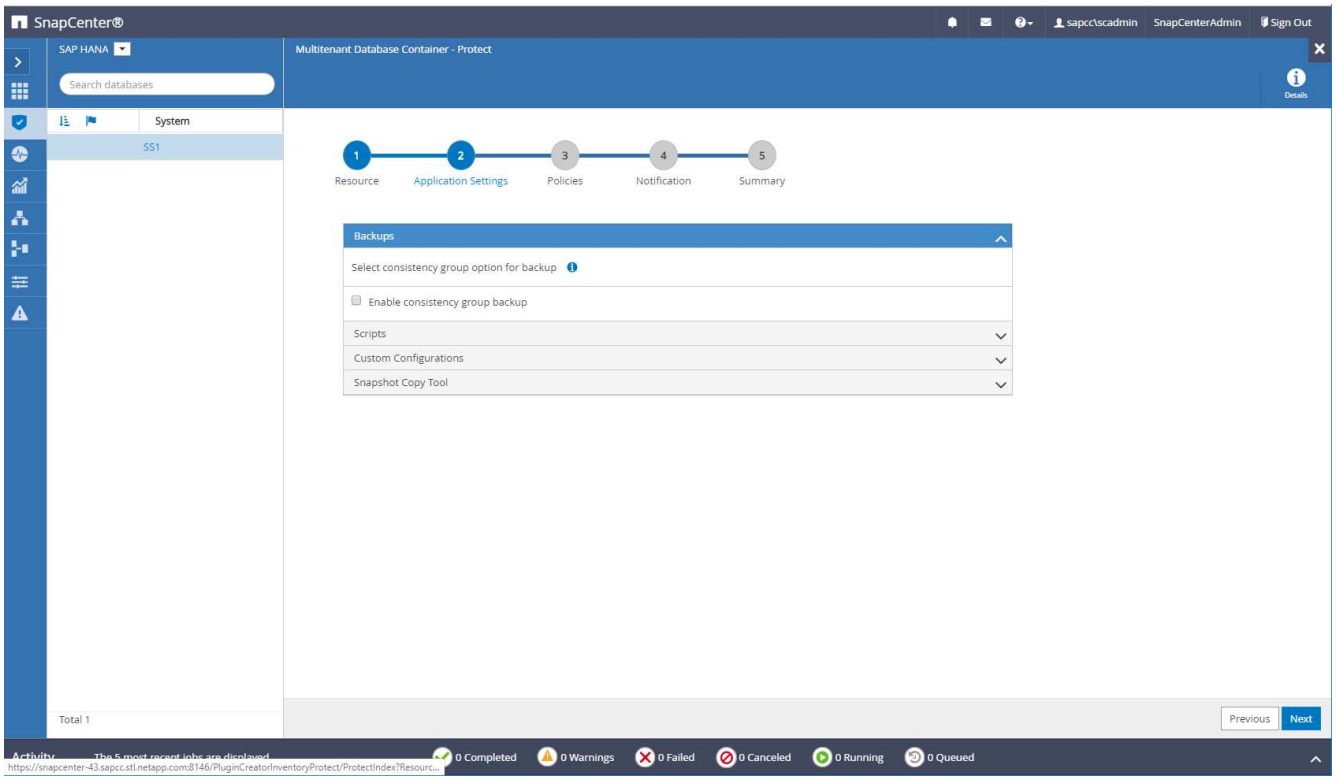
In der Konfiguration der folgenden Abbildung haben die Namen von Backup- und Snapshot-Kopien das folgende Format:

- Stündliches Backup geplant: `SnapCenter_LocalSnap_Hourly_<time_stamp>`
- Täglich geplantes Backup: `SnapCenter_LocalSnapAndSnapVault_Daily_<time_stamp>`
- Stündliches On-Demand-Backup: `SnapCenter_LocalSnap_<time_stamp>`
- Tägliches On-Demand Backup: `SnapCenter_LocalSnapAndSnapVault_<time_stamp>`

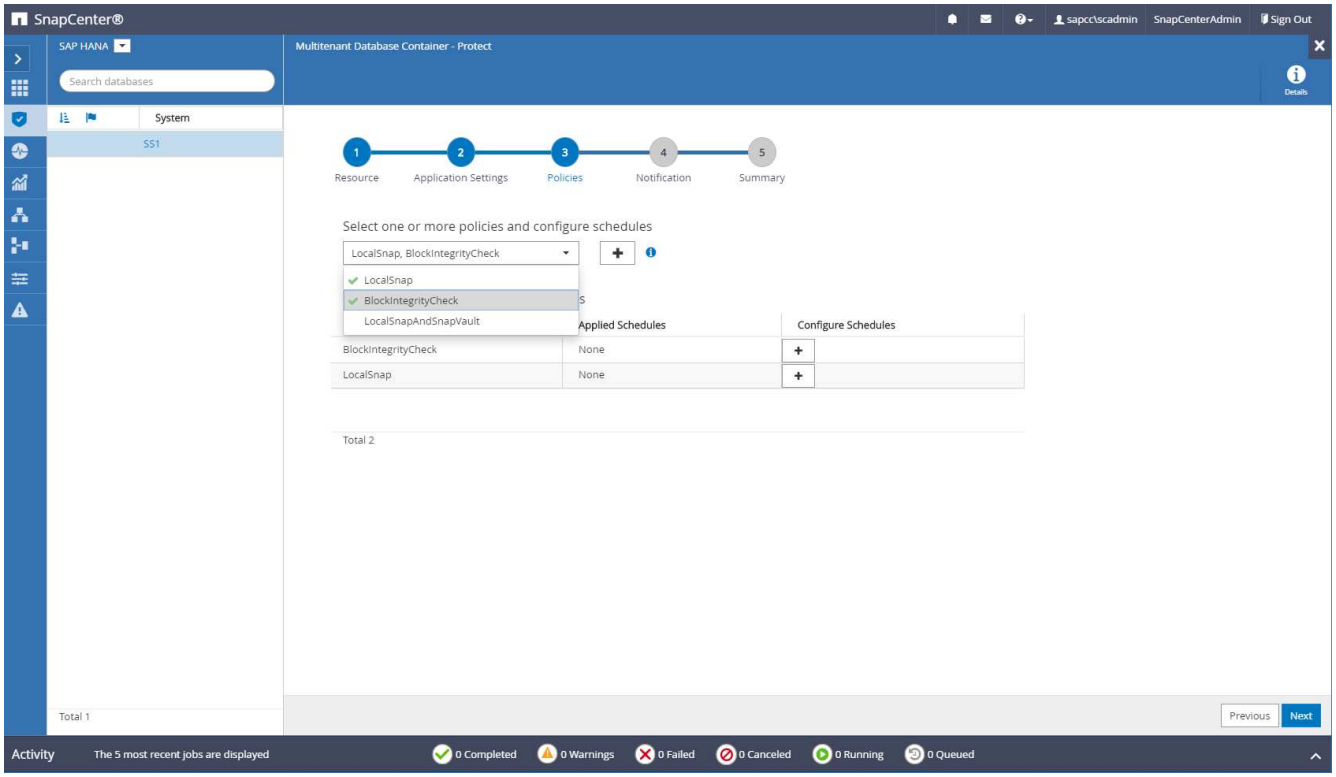
> Obwohl eine Aufbewahrung für On-Demand-Backups in der Richtlinienkonfiguration definiert wird, wird die allgemeine Ordnung und Sauberkeit nur dann ausgeführt, wenn ein weiteres On-Demand-Backup ausgeführt wird. Daher müssen On-Demand-Backups in der Regel manuell in SnapCenter gelöscht werden, um sicherzustellen, dass diese Backups auch im SAP HANA Backup-Katalog gelöscht werden und dass die allgemeine Ordnung der Protokollsicherung nicht auf einem alten On-Demand-Backup basiert.



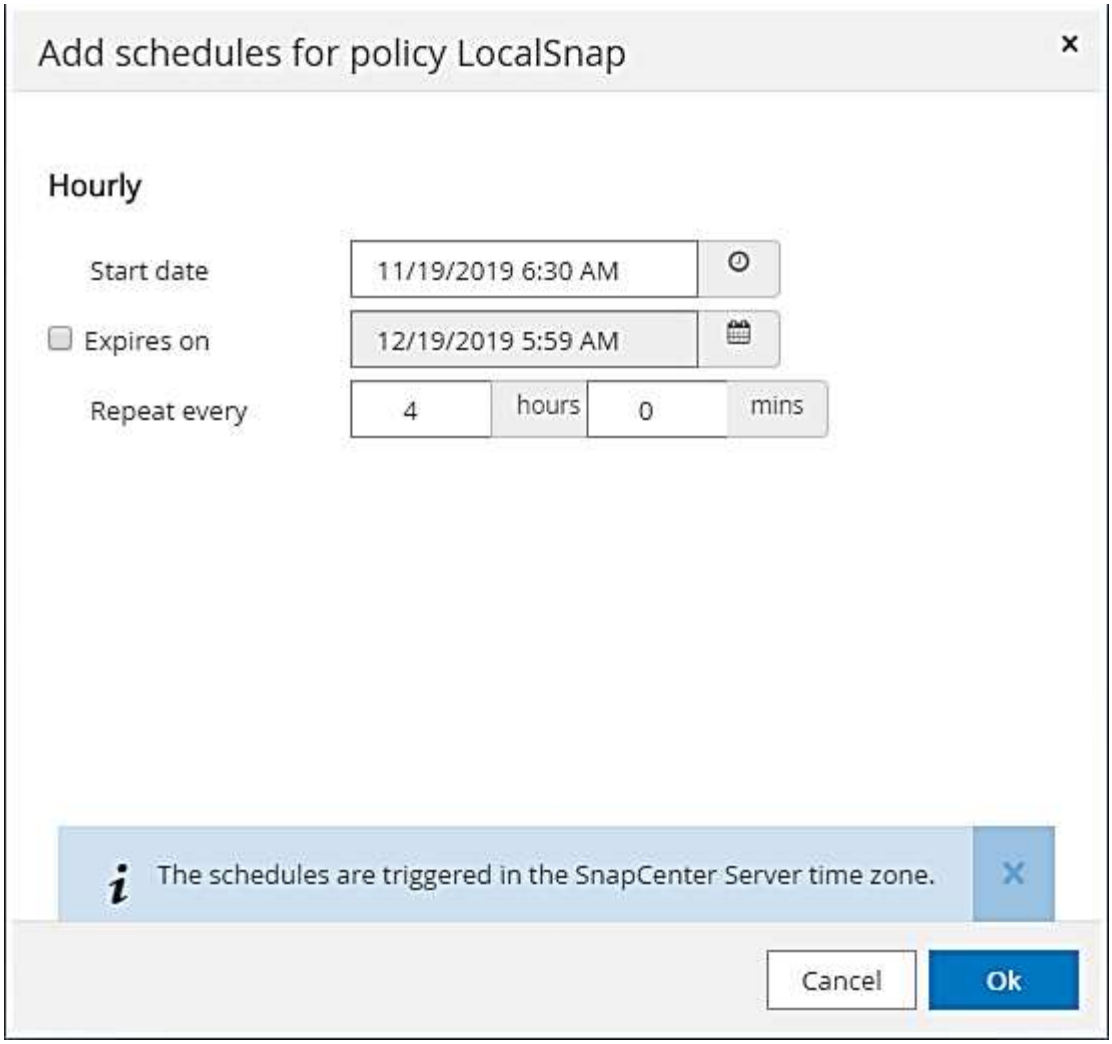
3. Auf der Seite „Anwendungseinstellungen“ müssen keine spezifischen Einstellungen vorgenommen werden. Klicken Sie Auf Weiter.



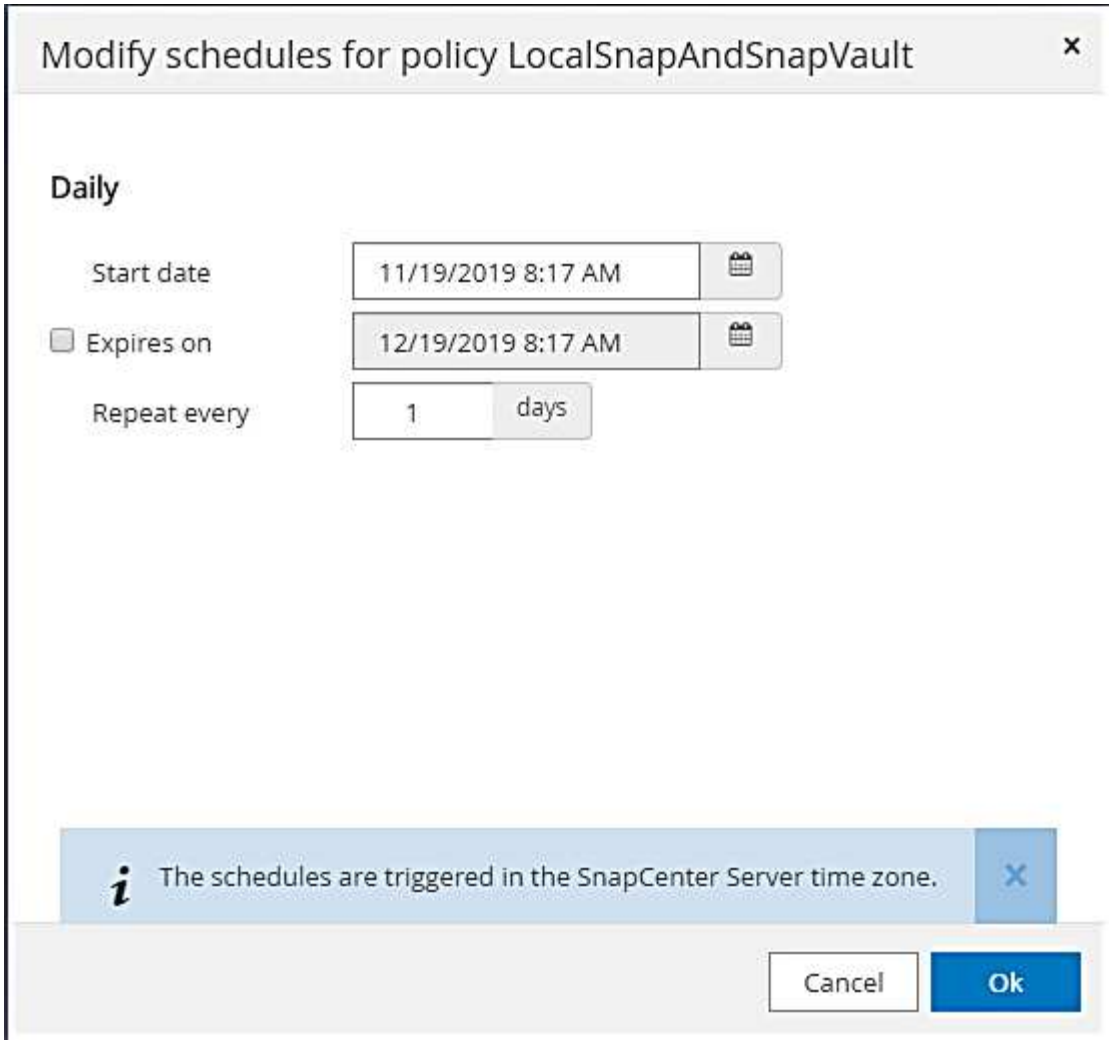
4. Wählen Sie die Richtlinien aus, die der Ressource hinzugefügt werden sollen.



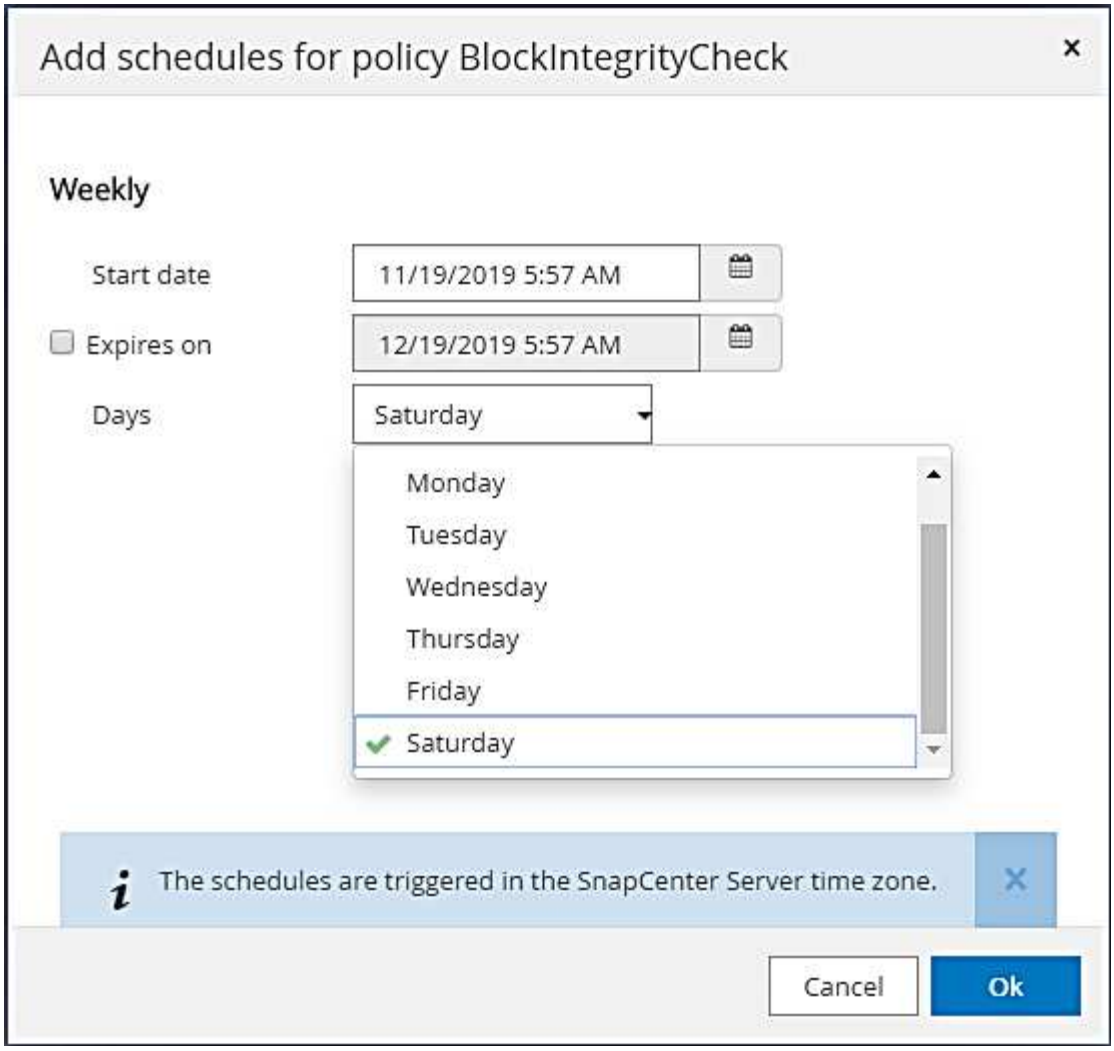
5. Legen Sie den Zeitplan für die LocalSnap-Richtlinie fest (in diesem Beispiel alle vier Stunden).



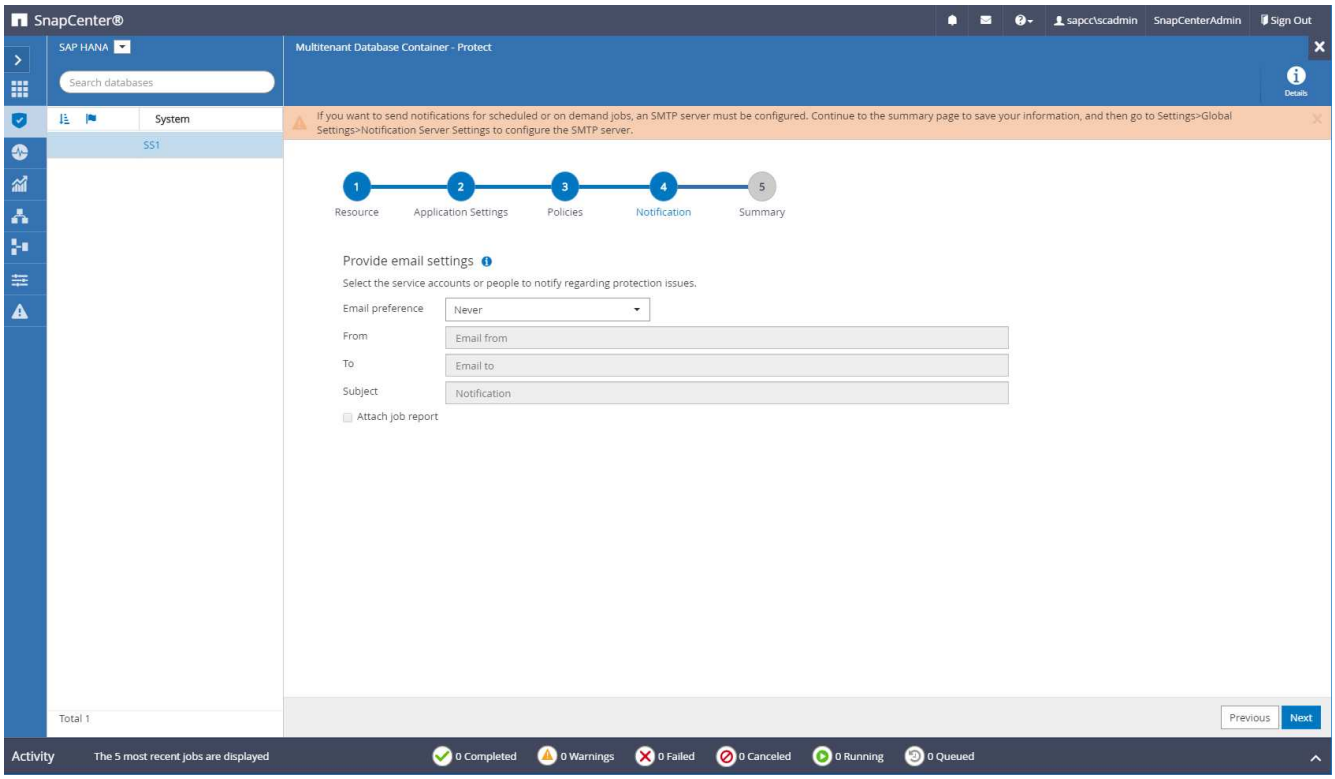
6. Legen Sie den Zeitplan für die LocalSnapAndSnapVault-Richtlinie fest (in diesem Beispiel einmal pro Tag).



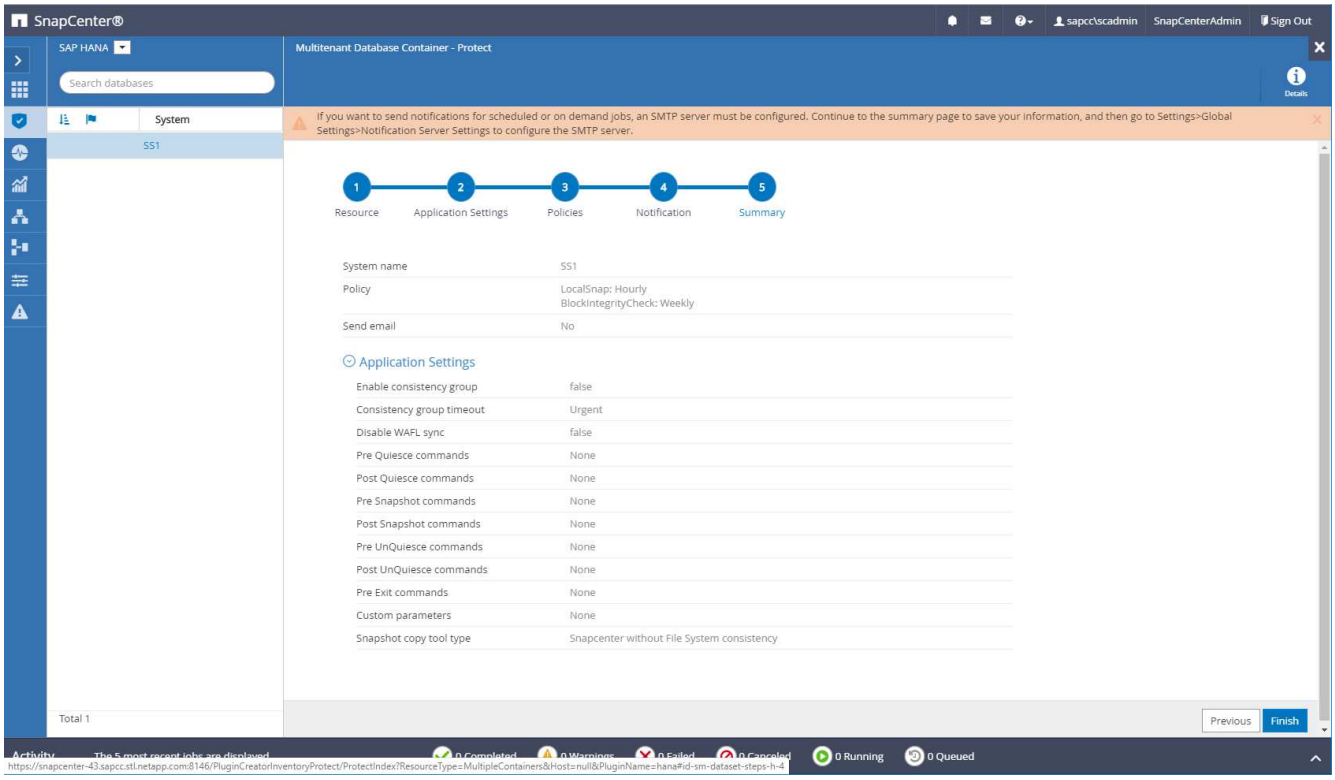
7. Legen Sie den Zeitplan für die Richtlinie zur Integritätsprüfung der Blöcke fest (in diesem Beispiel einmal pro Woche).



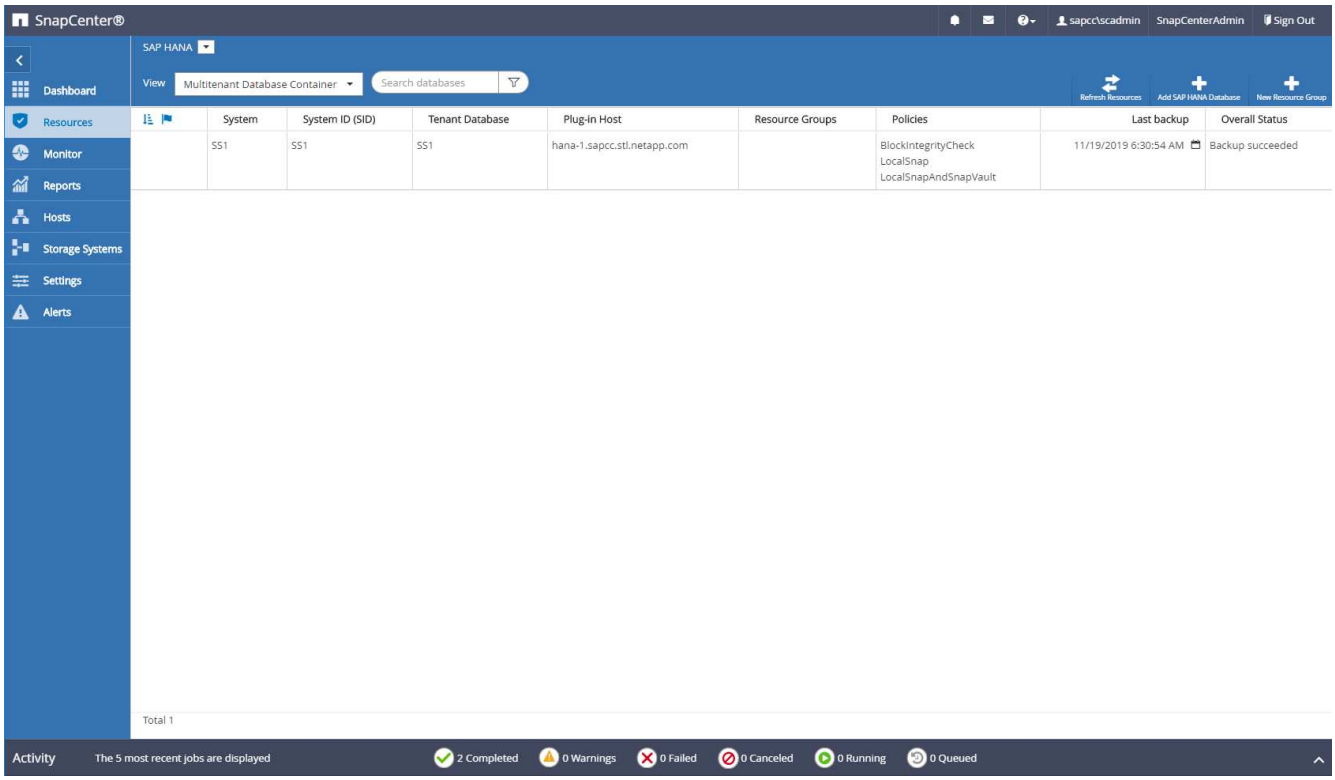
8. Geben Sie Informationen zur E-Mail-Benachrichtigung an.



9. Klicken Sie auf der Seite Zusammenfassung auf Fertig stellen.



10. On-Demand-Backups können jetzt auf der Topologieseite erstellt werden. Die geplanten Backups werden basierend auf den Konfigurationseinstellungen ausgeführt.



Zusätzliche Konfigurationsschritte für Fibre Channel SAN-Umgebungen

Je nach HANA-Version und HANA-Plug-in-Implementierung sind für Umgebungen, in denen die SAP HANA-Systeme Fibre Channel und das XFS-Dateisystem nutzen, zusätzliche Konfigurationsschritte erforderlich.

Diese zusätzlichen Konfigurationsschritte sind nur für HANA-Ressourcen erforderlich, die in SnapCenter manuell konfiguriert werden. Außerdem wird es nur für HANA 1.0 und HANA 2.0-Versionen bis SPS2 benötigt.

Wenn der Speicherpunkt für ein HANA Backup von SnapCenter in SAP HANA ausgelöst wird, schreibt SAP HANA als letzter Schritt Snapshot-ID-Dateien für jeden Mandanten und Datenbankservice (z. B. `/hana/data/SID/mnt00001/hdb00001/snapshot_databackup_0_1`). Diese Dateien sind Teil des Daten-Volumes im Storage und sind daher Teil der Storage-Snapshot-Kopie. Diese Datei ist bei der Durchführung einer Recovery in einer Situation, in der das Backup wiederhergestellt wird, obligatorisch. Durch Metadaten-Caching mit dem XFS-Dateisystem auf dem Linux-Host wird die Datei auf der Speicherebene nicht sofort sichtbar. Die standardmäßige XFS-Konfiguration für das Metadaten-Caching beträgt 30 Sekunden.

Mit HANA 2.0 SPS3 änderte SAP den Schreibvorgang dieser Snapshot ID-Dateien in synchron, sodass es kein Problem ist, Metadaten-Caching zu verwenden.

Wird bei SnapCenter 4.3 das HANA Plug-in auf dem Datenbank-Host bereitgestellt, führt das Linux Plug-in vor dem Auslösen des Storage-Snapshots einen Dateisystemputz-Vorgang auf dem Host durch. In diesem Fall stellt das Metadaten-Caching keine Probleme dar.

In SnapCenter müssen Sie ein konfigurieren `postquiesce` Befehl, der wartet, bis der XFS-Metadatencache auf die Festplattenebene gespeichert wird.

Die tatsächliche Konfiguration des Metadaten-Caching kann mit folgendem Befehl überprüft werden:

```
stlrx300s8-2:/ # sysctl -A | grep xfssyncd_centisecs
fs.xfs.xfssyncd_centisecs = 3000
```

NetApp empfiehlt, die Wartezeit auf eine doppelt so hohe Wartezeit von zu verwenden `fs.xfs.xfssyncd_centisecs` Parameter. Da der Standardwert 30 Sekunden beträgt, setzen Sie den Befehl „Sleep“ auf 60 Sekunden.

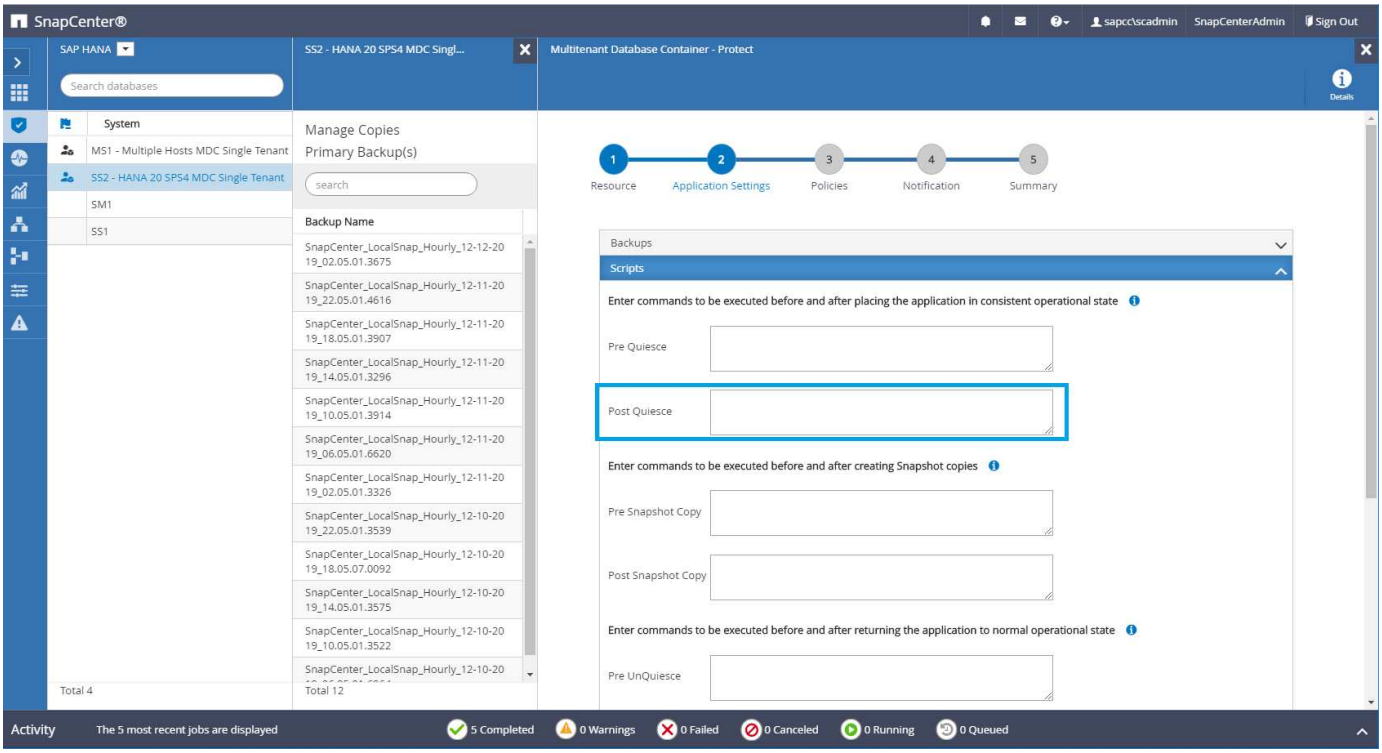
Wird der SnapCenter-Server als zentraler HANA-Plug-in-Host genutzt, kann eine Batch-Datei verwendet werden. Die Batch-Datei muss folgenden Inhalt haben:

```
@echo off
waitfor AnyThing /t 60 2>NUL
Exit /b 0
```

Die Batch-Datei kann z.B. als gespeichert werden `C:\Program Files\NetApp\Wait60Sec.bat`. In der Ressourcenschutzkonfiguration muss die Batch-Datei als Post Quiesce-Befehl hinzugefügt werden.

Wenn ein separater Linux-Host als zentraler HANA-Plug-in-Host verwendet wird, müssen Sie den Befehl konfigurieren `/bin/sleep 60` Als Post-Quiesce-Befehl in der SnapCenter-UI.

Die folgende Abbildung zeigt den Befehl Post Quiesce im Konfigurationsbildschirm für Ressourcenschutz.



Ressourcenspezifische SnapCenter Konfiguration für Backups außerhalb von Datenvolumen

Das Backup von nicht-Daten-Volumes ist ein integrierter Teil des SAP HANA Plug-ins. Der Schutz des Datenbankdatenvolumens reicht aus, um die SAP HANA Datenbank zu

einem bestimmten Zeitpunkt wiederherzustellen, vorausgesetzt, die Ressourcen zur Datenbankinstallation und die erforderlichen Protokolle sind weiterhin verfügbar.

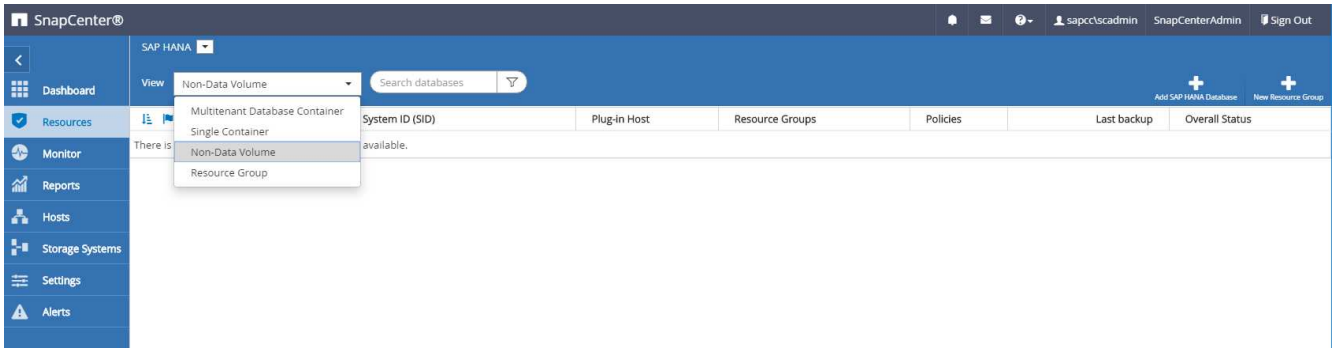
Um das Recovery von Situationen durchzuführen, in denen andere nicht-Datendateien wiederhergestellt werden müssen, empfiehlt NetApp, eine zusätzliche Backup-Strategie für nicht-Daten-Volumes zu entwickeln, um das SAP HANA Datenbank-Backup zu erweitern. Je nach Ihren spezifischen Anforderungen kann sich das Backup von nicht-Daten-Volumes in den Einstellungen für die Planungsfrequenz und -Aufbewahrung unterscheiden, und Sie sollten bedenken, wie oft nicht-Datendateien geändert werden. Zum Beispiel das HANA Volume `/hana/shared` Enthält ausführbare Dateien, aber auch SAP HANA Trace-Dateien. Zwar ändern sich ausführbare Dateien nur beim Upgrade der SAP HANA Datenbank, doch benötigen die SAP HANA Trace-Dateien möglicherweise eine höhere Backup-Häufigkeit, um Problemsituationen mit SAP HANA zu analysieren.

Dank des nicht-Daten-Volume-Backups von SnapCenter können Snapshot-Kopien aller relevanten Volumes in wenigen Sekunden mit derselben Speichereffizienz erstellt werden wie bei SAP HANA-Datenbank-Backups. Der Unterschied liegt darin, dass keine SQL Kommunikation mit der SAP HANA Datenbank erforderlich ist.

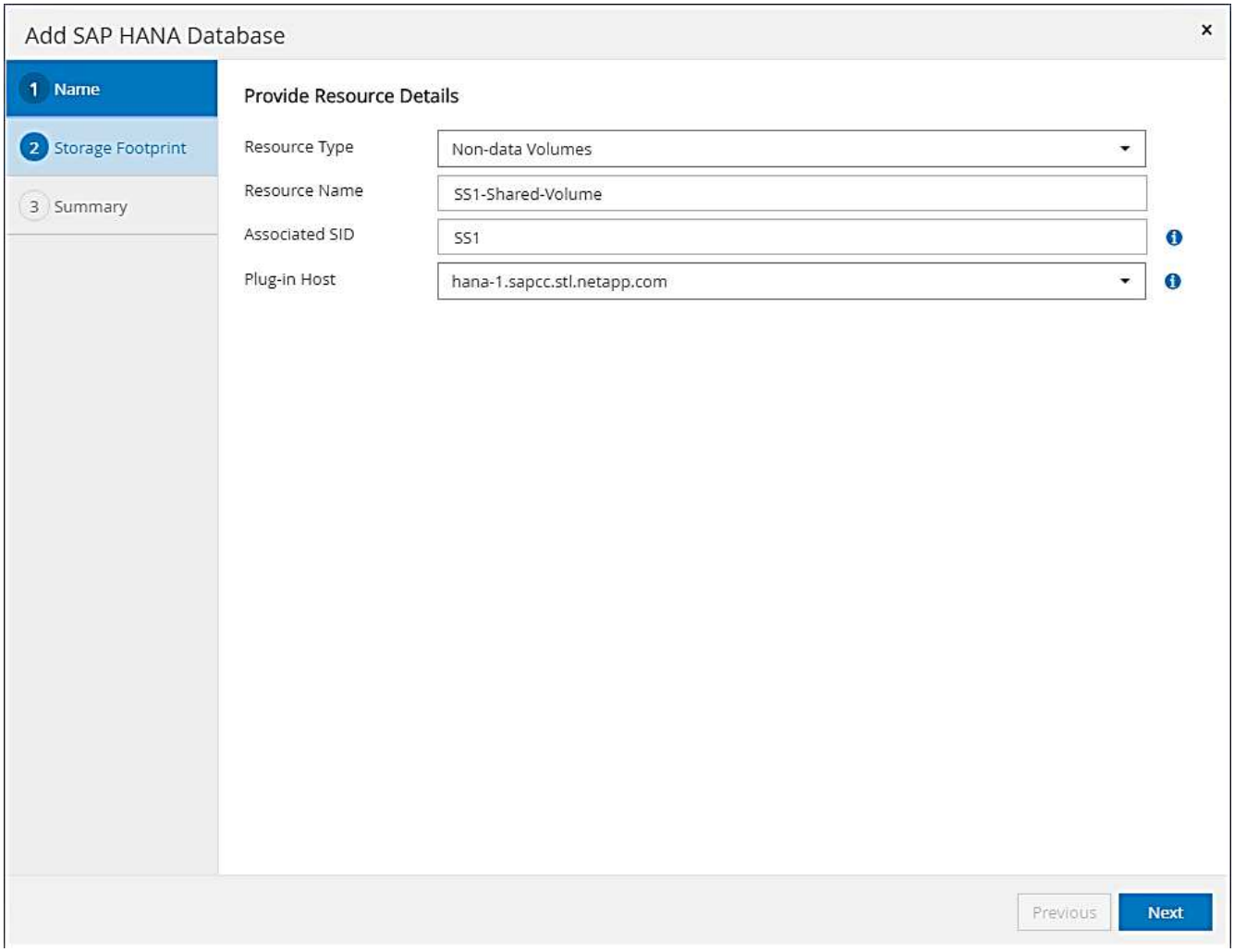
Konfiguration von Ressourcen, die nicht vom Datenvolumen stammen

In diesem Beispiel wollen wir die nicht-Daten-Volumes der SAP HANA Datenbank SS1 schützen.

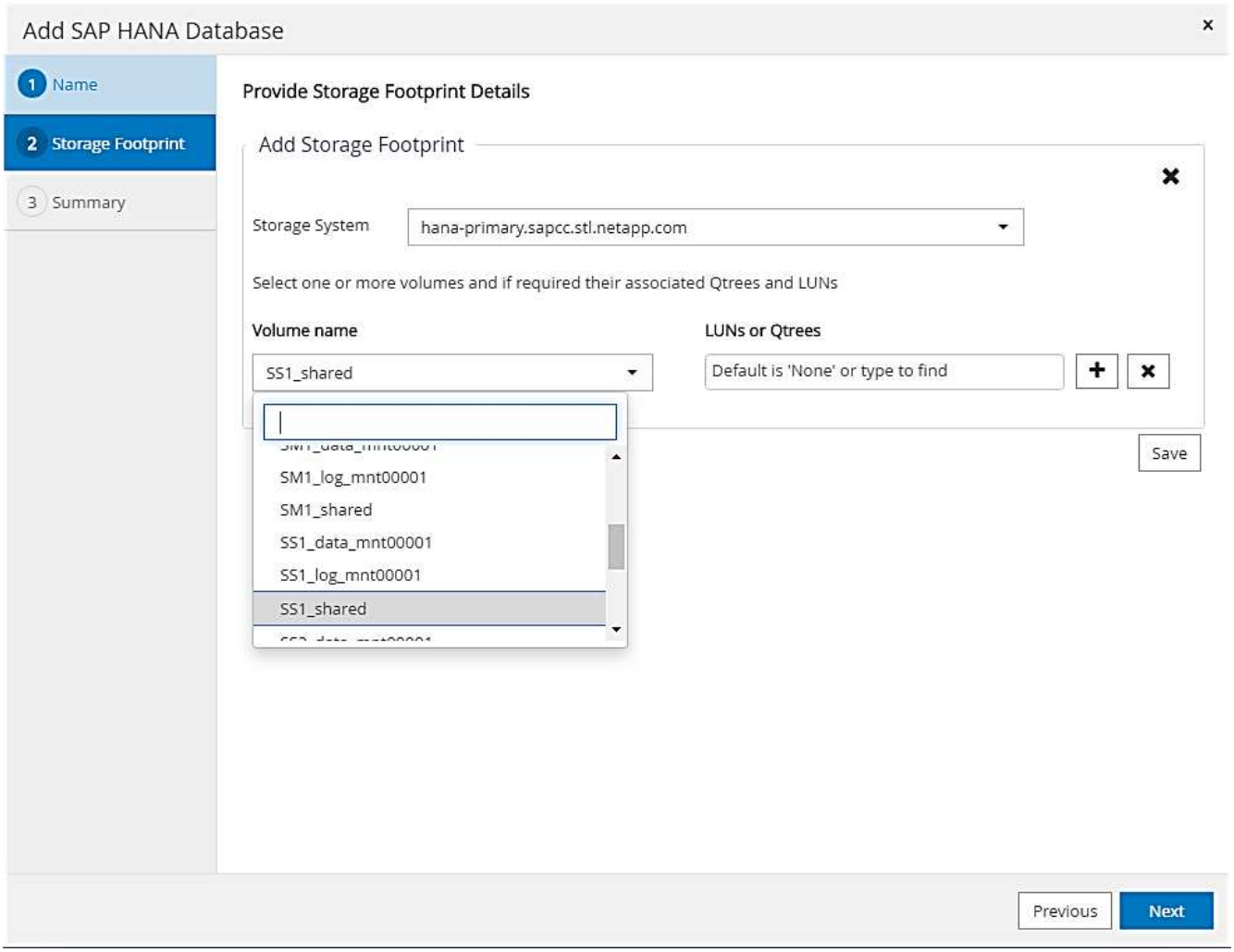
1. Wählen Sie auf der Registerkarte Ressource die Option nicht-Daten-Volume aus, und klicken Sie auf SAP HANA-Datenbank hinzufügen.



2. Wählen Sie in Schritt 1 des Dialogfelds SAP HANA-Datenbank hinzufügen in der Liste Ressourcentyp die Option nicht-Daten-Volumes aus. Geben Sie einen Namen für die Ressource und den zugehörigen SID und den SAP HANA Plug-in-Host an, den Sie für die Ressource verwenden möchten, und klicken Sie dann auf Weiter.



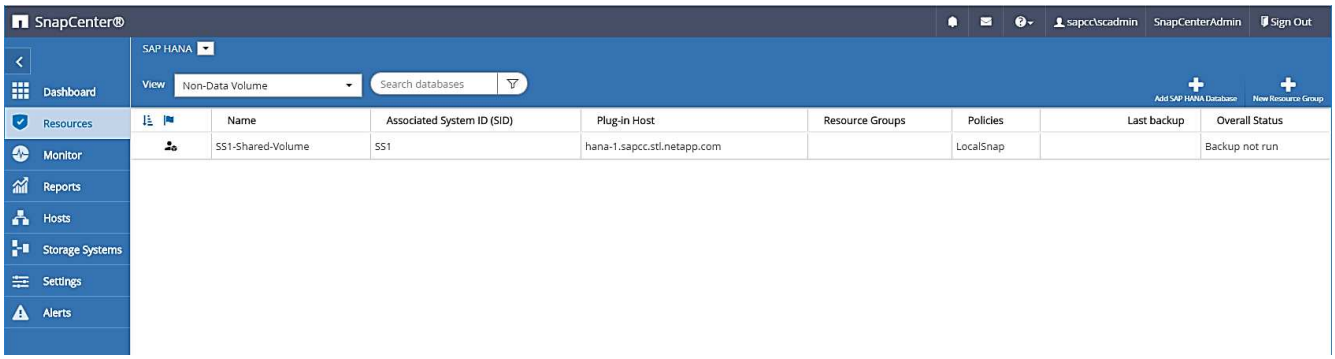
3. Fügen Sie die SVM und das Storage-Volume als Storage-Platzbedarf hinzu und klicken Sie dann auf Weiter.



4. Klicken Sie im Übersichtsschritt auf Fertig stellen, um die Einstellungen zu speichern.
5. Wiederholen Sie diese Schritte für alle erforderlichen nicht-Daten-Volumes.
6. Setzen Sie die Schutzkonfiguration der neuen Ressource fort.

> Die Datensicherung für nicht-Daten-Volume-Ressourcen ist identisch mit dem Workflow für SAP HANA Datenbankressourcen und kann auf individueller Ressourcenebene definiert werden.

Die folgende Abbildung zeigt eine Liste der konfigurierten Ressourcen, die keine Daten-Volumes enthalten.



Ressourcengruppen

Ressourcengruppen können den Schutz mehrerer Ressourcen bequem definieren, für die dieselben Sicherungsrichtlinien und denselben Zeitplan erforderlich sind. Einzelne Ressourcen, die zu einer Ressourcengruppe gehören, können weiterhin auf individueller Ebene geschützt werden.

Ressourcengruppen bieten die folgenden Funktionen:

- Sie können einer Ressourcengruppe mindestens eine Ressource hinzufügen. Alle Ressourcen müssen zum gleichen SnapCenter-Plug-in gehören.
- Der Schutz kann auf Ressourcengruppenebene definiert werden. Alle Ressourcen in der Ressourcengruppe verwenden die gleiche Richtlinie und den gleichen Zeitplan, wenn sie geschützt sind.
- Alle Backups im SnapCenter Repository und die Storage-Snapshot-Kopien haben denselben Namen wie im Ressourcenschutz definiert.
- Wiederherstellungsvorgänge werden auf nur einer Ressourcenebene und nicht als Teil einer Ressourcengruppe angewendet.
- Wenn Sie das Backup einer Ressource, die auf Ressourcengruppenebene erstellt wurde, mit SnapCenter löschen, wird dieses Backup für alle Ressourcen der Ressourcengruppe gelöscht. Das Backup wird gelöscht, das Backup aus dem SnapCenter Repository zu löschen und die Storage Snapshot Kopien zu löschen.
- Der Hauptanwendungsfall für Ressourcengruppen ist, wenn ein Kunde Backups verwenden möchte, die mit SnapCenter für das Systemklonen mit SAP Landscape Management erstellt wurden. Dies wird im nächsten Abschnitt beschrieben.

Nutzen Sie SnapCenter in Kombination mit dem SAP Landscape Management

Mit SAP Landscape Management (SAP Lama) können Kunden komplexe SAP Systemlandschaften in On-Premises-Datacentern und in Systemen, die in der Cloud ausgeführt werden, managen. SAP Lama ermöglicht zusammen mit dem NetApp Storage Services Connector (SSC) Storage-Vorgänge wie das Klonen und die Replizierung für SAP-Systemklone, Kopier- und Aktualisierungs-Anwendungsfälle mithilfe der Snapshot- und FlexClone-Technologie. Damit können Sie eine SAP Systemkopie auf Basis der Storage-Klontechnologie vollständig automatisieren und gleichzeitig die erforderliche SAP Nachbearbeitung erzielen. Weitere Informationen zu den Lösungen von NetApp für SAP Lama finden Sie unter "TR-4018: Integration von NetApp ONTAP-Systemen in SAP Landscape Management".

NetApp SSC und SAP Lama können On-Demand Snapshot-Kopien direkt mit NetApp SSC erstellen, können aber auch mithilfe von SnapCenter erstellte Snapshot-Kopien nutzen. Um SnapCenter Backups als Basis für Systemklonungs- und Kopiervorgänge bei SAP Lama zu nutzen, müssen folgende Voraussetzungen erfüllt werden:

- SAP Lama verlangt, dass alle Volumes in das Backup einbezogen werden; dazu gehören SAP HANA-Daten, Protokolle und gemeinsam genutzte Volumes.
- Alle Storage-Snapshot-Namen müssen identisch sein.
- Storage-Snapshot-Namen müssen mit VCM beginnen.

> Bei normalen Backup-Vorgängen empfiehlt NetApp nicht, das Protokoll-Volume einzubeziehen. Wenn Sie das Protokoll-Volume aus einem Backup wiederherstellen, werden die letzten aktiven Redo-Protokolle überschrieben und die Wiederherstellung der Datenbank in den letzten letzten Status verhindert.

SnapCenter Ressourcengruppen erfüllen alle diese Anforderungen. In SnapCenter werden drei Ressourcen

konfiguriert: Je eine Ressource für das Daten-Volume, das Protokoll-Volume und das gemeinsam genutzte Volume. Die Ressourcen werden einer Ressourcengruppe zugeordnet, und der Schutz wird dann auf Ressourcengruppenebene definiert. Im Ressourcengruppenschutz muss der benutzerdefinierte Snapshot-Name zu Beginn mit VCM definiert werden.

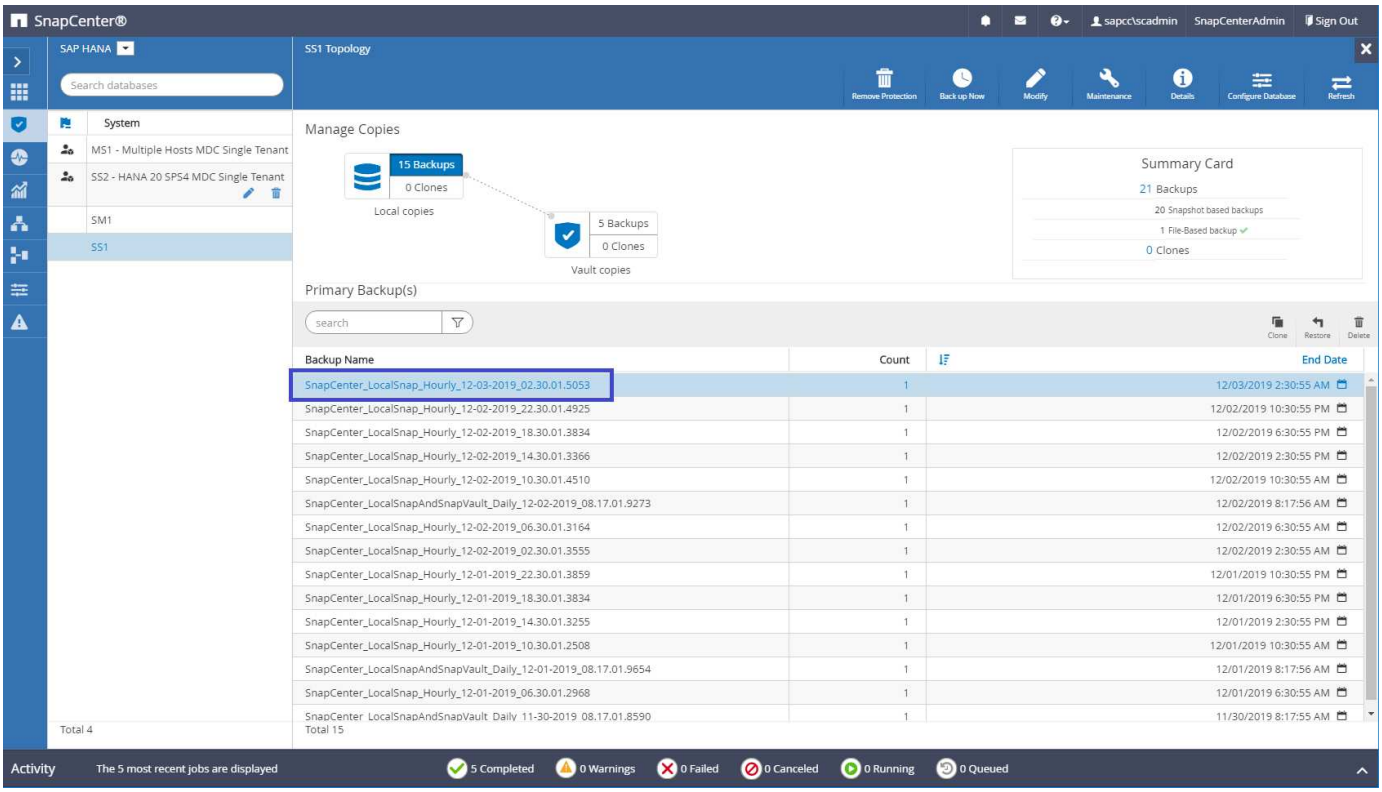
Datenbank-Backups

In SnapCenter werden Datenbank-Backups normalerweise mithilfe der Zeitpläne ausgeführt, die in der Ressourcenschutzkonfiguration der einzelnen HANA-Datenbanken definiert sind.

Ein On-Demand-Datenbank-Backup kann entweder über die SnapCenter GUI, eine PowerShell Befehlszeile oder REST-APIs durchgeführt werden.

Identifizierung von SnapCenter Backups in SAP HANA Studio

In der Topologie der SnapCenter Ressourcen wird eine Liste der mit SnapCenter erstellten Backups angezeigt. Die folgende Abbildung zeigt die auf dem primären Storage verfügbaren Backups und hebt das neueste Backup hervor.

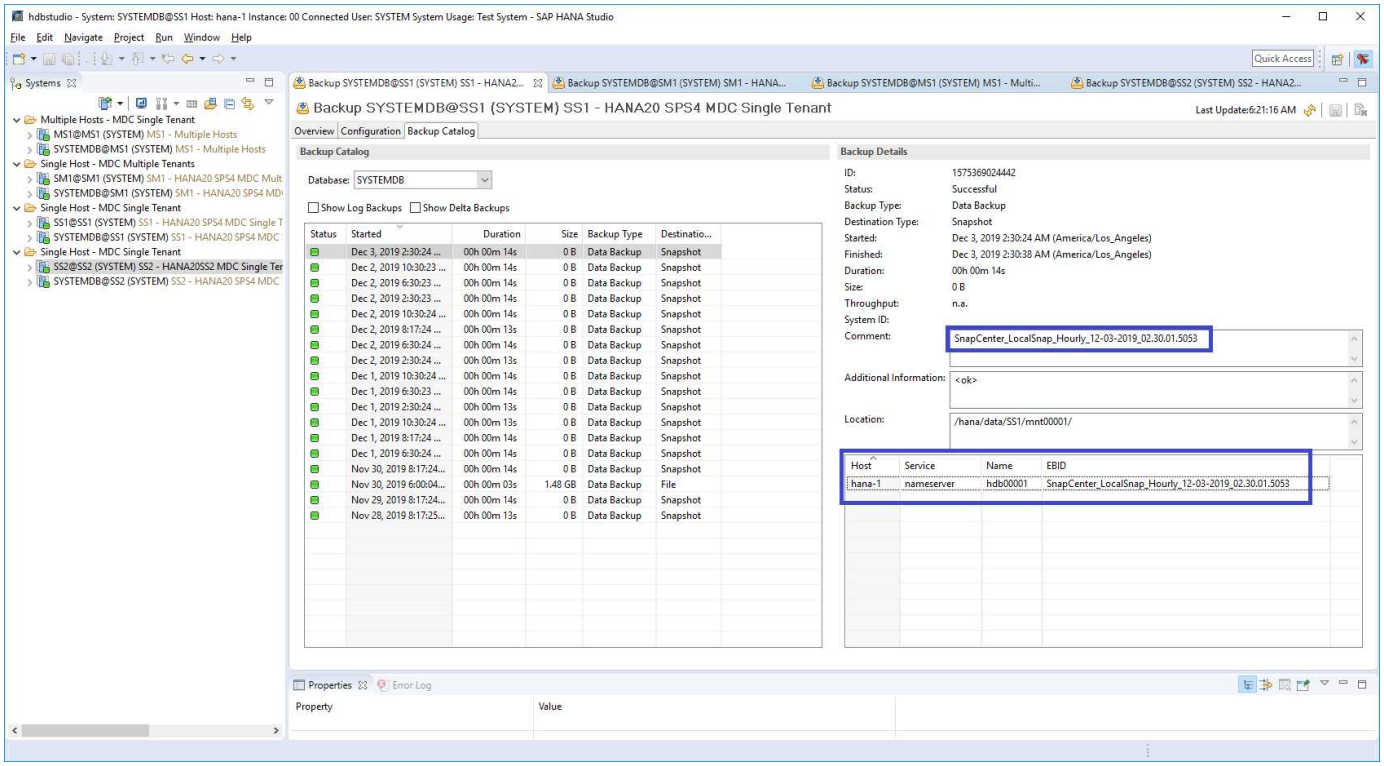


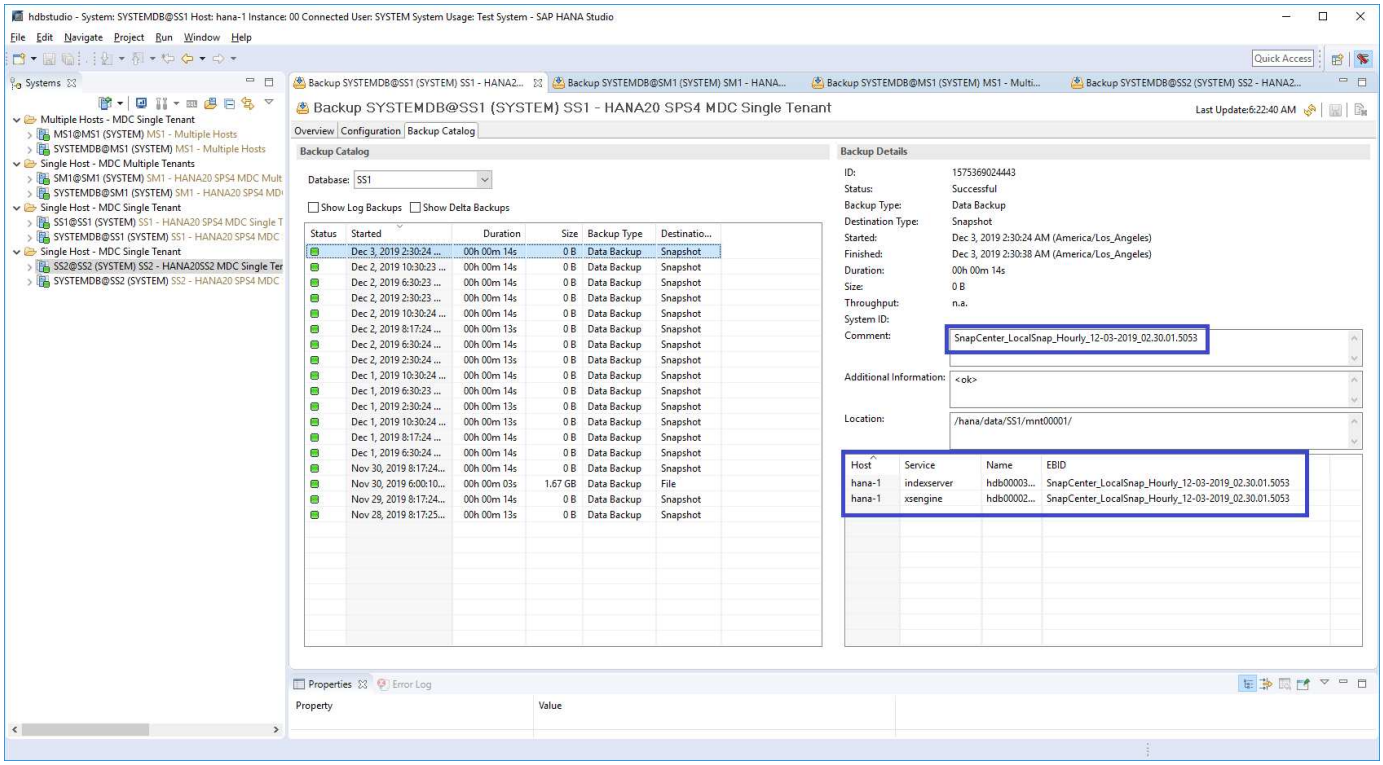
Bei einem Backup mit Storage Snapshot Kopien für ein SAP HANA MDC System wird eine Snapshot Kopie des Daten-Volumes erstellt. Dieses Daten-Volume enthält die Daten der Systemdatenbank sowie die Daten aller Mandantendatenbanken. Zur Berücksichtigung dieser physischen Architektur führt SAP HANA intern ein kombiniertes Backup der Systemdatenbank sowie aller Mandantendatenbanken durch, wenn SnapCenter ein Snapshot Backup auslöst. Das führt zu mehreren separaten Backup-Einträgen im SAP HANA Backup-Katalog: Einer für die Systemdatenbank und einer für jede Mandantendatenbank.

Bei SAP HANA Single-Container-Systemen enthält das Datenbank-Volume nur die einzige Datenbank, und es gibt nur einen Eintrag im SAP HANA Backup-Katalog.

Im SAP HANA Backup-Katalog wird der SnapCenter-Backup-Name als A gespeichert `Comment` Außerdem Feld `External Backup ID (EBID)`. Dies wird im folgenden Screenshot für die Systemdatenbank und in dem Screenshot danach für die Mandanten-Datenbank SS1 dargestellt. Beide Abbildungen zeigen den im Kommentarfeld gespeicherten SnapCenter Backup-Namen und EBID.

Die HANA 2.0 SPS4 Version (Revision 40 und 41) zeigt für Snapshot-basierte Backups immer eine Sicherungsgröße von null. Das wurde mit Revision 42 behoben. Weitere Informationen finden Sie im SAP-Hinweis "https://launchpad.support.sap.com/#/notes/2795010".

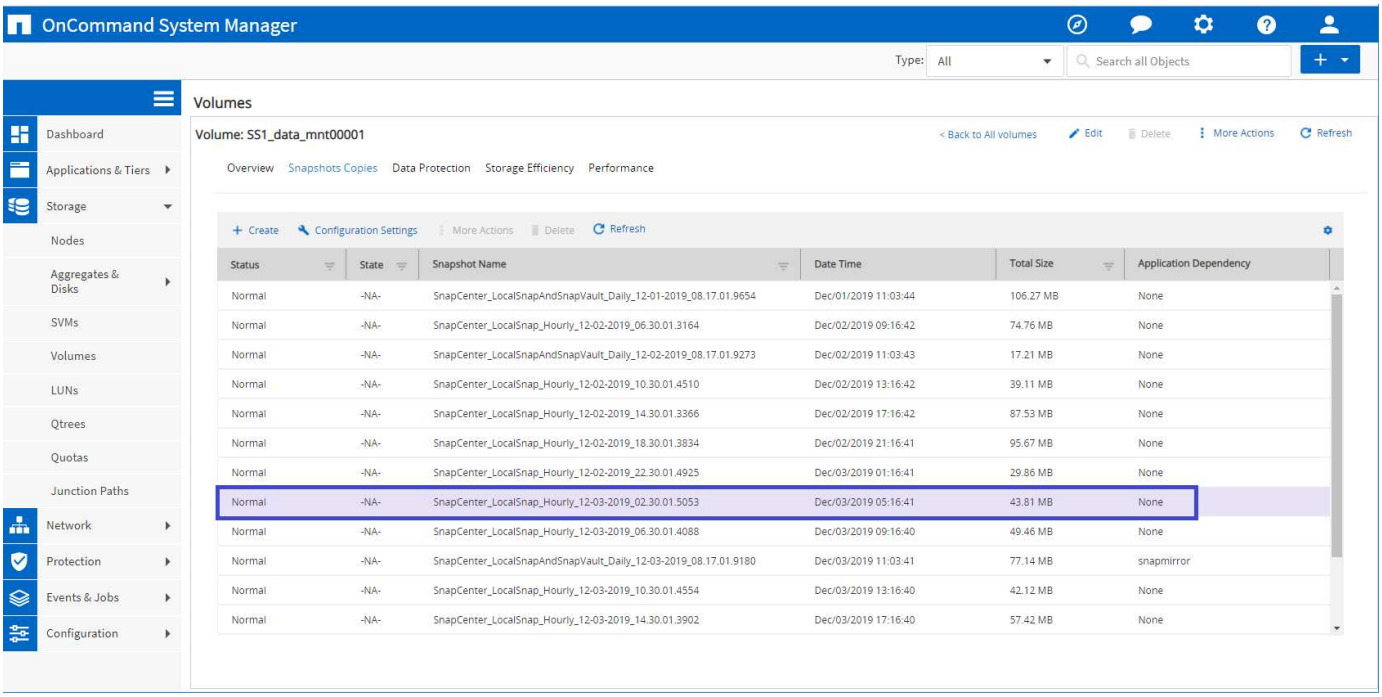




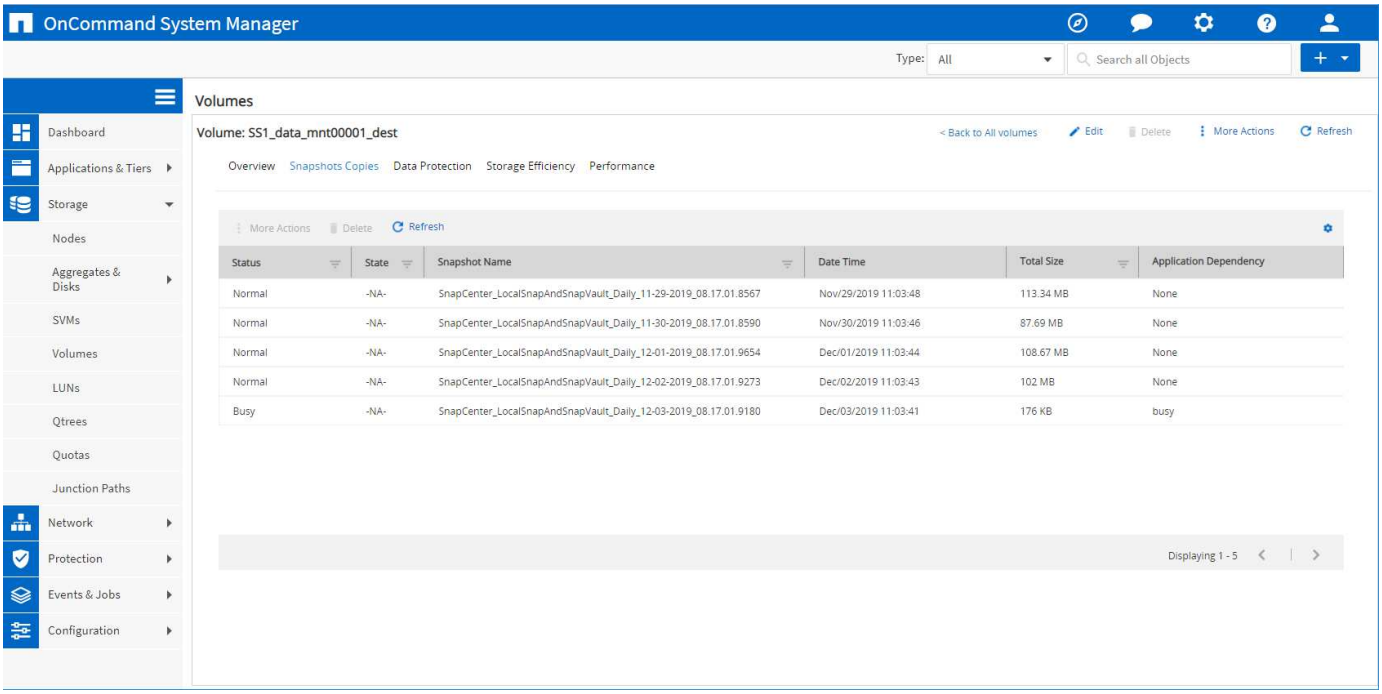
SnapCenter ist nur sich seiner eigenen Backups bewusst. Zusätzliche Backups, die beispielsweise mit SAP HANA Studio erstellt wurden, sind im SAP HANA Katalog sichtbar, jedoch nicht im SnapCenter.

Ermitteln von SnapCenter Backups auf den Storage-Systemen

Verwenden Sie NetApp OnCommand System Manager, um die Backups auf Storage-Ebene anzuzeigen, und wählen Sie das Datenbank-Volume in der Ansicht „SVM – Volume“ aus. Auf der unteren Registerkarte Snapshot Kopien werden die Snapshot Kopien des Volume angezeigt. Der folgende Screenshot zeigt die verfügbaren Backups für das Datenbank-Volume `SS1_data_mnt00001` Auf dem primären Storage. Das hervorgehobene Backup ist der in den vorherigen Bildern in SnapCenter und SAP HANA Studio angezeigte Backup mit derselben Namenskonvention.



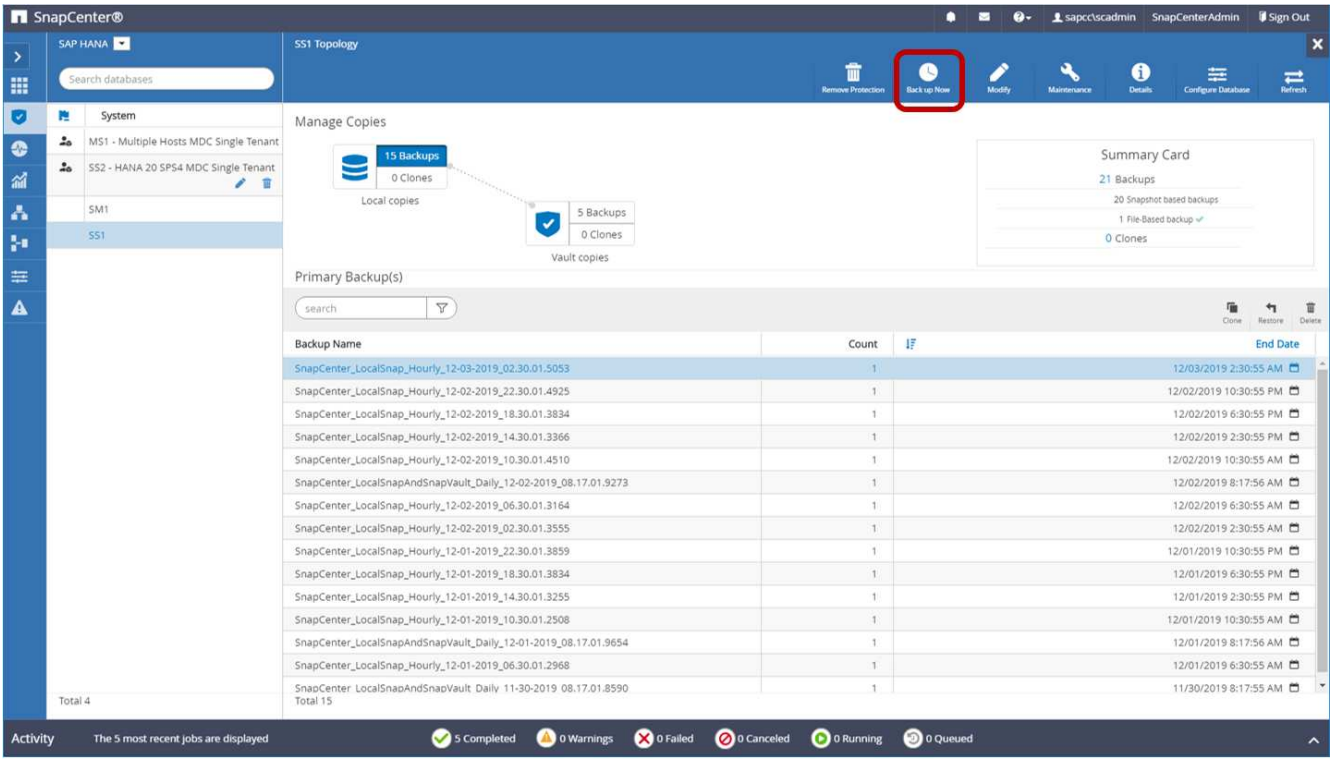
Der folgende Screenshot zeigt die verfügbaren Backups für das Replikationsziel-Volume `hana_SA1_data_mnt00001_dest` Auf dem sekundären Storage-System.



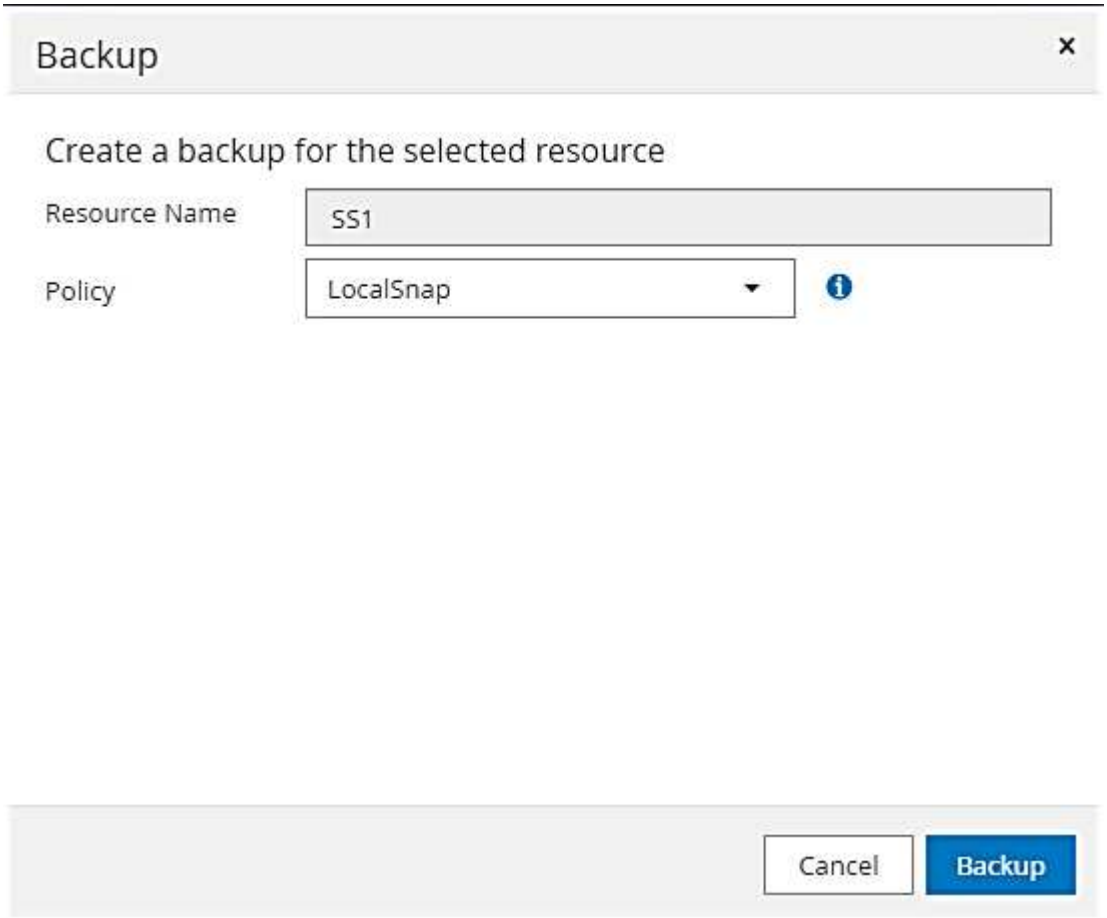
On-Demand-Datenbank-Backup auf dem Primärspeicher

1. Wählen Sie in der Ressourcenansicht die Ressource aus, und doppelklicken Sie auf die Linie, um zur Topologieansicht zu wechseln.

   Die Ansicht „Ressourcentopologie“ bietet einen Überblick über alle verfügbaren Backups, die mit SnapCenter erstellt wurden. Im oberen Bereich dieser Ansicht wird die Backup-Topologie angezeigt, die Backups im primären Storage (lokale Kopien) und, sofern verfügbar, im externen Backup-Storage (Vault-Kopien) angezeigt.

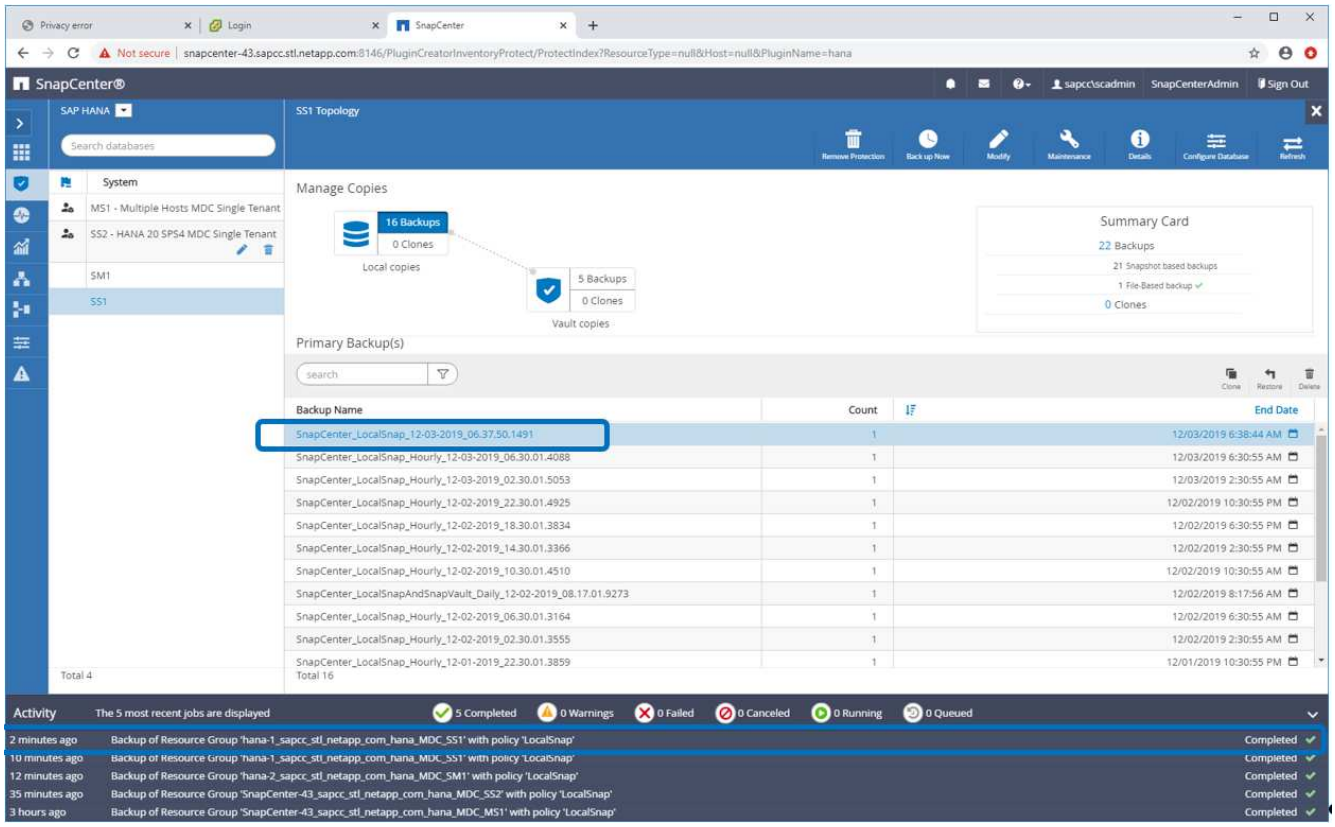


2. Klicken Sie in der oberen Zeile auf das Symbol Jetzt sichern, um ein On-Demand-Backup zu starten. Wählen Sie aus der Dropdown-Liste die Backup-Richtlinie aus `LocalSnap` Anschließend auf Backup klicken, um das On-Demand-Backup zu starten.

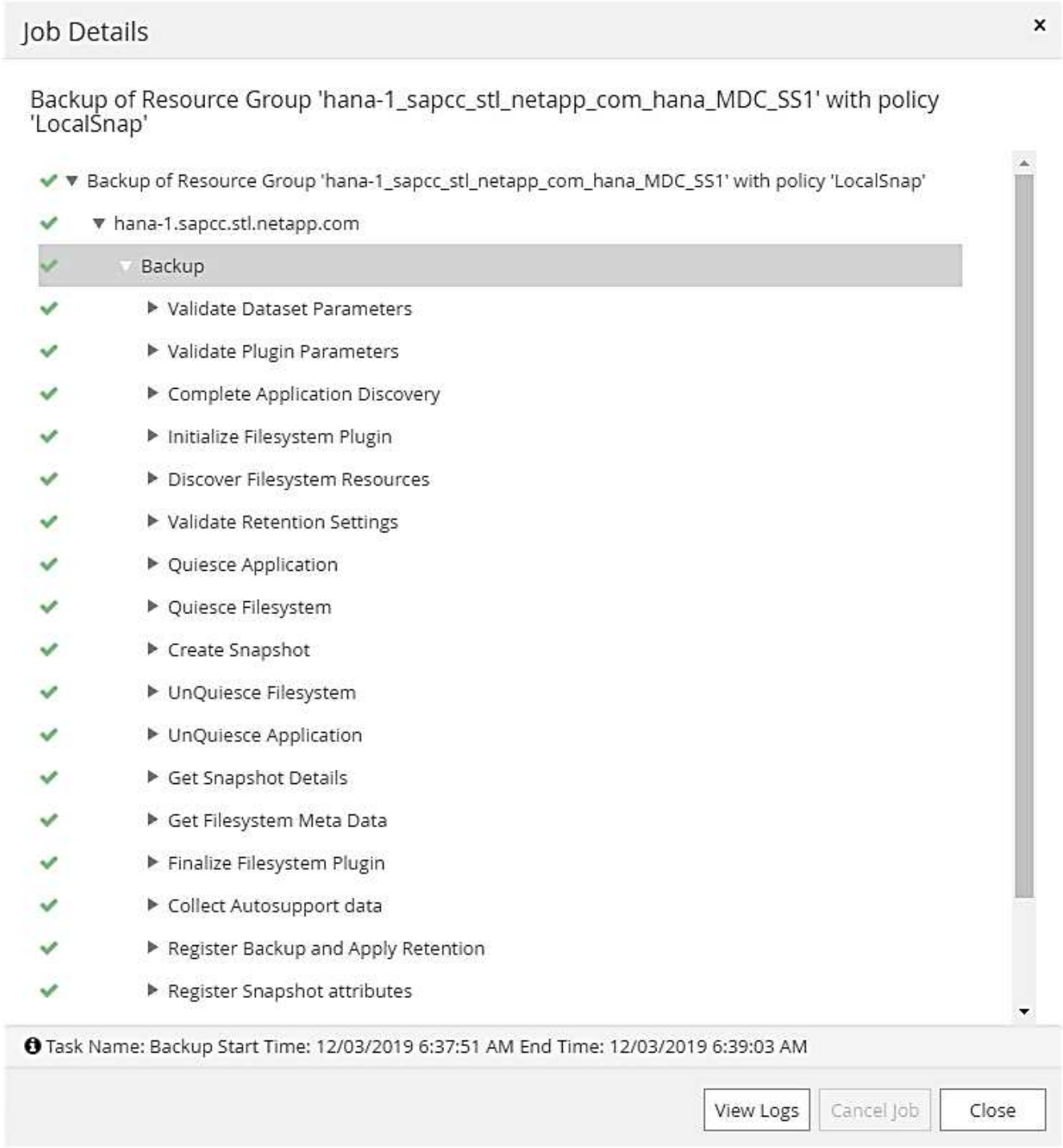


Dies startet den Sicherungsauftrag. Ein Protokoll der vorherigen fünf Jobs wird im Aktivitätsbereich unterhalb der Topologieansicht angezeigt. Nach Abschluss des Backups wird in der Topologieansicht ein neuer Eintrag angezeigt. Die Backup-Namen folgen derselben Namenskonvention wie der in Abschnitt definierte Snapshot Name "„Konfiguration des Ressourcenschutzes“."

Sie müssen die Topologieansicht schließen und erneut öffnen, um die aktualisierte Backup-Liste anzuzeigen.



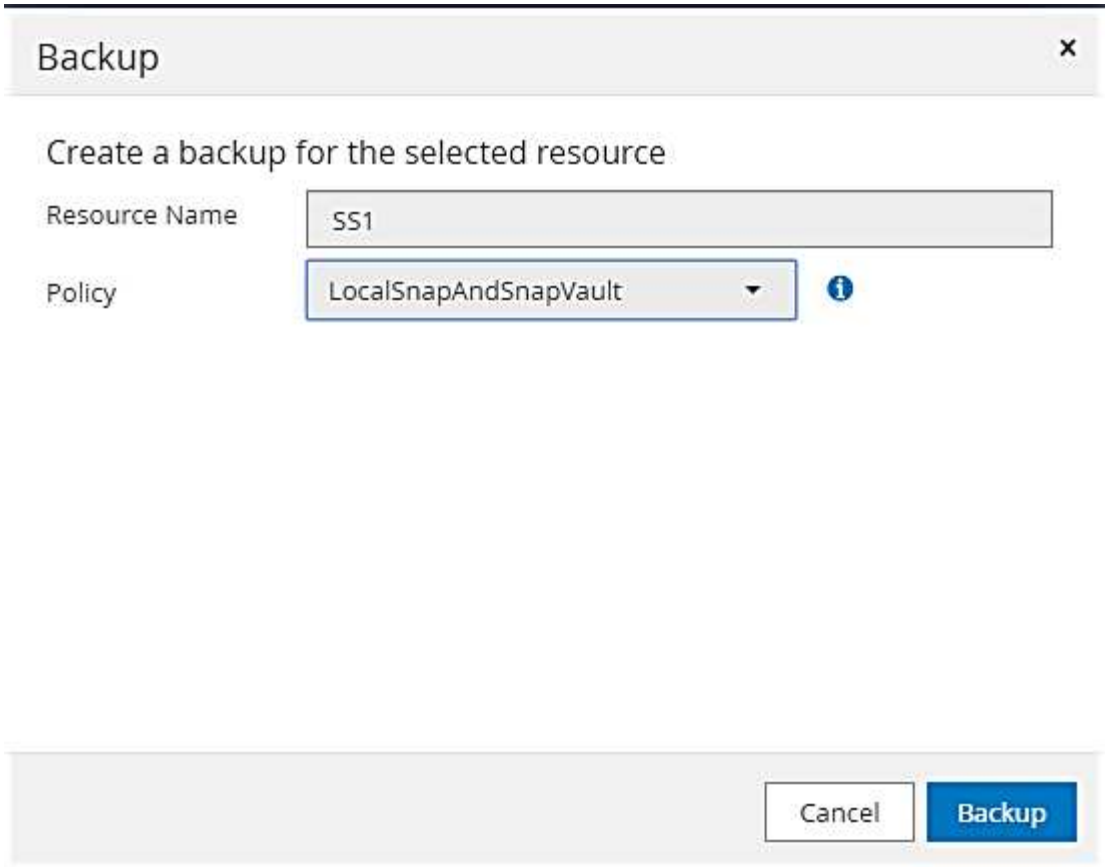
3. Die Jobdetails werden angezeigt, wenn Sie im Aktivitätsbereich auf die Vorgangszeile des Jobs klicken. Sie können ein detailliertes Jobprotokoll öffnen, indem Sie auf Protokolle anzeigen klicken.



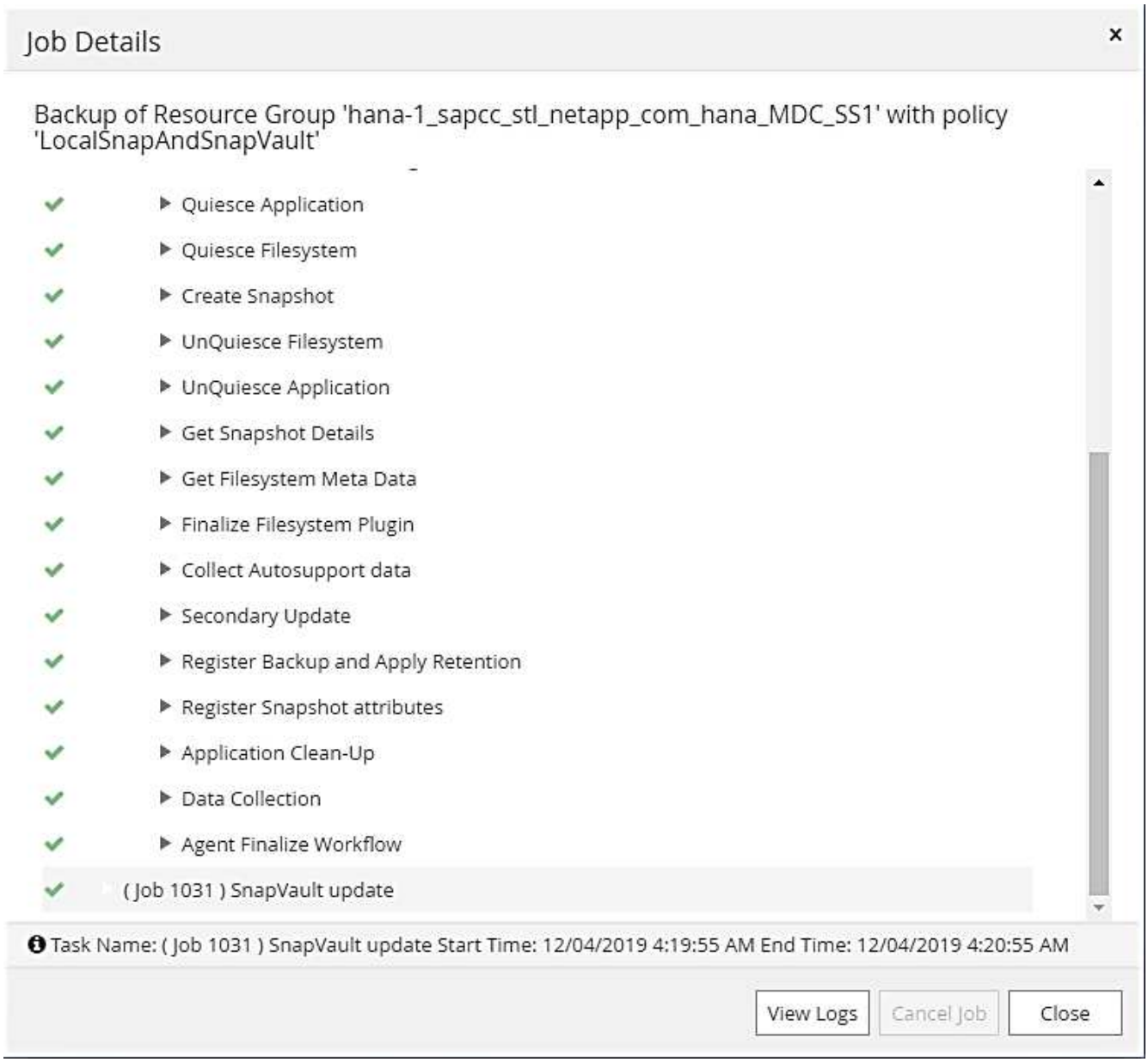
4. Im SAP HANA Studio ist das neue Backup im Backup-Katalog sichtbar. Derselbe Backup-Name in SnapCenter wird auch im Kommentar und im EBID-Feld im Backup-Katalog verwendet.

On-Demand-Datenbank-Backups mit SnapVault Replizierung

1. Wählen Sie in der Ressourcenansicht die Ressource aus, und doppelklicken Sie auf die Linie, um zur Topologieansicht zu wechseln.
2. Klicken Sie in der oberen Zeile auf das Symbol Jetzt sichern, um ein On-Demand-Backup zu starten. Wählen Sie aus der Dropdown-Liste die Backup-Richtlinie aus `LocalSnapAndSnapVault`, Dann klicken Sie auf Backup, um das On-Demand-Backup zu starten.

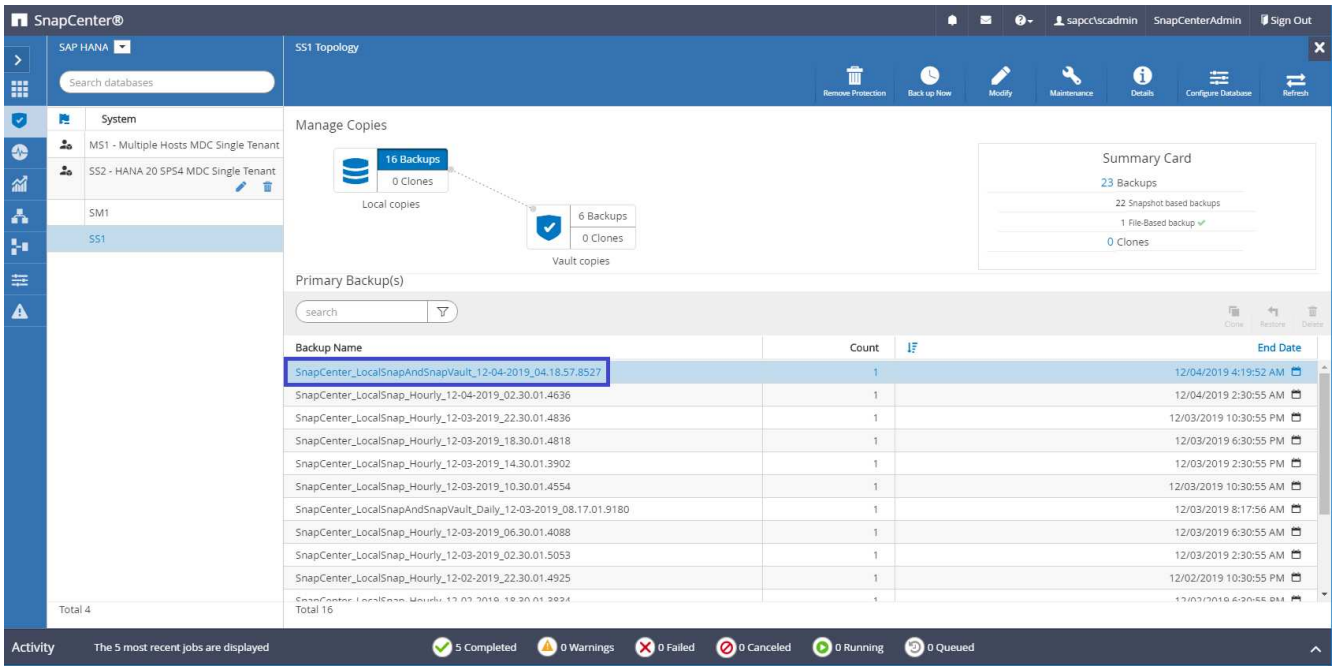


3. Die Jobdetails werden angezeigt, wenn Sie im Aktivitätsbereich auf die Vorgangszeile des Jobs klicken.

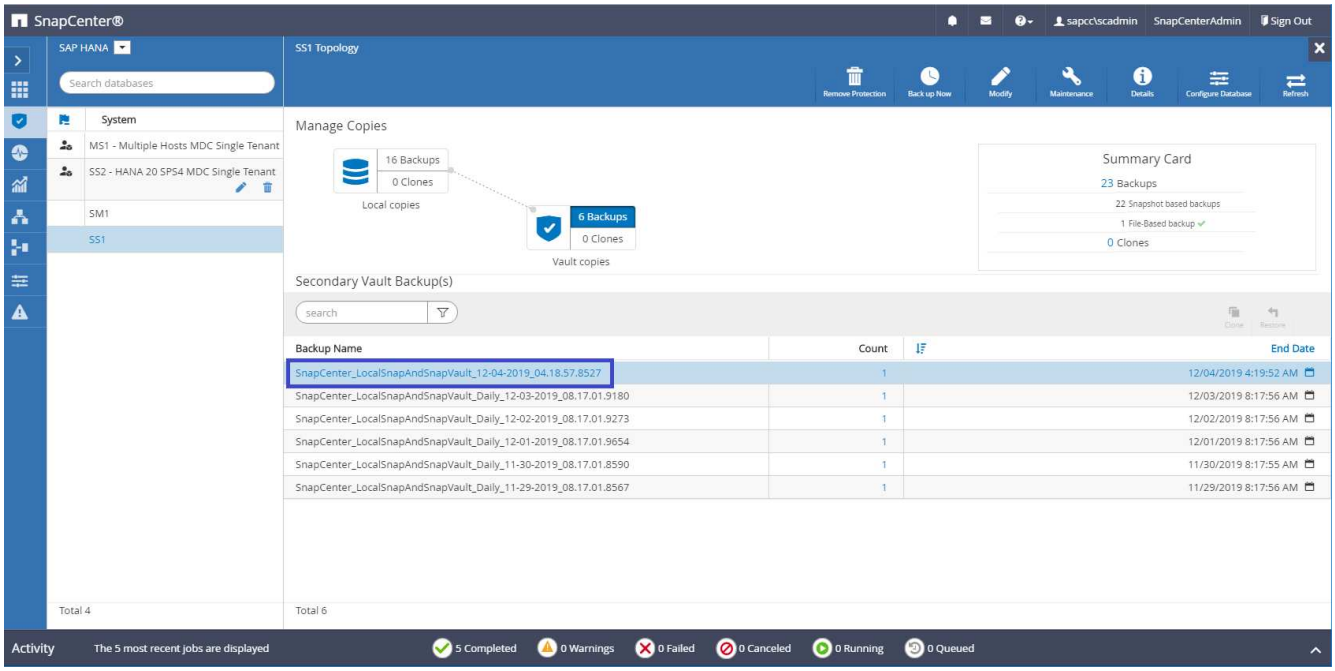


4. Nach Abschluss des Backups wird in der Topologieansicht ein neuer Eintrag angezeigt. Die Backup-Namen folgen derselben Namenskonvention wie der in Abschnitt definierte Snapshot Name "„Konfiguration des Ressourcenschutzes“."

Sie müssen die Topologieansicht schließen und erneut öffnen, um die aktualisierte Backup-Liste anzuzeigen.



5. Durch Auswahl von Vault Kopien werden Backups im sekundären Storage angezeigt. Der Name des replizierten Backups entspricht dem Backup-Namen im primären Storage.



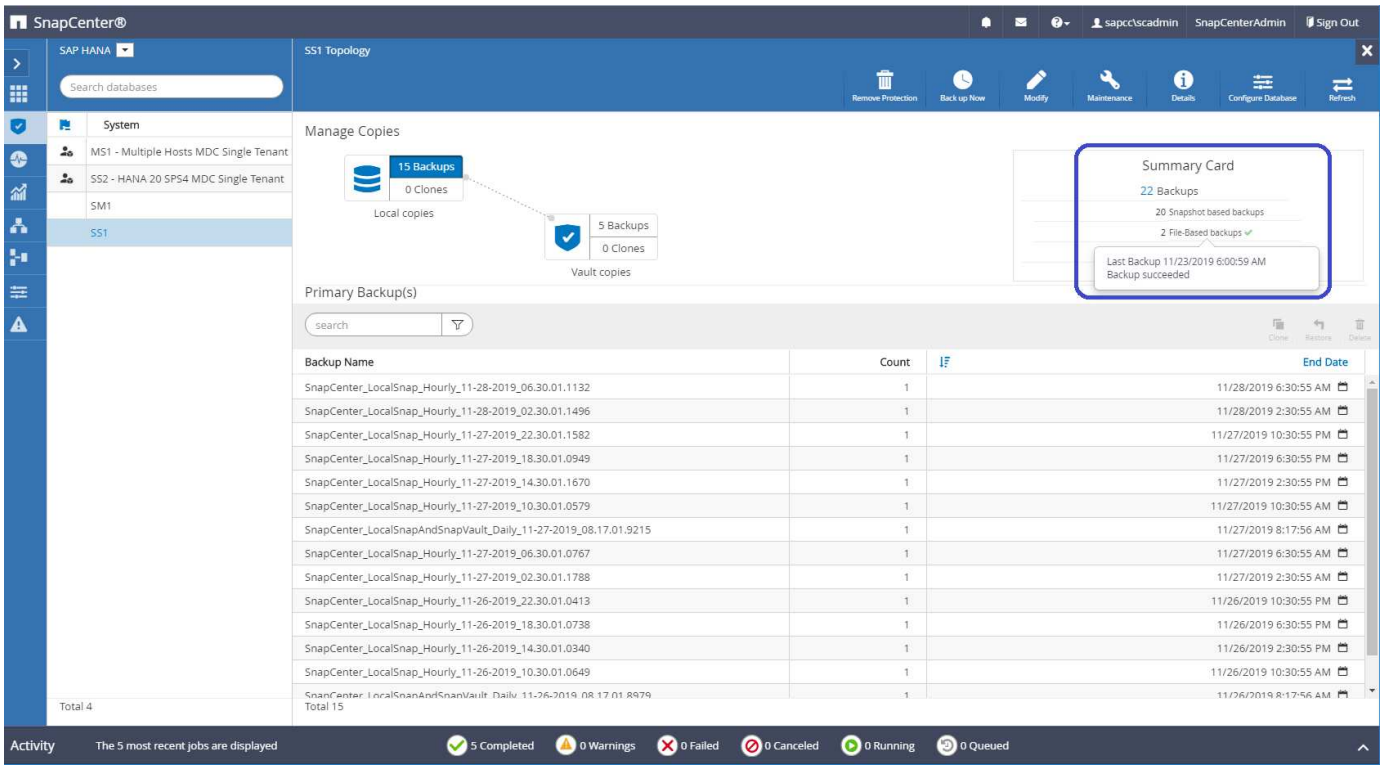
6. Im SAP HANA Studio ist das neue Backup im Backup-Katalog sichtbar. Derselbe Backup-Name in SnapCenter wird auch im Kommentar und im EBID-Feld im Backup-Katalog verwendet.

Block-Integritätsprüfung

SAP empfiehlt, Storage-basierte Snapshot-Backups mit einem wöchentlichen dateibasierten Backup zu kombinieren, um eine Integritätsprüfung für Blöcke durchzuführen. SnapCenter unterstützt die Ausführung einer Block-Integritätsprüfung, indem eine Richtlinie verwendet wird, in der das dateibasierte Backup als Backup-Typ ausgewählt wird.

Bei der Planung von Backups mithilfe dieser Richtlinie erstellt SnapCenter eine standardmäßige SAP HANA Datei-Backup für das System und die Mandantendatenbanken.

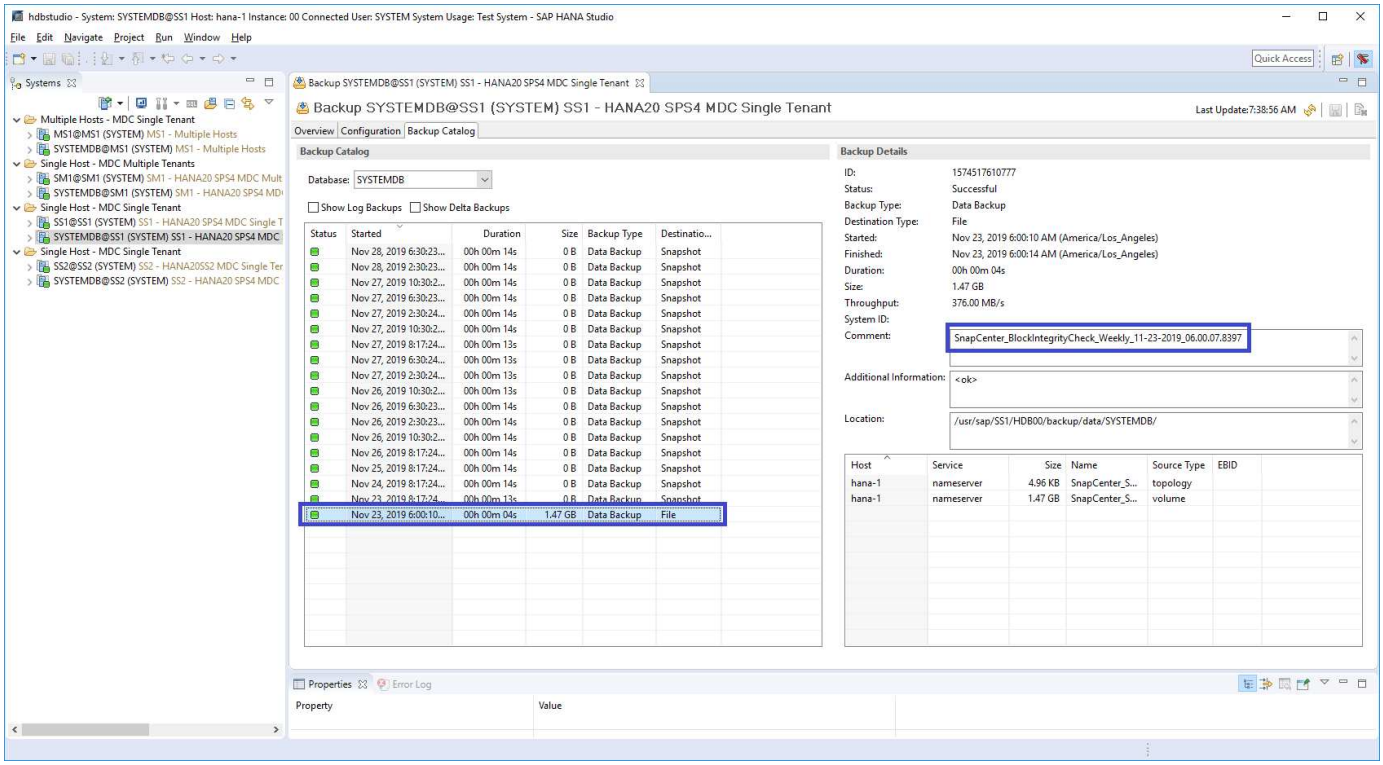
SnapCenter zeigt die Blockintegritätsprüfung nicht auf dieselbe Weise an wie Backups basierend auf Snapshot-Kopien. Stattdessen zeigt die Übersichtskarte die Anzahl der dateibasierten Backups und den Status des vorherigen Backups an.



Ein Backup zur Block-Integritätsprüfung kann nicht mithilfe der SnapCenter UI gelöscht werden, er kann jedoch mithilfe von PowerShell Befehlen gelöscht werden.

```
PS C:\Users\scadmin> Get-SmBackupReport -Resource SS1
SmBackupId                : 9
SmJobId                   : 42
StartDateTime             : 11/19/2019 8:26:32 AM
EndDateTime               : 11/19/2019 8:27:33 AM
Duration                  : 00:01:00.7652030
CreatedDateTime           : 11/19/2019 8:27:24 AM
Status                    : Completed
ProtectionGroupName       : hana-1_sapcc_stl_netapp_com_hana_MDC_SS1
SmProtectionGroupId       : 1
PolicyName                : BlockIntegrityCheck
SmPolicyId                : 5
BackupName                : SnapCenter_BlockIntegrityCheck_11-19-
2019_08.26.33.2913
VerificationStatus        : NotApplicable
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
PluginCode                : SCC
PluginName                : hana
JobTypeId                 : 0
JobHost                   :

PS C:\Users\scadmin> Remove-SmBackup -BackupIds 9

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"): y


BackupResult : {}
Result       : SMCoreContracts.SMResult
TotalCount   : 0
DisplayCount : 0
Context      :
Job          : SMCoreContracts.SmJob



PS C:\Users\scadmin>
```

Der SAP HANA-Backup-Katalog zeigt Einträge sowohl für das System als auch für die Mandanten-Datenbanken an. Die folgende Abbildung zeigt eine SnapCenter-Blockintegritätsprüfung im Backup-Katalog der Systemdatenbank.



Eine erfolgreiche Überprüfung der Blockintegrität erstellt standardisierte SAP HANA Daten-Backup-Dateien. SnapCenter verwendet den Backup-Pfad, der in der HANA-Datenbank für dateibasierte Daten-Backup-Vorgänge konfiguriert wurde.

```
hana-1:/usr/sap/SS1/HDB00/backup/data # ls -al *
DB_SS1:
total 1710840
drwxr-xr-- 2 ss1adm sapsys       4096 Nov 28 10:25 .
drwxr-xr-- 4 ss1adm sapsys       4096 Nov 19 05:11 ..
-rw-r----- 1 ss1adm sapsys     155648 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_0_1
-rw-r----- 1 ss1adm sapsys   83894272 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_2_1
-rw-r----- 1 ss1adm sapsys 1660952576 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_3_1
SYSTEMDB:
total 1546340
drwxr-xr-- 2 ss1adm sapsys       4096 Nov 28 10:24 .
drwxr-xr-- 4 ss1adm sapsys       4096 Nov 19 05:11 ..
-rw-r----- 1 ss1adm sapsys     159744 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_0_1
-rw-r----- 1 ss1adm sapsys 1577066496 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_1_1
```

Restore und Recovery

In den folgenden Abschnitten werden die Wiederherstellungs- und Recovery-Workflows von drei verschiedenen Szenarien und Beispielkonfigurationen beschrieben.

- Automatisierte Wiederherstellung und Wiederherstellung:
  - Automatisch ermittelte HANA-System SS1
  - SAP HANA ein einzelner Host, MDC ein Mandantensystem mit NFS
- Restore und Recovery einzelner Mandanten:
  - Automatisch ermittelte HANA-System SM1
  - SAP HANA einzelner Host, MDC mandantenfähiges System mit NFS
- Wiederherstellung mit manueller Wiederherstellung:
  - Manuell konfiguriertes HANA-System SS2
  - SAP HANA einzelner Host, MDC mandantenfähiges System mit NFS

In den folgenden Abschnitten werden die Unterschiede zwischen einem einzelnen SAP HANA Host und mehreren Hosts sowie in HANA-Systemen mit Fibre Channel-SAN-Anbindung hervorgehoben.

Die Beispiele zeigen, dass SAP HANA Studio als Tool zur manuellen Wiederherstellung dient. Sie können

auch SAP HANA Cockpit oder HANA SQL Statements verwenden.

Automatisiertes Restore und Recovery

Bei SnapCenter 4.3 werden automatisierte Restore- und Recovery-Vorgänge für einzelne HANA-Container oder MDC-Mandantensysteme unterstützt, die von SnapCenter automatisch erkannt wurden.

Sie können eine automatisierte Wiederherstellung und Operation mit den folgenden Schritten ausführen:

1. Wählen Sie das Backup aus, das für den Wiederherstellungsvorgang verwendet werden soll. Das Backup kann aus den folgenden Speicheroptionen ausgewählt werden:
   - Primärspeicher
   - Externer Backup-Storage (SnapVault Ziel)
2. Wählen Sie den Wiederherstellungstyp aus. Wählen Sie mit Volume Revert oder ohne Volume Revert die Option Complete Restore.

   Die Option Volume Revert ist nur für die Wiederherstellung von Vorgängen im primären Storage und, wenn die HANA Datenbank NFS als Storage-Protokoll verwendet.

3. Wählen Sie den Wiederherstellungstyp aus den folgenden Optionen aus:
   - Auf den letzten Stand
   - Zeitpunktgenau
   - Zu einem bestimmten Daten-Backup
   - Keine Wiederherstellung

   Der ausgewählte Wiederherstellungstyp wird für die Wiederherstellung des Systems und der Mandanten-Datenbank verwendet.

Als Nächstes führt SnapCenter die folgenden Operationen durch:

1. Die HANA-Datenbank wird gestoppt.
2. Die Datenbank wird wiederhergestellt.

   Abhängig vom ausgewählten Wiederherstellungstyp und dem verwendeten Storage-Protokoll werden verschiedene Operationen ausgeführt.

   - Wenn die Option „NFS“ und „Volume revert“ ausgewählt sind, hängt SnapCenter das Volume ab, stellt das Volume mithilfe von Volume-basierten SnapRestore auf der Storage-Ebene wieder her und hängt das Volume an.
   - Wenn NFS ausgewählt ist und die Volume-Zurücksetzung nicht ausgewählt ist, stellt SnapCenter alle Dateien mithilfe von SnapRestore-Vorgängen mit einer einzigen Datei auf der Storage-Ebene wieder her.
   - Wenn Fibre Channel SAN ausgewählt ist, hängt SnapCenter die LUN(s) ab, stellt die LUN(s) anhand einzelner Datei-SnapRestore-Vorgänge auf der Storage-Ebene wieder her und erkennt und hängt die LUN(s) an.
3. Es stellt die Datenbank wieder her:
   a. Es stellt die Systemdatenbank wieder her.

b. Die Mandantendatenbank wird wiederhergestellt.

   Bei HANA-Systemen mit einzelnen Containern erfolgt die Recovery in einem Schritt:

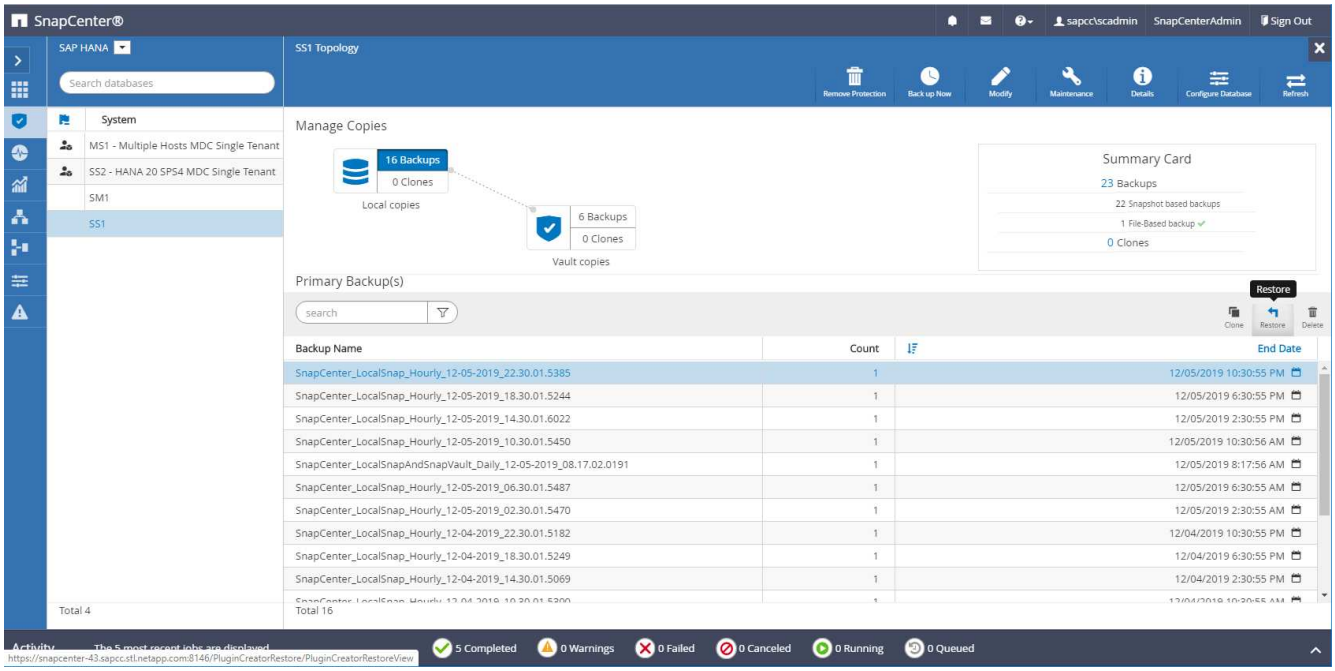
c. Es startet die HANA-Datenbank.

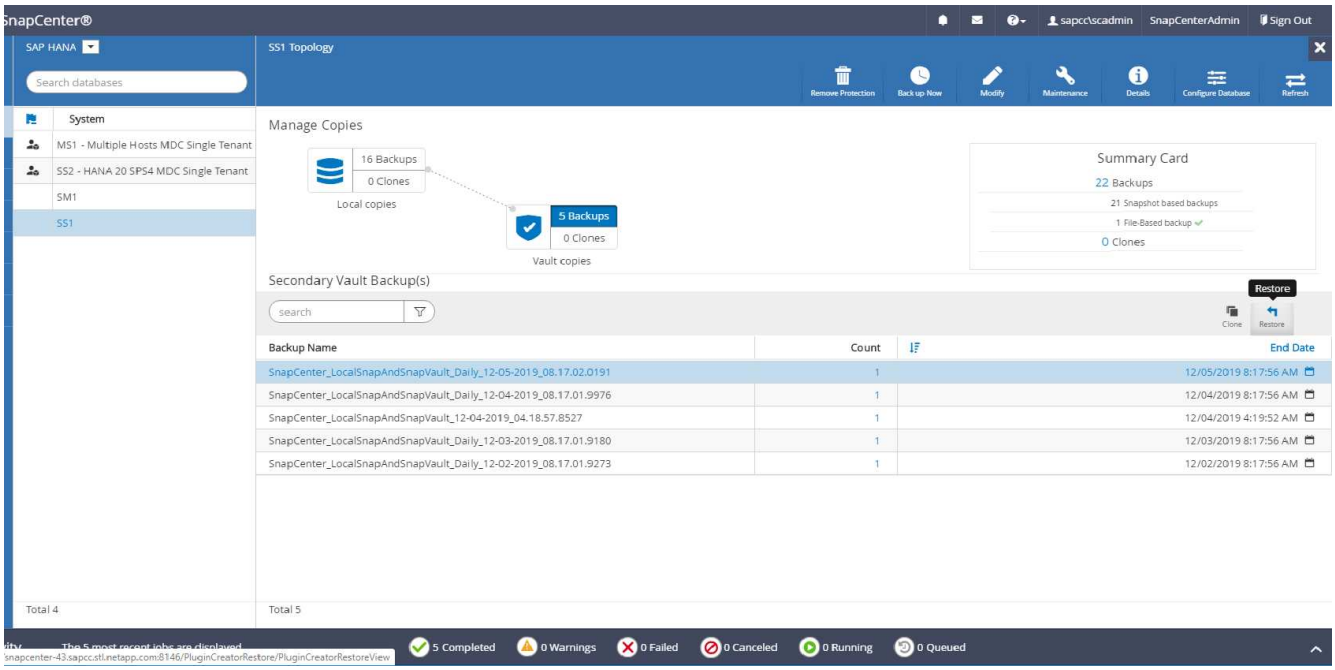
> Wenn keine Wiederherstellung ausgewählt ist, beendet SnapCenter und der Wiederherstellungsvorgang für das System, die Mandantendatenbank muss manuell durchgeführt werden.

Dieser Abschnitt enthält die Schritte für den automatisierten Restore- und Recovery-Vorgang des automatisch erkannten HANA-Systems SS1 (SAP HANA einzelner Host, MDC einzelnes Mandantensystem mit NFS).

1. Wählen Sie ein Backup in SnapCenter aus, das für den Wiederherstellungsvorgang verwendet werden soll.

   > Sie können Restores von primärem oder externem Backup-Storage wählen.



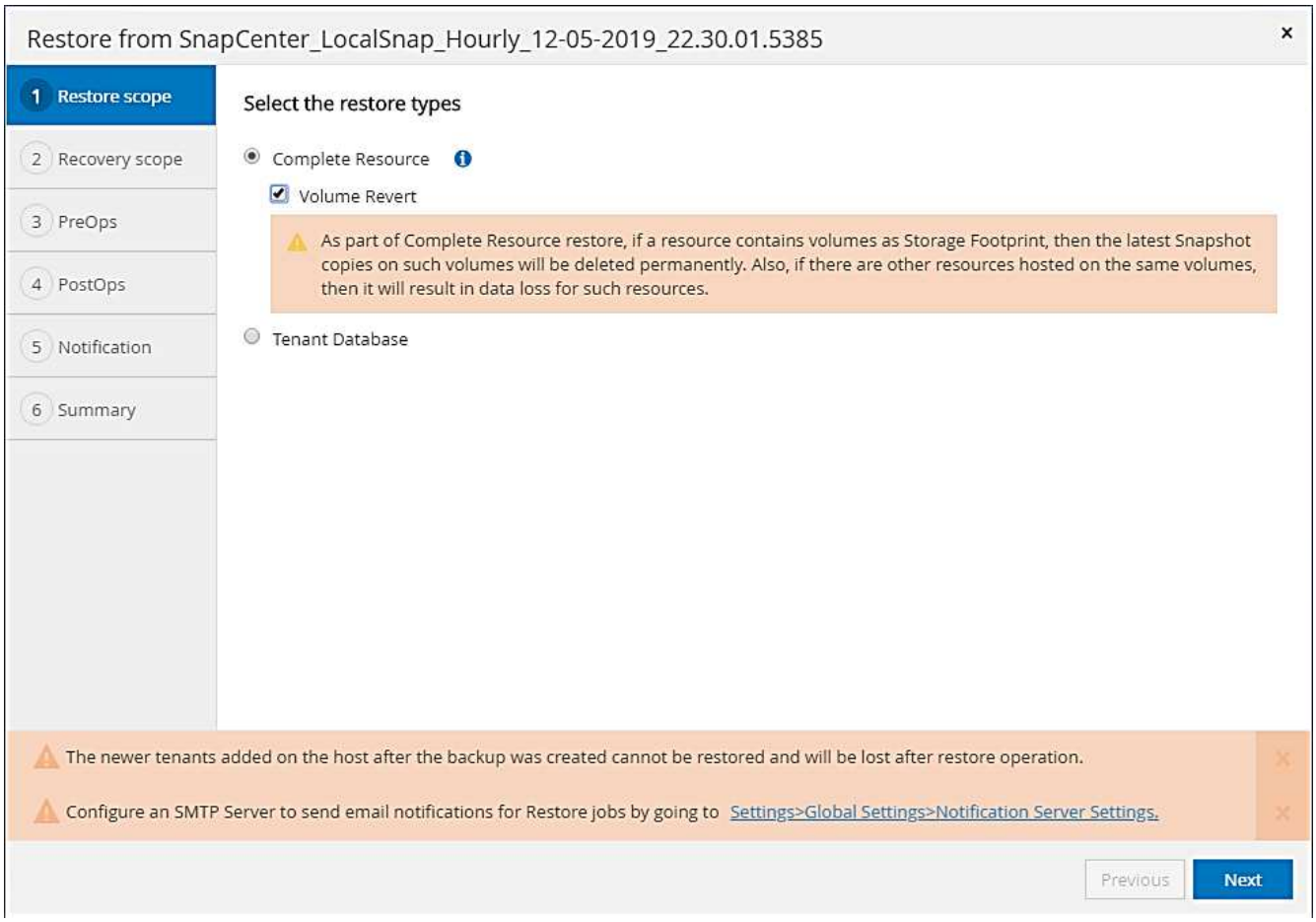


2. Wählen Sie den Umfang und den Typ der Wiederherstellung aus.

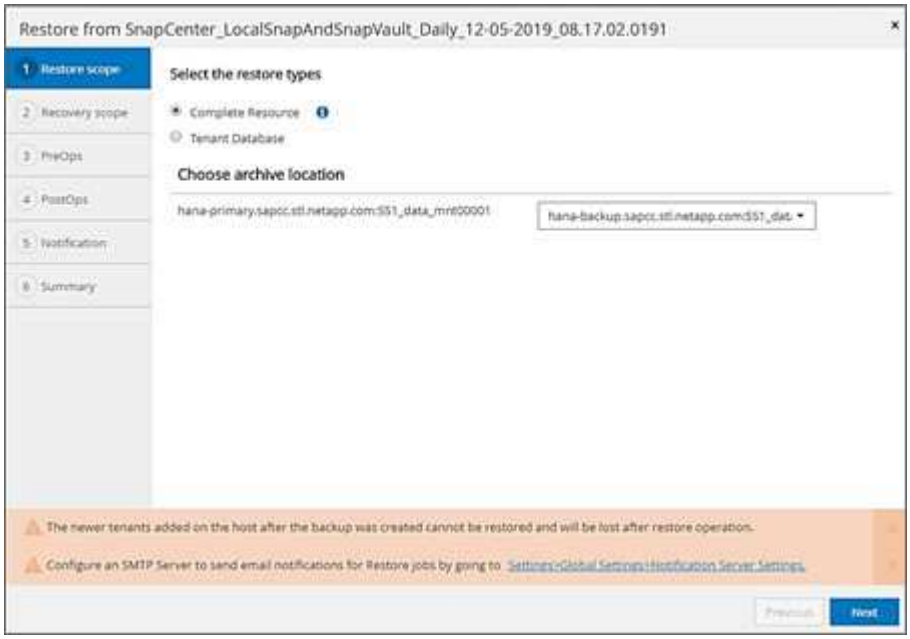
   Die folgenden drei Screenshots zeigen die Restore-Optionen für die Wiederherstellung vom primären Volume mit NFS, die Wiederherstellung vom sekundären mit NFS und die Wiederherstellung vom primären Speicher mit Fibre Channel SAN.

   Die Restore-Optionen für die Wiederherstellung aus dem primären Speicher.

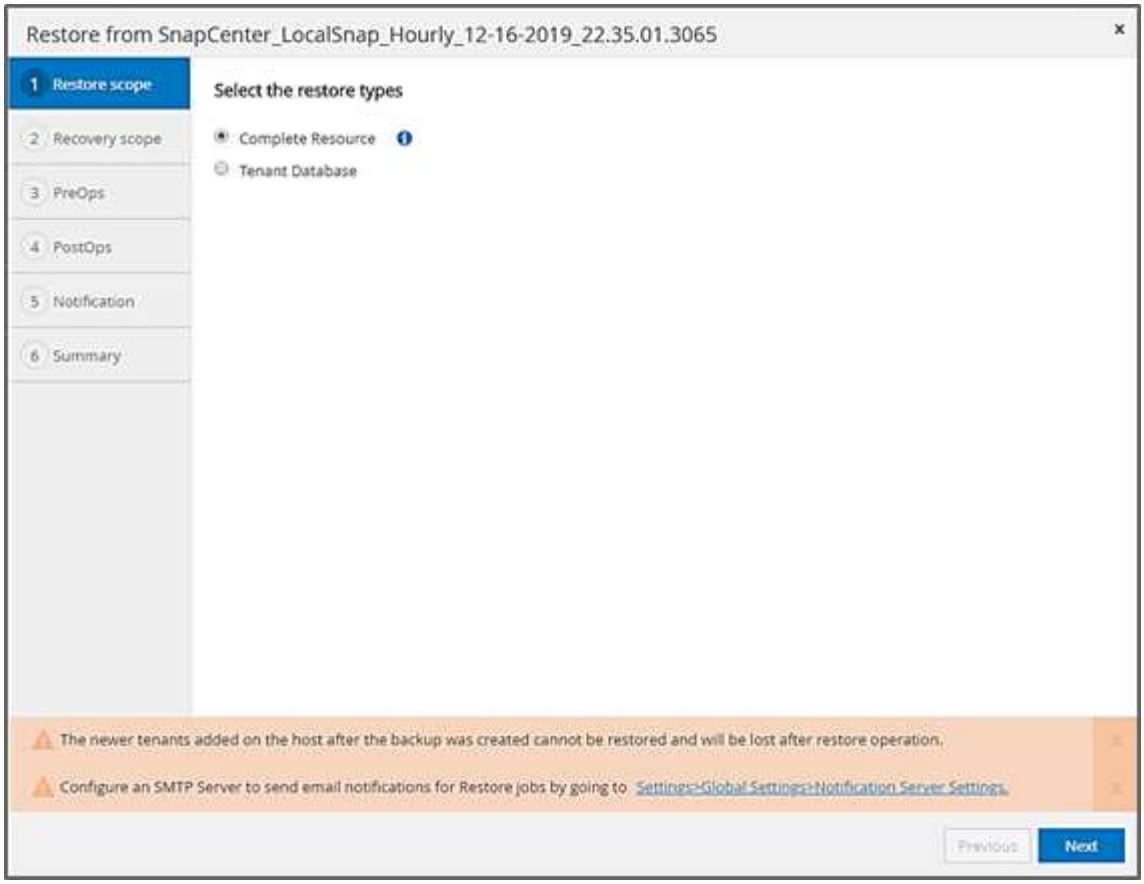
   > Die Option zur Umrüstung von Volumes ist nur für die Wiederherstellung von Vorgängen von Primärquelle mit NFS verfügbar.



Die Wiederherstellungsoptionen für die Wiederherstellung von einem externen Backup-Speicher.

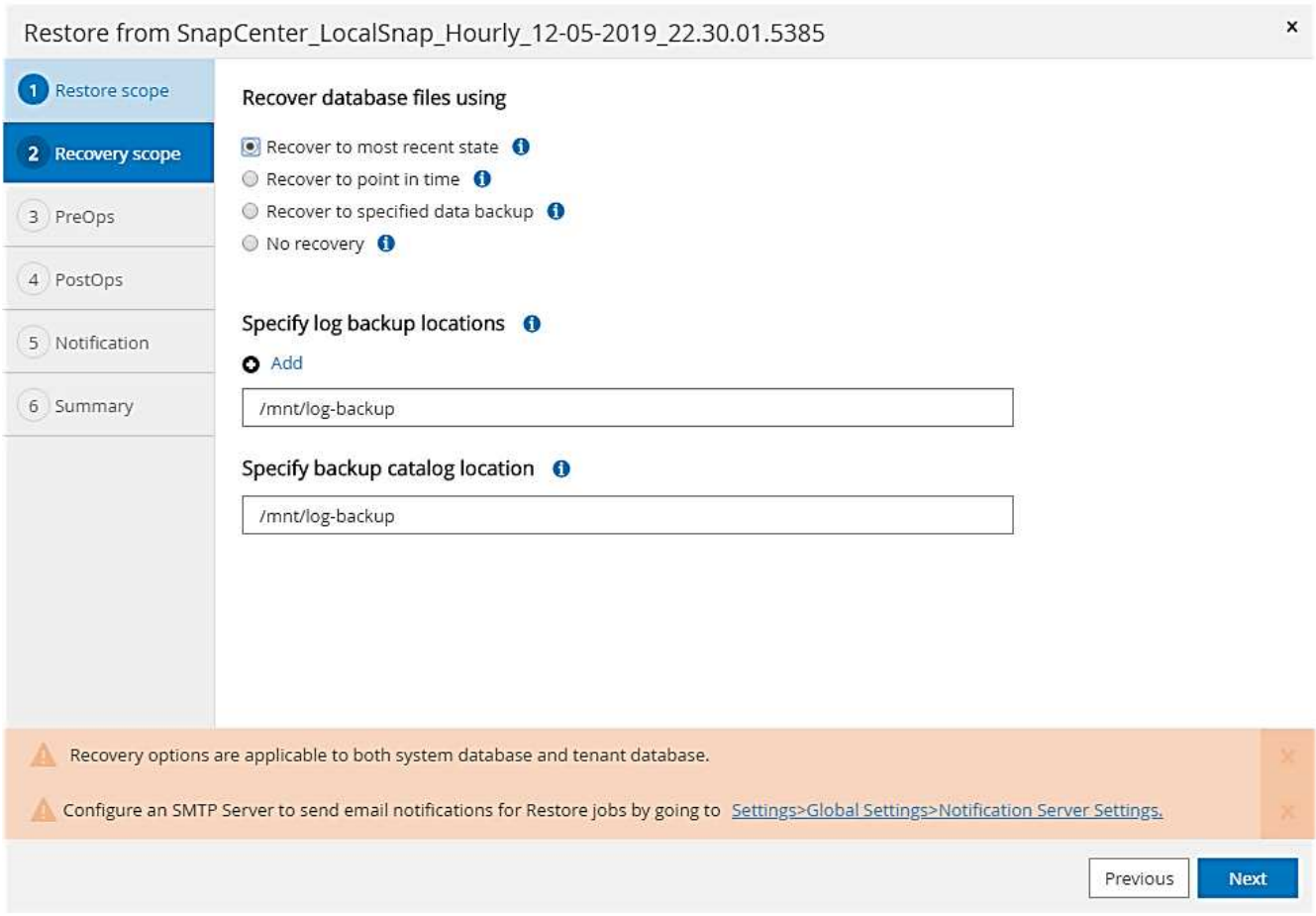


Die Wiederherstellungsoptionen für die Wiederherstellung aus dem primären Speicher mit Fibre Channel SAN.

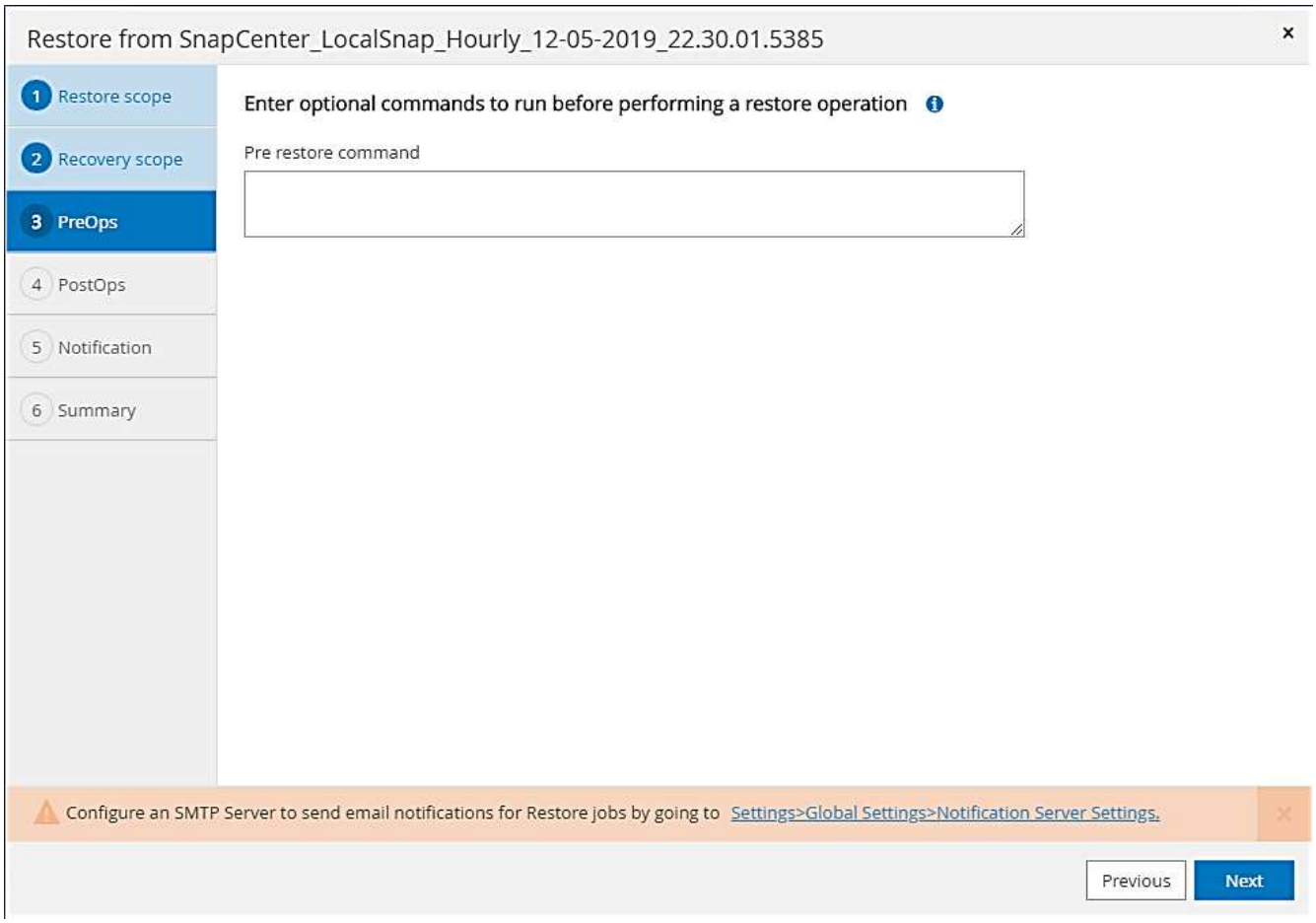


3. Wählen Sie „Recovery Scope“ aus, und stellen Sie den Speicherort für das Backup und das Katalog-Backup bereit.

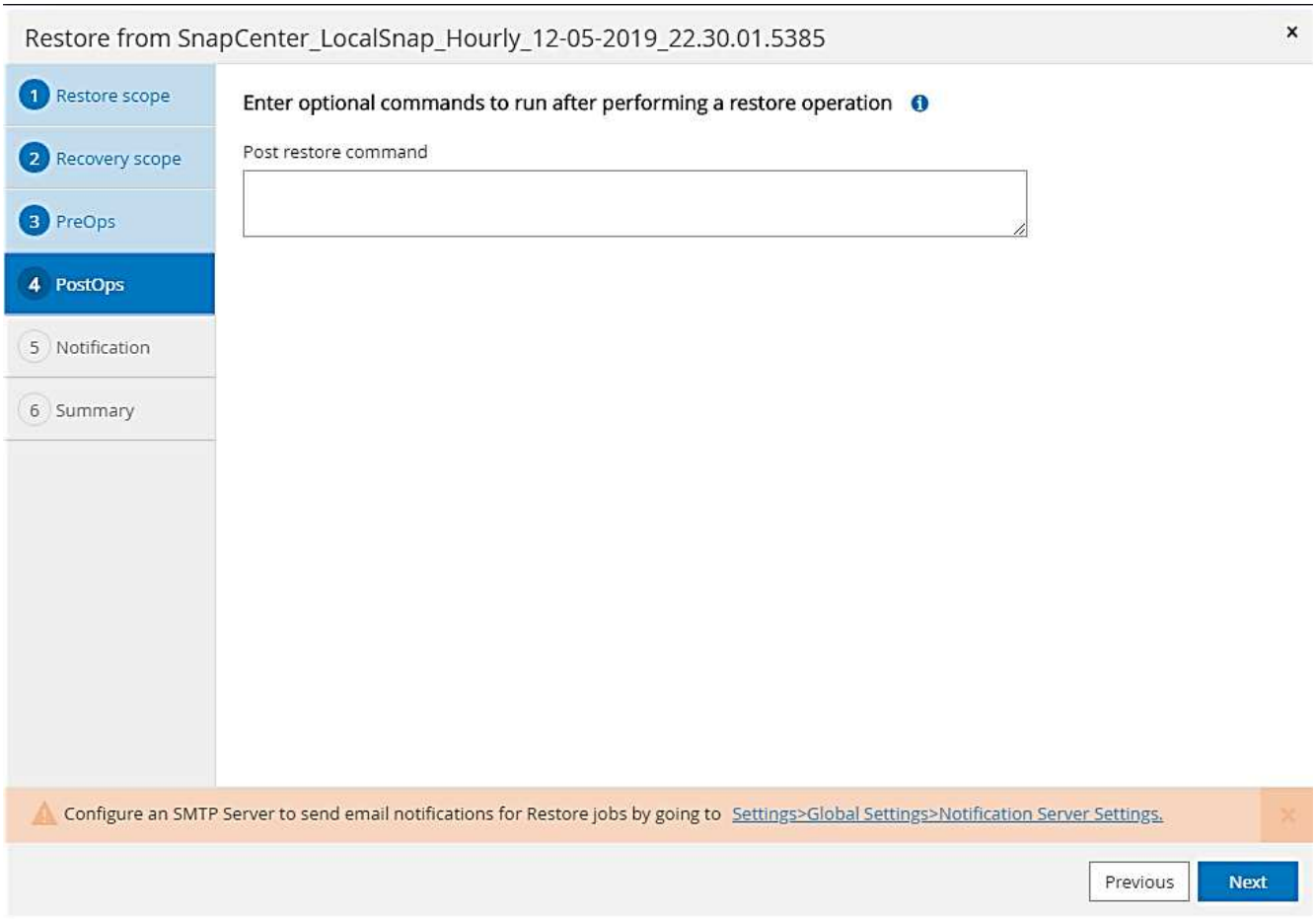
SnapCenter verwendet den Standardpfad oder die geänderten Pfade in der HANA global.ini-Datei, um die Backup-Standorte für das Protokoll und den Katalog vorab aufzufüllen.



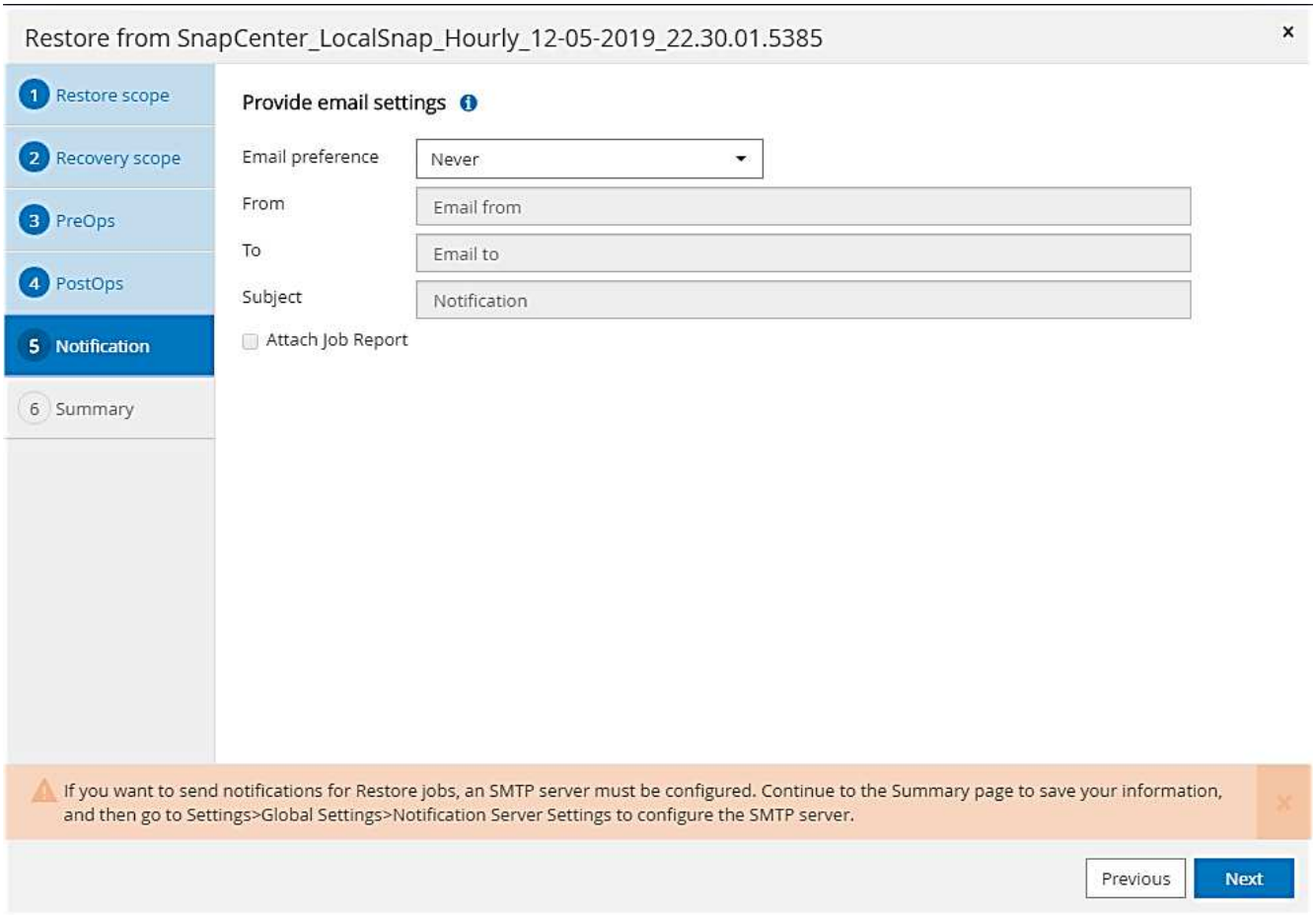
4. Geben Sie die optionalen Befehle zur Vorratspeicher ein.



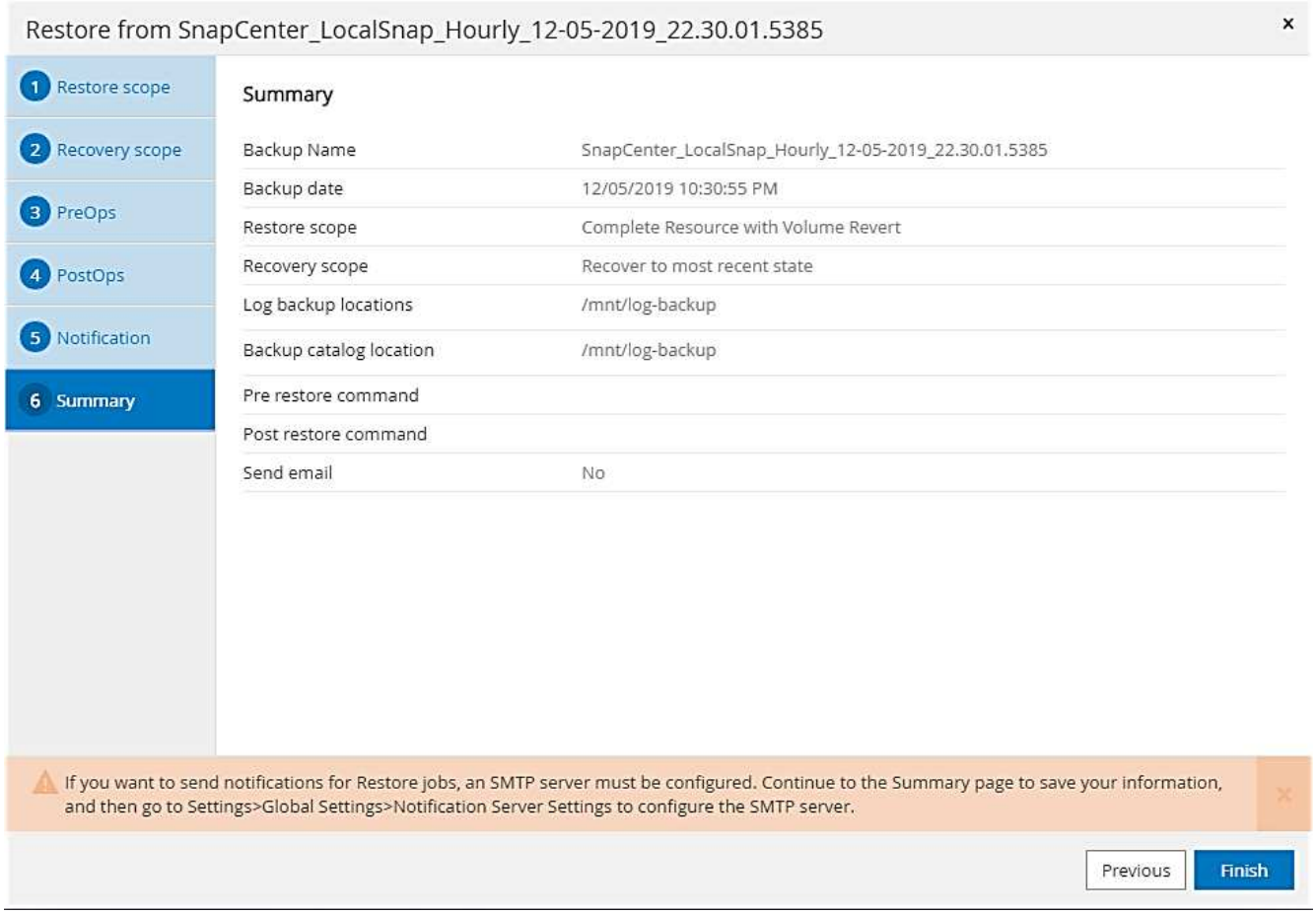
5. Geben Sie die optionalen Befehle nach der Wiederherstellung ein.



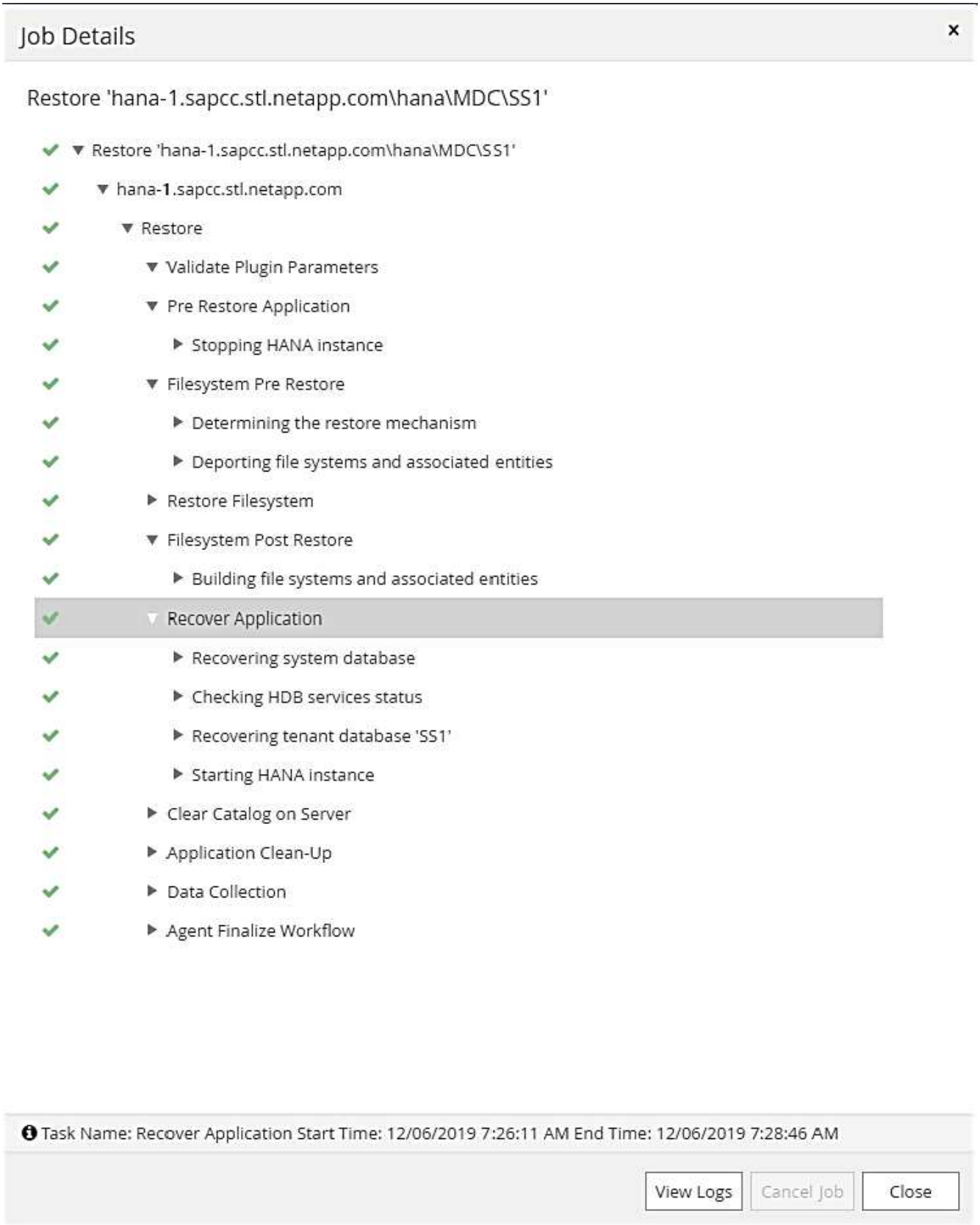
6. Geben Sie die optionalen E-Mail-Einstellungen ein.



7. Um den Wiederherstellungsvorgang zu starten, klicken Sie auf Fertig stellen.



8. SnapCenter führt den Wiederherstellungsvorgang und die Wiederherstellung aus. Dieses Beispiel zeigt die Jobdetails des Wiederherstellungsjobs.



Restore- und Recovery-Vorgang für einzelne Mandanten

Mit SnapCenter 4.3 werden Restore-Vorgänge für einzelne Mandanten für HANA MDC-Systeme mit einem einzelnen Mandanten oder mit mehreren Mandanten, die von SnapCenter automatisch erkannt wurden, unterstützt.

Sie können eine Restore- und Recovery-Operation mit nur einem Mandanten durchführen:

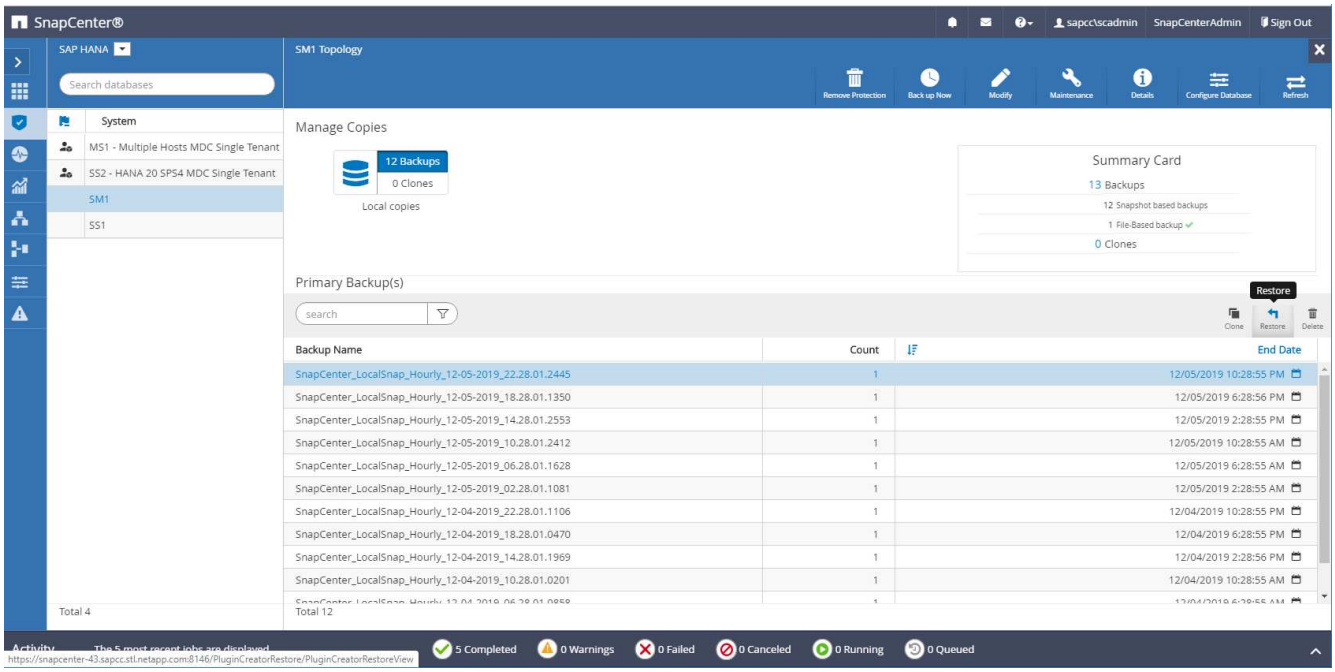
1. Stoppen Sie den Mieter wiederhergestellt werden.
2. Stellen Sie den Mandanten mit SnapCenter wieder her.
   - Bei einer Wiederherstellung vom primären Speicher führt SnapCenter folgende Operationen aus:
     - **NFS.** Speicher einzelne Datei SnapRestore Operationen für alle Dateien der Mandanten-Datenbank.
     - **SAN.** Klonen und verbinden Sie die LUN mit dem Datenbank-Host und kopieren Sie alle Dateien der Mandanten-Datenbank.
   - Bei einer Wiederherstellung vom sekundären Storage führt SnapCenter folgende Operationen aus:
     - **NFS.** Speicher-SnapVault Wiederherstellen von Vorgängen für alle Dateien der Mandanten-Datenbank
     - **SAN.** Klonen und verbinden Sie die LUN mit dem Datenbank-Host und kopieren Sie alle Dateien der Mandanten-Datenbank
3. Stellen Sie den Mandanten mit HANA Studio, Cockpit oder SQL-Anweisung wieder her.

Dieser Abschnitt enthält die Schritte für den Restore- und Recovery-Vorgang vom primären Storage des automatisch erkannten HANA-Systems SM1 (SAP HANA Single-Host, MDC Multiple-Tenant-System via NFS). Aus Benutzereingangsperspektive sind die Workflows bei Restores aus sekundärem oder bei einer Wiederherstellung in einem Fibre Channel SAN-Setup identisch.

1. Beenden Sie die Mandantendatenbank.

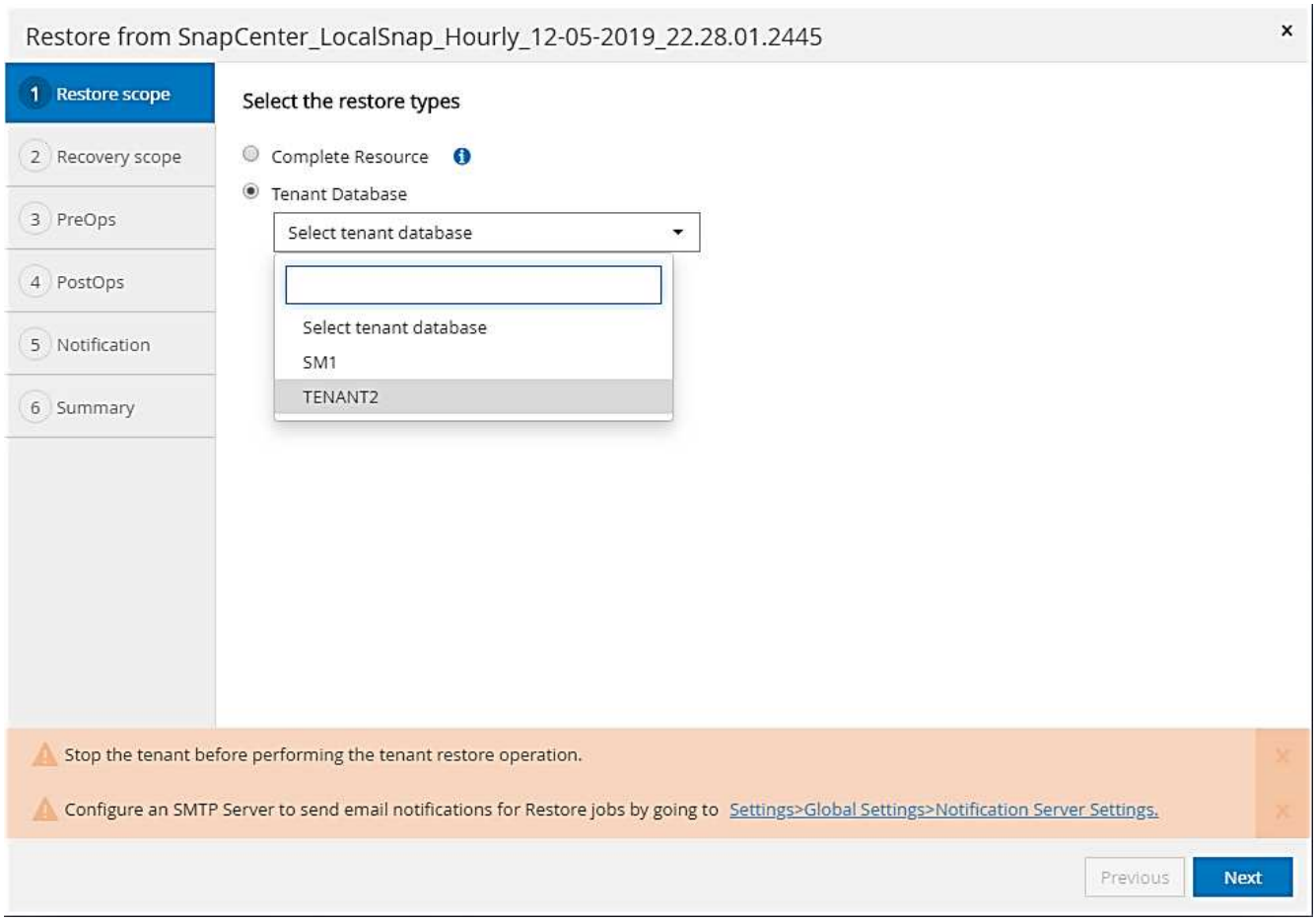
```
sm1adm@hana-2:/usr/sap/SM1/HDB00> hdbsql -U SYSKEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql=>
hdbsql SYSTEMDB=> alter system stop database tenant2;
0 rows affected (overall time 14.215281 sec; server time 14.212629 sec)
hdbsql SYSTEMDB=>
```

2. Wählen Sie ein Backup in SnapCenter aus, das für den Wiederherstellungsvorgang verwendet werden soll.



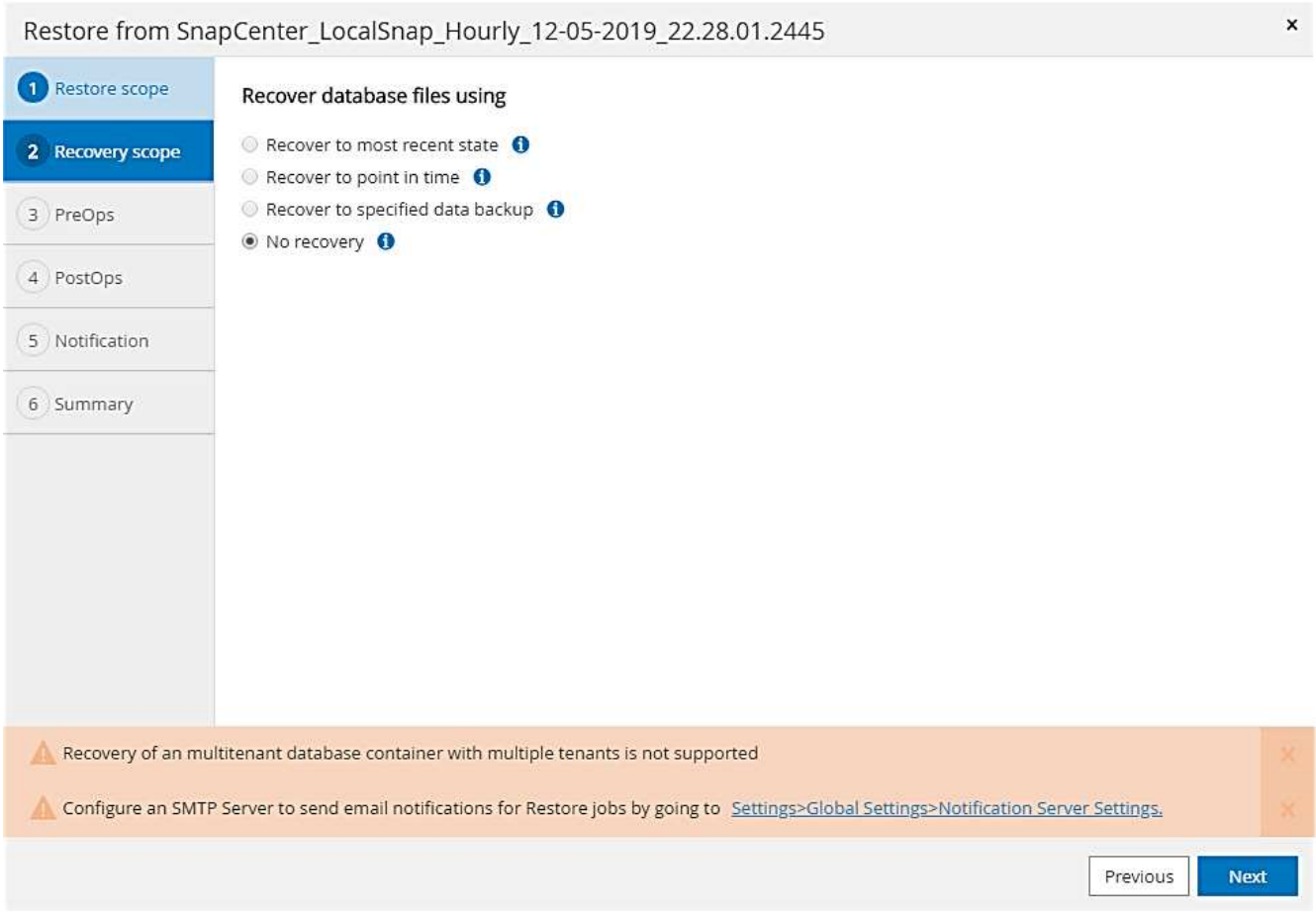
3. Wählen Sie den wiederherzustellenden Mandanten aus.

SnapCenter zeigt eine Liste aller Mandanten an, die im ausgewählten Backup enthalten sind.

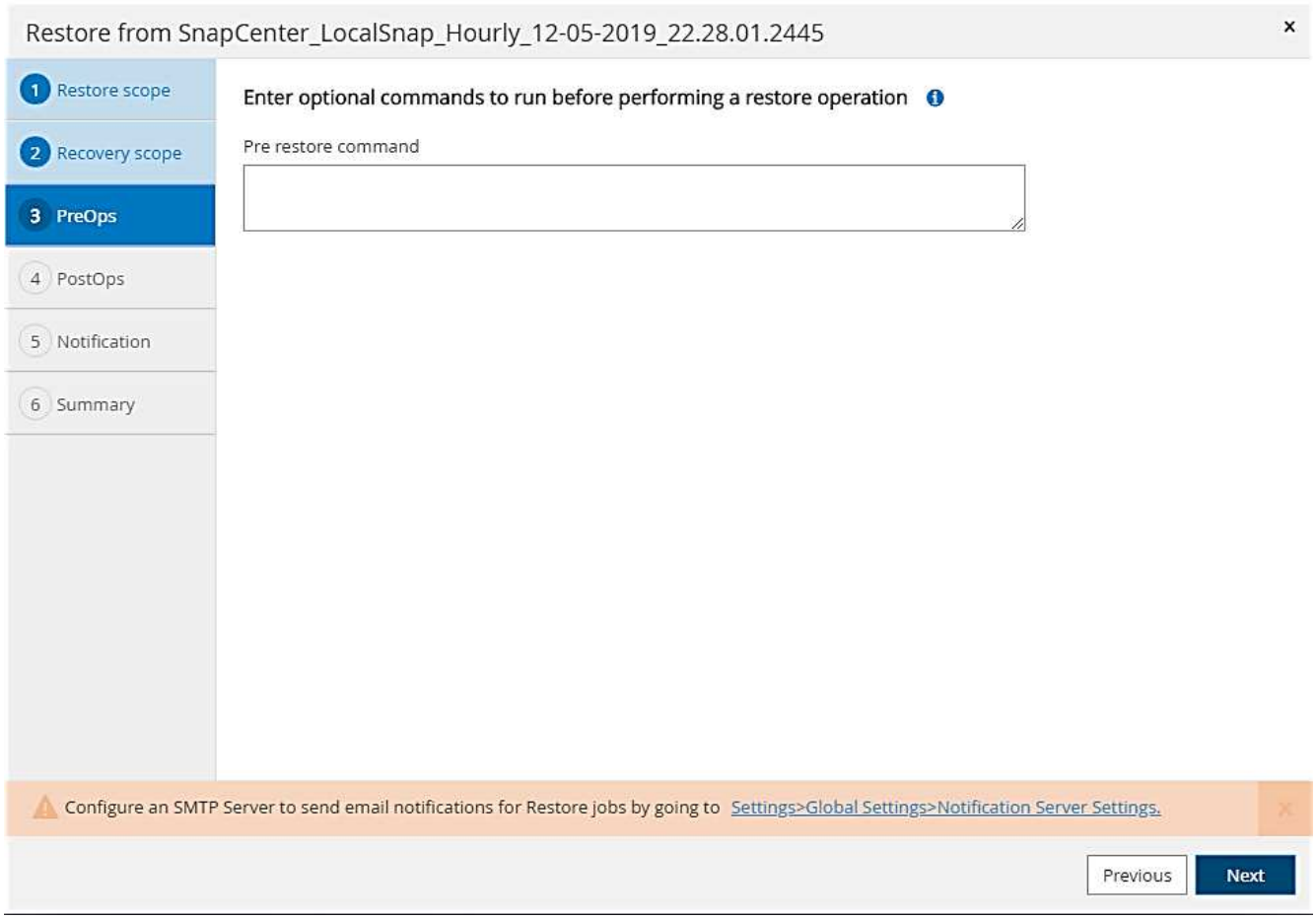


Die Recovery einzelner Mandanten wird mit SnapCenter 4.3 nicht unterstützt. Keine Wiederherstellung ist

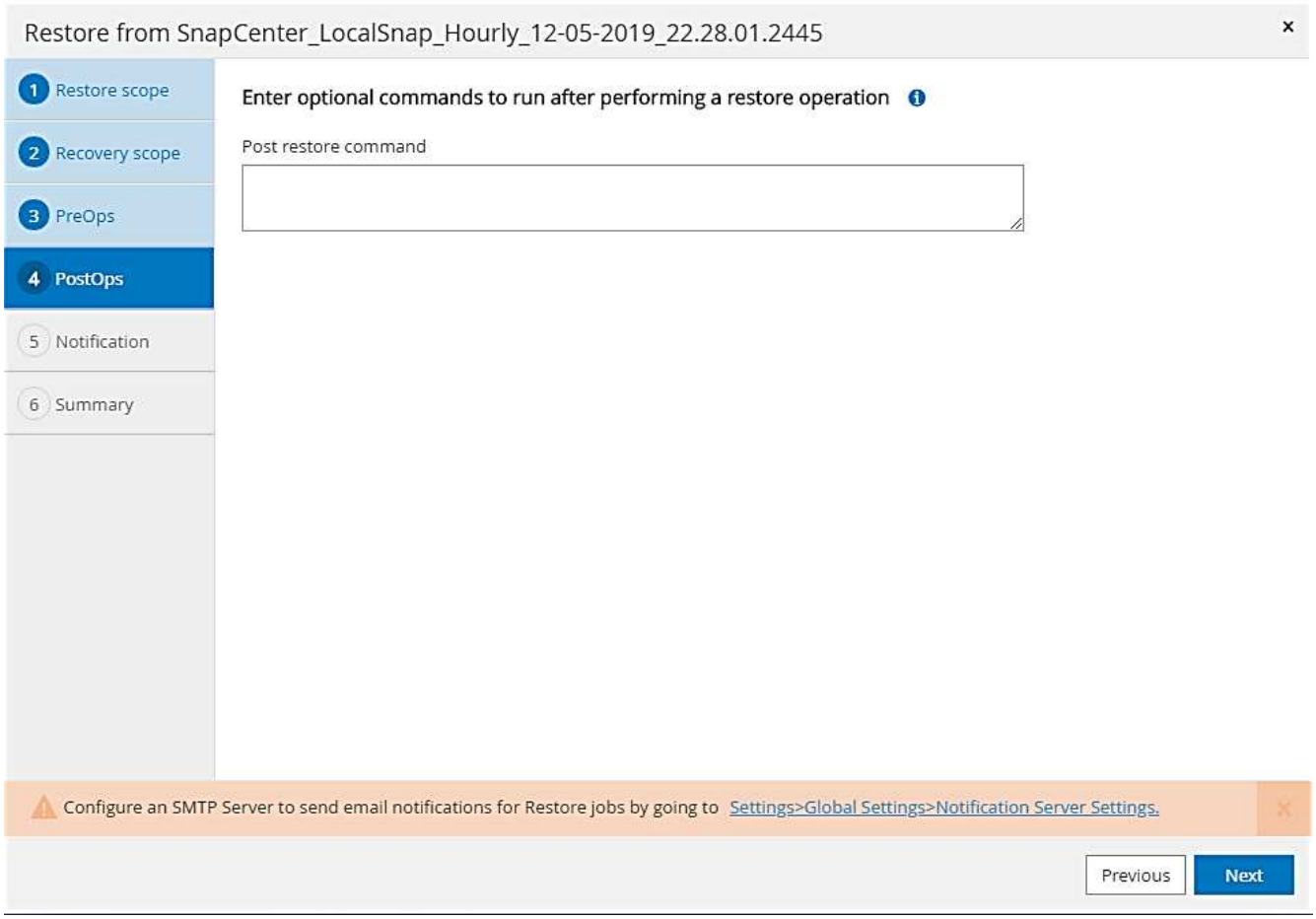
vorausgewählt und kann nicht geändert werden.



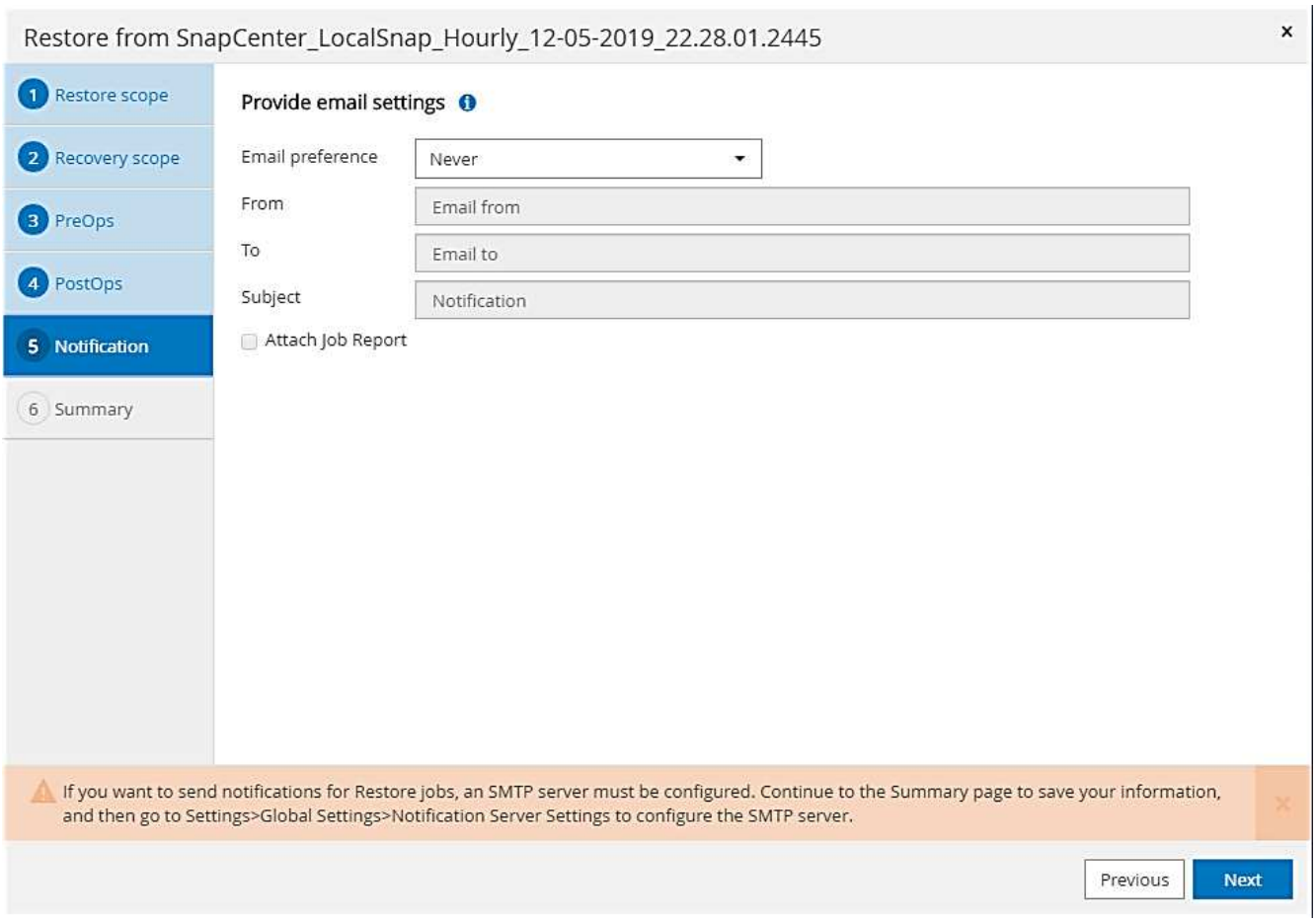
4. Geben Sie die optionalen Befehle zur Vorratspeicher ein.



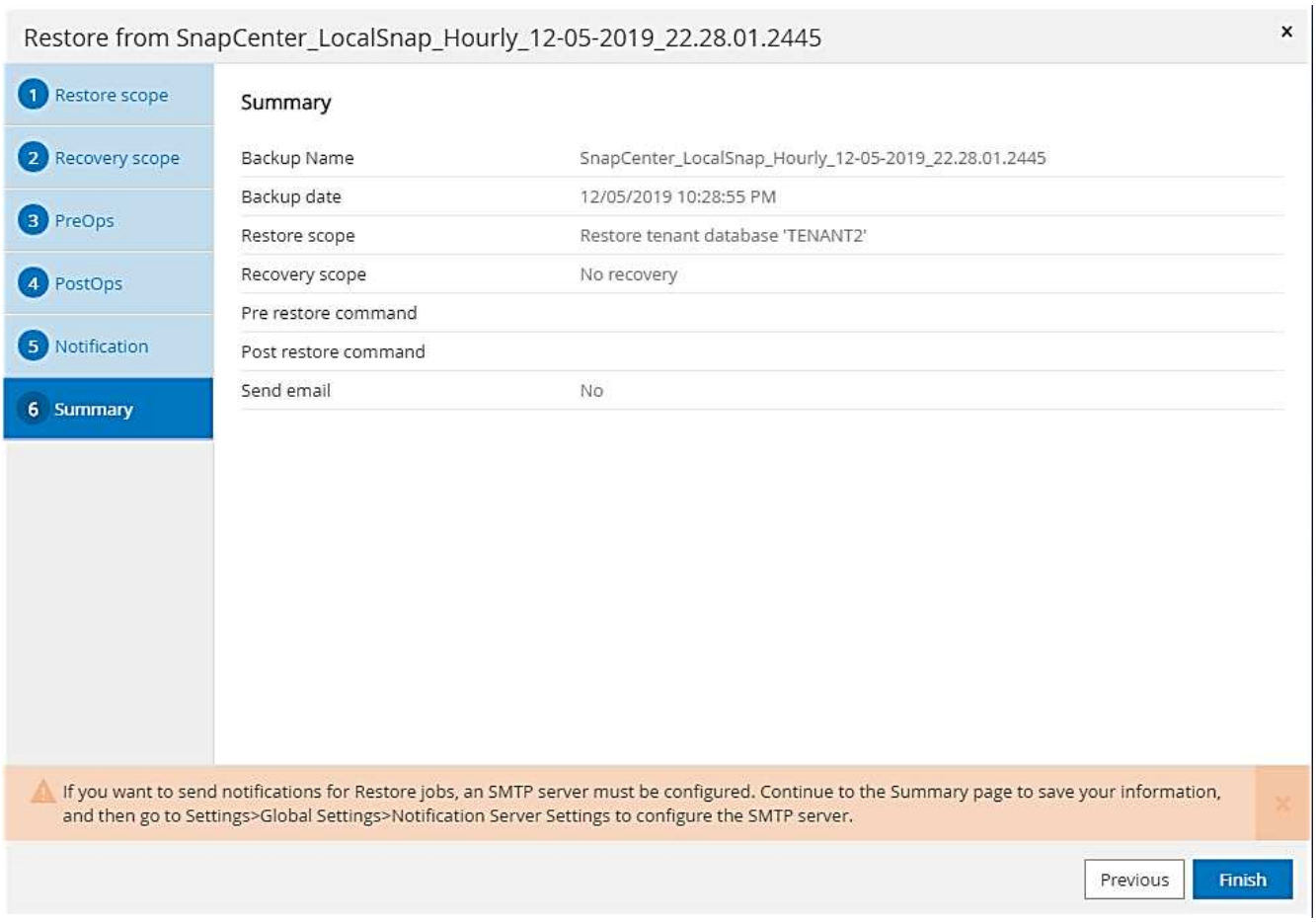
5. Geben Sie optionale Befehle nach der Wiederherstellung ein.



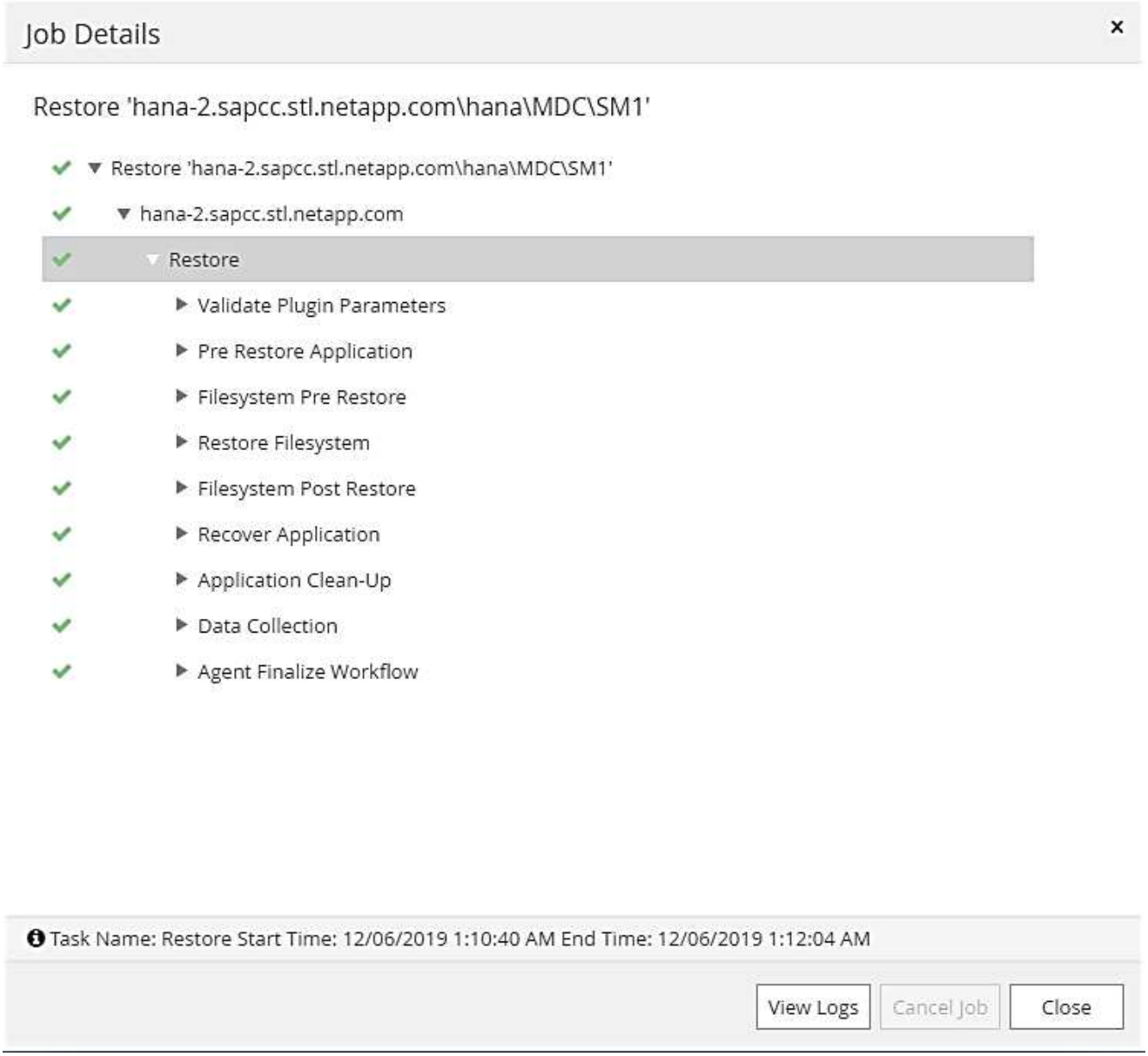
6. Geben Sie die optionalen E-Mail-Einstellungen ein.



7. Um den Wiederherstellungsvorgang zu starten, klicken Sie auf Fertig stellen.



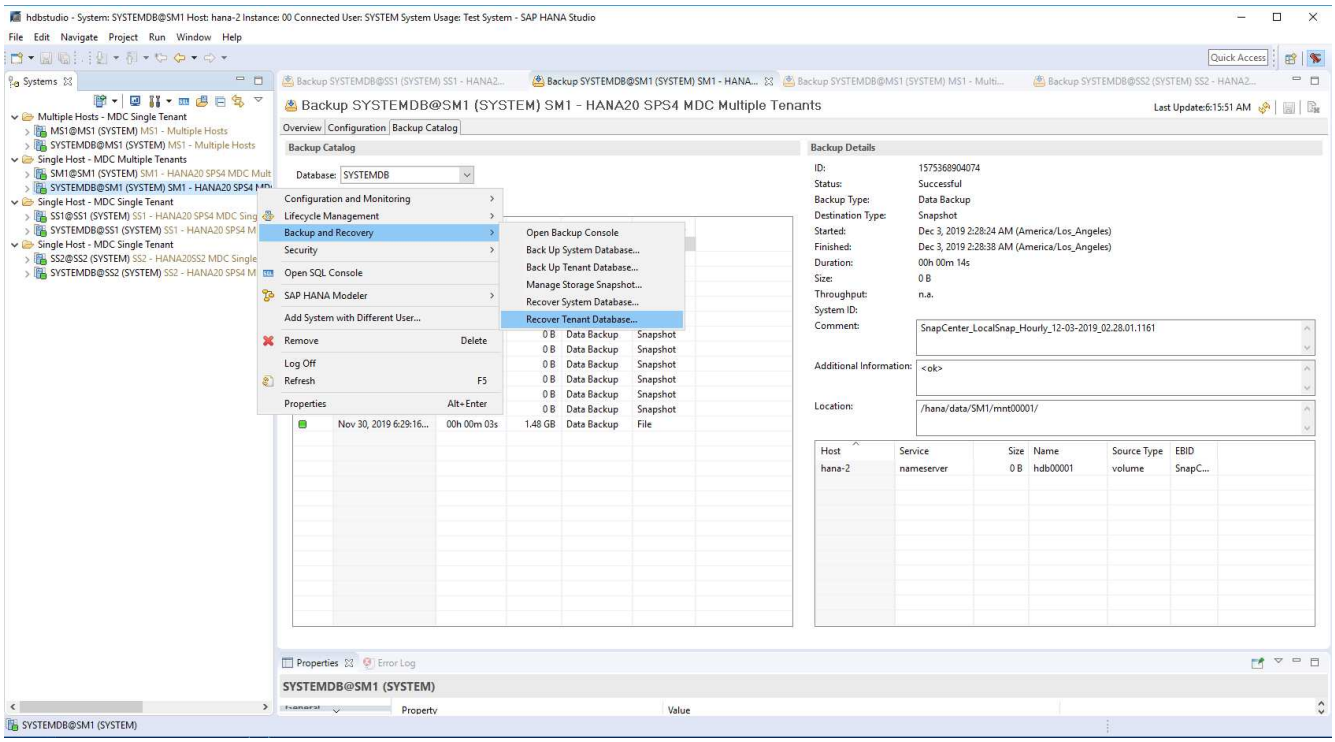
Der Wiederherstellungsvorgang wird von SnapCenter ausgeführt. Dieses Beispiel zeigt die Jobdetails des Wiederherstellungsjobs.



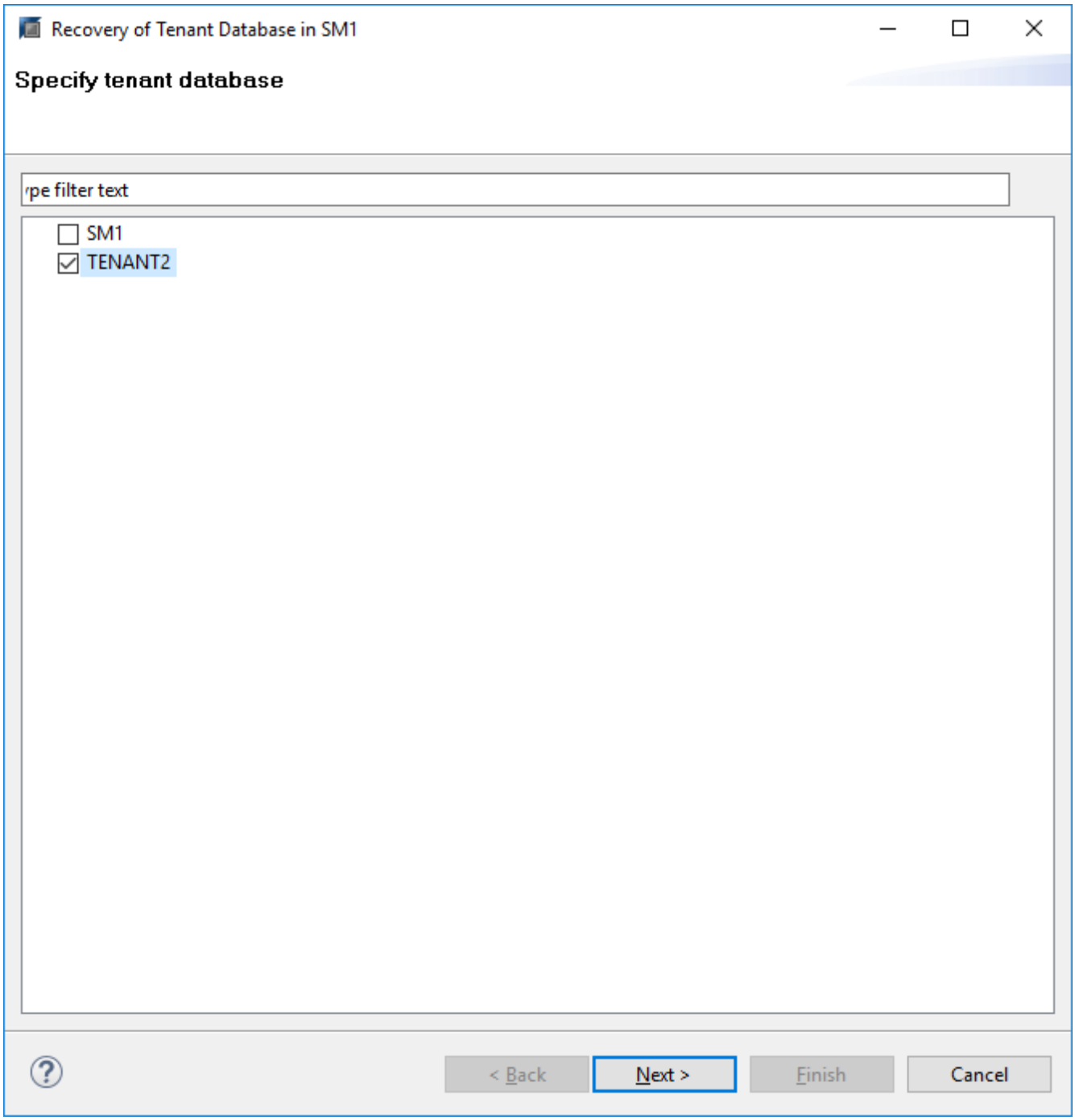
Nach Abschluss der Mandantenwiederherstellung werden nur die mandantenrelevanten Daten wiederhergestellt. Auf dem Filesystem des HANA-Datenbank-Hosts sind die wiederhergestellte Datendatei und die Snapshot Backup ID-Datei des Mandanten verfügbar.

```
sm1adm@hana-2:/usr/sap/SM1/HDB00> ls -al /hana/data/SM1/mnt00001/*
-rw-r--r-- 1 sm1adm sapsys   17 Dec  6 04:01
/hana/data/SM1/mnt00001/nameserver.lck
/hana/data/SM1/mnt00001/hdb00001:
total 3417776
drwxr-x--- 2 sm1adm sapsys       4096 Dec  6 01:14 .
drwxr-x--- 6 sm1adm sapsys       4096 Nov 20 09:35 ..
-rw-r----- 1 sm1adm sapsys 3758096384 Dec  6 03:59 datavolume_0000.dat
-rw-r----- 1 sm1adm sapsys          0 Nov 20 08:36
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r----- 1 sm1adm sapsys         36 Nov 20 08:37 landscape.id
/hana/data/SM1/mnt00001/hdb00002.00003:
total 67772
drwxr-xr-- 2 sm1adm sapsys      4096 Nov 20 08:37 .
drwxr-x--- 6 sm1adm sapsys      4096 Nov 20 09:35 ..
-rw-r--r-- 1 sm1adm sapsys 201441280 Dec  6 03:59 datavolume_0000.dat
-rw-r--r-- 1 sm1adm sapsys         0 Nov 20 08:37
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
/hana/data/SM1/mnt00001/hdb00002.00004:
total 3411836
drwxr-xr-- 2 sm1adm sapsys       4096 Dec  6 03:57 .
drwxr-x--- 6 sm1adm sapsys       4096 Nov 20 09:35 ..
-rw-r--r-- 1 sm1adm sapsys 3758096384 Dec  6 01:14 datavolume_0000.dat
-rw-r--r-- 1 sm1adm sapsys          0 Nov 20 09:35
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r----- 1 sm1adm sapsys     155648 Dec  6 01:14
snapshot_databackup_0_1
/hana/data/SM1/mnt00001/hdb00003.00003:
total 3364216
drwxr-xr-- 2 sm1adm sapsys       4096 Dec  6 01:14 .
drwxr-x--- 6 sm1adm sapsys       4096 Nov 20 09:35 ..
-rw-r--r-- 1 sm1adm sapsys 3758096384 Dec  6 03:59 datavolume_0000.dat
-rw-r--r-- 1 sm1adm sapsys          0 Nov 20 08:37
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
sm1adm@hana-2:/usr/sap/SM1/HDB00>
```

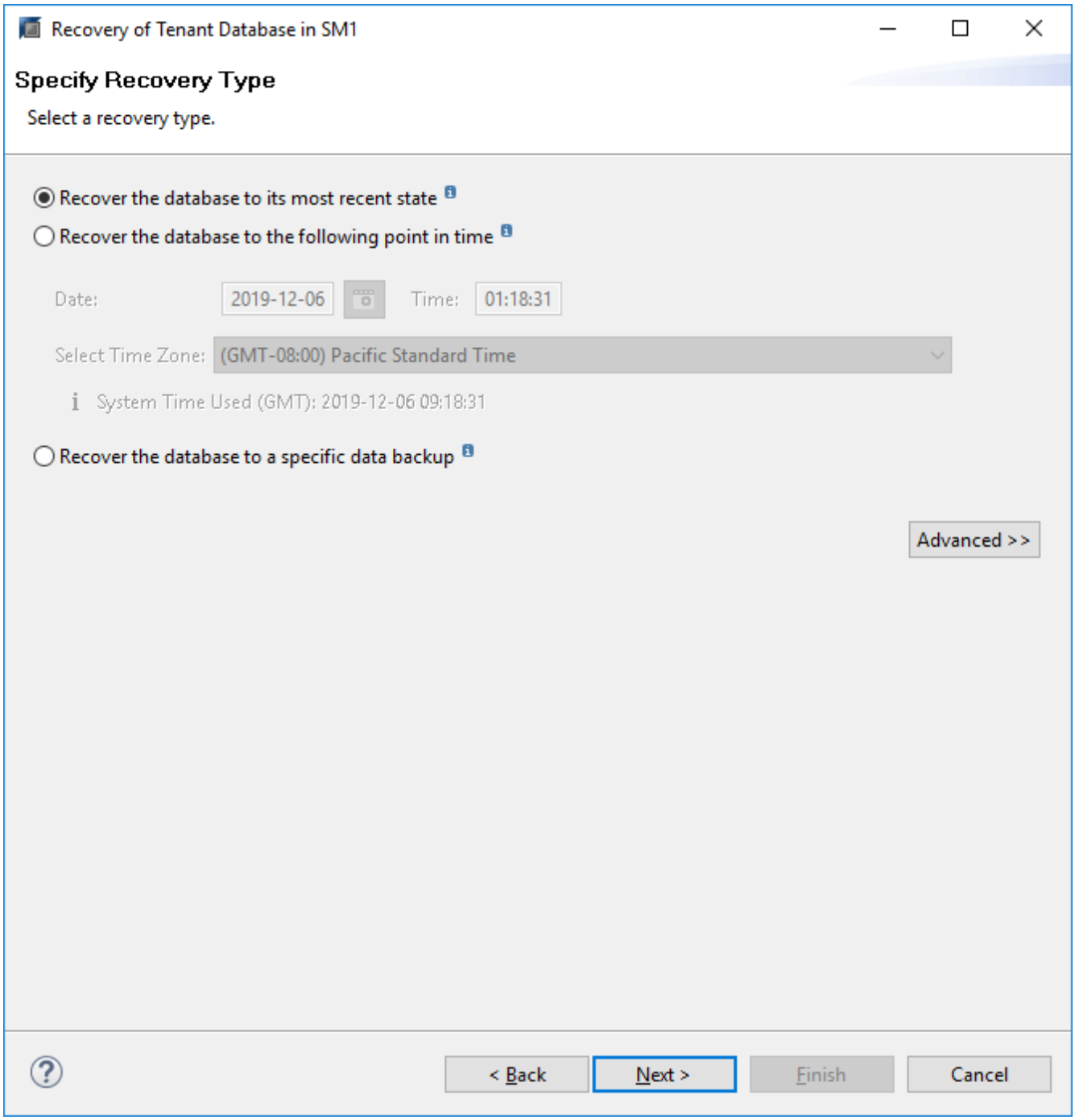
8. Starten Sie die Recovery mit HANA Studio.



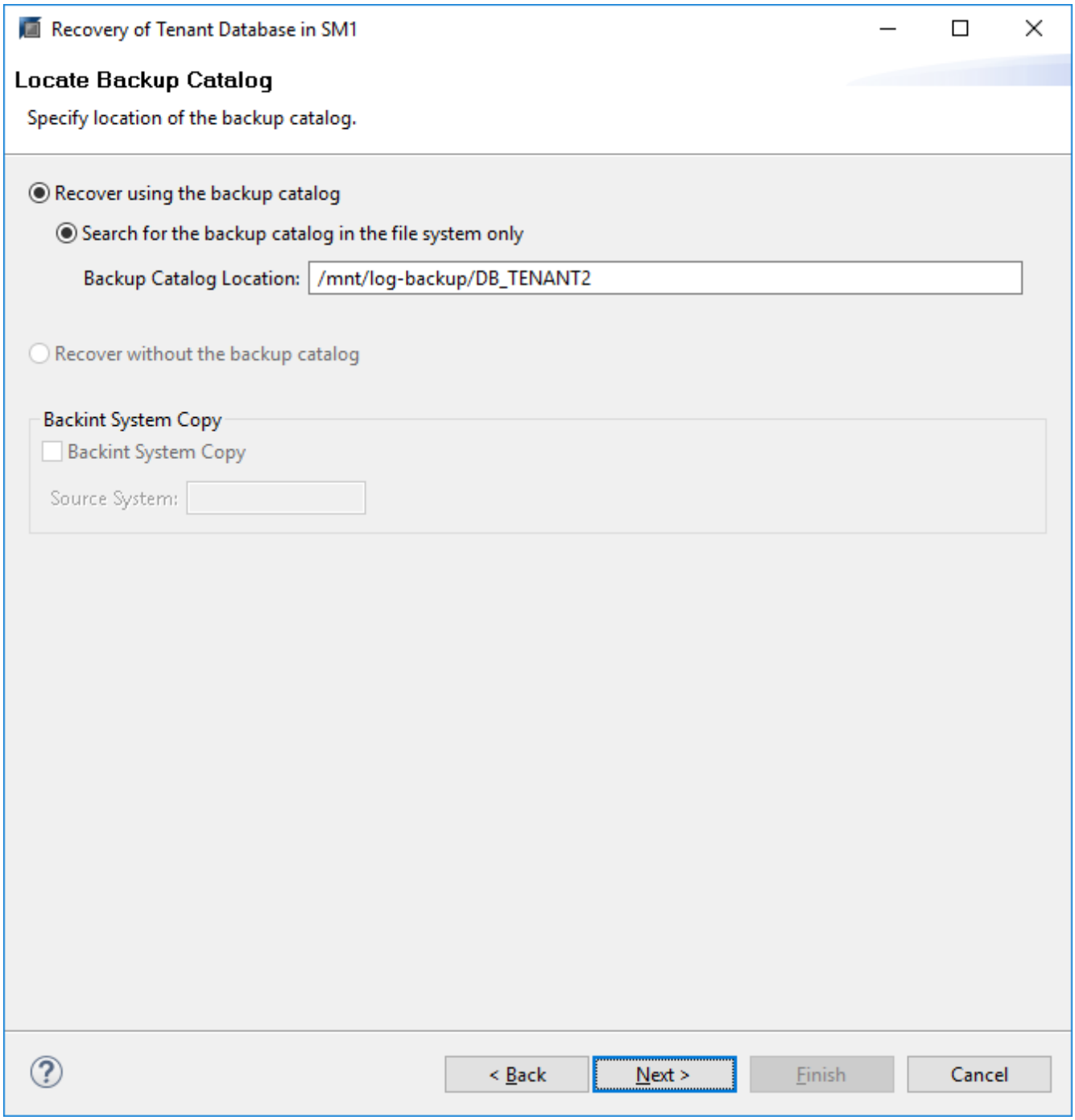
9. Wählen Sie den Mandanten aus.

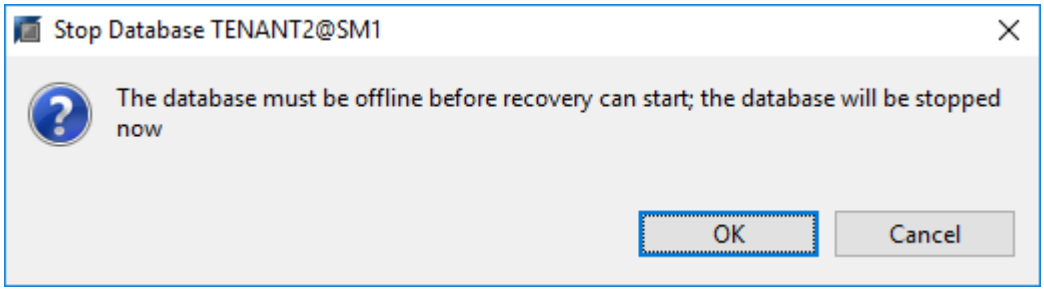


10. Wählen Sie den Wiederherstellungstyp aus.



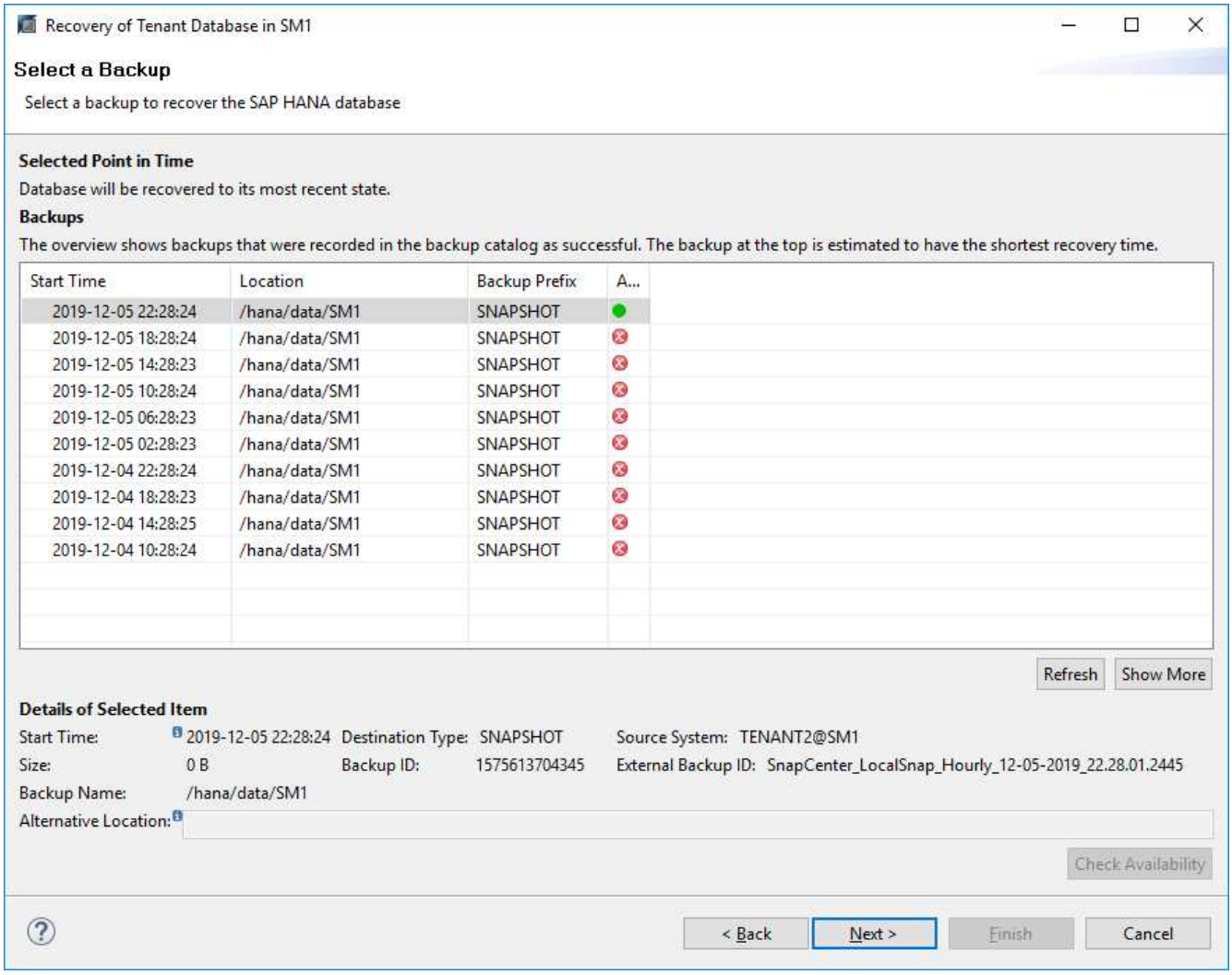
11. Stellen Sie den Speicherort des Backup-Katalogs bereit.



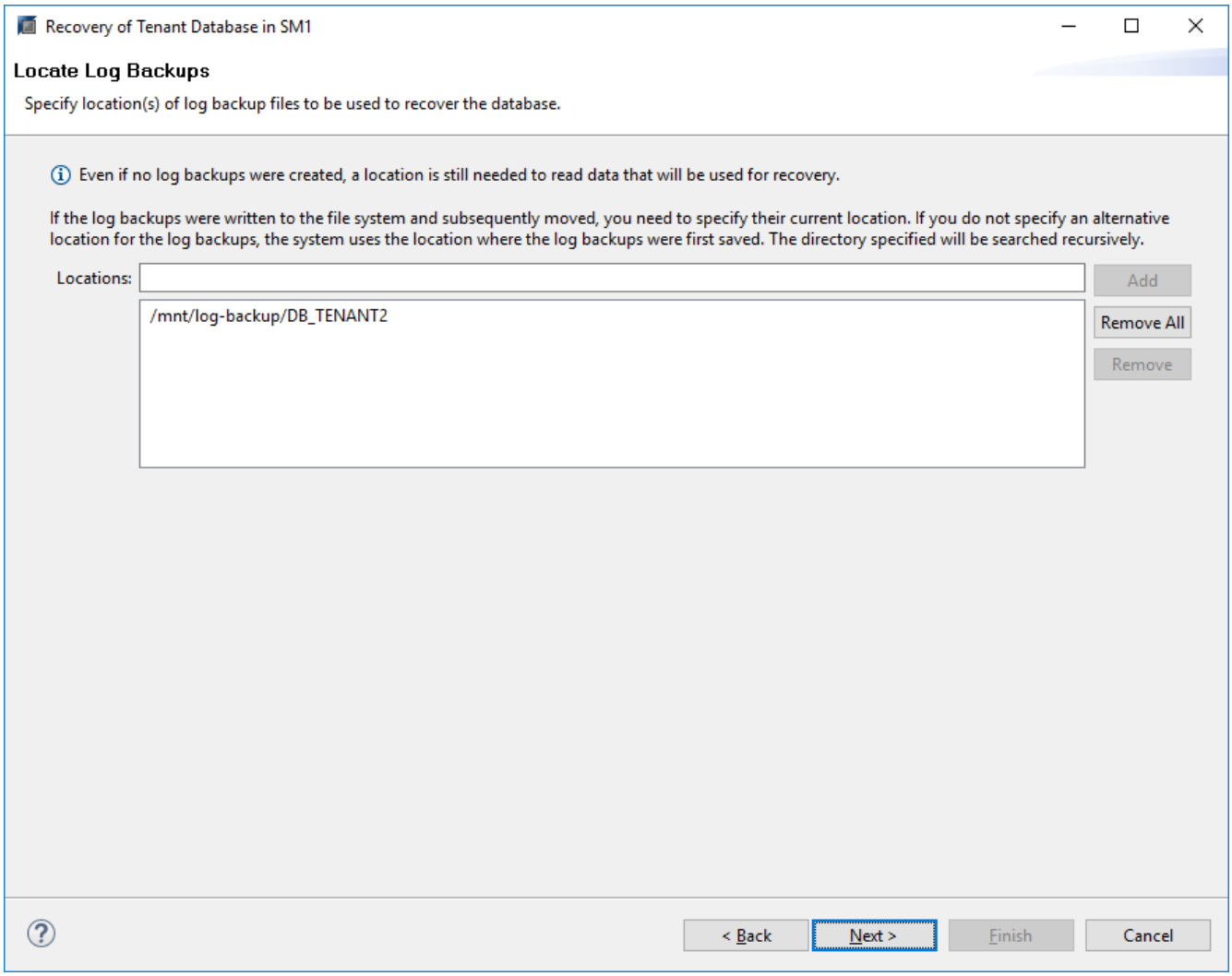


Im Backup-Katalog wird das wiederhergestellte Backup mit einem grünen Symbol hervorgehoben. Die externe Backup-ID zeigt den Backup-Namen an, der zuvor in SnapCenter ausgewählt wurde.

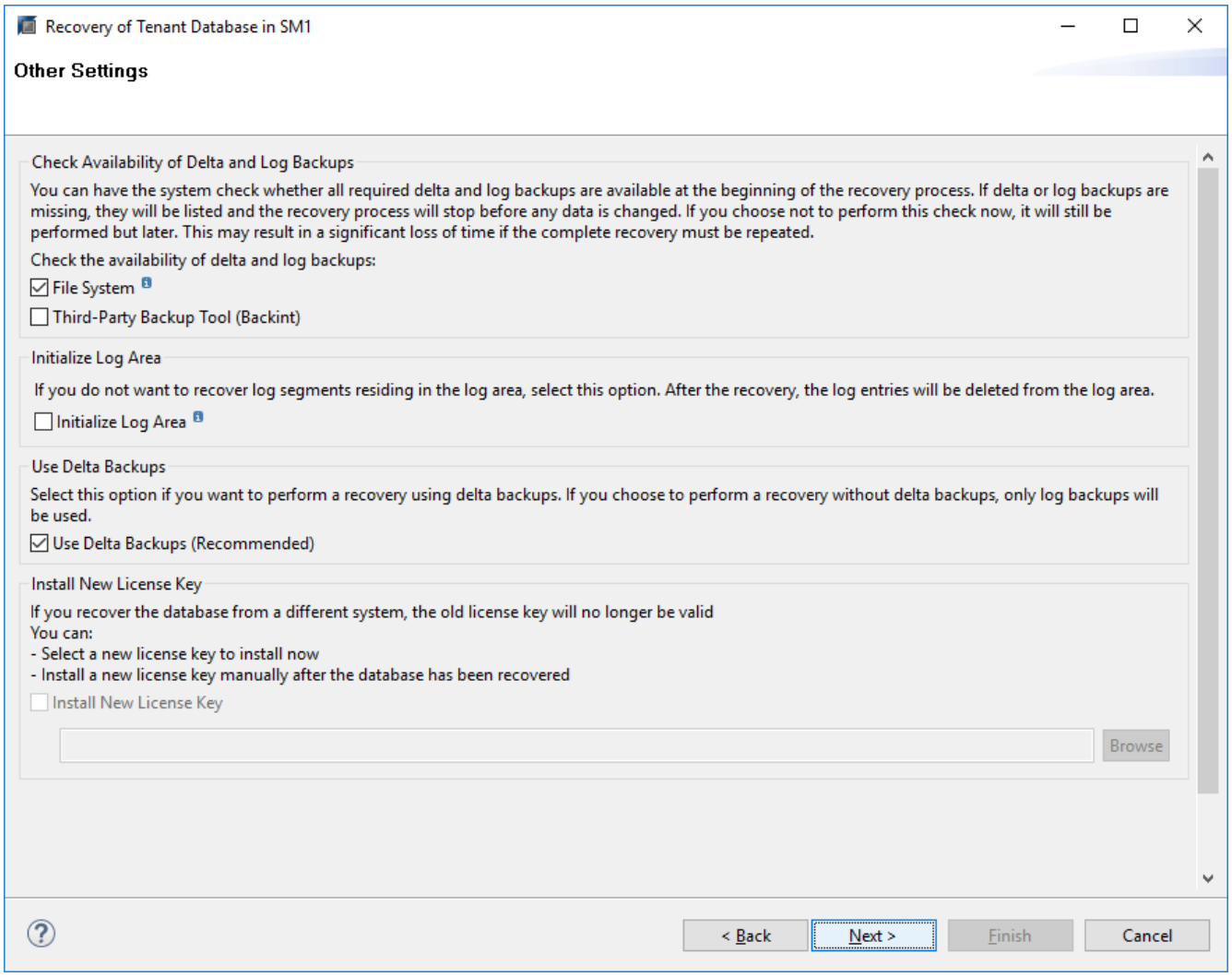
12. Wählen Sie den Eintrag mit dem grünen Symbol aus, und klicken Sie auf Weiter.



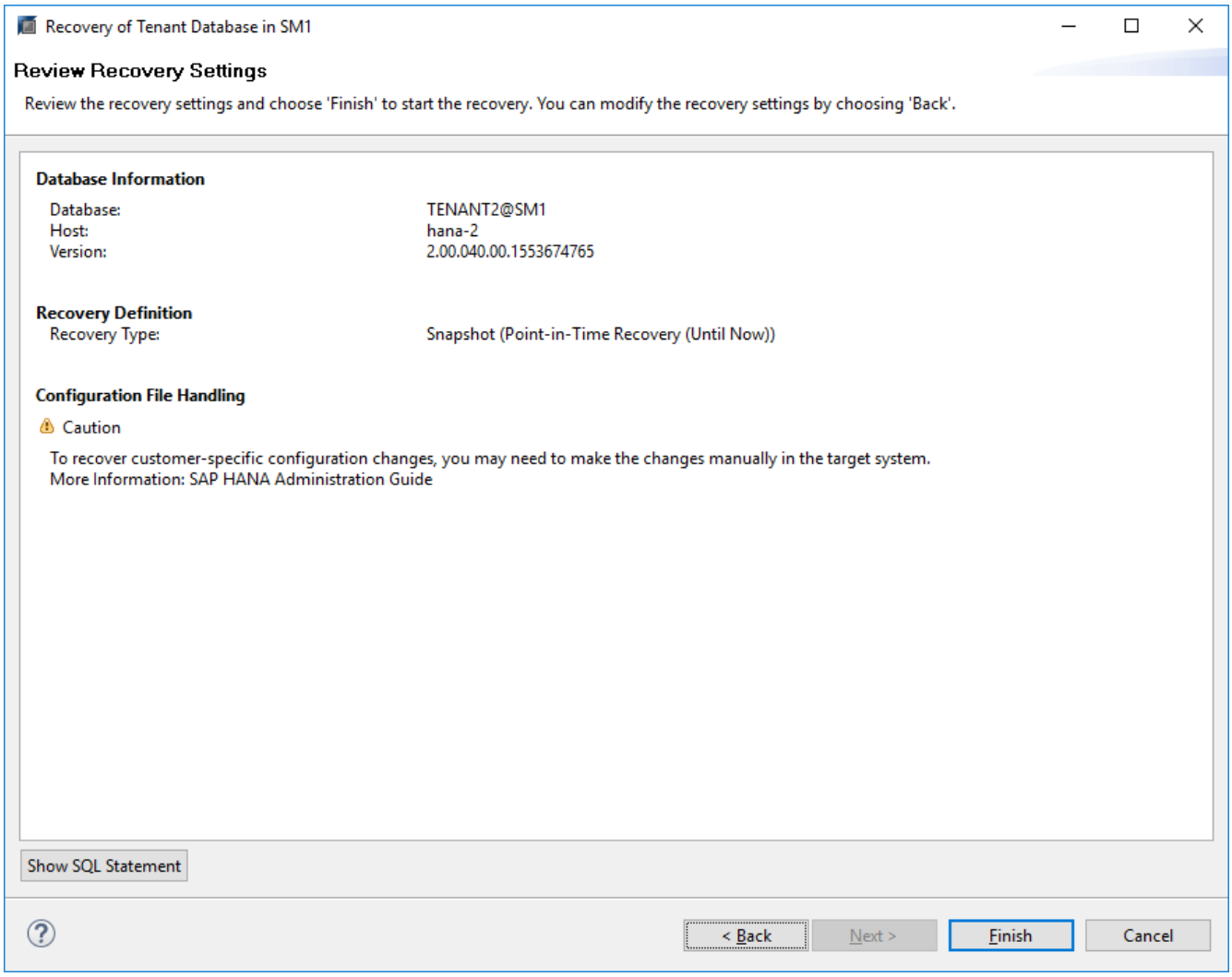
13. Geben Sie den Backup-Speicherort für das Protokoll an.

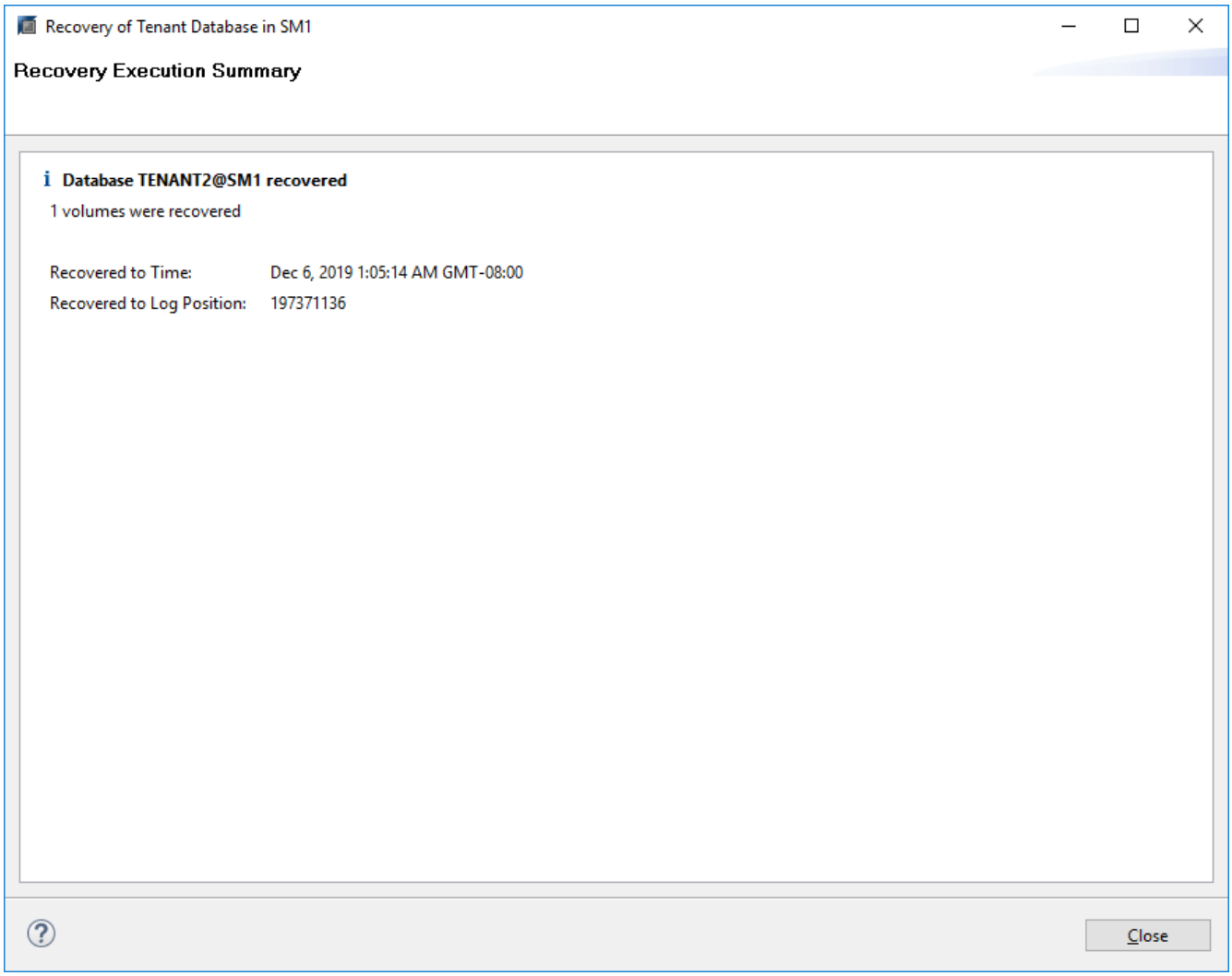


14. Wählen Sie die anderen Einstellungen nach Bedarf aus.



15. Starten Sie den Recovery-Vorgang des Mandanten.


Recovery of Tenant Database in SM1
Review Recovery Settings
Review the recovery settings and choose 'Finish' to start the recovery. You can modify the recovery settings by choosing 'Back'.
Database Information
Database: TENANT2@SM1
Host: hana-2
Version: 2.00.040.00.1553674765
Recovery Definition
Recovery Type: Snapshot (Point-in-Time Recovery (Until Now))
Configuration File Handling
Caution
To recover customer-specific configuration changes, you may need to make the changes manually in the target system.
More Information: SAP HANA Administration Guide
Show SQL Statement
< Back
Next >
Finish
Cancel



Manuelle Wiederherstellung

Gehen Sie wie folgt vor, um ein SAP HANA MDC-Einzelmandant-System mit SAP HANA Studio und SnapCenter wiederherzustellen:

1. Vorbereitung des Restore- und Recovery-Prozesses mit SAP HANA Studio:
   a. Wählen Sie Recover System Database und bestätigen Sie das Herunterfahren des SAP HANA-Systems.
   b. Wählen Sie den Wiederherstellungstyp und den Speicherort für die Protokollsicherung aus.
   c. Es wird eine Liste der Daten-Backups angezeigt. Wählen Sie Backup, um die externe Backup-ID anzuzeigen.
2. Führen Sie den Wiederherstellungsprozess mit SnapCenter aus:
   a. Wählen Sie in der Topologieansicht der Ressource lokale Kopien aus, die aus dem primären Storage oder Vault-Kopien wiederhergestellt werden sollen, wenn Sie eine Wiederherstellung aus einem externen Backup-Storage durchführen möchten.
   b. Wählen Sie das SnapCenter Backup aus, das mit der externen Backup-ID oder dem Kommentarfeld aus SAP HANA Studio übereinstimmt.
   c. Starten Sie den Wiederherstellungsprozess.

Wenn eine Volume-basierte Wiederherstellung aus dem primären Speicher ausgewählt wird, müssen die Daten-Volumes vor der Wiederherstellung von allen SAP HANA-Datenbank-Hosts abgehängt und nach Abschluss des Wiederherstellungsprozesses erneut gemountet werden.

Bei einer SAP HANA-Konfiguration mit mehreren Hosts mit FC werden die Unmount- und Mount-Vorgänge im Rahmen des Shutdown- und Startvorgangs der Datenbank vom SAP HANA-Namensserver ausgeführt.

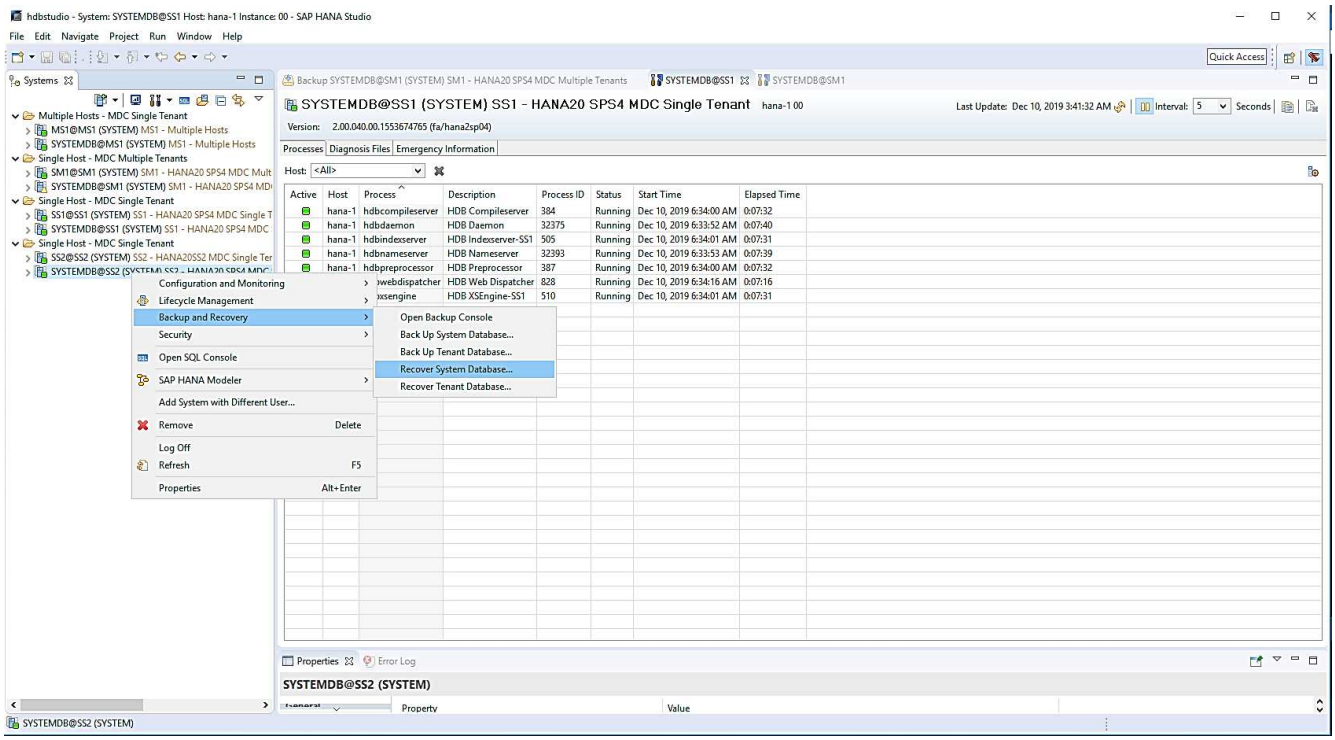
3. Führen Sie den Recovery-Prozess für die Systemdatenbank mit SAP HANA Studio aus:
   a. Klicken Sie in der Backup-Liste auf Aktualisieren, und wählen Sie das verfügbare Backup für die Recovery aus (wird durch ein grünes Symbol angezeigt).
   b. Starten Sie den Wiederherstellungsprozess. Nach Abschluss des Wiederherstellungsprozesses wird die Systemdatenbank gestartet.
4. Führen Sie den Recovery-Prozess für die Mandantendatenbank mit SAP HANA Studio aus:
   a. Wählen Sie die Option „Tenant Database wiederherstellen“ und wählen Sie den Mieter aus, der wiederhergestellt werden soll.
   b. Wählen Sie den Wiederherstellungstyp und den Speicherort für die Protokollsicherung aus.

      Es wird eine Liste der Daten-Backups angezeigt. Da das Daten-Volume bereits wiederhergestellt ist, wird das Mandanten-Backup als verfügbar angezeigt (in grün).

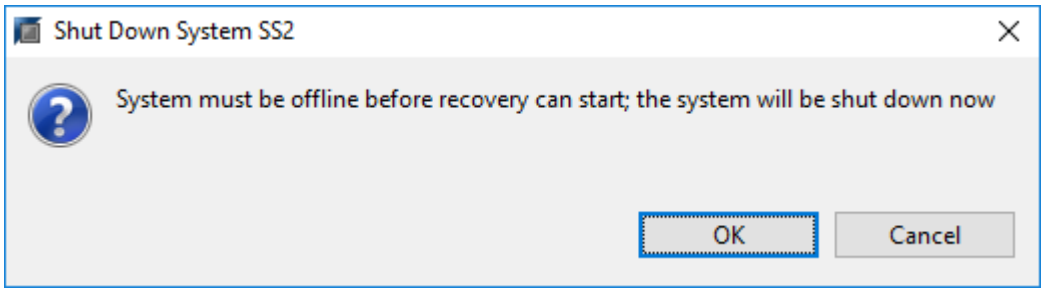
   c. Wählen Sie dieses Backup aus, und starten Sie den Wiederherstellungsprozess. Nach Abschluss des Recovery-Prozesses wird die Mandantendatenbank automatisch gestartet.

Im folgenden Abschnitt werden die Schritte der Wiederherstellungs- und Wiederherstellungsvorgänge des manuell konfigurierten HANA-Systems SS2 beschrieben (SAP HANA einzelner Host, MDC-Mehrmandantensystem mit NFS).

1. Wählen Sie in SAP HANA Studio die Option Systemdatenbank wiederherstellen aus, um die Wiederherstellung der Systemdatenbank zu starten.

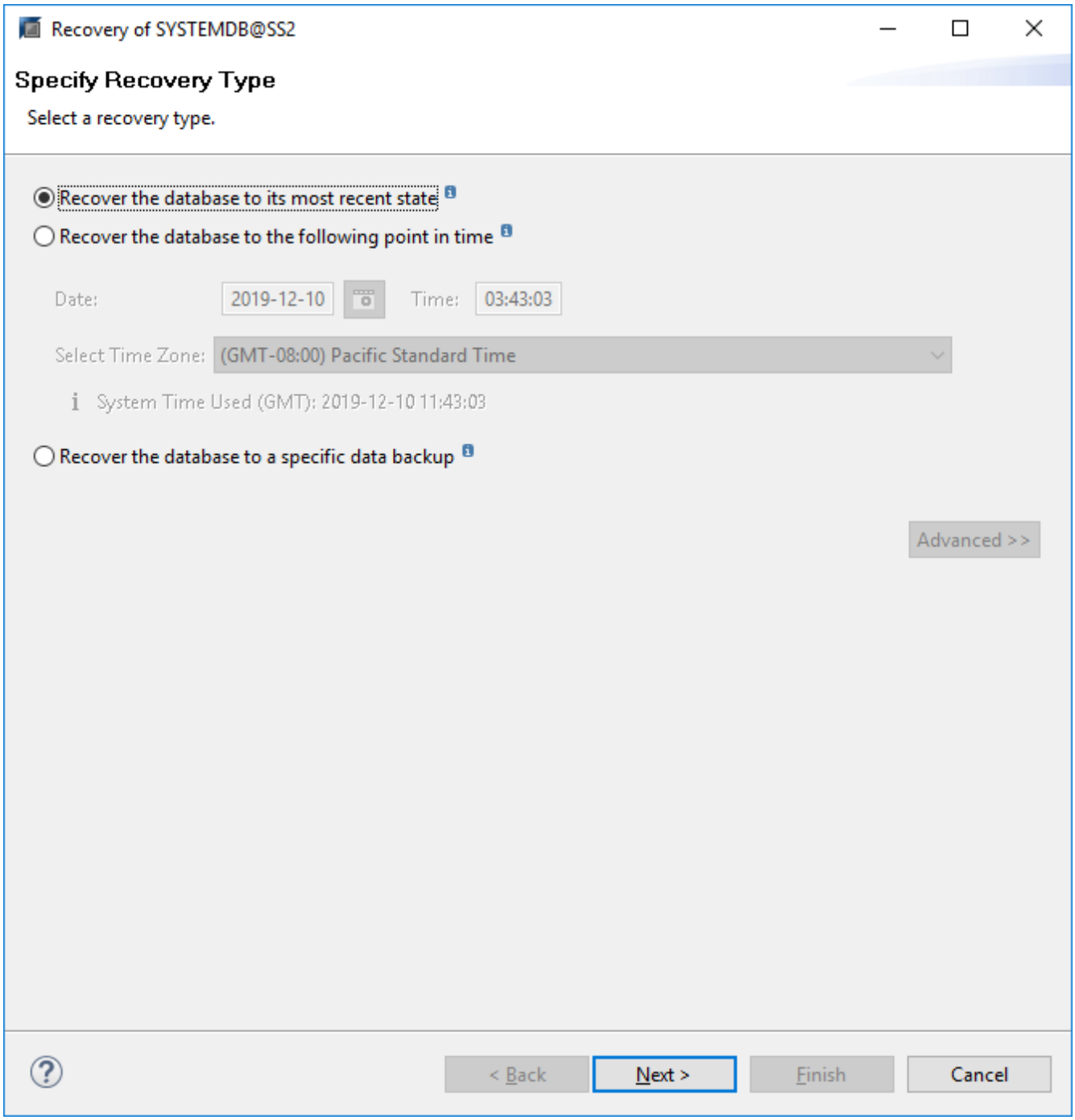


2. Klicken Sie auf OK, um die SAP HANA-Datenbank herunterzufahren.

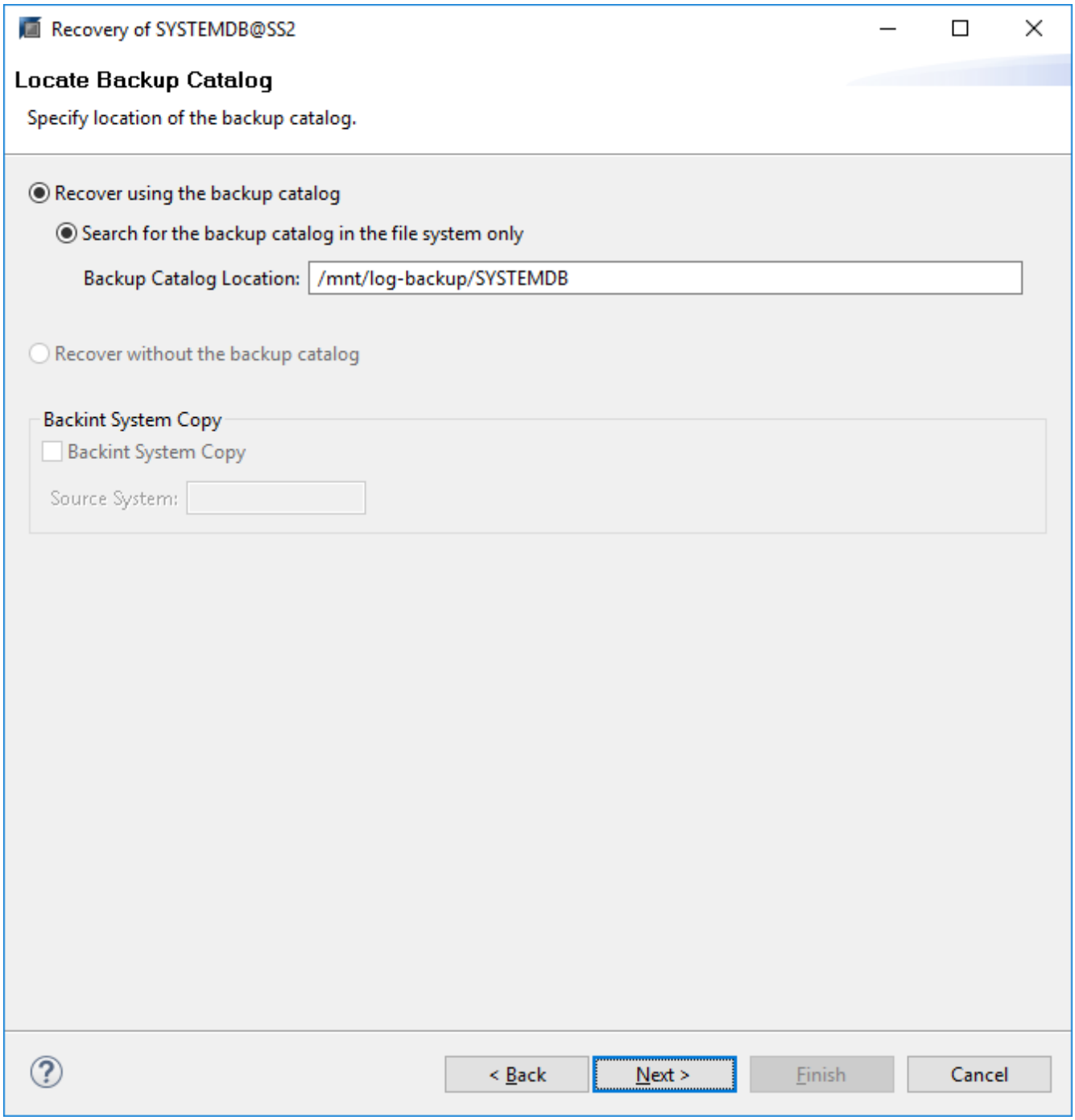


Das SAP HANA-System wird heruntergefahren und der Wiederherstellungsassistent wird gestartet.

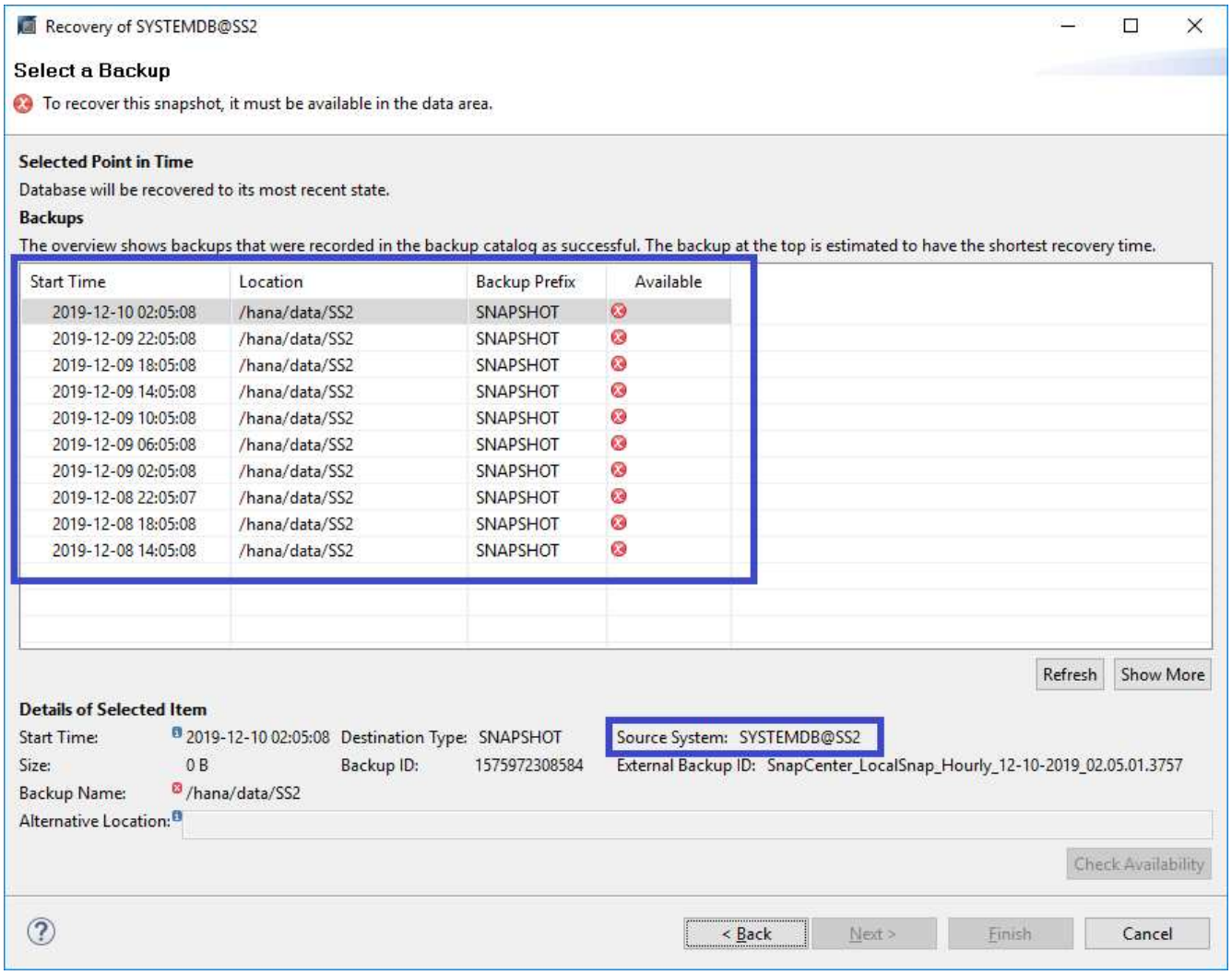
3. Wählen Sie den Wiederherstellungstyp aus, und klicken Sie auf Weiter.



4. Geben Sie den Speicherort des Backup-Katalogs an, und klicken Sie auf Weiter.



5. Eine Liste der verfügbaren Backups wird basierend auf dem Inhalt des Backup-Katalogs angezeigt. Wählen Sie das gewünschte Backup und notieren Sie sich die externe Backup ID: In unserem Beispiel das aktuellste Backup.



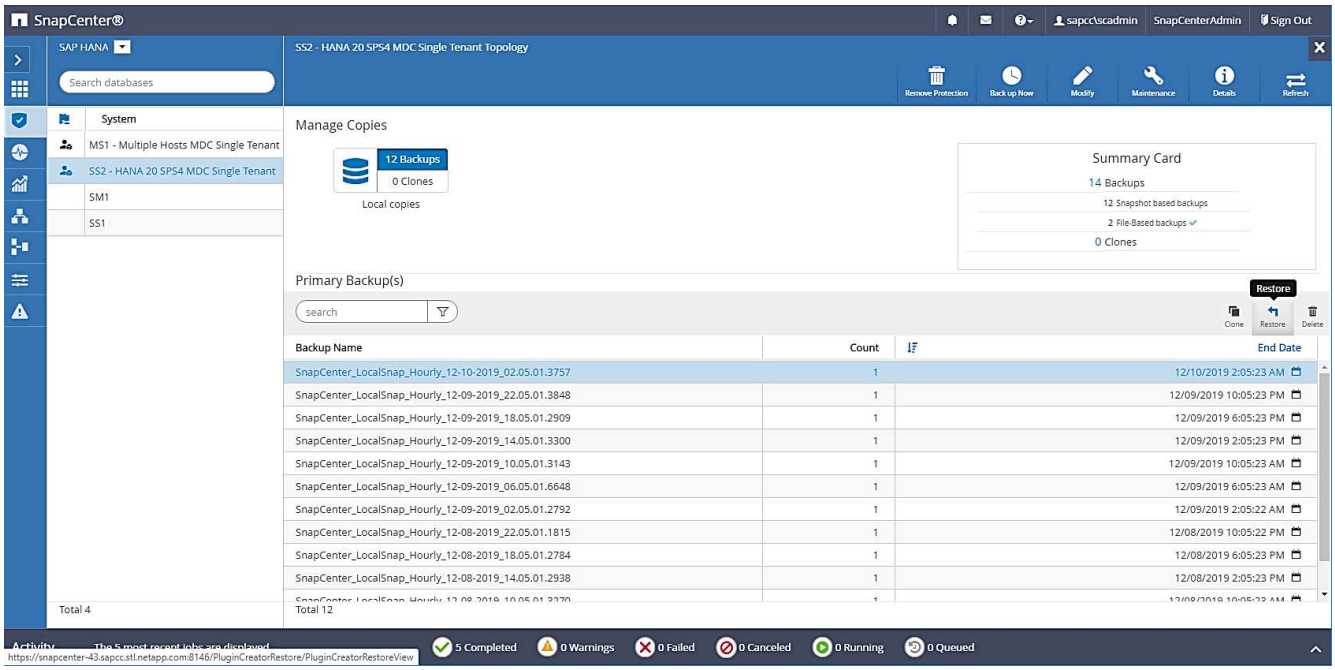
6. Heben Sie die Bereitstellung aller Daten-Volumes auf.

```
umount /hana/data/SS2/mnt00001
```

Bei einem SAP HANA mehrere Host-System mit NFS müssen alle Daten-Volumes auf jedem Host abgehängt werden.

Bei einer SAP HANA-Konfiguration mit mehreren Hosts mit FC wird der Unmount-Vorgang im Rahmen des Herunterfahrens vom SAP HANA-Namensserver ausgeführt.

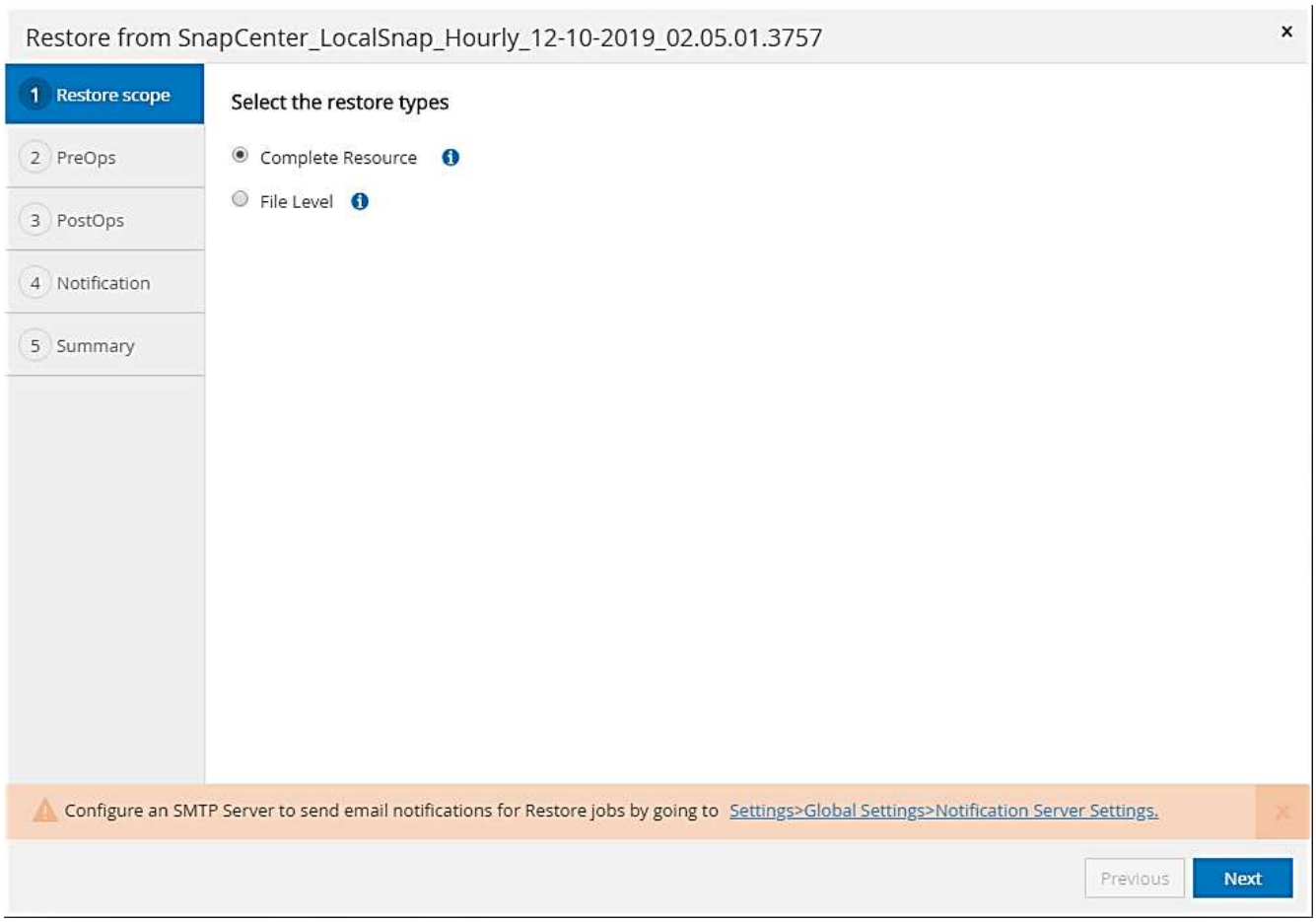
7. Wählen Sie in der SnapCenter GUI die Ansicht der Ressourcen-Topologie aus und wählen Sie das Backup aus, das wiederhergestellt werden soll, beispielsweise das aktuellste primäre Backup. Klicken Sie auf das Symbol Wiederherstellen, um die Wiederherstellung zu starten.



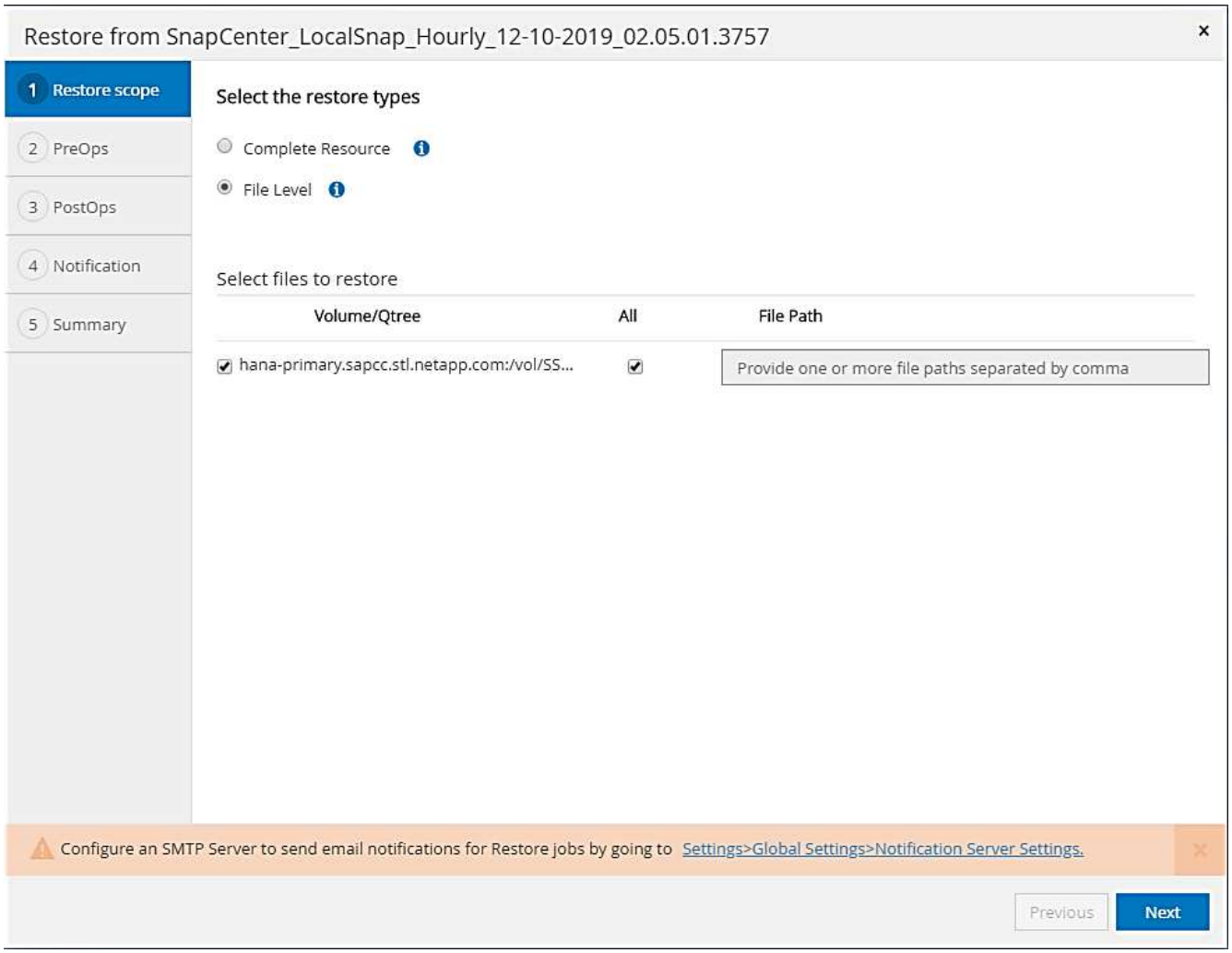
Der SnapCenter-Wiederherstellungsassistent wird gestartet.

8. Wählen Sie den Wiederherstellungstyp Complete Resource or File Level aus.

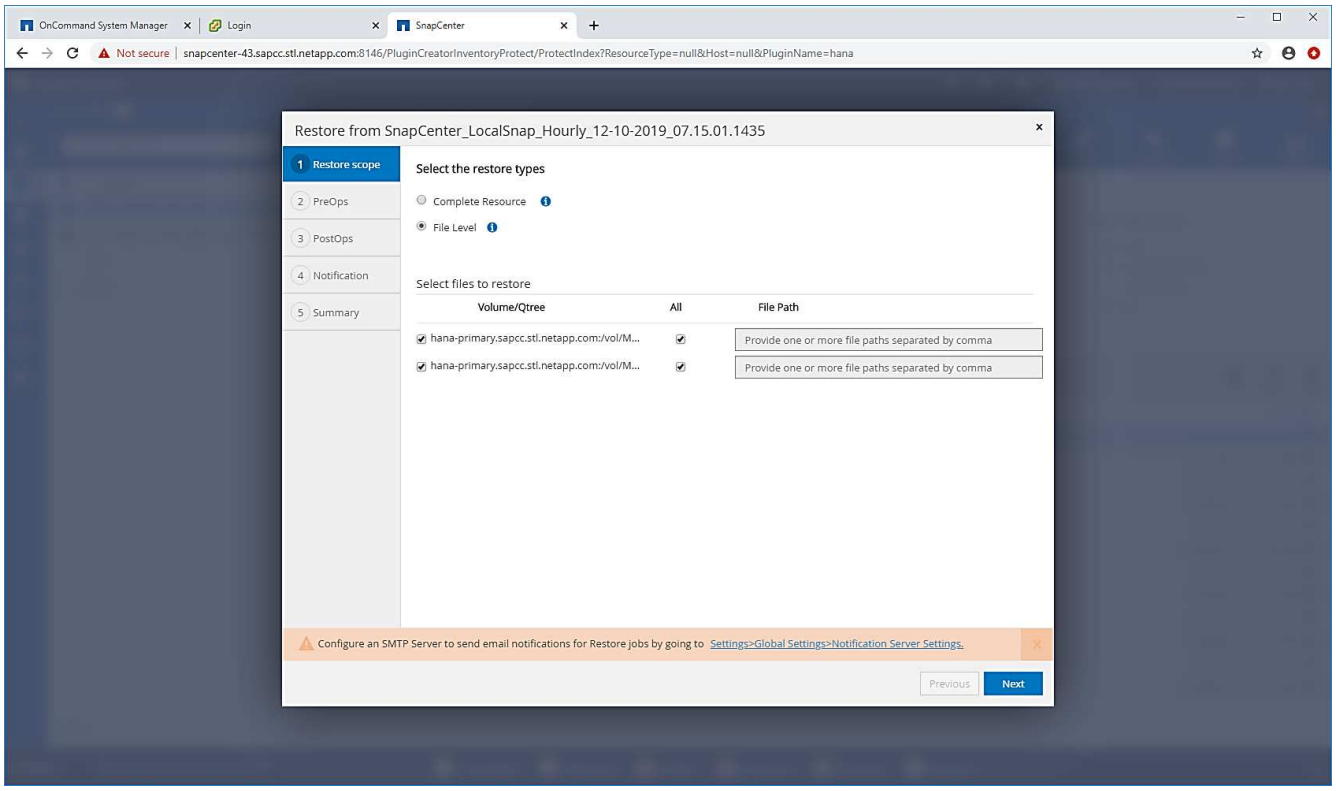
   Wählen Sie „Complete Resource“ aus, um eine Volume-basierte Wiederherstellung zu verwenden.



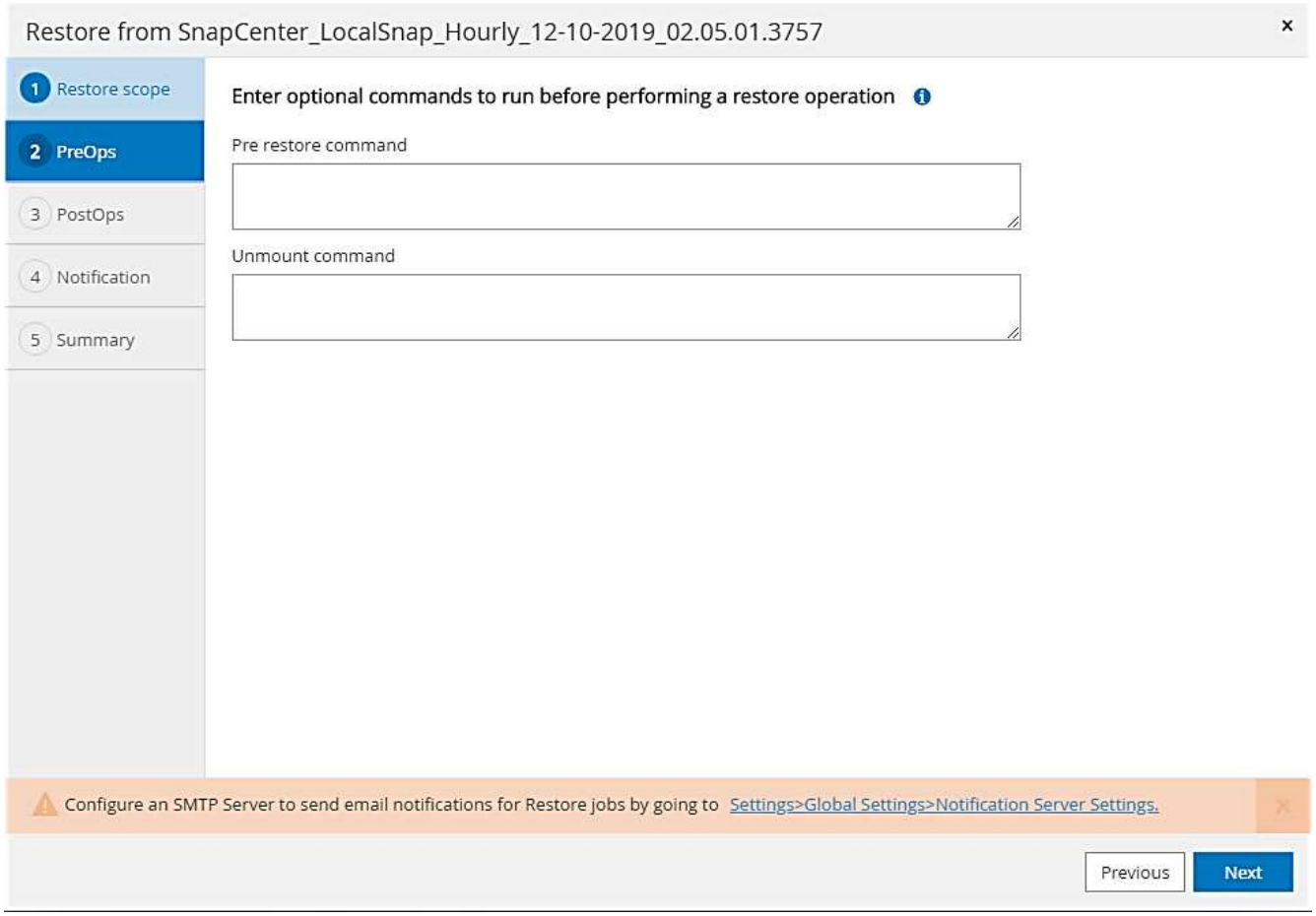
9. Wählen Sie Dateiebene und Alle, um einen SnapRestore-Vorgang mit einer einzigen Datei für alle Dateien zu verwenden.



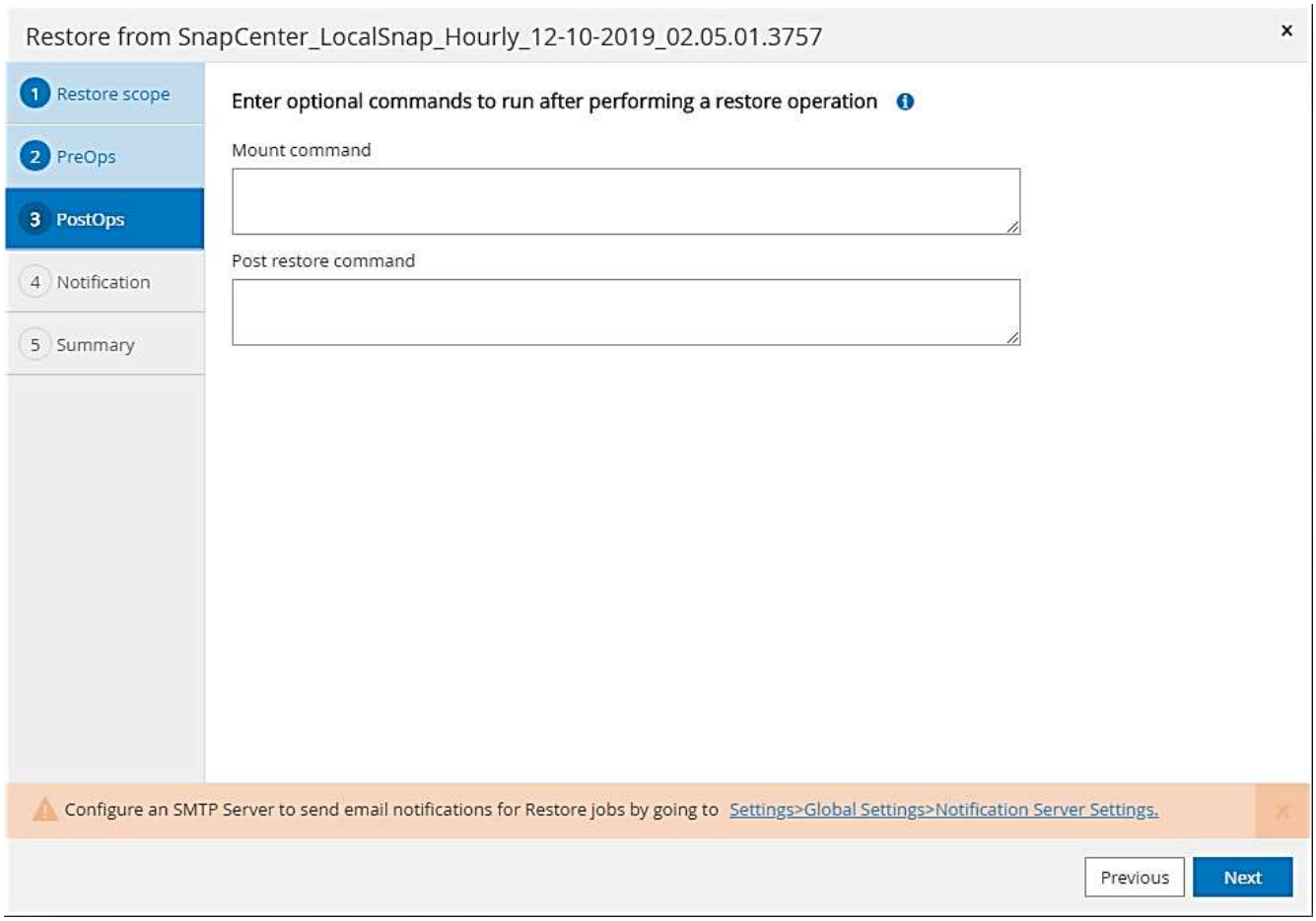
Wählen Sie für eine Wiederherstellung auf Dateiebene eines SAP HANA-Host-Systems mit mehreren Hosts alle Volumes aus.



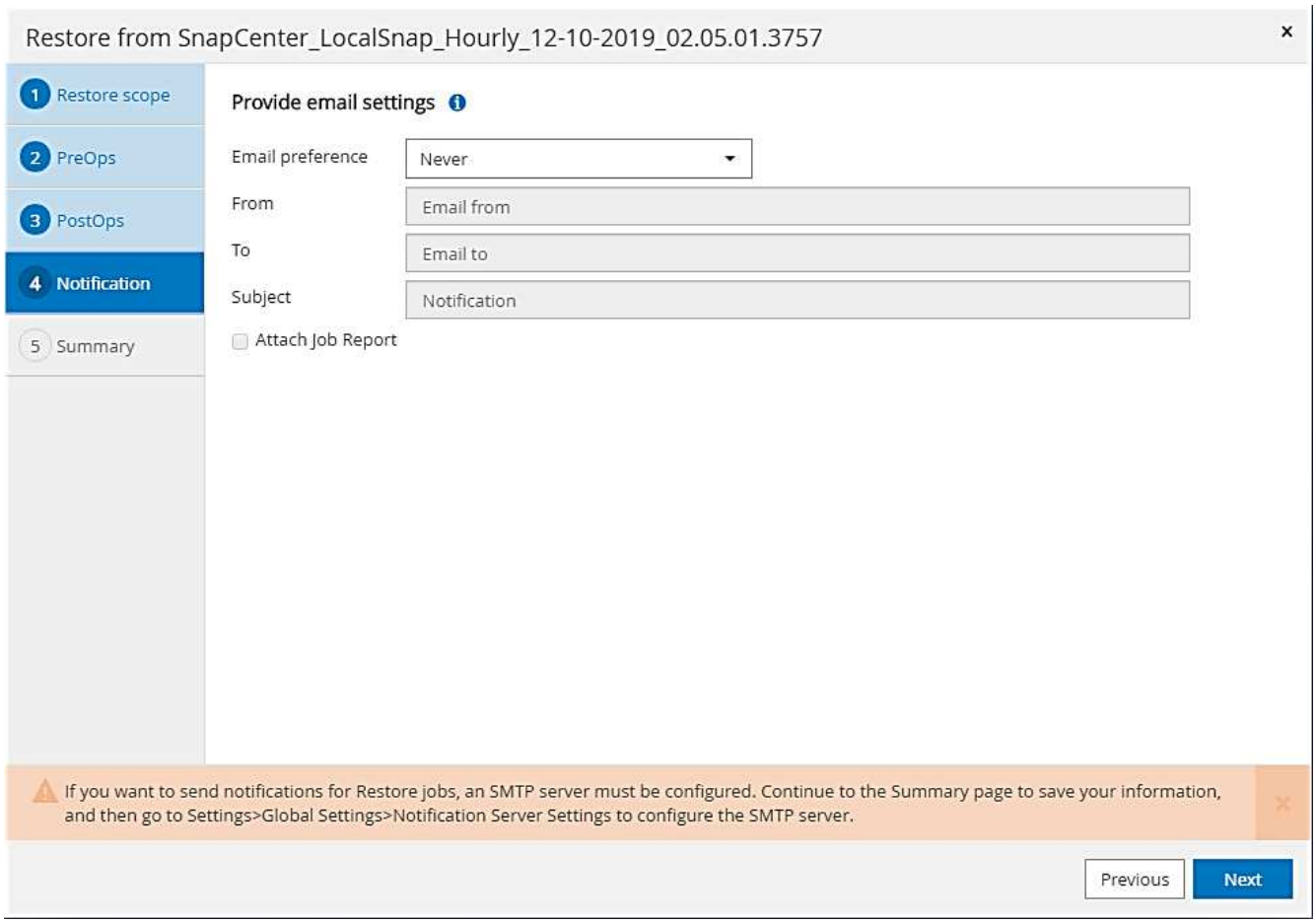
10. (Optional) Geben Sie die Befehle an, die aus dem SAP HANA-Plug-in ausgeführt werden sollen, das auf dem zentralen HANA-Plug-in-Host ausgeführt wird. Klicken Sie Auf Weiter.



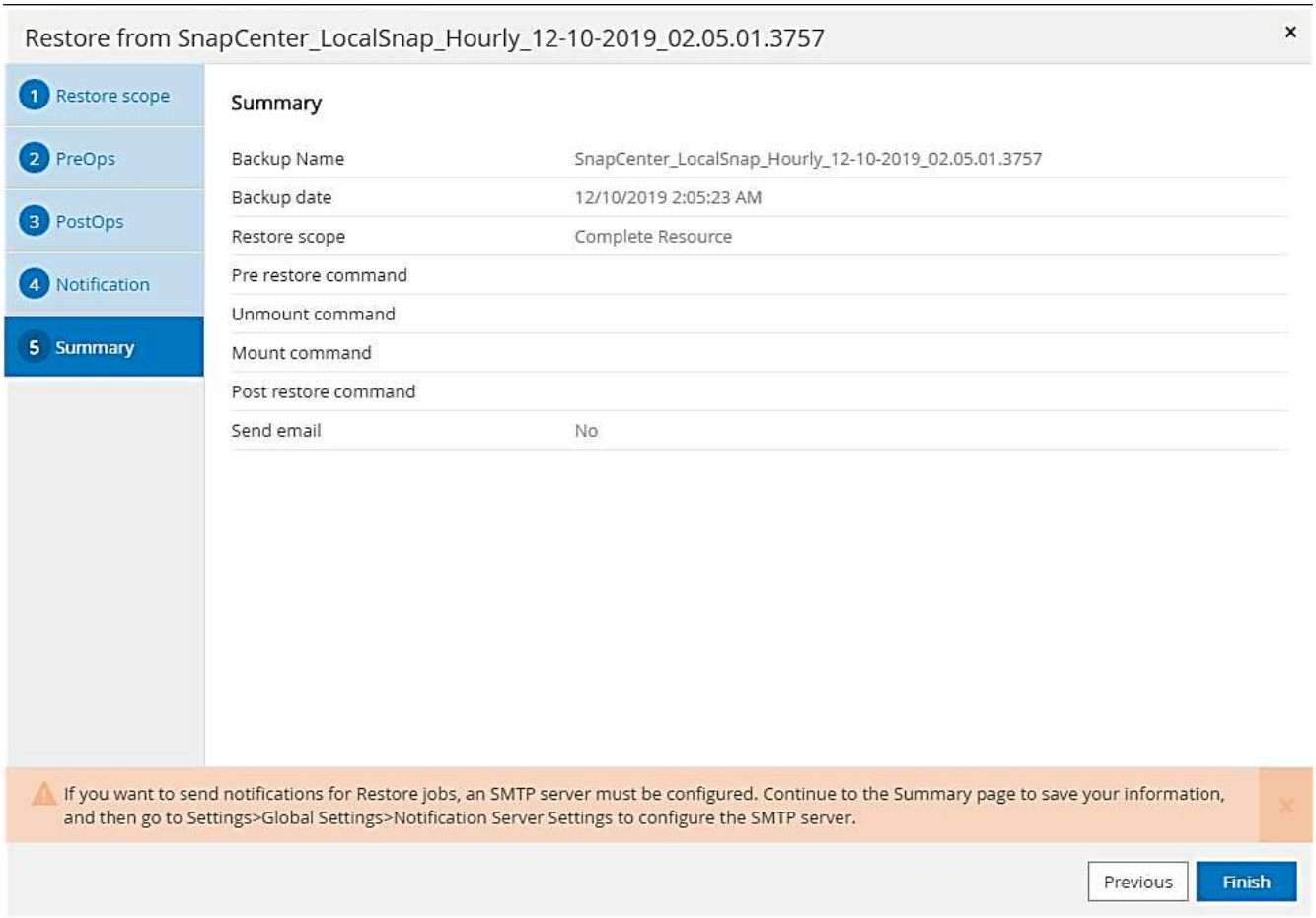
11. Geben Sie die optionalen Befehle an, und klicken Sie auf Weiter.



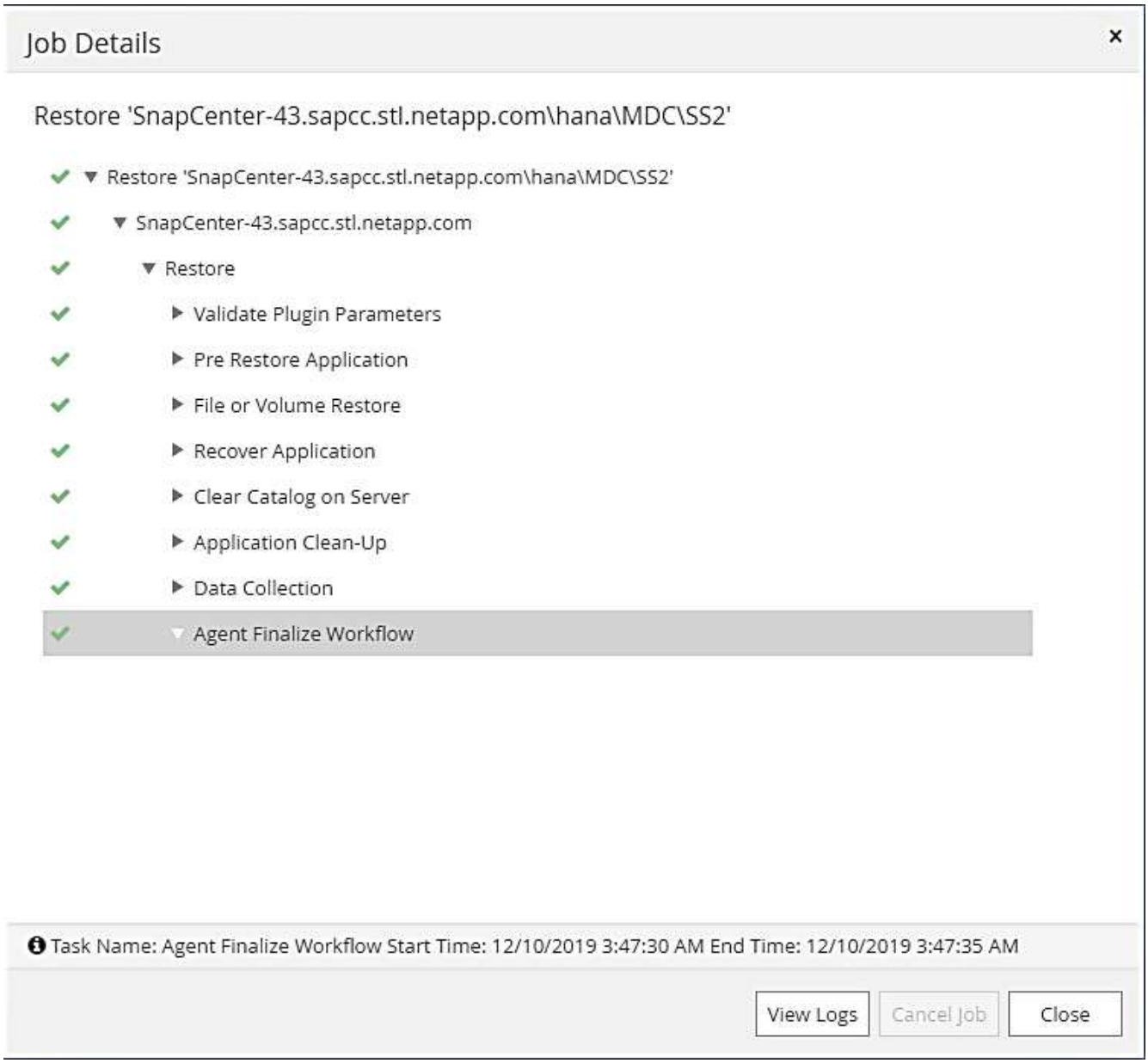
12. Geben Sie die Benachrichtigungseinstellungen an, damit SnapCenter eine Status-E-Mail und ein Jobprotokoll senden kann. Klicken Sie Auf Weiter.



13. Überprüfen Sie die Zusammenfassung und klicken Sie auf Fertig stellen, um die Wiederherstellung zu starten.



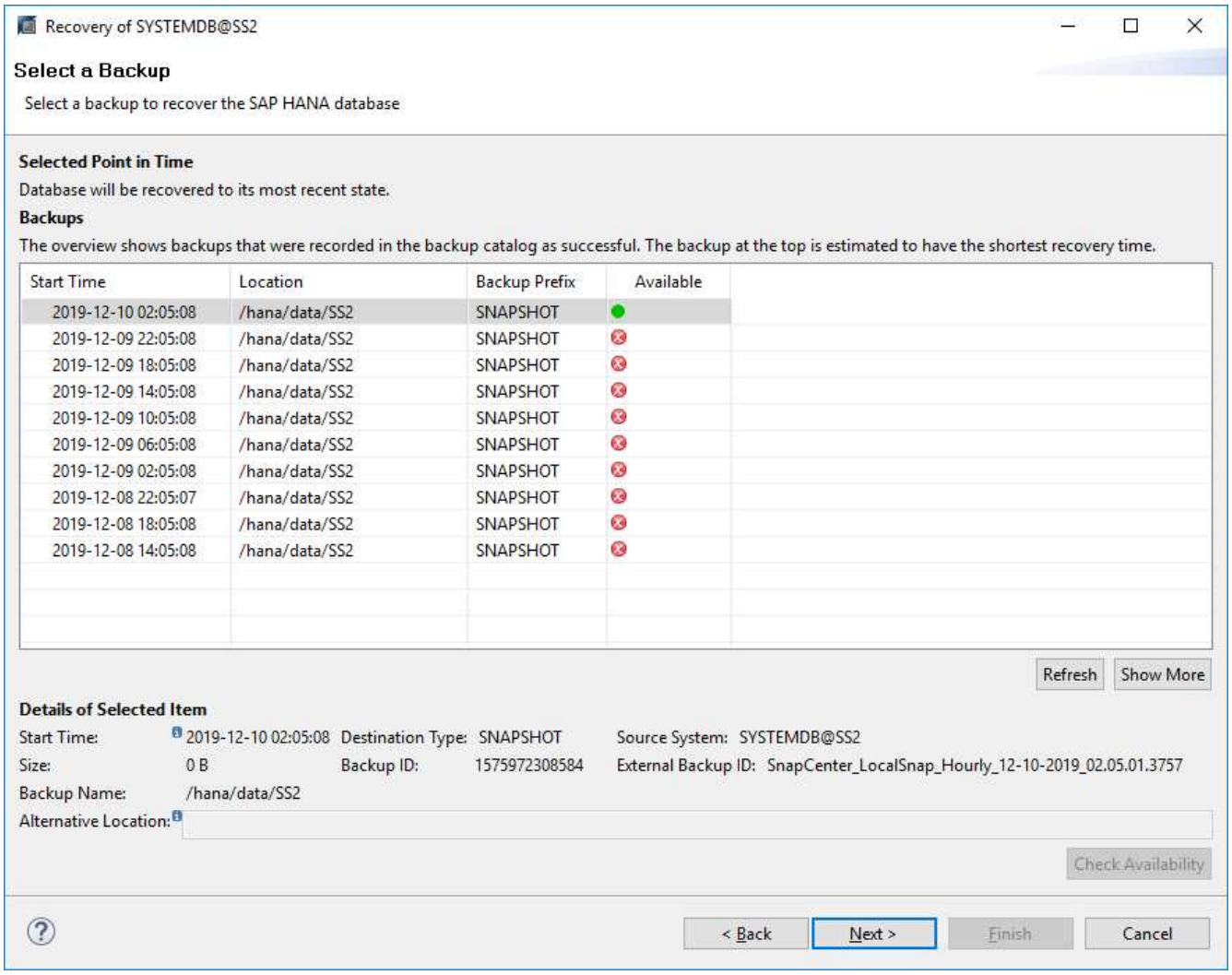
14. Der Wiederherstellungsauftrag wird gestartet, und das Jobprotokoll kann durch Doppelklicken auf die Protokollzeile im Aktivitätsfenster angezeigt werden.



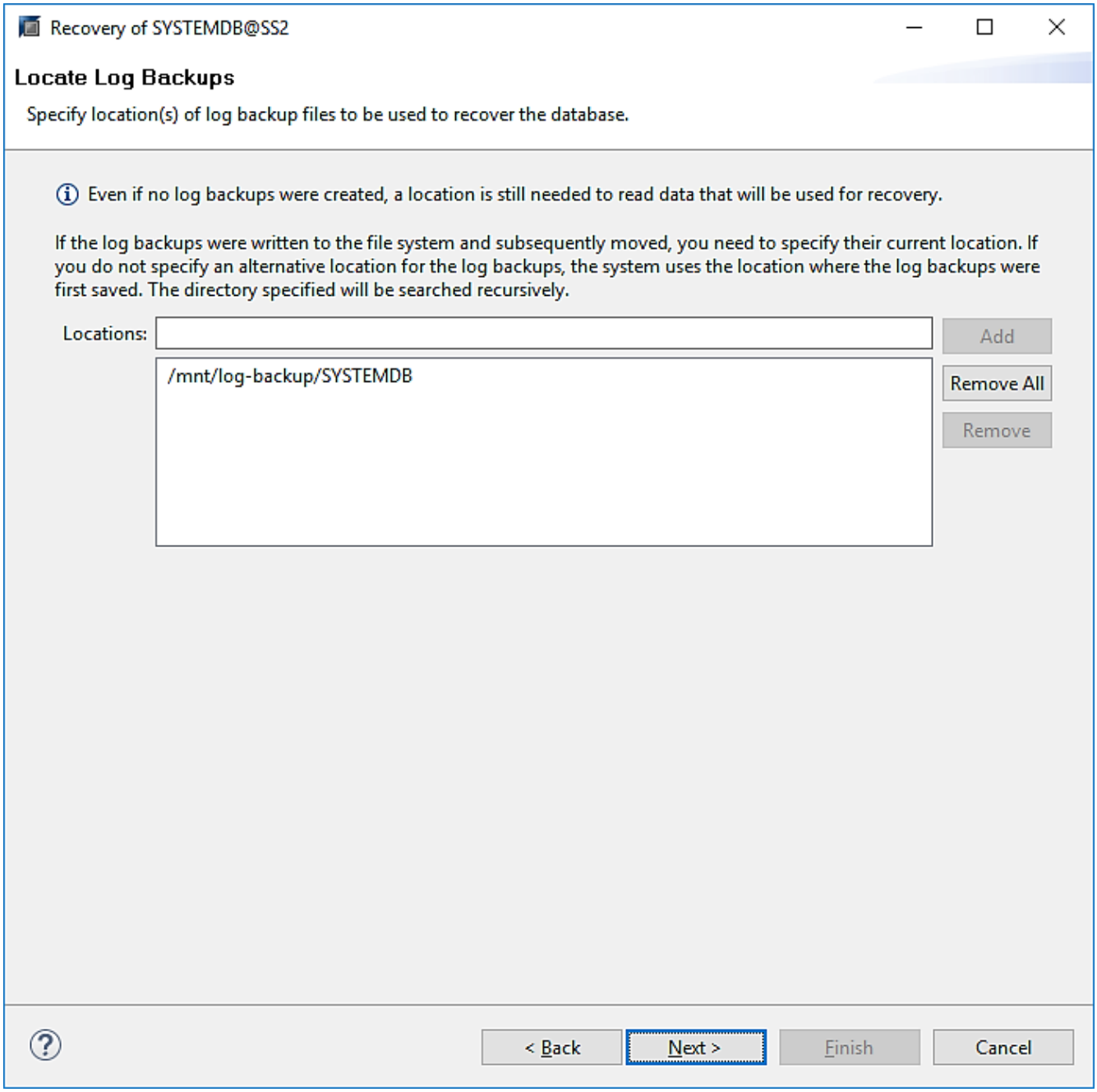
15. Warten Sie, bis der Wiederherstellungsvorgang abgeschlossen ist. Mounten Sie auf jedem Datenbank-Host alle Daten-Volumes. In unserem Beispiel muss nur ein Volume auf dem Datenbank-Host neu eingebunden werden.

```
mount /hana/data/SP1/mnt00001
```

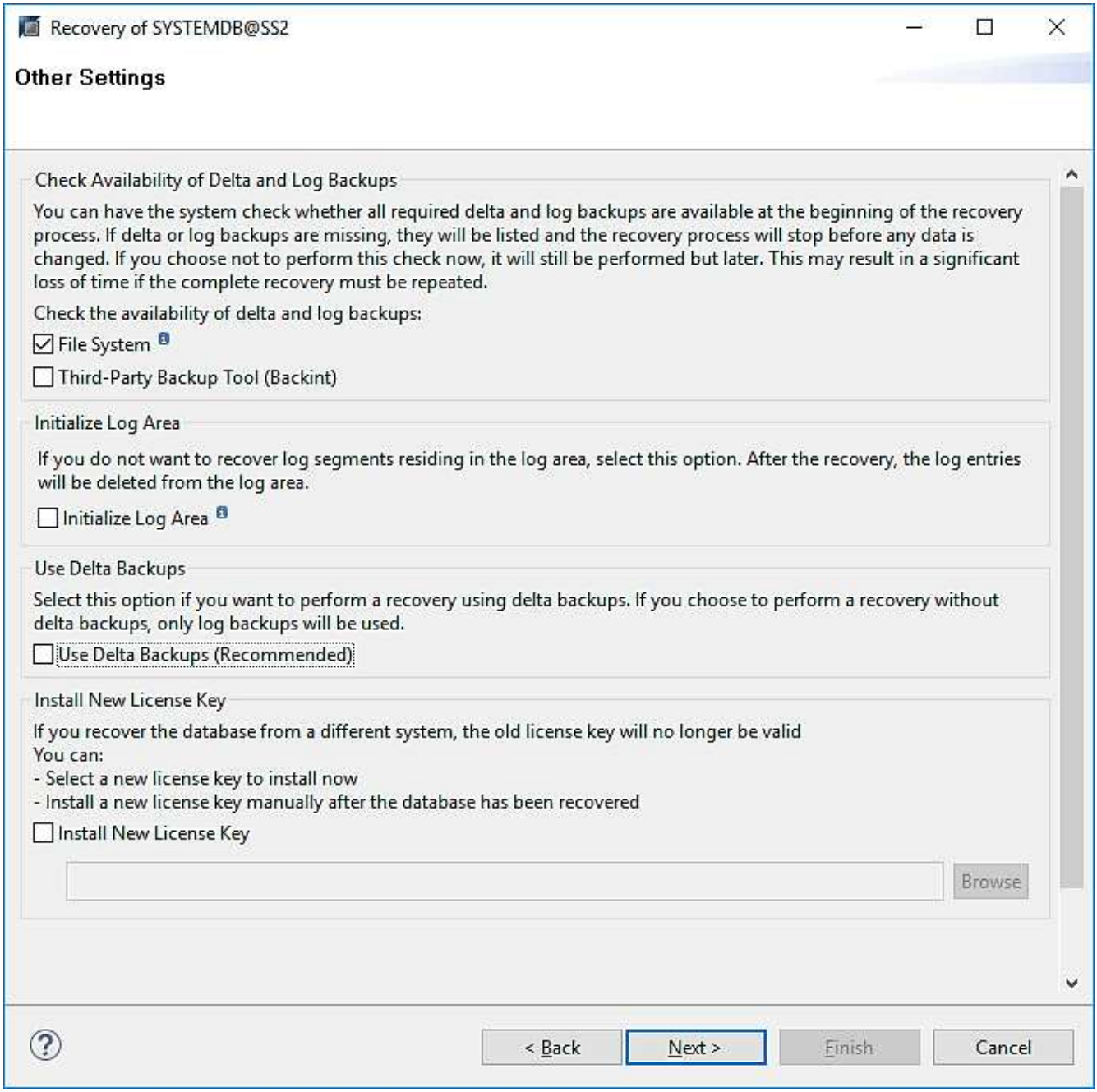
16. Gehen Sie zu SAP HANA Studio und klicken Sie auf Aktualisieren, um die Liste der verfügbaren Backups zu aktualisieren. Das mit SnapCenter wiederhergestellte Backup wird durch ein grünes Symbol in der Liste der Backups angezeigt. Wählen Sie das Backup aus, und klicken Sie auf Weiter.



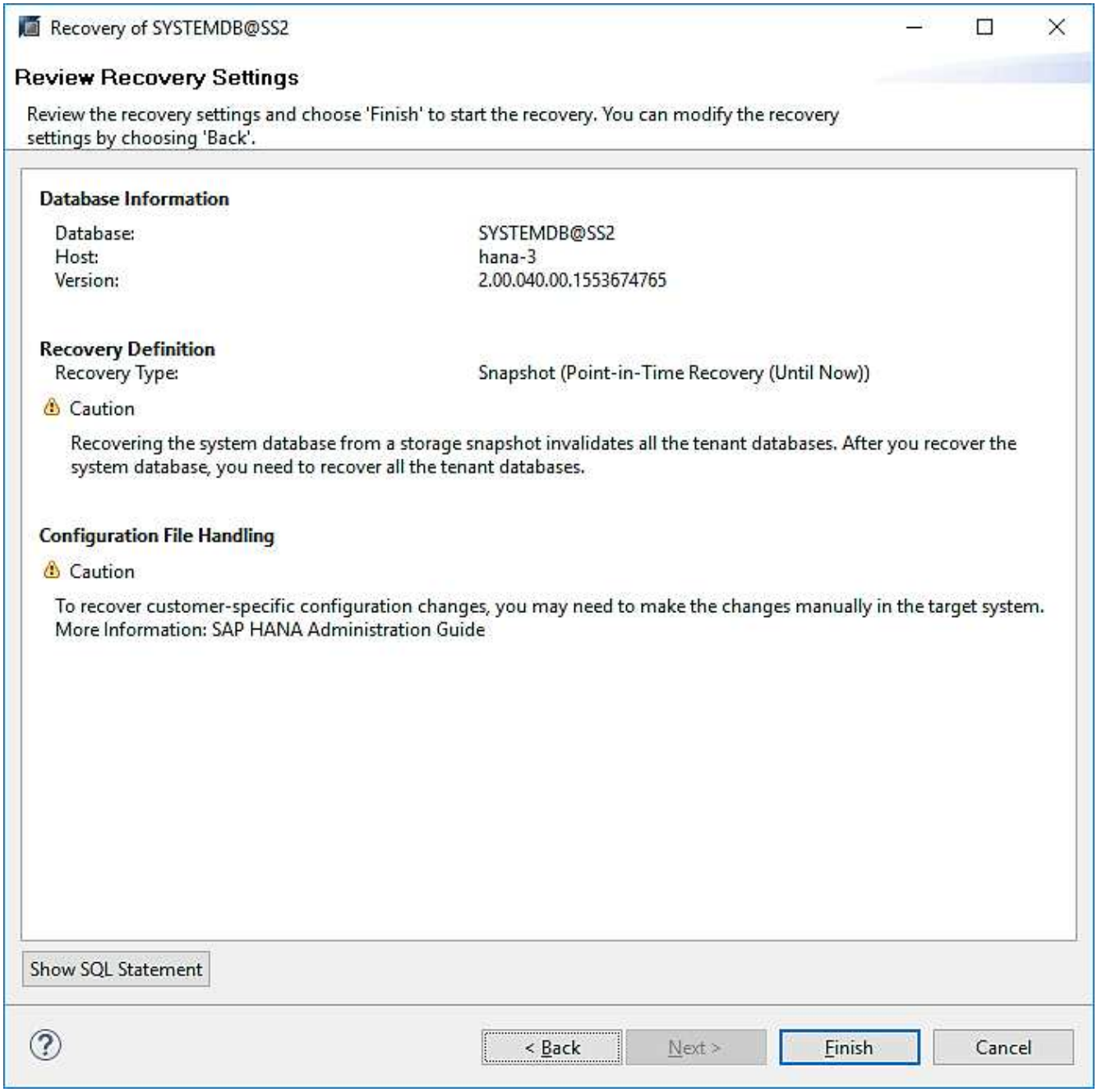
17. Stellen Sie den Speicherort der Protokoll-Backups bereit. Klicken Sie Auf Weiter.



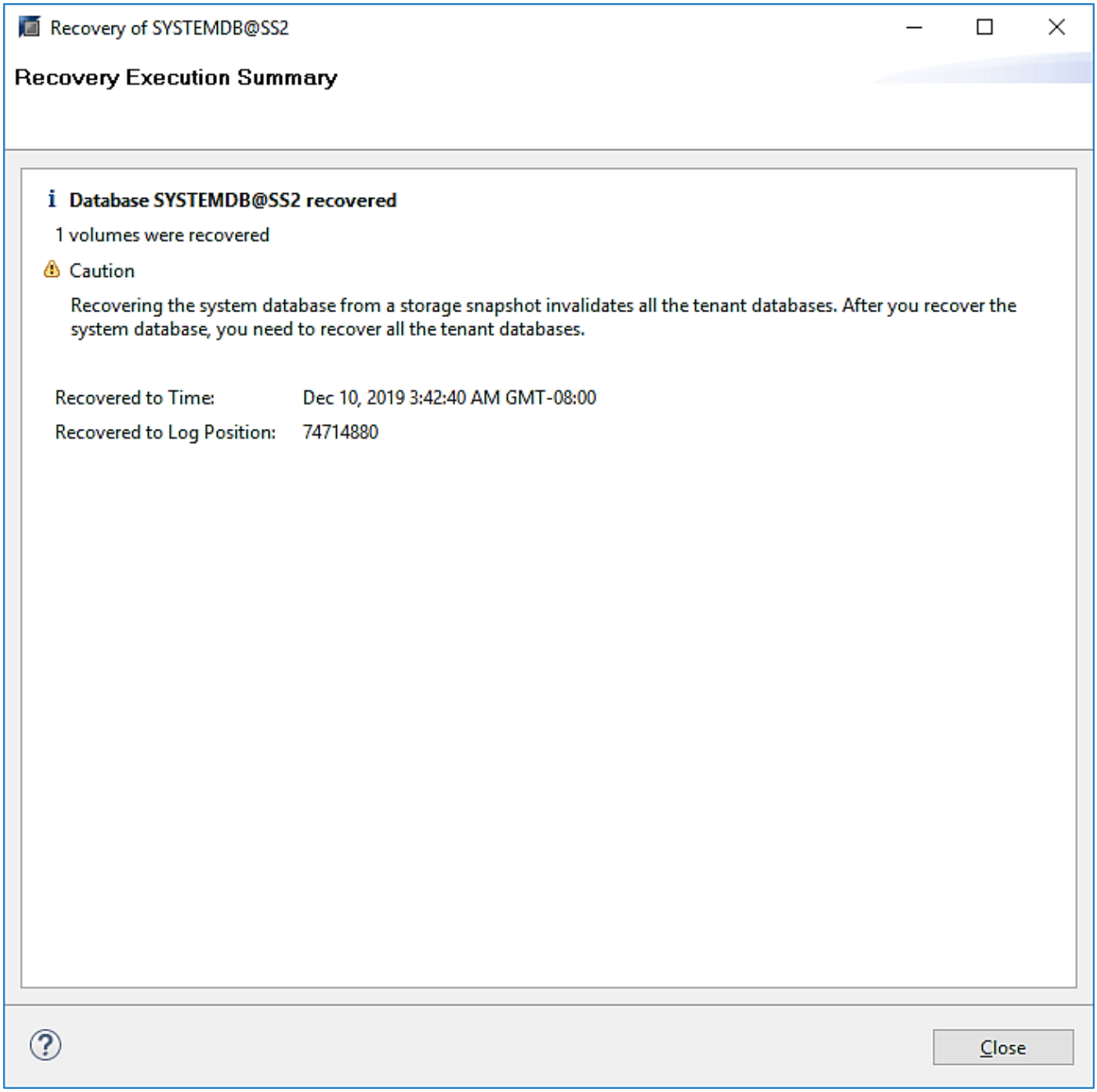
18. Wählen Sie je nach Bedarf andere Einstellungen aus. Stellen Sie sicher, dass Delta-Backups verwenden nicht ausgewählt ist. Klicken Sie Auf Weiter.



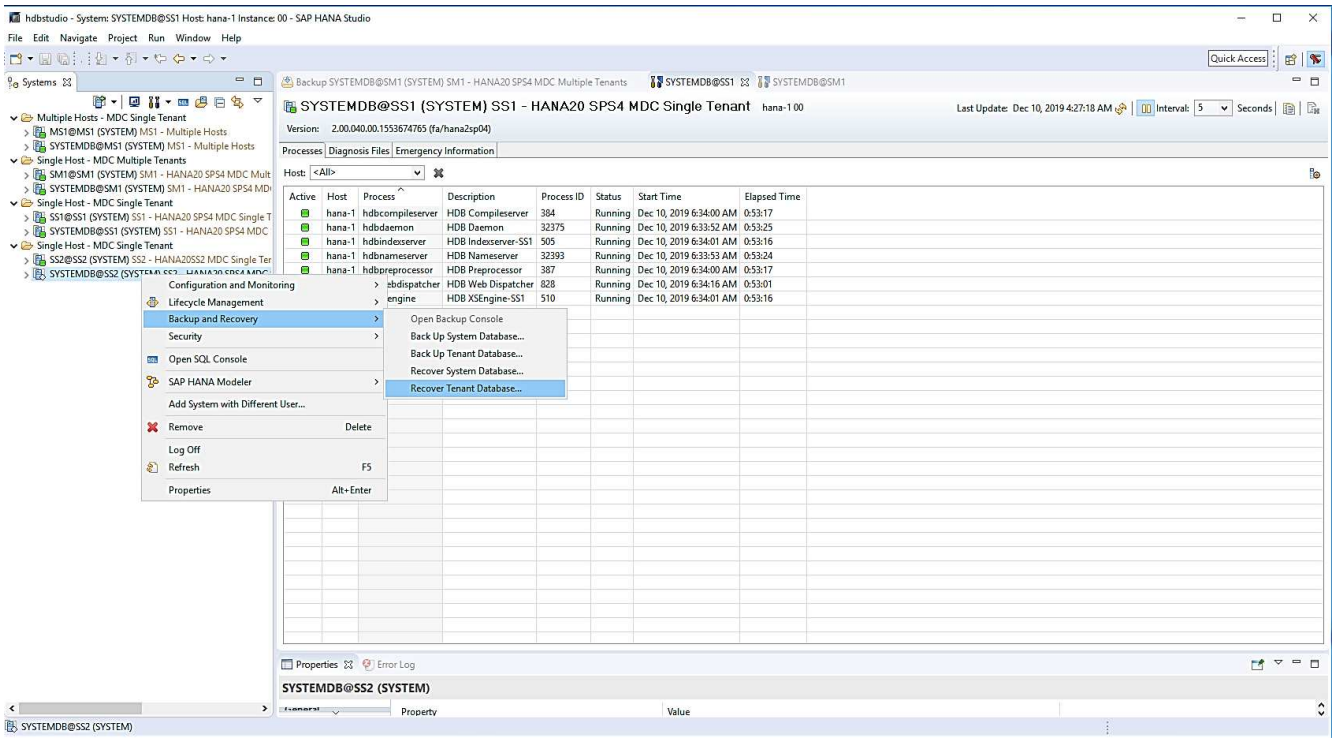
19. Überprüfen Sie die Wiederherstellungseinstellungen, und klicken Sie auf Fertig stellen.



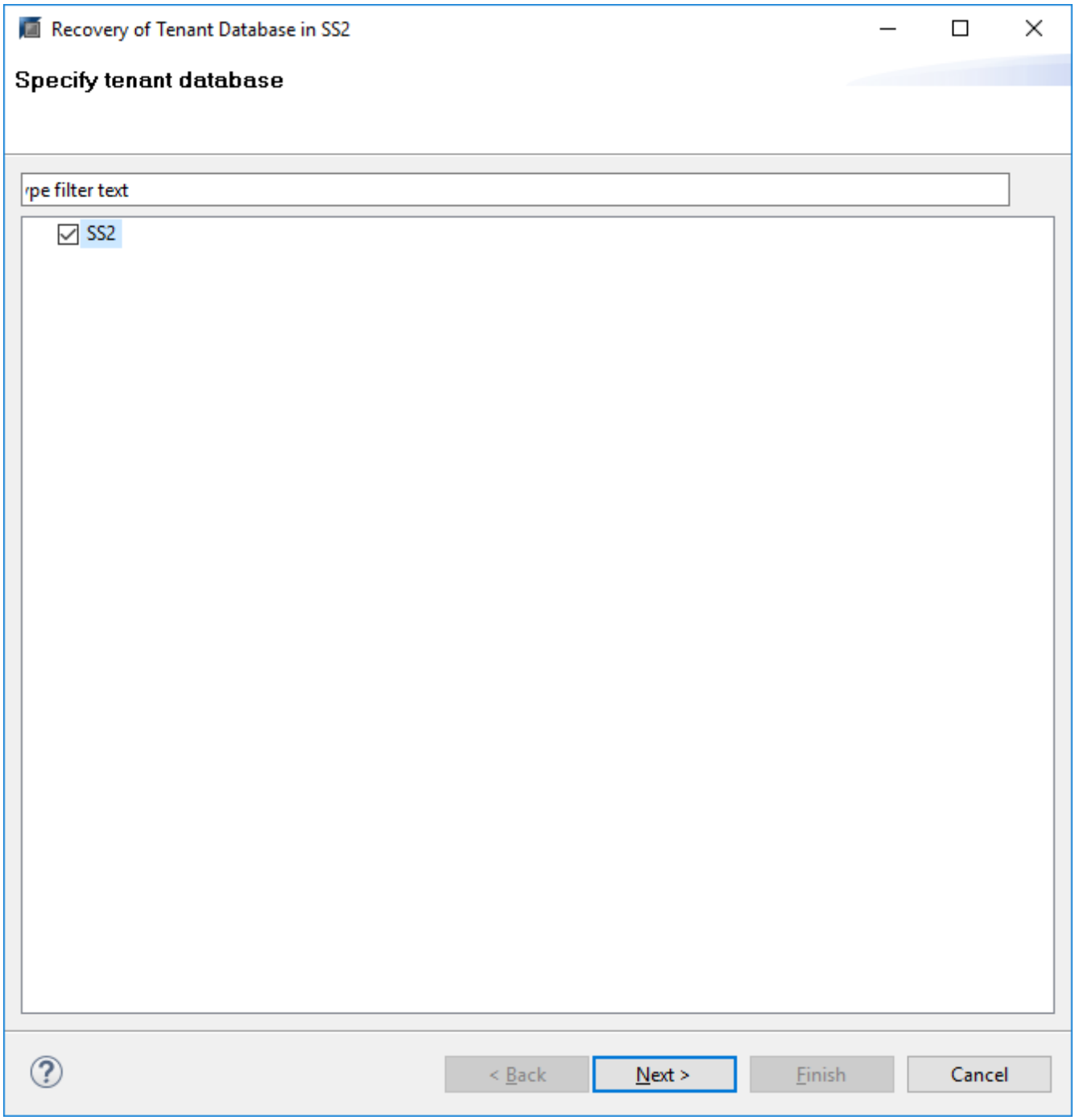
20. Der Wiederherstellungsprozess wird gestartet. Warten Sie, bis die Wiederherstellung der Systemdatenbank abgeschlossen ist.



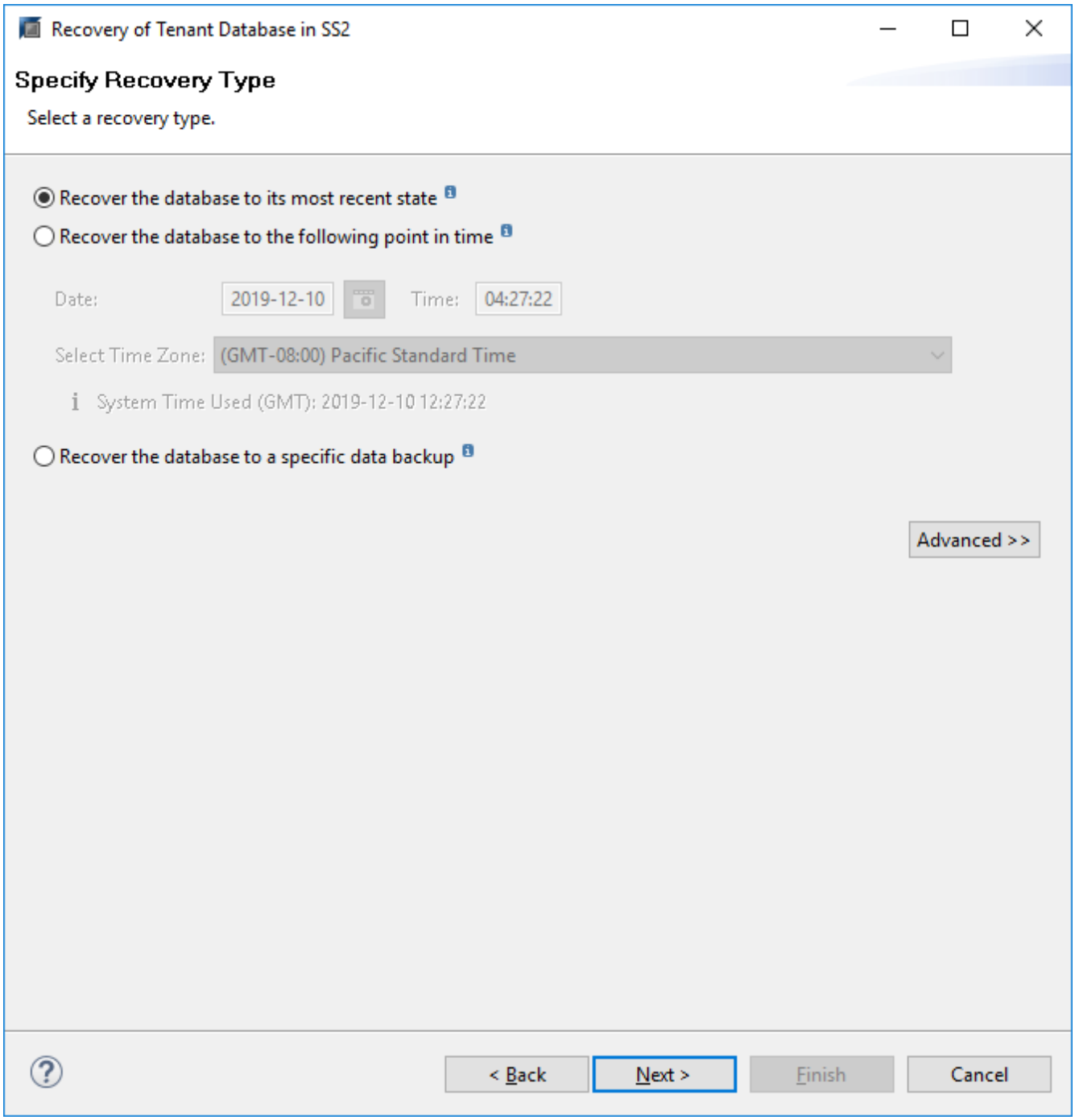
21. Wählen Sie in SAP HANA Studio den Eintrag für die Systemdatenbank aus, und starten Sie Backup Recovery - Rcover Tenant Database.



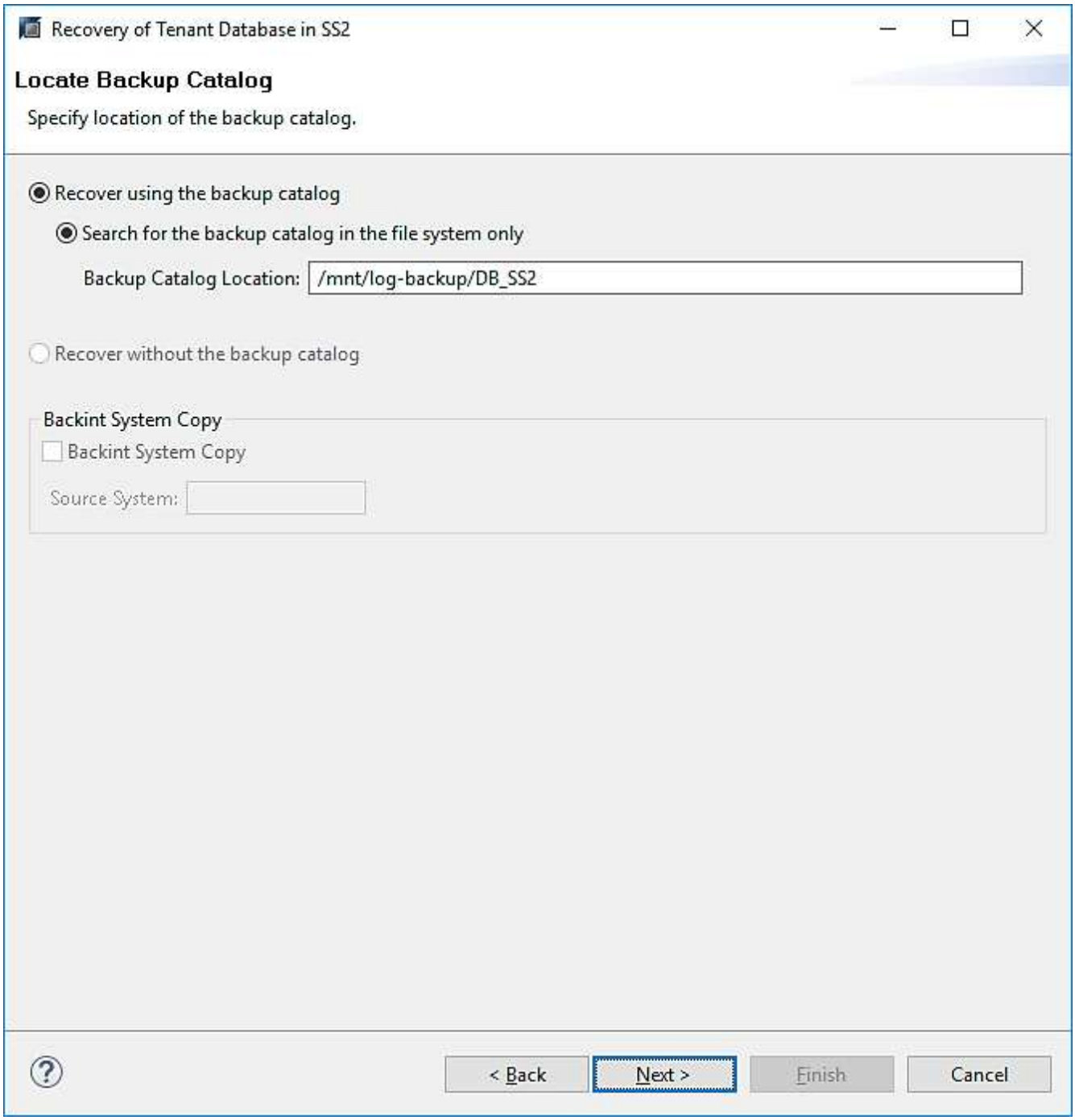
22. Wählen Sie den zu wiederherzuenden Mieter aus, und klicken Sie auf Weiter.



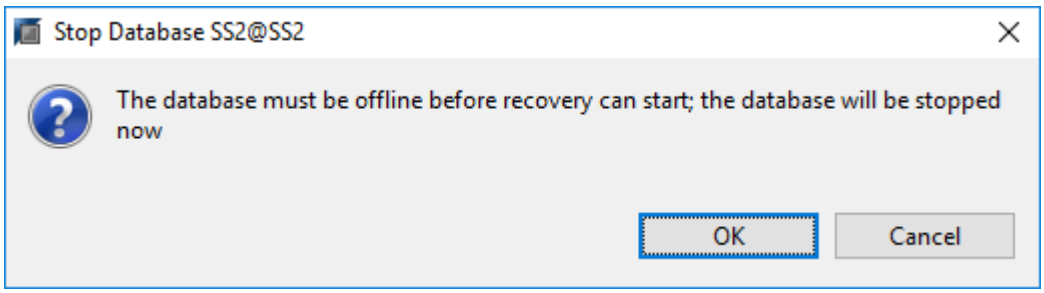
23. Geben Sie den Wiederherstellungstyp an, und klicken Sie auf Weiter.



24. Bestätigen Sie den Speicherort des Backup-Katalogs, und klicken Sie auf Weiter.

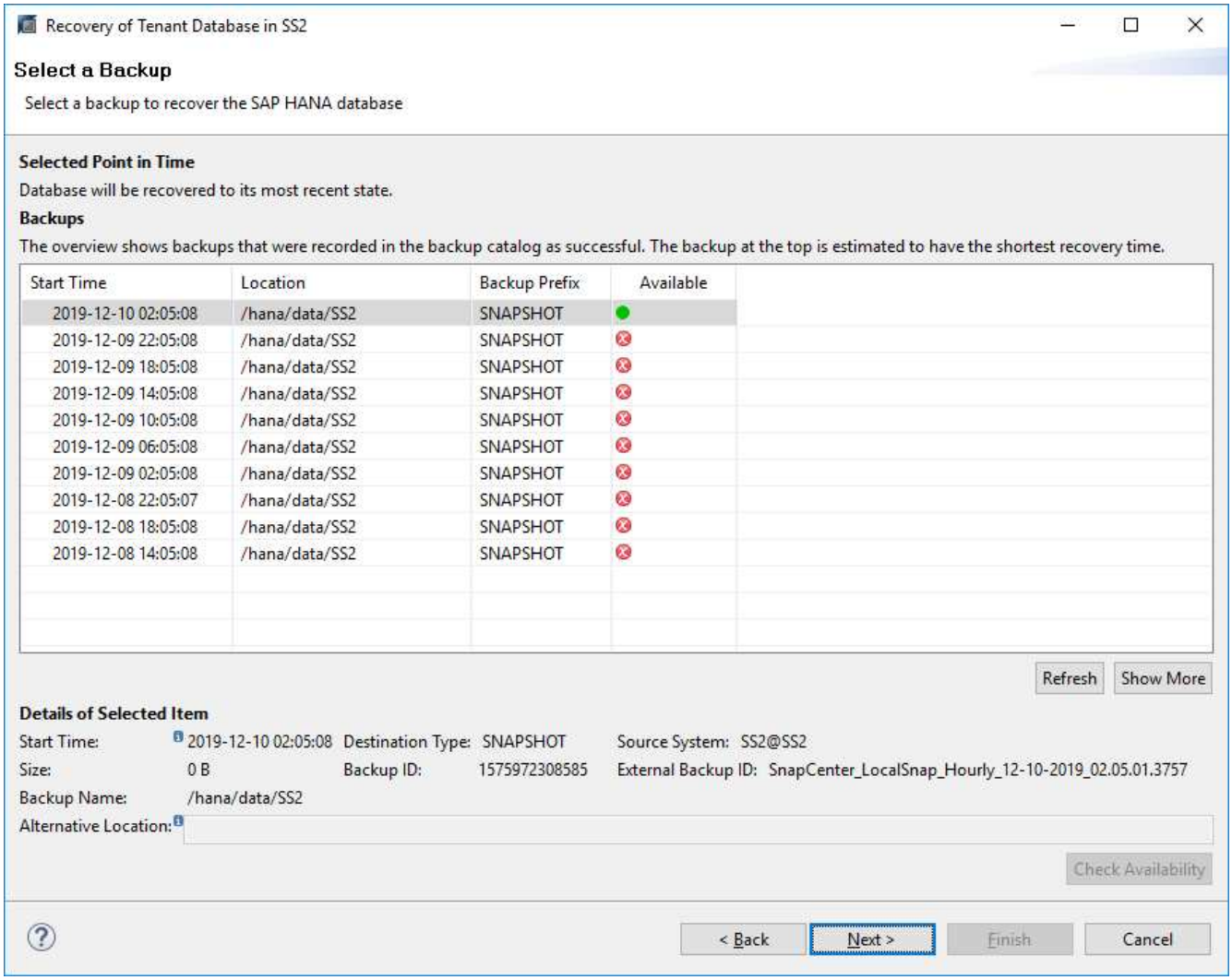


25. Vergewissern Sie sich, dass die Mandantendatenbank offline ist. Klicken Sie auf OK, um fortzufahren.

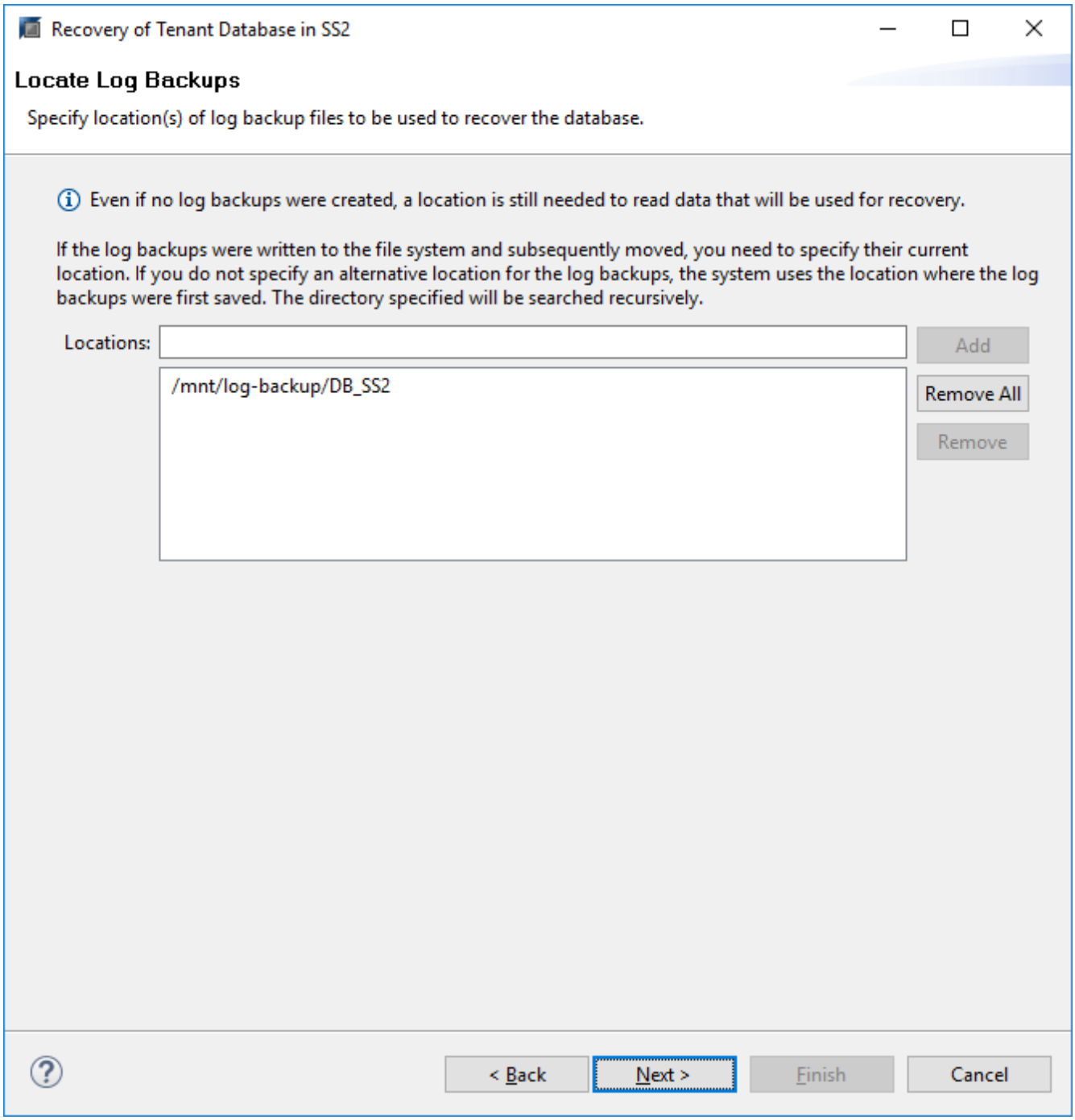


26. Da die Wiederherstellung des Daten-Volumes vor der Wiederherstellung der Systemdatenbank erfolgt ist, ist das Mandanten-Backup sofort verfügbar. Wählen Sie das grün markierte Backup aus, und klicken Sie

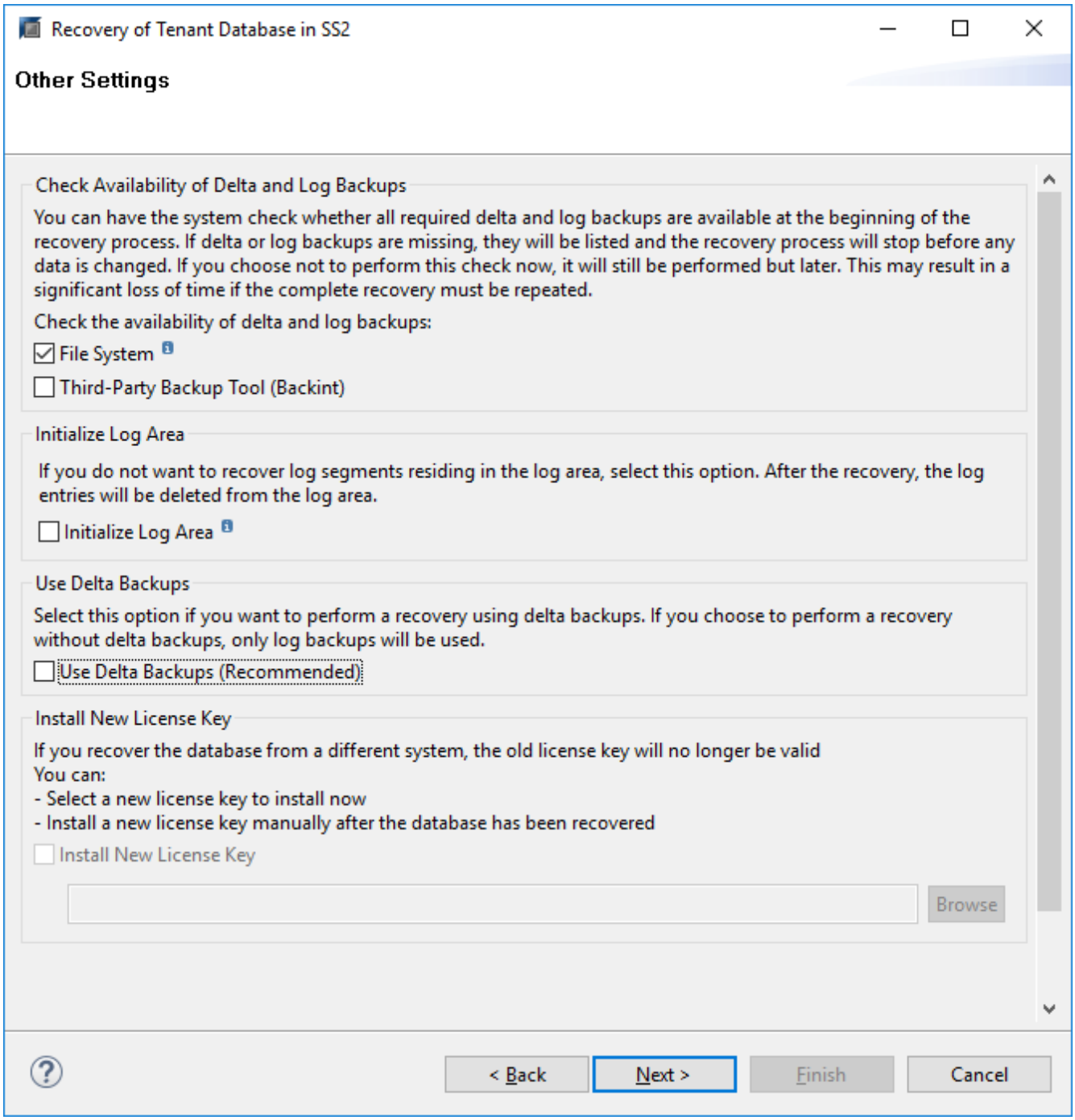
auf Weiter.



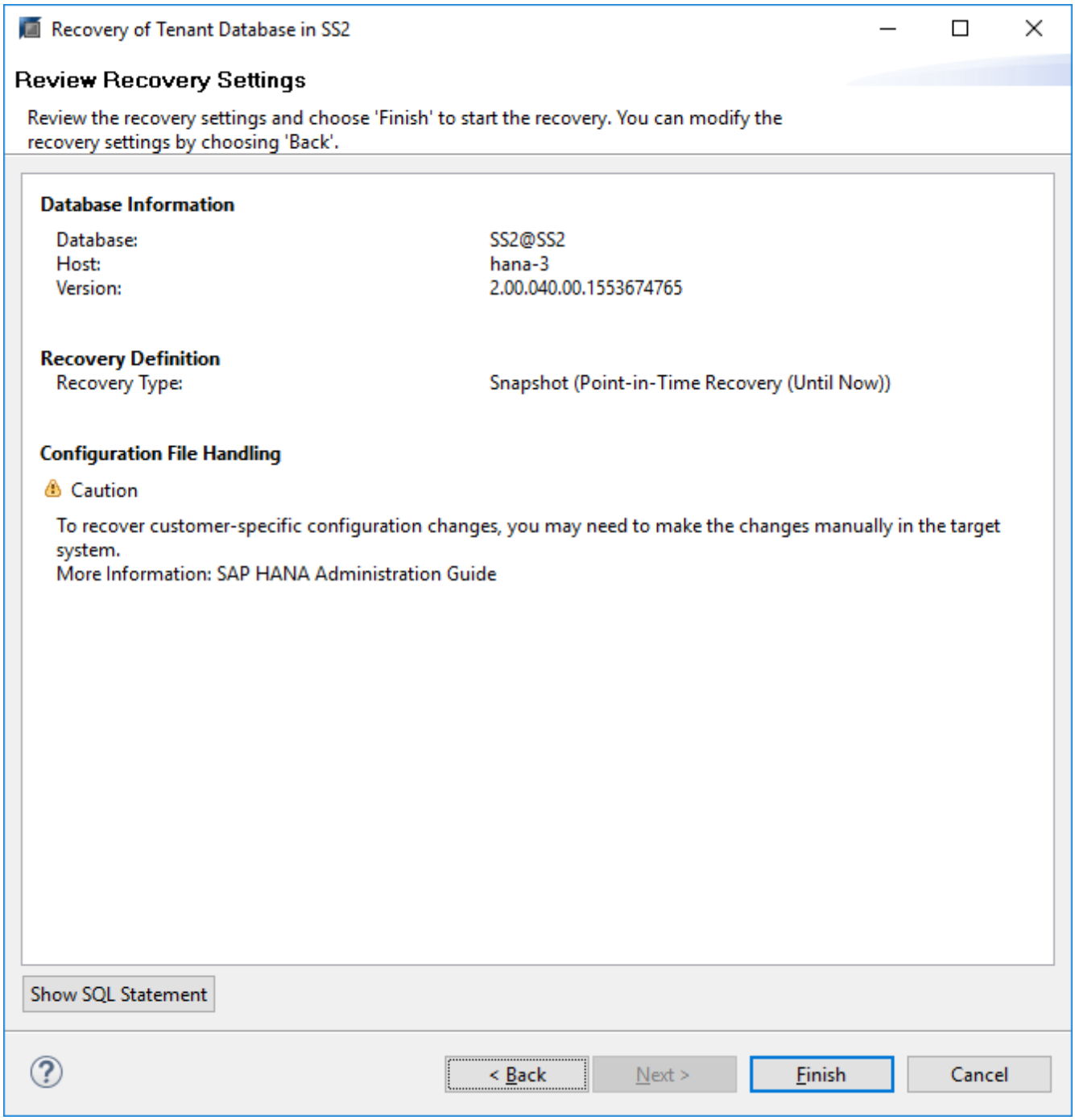
27. Bestätigen Sie den Speicherort für die Protokollsicherung und klicken Sie auf Weiter.



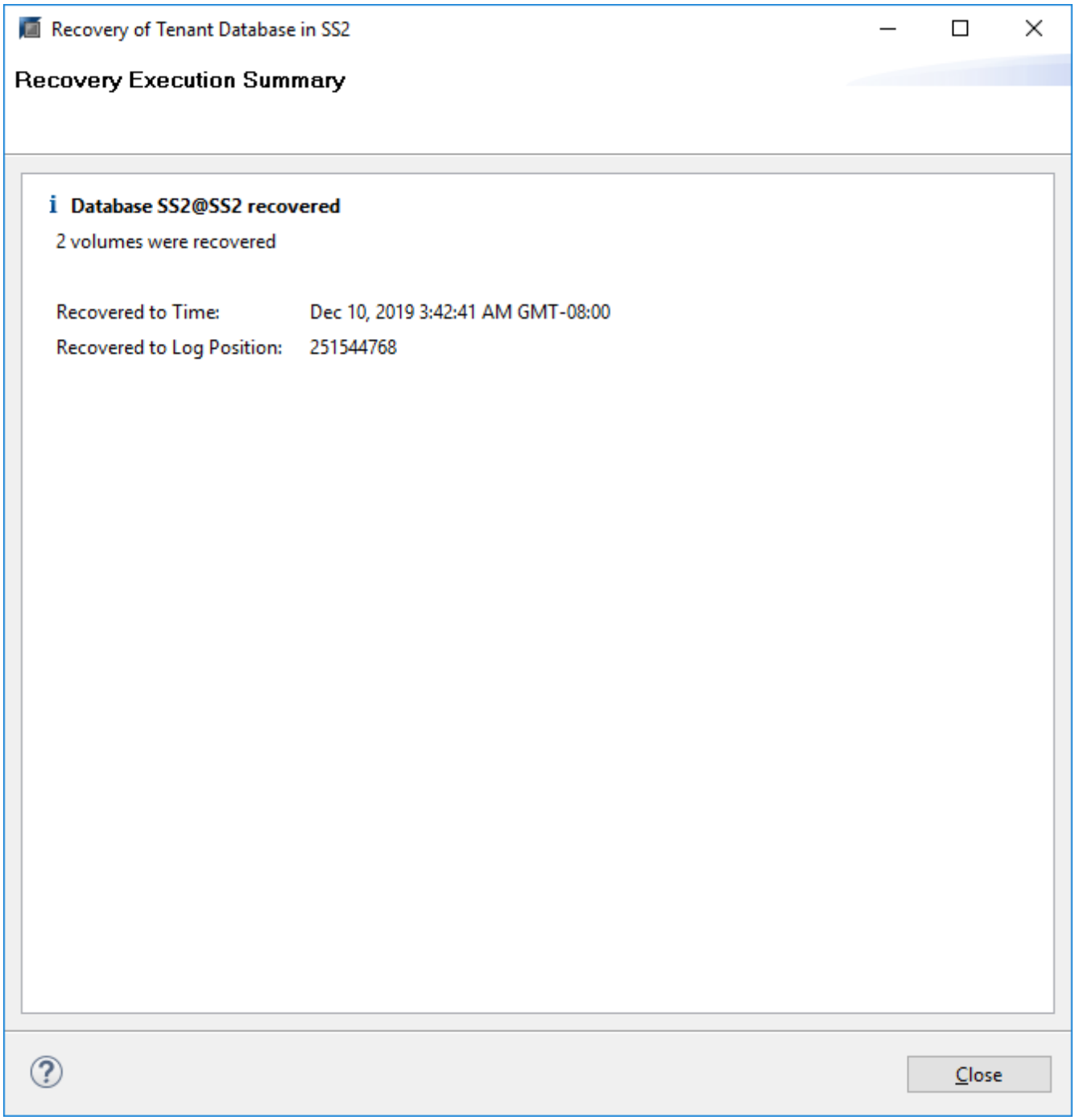
28. Wählen Sie je nach Bedarf andere Einstellungen aus. Stellen Sie sicher, dass Delta-Backups verwenden nicht ausgewählt ist. Klicken Sie Auf Weiter.



29. Überprüfen Sie die Wiederherstellungseinstellungen und starten Sie den Wiederherstellungsprozess der Mandantendatenbank, indem Sie auf Fertig stellen klicken.



30. Warten Sie, bis die Wiederherstellung abgeschlossen ist und die Mandantendatenbank gestartet wird.



Das SAP HANA System ist betriebsbereit.

Bei einem SAP HANA MDC-System mit mehreren Mandanten müssen Sie die Schritte 20 bis 29 für jeden Mandanten wiederholen.

Erweiterte Konfiguration und Optimierung

In diesem Abschnitt werden Konfigurations- und Tuning-Optionen beschrieben, mit denen Kunden das SnapCenter Setup an ihre spezifischen Anforderungen anpassen können. Möglicherweise gelten nicht alle Einstellungen für alle Kundenszenarien.

Sichere Kommunikation mit HANA-Datenbank ermöglichen

Sind die HANA-Datenbanken mit sicherer Kommunikation konfiguriert `hdbsql` Der von SnapCenter ausgeführte Befehl muss zusätzliche Befehlszeilenoptionen verwenden. Dies kann mit einem Wrapper-Skript erreicht werden, das aufruft `hdbsql` Mit den erforderlichen Optionen.

> Es gibt verschiedene Optionen zur Konfiguration der SSL-Kommunikation. In den folgenden Beispielen wird die einfachste Client-Konfiguration mit der Befehlszeilenoption beschrieben, bei der keine Server-Zertifikatvalidierung durchgeführt wird. Wenn eine Zertifikatvalidierung auf Server- und/oder Client-Seite erforderlich ist, sind unterschiedliche hdbsql-Befehlszeilenoptionen erforderlich, und Sie müssen die PSE-Umgebung entsprechend konfigurieren, wie im SAP HANA Security Guide beschrieben.

Anstatt die zu konfigurieren `hdbsql` Ausführbar in `hana.properties` Dateien, das Wrapper-Skript wird hinzugefügt.

Für einen zentralen HANA-Plug-in-Host auf dem SnapCenter-Windows-Server müssen Sie den folgenden Inhalt in hinzufügen `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\hana.properties`.

```
HANA_HDBSQL_CMD=C:\\Program Files\\sap\\hdbclient\\hdbsql-ssl.cmd
```

Das Wrapper-Skript `hdbsql-ssl.cmd` Anrufe `hdbsql.exe` Mit den erforderlichen Befehlszeilenoptionen.

```
@echo off
"C:\Program Files\sap\hdbclient\hdbsql.exe" -e -ssltrustcert %*
```

> Der `-e - ssltrustcert` Hdbsql-Befehlszeilenoption funktioniert auch für HANA-Systeme, bei denen SSL nicht aktiviert ist. Diese Option kann daher auch mit einem zentralen HANA-Plug-in-Host verwendet werden, auf dem nicht alle HANA-Systeme SSL aktiviert oder deaktiviert haben.

Wenn das HANA-Plug-in auf einzelnen HANA-Datenbank-Hosts implementiert wird, muss die Konfiguration auf jedem Linux-Host entsprechend vorgenommen werden.

```
HANA_HDBSQL_CMD = /usr/sap/SM1/HDB12/exe/hdbsqls
```

Das Wrapper-Skript `hdbsqls` Anrufe `hdbsql` Mit den erforderlichen Befehlszeilenoptionen.

```
#/bin/bash
/usr/sap/SM1/HDB12/exe/hdbsql -e -ssltrustcert $*
```

Deaktivieren Sie die automatische Erkennung auf dem HANA-Plug-in-Host

Gehen Sie wie folgt vor, um die automatische Erkennung auf dem HANA-Plug-in-Host zu deaktivieren:

1. Öffnen Sie auf dem SnapCenter-Server PowerShell. Stellen Sie eine Verbindung zum SnapCenter-Server her, indem Sie das ausführen `Open- SmConnection` Geben Sie im Anmeldefenster den Benutzernamen und das Passwort an.
2. Um die automatische Erkennung zu deaktivieren, führen Sie den aus `Set- SmConfigSettings` Befehl.

   Für einen HANA-Host `hana-2`, Der Befehl lautet wie folgt:

```
PS C:\Users\administrator.SAPCC> Set-SmConfigSettings -Agent -Hostname
hana-2 -configSettings @{"DISABLE_AUTO_DISCOVERY"="true"}
Name                           Value
----                           -----
DISABLE_AUTO_DISCOVERY         true
PS C:\Users\administrator.SAPCC>
```

3. Überprüfen Sie die Konfiguration, indem Sie den ausführen `Get- SmConfigSettings` Befehl.

```
PS C:\Users\administrator.SAPCC> Get-SmConfigSettings -Agent -Hostname
hana-2 -key all
Key: CUSTOMPLUGINS_OPERATION_TIMEOUT_IN_MSEC           Value: 3600000
Details: Plug-in API operation Timeout
Key: CUSTOMPLUGINS_HOSTAGENT_TO_SERVER_TIMEOUT_IN_SEC   Value: 1800
Details: Web Service API Timeout
Key: CUSTOMPLUGINS_ALLOWED_CMDS                         Value: *;
Details: Allowed Host OS Commands
Key: DISABLE_AUTO_DISCOVERY                             Value: true
Details:
Key: PORT                                               Value: 8145
Details: Port for server communication
PS C:\Users\administrator.SAPCC>
```

   Die Konfiguration wird in die Agent-Konfigurationsdatei auf dem Host geschrieben und ist nach einem Plug-in-Upgrade mit SnapCenter weiterhin verfügbar.

```
hana-2:/opt/NetApp/snapcenter/scc/etc # cat
/opt/NetApp/snapcenter/scc/etc/agent.properties | grep DISCOVERY
DISABLE_AUTO_DISCOVERY = true
hana-2:/opt/NetApp/snapcenter/scc/etc #
```

Deaktivieren der automatischen Backup-Organisation für Protokolle

Die allgemeine Ordnung und Sauberkeit der Protokollsicherung ist standardmäßig aktiviert und kann auf der HANA-Plug-in-Hostebene deaktiviert werden. Es gibt zwei Optionen, um diese Einstellungen zu ändern.

Bearbeiten Sie die Datei hana.property

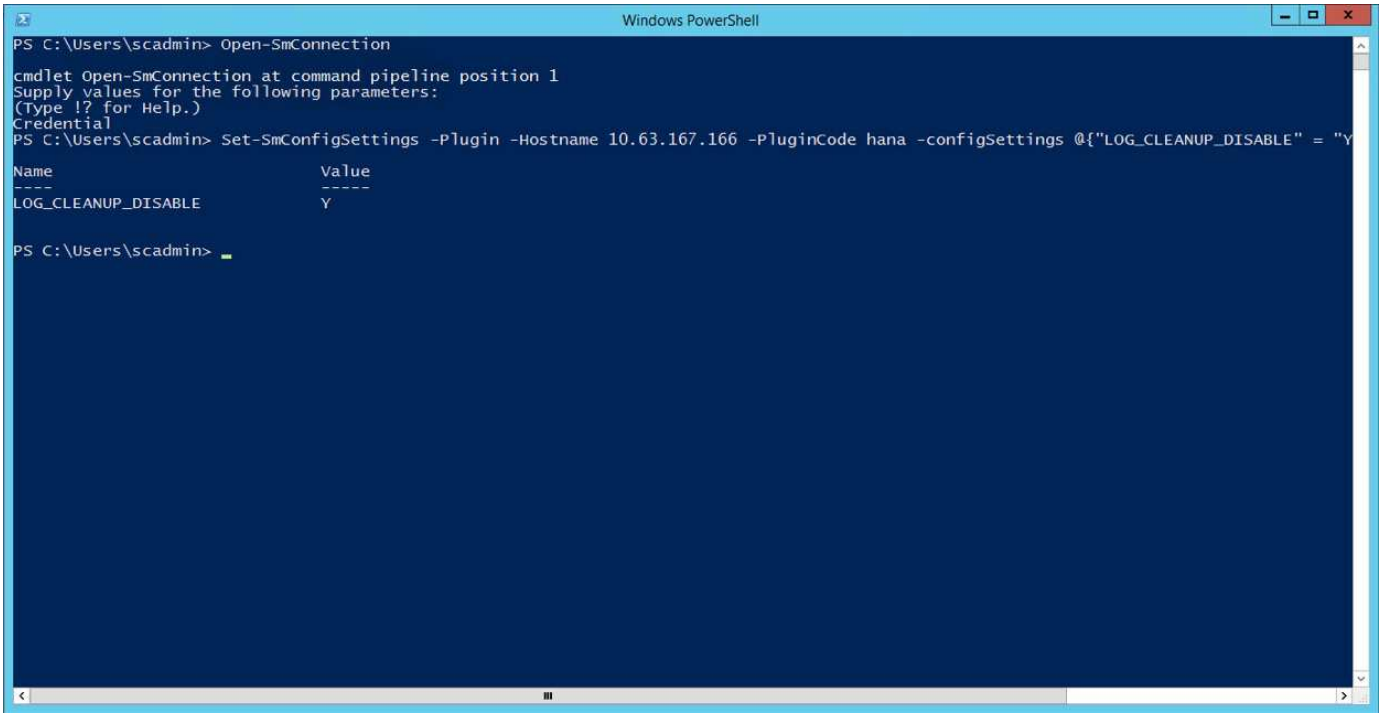
Einschließlich des Parameters `LOG_CLEANUP_DISABLE = Y` Im `hana.property` Die Konfigurationsdatei deaktiviert die allgemeine Ordnung und Sauberkeit der Protokollsicherung für alle Ressourcen, die diesen SAP HANA Plug-in-Host als Kommunikationshost verwenden:

- Für den Hdbsql Kommunikations-Host unter Windows, die `hana.property` Datei befindet sich unter `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc`.
- Für den Hdbsql-Kommunikations-Host unter Linux, die `hana.property` Datei befindet sich unter `/opt/NetApp/snapcenter/scc/etc`.

Verwenden Sie den PowerShell-Befehl

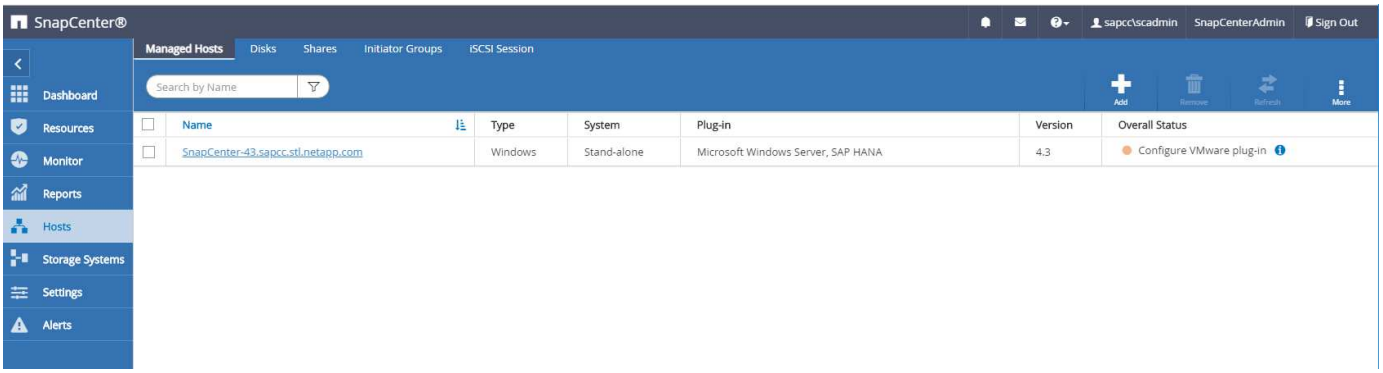
Eine zweite Option zum Konfigurieren dieser Einstellungen ist der SnapCenter PowerShell Befehl.

1. Öffnen Sie auf dem SnapCenter-Server eine PowerShell. Stellen Sie mit dem Befehl eine Verbindung zum SnapCenter-Server her `Open- SmConnection` Und geben Sie im Anmeldefenster den Benutzernamen und das Passwort an.
2. Mit dem Befehl `Set- SmConfigSettings -Plugin - HostName <pluginhostname> - PluginCode hana - configSettings @{"LOG_CLEANUP_DISABLE" = "Y"}`, Die Änderungen werden für den SAP HANA Plug-in-Host konfiguriert `<pluginhostname>` Durch den IP- oder Host-Namen angegeben (siehe folgende Abbildung).



Deaktivieren Sie die Warnung beim Ausführen des SAP HANA-Plug-ins in einer virtuellen Umgebung

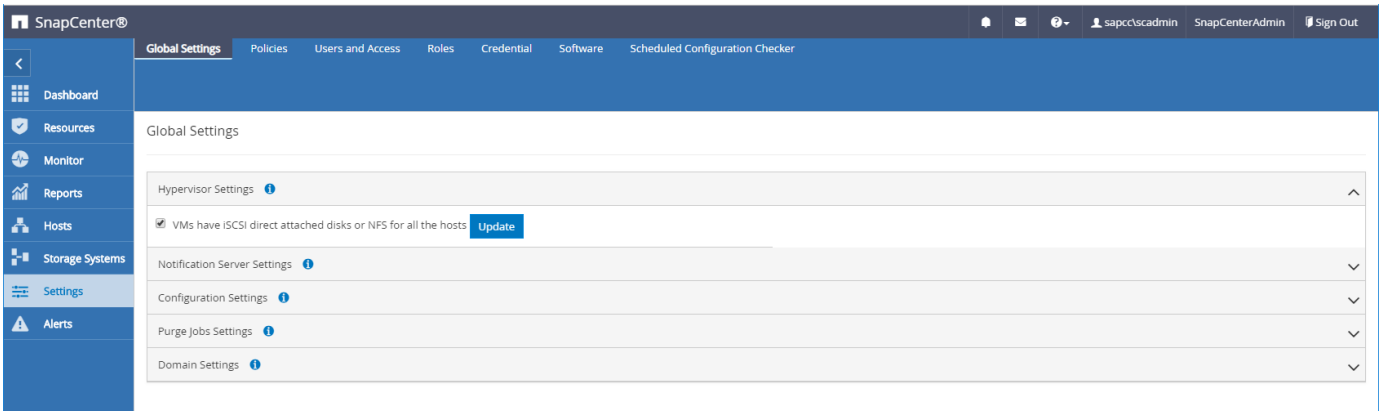
SnapCenter erkennt, ob das SAP HANA Plug-in in in einer virtualisierten Umgebung installiert ist. Dabei kann es sich um eine VMware Umgebung oder eine SnapCenter Installation bei einem Public Cloud Provider handelt. In diesem Fall zeigt SnapCenter eine Warnung für die Konfiguration des Hypervisors an, wie in der folgenden Abbildung dargestellt.



Diese Warnung kann global unterdrückt werden. In diesem Fall kennt SnapCenter virtualisierte Umgebungen nicht und weist daher keine derartigen Warnungen auf.

Um SnapCenter zu konfigurieren, um diese Warnung zu unterdrücken, muss die folgende Konfiguration angewendet werden:

1. Wählen Sie auf der Registerkarte Einstellungen die Option Globale Einstellungen.
2. Wählen Sie für die Hypervisor-Einstellungen die Option VMs mit iSCSI Direct Attached Disks oder NFS für alle Hosts aus, und aktualisieren Sie die Einstellungen.



Ändern Sie die Häufigkeit der Backup-Synchronisierung mit externen Backup-Storage

Wie im Abschnitt beschrieben "„Retention Management von Backups auf dem Sekundärspeicher“,"wird das Aufbewahrungsmanagement von Daten-Backups auf einen externen Backup-Storage von ONTAP übernommen. SnapCenter prüft regelmäßig, ob ONTAP Backups auf dem externen Backup-Storage gelöscht hat. Dazu wird ein Bereinigungsauftrag mit einem wöchentlichen Standardzeitplan ausgeführt.

Der SnapCenter-Bereinigungsauftrag löscht Backups im SnapCenter-Repository sowie im SAP HANA-Backup-Katalog, wenn gelöschte Backups im externen Backup-Speicher identifiziert wurden.

Der Bereinigungsauftrag führt auch die allgemeine Ordnung und Sauberkeit der SAP HANA-Log-Backups aus.

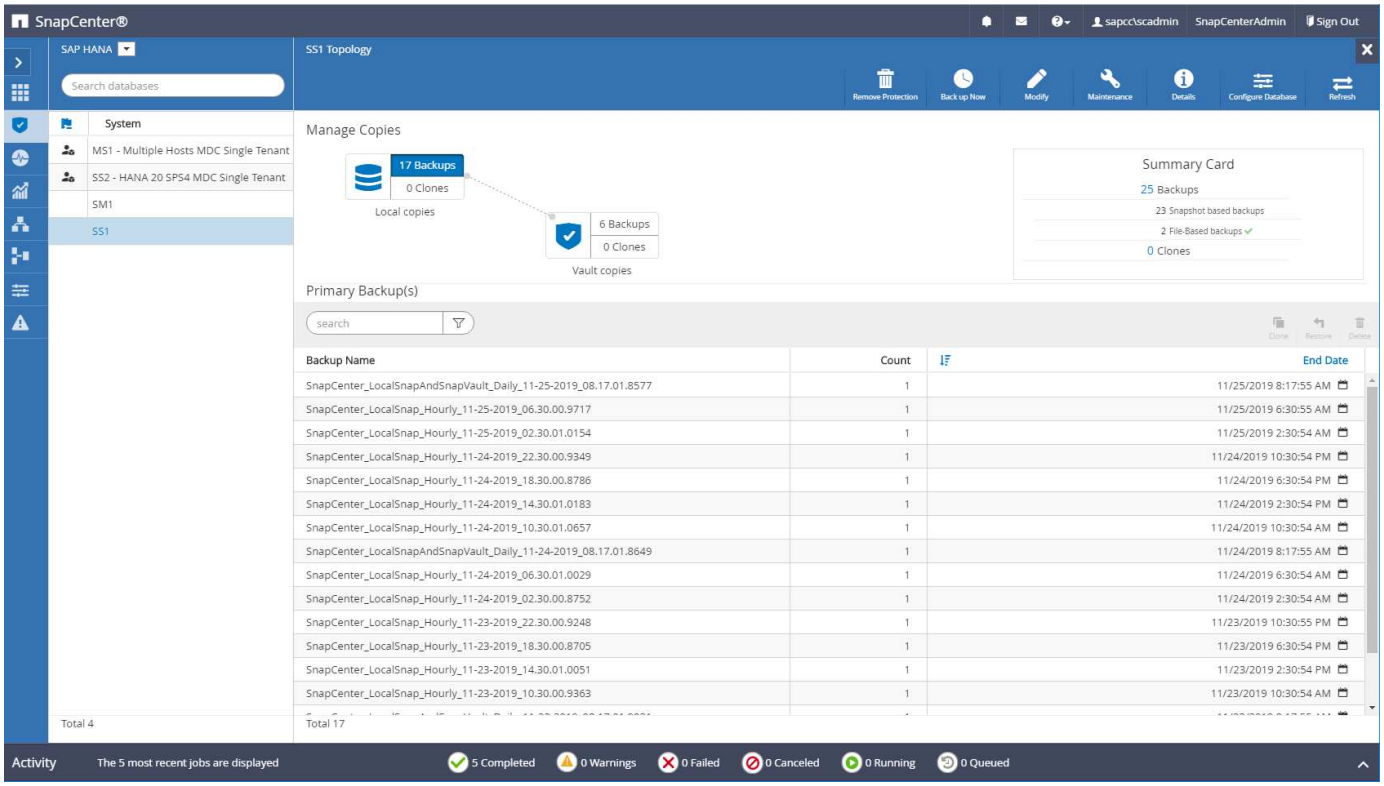
Bis diese geplante Bereinigung beendet ist, zeigen SAP HANA und SnapCenter noch Backups an, die bereits aus dem externen Backup-Storage gelöscht wurden.

Dies kann zu zusätzlichen Protokoll-Backups führen, die aufbewahrt werden, selbst wenn die entsprechenden Storage-basierten Snapshot Backups auf dem externen Backup Storage bereits gelöscht wurden.

In den folgenden Abschnitten werden zwei Möglichkeiten beschrieben, um diese temporäre Diskrepanz zu vermeiden.

Manuelle Aktualisierung auf Ressourcenebene

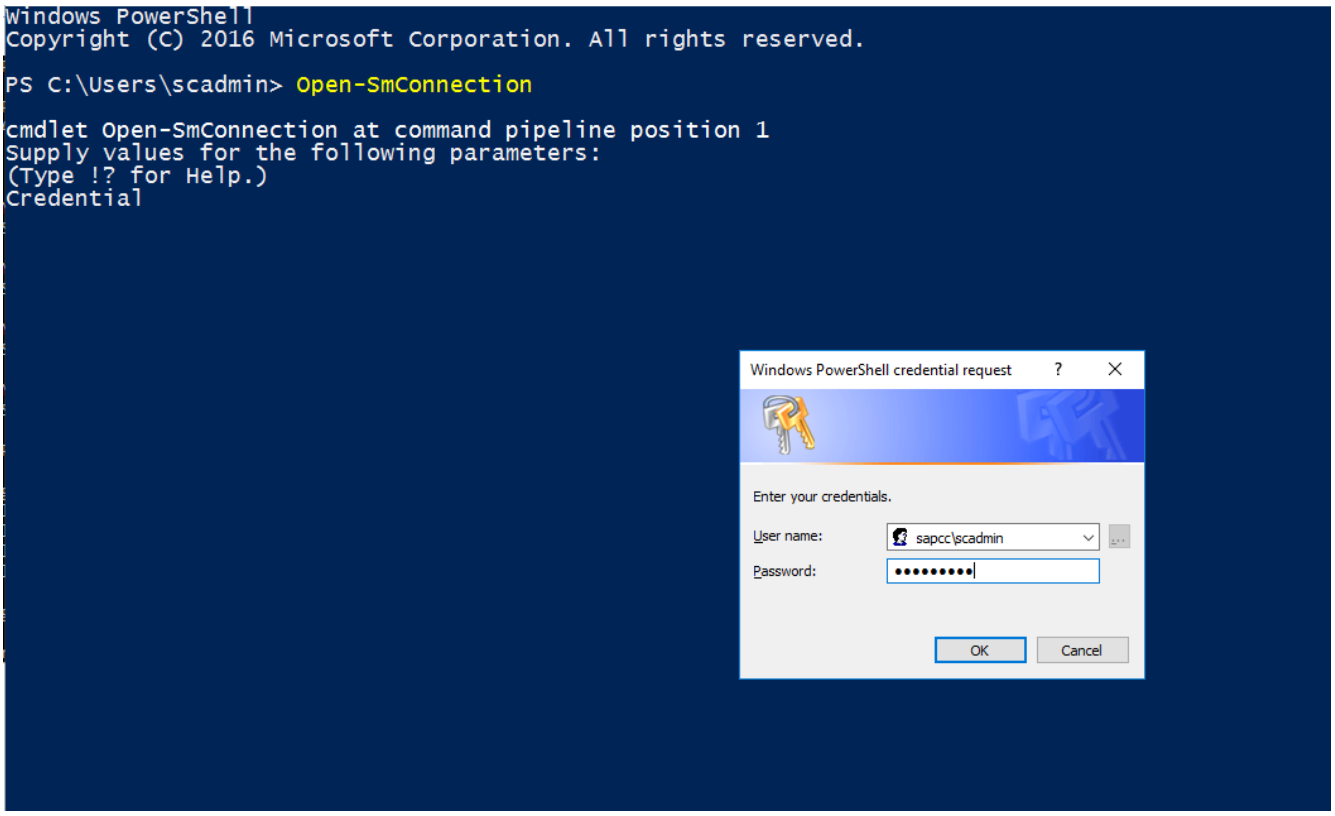
In der Topologieansicht einer Ressource zeigt SnapCenter bei der Auswahl der sekundären Backups die Backups auf dem externen Backup-Speicher an, wie im folgenden Screenshot dargestellt. SnapCenter führt eine Bereinigung mit dem Symbol „Aktualisieren“ aus, um die Backups für diese Ressource zu synchronisieren.



Ändern Sie die Häufigkeit des SnapCenter-Bereinigungsjobs

SnapCenter führt den Bereinigungsjob aus `SnapCenter_RemoveSecondaryBackup` Standardmäßig werden alle Ressourcen wöchentlich unter Verwendung des Windows-Arbeitsplanungsmechanismus verwendet. Dies kann mit einem SnapCenter PowerShell Cmdlet geändert werden.

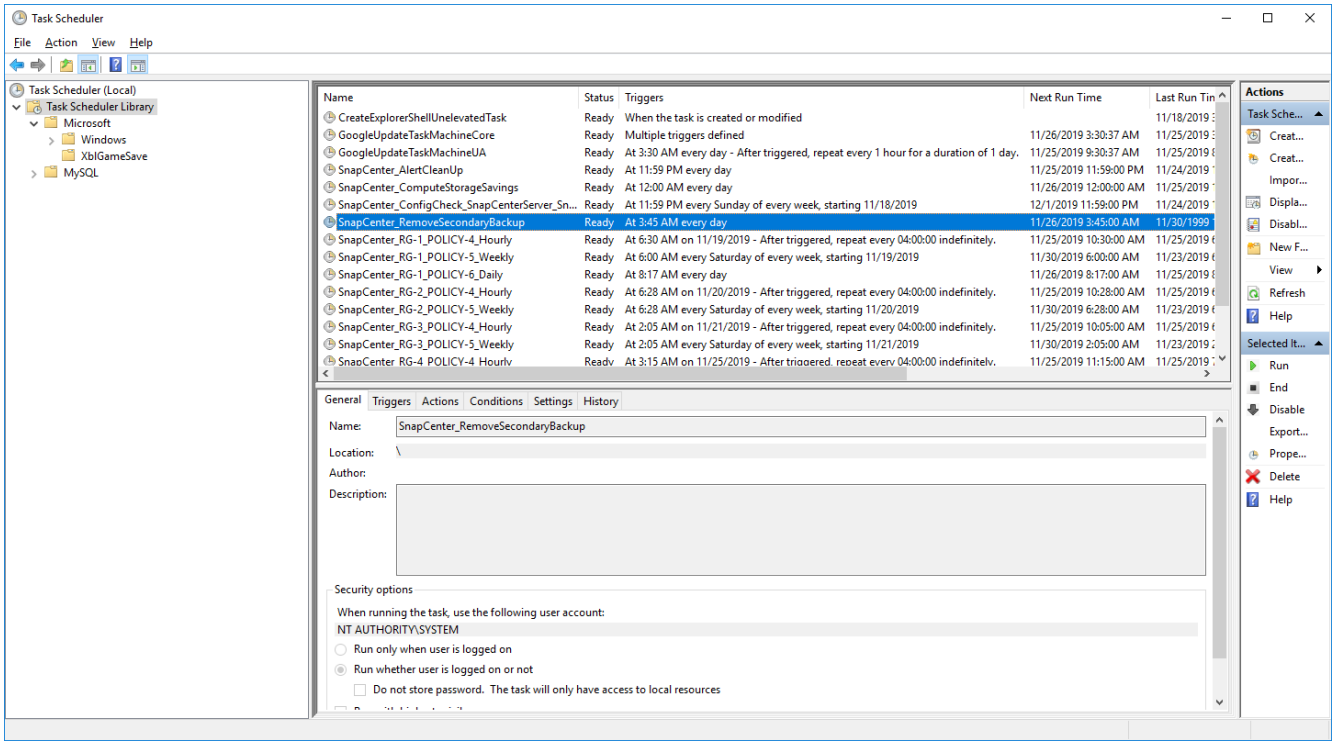
1. Starten Sie ein PowerShell Befehlsfenster auf dem SnapCenter-Server.
2. Öffnen Sie die Verbindung zum SnapCenter-Server, und geben Sie im Anmeldefenster die Anmeldedaten des SnapCenter-Administrators ein.



3. Um den Zeitplan von einer Woche auf eine tägliche Basis zu ändern, verwenden Sie das Cmdlet `Set-SmSchedule`.

```
PS C:\Users\scadmin> Set-SmSchedule -ScheduleInformation
@{"ScheduleType"="Daily";"StartTime"="03:45 AM";"DaysInterval"=
"1"} -TaskName SnapCenter_RemoveSecondaryBackup
TaskName              : SnapCenter_RemoveSecondaryBackup
Hosts                 : {}
StartTime             : 11/25/2019 3:45:00 AM
DaysoftheMonth        :
MonthsofTheYear       :
DaysInterval          : 1
DaysOfTheWeek         :
AllowDefaults         : False
ReplaceJobIfExist     : False
UserName              :
Password              :
SchedulerType         : Daily
RepeatTask_Every_Hour :
IntervalDuration      :
EndTime               :
LocalScheduler        : False
AppType               : False
AuthMode              :
SchedulerSQLInstance  : SMCoreContracts.SmObject
MonthlyFrequency      :
Hour                  : 0
Minute                : 0
NodeName              :
ScheduleID            : 0
RepeatTask_Every_Mins :
CronExpression        :
CronOffsetInMinutes   :
StrStartTime          :
StrEndTime            :
PS C:\Users\scadmin> Check the configuration using the Windows Task
Scheduler.
```

4. Sie können die Job-Eigenschaften im Windows Task Scheduler überprüfen.



Wo finden Sie weitere Informationen und Versionsverlauf

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- Seite „SnapCenter Ressourcen“

  "https://www.netapp.com/us/documentation/snapcenter-software.aspx"

- SnapCenter-Softwaredokumentation

  "https://docs.netapp.com/us-en/snapcenter/index.html"

- TR-4667: Automatisierung von SAP Systemkopien mit dem SnapCenter

  "SAP Systemkopien mithilfe der SnapCenter automatisieren"

- TR-4719: SAP HANA System Replication, Backup und Recovery mit SnapCenter

  "SAP HANA System Replication, Backup and Recovery mit SnapCenter"

- TR-4018: Integration von NetApp ONTAP-Systemen in SAP Landscape Management

  https://www.netapp.com/pdf.html?item=/media/17195-tr4018pdf.pdf

- TR-4646: SAP HANA Disaster Recovery with Storage Replication

  https://www.netapp.com/pdf.html?item=/media/8584-tr4646pdf.pdf

Versionsverlauf

Version	Datum	Versionsverlauf des Dokuments
Version 1.0	Juli 2017	• Erste Version.
Version 1.1	September 2017	• Der Abschnitt „Erweiterte Konfiguration und Anpassung“ wurde hinzugefügt. • Kleinere Korrekturen.
Version 2.0	März 2018	• Updates zu SnapCenter 4.0: Neue Ressource für das Datenvolumen Verbesserte SnapRestore-Operation einer einzelnen Datei
Version 3.0	Januar 2020	• Der Abschnitt „SnapCenter-Konzepte und Best-Practices“ wurde hinzugefügt. • Updates zu SnapCenter 4.3: Automatische Erkennung Automatisiertes Restore und Recovery Unterstützung für HANA MDC mehrere Mandanten Wiederherstellung eines Mandanten
Version 3.1	Juli 2020	• Kleinere Aktualisierungen und Korrekturen: NFSv4-Unterstützung mit SnapCenter 4.3.1 Konfiguration der SSL-Kommunikation Zentrale Plug-in-Implementierung für Linux auf IBM Power
Version 3.2	November 2020	• Die erforderlichen Benutzerberechtigungen für die Datenbank für HANA 2.0 SPS5 wurden hinzugefügt.
Version 3.3	Mai 2021	• Der Abschnitt SSL-hdbsql-Konfiguration wurde aktualisiert. • Linux LVM-Unterstützung hinzugefügt.

Version	Datum	Versionsverlauf des Dokuments
Version 3.4	August 2021	• Die Konfigurationsbeschreibung für die automatische Ermittlung deaktivieren wurde hinzugefügt.
Version 3.5	Februar 2022	• Kleinere Updates zu SnapCenter 4.6 und Unterstützung von automatischer Erkennung für HANA-Systeme mit Systemreplizierung

SAP HANA Datensicherung und Hochverfügbarkeit mit SnapCenter, SnapMirror Active Sync und VMware Metro Storage Cluster

SAP HANA Datensicherung und Hochverfügbarkeit mit SnapCenter, SnapMirror Active Sync und VMware Metro Storage Cluster

Dieses Dokument enthält Best Practices für die Datensicherung mit SnapCenter in einer VMware-Umgebung in Kombination mit SnapMirror Active Sync als Hochverfügbarkeitslösung für die HANA-Storage-Ressourcen.

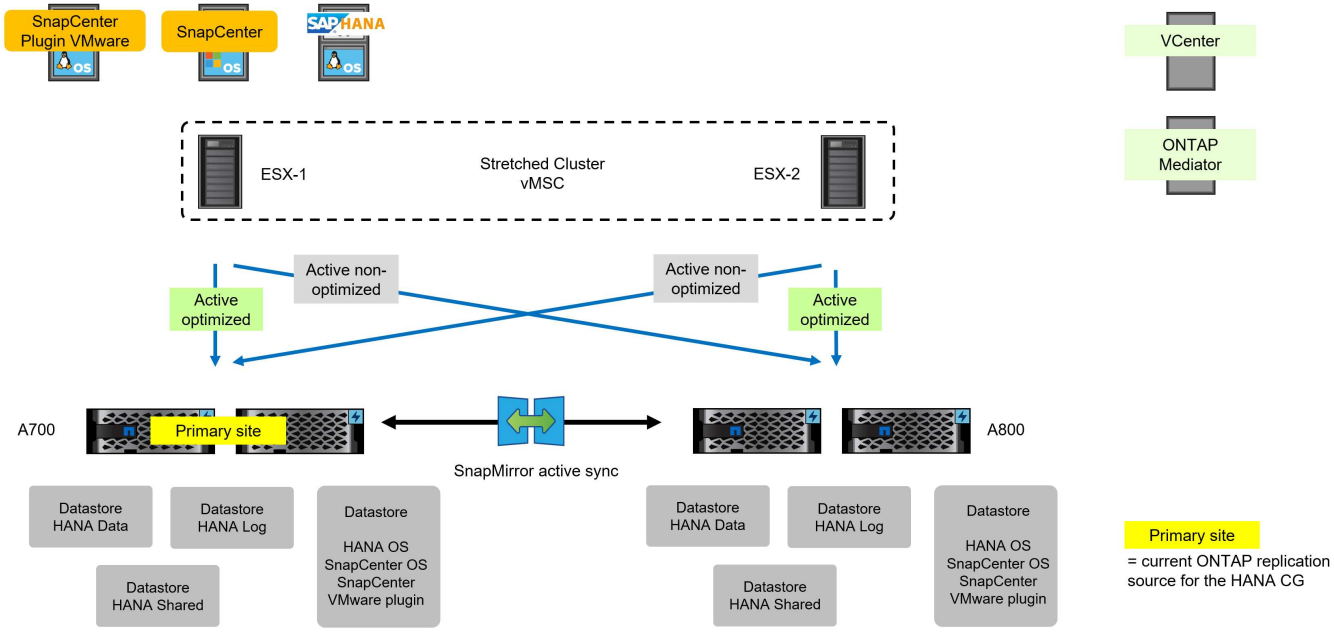
Autor: Nils Bauer, NetApp

Inhalt des vorliegenden Dokuments

Das Dokument soll keine Schritt-für-Schritt-Beschreibung der Einrichtung der gesamten Umgebung sein, sondern umfasst Konzepte und relevante Details zu:

- Setup von SAP HANA Systemen mit VMware VMFS
- SnapMirror Active Sync Konfiguration für SAP HANA
- SnapCenter-Konfiguration für HANA auf VMware mit VMFS
- SnapCenter-Konfiguration für SnapMirror Active Sync
- SnapCenter Betrieb mit HANA auf VMware und SnapMirror Active Sync

Wir werden uns auf eine VMware Metro Storage Cluster (vMSC) Konfiguration mit einem einheitlichen Zugriff Setup von SnapMirror Active Sync wie in der Abbildung unten gezeigt, aber wir werden auch kurz berühren Bare Metal sowie nicht-einheitliche Access-Konfigurationen.



Überblick über die Hochverfügbarkeit mit SAP HANA

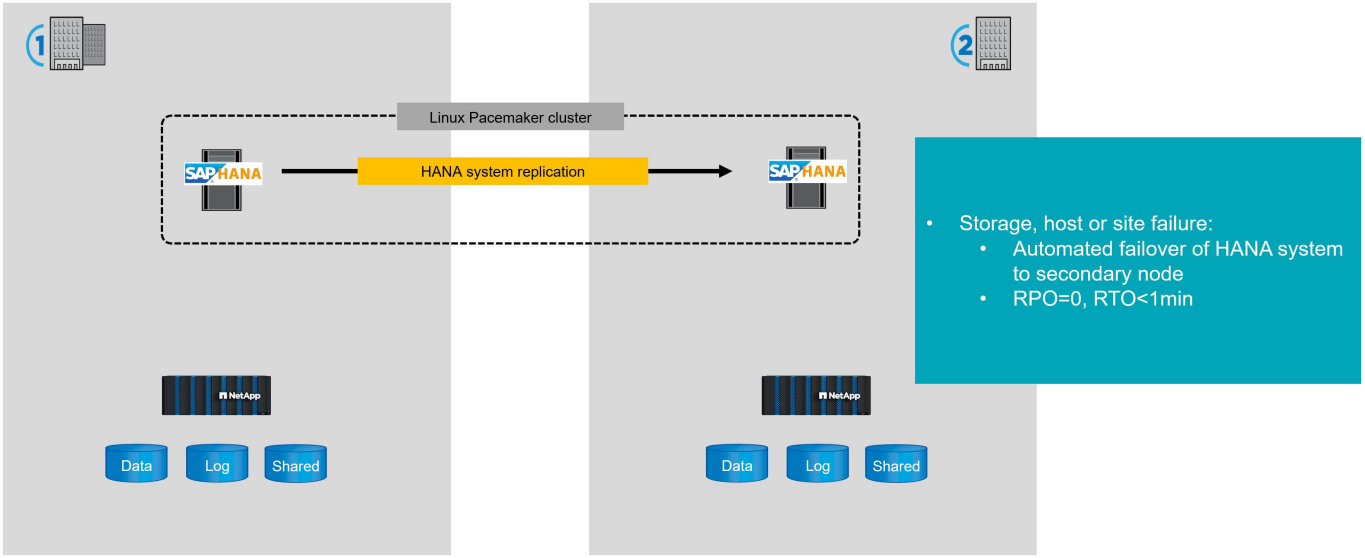
Dieses Kapitel bietet einen Überblick über Hochverfügbarkeitsoptionen für SAP HANA, bei denen die Replizierung auf Applikationsebene mit der Storage-Replizierung verglichen wird.

SAP HANA Systemreplizierung (HSR)

Die SAP HANA-Systemreplikation bietet einen Betriebsmodus, in dem die Daten synchron repliziert, in den Arbeitsspeicher vorgeladen und auf dem sekundären Host kontinuierlich aktualisiert werden. Dieser Modus ermöglicht sehr niedrige RTO-Werte, etwa eine Minute oder weniger, aber er erfordert auch einen dedizierten Server, der nur verwendet wird, um die Replikationsdaten vom Quellsystem zu empfangen. Aufgrund der geringen Failover-Zeit wird die SAP HANA Systemreplizierung auch für Wartungsarbeiten ohne Ausfallzeiten wie HANA-Software-Upgrades eingesetzt. Linux Pacemaker-Cluster-Lösungen werden in der Regel zur Automatisierung von Failover-Vorgängen eingesetzt.

Bei einem Ausfall am primären Standort, Speicher, Host oder kompletten Standort erfolgt automatisch ein Failover des HANA-Systems auf den sekundären Standort, der vom Linux Pacemaker-Cluster gesteuert wird.

Eine vollständige Beschreibung aller Konfigurationsoptionen und Replikationsszenarien finden Sie unter "SAP HANA System Replication SAP Help Portal".



Aktive NetApp SnapMirror-Synchronisierung

SnapMirror Active Sync ermöglicht Business Services auch bei einem vollständigen Standortausfall den Betrieb weiter und unterstützt Applikationen bei einem transparenten Failover mithilfe einer sekundären Kopie. Für die Auslösung eines Failover mit SnapMirror Active Sync sind keine manuellen Eingriffe oder benutzerdefinierten Skripts erforderlich. SnapMirror Active Sync wird auf AFF-Clustern, ASA-Clustern (All-Flash SAN Array) und C-Series (AFF oder ASA) unterstützt. SnapMirror Active Sync sichert Applikationen mit iSCSI- oder FCP-LUNs.

Ab ONTAP 9.15.1 unterstützt die SnapMirror Active Sync symmetrische aktiv/aktiv-Funktion. Symmetrische aktiv/aktiv-Konfiguration ermöglicht I/O-Vorgänge für Lese- und Schreibvorgänge von beiden Kopien einer geschützten LUN mit bidirektionaler synchroner Replizierung, sodass beide LUN-Kopien lokal für I/O-Vorgänge sorgen können.

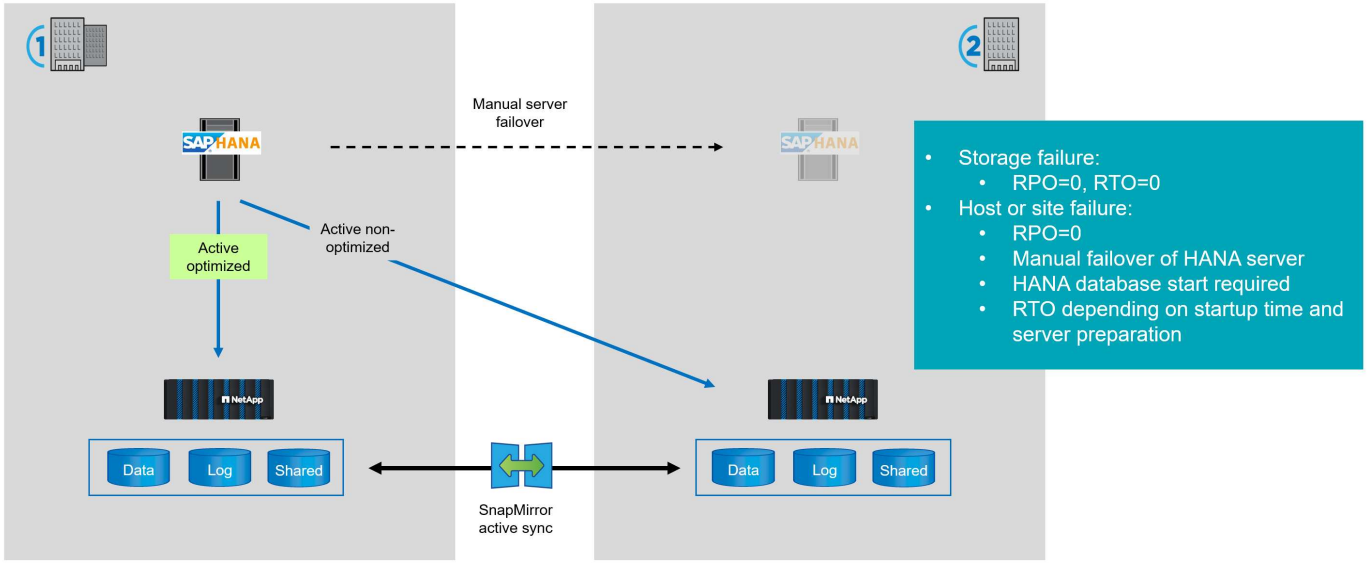
Weitere Details finden Sie unter "Übersicht über die aktive SnapMirror-Synchronisierung in ONTAP".

HANA Bare Metal

Wenn Sie SAP HANA auf einem Bare Metal-Server ausführen, können Sie SnapMirror Active Sync verwenden, um eine hochverfügbare Storage-Lösung bereitzustellen. Die Daten werden synchron repliziert und bieten daher ein RPO=0.

Bei einem Storage-Ausfall greift das HANA-System über den zweiten FCP-Pfad transparent auf die gespiegelte Kopie am sekundären Standort zu und bietet somit RTO=0.

Im Falle eines Host- oder vollständigen Standortausfalls muss ein neuer Server am sekundären Standort bereitgestellt werden, um auf die Daten vom ausgefallenen Host zugreifen zu können. Dabei handelt es sich normalerweise um ein Test- oder QA-System der gleichen Größe wie die Produktion, das nun heruntergefahren und für die Ausführung des Produktionssystems verwendet wird. Nachdem die LUNs am sekundären Standort mit dem neuen Host verbunden wurden, muss die HANA-Datenbank gestartet werden. Das gesamte RTO hängt daher von der für die Bereitstellung des Hosts benötigten Zeit und der Startzeit der HANA-Datenbank ab.

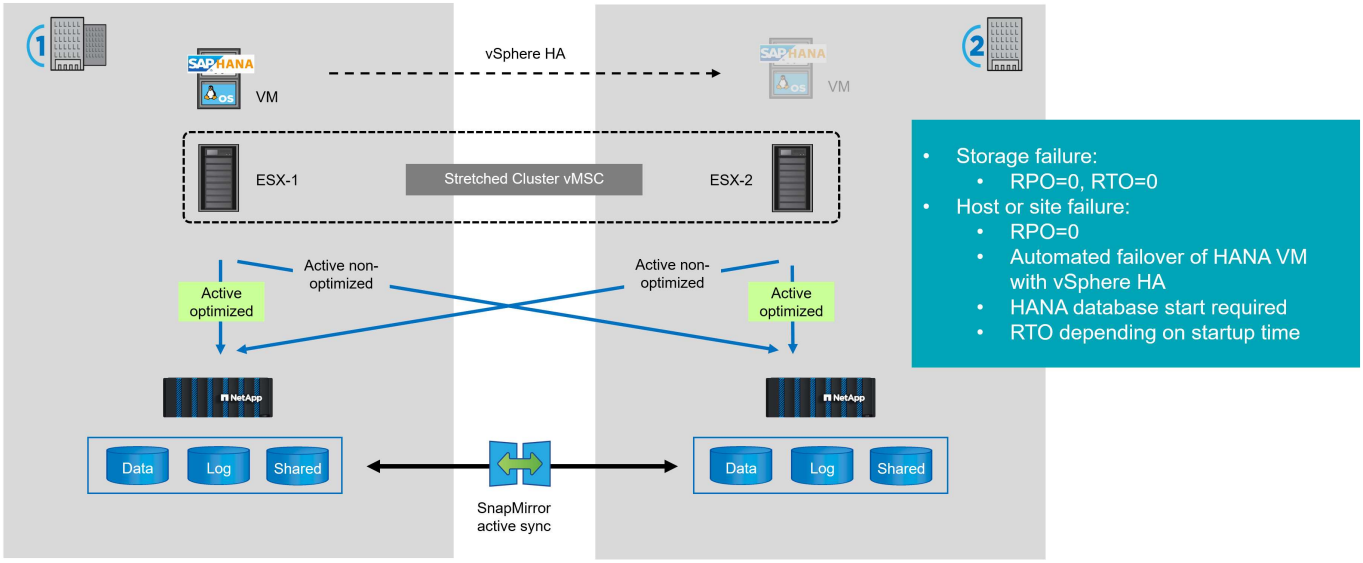


VSphere Metro Storage-Cluster (vMSC)

Wenn Sie SAP HANA in einer VMware-Umgebung mit FCP-verbundenen Datastores ausführen, können Sie SnapMirror Active Sync verwenden, um einen VMware Metro Storage-Cluster zu erstellen. In einem solchen Setup werden die vom HANA-System verwendeten Datastores synchron am sekundären Standort repliziert.

Bei einem Storage-Ausfall greift der ESX-Host automatisch auf die gespiegelte Kopie am sekundären Standort zu und liefert eine RTO=0.

Im Fall eines Host- oder vollständigen Standortausfalls wird vSphere HA verwendet, um die HANA-VM auf dem sekundären ESX-Host zu starten. Wenn die HANA VM ausgeführt wird, muss die HANA Datenbank gestartet werden. Die gesamte RTO hängt daher hauptsächlich von der Startzeit der HANA-Datenbank ab.



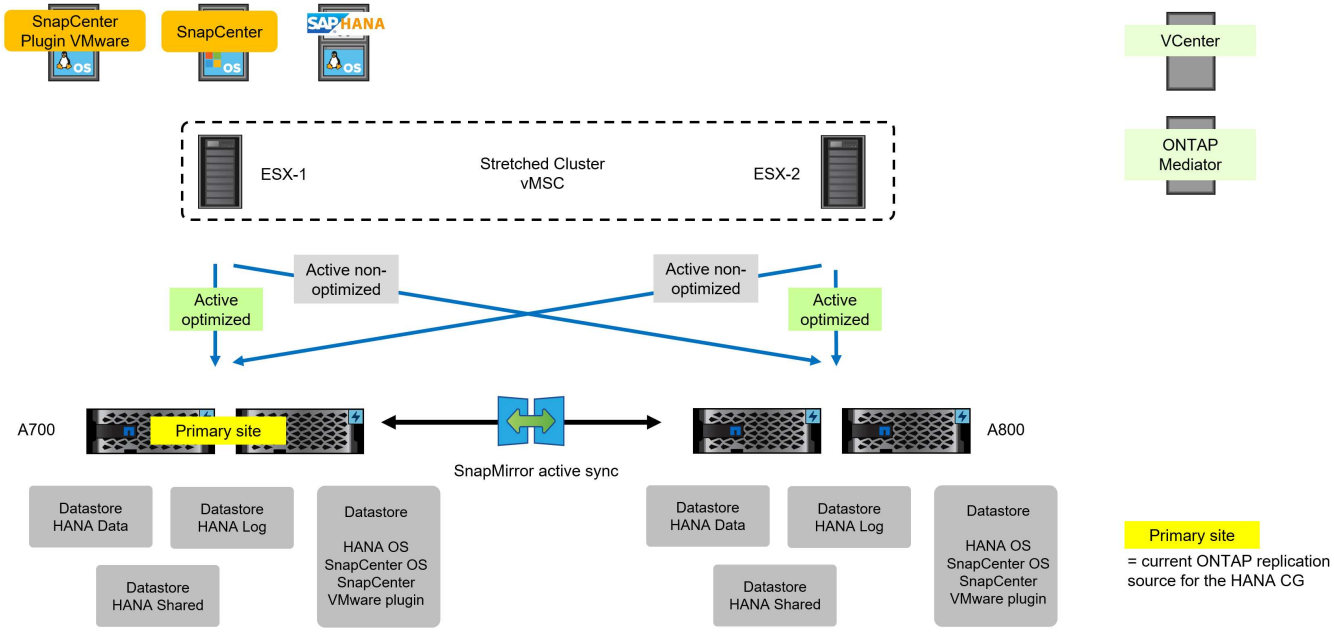
Lösungsvergleich

Die folgende Tabelle bietet eine Zusammenfassung der wichtigsten Merkmale der oben beschriebenen Lösungen.

	HANA System Replication	Aktive SnapMirror-Synchronisierung – Bare Metal	SnapMirror Active Sync – VMware vMSC
RPO bei jedem Ausfall	RPO=0 + synchrone Replikation		
RTO bei Storage-Ausfall	RTO +< 1 Min	RTO=0 + transparenter Storage-Failover	
RTO + bei Standort- oder Host-Ausfall	RTO +< 1 Min	RTO: Abhängig von der Zeit, die für die Servervorbereitung und den Start der HANA-Datenbank benötigt wird.	RTO: Abhängig von der für den Start der HANA-Datenbank erforderlichen Zeit.
Failover-Automatisierung	Ja, Automatisches Failover auf sekundären HSR-Host Gesteuert durch Schrittmachercluster.	Ja, bei Storage-Ausfällen Nein, bei Host- oder Standortausfall (Bereitstellung des Hosts, Verbinden von Storage-Ressourcen, Start der HANA-Datenbank)	Ja, bei Storage-Ausfällen Ja, bei Host- oder Standortausfall (Failover von VM zum anderen Standort automatisiert mit vSphere HA, Start der HANA-Datenbank)
Dedizierter Server am sekundären Standort erforderlich	Ja, Daten mussten vorab in den Speicher geladen und ein schnelles Failover ohne Datenbankstart ermöglicht werden.	Nein, Server ist nur bei Failover erforderlich. In der Regel wird der für die Qualitätssicherung verwendete Server dann für die Produktion genutzt.	Nein, Ressourcen auf ESX Host sind nur im Failover-Fall erforderlich. In der Regel werden QA-Ressourcen dann für die Produktion genutzt.

Beispiel für eine Konfigurationsübersicht

Im Lab Setup verwenden wir eine einheitliche Zugriffskonfiguration, auf der beide ESX Hosts Zugriff auf beide Storage Cluster haben. In den nächsten Abschnitten beschreiben wir die einheitliche Zugriffskonfiguration, heben aber auch die Unterschiede für ein nicht einheitliches Setup hervor.



Softwareversionen

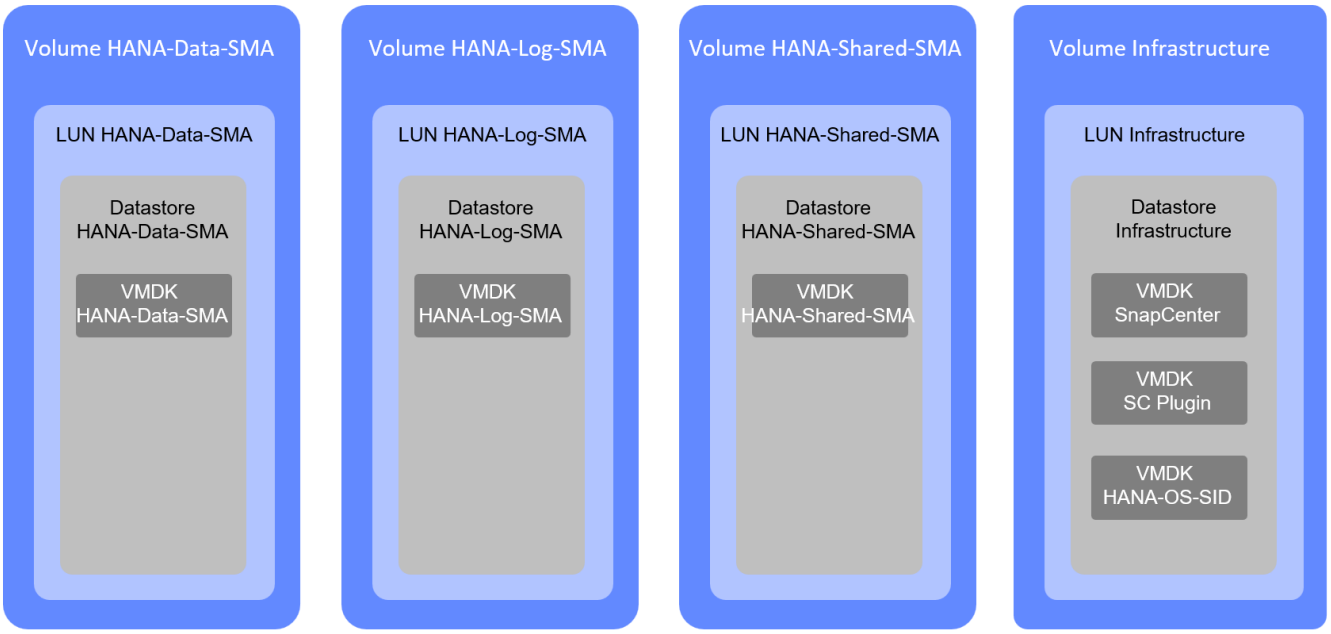
Software	Version
ONTAP	A700: 9.15.1 P7, A800: 9.16.1 RC1
VSphere Client	8.0.3
ESXi	8.0.3
SnapCenter Plug-in für vSphere	6.0.1
Linux BS	SLES FÜR SAP 15 SP5
SAP HANA	2,0 SPS8
SnapCenter	6.0.1

HANA-Systembereitstellung und -Installation

In diesem Kapitel werden die Installation und Konfiguration des für eine VMware-Einrichtung mithilfe von VMFS spezifischen SAP HANA-Systems beschrieben. Weitere allgemeine Best Practices finden Sie unter "Technischer Bericht: SAP HANA on NetApp AFF Systems with Fibre Channel Protocol".

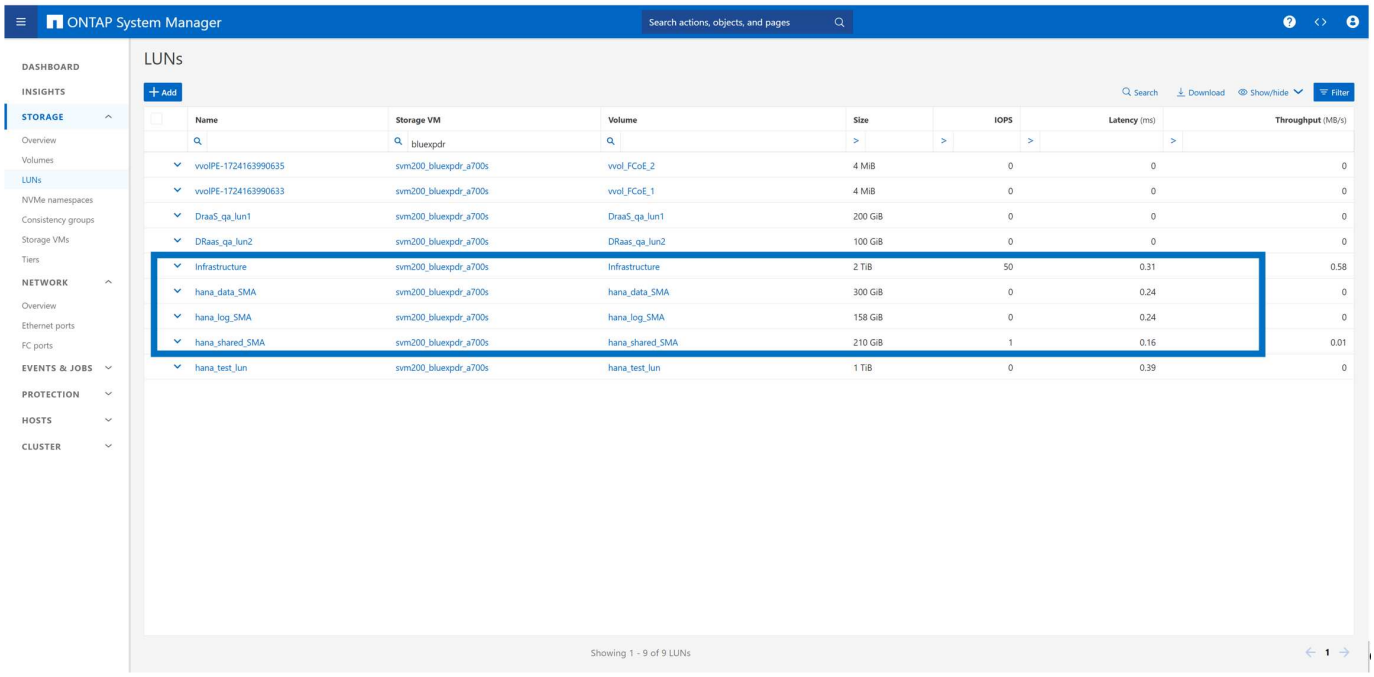
Storage-Konfiguration

Die Abbildung unten zeigt die Storage- und Datastore-Konfiguration für das HANA-System. Sie müssen für jedes Dateisystem des HANA-Systems ein dediziertes Volume, eine LUN oder einen Datastore konfigurieren. Datastores dürfen nicht über mehrere HANA-Systeme oder andere Workloads hinweg freigegeben werden.



Alle drei LUNs des HANA-Systems (hana_Data_SMA, hana_log+*SAM und hana+_shared*+++SMA) sowie die LUN für die OS-Images und SnapCenter-Komponenten wurden beim A700-Storage-Cluster bereitgestellt.

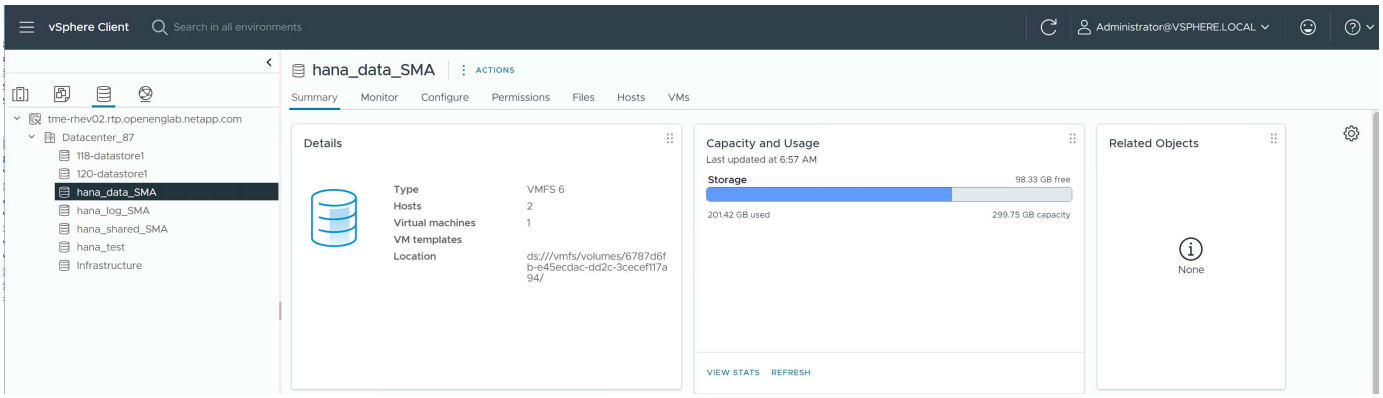
Alle Volumes des HANA-Systems müssen in derselben SVM bereitgestellt werden. In der später beschriebenen Konfiguration für aktive SnapMirror-Synchronisierung wird eine Konsistenzgruppe über alle drei HANA-Volumes erstellt, bei der sich die Volumes in derselben SVM befinden müssen. Das Infrastruktur-Volume wird sich in einer anderen Konsistenzgruppe befinden und könnte sich daher in einer anderen SVM befinden.



Eine Initiatorgruppe muss konfiguriert werden und die oben genannten LUNs müssen dem ESX-1 Host zugeordnet werden, der sich in unserem Lab-Setup in unmittelbarer Nähe des A700 Storage-Systems befindet.

Datastore-Bereitstellung

Wir haben drei Datastores für das HANA-System mit den drei LUNs erstellt, die wir zuvor bereitgestellt haben. Darüber hinaus haben wir mit der Infrastruktur-LUN einen Infrastruktur-Datastore erstellt.

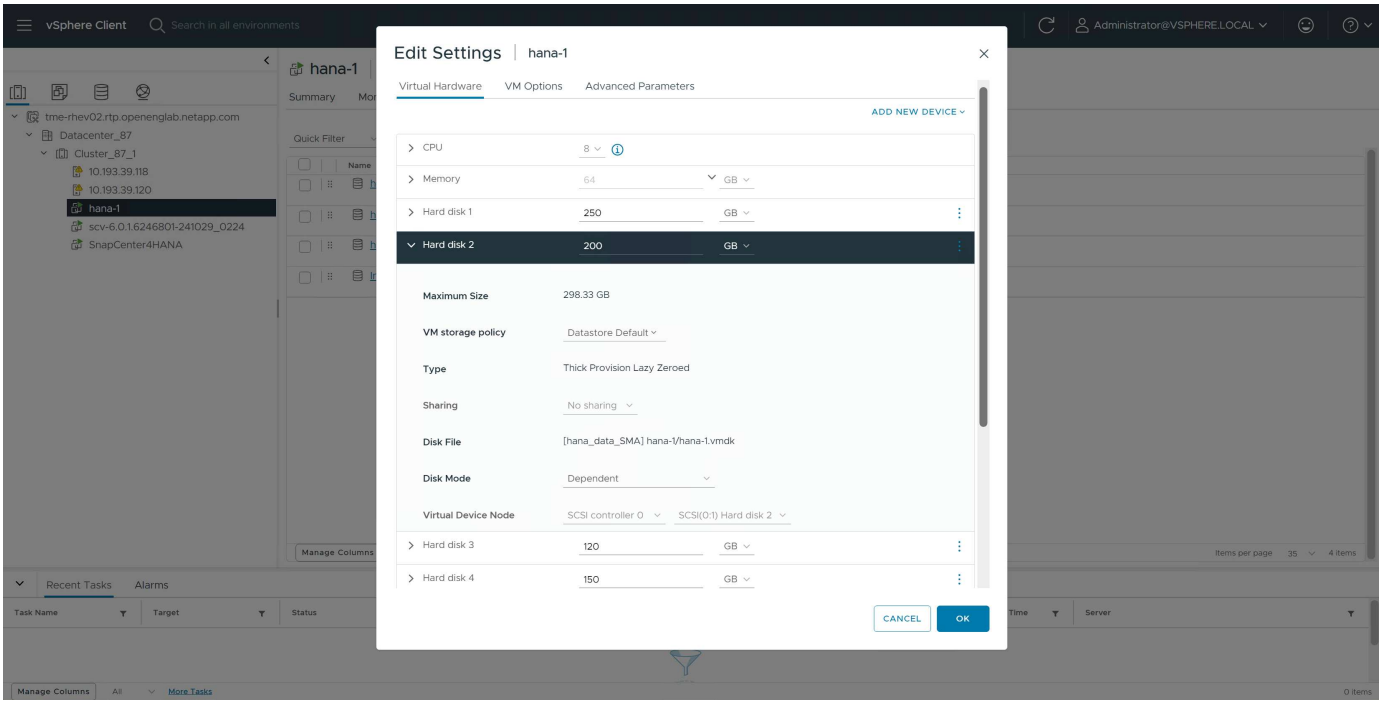


VM-Bereitstellung und Betriebssysteminstallation

In unserem Lab-Setup haben wir eine neue VM implementiert und die VMDK für das Linux Betriebssystem im Infrastruktur-Datenspeicher platziert.

Konfiguration von VM-Festplatten

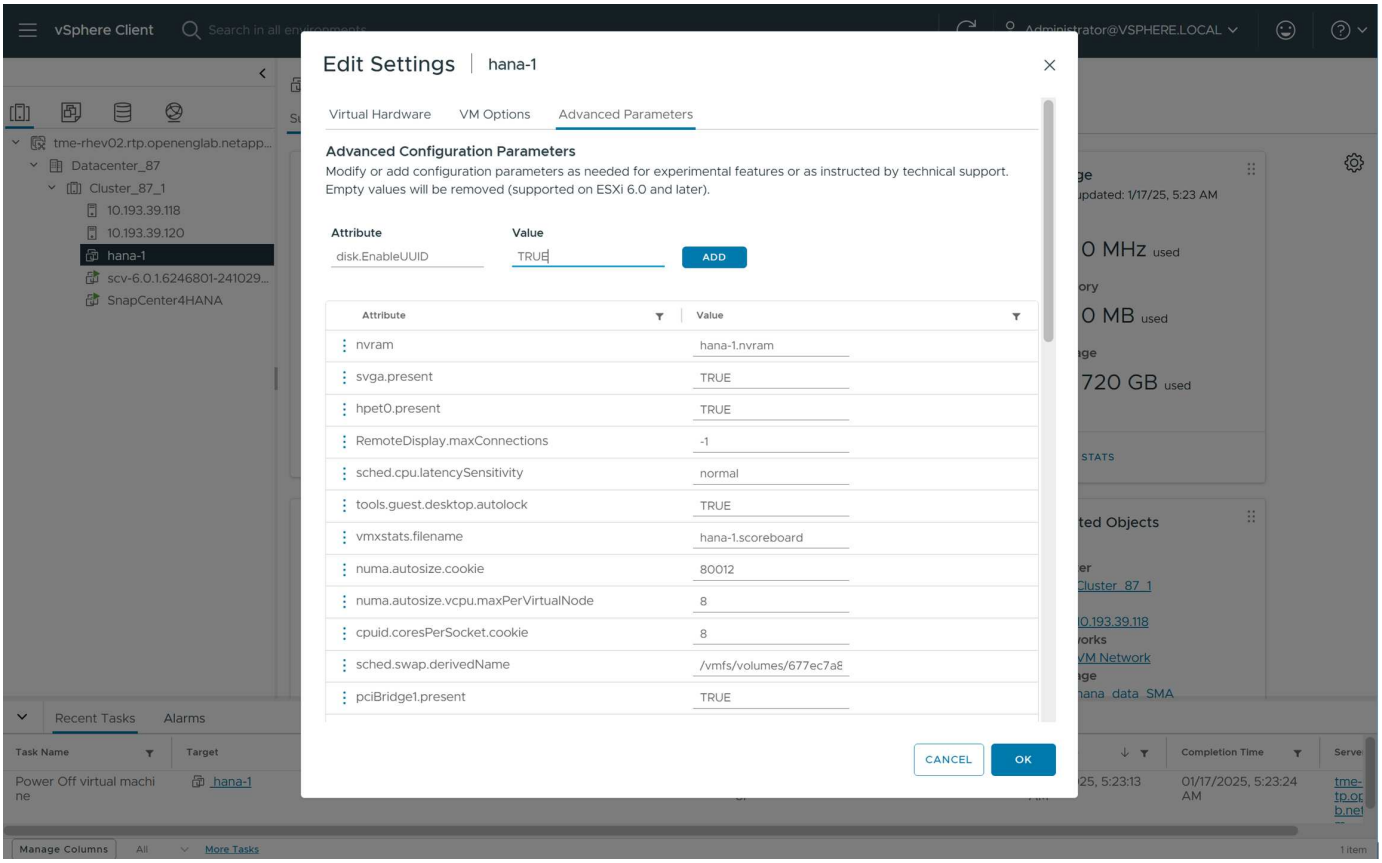
Der HANA VM wurden drei neue Festplatten hinzugefügt, jede Festplatte in einem der Datenspeicher, die für das HANA-System erstellt wurden.



VM-Parametereinstellung

Der Parameter Disk.EnableUUID muss hinzugefügt und auf TRUE gesetzt werden. Der Parameter wird von SnapCenter benötigt. Wenn nicht festgelegt, schlägt der SnapCenter-Vorgang „Ermittlung der virtuellen Ressource“ fehl.

Die VM muss angehalten werden, bevor Parameter hinzugefügt werden können.



Die Funktionalität kann mit dem folgenden Befehl überprüft werden.

```
hana-1:~ # sg_inq /dev/sdd
standard INQUIRY:
PQual=0 PDT=0 RMB=0 LU_CONG=0 hot_pluggable=0 version=0x06 [SPC-4]
[AERC=0] [TrmTsk=] NormACA=0 HiSUP=0 Resp_data_format=2
SCCS=0 ACC=0 TPGS=0 3PC=0 Protect=0 [BQue=0]
EncServ=0 MultiP=0 [MChngr=0] [ACKREQQ=0] Addr16=0
[RelAdr=0] WBus16=1 Sync=1 [Linked=0] [TranDis=0] CmdQue=1
length=36 (0x24) Peripheral device type: disk
Vendor identification: VMware
Product identification: Virtual disk
Product revision level: 2.0
Unit serial number: 6000c293fecf25ac6bc457af67fe1f54
```

Vorbereitung des Dateisystems auf Linux-Host

Erstellung des xfs-Dateisystems auf neuen Platten

Die Gerätenamen der neuen Festplatten können mit dem folgenden Befehl überprüft werden.

```
hana-1:/install # lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
sda 8:0 0 250G 0 disk
├─sda1 8:1 0 256M 0 part /boot/efi
└─sda2 8:2 0 82G 0 part
├─system-root 254:0 0 60G 0 lvm /root
│ /var
│ /usr/local
│ /tmp
│ /srv
│ /opt
│ /home
│ /boot/grub2/x86++_++64-efi
│ /boot/grub2/i386-pc
│ /.snapshots
│ /
└─system-swap 254:1 0 2G 0 lvm SWAP
sdb 8:16 0 200G 0 disk
sdc 8:32 0 120G 0 disk
sdd 8:48 0 150G 0 disk
sr0 11:0 1 1024M 0 rom
hana-1:/install #
```

Auf jedem der drei neuen Festplatten wurde ein xfs-Dateisystem erstellt.

```
hana-1:/install # mkfs.xfs /dev/sdb
meta-data=/dev/sdb isize=512 agcount=4, agsize=7864320 blks
sectsz=512 attr=2, projid32bit=1
crc=1 finobt=1, sparse=1, rmapbt=0
reflink=0 bigtime=0 inobtcount=0
data = bsize=4096 blocks=31457280, imaxpct=25
sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=15360, version=2
sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0

hana-1:/install # mkfs.xfs /dev/sdc
meta-data=/dev/sdc isize=512 agcount=4, agsize=7864320 blks
sectsz=512 attr=2, projid32bit=1
crc=1 finobt=1, sparse=1, rmapbt=0
reflink=0 bigtime=0 inobtcount=0
data = bsize=4096 blocks=31457280, imaxpct=25
sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=15360, version=2
sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0

hana-1:/install # mkfs.xfs /dev/sdd
meta-data=/dev/sdd isize=512 agcount=4, agsize=9830400 blks
sectsz=512 attr=2, projid32bit=1
crc=1 finobt=1, sparse=1, rmapbt=0
reflink=0 bigtime=0 inobtcount=0
data = bsize=4096 blocks=39321600, imaxpct=25
sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=19200, version=2
sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0
hana-1:/install #
```

Erstellung von Bereitstellungspunkten

```
hana-1:/ # mkdir -p /hana/data/SMA/mnt00001
hana-1:/ # mkdir -p /hana/log/SMA/mnt00001
hana-1:/ # mkdir -p /hana/shared
hana-1:/ # chmod –R 777 /hana/log/SMA
hana-1:/ # chmod –R 777 /hana/data/SMA
hana-1:/ # chmod -R 777 /hana/shared
```

Konfiguration von /etc/fstab

```
hana-1:/install # cat /etc/fstab
/dev/system/root / btrfs defaults 0 0
/dev/system/root /var btrfs subvol=/@/var 0 0
/dev/system/root /usr/local btrfs subvol=/@/usr/local 0 0
/dev/system/root /tmp btrfs subvol=/@/tmp 0 0
/dev/system/root /srv btrfs subvol=/@/srv 0 0
/dev/system/root /root btrfs subvol=/@/root 0 0
/dev/system/root /opt btrfs subvol=/@/opt 0 0
/dev/system/root /home btrfs subvol=/@/home 0 0
/dev/system/root /boot/grub2/x86_64-efi btrfs subvol=/@/boot/grub2/x86_64-
efi 0 0
/dev/system/root /boot/grub2/i386-pc btrfs subvol=/@/boot/grub2/i386-pc 0
0
/dev/system/swap swap swap defaults 0 0
/dev/system/root /.snapshots btrfs subvol=/@/.snapshots 0 0
UUID=2E8C-48E1 /boot/efi vfat utf8 0 2
/dev/sdb /hana/data/SMA/mnt00001 xfs relatime,inode64 0 0
/dev/sdc /hana/log/SMA/mnt00001 xfs relatime,inode64 0 0
/dev/sdd /hana/shared xfs defaults 0 0
hana-1:/install #

hana-1:/install # df -h
Filesystem Size Used Avail Use% Mounted on
devtmpfs 4.0M 8.0K 4.0M 1% /dev
tmpfs 49G 4.0K 49G 1% /dev/shm
tmpfs 13G 26M 13G 1% /run
tmpfs 4.0M 0 4.0M 0% /sys/fs/cgroup
/dev/mapper/system-root 60G 35G 25G 58% /
/dev/mapper/system-root 60G 35G 25G 58% /.snapshots
/dev/mapper/system-root 60G 35G 25G 58% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 35G 25G 58% /boot/grub2/x86_64-efi
/dev/mapper/system-root 60G 35G 25G 58% /home
/dev/mapper/system-root 60G 35G 25G 58% /opt
/dev/mapper/system-root 60G 35G 25G 58% /srv
/dev/mapper/system-root 60G 35G 25G 58% /tmp
/dev/mapper/system-root 60G 35G 25G 58% /usr/local
/dev/mapper/system-root 60G 35G 25G 58% /var
/dev/mapper/system-root 60G 35G 25G 58% /root
/dev/sda1 253M 5.1M 247M 3% /boot/efi
tmpfs 6.3G 56K 6.3G 1% /run/user/0
/dev/sdb 200G 237M 200G 1% /hana/data/SMA/mnt00001
/dev/sdc 120G 155M 120G 1% /hana/log/SMA/mnt00001
/dev/sdd 150G 186M 150G 1% /hana/shared
hana-1:/install #
```

HANA-Installation

Die HANA-Installation kann nun ausgeführt werden.

> Bei der beschriebenen Konfiguration befindet sich das Verzeichnis /usr/sap/SMA auf der OS VMDK. Wenn /usr/sap/SMA in der gemeinsam genutzten VMDK gespeichert werden soll, kann der gemeinsam genutzte hana-Datenträger partitioniert werden, um ein weiteres Dateisystem für /usr/sap/SMA bereitzustellen.

Userstore-Schlüssel für SnapCenter

Es muss ein Benutzerspeicher für einen Systemdatenbankbenutzer erstellt werden, der von SnapCenter verwendet werden soll. Die HANA-Instanznummer muss für den Kommunikations-Port entsprechend festgelegt werden. In unserem Setup wird die Instanznummer „00“ verwendet.

Eine ausführlichere Beschreibung finden Sie unter "Ressourcenspezifische SnapCenter Konfiguration für SAP HANA Datenbank-Backups"

```
smaadm@hana-1:/usr/sap/SMA/HDB00> hdbuserstore set SMAKEY hana-1:30013
SNAPCENTER <password>
Operation succeed.
```

Die Konnektivität kann mit dem folgenden Befehl überprüft werden.

```
smaadm@hana-1:/usr/sap/SMA/HDB00> hdbsql -U SMAKEY
Welcome to the SAP HANA Database interactive terminal.
Type: \h for help with commands
\q to quit
hdbsql SYSTEMDB=> exit
smaadm@hana-1:/usr/sap/SMA/HDB00
```

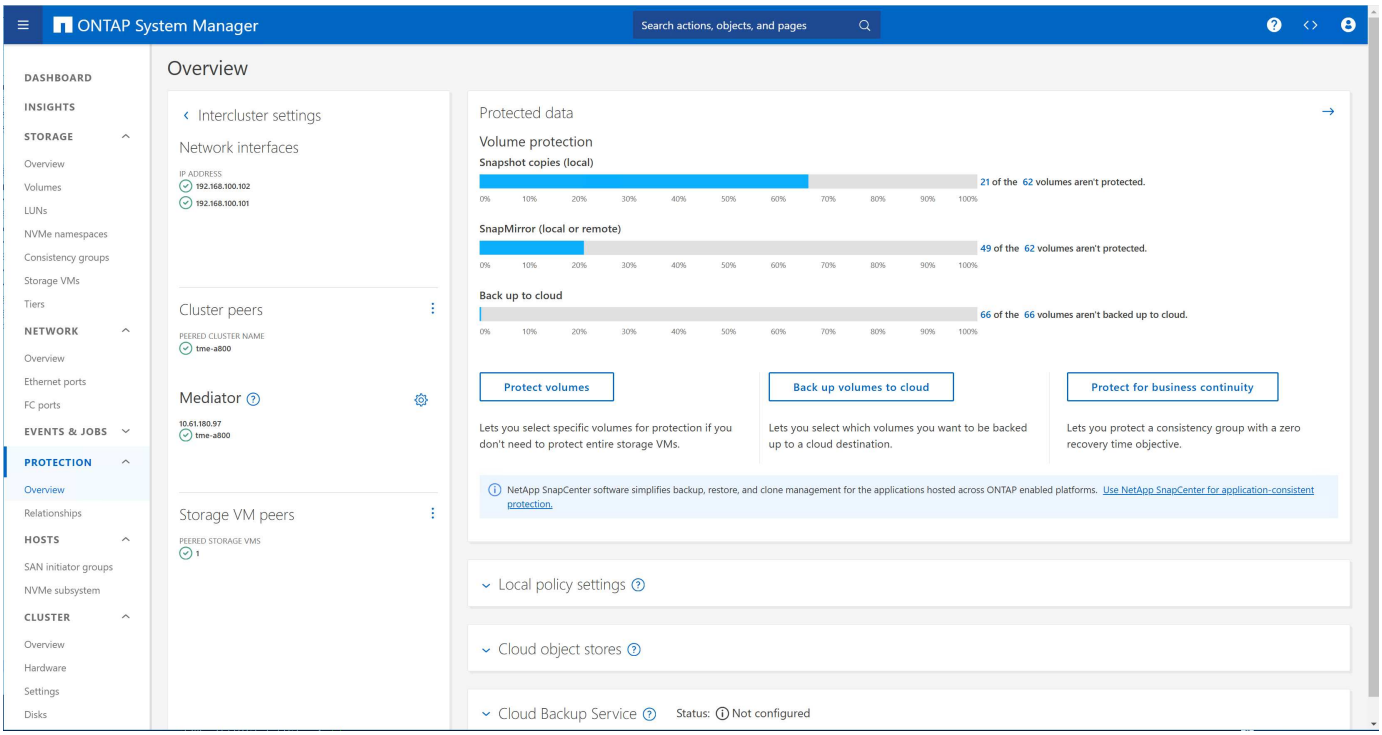
Konfiguration der aktiven SnapMirror-Synchronisierung

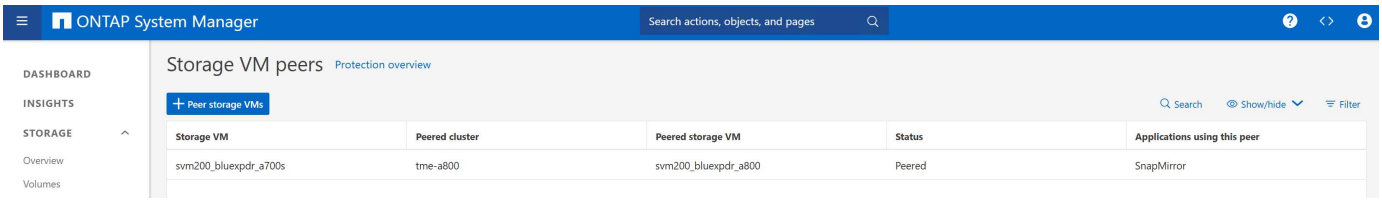
In diesem Artikel werden die für diese Lösung erforderlichen Konfigurationsschritte beschrieben.

Voraussetzungen

Storage-Cluster und relevante SVMs müssen aktiviert werden.

Der ONTAP Mediator muss auf beiden Storage-Clustern verfügbar und konfiguriert sein.





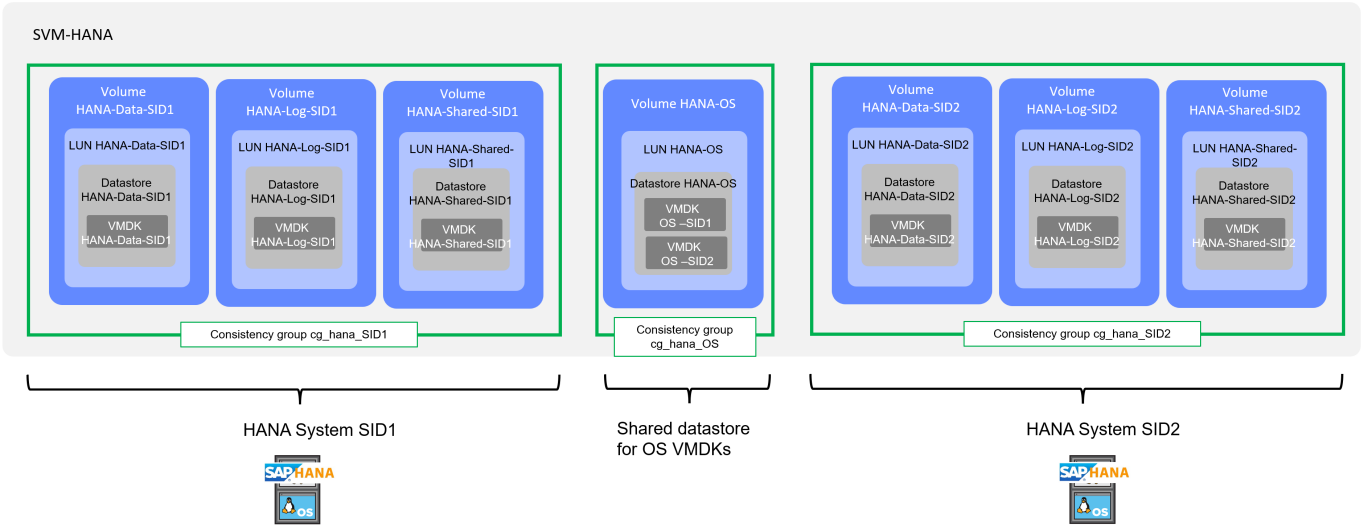
Konfiguration von Storage-Layout und Konsistenzgruppen

In der ONTAP-Dokumentation "Übersicht über die aktive SnapMirror-Synchronisierung in ONTAP" wird das Konzept der Konsistenzgruppen mit SnapMirror Active Sync wie folgt beschrieben:

Eine Konsistenzgruppe ist eine Sammlung von FlexVol Volumes, die eine Konsistenzgarantie für den Applikations-Workload bietet, der für Business Continuity geschützt werden muss.

Der Zweck einer Konsistenzgruppe besteht darin, gleichzeitige Snapshot Images mehrerer Volumes zu erstellen. Auf diese Weise wird sichergestellt, dass absturzkonsistente Kopien einer Sammlung von Volumes zu einem Zeitpunkt erstellt werden. Eine Konsistenzgruppe stellt sicher, dass alle Volumes eines Datensatzes stillgelegt und dann zu genau dem gleichen Zeitpunkt eingerastet werden. So erhalten Sie einen datenkonsistenten Restore-Zeitpunkt über Volumes hinweg, der den Datensatz unterstützt. Eine Konsistenzgruppe behält dabei die abhängige Konsistenz der Schreibreihenfolge bei. Wenn Sie Applikationen für Business Continuity schützen möchten, muss die Volume-Gruppe, die dieser Applikation entspricht, einer Konsistenzgruppe hinzugefügt werden, damit eine Datensicherungsbeziehung zwischen einer Quell- und einer Zielkonsistenzgruppe hergestellt wird. Die Quell- und Zielkonsistenz muss die gleiche Anzahl und den gleichen Typ von Volumes enthalten.

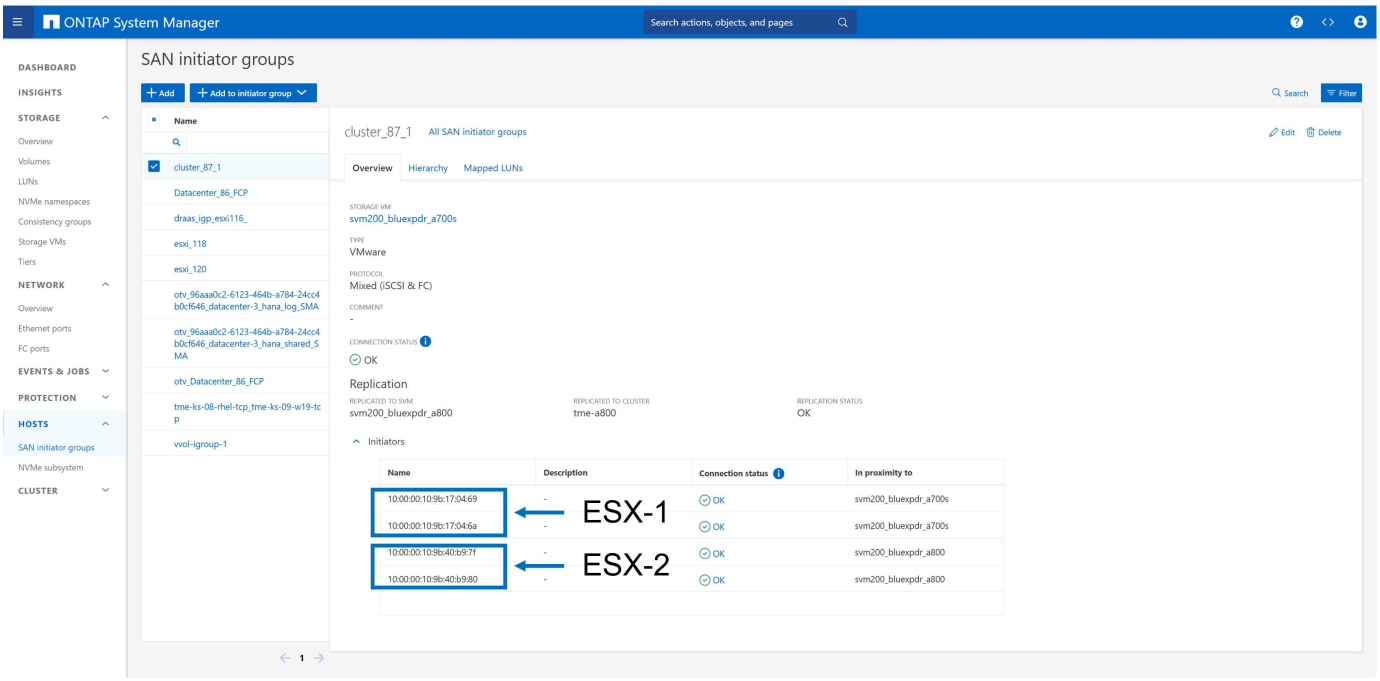
Für die Replizierung von HANA-Systemen muss die Konsistenzgruppe alle Volumes enthalten, die vom einzelnen HANA-System verwendet werden (Daten, Protokoll und Shared). Volumes, die Teil einer Konsistenzgruppe sein sollten, müssen auf derselben SVM gespeichert werden. Betriebssystem-Images können auf einem separaten Volume mit einer eigenen Konsistenzgruppe gespeichert werden. Die Abbildung unten zeigt ein Konfigurationsbeispiel mit zwei HANA-Systemen.

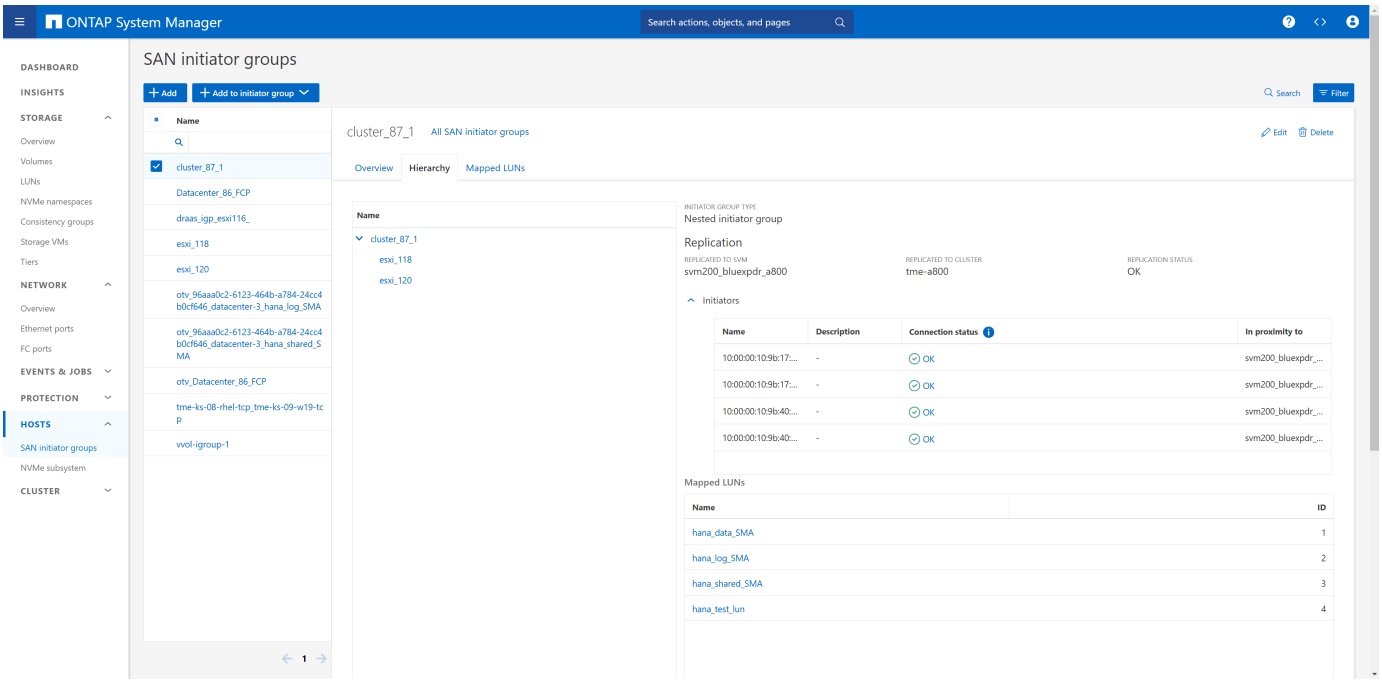


Konfiguration der Initiatorgruppe

In unserem Lab-Setup haben wir eine Initiatorgruppe erstellt, die beide Storage-SVMs für die aktive synchrone Replizierung mit SnapMirror verwendet. In der später beschriebenen Konfiguration für aktive SnapMirror-Synchronisierung wird festgelegt, dass die Initiatorgruppe Teil der Replizierung ist.

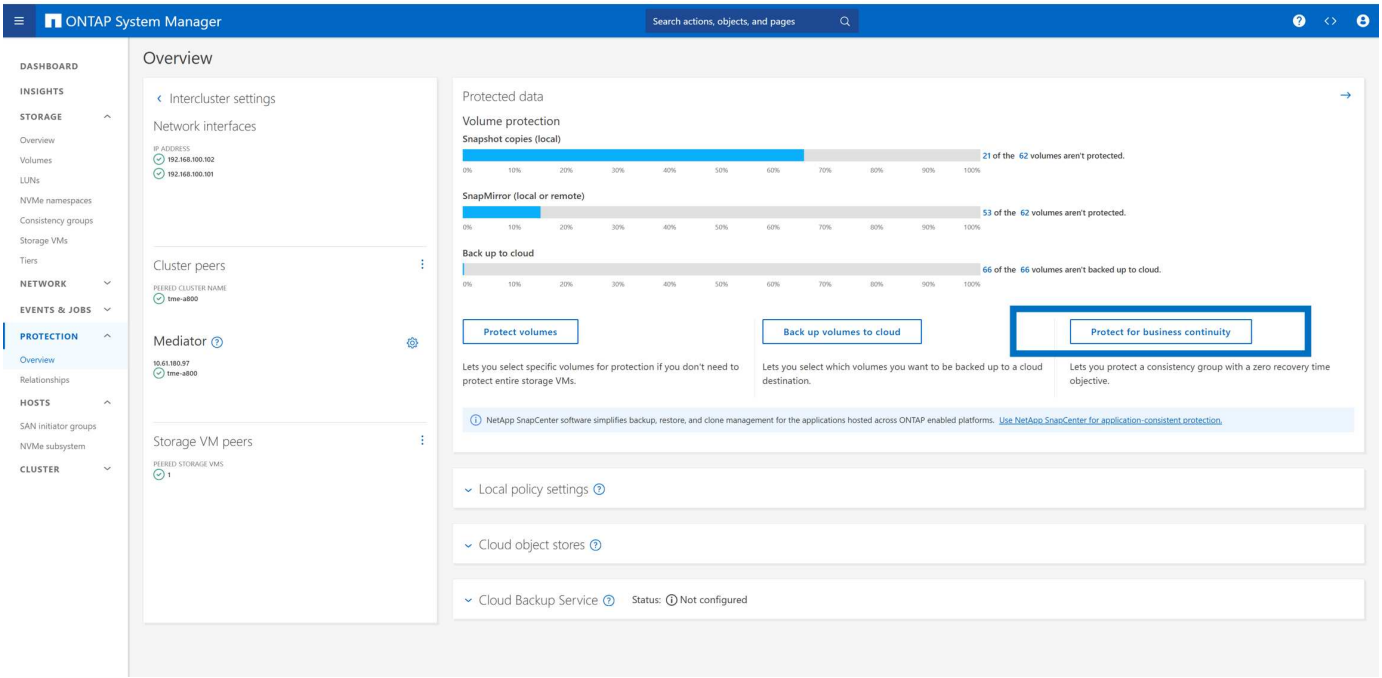
Mithilfe der Annäherungseinstellungen wurde festgelegt, welcher ESX Host sich in der Nähe des Storage-Clusters befindet. In unserem Fall liegt die A700 in der Nähe von ESX-1 und die A800 ist nah an ESX-2.





In einem nicht einheitlichen Access Setup darf die Initiatorgruppe im primären Storage-Cluster (A700) nur die Initiatoren des ESX-1-Hosts einschließen, da es keine SAN-Verbindung zu ESX-2 gibt. Darüber hinaus müssen Sie eine andere Initiatorgruppe auf dem zweiten Storage-Cluster (A800) konfigurieren, der nur die Initiatoren des ESX-2 Hosts enthalten. Die Proximity-Konfiguration und die Replizierung von Initiatorgruppen sind nicht erforderlich.

Konfigurieren Sie den Schutz mit ONTAP System Manager

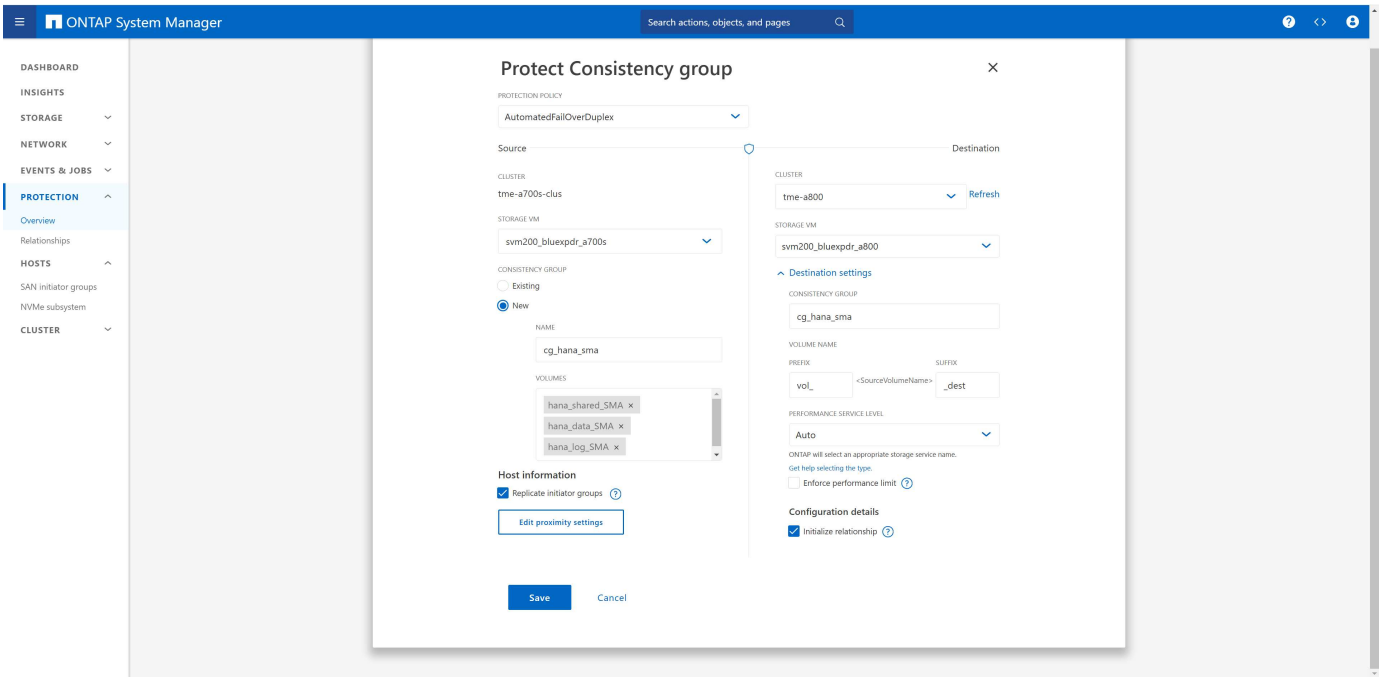


Replizierung von Konsistenzgruppen und Initiatorgruppen

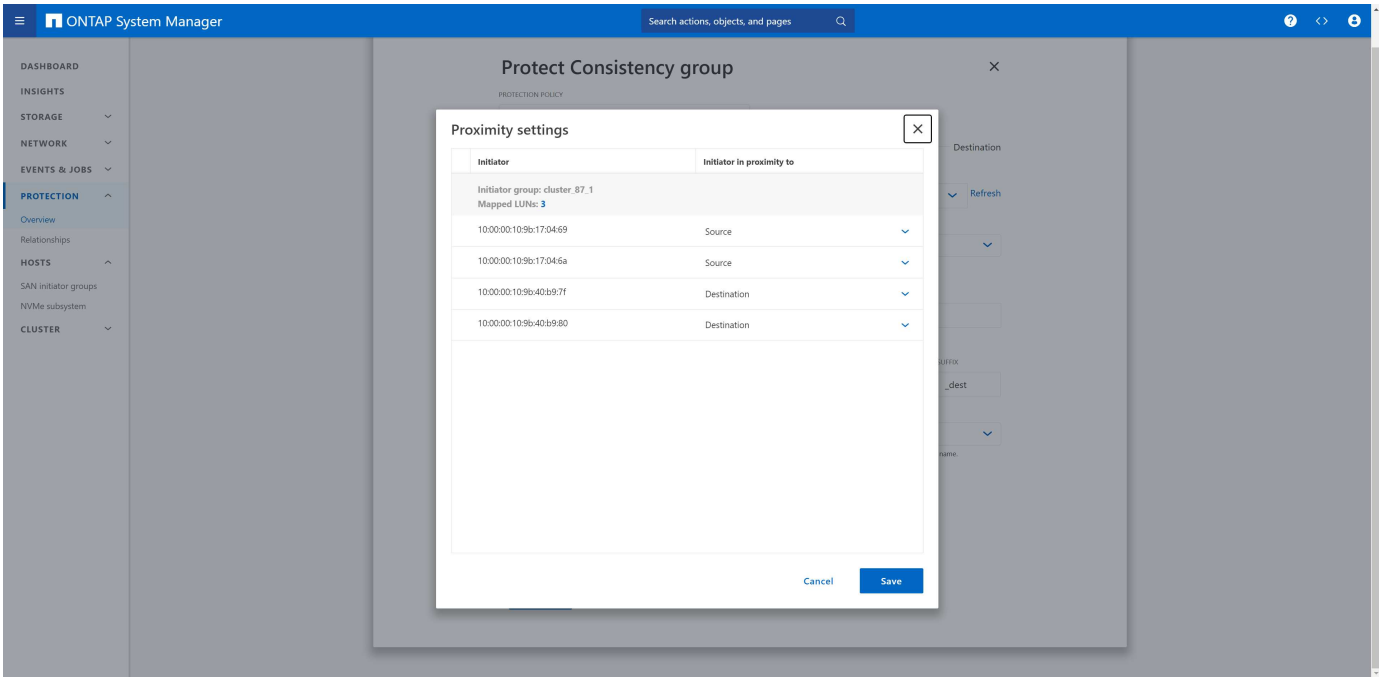
Eine neue Konsistenzgruppe muss erstellt werden, und alle drei LUNs des HANA-Systems müssen der Konsistenzgruppe hinzugefügt werden.

„Initiatorgruppe replizieren“ wurde aktiviert. Die Imitatorgruppe bleibt dann unabhängig, wo Änderungen vorgenommen werden.

In einer nicht einheitlichen Zugriffseinrichtung darf die Initiatorgruppe nicht repliziert werden, da auf dem zweiten Storage-Cluster eine separate Initiatorgruppe konfiguriert werden muss.



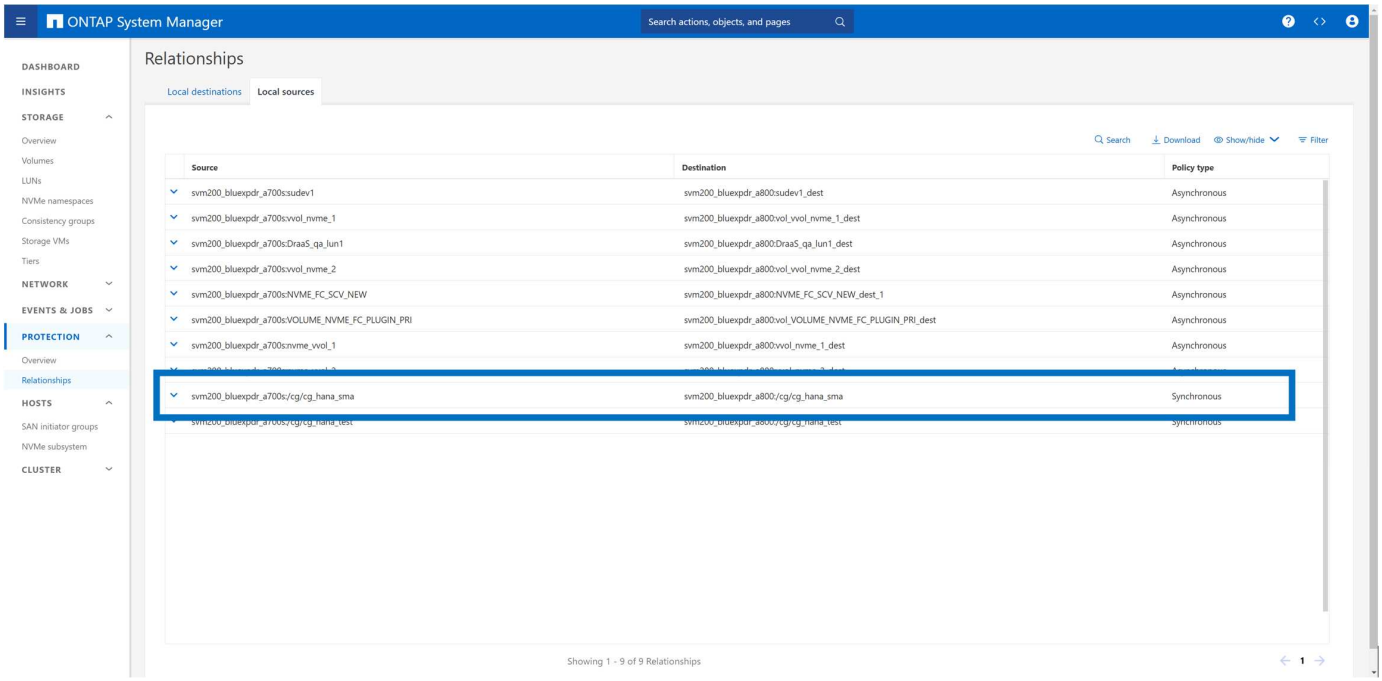
Indem Sie auf „Annäherungseinstellungen“ klicken, können Sie die zuvor im Setup der Initiatorgruppe vorgenommenen Konfigurationen überprüfen.



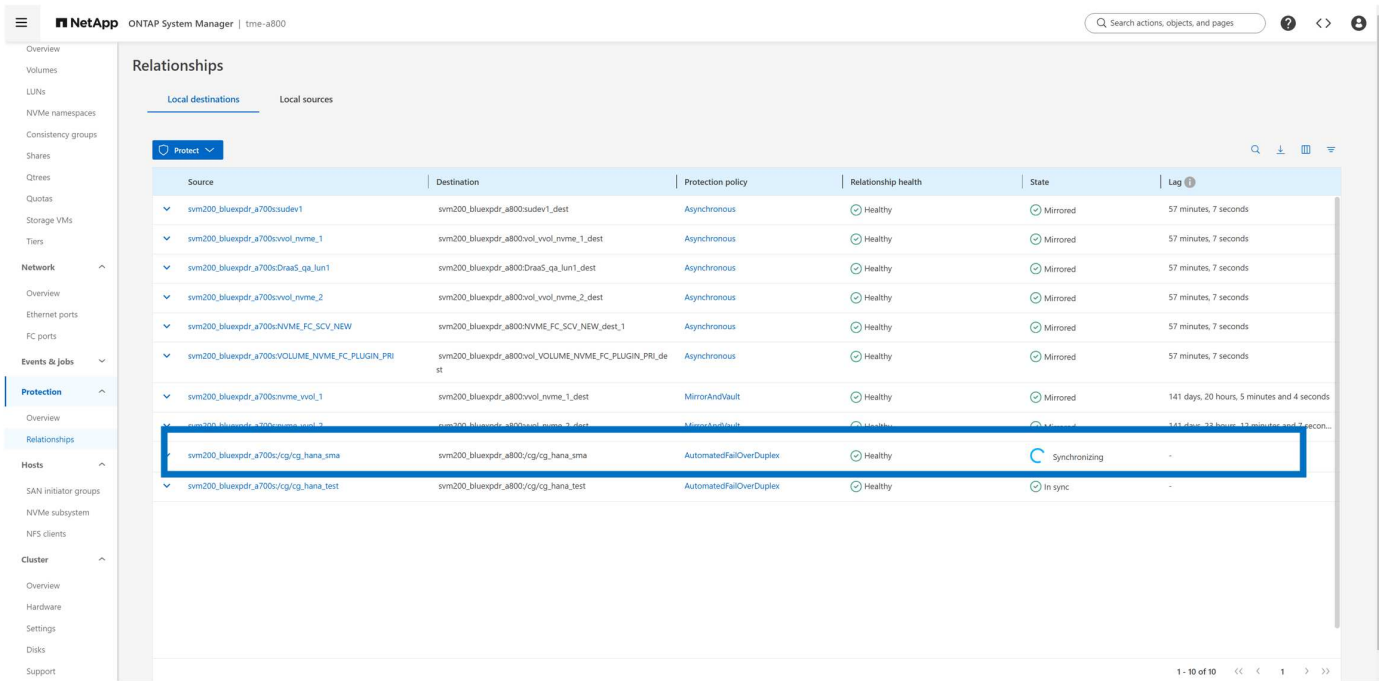
Der Ziel-Storage-Cluster muss konfiguriert und die „Initialisierungsbeziehung“ aktiviert sein.

Synchronisierung

Bei dem A700 Storage-Cluster (Quelle) ist die neue Beziehung jetzt aufgelistet.



Am A800 Storage-Cluster (Ziel) werden die neue Beziehung und der Status der Replizierung aufgeführt.



Infrastrukturdatenspeicher

Der Datastore, in dem die OS-Images des HANA-Systems, SnapCenter und das vSphere Plug-in gespeichert werden, wird in der gleichen Weise repliziert wie bei den HANA-Datenbankdatenspeichern beschrieben.

Primärer Standort

Das aktive Synchronisierungsverhalten von SnapMirror ist symmetrisch, mit einer wichtigen Ausnahme: Konfiguration des primären Standorts.

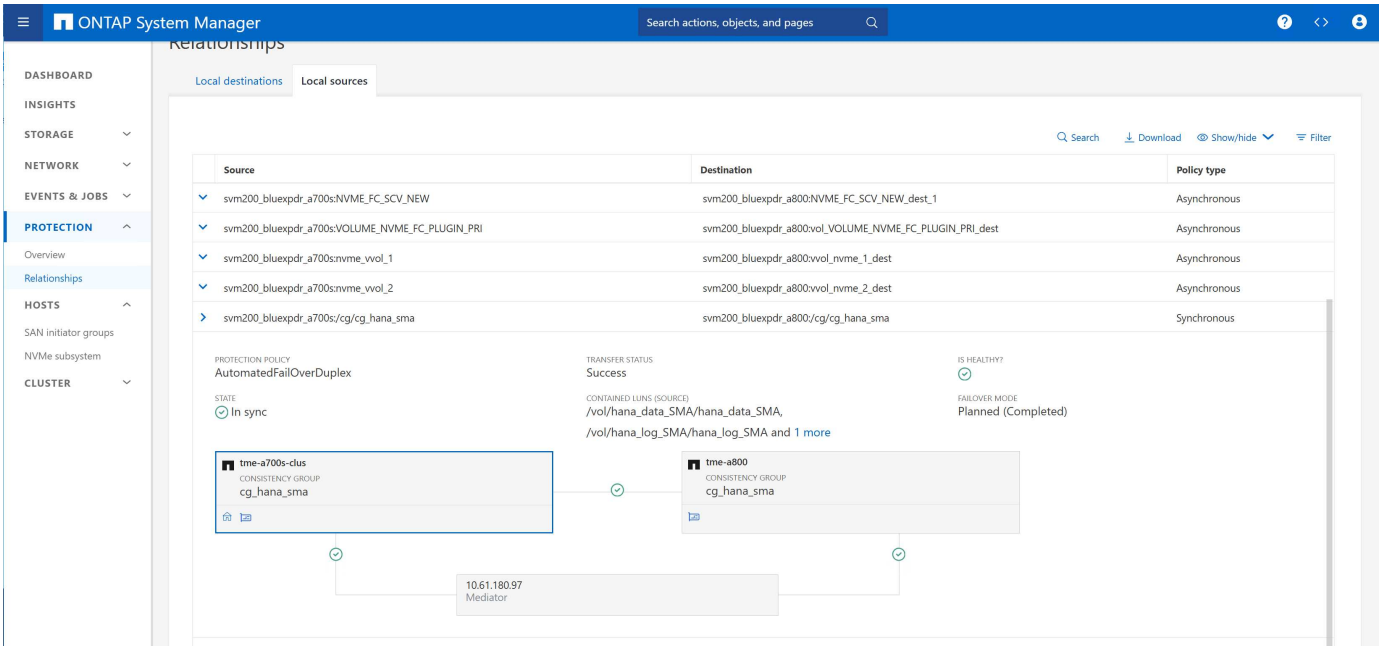
SnapMirror Active Sync betrachtet einen Standort als „Quelle“ und den anderen als „Ziel“. Dies impliziert eine One-Way-Replikationsbeziehung, aber dies gilt nicht für das IO-Verhalten. Die Replizierung ist bidirektional und symmetrisch, und die I/O-Reaktionszeiten sind auf beiden Seiten der Spiegelung identisch.

Wenn die Replikationsverbindung verloren geht, stellen die LUN-Pfade auf der Quellkopie weiterhin Daten bereit, während die LUN-Pfade auf der Zielkopie erst dann nicht mehr verfügbar sind, wenn die Replikation wiederhergestellt ist und SnapMirror wieder in den synchronen Zustand wechselt. Die Pfade setzen dann das Bereitstellen von Daten fort.

Der Effekt der Festlegung eines Clusters als Quelle steuert einfach, welches Cluster als Lese-/Schreib-Speichersystem überlebt, wenn die Replikationsverbindung verloren geht.

Der primäre Standort wird von SnapCenter erkannt und zur Durchführung von Backup-, Wiederherstellungs- und Klonvorgängen verwendet.

Beachten Sie, dass Quelle und Ziel nicht an SVM oder Storage-Cluster gebunden sind, sondern für jede Replizierungsbeziehung unterschiedlich sein können.



SnapCenter-Konfiguration

Wie bereits zu Beginn des Dokuments erwähnt, dient das Dokument dazu, Best Practices für eine HANA-Umgebung mit VMware mit VMFS und SnapMirror Active Sync bereitzustellen. Wir behandeln nur Details und wichtige Schritte, die für diese spezifische Lösung relevant sind, und erläutern die allgemeinen SnapCenter-Konzepte nicht. Diese Konzepte und weitere Informationen zu SnapCenter finden Sie unter:

"TR-4614: SAP HANA Backup und Recovery mit SnapCenter"

"TR-4719: SAP HANA System Replication – Backup und Recovery mit SnapCenter"

"TR-4667: Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter"

Voraussetzungen

Im Allgemeinen sollte SnapMirror Active Sync eingerichtet werden, bevor die geschützten Ressourcen zu SnapCenter hinzugefügt werden. Wenn Backups vor der Einrichtung von SnapMirror Active Sync erstellt wurden, sind sie nur im ursprünglichen primären Speicher vorhanden und werden danach nicht repliziert.

Die SnapCenter HANA-Ressource muss automatisch erkannt werden

Ressourcen, die mit VMware VMFS oder mit SnapMirror Active Sync geschützten Ressourcen konfiguriert sind, müssen automatisch von SnapCenter erkannt werden, damit bestimmte Vorgänge für diese Konfigurationen möglich sind.

Da HANA-nicht-Daten-Volumes immer manuell konfigurierte Ressourcen in SnapCenter sind, werden sie nicht von SnapCenter out of the box unterstützt. Im weiteren Verlauf dieses Dokuments besprechen wir Optionen und Problemumgehungen für nicht-Datenvolumes.

SAP HANA mehrere Hostsysteme müssen über ein zentrales HANA-Plugin konfiguriert werden und sind daher standardmäßig manuell konfigurierte Ressourcen. Solche HANA-Systeme werden von SnapCenter nicht unterstützt, wenn VMware VMFS oder SnapMirror Active Sync verwendet wird.

SnapCenter für VMware vSphere-Plugin

Das SnapCenter für VMware vSphere Plug-in muss in der VMware Umgebung implementiert werden.

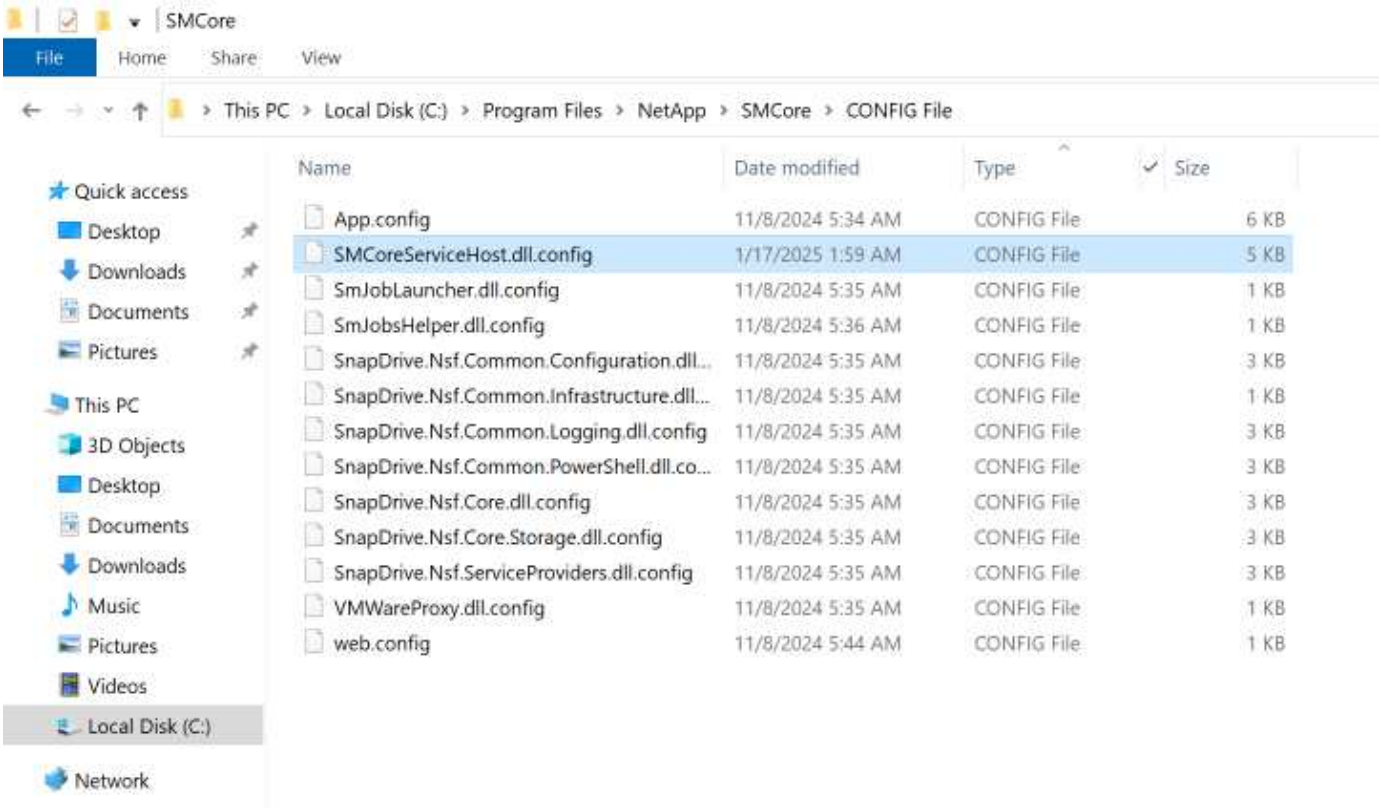
Management-IP-Adresse auf der SVM, die die Volumes hostet

Obwohl SnapCenter Cluster hinzugefügt werden, muss für die SVMs, die die Quell- und Ziel-Volumes hosten, eine Management-IP-Adresse konfiguriert sein.

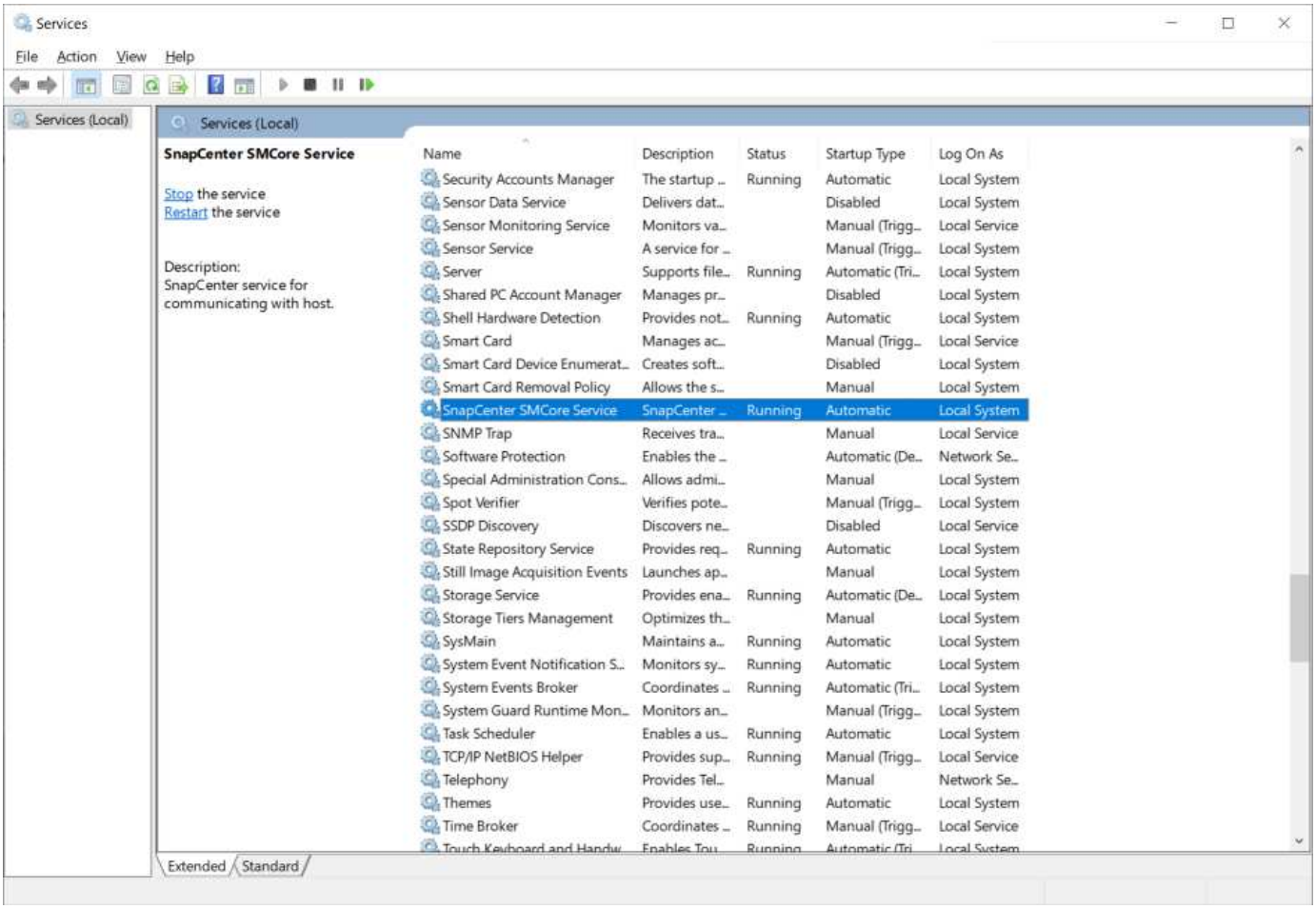
REST-APIs zur Storage-Kommunikation

Für das Management und die Überwachung der aktiven SnapMirror-Synchronisierung ist REST-API-Zugriff erforderlich. Daher muss SnapCenter so konfiguriert werden, dass es REST-APIs für Storage-Kommunikation verwendet. Der Parameter "IsRestEnabledForStorageConnection" in der Konfigurationsdatei + C:\Programme\NetApp++SMCore+\++SMCoreServiceHost.dll.config muss auf true gesetzt werden.

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

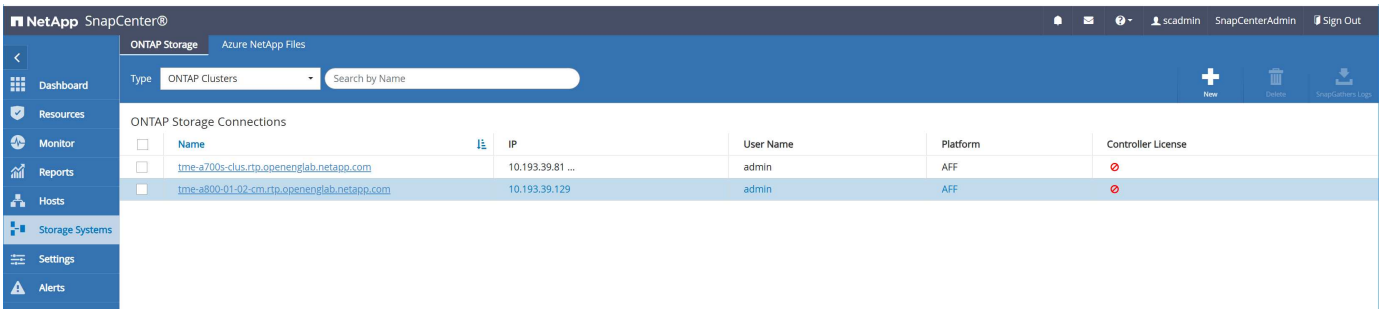


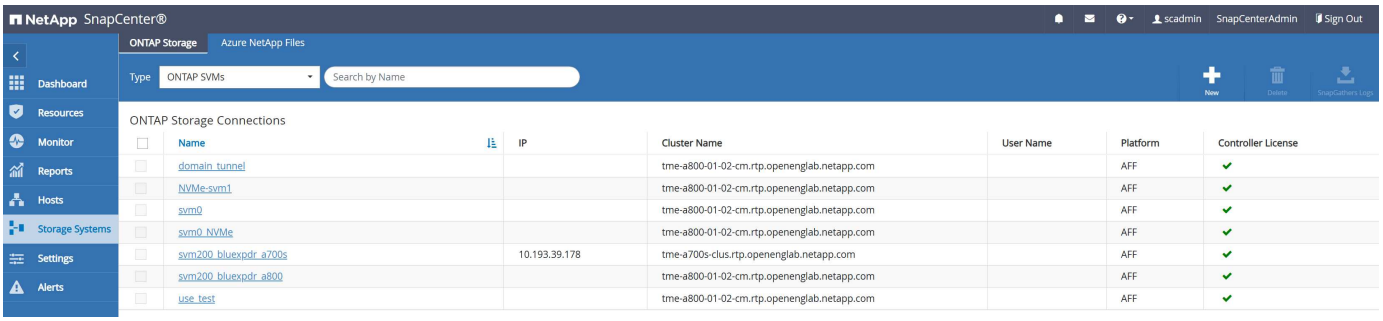
Nach der Parameteränderung muss der SnapCenter-SMCore-Dienst neu gestartet werden.



Storage-Systeme hinzufügen

Storage-Systeme können hinzugefügt werden, nachdem die REST-API für SnapCenter aktiviert ist. Es müssen nicht die einzelnen SVMs, sondern beide Storage-Cluster hinzugefügt werden.



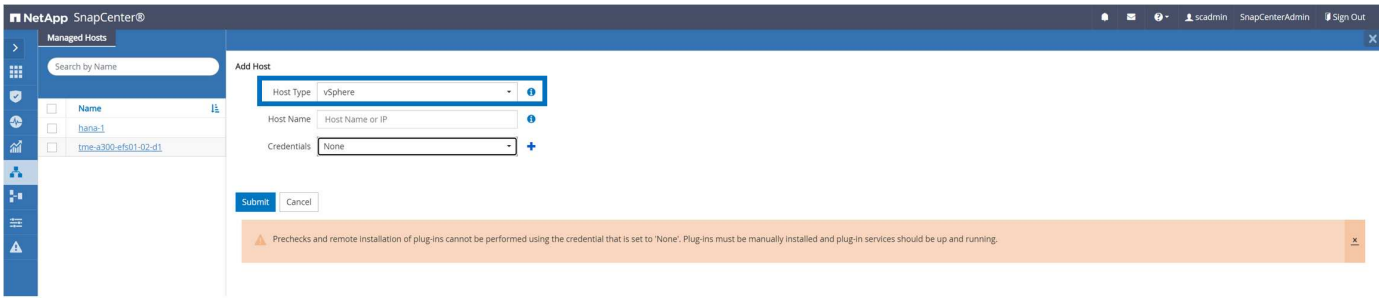


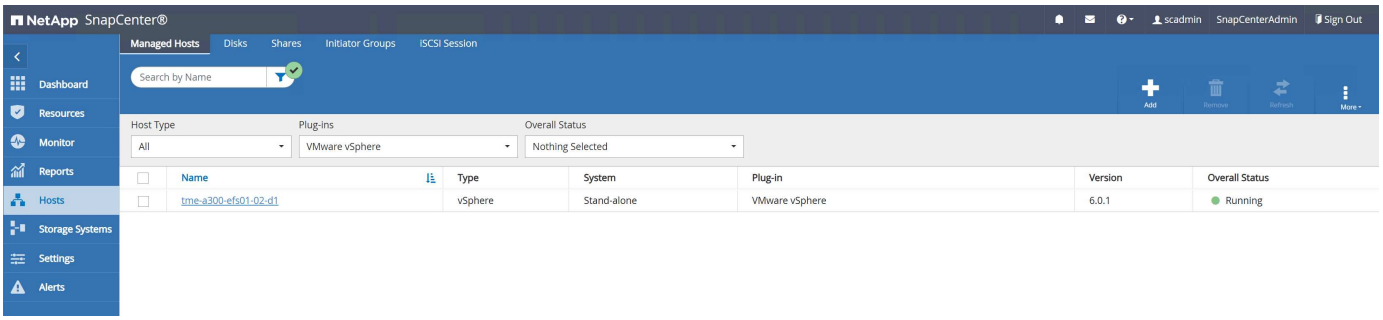
Host hinzufügen – SnapCenter für VMware vSphere Plug-in

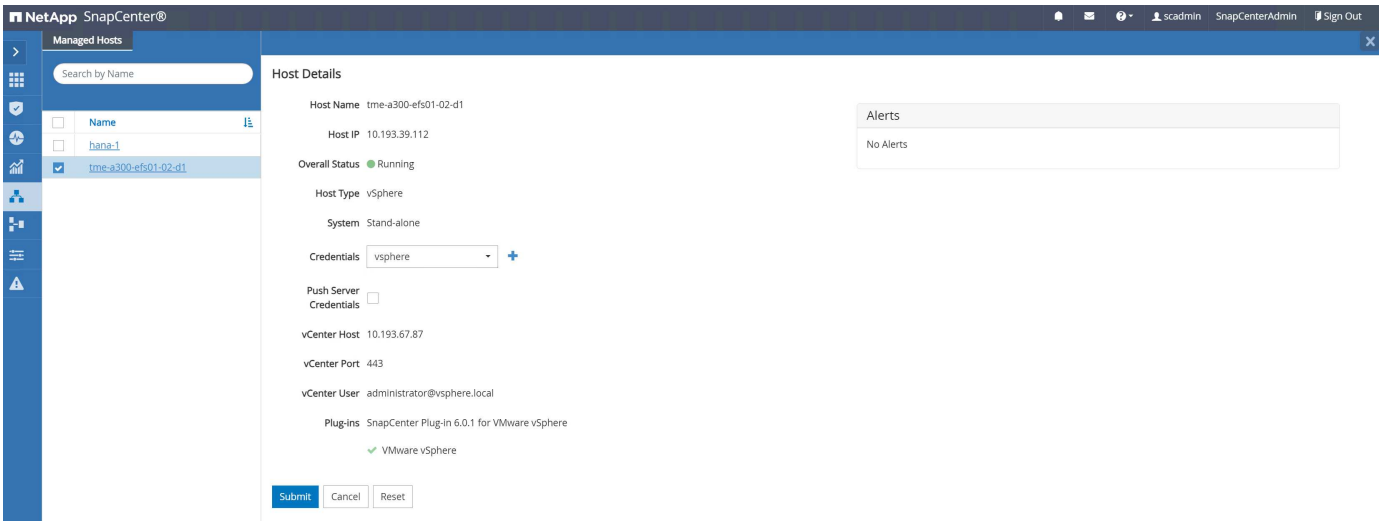
Wenn eine Ressource in SnapCenter in einer virtualisierten VMware Umgebung ausgeführt wird, nutzt SnapCenter das SnapCenter Plug-in für VMware vSphere, um die Backup-, Restore- und Klon-Workflows von SnapCenter mit den erforderlichen Schritten auf der VMware Ebene zu erweitern.

Bevor der Host in SnapCenter hinzugefügt werden kann, muss das SnapCenter Plug-in für VMware vSphere in der VMware Umgebung implementiert werden.

Die Anmeldeinformationen müssen während des Host-Add-Workflows festgelegt werden, wobei vSphere als Hosttyp ausgewählt werden kann.







Beim SnapCenter für vSphere Plugin selbst ist keine zusätzliche Konfiguration erforderlich.

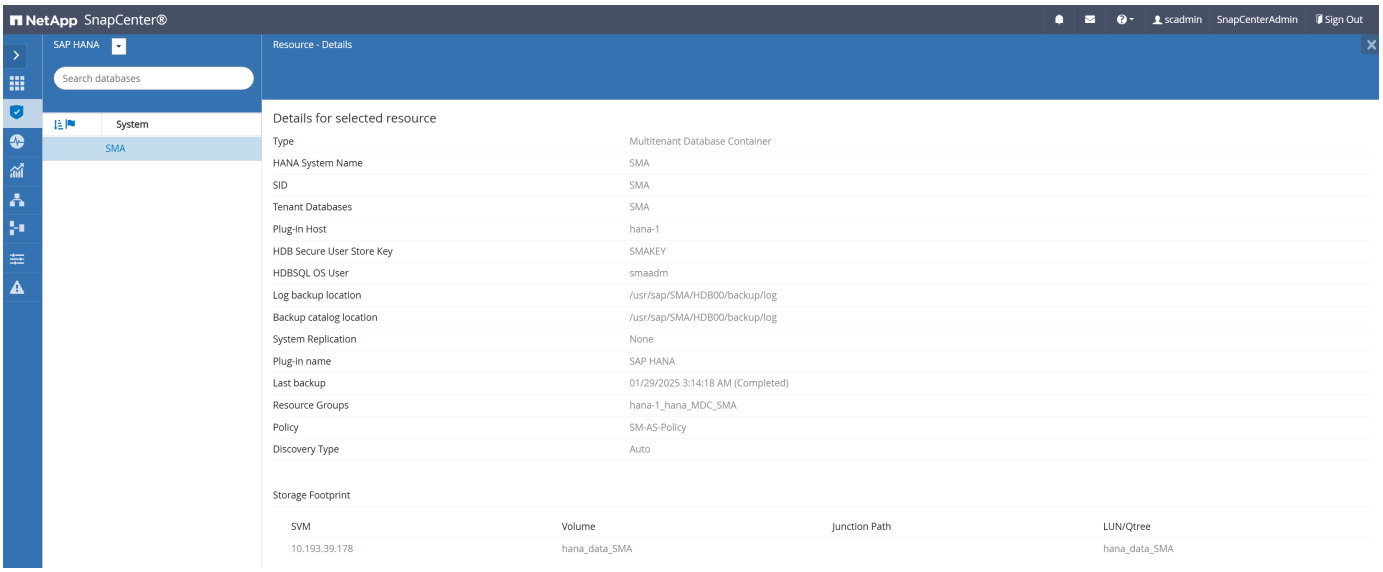
Host – HANA-System hinzufügen

Keine besonderen Anforderungen. Plugin-Bereitstellung und automatische Erkennung erfolgt wie gewohnt.

Durch den automatischen Erkennungsprozess erkennt SnapCenter, dass die HANA-Ressource virtualisiert mit VMFS/VMDKs ausgeführt wird. SnapCenter erkennt außerdem die SnapMirror Active Sync Einrichtung und identifiziert den aktuellen primären Standort.

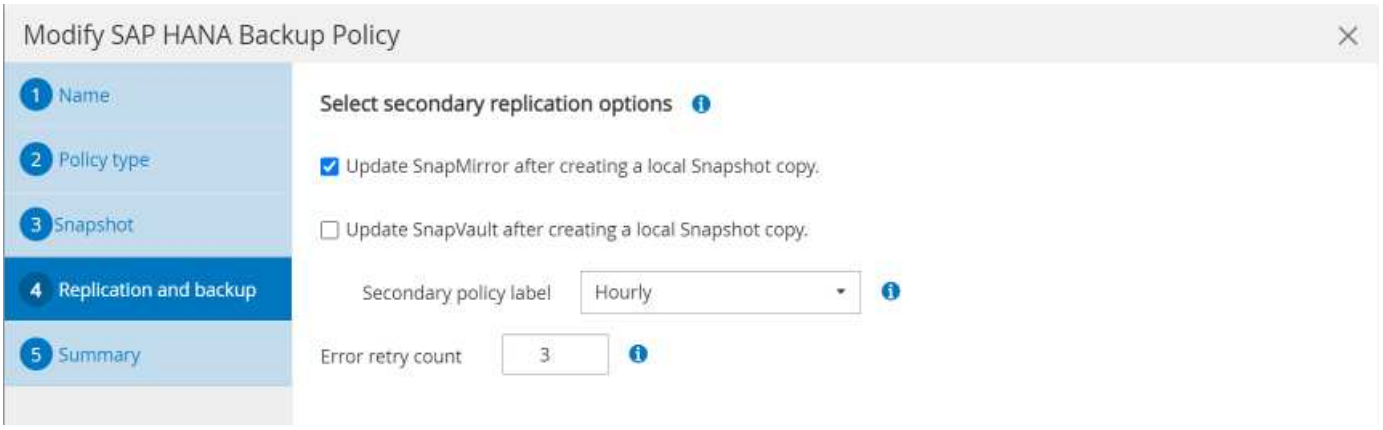
Nach der automatischen Ressourcenerkennung wird der aktuelle primäre Standort im Abschnitt Storage Footprint der Ressourcenansicht angezeigt. Die Erkennung, welches Storage-System Master ist, basiert auf der Ausgabe des Befehls ONTAP, der von SnapCenter verwendet wird.

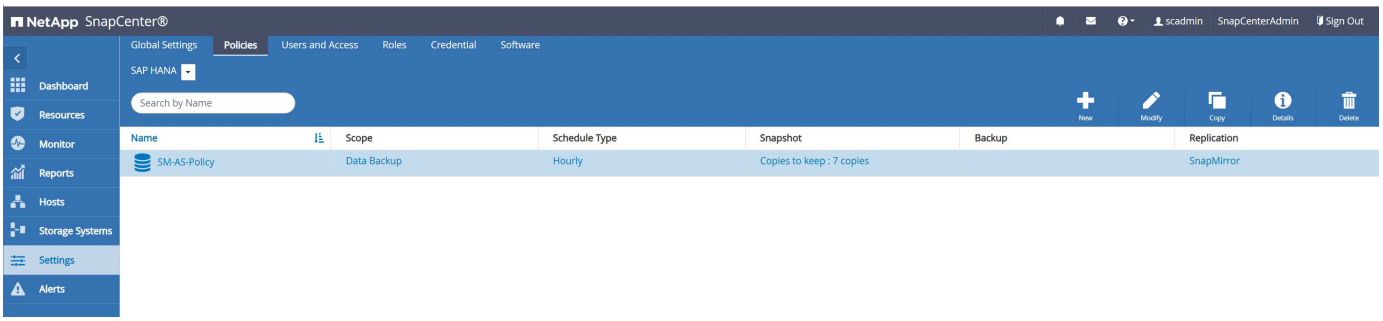
```
volume show -vserver <vs> -volume <vol> -fields smbc-consensus,is-smbc-
master
```



Konfiguration von Richtlinien

Die Richtlinie, die für die mit SnapMirror Active Sync geschützte Ressource verwendet wird, muss mithilfe der SnapMirror-Replizierung konfiguriert werden, auch wenn SnapCenter keine SnapMirror Update-Vorgänge auslöst.





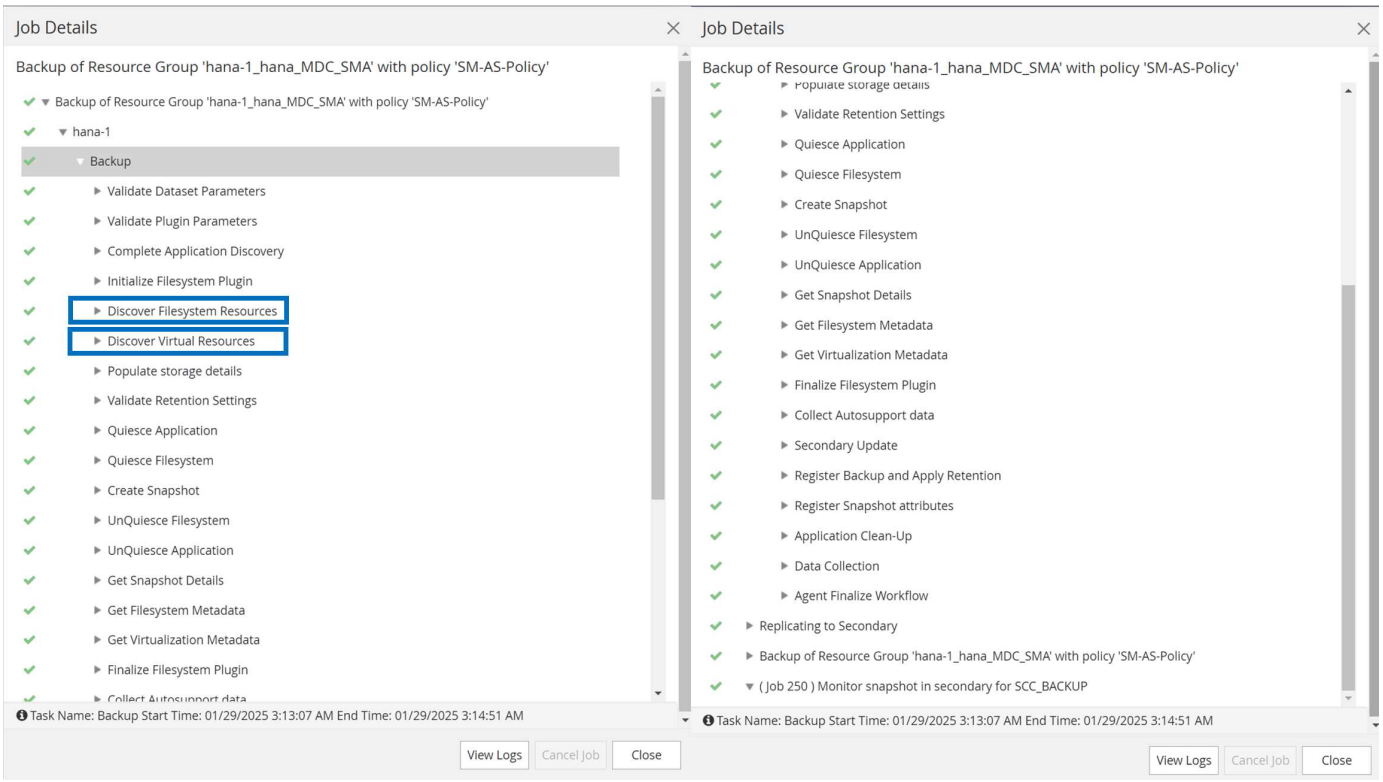
Konfiguration der HANA-Ressourcensicherung

Keine besonderen Anforderungen. Die Konfiguration des Ressourcenschutzes erfolgt wie gewohnt.

SnapCenter-Backup-Vorgänge

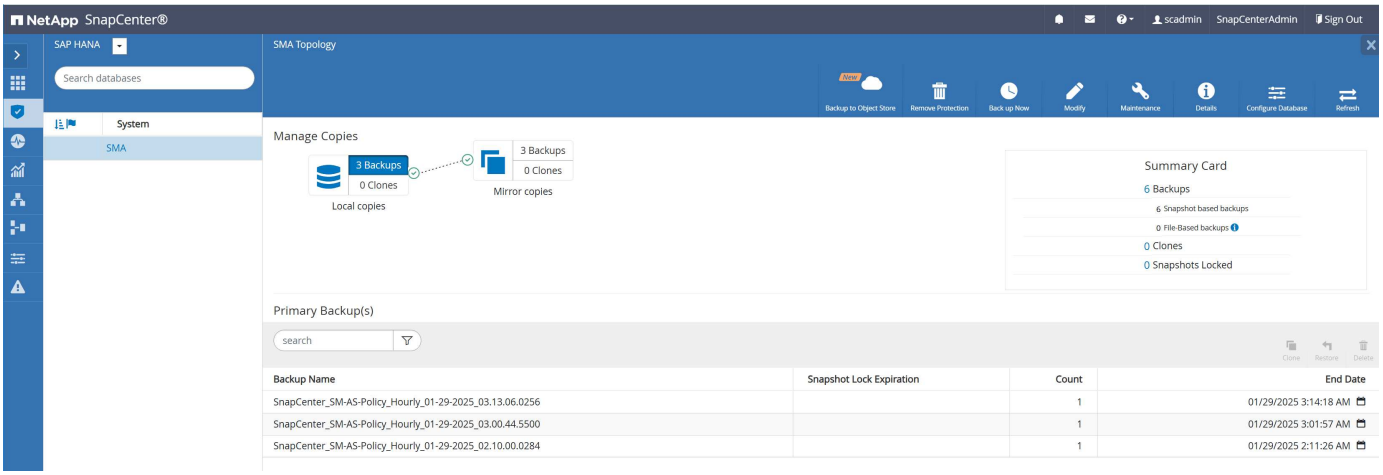
Bei jedem Backup-Vorgang führt SnapCenter die Erkennung auf VMware-Seite aus und

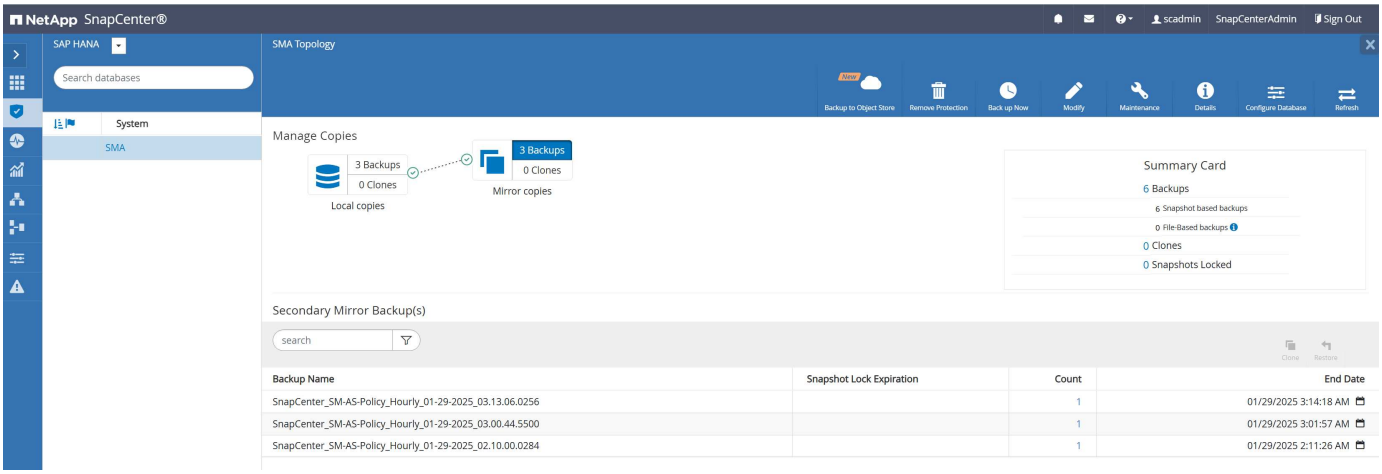
erkennt den primären Standort. Bei einem Storage-Failover erkennt SnapCenter den neuen primären Standort, sobald ein Backup für die Ressource ausgeführt wurde.



Topologieansicht

In der Topologieansicht zeigt SnapCenter die Backups sowohl des Quell- als auch des Ziel-Storage-Clusters.



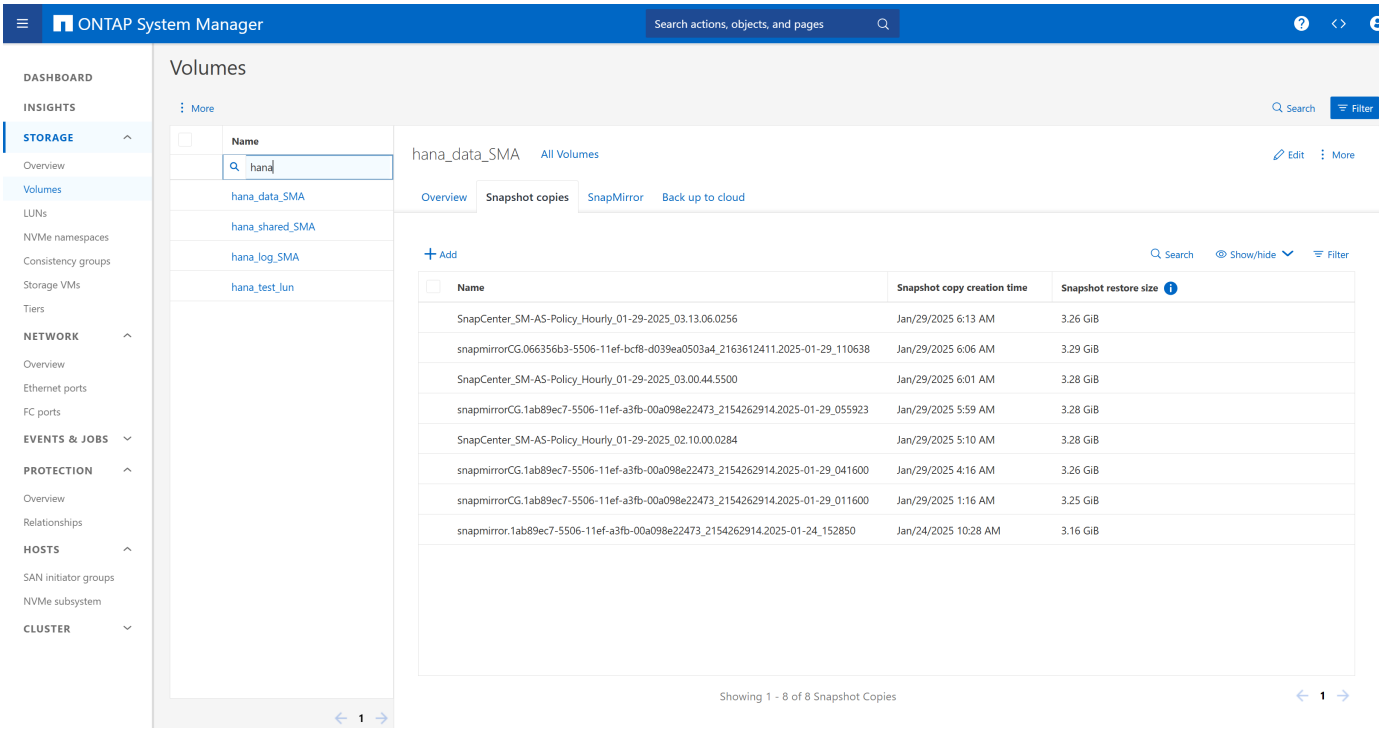


Durch Klicken auf die Zählzahl im sekundären Speicher wird die aktuelle Beziehung und Replikationsrichtung angezeigt. Die Quelle ist immer der aktuelle primäre Standort. Nach einem Speicher-Failover ändert sich der primäre Standort und die Anzeige wird entsprechend angepasst. Alle Backups verfügen immer über die gleiche Beziehung, je nach Speichersystem derzeit der primäre Standort ist.

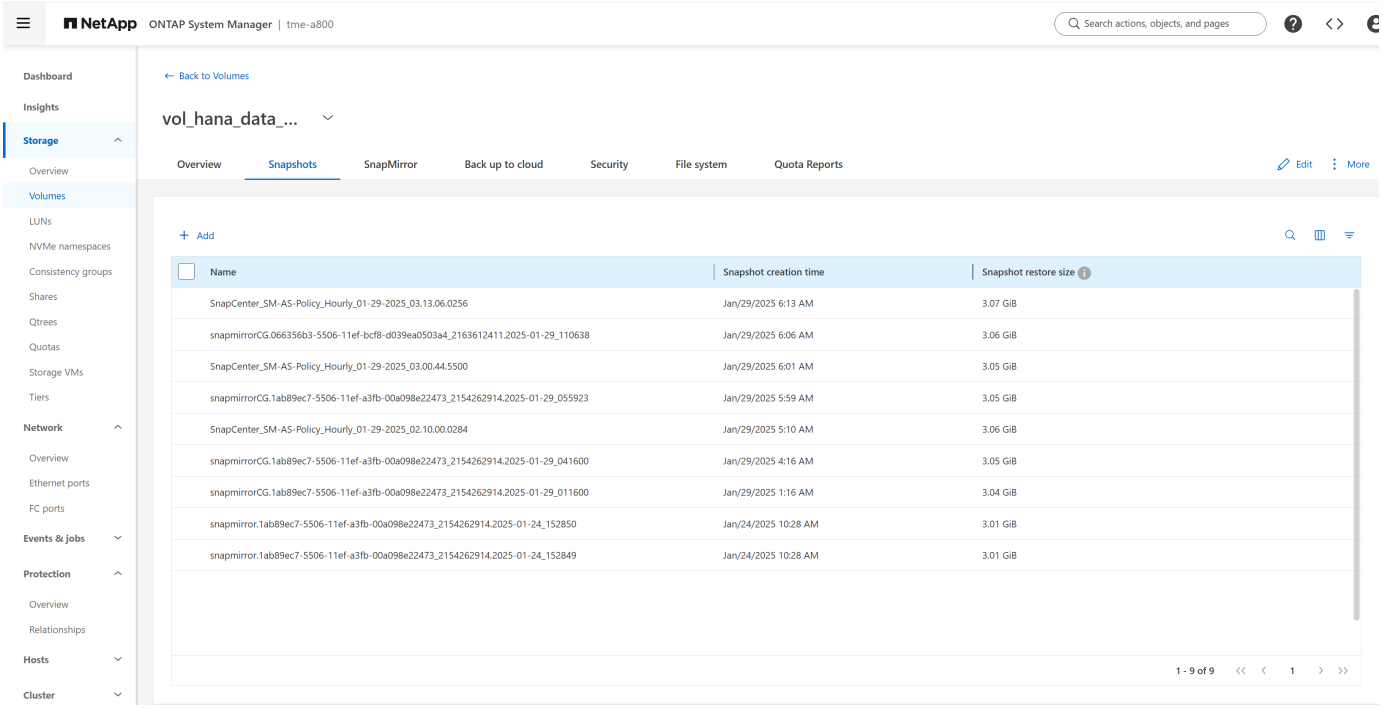
Snapshots auf Storage-Systemen

Die von SnapCenter erstellten Snapshot Backups sind bei beiden HANA Daten-Volumes auf beiden Storage-Systemen verfügbar. ONTAP erstellt zusätzliche Snapshots auf Konsistenzgruppenebene, die auch für alle anderen HANA-Volumes verfügbar sind.

Die Abbildung unten zeigt die Snapshots des HANA-Daten-Volumes beim A700-Cluster.



Die Abbildung unten zeigt die Snapshots des HANA-Daten-Volumes auf dem A800 Cluster.



SnapCenter Restore und Recovery

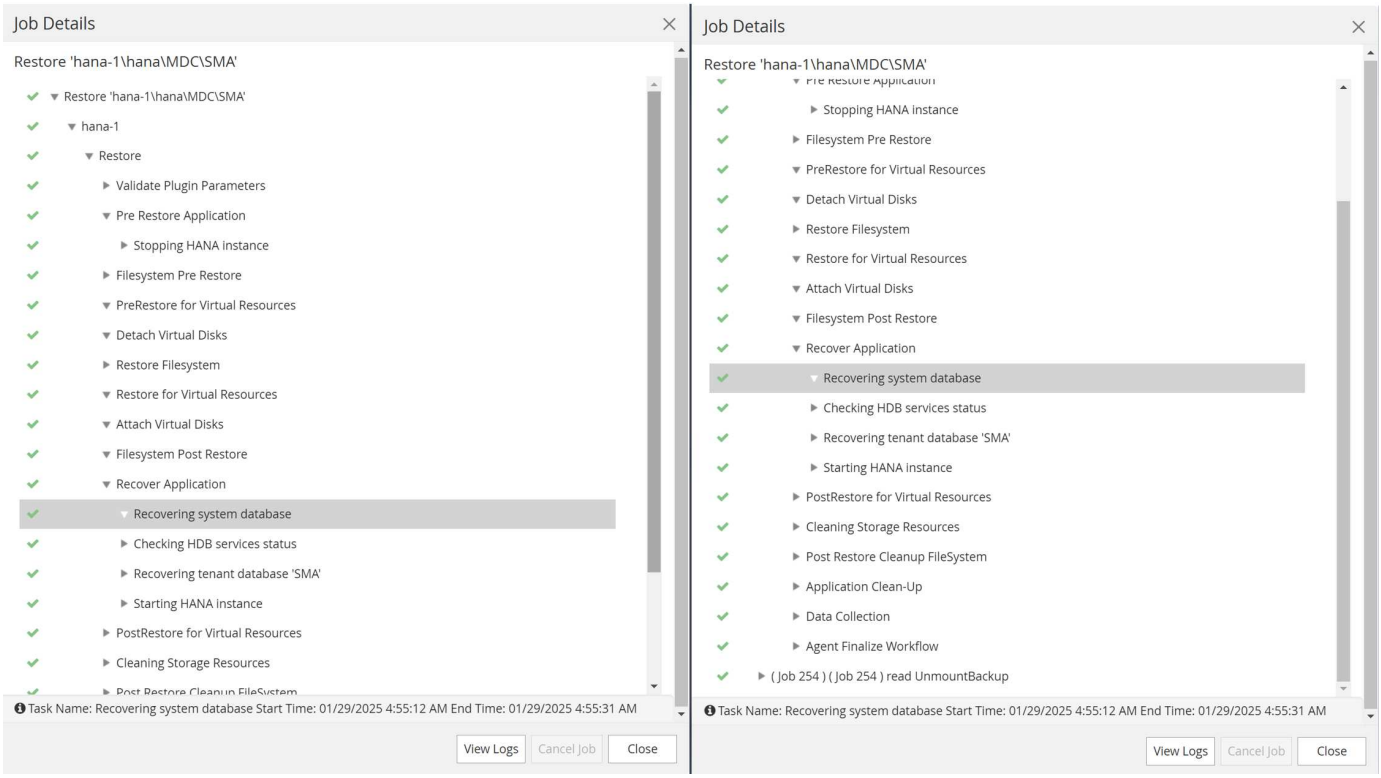
Wenn virtuelle Ressourcen auf VMFS/VMDK gespeichert sind, erfolgt eine SnapCenter-Wiederherstellung immer durch einen Klon-, Mount- und Kopiervorgang.

1. SnapCenter erstellt auf Basis des ausgewählten Snapshots einen Volume-Klon
2. SnapCenter bindet die LUN im geklonten Volume als neuen Datastore in den ESX Host ein

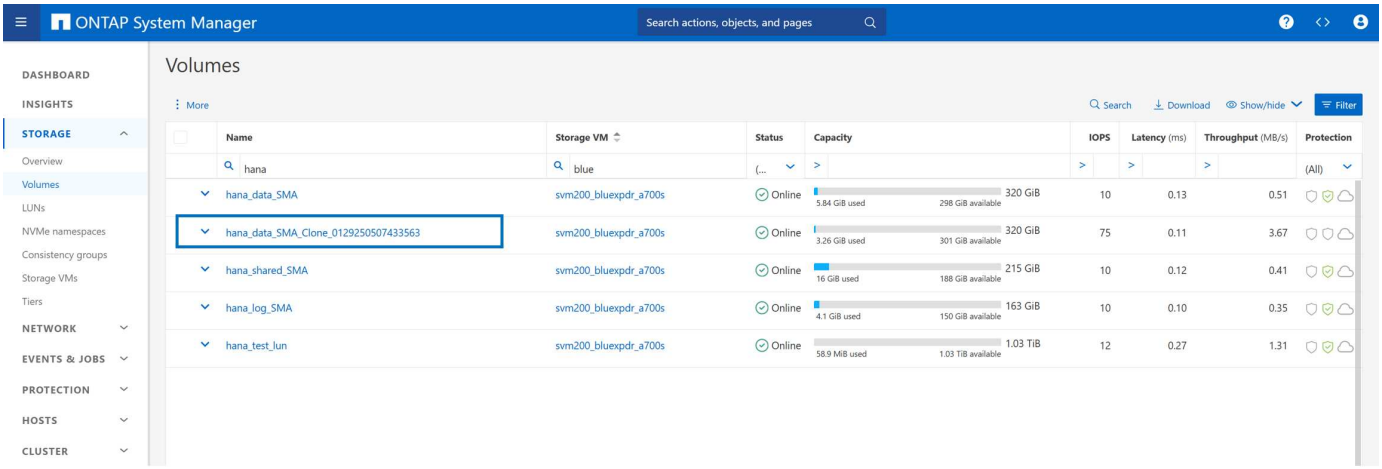
3. SnapCenter fügt die VMDK innerhalb des Datenspeichers der HANA-VM als neue Festplatte hinzu
4. SnapCenter bindet die neue Festplatte an das Linux Betriebssystem an
5. SnapCenter kopiert die Daten von der neuen Festplatte zurück in den ursprünglichen Speicherort
6. Wenn der Kopiervorgang abgeschlossen ist, werden alle oben genannten Ressourcen wieder entfernt
7. Die HANA-Wiederherstellung erfolgt wie gewohnt

Die Gesamtlaufzeit des Wiederherstellungsvorgangs ist daher abhängig von der Datenbankgröße und dem Durchsatz der FC-Verbindung zwischen den Storage-Clustern und den ESX-Hosts.

Wenn eine Ressource mit SnapMirror Active Sync konfiguriert ist, kann die SnapCenter-Wiederherstellung auch nur am aktuellen primären Standort ausgewählt werden.



Während der Restore- und Recovery-Vorgang ausgeführt wird, sehen Sie ein neues geklontes Volume, das am aktuellen Primärstandort erstellt wurde.



Auf dem HANA Linux Host sehen Sie eine neue Festplatte, die auf den Host gemountet wurde. Wenn die Wiederherstellung abgeschlossen ist, werden die Festplatte, Datenspeicher und Volumes von SnapCenter wieder entfernt.

```
hana-1:~ # df -h
Filesystem Size Used Avail Use% Mounted on
devtmpfs 4.0M 8.0K 4.0M 1% /dev
tmpfs 49G 4.0K 49G 1% /dev/shm
tmpfs 13G 58M 13G 1% /run
tmpfs 4.0M 0 4.0M 0% /sys/fs/cgroup
/dev/mapper/system-root 60G 36G 24G 60% /
/dev/mapper/system-root 60G 36G 24G 60% /.snapshots
/dev/mapper/system-root 60G 36G 24G 60% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 36G 24G 60% /home
/dev/mapper/system-root 60G 36G 24G 60% /boot/grub2/x86_64-efi
/dev/mapper/system-root 60G 36G 24G 60% /opt
/dev/mapper/system-root 60G 36G 24G 60% /srv
/dev/mapper/system-root 60G 36G 24G 60% /usr/local
/dev/mapper/system-root 60G 36G 24G 60% /tmp
/dev/mapper/system-root 60G 36G 24G 60% /root
/dev/mapper/system-root 60G 36G 24G 60% /var
/dev/sdb 200G 8.0G 192G 4% /hana/data/SMA/mnt00001
/dev/sdc 120G 7.0G 113G 6% /hana/log/SMA/mnt00001
/dev/sda1 253M 5.1M 247M 3% /boot/efi
/dev/sdd 150G 28G 123G 19% /hana/shared
tmpfs 6.3G 48K 6.3G 1% /run/user/467
tmpfs 6.3G 28K 6.3G 1% /run/user/0
/dev/sde 200G 8.0G 192G 4%
/var/opt/snapcenter/scu/clones/hana_data_SMAmnt00001_255_scu_clone_1
hana-1:~ #
```

Aktualisierung des SAP-Systems

Klonvorgänge können am primären Standort oder im sekundären Storage ausgeführt werden.

Das geklonte Volume ist nicht Teil der HANA-Konsistenzgruppe und wird nicht mit der aktiven SnapMirror-Synchronisierung repliziert.

Detaillierte Informationen zu den Workflows für die Systemaktualisierung sind verfügbar unter: "TR-4667: Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter"

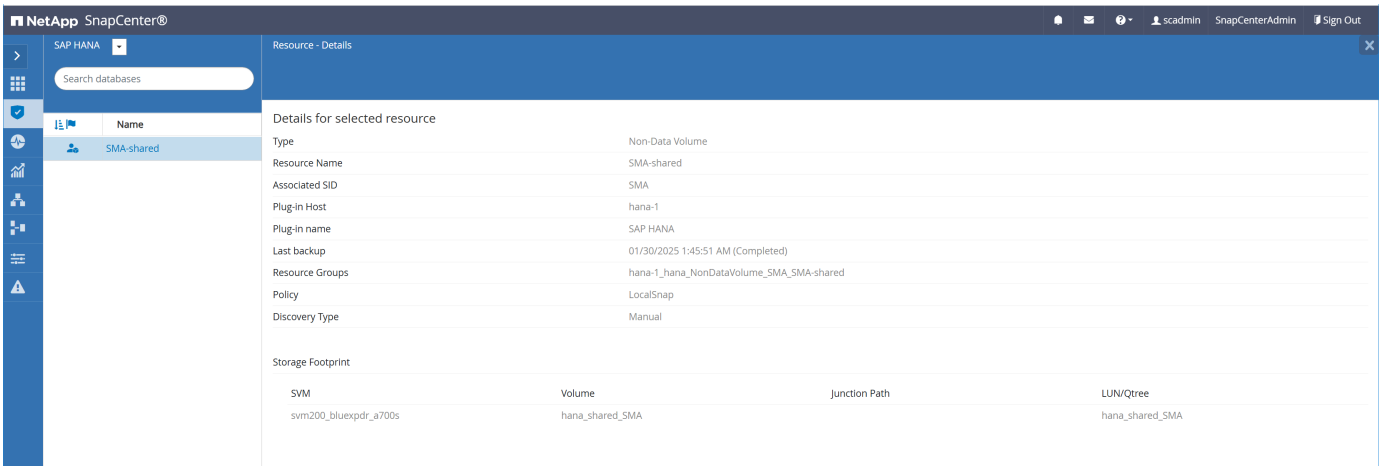
Nicht datenbasierte SnapCenter-Volumes

Wenn Ressourcen in SnapCenter manuell konfiguriert und nicht automatisch erkannt werden, erkennt SnapCenter die aktive Synchronisierung von VMware und SnapMirror nicht. Daher werden sie von SnapCenter nicht nativ unterstützt.

Bei nicht-Daten-Volumes wie HANA Shared könnten Backup- und Restore-Vorgänge unter Berücksichtigung zusätzlicher manueller Schritte weiterhin mit SnapCenter ausgeführt werden.

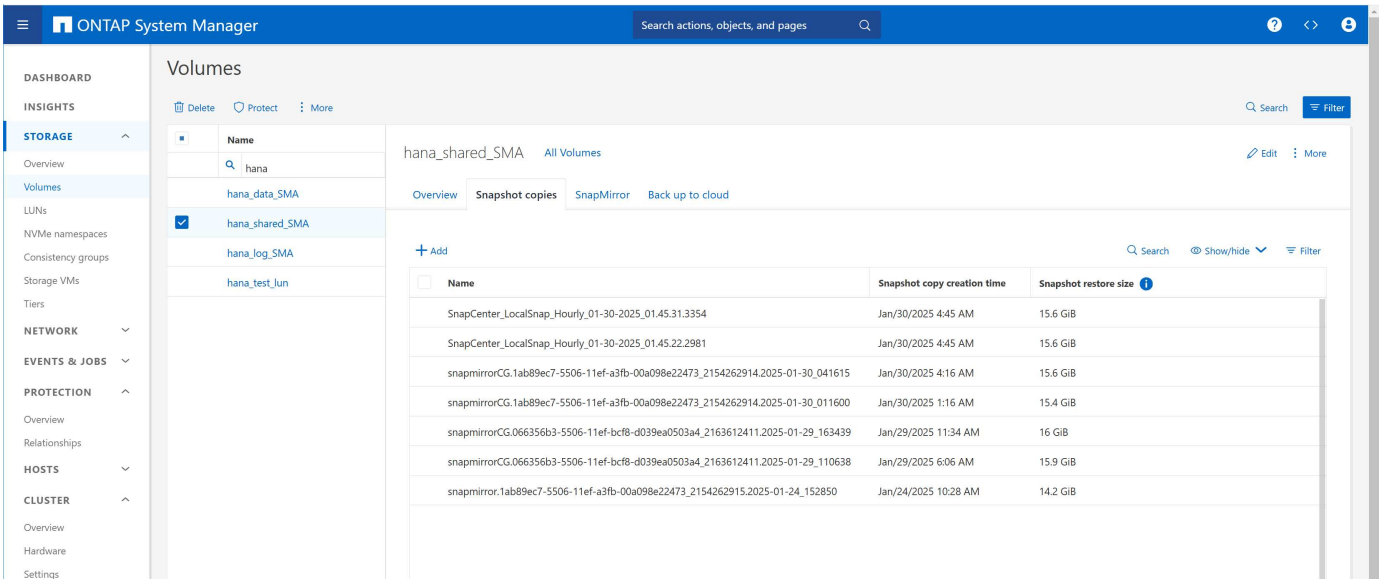
Ausfall des in SnapCenter konfigurierten Storage-Systems

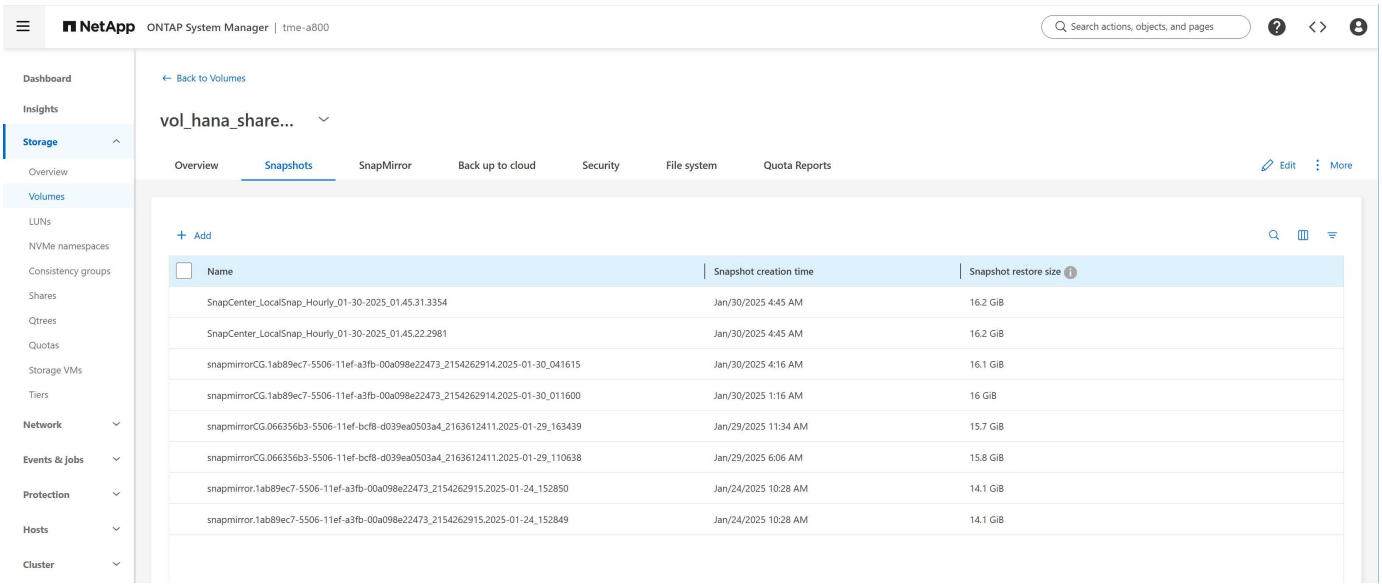
Bei einem Ausfall des in SnapCenter konfigurierten Storage-Systems wechselt SnapCenter nicht automatisch zu dem anderen Storage-System. Die nicht datenbezogene Volume-Ressource muss manuell angepasst werden, damit die gespiegelte Kopie des Volumes für Backup- und Restore-Vorgänge verwendet wird.



Backup-Vorgänge

Obwohl SnapCenter die SnapMirror Active Sync Konfiguration für das HANA Shared Volume nicht kennt, werden Snapshots an beiden Standorten repliziert.





Wiederherstellungsvorgang

Im Falle einer Wiederherstellung würde SnapCenter einfach eine Volume-Wiederherstellung ohne irgendwelche VMware spezifischen Schritte durchführen. Normalerweise müssten Sie das HANA Shared Volume auf dem Linux Host abmounten, den Datastore trennen und dann die Volume-Wiederherstellung durchführen, den Datastore erneut verbinden und dann das Filesystem auf dem Linux Host mounten. Als manuelle Operation könnten Sie die HANA VM stoppen, das HANA Shared Volume mit SnapCenter wiederherstellen und dann die VM erneut starten.

Failover-Szenarien

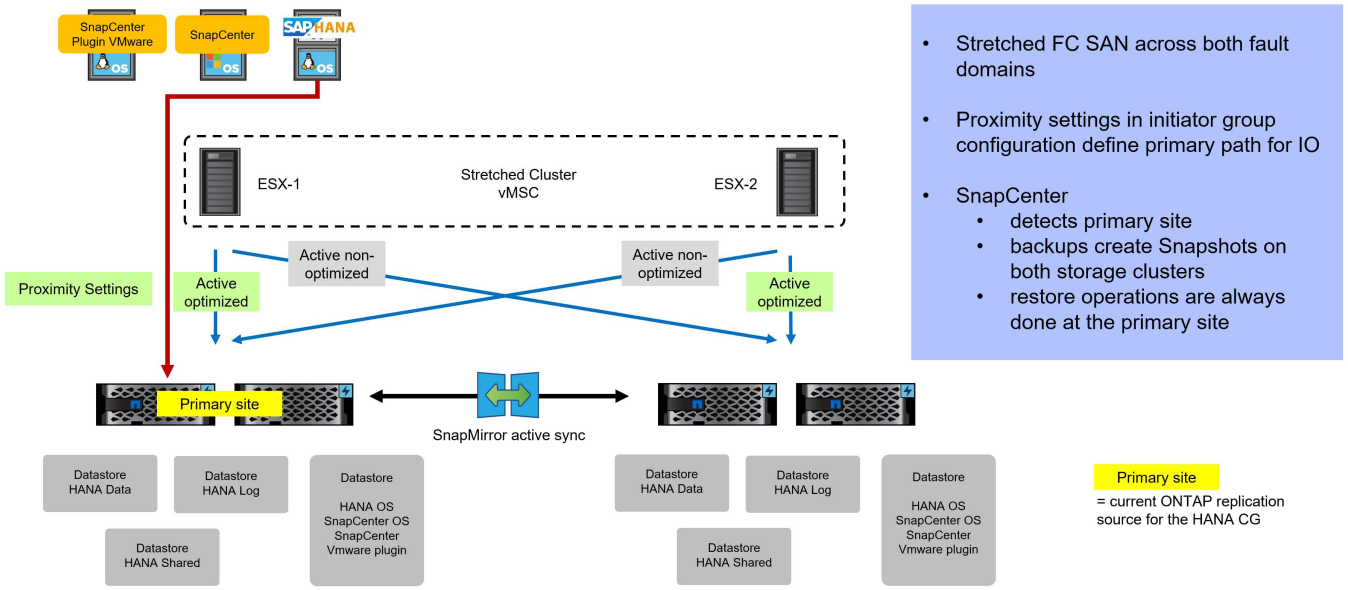
In diesem Artikel werden die Failover-Szenarien für diese Lösung hervorgehoben.

Einheitliche Zugriffseinrichtung

In einer einheitlichen Zugriffskonfiguration ist das Fibre-Channel-SAN auf beide Standorte verteilt. Die ESX Hosts an beiden Standorten könnten auf beide Kopien der Datensätze zugreifen. Während des normalen Betriebs greift der ESX Host, auf dem das HANA-System ausgeführt wird, basierend auf den Annäherungseinstellungen in der Konfiguration der Initiatorgruppe auf die lokale Kopie der Daten zu. Jeder ESX Host verfügt über einen aktiv optimierten Pfad zur lokalen Kopie und einen aktiven, nicht optimierten Pfad zur gespiegelten Kopie.

Normaler Betrieb

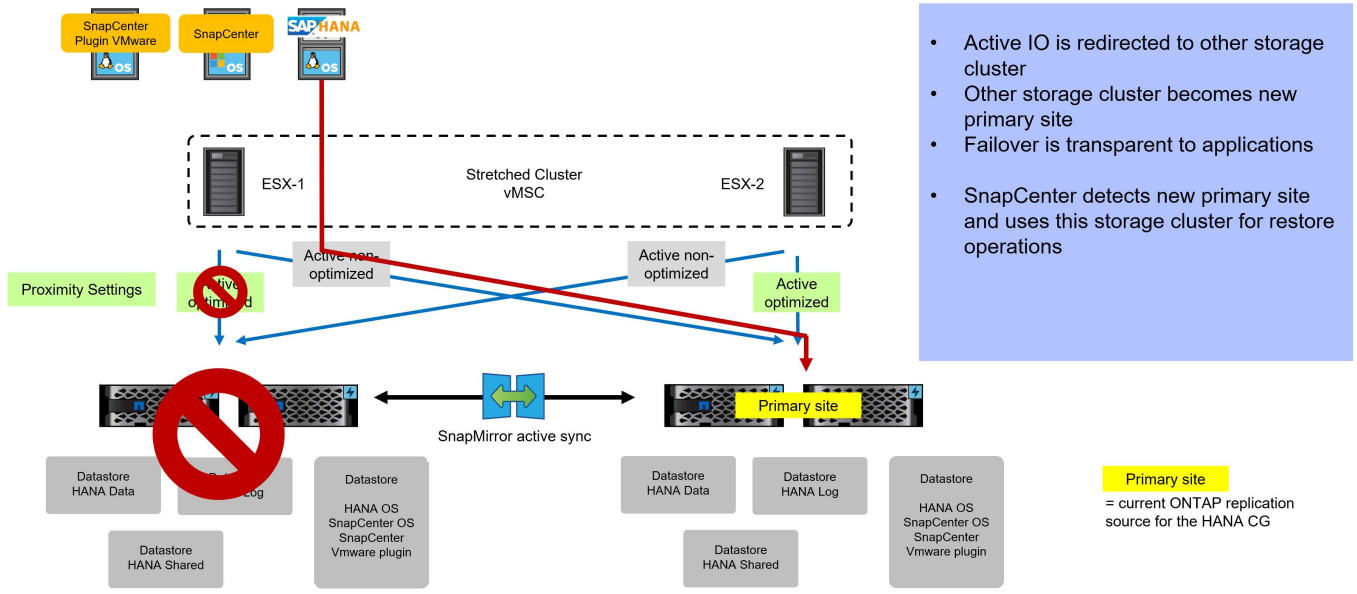
Im normalen Betrieb liest und schreibt das HANA-System basierend auf dem aktiv optimierten Pfad von ESX-Host ESX-1 von/auf die lokale Kopie. Bei jedem Backup-Vorgang erkennt SnapCenter den aktuellen primären Standort der Replizierungsbeziehung und führt die Backup-Vorgänge am primären Standort aus. Die Snapshots werden auf die gespiegelte Kopie repliziert und sind an beiden Standorten verfügbar. Am primären Standort würde eine SnapCenter-Wiederherstellung ausgeführt werden.



- Stretched FC SAN across both fault domains
- Proximity settings in initiator group configuration define primary path for IO
- SnapCenter
  - detects primary site
  - backups create Snapshots on both storage clusters
  - restore operations are always done at the primary site

Storage-Ausfall

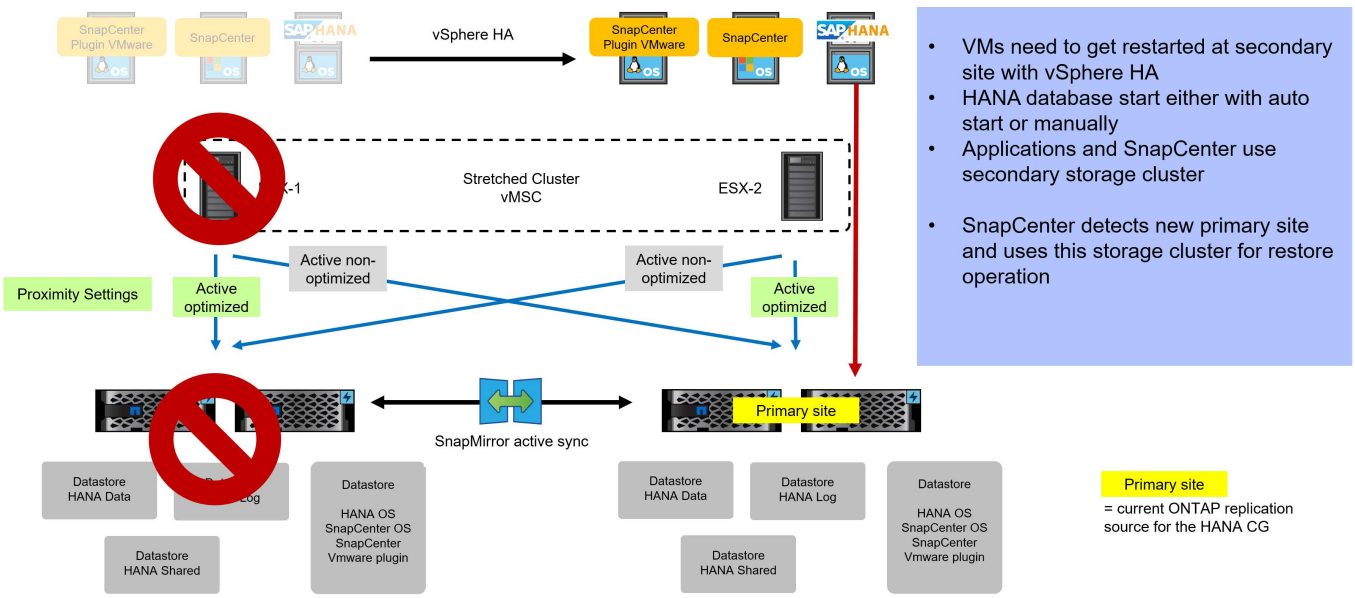
Fällt das Storage-System an Standort 1 aus, greifen die HANA-Systeme auf die gespiegelte Kopie an Standort 2 zu und setzen den Betrieb fort. Der primäre Standort schaltet auf den sekundären Standort um und SnapCenter führt nun Backup- und Restore-Vorgänge am neuen primären Standort aus.



- Active IO is redirected to other storage cluster
- Other storage cluster becomes new primary site
- Failover is transparent to applications
- SnapCenter detects new primary site and uses this storage cluster for restore operations

Standortausfall

Im Falle eines Standortausfalls werden sowohl die HANA VM als auch SnapCenter und das SnapCenter für VMware Plugin VM über vSphere HA auf den ESX-Host am sekundären Standort umschlagen. Die HANA-Datenbank muss gestartet werden und greift dann auf die gespiegelte Kopie am zweiten Standort zu. Der primäre Standort schaltet auf den sekundären Standort um und SnapCenter führt nun Backup- und Restore-Vorgänge am neuen primären Standort aus.

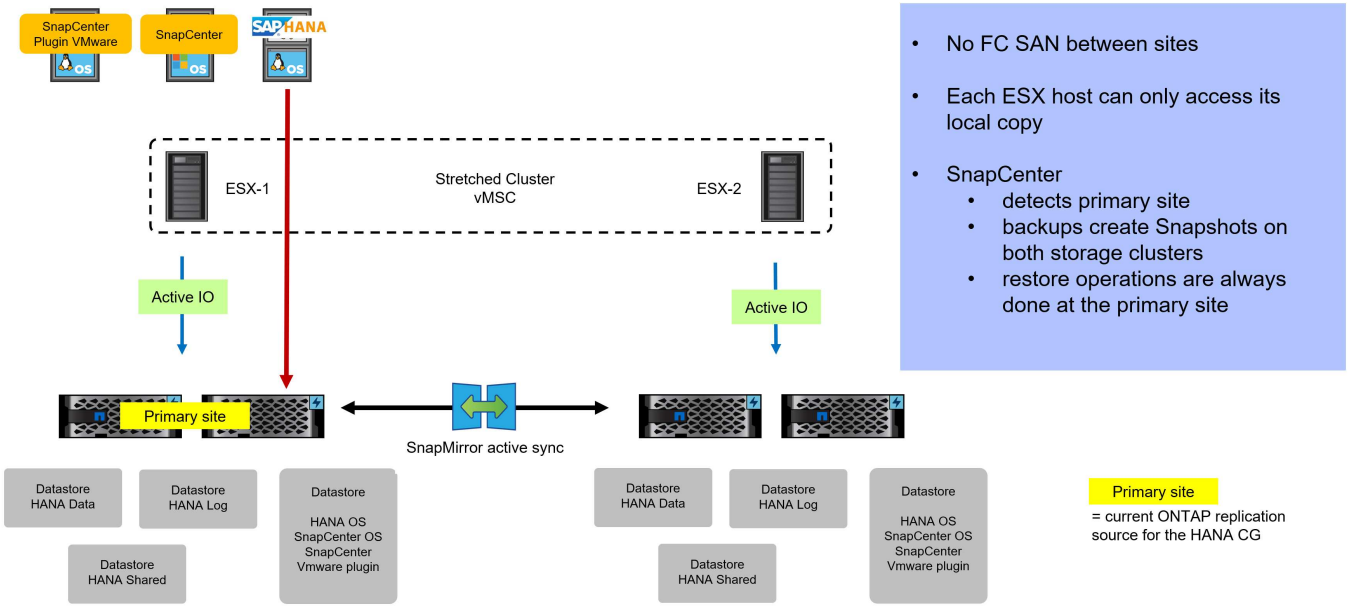


Uneinheitliche Zugriffseinrichtung

In einer nicht einheitlichen Zugriffskonfiguration wird das Fibre-Channel-SAN nicht auf beide Standorte ausgedehnt. Jeder ESX Host an jedem Standort kann nur auf die lokale Kopie der Datensätze zugreifen.

Normaler Betrieb

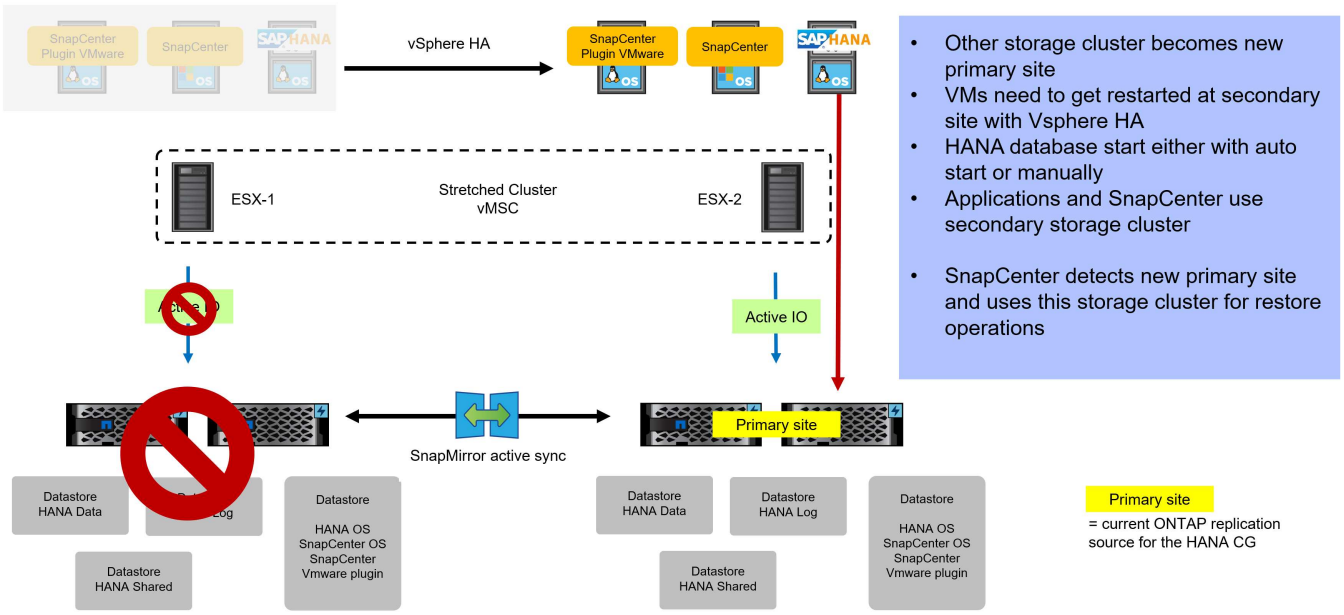
Im normalen Betrieb liest und schreibt das HANA-System von/auf die lokale Kopie. Bei jedem Backup-Vorgang erkennt SnapCenter den aktuellen primären Standort der Replizierungsbeziehung und führt die Backup-Vorgänge am primären Standort aus. Die Snapshots werden auf die gespiegelte Kopie repliziert und sind an beiden Standorten verfügbar. Am primären Standort würde eine SnapCenter-Wiederherstellung ausgeführt werden.



Storage-Ausfall

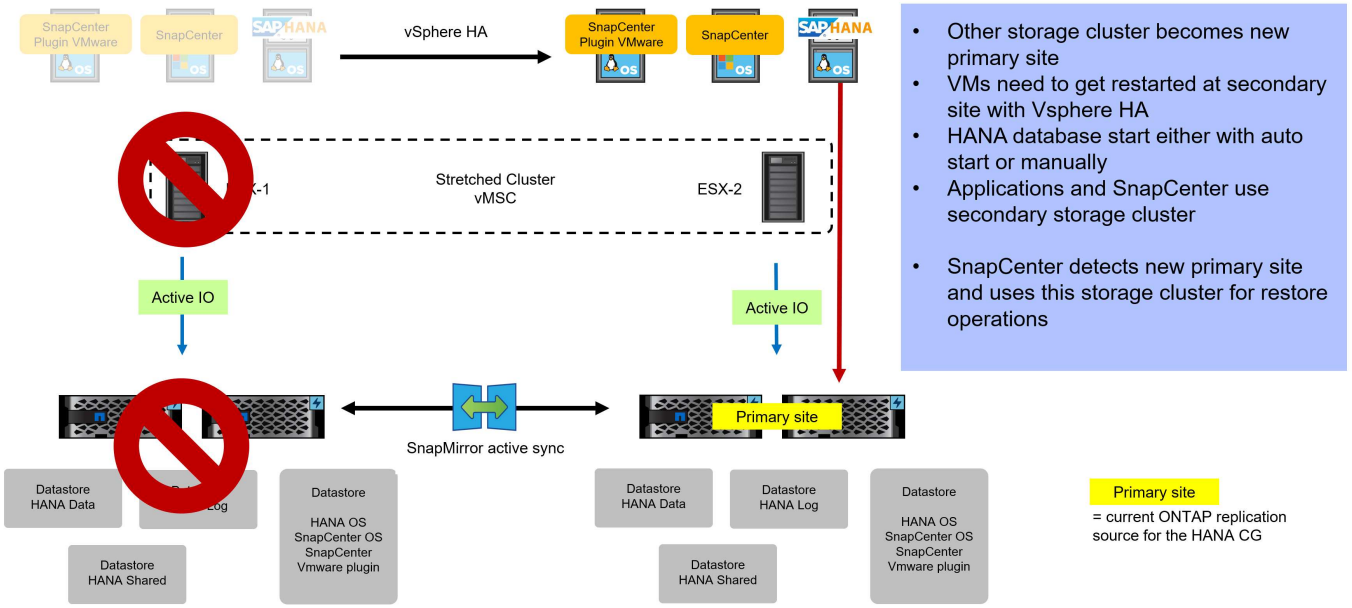
Im Falle eines Storage-Ausfalls werden sowohl die HANA VM als auch SnapCenter und das SnapCenter für VMware Plugin VM mithilfe von vSphere HA auf den ESX-Host am sekundären Standort umschlagen. Die

HANA-Datenbank muss gestartet werden und greift dann auf die gespiegelte Kopie am zweiten Standort zu. Der primäre Standort schaltet auf den sekundären Standort um und SnapCenter führt nun Backup- und Restore-Vorgänge am neuen primären Standort aus.



Standortausfall

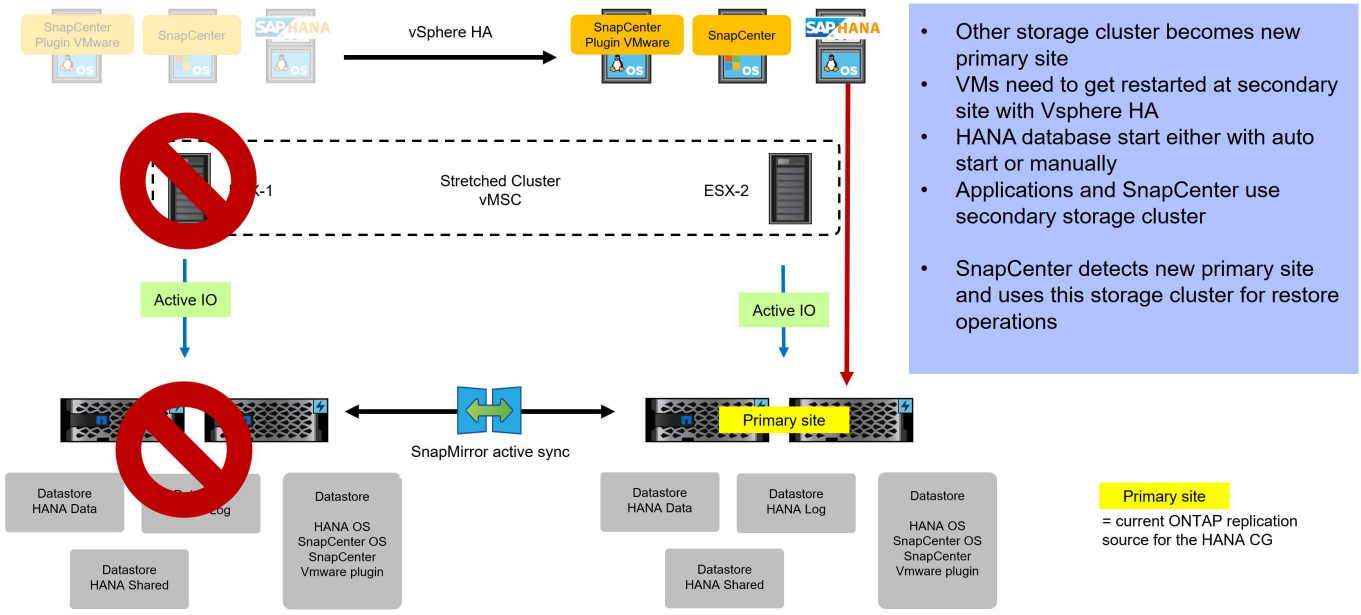
Das gleiche gilt für Storage-Ausfälle.



Verlagerung der HANA-VM oder des primären Standorts

Wenn die HANA VM auf den anderen ESX Host umgezogen wird und der primäre Standort des Storage unverändert bleibt, schlägt ein Wiederherstellungsvorgang mit SnapCenter fehl. Da SnapCenter zur Durchführung der Wiederherstellung den primären Standort nutzt, wird der Klon auf der linken Seite erstellt, während die HANA VM auf der rechten Seite ausgeführt wird. Da es keinen Datenpfad zwischen den Standorten gibt, wird SnapCenter die Daten nicht kopieren.

Als Behelfslösung müssen Sie sicherstellen, dass die Verschiebung der VM und der primären Seite gemeinsam durchgeführt wird oder Sie vor der Wiederherstellung mit SnapCenter einen Failover des primären Standorts durchführen müssen.



Zusätzliche Informationen und Versionsverlauf

Dieser Artikel enthält Links zu weiteren Ressourcen für diese Lösung.

SnapCenter

"TR-4614: SAP HANA Backup und Recovery mit SnapCenter"

"TR-4719: SAP HANA System Replication – Backup und Recovery mit SnapCenter"

"TR-4667: Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter"

"SnapCenter-Softwaredokumentation"

Aktive SnapMirror-Synchronisierung:

"Übersicht über die aktive SnapMirror-Synchronisierung in ONTAP"

"NetApp ONTAP mit NetApp SnapMirror Active Sync mit VMware vSphere Metro Storage Cluster (vMSC)."

"VMware vSphere Metro Storage-Cluster mit SnapMirror Active Sync"

"VMware vSphere Metro Storage-Cluster (vMSC)"

Versionsverlauf:

Version	Datum	Kommentar
Version 1.0	März 2025	Ausgangsversion

SAP HANA-Datenschutz mit SnapCenter mit VMware VMFS und NetApp ASA -Systemen

SAP HANA-Datenschutz mit SnapCenter mit VMware VMFS und NetApp ASA -Systemen

In diesem Dokument werden die Best Practices für den Datenschutz mit SnapCenter für HANA-Systeme beschrieben, die auf VMware mit Datenspeichern ausgeführt werden, die VMFS und LUNs verwenden, die auf NetApp ASA -Systemen gespeichert sind.

Autor: Nils Bauer, NetApp

Inhalt des vorliegenden Dokuments

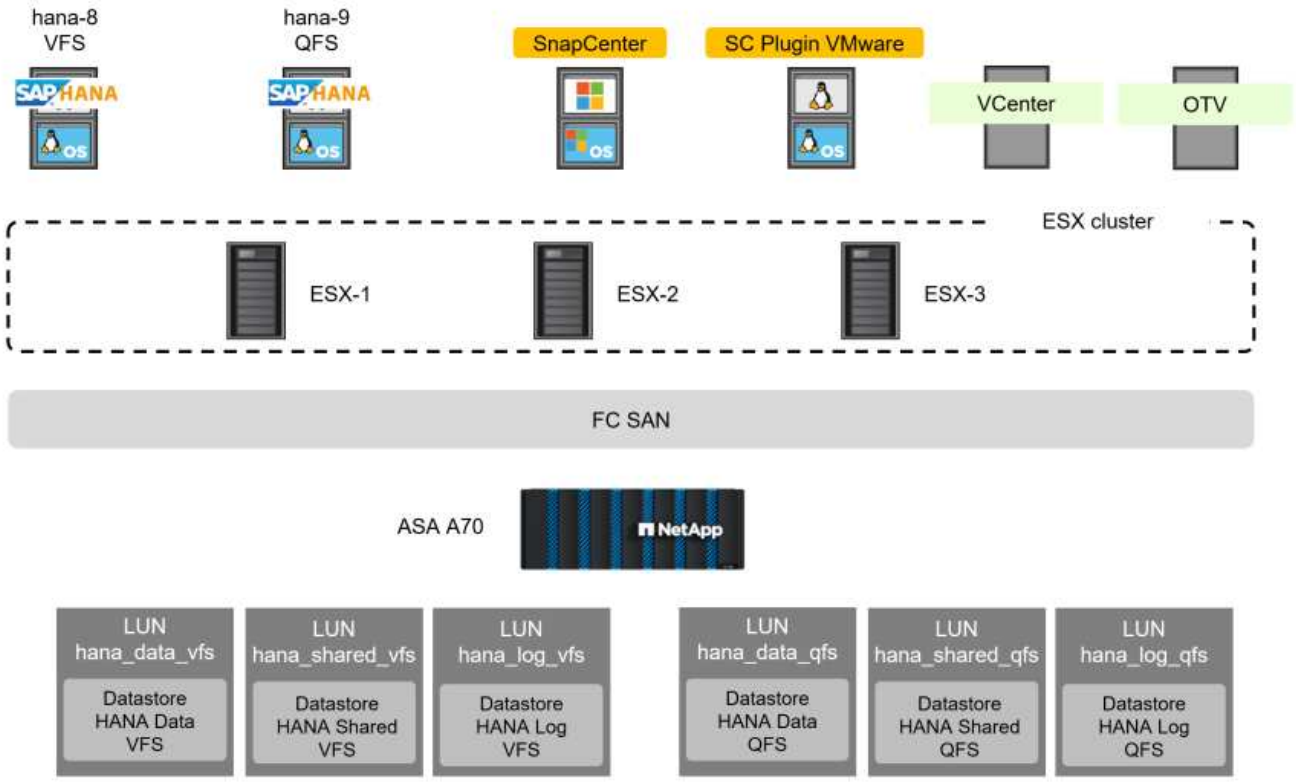
Es dient nicht als Schritt-für-Schritt-Anleitung zur Konfiguration der gesamten Umgebung, sondern konzentriert sich auf Details, die spezifisch für SnapCenter und HANA auf VMFS sind, darunter:

- Einrichten von SAP HANA-Systemen mit VMware VMFS
- Spezifische SnapCenter -Konfigurationen für HANA auf VMware mit VMFS
- SnapCenter -Sicherungs-, Wiederherstellungs- und Recovery-Vorgänge für HANA auf VMware mit VMFS
- SnapCenter SAP System Refresh-Vorgänge für HANA auf VMware mit VMFS

Weitere Informationen und detaillierte Konfigurationsanweisungen finden Sie in den Dokumenten im ""Weitere Informationen"" Kapitel.

Für dieses Dokument verwendeter Laboraufbau

Die folgende Abbildung bietet einen Überblick über das verwendete Labor-Setup. Zwei Single-Host-HANA-MDC-Systeme dienen zur Demonstration der verschiedenen Vorgänge. Das HANA-System VFS ist für die Ausführung von Sicherungs-, Wiederherstellungs- und Recovery-Vorgängen vorgesehen, während das HANA-System QFS als Zielsystem für SAP-Systemaktualisierungen dient. Das SnapCenter Plug-in für VMware ist unerlässlich, damit SnapCenter die mit VMware VMFS konfigurierten HANA-Ressourcen verwalten kann. Obwohl ONTAP Tools für VMware zur Bereitstellung der Speichereinheiten für die HANA-Systeme verwendet wurden, sind diese keine zwingende Komponente.



Softwareversionen

Software	Version
ONTAP	ASA A70 ONTAP 9.16.1
VSphere Client	8.0.3
ESXi	8.0.3
SnapCenter Plug-in für vSphere	6.1.0
ONTAP Tools für VMware vSphere	10,4
Linux BS	SLES FÜR SAP 15 SP6
SAP HANA	2,0 SPS8
SnapCenter	6.1P1

HANA-Systembereitstellung und -Installation

In diesem Kapitel werden die Installation und Konfiguration des für eine VMware-Einrichtung mithilfe von VMFS spezifischen SAP HANA-Systems beschrieben. Weitere allgemeine Best Practices finden Sie unter "Technischer Bericht: SAP HANA on NetApp ASA Systems with Fibre Channel Protocol".

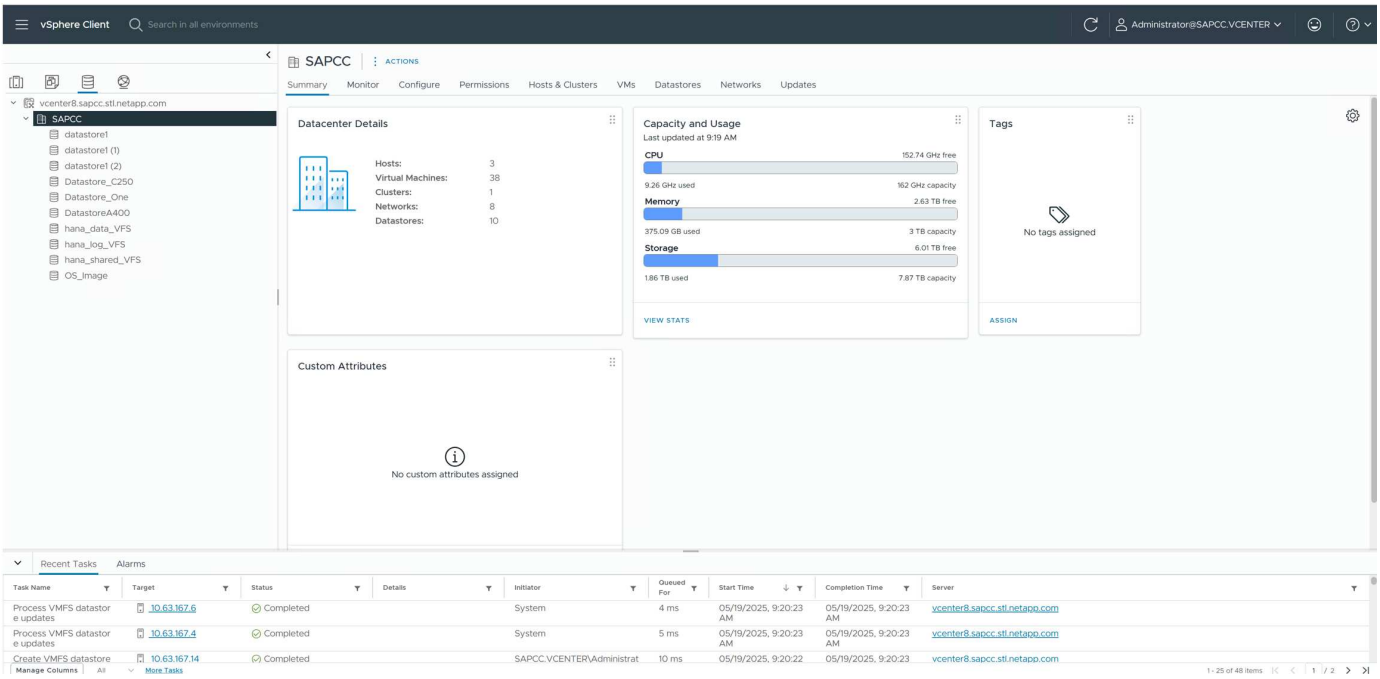
Storage-Konfiguration

Um die von SAP definierten Speicherleistungs-KPIs für HANA-Produktionssysteme zu erfüllen, müssen dedizierte LUNs und Datenspeicher für die Daten- und Protokolldateisysteme des HANA-Systems konfiguriert werden. Datenspeicher dürfen nicht von mehreren HANA-Systemen oder anderen Workloads gemeinsam genutzt werden.

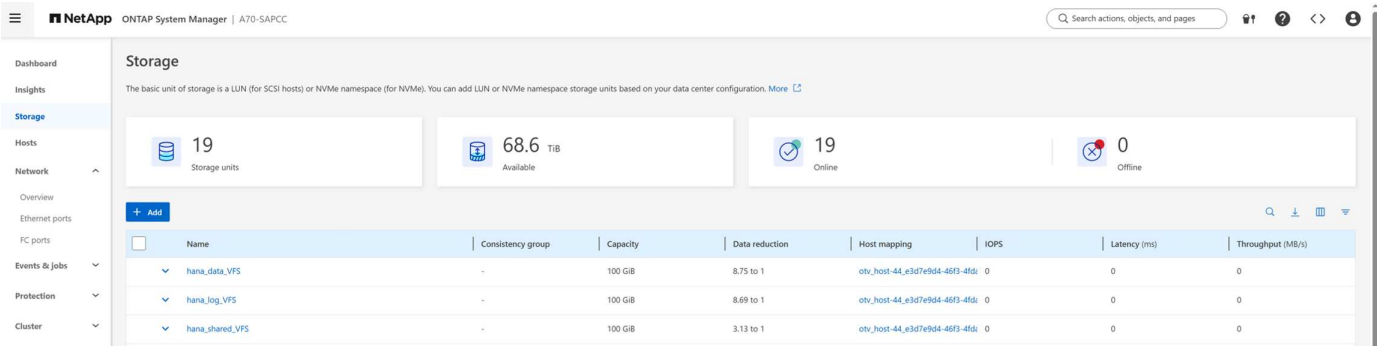
ONTAP Tools für VMware (OTV) wurden verwendet, um die drei Datenspeicher für das HANA-System VFS bereitzustellen.

- hana_data_VFS
- hana_log_VFS
- hana_shared_VFS

Der Datenspeicher für das gemeinsam genutzte HANA-Dateisystem kann auch von mehreren HANA-Systemen gemeinsam genutzt werden.

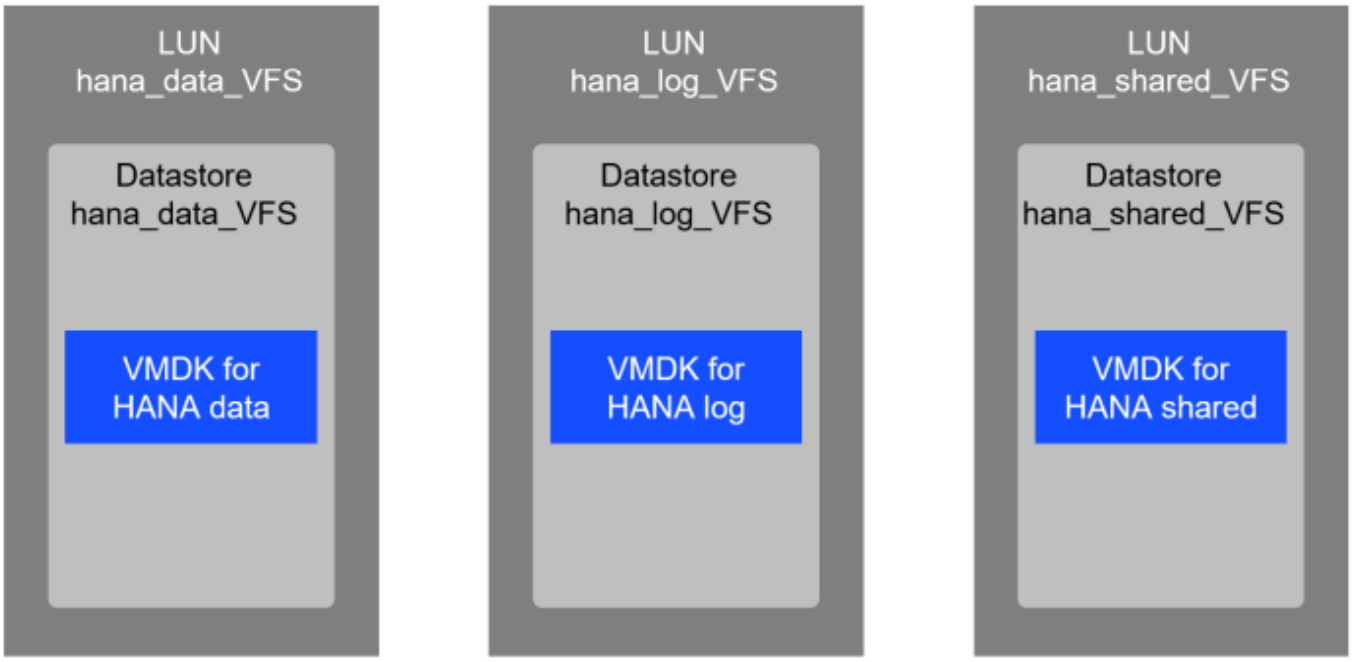


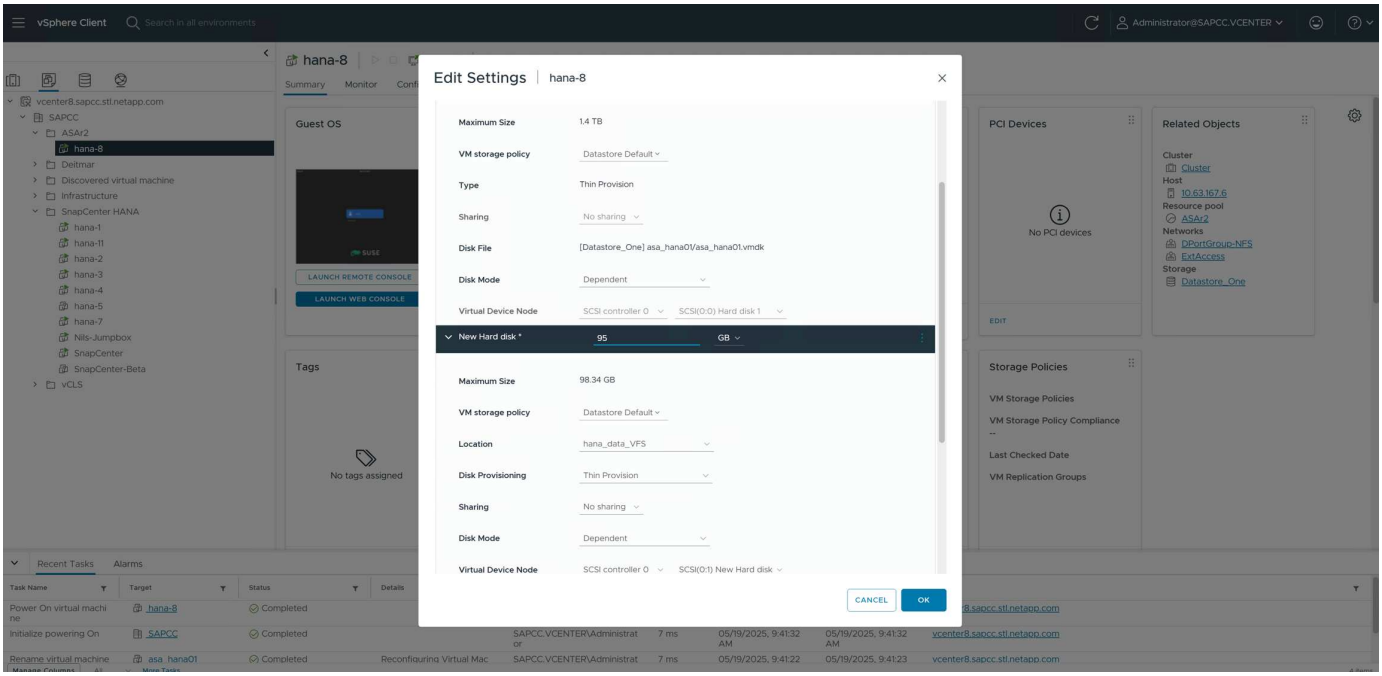
Auf dem Speichersystem wurden von OTV drei LUNs erstellt.

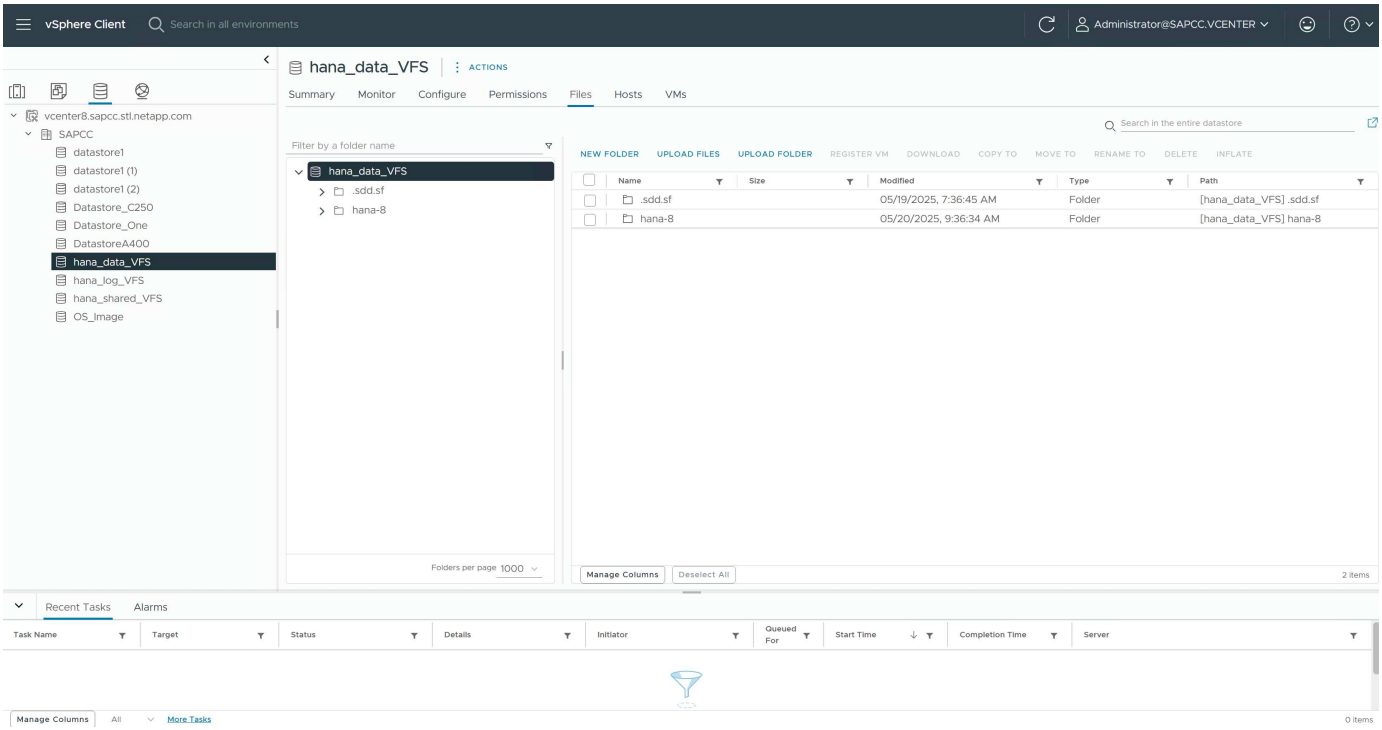


Konfiguration von VM-Festplatten

Der HANA-VM müssen drei neue Datenträger (VMDK) hinzugefügt werden. Jeder Datenträger befindet sich in einem der zuvor erstellten Datenspeicher, wie in der Abbildung unten dargestellt.


LUN
hana_data_VFS
Datastore
hana_data_VFS
VMDK for
HANA data
LUN
hana_log_VFS
Datastore
hana_log_VFS
VMDK for
HANA log
LUN
hana_shared_VFS
Datastore
hana_shared_VFS
VMDK for
HANA shared


vSphere Client
Edit Settings
hana-8
Maximum Size
1.4 TB
VM storage policy
Datastore Default
Type
Thin Provision
Sharing
No sharing
Disk File
[Datastore_One] asa_hana01/asa_hana01.vmdk
Disk Mode
Dependent
Virtual Device Node
SCSI controller 0
SCSI(0:0) Hard disk 1
New Hard disk *
95
GB
Maximum Size
98.34 GB
VM storage policy
Datastore Default
Location
hana_data_VFS
Disk Provisioning
Thin Provision
Sharing
No sharing
Disk Mode
Dependent
Virtual Device Node
SCSI controller 0
SCSI(0:1) New Hard disk
CANCEL
OK



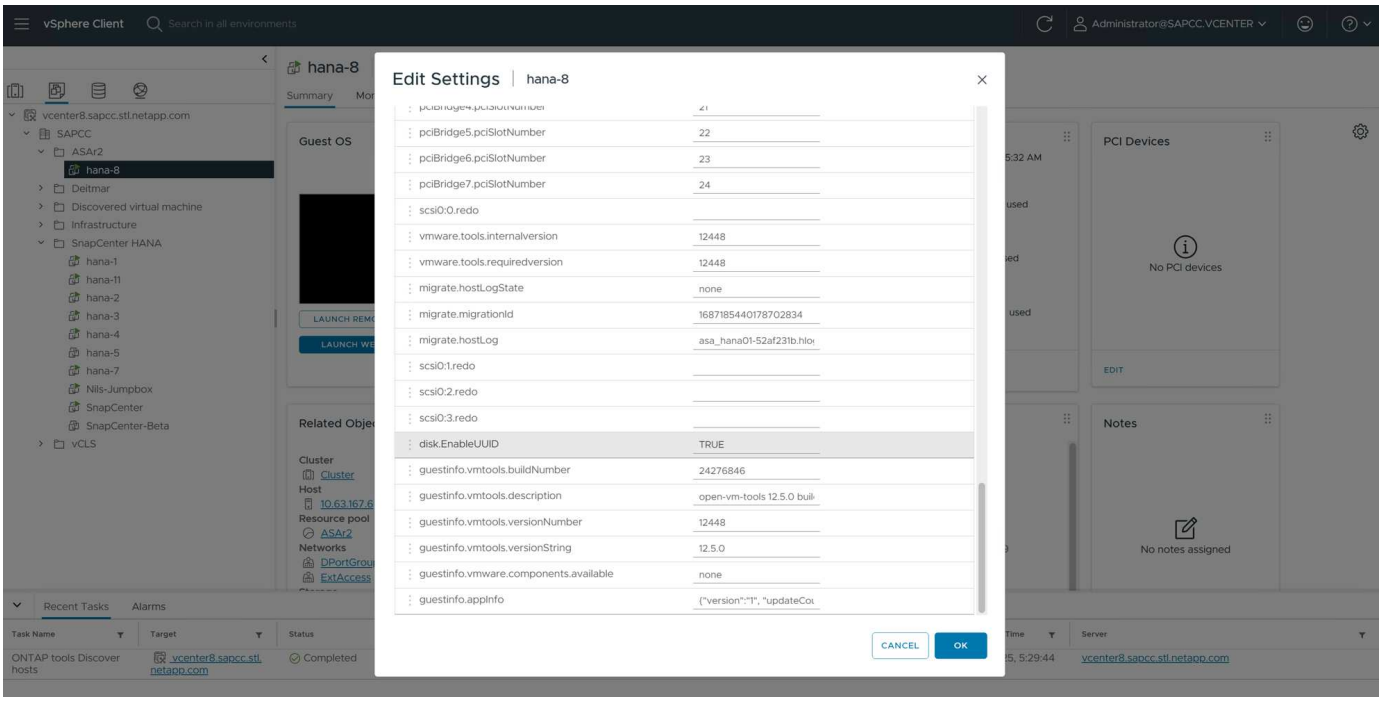
Wenn die drei Festplatten zur VM hinzugefügt wurden, können sie auf Betriebssystemebene aufgelistet werden.

```
hana-8:~ # lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
sda 8:0 0 100G 0 disk
├─sda1 8:1 0 256M 0 part /boot/efi
└─sda2 8:2 0 82G 0 part
├─system-root 254:0 0 60G 0 lvm /root
│ /var
│ /usr/local
│ /tmp
│ /srv
│ /opt
│ /home
│ /boot/grub2/x86++_++64-efi
│ /boot/grub2/i386-pc
│ /.snapshots
│ /
└─system-swap 254:1 0 2G 0 lvm [SWAP]
sdb 8:16 0 95G 0 disk
sdc 8:32 0 95G 0 disk
sdd 8:48 0 95G 0 disk
sr0 11:0 1 17.1G 0 rom
```

VM-Parameter disk.EnableUUID

Dieser Parameter muss entsprechend eingestellt werden, sonst schlägt die automatische Erkennung der SnapCenter Datenbank fehl.

1. VM herunterfahren
2. Neuen Parameter „disk.EnableUUID“ hinzufügen und auf „TRUE“ setzen
3. VM starten



Vorbereitung des Dateisystems auf Linux-Host

Erstellung des xfs-Dateisystems auf neuen Platten

Auf jedem der drei neuen Festplatten wurde ein xfs-Dateisystem erstellt.

```
hana-8:~ # mkfs.xfs /dev/sdb
meta-data=/dev/sdb isize=512 agcount=4, agsize=6225920 blks
= sectsz=512 attr=2, projid32bit=1
= crc=1 finobt=1, sparse=1, rmapbt=1
= reflink=1 bigtime=1 inobtcount=0 nrext64=0
data = bsize=4096 blocks=24903680, imaxpct=25
= sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=16384, version=2
= sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0
Discarding blocks...Done.

hana-8:~ # mkfs.xfs /dev/sdc
meta-data=/dev/sdc isize=512 agcount=4, agsize=6225920 blks
= sectsz=512 attr=2, projid32bit=1
= crc=1 finobt=1, sparse=1, rmapbt=1
= reflink=1 bigtime=1 inobtcount=0 nrext64=0
data = bsize=4096 blocks=24903680, imaxpct=25
= sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=16384, version=2
= sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0
Discarding blocks...Done.

hana-8:~ # mkfs.xfs /dev/sdd
meta-data=/dev/sdd isize=512 agcount=4, agsize=6225920 blks
= sectsz=512 attr=2, projid32bit=1
= crc=1 finobt=1, sparse=1, rmapbt=1
= reflink=1 bigtime=1 inobtcount=0 nrext64=0
data = bsize=4096 blocks=24903680, imaxpct=25
= sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=16384, version=2
= sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0
Discarding blocks...Done.

hana-8:~ #
```

Erstellung von Bereitstellungspunkten

```
hana-8:/ # mkdir -p /hana/data/VFS/mnt00001
hana-8:/ # mkdir -p /hana/log/VFS/mnt00001
hana-8:/ # mkdir -p /hana/shared
hana-8:/ # chmod –R 777 /hana/log/SMA
hana-8:/ # chmod –R 777 /hana/data/SMA
hana-8:/ # chmod -R 777 /hana/shared
```

Konfiguration von /etc/fstab

```
hana-8:/ # cat /etc/fstab

/dev/system/root / btrfs defaults 0 0
/dev/system/root /var btrfs subvol=/@/var 0 0
/dev/system/root /usr/local btrfs subvol=/@/usr/local 0 0
/dev/system/root /tmp btrfs subvol=/@/tmp 0 0
/dev/system/root /srv btrfs subvol=/@/srv 0 0
/dev/system/root /root btrfs subvol=/@/root 0 0
/dev/system/root /opt btrfs subvol=/@/opt 0 0
/dev/system/root /home btrfs subvol=/@/home 0 0
/dev/system/root /boot/grub2/x86++_++64-efi btrfs
subvol=/@/boot/grub2/x86++_++64-efi 0 0
/dev/system/root /boot/grub2/i386-pc btrfs subvol=/@/boot/grub2/i386-pc 0
0
/dev/system/swap swap swap defaults 0 0
/dev/system/root /.snapshots btrfs subvol=/@/.snapshots 0 0
UUID=FB79-24DC /boot/efi vfat utf8 0 2
### SAPCC_share
192.168.175.86:/sapcc_share /mnt/sapcc-share nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0
0
/dev/sdb /hana/data/VFS/mnt00001 xfs relatime,inode64 0 0
/dev/sdc /hana/log/VFS/mnt00001 xfs relatime,inode64 0 0
/dev/sdd /hana/shared xfs defaults 0 0
hana-8:/ #

hana-8:/ # df -h
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/system-root 60G 4.4G 54G 8% /
devtmpfs 4.0M 0 4.0M 0% /dev
tmpfs 49G 0 49G 0% /dev/shm
efivarfs 256K 57K 195K 23% /sys/firmware/efi/efivars
tmpfs 13G 18M 13G 1% /run
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev-
early.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysctl.service
```

```
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-vconsole-setup.service
/dev/mapper/system-root 60G 4.4G 54G 8% /.snapshots
/dev/mapper/system-root 60G 4.4G 54G 8% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 4.4G 54G 8% /boot/grub2/x86++_++64-efi
/dev/mapper/system-root 60G 4.4G 54G 8% /home
/dev/mapper/system-root 60G 4.4G 54G 8% /opt
/dev/mapper/system-root 60G 4.4G 54G 8% /srv
/dev/mapper/system-root 60G 4.4G 54G 8% /tmp
/dev/mapper/system-root 60G 4.4G 54G 8% /usr/local
/dev/mapper/system-root 60G 4.4G 54G 8% /var
/dev/sda1 253M 5.9M 247M 3% /boot/efi
/dev/mapper/system-root 60G 4.4G 54G 8% /root
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup.service
tmpfs 6.3G 72K 6.3G 1% /run/user/464
tmpfs 1.0M 0 1.0M 0% /run/credentials/getty@tty1.service
tmpfs 6.3G 52K 6.3G 1% /run/user/0
192.168.175.86:/sapcc_share 1.4T 840G 586G 59% /mnt/sapcc-share
/dev/sdb 95G 1.9G 94G 2% /hana/data/VFS/mnt00001
/dev/sdc 95G 1.9G 94G 2% /hana/log/VFS/mnt00001
/dev/sdd 95G 1.9G 94G 2% /hana/shared

hana-8:/ #
```

HANA-Installation

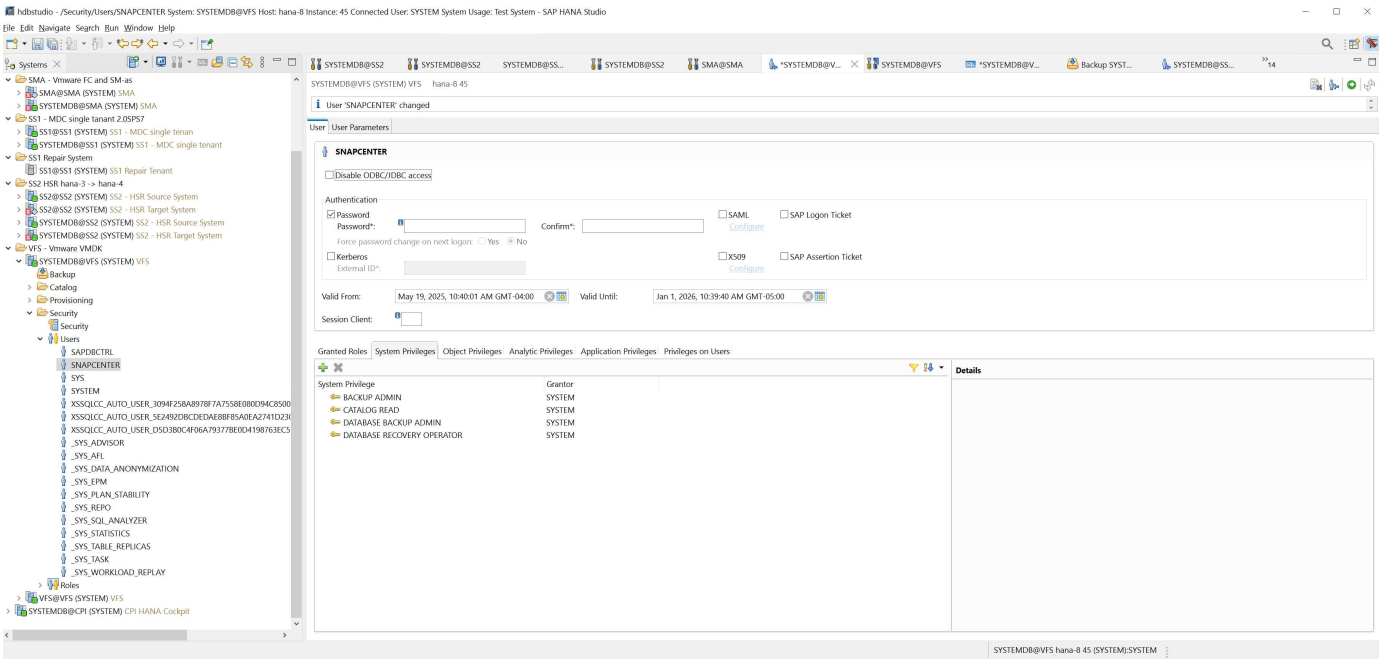
Die HANA-Installation kann nun ausgeführt werden.

> Bei der beschriebenen Konfiguration befindet sich das Verzeichnis /usr/sap/VFS auf der OS VMDK. Wenn /usr/sap/VFS in der gemeinsam genutzten VMDK gespeichert werden soll, kann der gemeinsam genutzte hana-Datenträger partitioniert werden, um ein weiteres Dateisystem für /usr/sap/VFS bereitzustellen.

HANA-Konfiguration

Konfigurieren des SnapCenter -Datenbankbenutzers

Es muss ein Benutzerspeicher für einen Systemdatenbankbenutzer erstellt werden, der von SnapCenter verwendet werden soll.



Konfigurieren des HDB-Benutzerspeicherschlüssels

Für den Benutzer vfsadm muss ein User Store Key angelegt werden. Für die Kommunikation mit dem Port muss die HANA-Instanznummer entsprechend gesetzt werden. In unserem Setup wird die Instanznummer „45“ verwendet.

```
vfsadm@hana-8:/usr/sap/VFS/HDB45> hdbuserstore SET VFSKEY hana-8:34513
SNAPCENTER <password>

Retroactive report: Operation succeed.
```

Zugriff prüfen mit:

```
vfsadm@hana-8:/usr/sap/VFS/HDB45> hdbsql -U VFSKEY

Welcome to the SAP HANA Database interactive terminal.
Type: \h for help with commands
\q to quit
hdbsql SYSTEMDB=> exit

vfsadm@hana-8:/usr/sap/VFS/HDB45>
```

SnapCenter-Konfiguration

Voraussetzungen

Die SnapCenter HANA-Ressource muss automatisch erkannt werden

Mit VMware VMFS konfigurierte Ressourcen müssen von SnapCenter automatisch erkannt werden, um bestimmte für diese Konfigurationen erforderliche Vorgänge zu ermöglichen.

Da es sich bei HANA-Nicht-Datenvolumes in SnapCenter immer um manuell konfigurierte Ressourcen handelt, werden sie von SnapCenter mit VMFS nicht unterstützt.

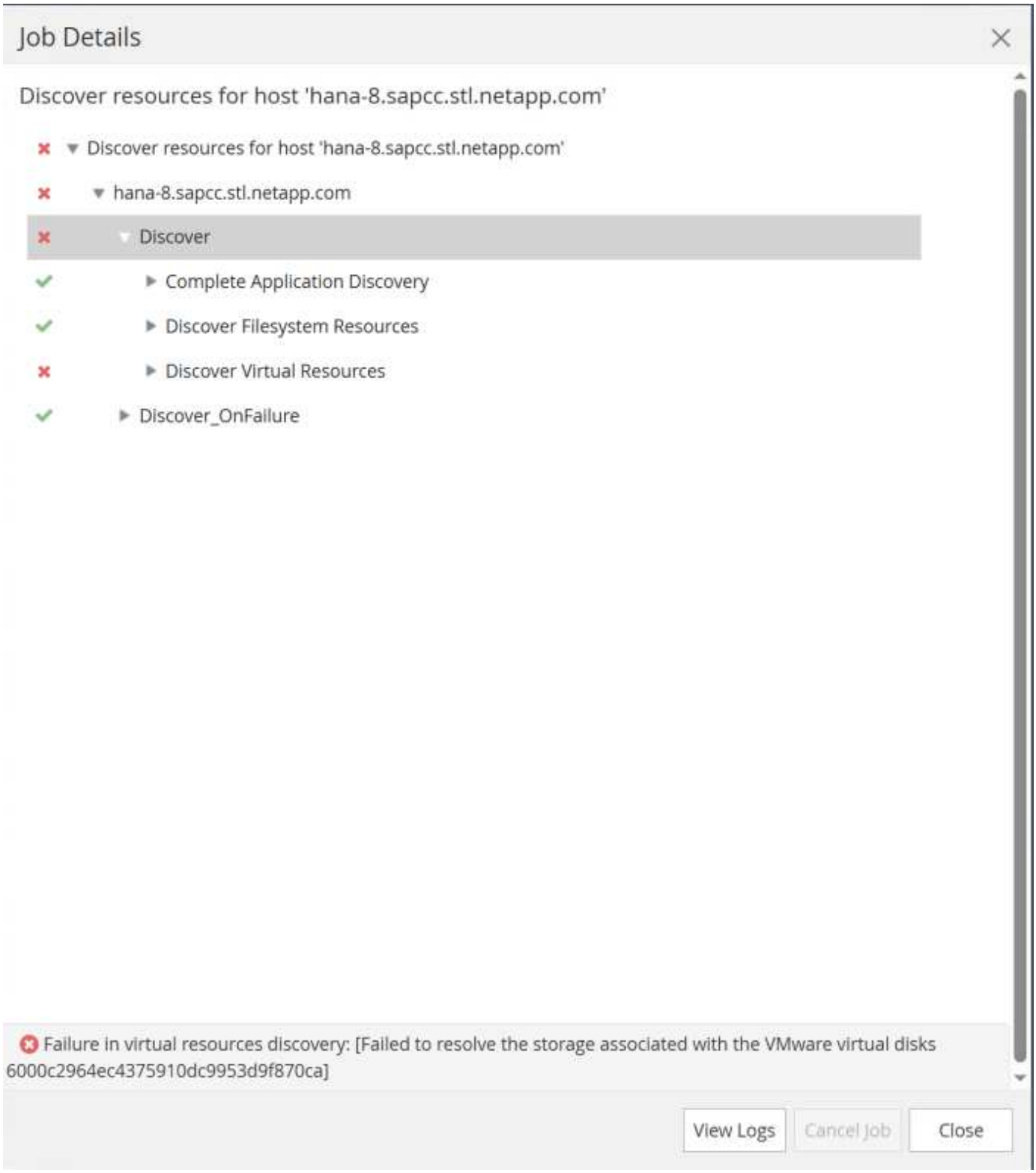
SAP HANA-Mehrfachhostsysteme müssen über ein zentrales HANA-Plugin konfiguriert werden und werden daher standardmäßig manuell konfiguriert. Solche Systeme werden von SnapCenter bei Verwendung von VMware VMFS auch nicht unterstützt.

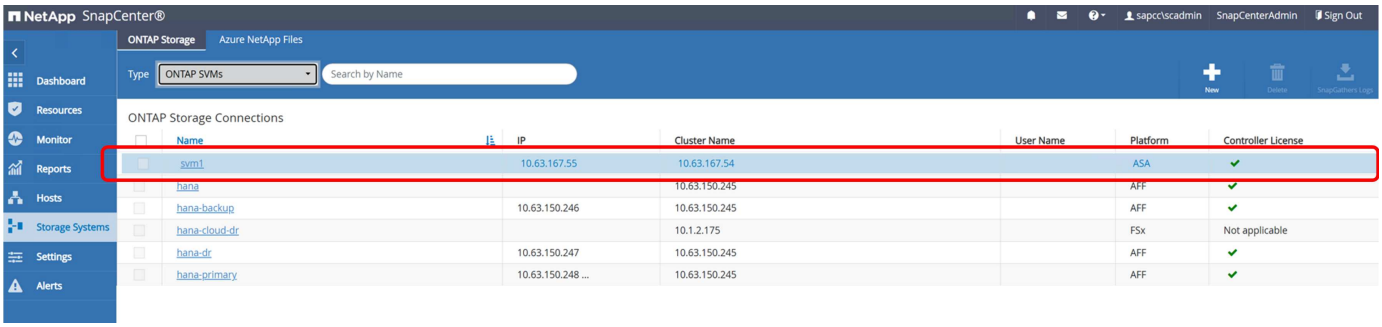
SnapCenter für VMware vSphere Plug-in

Das SnapCenter für VMware vSphere Plug-in muss in der VMware Umgebung implementiert werden.

Storage-SVM-Management-IP

Für Speicher-SVMs, die die LUNs hosten, muss eine Verwaltungsschnittstelle konfiguriert sein. Andernfalls werden die SVMs beim Hinzufügen von Speicher mit der Option „Cluster hinzufügen“ nicht in SnapCenter aufgeführt und der automatische Erkennungsvorgang schlägt fehl.


Job Details
Discover resources for host 'hana-8.sapcc.stl.netapp.com'
Discover resources for host 'hana-8.sapcc.stl.netapp.com'
hana-8.sapcc.stl.netapp.com
Discover
Complete Application Discovery
Discover Filesystem Resources
Discover Virtual Resources
Discover_OnFailure
Failure in virtual resources discovery: [Failed to resolve the storage associated with the VMware virtual disks 6000c2964ec4375910dc9953d9f870ca]
View Logs
Cancel Job
Close



VM-Festplattenparameter

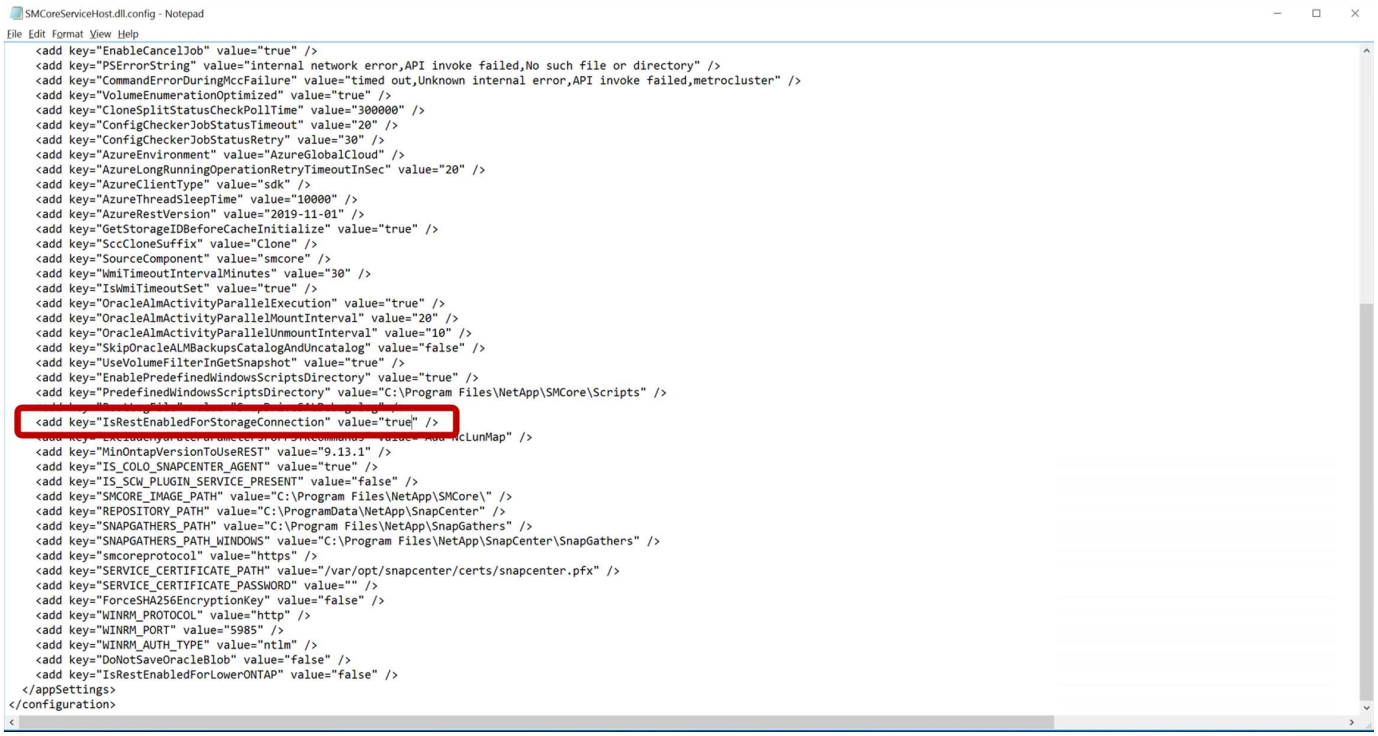
Der Parameter muss wie im Kapitel beschrieben eingestellt werden "„VM-Parameter disk.EnableUUID“" , andernfalls schlägt die automatische Erkennung der SnapCenter -Datenbank fehl.

Konfigurieren Sie SnapCenter für die Verwendung von REST-APIs für die Speicherkommunikation

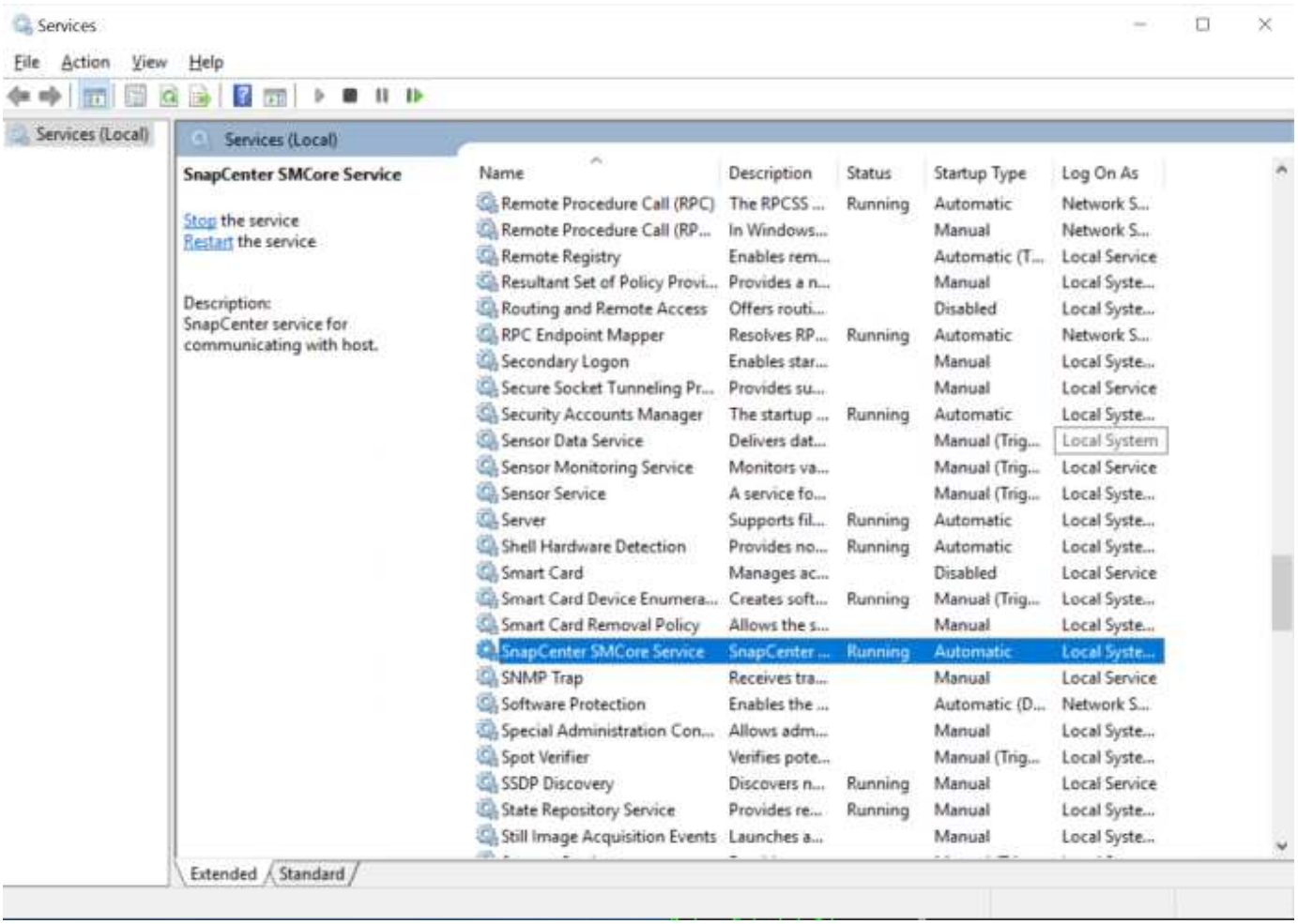
SnapCenter muss für die Speicherkommunikation REST-APIs verwenden. Andernfalls schlägt die Snapshot-Erstellung mit der unten gezeigten Fehlermeldung fehl.

Der Parameter „IsRestEnabledForStorageConnection“ in der Konfigurationsdatei + C:\Program Files\NetApp\SMCore\SMCoreServiceHost.dll.config muss auf „true“ gesetzt werden.

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



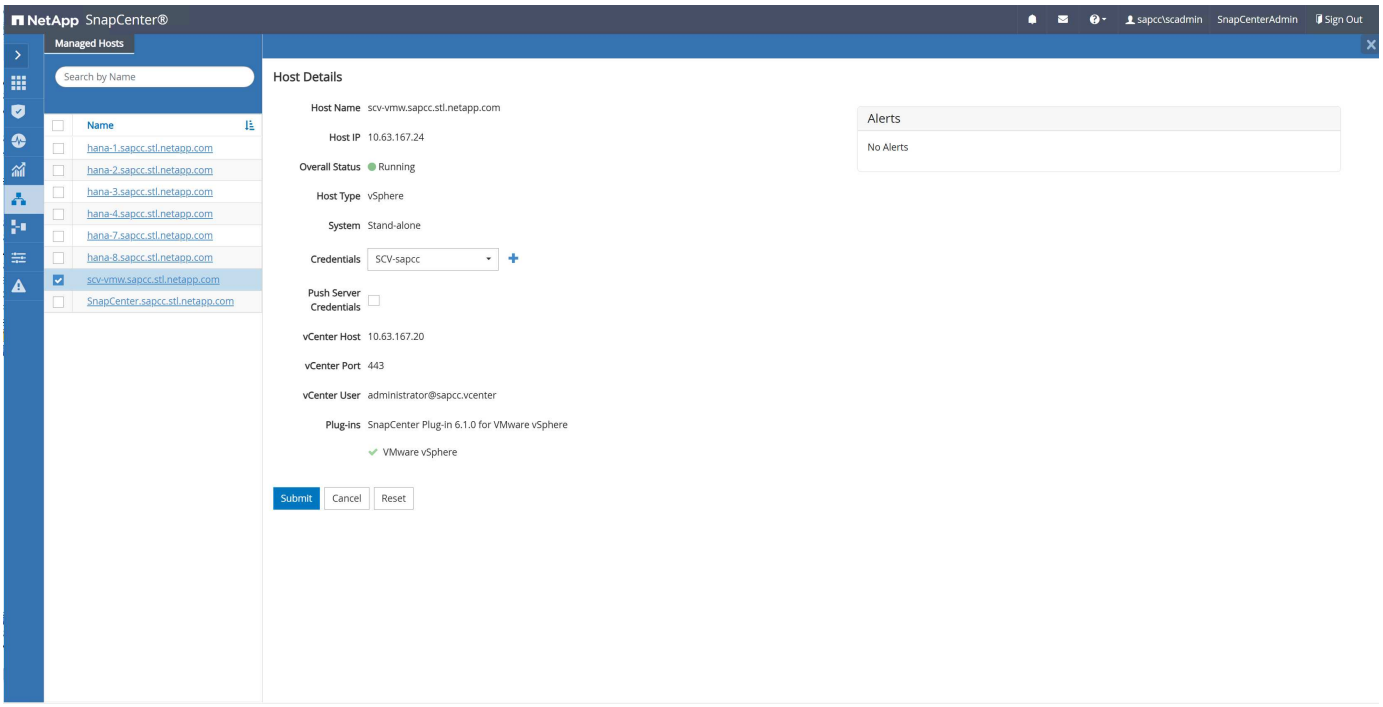
Nachdem die Änderung vorgenommen wurde, muss der SnapCenter SMCore-Dienst gestoppt und gestartet werden.



VMware-Plugin zu SnapCenter hinzufügen

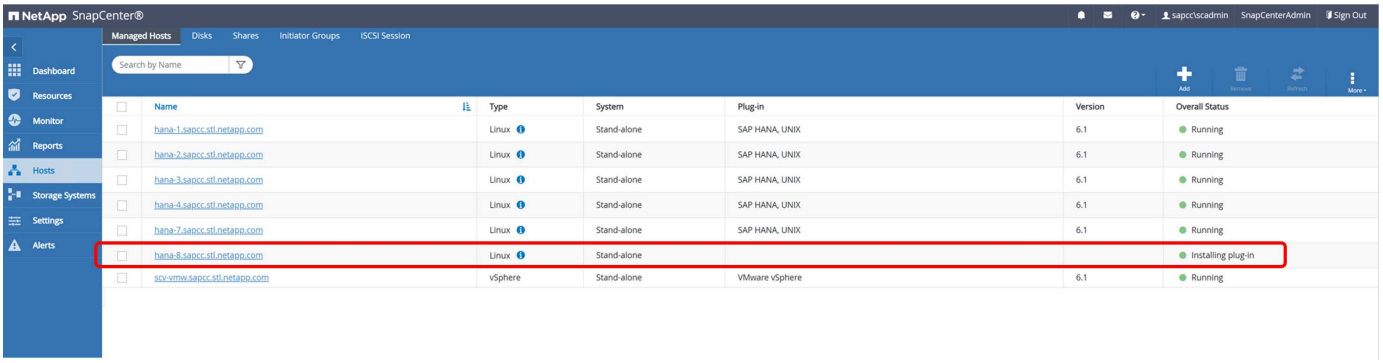
Bevor der Host in SnapCenter hinzugefügt werden kann, muss das SnapCenter Plug-in für VMware vSphere in der VMware Umgebung implementiert werden. Siehe auch "Implementieren Sie das SnapCenter Plug-in für VMware vSphere".

Die Anmeldeinformationen müssen während des Host-Add-Workflows festgelegt werden, wobei vSphere als Hosttyp ausgewählt werden kann.

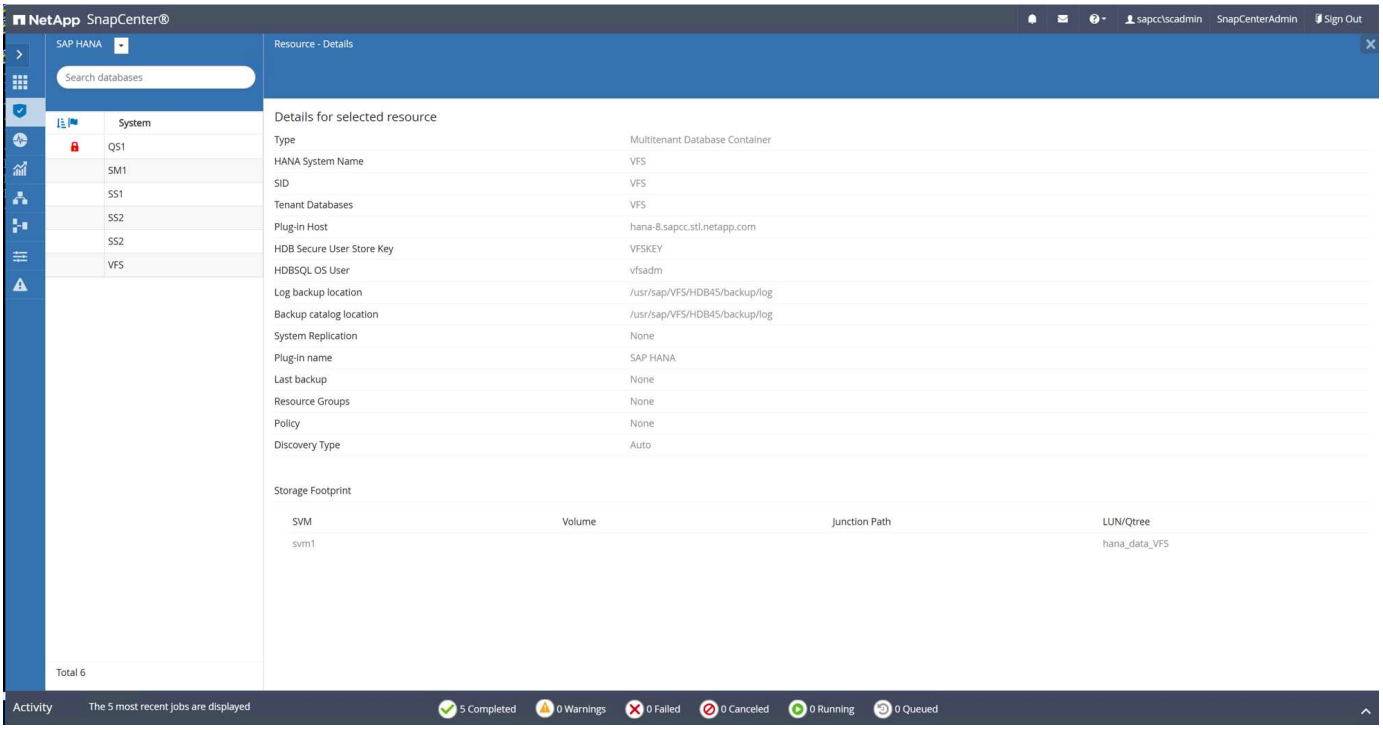


HANA-Host hinzufügen

Keine besonderen Anforderungen. Plugin-Bereitstellung und automatische Erkennung erfolgt wie gewohnt.



Mit dem automatischen Erkennungsprozess erkennt SnapCenter , dass die HANA-Ressource virtualisiert mit VMFS ausgeführt wird.

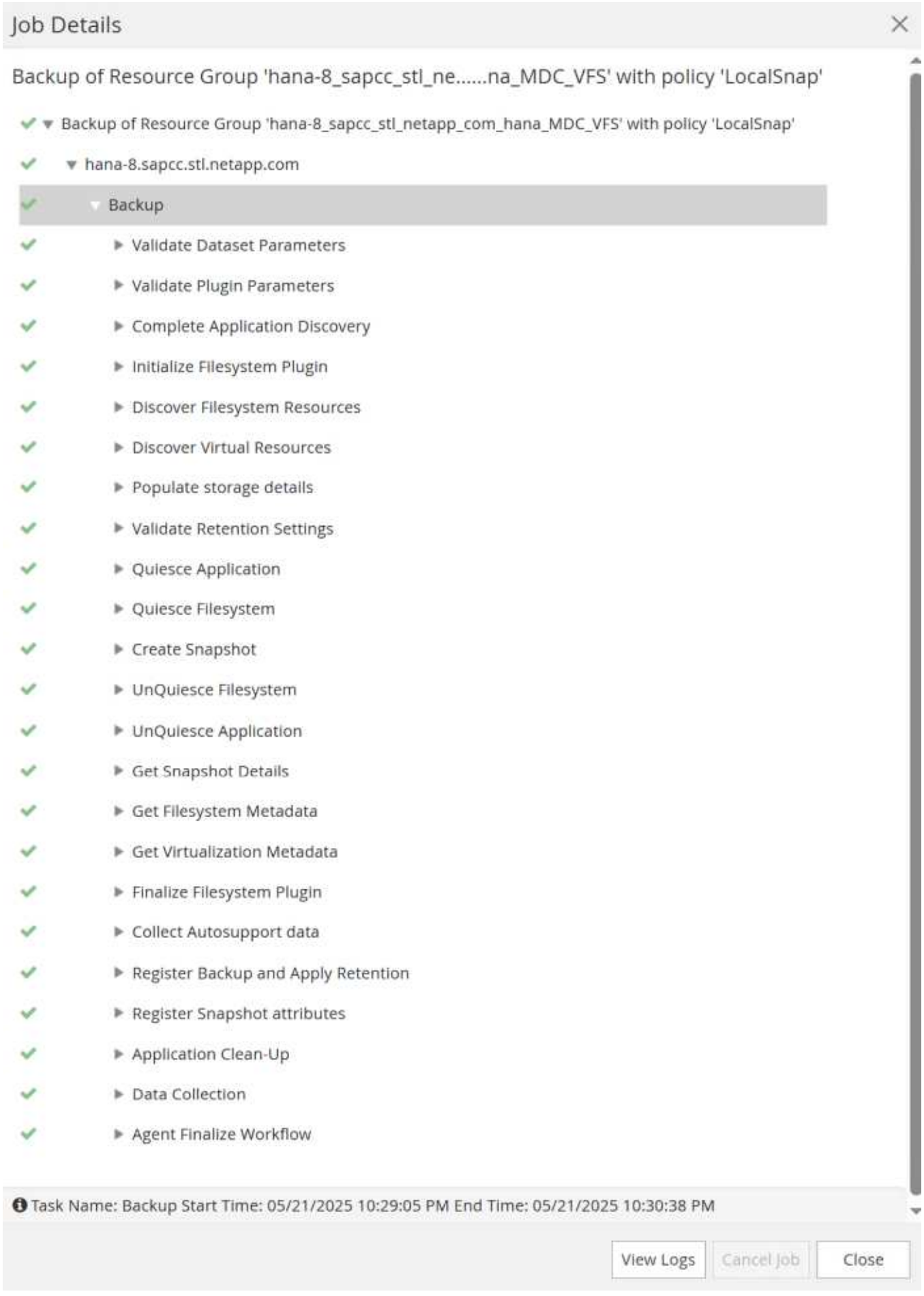


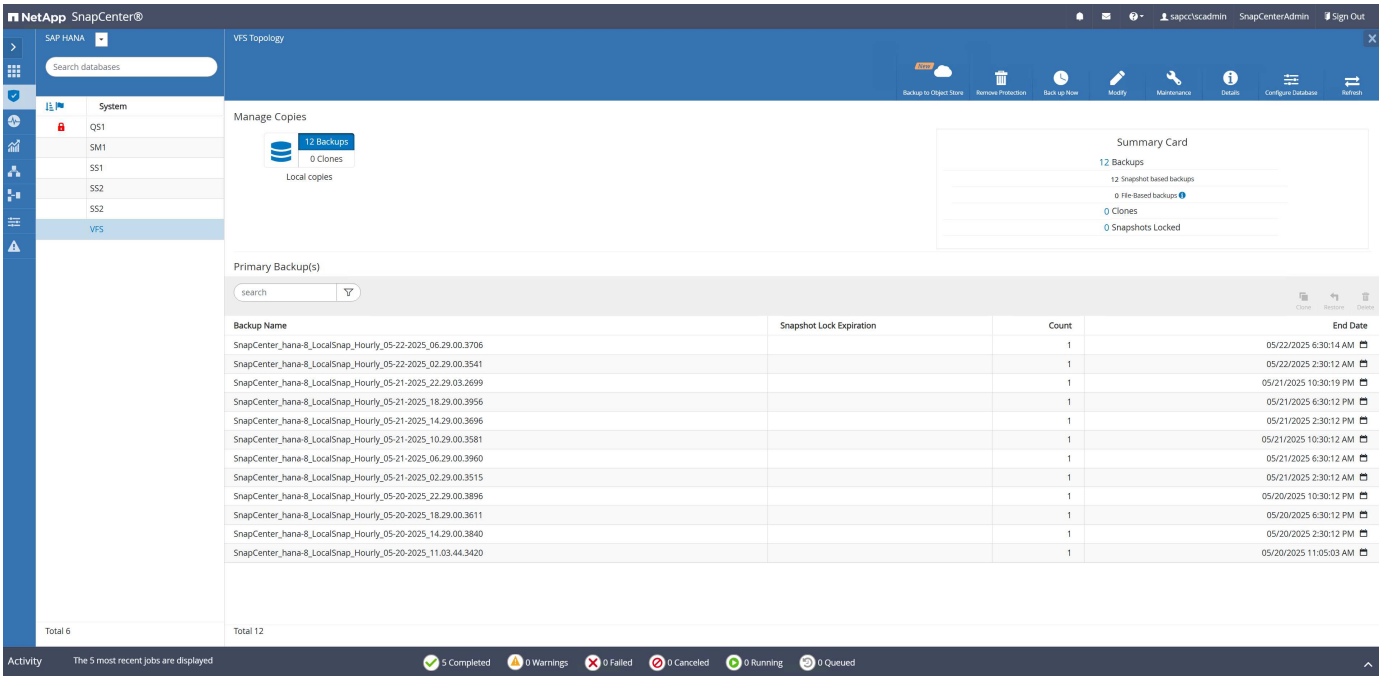
Konfiguration von Richtlinien und Ressourcenschutz

Nichts Spezifisches für VMware mit VMFS.

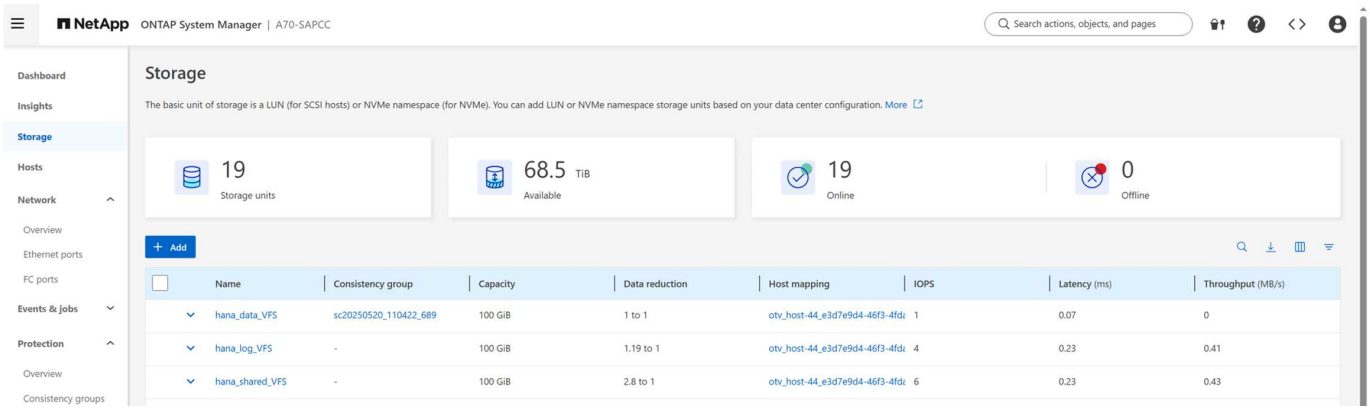
Backup-Vorgänge

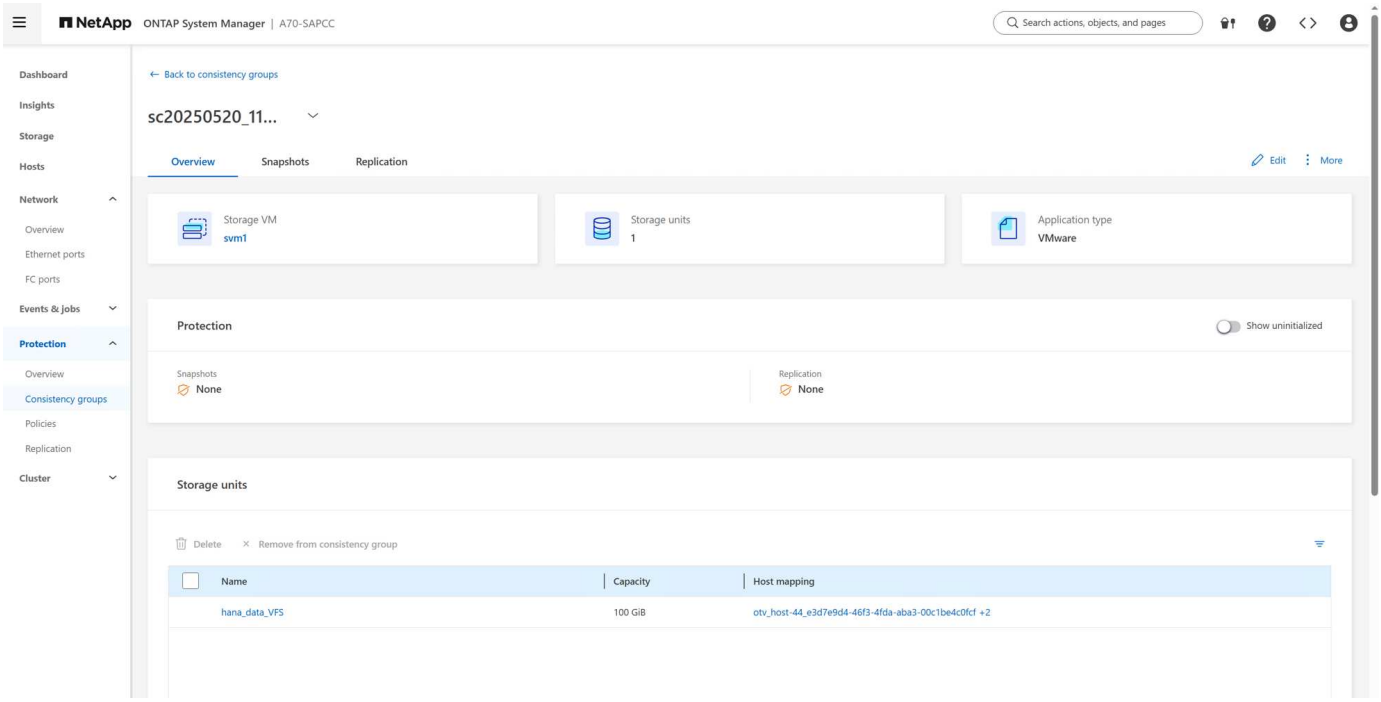
Nichts Spezifisches für VMware mit VMFS.

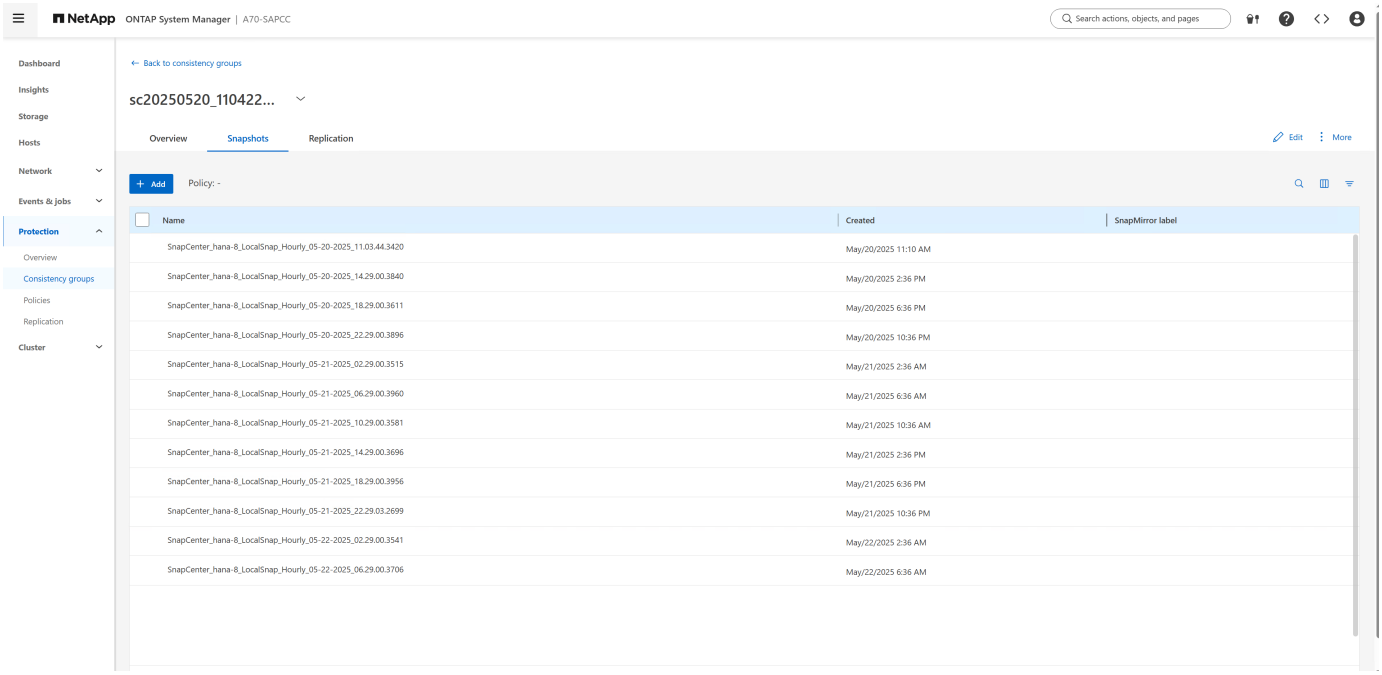

Job Details
Backup of Resource Group 'hana-8_sapcc_stl_ne.....na_MDC_VFS' with policy 'LocalSnap'
Backup of Resource Group 'hana-8_sapcc_stl_netapp_com_hana_MDC_VFS' with policy 'LocalSnap'
hana-8.sapcc.stl.netapp.com
Backup
Validate Dataset Parameters
Validate Plugin Parameters
Complete Application Discovery
Initialize Filesystem Plugin
Discover Filesystem Resources
Discover Virtual Resources
Populate storage details
Validate Retention Settings
Quiesce Application
Quiesce Filesystem
Create Snapshot
UnQuiesce Filesystem
UnQuiesce Application
Get Snapshot Details
Get Filesystem Metadata
Get Virtualization Metadata
Finalize Filesystem Plugin
Collect Autosupport data
Register Backup and Apply Retention
Register Snapshot attributes
Application Clean-Up
Data Collection
Agent Finalize Workflow
Task Name: Backup Start Time: 05/21/2025 10:29:05 PM End Time: 05/21/2025 10:30:38 PM
View Logs
Cancel Job
Close



SnapCenter erstellt eine Konsistenzgruppe (CG) und fügt der CG die Speichereinheit hana_data_VFS hinzu. Snapshots werden auf CG-Ebene erstellt.







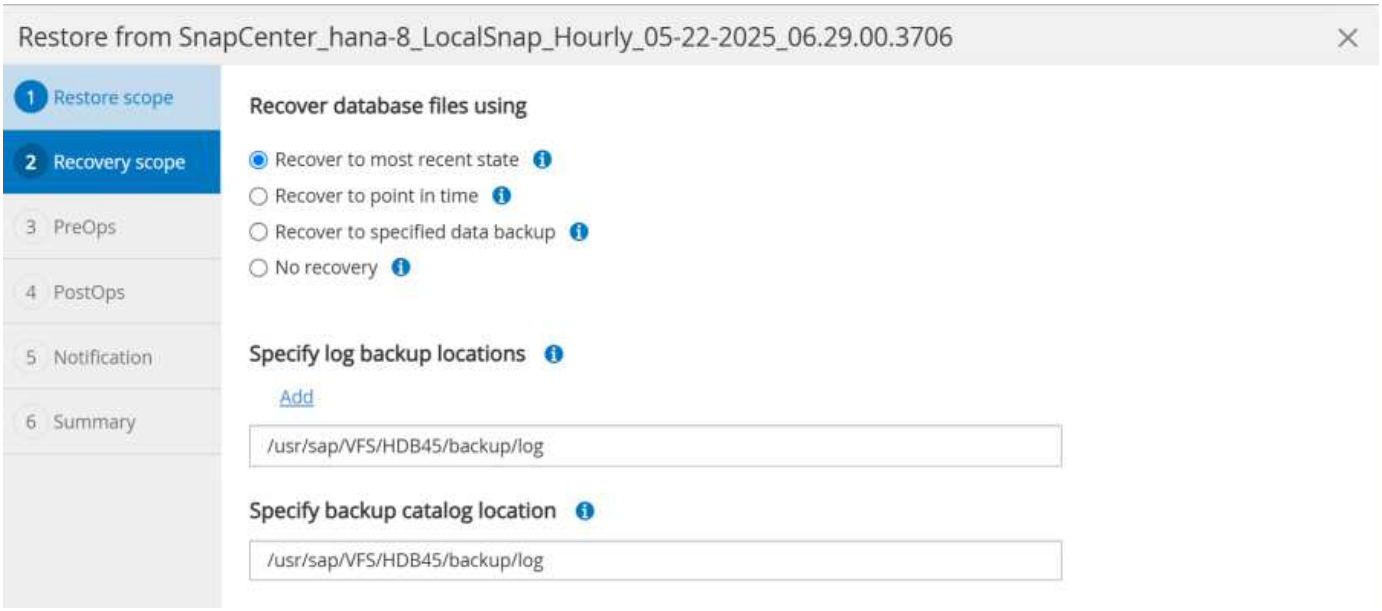
Restore- und Recovery-Vorgänge

Bei virtuellen Ressourcen, die auf dem SnapCenter von VMFS/VMDK gespeichert sind, werden Wiederherstellungsvorgänge immer durch einen Klon-, Mount- und Kopiervorgang durchgeführt.

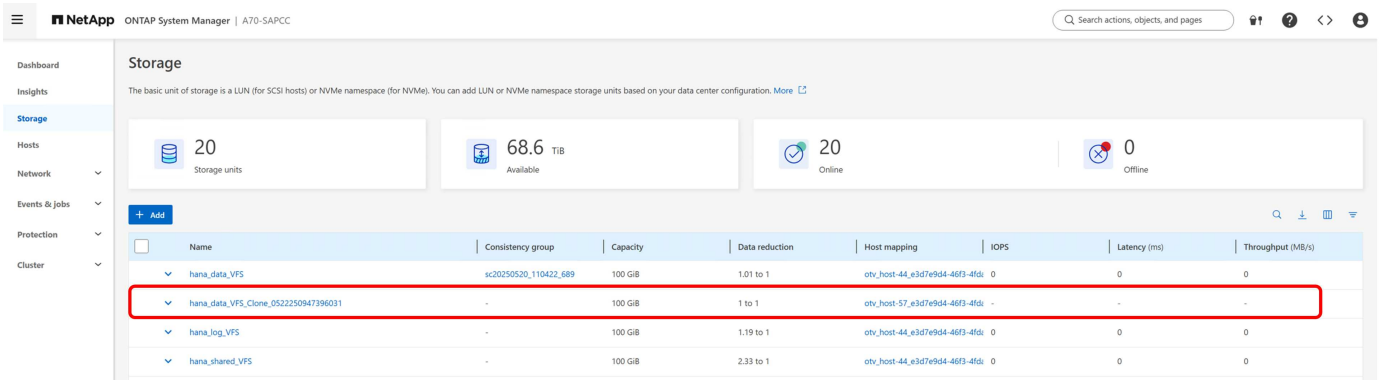
1. SnapCenter erstellt einen Speicherklon basierend auf dem ausgewählten Snapshot
2. SnapCenter mountet die LUN als neuen Datenspeicher auf dem ESX-Host
3. SnapCenter fügt die VMDK innerhalb des Datenspeichers der HANA-VM als neue Festplatte hinzu
4. SnapCenter bindet die neue Festplatte an das Linux Betriebssystem an
5. SnapCenter kopiert die Daten von der neuen Festplatte zurück in den ursprünglichen Speicherort

6. Wenn der Kopiervorgang abgeschlossen ist, werden alle oben genannten Ressourcen wieder entfernt
7. SnapCenter führt die Wiederherstellung der HANA-Systemdatenbank durch
8. SnapCenter führt die Wiederherstellung der HANA-Tenant-Datenbank durch

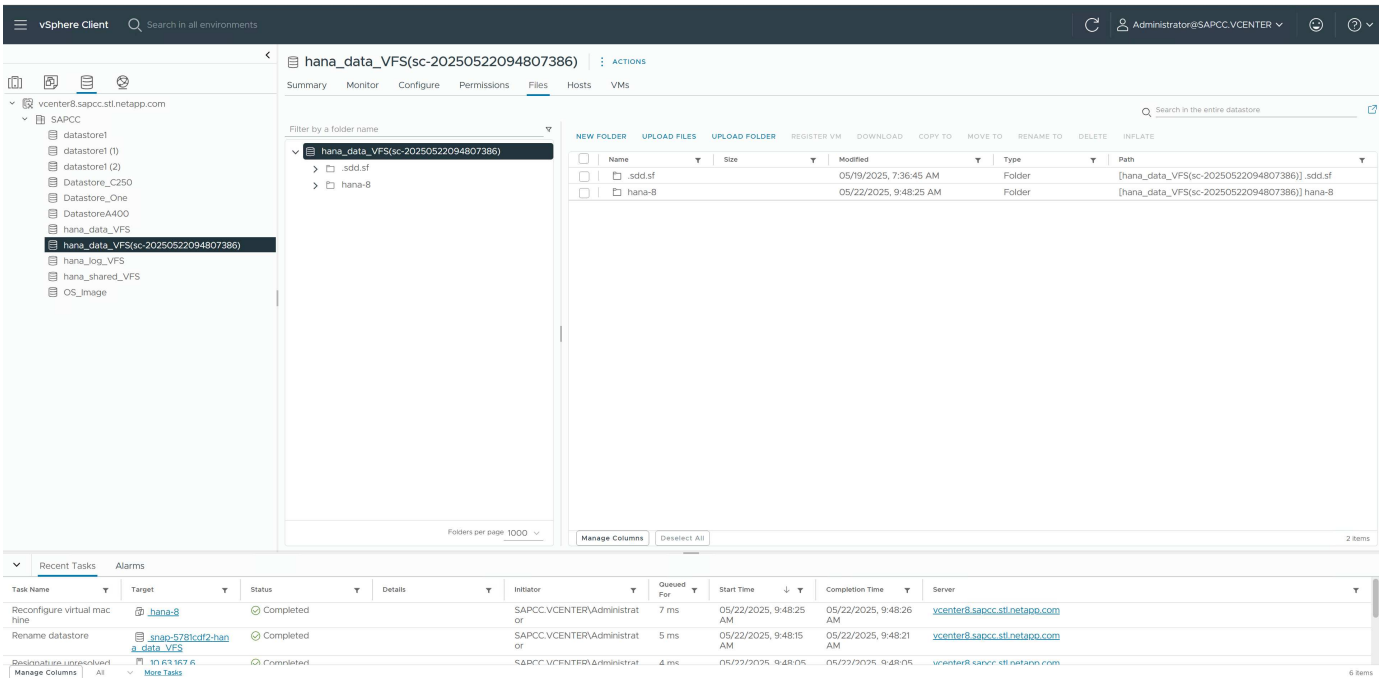
Die Gesamtlaufzeit des Wiederherstellungsvorgangs hängt von der Datenbankgröße und dem Durchsatz der FC-Verbindung zwischen den Storage-Clustern und den ESX-Hosts ab. In unserem Laboraufbau mit einer initialen HANA-Installation betrug die Laufzeit etwa 12 Minuten.



Während der Wiederherstellungsvorgang ausgeführt wird, können Sie eine neue geklonte Speichereinheit sehen.

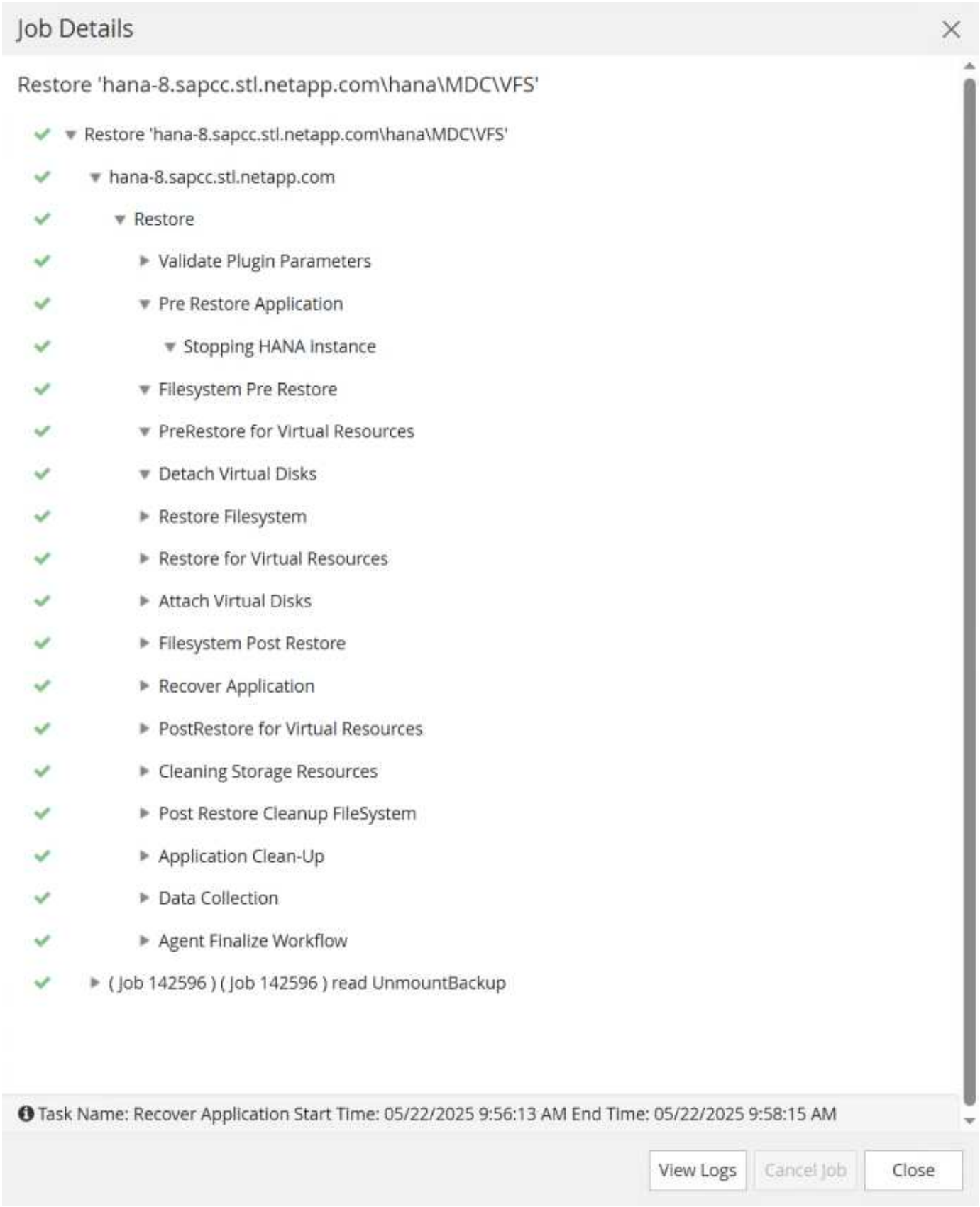


Die neue LUN (Datenspeicher) basierend auf der geklonten Speichereinheit wird an den ESX-Cluster angeschlossen.



Die VMDK im Datenspeicher wird der Ziel-HANA-VM zugeordnet und im HANA-System bereitgestellt.

```
hana-8:~ # df -h

Filesystem Size Used Avail Use% Mounted on
/dev/mapper/system-root 60G 5.3G 54G 9% /
devtmpfs 4.0M 8.0K 4.0M 1% /dev
tmpfs 49G 0 49G 0% /dev/shm
efivarfs 256K 57K 195K 23% /sys/firmware/efi/efivars
tmpfs 13G 26M 13G 1% /run
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev-
early.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysctl.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysusers.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev.service
/dev/mapper/system-root 60G 5.3G 54G 9% /.snapshots
/dev/mapper/system-root 60G 5.3G 54G 9% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 5.3G 54G 9% /boot/grub2/x86++_++64-efi
/dev/mapper/system-root 60G 5.3G 54G 9% /home
/dev/mapper/system-root 60G 5.3G 54G 9% /opt
/dev/mapper/system-root 60G 5.3G 54G 9% /root
/dev/mapper/system-root 60G 5.3G 54G 9% /srv
/dev/mapper/system-root 60G 5.3G 54G 9% /usr/local
/dev/mapper/system-root 60G 5.3G 54G 9% /tmp
/dev/mapper/system-root 60G 5.3G 54G 9% /var
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-vconsole-setup.service
/dev/sdc 95G 8.9G 87G 10% /hana/log/VFS/mnt00001
/dev/sdb 95G 7.6G 88G 8% /hana/data/VFS/mnt00001
/dev/sdd 95G 15G 81G 16% /hana/shared
/dev/sda1 253M 5.9M 247M 3% /boot/efi
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup.service
192.168.175.86:/sapcc_share 1.4T 858G 568G 61% /mnt/sapcc-share
tmpfs 6.3G 72K 6.3G 1% /run/user/464
tmpfs 1.0M 0 1.0M 0% /run/credentials/getty@tty1.service
tmpfs 6.3G 52K 6.3G 1% /run/user/0
/dev/sde 95G 9.2G 86G 10%
/var/opt/snapcenter/scu/clones/hana_data_VFS_mnt00001_142592_scu_clone_1

hana-8:~ #
```



SAP-Systemaktualisierung

Detaillierte Informationen zu SAP System Refresh-Operationen mit SnapCenter finden Sie unter "TR-4667: Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter" .

Das zweite HANA-System QFS wurde auf die gleiche Weise provisioniert wie im Kapitel "„Bereitstellung und Installation des HANA-Systems“" .

Voraussetzungen

Die aktuelle Version von SnapCenter (6.1P1) weist einige Einschränkungen auf, die mit den nächsten Versionen behoben werden sollen.

1. Es ist erforderlich, den SPL-Prozess nach jedem „Clone Create“- und „Clone Delete“-Workflow mit dem Befehl „systemctl restart spl“ auf dem Ziel-HANA-Host neu zu starten.
2. Die als Quelle und Ziel des SAP-Systemaktualisierungsvorgangs verwendeten HANA-VMs müssen auf demselben ESX-Host ausgeführt werden.

Workflow-Zusammenfassung

Bevor der erste SAP-Systemaktualisierungsvorgang ausgeführt werden kann, muss das HANA-Zielsystem installiert und der Host zu SnapCenter hinzugefügt werden. Anschließend muss das HANA-System heruntergefahren und der HANA-Datenträger vom Host getrennt werden.

SnapCenter Klon-Erstellungsworkflow

1. Speicherklon erstellen
2. Konfigurieren der Hostzuordnung für den Speicherklon
3. Speicherklon (Datenspeicher) an ESX-Host anhängen
4. Fügen Sie der HANA-Ziel-VM eine neue Festplatte aus dem Datenspeicher hinzu
5. Datenträger in HANA VM-Betriebssystem einbinden
6. Wiederherstellen des HANA-Systems mithilfe von Postscript

Laufzeit: 12 Minuten

> ⓘ Im Vergleich zum Wiederherstellungsvorgang ist die Laufzeit des Klonvorgangs unabhängig von der Größe der HANA-Datenbank. Die Laufzeit der Schritte 1 bis 5 ist auch bei sehr großen Datenbanken ähnlich. Die Wiederherstellung dauert bei größeren HANA-Systemen natürlich länger.

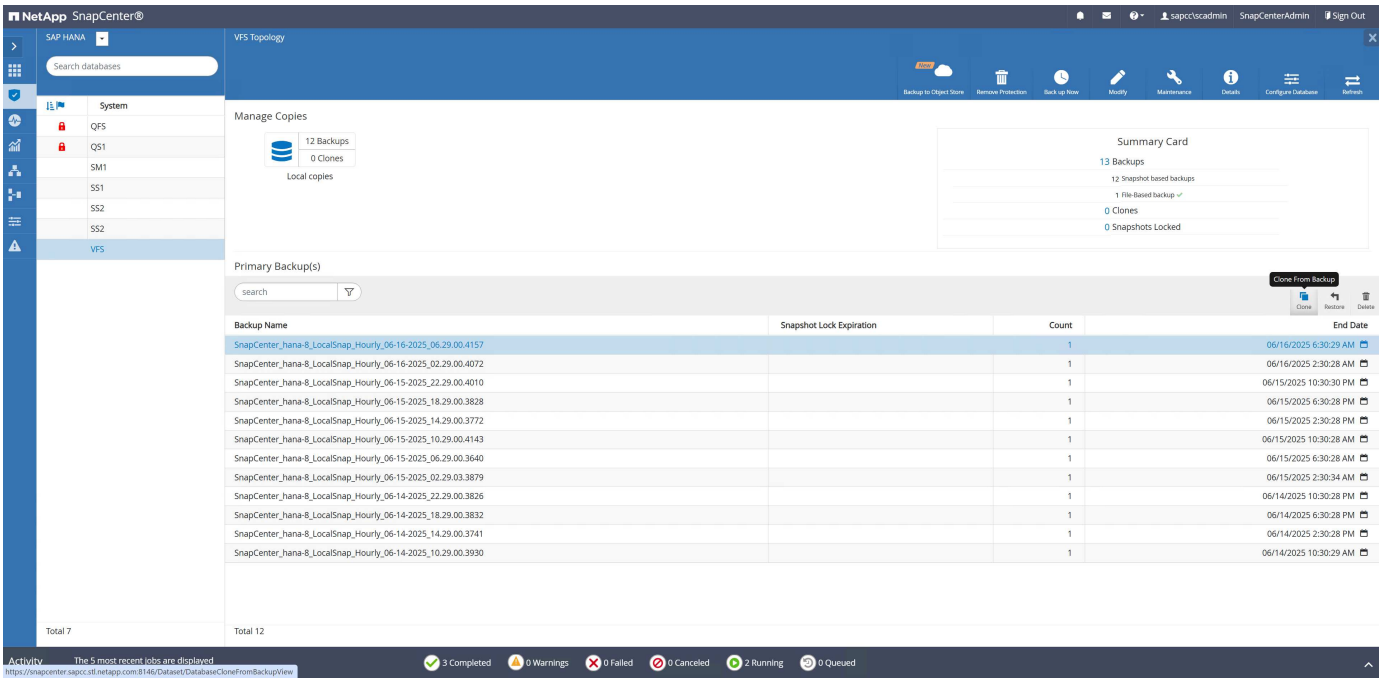
SnapCenter -Klon-Löschworkflow

1. Herunterfahren des HANA-Systems mithilfe eines vordefinierten Skripts
2. Datenträger vom HANA VM-Betriebssystem trennen
3. Datenträger aus HANA-VM entfernen
4. Entfernen des Datenspeichers vom ESX-Host
5. Storge-Klon löschen

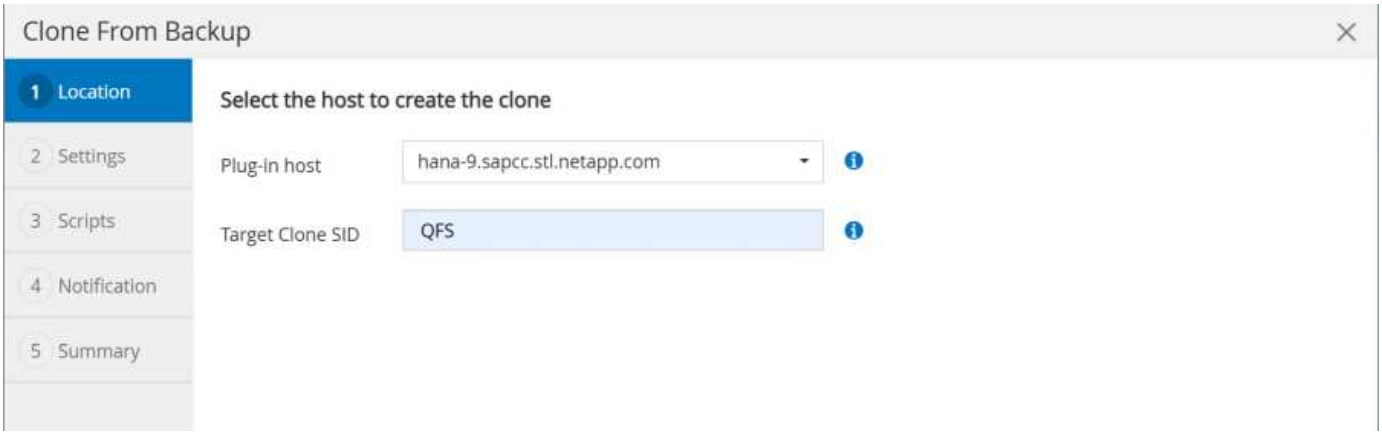
Laufzeit: 11 Minuten

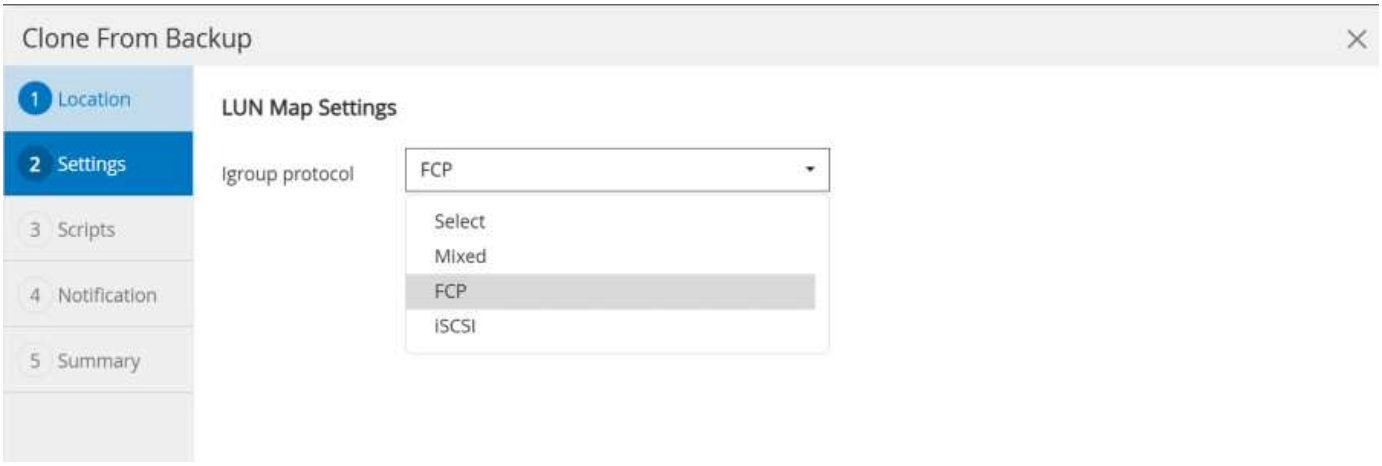
SnapCenter Klon-Erstellungsworkflow

Der Workflow zum Erstellen eines Klons wird durch Auswahl des gewünschten Snapshots und Klicken auf die Schaltfläche „Klonen“ gestartet.

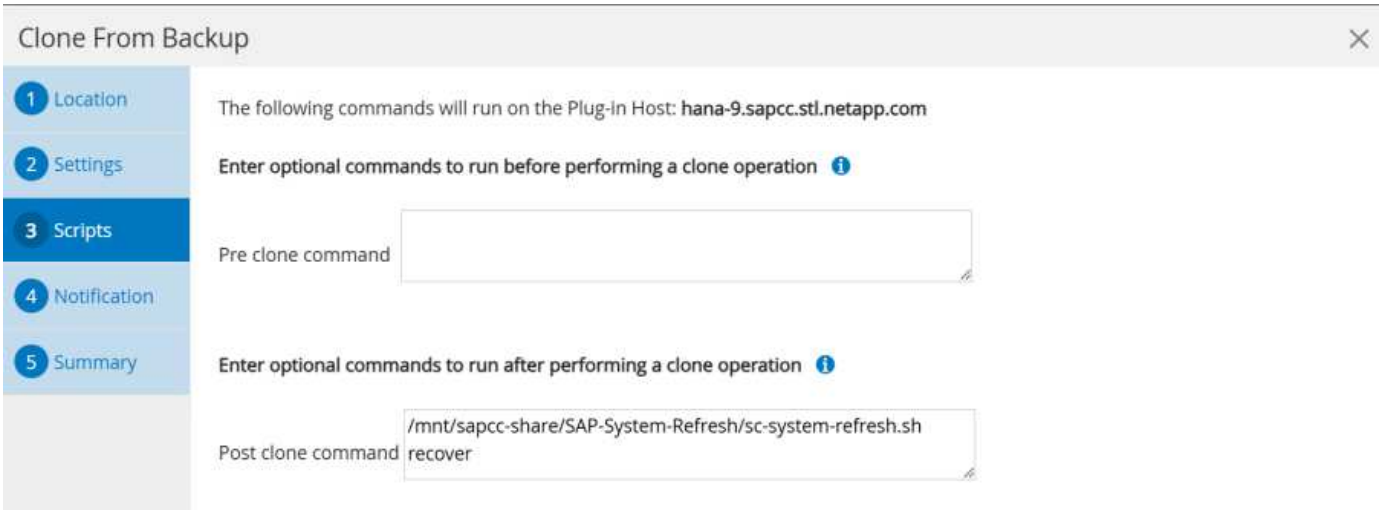


Der Zielhost und die SID müssen angegeben werden.

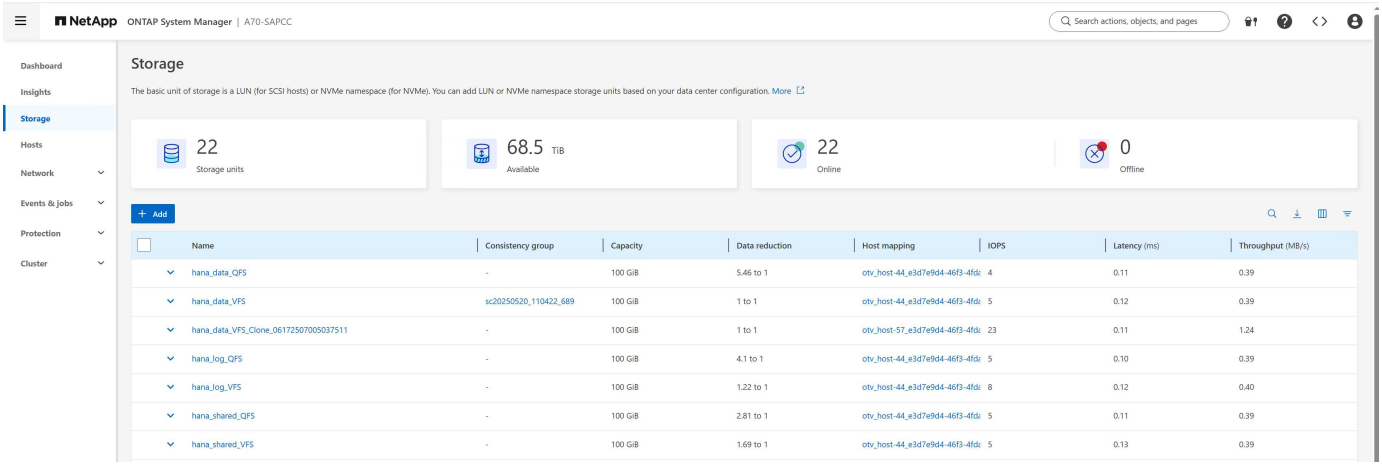




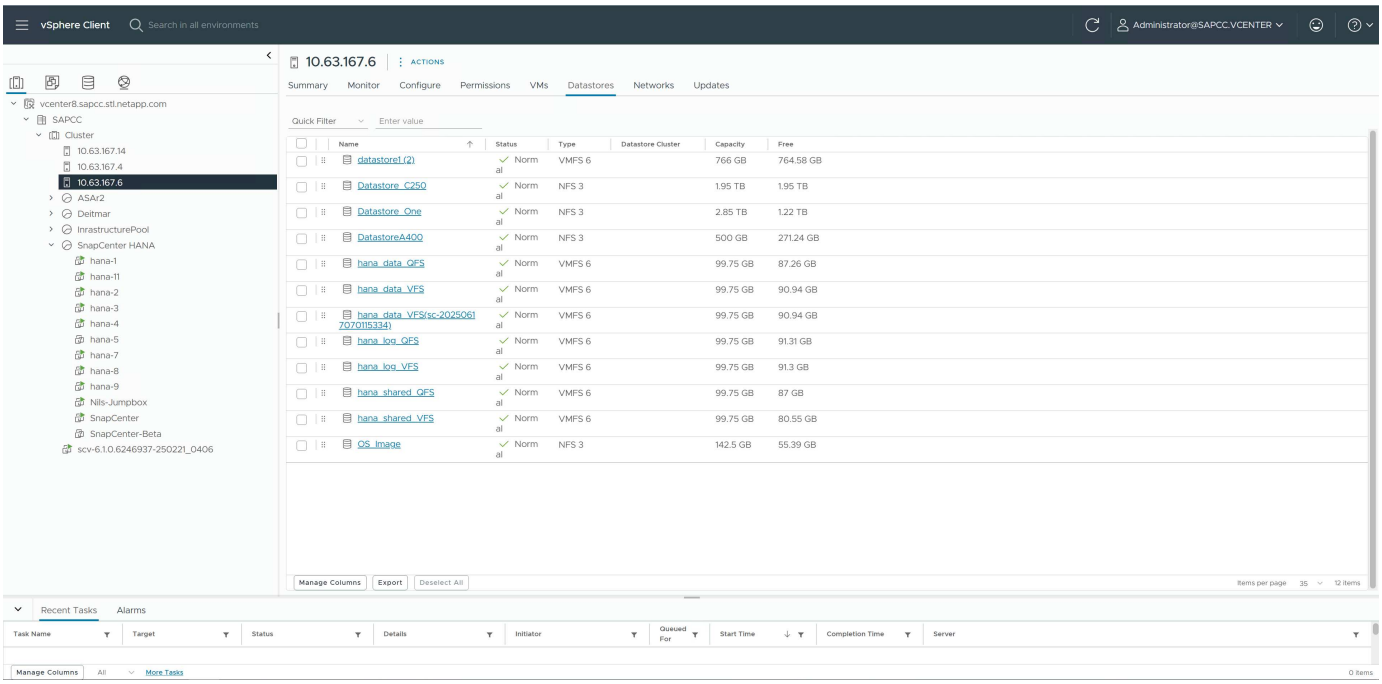
In unserem Beispiel verwenden wir ein Postskript, um die Wiederherstellung auf dem Zielhost auszuführen.



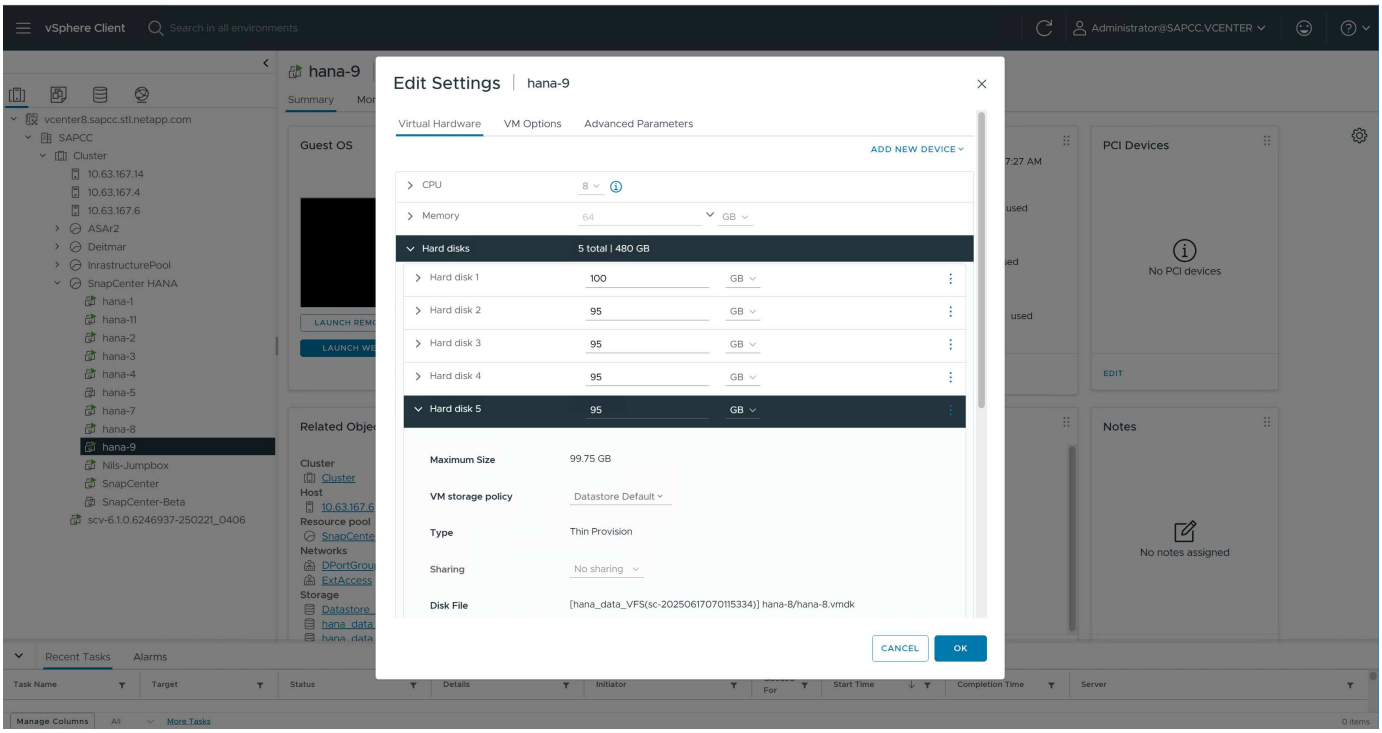
Wenn der Workflow gestartet wird, erstellt SnapCenter eine geklonte Speichereinheit basierend auf dem ausgewählten Snapshot.



SnapCenter verbindet dann die LUN (Datenspeicher) mit dem ESX-Host, auf dem die Ziel-HANA-VM ausgeführt wird.



Das VMDK im neuen Datenspeicher wird dann zur HANA-VM hinzugefügt.



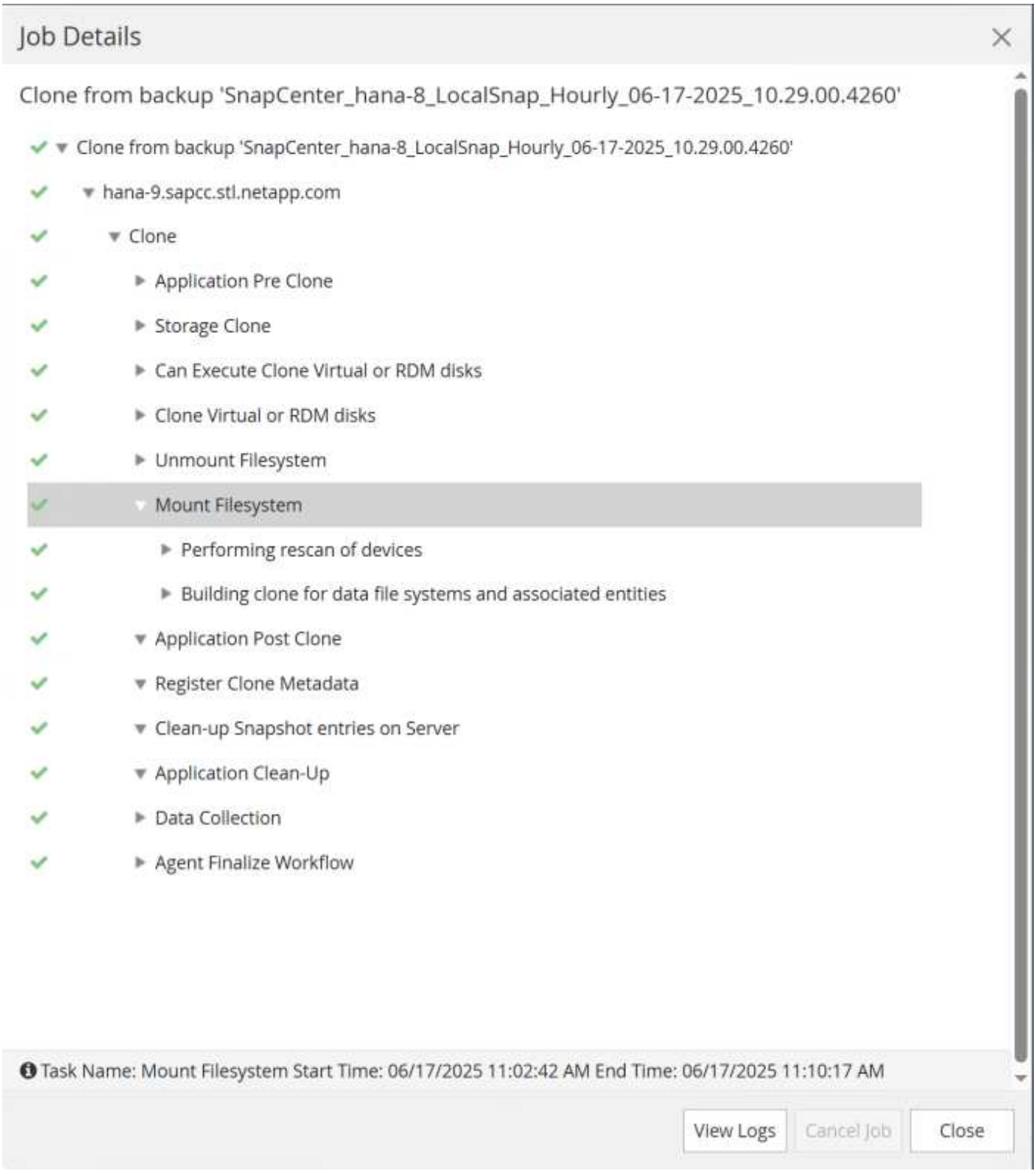
Anschließend konfiguriert und mountet SnapCenter die neue Festplatte im HANA-Linux-System.

```
hana-9:/mnt/sapcc-share/SAP-System-Refresh # df -h

Filesystem Size Used Avail Use% Mounted on
/dev/mapper/system-root 60G 5.2G 52G 10% /
devtmpfs 4.0M 4.0K 4.0M 1% /dev
tmpfs 49G 0 49G 0% /dev/shm
```

```
efivarfs 256K 57K 195K 23% /sys/firmware/efi/efivars
tmpfs 13G 26M 13G 1% /run
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev-
early.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysctl.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysusers.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev.service
/dev/mapper/system-root 60G 5.2G 52G 10% /.snapshots
/dev/mapper/system-root 60G 5.2G 52G 10% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 5.2G 52G 10% /boot/grub2/x86++_++64-efi
/dev/mapper/system-root 60G 5.2G 52G 10% /home
/dev/mapper/system-root 60G 5.2G 52G 10% /opt
/dev/mapper/system-root 60G 5.2G 52G 10% /srv
/dev/mapper/system-root 60G 5.2G 52G 10% /root
/dev/mapper/system-root 60G 5.2G 52G 10% /tmp
/dev/mapper/system-root 60G 5.2G 52G 10% /usr/local
/dev/mapper/system-root 60G 5.2G 52G 10% /var
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-vconsole-setup.service
/dev/sdc 95G 8.9G 87G 10% /hana/log/QFS/mnt00001
/dev/sdd 95G 14G 82G 14% /hana/shared
/dev/sda1 253M 5.9M 247M 3% /boot/efi
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup.service
192.168.175.86:/sapcc++_++share 1.4T 858G 568G 61% /mnt/sapcc-share
tmpfs 6.3G 72K 6.3G 1% /run/user/464
tmpfs 1.0M 0 1.0M 0% /run/credentials/getty@tty1.service
tmpfs 6.3G 52K 6.3G 1% /run/user/0
/dev/sde 95G 9.2G 86G 10% /hana/data/QFS/mnt00001
tmpfs 6.3G 56K 6.3G 1% /run/user/1001
hana-9:/mnt/sapcc-share/SAP-System-Refresh #

hana-9:/mnt/sapcc-share/SAP-System-Refresh # cat /etc/fstab
/dev/system/root / btrfs defaults 0 0
/dev/system/root /var btrfs subvol=/@/var 0 0
/dev/system/root /usr/local btrfs subvol=/@/usr/local 0 0
/dev/system/root /tmp btrfs subvol=/@/tmp 0 0
/dev/system/root /srv btrfs subvol=/@/srv 0 0
/dev/system/root /root btrfs subvol=/@/root 0 0
/dev/system/root /opt btrfs subvol=/@/opt 0 0
/dev/system/root /home btrfs subvol=/@/home 0 0
/dev/system/root /boot/grub2/x86++_++64-efi btrfs
subvol=/@/boot/grub2/x86++_++64-efi 0 0
/dev/system/root /boot/grub2/i386-pc btrfs subvol=/@/boot/grub2/i386-pc 0
0
/dev/system/swap swap swap defaults 0 0
/dev/system/root /.snapshots btrfs subvol=/@/.snapshots 0 0
UUID=FB79-24DC /boot/efi vfat utf8 0 2
```

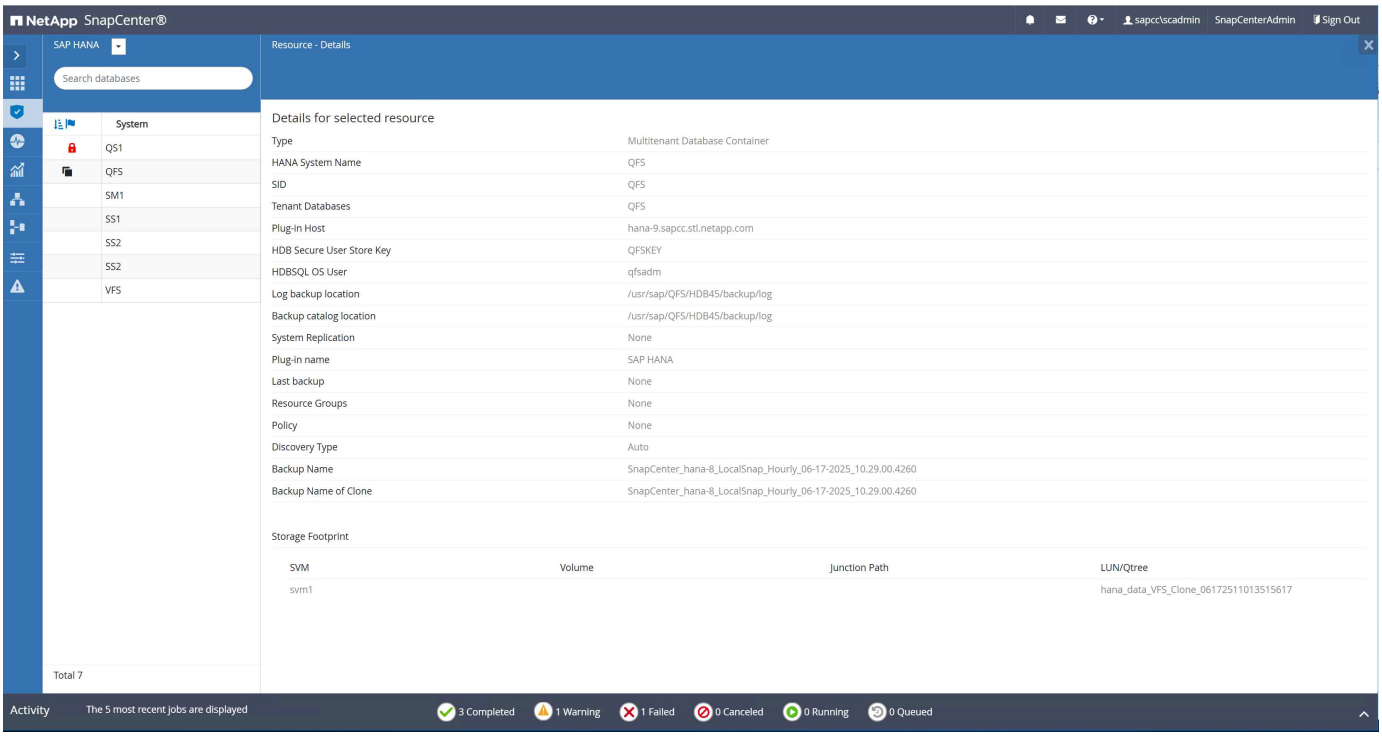
```
192.168.175.86:/sapcc++_++share /mnt/sapcc-share nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0
0
#/dev/sdb /hana/data/QFS/mnt00001 xfs relatime,inode64 0 0
/dev/sdc /hana/log/QFS/mnt00001 xfs relatime,inode64 0 0
/dev/sdd /hana/shared xfs defaults 0 0
# The following entry has been added by NetApp (SnapCenter Plug-in for
UNIX)
/dev/sde /hana/data/QFS/mnt00001 xfs
rw,relatime,attr2,inode64,logbufs=8,logbsize=32k,noquota 0 0
hana-9:/mnt/sapcc-share/SAP-System-Refresh #
```

Der folgende Screenshot zeigt die von SnapCenter ausgeführten Jobschritte.



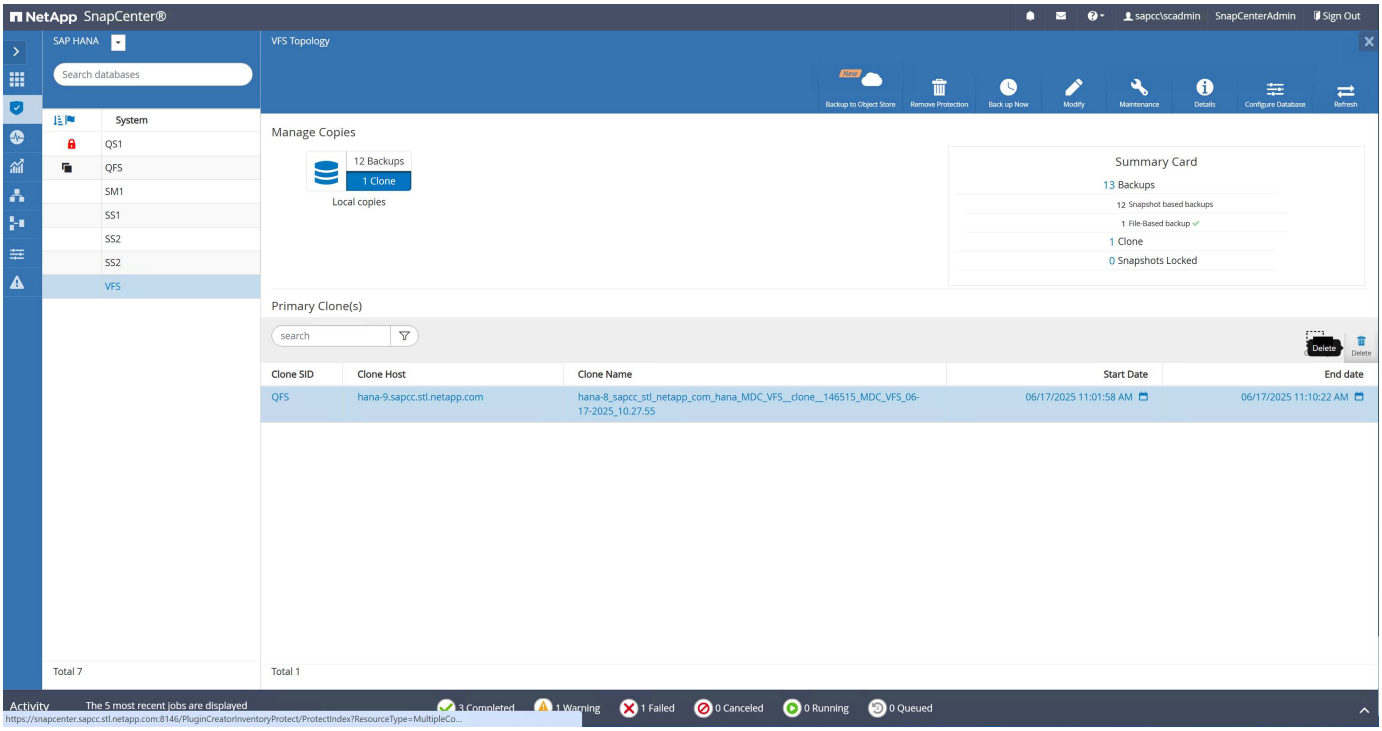
Wie im Abschnitt „Voraussetzungen“ erwähnt, muss der SnapCenter -SPL-Dienst auf dem HANA-Host mit dem Befehl „systemctl restart spl“ neu gestartet werden, um die ordnungsgemäße Bereinigung einzuleiten. Dies muss nach Abschluss des Auftrags erfolgen.

Sobald der Klon-Workflow abgeschlossen ist, kann die automatische Erkennung durch Klicken auf das Ressourcen-QFS gestartet werden. Sobald der automatische Erkennungsprozess abgeschlossen ist, wird der neue Speicherbedarf in der Detailansicht der Ressource angezeigt.

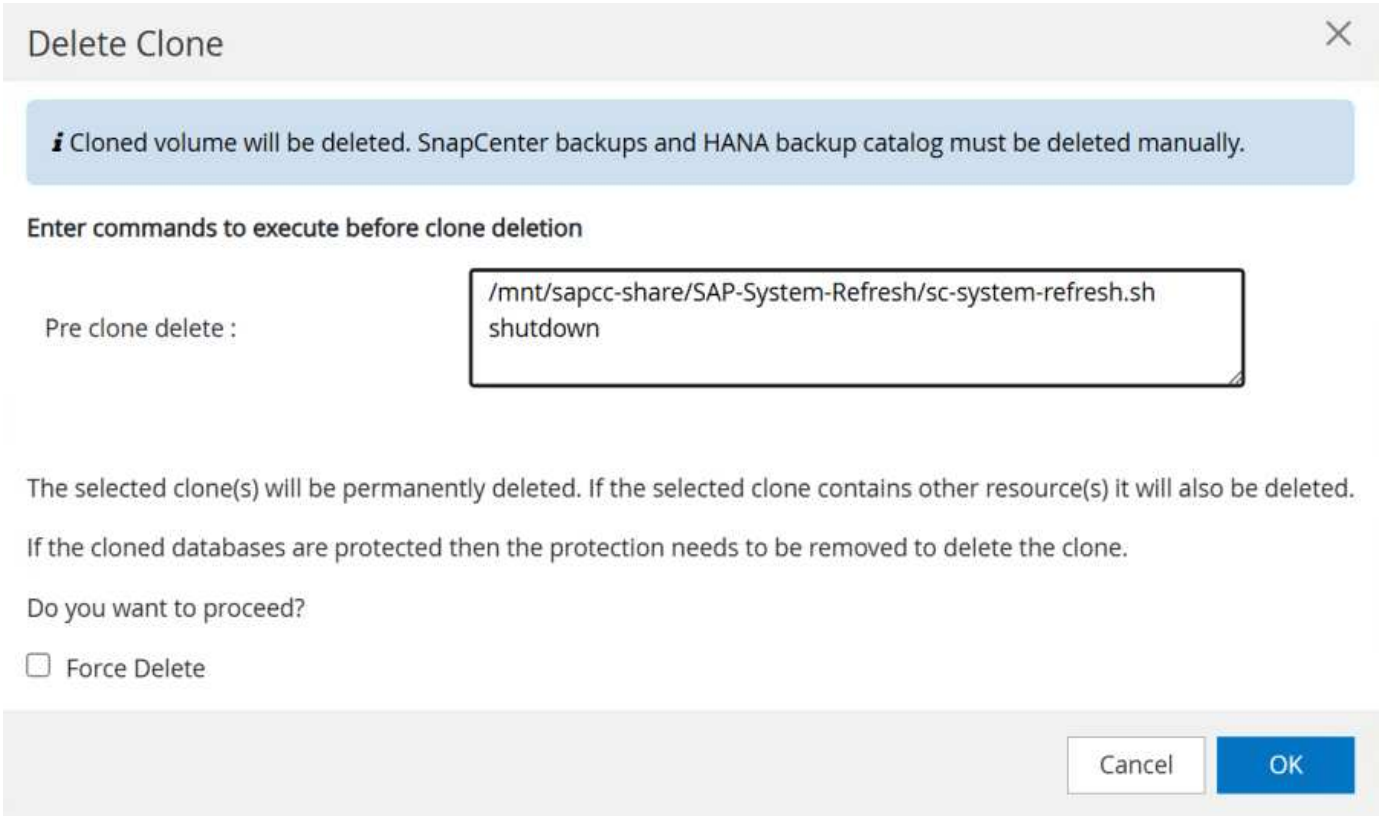


SnapCenter -Klon-Löschworkflow

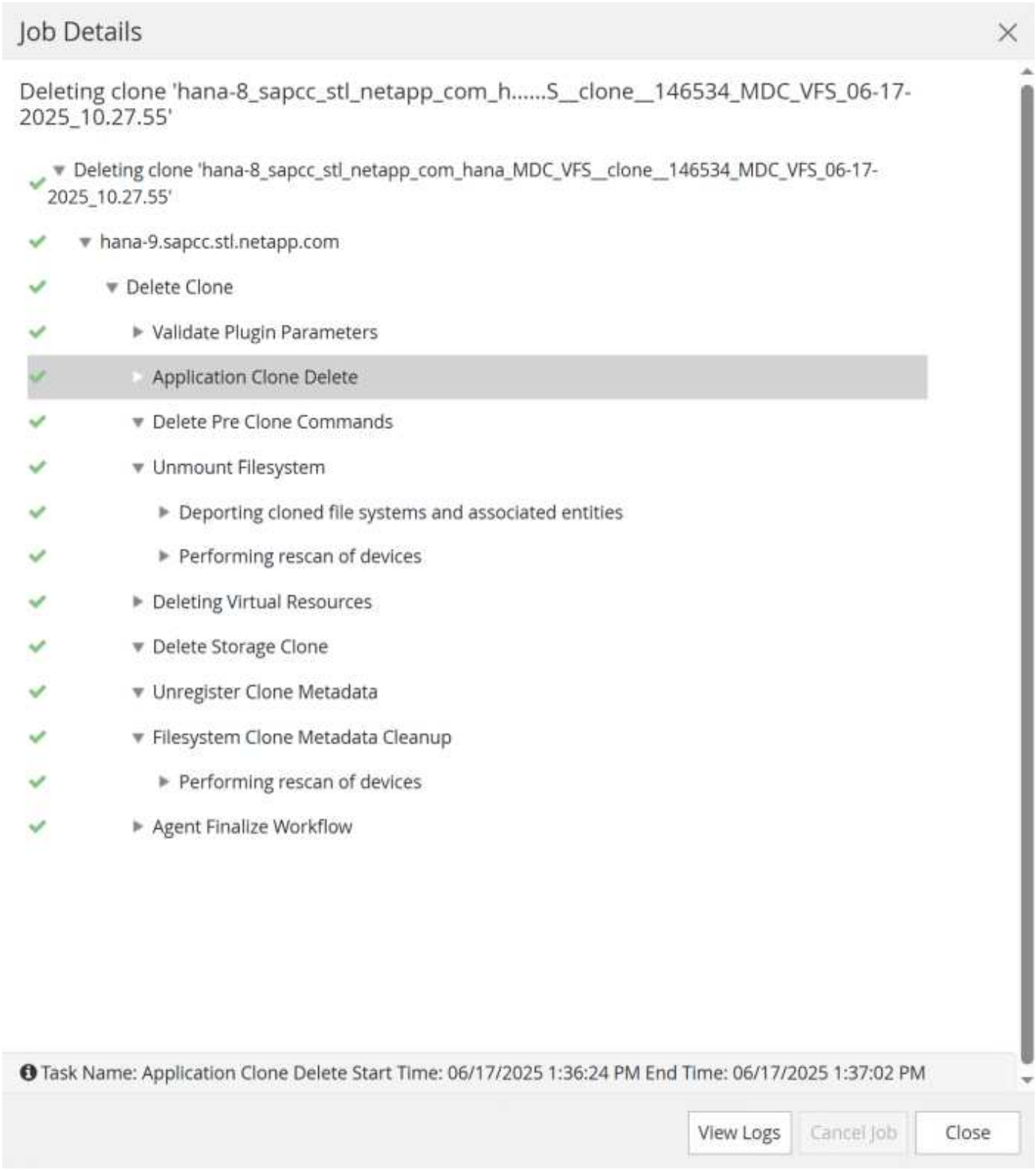
Der Klonlösch-Workflow wird gestartet, indem Sie den Klon bei der HANA-Quellressource auswählen und auf die Schaltfläche „Löschen“ klicken.



In unserem Beispiel verwenden wir ein Vorskript, um die Ziel-HANA-Datenbank herunterzufahren.



Der folgende Screenshot zeigt die von SnapCenter ausgeführten Jobschritte.



Wie im Abschnitt „Voraussetzungen“ erwähnt, muss der SnapCenter -SPL-Dienst auf dem HANA-Host mit dem Befehl „systemctl restart spl“ neu gestartet werden, um eine ordnungsgemäße Bereinigung einzuleiten.

Zusätzliche Informationen und Versionsverlauf

Bewährte Methoden für HANA:

- "Technischer Bericht: SAP HANA on NetApp ASA Systems with Fibre Channel Protocol".

SnapCenter

- "TR-4614: SAP HANA Backup und Recovery mit SnapCenter"
- "TR-4719: SAP HANA System Replication – Backup und Recovery mit SnapCenter"
- "TR-4667: Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter"
- "SAP HANA-Datenschutz und hohe Verfügbarkeit mit SnapCenter SnapMirror Active Sync und VMware Metro Storage Cluster"
- "SnapCenter-Softwaredokumentation"

Versionsverlauf:

Version	Datum	Kommentar
Version 1.0	07/2025	Ausgangsversion

BlueXP Backup and Recovery for SAP HANA – Cloud-Objekt-Storage als Backup-Ziel

BlueXP Backup and Recovery for SAP HANA – Cloud-Objekt-Storage als Backup-Ziel

Dieser technische Bericht enthält Best Practices für die SAP HANA Datensicherung mit NetApp BlueXP Backup nad Recovery für die Applikation. Dieses Dokument behandelt Konzepte, Konfigurationsempfehlungen und Betriebs-Workflows, einschließlich Konfiguration, Backup-Vorgänge, und Restore-Vorgänge.

Überblick

In diesem Dokument wird beschrieben, wie Sie SAP HANA für die Datensicherung mit NetApp BlueXP einrichten und konfigurieren – von lokalen bis hin zu Cloud-basierten Objektspeichern. Sie deckt den Backup- und Recovery-Teil der Lösung von BlueXP ab. Diese Lösung ist eine Erweiterung der lokalen SAP HANA Backup-Lösung mit NetApp Snap Center und bietet eine kostengünstige Möglichkeit für die langfristige Archivierung von SAP HANA-Backups in Cloud-basiertem Objekt-Storage. Außerdem bietet sie optionales Tiering von Objekt-Storage in Archiv-Storage wie AWS Glacier/Deep Glacier, Microsoft Azure Blob Archive und GCP Archive Storage.

Die Einrichtung und Konfiguration der On-Premises SAP HANA Backup- und Recovery-Lösung wird in beschrieben"TR-4614: SAP HANA Backup und Recovery mit SnapCenter (netapp.com)".

In dieser TR wird nur beschrieben, wie Sie die lokale SnapCenter-basierte SAP HANA Backup- und Recovery-Lösung mit BlueXP Backup und Recovery für SAP HANA erweitern können. Dabei kommen z. B. AWS S3 Objekt-Storage zum Einsatz. Das Setup und die Konfiguration mit Microsoft Azure und GCP-Objekt-Storage statt AWS S3 ist ähnlich, wird in diesem Dokument aber nicht beschrieben.

BlueXP Backup- und Recovery-Architektur

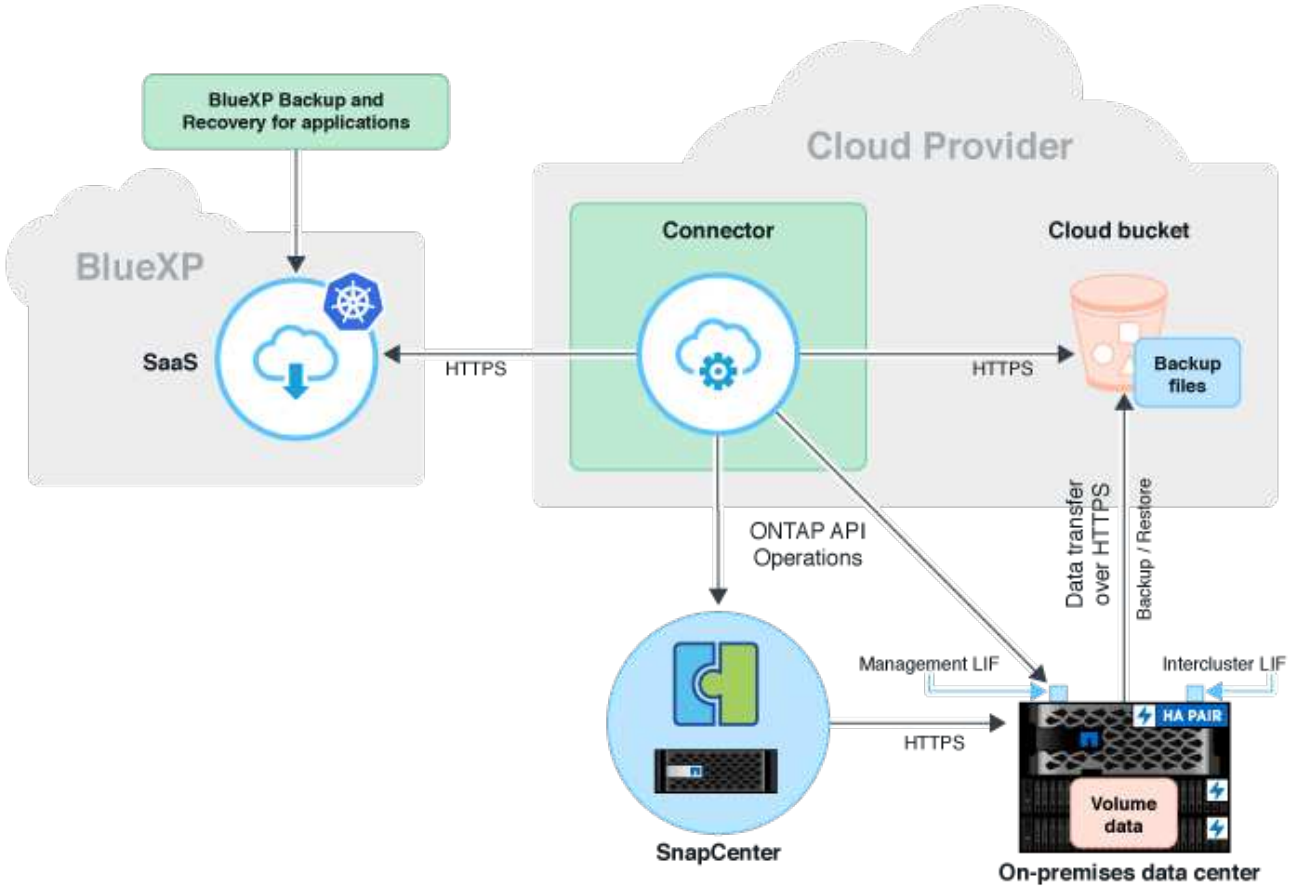
BlueXP Backup und Recovery ist eine SaaS-Lösung mit Datensicherungsfunktionen für Applikationen, die auf NetApp On-Premises-Storage in der Cloud ausgeführt werden. SAP HANA wird mithilfe von NetApp Storage effizient, applikationskonsistent und richtlinienbasiert gesichert. Darüber hinaus ermöglicht BlueXP Backup- und Recovery-Funktionen zentrale Kontrolle und Übersicht. Gleichzeitig werden Benutzern das Management

applikationsspezifischer Backup- und Restore-Vorgänge delegiert.

BlueXP Backup und Recovery läuft in NetApp BlueXP als SaaS und nutzt das Framework und die UI. Das BlueXP Arbeitsumgebungs-Framework wird verwendet, um die Zugangsdaten für NetApp ONTAP auf Basis des lokalen Storage und des NetApp SnapCenter Servers zu konfigurieren und zu managen.

Ein BlueXP Connector muss innerhalb des virtuellen Netzwerks des Kunden implementiert werden. Es ist eine Verbindung zwischen der On-Premises-Umgebung und der Cloud-Umgebung erforderlich, z. B. eine Site-to-Site-VPN-Verbindung. Die Kommunikation zwischen den NetApp-SaaS-Komponenten und der Kundenumgebung erfolgt ausschließlich über den Konnektor. Der Connector führt die Storage-Vorgänge mithilfe der ONTAP und SnapCenter Management-APIs aus.

Der Datentransfer zwischen dem lokalen Storage und dem Cloud-Bucket ist vollständig gesichert mit AES-256-Bit-Verschlüsselung im Ruhezustand, TLS/HTTPS-Verschlüsselung bei der Übertragung und CMK-Unterstützung (Customer Managed Key).
Die gesicherten Daten können in einem unveränderlichen und nicht löschbaren WORM-Zustand gespeichert werden. Die einzige Möglichkeit, auf die Daten aus dem Objekt-Storage zuzugreifen, besteht darin, sie in NetApp ONTAP-basiertem Storage wiederherzustellen, einschließlich NetApp CVO.



Überblick über die Installations- und Konfigurationsschritte

Die erforderlichen Installations- und Konfigurationsschritte lassen sich in drei Bereiche aufteilen. + Voraussetzung ist, dass die SAP HANA Backup Konfiguration im NetApp Snap Center konfiguriert wurde. Informationen zur Einrichtung von Snap Center für SAP HANA finden Sie in "SnapCenter-Konfiguration (netapp.com)".

1. Installation und Konfiguration von NetApp BlueXP Komponenten

   Muss einmal während der ersten Einrichtung der Datensicherungslösung durchgeführt werden.

2. Vorbereitungsschritte bei NetApp SnapCenter.

   Muss für jede SAP HANA-Datenbank durchgeführt werden, die geschützt werden sollte.

3. Konfigurationsschritte bei BlueXP Backup und Recovery.

   Muss für jede SAP HANA-Datenbank durchgeführt werden, die geschützt werden sollte.

Installation und Konfiguration von NetApp BlueXP Hybrid-Applikations-Backup

Die Installation und Konfiguration der NetApp BlueXP Komponenten finden Sie in "Sichern Sie Ihre On-Premises-Applikationsdaten in der NetApp Dokumentation".

1. Melden Sie sich bei BlueXP an und richten Sie ein NetApp Konto ein unter https://bluexp.netapp.com/.
2. Implementieren Sie den BlueXP Connector in Ihrer Umgebung. Beschreibung ist verfügbar unter "Weitere Informationen zu Steckverbindern finden Sie in der NetApp-Dokumentation".
3. Cloud-Backup-Lizenz bei BlueXP hinzufügen/kaufen: https://docs.netapp.com/us-en/cloud-manager-backup-restore/task-licensing-cloud-backup.html.
4. Erstellen Sie eine Arbeitsumgebung für NetApp On-Premises-Umgebungen und Ihr Cloud-Ziel in BlueXP durch Hinzufügen Ihres lokalen Storage.
5. Erstellen einer neuen Objektspeicher-Beziehung für den On-Premises-Storage in einen AWS S3 Bucket
6. SAP HANA-Systemressource bei SnapCenter konfigurieren
7. Fügen Sie Snap Center zu Ihrer Arbeitsumgebung hinzu.
8. Erstellen Sie eine Richtlinie für Ihre Umgebung.
9. Sicherung Ihres SAP HANA-Systems

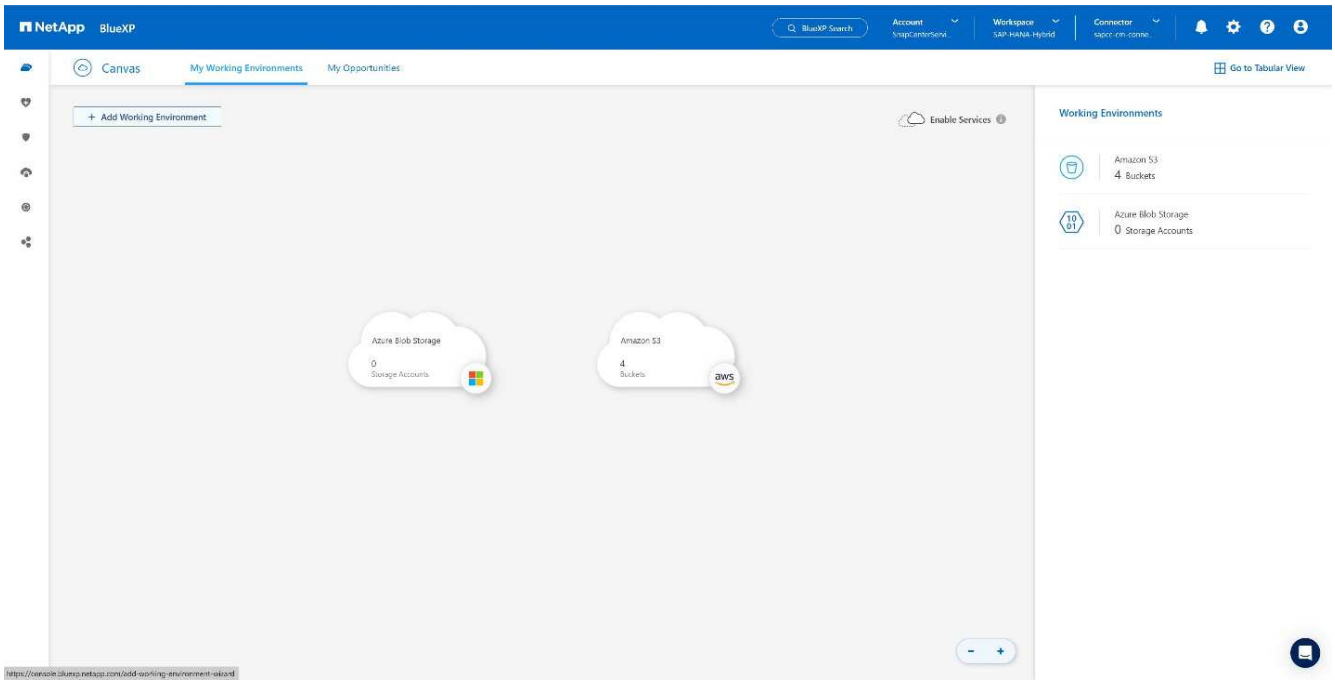
Konfigurieren von BlueXP Backup und Recovery für SAP HANA

In diesem Abschnitt wird beschrieben, wie Sie die Arbeitsumgebung einrichten, SnapCenter konfigurieren und SAP HANA-Backups in BlueXP konfigurieren und aktivieren.

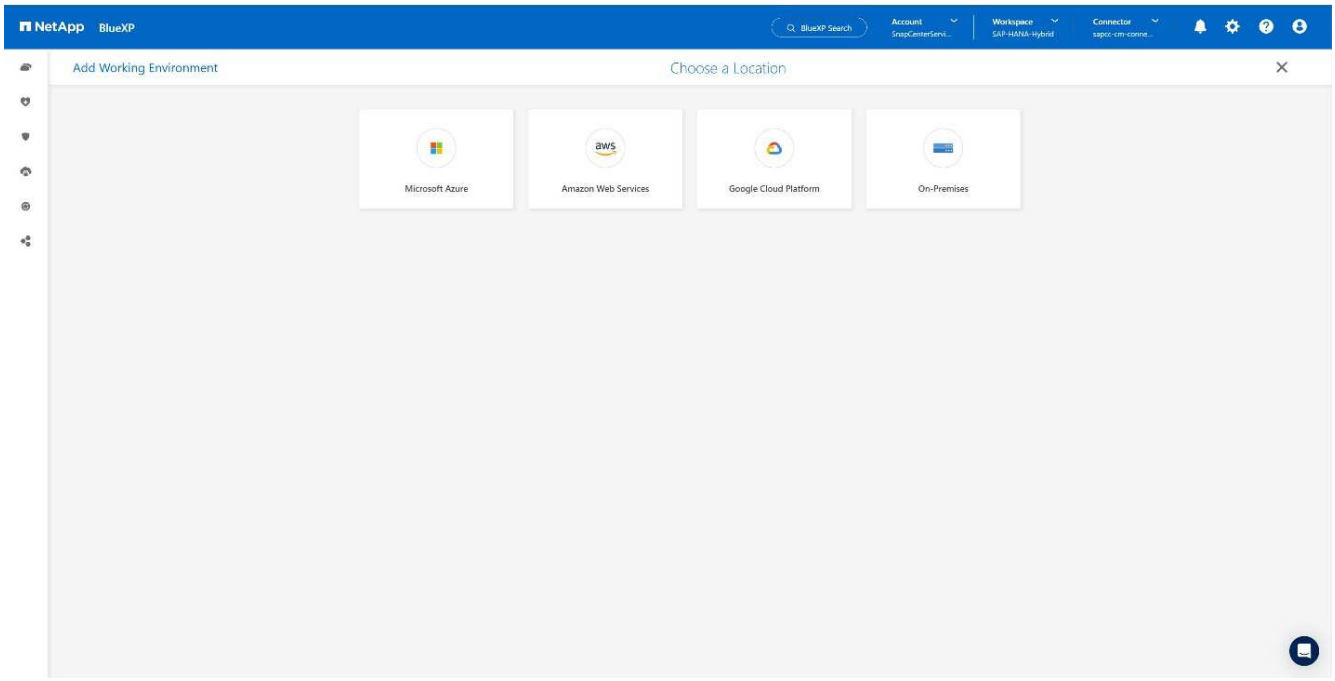
Arbeitsumgebung für BlueXP erstellen

Fügen Sie das lokale Storage-System zur Arbeitsumgebung hinzu.

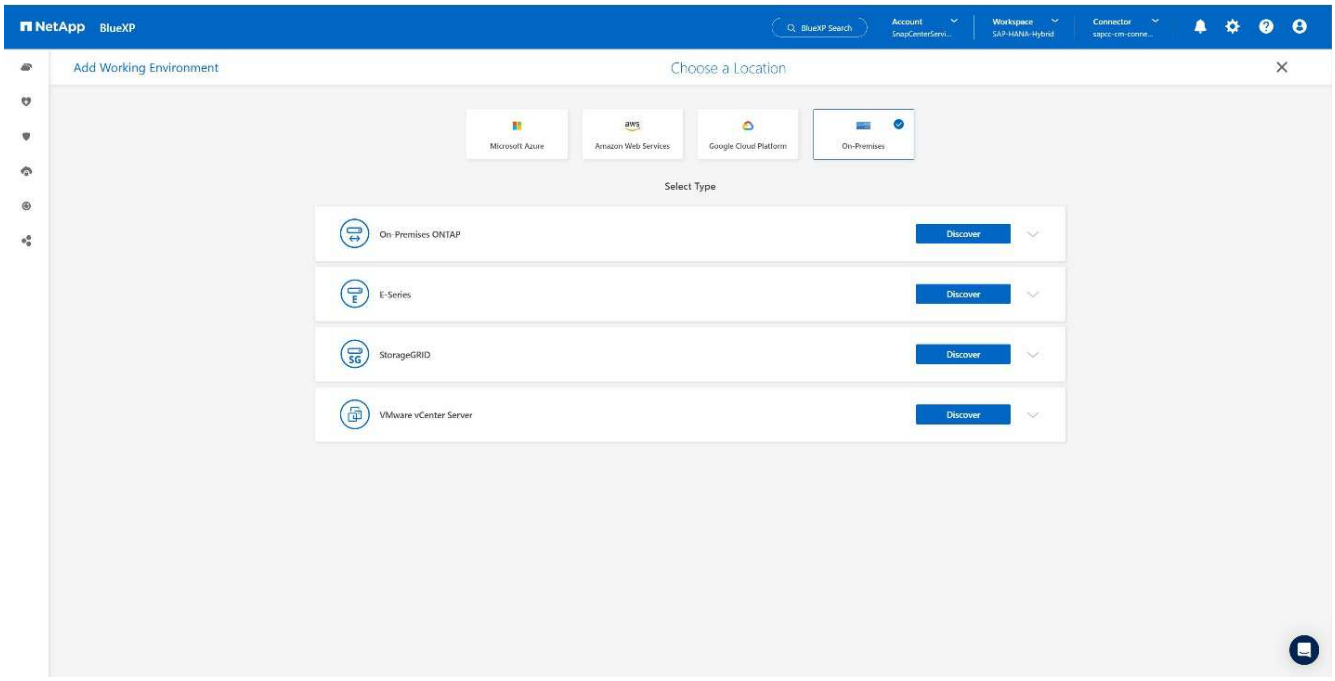
1. Wählen Sie im linken Menü **Storage** → **Canvas** → **My Working** Umgebung.
2. Drücken Sie **+ Arbeitsumgebung Hinzufügen**. +



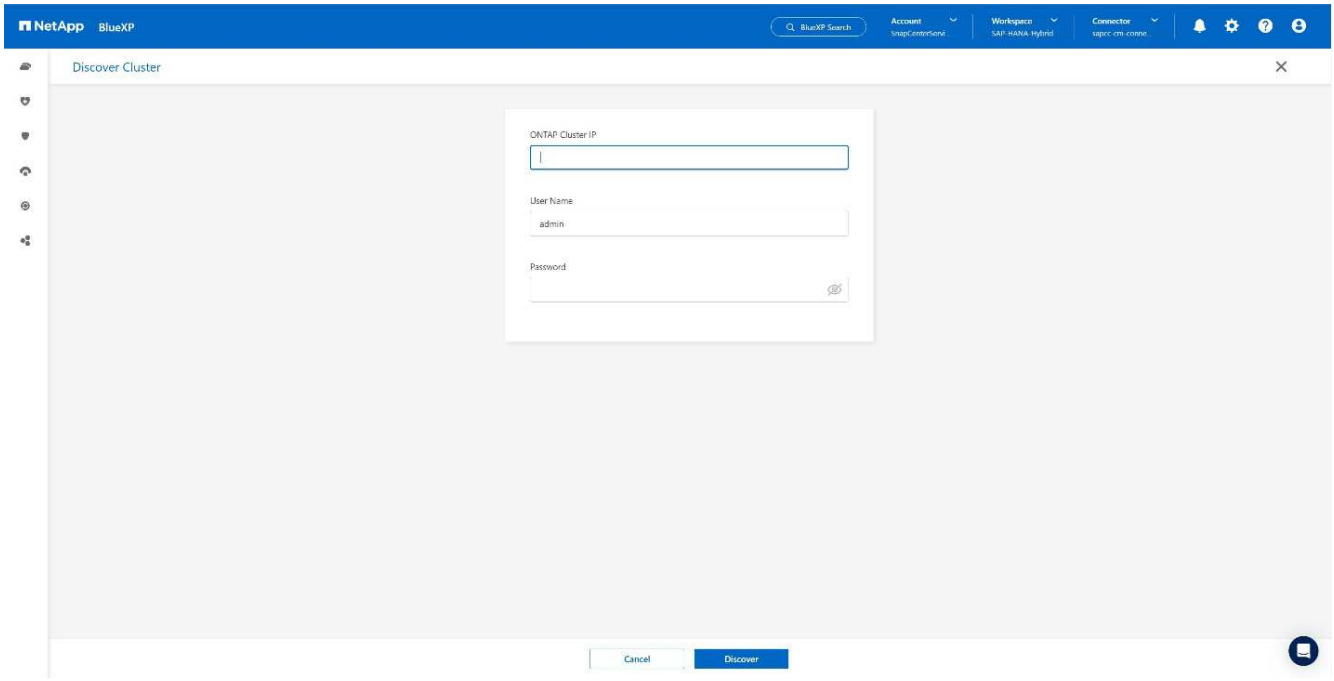
3. Wählen Sie **On-Premises**. +



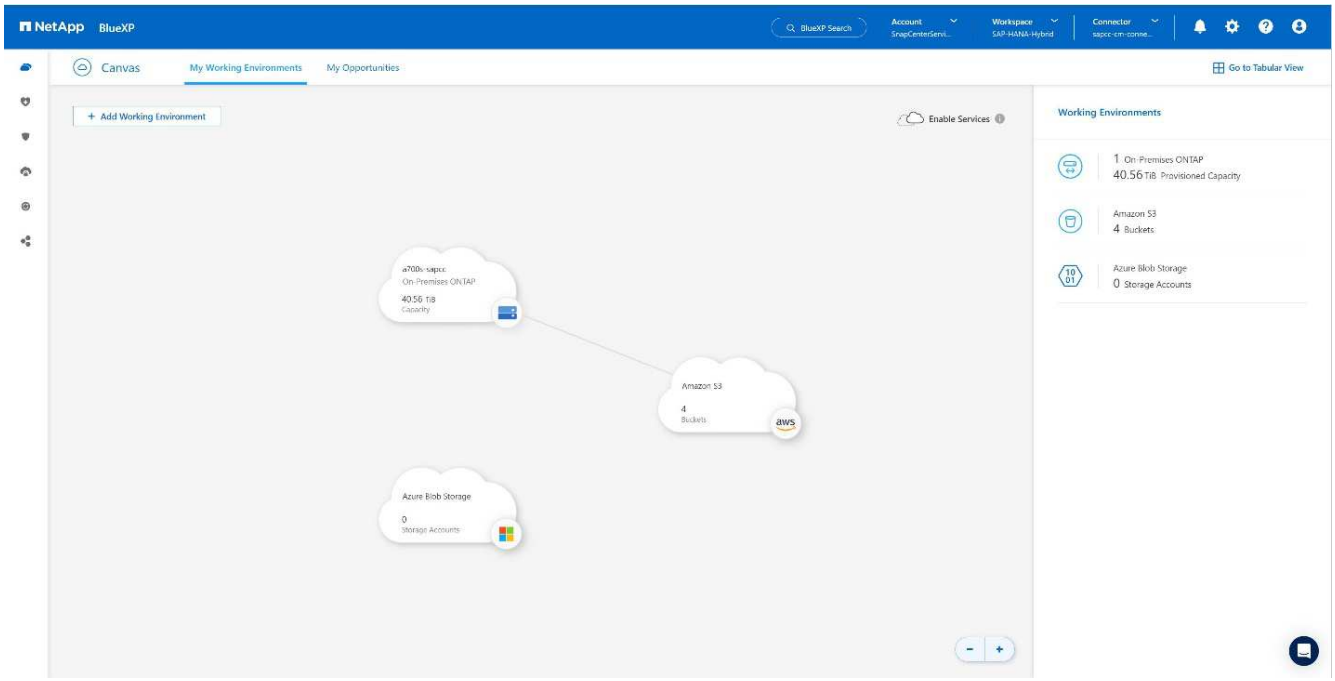
4. Wählen Sie **Entdecken Sie die On-Premises-ONTAP**. +



5. Geben Sie die IP-Adresse des ONTAP-Clusters und das Passwort ein und drücken Sie **Discover**. +



6. Der ONTAP Cluster ist jetzt verfügbar. +

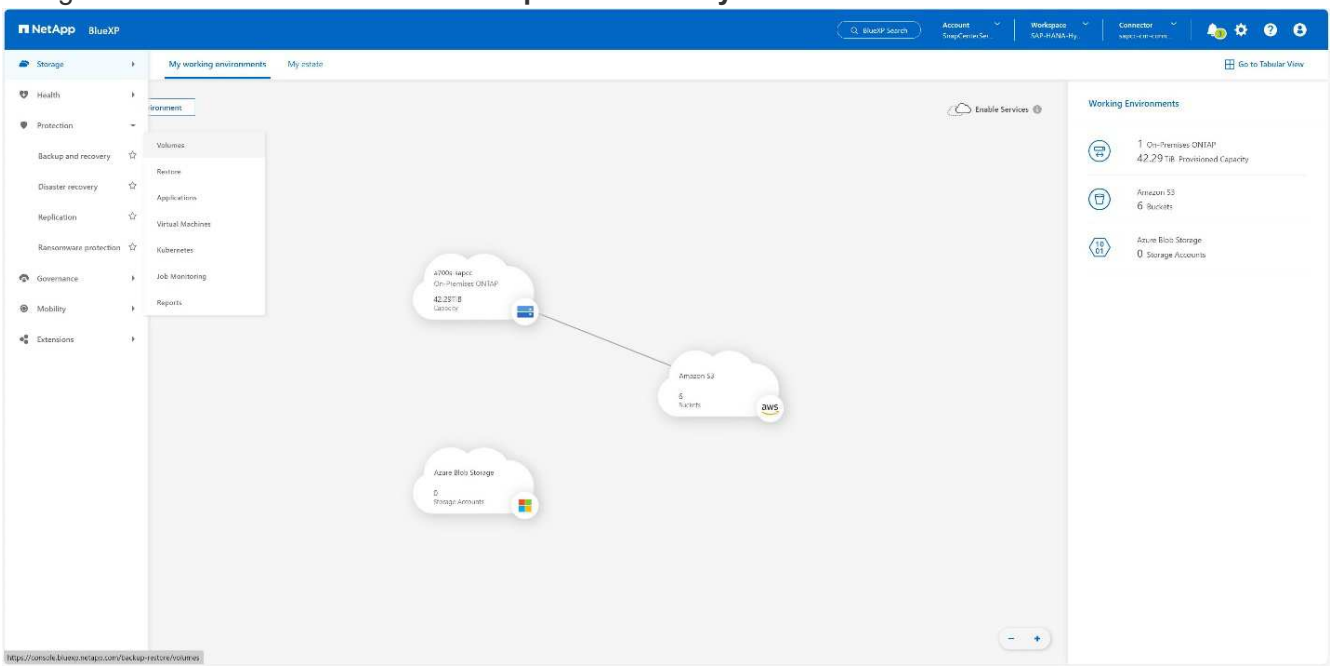


Erstellen einer Beziehung zwischen dem lokalen Storage-System und einem Objekt-Storage-Bucket

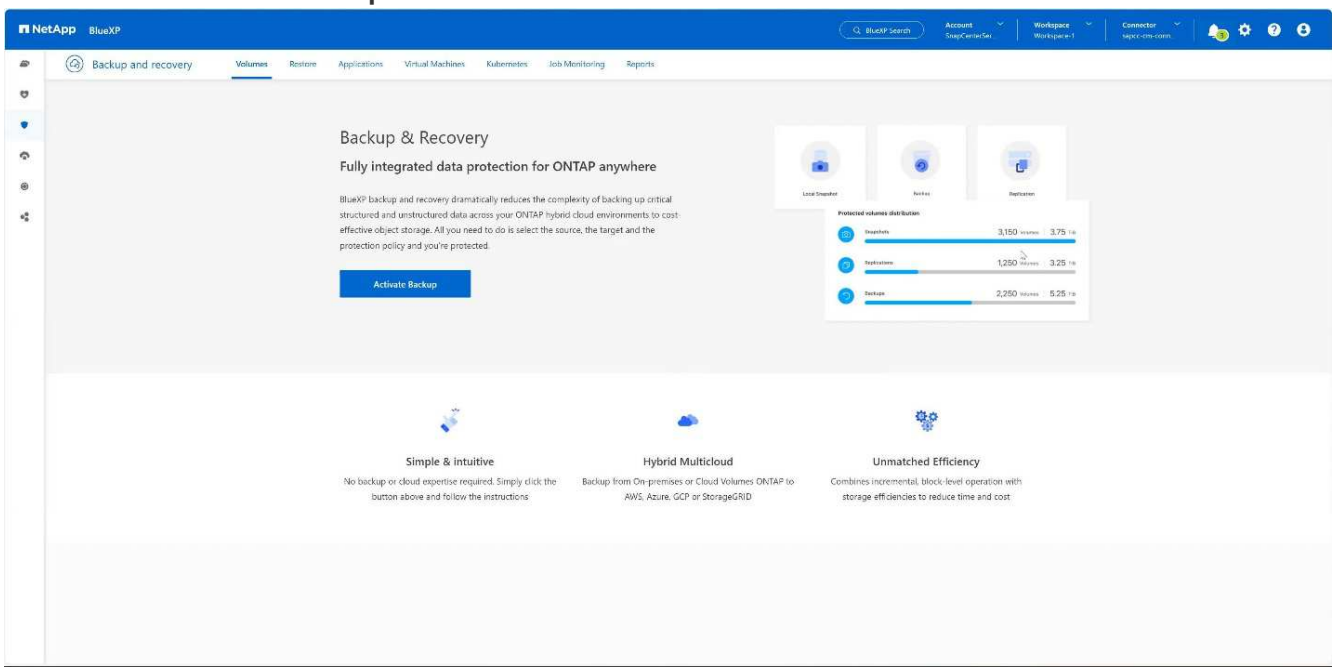
Die Beziehung zwischen dem On-Premises-Storage und dem S3-Bucket wird entweder ein Backup für ein Volume oder ein Backup einer Applikation erstellt. Bei der Übertragung der Daten von On-Premises-Storage zu S3 muss ein Volume-Backup für die Erstellung der Beziehung zwischen On-Premises-Storage und S3 Bucket verwendet werden, wenn VPC-Endpunkte verwendet werden müssen.
Bei Erstellung dieser Dokumentation bietet der Applikations-Backup-Workflow keine VPC-Endpunkte für den Zugriff auf S3 Buckets.
Siehe "Gateway-Endpunkte für Amazon S3 – Amazon Virtual Private Cloud" Einrichten von VPC-Endpunkten für S3 innerhalb der VPC

So erstellen Sie ein erstes Volume-Backup:

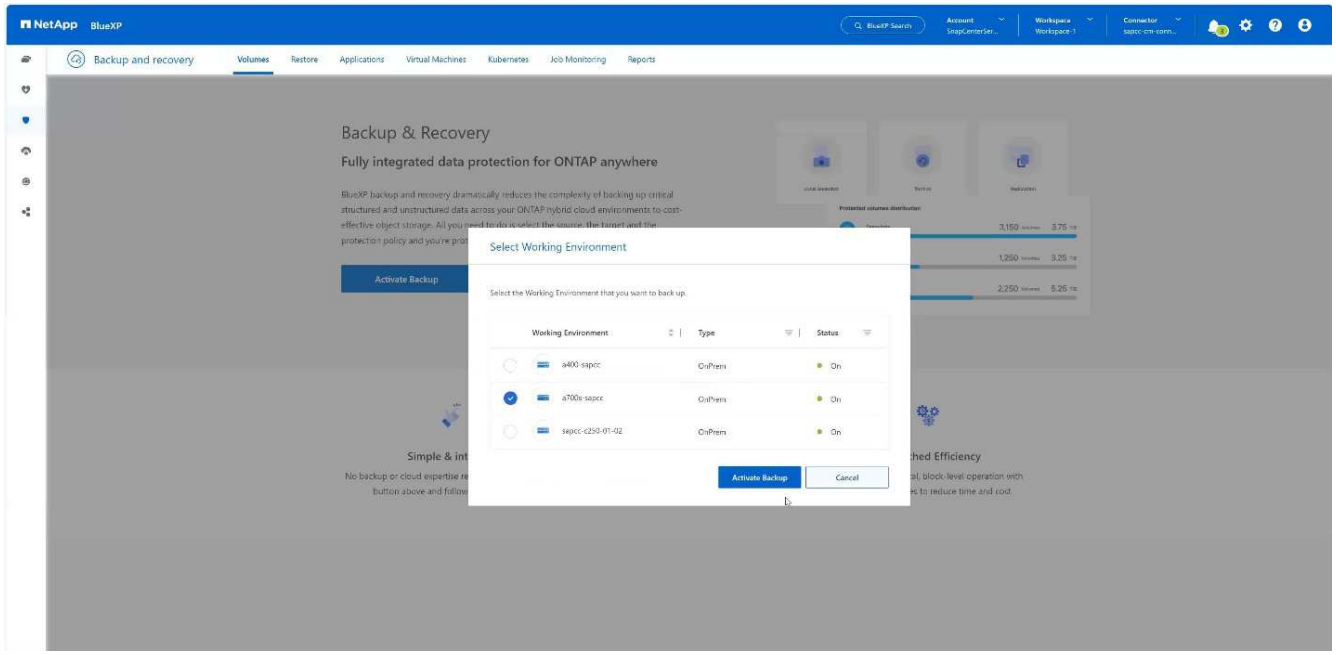
1. Navigieren Sie über **Protection** zu **Backup und Recovery** und wählen Sie **Volumes**. +



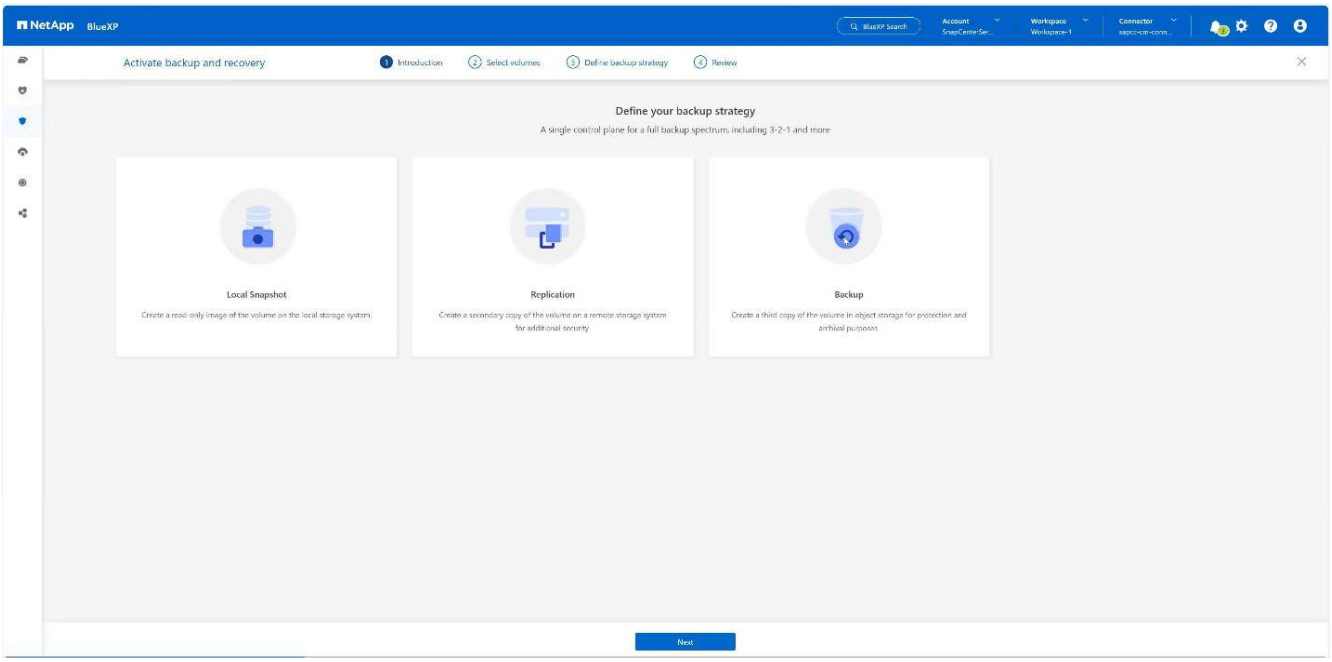
2. Drücken Sie die Taste **Backup aktivieren**. +



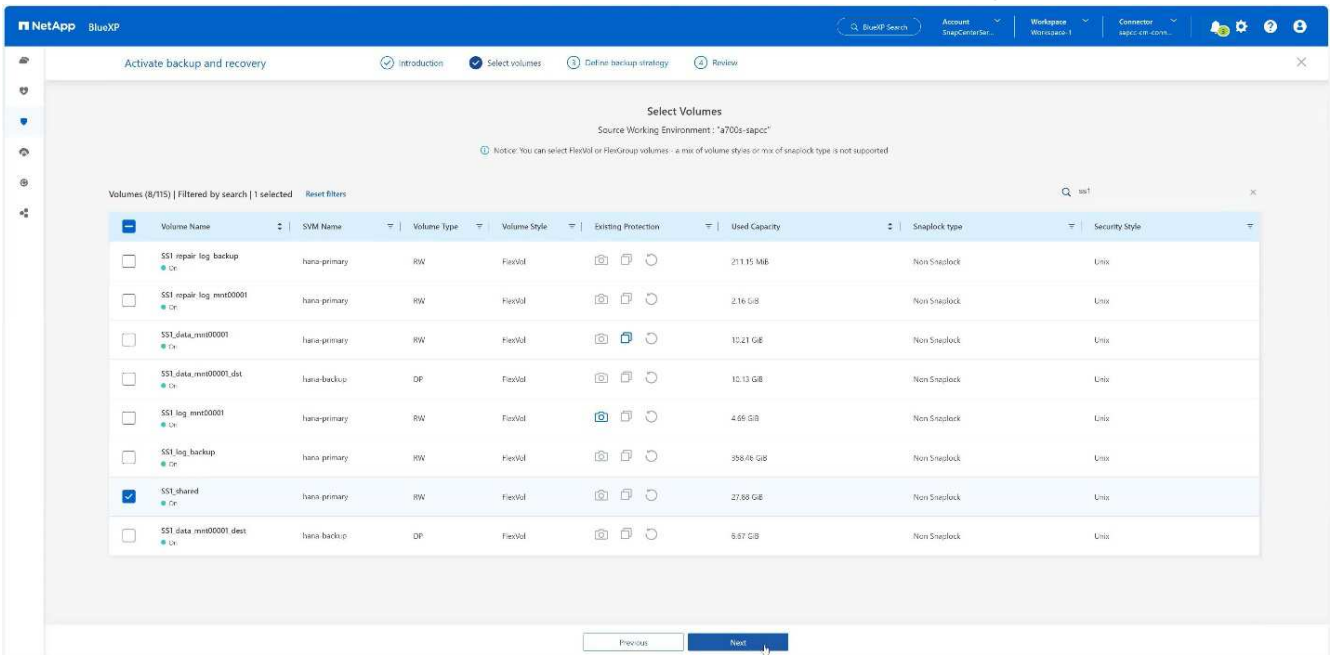
3. Wählen Sie das gewünschte lokale Speichersystem aus und klicken Sie auf **Backup aktivieren**. +



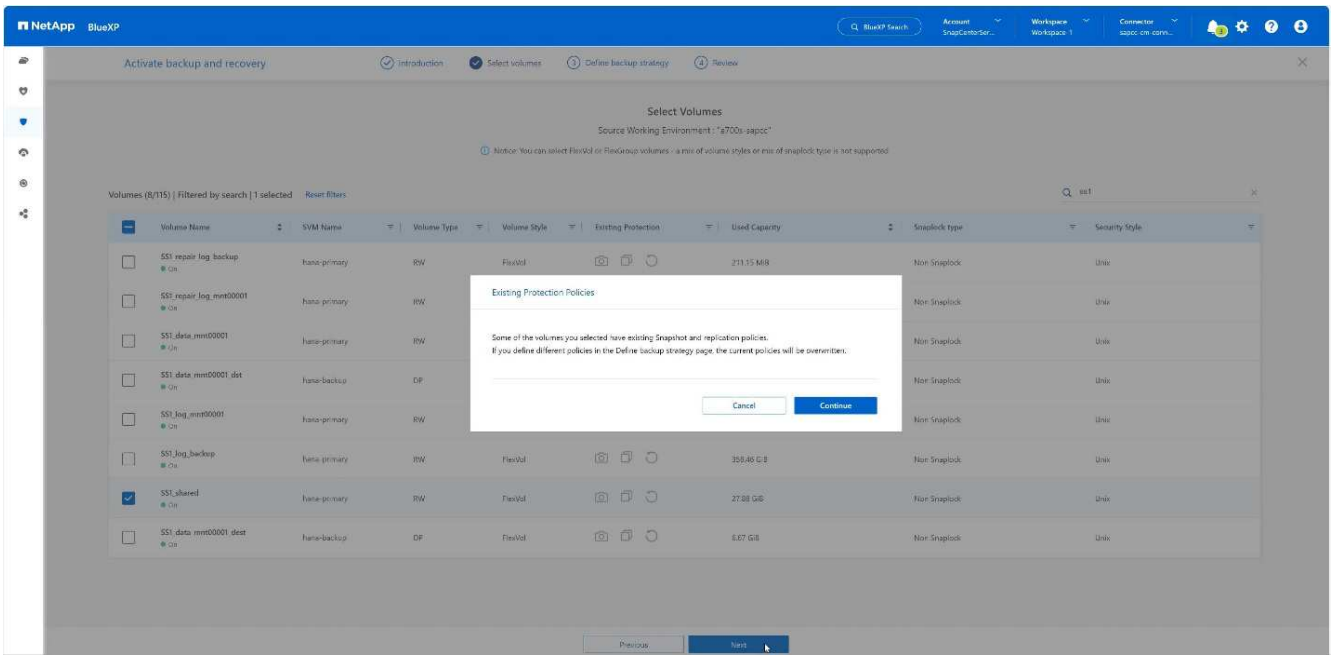
4. Wählen Sie **Backup**. +



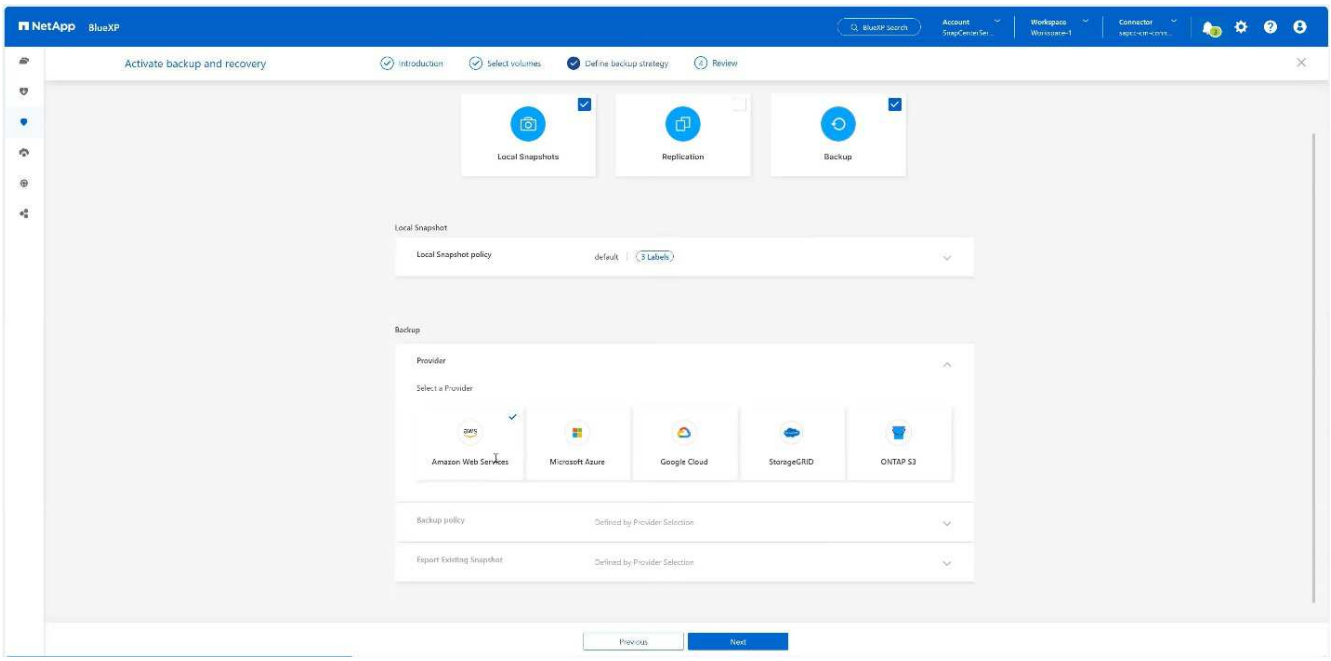
5. Wählen Sie ein Volume, das auf derselben SVM wie Ihre SAP HANA-Datendateien gespeichert ist, und drücken Sie **Weiter**. In diesem Beispiel wurde das Volume für /hana/shared ausgewählt. +



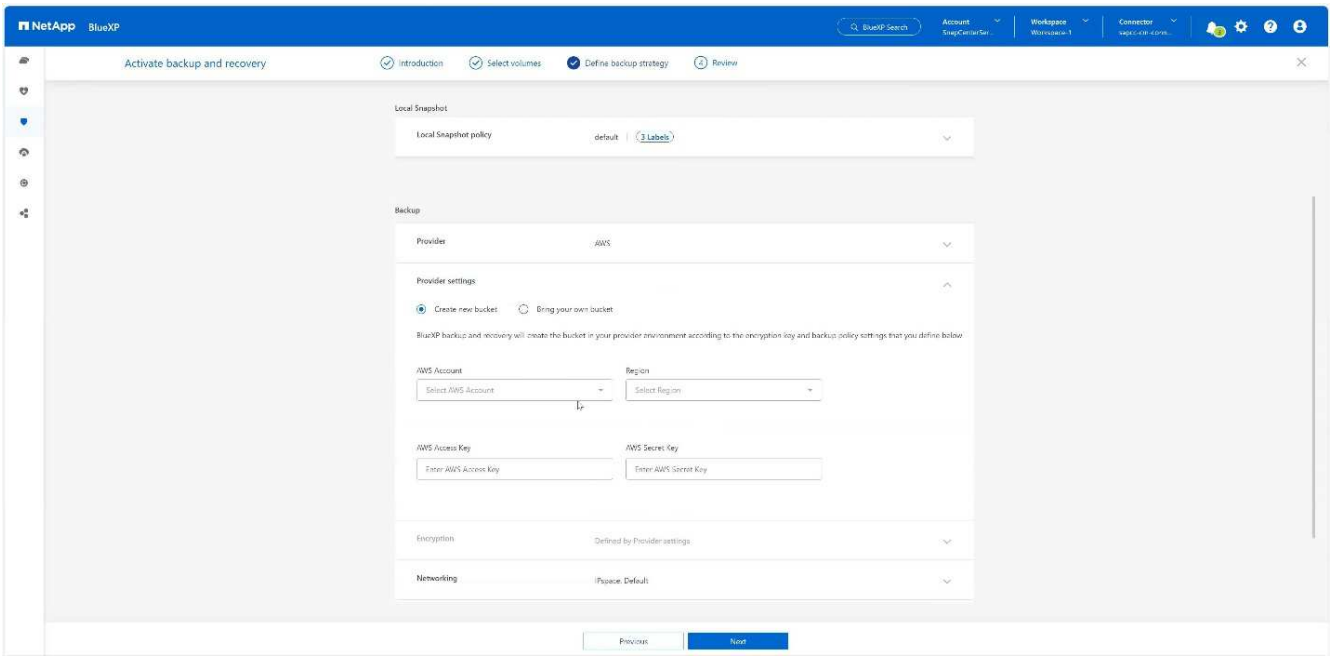
6. **Weiter**, wenn eine bestehende Richtlinie vorhanden ist. +



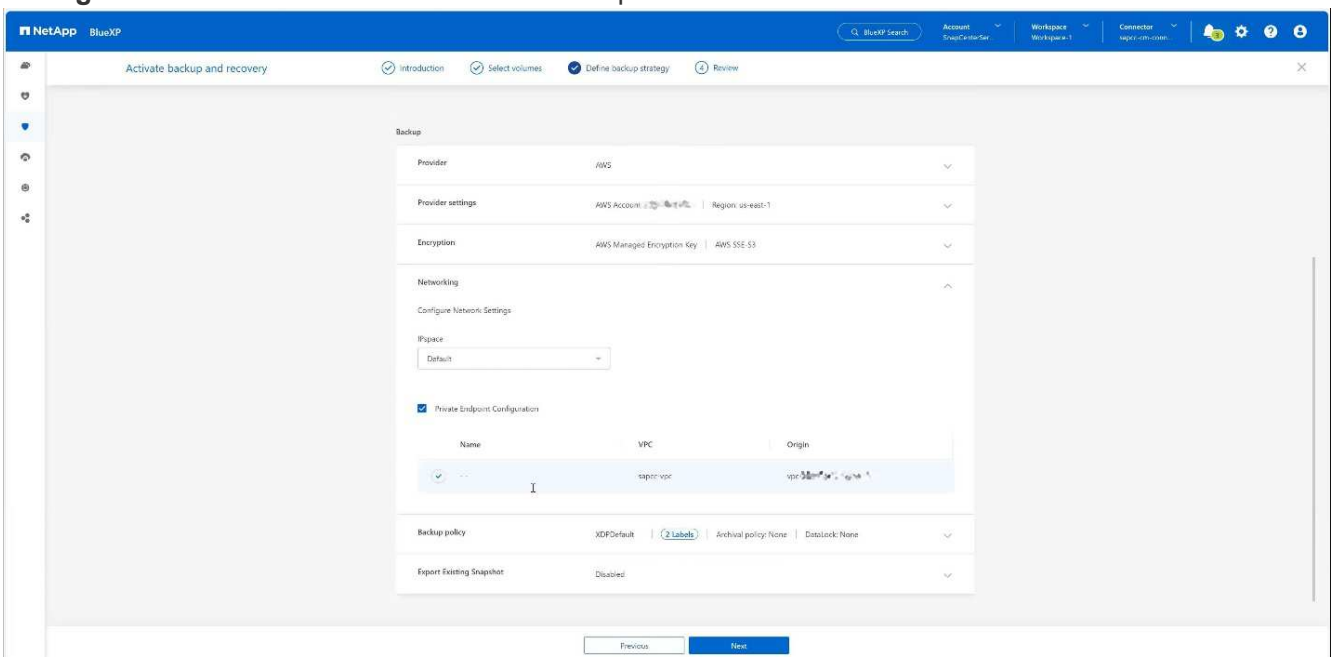
7. Aktivieren Sie die Option **Backup** und wählen Sie Ihren gewünschten Backup-Anbieter. In diesem Beispiel AWS. + die Option für bereits vorhandene Policen aktiviert lassen. + Uncheck-Optionen, die Sie nicht verwenden möchten. +



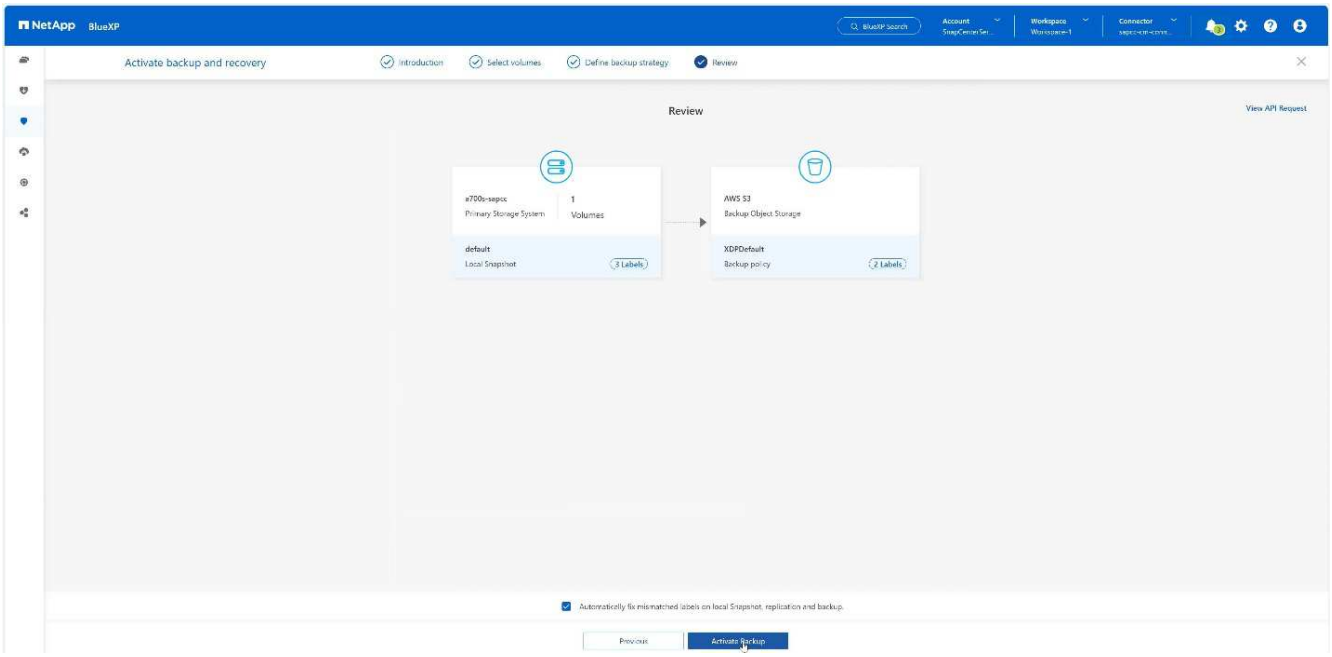
8. Erstellen Sie einen neuen Bucket, oder wählen Sie einen vorhandenen Bucket aus. Stellen Sie Ihre AWS-Kontoeinstellungen, den regio, Ihren Zugriffsschlüssel und den geheimen Schlüssel bereit. Drücken Sie **Weiter**. +



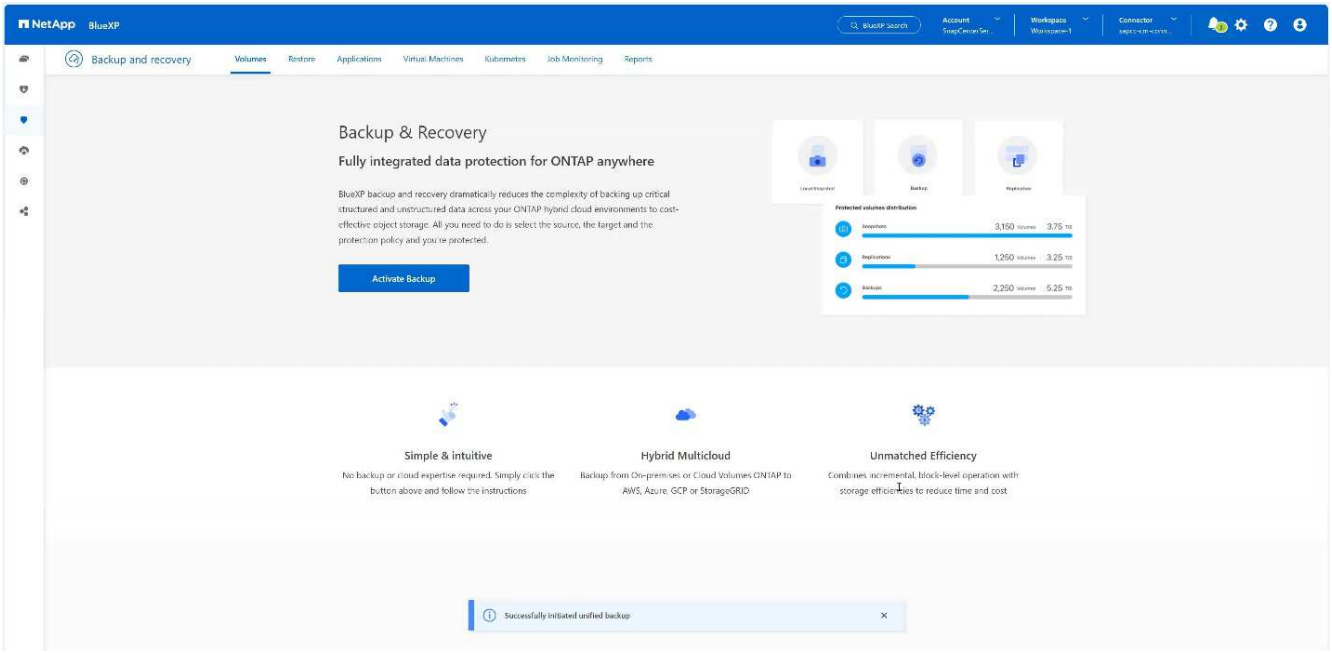
9. Wählen Sie den korrekten IPspace Ihres lokalen Storage-Systems aus, wählen Sie **Privat Endpoint Configuration** aus und wählen Sie den VPC-Endpunkt für S3 aus. Drücken Sie **Weiter**. +



10. Überprüfen Sie Ihre Konfiguration und drücken Sie **Sicherung aktivieren**. +

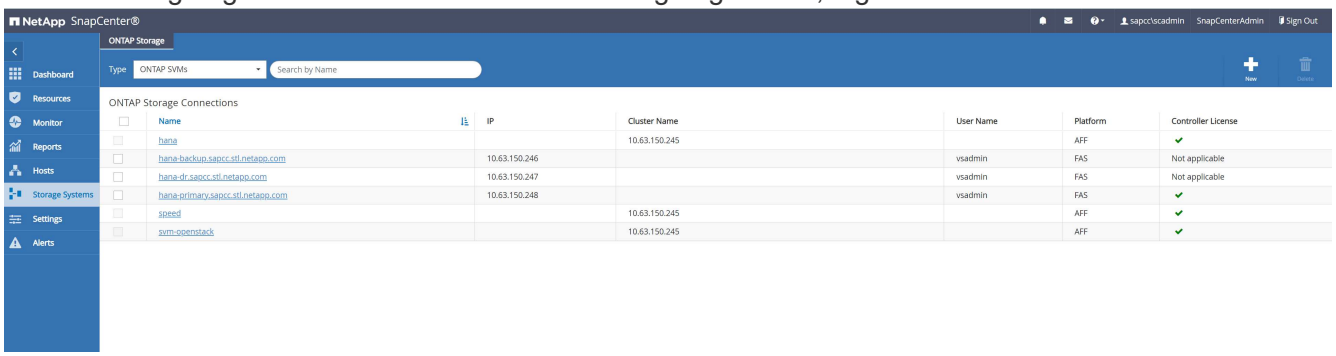


11. Die Sicherung wurde erfolgreich initiiert. +

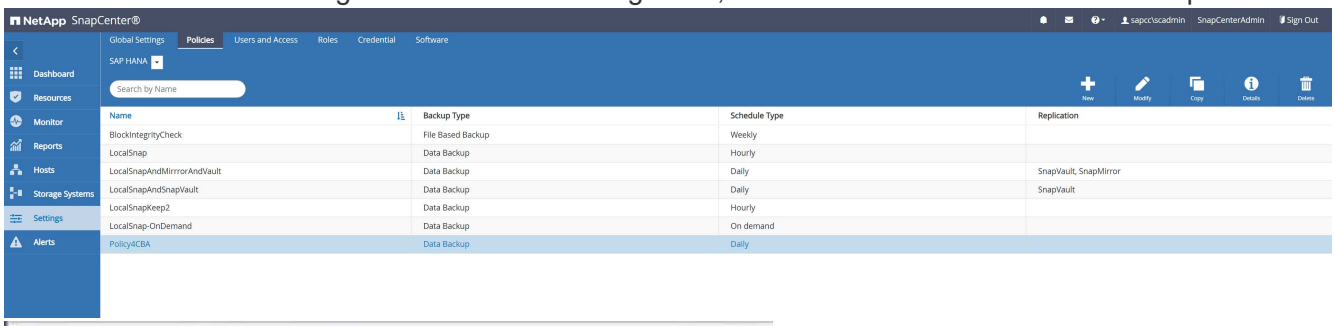


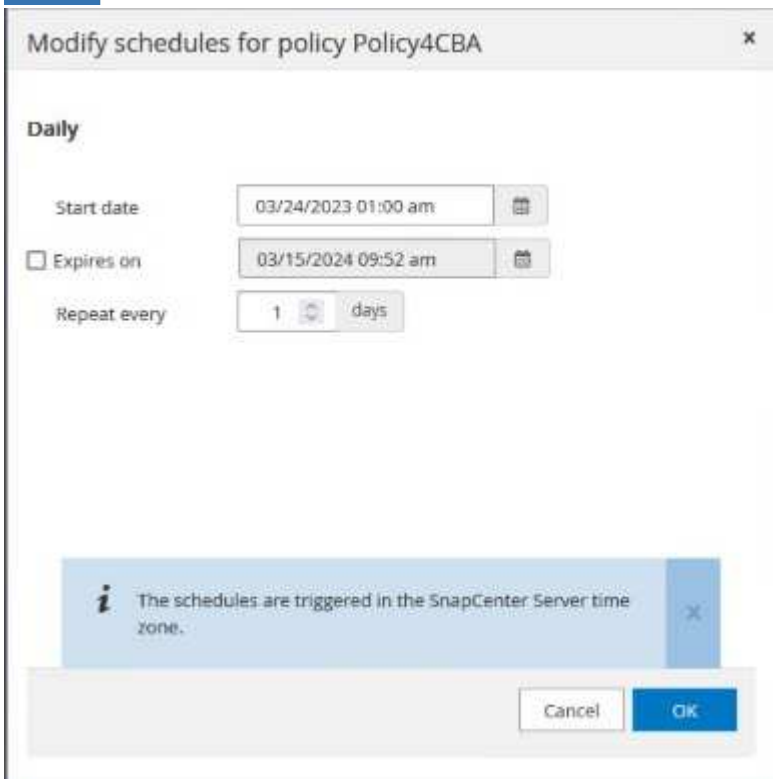
Konfigurieren Sie die SAP HANA-Systemressource bei SnapCenter

1. Prüfen Sie, ob die SVM (in diesem Beispiel hana), in der Ihr SAP HANA-System gespeichert ist, über den Cluster hinzugefügt wurde. Wenn nur die SVM hinzugefügt wurde, fügen Sie das Cluster hinzu. +

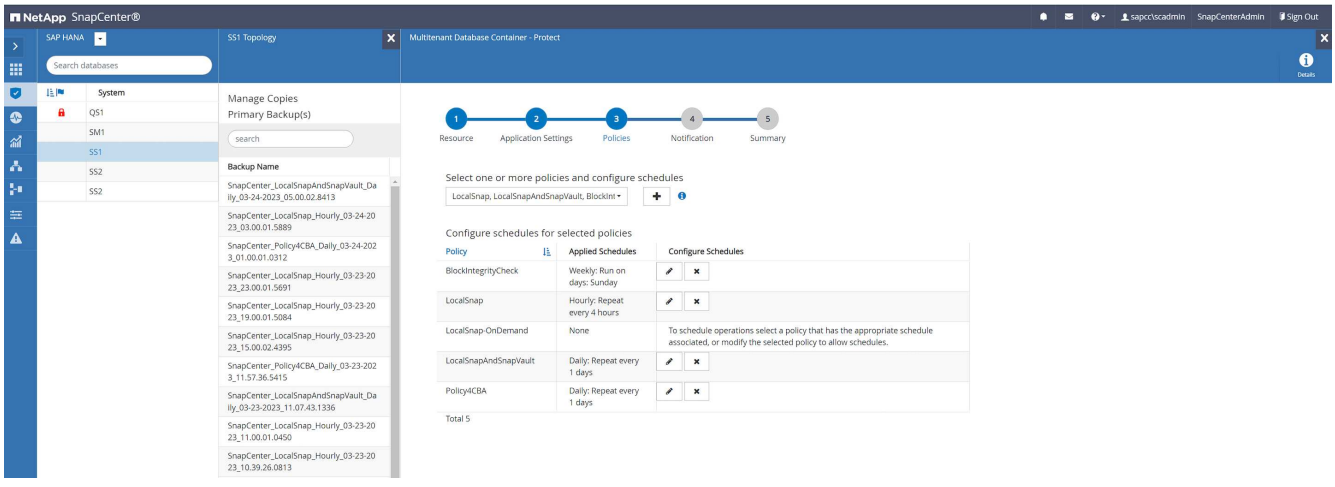


2. Definieren Sie eine Planungsrichtlinie mit einem täglichen, wöchentlichen oder monatlichen Zeitplan. +

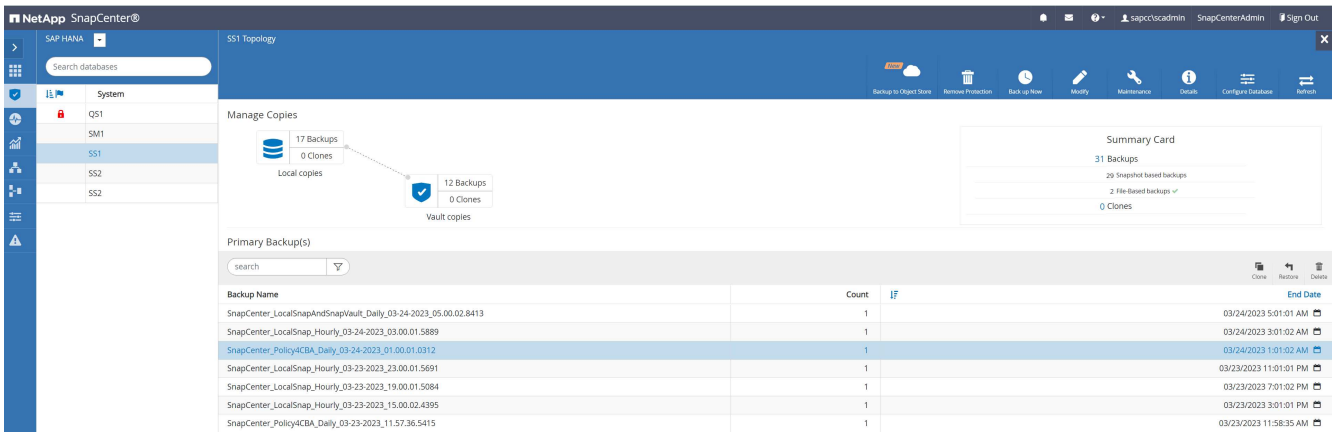




3. Fügen Sie die neue Richtlinie zu Ihrem SAP HANA-System hinzu und weisen Sie einen täglichen Zeitplan zu. +

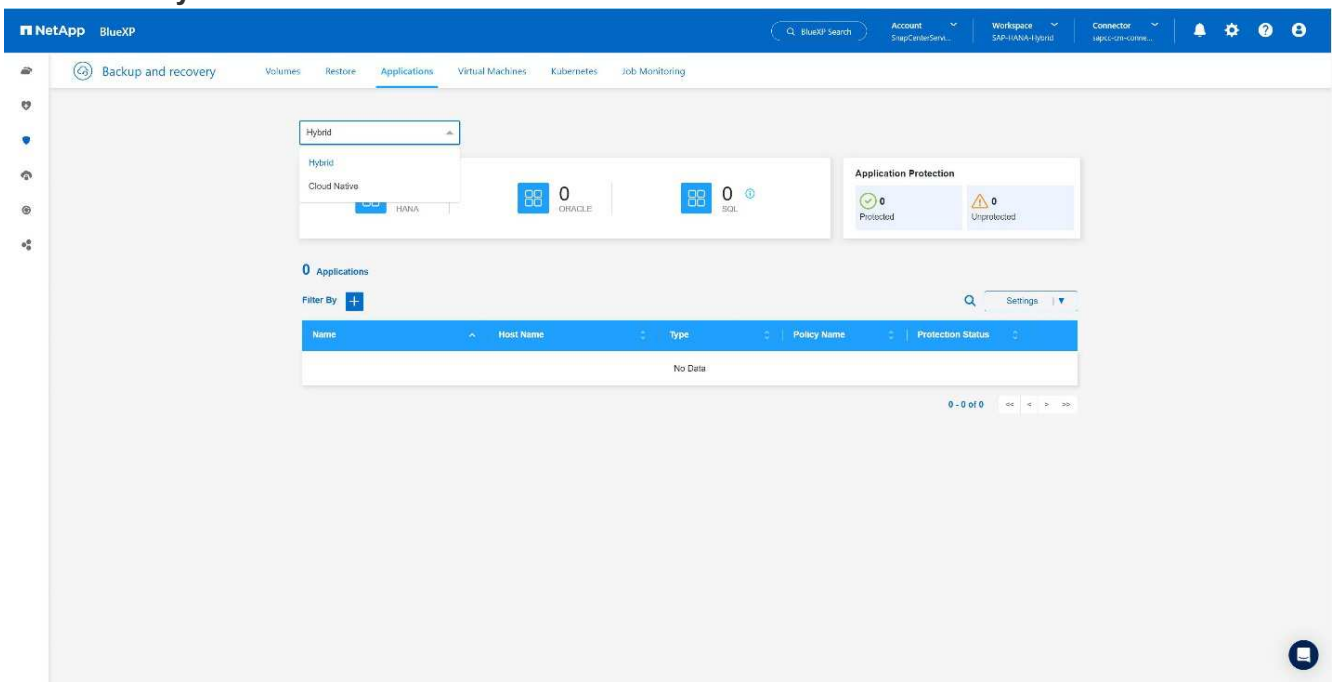


4. Nach der Konfiguration sind neue Backups mit dieser Richtlinie verfügbar, nachdem die Richtlinie gemäß dem definierten Zeitplan ausgeführt wurde.

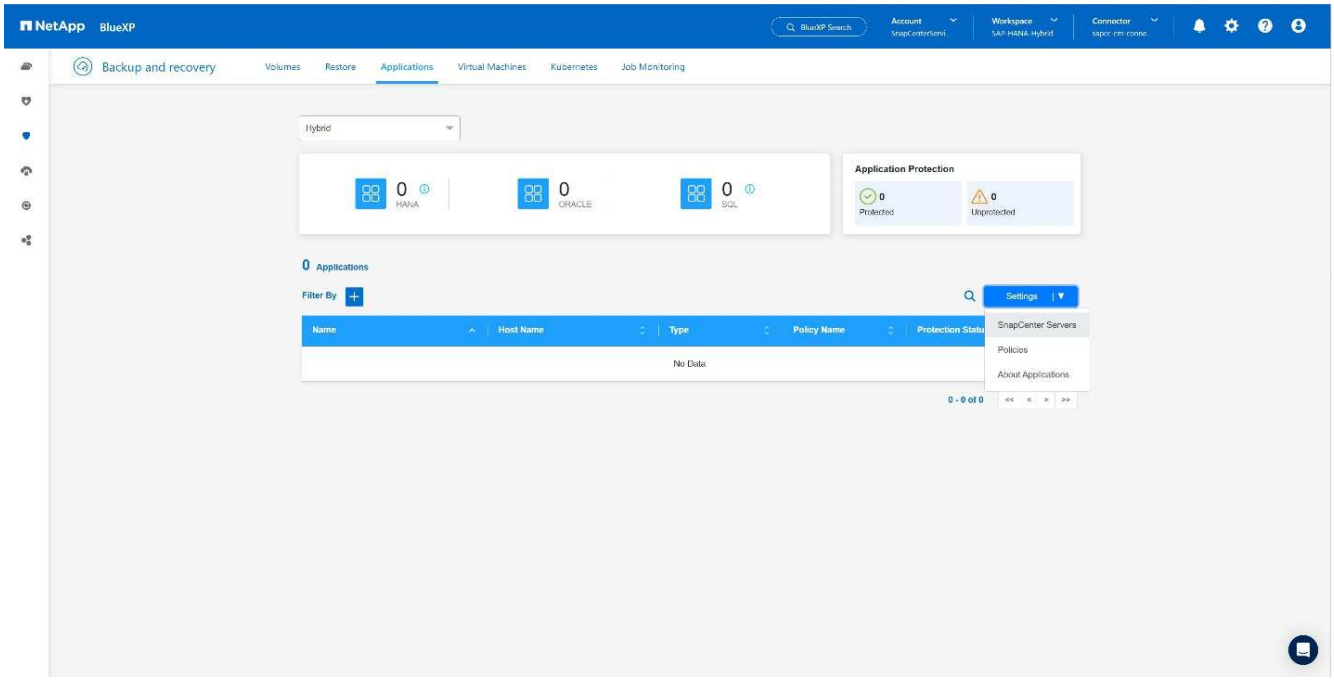


Hinzufügen von SnapCenter zur BlueXP Arbeitsumgebung

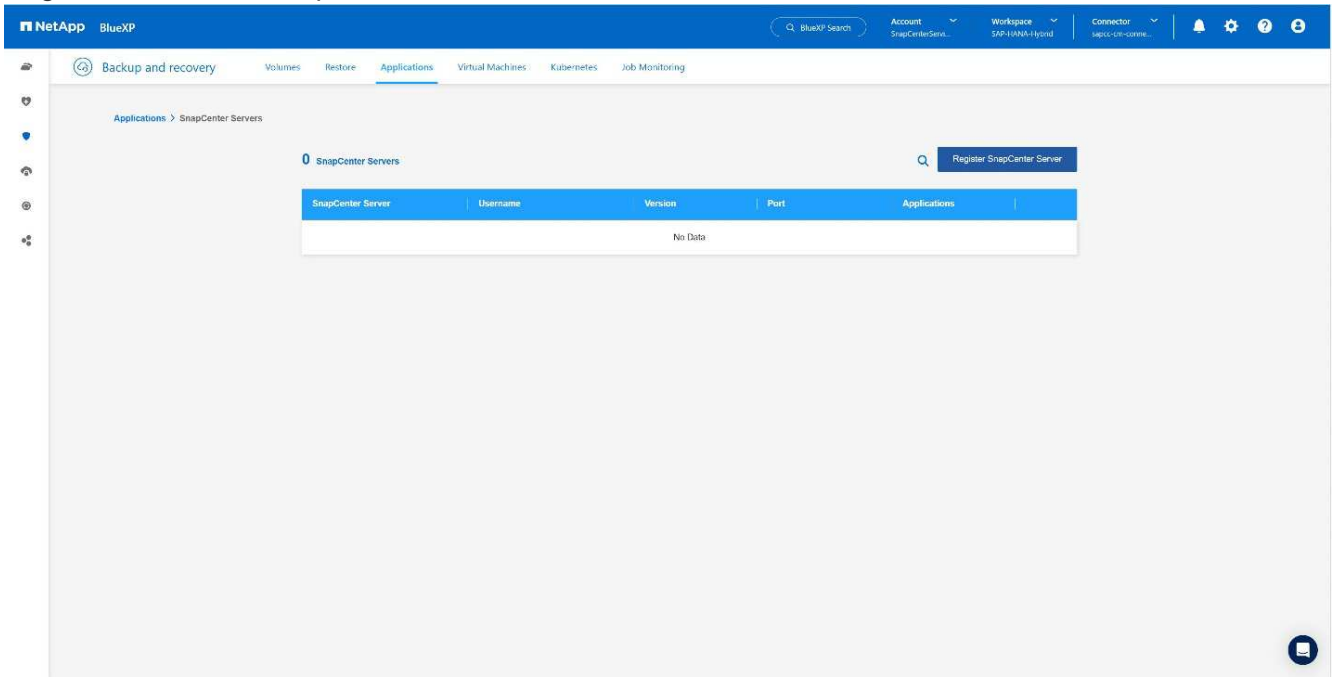
1. Wählen Sie im linken Menü **Schutz** → **Sicherung und Wiederherstellung** → **Anwendungen**.
2. Wählen Sie **Hybrid** aus dem Pulldown-Menü. +



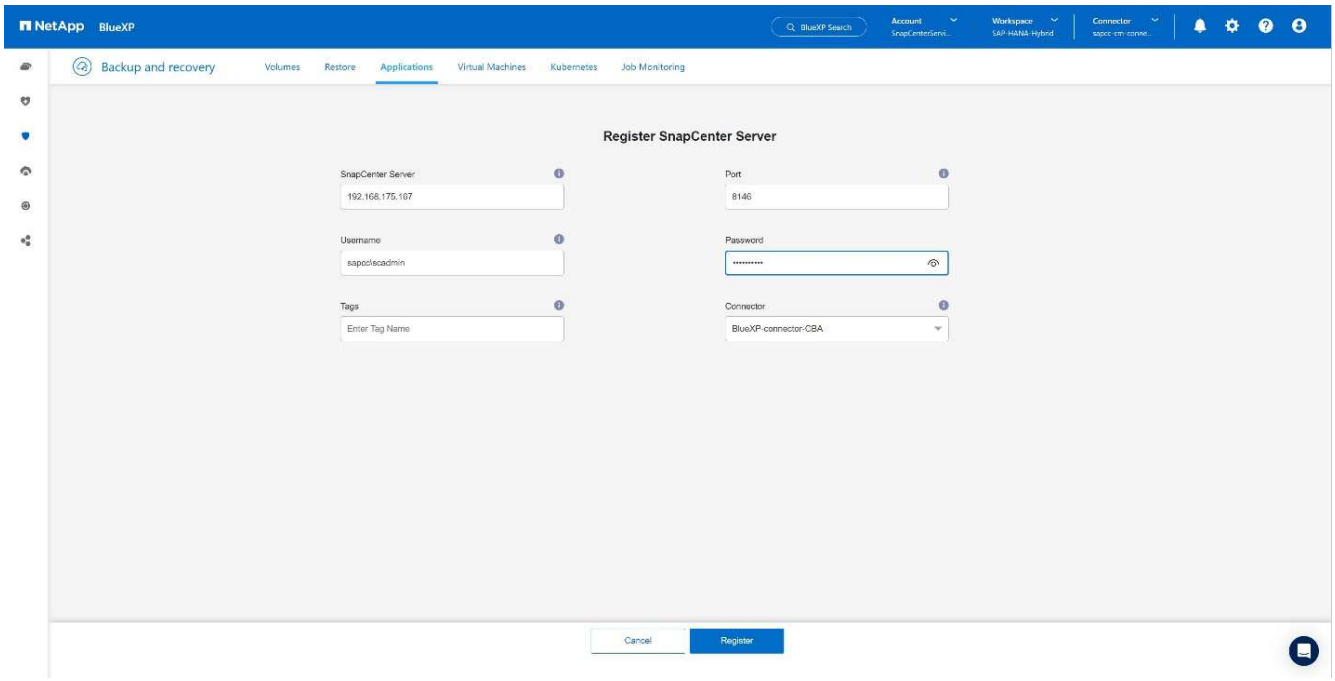
3. Wählen Sie im Einstellungsmenü **SnapCenter Server**. +



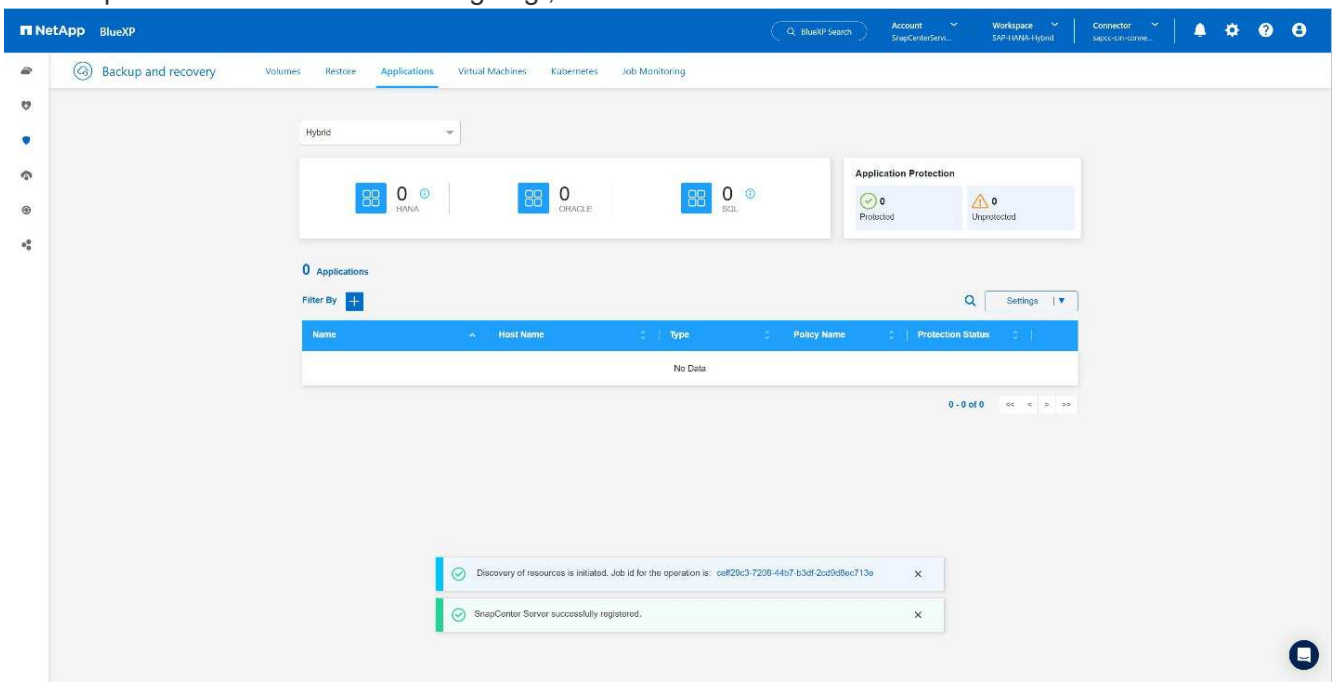
4. Registrieren Sie den SnapCenter-Server. +



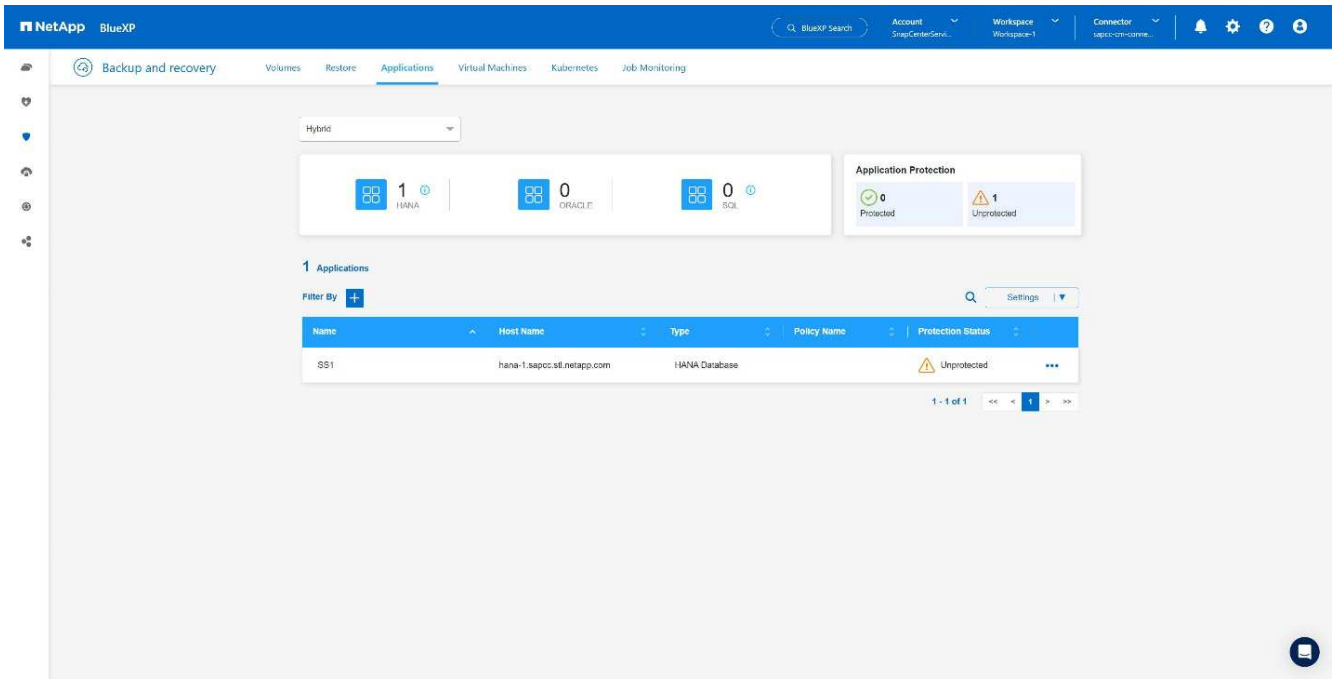
5. Fügen Sie die Anmeldeinformationen des SnapCenter-Servers hinzu. +



6. Die SnapCenter-Server wurden hinzugefügt, und Daten werden erkannt. +

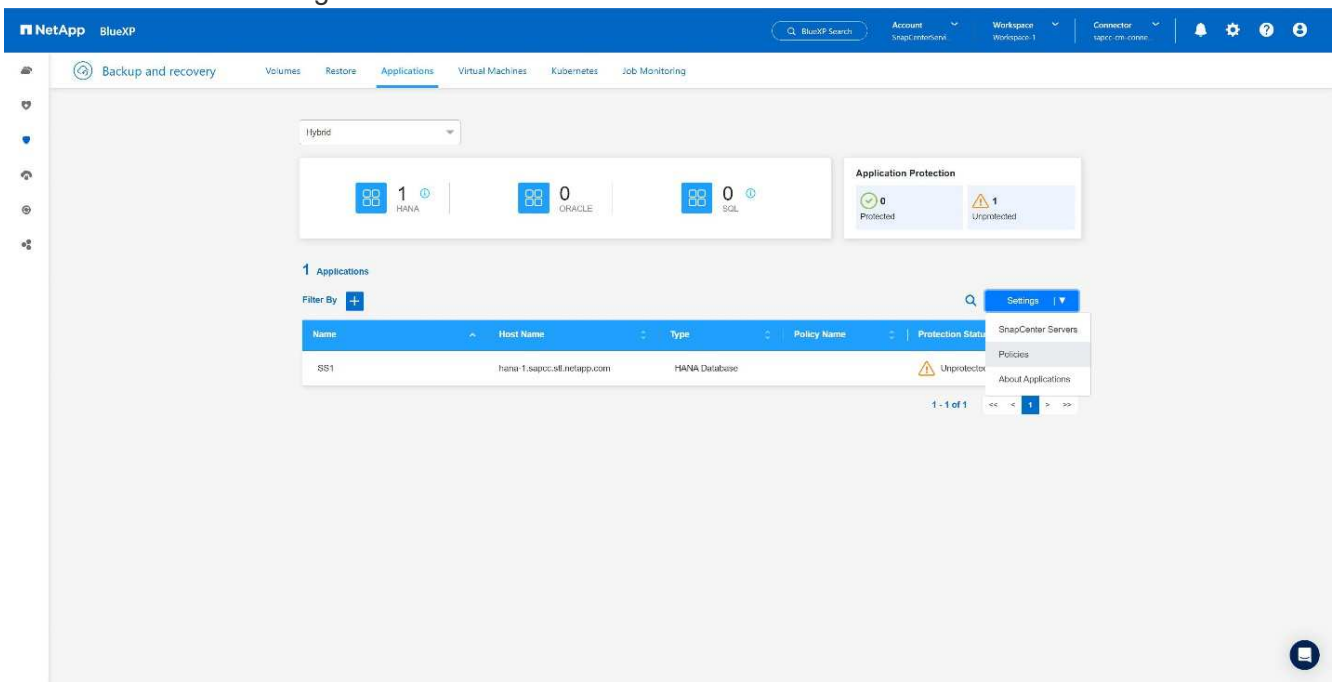


7. Sobald der Ermittlungsjob abgeschlossen ist, steht das SAP HANA-System zur Verfügung. +

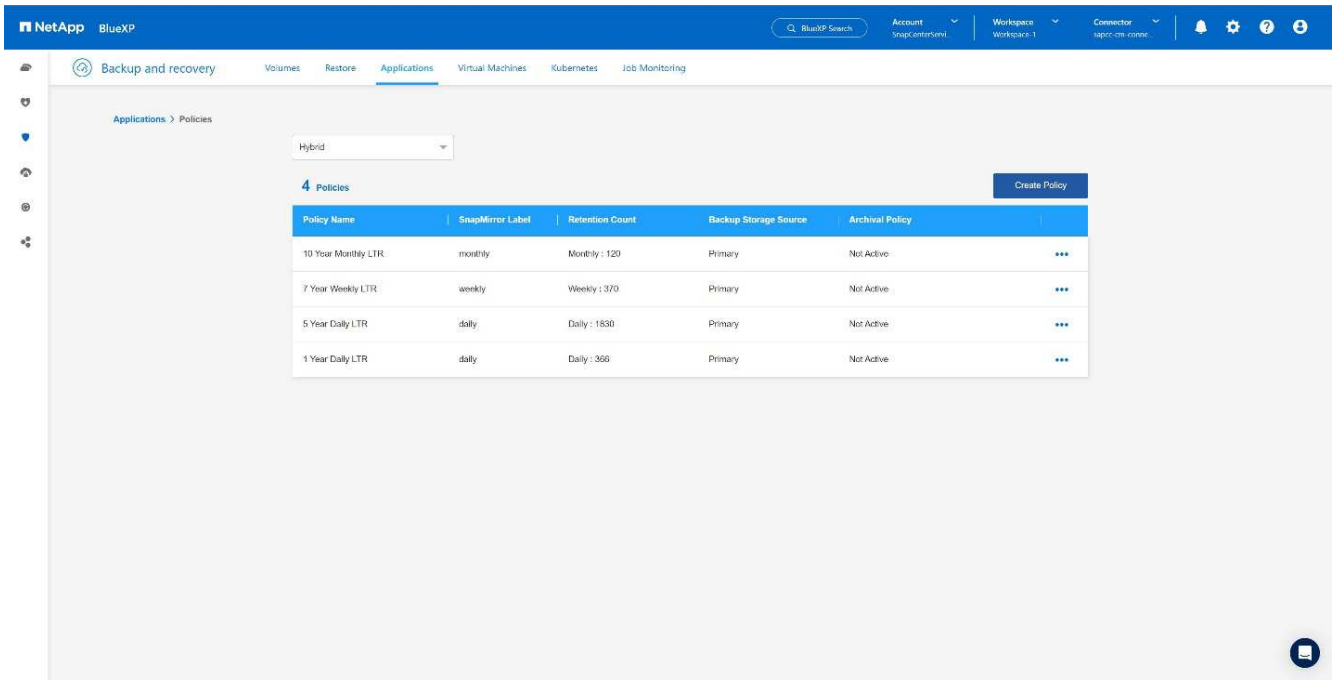


Erstellen einer Backup-Richtlinie für Anwendungsbackups

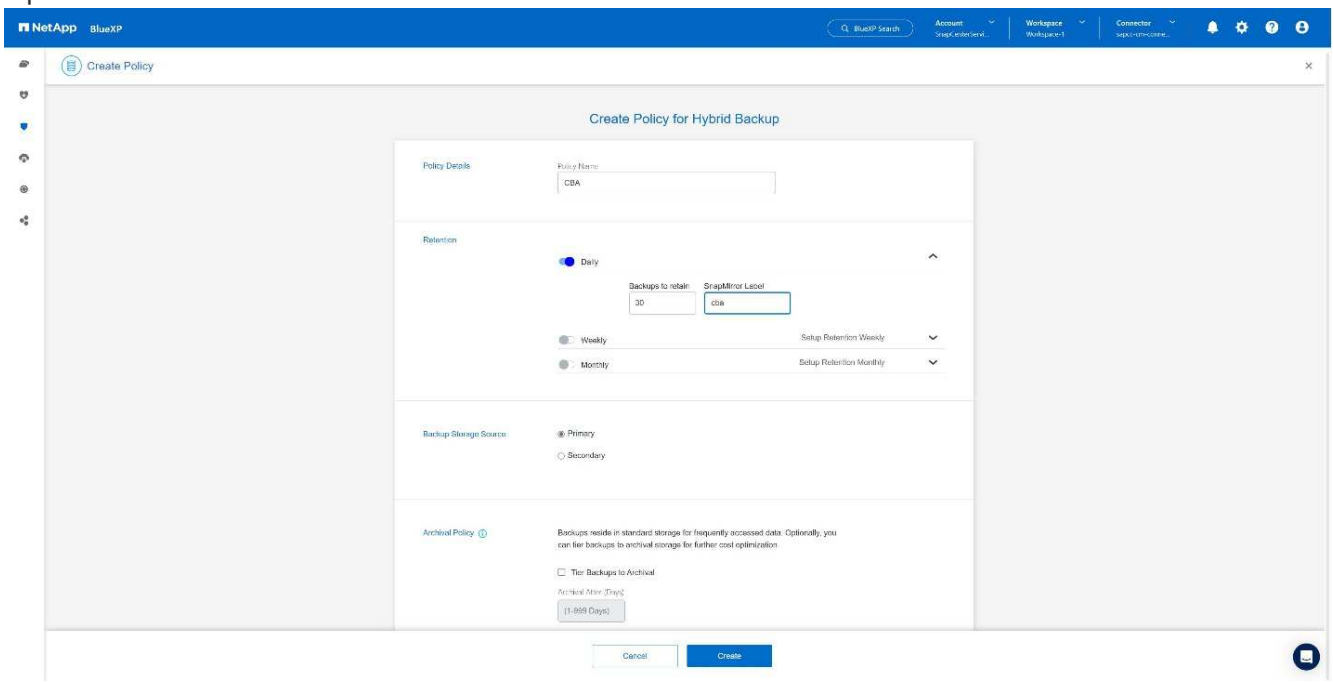
1. Wählen Sie im Einstellungsmenü **Policies** aus. +



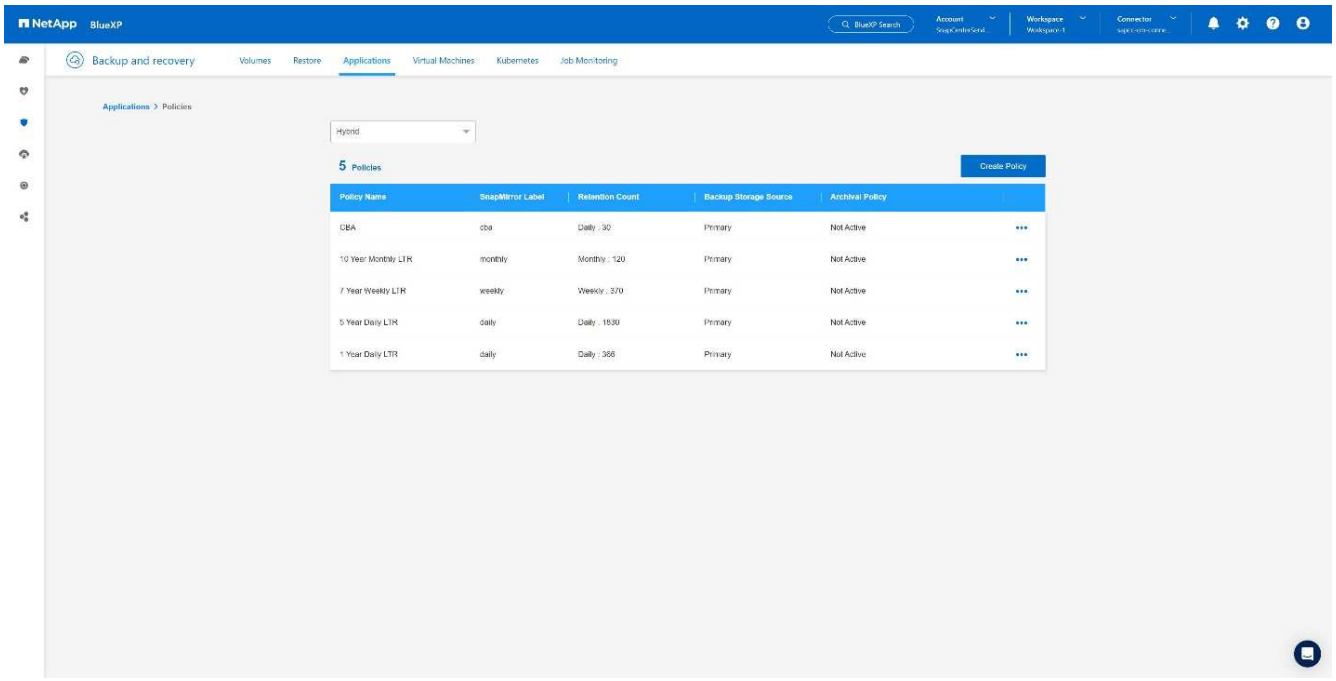
2. Erstellen Sie eine neue Richtlinie, falls gewünscht, indem Sie auf **Richtlinie erstellen** klicken. +



3. Geben Sie den Richtliniennamen an, das gewünschte SnapMirror-Label, wählen Sie Ihre gewünschten Optionen aus und drücken Sie **Create**. +

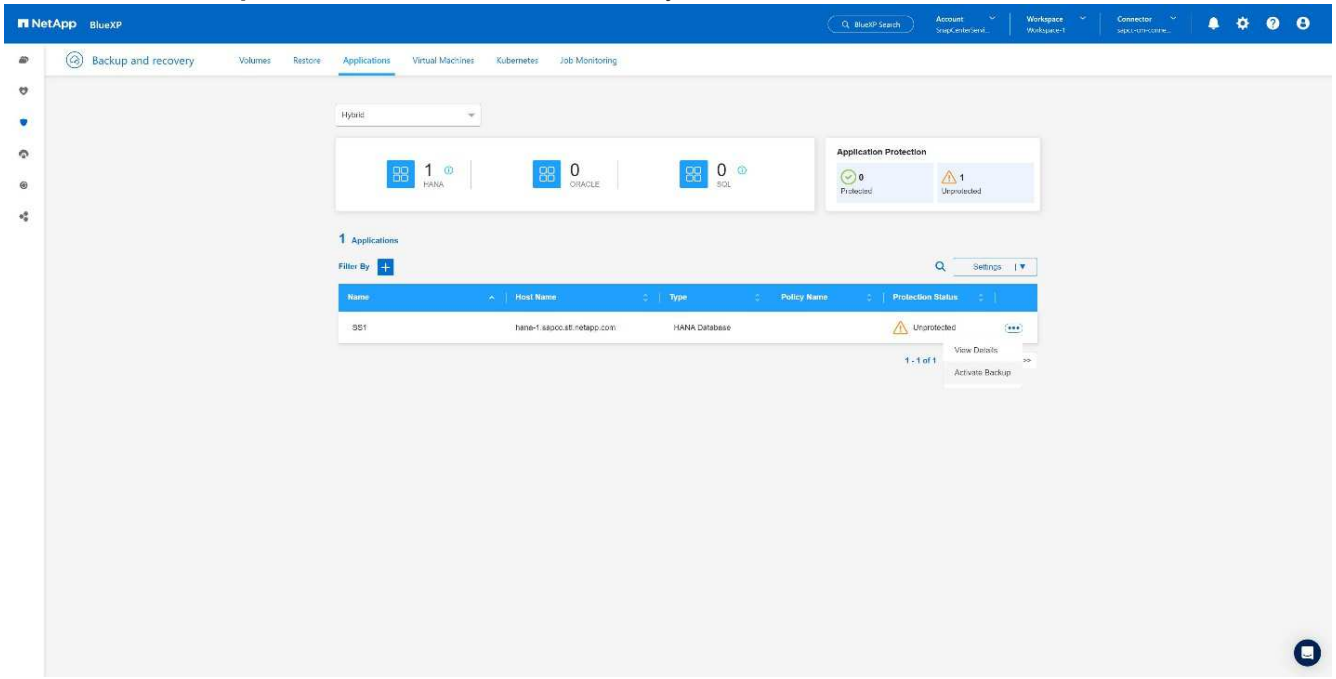


4. Die neue Richtlinie ist verfügbar. +

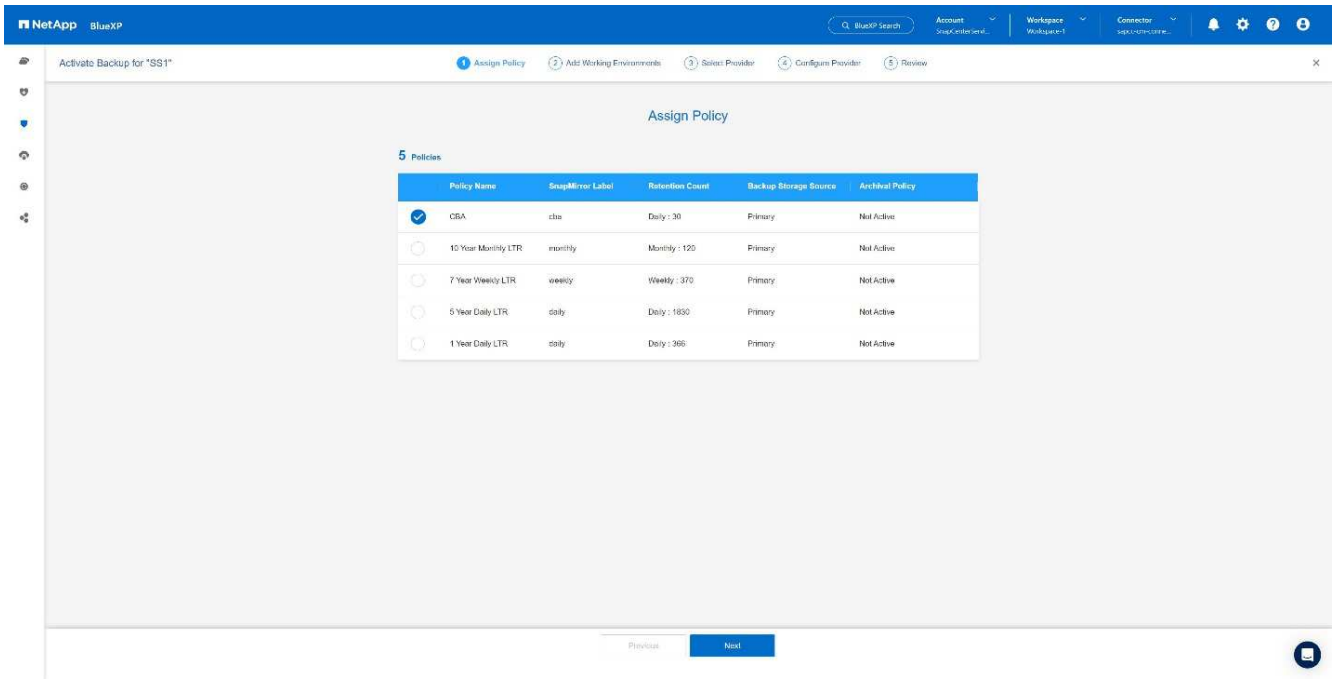


Sicherung der SAP HANA-Datenbank mit Cloud Backup für Applikationen

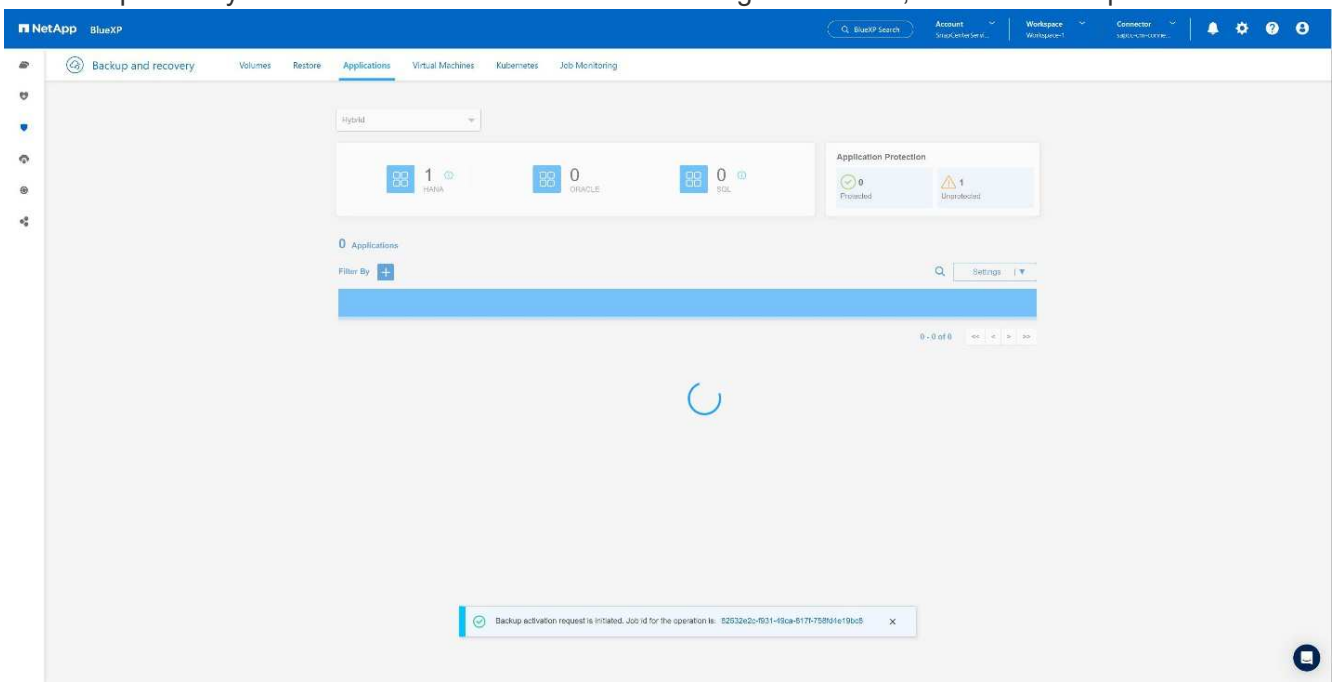
1. Wählen Sie **Backup aktivieren** für das SAP HANA-System. +



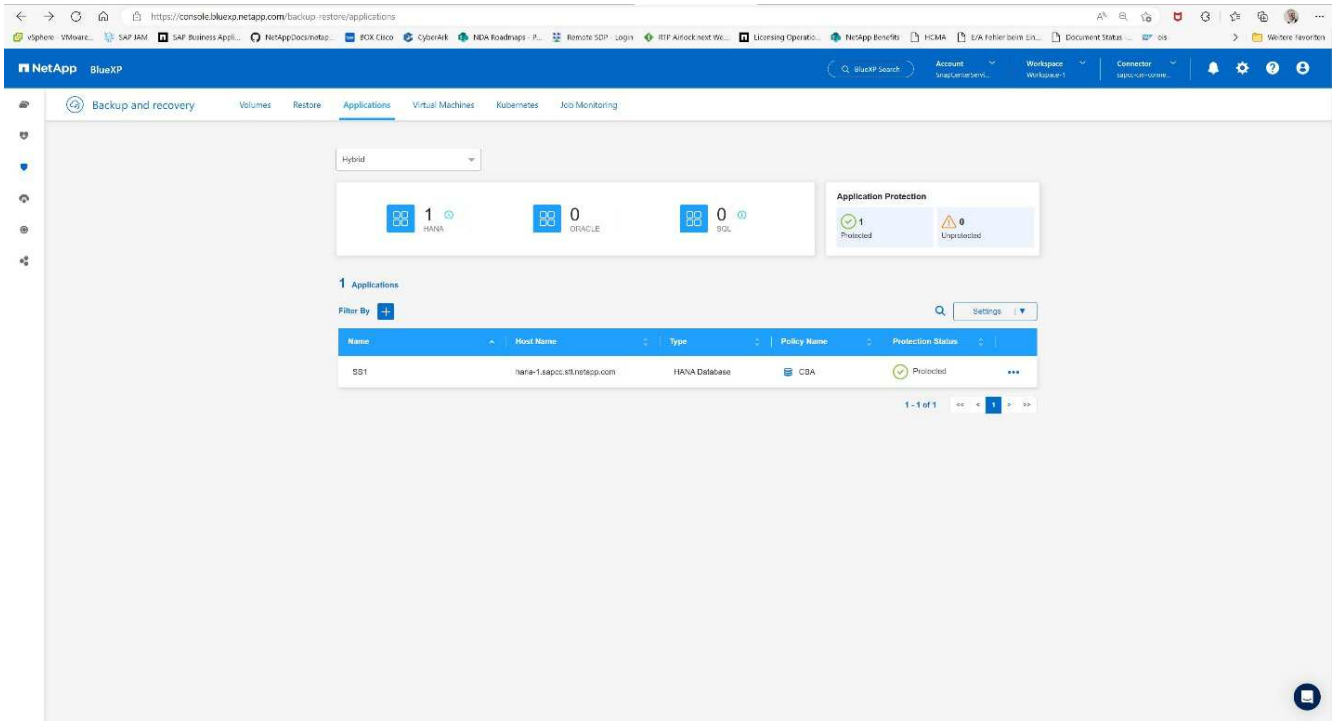
2. Wählen Sie die zuvor erstellte Richtlinie aus und klicken Sie auf **Weiter**. +



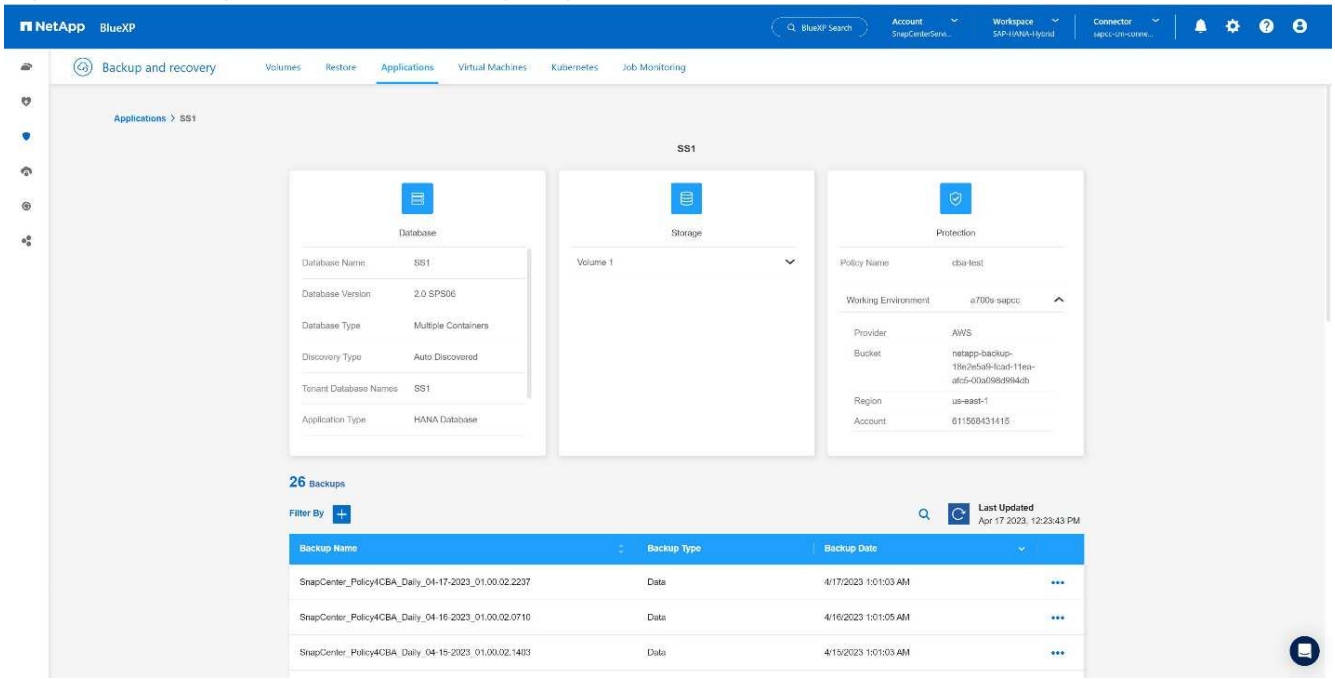
3. Da das Speichersystem und der Konnektor im Voraus konfiguriert haben, wird das Backup aktiviert. +



4. Sobald der Job abgeschlossen ist, wird das System aufgelistet. +



5. Nach einiger Zeit werden die Backups in der Detailansicht des SAP HANA Systems aufgelistet. + Eine tägliche Sicherung wird am nächsten Tag aufgelistet. +

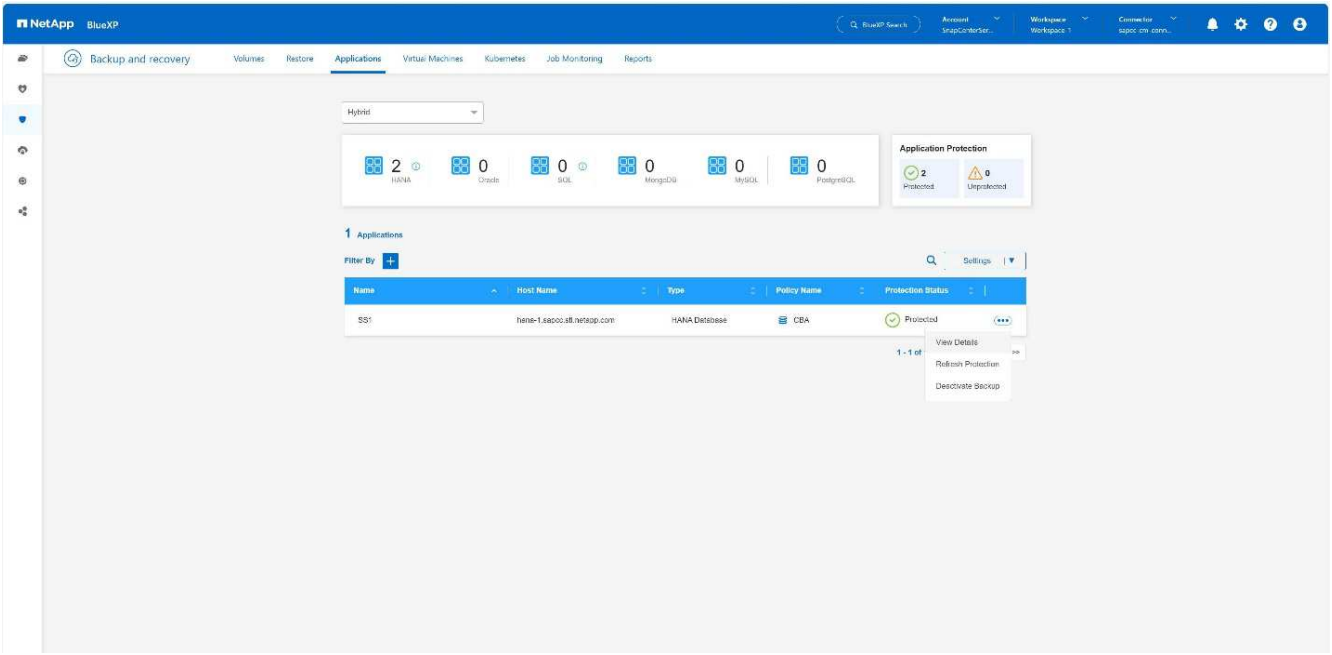


In einigen Umgebungen kann es notwendig sein, vorhandene Planungseinstellungen der snapmirror Quelle zu entfernen. Führen Sie dazu den folgenden Befehl am Quell-ONTAP-System aus: *snapmirror modify -Destination-path <hana-cloud-svm>:<SID_data_mnt00001>_copy -schedule ""* .

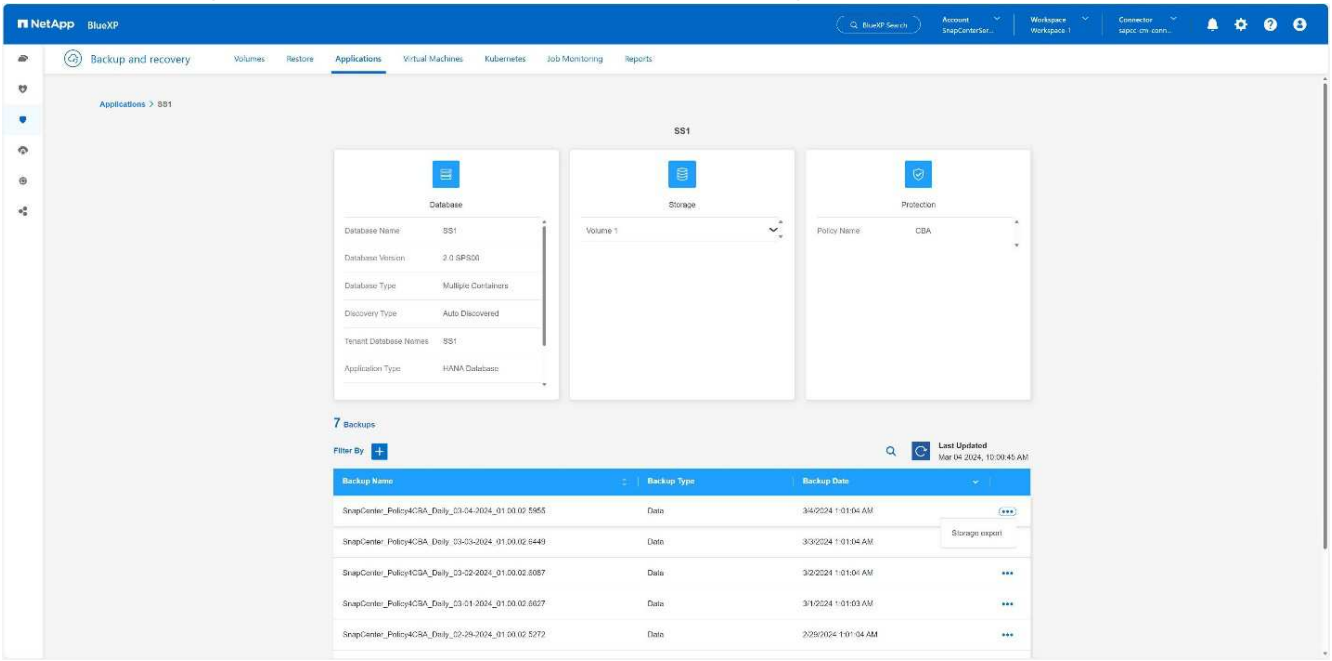
Wiederherstellung von SAP HANA BlueXP Backup

Eine Wiederherstellung aus dem Backup kann nur mit einem On-Premises-NetApp ONTAP-basierten Storage-System oder NetApp CVO in der Cloud erfolgen. Eine Wiederherstellung kann wie folgt durchgeführt werden:

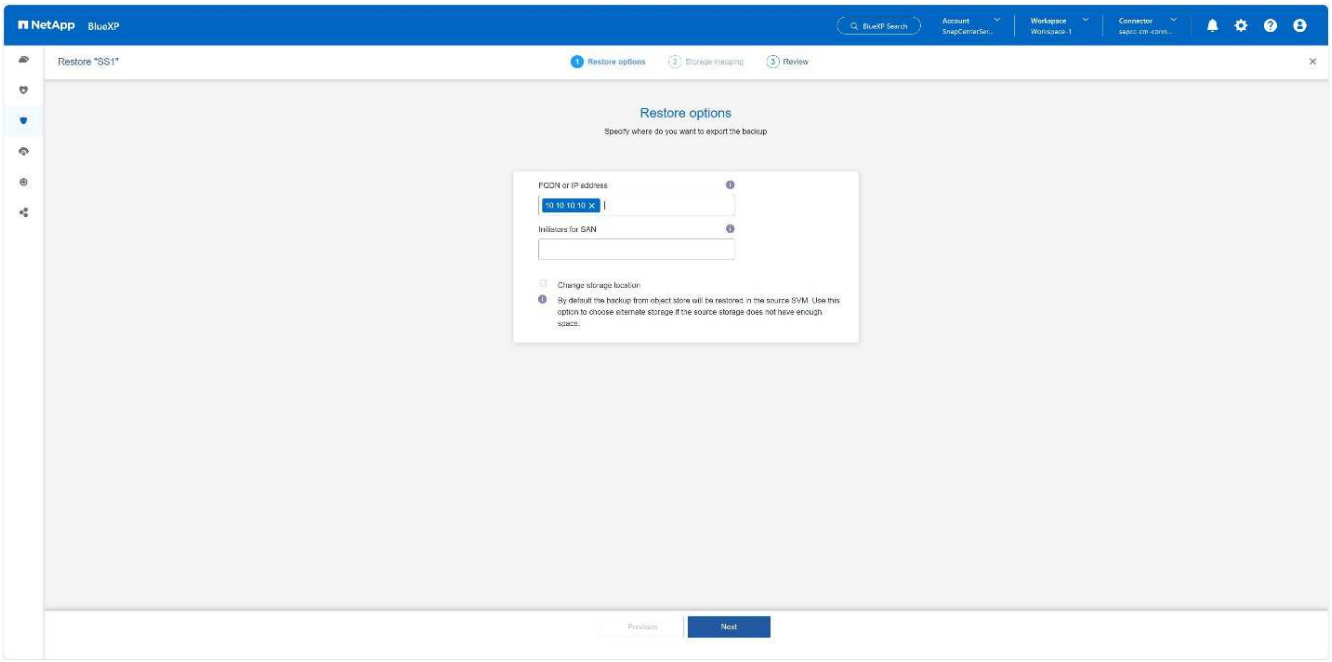
1. Klicken Sie in der Benutzeroberfläche von BlueXP auf **Schutz** > **Backup und Recovery** > **Anwendungen** und wählen Sie Hybrid.
2. Wählen Sie im Feld **Filtern nach** den Filter **Typ** und wählen Sie aus der Dropdown- Liste **HANA** aus.
3. Klicken Sie auf **View Details** für die Datenbank, die Sie wiederherstellen möchten. +



4. Wählen Sie das gewünschte Backup aus, und wählen Sie Storage Export. +



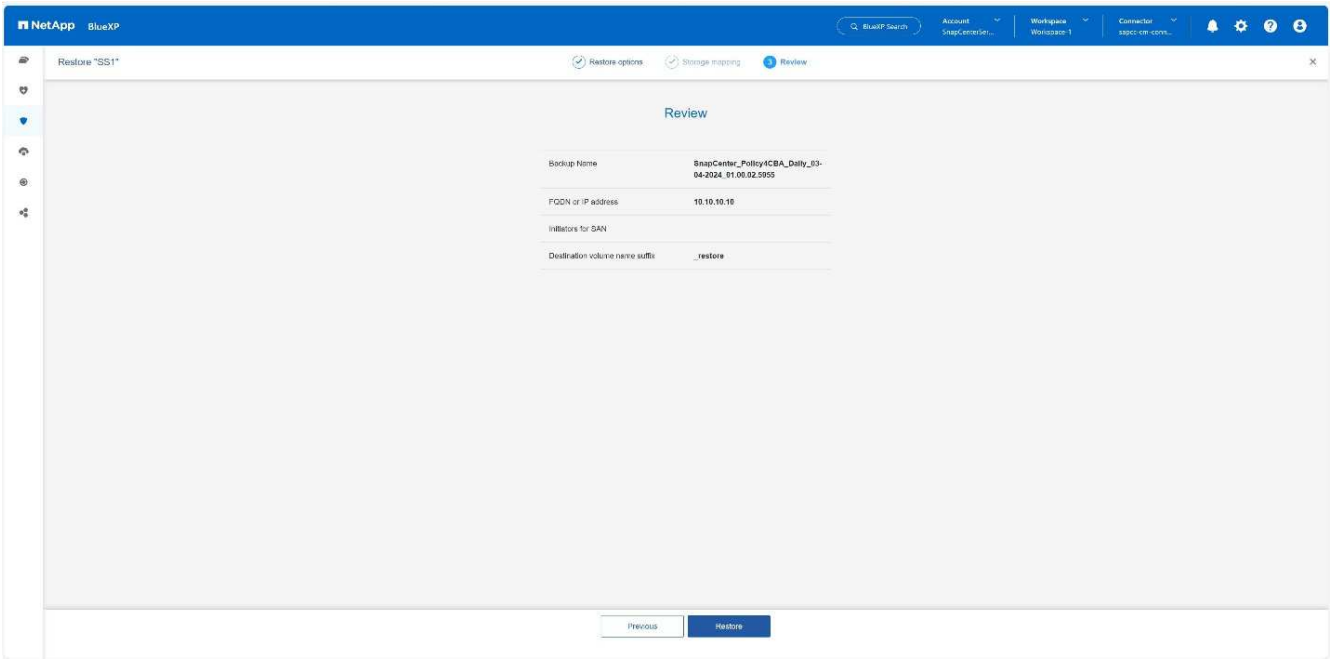
5. Geben Sie die gewünschten Optionen an: +



a. Geben Sie in der NAS-Umgebung den FQDN oder die IP-Adresse des Hosts an, auf den die aus dem Objektspeicher wiederhergestellten Volumes exportiert werden sollen.

b. Geben Sie in der SAN-Umgebung die Initiatoren des Hosts an, dem die LUNs der aus dem Objektspeicher wiederhergestellten Volumes zugeordnet werden sollen.

6. Wenn sich der Snapshot im Archiv-Speicher befindet, wählen Sie die Priorität für die Wiederherstellung der Daten aus dem Archiv-Speicher aus.
7. Wenn nicht genügend Speicherplatz auf dem Quellspeicher vorhanden ist oder der Quellspeicher nicht verfügbar ist, wählen Sie **Speicherort ändern**.
8. Wenn Sie **Speicherort ändern** auswählen, können Sie ein Suffix an das Ziel-Volume anhängen. Wenn Sie das Kontrollkästchen nicht aktiviert haben, wird standardmäßig **_restore** an das Zielvolume angehängt. Klicken Sie Auf **Weiter**.
9. Wenn Sie Speicherort ändern ausgewählt haben, geben Sie die Details zum alternativen Speicherort an, in denen die vom Objektspeicher wiederhergestellten Daten auf der Seite Speicherzuordnung gespeichert werden, und klicken Sie auf **Weiter**.
10. Überprüfen Sie die Details und klicken Sie auf * Wiederherstellen*.



+ + + + dieser Vorgang führt nur den Speicherexport des wiederhergestellten Backups für den angegebenen Host aus. Sie müssen das Dateisystem manuell am Host mounten und die Datenbank aufrufen. Nach der Nutzung des Volumes kann der Speicheradministrator das Volume aus dem ONTAP-Cluster löschen.

Zusätzliche Informationen und Versionsverlauf

In diesem Abschnitt werden weitere Informationen angezeigt und der Versionsverlauf wird angezeigt.

Wo Sie weitere Informationen finden

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- NetApp BlueXP Backup- und Recovery-Produktdokumentation
  "Sichern Sie Ihre On-Premises-Applikationsdaten in der NetApp Dokumentation"
- "Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter"

Versionsverlauf

Version	Datum	Versionsverlauf des Dokuments
Version 1.0	März 2024	Ausgangsversion

Siehe "Interoperabilitäts-Matrix-Tool (IMT)" Überprüfen Sie auf der NetApp Support-Website, ob die in diesem Dokument angegebenen Produktversionen und Funktionen in Ihrer IT-Umgebung unterstützt werden. Das NetApp IMT definiert die Produktkomponenten und -Versionen, die für von NetApp unterstützte Konfigurationen verwendet werden können. Die spezifischen Ergebnisse hängen von der Installation des jeweiligen Kunden gemäß den technischen Daten ab.

SAP HANA System Replication Backup und Recovery mit SnapCenter

TR-4719: SAP HANA System Replication – Backup und Recovery mit SnapCenter

SAP HANA System Replication wird häufig als Hochverfügbarkeits- oder Disaster-Recovery-Lösung für SAP HANA Datenbanken verwendet. SAP HANA System Replication bietet verschiedene Betriebsmodi, die Sie je nach Anwendungsfall oder Verfügbarkeitsanforderungen verwenden können.

Autor: Nils Bauer, NetApp

Es gibt zwei primäre Anwendungsfälle, die miteinander kombiniert werden können:

- Hochverfügbarkeit mit einem Recovery Point Objective (RPO) von null und einem minimalen Recovery Time Objective (RTO) unter Verwendung eines dedizierten sekundären SAP HANA-Hosts
- Disaster Recovery über große Entfernungen: Der sekundäre SAP HANA-Host kann auch im normalen Betrieb für Entwicklung oder Tests verwendet werden.

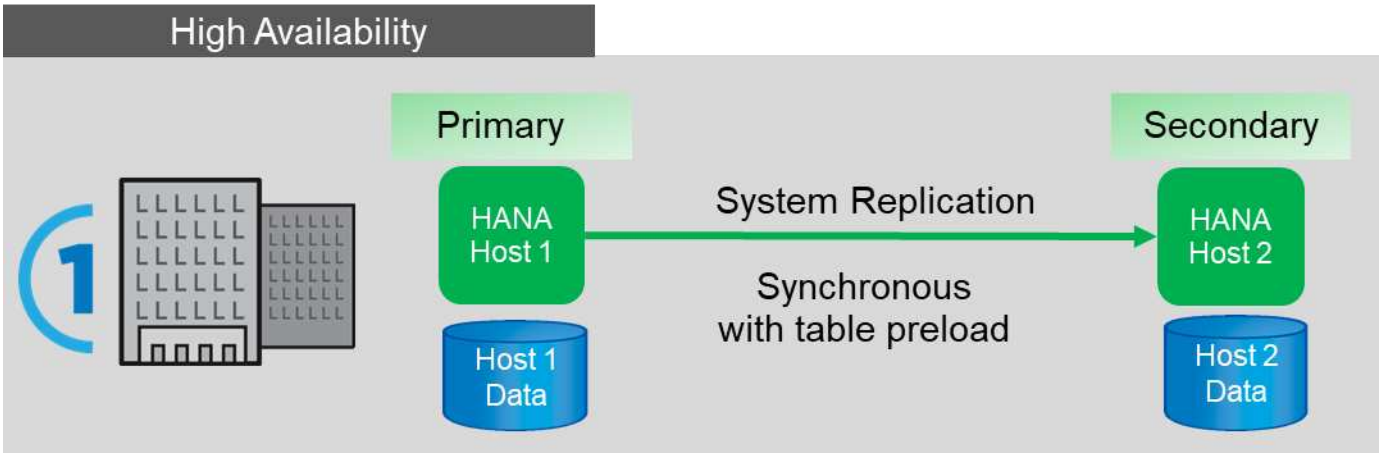
Hochverfügbarkeit ohne RPO und mit minimalem RTO-Aufwand

System Replication ist mit synchroner Replizierung konfiguriert und verwendet Tabellen, die auf dem sekundären SAP HANA-Host vorab in den Speicher geladen sind. Diese Hochverfügbarkeitslösung lässt sich bei Hardware- oder Softwareausfällen einsetzen und reduziert zudem geplante Ausfallzeiten während SAP HANA Software-Upgrades (Betrieb fast ohne Ausfallzeit).

Failover-Vorgänge werden oft mithilfe von Cluster-Software eines Drittanbieters oder mit einem Workflow mit SAP Landscape Management Software mit nur einem Klick automatisiert.

Aus der Perspektive der Backup-Anforderungen müssen Backups erstellt werden können, unabhängig davon, welcher SAP HANA Host primärer oder sekundärer ist. Eine gemeinsam genutzte Backup-Infrastruktur wird verwendet, um alle Backups wiederherzustellen, unabhängig davon, auf welchem Host das Backup erstellt wurde.

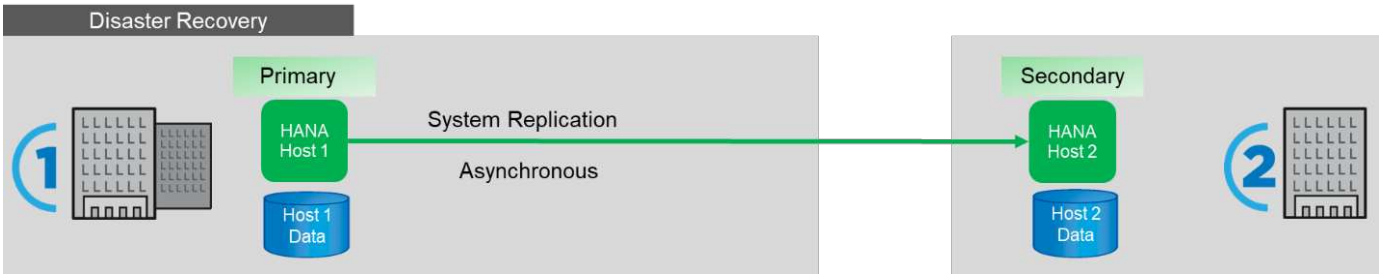
Der Rest dieses Dokuments konzentriert sich auf Backup-Vorgänge mit SAP System Replication, konfiguriert als Hochverfügbarkeitslösung.



Disaster Recovery über große Entfernungen

Die Systemreplizierung kann mit asynchroner Replizierung konfiguriert werden, ohne dass Tabelle auf dem sekundären Host vorab in den Speicher geladen wird. Diese Lösung dient der Behebung von Datacenter-Ausfällen. Failover-Vorgänge werden normalerweise manuell durchgeführt.

Hinsichtlich der Backup-Anforderungen müssen Sie in der Lage sein, Backups während des normalen Betriebs in Datacenter 1 und bei Disaster Recovery in Datacenter 2 zu erstellen. In Datacentern 1 und 2 ist eine separate Backup-Infrastruktur verfügbar, Backup-Vorgänge werden als Teil des Disaster Failover aktiviert. Die Backup-Infrastruktur ist in der Regel nicht gemeinsam genutzt und ein Restore eines Backups, das auf dem anderen Datacenter erstellt wurde, ist nicht möglich.



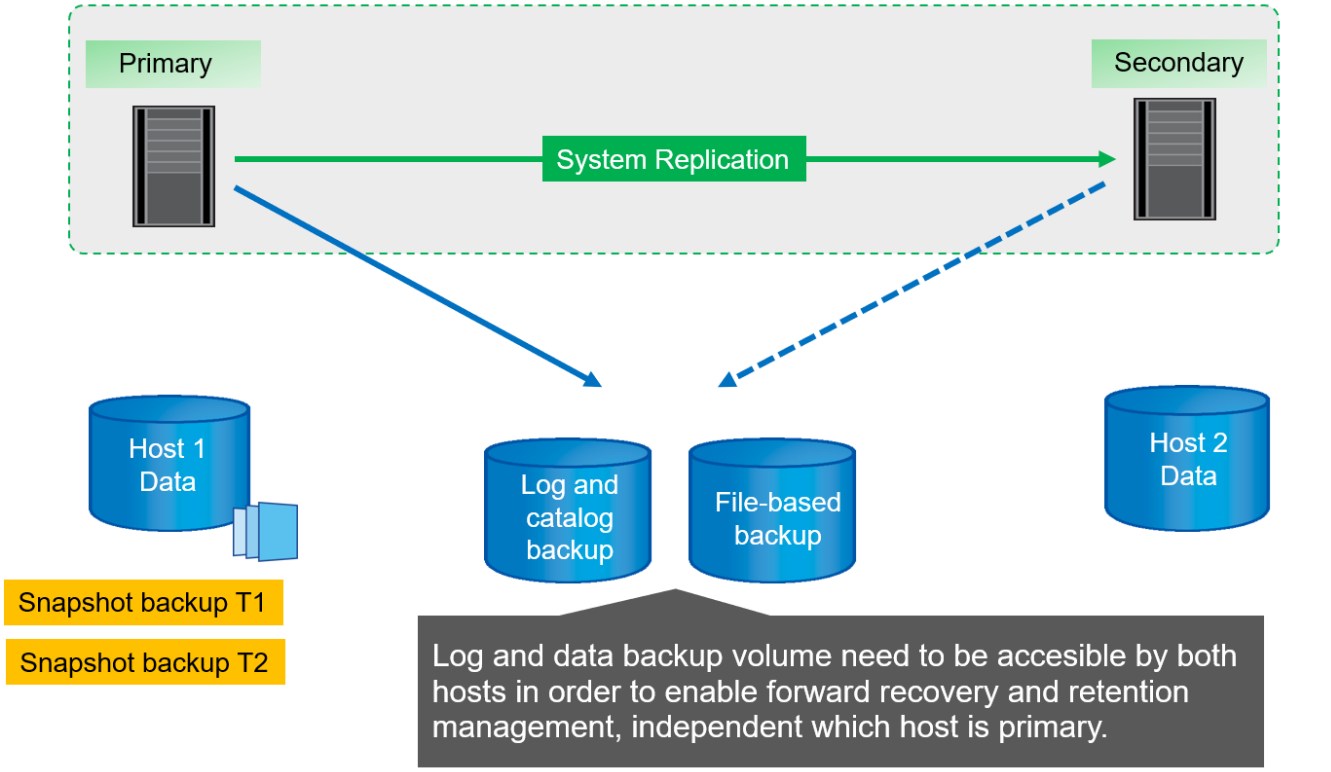
Storage Snapshot Backups und SAP System Replication

Backup-Vorgänge werden immer auf dem primären SAP HANA-Host durchgeführt. Die erforderlichen SQL-Befehle für den Backup-Vorgang können nicht auf dem sekundären SAP HANA-Host ausgeführt werden.

Für SAP HANA-Backup-Vorgänge sind die primären und sekundären SAP HANA-Hosts eine Einheit. Sie verwenden denselben SAP HANA Backup-Katalog und nutzen die Backups für die Wiederherstellung und das Recovery, unabhängig davon, ob das Backup auf dem primären oder sekundären SAP HANA-Host erstellt wurde.

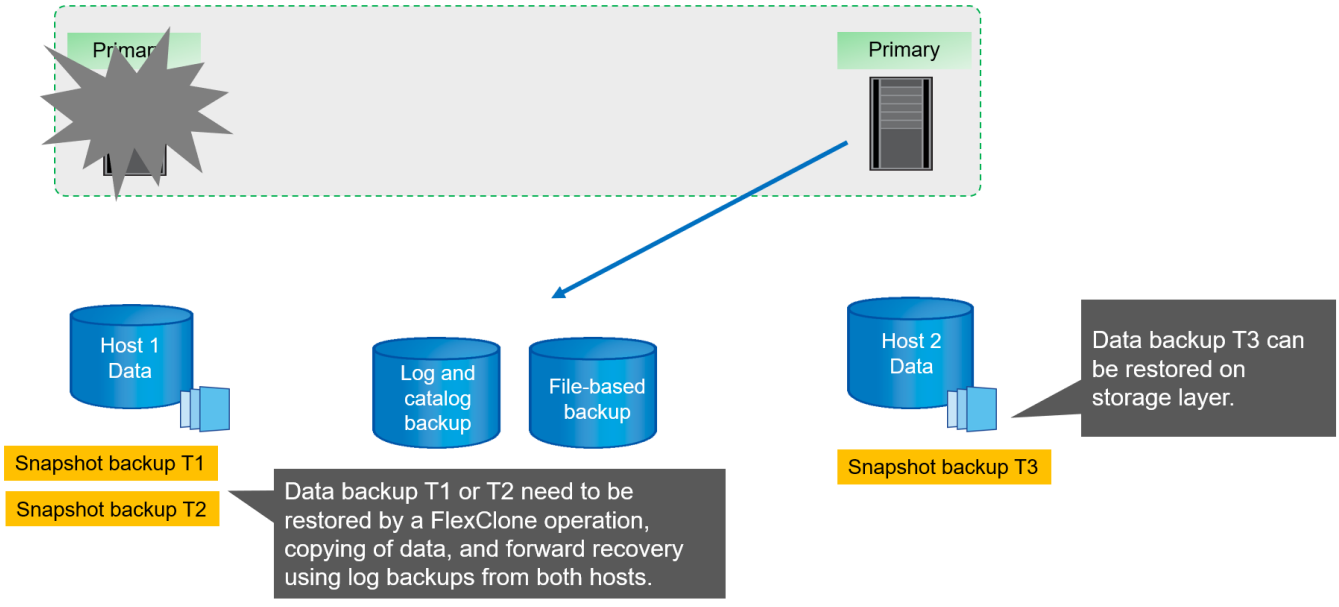
Da jedes Backup für die Wiederherstellung verwendet und mithilfe von Log-Backups von beiden Hosts durchgeführt werden kann, ist ein gemeinsamer Backup-Ort für Protokolle erforderlich, auf den von beiden Hosts zugegriffen werden kann. NetApp empfiehlt die Verwendung eines Shared Storage Volume. Sie sollten jedoch auch das Ziel der Protokollsicherung in Unterverzeichnisse innerhalb des gemeinsam genutzten Volumes trennen.

Jeder SAP HANA-Host verfügt über ein eigenes Storage-Volume. Wenn Sie einen Storage-basierten Snapshot für ein Backup verwenden, wird ein Datenbank-konsistenter Snapshot auf dem Speicher-Volume des primären SAP HANA-Hosts erstellt.



Wenn ein Failover zu Host 2 durchgeführt wird, wird Host 2 zum primären Host, die Backups werden auf Host 2 ausgeführt und Snapshot Backups werden auf dem Storage Volume von Host 2 erstellt.

Das auf Host 2 erstellte Backup kann direkt auf der Speicherebene wiederhergestellt werden. Wenn Sie ein Backup verwenden müssen, das auf Host 1 erstellt wurde, muss das Backup vom Host-1-Speicher-Volume auf das Host-2-Speicher-Volume kopiert werden. Die vorwärts-Wiederherstellung verwendet die Protokoll-Backups von beiden Hosts.

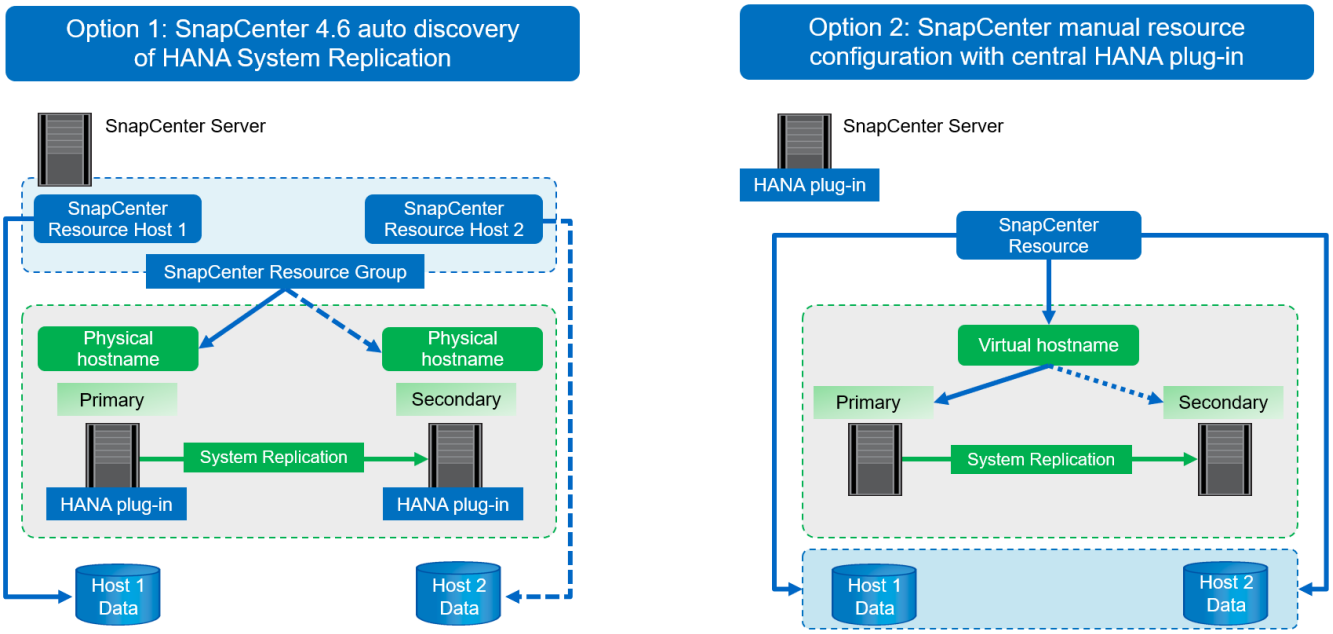


SnapCenter Konfigurationsoptionen für SAP System Replication

Es gibt zwei Optionen zur Konfiguration der Datensicherung mit der NetApp SnapCenter

Software in einer SAP HANA System Replication Umgebung:

- Eine SnapCenter-Ressourcengruppe, die sowohl SAP HANA-Hosts als auch automatische Erkennung mit SnapCenter Version 4.6 oder höher enthält
- Eine einzige SnapCenter-Ressource für beide SAP HANA-Hosts, die eine virtuelle IP-Adresse verwendet



Ab SnapCenter 4.6 unterstützt SnapCenter die automatische Erkennung von HANA-Systemen, die in einer HANA-System-Replizierungsbeziehung konfiguriert sind. Jeder Host wird mit seiner physischen IP-Adresse (Host-Name) und seinem individuellen Daten-Volume auf der Storage-Ebene konfiguriert. Die beiden SnapCenter Ressourcen werden zu einer Ressourcengruppe kombiniert. SnapCenter erkennt automatisch, welcher Host sich auf einem primären oder sekundären Volume befindet, und führt die erforderlichen Backup-Vorgänge entsprechend aus. Das Aufbewahrungsmanagement für Snapshot und dateibasierte Backups, die durch SnapCenter erstellt wurden, erfolgt über beide Hosts hinweg. So wird sichergestellt, dass alte Backups auch am aktuellen sekundären Host gelöscht werden.

Mit einer Einzelressourcenkonfiguration für beide SAP HANA-Hosts ist die einzelne SnapCenter-Ressource unter Verwendung der virtuellen IP-Adresse der SAP HANA System Replication-Hosts konfiguriert. Beide Datenvolumen der SAP HANA-Hosts sind in der SnapCenter-Ressource enthalten. Da es sich um eine einzelne SnapCenter Ressource handelt, funktioniert das Aufbewahrungsmanagement für Snapshot und dateibasierte Backups, die von SnapCenter erstellt wurden, unabhängig davon, welcher Host derzeit als primärer oder sekundärer Host gilt. Diese Option ist bei allen SnapCenter Versionen möglich.

In der folgenden Tabelle sind die wichtigsten Unterschiede der beiden Konfigurationsoptionen zusammengefasst.

	Ressourcengruppe mit SnapCenter 4.6	**Einzelne SnapCenter-Ressource und virtuelle IP-Adresse**
Backup-Vorgang (Snapshot und dateibasiert)	Automatische Identifizierung des primären Hosts in der Ressourcengruppe	Virtuelle IP-Adresse automatisch verwenden
Aufbewahrungsmanagement (Snapshot und dateibasiert)	Automatisch auf beiden Hosts ausgeführt	Automatische Verwendung einzelner Ressourcen

	Ressourcengruppe mit SnapCenter 4.6	Einzelne SnapCenter-Ressource und virtuelle IP-Adresse
Kapazitätsanforderungen des Backups	Backups werden nur auf dem primären Host Volume erstellt	Backups werden immer auf beiden Hosts Volumes erstellt. Das Backup des zweiten Hosts ist nur absturzkonsistent und kann nicht verwendet werden, um eine Rollback durchzuführen.
Wiederherstellungsvorgang	Backups von aktuell aktivem Host stehen für die Wiederherstellung zur Verfügung	Skript zur Vorsicherung erforderlich, um zu ermitteln, welche Backups gültig sind und für die Wiederherstellung verwendet werden können
Recovery-Vorgang	Alle verfügbaren Recovery-Optionen, wie bei jeder automatisch erkannten Ressource	Manuelle Wiederherstellung erforderlich

Im Allgemeinen empfiehlt NetApp, die Konfigurationsoption für Ressourcengruppen mit SnapCenter 4.6 zu verwenden, um HANA Systeme mit aktivierter HANA System Replication zu schützen. Eine einzelne SnapCenter-Ressourcenkonfiguration ist nur erforderlich, wenn der SnapCenter-Operationsansatz auf einem zentralen Plug-in-Host basiert und das HANA-Plug-in nicht auf den HANA-Datenbank-Hosts implementiert ist.

Die beiden Optionen werden in den folgenden Abschnitten näher erläutert.

Konfiguration von SnapCenter 4.6 unter Verwendung einer Ressourcengruppe

SnapCenter 4.6 unterstützt die automatische Erkennung von HANA-Systemen, die mit HANA System Replication konfiguriert sind. SnapCenter 4.6 umfasst die Logik zur Identifizierung primärer und sekundärer HANA-Hosts während des Backup-Betriebs sowie für das Management der Datenaufbewahrung über beide HANA-Hosts hinweg. Darüber hinaus sind jetzt auch automatisierte Wiederherstellungen und Recovery für HANA System Replication-Umgebungen verfügbar.

SnapCenter 4.6-Konfiguration von HANA System Replication-Umgebungen

Die folgende Abbildung zeigt die für dieses Kapitel verwendete Laboreinrichtung. Zwei HANA-Hosts, hana-3 und hana-4, wurden mit HANA System Replication konfiguriert.

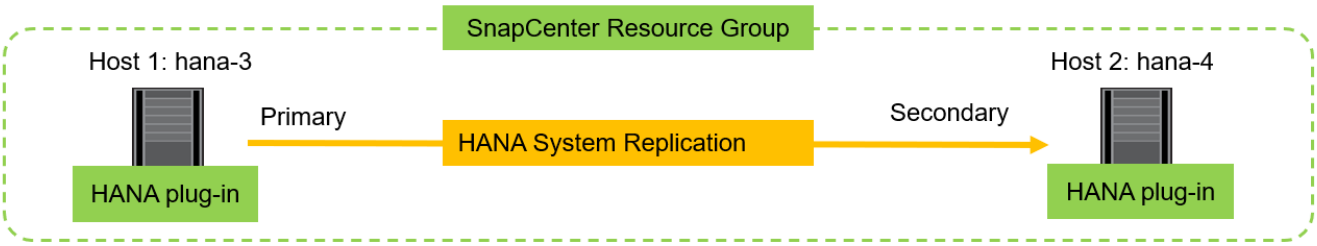
Für die HANA-Systemdatenbank wurde ein Datenbankbenutzer „SnapCenter“ mit den erforderlichen Privileges erstellt, um Backup- und Recovery-Vorgänge auszuführen (siehe "Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter"). Ein HANA-Benutzerspeicherschlüssel muss auf beiden Hosts mit dem oben genannten Datenbankbenutzer konfiguriert sein.

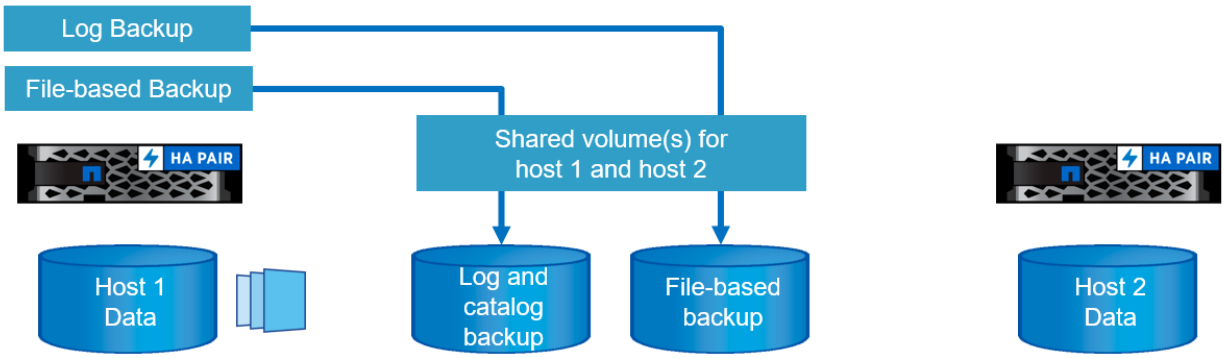
```
ss2adm@hana- 3: / > hdbuserstore set SS2KEY hana- 3:33313 SNAPCENTER
<password>
```

```
ss2adm@hana- 4:/ > hdbuserstore set SS2KEY hana-4:33313 SNAPCENTER
<password>
```

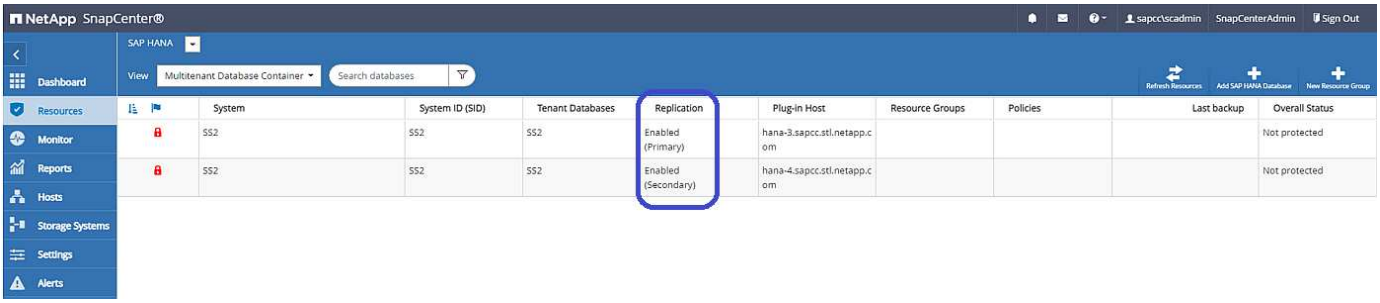
Aus einer übergeordneten Sicht müssen Sie die folgenden Schritte durchführen, um HANA System Replication in SnapCenter einzurichten.

1. Das HANA-Plug-in wird auf dem primären und sekundären Host installiert. Die automatische Ermittlung wird ausgeführt und der Status der HANA-Systemreplizierung wird für jeden primären oder sekundären Host erkannt.
2. Ausführen von SnapCenter `configure database` Und stellen die bereit `hdbuserstore` Taste. Weitere automatische Erkennungsvorgänge werden ausgeführt.
3. Erstellen Sie eine Ressourcengruppen, einschließlich beider Hosts, und konfigurieren Sie den Schutz.

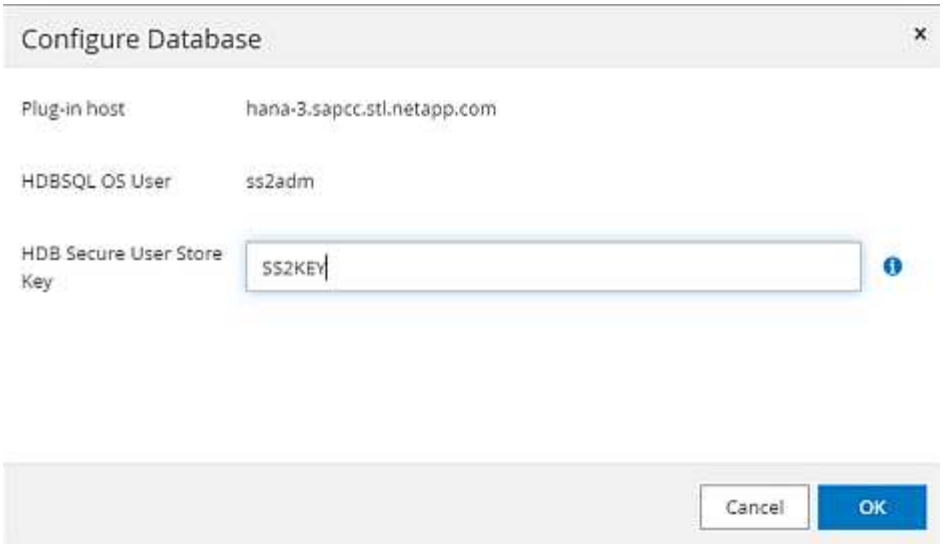




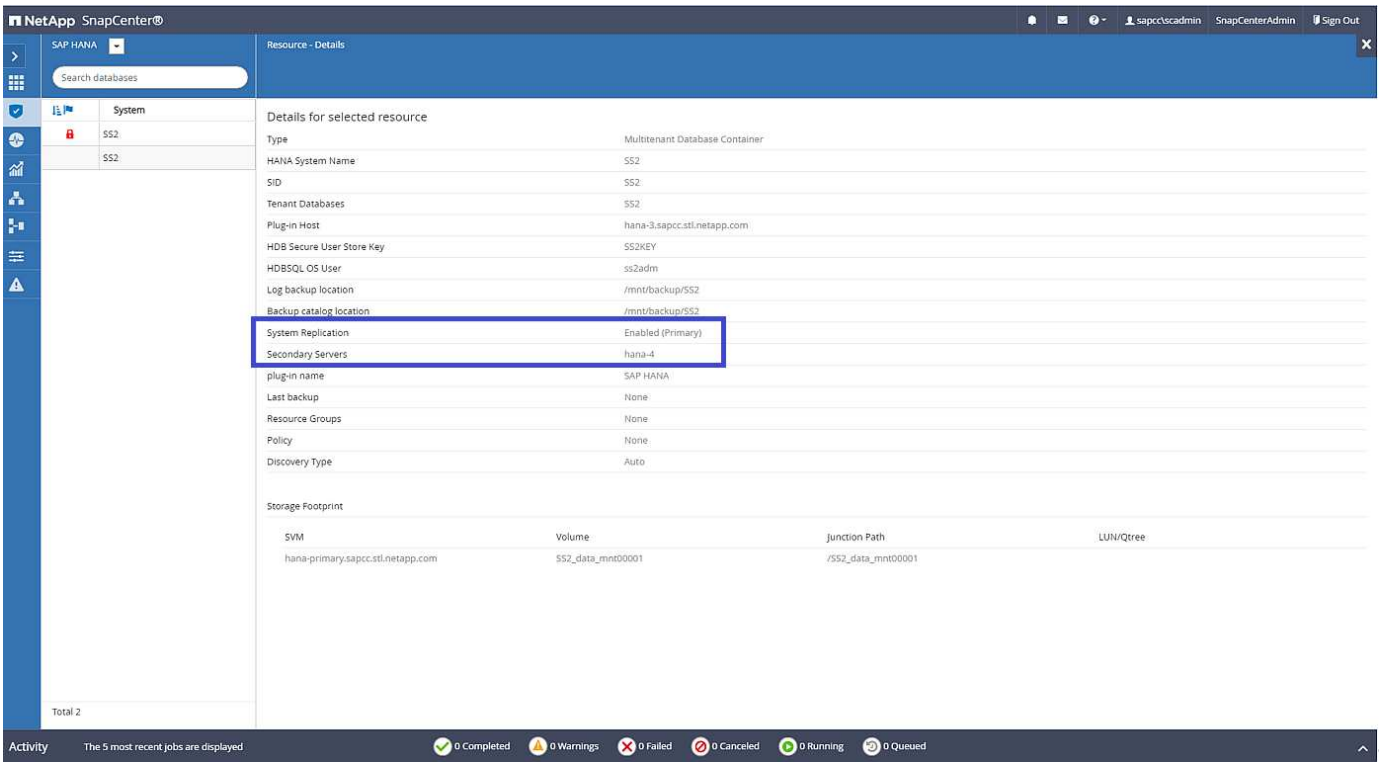
Nachdem Sie das SnapCenter HANA Plug-in auf beiden HANA-Hosts installiert haben, werden die HANA-Systeme in der Ansicht der SnapCenter-Ressourcen wie andere automatisch erkannte Ressourcen angezeigt. Ab SnapCenter 4.6 wird eine zusätzliche Spalte angezeigt, in der der Status der HANA-Systemreplizierung (aktiviert/deaktiviert, primär/sekundär) angezeigt wird.



Durch Klicken auf die Ressource fordert SnapCenter den HANA-Benutzerspeicherschlüssel für das HANA-System an.

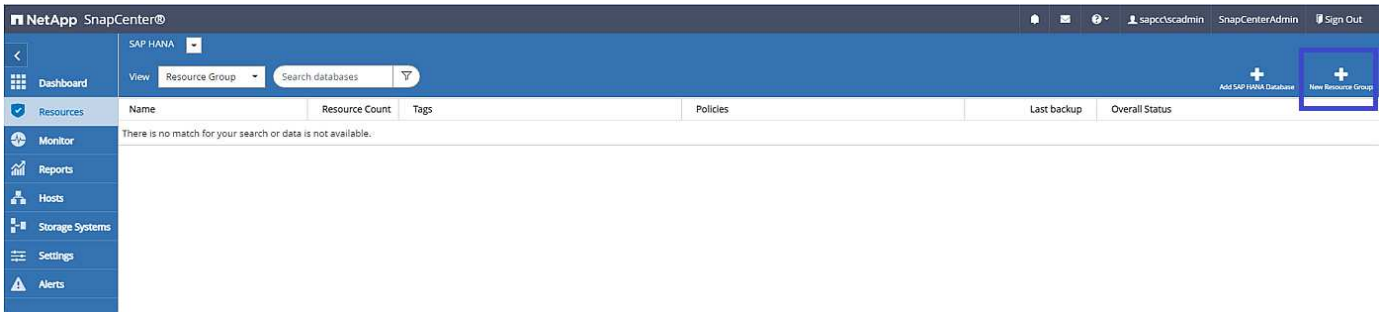


Weitere Schritte zur automatischen Ermittlung werden ausgeführt, und SnapCenter zeigen die Ressourcendetails an. In SnapCenter 4.6 werden der Replikationsstatus des Systems und der sekundäre Server in dieser Ansicht aufgelistet.

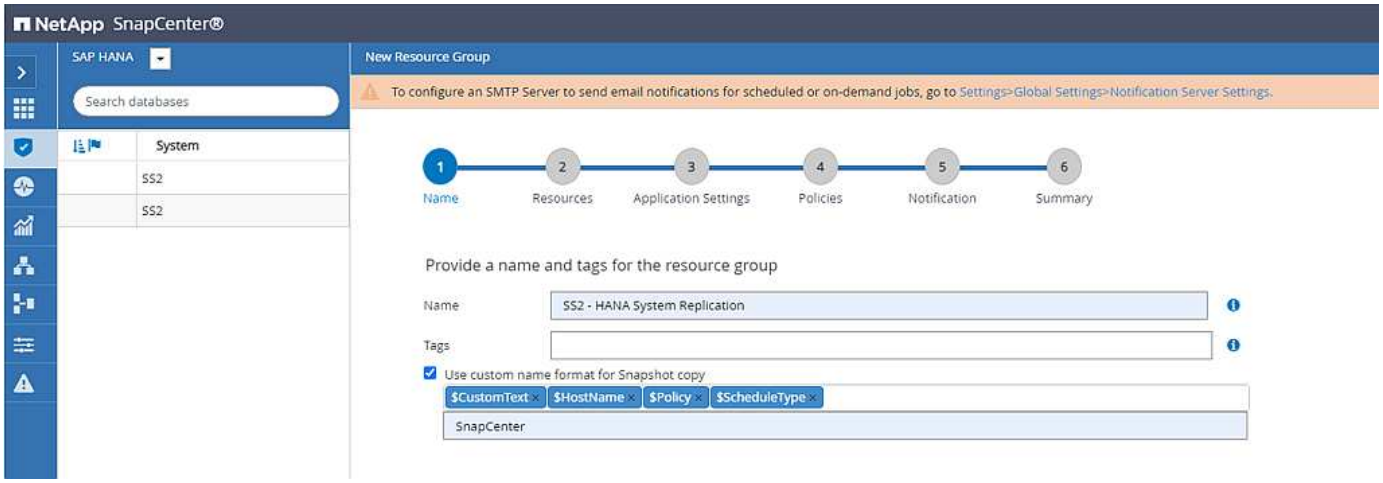


Nach Durchführung der gleichen Schritte für die zweite HANA-Ressource ist die automatische Ermittlung abgeschlossen, und beide HANA-Ressourcen werden in SnapCenter konfiguriert.

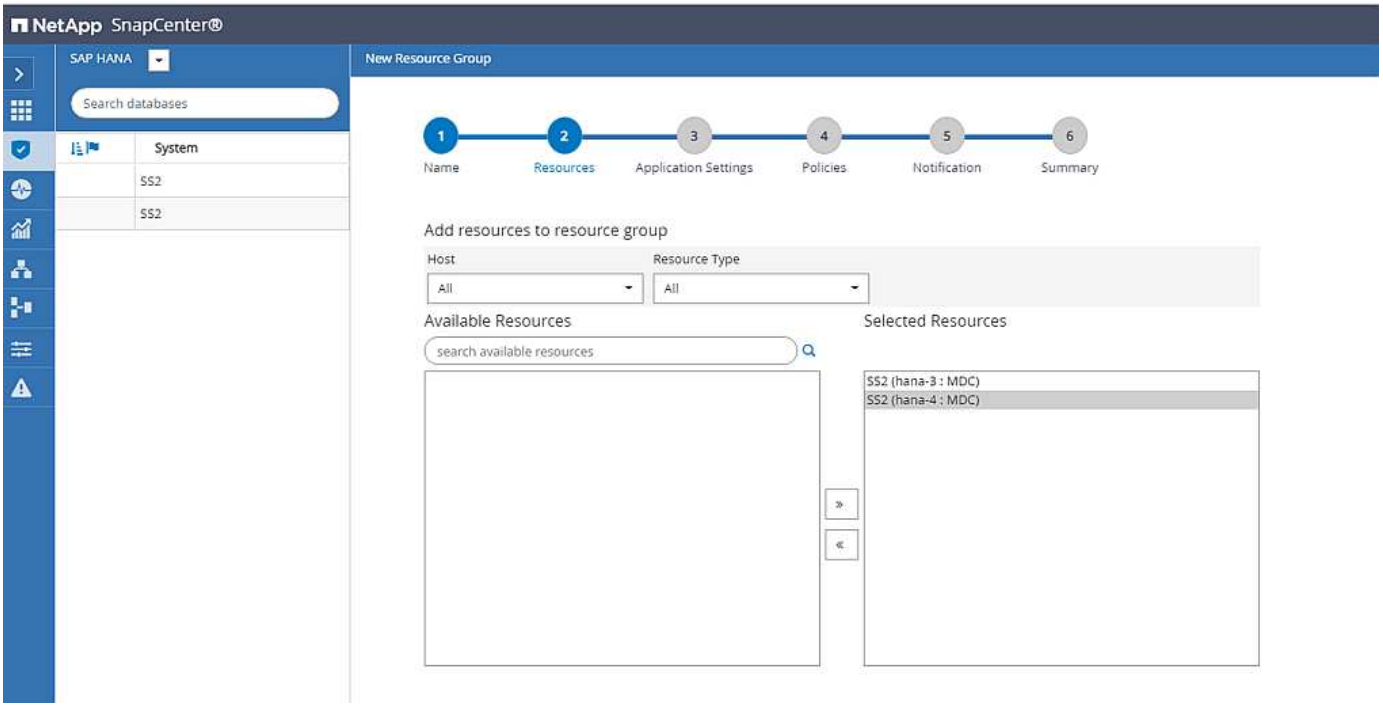
Für HANA System Replication-fähige Systeme müssen Sie eine SnapCenter-Ressourcengruppe, einschließlich beider HANA-Ressourcen, konfigurieren.



NetApp empfiehlt die Verwendung eines benutzerdefinierten Namensformats für den Snapshot-Namen. Dieser sollte den Hostnamen, die Richtlinie und den Zeitplan enthalten.

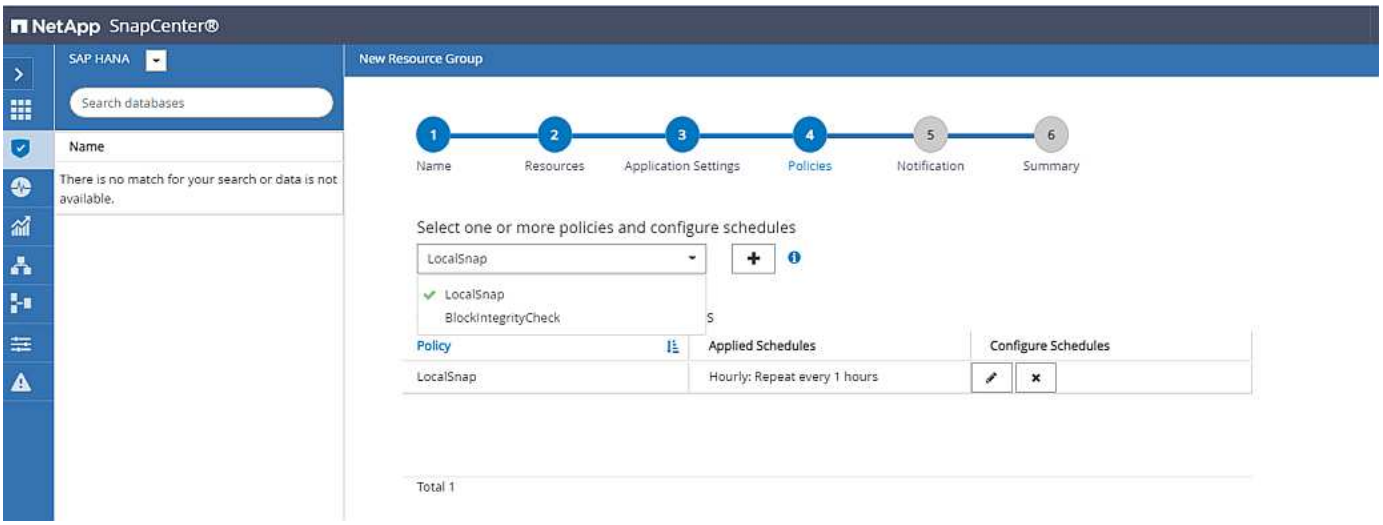


Sie müssen der Ressourcengruppe beide HANA-Hosts hinzufügen.

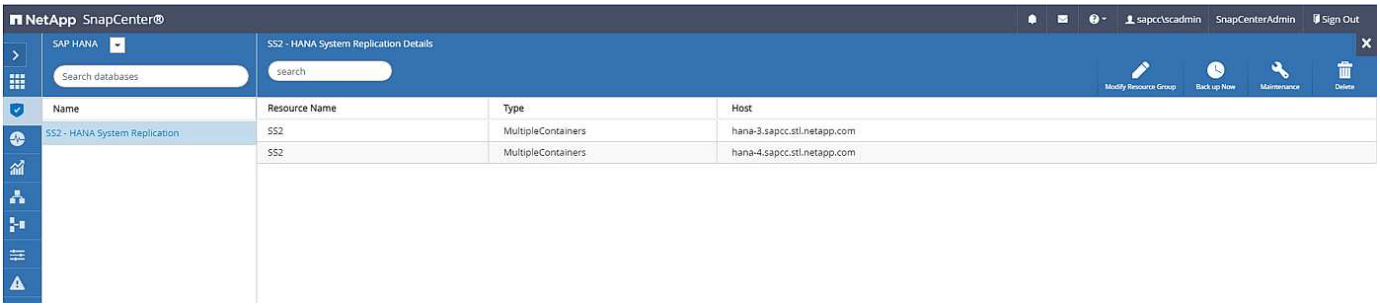


Die Richtlinien und Zeitpläne für die Ressourcengruppe werden konfiguriert.

Die in der Richtlinie definierte Aufbewahrung wird für beide HANA-Hosts verwendet. Wenn z. B. eine Aufbewahrung von 10 in der Richtlinie definiert ist, wird die Summe der Backups beider Hosts als Kriterien für das Löschen von Backups verwendet. SnapCenter löscht das älteste Backup unabhängig davon, wenn es auf dem aktuellen primären oder sekundären Host erstellt wurde.

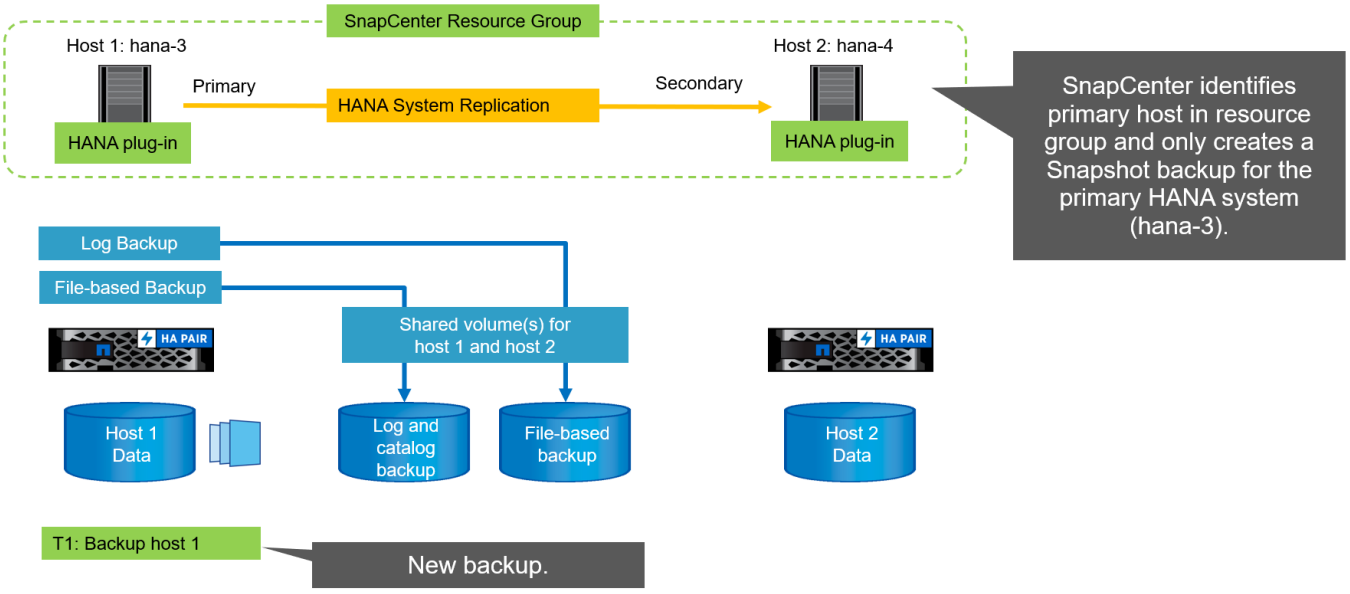


Die Konfiguration der Ressourcengruppe ist jetzt abgeschlossen und Backups können ausgeführt werden.

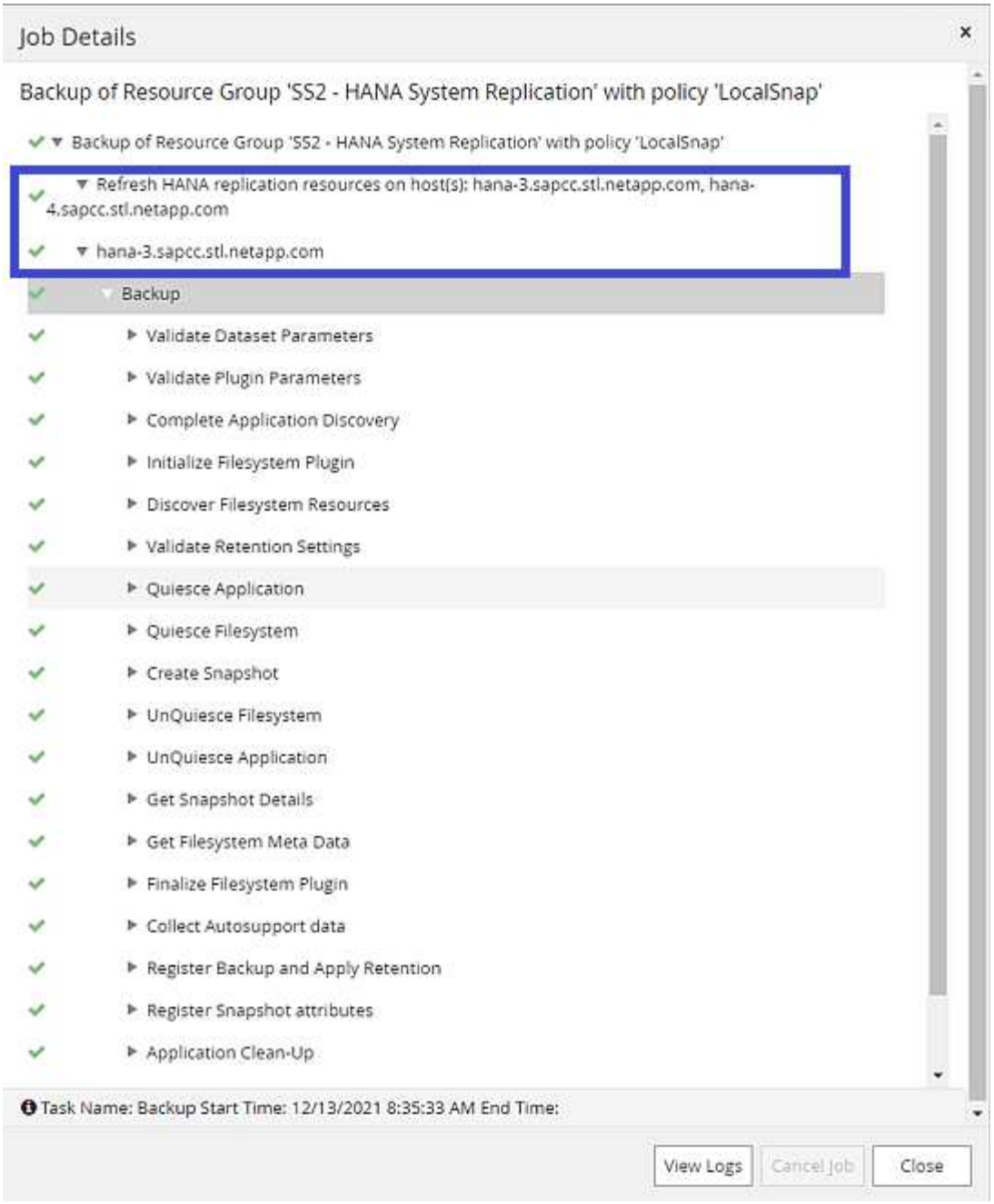


Snapshot-Backup-Vorgänge

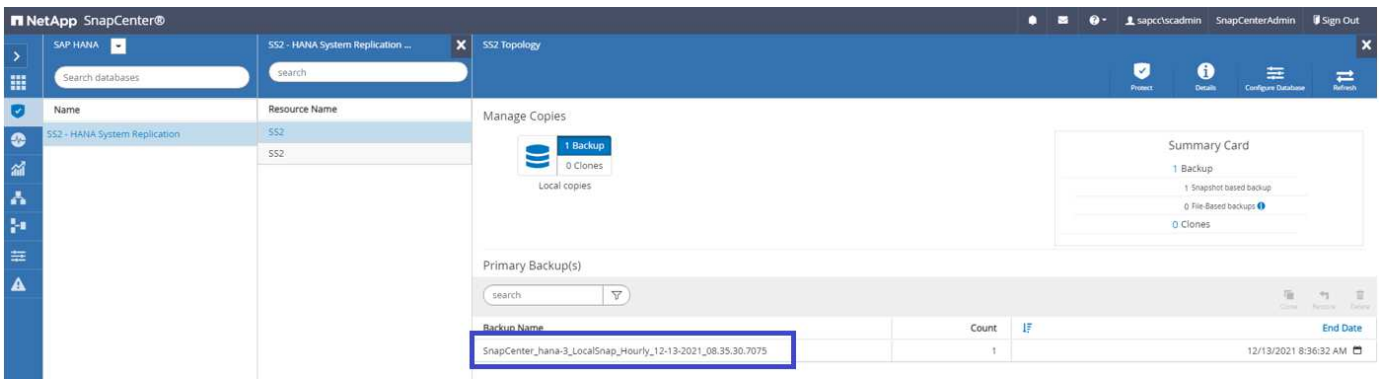
Wenn ein Backup-Vorgang der Ressourcengruppe ausgeführt wird, identifiziert SnapCenter den primären Host und löst nur ein Backup auf dem primären Host aus. Das bedeutet, dass nur das Daten-Volume des primären Hosts mit Snapshots erstellt werden wird. in unserem Beispiel ist hana-3 der aktuelle primäre Host und ein Backup wird auf diesem Host ausgeführt.



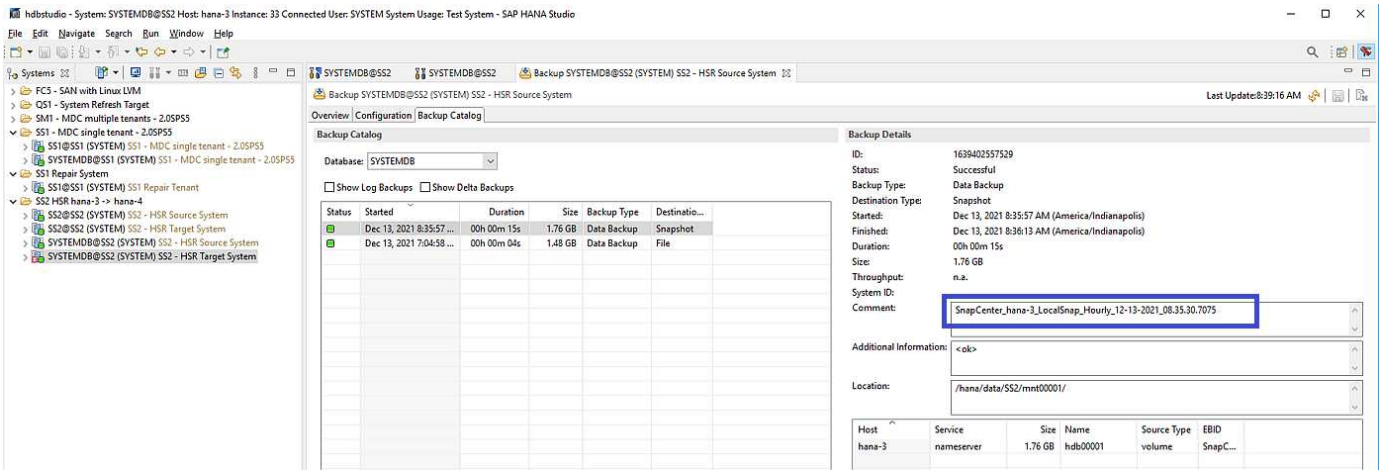
Das SnapCenter-Jobprotokoll zeigt den Identifizierungsvorgang und die Ausführung des Backups auf dem aktuellen primären Host hana-3.



Ein Snapshot-Backup wurde jetzt auf der primären HANA-Ressource erstellt. Der im Backup-Namen enthaltene Hostname zeigt hana-3.

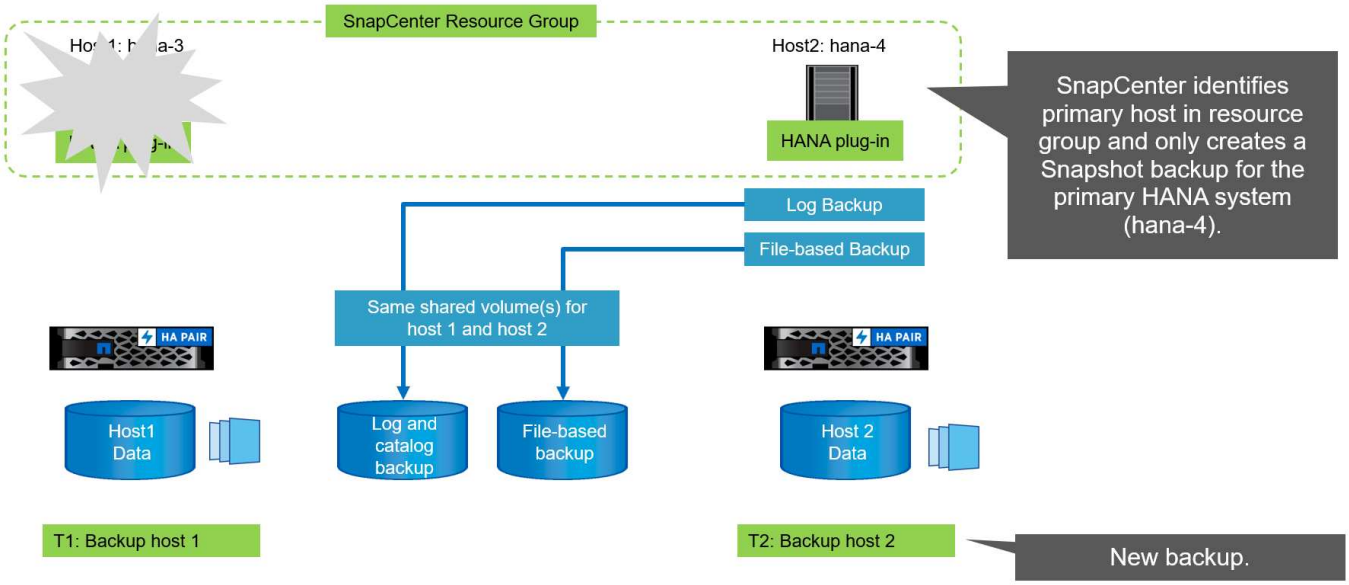


Das Snapshot-Backup ist auch im HANA-Backup-Katalog sichtbar.

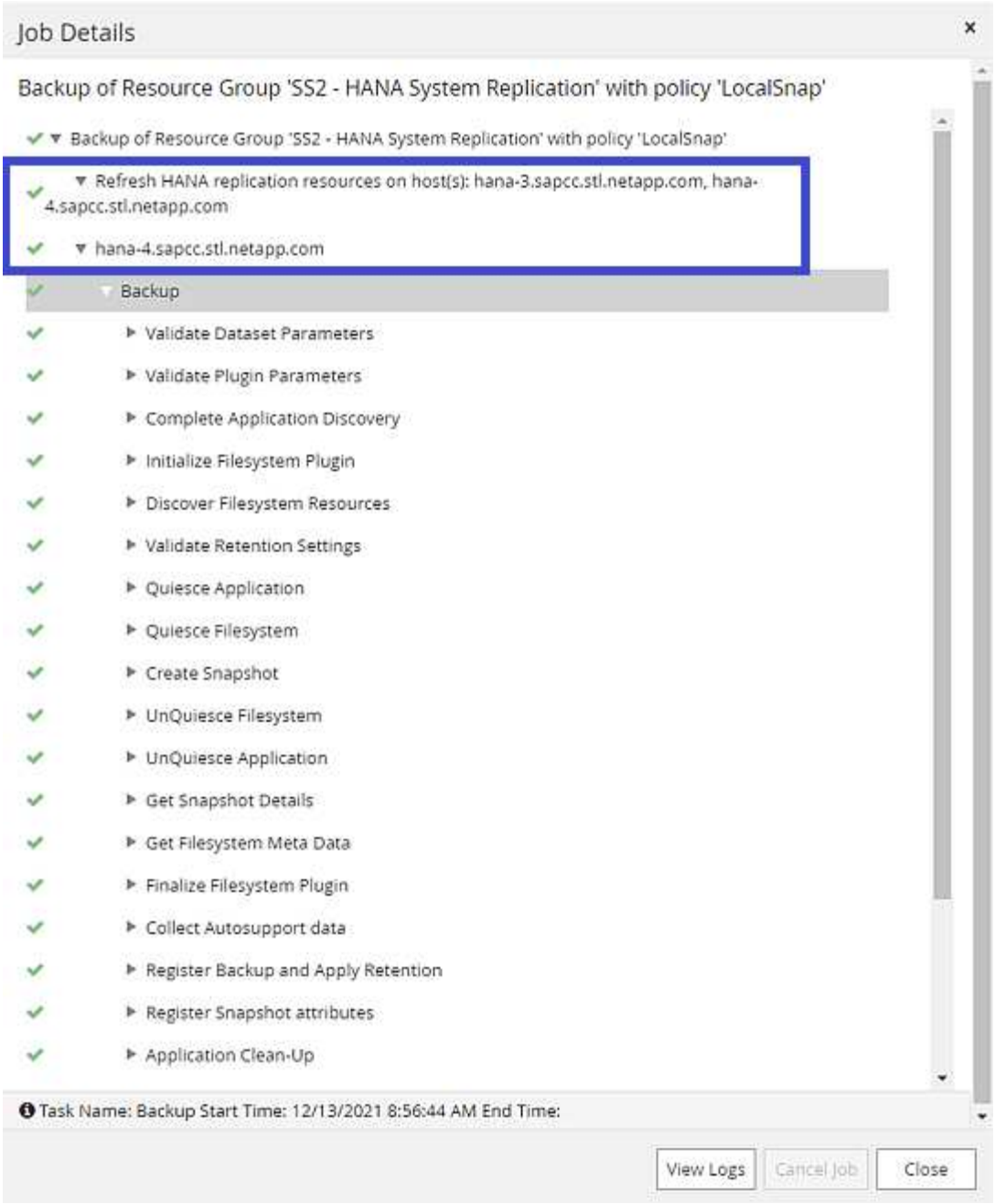


Falls ein Übernahmevorgang ausgeführt wird, identifizieren weitere SnapCenter Backups jetzt den früheren sekundären Host (hana-4) als primär und der Backup-Vorgang wird auf hana-4 ausgeführt. Erneut wird nur das Daten-Volume des neuen primären Hosts (hana-4) mit Snapshots erstellt.

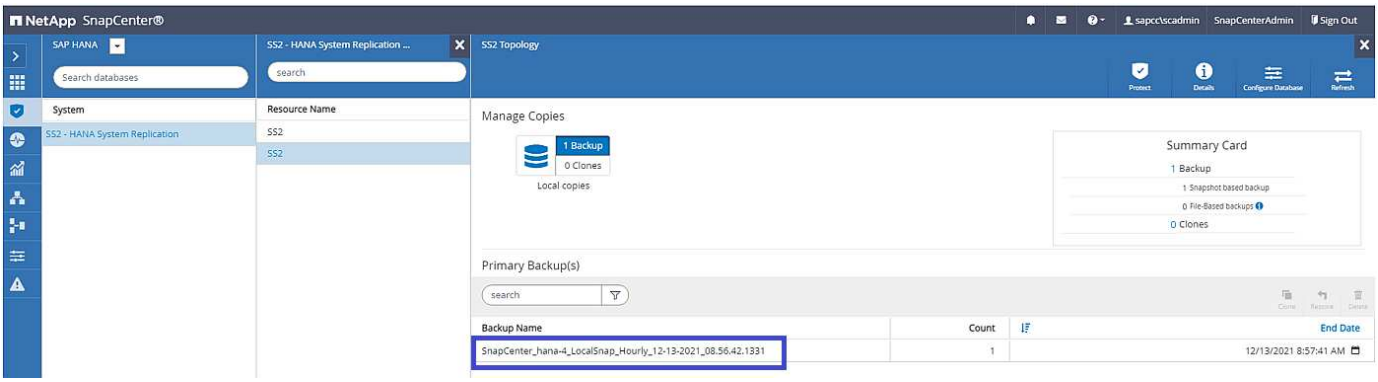
Die SnapCenter-Identifizierungslogik deckt nur Szenarien ab, in denen sich die HANA-Hosts in einer primären/sekundären Beziehung befinden oder wenn einer der HANA-Hosts offline ist.



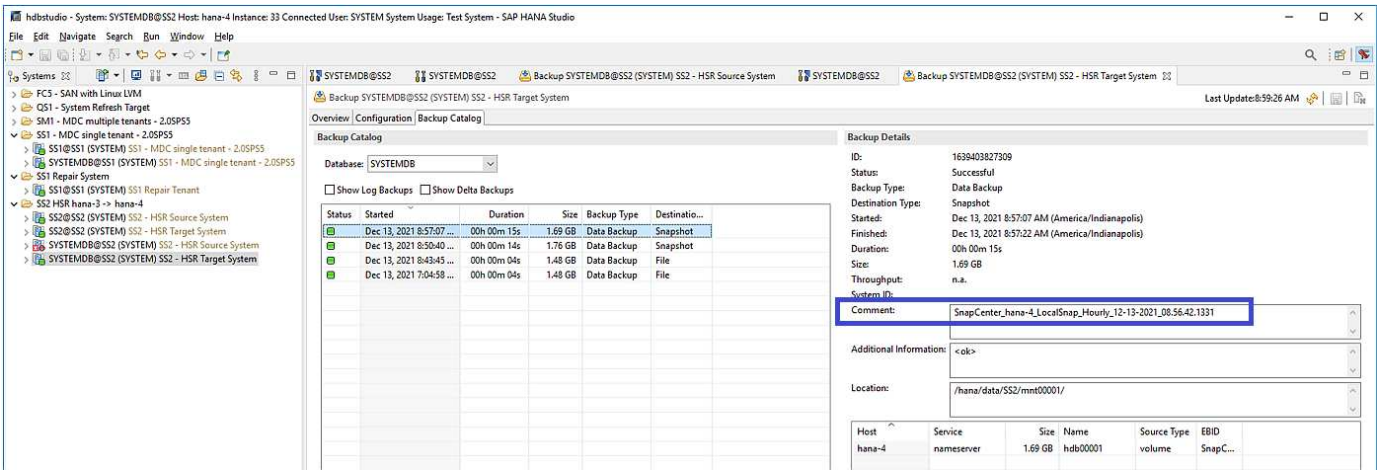
Das SnapCenter-Jobprotokoll zeigt den Identifizierungsvorgang und die Ausführung des Backups auf dem aktuellen primären Host hana-4.



Ein Snapshot-Backup wurde jetzt auf der primären HANA-Ressource erstellt. Der im Backup-Namen enthaltene Hostname zeigt hana-4.



Das Snapshot-Backup ist auch im HANA-Backup-Katalog sichtbar.



Block-Integritätsprüfung mit dateibasierten Backups

SnapCenter 4.6 verwendet dieselbe Logik wie für Snapshot Backup-Vorgänge bei dateibasierten Backups beschrieben zur Überprüfung der Blockintegrität. SnapCenter identifiziert den aktuellen primären HANA-Host und führt das dateibasierte Backup für diesen Host aus. Das Aufbewahrungsmanagement wird auch auf beiden Hosts durchgeführt, sodass das älteste Backup unabhängig davon, welcher Host sich derzeit im primären System befindet, gelöscht wird.

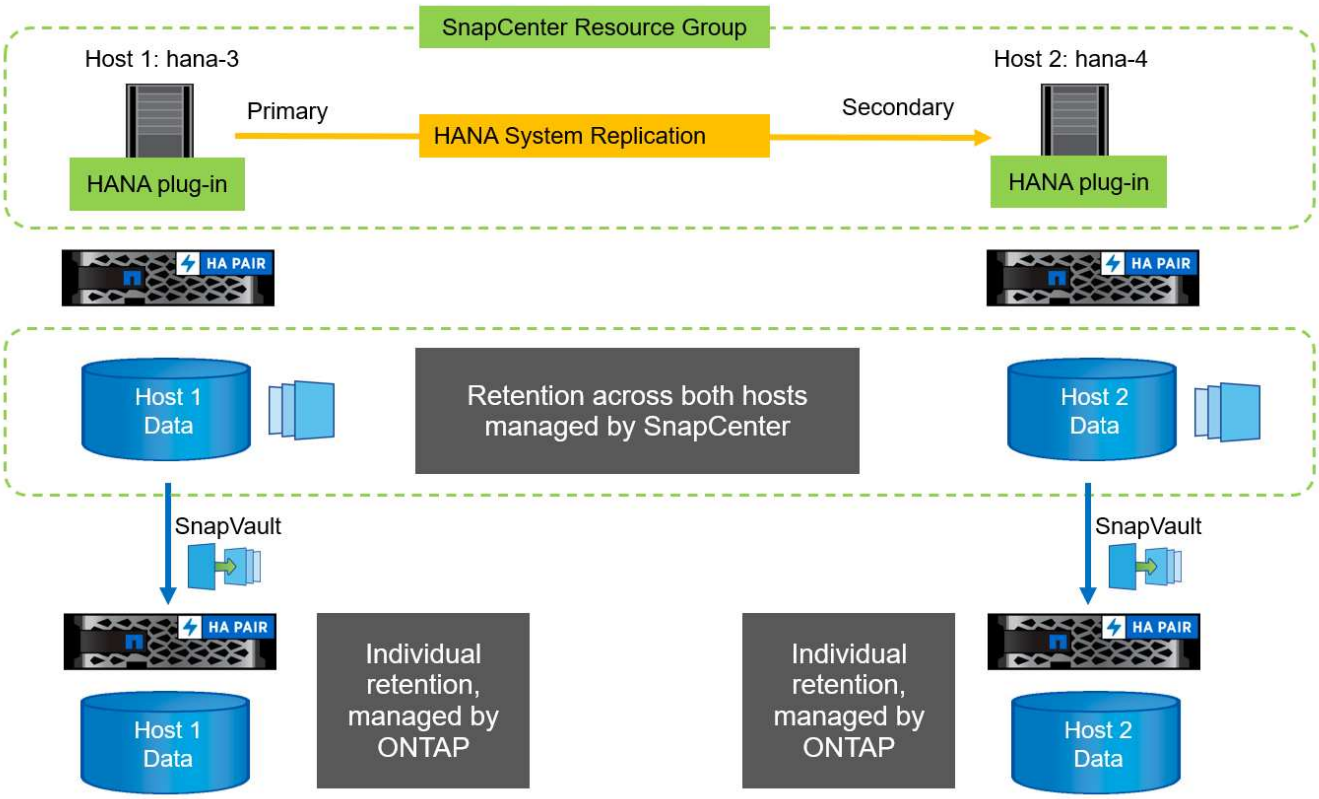
SnapVault Replizierung

Damit transparente Backup-Vorgänge ohne manuelle Interaktion möglich sind, muss im Falle einer Übernahme und unabhängig davon, dass der HANA-Host derzeit der primäre Host ist, eine SnapVault-Beziehung für die Daten-Volumes beider Hosts konfiguriert werden. SnapCenter führt bei jedem Backup-Durchlauf einen SnapVault Update-Vorgang für den aktuellen primären Host durch.

> Wenn ein Takeover an den sekundären Host nicht für lange Zeit ausgeführt wird, ist die Anzahl der geänderten Blöcke für das erste SnapVault Update am sekundären Host hoch.

Da die Retention Management am SnapVault-Ziel außerhalb von SnapCenter durch ONTAP verwaltet wird, kann die Aufbewahrung nicht über beide HANA-Hosts abgewickelt werden. Daher werden Backups, die vor einem Takeover erstellt wurden, nicht mit Backup-Vorgängen auf dem ehemaligen Sekundärstandort gelöscht. Diese Backups bleiben so lange erhalten, bis der frühere primäre wieder auf den primären Speicher zurückgeht. Damit diese Backups das Aufbewahrungsmanagement von Log-Backups nicht blockieren, müssen sie entweder am SnapVault-Ziel oder im HANA-Backup-Katalog manuell gelöscht werden.

> Eine Bereinigung aller SnapVault Snapshot-Kopien ist nicht möglich, da eine Snapshot-Kopie als Synchronisierungspunkt gesperrt wird. Wenn auch die neueste Snapshot Kopie gelöscht werden muss, muss die SnapVault Replizierungsbeziehung gelöscht werden. In diesem Fall empfiehlt NetApp, die Backups im HANA-Backup-Katalog zu löschen, um das Backup-Aufbewahrungsmanagement für das Protokoll abzulösen.



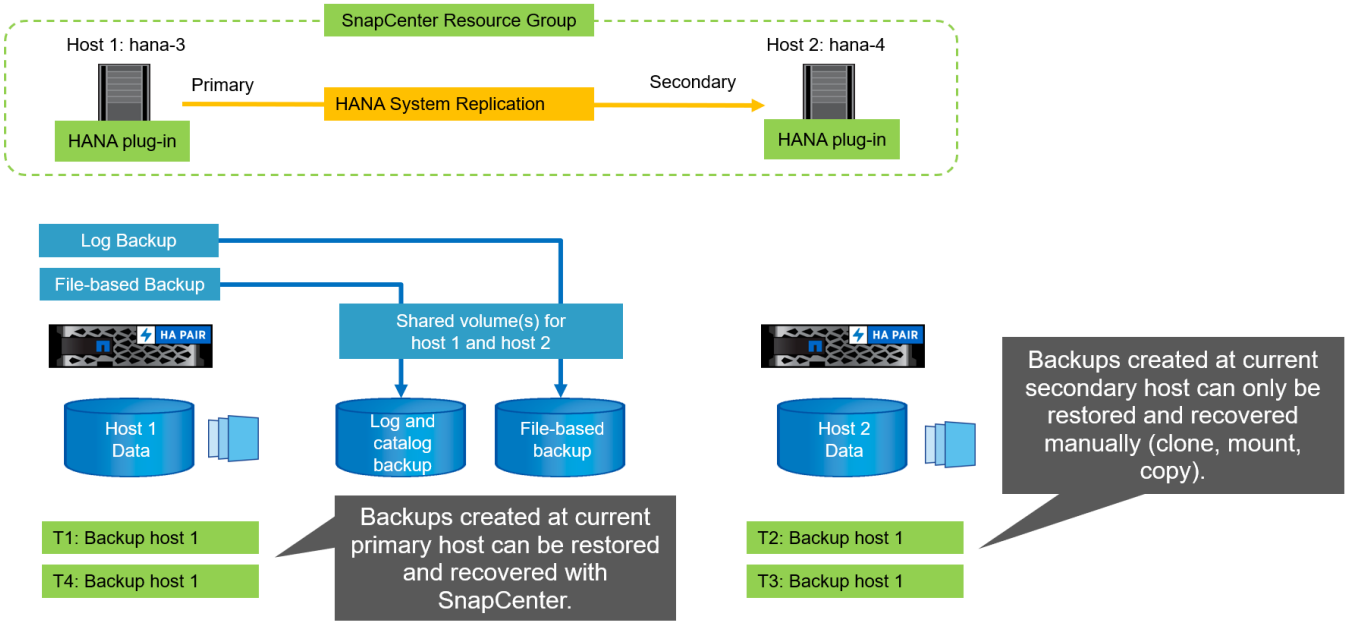
Retentionmanagement

SnapCenter 4.6 verwaltet Aufbewahrung für Snapshot-Backups, Block-Integrität-Check Operationen, HANA Backup-Katalog Einträge, und Log-Backups (wenn nicht deaktiviert) über beide HANA-Hosts, so ist es egal, welcher Host derzeit primär oder sekundär ist. Backups (Daten und Protokoll) und Einträge im HANA-Katalog werden basierend auf der definierten Aufbewahrung gelöscht, unabhängig davon, ob ein Löschvorgang auf dem aktuellen primären oder sekundären Host erforderlich ist. Das bedeutet, dass keine manuelle Interaktion erforderlich ist, wenn ein Übernahmemodus durchgeführt wird und/oder die Replizierung in andere Richtung konfiguriert wird.

Wenn die SnapVault-Replizierung Teil der Datensicherungsstrategie ist, ist für bestimmte Szenarien eine manuelle Interaktion erforderlich, wie in Abschnitt beschrieben "SnapVault-Replizierung"

Restore und Recovery

Die folgende Abbildung zeigt ein Szenario, in dem mehrere Übernahmen ausgeführt und Snapshot Backups an beiden Standorten erstellt wurden. Mit dem aktuellen Status ist der Host hana-3 der primäre Host und das neueste Backup T4, das auf Host hana-3 erstellt wurde. Wenn Sie einen Restore- und Recovery-Vorgang durchführen müssen, sind die Backups T1 und T4 für die Wiederherstellung im SnapCenter verfügbar. Die Backups, die auf dem Host hana-4 (T2, T3) erstellt wurden, können mit SnapCenter nicht wiederhergestellt werden. Diese Backups müssen zur Wiederherstellung manuell auf das Datenvolumen von hana-3 kopiert werden.



Die Wiederherstellungs- und Recovery-Vorgänge für eine SnapCenter 4.6-Ressourcengruppe sind identisch mit einer automatisch erkannten Konfiguration, die nicht vom System stammt. Alle Optionen für Restores und automatisiertes Recovery sind verfügbar. Weitere Einzelheiten finden Sie im technischen Bericht "TR-4614: SAP HANA Backup and Recovery with SnapCenter".

Ein Wiederherstellungsvorgang aus einem Backup, das auf dem anderen Host erstellt wurde, wird im Abschnitt beschrieben"Wiederherstellung aus einem Backup, das auf dem anderen Host erstellt wurde".

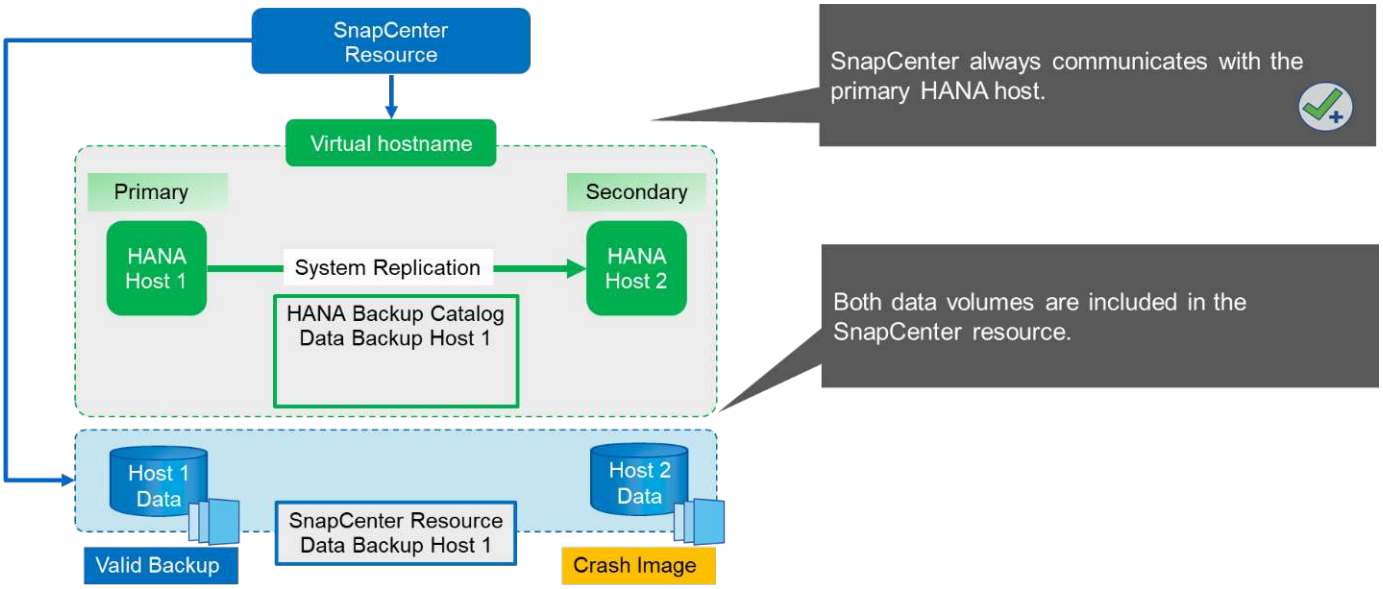
SnapCenter Konfiguration mit einer einzigen Ressource

Eine SnapCenter-Ressource wird mit der virtuellen IP-Adresse (Hostname) der HANA System Replication-Umgebung konfiguriert. Bei diesem Ansatz kommuniziert SnapCenter immer mit dem primären Host, unabhängig davon, ob Host 1 oder Host 2 der primäre Host ist. Die Datenvolumen beider SAP HANA-Hosts sind in der SnapCenter Ressource enthalten.

Wir gehen davon aus, dass die virtuelle IP-Adresse immer an den primären SAP HANA-Host gebunden ist. Das Failover der virtuellen IP-Adresse erfolgt außerhalb von SnapCenter im Rahmen des Failover-Workflows zur HANA-Systemreplizierung.

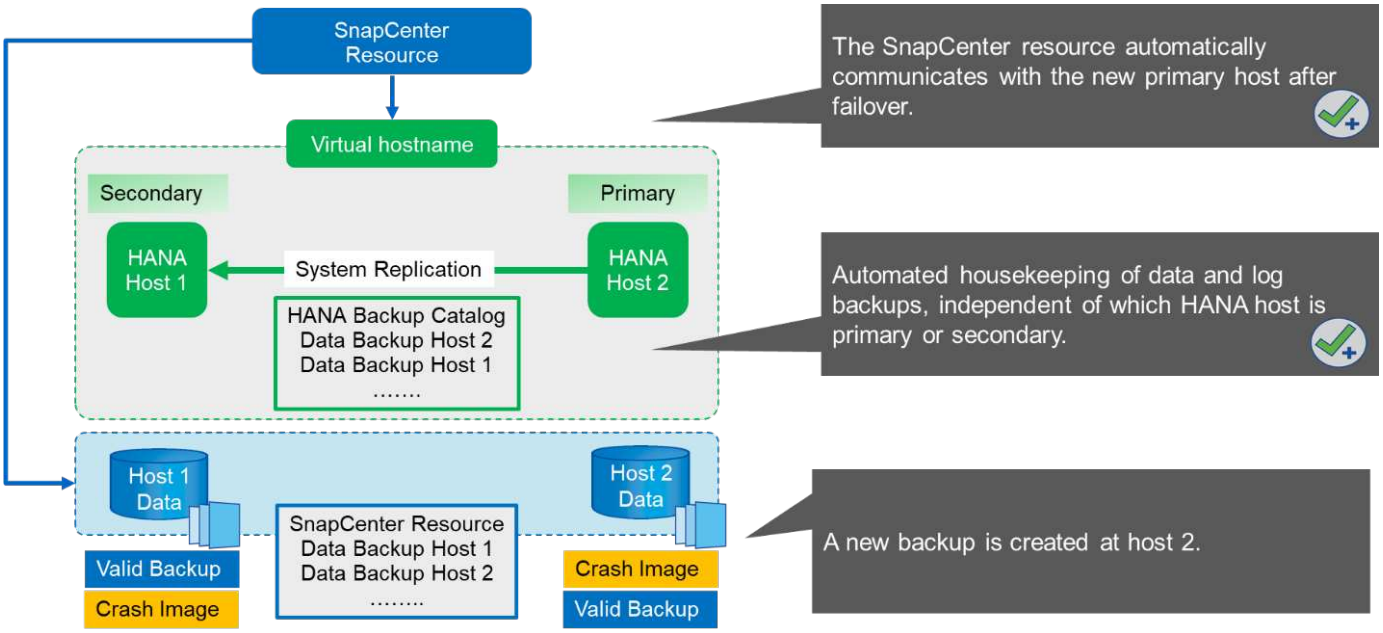
Wird ein Backup mit Host 1 als primärer Host ausgeführt, wird ein datenbankkonsistentes Snapshot-Backup auf dem Datenvolumen von Host 1 erstellt. Da das Daten-Volume des Hosts 2 Teil der SnapCenter Ressource ist, wird für dieses Volume eine weitere Snapshot Kopie erstellt. Diese Snapshot Kopie ist nicht datenbankkonsistent, sondern nur ein Crash-Image des sekundären Hosts.

Der SAP HANA Backup-Katalog und die SnapCenter-Ressource umfassen das auf Host 1 erstellte Backup.



Die folgende Abbildung zeigt den Backup-Vorgang nach dem Failover auf Host 2 und die Replizierung von Host 2 zu Host 1. SnapCenter kommuniziert automatisch mit Host 2, indem die in der SnapCenter-Ressource konfigurierte virtuelle IP-Adresse verwendet wird. Backups werden jetzt auf Host 2 erstellt. Von SnapCenter werden zwei Snapshot-Kopien erstellt: Ein datenbankkonsistentes Backup auf dem Daten-Volume bei Host 2 und eine Snapshot-Kopie des Crash-Images am Daten-Volume beim Host 1. Der SAP HANA-Backup-Katalog und die SnapCenter-Ressource enthalten nun das bei Host 1 erstellte Backup und das auf Host 2 erstellte Backup.

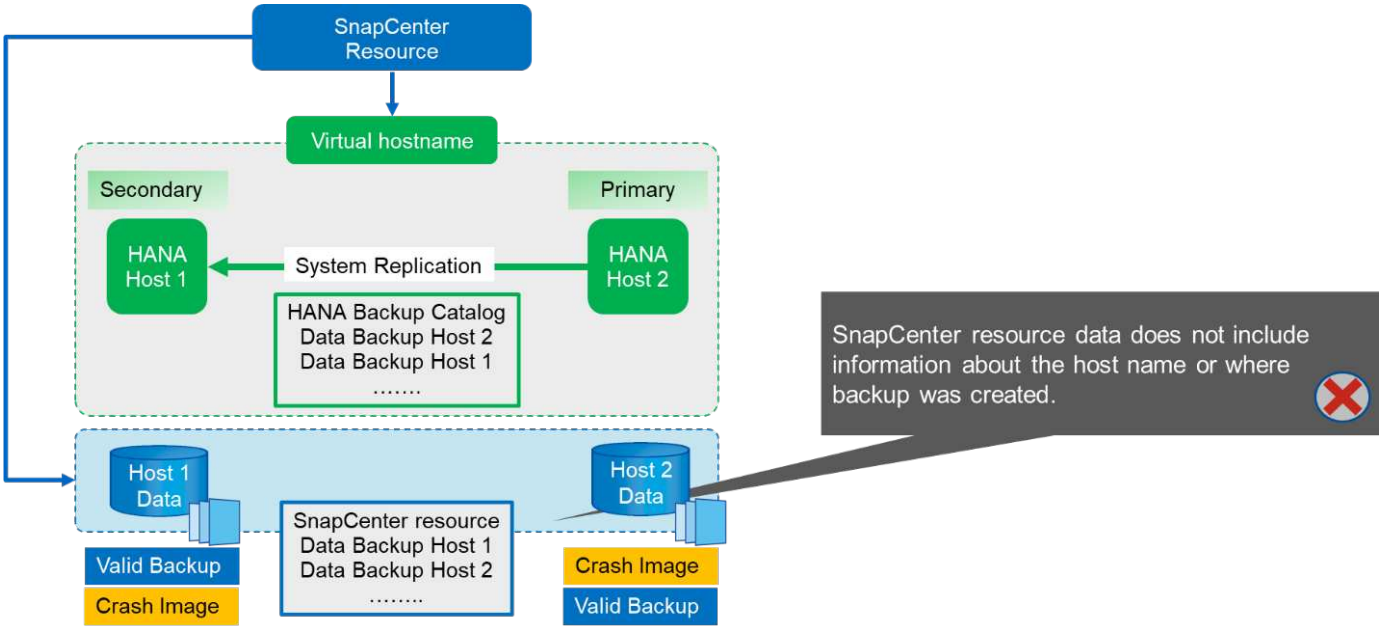
Die allgemeine Ordnung und Sauberkeit der Daten- und Log-Backups basiert auf der definierten SnapCenter-Aufbewahrungsrichtlinie und die Backups werden unabhängig vom primären oder sekundären Host gelöscht.



Wie im Abschnitt erläutert"Storage Snapshot Backups und SAP System Replication", unterscheidet sich ein Restore-Vorgang mit Storage-basierten Snapshot Backups, je nachdem, welches Backup wiederhergestellt werden muss. Es ist wichtig zu ermitteln, auf welchem Host das Backup erstellt wurde, um festzustellen, ob die Wiederherstellung auf dem lokalen Speichervolumen durchgeführt werden kann, oder ob die Wiederherstellung auf dem Speichervolumen des anderen Hosts durchgeführt werden muss.

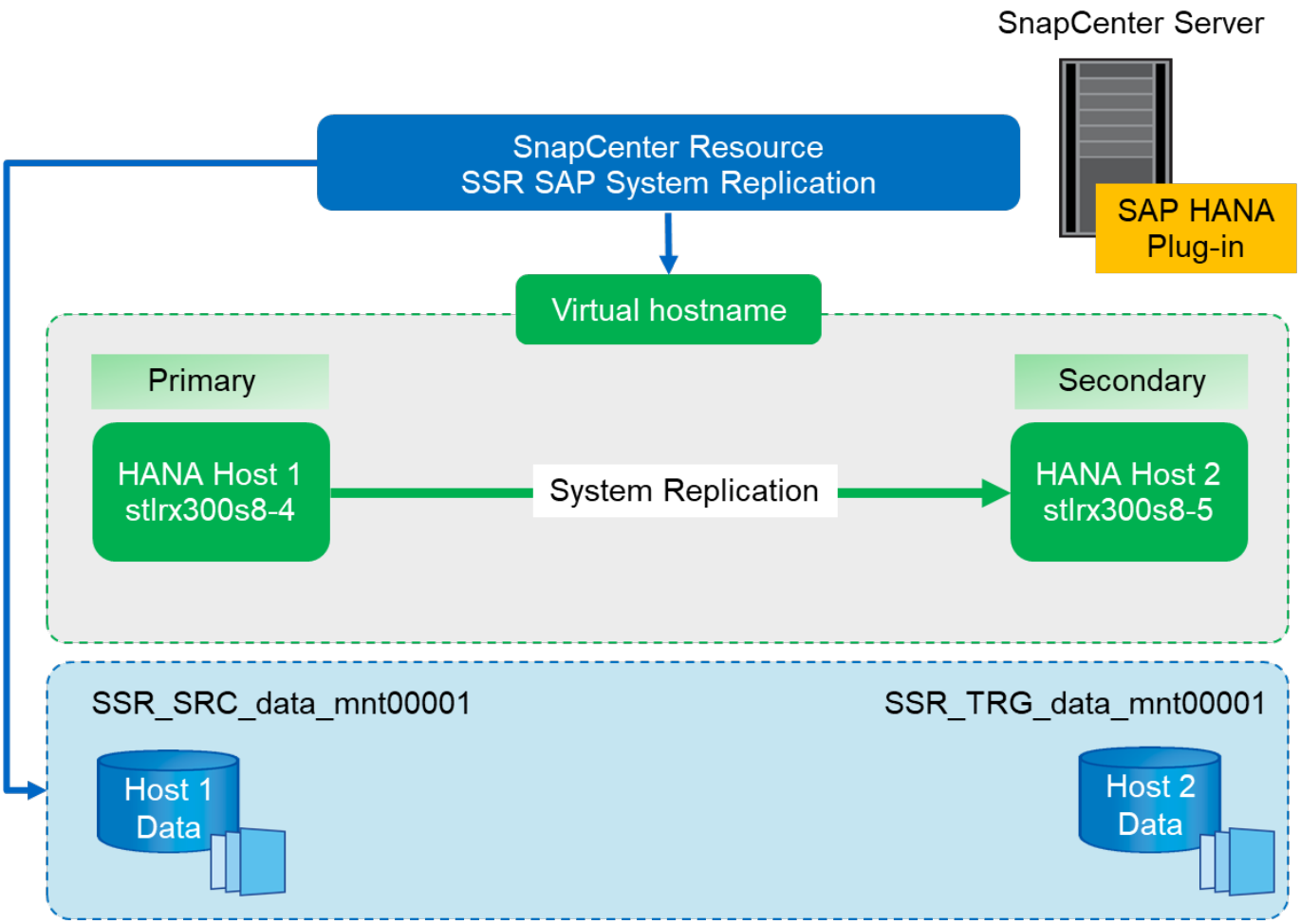
Bei einer SnapCenter-Konfiguration mit nur einem Mitarbeiter ist SnapCenter nicht bewusst, wo das Backup erstellt wurde. NetApp empfiehlt daher, dem SnapCenter Backup-Workflow ein Pre-Backup-Skript hinzuzufügen, um zu ermitteln, welcher Host derzeit der primäre SAP HANA-Host ist.

Die folgende Abbildung zeigt die Identifikation des Backup-Hosts.



SnapCenter-Konfiguration

Die folgende Abbildung zeigt das Lab-Setup und eine Übersicht über die erforderliche SnapCenter-Konfiguration.



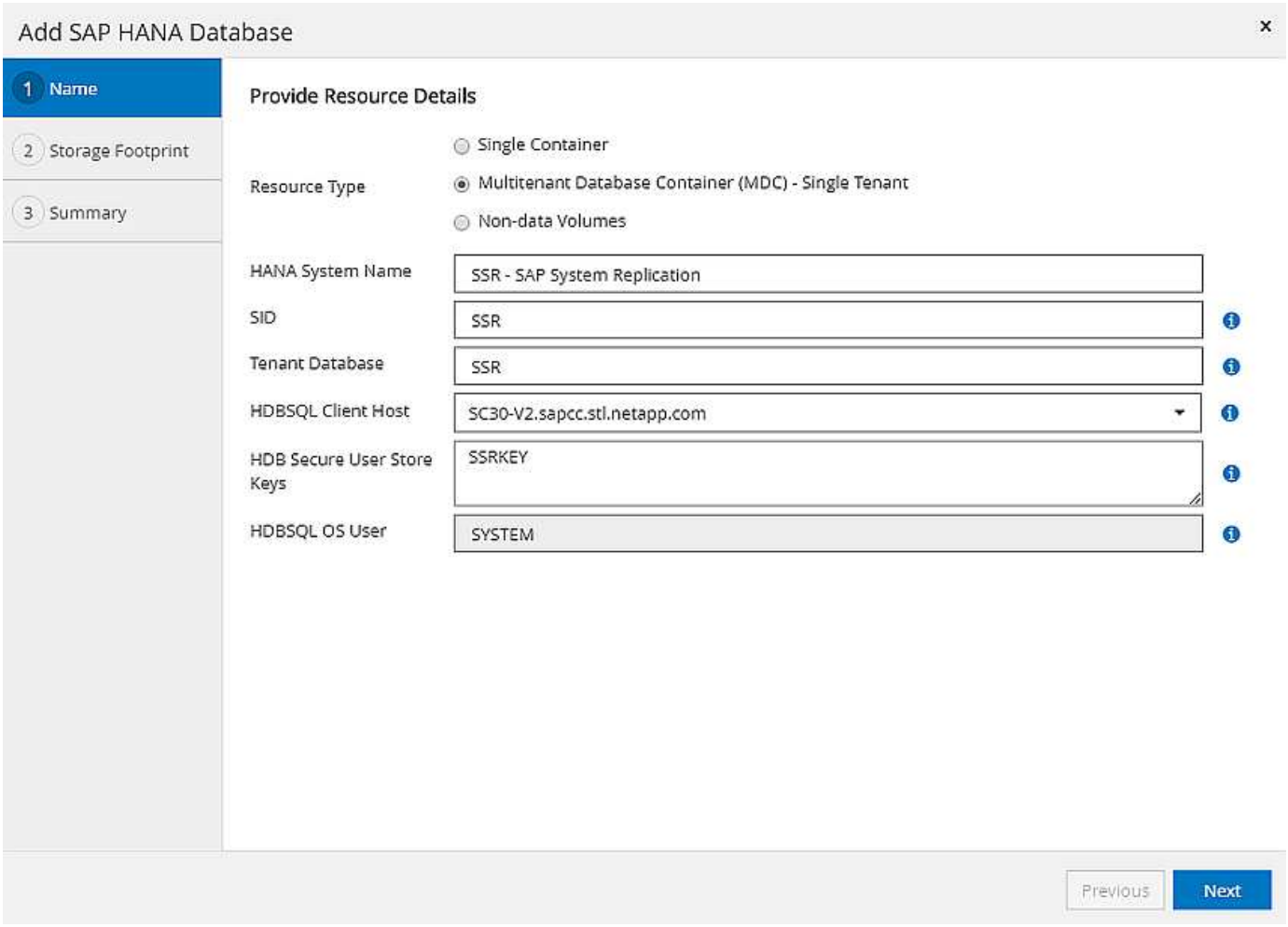
Um Backup-Vorgänge unabhängig davon durchzuführen, welcher SAP HANA Host primär ist und selbst wenn ein Host ausfällt, muss das SnapCenter SAP HANA Plug-in auf einem zentralen Plug-in-Host implementiert werden. In unserer Lab-Einrichtung wurde der SnapCenter Server als zentraler Plug-in-Host verwendet, und wir haben das SAP HANA Plug-in auf dem SnapCenter Server implementiert.

In der HANA-Datenbank wurde ein Benutzer erstellt, um Backup-Vorgänge durchzuführen. Auf dem SnapCenter-Server, auf dem das SAP HANA-Plug-in installiert wurde, wurde ein User-Store-Schlüssel konfiguriert. Der Benutzerspeicherschlüssel enthält die virtuelle IP-Adresse der SAP HANA System Replication Hosts (`ssr-vip`).

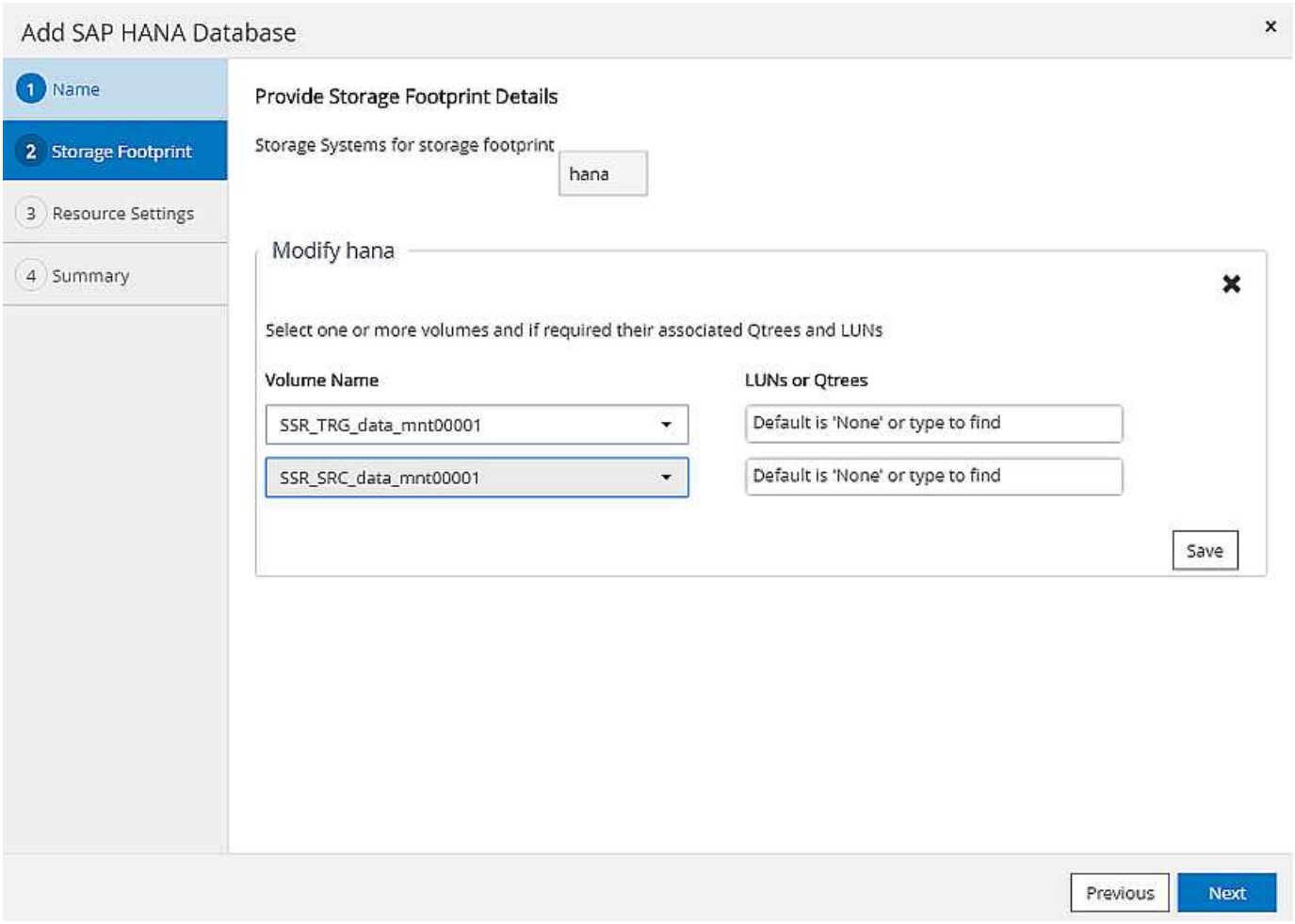
```
hdbuserstore.exe -u SYSTEM set SSRKEY ssr-vip:31013 SNAPCENTER <password>
```

Weitere Informationen zu den Bereitstellungsoptionen des SAP HANA-Plug-ins und zur Konfiguration des Benutzerspeichers finden Sie im technischen Bericht TR-4614: "Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter".

In SnapCenter wird die Ressource wie in der folgenden Abbildung dargestellt mit dem Benutzer-Speicherschlüssel konfiguriert, vorher konfiguriert, und dem SnapCenter-Server als der konfiguriert `hdbsql` Kommunikations-Host.

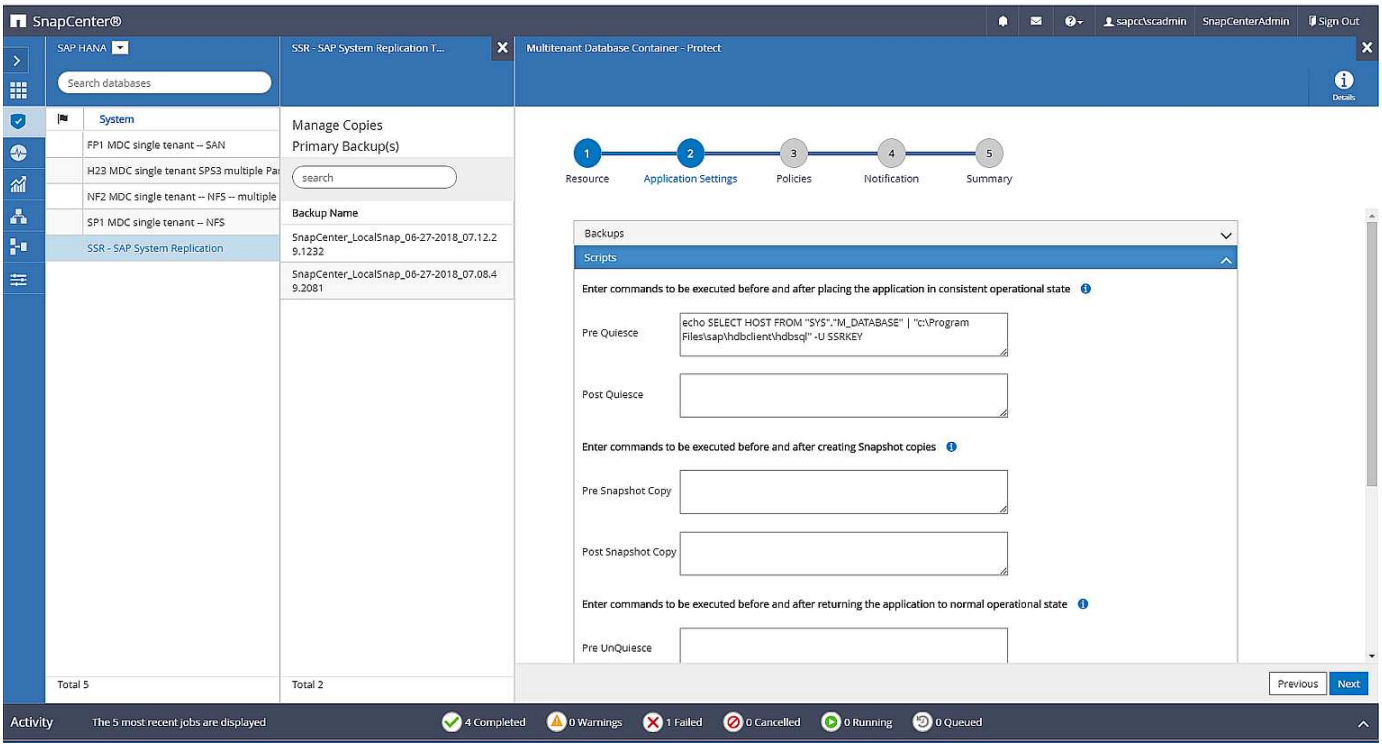


Die Datenvolumen der beiden SAP HANA-Hosts sind in der Storage-Platzbedarf-Konfiguration enthalten, wie die folgende Abbildung zeigt.



Wie zuvor bereits besprochen, ist bei SnapCenter nicht bekannt, wo das Backup erstellt wurde. NetApp empfiehlt daher, ein Skript vor dem Backup im SnapCenter Backup Workflow hinzuzufügen, um zu ermitteln, welcher Host derzeit der primäre SAP HANA Host ist. Sie können diese Identifizierung mithilfe einer SQL-Anweisung durchführen, die dem Backup-Workflow hinzugefügt wird, wie die folgende Abbildung zeigt.

```
Select host from "SYS".M_DATABASE
```

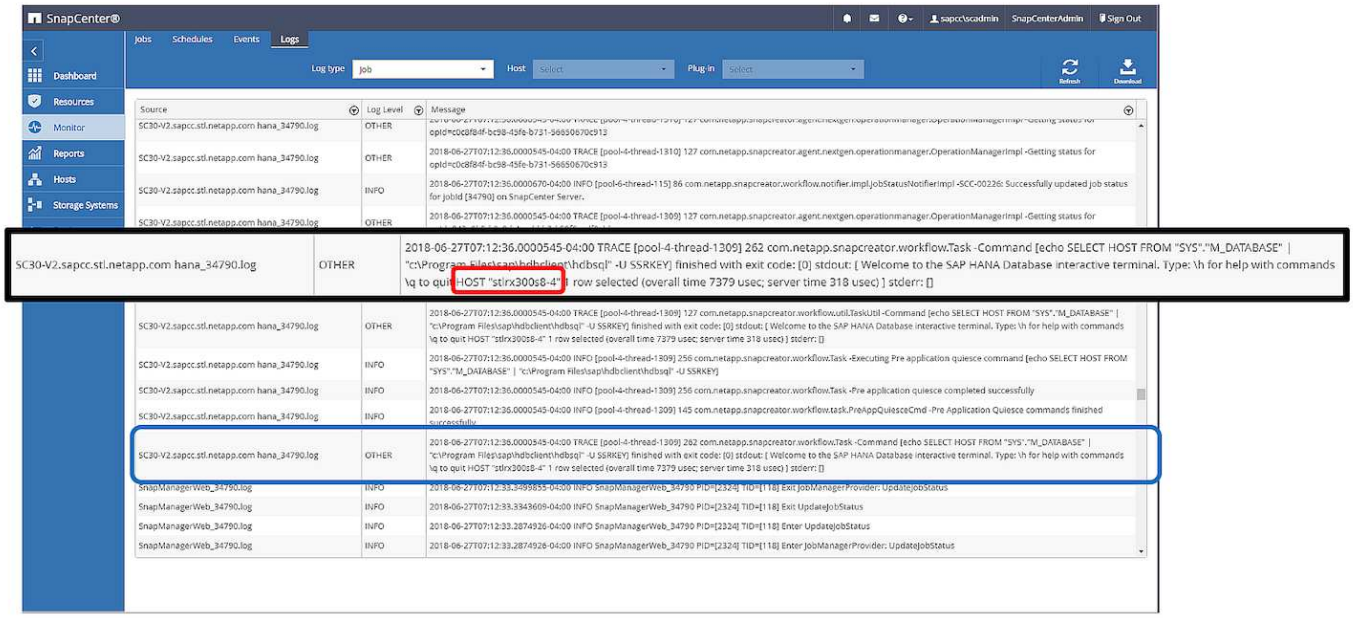


SnapCenter Backup-Vorgang

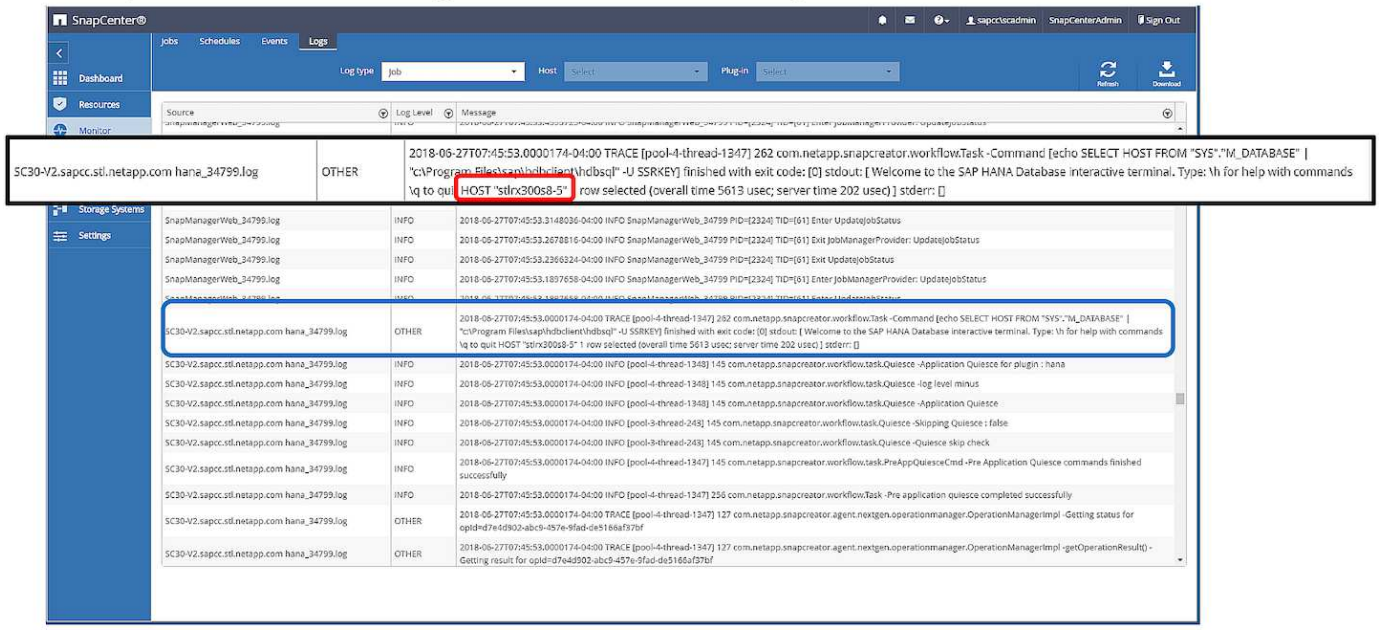
Backup-Vorgänge werden jetzt wie gewohnt ausgeführt. Die allgemeine Ordnung und Sauberkeit der Daten und Log-Backups wird unabhängig davon durchgeführt, welcher SAP HANA-Host primärer oder sekundärer ist.

Die Backup-Jobprotokolle enthalten die Ausgabe der SQL-Anweisung, mit der Sie den SAP HANA-Host identifizieren können, auf dem das Backup erstellt wurde.

Die folgende Abbildung zeigt das Backup-Jobprotokoll mit Host 1 als primärer Host.

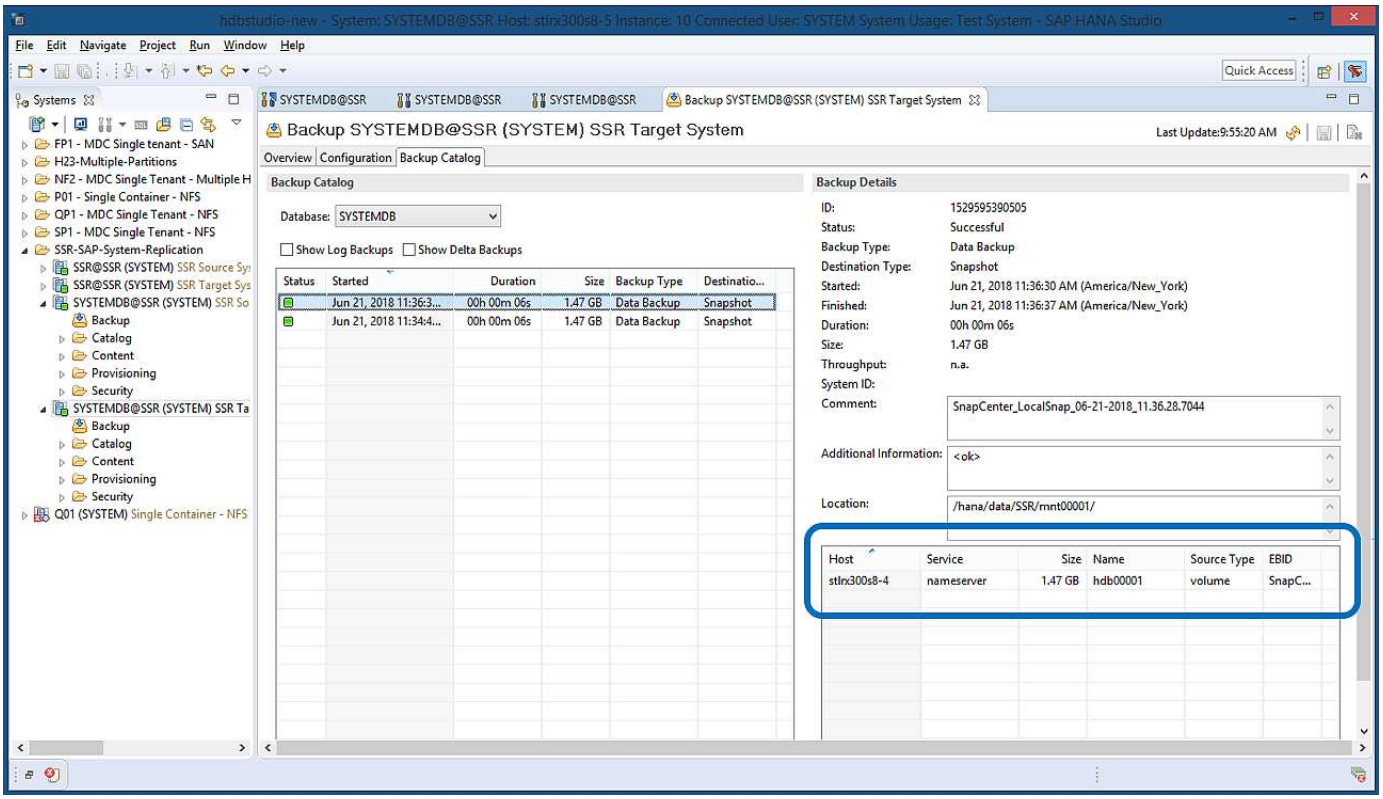


Diese Abbildung zeigt das Backup-Jobprotokoll mit Host 2 als primärer Host.



Die folgende Abbildung zeigt den SAP HANA Backup-Katalog in SAP HANA Studio. Ist die SAP HANA-Datenbank online, ist der SAP HANA-Host, auf dem das Backup erstellt wurde, im SAP HANA Studio sichtbar.

Der SAP HANA-Backup-Katalog auf dem Filesystem, der während eines Restore- und Recovery-Vorgangs verwendet wird, enthält nicht den Host-Namen, in dem das Backup erstellt wurde. Der einzige Weg, um den Host zu identifizieren, wenn die Datenbank ausfällt, ist die Kombination der Backup-Katalog-Einträge mit dem `backup.log` Datei beider SAP HANA-Hosts.



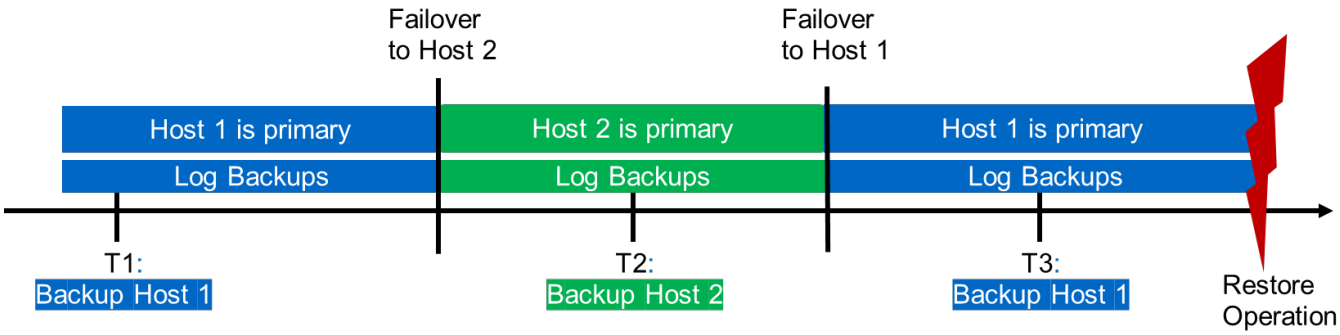
Restore und Recovery

Wie bereits besprochen, müssen Sie feststellen können, wo das ausgewählte Backup erstellt wurde, um den erforderlichen Wiederherstellungsvorgang zu definieren. Wenn die SAP HANA Datenbank noch online ist, kann mit SAP HANA Studio der Host identifiziert werden, auf dem das Backup erstellt wurde. Wenn die Datenbank offline ist, sind die Informationen nur im SnapCenter-Backup-Jobprotokoll verfügbar.

Die folgende Abbildung zeigt die verschiedenen Wiederherstellungsvorgänge je nach ausgewähltem Backup.

Wenn ein Wiederherstellungsvorgang nach dem Zeitstempel T3 ausgeführt werden muss und Host 1 der primäre ist, können Sie das bei T1 oder T3 erstellte Backup mithilfe von SnapCenter wiederherstellen. Diese Snapshot-Backups sind auf dem an Host 1 angebundenen Storage Volume verfügbar.

Wenn Sie mithilfe des Backup wiederherstellen müssen, der am Host 2 (T2) erstellt wurde, eine Snapshot-Kopie im Storage Volume von Host 2 ist, muss der Backup für den Host 1 zur Verfügung gestellt werden. Sie können dieses Backup zur Verfügung stellen, indem Sie eine NetApp FlexClone Kopie aus dem Backup erstellen, die FlexClone Kopie in Host 1 mounten und die Daten am ursprünglichen Speicherort kopieren.



Restore Operation With	
Backup T1	SnapCenter
Backup T2	Create FlexClone from „Backup host 2“, mount and copy
Backup T3	SnapCenter

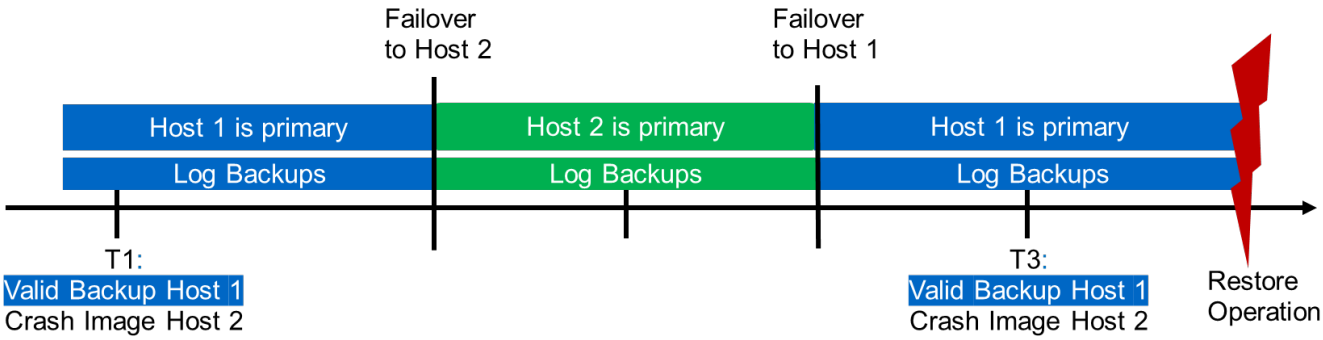
Mit einer einzelnen SnapCenter Ressourcenkonfiguration werden Snapshot Kopien auf beiden Storage-Volumes sowohl von SAP HANA System Replication Hosts erstellt. Nur das Snapshot-Backup, das auf dem Storage-Volume des primären SAP HANA-Hosts erstellt wird, ist für die zukünftige Recovery gültig. Die auf dem Storage Volume des sekundären SAP HANA-Hosts erstellte Snapshot Kopie ist ein Crash-Image, das nicht für die zukünftige Recovery verwendet werden kann.

Eine Wiederherstellung mit SnapCenter kann auf zwei verschiedene Arten durchgeführt werden:

- Stellen Sie nur das gültige Backup wieder her
- Stellen Sie die komplette Ressource einschließlich des gültigen Backups und des Crash-imageIn den folgenden Abschnitten werden die beiden verschiedenen Wiederherstellungsvorgänge näher erläutert.

Ein Wiederherstellungsvorgang aus einem Backup, das auf dem anderen Host erstellt wurde, wird im Abschnitt beschrieben"Wiederherstellung aus einem Backup, das auf dem anderen Host erstellt wurde".

Die folgende Abbildung zeigt die Wiederherstellungen mit einer einzelnen SnapCenter Ressourcenkonfiguration.

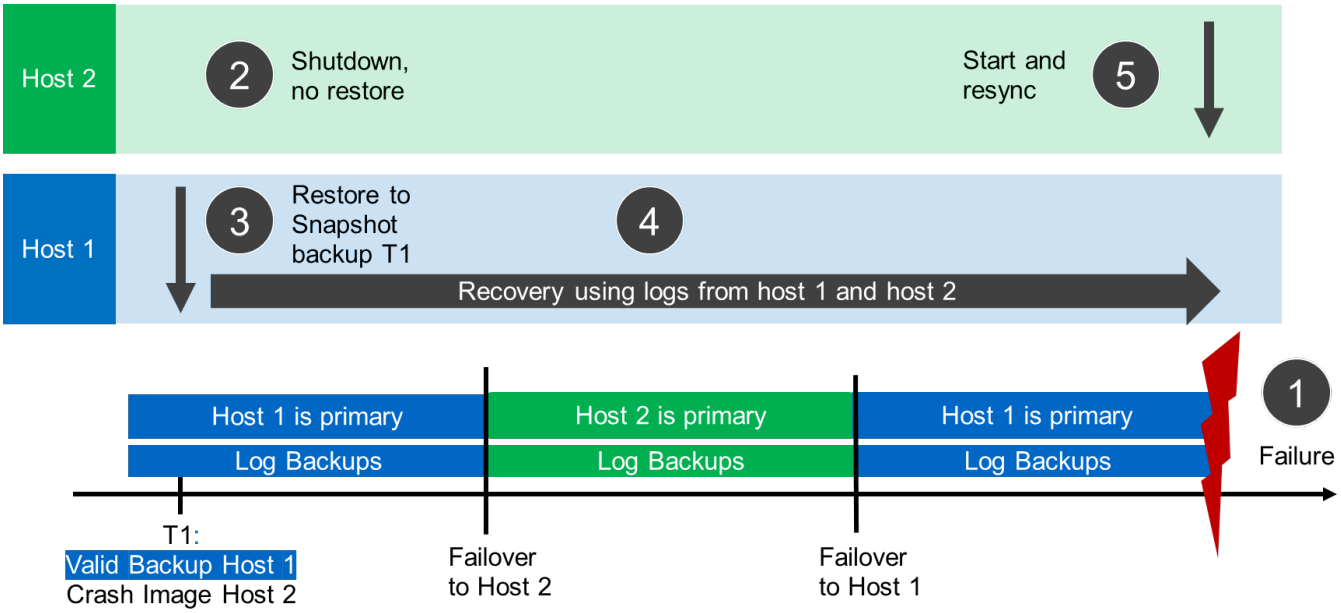


SnapCenter Restore nur für gültige Backups

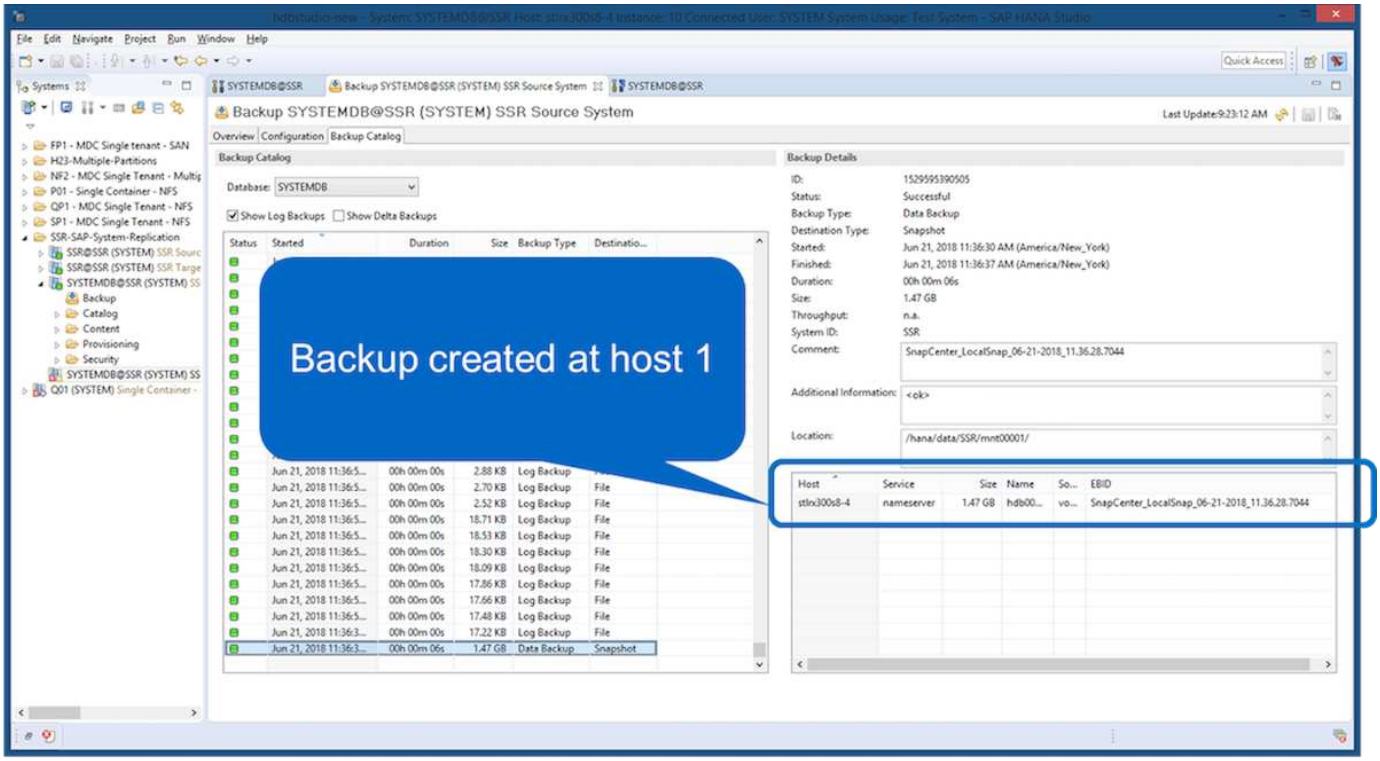
Die folgende Abbildung zeigt einen Überblick über das in diesem Abschnitt beschriebene Wiederherstellungsszenario.

Bei T1 am Host 1 wurde ein Backup erstellt. Ein Failover wurde an Host 2 durchgeführt. Nach einem bestimmten Zeitpunkt wurde ein weiteres Failover zurück zu Host 1 durchgeführt. Zum aktuellen Zeitpunkt ist Host 1 der primäre Host.

1. Es ist ein Fehler aufgetreten, und Sie müssen das am T1 erstellte Backup am Host 1 wiederherstellen.
2. Der sekundäre Host (Host 2) wird heruntergefahren, aber es wird kein Wiederherstellungsvorgang ausgeführt.
3. Das Speichervolumen von Host 1 wird auf dem bei T1 erstellten Backup wiederhergestellt.
4. Eine vorwärts gerichteten Wiederherstellung wird mit Protokollen von Host 1 und Host 2 durchgeführt.
5. Host 2 wird gestartet, und die Neusynchronisierung der Systemreplizierung von Host 2 wird automatisch gestartet.



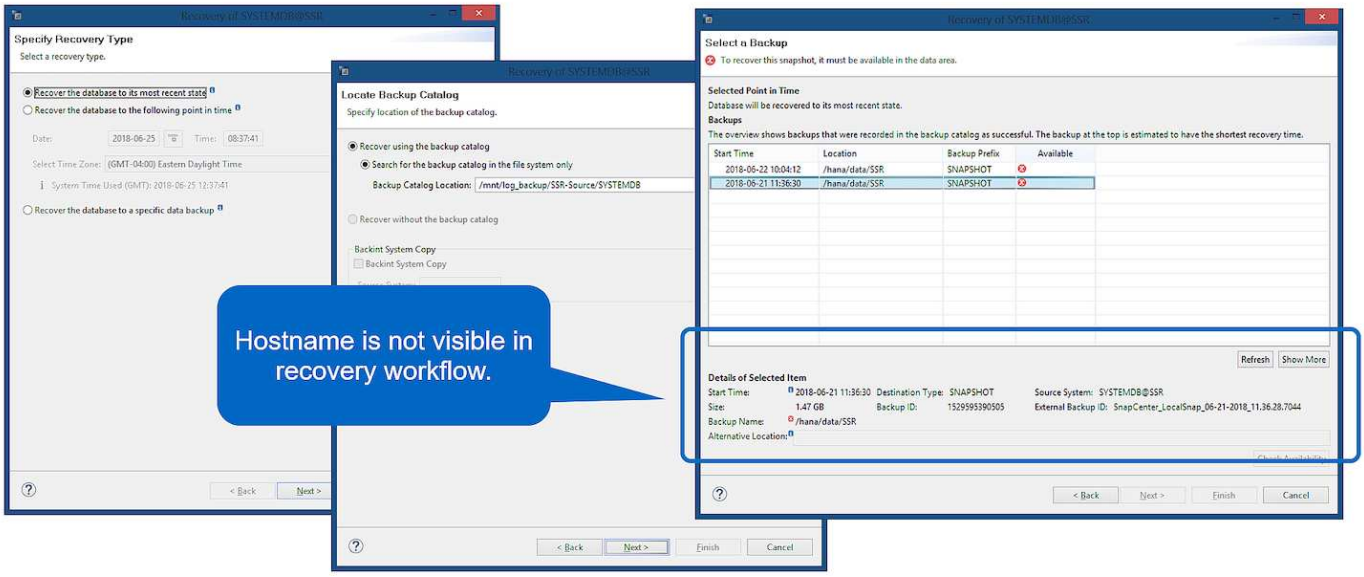
Die folgende Abbildung zeigt den SAP HANA Backup-Katalog in SAP HANA Studio. Die hervorgehobene Sicherung zeigt die Sicherung, die am T1 bei Host 1 erstellt wurde.



25

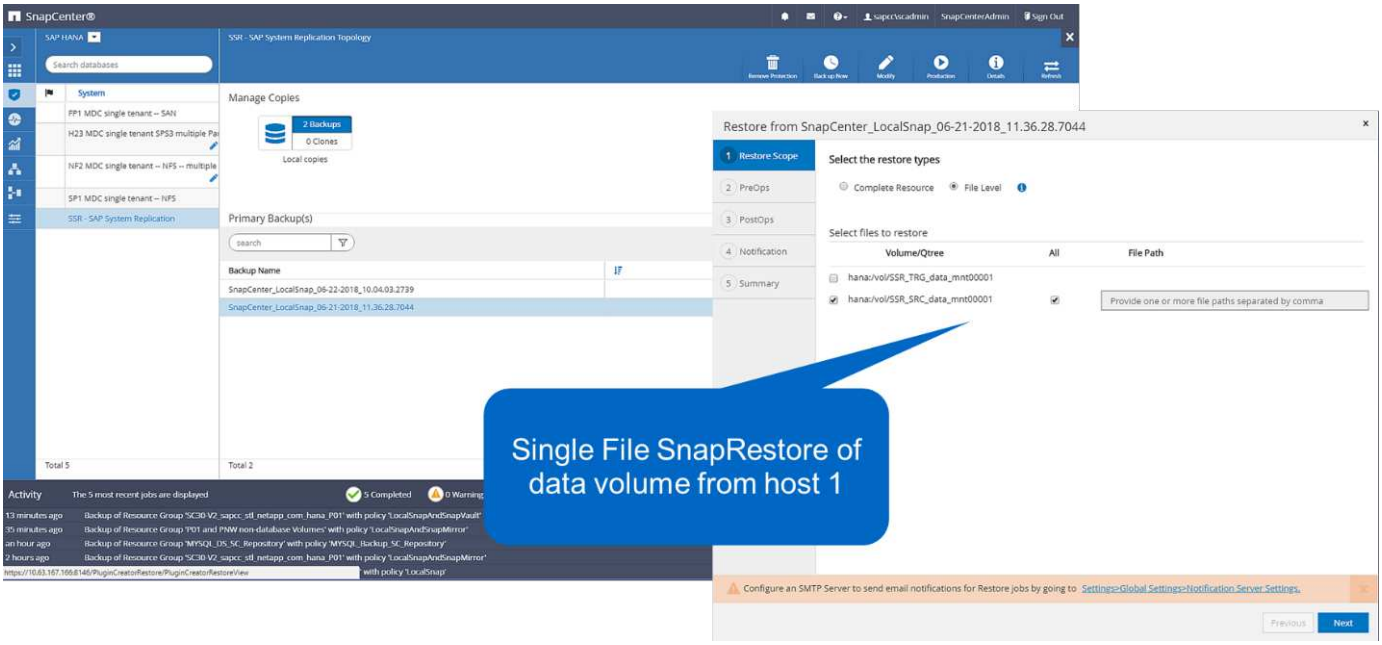
Im SAP HANA Studio wird eine Wiederherstellung gestartet. Wie die folgende Abbildung zeigt, ist der Name des Hosts, auf dem das Backup erstellt wurde, im Wiederherstellungsworkflow nicht sichtbar.

In unserem Testszenario waren wir in der Lage, das richtige Backup (das Backup beim Host 1 erstellt wurde) in SAP HANA Studio zu identifizieren, als die Datenbank noch online war. Wenn die Datenbank nicht verfügbar ist, müssen Sie das SnapCenter Backup-Jobprotokoll prüfen, um das richtige Backup zu finden.

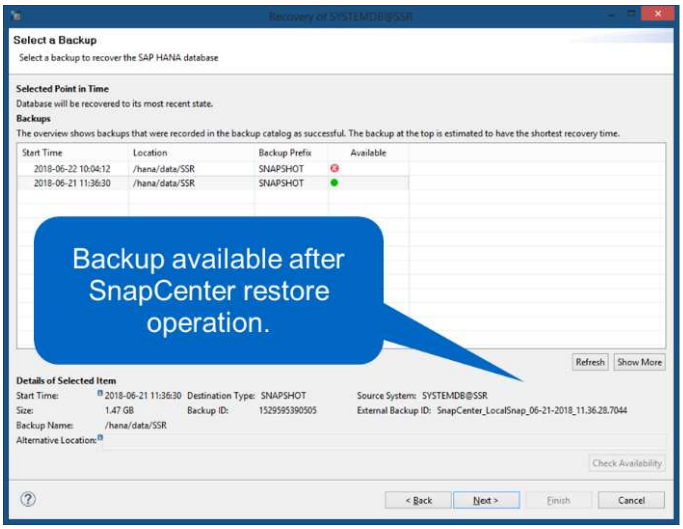


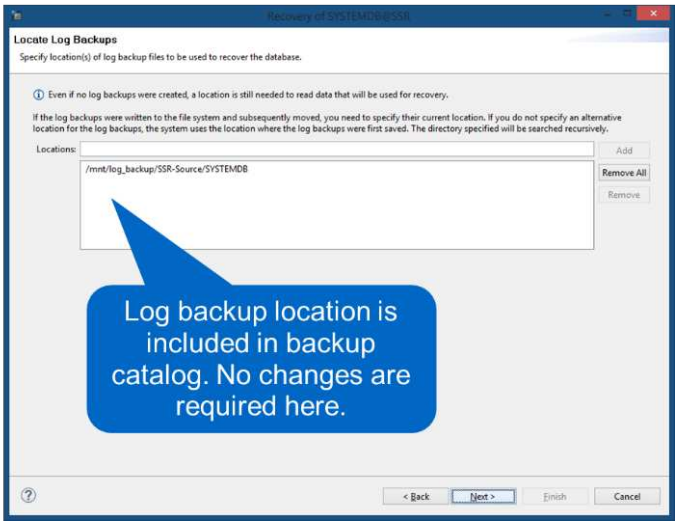
In SnapCenter wird das Backup ausgewählt und ein Restore-Vorgang auf Dateiebene durchgeführt. Auf dem Bildschirm Wiederherstellung auf Dateiebene wird nur das Host 1 Volume ausgewählt, sodass nur das gültige

Backup wiederhergestellt wird.



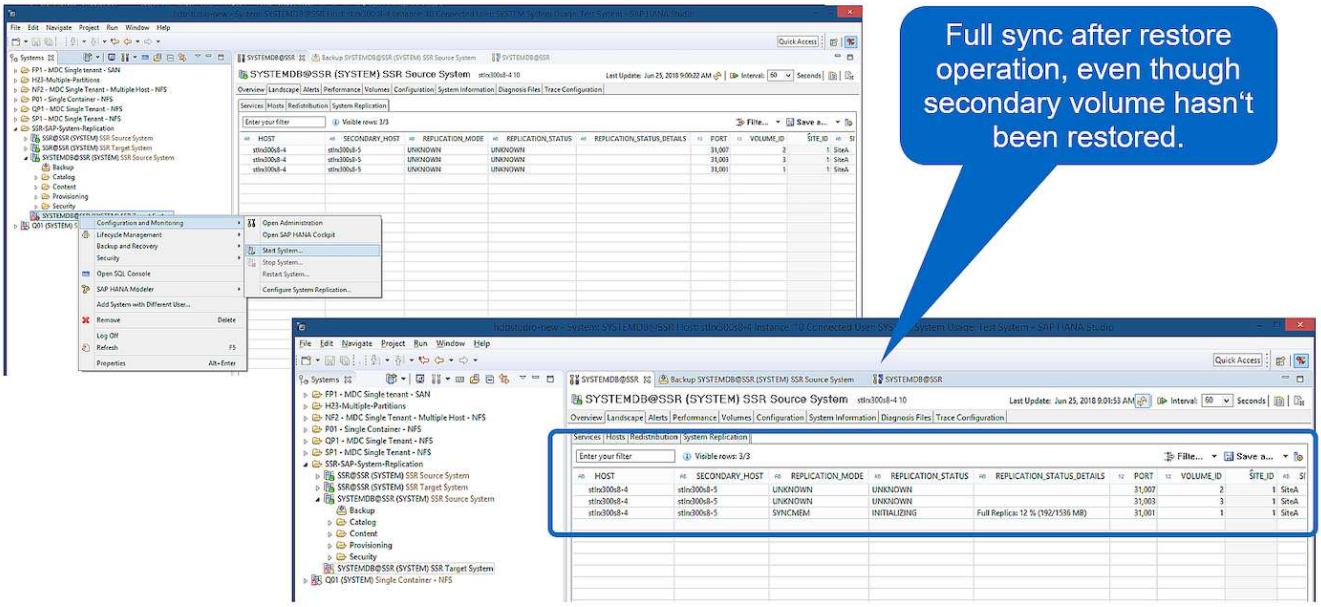
Nach der Wiederherstellung wird das Backup in SAP HANA Studio grün hervorgehoben. Sie müssen nicht einen zusätzlichen Log-Backup-Speicherort eingeben, weil der Dateipfad der Log-Backups von Host 1 und Host 2 im Backup-Katalog enthalten sind.





Nach Abschluss der vorwärts gerichteten Recovery wird der sekundäre Host (Host 2) gestartet und die Resynchronisierung der SAP HANA System Replication gestartet.

Obwohl der sekundäre Host aktuell ist (kein Restore-Vorgang für Host 2 durchgeführt), führt SAP HANA eine vollständige Replizierung aller Daten durch. Dieses Verhalten ist Standard nach einem Restore- und Recovery-Vorgang mit SAP HANA System Replication.

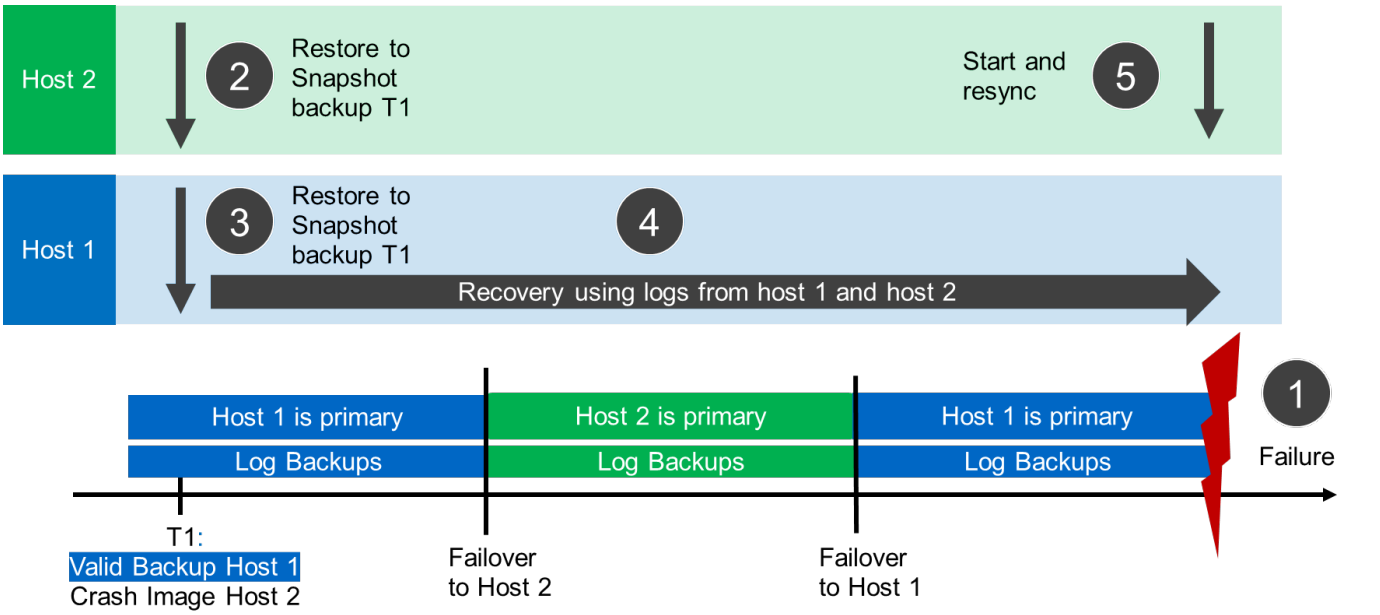


SnapCenter Restore von gültigem Backup- und Crash-Image

Die folgende Abbildung zeigt einen Überblick über das in diesem Abschnitt beschriebene Wiederherstellungsszenario.

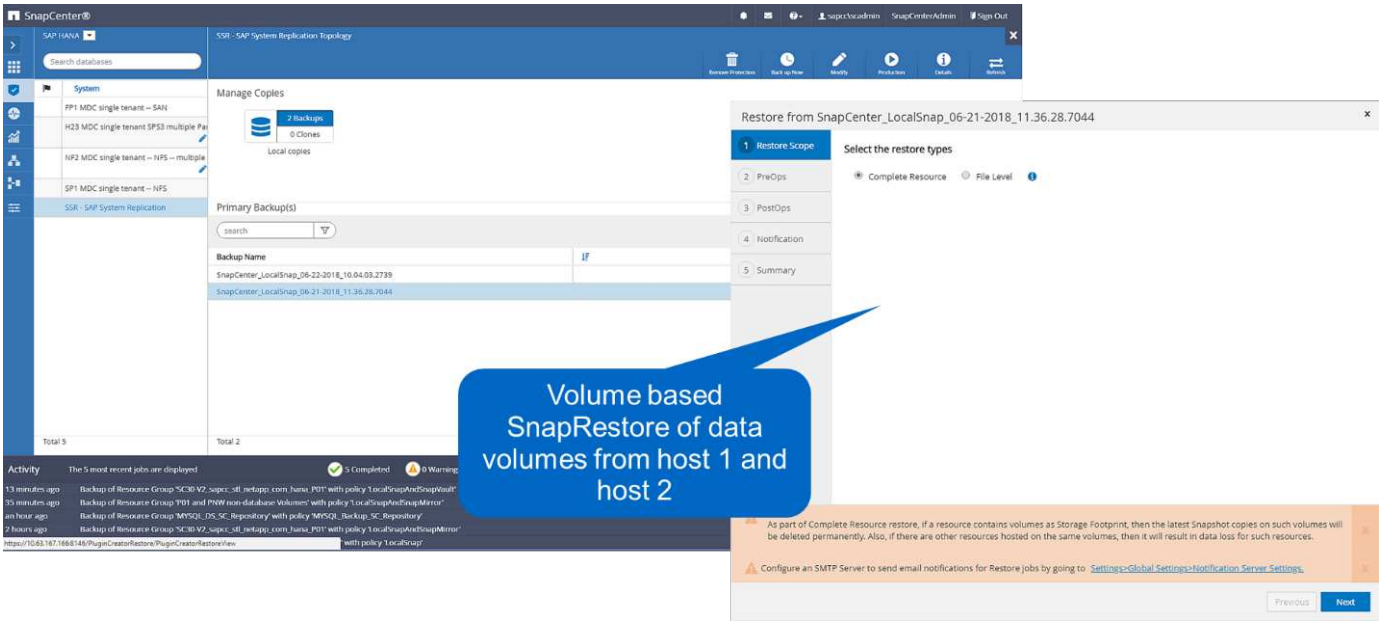
Bei T1 am Host 1 wurde ein Backup erstellt. Ein Failover wurde an Host 2 durchgeführt. Nach einem bestimmten Zeitpunkt wurde ein weiteres Failover zurück zu Host 1 durchgeführt. Zum aktuellen Zeitpunkt ist Host 1 der primäre Host.

1. Es ist ein Fehler aufgetreten, und Sie müssen das am T1 erstellte Backup am Host 1 wiederherstellen.
2. Der sekundäre Host (Host 2) wird heruntergefahren und das T1-Absturzabbild wird wiederhergestellt.
3. Das Speichervolumen von Host 1 wird auf dem bei T1 erstellten Backup wiederhergestellt.
4. Eine vorwärts gerichteten Wiederherstellung wird mit Protokollen von Host 1 und Host 2 durchgeführt.
5. Host 2 wird gestartet und eine Resynchronisierung der Systemreplizierung von Host 2 wird automatisch gestartet.

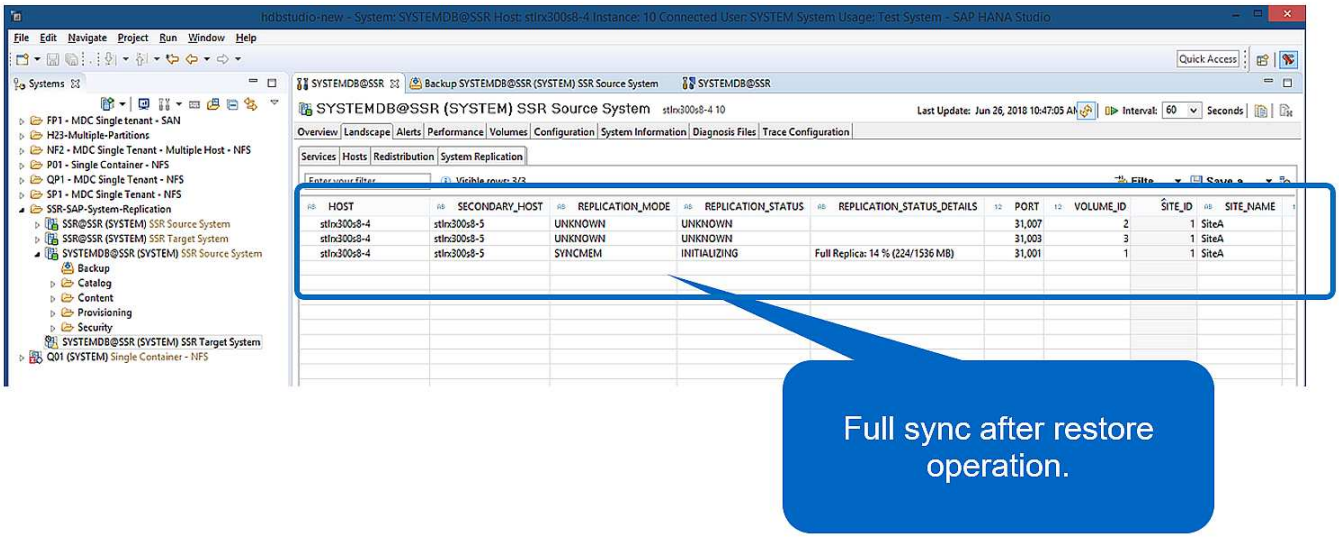


Der Wiederherstellungs- und Wiederherstellungsvorgang mit SAP HANA Studio ist identisch mit den im Abschnitt beschriebenen Schritten "SnapCenter Restore nur für gültige Backups".

Um den Wiederherstellungsvorgang durchzuführen, wählen Sie in SnapCenter die Option Ressource abschließen. Die Volumes beider Hosts werden wiederhergestellt.



Nach Abschluss der erweiterten Recovery wird der sekundäre Host (Host 2) gestartet und die Resynchronisierung von SAP HANA System Replication gestartet. Eine vollständige Replizierung aller Daten wird durchgeführt.



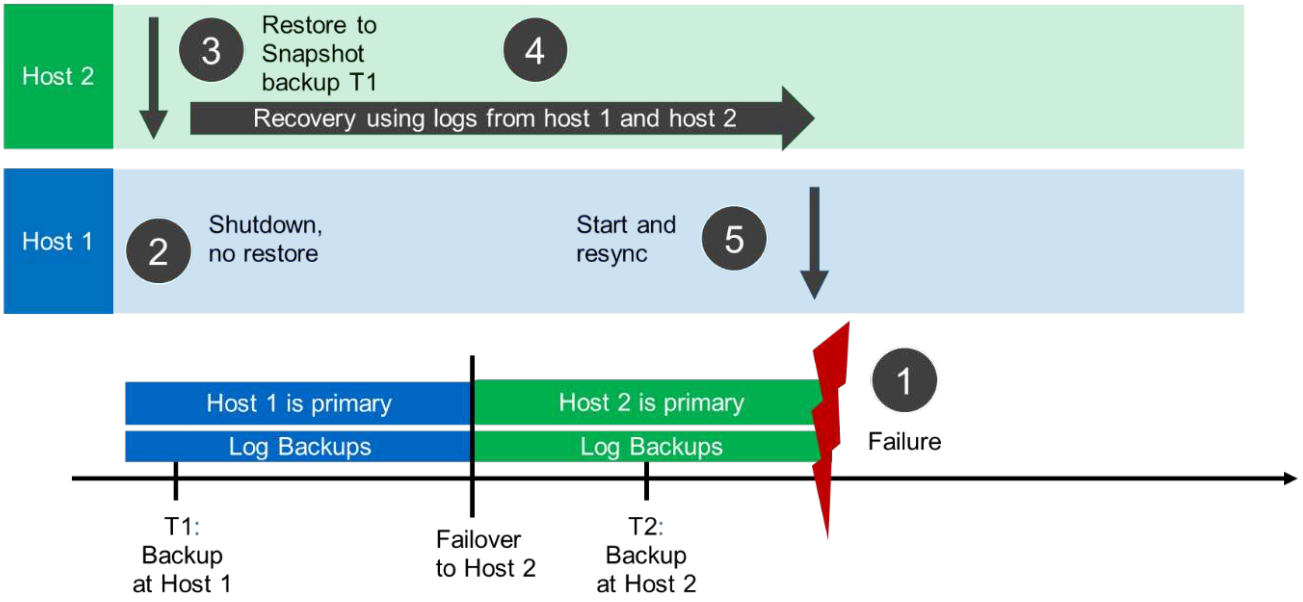
Wiederherstellung und Recovery von einem auf dem anderen Host erstellten Backup

Ein Restore-Vorgang aus einem Backup, das auf dem anderen SAP HANA-Host erstellt wurde, ist ein gültiges Szenario für beide SnapCenter-Konfigurationsoptionen.

Die folgende Abbildung zeigt einen Überblick über das in diesem Abschnitt beschriebene Wiederherstellungsszenario.

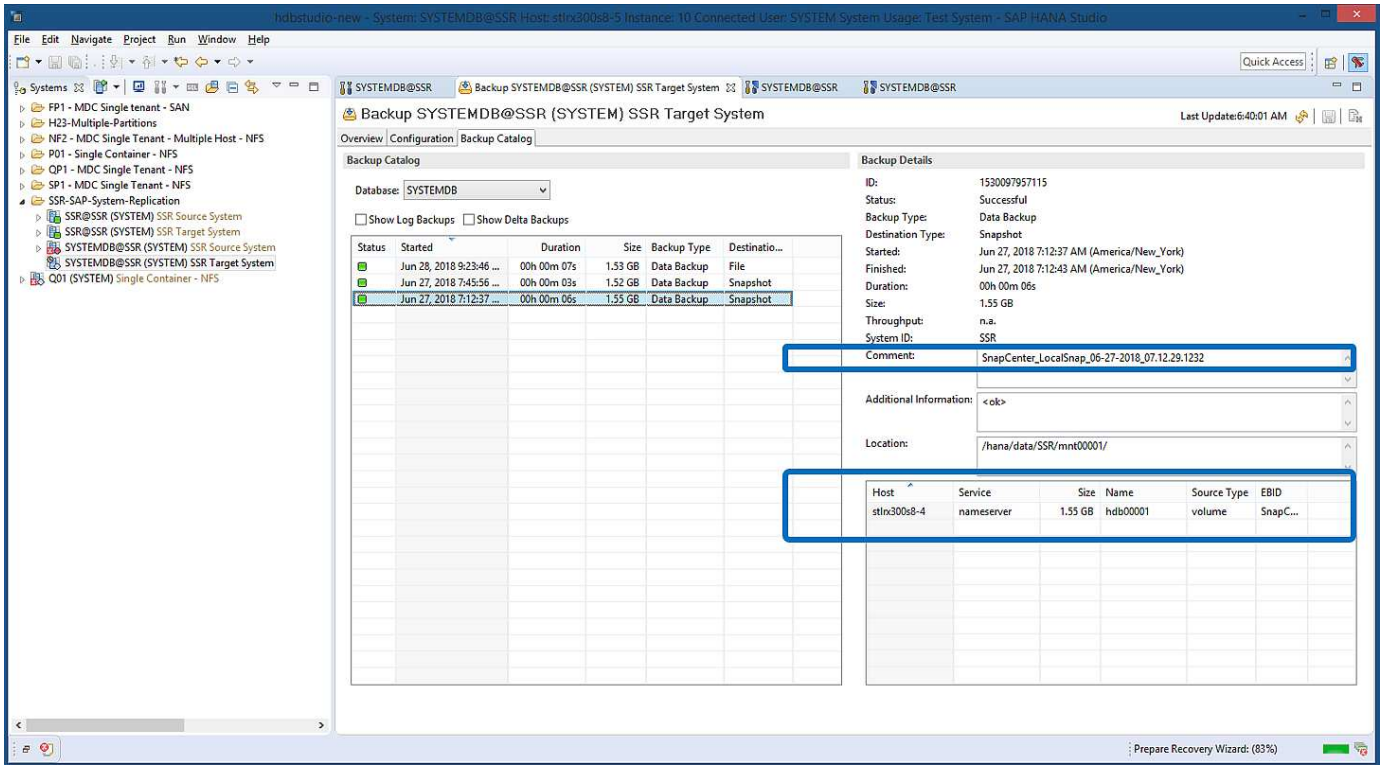
Bei T1 am Host 1 wurde ein Backup erstellt. Ein Failover wurde an Host 2 durchgeführt. Zum aktuellen Zeitpunkt ist Host 2 der primäre Host.

1. Es ist ein Fehler aufgetreten, und Sie müssen das am T1 erstellte Backup am Host 1 wiederherstellen.
2. Der primäre Host (Host 1) wird heruntergefahren.
3. Die Backup-Daten T1 von Host 1 wird auf Host 2 wiederhergestellt.
4. Eine Weiterleitung der Recovery erfolgt mithilfe von Protokollen von Host 1 und Host 2.
5. Host 1 wird gestartet, und die Neusynchronisierung der Systemreplizierung von Host 1 wird automatisch gestartet.



31

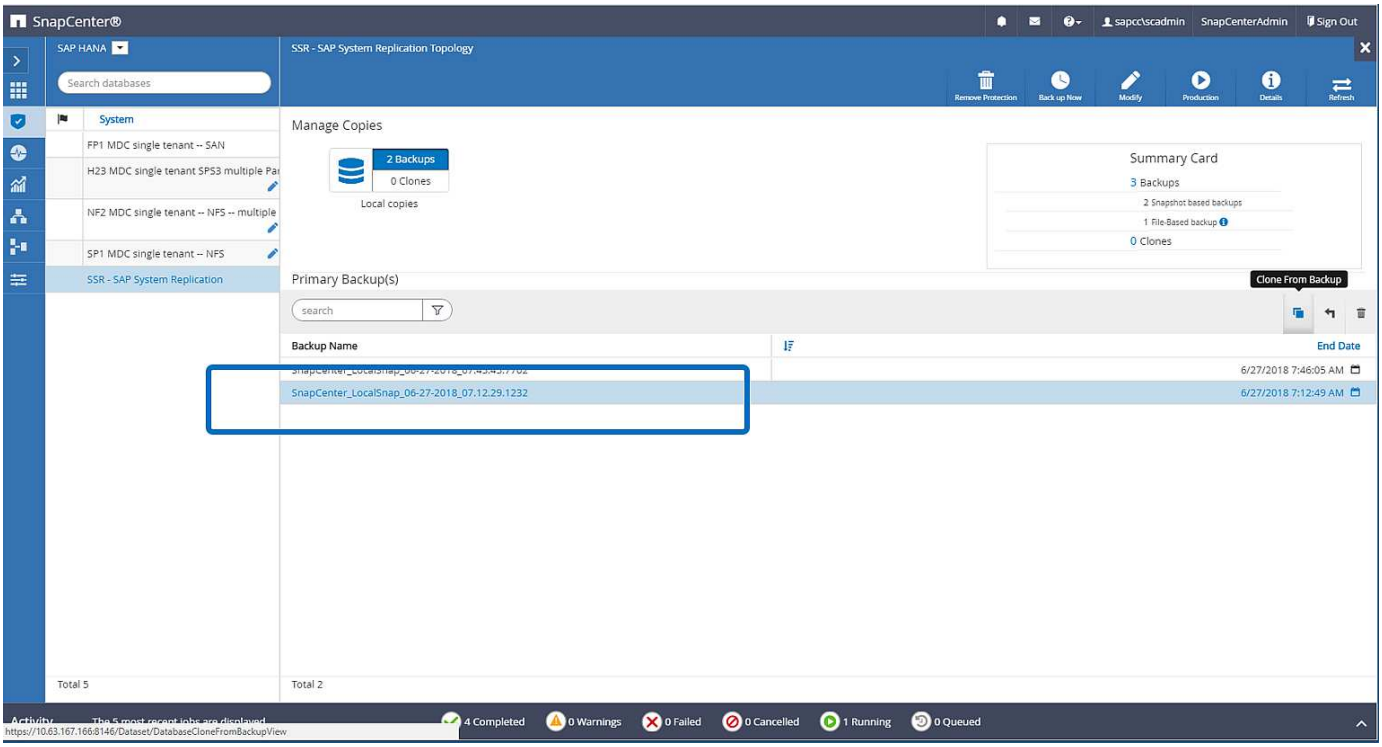
Die folgende Abbildung zeigt den SAP HANA Backup-Katalog und hebt das auf Host 1 erstellte Backup hervor, das für den Restore- und Recovery-Vorgang verwendet wurde.



Die Wiederherstellung umfasst die folgenden Schritte:

1. Erstellen Sie einen Klon aus dem Backup, das auf Host 1 erstellt wurde.
2. Mounten Sie das geklonte Volume unter Host 2.
3. Kopieren Sie die Daten vom geklonten Volume in den ursprünglichen Speicherort.

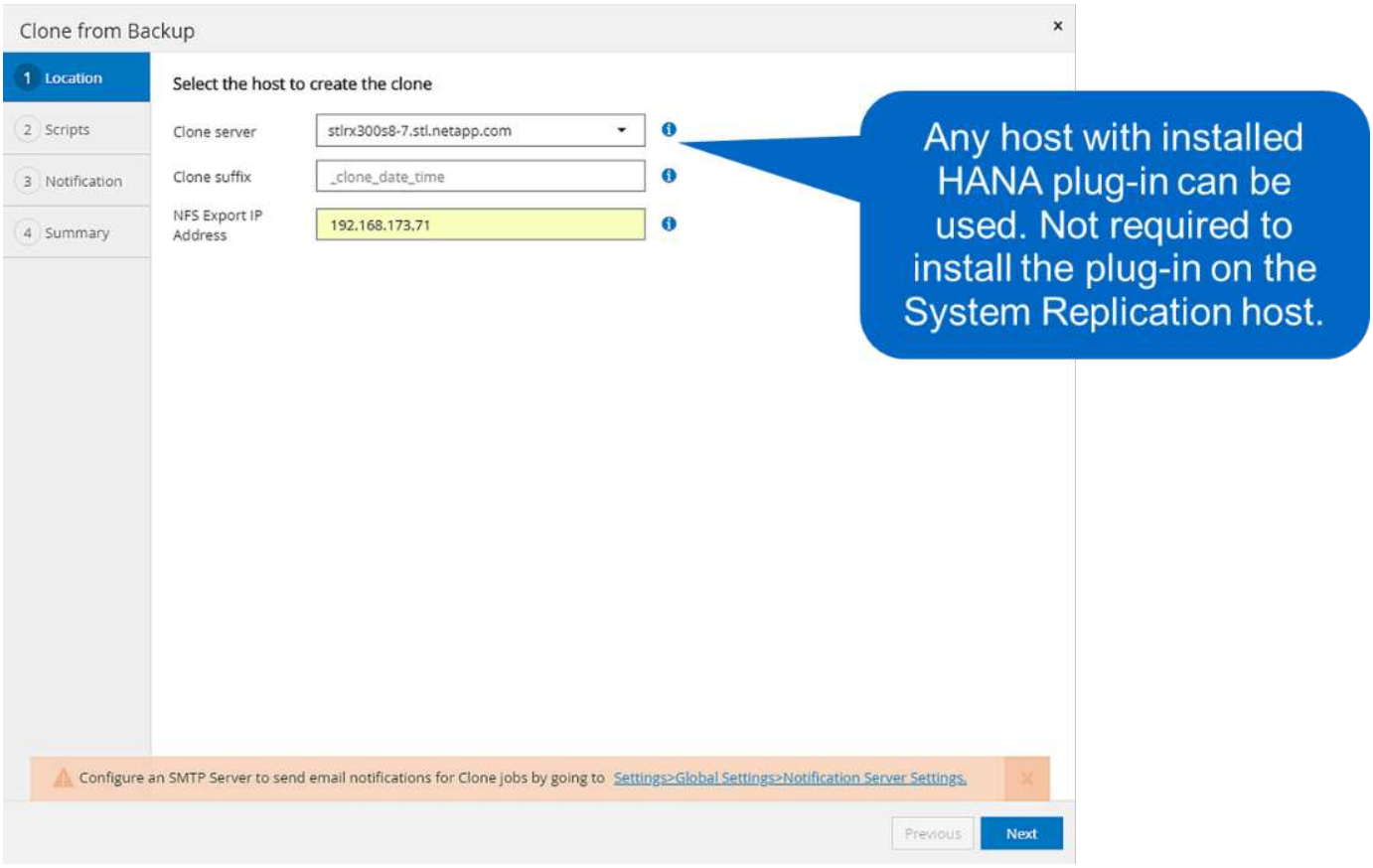
In SnapCenter wird das Backup ausgewählt und der Klonvorgang gestartet.



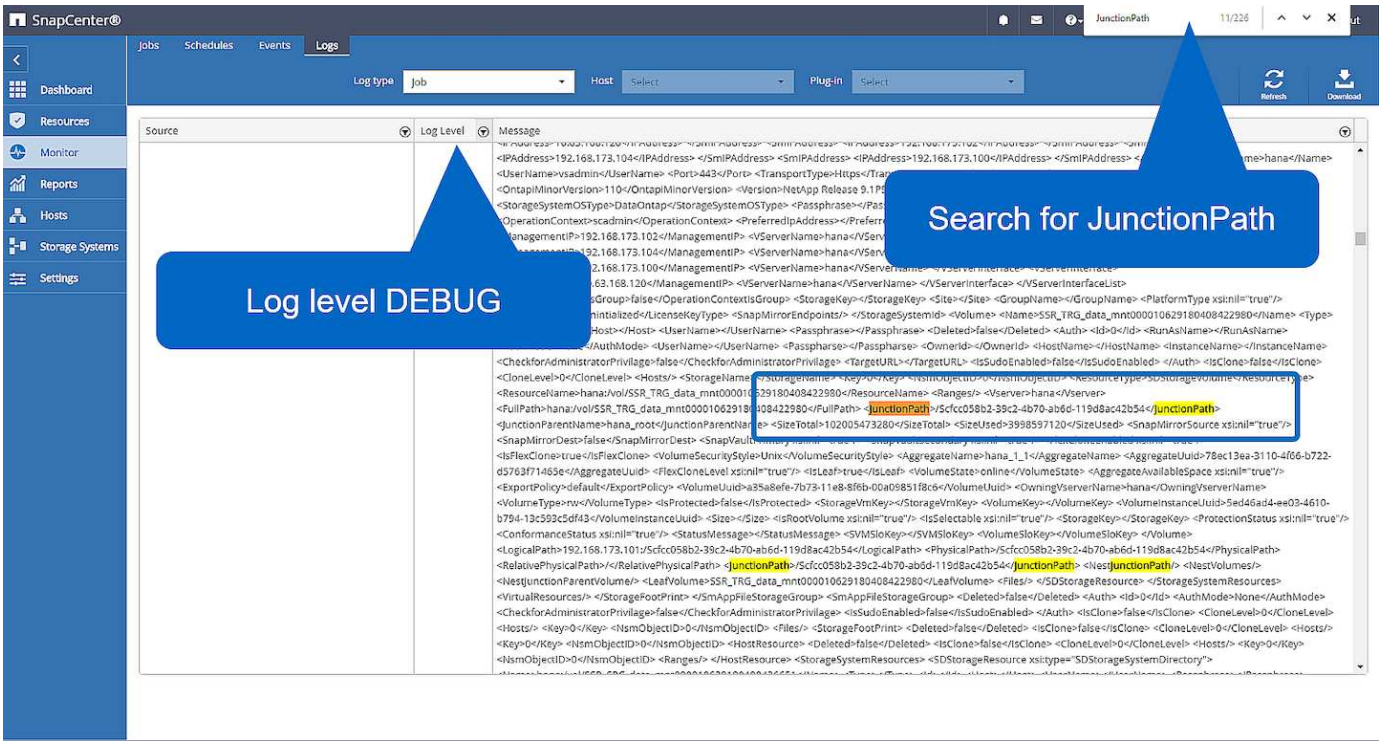
Sie müssen den Klon-Server und die NFS-Export-IP-Adresse angeben.

Bei einer SnapCenter-Konfiguration mit einer Einzelressource ist das SAP HANA-Plug-in nicht auf dem Datenbank-Host installiert. Zum Ausführen des SnapCenter Clone Workflows kann jeder Host mit einem installierten HANA-Plug-in als Klon-Server verwendet werden.

+ in einer SnapCenter-Konfiguration mit separaten Ressourcen wird der HANA-Datenbank-Host als Klon-Server ausgewählt, und ein Mount-Skript wird verwendet, um den Klon auf dem Ziel-Host zu mounten.



Um den Verbindungspfad zu bestimmen, der zum Mounten des geklonten Volume erforderlich ist, prüfen Sie das Jobprotokoll des Klonjobs, wie in der folgenden Abbildung dargestellt.



Das geklonte Volume kann jetzt angehängt werden.

```
stlrx300s8-5:/mnt/tmp # mount 192.168.173.101:/Scc373da37-00ff-4694-b1e1-
8153dbd46caf /mnt/tmp
```

Das geklonte Volume enthält die Daten der HANA-Datenbank.

```
stlrx300s8-5:/mnt/tmp/# ls -al
drwxr-x--x 2 ssradm sapsys 4096 Jun 27 11:12 hdb00001
drwx------ 2 ssradm sapsys 4096 Jun 21 09:38 hdb00002.00003
drwx------ 2 ssradm sapsys 4096 Jun 27 11:12 hdb00003.00003
-rw-r--r-- 1 ssradm sapsys   22 Jun 27 11:12 nameserver.lck
```

Die Daten werden an den ursprünglichen Speicherort kopiert.

```
stlrx300s8-5:/mnt/tmp # cp -Rp hdb00001 /hana/data/SSR/mnt00001/
stlrx300s8-5:/mnt/tmp # cp -Rp hdb00002.00003/ /hana/data/SSR/mnt00001/
stlrx300s8-5:/mnt/tmp # cp -Rp hdb00003.00003/ /hana/data/SSR/mnt00001/
```

Die Wiederherstellung mit SAP HANA Studio erfolgt wie im Abschnitt beschrieben"SnapCenter Restore nur für gültige Backups".

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten:

- "Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter"
- "Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter"
- Technischer Bericht: SAP HANA Disaster Recovery with Storage Replication

  "https://www.netapp.com/us/media/tr-4646.pdf"

Versionsverlauf

Versionsverlauf:

Version	Datum	Versionsverlauf Des Dokuments
Version 1.0	Oktober 2018	Ausgangsversion
Version 2.0	Januar 2022	Update zur Unterstützung von SnapCenter 4.6 HANA System Replication

Technischer Bericht: SAP HANA Disaster Recovery with Azure NetApp Files

TR-4891: SAP HANA Disaster Recovery mit Azure NetApp Files

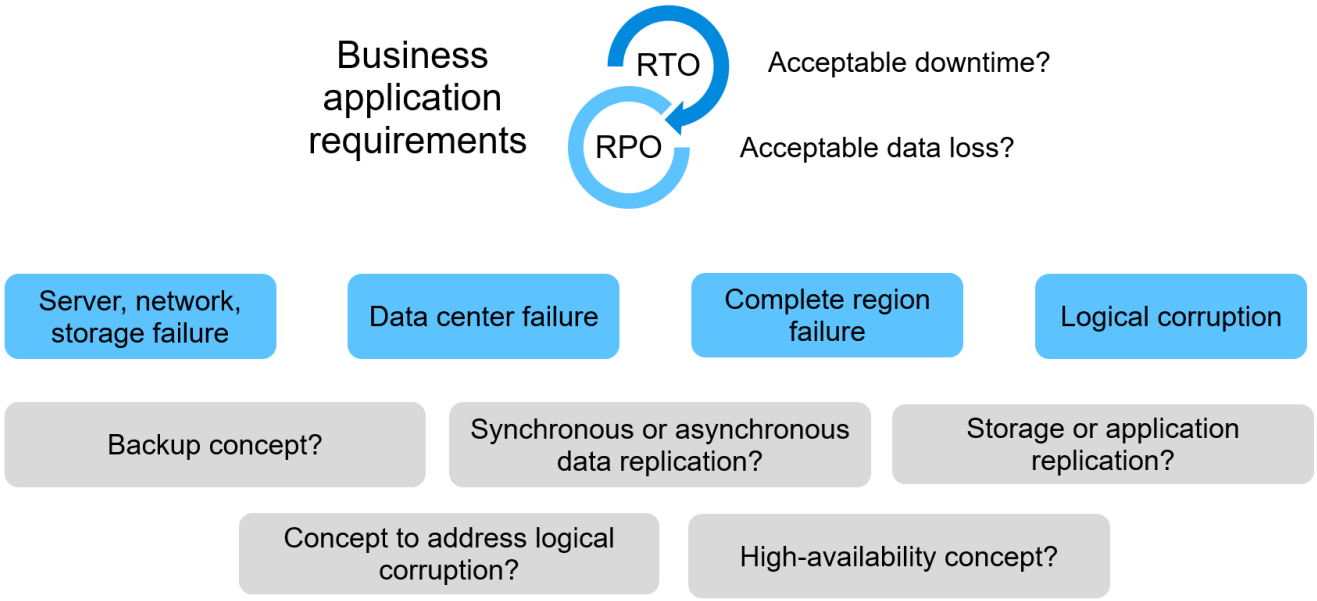
Studien haben gezeigt, dass Ausfallzeiten von Business-Applikationen erhebliche negative Auswirkungen auf das Geschäft von Unternehmen haben.

Autoren: Nils Bauer, NetApp Ralf Klahr, Microsoft

Neben den finanziellen Auswirkungen können Ausfallzeiten auch den Ruf des Unternehmens, die Arbeitsmoral des Personals und die Kundenbindung schädigen. Überraschenderweise haben nicht alle Unternehmen eine umfassende Disaster Recovery-Richtlinie.

Wenn SAP HANA auf Azure NetApp Files (ANF) läuft, erhalten Kunden Zugriff auf zusätzliche Funktionen, mit denen die integrierte Datensicherung und Disaster Recovery-Funktionen von SAP HANA erweitert und verbessert werden können. In der Übersicht werden die folgenden Optionen erläutert, mit denen Kunden Optionen auswählen können, die ihre geschäftlichen Anforderungen unterstützen.

Zur Entwicklung einer umfassenden Disaster Recovery-Richtlinie müssen Kunden die Anforderungen ihrer Business-Applikationen und die technischen Funktionen kennen, die sie für Datensicherung und Disaster Recovery benötigen. Die folgende Abbildung bietet einen Überblick über die Datensicherung.



Anforderungen von Business-Applikationen

Für Geschäftsanwendungen gibt es zwei wichtige Indikatoren:

- Der Recovery-Zeitpunkt (Recovery Point Objective, RPO) oder der maximal tolerierbare Datenverlust
- Die Recovery-Zeitvorgabe (Recovery Time Objective, RTO) bzw. die maximal tolerierbare Ausfallzeit von Business-Applikationen

Diese Anforderungen werden durch die Art der verwendeten Applikation und die Art der Geschäftsdaten definiert. RPO und RTO können unterschiedlich sein, wenn Sie vor Ausfällen in einer einzelnen Azure Region

schützen. Sie können auch voneinander abweichen, wenn Sie sich auf katastrophale Katastrophen wie den Verlust einer kompletten Azure-Region vorbereiten. Es ist wichtig, die geschäftlichen Anforderungen zu bewerten, die RPO und RTO definieren, da diese Anforderungen erhebliche Auswirkungen auf die verfügbaren technischen Optionen haben.

Hochverfügbarkeit

Die Infrastruktur für SAP HANA wie Virtual Machines, Netzwerk und Storage muss über redundante Komponenten verfügen, um sicherzustellen, dass es keinen Single Point of Failure gibt. MS Azure bietet Redundanz für die verschiedenen Infrastrukturkomponenten.

Um auf der Computing- und Applikationsseite Hochverfügbarkeit zu gewährleisten, können Standby-SAP HANA-Hosts mit einem SAP HANA System mit mehreren Hosts für integrierte Hochverfügbarkeit konfiguriert werden. Wenn ein Server oder ein SAP HANA-Service ausfällt, erfolgt ein Failover des SAP HANA-Service auf den Standby-Host, was zu einem Ausfall von Applikationen führt.

Wenn eine Applikationsausfallzeit im Falle eines Server- oder Applikationsausfalls nicht akzeptabel ist, kann auch die SAP HANA Systemreplizierung als Hochverfügbarkeitslösung eingesetzt werden, die Failover in einem sehr kurzen Zeitrahmen ermöglicht. SAP-Kunden nutzen HANA-Systemreplizierung, um Hochverfügbarkeit bei ungeplanten Ausfällen sicherzustellen, aber auch die Ausfallzeiten bei geplanten Vorgängen wie HANA-Software-Upgrades zu minimieren.

Logische Beschädigung

Logische Beschädigungen können durch Softwarefehler, menschliche Fehler oder Sabotage verursacht werden. Leider können logische Beschädigungen oft nicht mit standardmäßigen Hochverfügbarkeits- und Disaster Recovery-Lösungen behoben werden. Daher können in manchen Fällen RTO- und RPO-Anforderungen in Abhängigkeit von der Ebene, der Applikation, dem File-System oder dem Storage mit der logischen Beschädigung nicht erfüllt werden.

Schlimmstenfalls ist die SAP-Applikation beschädigt oder logisch. SAP Applikationen laufen oft in einer Landschaft, in der verschiedene Applikationen miteinander kommunizieren und Daten austauschen. Daher wird die Wiederherstellung eines SAP-Systems, bei dem eine logische Beschädigung aufgetreten ist, nicht empfohlen. Das Wiederherstellen des Systems zu einem Zeitpunkt vor der Beschädigung führt zu Datenverlusten, sodass die RPO größer als null ist. Außerdem würde die SAP-Landschaft nicht mehr synchron sein und eine zusätzliche Nachbearbeitung erfordern.

Anstatt das SAP-System wiederherzustellen, ist es besser, den logischen Fehler innerhalb des Systems zu beheben, indem das Problem in einem separaten Reparatursystem analysiert wird. Zur Ursachenanalyse ist die Einbindung des Geschäftsprozesses und der Applikationseigentümer erforderlich. Für dieses Szenario erstellen Sie ein Reparatursystem (ein Klon des Produktionssystems) auf Basis der Daten, die vor dem Auftreten der logischen Beschädigung gespeichert wurden. Innerhalb des Reparatursystems können die erforderlichen Daten exportiert und in das Produktionssystem importiert werden. Bei diesem Ansatz muss das produktive System nicht gestoppt werden, und im besten Fall gehen keine Daten oder nur ein Bruchteil der Daten verloren.

Die zum Einrichten eines Reparatursystems erforderlichen Schritte sind mit einem in diesem Dokument beschriebenen Disaster-Recovery-Testszenario identisch. Somit kann die beschriebene Disaster Recovery-Lösung problemlos auf logische Beschädigungen erweitert werden.

Backups

Backups werden erstellt, um Restores und Recovery von unterschiedlichen zeitpunktgenauen Datensätzen zu

ermöglichen. In der Regel werden diese Backups einige Tage bis einige Wochen aufbewahrt.

Je nach Art der Beschädigung können Restores und Recovery mit oder ohne Datenverlust durchgeführt werden. Wenn das RPO null beträgt, selbst bei einem Verlust des Primär- und Backup-Storage, muss das Backup mit der synchronen Datenreplizierung kombiniert werden.

Die RTO für Restore und Recovery wird durch die erforderliche Wiederherstellungszeit, die Recovery-Zeit (einschließlich Datenbankstart) und das Laden der Daten in den Arbeitsspeicher definiert. Bei großen Datenbanken und herkömmlichen Backup-Ansätzen kann die RTO problemlos mehrere Stunden betragen, was unter Umständen nicht akzeptabel ist. Um eine sehr geringe RTO-Werte zu erzielen, muss ein Backup mit einer Hot-Standby-Lösung kombiniert werden, die das Vorladen von Daten in den Speicher beinhaltet.

Eine Backup-Lösung muss dagegen die logische Beschädigung beheben, da Datenreplizierungslösungen nicht alle Arten von logischen Beschädigungen abdecken können.

Synchrone oder asynchrone Datenreplizierung

Der RPO bestimmt hauptsächlich, welche Datenreplizierungsmethode Sie verwenden sollten. Bei einem RPO von null muss auch bei einem Ausfall des primären und des Backup-Storage die Daten synchron repliziert werden. Allerdings gibt es technische Einschränkungen bei der synchronen Replizierung, beispielsweise die Entfernung zwischen zwei Azure Regionen. In den meisten Fällen ist synchrone Replizierung aufgrund von Latenz bei Entfernungen von mehr als 100 km nicht geeignet. Daher ist diese Lösung keine Option für die Datenreplizierung zwischen Azure Regionen.

Wenn ein größerer RPO-Wert akzeptabel ist, kann die asynchrone Replizierung über große Entfernungen hinweg verwendet werden. Der RPO in diesem Fall wird durch die Replizierungsfrequenz definiert.

HANA System-Replizierung mit oder ohne vorab geladen

Die Startzeit einer SAP HANA-Datenbank ist wesentlich länger als die von herkömmlichen Datenbanken, da eine große Datenmenge in den Arbeitsspeicher geladen werden muss, bevor die Datenbank die erwartete Performance liefern kann. Daher ist ein großer Teil der RTO die Zeit, die zum Starten der Datenbank benötigt wird. Mit jeder Storage-basierten Replizierung sowie mit HANA System Replication ohne vorab geladen werden, muss die SAP HANA-Datenbank für den Failover zum Disaster-Recovery-Standort gestartet werden.

Die SAP HANA Systemreplizierung bietet einen Betriebsmodus, in dem die Daten vorgeladen und kontinuierlich am sekundären Host aktualisiert werden. Dieser Modus ermöglicht sehr niedrige RTO-Werte, benötigt aber auch einen dedizierten Server, der nur für den Empfang der Replizierungsdaten vom Quellsystem verwendet wird.

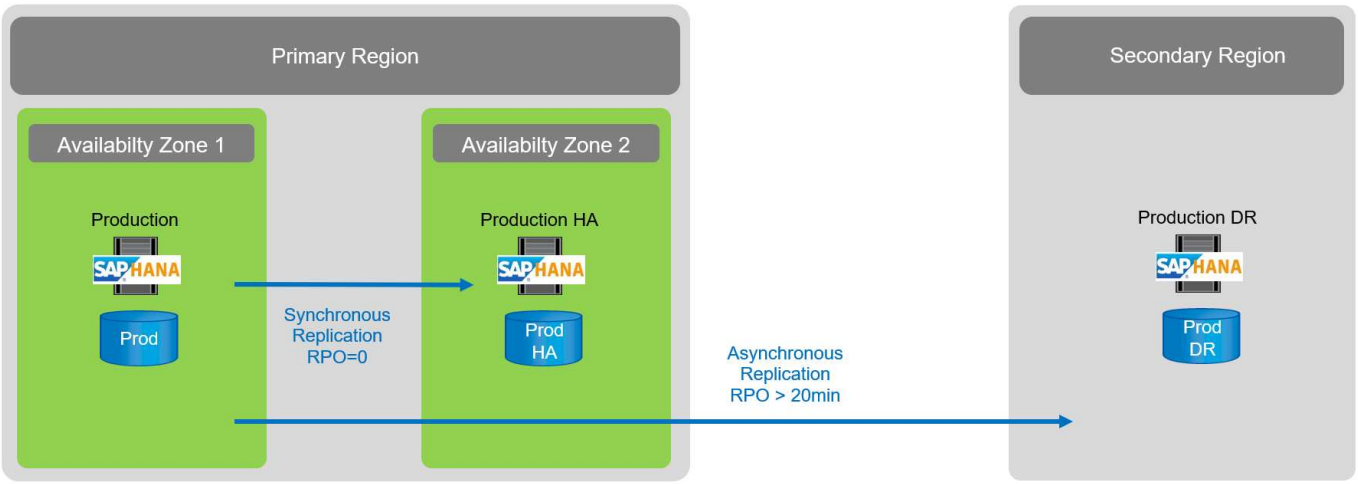
Disaster-Recovery-Lösungsvergleich

Eine umfassende Disaster Recovery-Lösung muss Kunden nach einem vollständigen Ausfall des primären Standorts die Wiederherstellung ermöglichen. Daher müssen die Daten an einen sekundären Standort übertragen werden und eine komplette Infrastruktur ist erforderlich, um bei einem Standortausfall die erforderlichen SAP HANA Produktionssysteme auszuführen. Abhängig von den Verfügbarkeitsanforderungen der Applikation und der Art des zu schützenden Disaster ist eine Disaster Recovery-Lösung mit zwei oder drei Standorten zu berücksichtigen.

Die folgende Abbildung zeigt eine typische Konfiguration, bei der die Daten innerhalb derselben Azure-Region synchron in eine zweite Verfügbarkeitszone repliziert werden. Durch die kurze Entfernung können Sie die Daten synchron replizieren und ein RPO von null (normalerweise HA-Bereitstellung) erreichen.

Darüber hinaus werden Daten asynchron in eine sekundäre Region repliziert, um sie vor Ausfällen zu schützen, wenn die primäre Region betroffen ist. Der erzielbare MindestRPO hängt von der Datenreplizierungsfrequenz ab, die durch die verfügbare Bandbreite zwischen dem primären und dem sekundären Bereich begrenzt ist. Ein typischer minimaler RPO liegt im Bereich von 20 Minuten bis mehreren Stunden.

Dieses Dokument erläutert verschiedene Implementierungsoptionen für eine Disaster Recovery-Lösung für zwei Regionen.



SAP HANA System Replication

SAP HANA System Replication arbeitet auf Datenbankebene. Die Lösung basiert auf einem zusätzlichen SAP HANA-System am Disaster-Recovery-Standort, das die Änderungen vom Primärsystem empfängt. Dieses sekundäre System muss mit dem Primärsystem identisch sein.

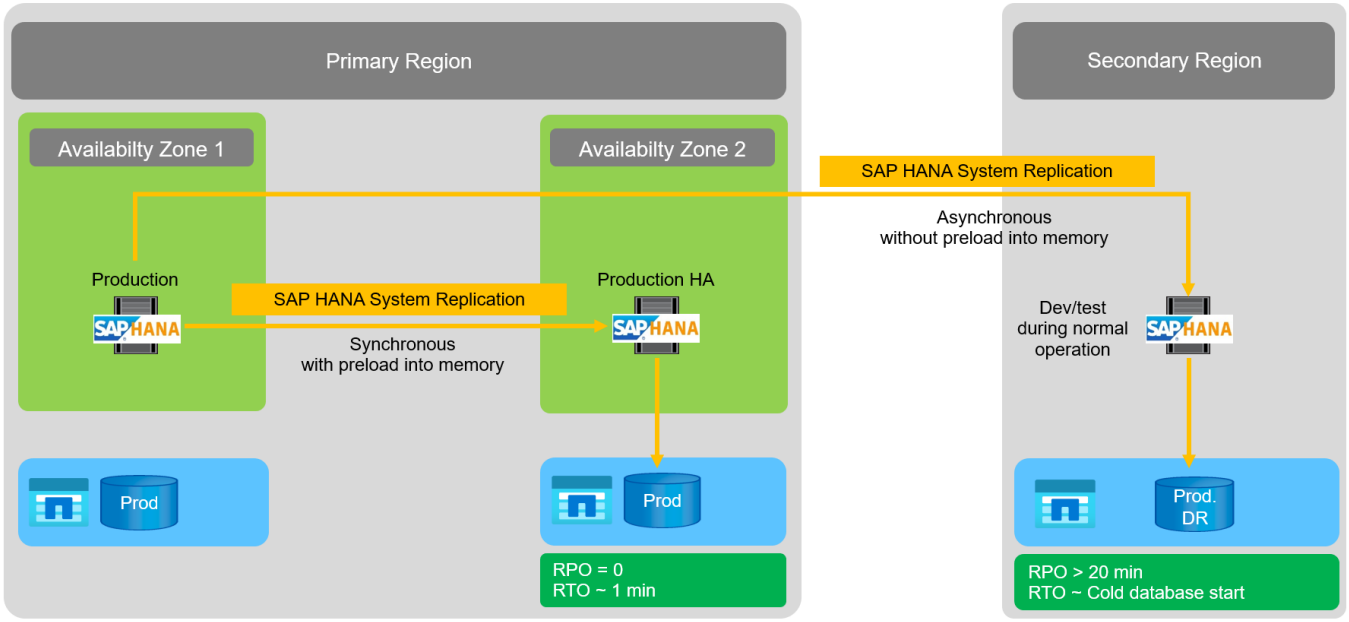
SAP HANA System Replication kann in einem von zwei Modi betrieben werden:

- Mit vorab in den Arbeitsspeicher geladenen Daten und einem dedizierten Server am Disaster-Recovery-Standort:
  - Der Server wird ausschließlich als sekundärer SAP HANA System Replication Host verwendet.
  - Sehr geringe RTO-Werte können erzielt werden, weil die Daten bereits in den Speicher geladen sind und bei einem Failover kein Datenbankstart erforderlich ist.
- Ohne Daten, die vorab in den Arbeitsspeicher geladen sind und einen gemeinsam genutzten Server am Disaster Recovery-Standort nutzen:
  - Der Server wird als sekundäres SAP HANA System Replication und als Entwicklungs-/Testsystem gemeinsam genutzt.
  - RTO hängt hauptsächlich von der Zeit ab, die zum Starten der Datenbank und Laden der Daten in den Arbeitsspeicher benötigt wird.

Eine vollständige Beschreibung aller Konfigurationsoptionen und Replikationsszenarien finden Sie im "SAP HANA Administration Guide".

Die folgende Abbildung zeigt das Setup einer Disaster-Recovery-Lösung für zwei Regionen mit SAP HANA System Replication. Die synchrone Replizierung mit vorab in den Speicher geladenen Daten wird für lokale HA in derselben Azure-Region verwendet, allerdings in verschiedenen Verfügbarkeitszonen. Die asynchrone Replizierung ohne vorab geladene Daten wird für die Remote Disaster-Recovery-Region konfiguriert.

Die folgende Abbildung zeigt die SAP HANA System Replication.



SAP HANA System Replication mit vorab in den Speicher geladenen Daten

Sehr geringe RTO-Werte mit SAP HANA können nur mit SAP HANA System Replication erreicht werden, wobei Daten vorab in den Speicher geladen sind. Der Betrieb von SAP HANA System Replication mit einem dedizierten sekundären Server am Disaster-Recovery-Standort ermöglicht einen RTO-Wert von maximal einer Minute. Die replizierten Daten werden empfangen und im sekundären System vorgeladen. Aus diesem Grund wird SAP HANA System Replication häufig auch für Wartungsvorgänge ohne Ausfallzeiten eingesetzt, beispielsweise für HANA-Software-Upgrades.

In der Regel ist SAP HANA System Replication so konfiguriert, dass sie synchron repliziert wird, wenn eine vorab-Datenlast ausgewählt wird. Die maximal unterstützte Entfernung bei synchroner Replizierung liegt im Bereich von 100 km.

SAP System Replication ohne vorab in den Speicher geladene Daten

Für weniger strenge RTO-Anforderungen kann SAP HANA System Replication ohne vorab geladene Daten verwendet werden. In diesem Betriebsmodus werden die Daten der Disaster-Recovery-Region nicht in den Arbeitsspeicher geladen. Der Server in der DR-Region wird weiterhin zur Verarbeitung von SAP HANA System Replication verwendet, auf dem alle erforderlichen SAP HANA-Prozesse ausgeführt werden. Der Großteil des Serverspeichers ist jedoch für andere Dienste verfügbar, wie zum Beispiel SAP HANA Entwicklungs-/Testsysteme.

Bei einem Notfall muss das Entwicklungs-/Testsystem heruntergefahren, der Failover initiiert und die Daten in den Arbeitsspeicher geladen werden. Das RTO dieses Cold-Standby-Ansatzes hängt von der Größe der Datenbank und dem Lesedurchsatz während der Last des Zeilen- und Spaltenspeichers ab. Mit der Annahme, dass die Daten mit einem Durchsatz von 1000 MBit/s gelesen werden, dass das Laden von 1 TB Daten ungefähr 18 Minuten dauert.

Technischer Bericht: SAP HANA Disaster Recovery with ANF Cross-Region Replication

ANF Cross-Region Replication ist in ANF als Disaster-Recovery-Lösung mit asynchroner Datenreplizierung integriert. ANF regionsübergreifende Replizierung wird über eine Datensicherungsbeziehung zwischen zwei ANF-Volumes in einer primären und einer sekundären Azure-Region konfiguriert. ANF-Cross-Region

Replication aktualisiert das sekundäre Volume mithilfe effizienter Block-Delta-Replikationen. Update-Zeitpläne können während der Replikationskonfiguration definiert werden.

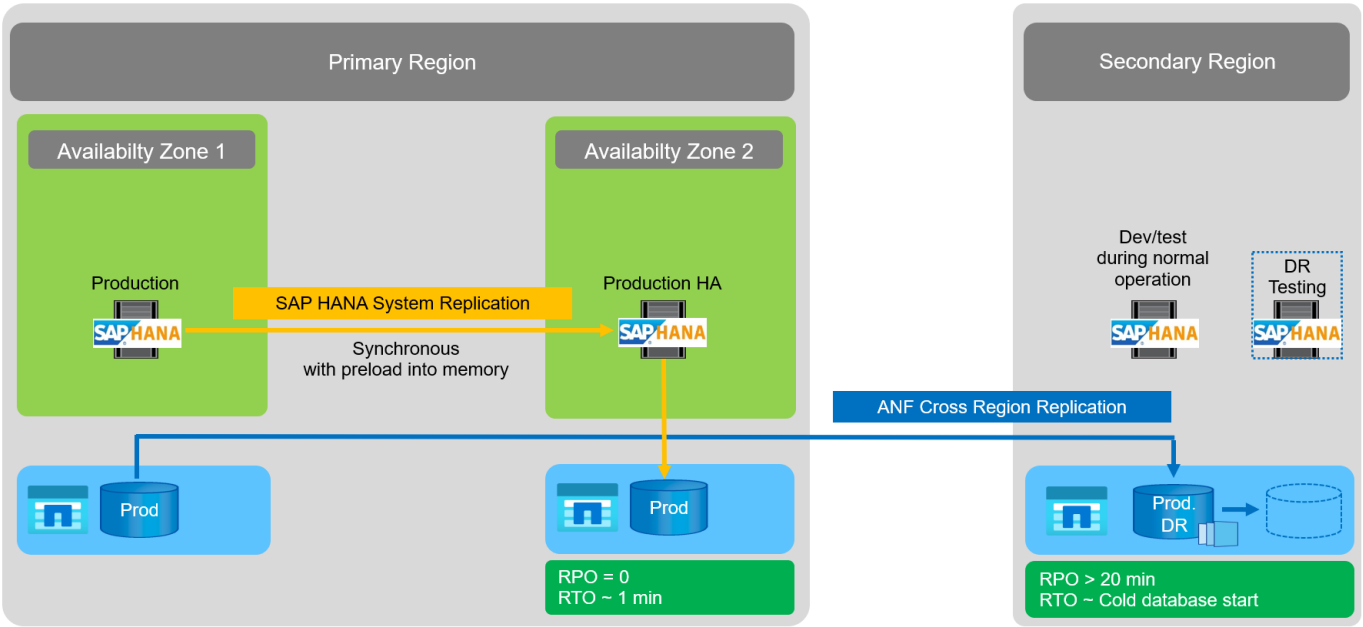
Die folgende Abbildung zeigt ein Beispiel für eine Disaster-Recovery-Lösung für zwei Regionen mithilfe von ANF-bereichsübergreifender Replizierung. In diesem Beispiel ist das HANA-System mit HANA System Replication innerhalb der primären Region geschützt, wie im vorherigen Kapitel erläutert. Die Replikation in eine sekundäre Region wird mittels ANF-bereichsübergreifender Replikation durchgeführt. Der RPO-Wert wird durch den Replizierungszeitplan und die Replizierungsoptionen definiert.

Das RTO hängt hauptsächlich von der Zeit ab, die zum Starten der HANA-Datenbank am Disaster-Recovery-Standort und zum Laden der Daten in den Arbeitsspeicher benötigt wird. Mit der Annahme, dass die Daten mit einem Durchsatz von 1000 MB/s gelesen werden, dass das Laden von 1 TB Daten ungefähr 18 Minuten dauert. Je nach Replizierungskonfiguration ist auch Recovery-Prozesse erforderlich und wird der RTO-Gesamtwert steigern.

Weitere Details zu den verschiedenen Konfigurationsoptionen finden Sie in Kapitel "Konfigurationsoptionen für regionsübergreifende Replizierung mit SAP HANA".

Die Server an den Disaster-Recovery-Standorten können als Entwicklungs-/Testsysteme im normalen Betrieb eingesetzt werden. Bei einem Notfall müssen die Entwicklungs-/Testsysteme heruntergefahren und als DR-Produktionsserver gestartet werden.

Mit der standortübergreifenden ANF Replizierung können Sie den DR-Workflow testen, ohne dass RPO und RTO beeinträchtigt werden. Dazu werden Volume-Klone erstellt und an den DR-Testserver angeschlossen.



Zusammenfassung der Disaster Recovery-Lösungen

In der folgenden Tabelle werden die in diesem Abschnitt beschriebenen Disaster-Recovery-Lösungen verglichen und die wichtigsten Kennzahlen hervorgehoben.

Die wichtigsten Ergebnisse:

- Ist ein sehr niedriges RTO erforderlich, ist SAP HANA System Replication mit vorab-Load in den Speicher die einzige Option.
  - Am DR-Standort ist ein dedizierter Server erforderlich, um die replizierten Daten zu erhalten und die

Daten in den Arbeitsspeicher zu laden.

- Darüber hinaus ist eine Storage-Replizierung für die Daten erforderlich, die sich außerhalb der Datenbank befinden (z. B. gemeinsam genutzte Dateien, Schnittstellen usw.).
- Bei einer geringeren RTO/RPO-Anforderung kann auch eine regionale ANF-Replizierung verwendet werden, um:
  - Kombinieren Sie Datenreplizierung außerhalb von Datenbanken.
  - Behandeln Sie zusätzliche Anwendungsfälle wie Disaster-Recovery-Tests und Aktualisierungen von Entwicklung/Tests.
  - Bei der Storage-Replizierung kann der Server am DR-Standort im normalen Betrieb als QA- oder Testsystem verwendet werden.
- Eine Kombination aus SAP HANA System Replication als HA-Lösung mit RPO=0 mit Storage-Replizierung für große Entfernungen ist sinnvoll, um die unterschiedlichen Anforderungen zu erfüllen.

In der folgenden Tabelle werden die Disaster-Recovery-Lösungen verglichen.

	Storage-Replizierung	**SAP HANA Systemreplizierung**	
	Regionenübergreifende Replikation	* Mit Datenvorladung*	**Ohne Datenvorladung**
RTO	Gering bis mittel; abhängig von der Startzeit der Datenbank und der Vorwärtswiederherstellung	Sehr niedrig	Gering bis mittel; abhängig von der Datenbank-Startzeit
RPO	RPO > 20 Min. Asynchrone Replizierung	RPO > 20 Min. Asynchrone Replikation RPO = 0 synchrone Replizierung	RPO > 20 Min. Asynchrone Replikation RPO = 0 synchrone Replizierung
Server am DR-Standort können für Entwicklung/Test genutzt werden	Ja.	Nein	Ja.
Replizierung von nicht aus Datenbanken stammenden Daten	Ja.	Nein	Nein
DR-Daten können zur Aktualisierung von Entwicklungs-/Testsystemen genutzt werden	Ja.	Nein	Nein
DR-Tests ohne Auswirkungen auf RTO und RPO	Ja.	Nein	Nein

ANF: Regionale Replizierung mit SAP HANA

ANF: Regionale Replizierung mit SAP HANA

Anwendungsunabhängige Informationen zur regionsübergreifenden Replikation finden Sie an folgendem Speicherort.

"Azure NetApp Files Dokumentation – Microsoft Docs" In den Abschnitten Konzepte und Anleitungen.

Konfigurationsoptionen für Regionalreplizierung mit SAP HANA

Die folgende Abbildung zeigt die Volume-Replizierungsbeziehungen für ein SAP HANA-System mit ANF-bereichsübergreifender Replizierung. Bei ANF-Cross-Region Replication müssen die HANA-Daten und das gemeinsame HANA-Volume repliziert werden. Wenn nur das HANA-Daten-Volume repliziert wird, liegen die typischen RPO-Werte im Bereich von einem Tag. Wenn niedrigere RPO-Werte erforderlich sind, müssen die HANA-Protokoll-Backups auch für die zukünftige Recovery repliziert werden.

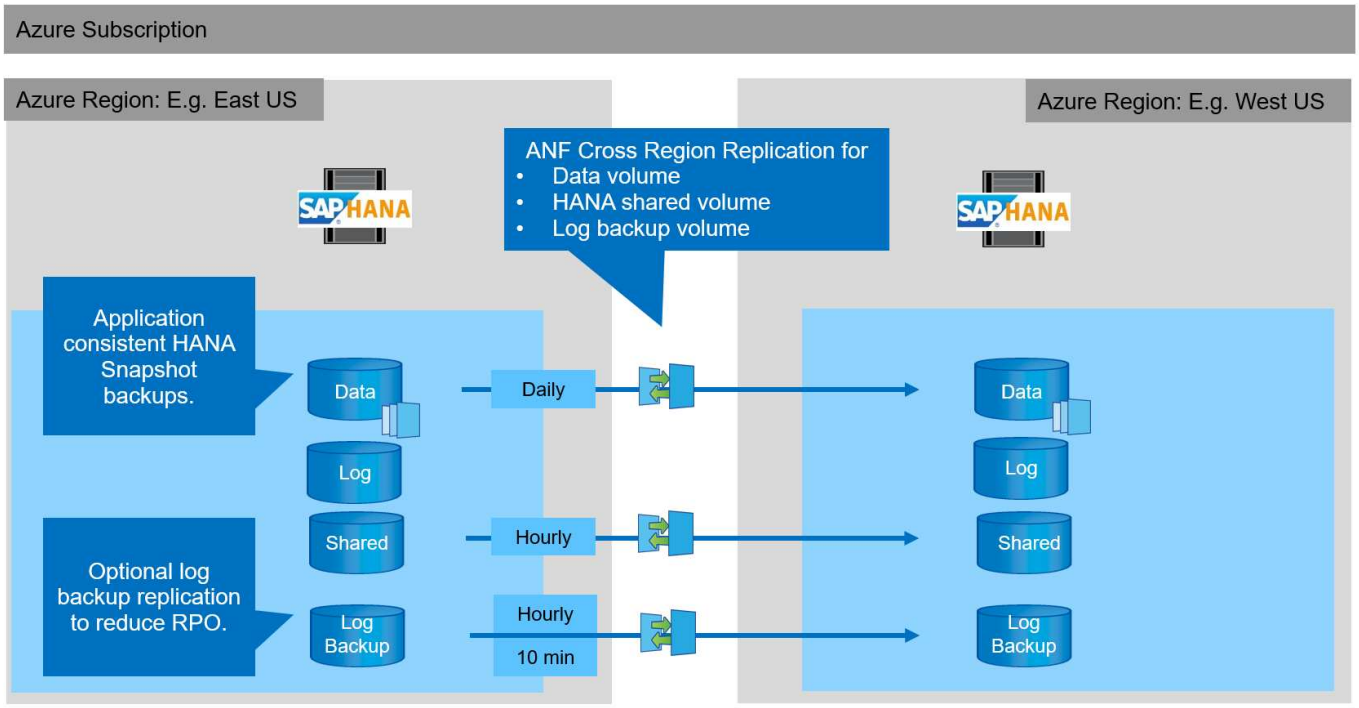
> ⓘ Der in diesem Dokument verwendete Begriff „Protokollsicherung“ umfasst die Protokollsicherung und die Sicherung des HANA-Backup-Katalogs. Der HANA-Backup-Katalog ist erforderlich, um Recovery-Vorgänge durchzuführen.

> ⓘ Die folgende Beschreibung und der Schwerpunkt der Laboreinrichtung sind auf die HANA-Datenbank. Andere gemeinsam genutzte Dateien, zum Beispiel das SAP-Transportverzeichnis, würden auf die gleiche Weise gesichert und repliziert werden wie das freigegebene HANA-Volume.

Für die HANA-Speicherpunktwiederherstellung oder Forward-Recovery mit den Backup-Protokollen müssen am primären Standort für das HANA-Daten-Volume applikationskonsistente Snapshot Backups erstellt werden. Dies kann zum Beispiel mit dem ANF-Backup-Tool AzAcSnap (siehe auch "Was ist Azure Application konsistente Snapshot Tool für Azure NetApp Files Microsoft Docs"). Die am primären Standort erstellten Snapshot Backups werden anschließend am DR-Standort repliziert.

Bei einem Disaster Failover muss die Replizierungsbeziehung beschädigt werden, die Volumes müssen auf dem DR-Produktionsserver eingebunden werden, und die HANA-Datenbank muss wiederhergestellt werden, entweder zum letzten HANA-Speicherpunkt oder bei einer Forward-Recovery mit den replizierten Log-Backups. Das Kapitel "Disaster-Recovery-Failover", beschreibt die erforderlichen Schritte.

In der folgenden Abbildung sind die HANA-Konfigurationsoptionen für die regionsübergreifende Replizierung dargestellt.



Mit der aktuellen Version der Cross-Region-Replikation können nur feste Zeitpläne ausgewählt werden, und die tatsächliche Replikationsaktualisierungszeit kann nicht vom Benutzer definiert werden. Verfügbare Termine sind täglich, stündlich und alle 10 Minuten. Bei Verwendung dieser Zeitplanoptionen sind zwei verschiedene Konfigurationen je nach RPO-Anforderungen sinnvoll: Daten-Volume-Replizierung ohne Backup-Replizierung bei Protokolldaten sowie Backup-Replizierung mit verschiedenen Zeitplänen entweder stündlich oder alle 10 Minuten. Die niedrigste mögliche RPO beträgt etwa 20 Minuten. In der folgenden Tabelle sind die Konfigurationsoptionen sowie die resultierenden RPO- und RTO-Werte zusammengefasst.

	Replizierung von Daten-Volumes	**Replizierung von Daten und Backup Volumes protokollieren**	**Replizierung von Daten und Backup Volumes protokollieren**
CRR-Volumen planen	Täglich	Täglich	Täglich
CRR-Protokoll Backup-Volumen planen	k. A.	Stündlich	10 Min
Max. RPO	24 Stunden + Snapshot Zeitplan (z. B. 6 Stunden)	1 Stunde	2 x 10 Min
Max RTO	In erster Linie durch die HANA-Startzeit definiert	+ HANA Startzeit + Wiederherstellungszeit+	+ HANA Startzeit + Wiederherstellungszeit+
Wiederherstellung vorwärts	NA	Logs der letzten 24 Stunden + Snapshot Zeitplan (z.B. 6 Stunden)	Logs der letzten 24 Stunden + Snapshot Zeitplan (z.B. 6 Stunden)

Anforderungen und Best Practices

Microsoft Azure übernimmt keine Garantie für die Verfügbarkeit eines bestimmten VM-Typs (Virtual Machine) bei der Erstellung oder beim Starten einer nicht zugewiesenen VM. Insbesondere im Falle eines regionalen Ausfalls benötigen viele Clients möglicherweise zusätzliche VMs in der Disaster Recovery-Region. Daher wird

empfohlen, eine VM mit der erforderlichen Größe für Disaster Failover aktiv als Test- oder QA-System in der Disaster Recovery-Region zu verwenden, um den erforderlichen VM-Typ zugewiesen zu haben.

Es empfiehlt sich, einen ANF-Kapazitätspool mit einer niedrigeren Performance Tier im normalen Betrieb zu verwenden, um eine Kostenoptimierung zu ermöglichen. Die Datenreplizierung erfordert keine hohe Performance und kann daher einen Kapazitäts-Pool mit einer Standard-Performance-Tier verwenden. Bei Disaster-Recovery-Tests oder bei einem Ausfall muss die Volume in einen Kapazitäts-Pool mit einer hochperformanten Tier verschoben werden.

Wenn ein zweiter Kapazitäts-Pool keine Option ist, sollten die Ziel-Volumes für die Replizierung auf Basis der Kapazitätsanforderungen konfiguriert werden und nicht auf die Performance-Anforderungen während des normalen Betriebs. Das Kontingent oder der Durchsatz (für manuelle QoS) kann dann für Disaster-Recovery-Tests angepasst werden, falls ein Notfall besteht.

Weitere Informationen finden Sie unter "Anforderungen und Überlegungen für die Verwendung von Azure NetApp Files-Volume-regionsübergreifende Replikation mit Microsoft Docs".

Laboreinrichtung

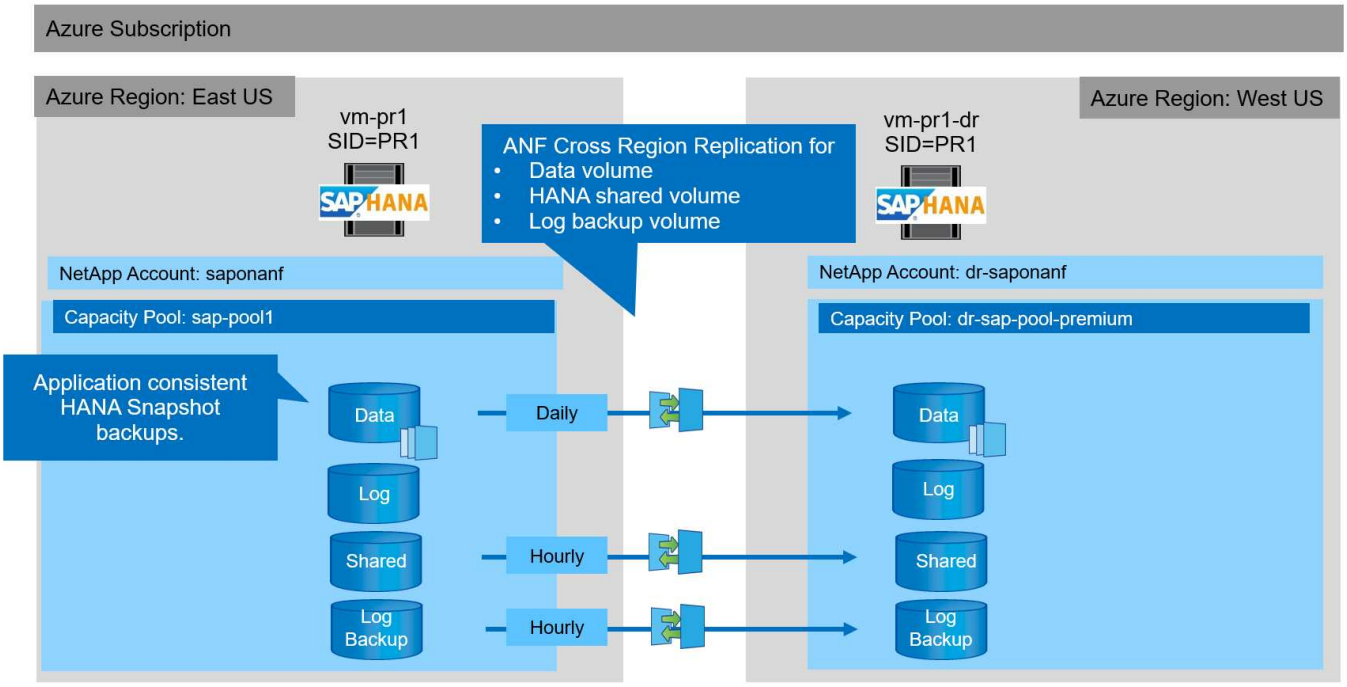
Die Lösungsvalidierung wurde mit einem Single-Host-System für SAP HANA durchgeführt. Das Microsoft AzAcSnap Snapshot Backup-Tool für ANF wurde verwendet, um applikationskonsistente HANA Snapshot Backups zu konfigurieren. Es wurden ein tägliches Datenvolumen, ein stündliches Log Backup und die gemeinsame Volume-Replizierung konfiguriert. Disaster Recovery-Tests und Failover wurden mit einem Speicherpunkt sowie bei vorwärts gerichteten Recovery-Vorgängen validiert.

Die folgenden Softwareversionen wurden für die Laboreinrichtung verwendet:

- Ein einziges Host-System SAP HANA 2.0 SPS5 mit einem einzelnen Mandanten
- SUSE SLES FÜR SAP 15 SP1
- AzAcSnap 5.0

Am DR-Standort wurde ein einzelner Kapazitäts-Pool mit manueller QoS konfiguriert.

Die folgende Abbildung zeigt die Laboreinrichtung.

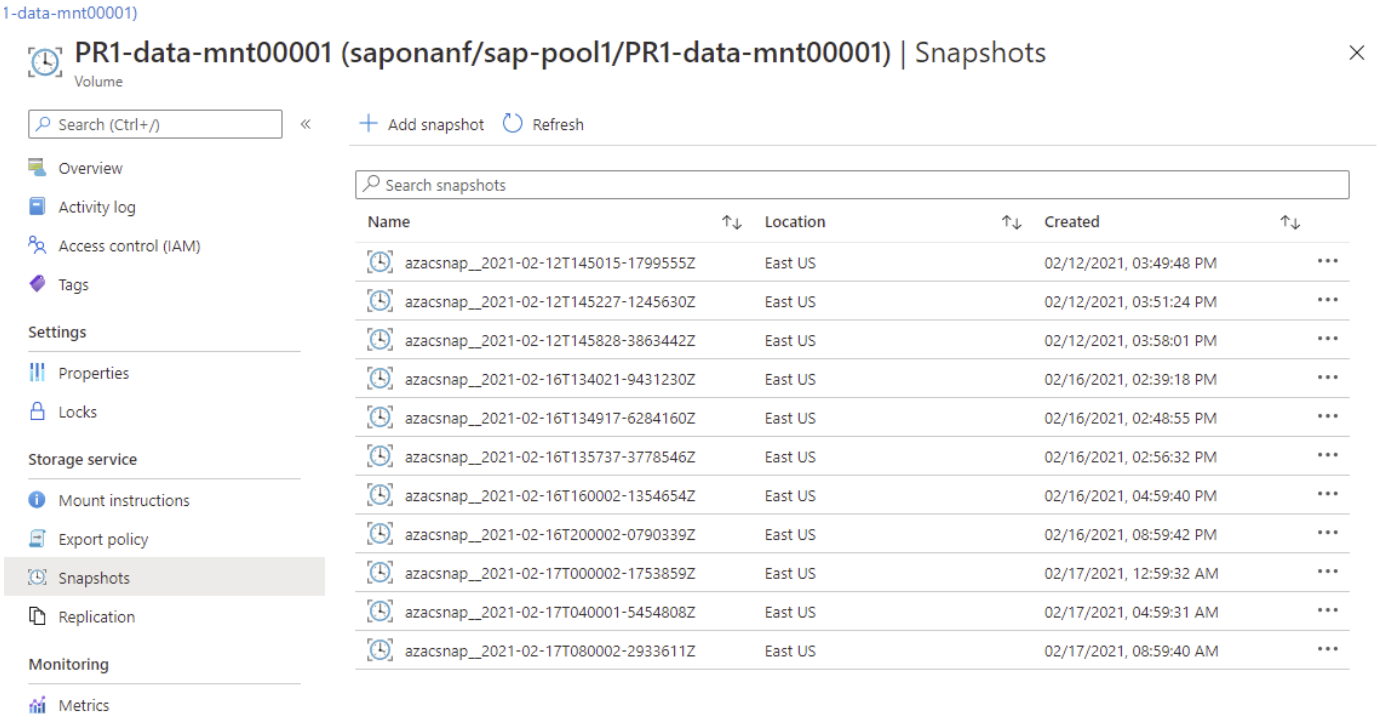


Snapshot Backup-Konfiguration mit AzAcSnap

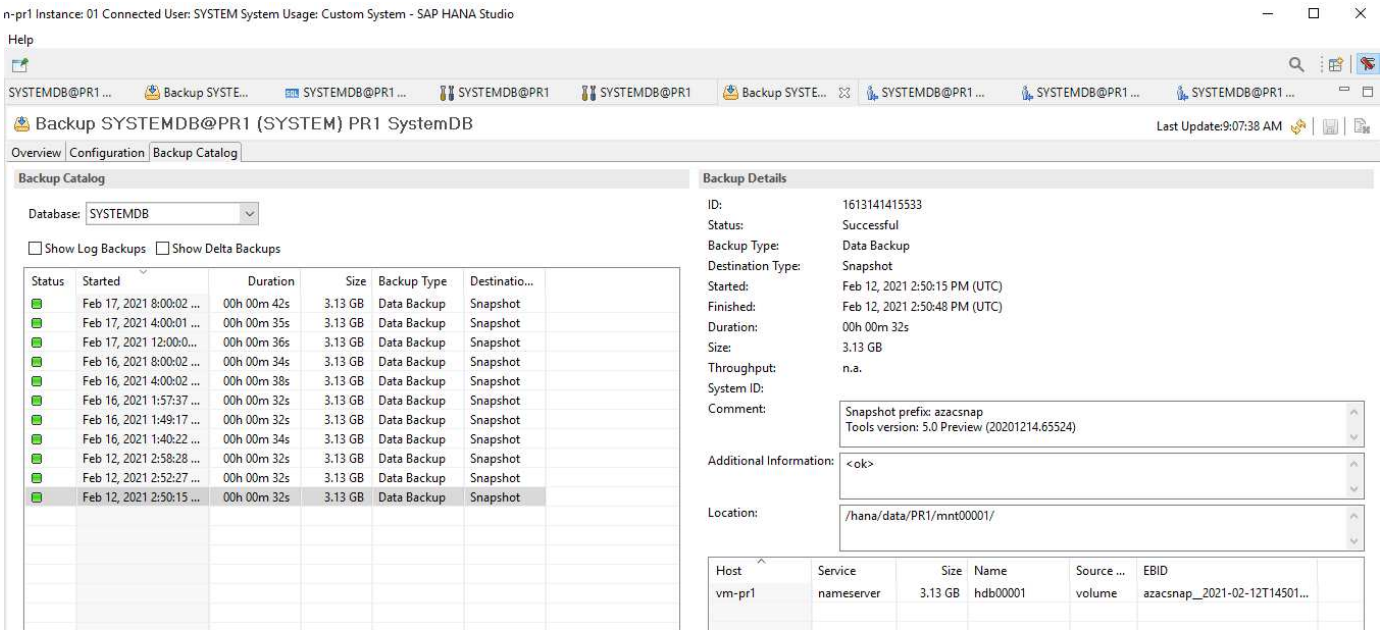
Am primären Standort wurde AzAcSnap für die Erstellung applikationskonsistenter Snapshot-Backups des HANA-Systems PR1 konfiguriert. Diese Snapshot-Backups sind im ANF-Datenvolumen des PR1 HANA Systems verfügbar und sind auch im SAP HANA Backup-Katalog registriert, wie in den beiden folgenden Abbildungen dargestellt. Snapshot Backups wurden alle 4 Stunden geplant.

Bei der Replizierung des Daten-Volumes mithilfe von ANF Cross-Region Replication werden diese Snapshot-Backups am Disaster Recovery-Standort repliziert und können zur Wiederherstellung der HANA-Datenbank verwendet werden.

Die folgende Abbildung zeigt die Snapshot Backups des HANA Daten-Volumes.



Die folgende Abbildung zeigt den SAP HANA-Backup-Katalog.



Konfigurationsschritte für ANF-bereichsübergreifende Replikation

Am Disaster Recovery-Standort sind einige Vorbereitungsschritte durchzuführen, bevor die Volume-Replizierung konfiguriert werden kann.

- Ein NetApp Konto muss verfügbar und mit demselben Azure Abonnement wie die Quelle konfiguriert sein.
- Ein Kapazitäts-Pool muss über das oben genannte NetApp Konto verfügbar und konfiguriert sein.
- Ein virtuelles Netzwerk muss verfügbar und konfiguriert sein.
- Innerhalb des virtuellen Netzwerks muss ein delegiertes Subnetz zur Verwendung mit ANF verfügbar und

konfiguriert sein.

Protection Volumes können nun für HANA-Daten, HANA Shared IT und das HANA-Log-Backup-Volume erstellt werden. Die folgende Tabelle zeigt die konfigurierten Ziel-Volumes in unserer Laboreinrichtung.

> Um eine optimale Latenz zu erzielen, müssen die Volumes in der Nähe der VMs platziert werden, die im Falle eines Disaster-Failover den SAP HANA ausführen. Daher ist für die DR-Volumes derselbe Pinning-Prozess wie für jedes andere SAP HANA-Produktionssystem erforderlich.

HANA Volume	Quelle	Ziel	Replizierungsplan
HANA-Datenvolumen	PR1-Data-mnt00001	PR1-Data-mnt00001-SM-dest	Täglich
HANA Shared Volume	PR1 freigegeben	PR1-shared-SM-dest	Stündlich
HANA-Protokoll-/Katalogbackup-Volume	Hanabackup	Hanabackup-SM-dest	Stündlich

Für jedes Volume müssen folgende Schritte durchgeführt werden:

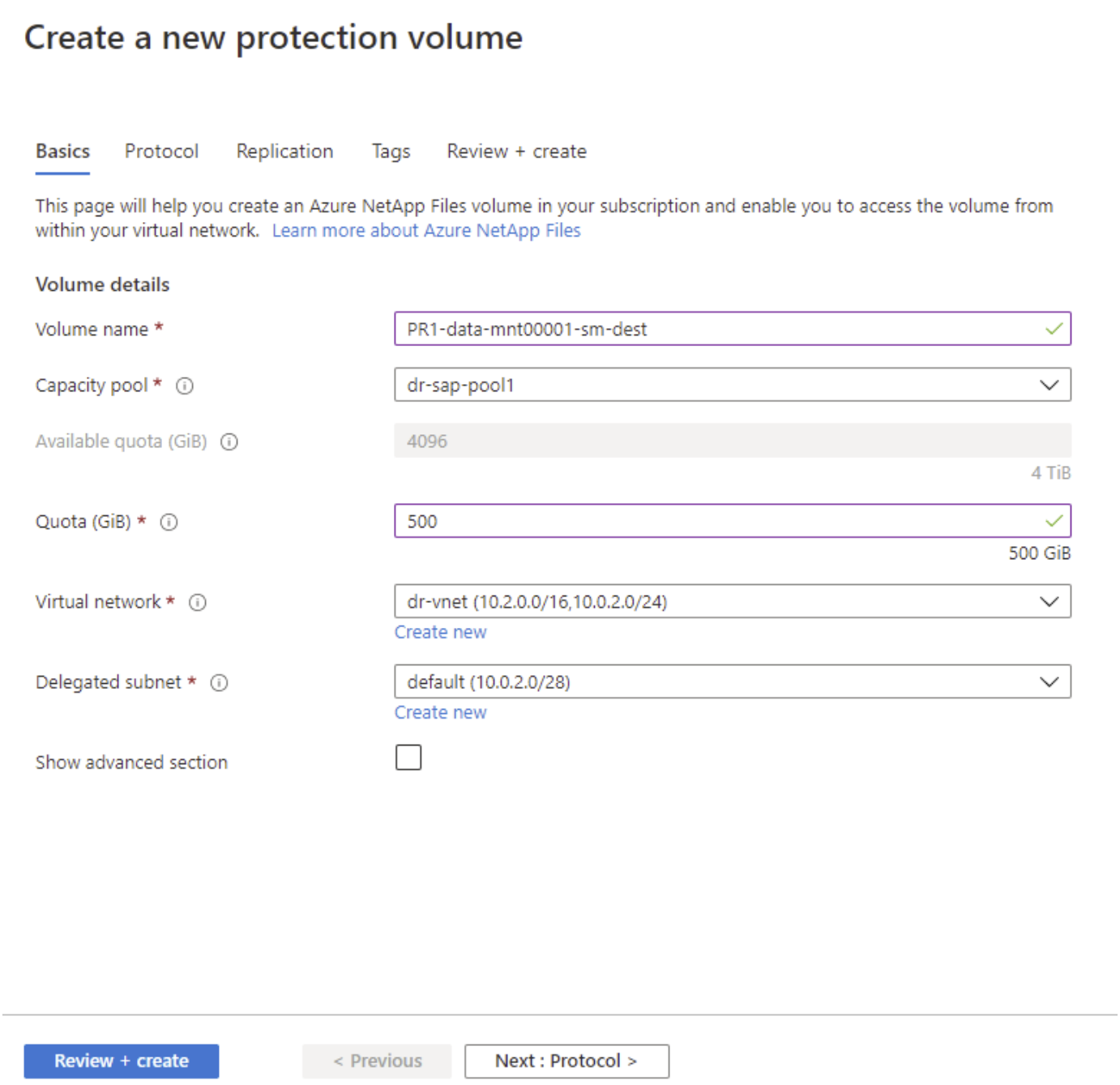
1. Erstellen eines neuen Sicherungs-Volumes am DR-Standort:
   a. Stellen Sie Volume-Namen, den Kapazitäts-Pool, die Quota- und Netzwerkinformationen bereit.
   b. Bereitstellen der Zugriffsinformationen für Protokolle und Volumes
   c. Geben Sie die Quell-Volume-ID und einen Replizierungsplan an.
   d. Erstellen eines Ziel-Volumes
2. Autorisieren Sie die Replikation auf dem Quell-Volume.
   - Geben Sie die ID des Zielvolumens an.

Die folgenden Screenshots zeigen die Konfigurationsschritte im Detail.

Am Disaster Recovery-Standort wird ein neues Datensicherungs-Volume erstellt, indem Sie Volumes auswählen und auf Datenreplizierung hinzufügen klicken. Auf der Registerkarte „Grundlagen“ müssen Sie den Namen des Volumes, den Kapazitäts-Pool und die Netzwerkinformationen angeben.

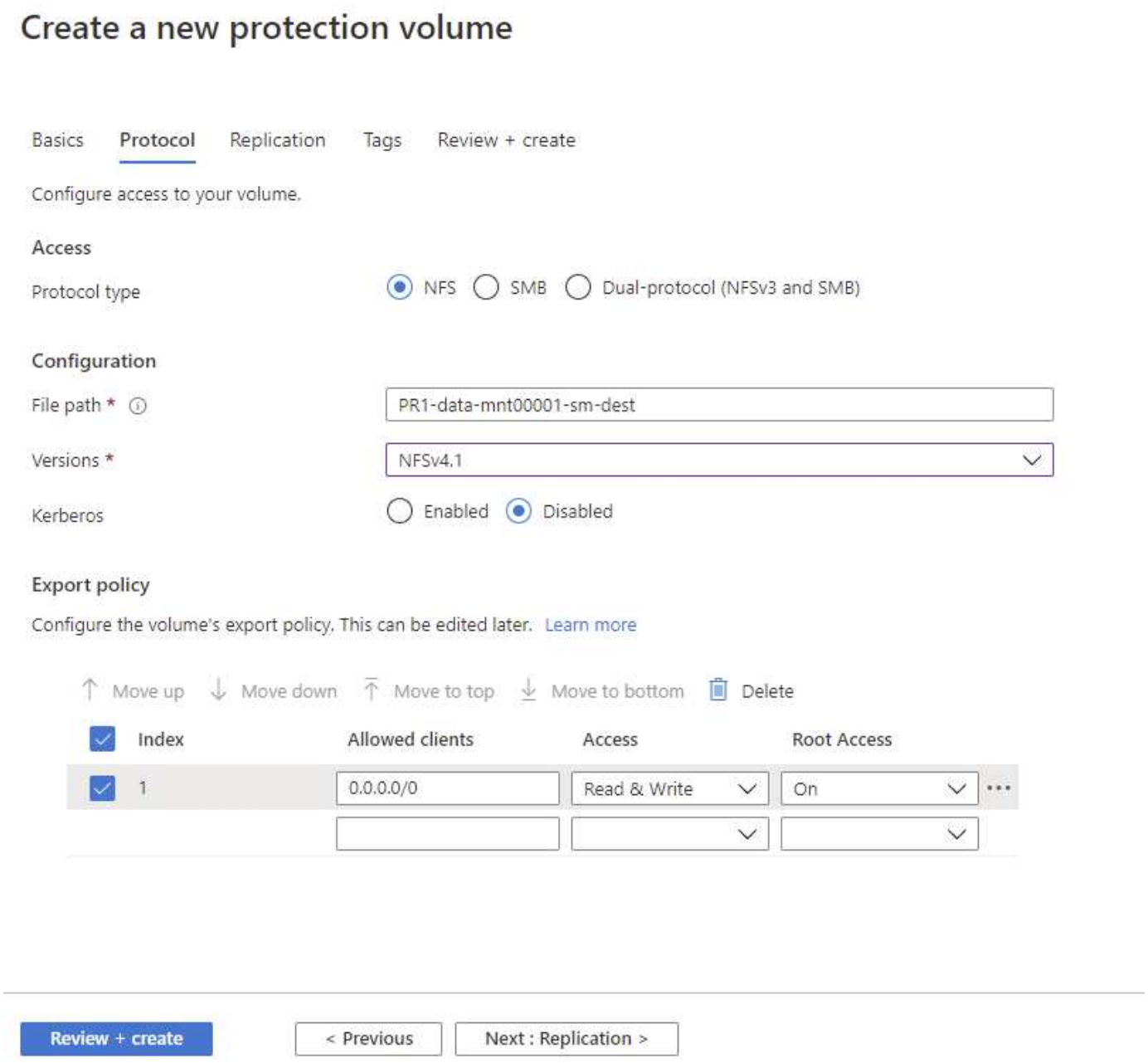
> Das Kontingent kann auf Basis der Kapazitätsanforderungen festgelegt werden, da die Volume-Performance sich nicht auf den Replizierungsprozess auswirkt. Bei einem Disaster Recovery-Failover muss die Quote an die tatsächlichen Performance-Anforderungen angepasst werden.

> Wenn der Kapazitäts-Pool mit manueller QoS konfiguriert wurde, können Sie den Durchsatz zusätzlich zu den Kapazitätsanforderungen konfigurieren. Wie oben angegeben können Sie den Durchsatz auch im normalen Betrieb mit niedrigem Wert konfigurieren und im Falle eines Disaster Recovery Failover diesen erhöhen.



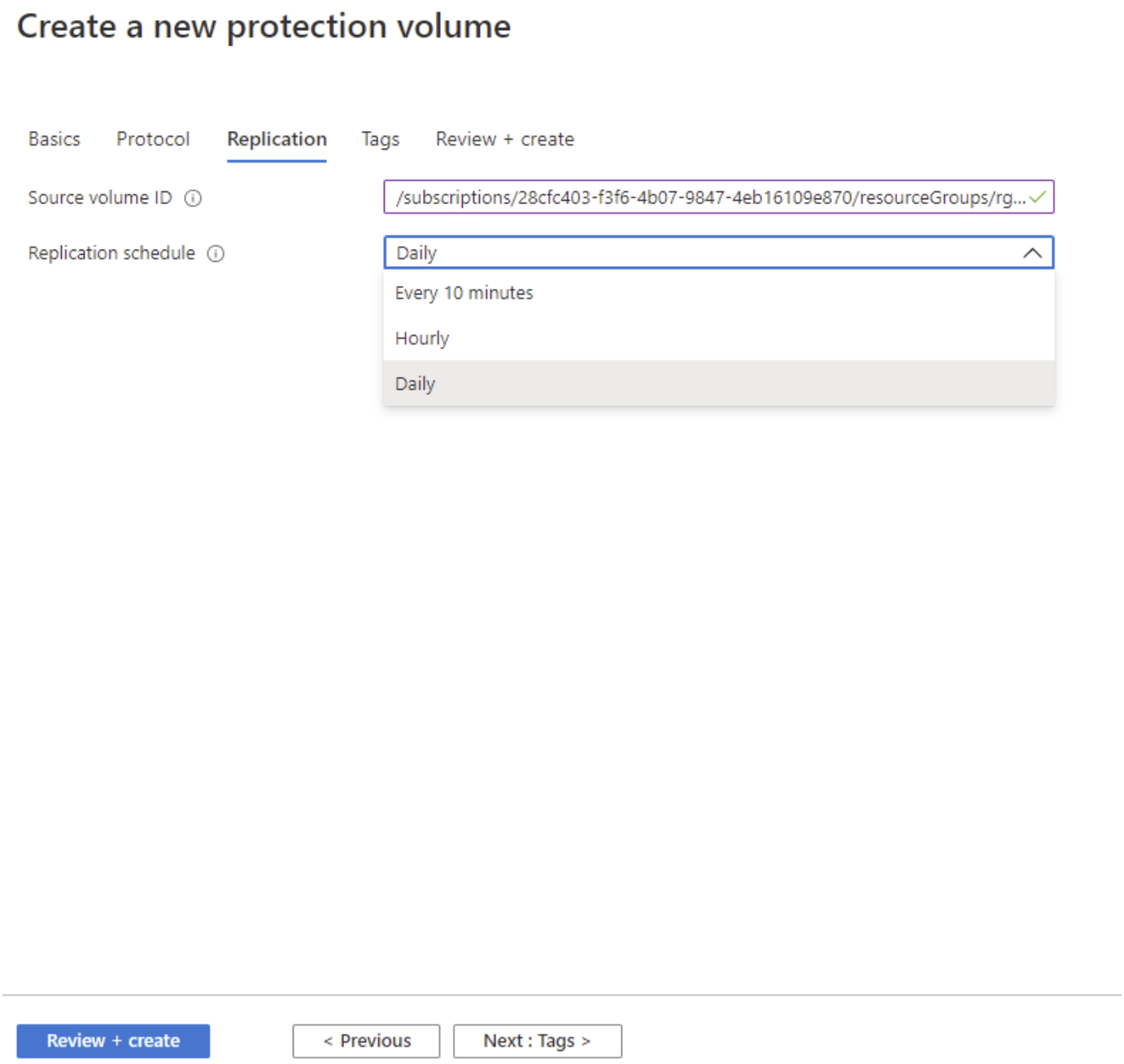
Auf der Registerkarte Protokoll müssen Sie das Netzwerkprotokoll, den Netzwerkpfad und die Exportrichtlinie angeben.

Das Protokoll muss dasselbe sein wie das für das Quell-Volume verwendete Protokoll.



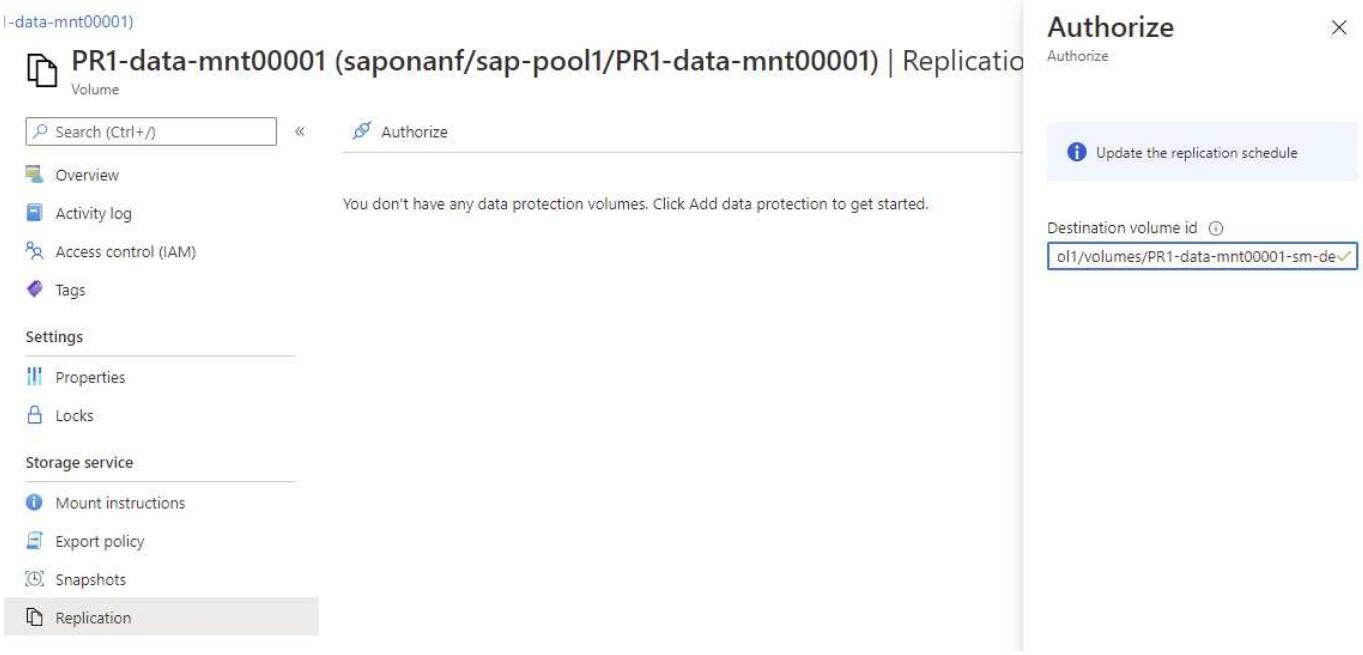
Auf der Registerkarte „Replikation“ müssen Sie die Quell-Volume-ID und den Replizierungsplan konfigurieren. Für die Datenreplizierung mit Daten-Volumes haben wir einen täglichen Replizierungszeitplan für unsere Einrichtung im Labor konfiguriert.

Die Quell-Volume-ID kann vom Bildschirm Eigenschaften des Quell-Volumes kopiert werden.



Als letzter Schritt müssen Sie die Replikation am Quell-Volume durch Angabe der ID des Ziel-Volume autorisieren.

Sie können die Ziel-Volume-ID vom Bildschirm Eigenschaften des Ziel-Volumes kopieren.



Für das freigegebene HANA und das Protokoll-Backup-Volume müssen dieselben Schritte durchgeführt werden.

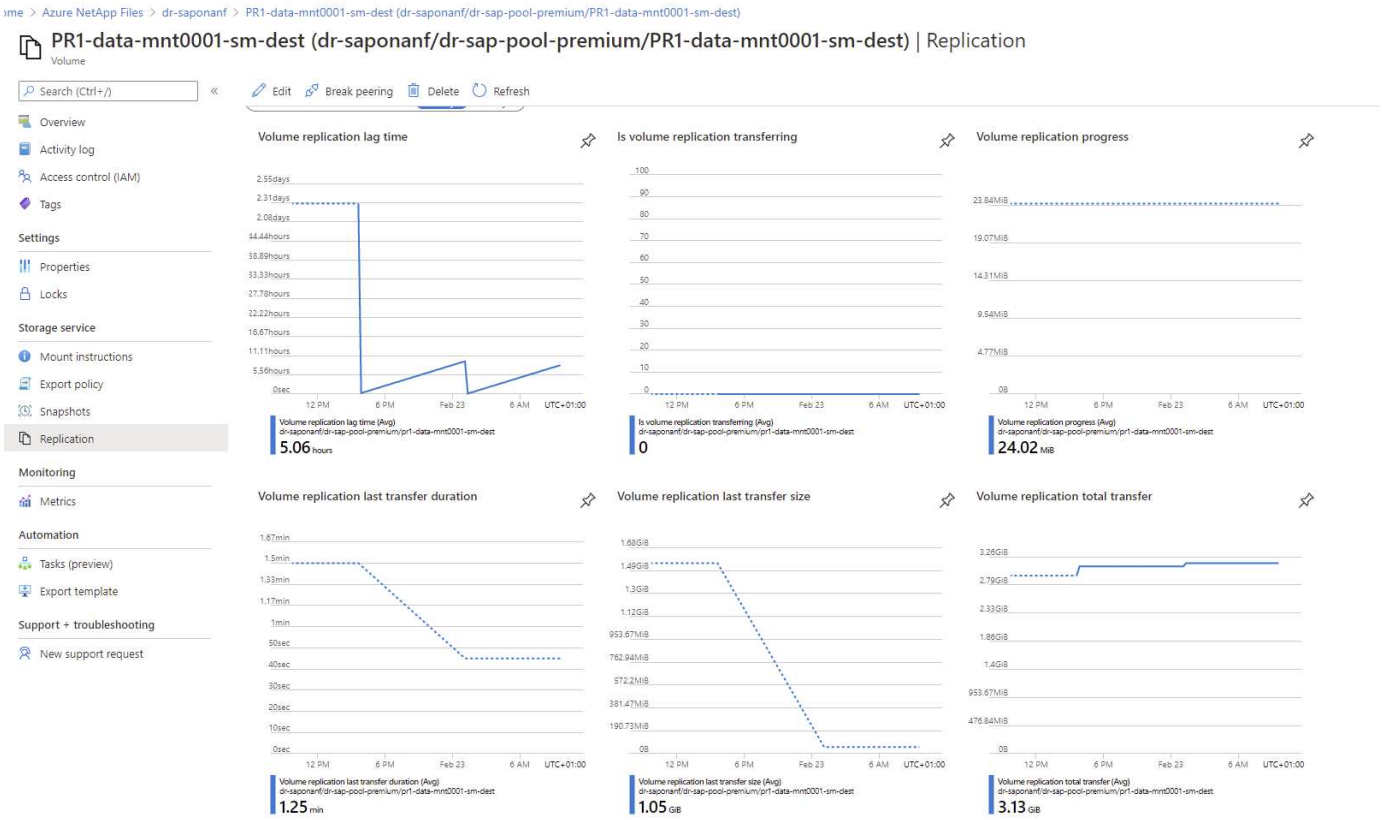
Überwachung der standortübergreifenden ANF-Replikation

Die folgenden drei Screenshots zeigen den Replikationsstatus für die Daten, Backup-Protokollierung und gemeinsam genutzte Volumes.

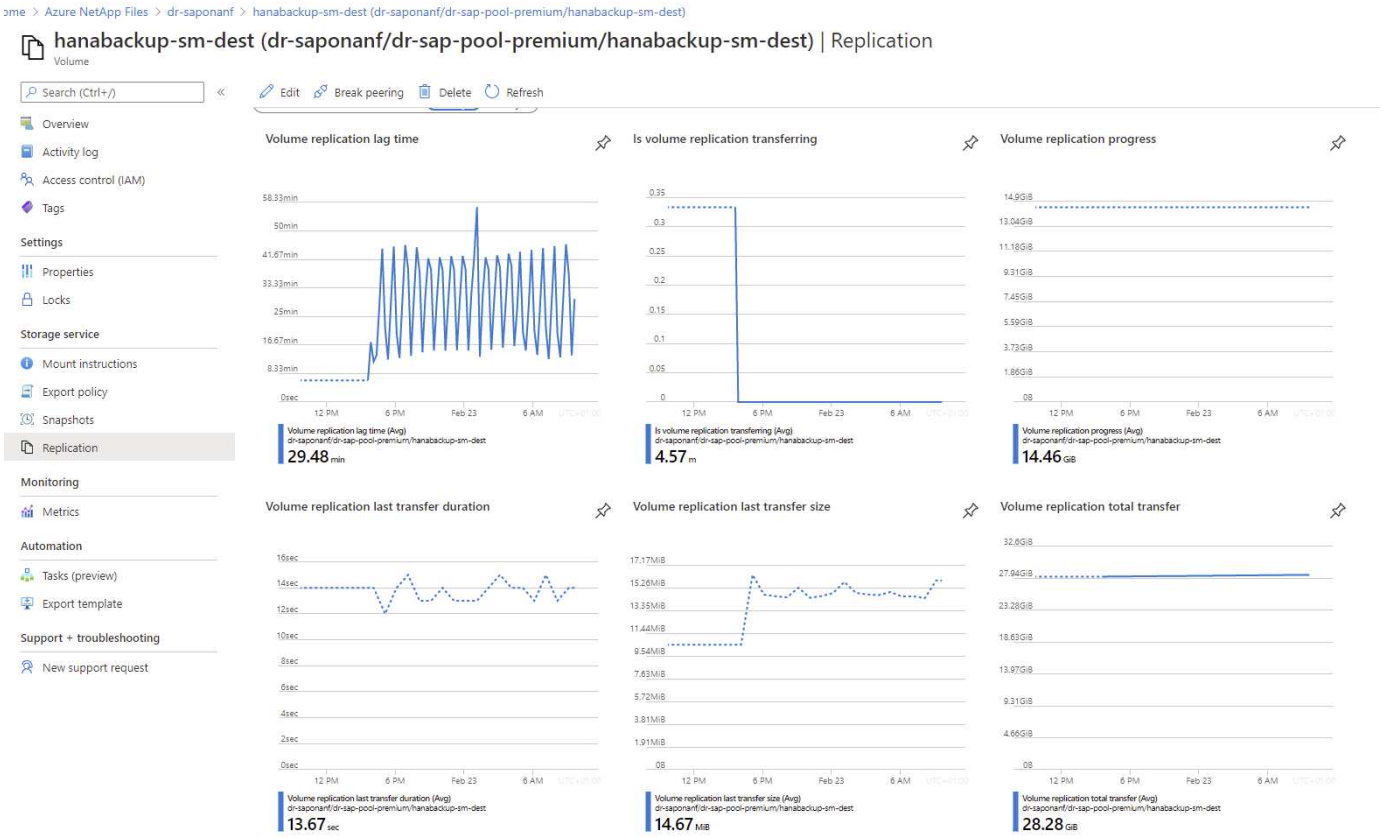
Die Verzögerung bei der Volume-Replizierung ist ein nützlicher Wert, um die RPO-Erwartungen zu verstehen. Beispielsweise zeigt die Replizierung des Backup-Volumes für das Protokoll eine maximale Verzögerungszeit von 58 Minuten, das heißt, dass der maximale RPO den gleichen Wert hat.

Die Übertragungsdauer und Übertragungsgröße bieten wertvolle Informationen zu den Bandbreitenanforderungen und ändern die Rate des replizierten Volumes.

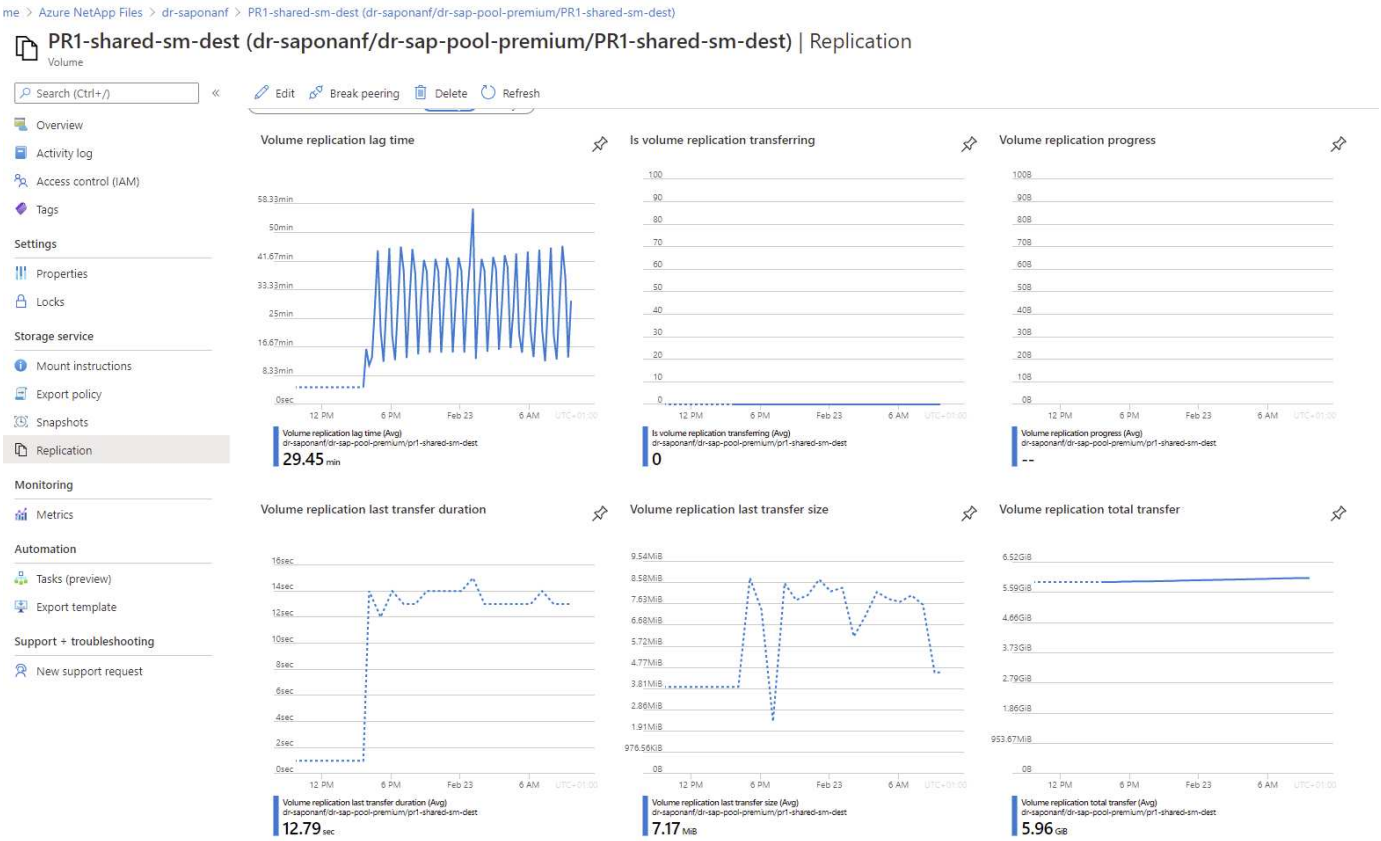
Der folgende Screenshot zeigt den Replizierungsstatus eines HANA Daten-Volumes.



Der folgende Screenshot zeigt den Replizierungsstatus eines HANA-Protokoll-Backup-Volumes.



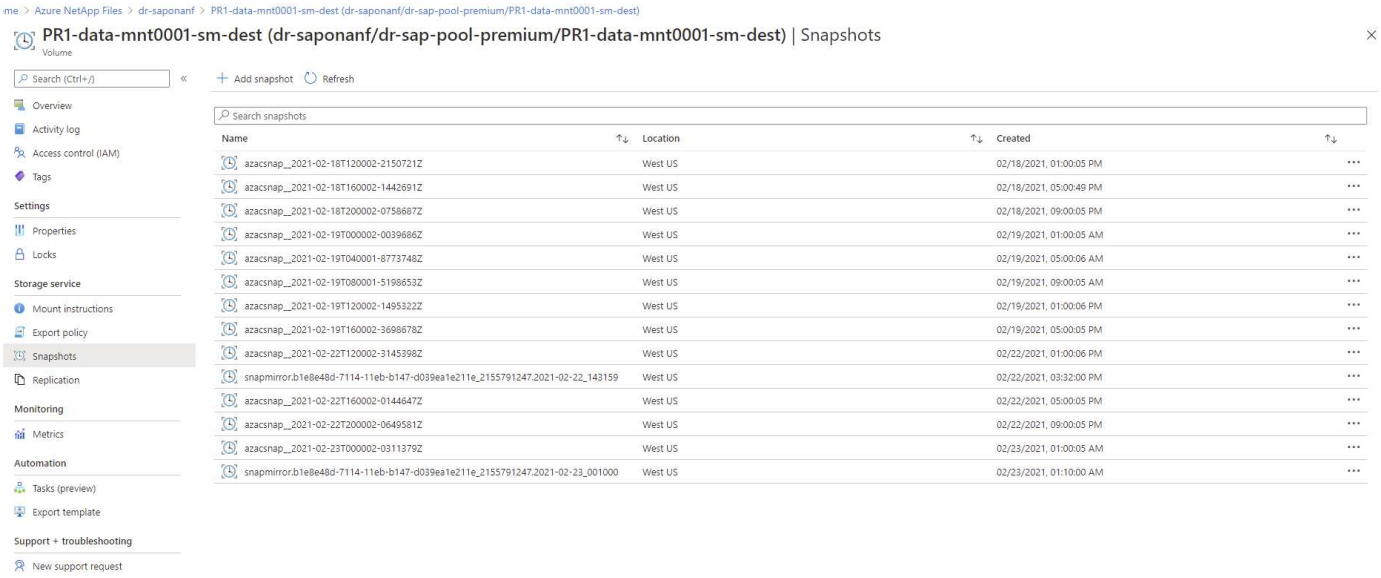
Der folgende Screenshot zeigt den Replizierungsstatus von einem Shared HANA Volume.



Replizierte Snapshot Backups

Bei jedem Replizierungs-Update vom Quell- zum Ziel-Volume werden alle Blockänderungen, die zwischen dem letzten und dem aktuellen Update stattgefunden haben, auf das Ziel-Volume repliziert. Dies umfasst auch die Snapshots, die auf dem Quell-Volume erstellt wurden. Der folgende Screenshot zeigt die Snapshots, die auf dem Zielvolume verfügbar sind. Wie bereits erwähnt, sind alle Snapshots, die vom Tool AzAcSnap erstellt wurden, applikationskonsistente Images der HANA Datenbank, die zur Ausführung eines Speicherpunktes oder einer vorwärts gerichteten Recovery verwendet werden können.

Innerhalb des Quell- und Ziel-Volume werden auch SnapMirror Snapshot Kopien erstellt, die für Resynchronisierung und Replizierungs-Updates verwendet werden. Diese Snapshot-Kopien sind aus Sicht der HANA-Datenbank nicht applikationskonsistent. Bei HANA-Recovery-Vorgängen können nur die über AzaCSnap erstellten applikationskonsistenten Snapshots verwendet werden.



Disaster Recovery-Tests

Disaster Recovery-Tests

Um eine effiziente Disaster Recovery-Strategie zu implementieren, müssen Sie den erforderlichen Workflow testen. Der Test zeigt, ob die Strategie funktioniert und ob die interne Dokumentation ausreichend ist, und ermöglicht es Administratoren auch, die erforderlichen Verfahren zu trainieren.

Die regionale ANF Replizierung ermöglicht Disaster-Recovery-Tests ohne Risiko für RTO und RPO. Disaster-Recovery-Tests können ohne Unterbrechung der Datenreplizierung durchgeführt werden.

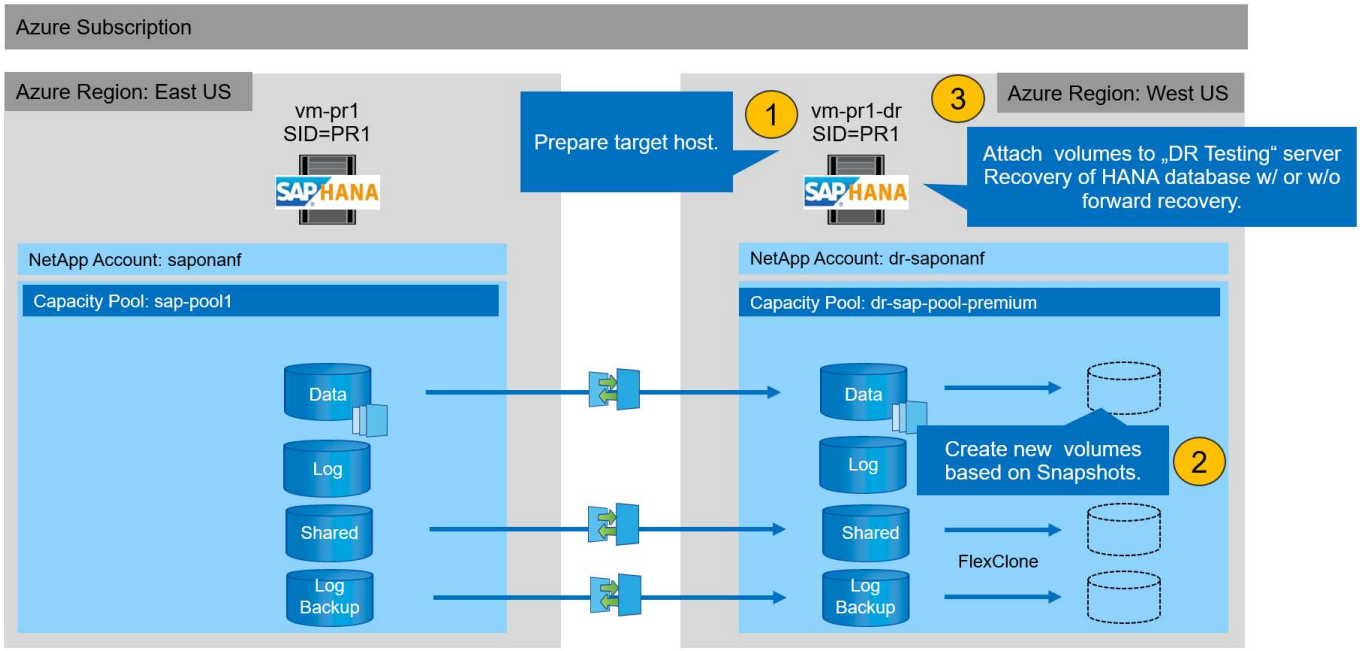
Der Workflow für Disaster Recovery-Tests nutzt die ANF-Funktionen, um auf Basis vorhandener Snapshot-Backups am Disaster-Recovery-Ziel neue Volumes zu erstellen. Siehe "Wie Azure NetApp Files Snapshots funktionieren - Microsoft Docs".

Je nachdem, ob die Backup-Replizierung des Protokolls Bestandteil der Disaster Recovery-Einrichtung ist oder nicht, unterscheiden sich die Schritte für die Disaster Recovery leicht. In diesem Abschnitt werden die Disaster Recovery-Tests für die reine Daten-Backup-Replizierung sowie für die Replizierung von Daten-Volumes in Kombination mit der Replizierung des Backup-Volumes für das Protokoll beschrieben.

Gehen Sie wie folgt vor, um Disaster-Recovery-Tests durchzuführen:

1. Bereiten Sie den Zielhost vor.
2. Erstellen neuer Volumes auf Basis von Snapshot Backups am Disaster-Recovery-Standort
3. Mounten Sie die neuen Volumes am Ziel-Host.
4. Stellen Sie die HANA Datenbank wieder her.
    - Nur Daten-Volume-Recovery.
    - Recovery mit replizierten Protokoll-Backups vorführen.

In den folgenden Abschnitten werden diese Schritte detailliert beschrieben.



Bereiten Sie den Zielhost vor

In diesem Abschnitt werden die Vorbereitungsschritte beschrieben, die auf dem Server für das Disaster-Recovery-Failover erforderlich sind.

Im normalen Betrieb wird der Zielhost normalerweise für andere Zwecke verwendet, beispielsweise als HANA QA- oder Testsystem. Daher müssen die meisten der beschriebenen Schritte bei der Ausführung von Disaster Failover-Tests ausgeführt werden. Zum anderen die relevanten Konfigurationsdateien, wie `/etc/fstab` Und `/usr/sap/sapservices`, Kann vorbereitet werden und dann in die Produktion durch einfaches Kopieren der Konfigurationsdatei. Das Disaster Recovery-Failover-Verfahren stellt sicher, dass die relevanten vorbereiteten Konfigurationsdateien korrekt konfiguriert sind.

Die Vorbereitung des Ziel-Hosts umfasst auch das Herunterfahren des HANA QA- oder Testsystems sowie das Anhalten aller Services mit `systemctl stop sapinit`.

Hostname und IP-Adresse des Zielservers

Der Hostname des Zielservers muss mit dem Hostnamen des Quellsystems identisch sein. Die IP-Adresse kann unterschiedlich sein.

Ein ordnungsgemäßes Fechten des Zielservers muss eingerichtet werden, damit er nicht mit anderen Systemen kommunizieren kann. Wenn keine ordnungsgemäße Fechten vorhanden sind, kann das geklonte Produktionssystem Daten mit anderen Produktionssystemen austauschen, was zu logisch beschädigten Daten führt.

Installieren Sie die erforderliche Software

Die SAP-Hostagent-Software muss auf dem Zielserver installiert sein. Ausführliche Informationen finden Sie im "SAP Host Agent" Im SAP-Hilfeportal.

Wenn der Host als HANA QA- oder Testsystem verwendet wird, ist die SAP-Hostagent-Software bereits installiert.

Konfiguration von Benutzern, Ports und SAP-Diensten

Die erforderlichen Anwender und Gruppen für die SAP HANA-Datenbank müssen auf dem Zielserver verfügbar sein. In der Regel wird die zentrale Benutzerverwaltung verwendet. Daher sind keine Konfigurationsschritte auf dem Zielserver erforderlich. Die erforderlichen Ports für die HANA-Datenbank müssen auf den Ziel-Hosts konfiguriert sein. Die Konfiguration kann durch Kopieren des aus dem Quellsystem kopiert werden `/etc/services` Datei auf dem Zielserver.

Die erforderlichen SAP Services-Einträge müssen auf dem Zielhost verfügbar sein. Die Konfiguration kann durch Kopieren des aus dem Quellsystem kopiert werden `/usr/sap/sapservices` Datei auf dem Zielserver. Die folgende Ausgabe zeigt die erforderlichen Einträge für die im Lab-Setup verwendete SAP HANA-Datenbank.

```
vm-pr1:~ # cat /usr/sap/sapservices
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/PR1/HDB01/exe:$LD_LIBRARY_PATH;export
LD_LIBRARY_PATH;/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
limit.descriptors=1048576
```

HANA-Protokollvolumen vorbereiten

Da das HANA-Protokoll-Volume nicht Teil der Replikation ist, muss auf dem Ziel-Host ein leeres Protokoll-Volume vorhanden sein. Das Protokoll-Volume muss dieselben Unterverzeichnisse enthalten wie das Quell-HANA-System.

```
vm-pr1:~ # ls -al /hana/log/PR1/mnt00001/
total 16
drwxrwxrwx 5 root   root   4096 Feb 19 16:20 .
drwxr-xr-x 3 root   root     22 Feb 18 13:38 ..
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00001
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00002.00003
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00003.00003
vm-pr1:~ #
```

Erstellen des Backup-Volumes für das Protokoll

Da das Quellsystem für die HANA-Protokoll-Backups mit einem separaten Volume konfiguriert ist, muss auch ein Protokoll-Backup-Volume auf dem Zielhost verfügbar sein. Ein Volume für die Protokoll-Backups muss konfiguriert und auf dem Ziel-Host gemountet werden.

Wenn die Protokollsicherung Teil der Disaster Recovery-Einrichtung ist, wird das replizierte Backup-Volume für das Protokoll auf dem Zielhost gemountet und es ist nicht erforderlich, ein zusätzliches Protokoll-Backup-Volume vorzubereiten.

Bereiten Sie Dateisystemeinhängungen vor

In der folgenden Tabelle sind die Namenskonventionen aufgeführt, die für das Lab-Setup verwendet werden. Die Volume-Namen am Disaster-Recovery-Standort sind in enthalten `/etc/fstab`.

HANA PR1-Volumes	Volumes und Unterverzeichnisse am Disaster Recovery-Standort	Bereitstellungspunkt am Zielhost
Datenvolumen	PR1-Data-mnt00001-SM-dest	/hana/Data/PR1/mnt00001
Freigegebenes Volume	PR1-shared-sm-dest/shared PR1-shared-SM-dest/usr-sap-PR1	/hana/shared /usr/sap/PR1
Backup-Volume protokollieren	Hanabackup-SM-dest	/Hanabackup

Die Mount-Punkte aus dieser Tabelle müssen auf dem Zielhost erstellt werden.

Hier sind die erforderlichen `/etc/fstab` Einträge.

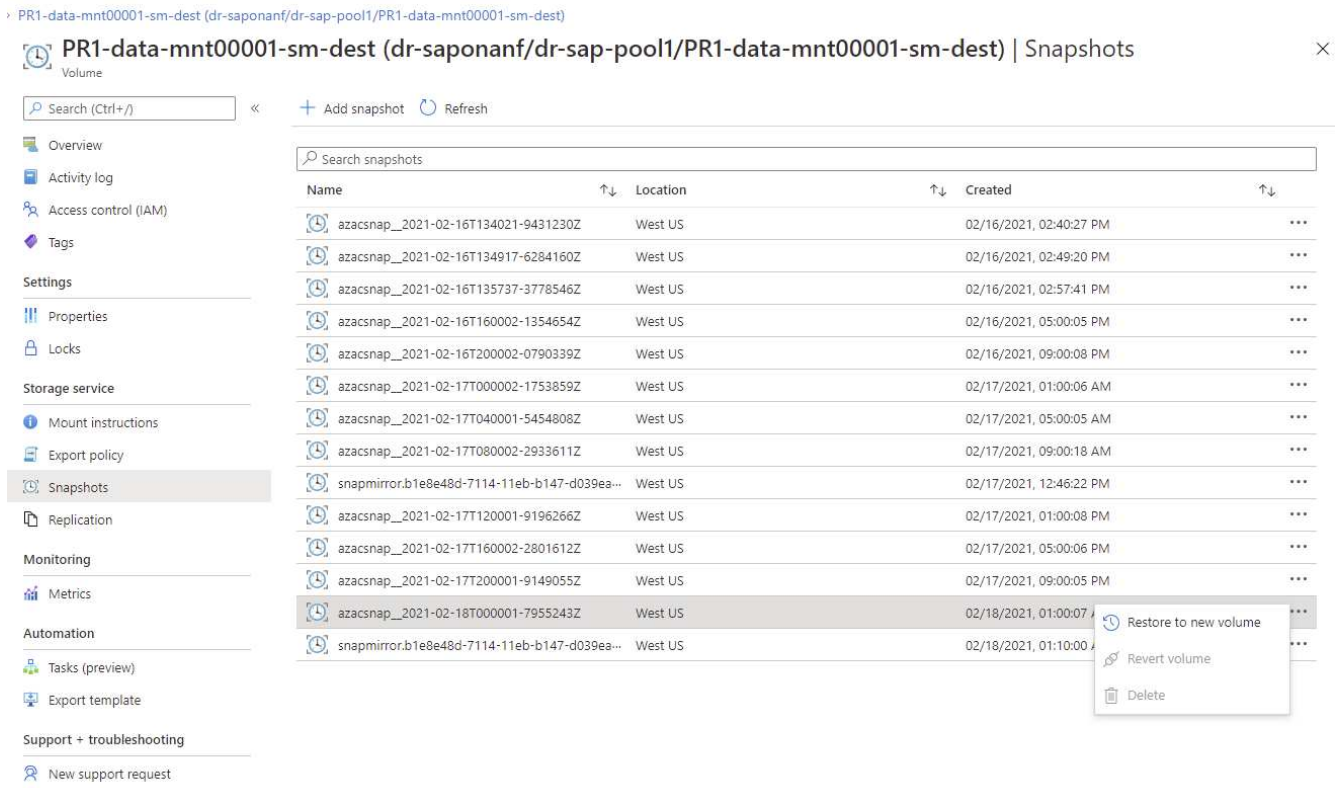
```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt0001-sm-dest /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA ANF Shared Mounts
10.0.2.4:/PR1-shared-sm-dest/hana-shared /hana/shared nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-shared-sm-dest/usr-sap-PR1 /usr/sap/PR1 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA file and log backup destination
10.0.2.4:/hanabackup-sm-dest    /hanabackup nfs
rw,vers=3,hard,timeo=600,rsize=262144,wsize=262144,nconnect=8,bg,noatime,n
olock 0 0
```

Erstellen Sie neue Volumes auf Basis von Snapshot-Backups am Disaster-Recovery-Standort

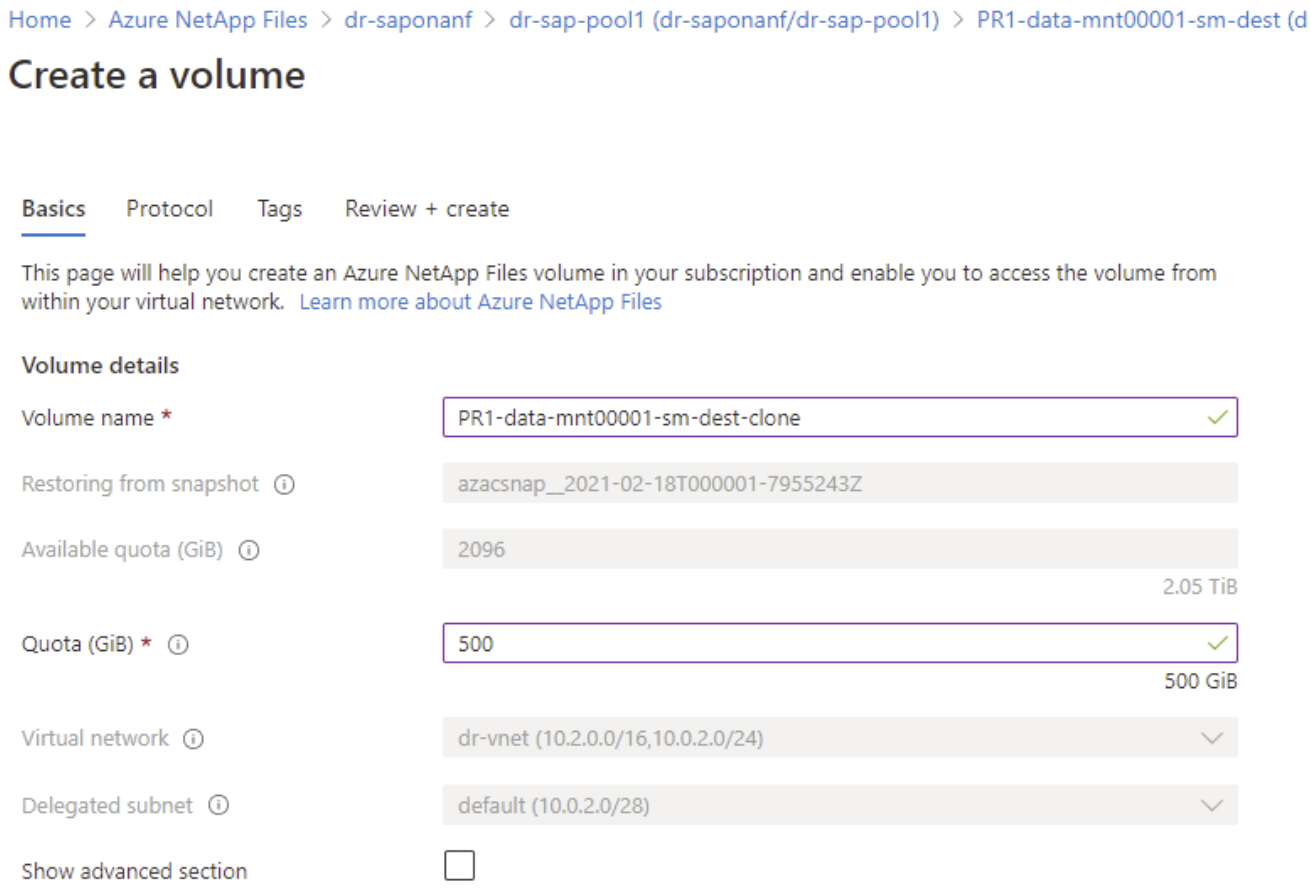
Abhängig vom Disaster Recovery Setup (mit oder ohne Log-Backup-Replikation) müssen zwei oder drei neue Volumes auf der Basis von Snapshot-Backups erstellt werden. In beiden Fällen muss ein neues Volume der Daten und das gemeinsame HANA Volume erstellt werden.

Wenn auch die Backup-Daten für das Protokoll repliziert werden, muss ein neues Volume des Backup-Volumes erstellt werden. In unserem Beispiel wurden die Daten und das Protokoll-Backup-Volume an den Disaster Recovery-Standort repliziert. In den folgenden Schritten wird das Azure-Portal verwendet.

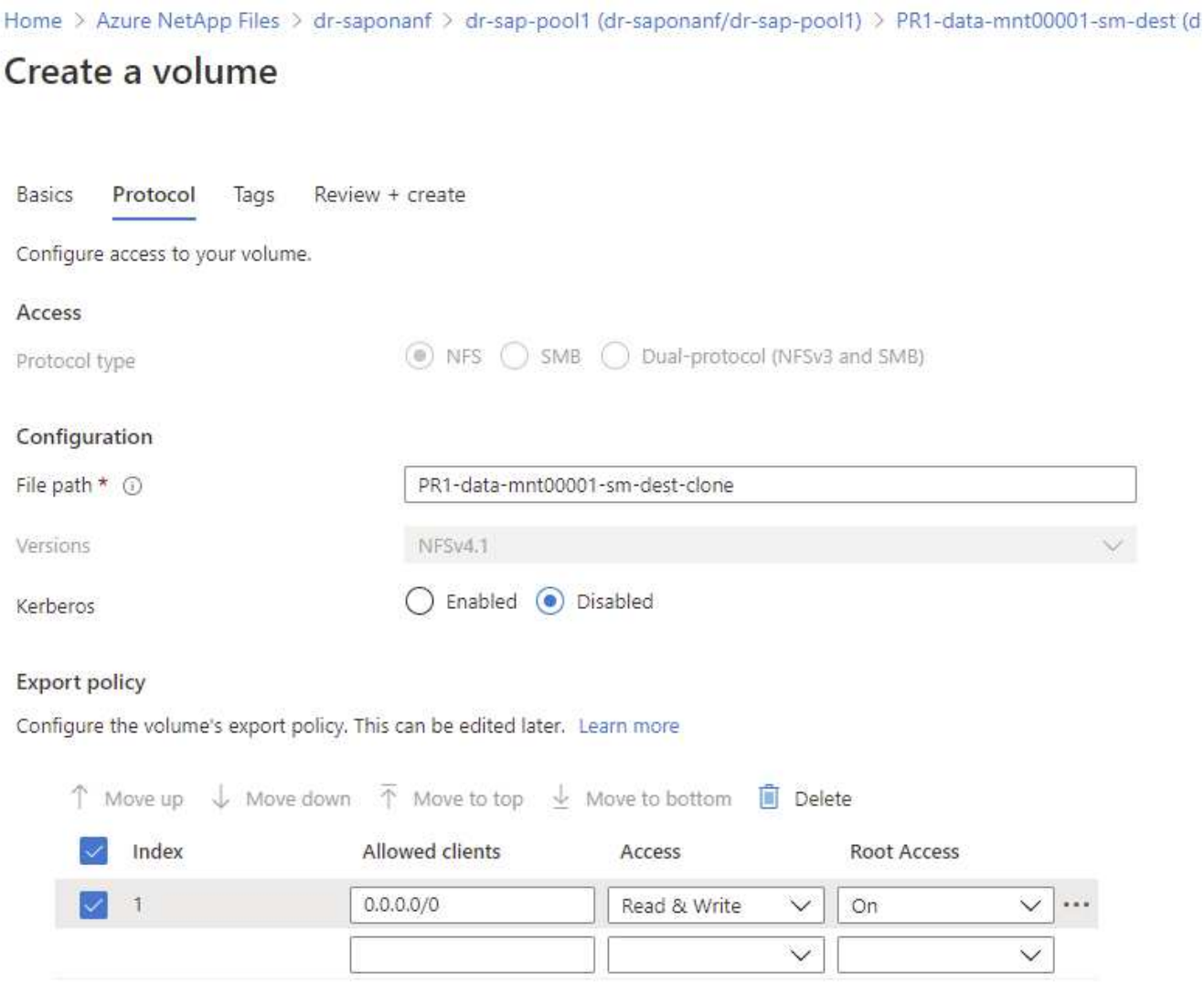
1. Eines der applikationskonsistenten Snapshot-Backups wird als Quelle für das neue Volume des HANA-Daten-Volumes ausgewählt. Restore to New Volume ist ausgewählt, um ein neues Volume basierend auf der Snapshot-Sicherung zu erstellen.



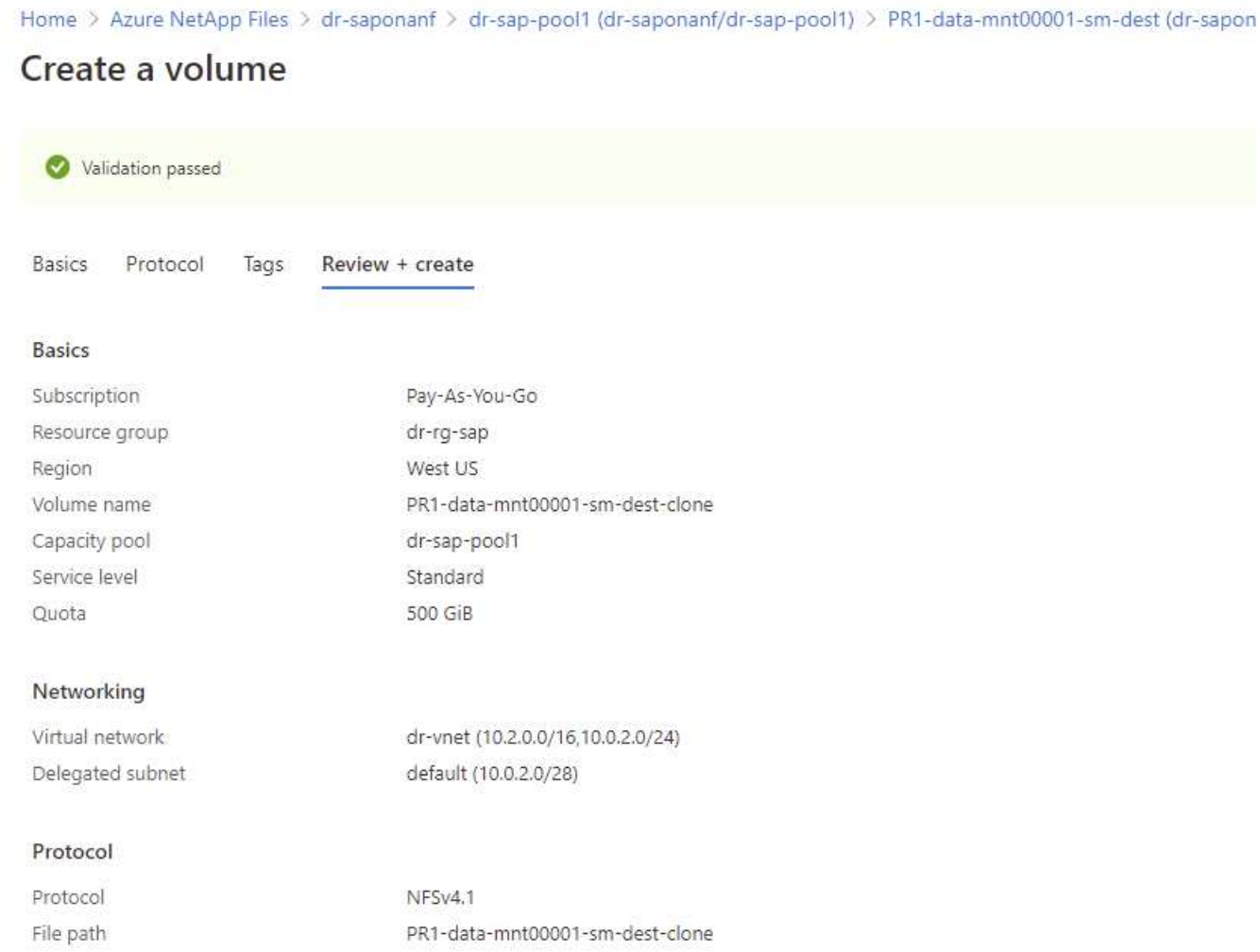
2. Der neue Volume-Name und die neue Quote müssen in der Benutzeroberfläche angegeben werden.



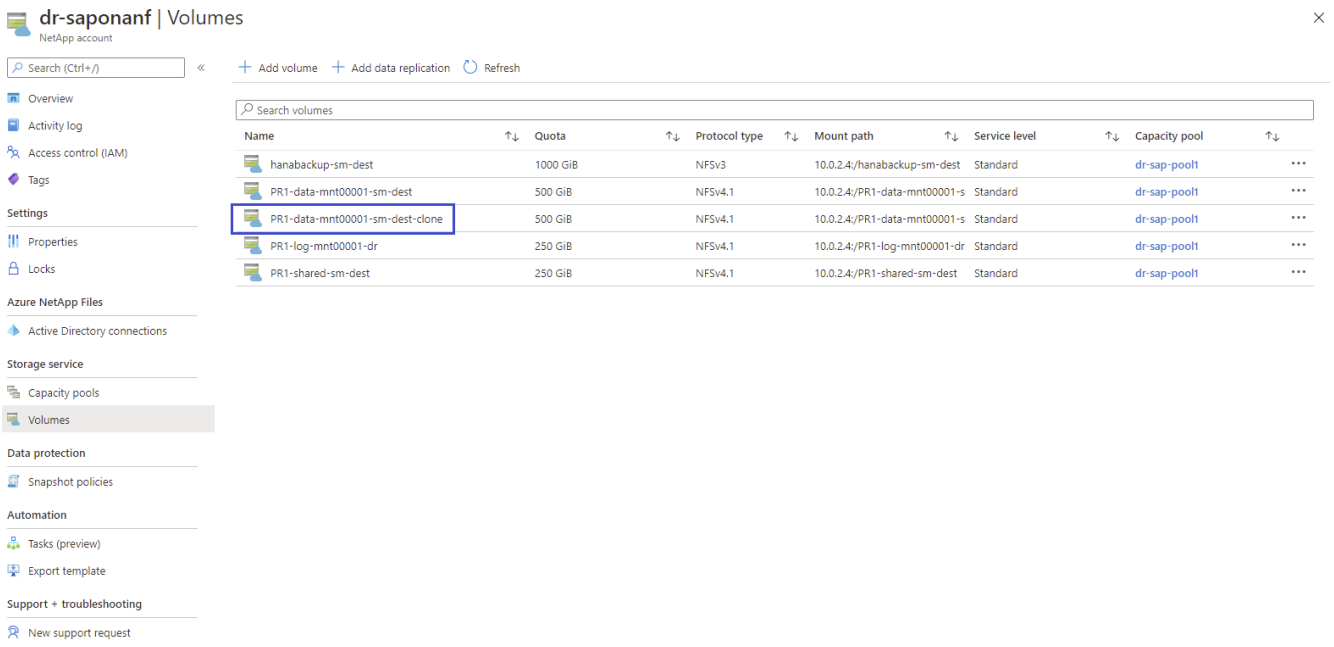
3. Auf der Registerkarte Protokoll werden der Dateipfad und die Exportrichtlinie konfiguriert.



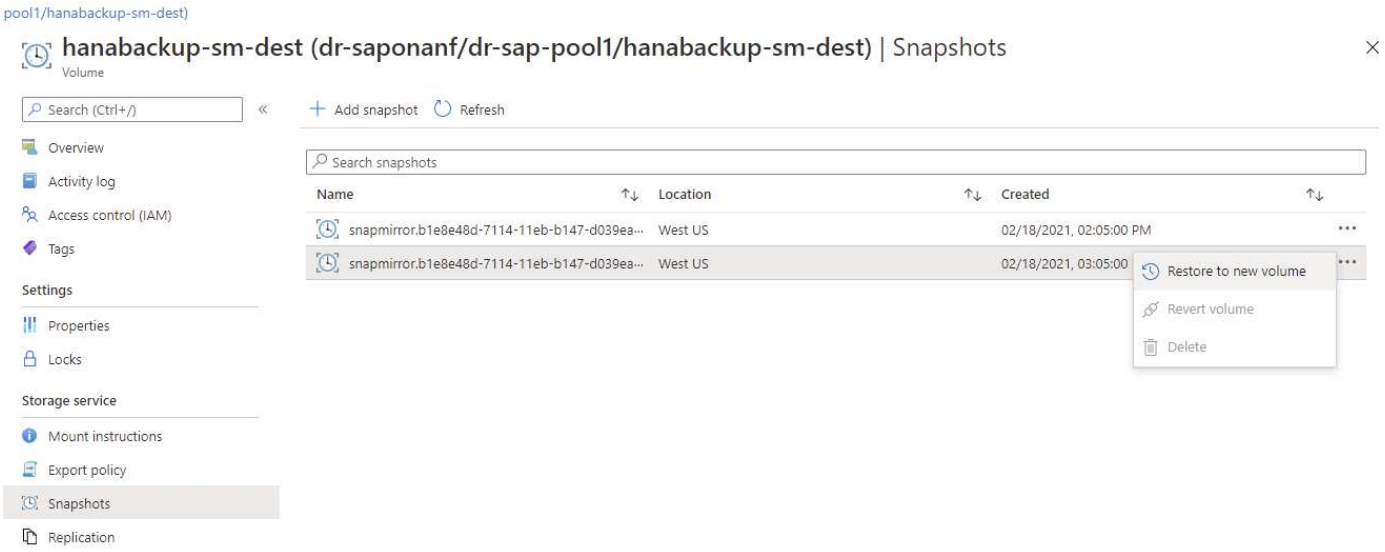
4. Der Bildschirm Erstellen und Prüfen fasst die Konfiguration zusammen.



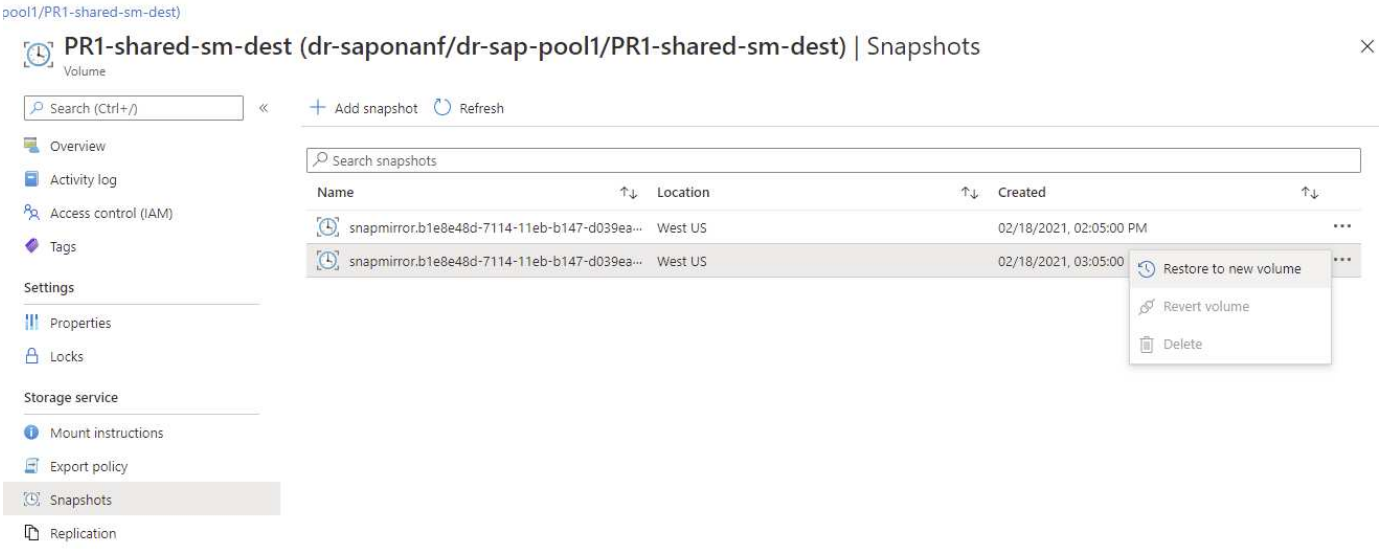
5. Auf Basis des HANA-Snapshot-Backups wurde jetzt ein neues Volume erstellt.



Die gleichen Schritte müssen nun für das freigegebene HANA und das Protokoll-Backup-Volumen, wie in den folgenden beiden Screenshots dargestellt, durchgeführt werden. Da keine zusätzlichen Snapshots für das HANA Shared-Backup-Volume und das Log-Backup-Volume erstellt wurden, muss die neueste SnapMirror Snapshot Kopie als Quelle für das neue Volume ausgewählt werden. Das sind unstrukturierte Daten, und die SnapMirror Snapshot Kopie kann für diesen Anwendungsfall genutzt werden.



Der folgende Screenshot zeigt das HANA Shared Volume, das auf dem neuen Volume wiederhergestellt ist.



Wenn ein Kapazitäts-Pool mit einer Tier mit niedriger Performance verwendet wurde, müssen die Volumes nun in einen Kapazitäts-Pool verschoben werden, der die erforderliche Performance bietet.

Alle drei neuen Volumes sind jetzt verfügbar und können auf dem Zielhost eingebunden werden.

Mounten Sie die neuen Volumes am Ziel-Host

Die neuen Volumes können jetzt auf Basis des auf dem Zielhost eingebunden werden `/etc/fstab` Datei zuvor erstellt.

```
vm-pr1:~ # mount -a
```

Die folgende Ausgabe zeigt die erforderlichen Dateisysteme.

```
vm-pr1:/hana/data/PR1/mnt00001/hdb00001 # df
Filesystem                                          1K-blocks     Used
Available Use% Mounted on
devtmpfs                                              8190344        8
8190336   1% /dev
tmpfs                                                12313116        0
12313116   0% /dev/shm
tmpfs                                                 8208744    17292
8191452   1% /run
tmpfs                                                 8208744        0
8208744   0% /sys/fs/cgroup
/dev/sda4                                            29866736  2438052
27428684   9% /
/dev/sda3                                             1038336   101520
936816  10% /boot
/dev/sda2                                              524008     1072
522936   1% /boot/efi
/dev/sdb1                                            32894736    49176
31151560   1% /mnt
tmpfs                                                 1641748        0
1641748   0% /run/user/0
10.0.2.4:/PR1-log-mnt00001-dr                    107374182400      256
107374182144   1% /hana/log/PR1/mnt00001
10.0.2.4:/PR1-data-mnt00001-sm-dest-clone      107377026560  6672640
107370353920   1% /hana/data/PR1/mnt00001
10.0.2.4:/PR1-shared-sm-dest-clone/hana-shared 107377048320 11204096
107365844224   1% /hana/shared
10.0.2.4:/PR1-shared-sm-dest-clone/usr-sap-PR1 107377048320 11204096
107365844224   1% /usr/sap/PR1
10.0.2.4:/hanabackup-sm-dest-clone             107379429120 35293440
107344135680   1% /hanabackup
```

HANA Datenbank-Recovery

Im Folgenden werden die Schritte für das HANA-Datenbank-Recovery aufgeführt

Starten Sie die erforderlichen SAP-Dienste.

```
vm-pr1:~ # systemctl start sapinit
```

Die folgende Ausgabe zeigt die erforderlichen Prozesse.

```
vm-pr1:/ # ps -ef | grep sap
root     23101     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saphostexec pf=/usr/sap/hostctrl/exe/host_profile
pr1adm   23191     1  3 11:29 ?        00:00:00
/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
sapadm   23202     1  5 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/hostctrl/exe/host_profile -D
root     23292     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saposcol -l -w60
pf=/usr/sap/hostctrl/exe/host_profile
root     23359  2597  0 11:29 pts/1    00:00:00 grep --color=auto sap
```

In den folgenden Abschnitten wird der Recovery-Prozess mit und ohne Forward Recovery mit den replizierten Log-Backups beschrieben. Die Recovery wird mit dem HANA-Recovery-Skript für die Systemdatenbank und hdbsql-Befehle für die Mandanten-Datenbank ausgeführt.

Recovery zum aktuellen Backup-Speicherpunkt für das HANA-Datenvolumen

Die Wiederherstellung zum neuesten Backup savepoint wird mit folgenden Befehlen als User pr1adm ausgeführt:

- Systemdatenbank

```
recoverSys.py --command "RECOVER DATA USING SNAPSHOT CLEAR LOG”
```

- Mandantendatenbank

```
Within hdbsql: RECOVER DATA FOR PR1 USING SNAPSHOT CLEAR LOG
```

Sie können auch HANA Studio oder Cockpit verwenden, um die Wiederherstellung des Systems und der Mandanten-Datenbank auszuführen.

Die folgende Befehlsausgabe zeigt die Ausführung der Wiederherstellung.

Recovery der Systemdatenbank

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py
--command="RECOVER DATA USING SNAPSHOT CLEAR LOG"
[139702869464896, 0.008] >> starting recoverSys (at Fri Feb 19 14:32:16
2021)
[139702869464896, 0.008] args: ()
[139702869464896, 0.009] keys: {'command': 'RECOVER DATA USING SNAPSHOT
CLEAR LOG'}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: ============2021-02-19 14:32:16 ============
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-19 14:32:16
stopped system: 2021-02-19 14:32:16
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-19 14:32:21
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-19T14:32:56+00:00  P0027646      177bab4d610 INFO    RECOVERY
RECOVER DATA finished successfully
recoverSys finished successfully: 2021-02-19 14:32:58
[139702869464896, 42.017] 0
[139702869464896, 42.017] << ending recoverSys, rc = 0 (RC_TEST_OK), after
42.009 secs
pr1adm@vm-pr1:/usr/sap/PR1/HDB01>
```

Recovery von Mandanten-Datenbanken

Wenn für den Benutzer pr1adm am Quellsystem kein Benutzerspeicherschlüssel erstellt wurde, muss auf dem Zielsystem ein Schlüssel erstellt werden. Der im Schlüssel konfigurierte Datenbankbenutzer muss über Berechtigungen zur Ausführung von Mandanten-Recovery-Vorgängen verfügen.

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbuserstore set PR1KEY vm-pr1:30113
<backup-user> <password>
```

Die Mandantenwiederherstellung wird jetzt mit hdbsql ausgeführt.

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql SYSTEMDB=> RECOVER DATA FOR PR1 USING SNAPSHOT CLEAR LOG
0 rows affected (overall time 66.973089 sec; server time 66.970736 sec)
hdbsql SYSTEMDB=>
```

Die HANA-Datenbank ist jetzt betriebsbereit, und der Disaster-Recovery-Workflow für die HANA-Datenbank wurde getestet.

Recovery mit vorwärtsgerichteten Recovery mithilfe von Log-/Katalog-Backups

Log-Backups und der HANA-Backup-Katalog werden aus dem Quellsystem repliziert.

Die Wiederherstellung mit allen verfügbaren Log-Backups wird mit den folgenden Befehlen als Benutzer pr1adm ausgeführt:

- Systemdatenbank

```
recoverSys.py --command "RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT"
```

- Mandantendatenbank

```
Within hdbsql: RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
```

Um eine Wiederherstellung mit allen verfügbaren Protokollen durchzuführen, können Sie jederzeit als Zeitstempel in der Recovery-Anweisung verwenden.

Sie können auch HANA Studio oder Cockpit verwenden, um die Wiederherstellung des Systems und der Mandanten-Datenbank auszuführen.

Die folgende Befehlsausgabe zeigt die Ausführung der Wiederherstellung.

Recovery der Systemdatenbank

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py --command
"RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20 00:00:00' CLEAR LOG USING
SNAPSHOT"
[140404915394368, 0.008] >> starting recoverSys (at Fri Feb 19 16:06:40
2021)
[140404915394368, 0.008] args: ()
[140404915394368, 0.008] keys: {'command': "RECOVER DATABASE UNTIL
TIMESTAMP '2021-02-20 00:00:00' CLEAR LOG USING SNAPSHOT"}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: ============2021-02-19 16:06:40 ============
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-19 16:06:40
stopped system: 2021-02-19 16:06:41
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-19 16:06:46
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-19T16:07:19+00:00  P0009897      177bb0b4416 INFO    RECOVERY
RECOVER DATA finished successfully, reached timestamp 2021-02-
19T15:17:33+00:00, reached log position 38272960
recoverSys finished successfully: 2021-02-19 16:07:20
[140404915394368, 39.757] 0
[140404915394368, 39.758] << ending recoverSys, rc = 0 (RC_TEST_OK), after
39.749 secs
```

Recovery von Mandanten-Datenbanken

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit

hdbsql SYSTEMDB=> RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
0 rows affected (overall time 63.791121 sec; server time 63.788754 sec)

hdbsql SYSTEMDB=>
```

Die HANA-Datenbank ist jetzt betriebsbereit, und der Disaster-Recovery-Workflow für die HANA-Datenbank wurde getestet.

Überprüfen Sie die Konsistenz der neuesten Protokoll-Backups

Da die Volume-Replizierung für das Protokoll unabhängig vom von dem von der SAP HANA Datenbank ausgeführten Backup-Prozess durchgeführt wird, können am Disaster Recovery-Standort inkonsistente Backup-Dateien für Protokolle vorhanden sein. Nur die letzten Backup-Dateien für Protokolle sind möglicherweise inkonsistent und diese Dateien sollten überprüft werden, bevor eine Weiterleitung der Recovery am Disaster Recovery-Standort mithilfe der erfolgt `hdbbackupcheck` Werkzeug.

Wenn der `hdbbackupcheck` Tool meldet Fehler bei den letzten Protokollsicherungen muss der neueste Satz von Protokollsicherungen entfernt oder gelöscht werden.

```
pr1adm@hana-10: > hdbbackupcheck
/hanabackup/PR1/log/SYSTEMDB/log_backup_0_0_0_0.1589289811148
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivecache'
Backup '/mnt/log-backup/SYSTEMDB/log_backup_0_0_0_0.1589289811148'
successfully checked.
```

Die Prüfung muss für die aktuellen Log-Backup-Dateien des Systems und der Mandanten-Datenbank ausgeführt werden.

Wenn der `hdbbackupcheck` Tool meldet Fehler bei den letzten Protokollsicherungen muss der neueste Satz von Protokollsicherungen entfernt oder gelöscht werden.

Disaster-Recovery-Failover

Disaster-Recovery-Failover

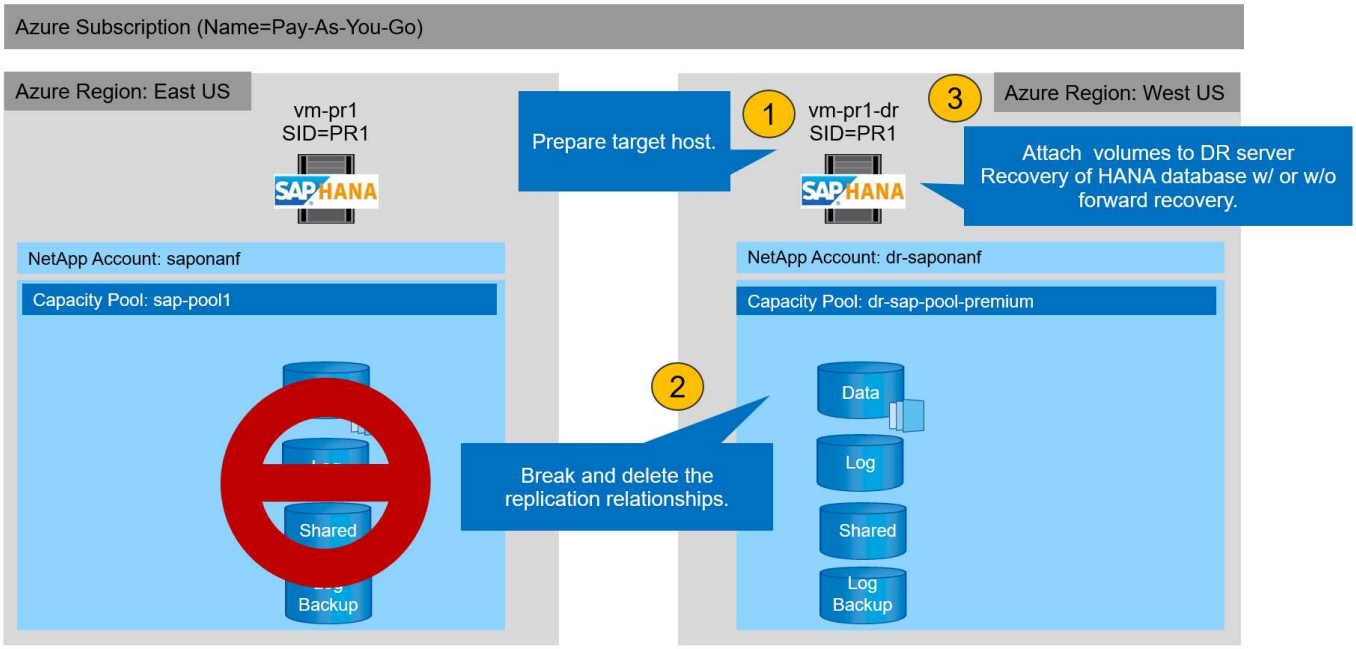
Je nachdem, ob die Backup-Replizierung des Protokolls Teil der Disaster Recovery-Einrichtung ist, unterscheiden sich die Schritte für Disaster Recovery leicht. In diesem Abschnitt wird das Disaster Recovery Failover für die reine Daten-Backup-Replizierung sowie für die Replizierung von Daten-Volumes in Kombination mit der Replizierung des Backup-Volumes für das Protokoll beschrieben.

Um Disaster Recovery-Failover auszuführen, gehen Sie wie folgt vor:

1. Bereiten Sie den Zielhost vor.
2. Brechen Sie die Replikationsbeziehungen auf und löschen Sie sie.
3. Wiederherstellung des Datenvolumens im letzten applikationskonsistenten Snapshot-Backup
4. Mounten Sie die Volumes am Ziel-Host.
5. Stellen Sie die HANA Datenbank wieder her.
    - Nur Daten-Volume-Recovery.
    - Recovery mit replizierten Protokoll-Backups vorführen.

In den folgenden Abschnitten werden diese Schritte detailliert beschrieben und die folgende Abbildung zeigt

Disaster-Failover-Tests.



Bereiten Sie den Zielhost vor

In diesem Abschnitt werden die Vorbereitungsschritte beschrieben, die auf dem Server für das Disaster-Recovery-Failover erforderlich sind.

Im normalen Betrieb wird der Zielhost normalerweise für andere Zwecke verwendet, beispielsweise als HANA QA- oder Testsystem. Daher müssen die meisten der beschriebenen Schritte bei der Ausführung von Disaster Failover-Tests ausgeführt werden. Zum anderen die relevanten Konfigurationsdateien, wie `/etc/fstab` Und `/usr/sap/sapservices`, Kann vorbereitet werden und dann in die Produktion durch einfaches Kopieren der Konfigurationsdatei. Das Disaster Recovery-Failover-Verfahren stellt sicher, dass die relevanten vorbereiteten Konfigurationsdateien korrekt konfiguriert sind.

Die Vorbereitung des Ziel-Hosts umfasst auch das Herunterfahren des HANA QA- oder Testsystems sowie das Anhalten aller Services mit `systemctl stop sapinit`.

Hostname und IP-Adresse des Zielservers

Der Hostname des Zielservers muss mit dem Hostnamen des Quellsystems identisch sein. Die IP-Adresse kann unterschiedlich sein.

> Ein ordnungsgemäßes Fechten des Zielservers muss eingerichtet werden, damit er nicht mit anderen Systemen kommunizieren kann. Wenn keine ordnungsgemäße Fechten vorhanden sind, kann das geklonte Produktionssystem Daten mit anderen Produktionssystemen austauschen, was zu logisch beschädigten Daten führt.

Installieren Sie die erforderliche Software

Die SAP-Hostagent-Software muss auf dem Zielserver installiert sein. Ausführliche Informationen finden Sie im "SAP Host Agent" Im SAP-Hilfeportal.

Wenn der Host als HANA QA- oder Testsystem verwendet wird, ist die SAP-Hostagent-Software bereits installiert.

Konfiguration von Benutzern, Ports und SAP-Diensten

Die erforderlichen Anwender und Gruppen für die SAP HANA-Datenbank müssen auf dem Zielserver verfügbar sein. In der Regel wird die zentrale Benutzerverwaltung verwendet. Daher sind keine Konfigurationsschritte auf dem Zielserver erforderlich. Die erforderlichen Ports für die HANA-Datenbank müssen auf den Ziel-Hosts konfiguriert sein. Die Konfiguration kann durch Kopieren des aus dem Quellsystem kopiert werden `/etc/services` Datei auf dem Zielserver.

Die erforderlichen SAP Services-Einträge müssen auf dem Zielhost verfügbar sein. Die Konfiguration kann durch Kopieren des aus dem Quellsystem kopiert werden `/usr/sap/sapservices` Datei auf dem Zielserver. Die folgende Ausgabe zeigt die erforderlichen Einträge für die im Lab-Setup verwendete SAP HANA-Datenbank.

```
vm-pr1:~ # cat /usr/sap/sapservices
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/PR1/HDB01/exe:$LD_LIBRARY_PATH;export
LD_LIBRARY_PATH;/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
limit.descriptors=1048576
```

HANA-Protokollvolumen vorbereiten

Da das HANA-Protokoll-Volume nicht Teil der Replikation ist, muss auf dem Ziel-Host ein leeres Protokoll-Volume vorhanden sein. Das Protokoll-Volume muss dieselben Unterverzeichnisse enthalten wie das Quell-HANA-System.

```
vm-pr1:~ # ls -al /hana/log/PR1/mnt00001/
total 16
drwxrwxrwx 5 root   root   4096 Feb 19 16:20 .
drwxr-xr-x 3 root   root     22 Feb 18 13:38 ..
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00001
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00002.00003
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00003.00003
vm-pr1:~ #
```

Erstellen des Backup-Volumes für das Protokoll

Da das Quellsystem für die HANA-Protokoll-Backups mit einem separaten Volume konfiguriert ist, muss auch ein Protokoll-Backup-Volume auf dem Zielhost verfügbar sein. Ein Volume für die Protokoll-Backups muss konfiguriert und auf dem Ziel-Host gemountet werden.

Wenn die Protokollsicherung Teil der Disaster Recovery-Einrichtung ist, wird das replizierte Backup-Volume für das Protokoll auf dem Zielhost gemountet und es ist nicht erforderlich, ein zusätzliches Protokoll-Backup-Volume vorzubereiten.

Bereiten Sie Dateisystemeinhängungen vor

In der folgenden Tabelle sind die Namenskonventionen aufgeführt, die für das Lab-Setup verwendet werden. Die Volume-Namen am Disaster-Recovery-Standort sind in enthalten `/etc/fstab`.

HANA PR1-Volumes	Volumes und Unterverzeichnisse am Disaster Recovery-Standort	Bereitstellungspunkt am Zielhost
Datenvolumen	PR1-Data-mnt00001-SM-dest	/hana/Data/PR1/mnt00001
Freigegebenes Volume	PR1-shared-sm-dest/shared PR1-shared-SM-dest/usr-sap-PR1	/hana/shared /usr/sap/PR1
Backup-Volume protokollieren	Hanabackup-SM-dest	/Hanabackup

Die Mount-Punkte aus dieser Tabelle müssen auf dem Zielhost erstellt werden.

Hier sind die erforderlichen `/etc/fstab` Einträge.

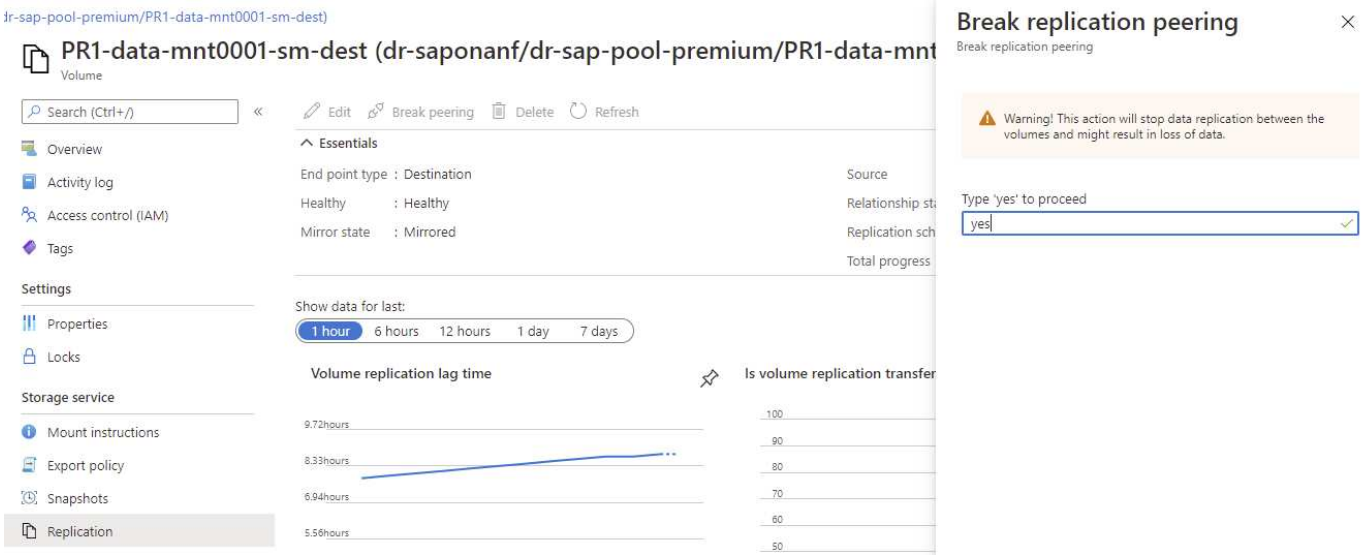
```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt0001-sm-dest /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA ANF Shared Mounts
10.0.2.4:/PR1-shared-sm-dest/hana-shared /hana/shared nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-shared-sm-dest/usr-sap-PR1 /usr/sap/PR1 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA file and log backup destination
10.0.2.4:/hanabackup-sm-dest    /hanabackup nfs
rw,vers=3,hard,timeo=600,rsize=262144,wsize=262144,nconnect=8,bg,noatime,n
olock 0 0
```

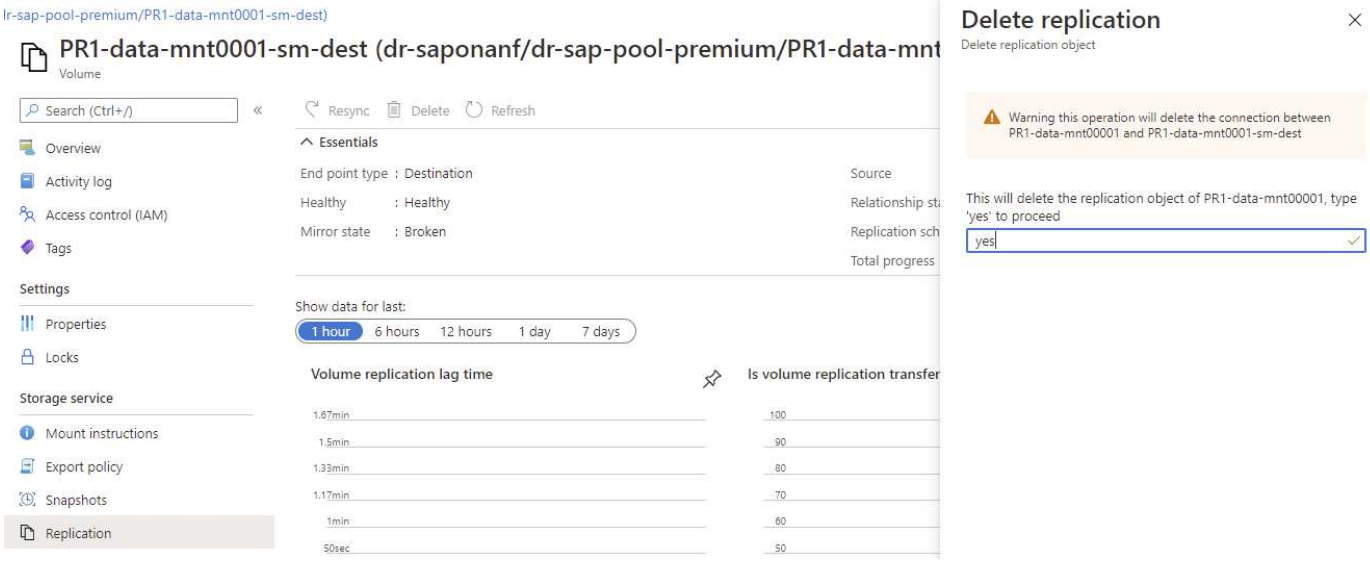
Peering der Replizierung unterbrechen und löschen

Im Falle eines Disaster-Failovers müssen die Ziel-Volumes unterbrochen werden, damit der Zielhost die Volumes für Lese- und Schreibvorgänge mounten kann.

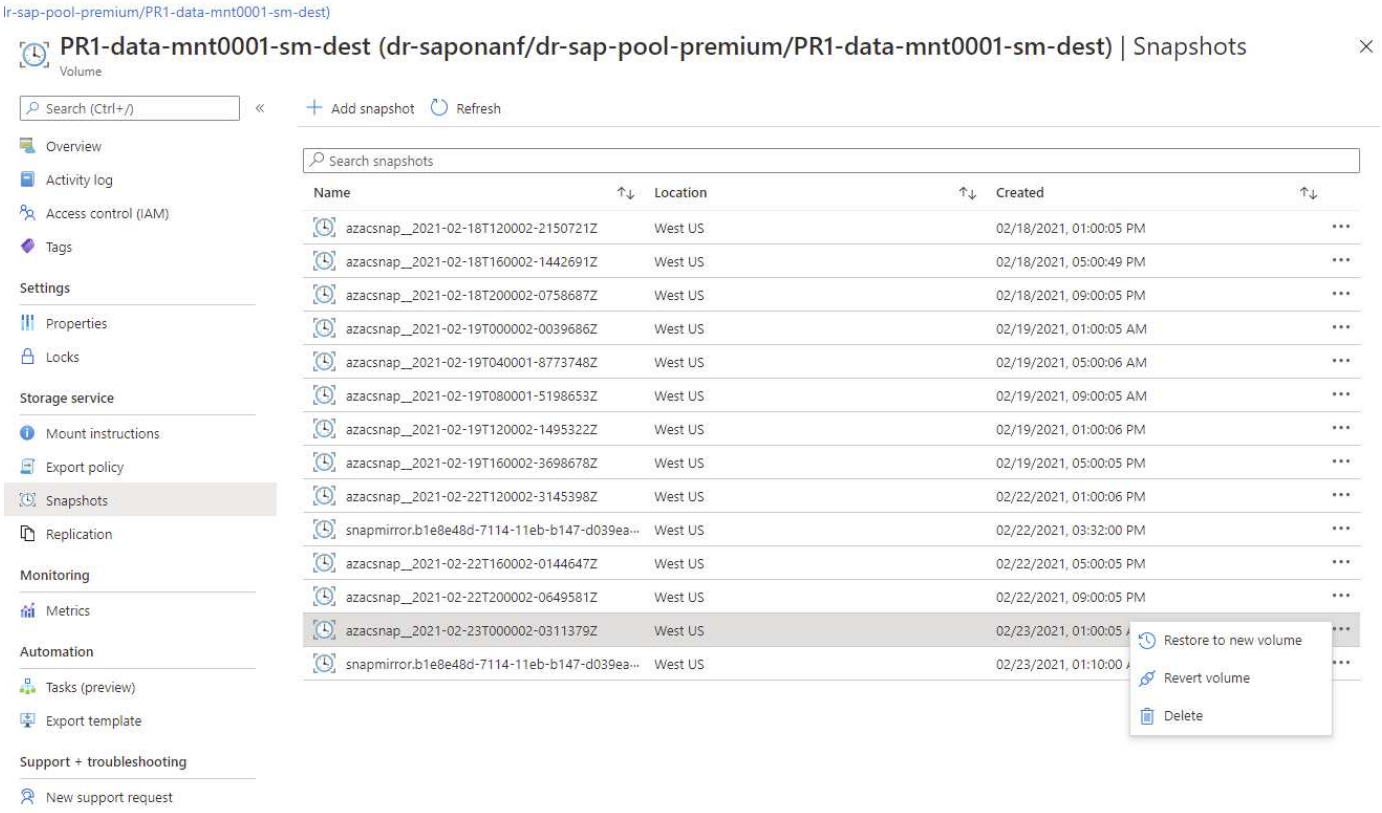
Für das HANA Daten-Volume müssen Sie das aktuelle HANA Snapshot-Backup wiederherstellen, das mit AzAcSnap erstellt wurde. Dieser Vorgang zum Zurücksetzen des Volumes ist nicht möglich, wenn der neueste ReplikationssSnapshot aufgrund des Replication Peering als belegt markiert wird. Deshalb müssen Sie auch das Replication Peering löschen.

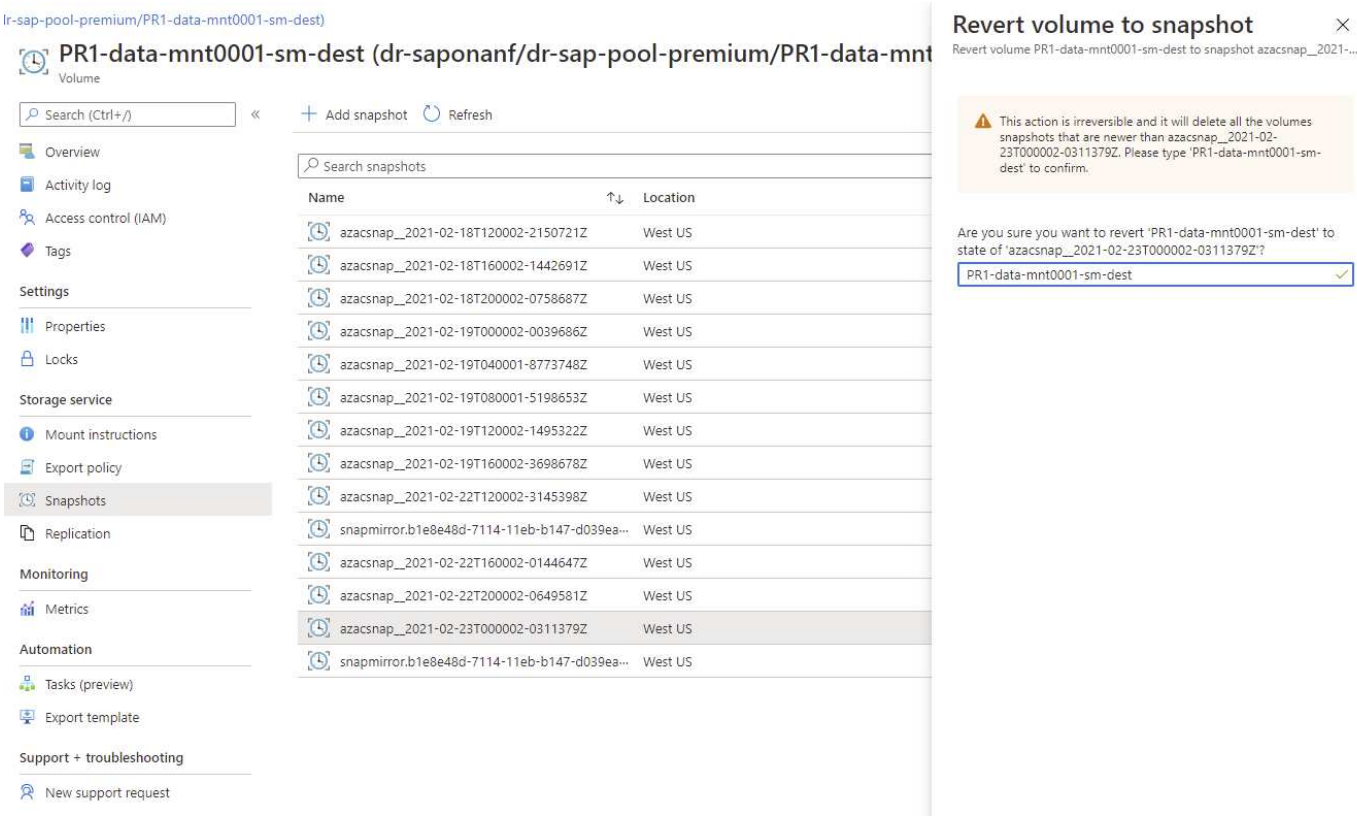
Die nächsten beiden Screenshots zeigen den Break and delete Peering-Vorgang für das HANA-Datenvolumen. Dieselben Vorgänge müssen auch für das Log-Backup und das gemeinsame HANA-Volume durchgeführt werden.





Da Replication Peering gelöscht wurde, ist es möglich, das Volume auf das neueste HANA Snapshot Backup zurückzusetzen. Wenn Peering nicht gelöscht wird, wird die Auswahl des Revert-Volumes ausgegraut und ist nicht wählbar. Die folgenden zwei Screenshots zeigen den Vorgang zur Zurücksetzen des Volumens.





Nach der Wiederherstellung des Volumes basiert das Daten-Volume auf einem konsistenten HANA-Snapshot-Backup und kann nun für Recovery-Vorgänge genutzt werden.

Wenn ein Kapazitäts-Pool mit einer Tier mit niedriger Performance verwendet wurde, müssen die Volumes nun in einen Kapazitäts-Pool verschoben werden, der die erforderliche Performance bietet.

Mounten Sie die Volumes am Ziel-Host

Die Volumes können jetzt auf der Grundlage des auf dem Zielhost eingebunden werden `/etc/fstab` Datei zuvor erstellt.

```
vm-pr1:~ # mount -a
```

Die folgende Ausgabe zeigt die erforderlichen Dateisysteme.

```
vm-pr1:~ # df
Filesystem                                      1K-blocks     Used
Available Use% Mounted on
devtmpfs                                          8201112        0
8201112   0% /dev
tmpfs                                            12313116        0
12313116   0% /dev/shm
tmpfs                                             8208744     9096
8199648   1% /run
tmpfs                                             8208744        0
8208744   0% /sys/fs/cgroup
/dev/sda4                                        29866736  2543948
27322788   9% /
/dev/sda3                                         1038336    79984
958352   8% /boot
/dev/sda2                                          524008     1072
522936   1% /boot/efi
/dev/sdb1                                        32894736    49180
31151556   1% /mnt
10.0.2.4:/PR1-log-mnt00001-dr                107374182400     6400
107374176000   1% /hana/log/PR1/mnt00001
tmpfs                                             1641748        0
1641748   0% /run/user/0
10.0.2.4:/PR1-shared-sm-dest/hana-shared 107377178368 11317248
107365861120   1% /hana/shared
10.0.2.4:/PR1-shared-sm-dest/usr-sap-PR1 107377178368 11317248
107365861120   1% /usr/sap/PR1
10.0.2.4:/hanabackup-sm-dest                 107379678976 35249408
107344429568   1% /hanabackup
10.0.2.4:/PR1-data-mnt0001-sm-dest           107376511232  6696960
107369814272   1% /hana/data/PR1/mnt00001
vm-pr1:~ #
```

HANA Datenbank-Recovery

Im Folgenden werden die Schritte für das HANA-Datenbank-Recovery aufgeführt

Starten Sie die erforderlichen SAP-Dienste.

```
vm-pr1:~ # systemctl start sapinit
```

Die folgende Ausgabe zeigt die erforderlichen Prozesse.

```
vm-pr1:/ # ps -ef | grep sap
root     23101     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saphostexec pf=/usr/sap/hostctrl/exe/host_profile
pr1adm   23191     1  3 11:29 ?        00:00:00
/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
sapadm   23202     1  5 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/hostctrl/exe/host_profile -D
root     23292     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saposcol -l -w60
pf=/usr/sap/hostctrl/exe/host_profile
root     23359  2597  0 11:29 pts/1    00:00:00 grep --color=auto sap
```

In den folgenden Abschnitten wird der Recovery-Prozess mit und ohne Forward Recovery mit den replizierten Log-Backups beschrieben. Die Recovery wird mit dem HANA-Recovery-Skript für die Systemdatenbank und hdbsql-Befehle für die Mandanten-Datenbank ausgeführt.

Recovery zum aktuellen Backup-Speicherpunkt für das HANA-Datenvolumen

Die Wiederherstellung zum neuesten Backup savepoint wird mit folgenden Befehlen als User pr1adm ausgeführt:

- Systemdatenbank

```
recoverSys.py --command "RECOVER DATA USING SNAPSHOT CLEAR LOG”
```

- Mandantendatenbank

```
Within hdbsql: RECOVER DATA FOR PR1 USING SNAPSHOT CLEAR LOG
```

Sie können auch HANA Studio oder Cockpit verwenden, um die Wiederherstellung des Systems und der Mandanten-Datenbank auszuführen.

Die folgende Befehlsausgabe zeigt die Ausführung der Wiederherstellung.

Recovery der Systemdatenbank

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py
--command="RECOVER DATA USING SNAPSHOT CLEAR LOG"
[139702869464896, 0.008] >> starting recoverSys (at Fri Feb 19 14:32:16
2021)
[139702869464896, 0.008] args: ()
[139702869464896, 0.009] keys: {'command': 'RECOVER DATA USING SNAPSHOT
CLEAR LOG'}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: ============2021-02-19 14:32:16 ============
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-19 14:32:16
stopped system: 2021-02-19 14:32:16
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-19 14:32:21
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-19T14:32:56+00:00  P0027646      177bab4d610 INFO    RECOVERY
RECOVER DATA finished successfully
recoverSys finished successfully: 2021-02-19 14:32:58
[139702869464896, 42.017] 0
[139702869464896, 42.017] << ending recoverSys, rc = 0 (RC_TEST_OK), after
42.009 secs
pr1adm@vm-pr1:/usr/sap/PR1/HDB01>
```

Recovery von Mandanten-Datenbanken

Wenn für den Benutzer pr1adm am Quellsystem kein Benutzerspeicherschlüssel erstellt wurde, muss auf dem Zielsystem ein Schlüssel erstellt werden. Der im Schlüssel konfigurierte Datenbankbenutzer muss über Berechtigungen zur Ausführung von Mandanten-Recovery-Vorgängen verfügen.

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbuserstore set PR1KEY vm-pr1:30113
<backup-user> <password>
```

Die Mandantenwiederherstellung wird jetzt mit hdbsql ausgeführt.

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql SYSTEMDB=> RECOVER DATA FOR PR1 USING SNAPSHOT CLEAR LOG
0 rows affected (overall time 66.973089 sec; server time 66.970736 sec)
hdbsql SYSTEMDB=>
```

Die HANA-Datenbank ist jetzt betriebsbereit, und der Disaster-Recovery-Workflow für die HANA-Datenbank wurde getestet.

Recovery mit vorwärtsgerichteten Recovery mithilfe von Log-/Katalog-Backups

Log-Backups und der HANA-Backup-Katalog werden aus dem Quellsystem repliziert.

Die Wiederherstellung mit allen verfügbaren Log-Backups wird mit den folgenden Befehlen als Benutzer pr1adm ausgeführt:

- Systemdatenbank

```
recoverSys.py --command "RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT"
```

- Mandantendatenbank

```
Within hdbsql: RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
```

Um eine Wiederherstellung mit allen verfügbaren Protokollen durchzuführen, können Sie jederzeit als Zeitstempel in der Recovery-Anweisung verwenden.

Sie können auch HANA Studio oder Cockpit verwenden, um die Wiederherstellung des Systems und der Mandanten-Datenbank auszuführen.

Die folgende Befehlsausgabe zeigt die Ausführung der Wiederherstellung.

Recovery der Systemdatenbank

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py --command
"RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20 00:00:00' CLEAR LOG USING
SNAPSHOT"
[140404915394368, 0.008] >> starting recoverSys (at Fri Feb 19 16:06:40
2021)
[140404915394368, 0.008] args: ()
[140404915394368, 0.008] keys: {'command': "RECOVER DATABASE UNTIL
TIMESTAMP '2021-02-20 00:00:00' CLEAR LOG USING SNAPSHOT"}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: ============2021-02-19 16:06:40 ============
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-19 16:06:40
stopped system: 2021-02-19 16:06:41
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-19 16:06:46
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-19T16:07:19+00:00  P0009897      177bb0b4416 INFO    RECOVERY
RECOVER DATA finished successfully, reached timestamp 2021-02-
19T15:17:33+00:00, reached log position 38272960
recoverSys finished successfully: 2021-02-19 16:07:20
[140404915394368, 39.757] 0
[140404915394368, 39.758] << ending recoverSys, rc = 0 (RC_TEST_OK), after
39.749 secs
```

Recovery von Mandanten-Datenbanken

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit

hdbsql SYSTEMDB=> RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
0 rows affected (overall time 63.791121 sec; server time 63.788754 sec)

hdbsql SYSTEMDB=>
```

Die HANA-Datenbank ist jetzt betriebsbereit, und der Disaster-Recovery-Workflow für die HANA-Datenbank wurde getestet.

Überprüfen Sie die Konsistenz der neuesten Protokoll-Backups

Da die Volume-Replizierung für das Protokoll unabhängig vom von dem von der SAP HANA Datenbank ausgeführten Backup-Prozess durchgeführt wird, können am Disaster Recovery-Standort inkonsistente Backup-Dateien für Protokolle vorhanden sein. Nur die letzten Backup-Dateien für Protokolle sind möglicherweise inkonsistent und diese Dateien sollten überprüft werden, bevor eine Weiterleitung der Recovery am Disaster Recovery-Standort mithilfe der erfolgt `hdbbackupcheck` Werkzeug.

Wenn der `hdbbackupcheck` Tool meldet Fehler bei den letzten Protokollsicherungen muss der neueste Satz von Protokollsicherungen entfernt oder gelöscht werden.

```
pr1adm@hana-10: > hdbbackupcheck
/hanabackup/PR1/log/SYSTEMDB/log_backup_0_0_0_0.1589289811148
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivecache'
Backup '/mnt/log-backup/SYSTEMDB/log_backup_0_0_0_0.1589289811148'
successfully checked.
```

Die Prüfung muss für die aktuellen Log-Backup-Dateien des Systems und der Mandanten-Datenbank ausgeführt werden.

Wenn der `hdbbackupcheck` Tool meldet Fehler bei den letzten Protokollsicherungen muss der neueste Satz von Protokollsicherungen entfernt oder gelöscht werden.

Aktualisierungsverlauf

An dieser Lösung wurden seit ihrer ersten Veröffentlichung folgende technische Änderungen vorgenommen:

Version	Datum	Zusammenfassung aktualisieren
Version 1.0	April 2021	Ausgangsversion

TR-4646: SAP HANA Disaster Recovery with Storage Replication

Der TR-4646 bietet einen Überblick über die Optionen für Disaster-Recovery-Schutz für SAP HANA. Sie enthält detaillierte Setup-Informationen und eine Beschreibung des Anwendungsfalls für eine Disaster-Recovery-Lösung an drei Standorten, die auf synchroner und asynchroner NetApp SnapMirror Storage-Replizierung basiert. Bei der beschriebenen Lösung wird NetApp SnapCenter mit dem SAP HANA Plug-in eingesetzt, um die Datenbankkonsistenz zu managen.

Autor: Nils Bauer, NetApp

https://www.netapp.com/pdf.html?item=/media/8584-tr4646pdf.pdf

TR-4711: SAP HANA Backup and Recovery Using NetApp Storage Systems and CommVault Software

TR-4711 beschreibt das Design einer NetApp und CommVault Lösung für SAP HANA, die CommVault IntelliSnap Snapshot-Managementtechnologie und NetApp Snapshot Technologie umfasst. Die Lösung basiert auf NetApp Storage und der CommVault Datensicherungssuite.

Autoren: Marco Schoen, NetApp; Dr. Tristan Daude, CommVault Systems

https://www.netapp.com/pdf.html?item=/media/17050-tr4711pdf.pdf

SnapCenter Integration für SAP ASE Database

In diesem Dokument werden die Besonderheiten der SnapCenter-Integration für die in einer SAP-Umgebung verwendete SAP ASE-Datenbank beschrieben.

Einführung

Das Dokument soll keine Schritt-für-Schritt-Beschreibung der Einrichtung der gesamten Umgebung sein, sondern umfasst Konzepte und relevante Details zu:

- Beispiel für eine Konfigurationsübersicht
- Beispiellayout
- Schutz der SAP ASE Instanz
- Wiederherstellung und Wiederherstellung von SAP ASE Instanz

Autor: Michael Schlosser, NetApp

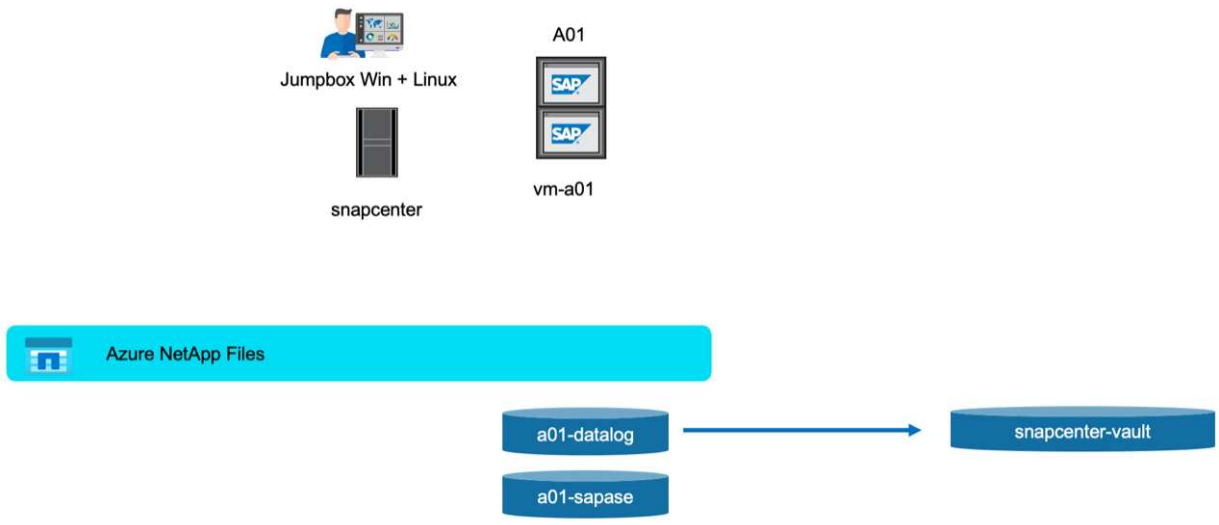
Beispiel für eine Konfigurationsübersicht

Beispiel für eine Implementierung des SnapCenter ASE Plug-ins für ein SAP-System auf der Azure Plattform.

Diese Implementierung beschreibt die minimal erforderliche Volume-Konfiguration. Data Dump Backups und Log Dump Backups werden gemäß SAP Note 1588316 konfiguriert.

Alternativ könnte die in diesem Abschnitt beschriebene Volume-Struktur "MS Technical Community Blog"verwendet werden.

Demo-Umgebung



Softwareversionen

Software	Version
Linux BS	SLES FÜR SAP 15 SP5
SAP	SAP NetWeaver 7.5 unterstützt
SAP ASE	16.0 SP04 PL06 HF1
SnapCenter	6,1

ASE Volume Design

Das nachstehende „Least Volume Layout“ muss verwendet werden, um Backup-/Recovery- und Klonfälle für die SAP ASE-Datenbank zu ermöglichen. Die Beispielkonfiguration verwendet <SID>: A01.

Volumenname	Verzeichnis (qtree) auf Volumen	Mount-Punkt auf Server	Kommentar
<SID>-sapase	sybase	/sybase	Übergeordnetes Verzeichnis für ASE-bezogene Dateien
		/sybase/<SID>/Backups	Data Dump Backups (können auf einem anderen Volume abgelegt werden)
		/sybase/<SID>/log_Archives	Log-Dump-Backups (können auf einem anderen Volume abgelegt werden)
	<sid>-Lösungen m	/Home/<sid>-Programm m	Home Verzeichnis der Benutzer <sid> Hmm
	Usrsaptrans	/Usr/sap/trans	Transportverzeichnis
	<SID>	/Usr/sap/<SID>	Usr sap
	<SID>	/Sapmnt/<SID>	SAP GlobalHost-Verzeichnis

Volumenname	Verzeichnis (qtree) auf Volumen	Mount-Punkt auf Server	Kommentar
<SID>-Datalog	sapdata_1	/sybase/<SID>/sapdata_1	DB-Daten (SID)
	saplog_1	/sybase/<SID>/saklog_1	DB-Protokoll (SID)
	Saptemp	/sybase/<SID>/saptemp	PSAPTEMP
	Systemsicherheit	/sybase/<SID>/sybsicherheit	Sybase Sicherheits-DB
	Sybsystem	/sybase/<SID>/sybsystem	Sybase System-DB
	Sybtemp	/sybase/<SID>/sybtemp	Sybase System-DB - Temp
	Sapdiag	/sybase/<SID>/sapdiag	'saptools'-Datenbank

Schritte zum Schutz von Datenbank A01

- Prüfen Sie die Dateiverteilung gemäß dem Beispiellayout
- Prüfen Sie die Voraussetzungen für den Host (vm-a01).
- Voraussetzungen für die Datenbank prüfen (A01)
- SnapCenter-Agent auf Host bereitstellen/installieren (vm-a01)
- Erstellen Sie die Ressourcenkonfiguration der SnapCenter-Instanz

Voraussetzungen auf Host

Weitere aktuelle Informationen stehen zur Verfügung"Hier".

Bevor Sie einen Host hinzufügen und das Plug-in-Paket für Linux installieren, müssen Sie alle Anforderungen erfüllen.

- Wenn Sie iSCSI verwenden, muss der iSCSI-Dienst ausgeführt werden.
- Sie können entweder die passwortbasierte Authentifizierung für den Root- oder nicht-Root-Benutzer oder die SSH-Schlüsselauthentifizierung verwenden.
- Das SnapCenter-Plug-in für Unix-Dateisysteme kann von einem Benutzer installiert werden, der kein Root-Benutzer ist. Sie sollten jedoch die sudo-Berechtigungen für den nicht-Root-Benutzer konfigurieren, um den Plug-in-Prozess zu installieren und zu starten. Nach der Installation des Plug-ins werden die Prozesse als effektiver nicht-Root-Benutzer ausgeführt.
- Anmeldedaten mit Authentifizierungsmodus als Linux für den Installationsbenutzer erstellen.
- Sie müssen Java 11 auf Ihrem Linux-Host installiert haben.
- Stellen Sie sicher, dass Sie nur die zertifizierte Version von JAVA 11 auf dem Linux-Host installiert haben
- Informationen zum Herunterladen von JAVA finden Sie unter Java Downloads für alle Betriebssysteme
- Sie sollten bash als Standard-Shell für die Plug-in-Installation verwenden.

Voraussetzungen für die Datenbank – Aktivieren Sie Protokollierung und Backups

- Verzeichnisse für Backups und log_Archives erstellen (/sybase/A01/Backups, /sybase/A01/log_Archives)
- Verbindung zur Datenbank A01 (als OS-User syba01)
  - Isql -S A01 -U sapsa -X -w 1024

- Erstellen Sie eine Dump-Konfiguration für DATEN (A01DB) gemäß SAP Note 1588316
  - Master verwenden
  - Los
  - exec SP_config_dump @config_Name='A01DB', @Stripe_dir = '/sybase/A01/Backups' , @Komprimierung = '101' , @verify = 'header'
  - Los
- Erstellen Sie eine Dump-Konfiguration für das PROTOKOLL (A01LOG) gemäß SAP Note 1588316
  - Master verwenden
  - Los
  - SP_config_dump @config_Name='A01LOG', @Stripe_dir = '/sybase/A01/log_Archives' , @Komprimierung = '101' , @verify = 'header'
  - Los
- Aktivieren Sie die vollständige Protokollierung für Datenbank A01
  - SP_dboption A01, 'trunc log on chkpt' , false
  - Los
  - SP_dboption A01, 'vollständige Protokollierung für alle', 'true'
  - Los
  - SP_dboption A01, 'Enforce Dump tran Sequence', 'true'
  - Los
- Datenbank-DUMP-Backup zum Aktivieren von Log-DUMP-Backup
  - Dump-Datenbank A01 mit config ='A01DB'
  - Los
  - Protokollabfall
  - Dump-Transaktion A01 mit config = 'A01LOG'
  - Los
- Stellen Sie sicher, dass regelmäßige Protokollsicherungen gemäß SAP Note 1588316 konfiguriert sind

Optional – Erstellen Sie einen dedizierten Datenbankbenutzer

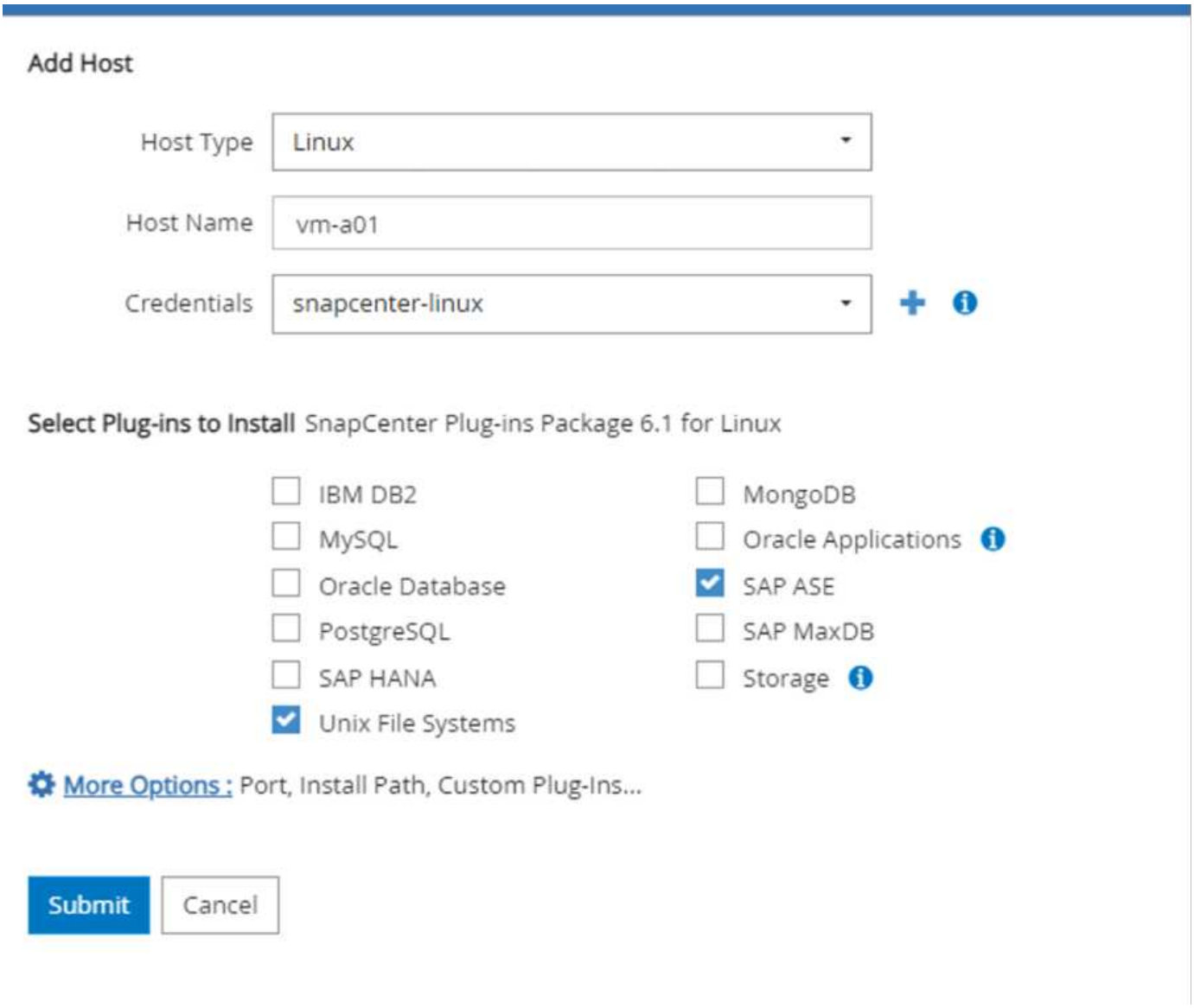
Für SAP Umgebungen könnte User sapsa genutzt werden.

- Verbindung zur Datenbank A01 (als OS-User syba01)
  - Isql -S A01 -U sapsa -X -w 1024
- Benutzer erstellen
  - Erstellen Sie ein Anmelde-Backup mit Passwort <password>
  - Los
- Weisen Sie dem Benutzer Permisssons/Rollen zu
  - Rolle sa_role,sso_role,oper_role,sybase_ts_role für Backup gewähren
  - Los

SnapCenter-Agent auf Host-vm-a01 bereitstellen

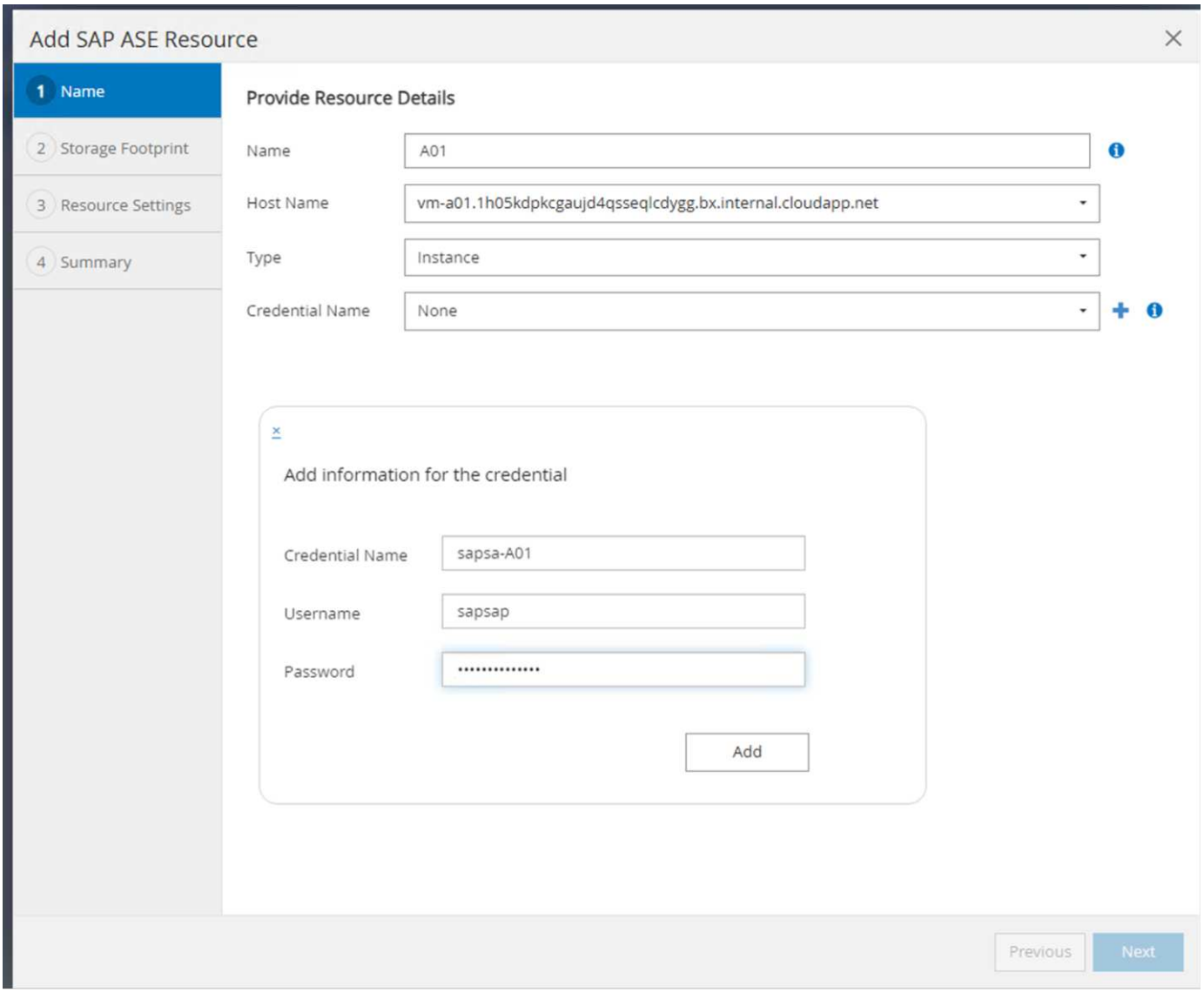
Weitere Informationen finden Sie im "SnapCenter-Dokumentation".

Wählen Sie die Plug-ins für SAP ASE und Unix File Systems aus.

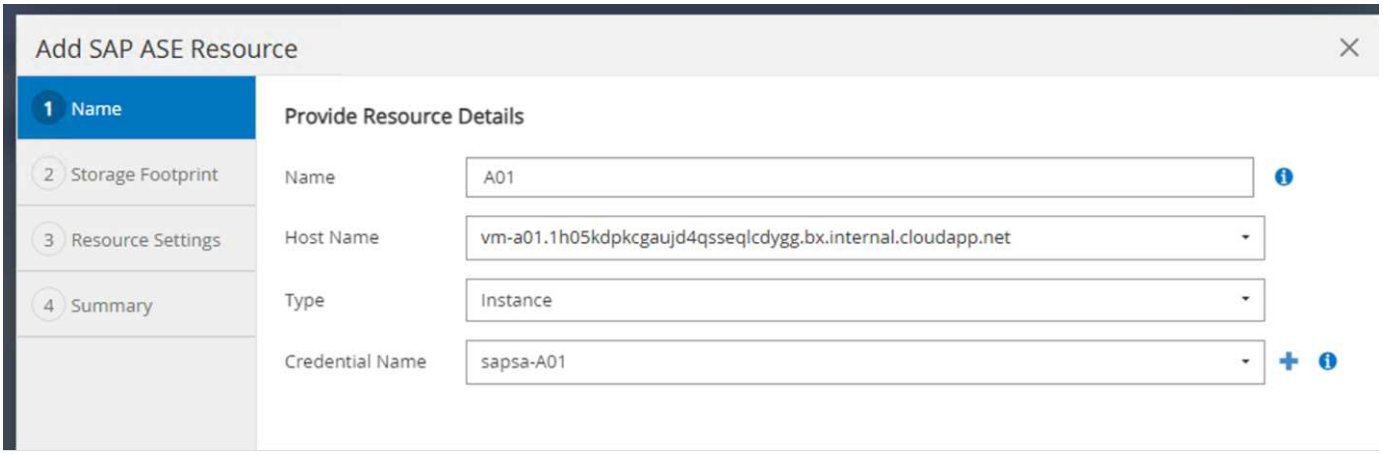


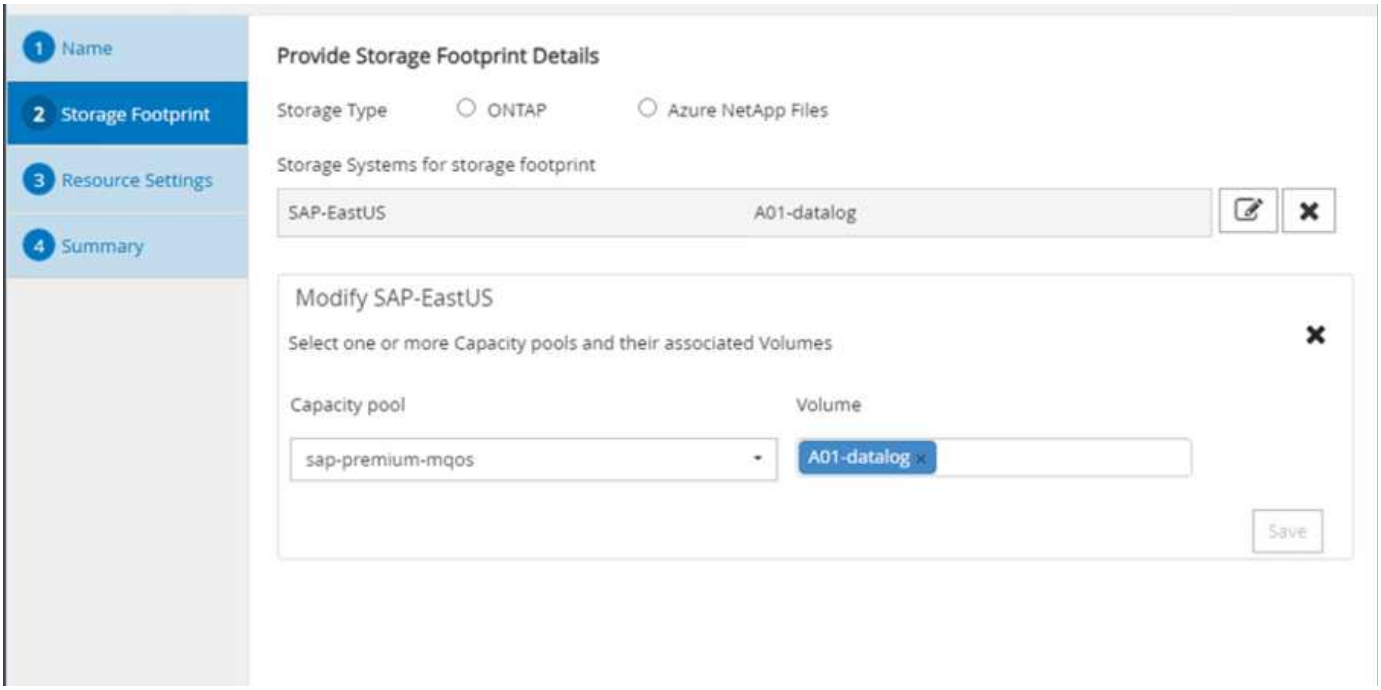
Erstellen Sie die Ressourcenkonfiguration der SnapCenter-Instanz für Datenbank A01

Ressourcen → SAP ASE → Ressourcen hinzufügen



Wenn das Passwort Sonderzeichen enthält, müssen diese mit einem umgekehrten Schrägstrich maskiert werden. Z. B. Test!123! → Test\!123\!

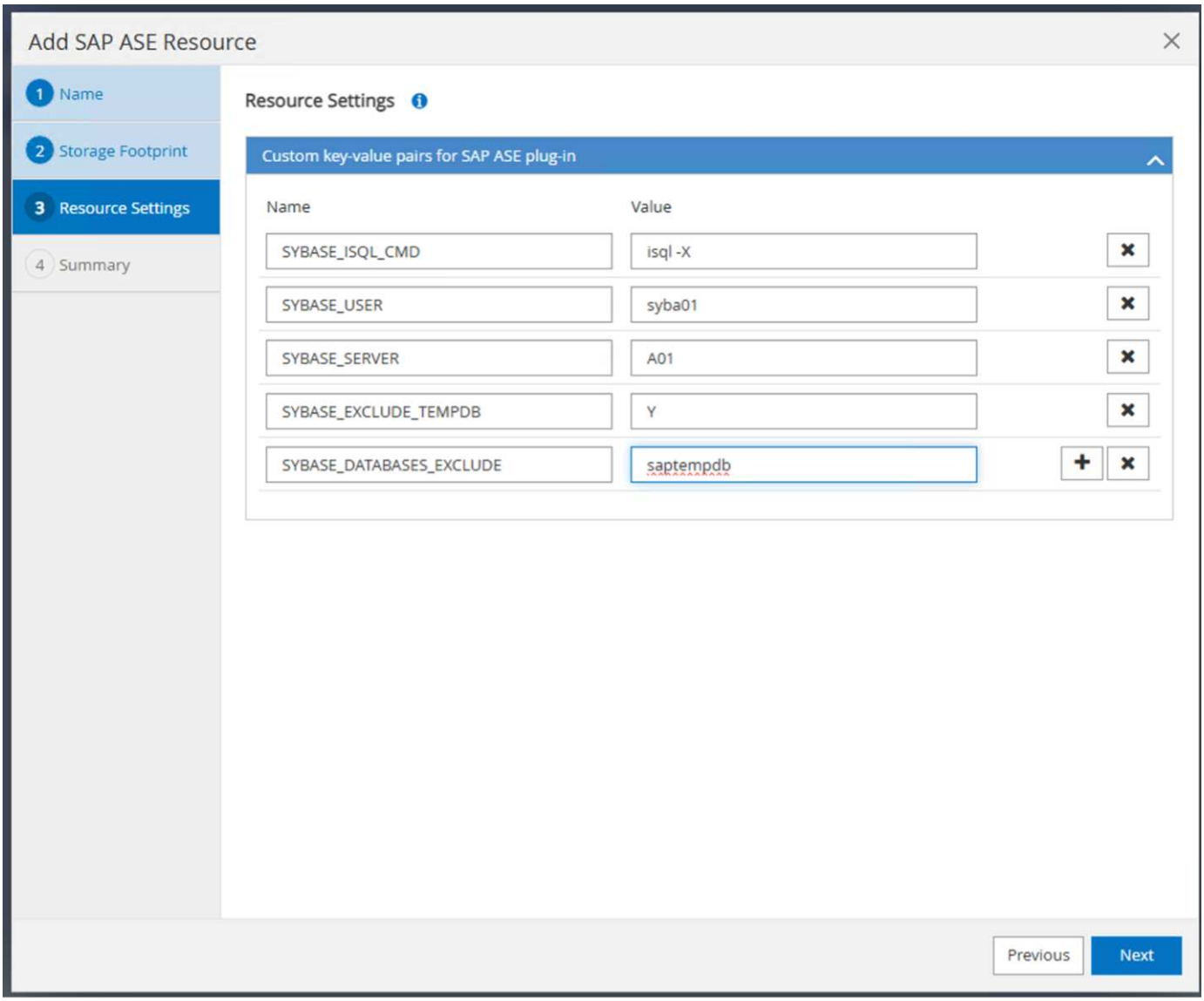




Wenn Sie das Volumendesign aus dem verwenden"MS Technical Community Blog".

Volumes /<SID> uncausage base, /uncauso <SID> uncauso, /<SID> begleichen muss als Storage Footprint konfiguriert werden

Im Anschluss an die Ressourceneinstellungen müssen (mindestens) benutzerdefinierte Schlüssel-Wert-Paare erstellt werden.



In der folgenden Tabelle sind die Sybase Plug-in-Parameter aufgeführt, ihre Einstellungen aufgeführt und beschrieben:

Parameter	Einstellung	Beschreibung
SYBASE_ISQL_CMD	Beispiel: /Opt/sybase/OCS-15__0/bin/isql -X	Definiert den Pfad zum Befehl isql. Verfügbare Optionen: https://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.infocenter.dc34237.1500/html/mvsinst/CIHHFDGC.htm
SYBASE_USER	Benutzername	Gibt den Betriebssystembenutzer an, der den Befehl isql ausführen kann. Dieser Parameter ist für UNIX erforderlich. Dieser Parameter ist erforderlich, wenn der Benutzer, der die Snap Creator Agentstart- und STOP-Befehle ausführt (normalerweise der Root-Benutzer) und der Benutzer, der den isql-Befehl ausführt, unterschiedlich ist.
SYBASE_SERVER	Name_Data_Server	Gibt den Namen des Sybase-Datenservers an (-S Option auf isql Befehl).Beispiel: A01

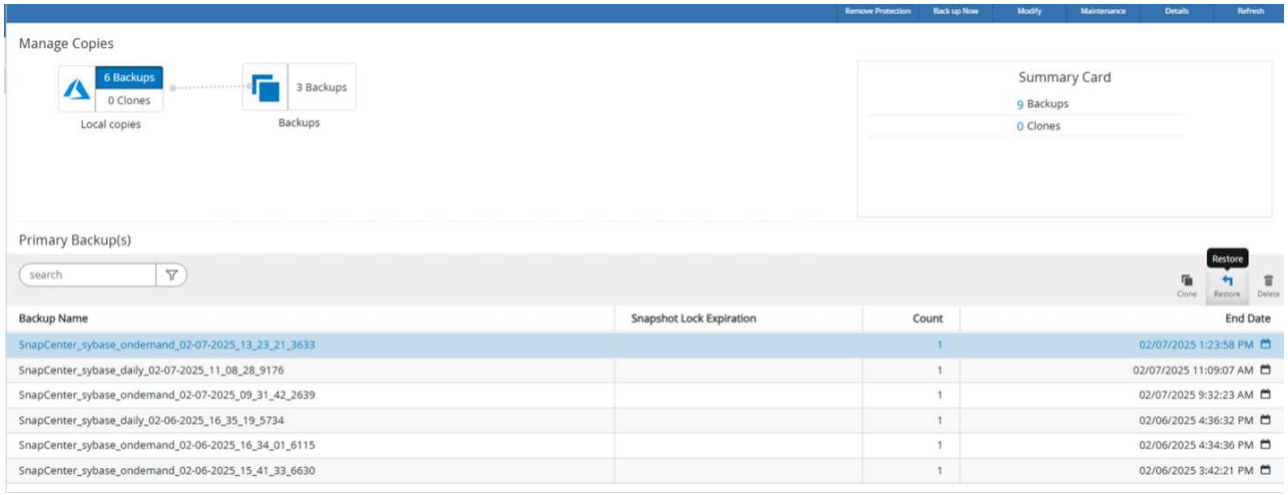
Parameter	Einstellung	Beschreibung
SYBASE_DATENBANKEN	db_Name:user_Name/password	Listet die Datenbanken innerhalb der Instanz auf, die gesichert werden sollen. Die Master-Datenbank wird hinzugefügt, zum Beispiel: DBATest2:sa/53616c7404351e.wird eine Datenbank mit dem Namen +ALL verwendet, wird die automatische Datenbankerkennung verwendet und die sybsyntax, sybsystemdb, sybsystemprocs und tempdb-Datenbanken werden ausgeschlossen. Ein Beispiel: +ALL:sa/53616c71a6351e Verschlüsselte Passwörter werden unterstützt, wenn der Parameter NTAP_PWD_PROTECTION eingestellt ist.
SYBASE_DATABASES_EXCLUDE	db_Name	Ermöglicht den Ausschluss von Datenbanken, wenn das +ALLE-Konstrukt verwendet wird. Sie können mehrere Datenbanken mit Hilfe einer durch Semikolon getrennten Liste angeben.Beispiel: Pubs2;Test_db1
SYBASE_TRAN_DUMP	db_Name:Directory_PATH	Ermöglicht Ihnen die Durchführung eines Sybase Transaktions-Dump nach dem Erstellen einer Snapshot-Kopie.Beispiel: Pubs2:/sybasedumps/pubs2 Sie müssen jede Datenbank angeben, die einen Transaktions-Dump benötigt.
SYBASE_TRAN_DUMP_FORMAT	%S_%D_%T.CMN	Ermöglicht Ihnen die Angabe der Namenskonvention für Dump. Die folgenden Schlüssel können angegeben werden: %S = Instanzname von SYBASE_SERVER %D = Datenbank von SYBASE_DATABASES %T = eindeutiger Zeitstempel Hier ist ein Beispiel: %S_%D_%T.log
SYBASE_TRAN_DUMP_COMPRESS	(J/N)	Aktiviert oder deaktiviert die native Sybase Transaktions-Dump-Komprimierung.
SYBASE	Beispiel: /Sybase	Gibt den Speicherort der Sybase-Installation an.
SYBASE_MANIFEST	Beispiel: A01:/sybase/A01/sapdiag	Gibt die Datenbanken an, für die die Manifestdatei erstellt werden soll, zusammen mit dem Speicherort, an dem die Manifestdatei platziert werden soll.
SYBASE_MANIFEST_FORMAT	%S__%D_.Manifest Beispiel: %S_%D_.Manifest	Ermöglicht Ihnen die Angabe der Namenskonvention für die Manifestdatei. Folgende Schlüssel können angegeben werden: %S = Instanzname von SYBASE_SERVER %D = Datenbank von SYBASE_DATABASES
SYBASE_MANIFEST_DELETE	(J/N)	Ermöglicht das Löschen des Manifests nach dem Erstellen der Snapshot Kopie. Die Manifest-Datei sollte in der Snapshot-Kopie erfasst werden, damit sie immer für das Backup verfügbar ist.
SYBASE_EXCLUDE_TEMPDB	(J/N)	Ermöglicht den automatischen Ausschluss von vom Benutzer erstellten temporären Datenbanken.

Sequenz zum Wiederherstellen von System A01

1. SAP System A01 stoppen (einschließlich Datenbank), sapinit stoppen
2. Umount Dateisysteme
3. Volumes A01-Datalog wiederherstellen (mit SnapCenter)
4. Mounten Sie Dateisysteme
5. Start Datenbank A01 (mit Option –q, um automatische Online zu vermeiden und Datenbank vorwärts wiederherstellbar zu halten – gemäß SAP Note 1887068)
6. Starten Sie BackupServer A01
7. Online-Datenbank saptools, sybsicherheit, sybmgmtdb
8. Datenbank A01 wiederherstellen (mit isql)
9. Online-Datenbank A01
10. Starten Sie sapinit, SAP System A01

Instanz A01 wiederherstellen

- Beenden Sie SAP System + DB A01 auf Host vm-a01
  - User a01adm: Stopsap
  - User root: /Etc/init.d/sapinit stop
  - Benutzer root: Umount -a -t nfs
- Backup Wiederherstellen
  - SnapCenter GUI: Wählen Sie erforderliche Sicherung für Wiederherstellung



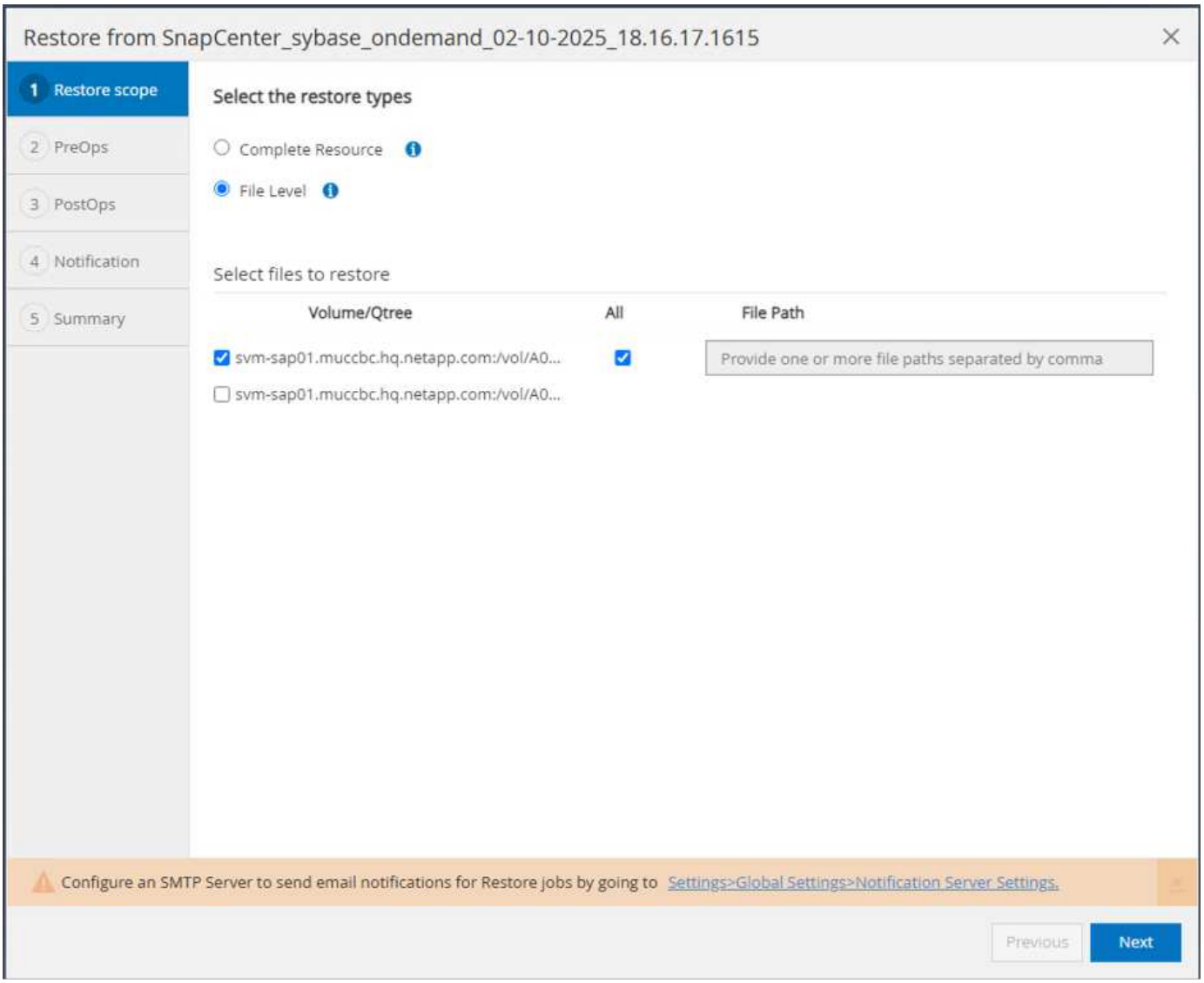
  - Für die ANF Implementierung – nur vollständige Ressource verfügbar

Wenn Sie die Option „Complete Resource“ auswählen, wird eine Volume-basierte Snap Restore (VBSR) ausgelöst. Innerhalb von Azure wird sie aufgerufen"Lautstärke zurücksetzen".

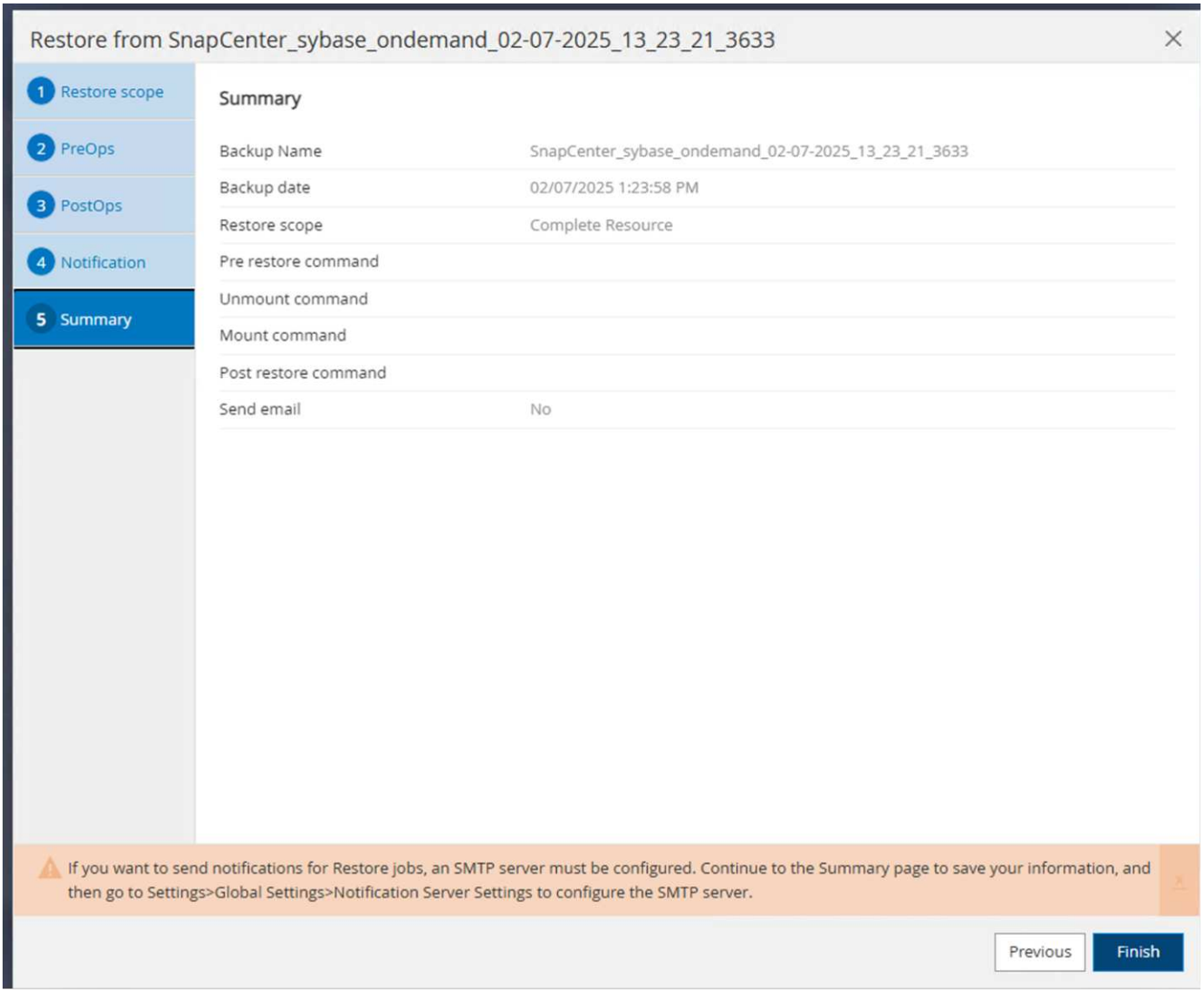
Important

Active filesystem data and snapshots that were taken after the selected snapshot will be lost. The snapshot revert operation will replace *all* the data in the targeted volume with the data in the selected snapshot. You should pay attention to the snapshot contents and creation date when you select a snapshot. You cannot undo the snapshot revert operation.

Für andere Implementierungstypen (z. B. On-Premises-ANF) könnte ein SFSR-Vorgang (Single File Snap Restore) orchestriert werden. Wählen Sie File Level und das entsprechende Volume und aktivieren Sie „All“ – siehe folgenden Screenshot.



Die Zusammenfassung wird angezeigt und mit „Fertig stellen“ wird die eigentliche Wiederherstellung gestartet.



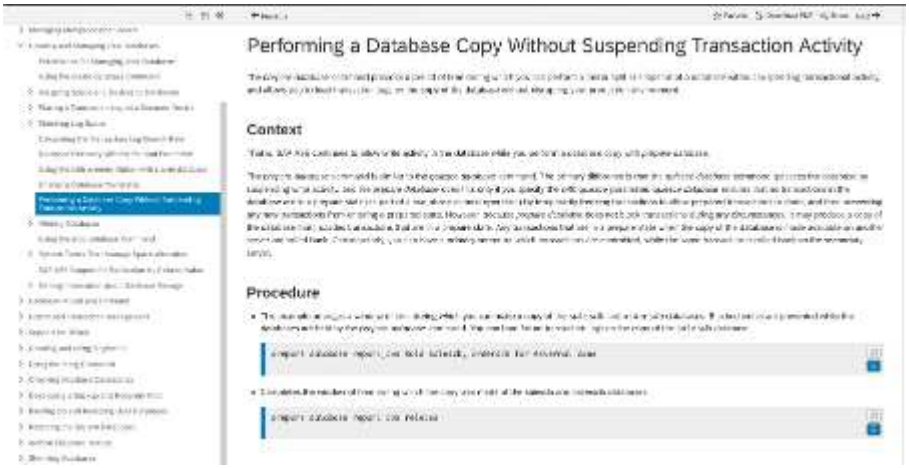
- Dateisysteme mounten (vm-a01)
  - User root: Mount -a -t nfs
- Starten Sie Datenbank A01 + BackupServer
  - RUN_A01 ändern und -q \ hinzufügen (gemäß SAP Note 1887068)
  - User syba01: RUN_A01 &
  - User syba01: RUN_A01_BS&
- Online-Datenbanken saptools, sybsicherheit, sybmgmtdb
  - User syba01: Isql -S A01 -U sapsa -X -w 1024
  - Online-Datenbank-Saptools
  - Los
  - Systemsicherheit der Online-Datenbank
  - Los
  - Online-Datenbank sybmgmtdb
  - Los

- Datenbank A01 wiederherstellen
  - SP_dump_history (Anzeige der Transaktions-Log-Dumps)
  - Los
  - Laden Sie Transaktionsprotokoll-Dumps entsprechend Ihren Anforderungen – weitere Informationen finden Sie in der Dokumentation: https://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.infocenter.dc36272.1572/html/commands/X75212.htm
  - Beispiel: LADEN SIE TRAN A01 VON '/sybase/A01/log_Archives/A01.TRAN.20250207.140248.6.000'
  - Los
  - Online-Datenbank A01
  - Los
- Entfernen Sie -q aus RUN_A01
- Starten Sie das SAP-System
  - User root: /Etc/init.d/sapinit Start
  - User a01ADM: Startsap

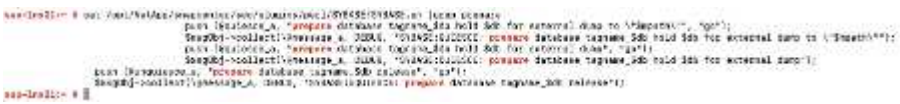
Zusätzliche Informationen und Versionsverlauf

Stilllegen vs. Vorbereiten

Siehe Dokumentation auf Link: SAP Hilfe Seite.



Das SnapCenter SAP ASE Plugin verwendet den Befehl Quiesce Database, könnte jedoch durch den Befehl Prepare ersetzt werden. Falls erforderlich, muss sie in SYBASE.pm in Zeile 473, 475, 675, 481, 673, 479 z.B. geändert werden



Aufgezeichnete Demos

Folgende neu kodierte Demos stehen zur Unterstützung der Dokumentation zur Verfügung.

Installation und Konfiguration ASE Plugin, Backup der ASE-Datenbank

Restore und Recovery von ASE-Datenbanken

Externe Dokumentation

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- "SAP Installation Azure auf ANF"
- "SnapCenter-Voraussetzungen für Plugins"
- "SnapCenter Installations-Plugins"
- "Sybase Infocenter - Isql"
- "Sybase Infocenter - Load Transaktions-Log Dumps"
- SAP-Hinweise (Anmeldung erforderlich)
  - 1887068 - SYB: Externe Sicherung und Wiederherstellung mit SAP ASE: https://me.sap.com/notes/1887068/E
  - 1618817 - SYB: Wiederherstellen eines SAP ASE-Datenbankservers (UNIX): https://me.sap.com/notes/1618817/E
  - 1585981 – SYB: Sicherstellung der Recovery-Fähigkeit für SAP ASE: https://me.sap.com/notes/1585981/E
  - 1588316 - SYB: Automatische Datenbank- und Protokollsicherungen konfigurieren: https://me.sap.com/notes/1588316/E
  - NetApp Produktdokumentation: https://www.netapp.com/support-and-training/documentation/
  - "NetApp SAP-Lösungen – Informationen zu Anwendungsfällen, Best Practices und Vorteilen"

Versionsverlauf

Version	Datum	Versionsverlauf des Dokuments
Version 1.0	April 2025	Erstversion – Backup/Recovery ASE-Datenbank

SnapCenter Integration für IBM DB2 Database

In diesem Dokument werden die Besonderheiten der SnapCenter-Integration für die in einer SAP-Umgebung verwendete IBM DB2-Datenbank beschrieben.

Einführung

Das Dokument soll keine Schritt-für-Schritt-Beschreibung der Einrichtung der gesamten Umgebung sein, sondern umfasst Konzepte und relevante Details zu:

- Beispiel für eine Konfigurationsübersicht
- Beispiellayout
- Schutz von DB2-Datenbanken
- Wiederherstellung und Wiederherstellung der DB2-Datenbank

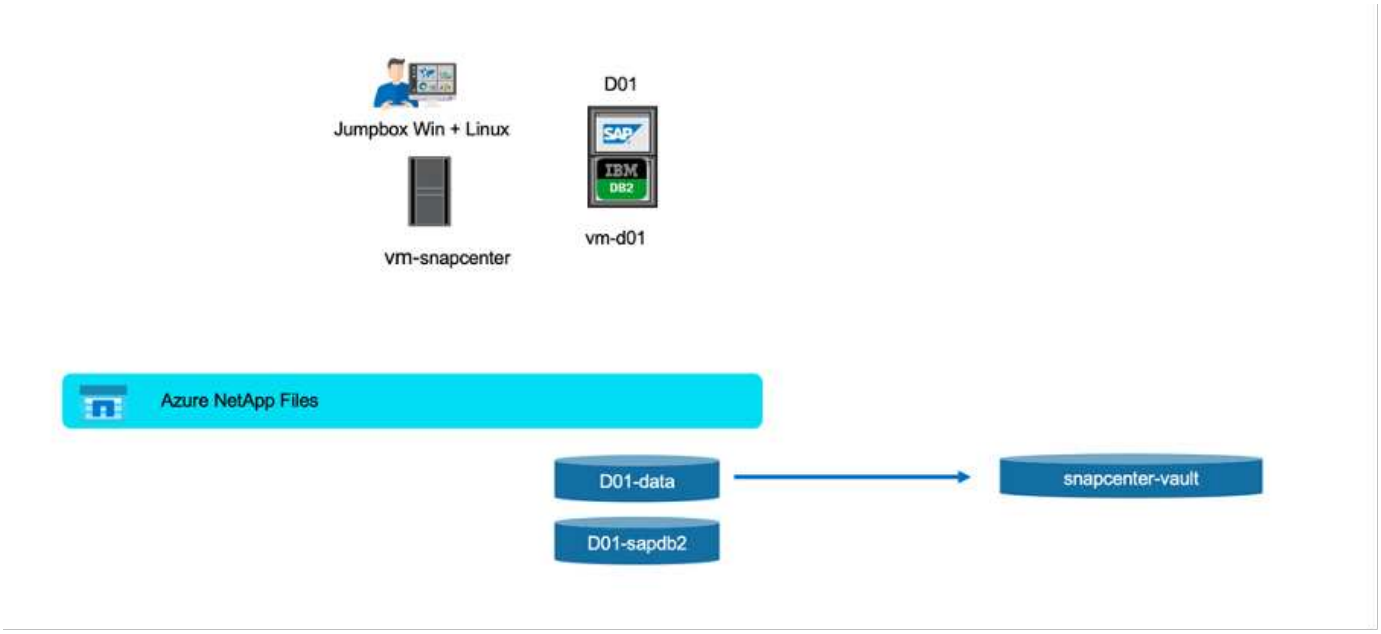
Autor: Michael Schlosser, NetApp

Beispiel für eine Konfigurationsübersicht

Beispiel für eine Implementierung für das SnapCenter DB2 Plug-in für ein SAP-System auf der Azure Plattform.

Diese Implementierung beschreibt die minimal erforderliche Volume-Konfiguration.

Alternativ könnte die in diesem Abschnitt beschriebene Volume-Struktur "MS Technical Community-Blog"verwendet werden.



Demo-Umgebung

Softwareversionen

Software	Version
Linux BS	SLES FÜR SAP 15 SP5
SAP	SAP NetWeaver 7.5 unterstützt
DB2	10.5.0.7
SnapCenter	6,1

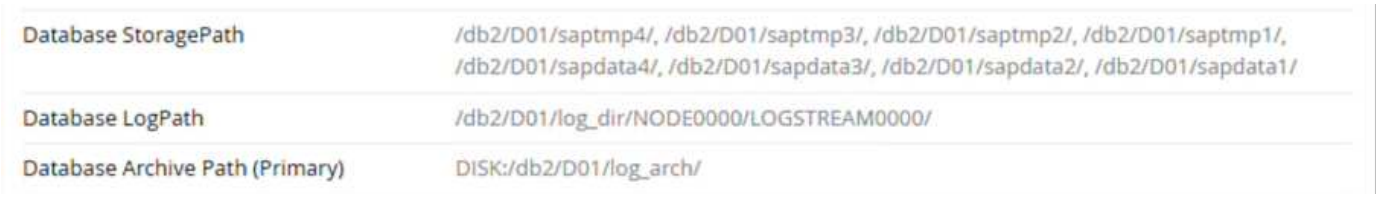
DB2-Volume-Design

Das folgende Least-Volume-Layout muss verwendet werden, um Backup-/Recovery- und Klonfälle für die DB2-Datenbank zu ermöglichen. Die Beispielkonfiguration verwendet <SID>: D01.

Volumenname	Verzeichnis (qtree) auf Volumen	Mount-Punkt auf Server	Kommentar
<SID>-sapdb2	db2	/db2	
		/db2/<SID>	Übergeordnetes Verzeichnis für DB2-bezogene Dateien

Volumenname	Verzeichnis (qtree) auf Volumen	Mount-Punkt auf Server	Kommentar
		/db2/db2<sid>	Home-Verzeichnis der Benutzer db2 <sid> und DB2 Software
		/db2/<SID>/db2dump	DB2-Diagnoseprotokoll und Dump-Dateien
		/db2/<SID>/Backup	Backup-Speicherort (kann auf einem anderen Volume platziert werden)
		/db2/<SID>/log_ARCH	Offline Redo Logs (möglicherweise auf einem anderen Volume platziert – Snapshot wird ausgelöst)
		/db2/<SID>/log_dir	Online Redo Logs (können auf einem anderen Volume platziert werden – Snapshot wird ausgelöst)
	<sid>-Lösungen m	/Home/<sid>-Programm m	Home Verzeichnis der Benutzer <sid> Hmm
	<sid> auslassen	/Home/<sid>	Home Verzeichnis des Benutzers <sid>
	Usrsaptrans	/Usr/sap/trans	Transportverzeichnis
	<SID>	/Usr/sap/<SID>	Usr sap
	<SID>	/Sapmnt/<SID>	SAP GlobalHost-Verzeichnis
<SID>-Daten	sapdata1	/db2/<SID>/sapdata1	DB-Daten
	sapdata2	/db2/<SID>/sapdata2	DB-Daten
	sapdata3	/db2/<SID>/sapdata3	DB-Daten
	sapdata4	/db2/<SID>/sapdata4	DB-Daten
	saptmp1	/db2/<SID>/saptmp1	DB Temp-Dateien
	saptmp2	/db2/<SID>/saptmp2	DB Temp-Dateien
	saptmp3	/db2/<SID>/saptmp3	DB Temp-Dateien
	saptmp4	/db2/<SID>/saptmp4	DB Temp-Dateien
	Db2 <sid>	/db2/<SID>/db2<sid>	Instanzdateien

Da die automatische Ermittlung standardmäßig für das DB2-Plug-in aktiviert ist, wird ein Snapshot für Volumes erstellt, die den folgenden Dateipfaden entsprechen.



Schritte zum Schutz von Datenbank D01

- Prüfen Sie die Dateiverteilung gemäß dem Beispiellayout
- Prüfen Sie die Voraussetzungen für den Host (vm-d01).
- Voraussetzungen für die Datenbank prüfen (D01)
- SnapCenter-Agent auf Host bereitstellen/installieren (vm-d01)
- Erstellen Sie die Ressourcenkonfiguration der SnapCenter-Instanz

Voraussetzungen auf Host

Weitere aktuelle Informationen finden Sie hier:

- https://docs.netapp.com/us-en/snapcenter/protect-scu/reference_prerequisites_for_adding_hosts_and_installing_snapcenter_plug_ins_package_for_linux.html
- https://docs.netapp.com/us-en/snapcenter/protect-db2/prerequisites-for-using-snapcenter-plug-in-for-ibm-db2.html

Bevor Sie einen Host hinzufügen und das Plug-in-Paket für Linux installieren, müssen Sie alle Anforderungen erfüllen.

- Wenn Sie iSCSI verwenden, muss der iSCSI-Dienst ausgeführt werden.
- Sie können entweder die passwortbasierte Authentifizierung für den Root- oder nicht-Root-Benutzer oder die SSH-Schlüsselauthentifizierung verwenden.
- Das SnapCenter-Plug-in für Unix-Dateisysteme kann von einem Benutzer installiert werden, der kein Root-Benutzer ist. Sie sollten jedoch die sudo-Berechtigungen für den nicht-Root-Benutzer konfigurieren, um den Plug-in-Prozess zu installieren und zu starten. Nach der Installation des Plug-ins werden die Prozesse als effektiver nicht-Root-Benutzer ausgeführt.
- Anmeldedaten mit Authentifizierungsmodus als Linux für den Installationsbenutzer erstellen.
- Sie müssen Java 11 auf Ihrem Linux-Host installiert haben.
- Stellen Sie sicher, dass Sie nur die zertifizierte Version von JAVA 11 auf dem Linux-Host installiert haben
- Informationen zum Herunterladen von JAVA finden Sie unter Java Downloads für alle Betriebssysteme
- Sie sollten bash als Standard-Shell für die Plug-in-Installation verwenden.

Voraussetzungen für die Datenbank – Aktivieren Sie Protokollierung und Backups

Um Offline-Protokolle zu aktivieren, ist ein vollständiges Offline-Backup der Datenbank erforderlich. In der Regel ist es bereits für produktive Systeme aktiviert.

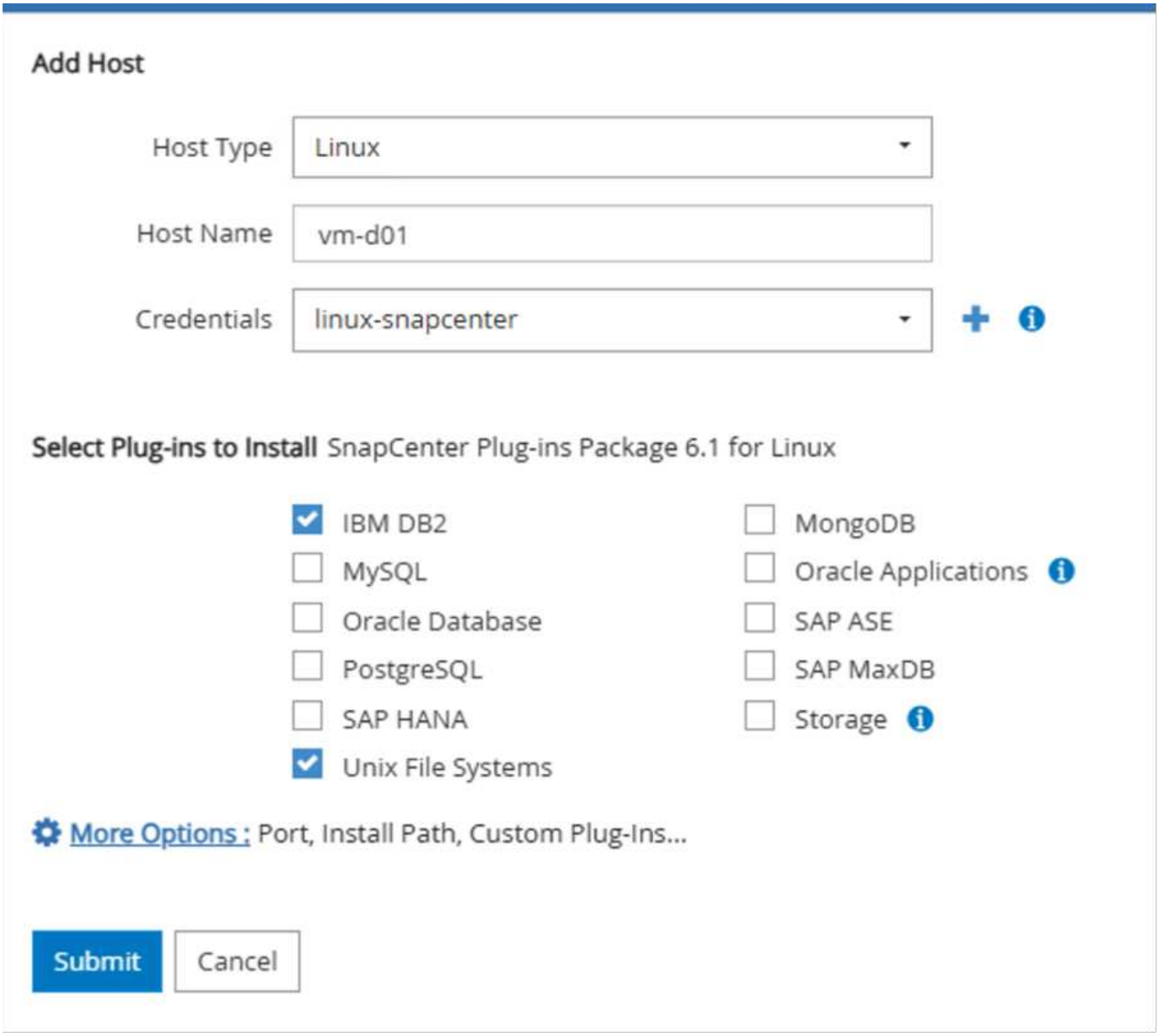
- Verzeichnisse für Backup und log_ARCH erstellen (/db2/D01/Backup, /sybase/D01/log_ARCH)
- Logarchmeth1 aktivieren (als OS-user db2d01)
  - db2-Update db cfg für D01 mit logarchmeth1-LAUFWERK:/db2/D01/log_ARCH/
- Offline-Backup erstellen (als OS-user db2d01)
  - Db2STOP-Kraft
  - Db2start Admin-Modus eingeschränkter Zugriff
  - db2 Backup db D01 auf /db2/D01/Backup

- db2 aktiviert db D01

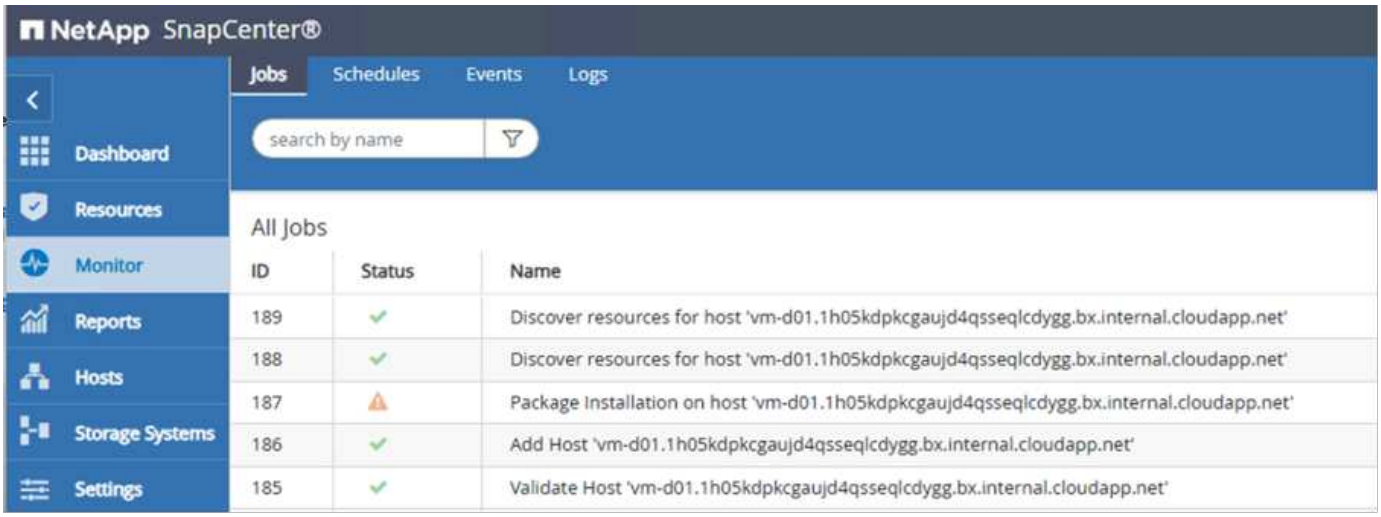
Bereitstellen des SnapCenter-Agenten auf der Host-vm-d01

Weitere Informationen finden Sie im "SnapCenter-Dokumentation".

Wählen Sie IBM DB2 und Unix File Systems Plugins aus.



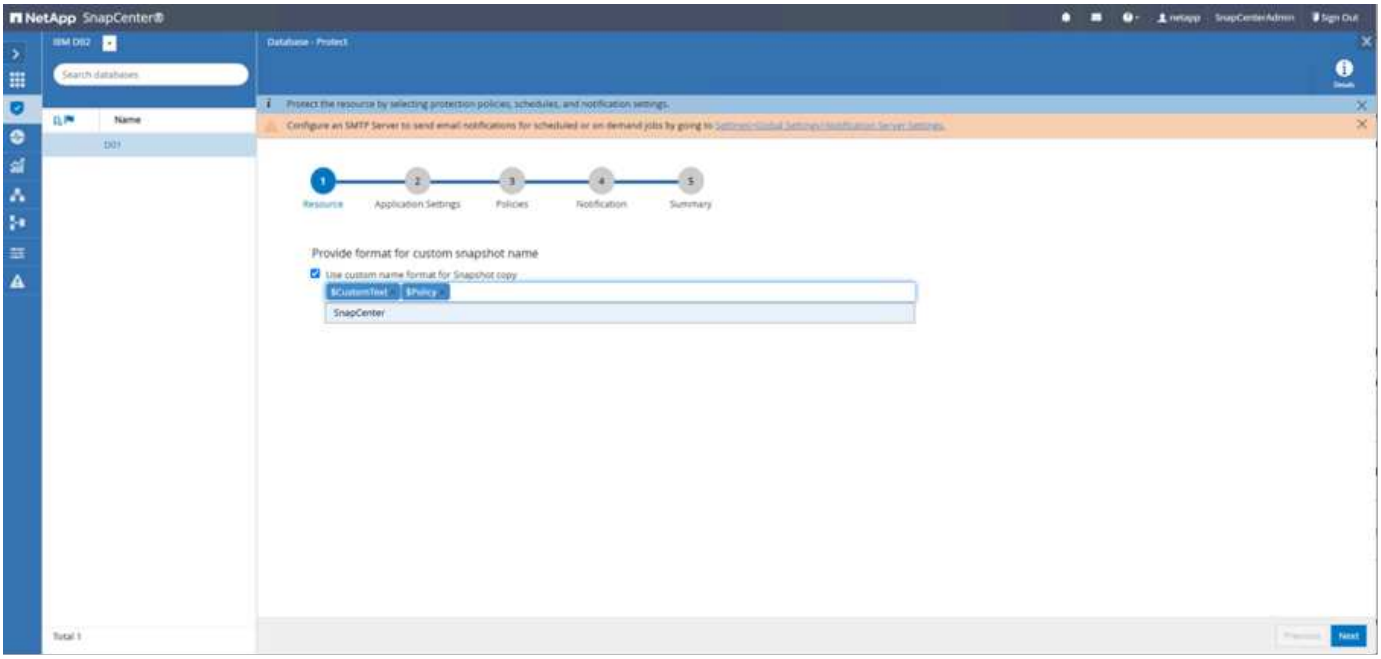
Nach der Installation wird eine Erkennung der Datenbanken auf dem Host ausgelöst.



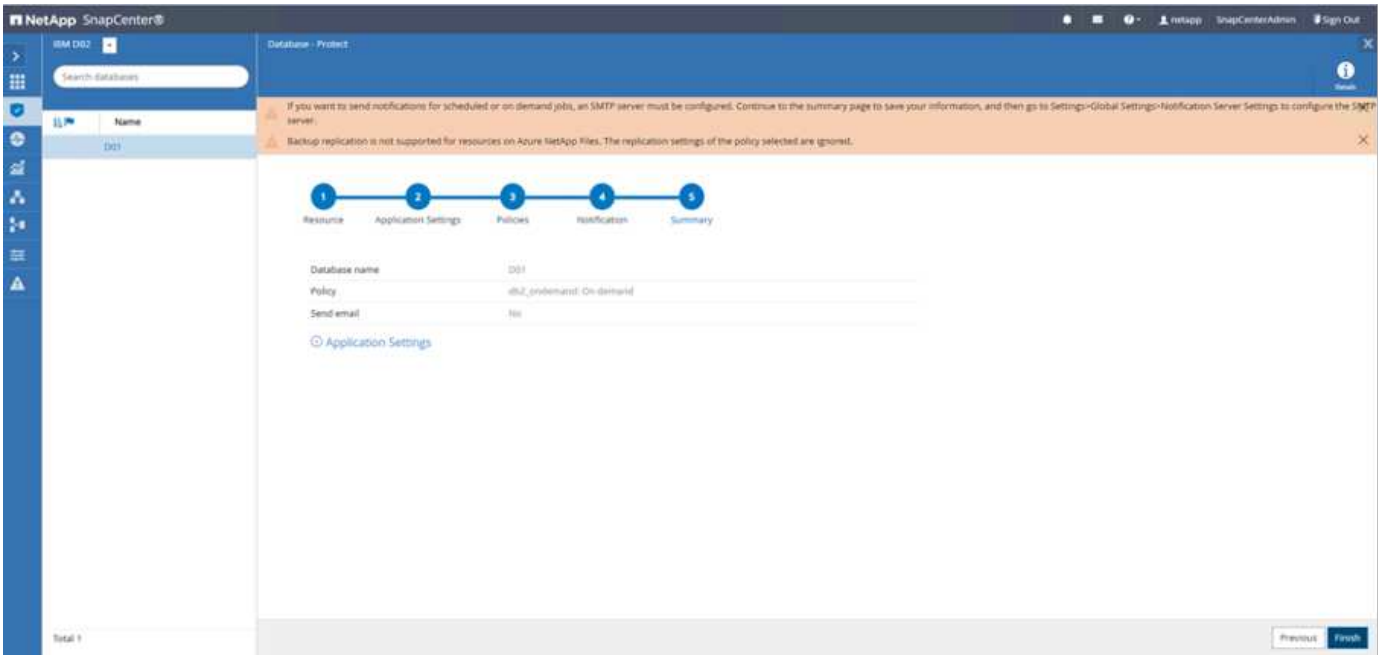
Ressourcenkonfiguration für Datenbank D01 erstellen

Wählen Sie erkannte Ressource D01

Konfigurieren Sie Den Snapshot-Namen



Es sind keine spezifischen Anwendungseinstellungen erforderlich. Konfigurieren Sie Richtlinien- und Benachrichtigungseinstellungen nach Bedarf.



Und beenden Sie die Konfiguration.

Sequenz zum Wiederherstellen von System D01

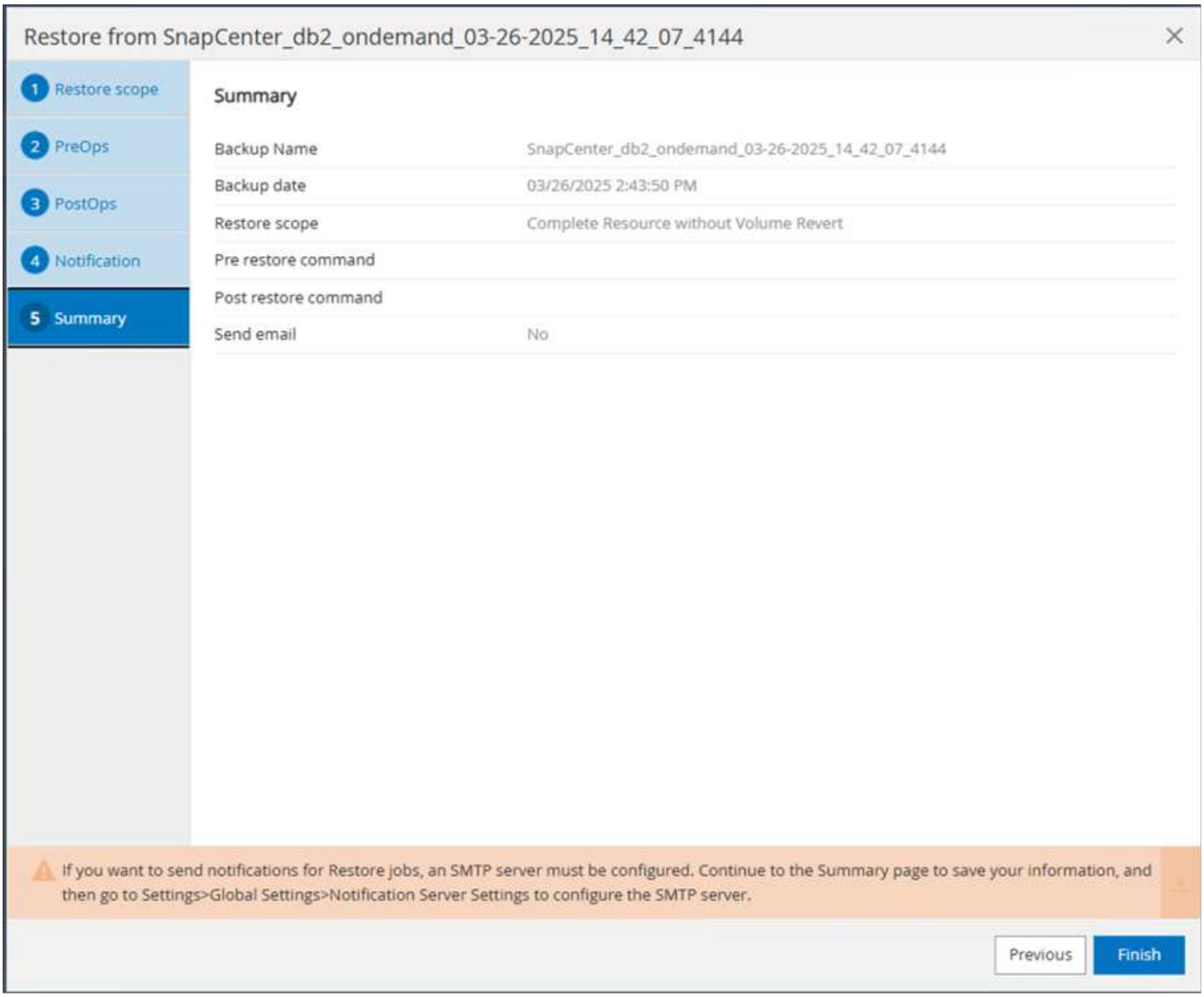
1. SAP System D01 stoppen (einschließlich Datenbank)
2. SnapCenter-Sicherung wiederherstellen (Volume D01-Daten)
   a. Unmounten Sie Dateisysteme
   b. Volume Wiederherstellen
   c. Mounten Sie Dateisysteme
   d. Initialisieren Sie die Datenbank als Spiegel db
3. Datenbank D01 wiederherstellen (mit db2 Rollforward)
4. Starten Sie SAP System D01

Datenbank D01 wiederherstellen

- Beenden Sie SAP System + DB D01 auf Host vm-d01
  - User d01adm: Stopp
- Backup Wiederherstellen
  - SnapCenter GUI: Wählen Sie erforderliche Sicherung für Wiederherstellung

- Für die ANF Implementierung – nur vollständige Ressource verfügbar

Die Zusammenfassung wird angezeigt und mit „Fertig stellen“ wird die eigentliche Wiederherstellung gestartet.



„Db2inidb D01 als Spiegel“ wird im Rahmen des SnapCenter-Wiederherstellungs-Workflows ausgeführt.

- Überprüfen Sie den Wiederherstellungsstatus Datenbank D01 (als Benutzer db2d01)
  - db2 Rollforward db D01 Abfragestatus
- Datenbank nach Bedarf wiederherstellen – hier ist eine verlustfreie Wiederherstellung angestachelt (als Benutzer db2d01)
  - db2 Rollforward db D01 zum Ende der Protokolle
- Stoppen Sie die Datenbankwiederherstellung und Online-Datenbank D01 (als Benutzer db2d01)
  - db2 Rollforward db D01 Stopp
- SAP-System starten (als Benutzer d01adm)
  - Startsap

Zusätzliche Informationen und Versionsverlauf

Folgende neu kodierte Demos stehen zur Unterstützung der Dokumentation zur Verfügung.

Installation und Konfiguration DB2 Plugin, Backup der DB2-Datenbank

Wiederherstellung und Recovery von DB2-Datenbanken

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- "SAP auf DB2 Installation Azure auf ANF"
- "SnapCenter-Voraussetzungen für Plugins"
- "SnapCenter Installations-Plugins"
- "Dokumentation zum SnapCenter DB2 Plug-in"
- SAP-Hinweise (Anmeldung erforderlich)
  - 83000 - DB2/390: Backup- und Recovery-Optionen: https://me.sap.com/notes/83000
  - 594301 - DB6: Admin Tools und Split Mirror: https://me.sap.com/notes/594301
- NetApp Produktdokumentation: https://www.netapp.com/support-and-training/documentation/
- "NetApp SAP-Lösungen – Informationen zu Anwendungsfällen, Best Practices und Vorteilen"

Versionsverlauf

Version	Datum	Versionsverlauf des Dokuments
Version 1.0	April 2025	Erste Version – Backup / Recovery DB2-Datenbank

SnapCenter Integration für SAP MaxDB Datenbank

In diesem Dokument werden die Besonderheiten der SnapCenter Integration für die in einer SAP-Umgebung verwendete SAP MaxDB Datenbank beschrieben.

Einführung

Das Dokument soll keine Schritt-für-Schritt-Beschreibung der Einrichtung der gesamten Umgebung sein, sondern umfasst Konzepte und relevante Details zu:

- Beispiel für eine Konfigurationsübersicht
- Beispiellayout
- Sicherung der SAP MaxDB Instanz
- Wiederherstellung der SAP MaxDB Instanz

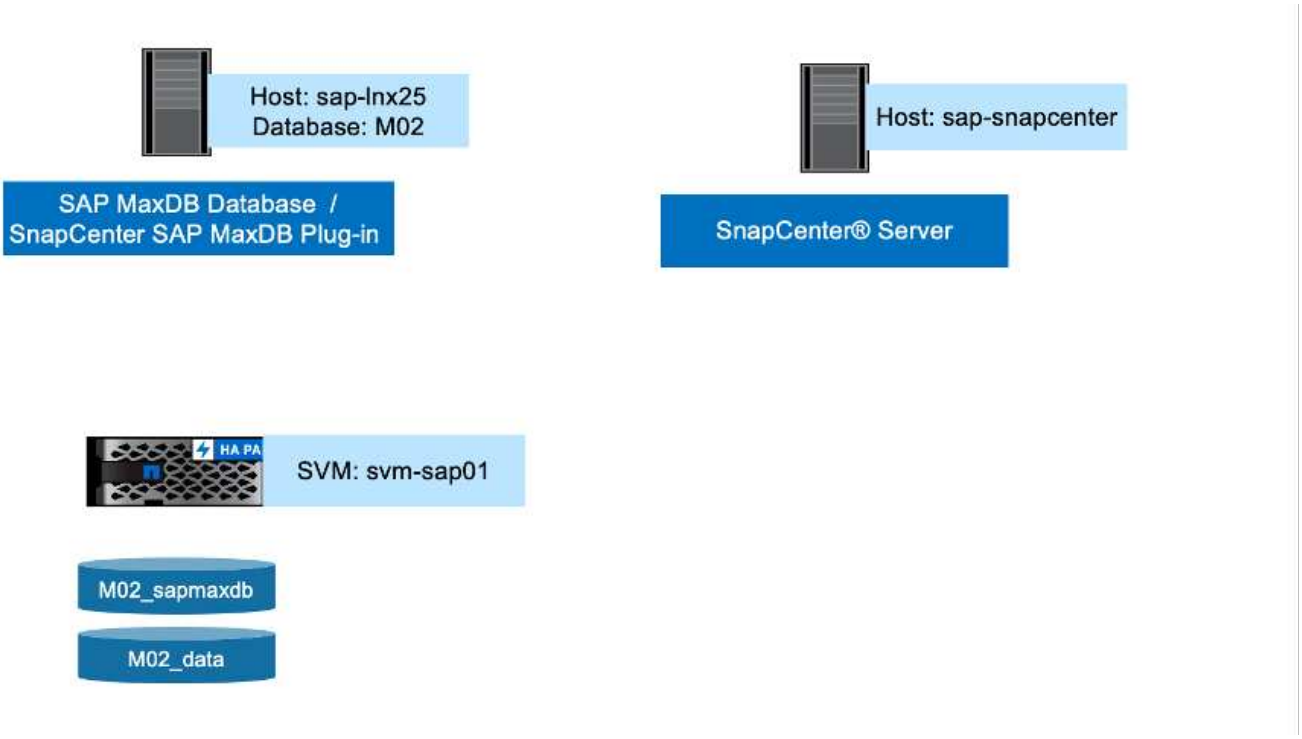
Beispiel für eine Konfigurationsübersicht

Beispiel Implementierung für das SnapCenter MaxDB Plugin für ein SAP System in unserem Demo Center.

Diese Implementierung beschreibt die minimal erforderliche Volume-Konfiguration. Data Dump Backups und Log Dump Backups, Backup Templates, etc. Werden nach SAP Note „1928060 - Datensicherung und Recovery mit Dateisystem Backup“ konfiguriert und von dort aus auf Notes verwiesen.

Alternativ kann die in beschriebene Volume-Struktur "MS TechCommunity Blog"verwendet werden.

Demo-Umgebung



Softwareversionen

Software	Version
Linux BS	SLES FÜR SAP 15 SP5
SAP	SAP NetWeaver 7.5 unterstützt
SAP MaxDB	DBMServer 7.9.10 Build 004-123-265-969
SnapCenter	6,1

MaxDB Volume-Design

Das folgende Least-Volume-Layout muss verwendet werden, um Backup / Recovery und Klonfälle für die SAP MaxDB Datenbank zu ermöglichen. Die Beispielkonfiguration verwendet <SID>: M02.

Volumenname	Verzeichnis (qtree) auf Volumen	Mount-Punkt auf Server	Kommentar
<SID>_sapmaxdb	sapdb	/Sapdb	Übergeordnetes Verzeichnis für MaxDB-bezogene Dateien
		/Sapdb/<SID>/saplog	Redo-Logs (können auf einem anderen Volume platziert werden)
		/Sapdb/<SID>/Backup	Dump Backups (Daten + Protokoll) (kann auf einem anderen Volume platziert werden)

Volumenname	Verzeichnis (qtree) auf Volumen	Mount-Punkt auf Server	Kommentar
	<sid>-Lösungen m	/Home/<sid>-Programm m	Home Verzeichnis der Benutzer <sid> Hmm
	sdb	/Home/sdb	Home-Verzeichnis von Benutzer sdb
	<sid>	/Home/<sid>	Home-Verzeichnis von Benutzer <sid>
	Usrsaptrans	/Usr/sap/trans	Transportverzeichnis
	<SID>	/Usr/sap/<SID>	Usr sap
	<SID>	/Sapmnt/<SID>	SAP GlobalHost-Verzeichnis
<SID>_Data	Sapdata	/Sapdb/<SID>/sapdata	DB-Datendateien (SID)

Schritte zum Schutz von Datenbank M02

- Prüfen Sie die Dateiverteilung gemäß dem Beispiellayout
- Voraussetzungen für den Host prüfen (sap-lnx25)
- Voraussetzungen für die Datenbank prüfen (M02)
- SnapCenter-Agent auf Host bereitstellen/installieren (sap-lnx25)
- Erstellen Sie die Ressourcenkonfiguration der SnapCenter-Instanz

Voraussetzungen auf Host

Weitere aktuelle Informationen stehen zur Verfügung"Hier".

Bevor Sie einen Host hinzufügen und das Plug-in-Paket für Linux installieren, müssen Sie alle Anforderungen erfüllen.

- Wenn Sie iSCSI verwenden, muss der iSCSI-Dienst ausgeführt werden.
- Sie können entweder die passwortbasierte Authentifizierung für den Root- oder nicht-Root-Benutzer oder die SSH-Schlüsselauthentifizierung verwenden.
- Das SnapCenter-Plug-in für Unix-Dateisysteme kann von einem Benutzer installiert werden, der kein Root-Benutzer ist. Sie sollten jedoch die sudo-Berechtigungen für den nicht-Root-Benutzer konfigurieren, um den Plug-in-Prozess zu installieren und zu starten. Nach der Installation des Plug-ins werden die Prozesse als effektiver nicht-Root-Benutzer ausgeführt.
- Anmeldedaten mit Authentifizierungsmodus als Linux für den Installationsbenutzer erstellen.
- Sie müssen Java 11 auf Ihrem Linux-Host installiert haben.
- Stellen Sie sicher, dass Sie nur die zertifizierte Version von JAVA 11 auf dem Linux-Host installiert haben
- Informationen zum Herunterladen von JAVA finden Sie unter Java Downloads für alle Betriebssysteme
- Sie sollten bash als Standard-Shell für die Plug-in-Installation verwenden.

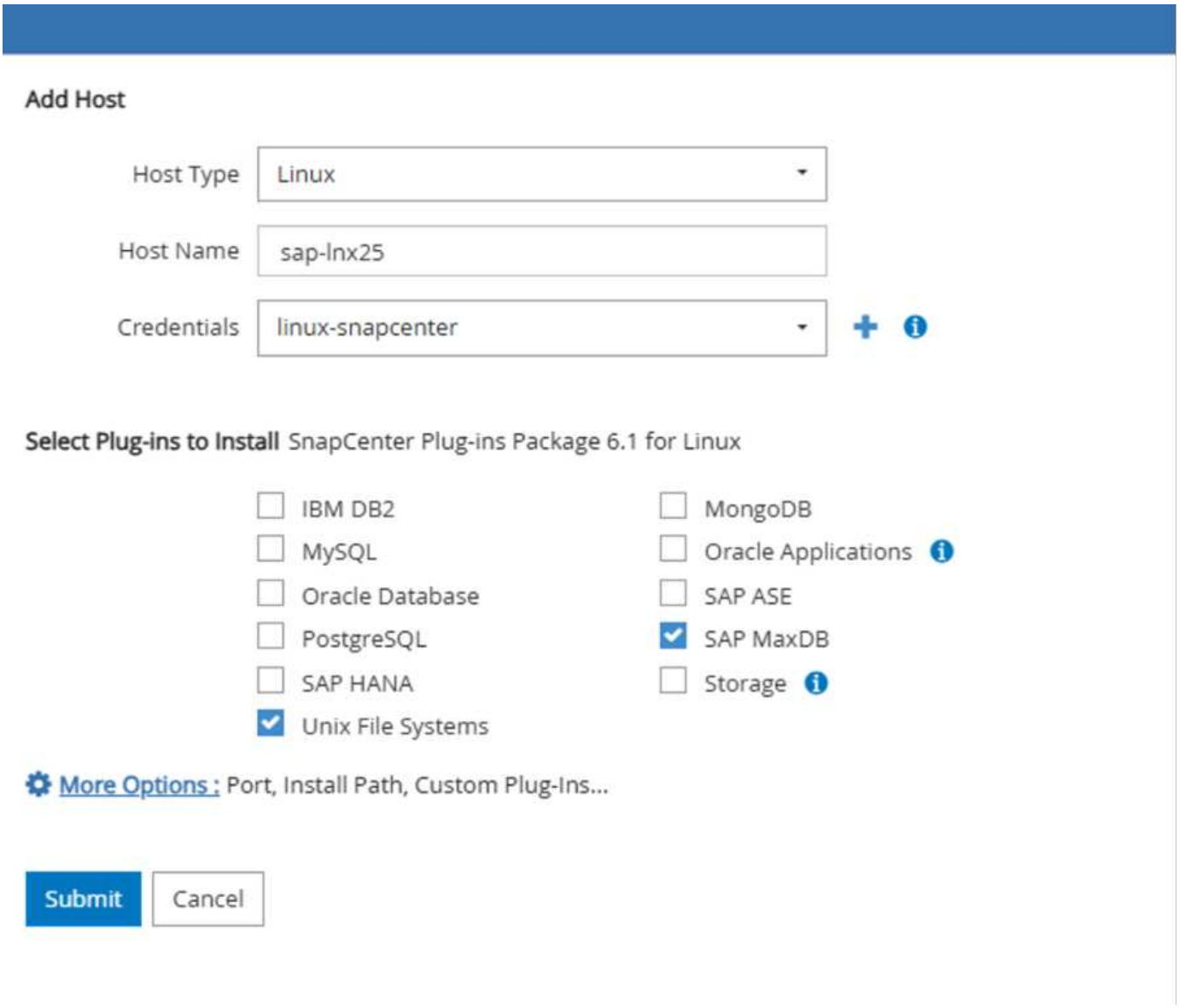
Voraussetzungen für die Datenbank – Backup-Vorlagen erstellen, Logbackup aktivieren

- Erstellen von Verzeichnissen für Daten- und Protokollsicherungen (/sapdb/M02/Backup/Data, /sapdb/M02/Backup/log – owner sdb:sdba – Permissions 755)
- Verbindung zur Datenbank M02 (als OS-User sqdm02)
  - Dbmcli -d M02 -U CONTROL,<password>
- Erstellen Sie eine Data File Backup Template (M02_DATA) gemäß SAP Note 1928060
  - Backup_template_create M02_DATA in DATEI /sapdb/M02/Backup/Data/M02_DATA INHALTSDATEN
- Erstellen Sie eine Data Backup Template (M02_LOG) gemäß SAP Note 1928060
  - Backup_template_create M02_LOG in DATEI /sapdb/M02/Backup/LOG/M02_LOG content LOG
- Erstellen Sie eine Data Snapshot Backup Template (M02_SNAP) gemäß SAP Note 1928060
  - Backup_template_create M02_SNAP auf EXTERNEN SNAPSHOT
- Erstellen Sie Fake-Backup, um die PROTOKOLLSICHERUNG zu aktivieren
  - Util_connect
  - Backup_Start M02_SNAP
  - Backup_Finish M02_SNAP ExternalBackupID First_Full_Fake_Backup
- Wechseln Sie In Den Datenbank-Protokollierungsmodus
  - autolog_off
  - autolog_ON M02_LOG INTERVALL 300
  - autolog_show

Bereitstellung von SnapCenter-Agent für das Hosting von sap-lnx25

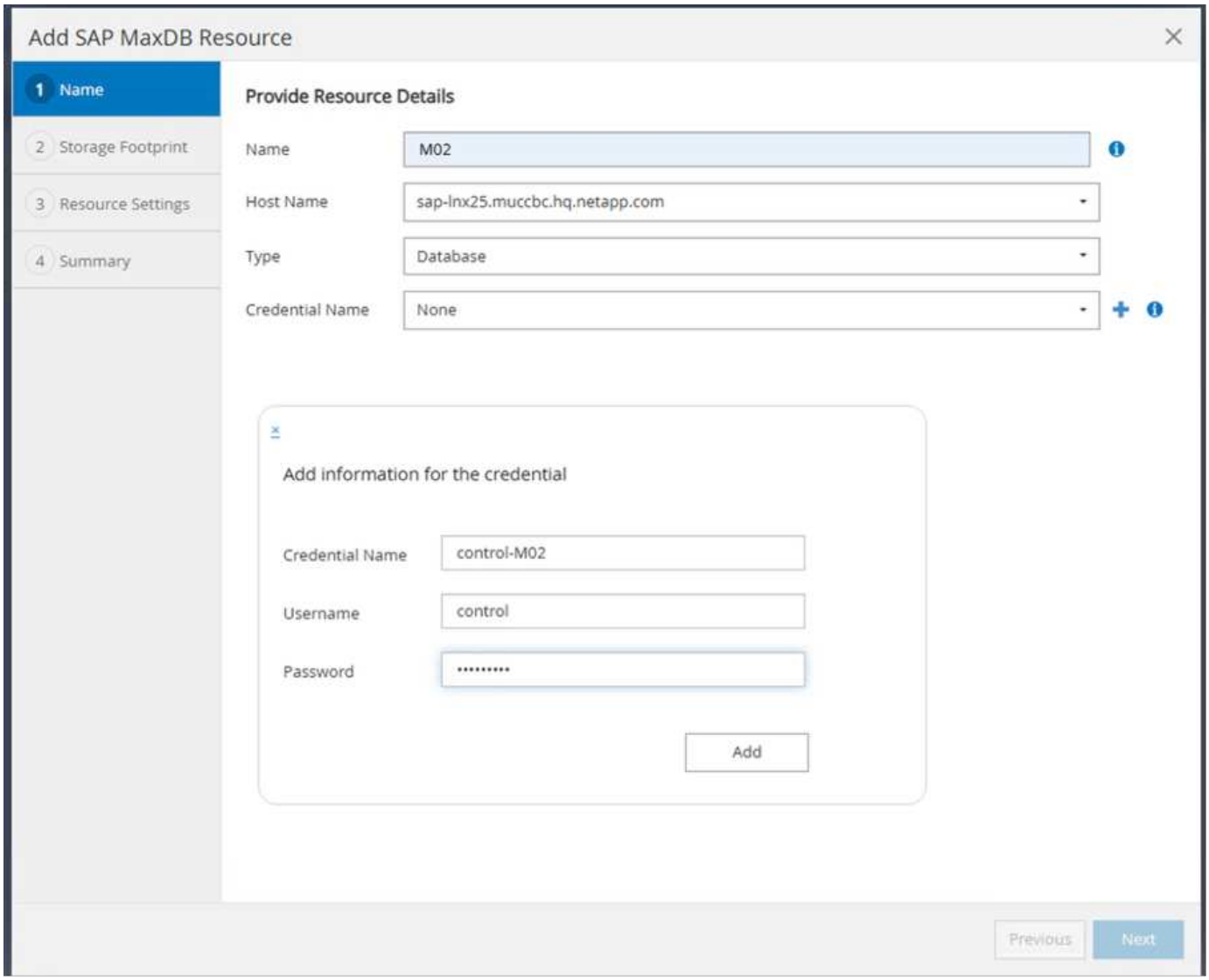
Weitere Informationen finden Sie im "SnapCenter-Dokumentation".

Wählen Sie SAP MaxDB und Unix File Systems Plugins aus.

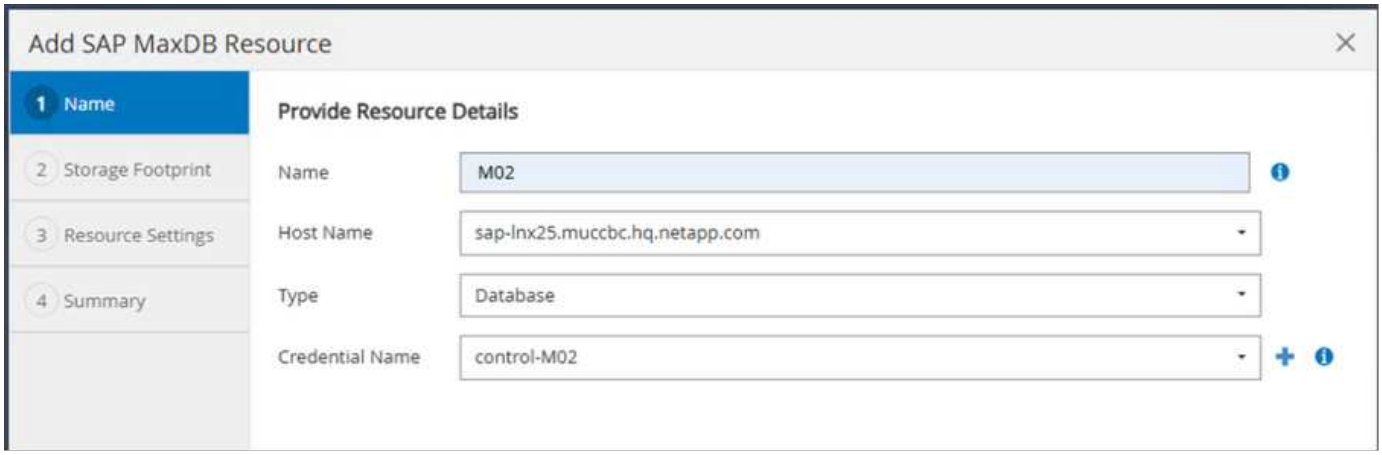


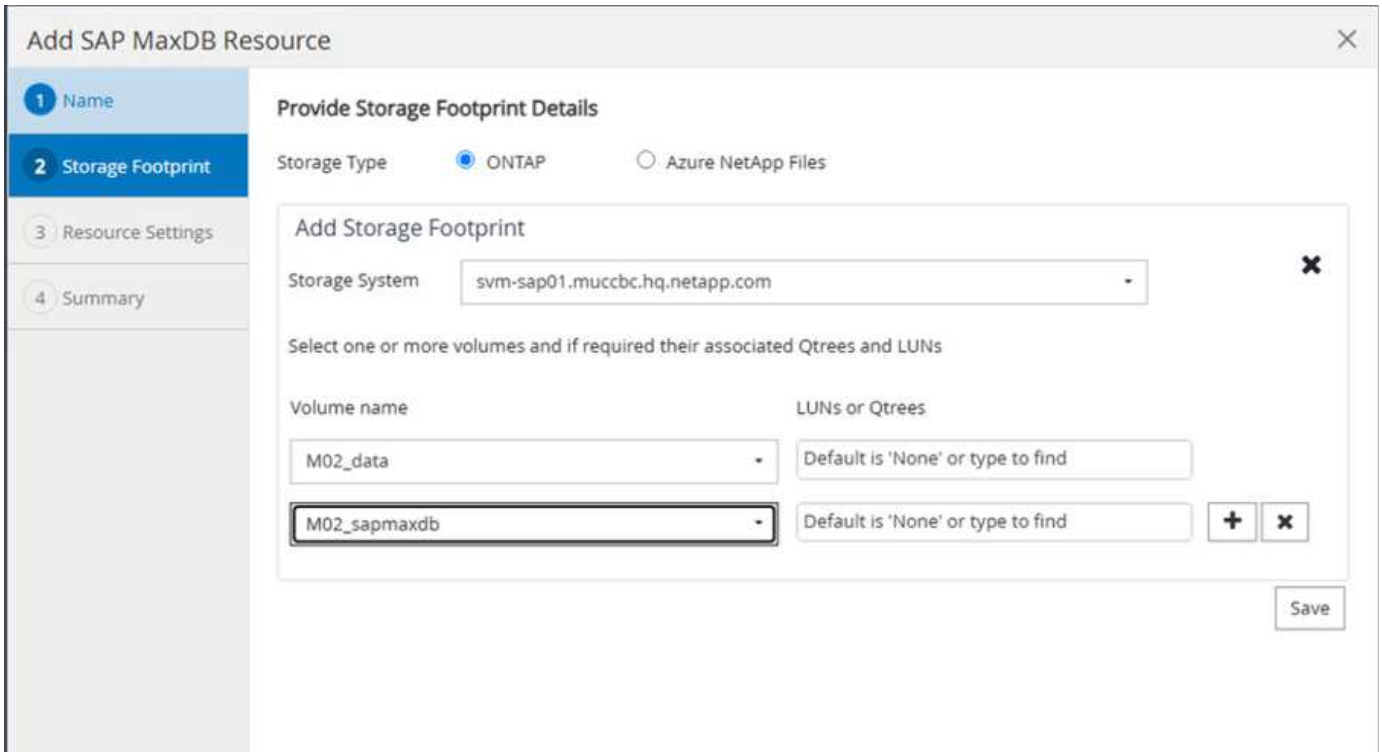
Erstellen Sie eine SnapCenter-Ressourcenkonfiguration für Datenbank M02

Ressourcen → SAP MaxDB → Ressourcen hinzufügen

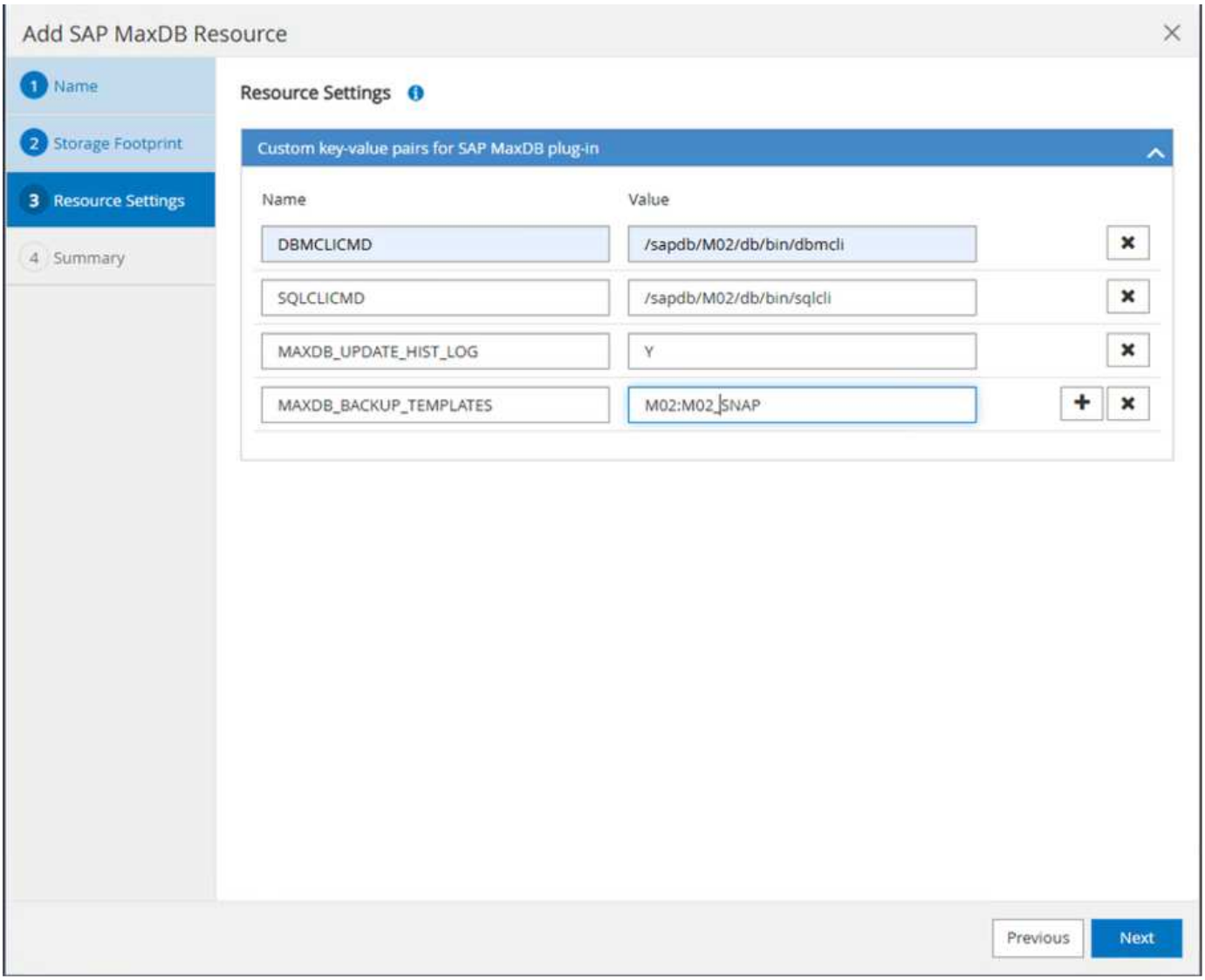


Wenn das Passwort Sonderzeichen enthält, müssen diese mit einem Backslash maskiert werden (z. B. Test!123! → Test\!123\!).





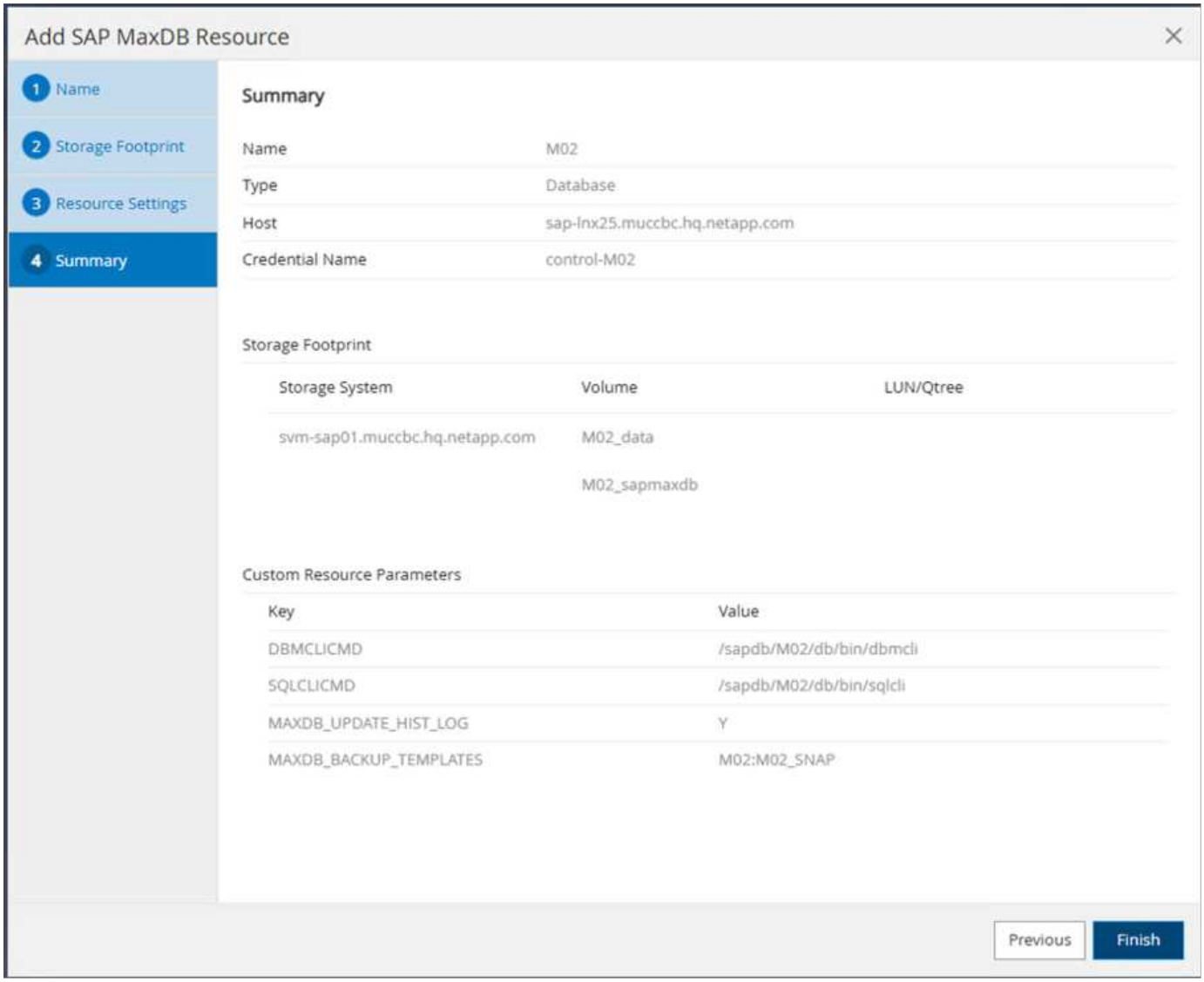
Im Anschluss an die Ressourceneinstellungen müssen (mindestens) benutzerdefinierte Schlüssel-Wert-Paare erstellt werden.



In der folgenden Tabelle sind die MaxDB Plug-in-Parameter aufgeführt, ihre Einstellungen aufgeführt und beschrieben:

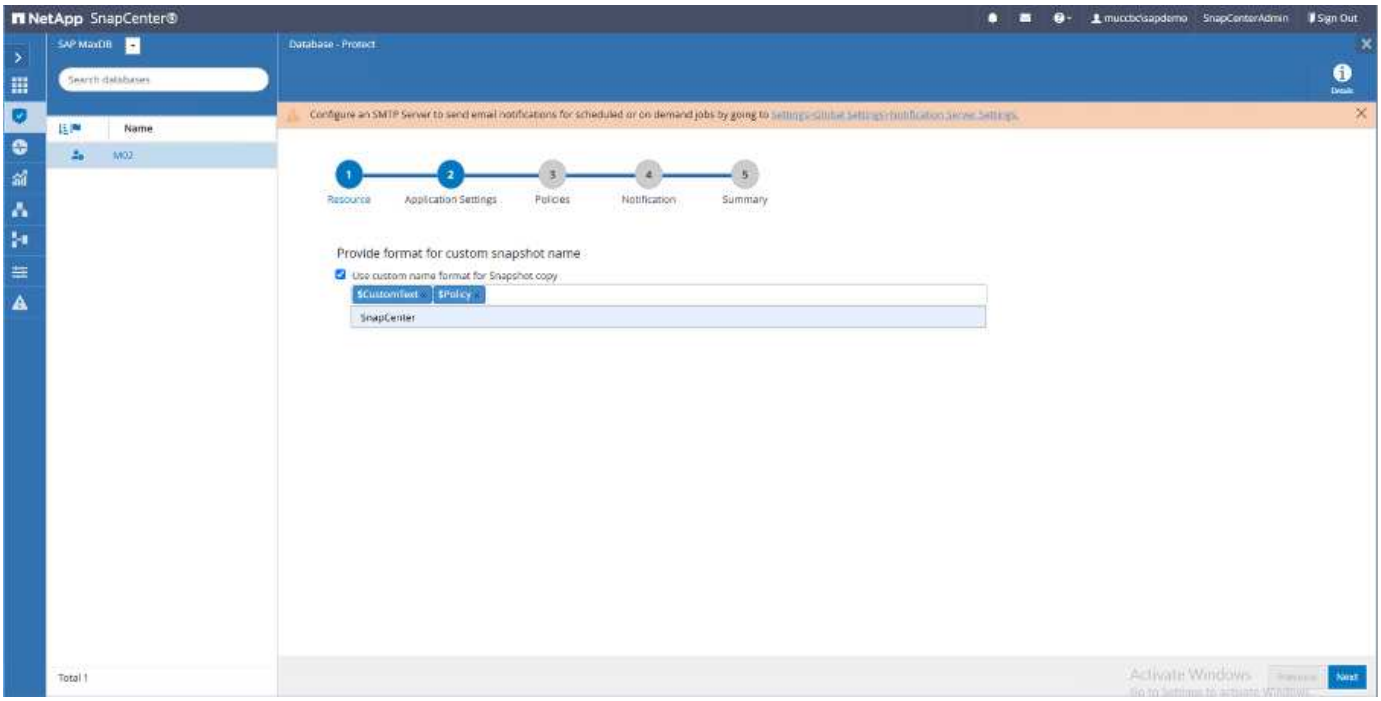
Parameter	Einstellung	Beschreibung
HANDLE_LOGWRITER	(J/N)	Führt die Vorgänge zum Anhalten des Logwriters (N) aus oder führt den Protokollwriter (Y) wieder aus.
DBMCLICMD	Pfad_zu_dbmcli_cmd	Gibt den Pfad zum Befehl MaxDB dbmcli an.Falls nicht gesetzt, wird dbmcli auf dem Suchpfad verwendet.
SQLCLICMD	Pfad_zu_sqlcli_cmd	Gibt den Pfad für den MaxDB sqlcli Befehl an.Wenn nicht festgelegt, wird sqlcli auf dem Suchpfad verwendet.
MAXDB_UPDATE_HIST_LOG	(J/N)	Weist das MaxDB Backup-Programm an, unabhängig davon, ob das MaxDB-Verlaufsprotokoll aktualisiert wird.

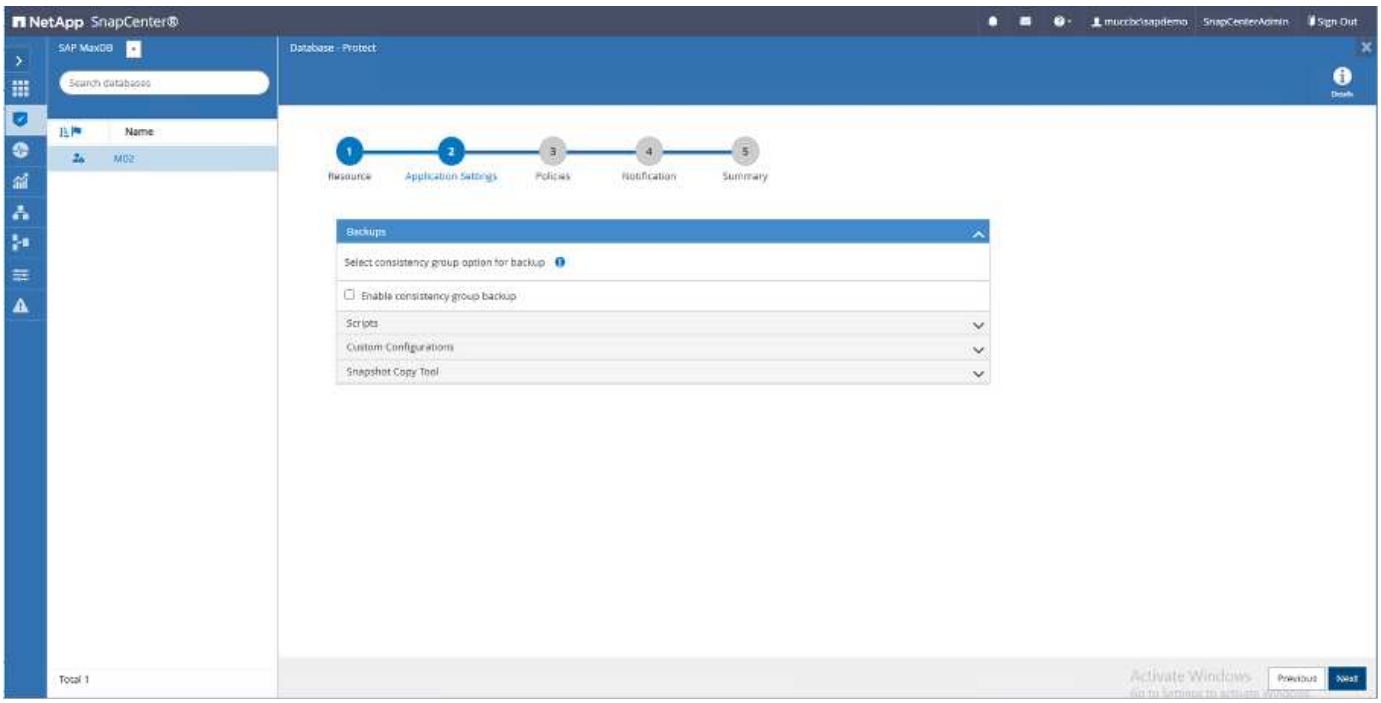
Parameter	Einstellung	Beschreibung
MAXDB_BACKUP_TEMPLATES	Template_Name (z.B. `M02_SNAP`)	Gibt eine Sicherungsvorlage für jede Datenbank an.die Vorlage muss bereits vorhanden sein und ein externer Typ von Backup-Vorlage sein. Um die Integration von Snapshot Kopien für MaxDB 7.8 und höher zu aktivieren, müssen Sie über eine Hintergrundserverfunktion von MaxDB und bereits konfigurierte MaxDB Backup-Vorlage verfügen.
MAXDB_BG_SERVER_PREFIX	bg_Server_PREFIX (z.B. `na_bg`)	Gibt das Präfix für den Namen des Hintergrundservers an. Wenn der Parameter MAXDB_BACKUP_TEMPLATES festgelegt ist, müssen Sie auch DEN PARAMETER MAXDB_BG_SERVER_PREFIX festlegen. Wenn Sie das Präfix nicht festlegen, wird der Standardwert na_bg_DATABASE verwendet.

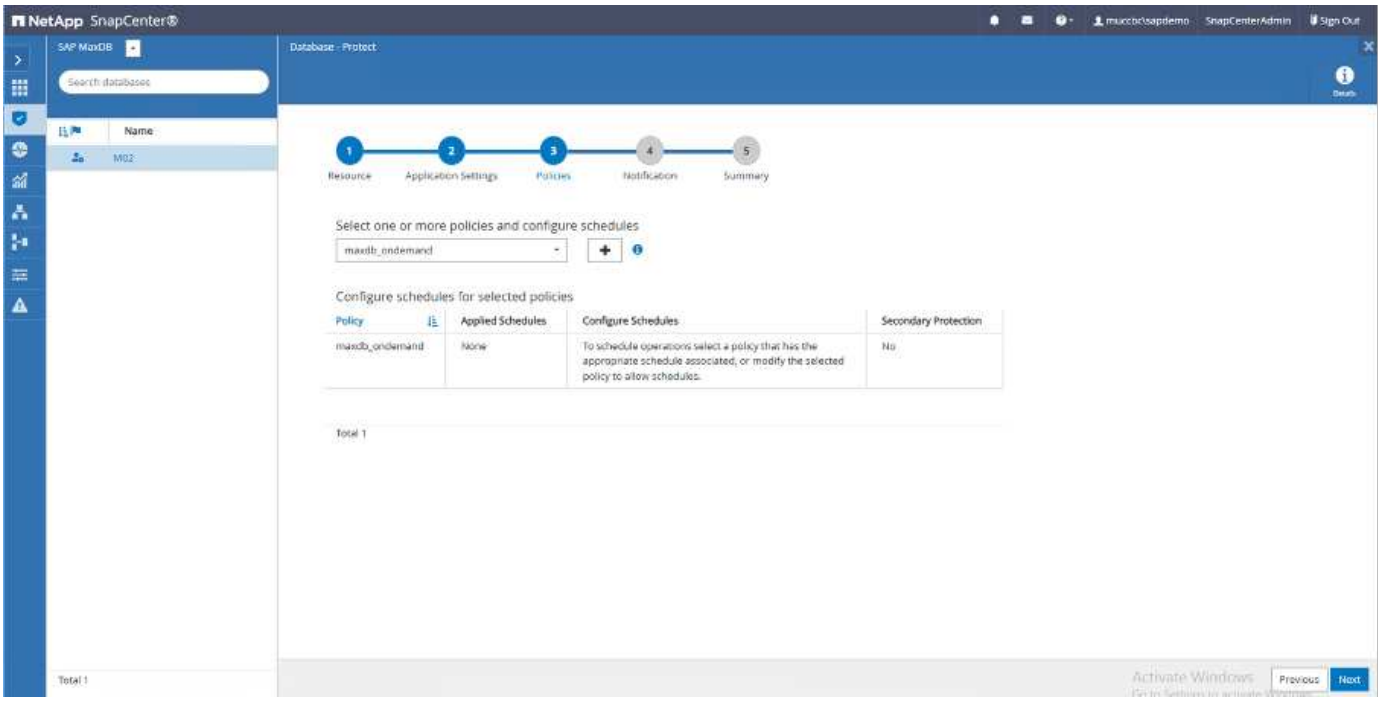


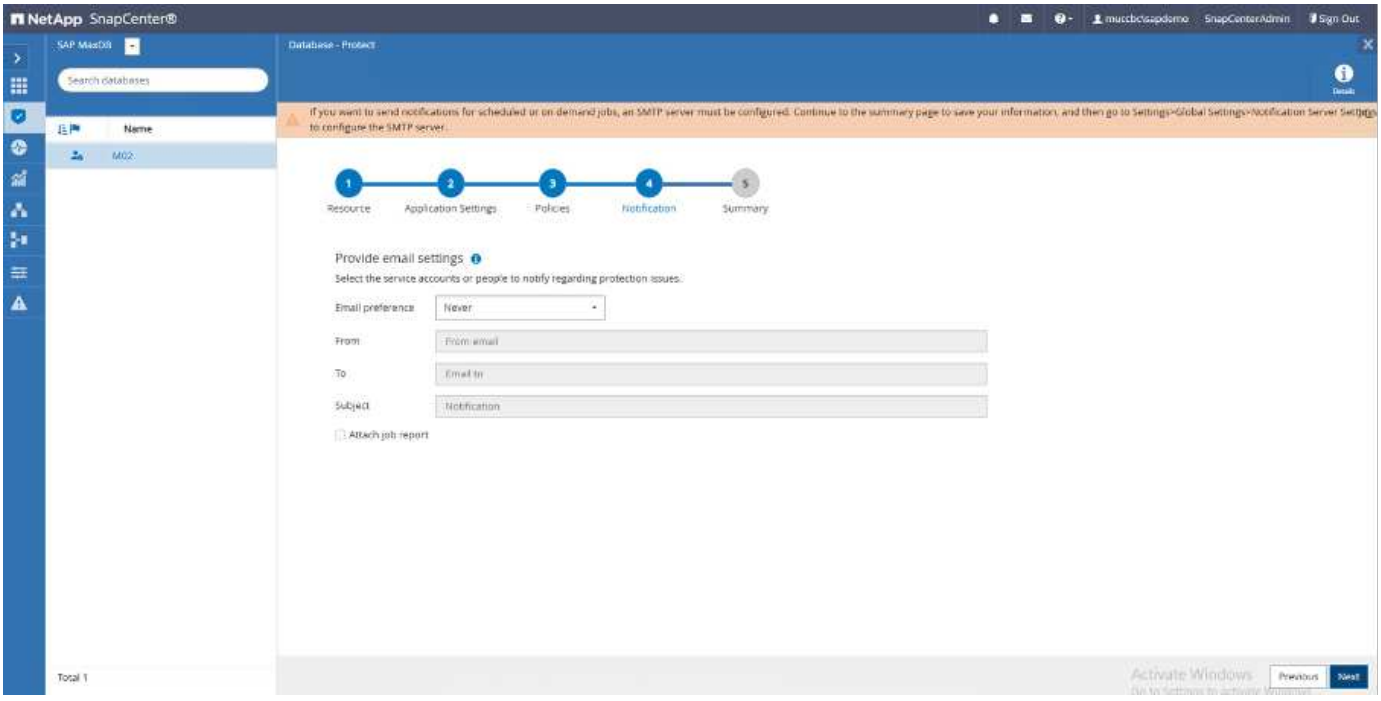
Nun könnte die Konfiguration abgeschlossen und die Sicherung nach dem Gesamtschutzkonzept geplant werden.

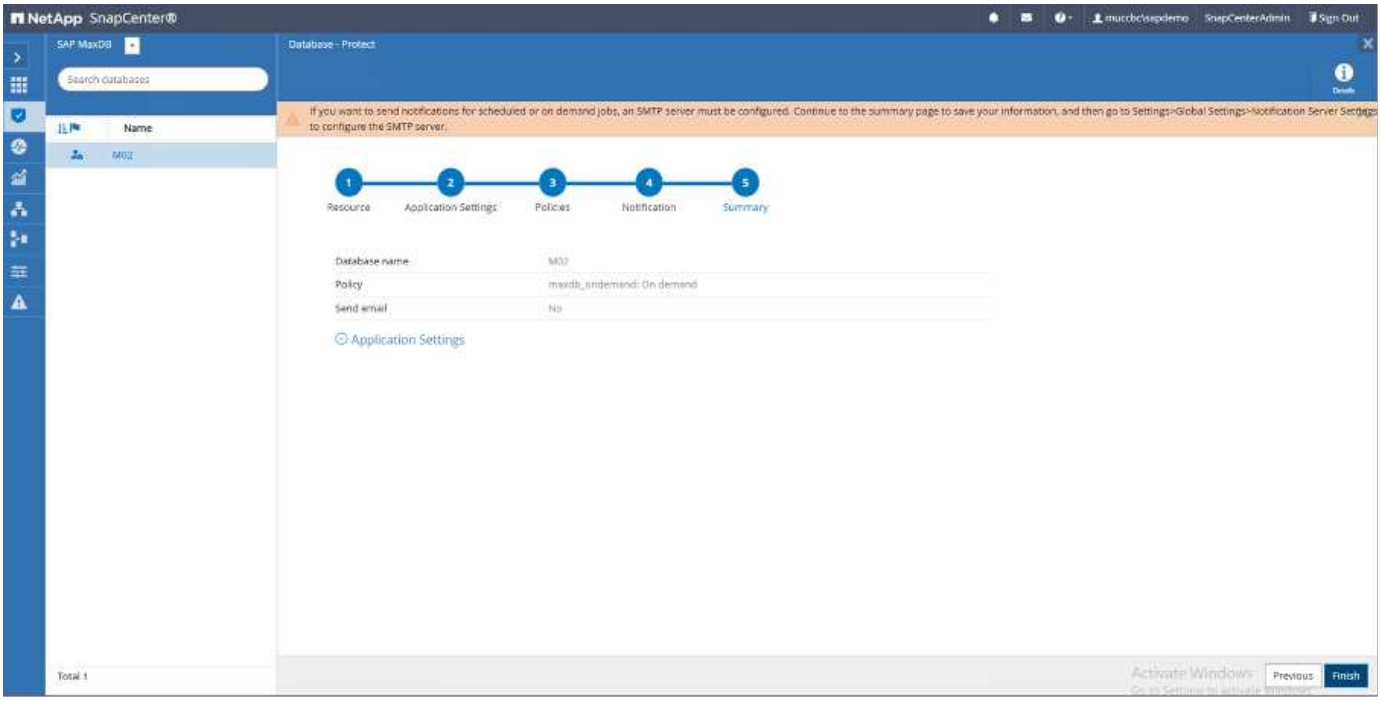
NetApp SnapCenter®
SAP MaxDB
View
Database
Search databases
Dashboard
Resources
Monitor
Reports
Hosts
Storage Systems
Settings
Alerts
Name
Type
Host
Resource Groups
Policies
Last backup
Overall Status
M02
Database
Not protected


NetApp SnapCenter®
SAP MaxDB
Search databases
Name
M02
Total 1
Database - Protect
Configure an SMTP Server to send email notifications for scheduled or on demand jobs by going to Settings>Global Settings>Notification Server Settings.
1 Resource
2 Application Settings
3 Policies
4 Notification
5 Summary
Provide format for custom snapshot name
Use custom name format for Snapshot copy
$CustomText
$Policy
SnapCenter
Next


NetApp SnapCenter®
SAP MaxDB
Search databases
Name
M02
Total 1
Database - Protect
1 Resource
2 Application Settings
3 Policies
4 Notification
5 Summary
Backups
Select consistency group option for backup
Enable consistency group backup
Scripts
Custom Configurations
Snapshot Copy Tool
Previous
Next


NetApp SnapCenter®
muccbc\sapdemo
SnapCenterAdmin
Sign Out
SAP MaxDB
Search databases
Name
M02
Total 1
Database - Protect
Details
1 Resource
2 Application Settings
3 Policies
4 Notification
5 Summary
Select one or more policies and configure schedules
maxdb_ondemand
Configure schedules for selected policies
Policy
Applied Schedules
Configure Schedules
Secondary Protection
maxdb_ondemand
None
To schedule operations select a policy that has the appropriate schedule associated, or modify the selected policy to allow schedules.
No
Total 1
Activate Windows
Previous
Next


NetApp SnapCenter®
muccbc\sapdemo
SnapCenterAdmin
Sign Out
SAP MaxDB
Search databases
Name
M02
Total 1
Database - Protect
Details
If you want to send notifications for scheduled or on demand jobs, an SMTP server must be configured. Continue to the summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.
1 Resource
2 Application Settings
3 Policies
4 Notification
5 Summary
Provide email settings
Select the service accounts or people to notify regarding protection issues.
Email preference
Never
From
From email
To
Email to
Subject
Notification
Attach job report
Activate Windows
Previous
Next

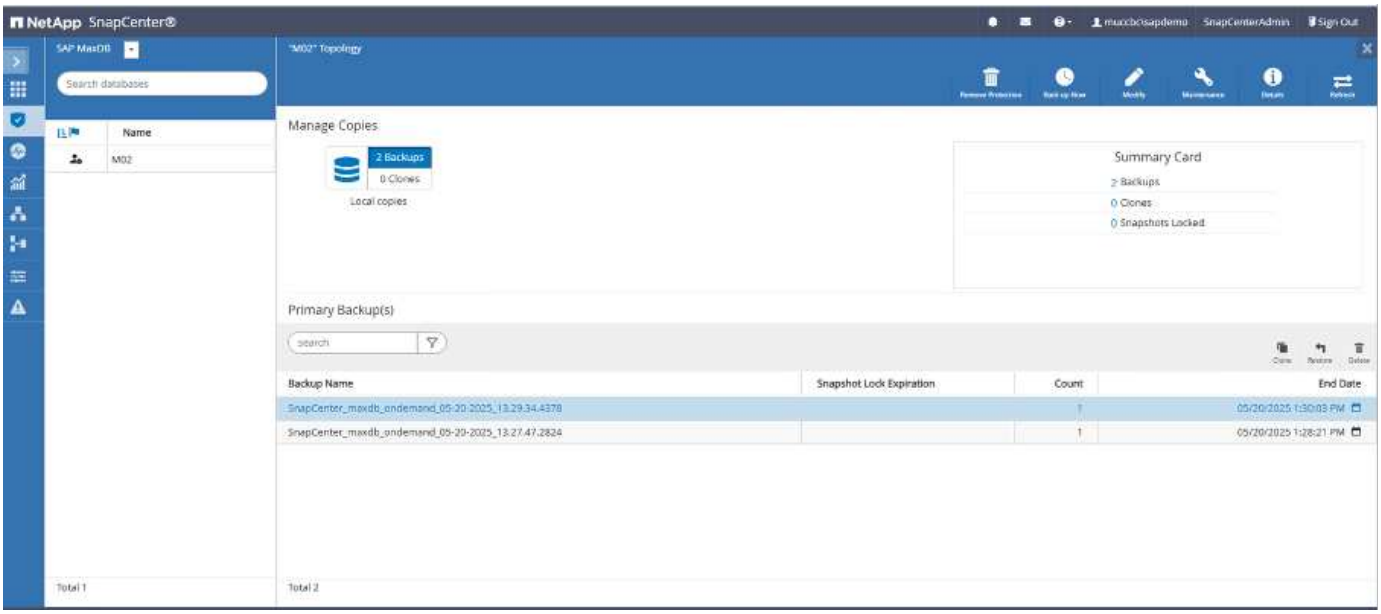


Sequenz zum Wiederherstellen von System M02

1. SAP System M02 stoppen (einschließlich Datenbank), sapinit stoppen
2. Umount Filesystem /sapdb/M02/sapdata
3. Wiederherstellen von Volumes M02_Data (mit SnapCenter)
4. Mounten Sie das Dateisystem /sapdb/M02/sapdata
5. Datenbank M02 starten und verbinden (Admin-Modus)
6. Backup-Informationen Erfassen
7. Stellen Sie das Backup von Datenbankdaten wieder her
8. Stellen Sie die Datenbank-Protokollsicherungen wieder her
9. Datenbank anhalten
10. Starten Sie sapinit, SAP System M02

Instanz M02 wiederherstellen

- Beenden Sie SAP System + DB M02 auf Host sap-lnx25
  - User m02adm: Stopsap
  - Optional – Wenn die Datenbank nicht erfolgreich angehalten wurde – Benutzer: Sqdm02
  - Dbmcli -d M02 -U CONTROL,<password>
    - db_offline
  - User root: /Etc/init.d/sapinit stop
  - User root: Umount /sapdb/M02/sapdata
- Backup Wiederherstellen
  - SnapCenter GUI: Wählen Sie erforderliche Bacukp für die Wiederherstellung

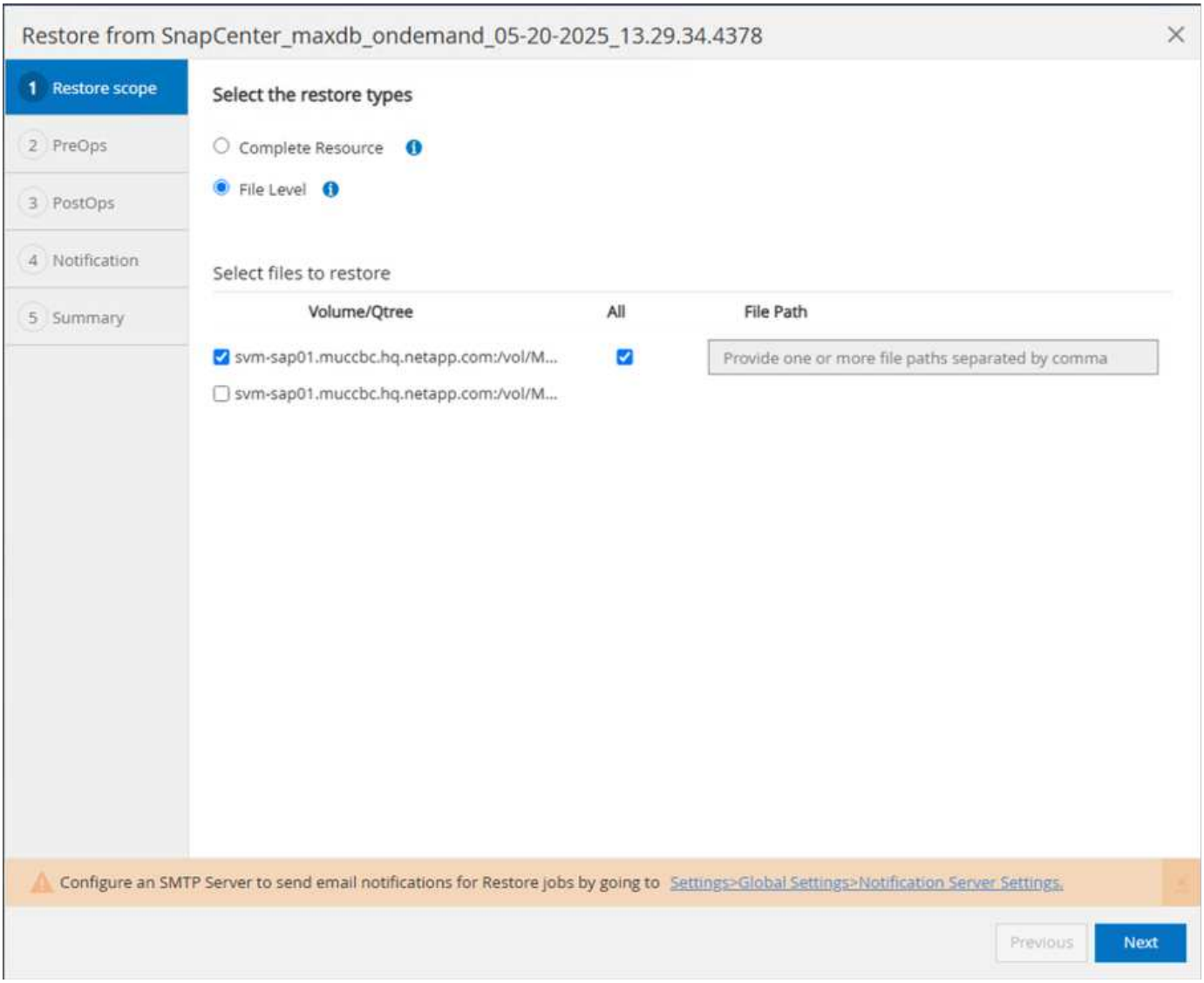


Wenn Sie die Option „Complete Resource“ auswählen, wird eine Volume-basierte Snap Restore (VBSR) ausgelöst. Innerhalb von Azure wird sie aufgerufen"Lautstärke zurücksetzen". Für die ANF-Bereitstellung * nur vollständige Ressource verfügbar*.

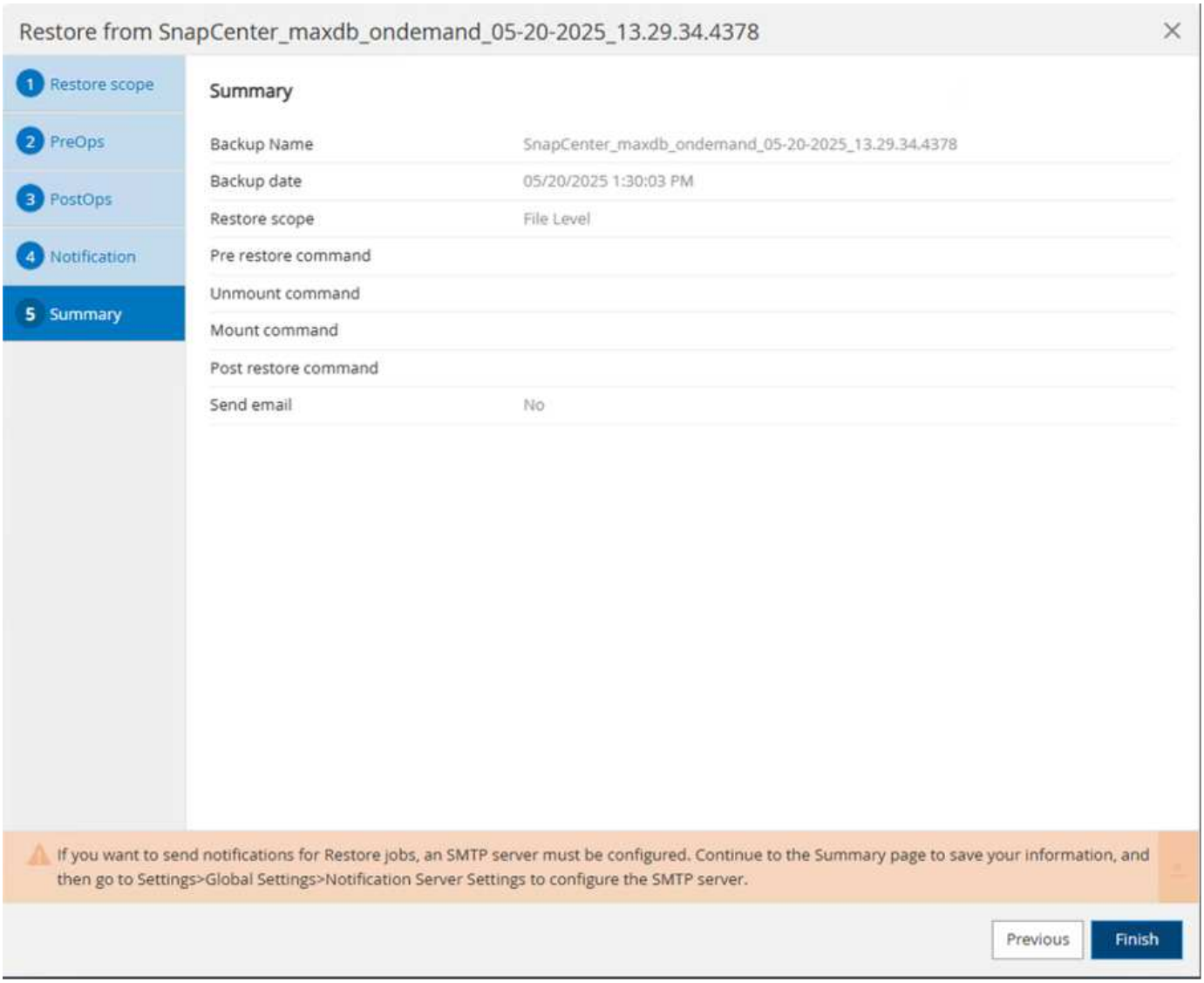
Important

Active filesystem data and snapshots that were taken after the selected snapshot will be lost. The snapshot revert operation will replace *all* the data in the targeted volume with the data in the selected snapshot. You should pay attention to the snapshot contents and creation date when you select a snapshot. You cannot undo the snapshot revert operation.

Für andere Implementierungstypen (z. B. On-Premises-ANF) könnte ein SFSR-Vorgang (Single File Snap Restore) orchestriert werden. Wählen Sie File Level und das entsprechende Volume und aktivieren Sie „All“ – siehe folgenden Screenshot.



Die Zusammenfassung wird angezeigt und mit „Fertig stellen“ wird die eigentliche Wiederherstellung gestartet.



- Dateisysteme mounten (sap-lnx25)
  - User root: Mount /sapdb/M02/sapdata
- Datenbank M02 im Admin-Modus starten und verbinden
  - Benutzer: Sqdm02: Dbmcli -d M02 -U CONTROL,<password>
    - db_admin
    - db_Connect
- Backup-Informationen Erfassen
  - Backup_history_open
  - Backup_history_list -c Label,Aktion,Seiten,stop,media -r Last

```
dbmcli on M02>backup_history_list -c label,action,pages,stop,media -r last
OK
END
DAT_000000008|SAVE WARM|         0|2025-05-20 13:29:50|M02_SNAP

---
```

- Stellen Sie Die Datenbank Wieder Her

- Wiederherstellung Von Daten-Backups
  - Recover_Start M02_SNAP Data ExternalBackupID DAT_000000008

```
dbmcli on M02>recover_start M02_SNAP data ExternalBackupID DAT_000000008
OK
Returncode              0
Date                    20250520
Time                    00151550
Server                  sap-lnx25
Database                M02
Kernel Version          Kernel    7.9.10   Build 004-123-265-969
Pages Transferred       0
Pages Left
Volumes
Medianame               M02_SNAP
Location
Errortext
Label                   DAT_000000008
Is Consistent           true
First LOG Page          512226
Last LOG Page
DB Stamp 1 Date         20250520
DB Stamp 1 Time         00132933
DB Stamp 2 Date
DB Stamp 2 Time
Page Count
Devices Used            0
Database ID             sap-lnx25:M02_20241203_104036
Max Used Data Page      3187892
Converter Page Count

---
```

- Protokollsicherung bei Bedarf wiederherstellen
  - Z. B. Recover_Start M02_LOG LOG 147

```
[dbmcli on M02>recover_start M02_LOG LOG 147
OK
Returncode              0
Date                    20250521
Time                    00112001
Server                  sap-lnx25
Database                M02
Kernel Version          Kernel    7.9.10   Build 004-123-265-969
Pages Transferred       24
Pages Left              0
Volumes                 1
Medianame               M02_LOG
Location                /sapdb/M02/backup/log/M02_LOG.147
Errortext
Label                   LOG_000000147
Is Consistent
First LOG Page          514072
Last LOG Page           514075
DB Stamp 1 Date         20250520
DB Stamp 1 Time         00180238
DB Stamp 2 Date         20250520
DB Stamp 2 Time         00180539
Page Count              4
Devices Used            1
Database ID             sap-lnx25:M02_20241203_104036
Max Used Data Page
Converter Page Count
```

- Optionale Informationen – autorecover auf einen bestimmten Zeitstempel (ohne Angabe dedizierter Daten/Protokollbackp
  - Z. B. autorecover bis 20250520 200000

```
---
[dbmcli on M02>autorecover until 20250520 200000
OK
Returncode              0
Date                    20250521
Time                    00131559
Server                  sap-lnx25
Database                M02
Kernel Version          Kernel    7.9.10   Build 004-123-265-969
Pages Transferred       10096
Pages Left              0
Volumes                 1
Medianame               M02_LOG
Location                /sapdb/M02/backup/log/M02_LOG.102
Errortext
Label                   LOG_000000102
Is Consistent
First LOG Page          256227
Last LOG Page           341559
DB Stamp 1 Date         20241203
DB Stamp 1 Time         00190348
DB Stamp 2 Date         20241226
DB Stamp 2 Time         00193615
Page Count              85333
Devices Used            1
Database ID             sap-lnx25:M02_20241203_104036
Max Used Data Page
Converter Page Count

---
```

- Recovery beenden und Datenbank anhalten

- db_offline

> Weitere Informationen über Recovery finden Sie im "MaxDB-Dokumentation"

- Starten Sie das SAP-System
  - User root: /Etc/init.d/sapinit Start
  - Benutzer m02adm: Startsap

Zusätzliche Informationen und Versionsverlauf

Aufgezeichnete Demos

Folgende neu kodierte Demos stehen zur Unterstützung der Dokumentation zur Verfügung.

Installation MaxDB Plugin, Konfiguration MaxDB Plugin, Sicherung der MaxDB Datenbank

Restore und Recovery der MaxDB Datenbank

Externe Dokumentation

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- "SAP Installation Azure auf ANF"
- "SnapCenter-Voraussetzungen für Plugins"
- "SnapCenter Installations-Plugins"
- "MaxDB Recovery-Dokumentation"
- SAP-Hinweise (Anmeldung erforderlich)
  - "1928060 - Datensicherung und -Wiederherstellung mit Dateisystemsicherung"
  - "2282054 - DBM-Hintergrundserver"
  - "616814 - Protokollschreiber für Split Mirror oder Snapshot unterbrechen"
- "Howto - SAP MaxDB Backup mit Datenbank-Manager CLI"
- "Howto - SAP MaxDB Wiederherstellung mit Datenbank-Manager CLI"
- "NetApp Produktdokumentation"
- "NetApp SAP-Lösungen – Informationen zu Anwendungsfällen, Best Practices und Vorteilen"

Versionsverlauf

Version	Datum	Versionsverlauf des Dokuments
Version 1.0	Mai 2025	Erste Version – Backup / Recovery MaxDB-Datenbank

Lifecycle Management

NetApp Integration des SAP Landscape Managements mit Ansible

TR-4953: NetApp SAP Landscape Management Integration Using Ansible

SAP Landscape Management (Lama) ermöglicht SAP-Systemadministratoren die Automatisierung von SAP-Systemprozessen. Dazu gehören ein lückenloses SAP-Systemklonen, -Kopien und -Aktualisierungen.

Autoren: Michael Schlosser, Nils Bauer, NetApp

NetApp bietet eine umfassende Auswahl an Ansible-Modulen, in denen SAP Lama über SAP Lama Automation Studio auf Technologien wie NetApp Snapshot und FlexClone zugreifen kann. Diese Technologien unterstützen die Vereinfachung und Beschleunigung von SAP Systemkopien, Kopien und Aktualisierungen.

Die Integration kann von Kunden genutzt werden, die NetApp Storage-Lösungen vor Ort ausführen, oder von Kunden, die NetApp Storage-Services bei Public-Cloud-Providern wie Amazon Web Services, Microsoft Azure oder der Google Cloud Platform nutzen.

In diesem Dokument wird die Konfiguration von SAP Lama mit NetApp Storage-Funktionen für SAP-Systemkopierungs-, Klon- und Aktualisierungsvorgänge mithilfe der Ansible-Automatisierung beschrieben.

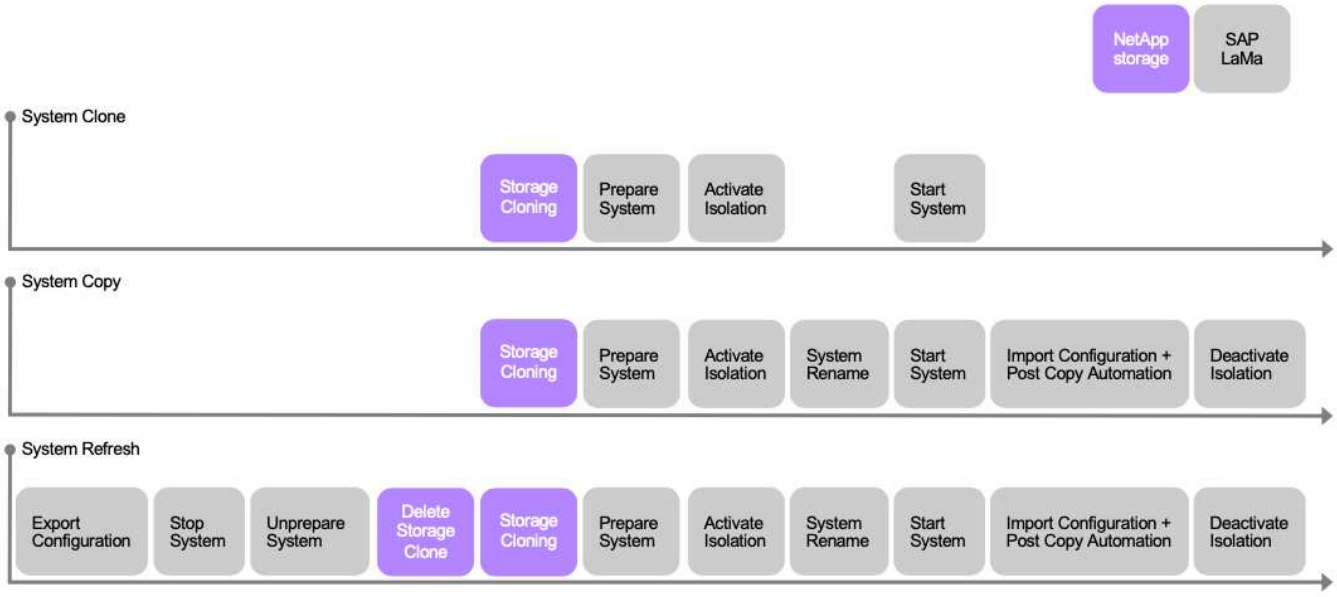
SAP Szenarien für Klonen, Kopieren und Aktualisieren von Systemen

Der Begriff SAP Systemkopie wird oft als Synonym für drei verschiedene Prozesse verwendet: SAP Systemklon, SAP Systemkopie oder SAP Systemaktualisierung. Es ist wichtig, zwischen den verschiedenen Vorgängen zu unterscheiden, da sich Workflows und Anwendungsfälle für jedes einzelne unterscheiden.

- **SAP-Systemklon.** ein SAP-Systemklon ist ein identischer Klon eines Quell-SAP-Systems. SAP Systemklone werden typischerweise zur Beseitigung logischer Beschädigungen oder zum Testen von Disaster-Recovery-Szenarien eingesetzt. Bei einem Systemklonvorgang bleiben der Hostname, die Instanznummer und die SID unverändert. Daher ist es wichtig, für das Zielsystem ein ordnungsgemäßes Netzwerkfechten einzurichten, um sicherzustellen, dass keine Kommunikation mit der Produktionsumgebung besteht.
- **SAP-Systemkopie.** eine SAP-Systemkopie ist ein Setup eines neuen SAP-Zielsystems mit Daten aus einem SAP-Quellsystem. Dabei könnte das neue Zielsystem beispielsweise ein zusätzliches Testsystem mit den Daten aus dem Produktionssystem sein. Hostname, Instanznummer und SID unterscheiden sich für die Quell- und Zielsysteme.
- **SAP-Systemaktualisierung.** ein SAP-Systemaktualisierung ist eine Aktualisierung eines bestehenden SAP-Zielsystems mit Daten aus einem SAP-Quellsystem. Das Zielsystem ist in der Regel Teil einer SAP-Transportlandschaft, beispielsweise ein Qualitätssicherungssystem, das mit den Daten des Produktionssystems aktualisiert wird. Hostname, Instanznummer und SID unterscheiden sich für die Quell- und Zielsysteme.

Die folgende Abbildung zeigt die wichtigsten Schritte, die während eines Systemklonens, einer Systemkopie oder einer Systemaktualisierung ausgeführt werden müssen. Die violetten Felder zeigen die Schritte an, in die NetApp Storage-Funktionen integriert werden können. Alle drei Operationen lassen sich mithilfe von SAP

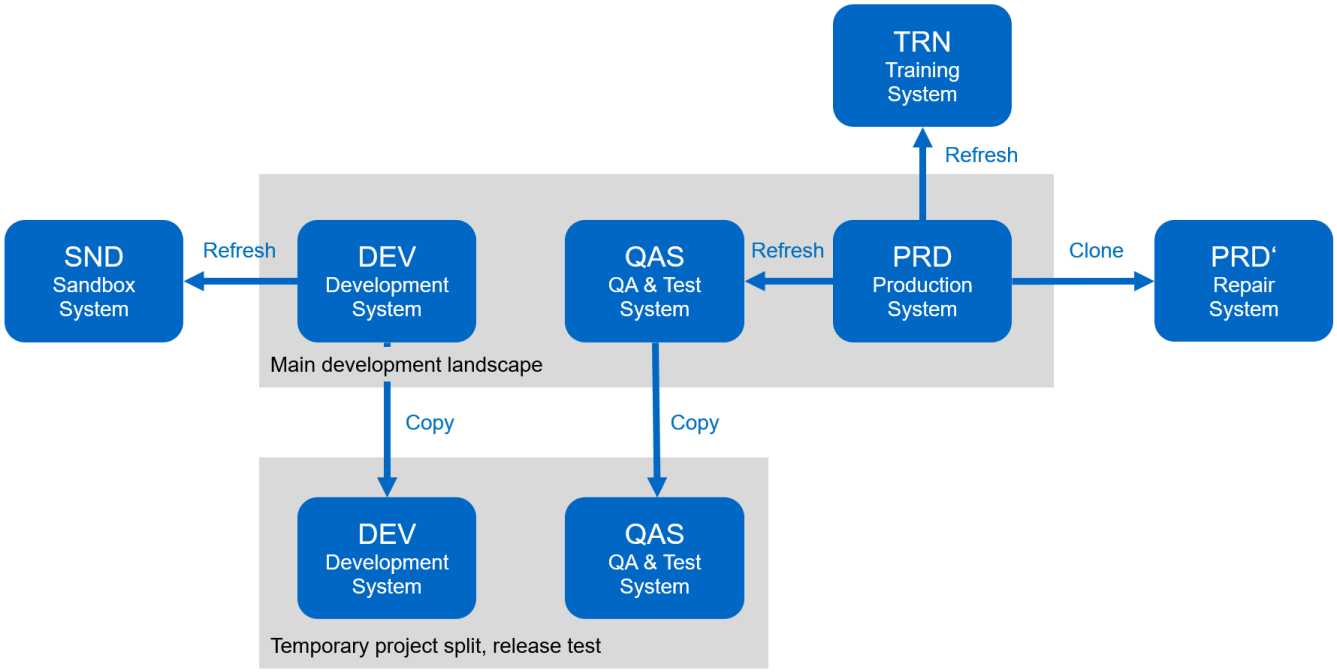
Lama vollständig automatisieren.



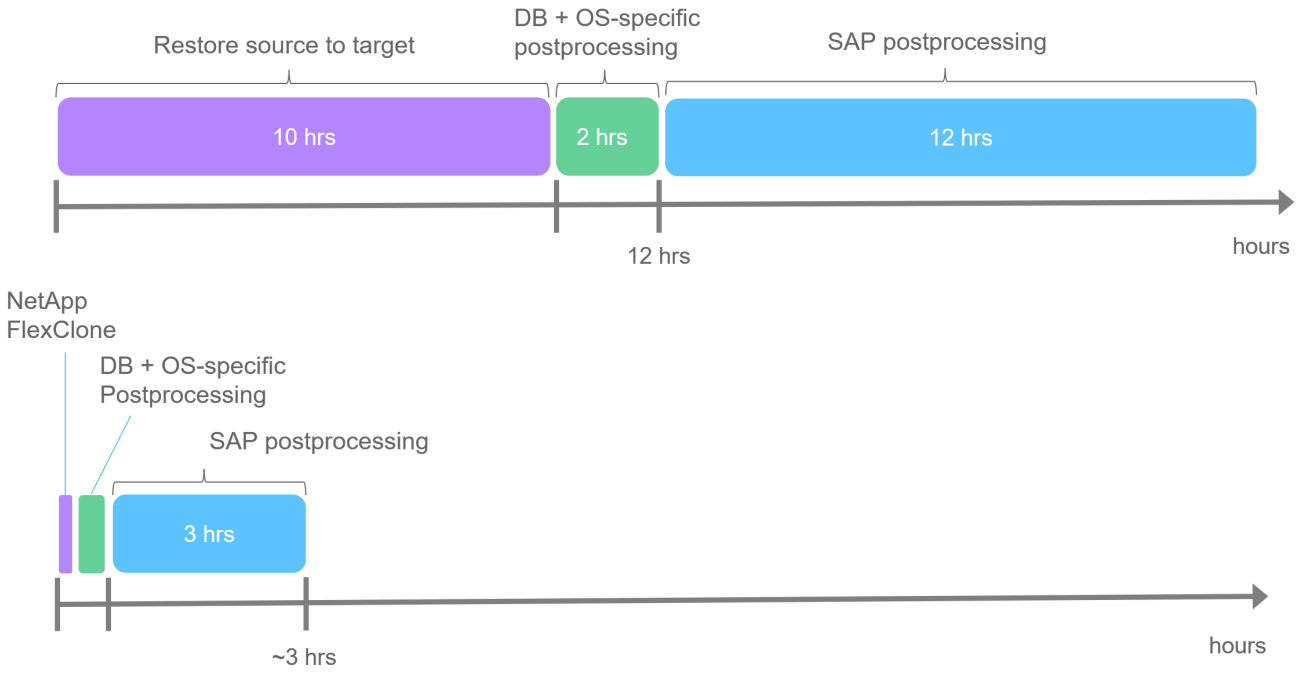
Anwendungsfälle für Systemaktualisierung, Kopie und Klonen

Es gibt verschiedene Szenarien, in denen Daten aus einem Quellsystem zu Test- oder Schulungszwecken einem Zielsystem zur Verfügung gestellt werden müssen. Diese Test- und Trainingssysteme müssen regelmäßig mit Daten des Quellsystems aktualisiert werden, um sicherzustellen, dass die Test- und Schulungsmaßnahmen mit dem aktuellen Datensatz durchgeführt werden.

Diese Systemaktualisierungen bestehen aus mehreren Aufgaben auf Infrastruktur-, Datenbank- und Applikationsebene und können je nach Automatisierungsgrad mehrere Tage dauern.



Mit den Klon-Workflows von SAP Lama und NetApp werden die erforderlichen Aufgaben in der Infrastruktur- und Datenbankebene beschleunigt und automatisiert. Anstatt ein Backup vom Quellsystem auf das Zielsystem wiederherzustellen, verwendet SAP Lama NetApp Snapshot-Kopie und NetApp FlexClone-Technologie, damit erforderliche Aufgaben bis zu einer gestarteten HANA-Datenbank in Minuten anstelle von Stunden ausgeführt werden können, wie in der folgenden Abbildung dargestellt. Der für das Klonen erforderliche Zeitaufwand ist unabhängig von der Größe der Datenbank, sodass selbst sehr große Systeme in wenigen Minuten erstellt werden können. Eine weitere Reduzierung der Laufzeit erfolgt durch die Automatisierung von Aufgaben auf Betriebssystem- und Datenbankebene sowie auf der Seite SAP-Nachbearbeitung.



Beseitigung logischer Beschädigungen

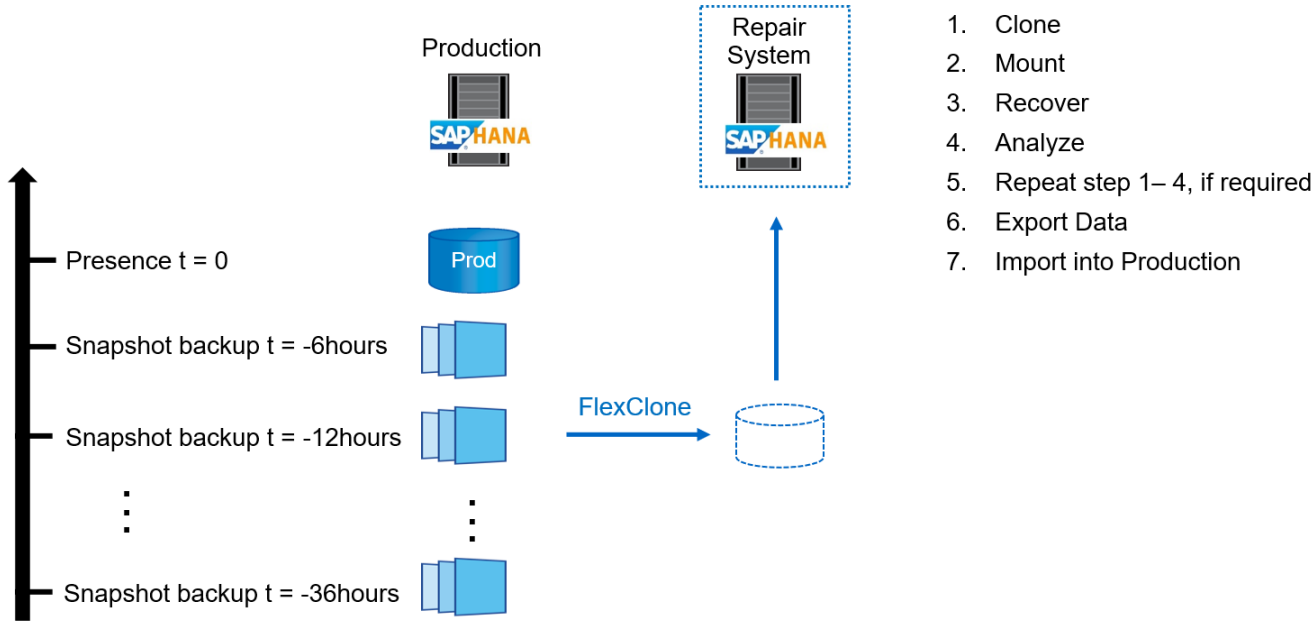
Logische Beschädigungen können durch Softwarefehler, menschliche Fehler oder Sabotage verursacht werden. Leider können logische Beschädigungen oft nicht mit standardmäßigen Hochverfügbarkeits- und Disaster Recovery-Lösungen behoben werden. Daher können abhängig von der Schicht, Applikation, dem File-System oder dem Storage mit der logischen Beschädigung minimale Ausfallzeiten und akzeptable Datenverluste in manchen Fällen nicht erfüllt werden.

Schlimmstenfalls ist die SAP-Anwendung logisch beschädigt. SAP Applikationen laufen oft in einer Landschaft, in der verschiedene Applikationen miteinander kommunizieren und Daten austauschen. Daher wird die Wiederherstellung eines SAP-Systems, bei dem eine logische Beschädigung aufgetreten ist, nicht empfohlen. Wenn Sie das System auf einen Zeitpunkt vor der Beschädigung wiederherstellen, führt dies zu Datenverlust. Außerdem würde die SAP-Landschaft nicht mehr synchron sein und eine zusätzliche Nachbearbeitung erfordern.

Anstatt das SAP-System wiederherzustellen, ist es besser, den logischen Fehler innerhalb des Systems zu beheben, indem das Problem in einem separaten Reparatursystem analysiert wird. Zur Ursachenanalyse ist die Einbindung des Geschäftsprozesses und der Applikationseigentümer erforderlich. Für dieses Szenario erstellen Sie ein Reparatursystem (ein Klon des Produktionssystems) auf Basis der Daten, die vor dem Auftreten der logischen Beschädigung gespeichert wurden. Innerhalb des Reparatursystems können die erforderlichen Daten exportiert und in das Produktionssystem importiert werden. Bei diesem Ansatz muss das Produktionssystem nicht angehalten werden. Im besten Fall gehen keine Daten oder nur ein Bruchteil der

Daten verloren.

Bei der Einrichtung des Reparatursystems sind Flexibilität und Geschwindigkeit entscheidend. NetApp Storage-basierte Snapshot Backups bieten mehrere konsistente Datenbank-Images, um mithilfe der NetApp FlexClone Technologie einen Klon des Produktionssystems zu erstellen. Die Erstellung von FlexClone Volumes dauert nur wenige Sekunden, anstatt mehrerer Stunden, wenn zum Einrichten des Reparatursystems eine umgeleitete Wiederherstellung aus einem dateibasierten Backup verwendet wird.

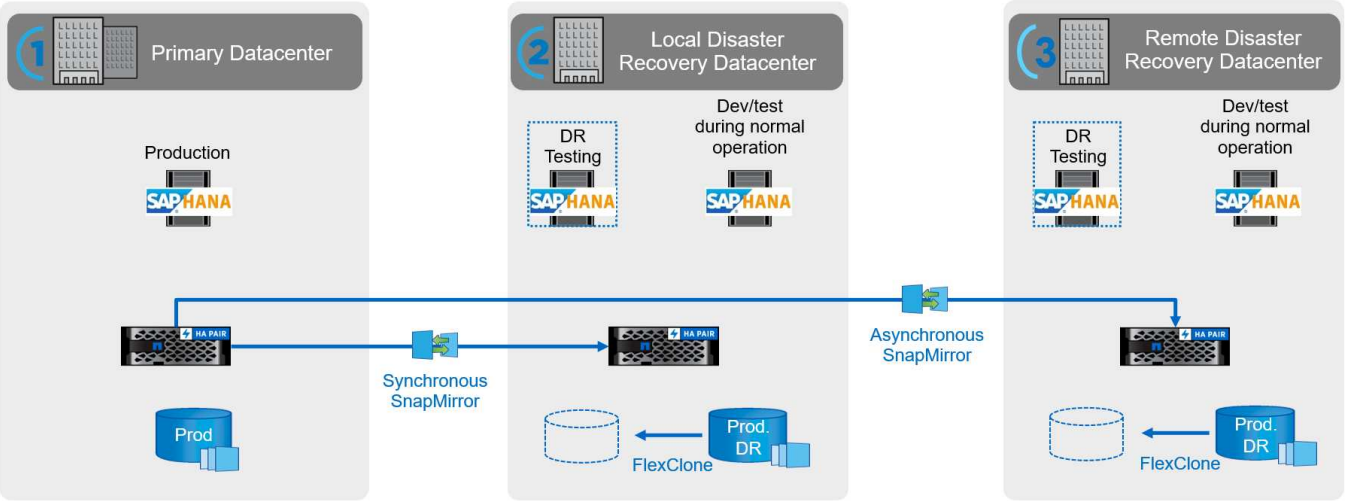


Disaster Recovery-Tests

Für eine effiziente Disaster Recovery-Strategie müssen die erforderlichen Workflows getestet werden. Die Tests zeigen, ob die Strategie funktioniert und ob die interne Dokumentation ausreichend ist. Darüber hinaus können Administratoren die erforderlichen Verfahren Schulen.

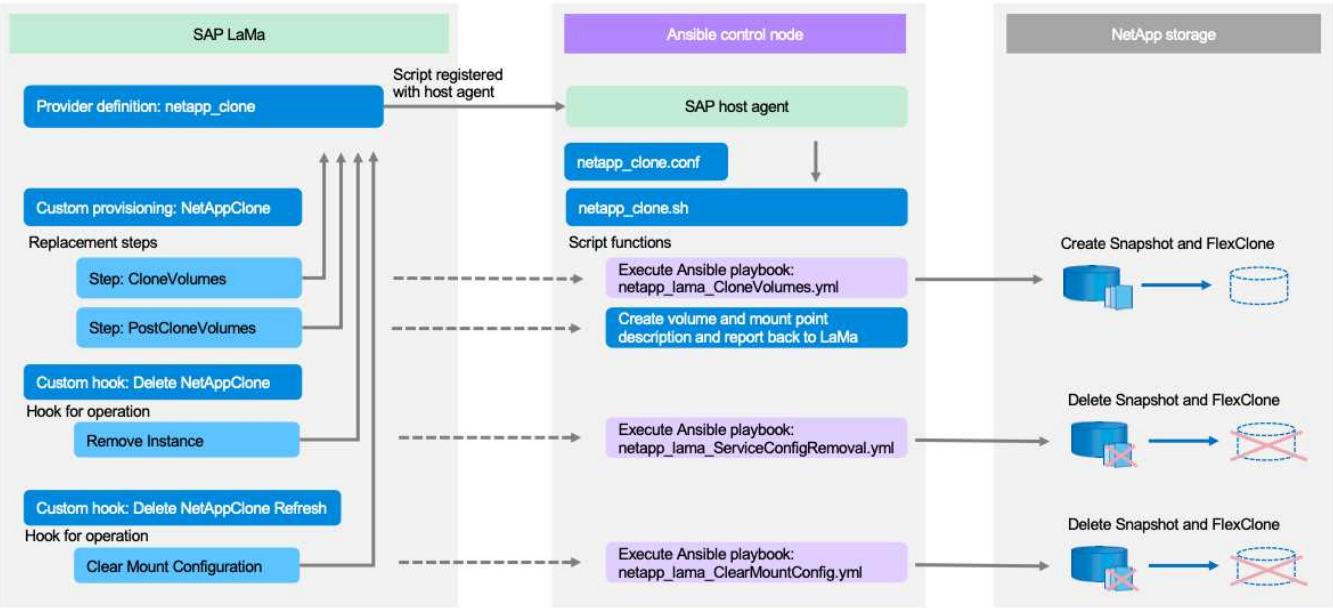
Die Storage-Replizierung mit SnapMirror ermöglicht die Ausführung von Disaster-Recovery-Tests ohne Risiko von RTO und RPO. Disaster-Recovery-Tests können ohne Unterbrechung der Datenreplizierung durchgeführt werden. Disaster Recovery-Tests für asynchronen und synchronen SnapMirror verwenden Snapshot Backups und FlexClone Volumes am Disaster Recovery-Ziel.

SAP Lama kann für die Orchestrierung des gesamten Testvorgangs verwendet werden, aber auch für Netzwerkfencing, Ziel-Host-Wartung usw.



Integration von NetApp SAP Lama mithilfe von Ansible

Bei dem Integrationsansatz werden individuelle Provisionierungs- und Hooks von SAP Lama in Kombination mit Ansible-Playbooks für das NetApp Storage-Management verwendet. Die folgende Abbildung zeigt einen allgemeinen Überblick über die Konfiguration auf Lama-Seite sowie die entsprechenden Komponenten der Beispielimplementierung.



Über einen zentralen Host, der als Ansible-Kontroll-Node fungiert, werden Anfragen von SAP Lama ausgeführt und die NetApp Storage-Vorgänge mit Ansible Playbooks ausgelöst. Die Komponenten des SAP-Hostagenten müssen auf diesem Host installiert sein, damit der Host als Kommunikationstor zu SAP Lama verwendet werden kann.

Innerhalb von Lama Automation Studio wird ein Anbieter definiert, der beim SAP-Host-Agent des Ansible-Hosts registriert ist. Eine Host-Agent-Konfigurationsdatei verweist auf ein Shell-Skript, das von SAP Lama mit einer Reihe von Befehlszeilenparametern aufgerufen wird, abhängig von der angeforderten Operation.

Innerhalb von Lama Automation Studio werden benutzerdefinierte Bereitstellung und ein individueller Haken definiert, um Storage-Klonvorgänge während der Bereitstellung und auch bei Clean-up-Vorgängen auszuführen, wenn das System deprovisioniert wird. Das Shell-Skript auf dem Ansible Kontroll-Node führt dann die entsprechenden Ansible-Playbooks aus, die die Snapshot- und FlexClone-Vorgänge sowie das Löschen der Klone mit dem Deprovisioning-Workflow auslösen.

Weitere Informationen zu NetApp Ansible-Modulen und den Lama-Provider-Definitionen finden Sie unter:

- "NetApp Ansible Module"
- "Dokumentation zu SAP Lama – Anbieterdefinitionen"

Beispiel für eine Implementierung

Aufgrund der großen Anzahl an Optionen für System- und Speichereinrichtung sollte die Beispielimplementierung als Vorlage für Ihre individuellen System-Setup- und Konfigurationsanforderungen verwendet werden.

Die Beispielskripte werden wie IS bereitgestellt und von NetApp nicht unterstützt. Sie können die aktuelle Version der Skripte per E-Mail an ng-sapcc@netapp.com anfordern.

Validierte Konfigurationen und Einschränkungen

Die folgenden Grundsätze wurden für die Beispielumsetzung angewendet und müssen möglicherweise an die Bedürfnisse des Kunden angepasst werden:

- Verwaltete SAP Systeme greifen über NFS auf NetApp Storage Volumes zu und wurden basierend auf dem adaptiven Designprinzip eingerichtet.
- Sie können alle von NetApp Ansible Modulen unterstützten ONTAP-Versionen (ZAPI und REST API) verwenden.
- Die Anmeldeinformationen für ein einzelnes NetApp Cluster und eine SVM wurden als Variablen im Provider-Skript hartcodiert.
- Das Storage-Klonen wurde auf demselben Storage-System durchgeführt, das vom Quell-SAP System verwendet wurde.
- Die Storage Volumes für das SAP Ziel-System hatten dieselben Namen wie die Quelle mit einem Anhang.
- Es wurde kein Klonen auf dem Sekundärspeicher (SV/SM) implementiert.
- FlexClone Split wurde nicht implementiert.
- Für Quell- und Ziel-SAP-Systeme waren die Instanznummern identisch.

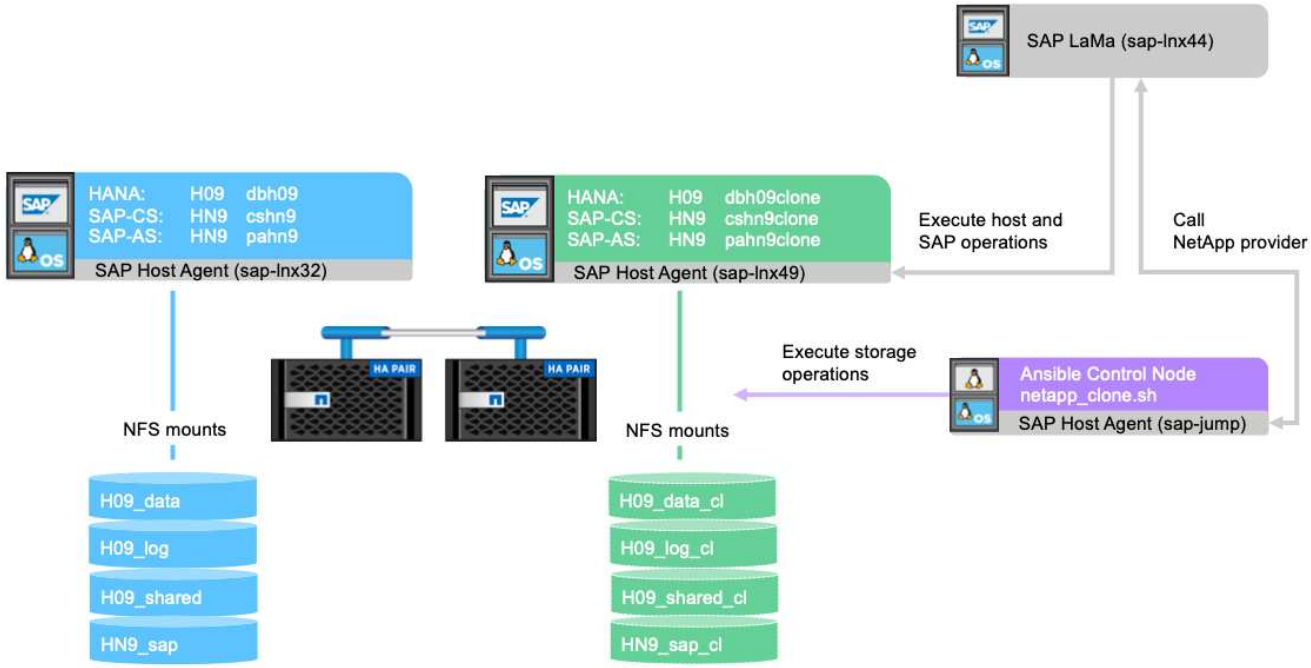
Laboreinrichtung

Die folgende Abbildung zeigt die von uns verwendete Lab-Einrichtung. Das für den Systemklonvorgang verwendete Quell-SAP-System HN9 bestand aus der Datenbank H09, dem SAP CS und den SAP ALS Diensten, die auf demselben Host (sap-lnx32) mit installiert ausgeführt werden "Anpassungsfähiges Design" Aktiviert. Ein Ansible-Kontroll-Node wurde gemäß vorbereitet "Ansible Playbooks für NetApp ONTAP" Dokumentation.

Der SAP-Host-Agent wurde auch auf diesem Host installiert. Das NetApp-Provider-Skript und die Ansible Playbooks wurden auf dem Ansible-Steuerungsknoten konfiguriert, wie in beschrieben "„Anhang: Provider Script-Konfiguration.“"

Der Host `sap-lnx49` Wurde als Ziel für den Klonbetrieb von SAP Lama verwendet und die Funktion zur Isolation wurde dort konfiguriert.

Verschiedene SAP-Systeme (HNA als Quelle und HN2 als Ziel) wurden für Systemkopierungs- und Aktualisierungsvorgänge verwendet, da dort Post Copy Automation (PCA) aktiviert wurde.



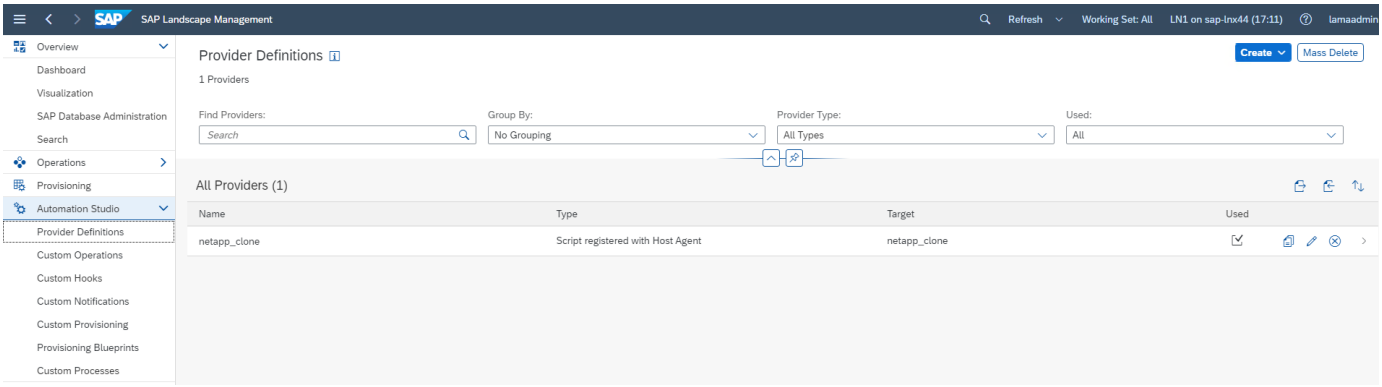
Die folgenden Softwareversionen wurden für die Laboreinrichtung verwendet:

- SAP Lama Enterprise Edition 3.00 SP23_2
- SAP HANA 2.00.052.00.1599235305
- SAP 7.77 PATCH 27 (S/4 HANA 1909)
- SAP Host Agent 7.22 Patch 56
- SAPACEXT 7.22 Patch 69
- Linux SLES 15 SP2
- Ansible 2: 13.7
- NetApp ONTAP 9.8P8

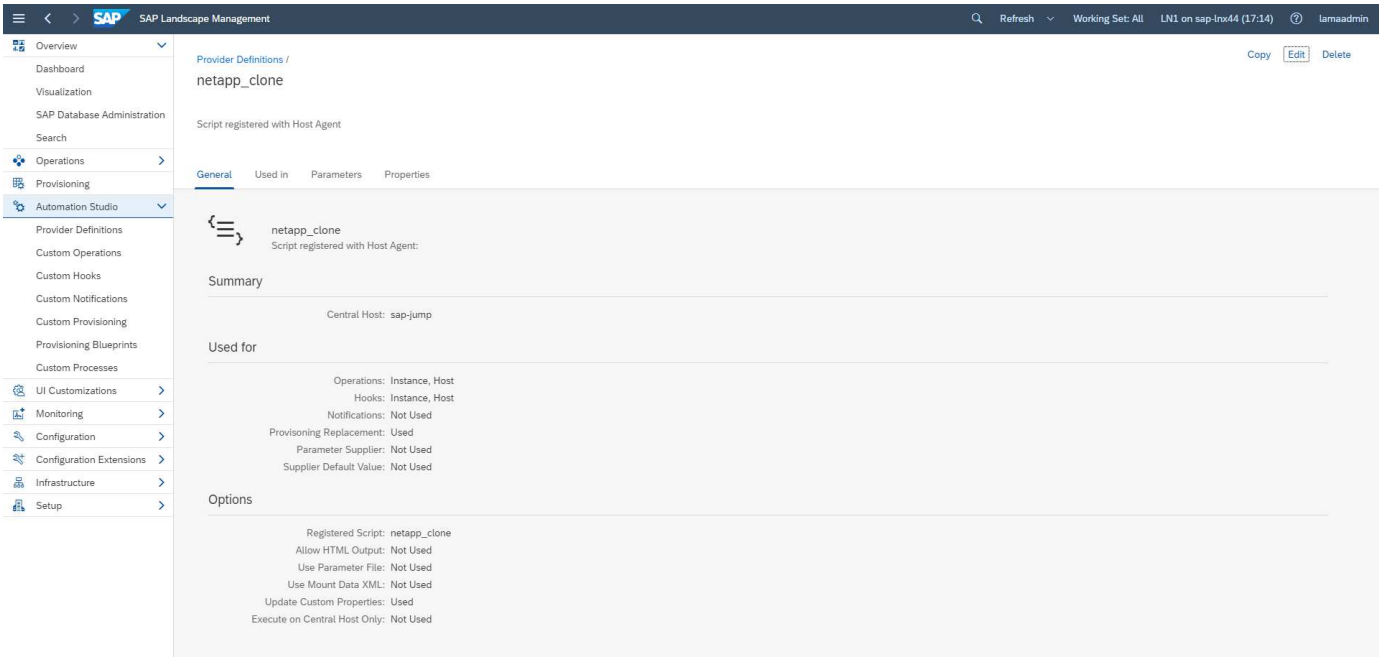
Konfiguration von SAP Lama

Definition eines SAP Lama-Providers

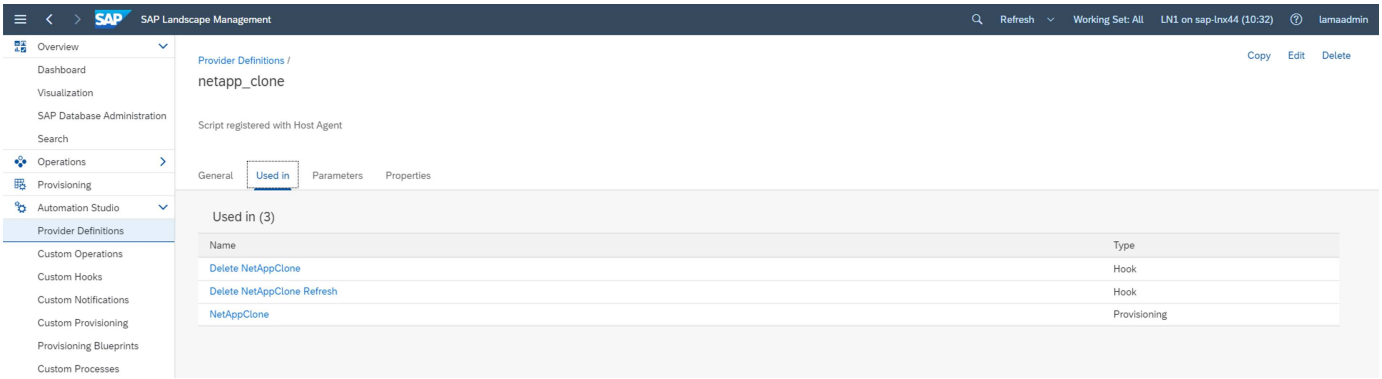
Die Provider-Definition wird in Automation Studio von SAP Lama wie im folgenden Screenshot dargestellt ausgeführt. Die Beispielimplementierung verwendet eine Definition eines einzelnen Providers, die wie zuvor erläutert für verschiedene benutzerdefinierte Bereitstellungsschritte und Hooks verwendet wird.



Dem Provider `netapp_clone` Wird als Skript definiert `netapp_clone.sh` Registriert beim SAP-Host-Agent. Der SAP-Host-Agent wird auf dem zentralen Host ausgeführt `sap-jump`, Die auch als Ansible-Steuerungsknoten fungiert.

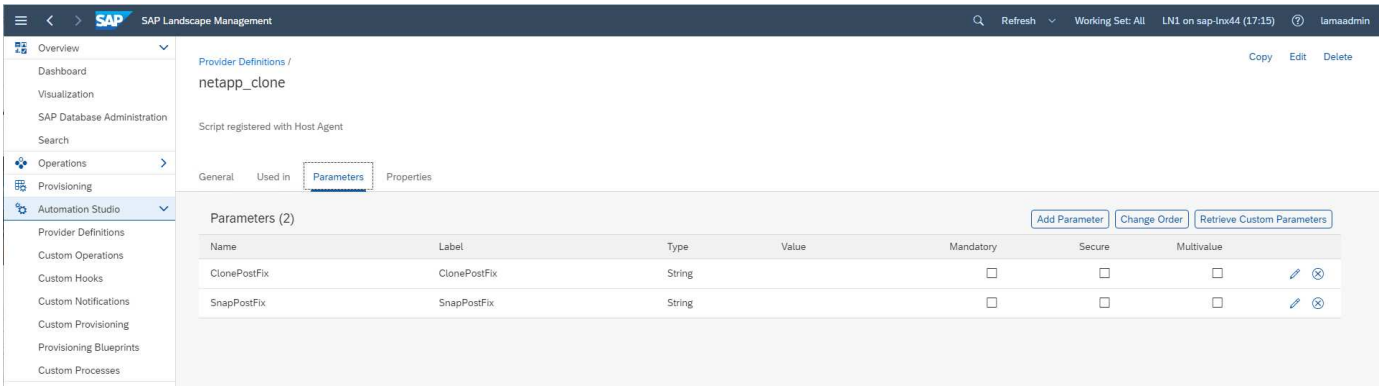


Auf der Registerkarte **used in** wird angezeigt, für welche benutzerdefinierten Vorgänge der Provider verwendet wird. Die Konfiguration für die benutzerdefinierte Bereitstellung **NetAppClone** und die benutzerdefinierten Hooks **NetAppClone löschen** und **NetAppClone Refresh löschen** werden in den nächsten Kapiteln angezeigt.



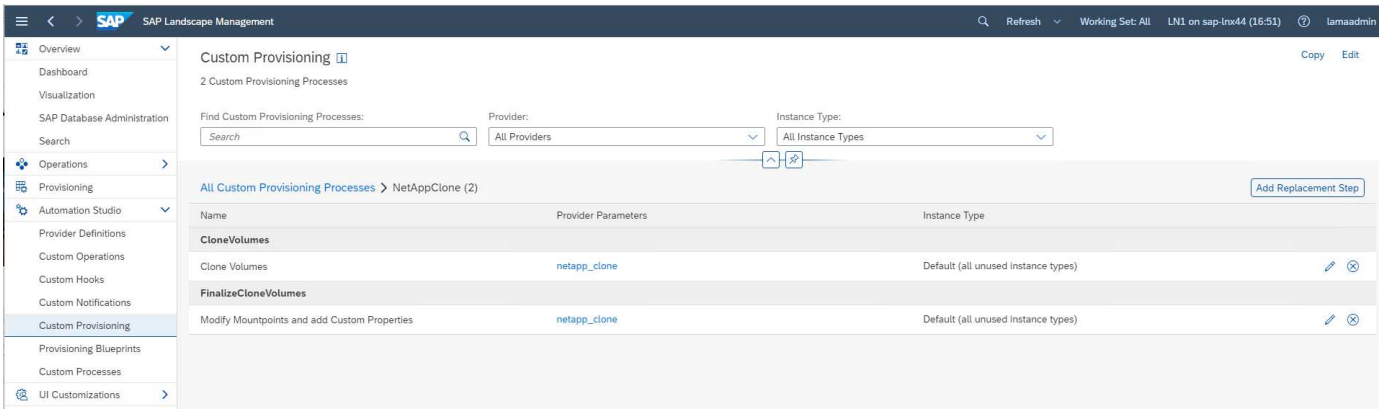
Die Parameter **ClonePostFix** und **SnapPostFix** werden während der Ausführung des Provisioning Workflows

angefordert und für die Snapshot- und FlexClone-Volume-Namen verwendet.



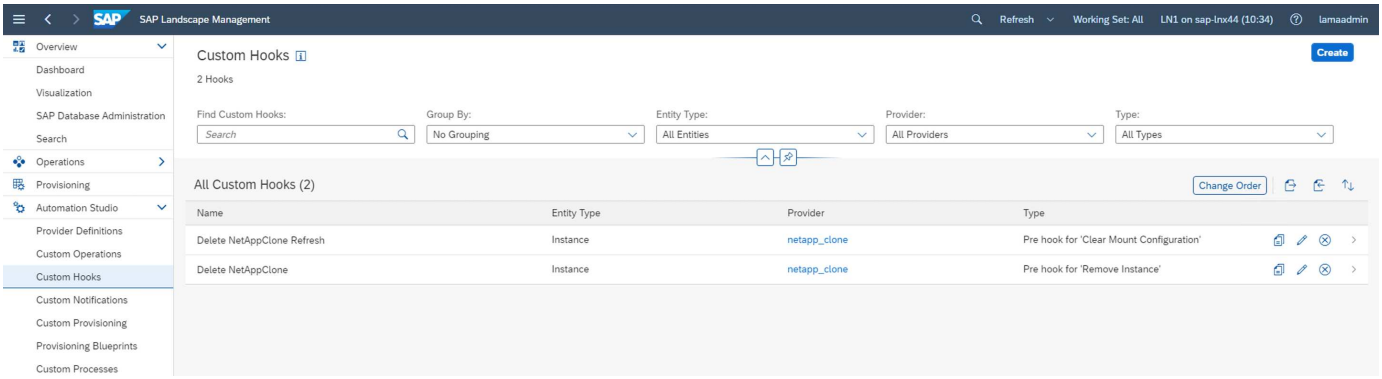
Individuelle Bereitstellung mit SAP Lama

In der zuvor beschriebenen benutzerdefinierten SAP Lama-Bereitstellungskonfiguration wird der zuvor beschriebene Kundenanbieter verwendet, um die Bereitstellungsworkflows **Clone Volumes** und **PostCloneVolumes** zu ersetzen.

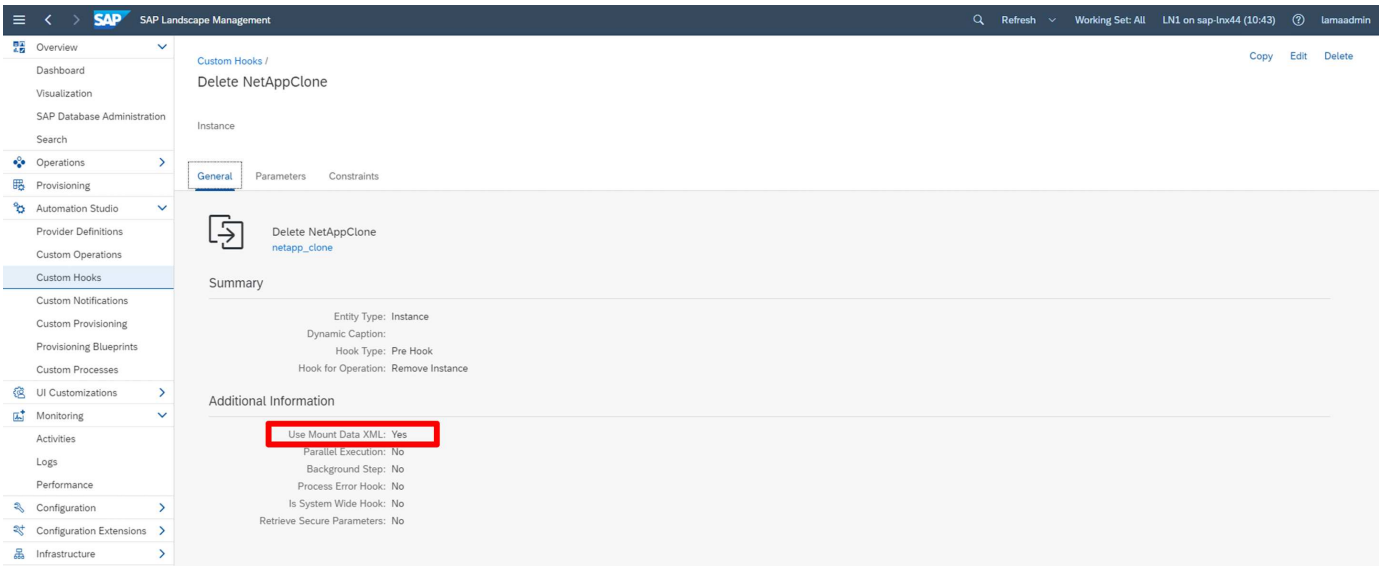


Custom-Hook von SAP Lama

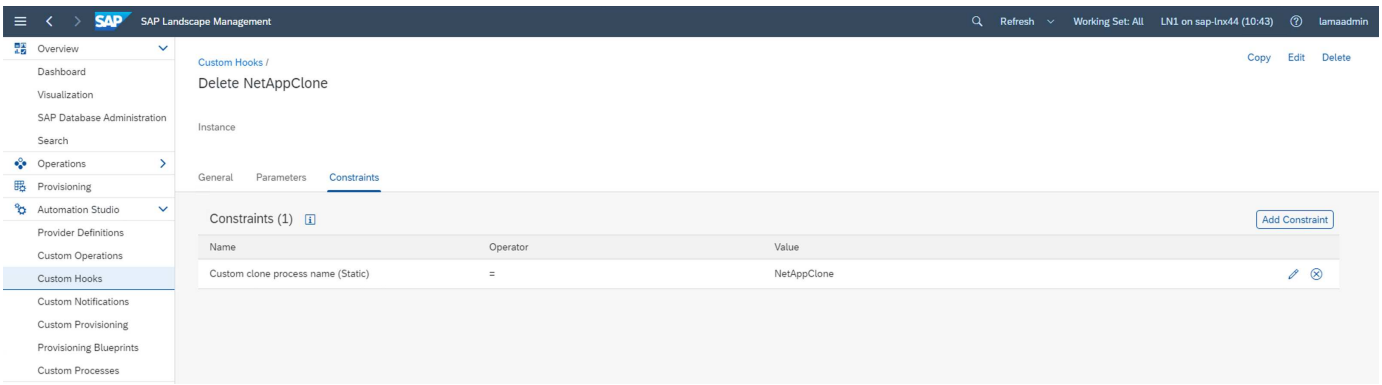
Wenn ein System mit dem Workflow zum Löschen des Systems gelöscht wird, wird der Haken **NetAppClone löschen** verwendet, um die Provider-Definition aufzurufen `netapp_clone`. Der Haken **NetApp Clone Refresh löschen** wird während der Systemaktualisierung verwendet, da die Instanz während der Ausführung erhalten bleibt.



Es ist wichtig, **Mount Data XML** für den Custom Hook zu konfigurieren, damit SAP Lama dem Provider die Informationen über die Mount Point-Konfiguration bereitstellt.



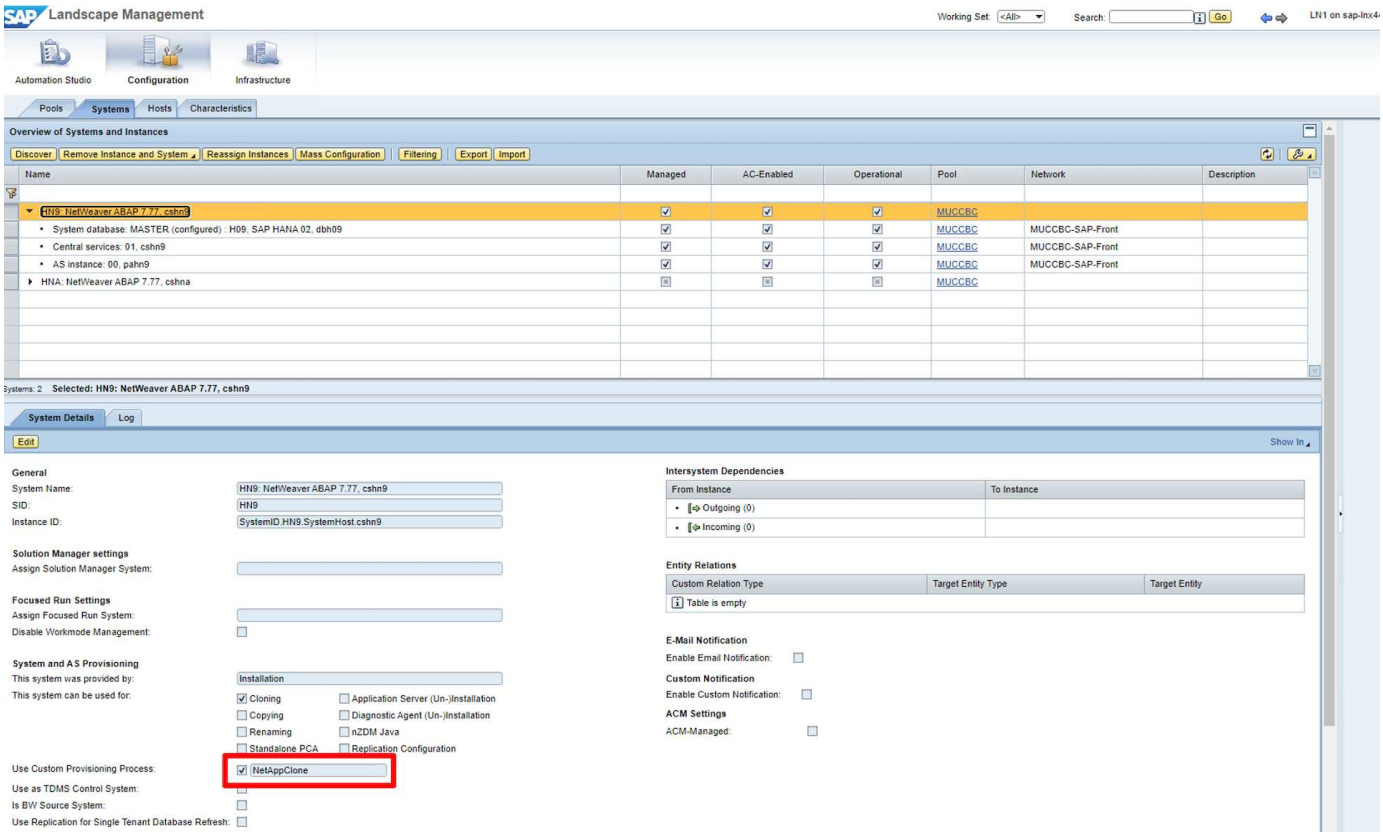
Um sicherzustellen, dass der benutzerdefinierte Haken nur verwendet und ausgeführt wird, wenn das System mit einem benutzerdefinierten Bereitstellungs-Workflow erstellt wurde, wird ihm die folgende Einschränkung hinzugefügt.



Weitere Informationen zur Verwendung von benutzerdefinierten Haken finden Sie im "SAP Lama-Dokumentation".

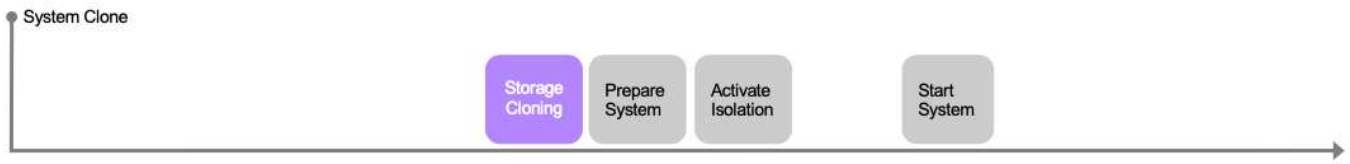
Benutzerdefinierten Bereitstellungs-Workflow für SAP Quellsystem aktivieren

Er muss in der Konfiguration angepasst werden, um den individuellen Bereitstellungs-Workflow für das Quellsystem zu ermöglichen. Das Kontrollkästchen **Benutzerdefinierte Provisioning-Prozess verwenden** mit der entsprechenden benutzerdefinierten Bereitstellungsdefinition muss ausgewählt werden.

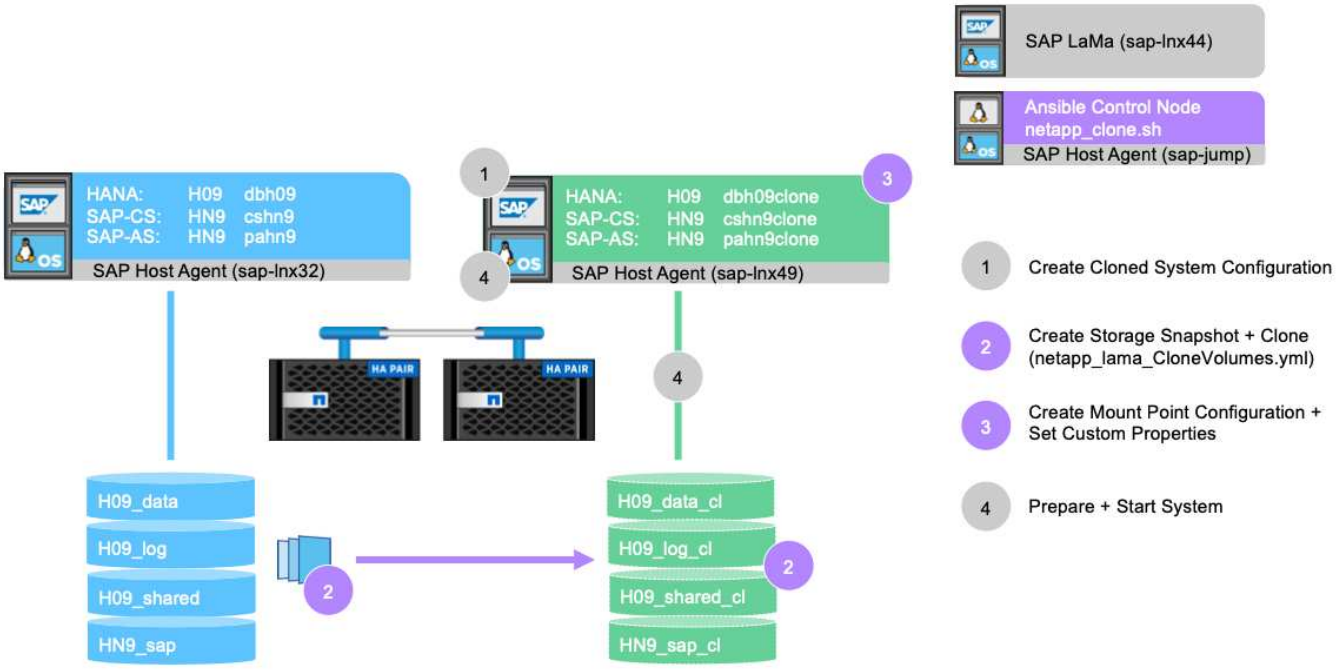


Workflow zur Bereitstellung von SAP Lama – Klon-System

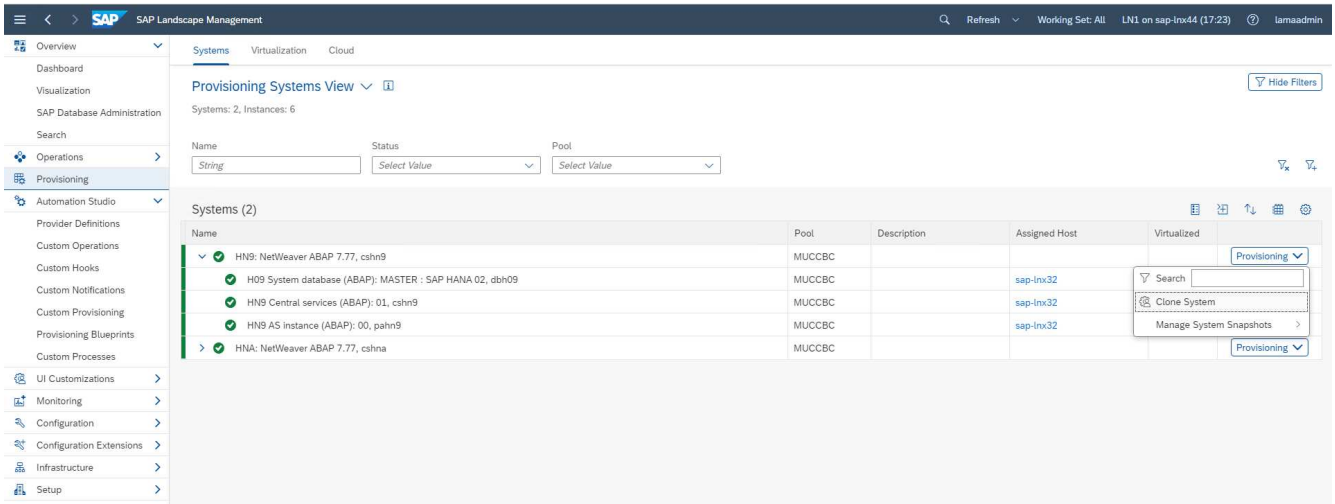
Die folgende Abbildung zeigt die Hauptschritte, die beim Systemklonworkflow ausgeführt werden.



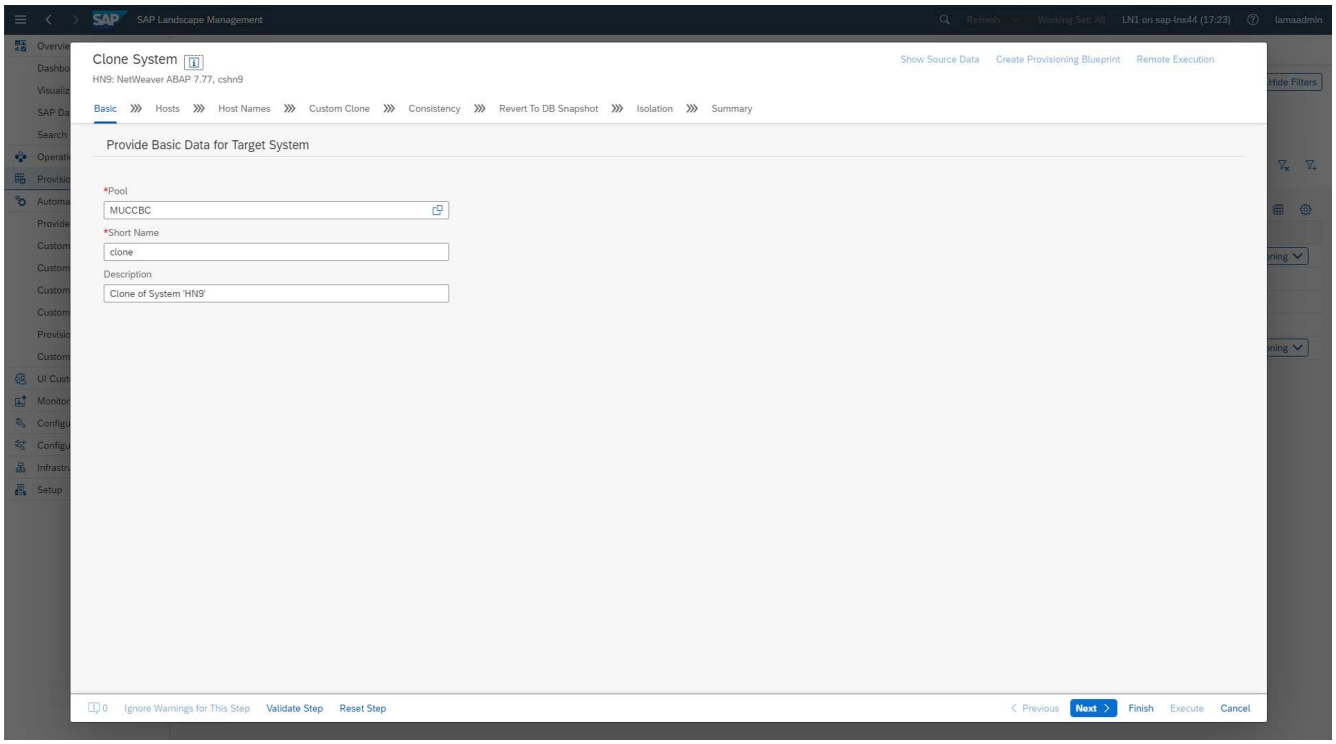
In diesem Abschnitt wird der gesamte Workflow zum Klonen von SAP Lama-Systemen anhand des SAP-Quellsystems HN9 mit HANA-Datenbank H09 erläutert. Das folgende Bild gibt einen Überblick über die während des Workflows ausgeführten Schritte.



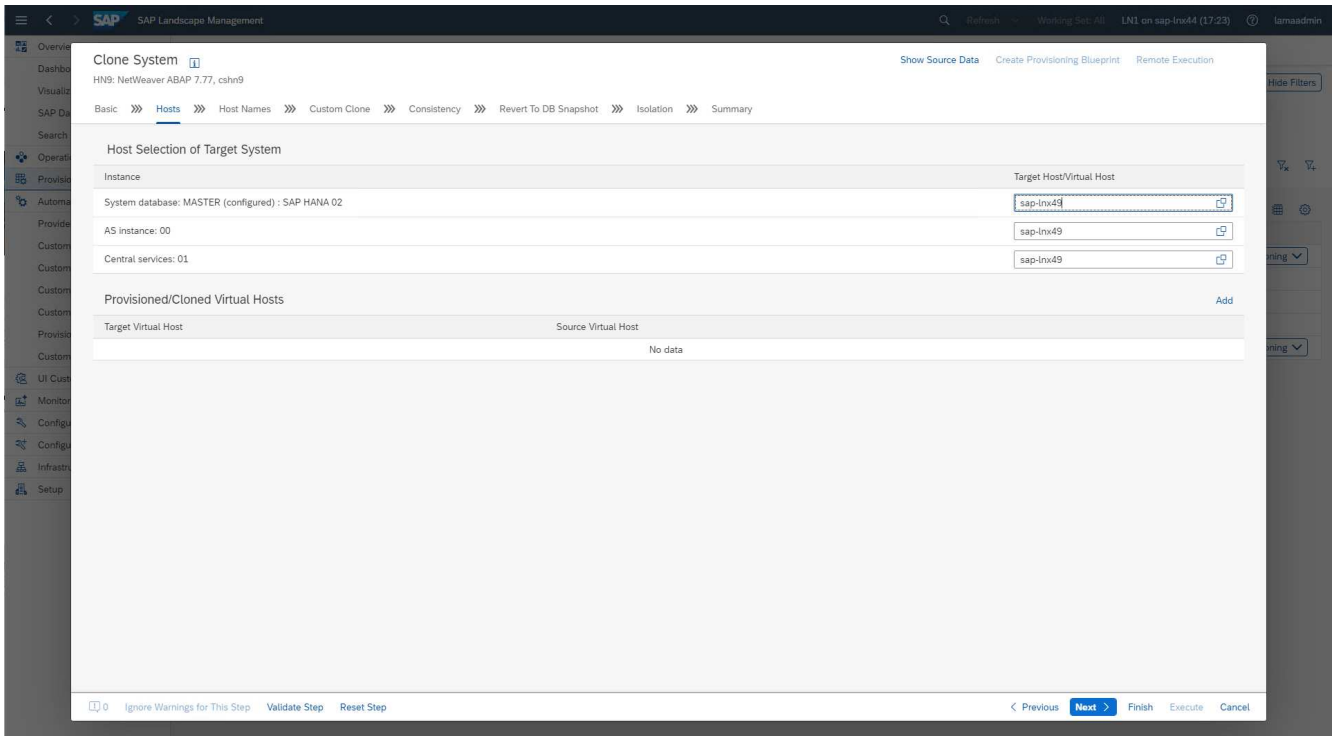
1. Um den Klon-Workflow zu starten, öffnen Sie **Provisioning** in der Menüstruktur und wählen Sie das Quellsystem (in unserem Beispiel HN9) aus. Starten Sie dann den Assistenten * Clone System*.



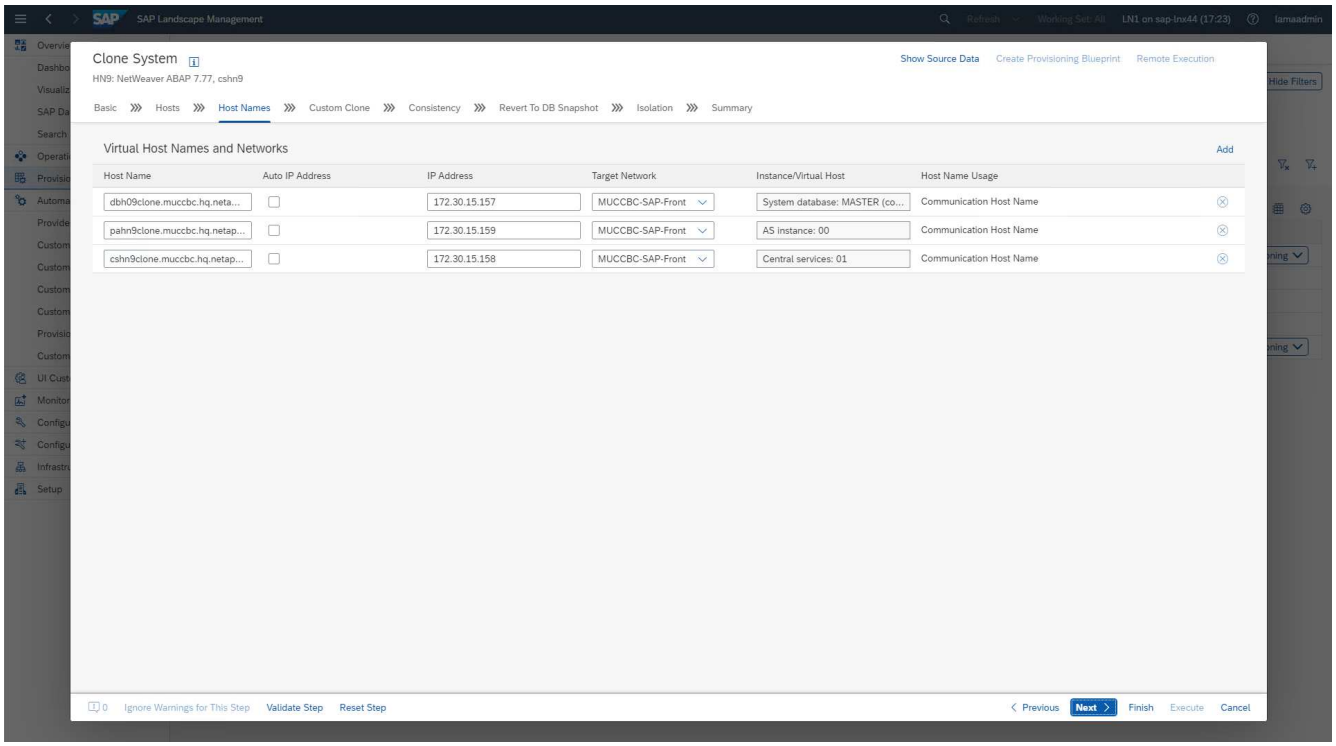
2. Geben Sie die angeforderten Werte ein. Bildschirm 1 des Assistenten fragt nach dem Poolnamen für das geklonte System. Dieser Schritt gibt die Instanzen (virtuell oder physisch) an, auf denen das geklonte System gestartet werden soll. Standardmäßig wird das System in demselben Pool wie das Zielsystem geklont.



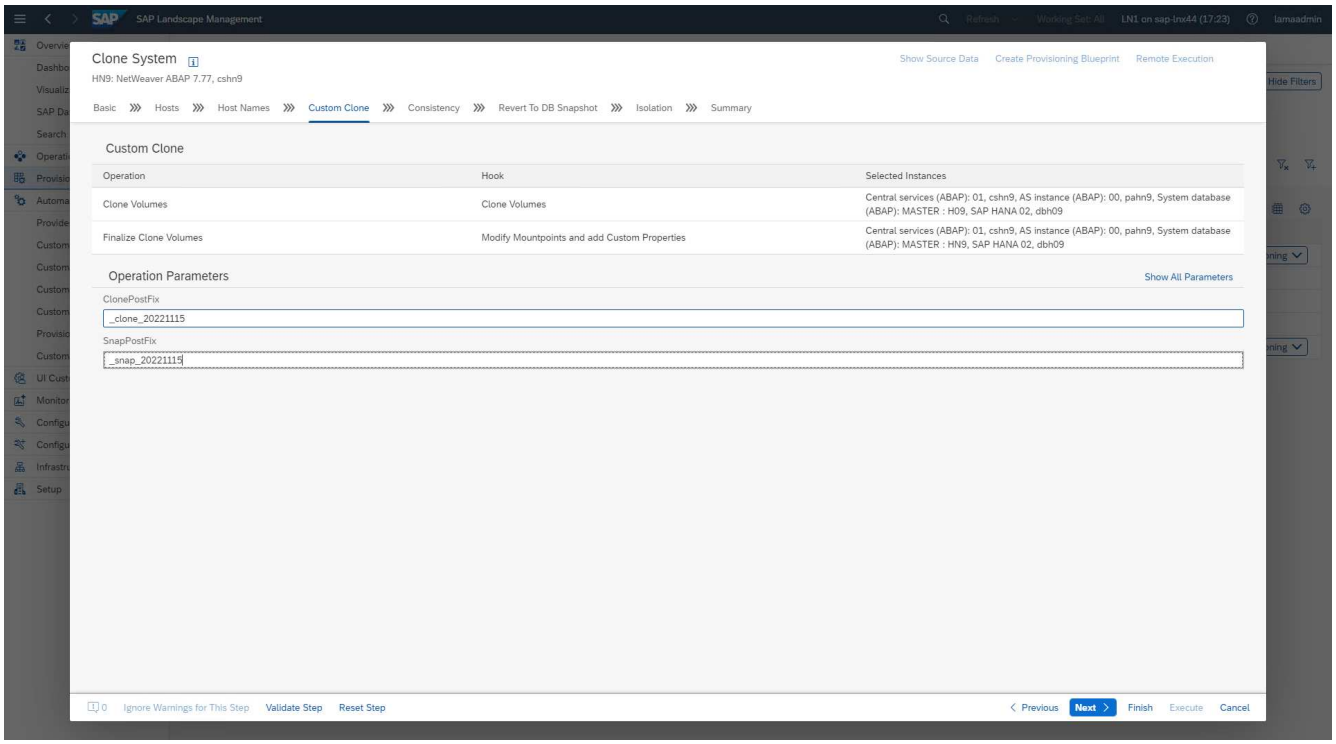
3. Bildschirm 2 des Assistenten fordert die Zielhosts auf, auf denen die neuen SAP-Instanzen gestartet werden. Die Zielhosts für diese Instanz können aus dem im vorherigen Bildschirm angegebenen Host-Pool ausgewählt werden. Jede Instanz oder jeder Service kann auf einem anderen Host gestartet werden. In unserem Beispiel laufen alle drei Dienste auf demselben Host.



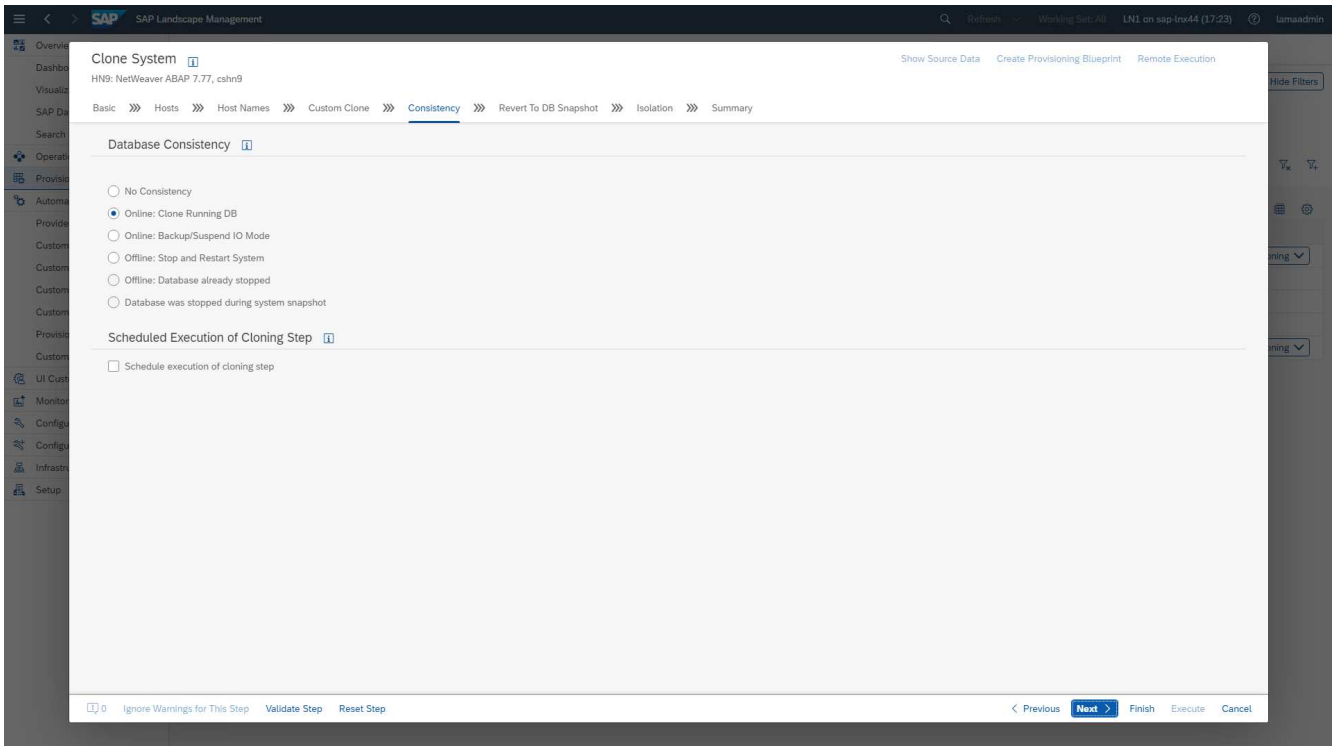
4. Stellen Sie die in Bildschirm 3 angeforderten Informationen bereit, die Sie nach virtuellen Hostnamen und Netzwerken fragen. In der Regel werden die Hostnamen in DNS gehalten, sodass die IP-Adressen entsprechend vorbelegt sind.



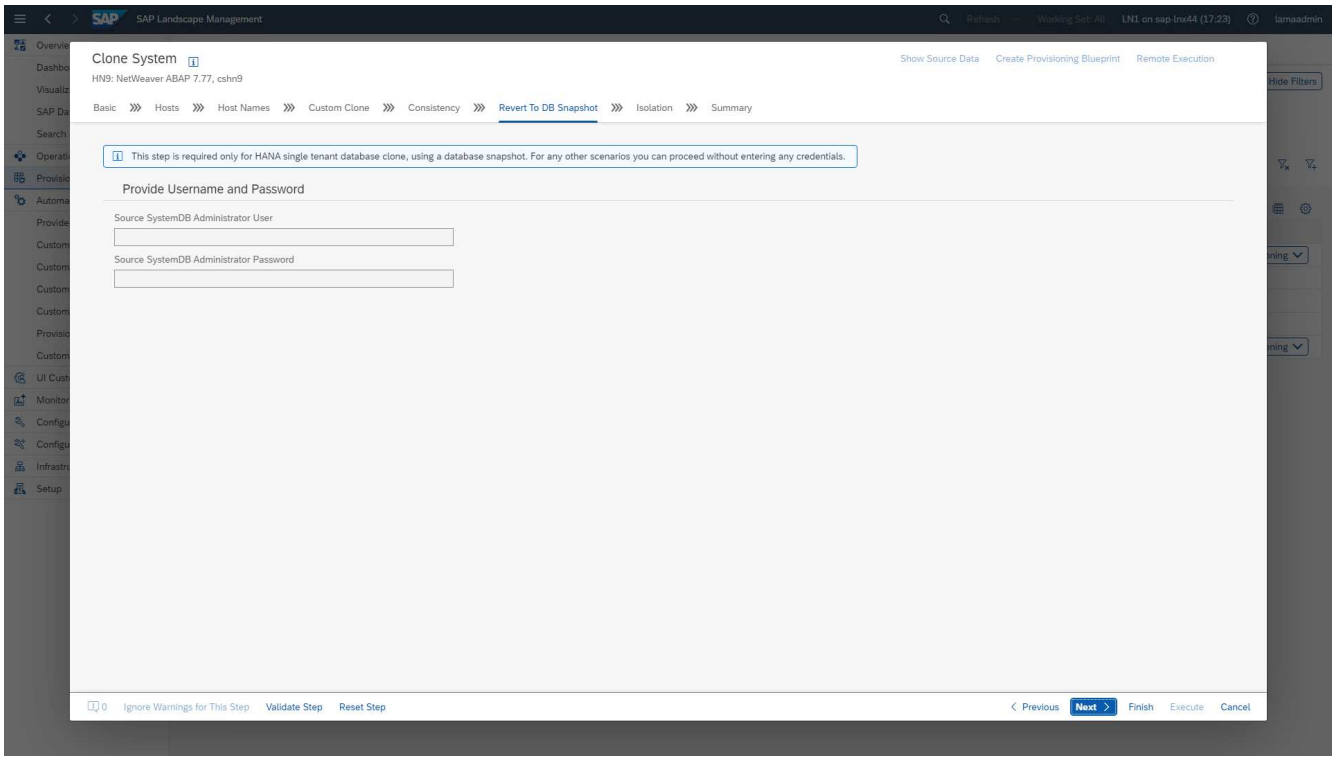
5. In Bildschirm 4 werden die benutzerdefinierten Klonvorgänge aufgelistet. Es werden ein Klon und ein **SnapPostfix** Name bereitgestellt, die während der Speicherklonoperation für das FlexClone Volume bzw. den Snapshot-Namen verwendet werden. Wenn Sie diese Felder leer lassen, wird der Standardwert im Bereich Variable des Provider-Skripts konfiguriert `netapp_clone.sh` Verwendet wird.



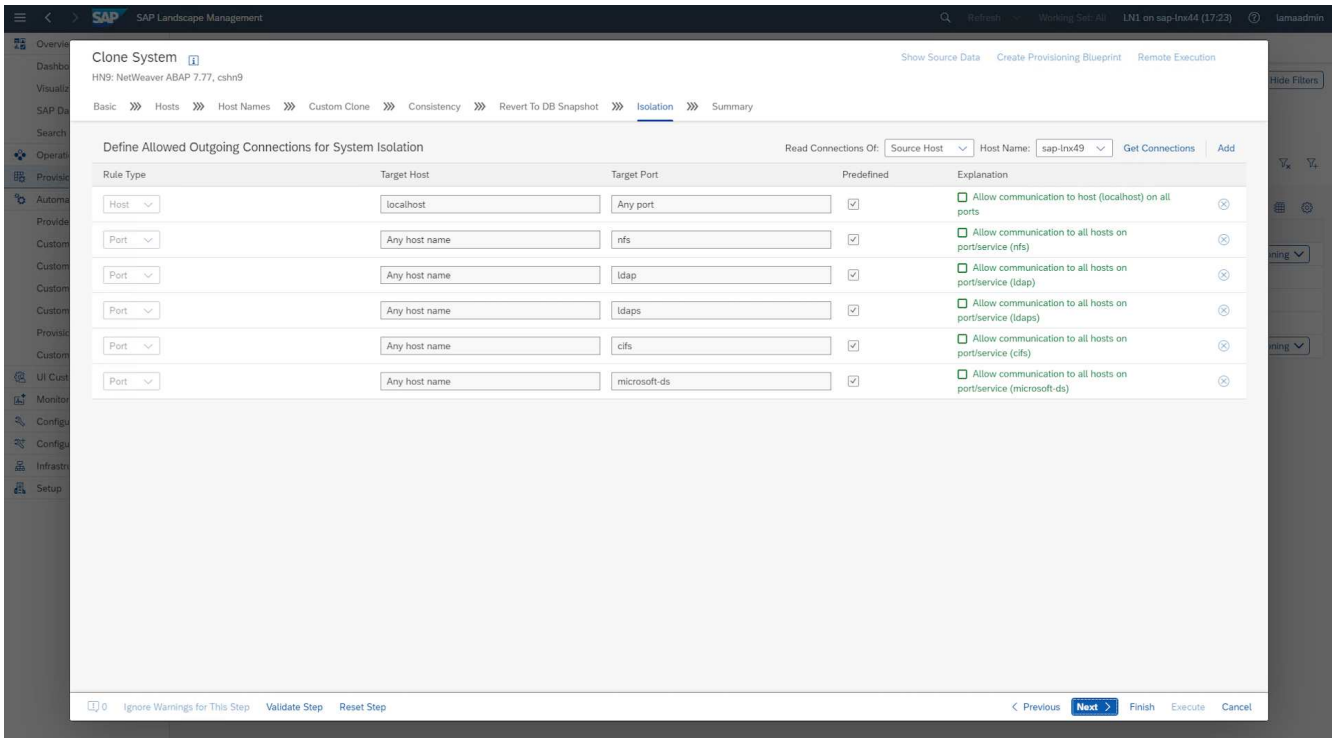
6. In Bildschirm 5 ist die Option Datenbankkonsistenz ausgewählt. In unserem Beispiel haben wir **Online: Clone mit DB** ausgewählt.



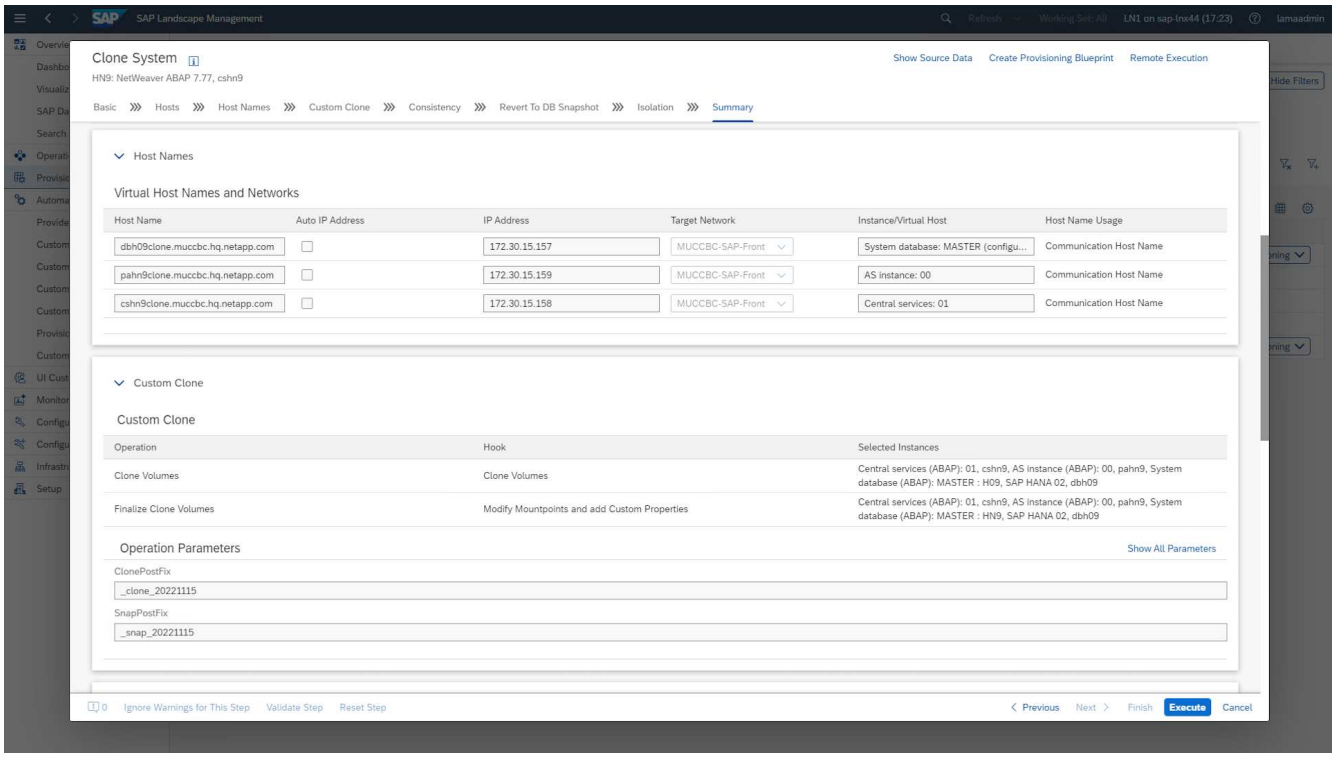
7. In Bildschirm 6 ist eine Eingabe nur erforderlich, wenn Sie einen Mandantenklon durchführen.



8. In Bildschirm 7 kann die Systemisolierung konfiguriert werden.

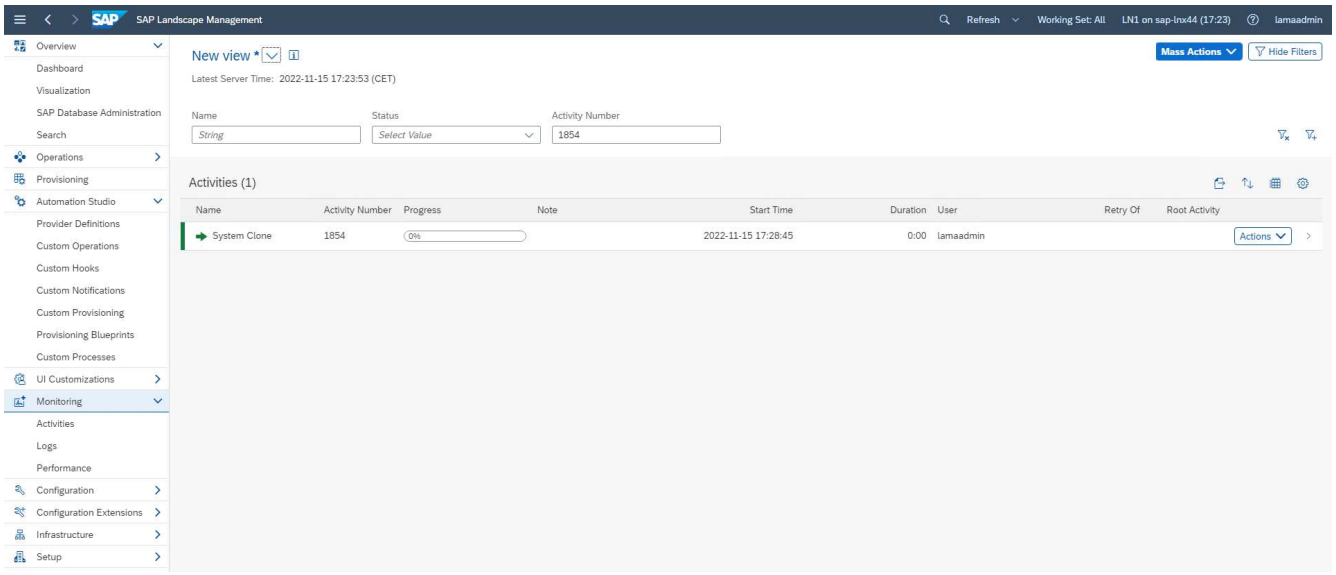


9. In Bildschirm 8 enthält eine Übersichtsseite alle Einstellungen zur endgültigen Bestätigung, bevor der Workflow gestartet wird. Klicken Sie auf **Ausführen**, um den Workflow zu starten.

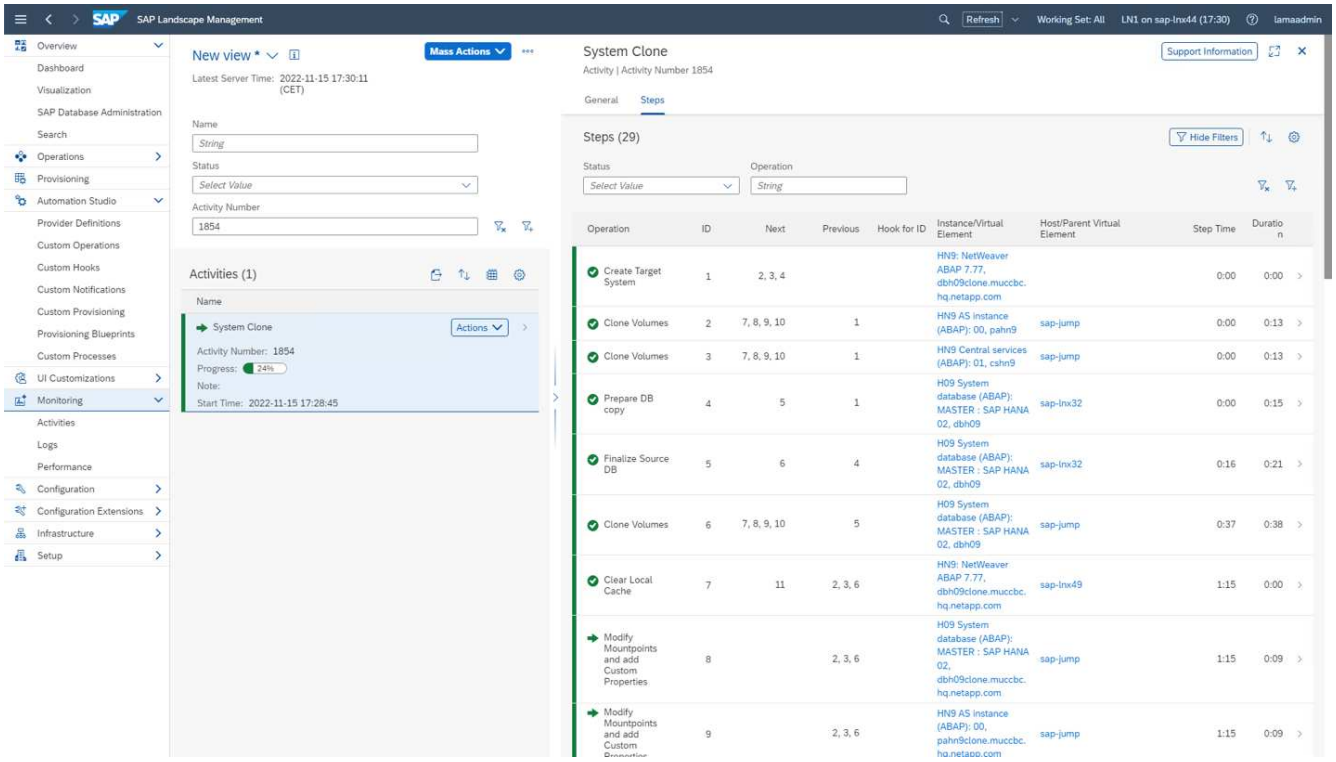


SAP Lama führt nun alle in der Konfiguration angegebenen Aktionen durch. Dazu gehören die Erstellung von Klonen und Exports für das Storage-Volume, das Mounten auf dem Ziel-Host, das Hinzufügen von Firewall-Regeln zur Isolierung sowie der Start der HANA-Datenbank und der SAP-Services.

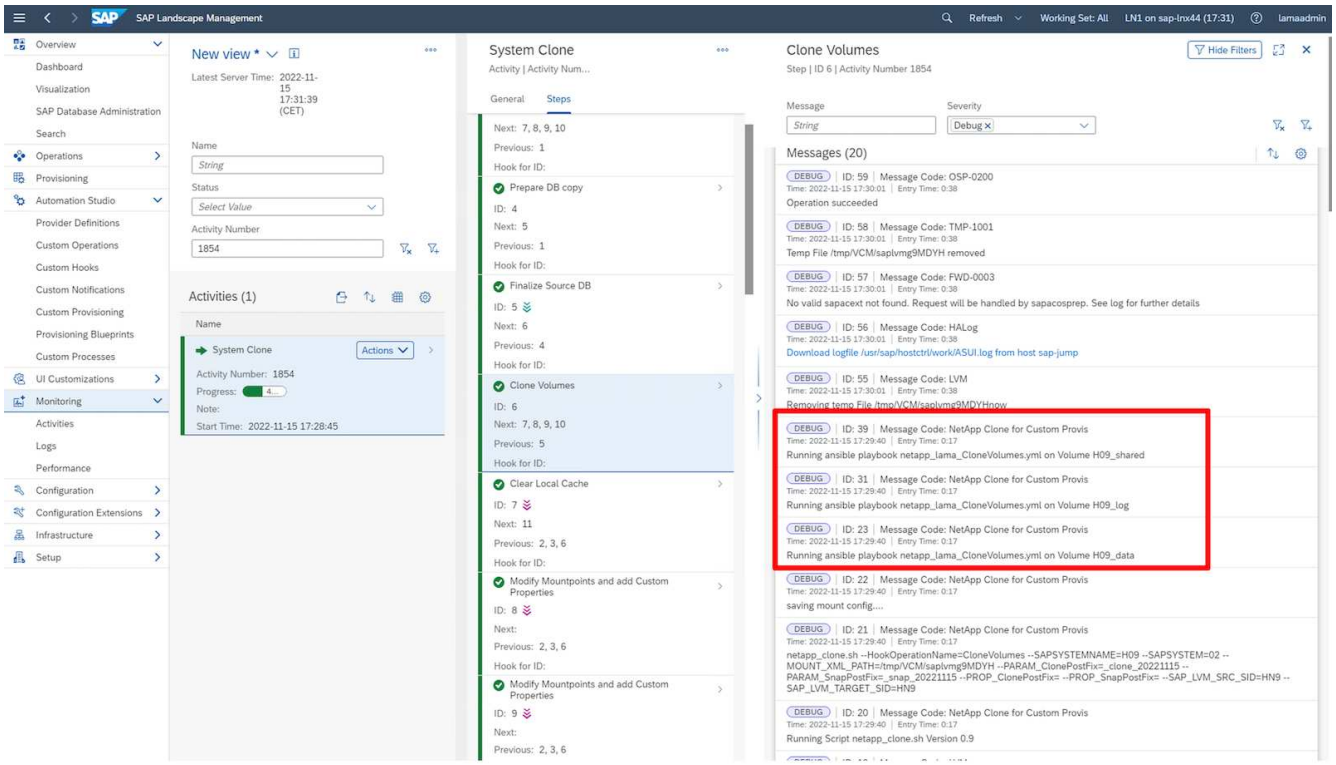
10. Sie können den Fortschritt des Klon-Workflows im Menü **Überwachung** überwachen.



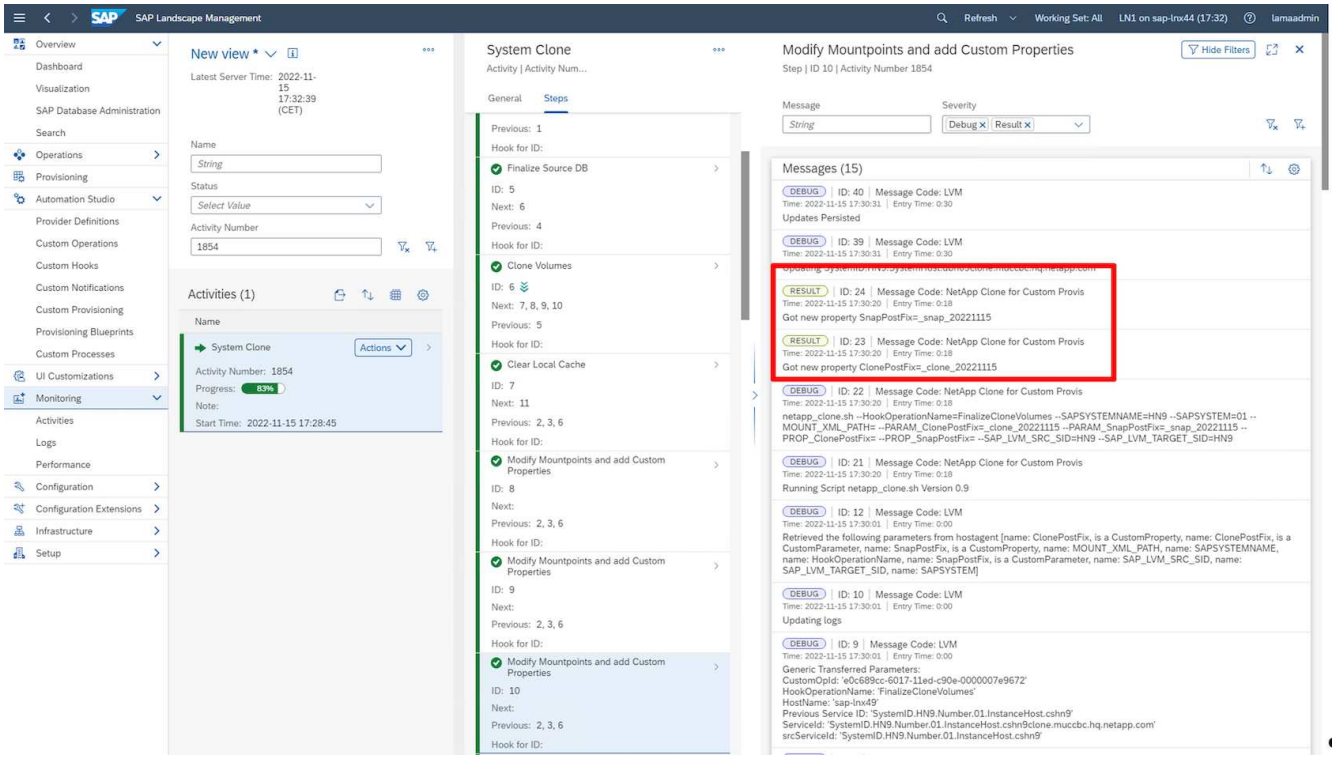
Innerhalb des detaillierten Protokolls werden die Vorgänge **Clone Volume** und **Mountpunkte ändern und Benutzerdefinierte Eigenschaften hinzufügen** auf dem Ansible-Knoten ausgeführt, dem `sap-jump` Host: Diese Schritte werden für jeden Service, die HANA-Datenbank, die SAP-Zentraldienste und den SAP-ALS-Service ausgeführt.



11. Durch Auswahl der Task **Clone Volumes** wird das detaillierte Protokoll für diesen Schritt angezeigt und die Ausführung des Ansible Playbook wird hier angezeigt. Wie Sie sehen, das Ansible-Playbook `netapp_lama_CloneVolumes.yml` Wird für jedes HANA Datenbank-Volume, die Daten, das Protokoll und die gemeinsame Nutzung ausgeführt.



12. In der Detailansicht des Schritts **Mountpoints ändern und Benutzerdefinierte Eigenschaften hinzufügen** finden Sie Informationen zu den Mount-Punkten und den vom Ausführungsskript übergebenen benutzerdefinierten Eigenschaften.

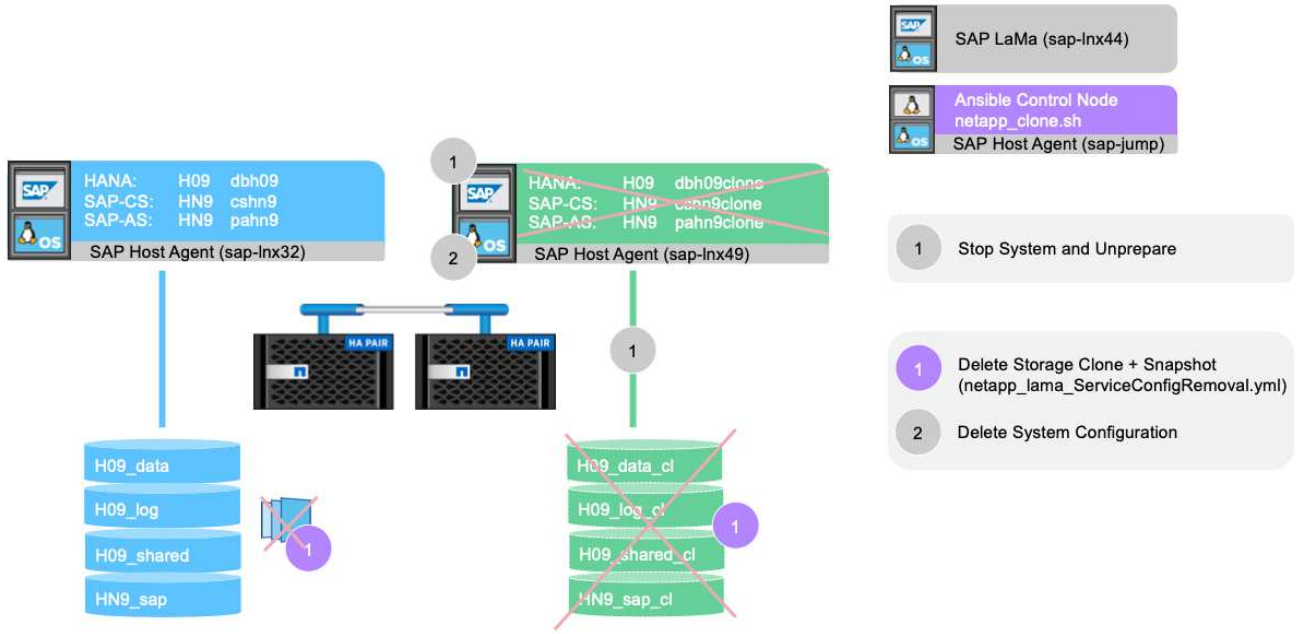


Nach Abschluss des Workflows ist das geklonte SAP-System vorbereitet, gestartet und betriebsbereit.

Workflow zur Deprovisionierung von SAP Lama – Systemzerstöre

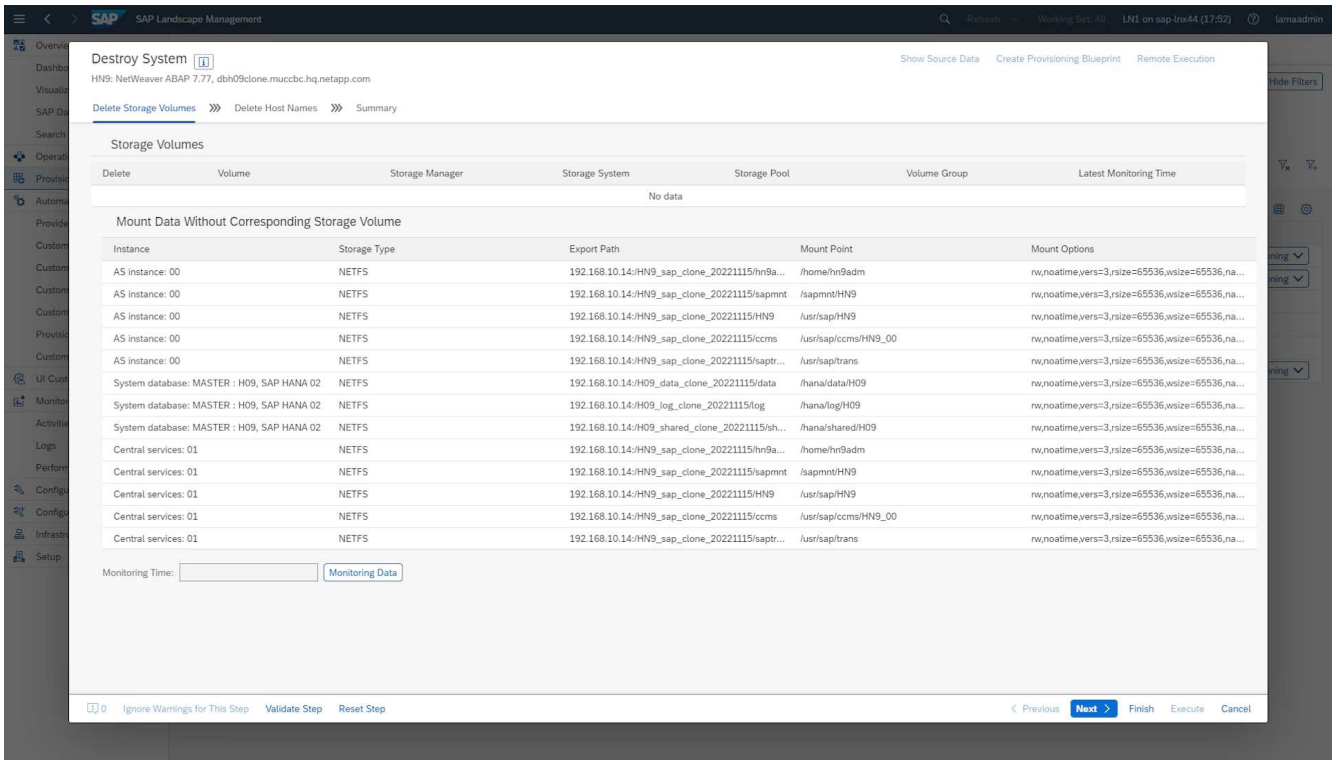
Die folgende Abbildung zeigt die wichtigsten Schritte, die mit dem Workflow zum Löschen des Systems ausgeführt werden.

1. Um ein geklontes System außer Betrieb zu nehmen, muss es vorab angehalten und vorbereitet werden. Anschließend kann der Workflow zum Löschen des Systems gestartet werden.

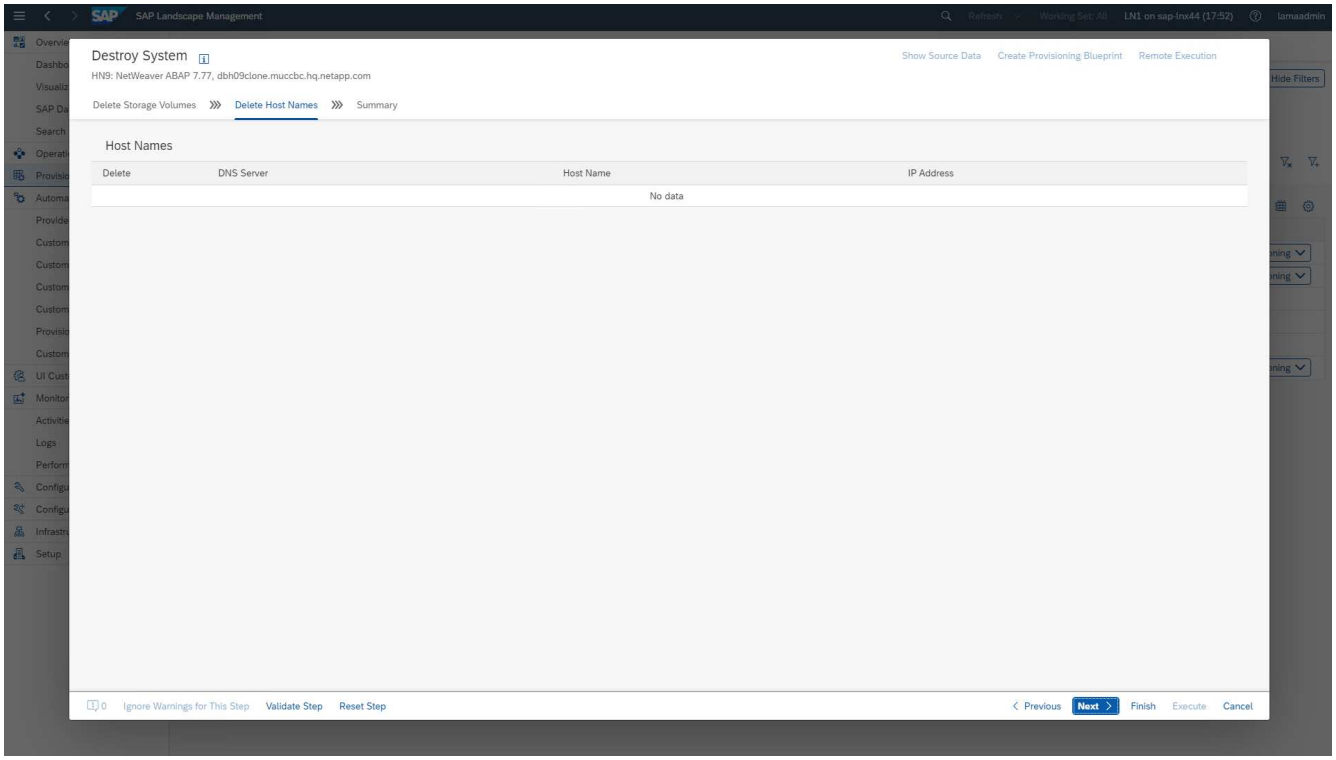


2. In diesem Beispiel wird für das zuvor erstellte System ein Workflow zur Systemzerstörung ausgeführt. Wir wählen das System im Bildschirm **Systemansicht** aus und starten den System Workflow zerstören unter **Prozesse zerstören**.

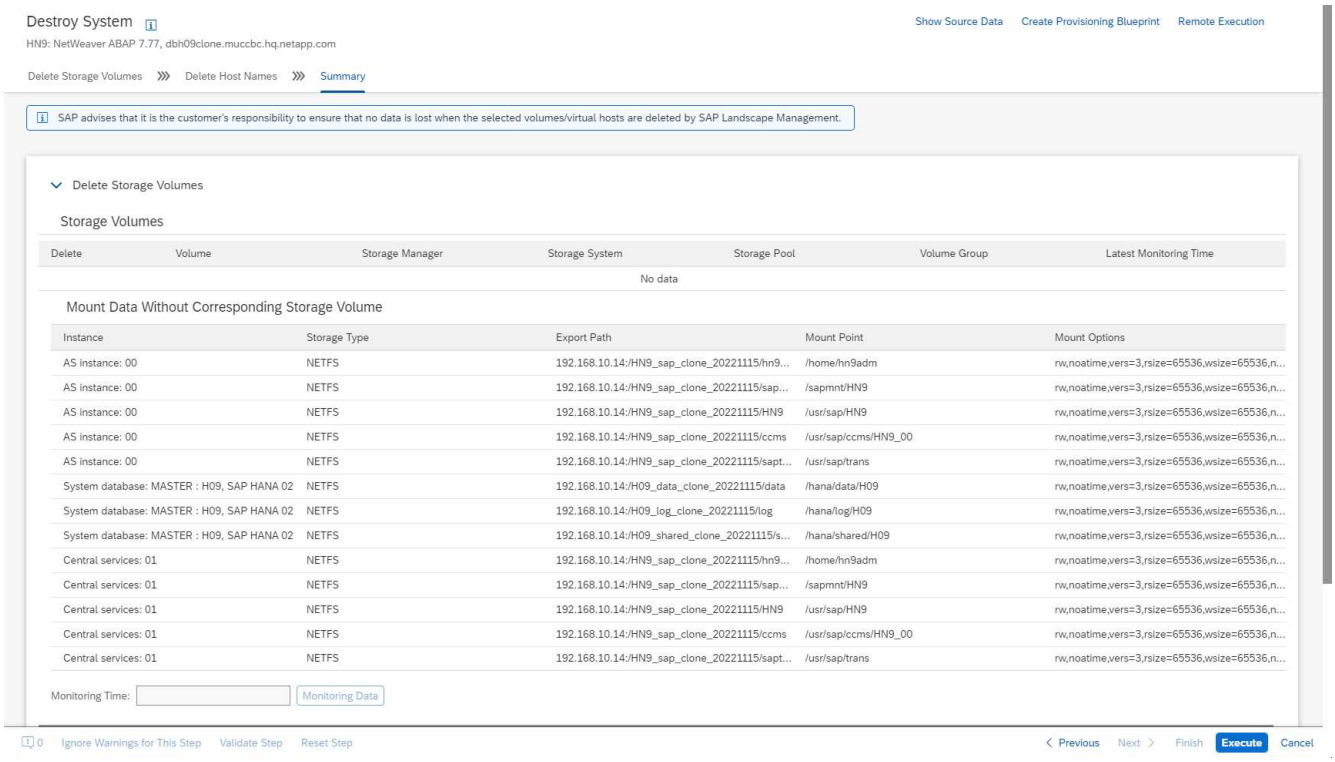
3. Hier werden alle während der Bereitstellungsphase gepflegten Mount-Punkte angezeigt und während des Workflow-Prozesses zur Systemzerstörung gelöscht.



Es werden keine virtuellen Hostnamen gelöscht, da sie über DNS gepflegt und automatisch zugewiesen wurden.

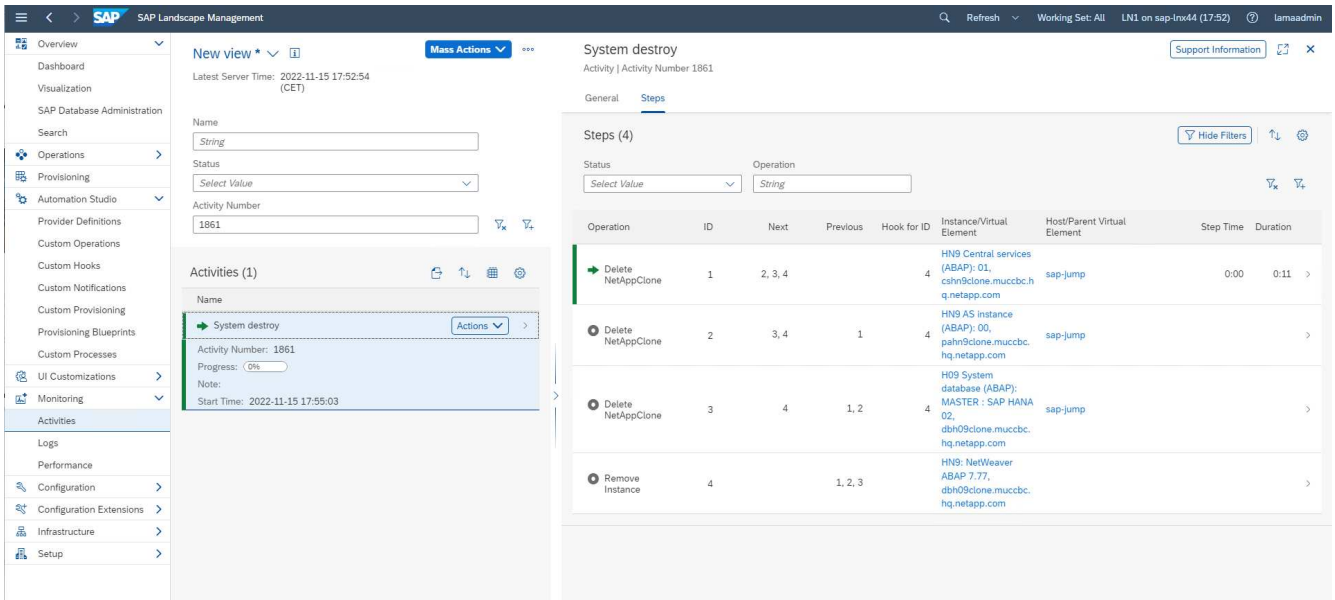


4. Klicken Sie auf die Schaltfläche Ausführen, um den Vorgang zu starten.

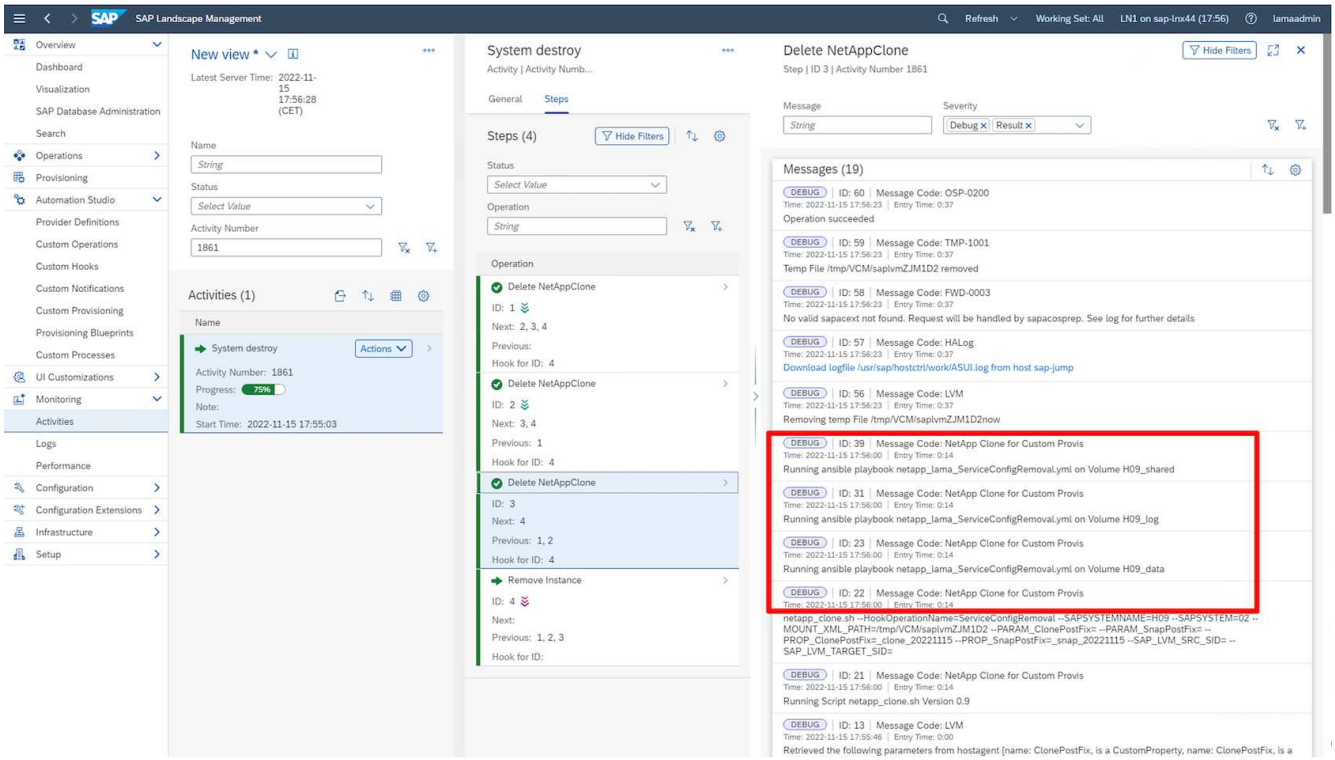


SAP Lama führt jetzt das Löschen der Volume-Klone durch und löscht die Konfiguration des geklonten Systems.

5. Sie können den Fortschritt des Klon-Workflows im Menü **Überwachung** überwachen.

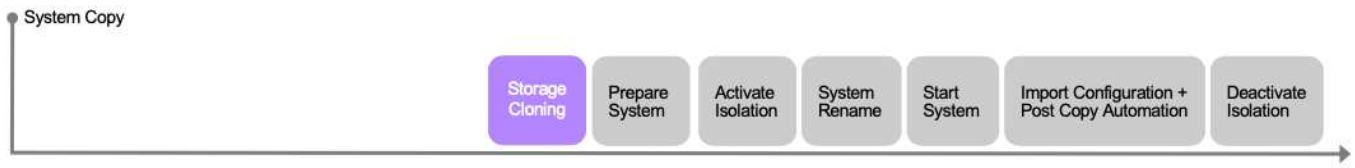


6. Durch Auswahl der Task **NetAppClone löschen** wird das detaillierte Protokoll für diesen Schritt angezeigt. Die Ausführung des Ansible Playbook ist hier dargestellt. Wie Sie sehen, das Ansible Playbook `netapp_lama_ServiceConfigRemoval.yml` Wird für jedes HANA Datenbank-Volume, die Daten, das Protokoll und die gemeinsame Nutzung ausgeführt.

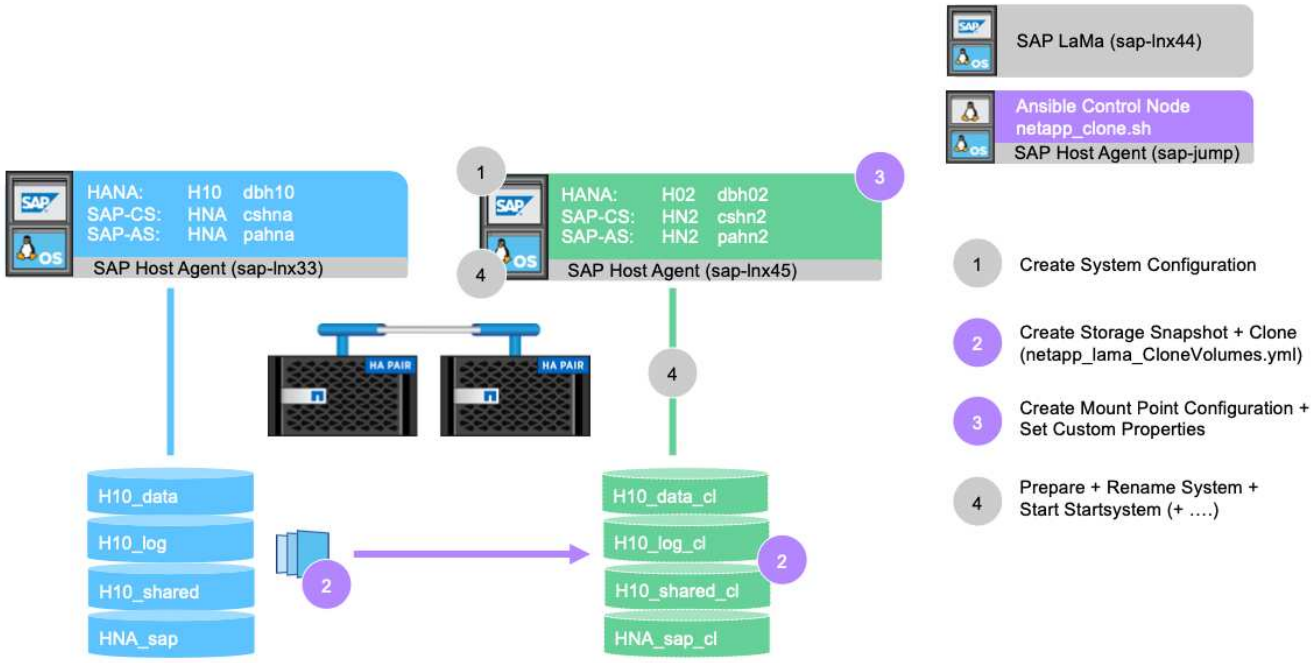


Workflow zur Bereitstellung von SAP Lama – Kopiersystem

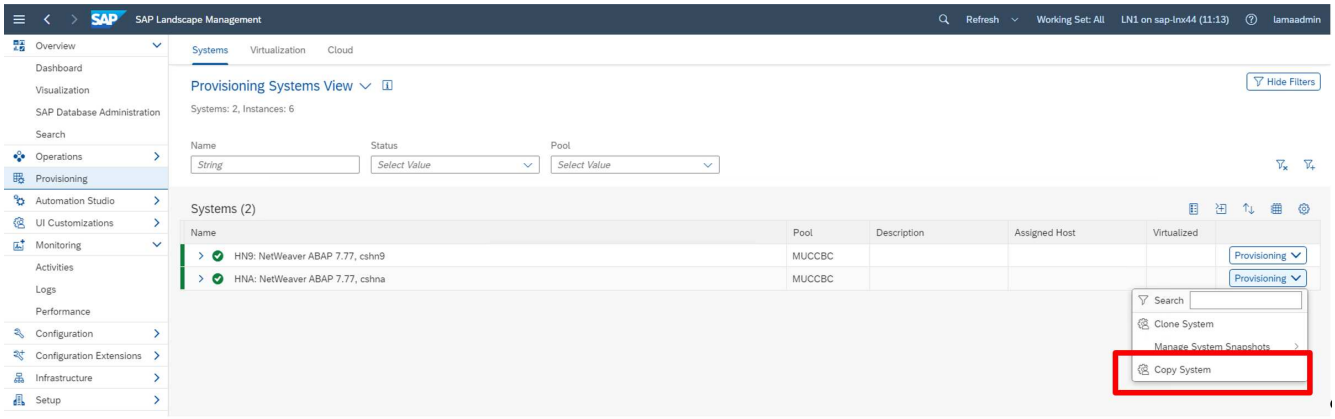
Die folgende Abbildung zeigt die primären Schritte, die mit dem Workflow für Systemkopien ausgeführt werden.



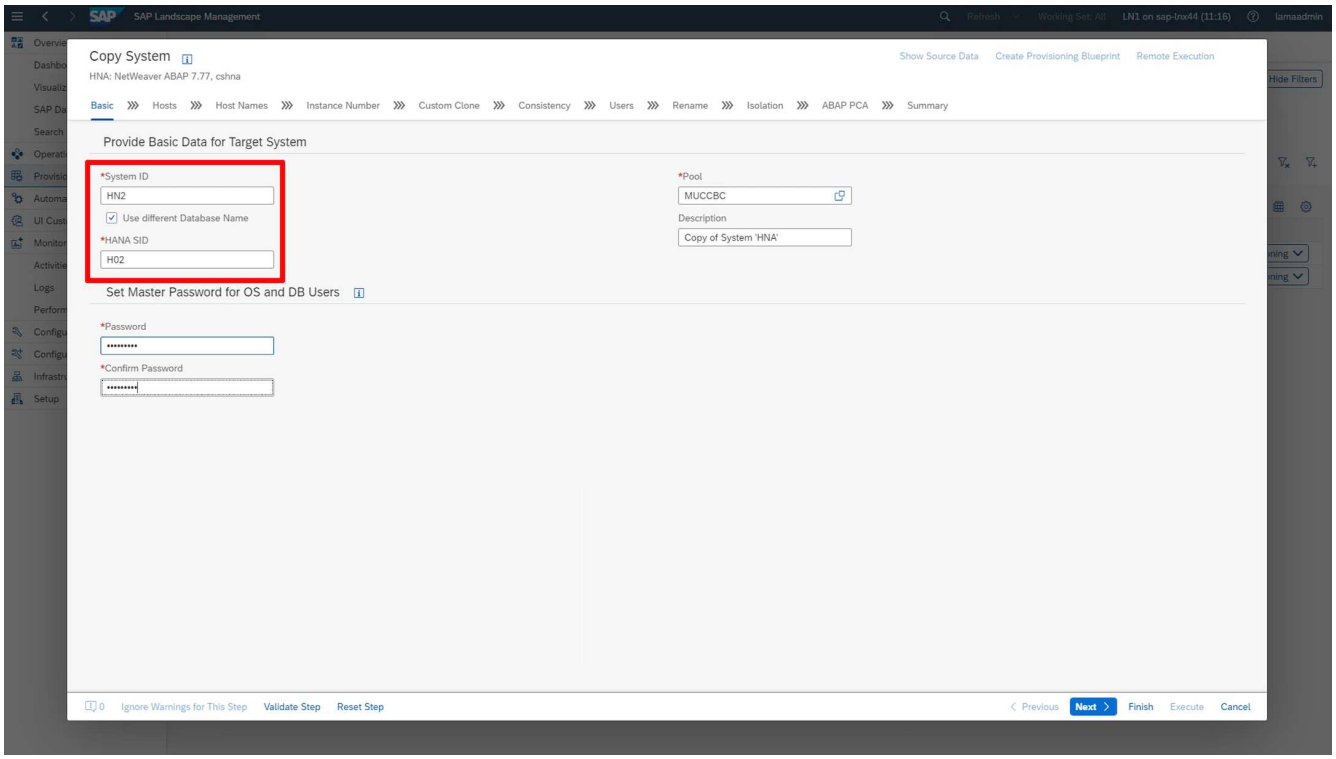
In diesem Kapitel besprechen wir kurz die Unterschiede zwischen dem Workflow und den Eingabebildschirmen von Systemklonen. Wie im folgenden Bild zu sehen ist, werden im Storage-Workflow keine Änderungen vorgenommen.



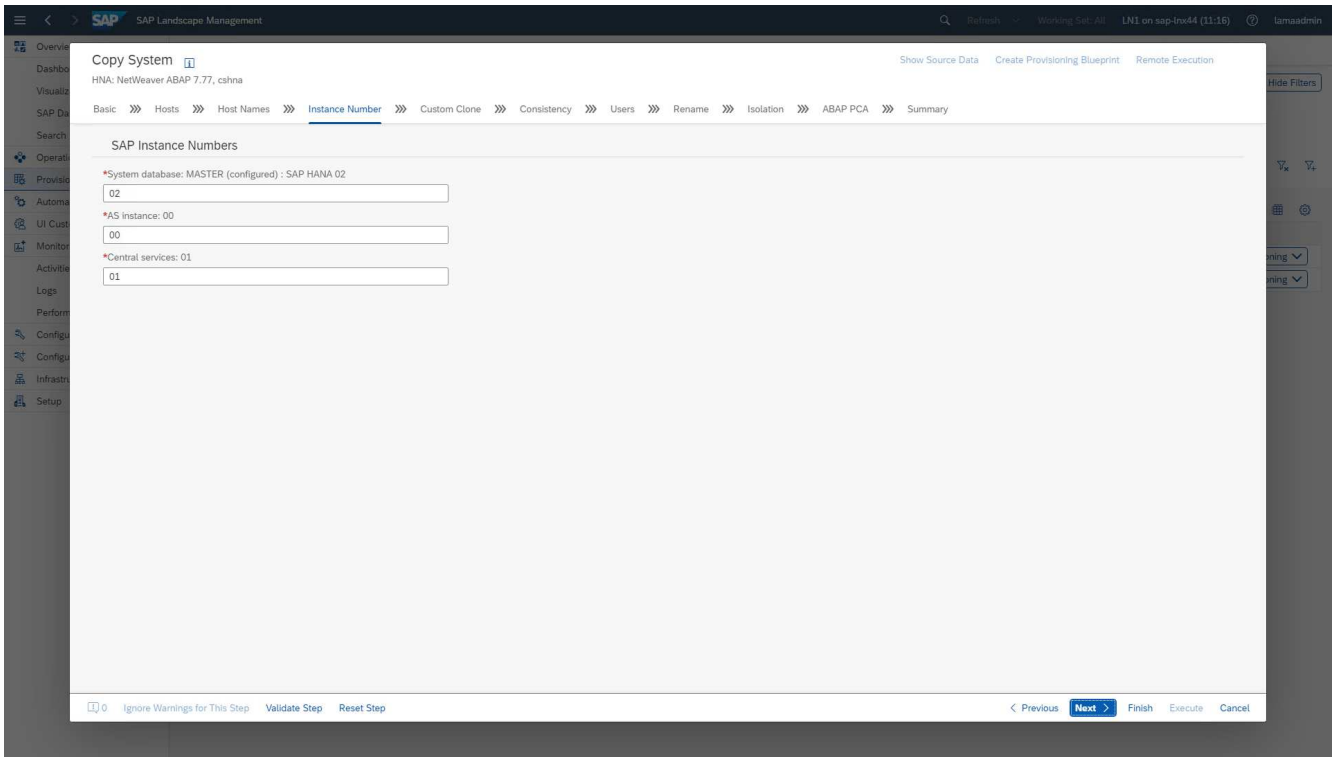
1. Der Workflow der Systemkopie kann gestartet werden, wenn das System entsprechend vorbereitet wird. Dies ist für diese Konfiguration keine spezifische Aufgabe, und wir erklären sie nicht im Detail. Weitere Informationen finden Sie in der Dokumentation zu SAP Lama.



2. Während des Kopieworkflows wird das System umbenannt, was im ersten Bildschirm angegeben werden muss.

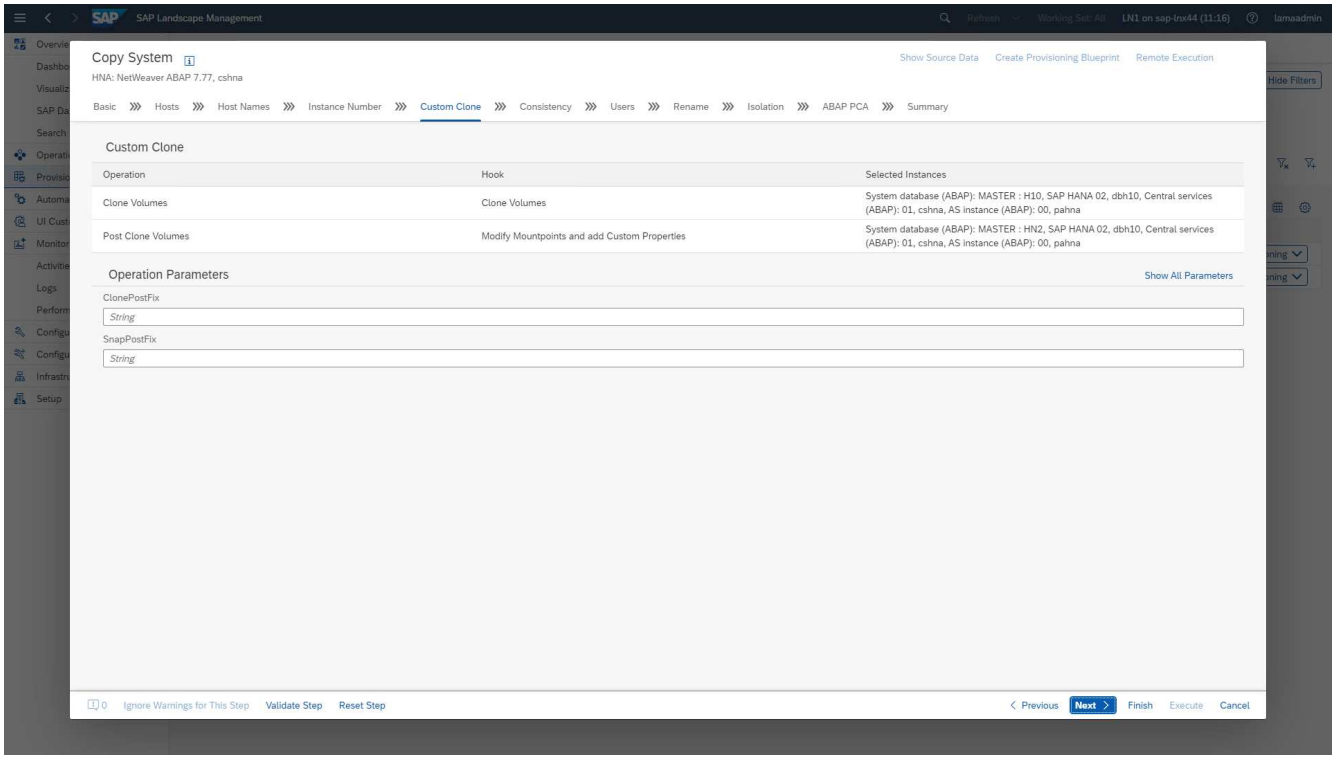


3. Während des Workflows können Sie die Instanznummern ändern.

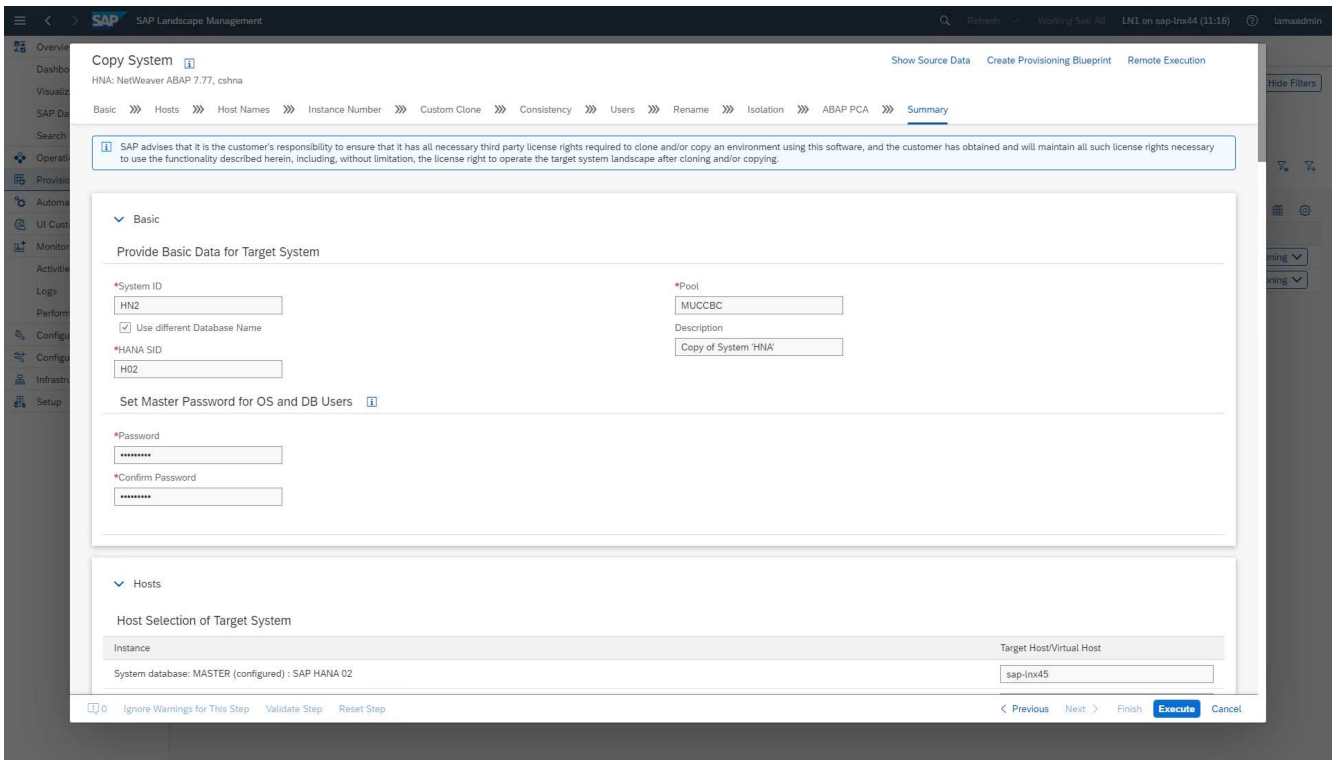


Das Ändern von Instanznummern wurde nicht getestet und erfordert möglicherweise Änderungen im Provider-Skript.

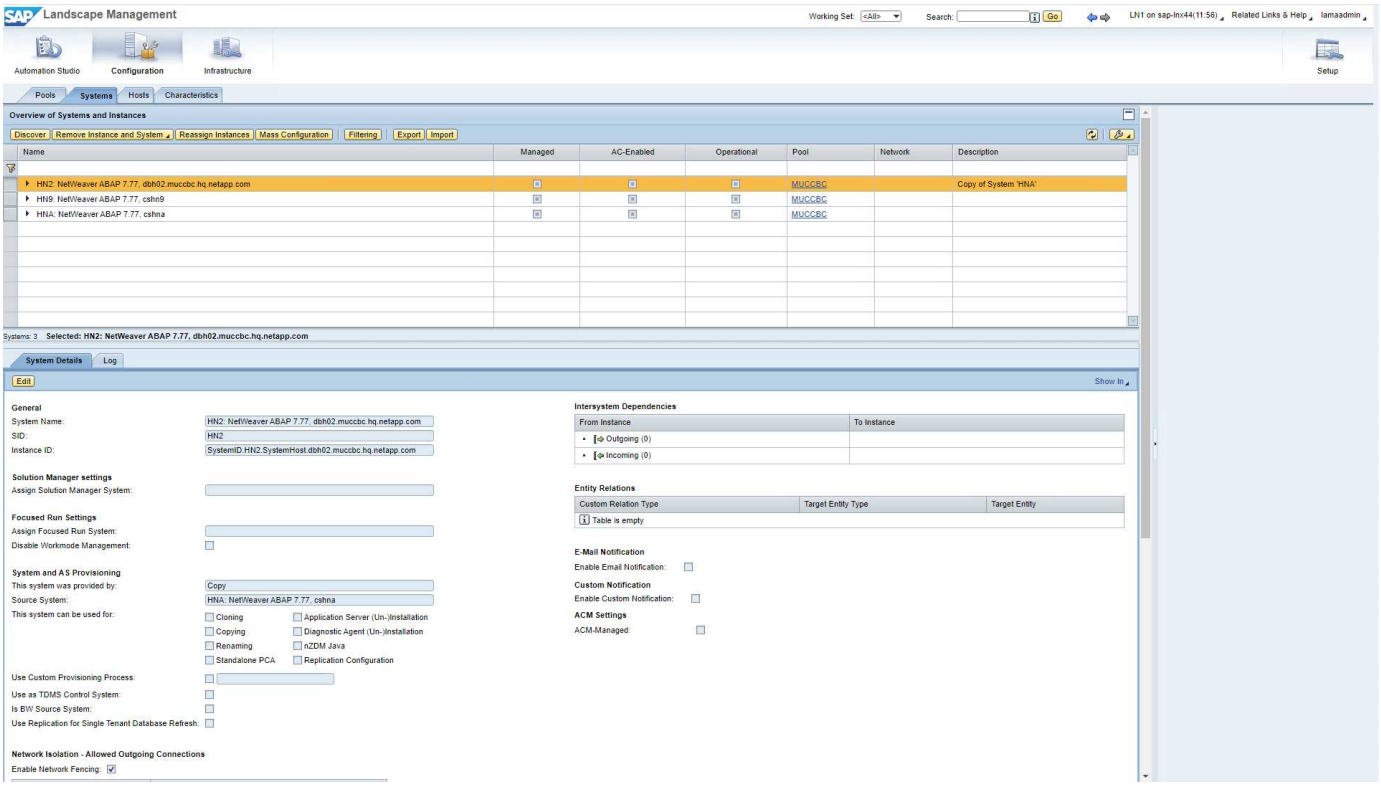
4. Wie hier beschrieben, unterscheidet sich der **Custom Clone**-Bildschirm nicht vom Klon-Workflow, wie hier dargestellt.



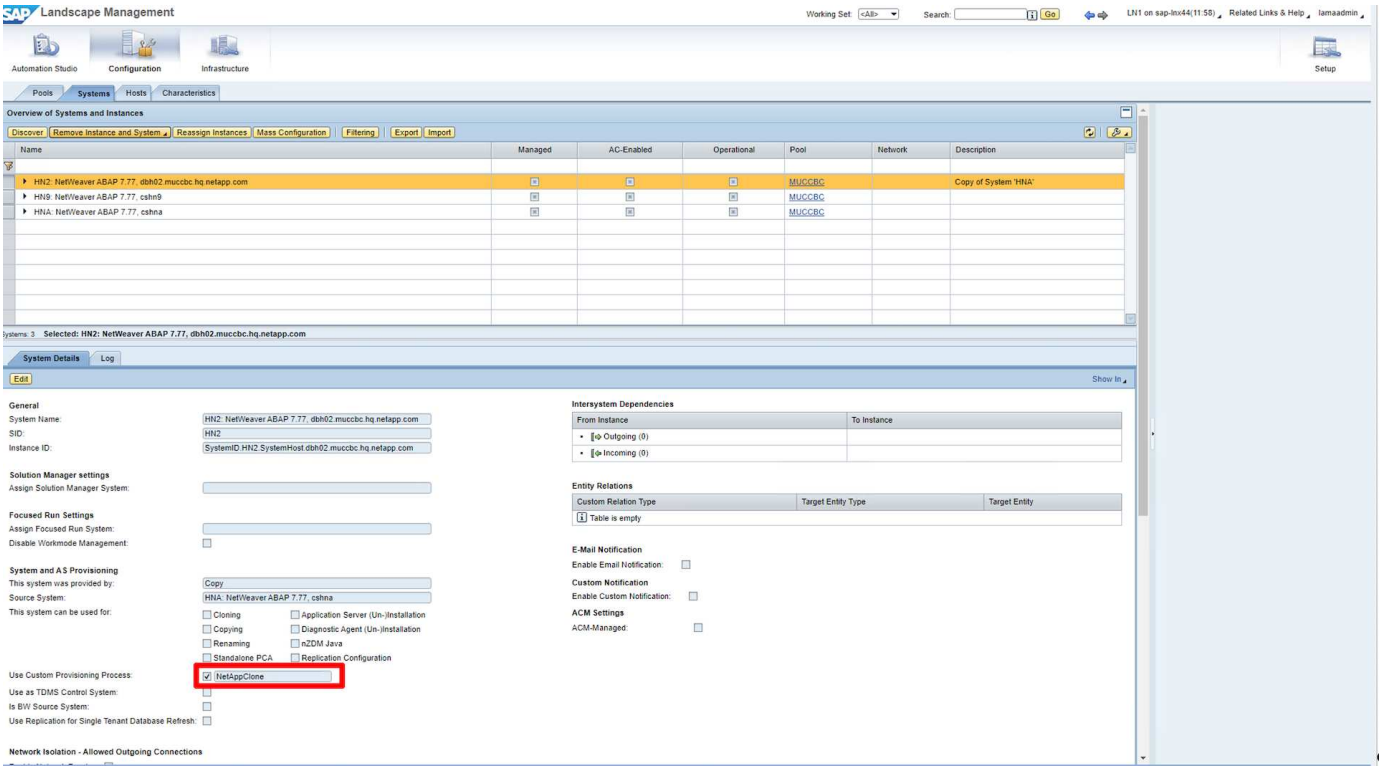
5. Wie wir bereits beschrieben haben, weichen die restlichen Eingabemasken nicht vom Standard ab, und wir gehen hier nicht weiter hinein. Der letzte Bildschirm zeigt eine Zusammenfassung, und die Ausführung kann nun gestartet werden.



Nach dem Kopiervorgang ist die Zielinstanz für den benutzerdefinierten Klonprozess nicht aktiviert.

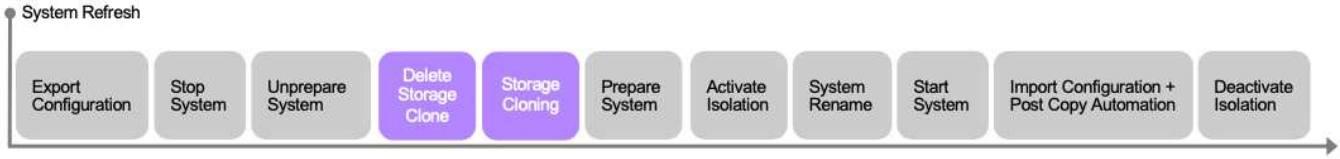


Es muss manuell angenommen werden, um den Pre-Hook-Schritt während des System Destroy-Prozesses auszuführen, weil eine Bedingung festgelegt ist und die Ausführung verhindert.

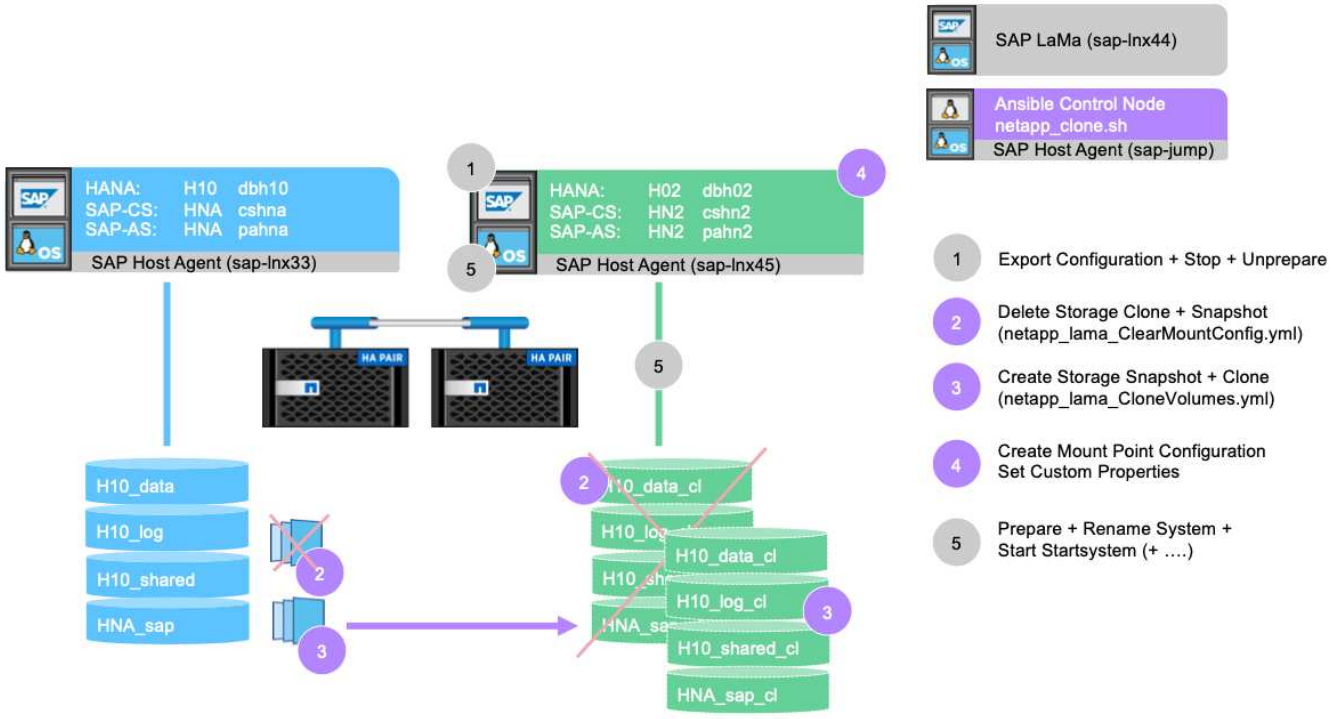


SAP Lama-Bereitstellungs-Workflow – Systemaktualisierung

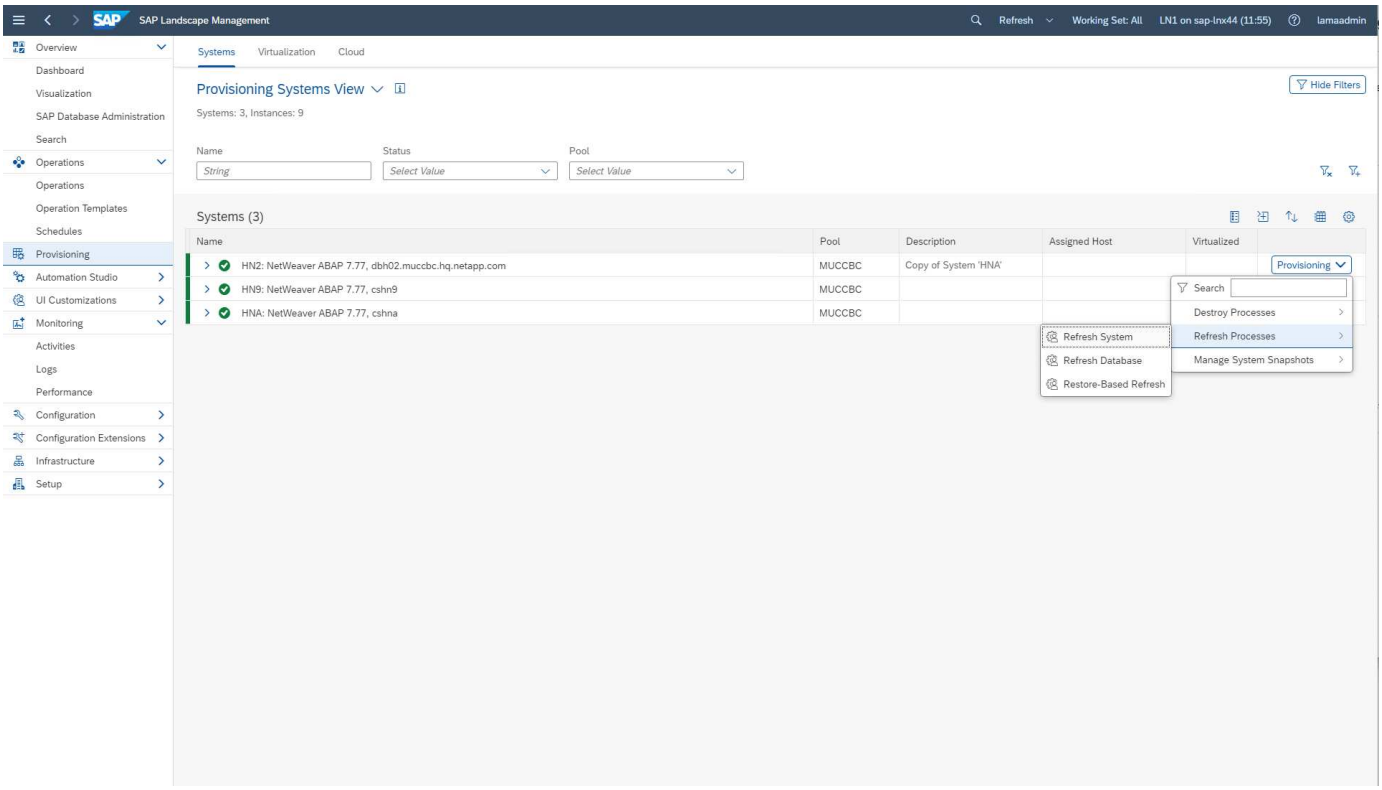
Die folgende Abbildung zeigt die wichtigsten Schritte, die bei der Systemaktualisierung ausgeführt werden.



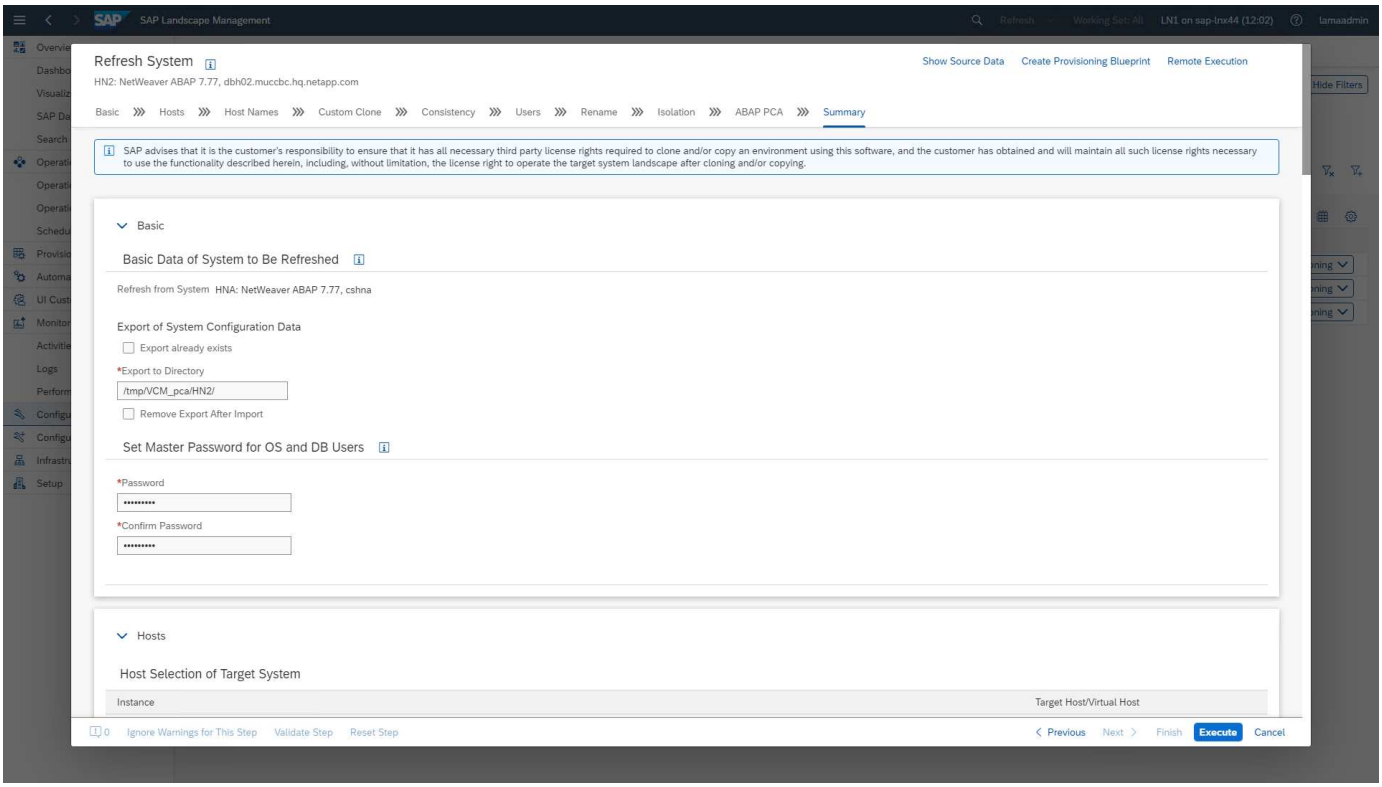
Während des Aktualisierungs-Workflows muss der Storage-Klon gelöscht werden. Sie können dasselbe Ansible-Playbook wie für den Workflow zum Zerstören des Systems verwenden. Der Custom Hook wird jedoch in einem anderen Schritt definiert, sodass das Playbook entsprechend benannt wird. Der Prozessschrittn´t Klons unterscheidet sich nicht.



Der Aktualisierungs-Workflow kann über den Bereitstellungsbildschirm für ein kopiertes System ausgelöst werden.



Auch hier unterscheidet sich nichts von den Eingabemasken vom Standard, und die Workflow-Ausführung kann über den Übersichtsbildschirm gestartet werden.



Provider-Skriptkonfiguration und Ansible Playbooks

Die folgende Provider-Konfigurationsdatei, das Ausführungsskript und Ansible-Playbooks

werden während der Beispielimplementierung und der Workflow-Ausführung in dieser Dokumentation verwendet.

> Die Beispielskripte werden wie IS bereitgestellt und von NetApp nicht unterstützt. Sie können die aktuelle Version der Skripte per E-Mail an ng-sapcc@netapp.com anfordern.

Konfigurationsdatei des Anbieters netapp_Clone.conf

Die Konfigurationsdatei wird wie im beschrieben erstellt "SAP Lama Documentation – Konfigurieren von registrierten Skripten für SAP-Host-Agent". Diese Konfigurationsdatei muss sich auf dem Ansible-Steuerungsknoten befinden, auf dem der SAP-Host-Agent installiert ist.

Der konfigurierte os-Benutzer `sapuser` Zum Ausführen des Skripts und der sogenannten Ansible Playbooks müssen die entsprechenden Berechtigungen vorhanden sein. Sie können das Skript in einem gemeinsamen Skriptverzeichnis platzieren. SAP Lama kann beim Aufruf des Skripts mehrere Parameter bereitstellen.

Zusätzlich zu den benutzerdefinierten Parametern `PARAM_ClonePostFix`, `PROP_ClonePostFix`, `PARAM_ClonePostFix`, und `PROP_ClonePostFix`, Viele andere können übergeben werden, wie in der gezeigt "SAP Lama-Dokumentation".

```
root@sap-jump:~# cat /usr/sap/hostctrl/exe/operations.d/netapp_clone.conf
Name: netapp_clone
Username: sapuser
Description: NetApp Clone for Custom Provisioning
Command: /usr/sap/scripts/netapp_clone.sh
--HookOperationName=$[HookOperationName] --SAPSYSTEMNAME=$[SAPSYSTEMNAME]
--SAPSYSTEM=$[SAPSYSTEM] --MOUNT_XML_PATH=$[MOUNT_XML_PATH]
--PARAM_ClonePostFix=$[PARAM-ClonePostFix] --PARAM_SnapPostFix=$[PARAM
-SnapPostFix] --PROP_ClonePostFix=$[PROP-ClonePostFix]
--PROP_SnapPostFix=$[PROP-SnapPostFix]
--SAP_LVM_SRC_SID=$[SAP_LVM_SRC_SID]
--SAP_LVM_TARGET_SID=$[SAP_LVM_TARGET_SID]
ResulConverter: hook
Platform: Unix
```

Provider-Skript netapp_clone.sh

Das Provider-Skript muss in gespeichert sein `/usr/sap/scripts` Wie in der Provider-Konfigurationsdatei konfiguriert.

Variablen

Die folgenden Variablen sind im Skript hartcodiert und müssen entsprechend angepasst werden.

- `PRIMARY_CLUSTER=`<hostname of netapp cluster>
- `PRIMARY_SVM=`<SVM name where source system volumes are stored>

Die Zertifikatdateien `PRIMARY_KEYFILE=/usr/sap/scripts/ansible/certs/ontap.key` Und `PRIMARY_CERTFILE=/usr/sap/scripts/ansible/certs/ontap.pem` Muss wie in beschrieben

bereitgestellt werden "NetApp Ansible Module – ONTAP vorbereiten".

> Wenn für verschiedene SAP-Systeme unterschiedliche Cluster oder SVMs erforderlich sind, können diese Variablen als Parameter in der SAP Lama-Provider-Definition hinzugefügt werden.

Funktion: Inventurdatei erstellen

Um die Ansible-Playbook-Ausführung dynamischer zu machen `inventory. yml` Datei wird während des Betriebs erstellt. Einige statische Werte werden im Abschnitt Variable konfiguriert und einige werden während der Ausführung dynamisch erzeugt.

Funktion: Ansible-Playbook ausführen

Diese Funktion wird verwendet, um das Ansible-Playbook zusammen mit dem dynamisch erstellten auszuführen `inventory.yml` Datei: Die Namenskonvention für Playbooks lautet `netapp_lama_${HookOperationName}.yml`. Die Werte für `${HookOperationName}` Ist von der Lama-Operation abhängig und wird von Lama als Kommandozeilenparameter übergeben.

Abschnitt Main

Dieser Abschnitt enthält den Hauptausführungsplan. Die Variable `${HookOperationName}` Enthält den Namen des Lama-Ersatzschritts und wird von Lama zur Verfügung gestellt, wenn das Skript aufgerufen wird.

- Werte mit dem Bereitstellungs-Workflow für Systemklone und Systemkopien:
  - KlonVolumes
  - PostCloneVolumes
- Wert mit dem Workflow zum Löschen des Systems:
  - ServiceConfigRemoval
- Nutzen des Workflows zur Systemaktualisierung:
  - ClearMountConfig

HookOperationName = CloneVolumes

Mit diesem Schritt wird das Ansible Playbook ausgeführt und der Snapshot Kopier- und Klonvorgang wird gestartet. Die Volume-Namen und Mount-Konfiguration werden von SAP Lama über eine in der Variable definierte XML-Datei übergeben `$MOUNT_XML_PATH`. Diese Datei wird gespeichert, da sie später im Schritt verwendet wird `FinalizeCloneVolumes` So erstellen Sie die neue Mount-Point-Konfiguration. Die Volume-Namen werden aus der XML-Datei extrahiert und das Ansible-Klon-Playbook für jedes Volume wird ausgeführt.

> In diesem Beispiel teilen sich DIE AS-Instanz und die zentralen Dienste dasselbe Volume. Daher wird das Klonen von Volumes nur dann ausgeführt, wenn die SAP Instanznummer angegeben ist (`$SAPSYSTEM`) Ist nicht `01`. Dies kann in anderen Umgebungen variieren und muss entsprechend geändert werden.

HookOperationName = PostCloneVolumes

In diesem Schritt werden die benutzerdefinierten Eigenschaften angezeigt `ClonePostFix` Und `SnapPostFix` Und die Mount-Point-Konfiguration für das Zielsystem bleibt erhalten.

Die benutzerdefinierten Eigenschaften werden zu einem späteren Zeitpunkt als Eingabe verwendet, wenn das

System während des außer Betrieb gesetzt wird `ServiceConfigRemoval` Oder `ClearMountConfig` Signifikant. Das System ist so entworfen, dass die Einstellungen der benutzerdefinierten Parameter beibehalten werden, die während des Workflows zur Systembereitstellung angegeben wurden.

Die in diesem Beispiel verwendeten Werte sind `ClonePostFix=_clone_20221115` Und `SnapPostFix=_snap_20221115`.

Für das Volume `HN9_sap`, Die dynamisch erstellte Ansible-Datei enthält die folgenden Werte: `datavolumename: HN9_sap`, `snapshotpostfix: _snap_20221115`, und `clonepostfix: _clone_20221115`.

Was zu dem Snapshot-Namen auf dem Volume HN9_sap führt `HN9_sap_snap_20221115` Und den Namen des erstellten Volume-Klons `HN9_sap_clone_20221115`.

Benutzerdefinierte Eigenschaften können in jeder Hinsicht verwendet werden, um Parameter zu erhalten, die während des Bereitstellungsprozesses verwendet werden.

Die Mount-Point-Konfiguration wird aus der XML-Datei extrahiert, die Lama im übergeben hat `CloneVolume` Schritt: Der `ClonePostFix` Wird den Volume-Namen hinzugefügt und über die Standard-Skriptausgabe an Lama zurückgesendet. Die Funktionalität wird in beschrieben "SAP-Hinweis 1889590".

In diesem Beispiel werden qtrees auf dem Storage-System als gemeinsame Methode zum Speichern verschiedener Daten auf einem einzelnen Volume verwendet. Beispiel: `HN9_sap` Hält die Mount-Punkte für `/usr/sap/HN9`, `/sapmnt/HN9`, und `/home/hn9adm`. Unterverzeichnisse funktionieren auf die gleiche Weise. Dies kann in anderen Umgebungen variieren und muss entsprechend geändert werden.

HookOperationName = ServiceConfigRemoval

In diesem Schritt wird das Ansible-Playbook, das für das Löschen der Volume-Klone verantwortlich ist, ausgeführt.

Die Volume-Namen werden von SAP Lama über die Mount-Konfigurationsdatei und die benutzerdefinierten Eigenschaften übergeben `ClonePostFix` Und `SnapPostFix` Werden verwendet, um die Werte der Parameter, die ursprünglich während des System-Provisioning-Workflows angegeben wurden, zu übergeben (siehe Hinweis unter `HookOperationName = PostCloneVolumes`).

Die Volume-Namen werden aus der XML-Datei extrahiert und das Ansible-Klon-Playbook für jedes Volume wird ausgeführt.

In diesem Beispiel teilen sich DIE AS-Instanz und die zentralen Dienste dasselbe Volume. Daher wird das Volume-Löschen nur bei der SAP-Instanznummer ausgeführt (`$SAPSYSTEM`) Ist nicht `01`. Dies kann in anderen Umgebungen variieren und muss entsprechend geändert werden.

HookOperationName = ClearMountConfig

In diesem Schritt wird das Ansible-Playbook ausgeführt, das während der Systemaktualisierung die Löschung von Volume-Klonen übernimmt.

Die Volume-Namen werden von SAP Lama über die Mount-Konfigurationsdatei und die benutzerdefinierten Eigenschaften übergeben `ClonePostFix` Und `SnapPostFix` Werden verwendet, um die Werte der

Parameter zu übergeben, die ursprünglich während des System-Provisioning-Workflows angegeben wurden.

Die Volume-Namen werden aus der XML-Datei extrahiert und das Ansible-Klon-Playbook für jedes Volume wird ausgeführt.

> In diesem Beispiel teilen sich DIE AS-Instanz und die zentralen Dienste dasselbe Volume. Daher wird das Löschen von Volumes nur bei der SAP-Instanznummer ausgeführt (`$SAPSYSTEM`) Ist nicht `01`. Dies kann in anderen Umgebungen variieren und muss entsprechend geändert werden.

```
root@sap-jump:~# cat /usr/sap/scripts/netapp_clone.sh
#!/bin/bash
#Section - Variables
########################################
VERSION="Version 0.9"
#Path for ansible play-books
ANSIBLE_PATH=/usr/sap/scripts/ansible
#Values for Ansible Inventory File
PRIMARY_CLUSTER=grenada
PRIMARY_SVM=svm-sap01
PRIMARY_KEYFILE=/usr/sap/scripts/ansible/certs/ontap.key
PRIMARY_CERTFILE=/usr/sap/scripts/ansible/certs/ontap.pem
#Default Variable if PARAM ClonePostFix / SnapPostFix is not maintained in
LaMa
DefaultPostFix=_clone_1
#TMP Files - used during execution
YAML_TMP=/tmp/inventory_ansible_clone_tmp_$$.yml
TMPFILE=/tmp/tmpfile.$$
MY_NAME="`basename $0`"
BASE_SCRIPT_DIR="`dirname $0`"
#Sendig Script Version and run options to LaMa Log
echo "[DEBUG]: Running Script $MY_NAME $VERSION"
echo "[DEBUG]: $MY_NAME $@"
#Command declared in the netapp_clone.conf Provider definition
#Command: /usr/sap/scripts/netapp_clone.sh
--HookOperationName=$[HookOperationName] --SAPSYSTEMNAME=$[SAPSYSTEMNAME]
--SAPSYSTEM=$[SAPSYSTEM] --MOUNT_XML_PATH=$[MOUNT_XML_PATH]
--PARAM_ClonePostFix=$[PARAM-ClonePostFix] --PARAM_SnapPostFix=$[PARAM
-SnapPostFix] --PROP_ClonePostFix=$[PROP-ClonePostFix]
--PROP_SnapPostFix=$[PROP-SnapPostFix]
--SAP_LVM_SRC_SID=$[SAP_LVM_SRC_SID]
--SAP_LVM_TARGET_SID=$[SAP_LVM_TARGET_SID]
#Reading Input Variables hand over by LaMa
for i in "$@"
do
case $i in
--HookOperationName=*)
```

```
HookOperationName="${i#*=}";shift;;
--SAPSYSTEMNAME=*)
SAPSYSTEMNAME="${i#*=}";shift;;
--SAPSYSTEM=*)
SAPSYSTEM="${i#*=}";shift;;
--MOUNT_XML_PATH=*)
MOUNT_XML_PATH="${i#*=}";shift;;
--PARAM_ClonePostFix=*)
PARAM_ClonePostFix="${i#*=}";shift;;
--PARAM_SnapPostFix=*)
PARAM_SnapPostFix="${i#*=}";shift;;
--PROP_ClonePostFix=*)
PROP_ClonePostFix="${i#*=}";shift;;
--PROP_SnapPostFix=*)
PROP_SnapPostFix="${i#*=}";shift;;
--SAP_LVM_SRC_SID=*)
SAP_LVM_SRC_SID="${i#*=}";shift;;
--SAP_LVM_TARGET_SID=*)
SAP_LVM_TARGET_SID="${i#*=}";shift;;
*)
# unknown option
;;
esac
done
#If Parameters not provided by the User - defaulting to DefaultPostFix
if [ -z $PARAM_ClonePostFix ]; then PARAM_ClonePostFix=$DefaultPostFix;fi
if [ -z $PARAM_SnapPostFix ]; then PARAM_SnapPostFix=$DefaultPostFix;fi
#Section - Functions
########################################
#Function Create (Inventory) YML File
########################################
create_yml_file()
{
echo "ontapservers:">$YAML_TMP
echo " hosts:">>$YAML_TMP
echo "  ${PRIMARY_CLUSTER}:">>$YAML_TMP
echo "   ansible_host: "'"'$PRIMARY_CLUSTER'"'">>$YAML_TMP
echo "   keyfile: "'"'$PRIMARY_KEYFILE'"'">>$YAML_TMP
echo "   certfile: "'"'$PRIMARY_CERTFILE'"'">>$YAML_TMP
echo "   svmname: "'"'$PRIMARY_SVM'"'">>$YAML_TMP
echo "   datavolumename: "'"'$datavolumename'"'">>$YAML_TMP
echo "   snapshotpostfix: "'"'$snapshotpostfix'"'">>$YAML_TMP
echo "   clonepostfix: "'"'$clonepostfix'"'">>$YAML_TMP
}
#Function run ansible-playbook
########################################
```

```
run_ansible_playbook()
{
echo "[DEBUG]: Running ansible playbook
netapp_lama_${HookOperationName}.yml on Volume $datavolumename"
ansible-playbook -i $YAML_TMP
$ANSIBLE_PATH/netapp_lama_${HookOperationName}.yml
}
#Section - Main
########################################
#HookOperationName - CloneVolumes
########################################
if [ $HookOperationName = CloneVolumes ] ;then
#save mount xml for later usage - used in Section FinalizeCloneVolues to
generate the mountpoints
echo "[DEBUG]: saving mount config...."
cp $MOUNT_XML_PATH /tmp/mount_config_${SAPSYSTEMNAME}_${SAPSYSTEM}.xml
#Instance 00 + 01 share the same volumes - clone needs to be done once
if [ $SAPSYSTEM != 01 ]; then
#generating Volume List - assuming usage of qtrees - "IP-
Adress:/VolumeName/qtree"
xmlFile=/tmp/mount_config_${SAPSYSTEMNAME}_${SAPSYSTEM}.xml
if [ -e $TMPFILE ];then rm $TMPFILE;fi
numMounts=`xml_grep --count "/mountconfig/mount" $xmlFile | grep "total: "
| awk '{ print $2 }'`
i=1
while [ $i -le $numMounts ]; do
     xmllint --xpath "/mountconfig/mount[$i]/exportpath/text()" $xmlFile
|awk -F"/" '{print $2}' >>$TMPFILE
i=$((i + 1))
done
DATAVOLUMES=`cat  $TMPFILE |sort -u`
#Create yml file and rund playbook for each volume
for I in $DATAVOLUMES; do
datavolumename="$I"
snapshotpostfix="$PARAM_SnapPostFix"
clonepostfix="$PARAM_ClonePostFix"
create_yml_file
run_ansible_playbook
done
else
echo "[DEBUG]: Doing nothing .... Volume cloned in different Task"
fi
fi
#HookOperationName - PostCloneVolumes
########################################
if [ $HookOperationName = PostCloneVolumes] ;then
```

```
#Reporting Properties back to LaMa Config for Cloned System
echo "[RESULT]:Property:ClonePostFix=$PARAM_ClonePostFix"
echo "[RESULT]:Property:SnapPostFix=$PARAM_SnapPostFix"
#Create MountPoint Config for Cloned Instances and report back to LaMa
according to SAP Note: https://launchpad.support.sap.com/#/notes/1889590
echo "MountDataBegin"
echo '<?xml version="1.0" encoding="UTF-8"?>'
echo "<mountconfig>"
xmlFile=/tmp/mount_config_${SAPSYSTEMNAME}_${SAPSYSTEM}.xml
numMounts=`xml_grep --count "/mountconfig/mount" $xmlFile | grep "total: "
| awk '{ print $2 }'`
i=1
while [ $i -le $numMounts ]; do
MOUNTPOINT=`xmllint --xpath "/mountconfig/mount[$i]/mountpoint/text()"
$xmlFile`;
        EXPORTPATH=`xmllint --xpath
"/mountconfig/mount[$i]/exportpath/text()" $xmlFile`;
        OPTIONS=`xmllint --xpath "/mountconfig/mount[$i]/options/text()"
$xmlFile`;
#Adopt Exportpath and add Clonepostfix - assuming usage of qtrees - "IP-
Adress:/VolumeName/qtree"
TMPFIELD1=`echo $EXPORTPATH|awk -F":/" '{print $1}'`
TMPFIELD2=`echo $EXPORTPATH|awk -F"/" '{print $2}'`
TMPFIELD3=`echo $EXPORTPATH|awk -F"/" '{print $3}'`
EXPORTPATH=$TMPFIELD1":/"${TMPFIELD2}$PARAM_ClonePostFix"/"$TMPFIELD3
echo -e '\t<mount fstype="nfs" storagetype="NETFS">'
echo -e "\t\t<mountpoint>${MOUNTPOINT}</mountpoint>"
echo -e "\t\t<exportpath>${EXPORTPATH}</exportpath>"
echo -e "\t\t<options>${OPTIONS}</options>"
echo -e "\t</mount>"
i=$((i + 1))
done
echo "</mountconfig>"
echo "MountDataEnd"
#Finished MountPoint Config
#Cleanup Temporary Files
rm $xmlFile
fi
#HookOperationName - ServiceConfigRemoval
########################################
if [ $HookOperationName = ServiceConfigRemoval ] ;then
#Assure that Properties ClonePostFix and SnapPostfix has been configured
through the provisioning process
if [ -z $PROP_ClonePostFix ]; then echo "[ERROR]: Propertiy ClonePostFix
is not handed over - please investigate";exit 5;fi
if [ -z $PROP_SnapPostFix ]; then echo "[ERROR]: Propertiy SnapPostFix is
```

```
not handed over - please investigate";exit 5;fi
#Instance 00 + 01 share the same volumes - clone delete needs to be done
once
if [ $SAPSYSTEM != 01 ]; then
#generating Volume List - assuming usage of qtrees - "IP-
Adress:/VolumeName/qtree"
xmlFile=$MOUNT_XML_PATH
if [ -e $TMPFILE ];then rm $TMPFILE;fi
numMounts=`xml_grep --count "/mountconfig/mount" $xmlFile | grep "total: "
| awk '{ print $2 }'`
i=1
while [ $i -le $numMounts ]; do
     xmllint --xpath "/mountconfig/mount[$i]/exportpath/text()" $xmlFile
|awk -F"/" '{print $2}' >>$TMPFILE
i=$((i + 1))
done
DATAVOLUMES=`cat  $TMPFILE |sort -u| awk -F $PROP_ClonePostFix '{ print $1
}'`
#Create yml file and rund playbook for each volume
for I in $DATAVOLUMES; do
datavolumename="$I"
snapshotpostfix="$PROP_SnapPostFix"
clonepostfix="$PROP_ClonePostFix"
create_yml_file
run_ansible_playbook
done
else
echo "[DEBUG]: Doing nothing .... Volume deleted in different Task"
fi
#Cleanup Temporary Files
rm $xmlFile
fi
#HookOperationName - ClearMountConfig
########################################
if [ $HookOperationName = ClearMountConfig ] ;then
        #Assure that Properties ClonePostFix and SnapPostfix has been
configured through the provisioning process
        if [ -z $PROP_ClonePostFix ]; then echo "[ERROR]: Propertiy
ClonePostFix is not handed over - please investigate";exit 5;fi
        if [ -z $PROP_SnapPostFix ]; then echo "[ERROR]: Propertiy
SnapPostFix is not handed over - please investigate";exit 5;fi
        #Instance 00 + 01 share the same volumes - clone delete needs to
be done once
        if [ $SAPSYSTEM != 01 ]; then
                #generating Volume List - assuming usage of qtrees - "IP-
Adress:/VolumeName/qtree"
```

```
                xmlFile=$MOUNT_XML_PATH
                if [ -e $TMPFILE ];then rm $TMPFILE;fi
                numMounts=`xml_grep --count "/mountconfig/mount" $xmlFile
| grep "total: " | awk '{ print $2 }'`
                i=1
                while [ $i -le $numMounts ]; do
                        xmllint --xpath
"/mountconfig/mount[$i]/exportpath/text()" $xmlFile |awk -F"/" '{print
$2}' >>$TMPFILE
                        i=$((i + 1))
                done
                DATAVOLUMES=`cat  $TMPFILE |sort -u| awk -F
$PROP_ClonePostFix '{ print $1 }'`
                #Create yml file and rund playbook for each volume
                for I in $DATAVOLUMES; do
                        datavolumename="$I"
                        snapshotpostfix="$PROP_SnapPostFix"
                        clonepostfix="$PROP_ClonePostFix"
                        create_yml_file
                        run_ansible_playbook
                done
        else
                echo "[DEBUG]: Doing nothing .... Volume deleted in
different Task"
        fi
        #Cleanup Temporary Files
        rm $xmlFile
fi
#Cleanup
########################################
#Cleanup Temporary Files
if [ -e $TMPFILE ];then rm $TMPFILE;fi
if [ -e $YAML_TMP ];then rm $YAML_TMP;fi
exit 0
```

Ansible-Playbook netapp_lama_KlonVolumes.yml

Das Playbook, das während des CloneVolumes-Schritts des Arbeitsablaufs des Lama-Systems ausgeführt wird, ist eine Kombination aus `create_snapshot.yml` Und `create_clone.yml` (Siehe "NetApp Ansible Module – YAML-Dateien"). Dieses Playbook kann einfach erweitert werden, um weitere Anwendungsfälle wie das Klonen von sekundären Operationen und Klontrennungen abzudecken.

```
root@sap-jump:~# cat /usr/sap/scripts/ansible/netapp_lama_CloneVolumes.yml
---
- hosts: ontapservers
  connection: local
  collections:
    - netapp.ontap
  gather_facts: false
  name: netapp_lama_CloneVolumes
  tasks:
  - name: Create SnapShot
    na_ontap_snapshot:
      state: present
      snapshot: "{{ datavolumename }}{{ snapshotpostfix }}"
      use_rest: always
      volume: "{{ datavolumename }}"
      vserver: "{{ svmname }}"
      hostname: "{{ inventory_hostname }}"
      cert_filepath: "{{ certfile }}"
      key_filepath: "{{ keyfile }}"
      https: true
      validate_certs: false
  - name: Clone Volume
    na_ontap_volume_clone:
      state: present
      name: "{{ datavolumename }}{{ clonepostfix }}"
      use_rest: always
      vserver: "{{ svmname }}"
      junction_path: '/{{ datavolumename }}{{ clonepostfix }}'
      parent_volume: "{{ datavolumename }}"
      parent_snapshot: "{{ datavolumename }}{{ snapshotpostfix }}"
      hostname: "{{ inventory_hostname }}"
      cert_filepath: "{{ certfile }}"
      key_filepath: "{{ keyfile }}"
      https: true
      validate_certs: false
```

Ansible-Playbook netapp_lama_ServiceConfigRemoval.yml

Das Playbook, das während des ausgeführt wird `ServiceConfigRemoval` Phase des Lama-System zerstörenden Workflows ist eine Kombination von `delete_clone.yml` Und `delete_snapshot.yml` (Siehe "NetApp Ansible Module – YAML-Dateien"). Sie muss an den Ausführungsschritten des ausgerichtet sein `netapp_lama_CloneVolumes` playbook.

```
root@sap-jump:~# cat
/usr/sap/scripts/ansible/netapp_lama_ServiceConfigRemoval.yml
---
- hosts: ontapservers
  connection: local
  collections:
    - netapp.ontap
  gather_facts: false
  name: netapp_lama_ServiceConfigRemoval
  tasks:
  - name: Delete Clone
    na_ontap_volume:
      state: absent
      name: "{{ datavolumename }}{{ clonepostfix }}"
      use_rest: always
      vserver: "{{ svmname }}"
      wait_for_completion: True
      hostname: "{{ inventory_hostname }}"
      cert_filepath: "{{ certfile }}"
      key_filepath: "{{ keyfile }}"
      https: true
      validate_certs: false
  - name: Delete SnapShot
    na_ontap_snapshot:
      state: absent
      snapshot: "{{ datavolumename }}{{ snapshotpostfix }}"
      use_rest: always
      volume: "{{ datavolumename }}"
      vserver: "{{ svmname }}"
      hostname: "{{ inventory_hostname }}"
      cert_filepath: "{{ certfile }}"
      key_filepath: "{{ keyfile }}"
      https: true
      validate_certs: false
root@sap-jump:~#
```

Ansible Playbook netapp_lama_ClearMountConfig.Yml

Das Playbook, das während des ausgeführt wird `netapp_lama_ClearMountConfig` Die Phase des Arbeitsablaufs zur Systemaktualisierung ist eine Kombination aus `delete_clone.yml` Und `delete_snapshot.yml` (Siehe "NetApp Ansible Module – YAML-Dateien"). Sie muss an den Ausführungsschritten des ausgerichtet sein `netapp_lama_CloneVolumes` playbook.

```
root@sap-jump:~# cat
/usr/sap/scripts/ansible/netapp_lama_ServiceConfigRemoval.yml
---
- hosts: ontapservers
  connection: local
  collections:
    - netapp.ontap
  gather_facts: false
  name: netapp_lama_ServiceConfigRemoval
  tasks:
  - name: Delete Clone
    na_ontap_volume:
      state: absent
      name: "{{ datavolumename }}{{ clonepostfix }}"
      use_rest: always
      vserver: "{{ svmname }}"
      wait_for_completion: True
      hostname: "{{ inventory_hostname }}"
      cert_filepath: "{{ certfile }}"
      key_filepath: "{{ keyfile }}"
      https: true
      validate_certs: false
  - name: Delete SnapShot
    na_ontap_snapshot:
      state: absent
      snapshot: "{{ datavolumename }}{{ snapshotpostfix }}"
      use_rest: always
      volume: "{{ datavolumename }}"
      vserver: "{{ svmname }}"
      hostname: "{{ inventory_hostname }}"
      cert_filepath: "{{ certfile }}"
      key_filepath: "{{ keyfile }}"
      https: true
      validate_certs: false
root@sap-jump:~#
```

Beispiel für Ansible-Inventar.YML

Diese Bestandsdatei wird während der Workflow-Ausführung dynamisch erstellt, und sie wird hier nur zur Illustration angezeigt.

```
ontapservers:
 hosts:
  grenada:
   ansible_host: "grenada"
   keyfile: "/usr/sap/scripts/ansible/certs/ontap.key"
   certfile: "/usr/sap/scripts/ansible/certs/ontap.pem"
   svmname: "svm-sap01"
   datavolumename: "HN9_sap"
   snapshotpostfix: " _snap_20221115"
   clonepostfix: "_clone_20221115"
```

Schlussfolgerung

Die Integration eines modernen Automatisierungs-Frameworks wie Ansible in SAP Lama-Bereitstellungs-Workflows bietet Kunden eine flexible Lösung, die Standardanforderungen und komplexere Infrastrukturanforderungen erfüllt.

Wo Sie weitere Informationen finden

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- Sammlungen im NetApp Namespace

  "https://docs.ansible.com/ansible/latest/collections/netapp/index.html"

- Dokumentation zu Ansible Integration und Beispiel Ansible Playbooks

  "https://github.com/sap-linuxlab/demo.netapp_ontap"

- Allgemeine Integration mit Ansible und NetApp

  "https://www.ansible.com/integrations/infrastructure/netapp"

- Blog zum Thema Integration von SAP Lama mit Ansible

  "https://blogs.sap.com/2020/06/08/outgoing-api-calls-from-sap-landscape-management-lama-with-automation-studio/"

- SAP Landscape Management 3.0, Enterprise Edition Documentation

  "https://help.sap.com/doc/700f9a7e52c7497cad37f7c46023b7ff/3.0.11.0/en-US/4df88a8f418c5059e10000000a42189c.html#loio4df88a8f418c5059e10000000a42189c"

- SAP Lama-Dokumentation – Provider-Definitionen

  "https://help.sap.com/doc/700f9a7e52c7497cad37f7c46023b7ff/3.0.11.0/en-US/bf6b3e43340a4cbcb0c0f3089715c068.html"

- SAP Lama-Dokumentation - Custom Hooks

"https://help.sap.com/doc/700f9a7e52c7497cad37f7c46023b7ff/3.0.11.0/en-US/139eca2f925e48738a20dbf0b56674c5.html"

- SAP Lama Documentation – Konfigurieren von registrierten Skripten für SAP-Host-Agent

  "https://help.sap.com/doc/700f9a7e52c7497cad37f7c46023b7ff/3.0.11.0/en-US/250dfc5eef4047a38bab466c295d3a49.html"

- SAP Lama-Dokumentation - Parameter für benutzerdefinierte Operationen und benutzerdefinierte Haken

  "https://help.sap.com/doc/700f9a7e52c7497cad37f7c46023b7ff/3.0.11.0/en-US/0148e495174943de8c1c3ee1b7c9cc65.html"

- SAP Lama-Dokumentation - Adaptive Design

  "https://help.sap.com/doc/700f9a7e52c7497cad37f7c46023b7ff/3.0.11.0/en-US/737a99e86f8743bdb8d1f6cf4b862c79.html"

- NetApp Produktdokumentation

  "https://www.netapp.com/support-and-training/documentation/"

Versionsverlauf

Version	Datum	Versionsverlauf des Dokuments
Version 1.0	Januar 2023	Erste Version

Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter

TR-4667: Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter

Im dynamischen Geschäftsumfeld von heute müssen Unternehmen kontinuierlich Innovationen liefern und schnell auf sich ändernde Märkte reagieren. Unter diesen Wettbewerbsbedingungen können sich Unternehmen, die mehr Flexibilität in ihren Arbeitsprozessen implementieren, effektiver an die Marktanforderungen anpassen.

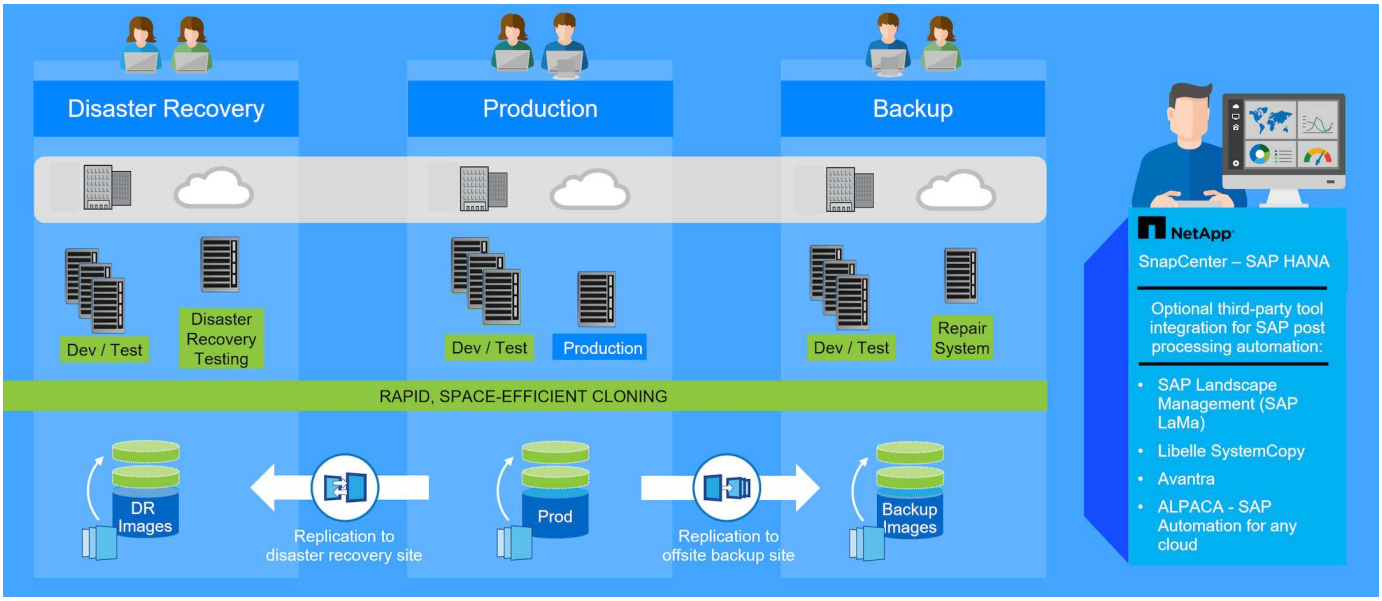
Autor: Nils Bauer, NetApp

Einführung

Wechselnde Marktanforderungen betreffen auch die SAP-Umgebungen eines Unternehmens, so dass sie regelmäßige Integrationen, Änderungen und Updates erfordern. DIE IT-Abteilungen müssen diese Veränderungen mit weniger Ressourcen und über kürzere Zeiträume hinweg umsetzen. Die Minimierung des Risikos bei der Implementierung dieser Änderungen erfordert gründliche Tests und Schulungen, für die zusätzliche SAP-Systeme mit tatsächlichen Daten aus der Produktion erforderlich sind.

Herkömmliche Ansätze für das SAP Lifecycle Management zur Bereitstellung dieser Systeme basieren in erster Linie auf manuellen Prozessen. Diese manuellen Prozesse sind oft fehleranfällig und zeitaufwendig, wodurch Innovationen und die Reaktion auf geschäftliche Anforderungen verzögert werden.

NetApp Lösungen zur Optimierung des SAP Lifecycle Managements sind in SAP HANA Datenbank- und Lifecycle-Management-Tools integriert und kombinieren effiziente applikationsintegrierte Datensicherung mit der flexiblen Bereitstellung von SAP Testsystemen, wie in der folgenden Abbildung dargestellt. Diese Lösungen sind für SAP HANA verfügbar, die lokal oder in der Cloud ausgeführt werden – On-Premises Azure NetApp Files (ANF) oder Amazon FSX for NetApp ONTAP (FSX for ONTAP).



Applikationsintegrierte Snapshot Backup-Vorgänge

Die Fähigkeit, applikationskonsistente Snapshot Backups auf Storage-Ebene zu erstellen, ist die Grundlage für die in diesem Dokument beschriebenen Systemkopien- und Systemklonvorgänge. Storage-basierte Snapshot Backups werden mit dem NetApp SnapCenter Plug-in für SAP HANA und Schnittstellen der SAP HANA Datenbank erstellt. SnapCenter registriert Snapshot-Backups im SAP HANA Backup-Katalog, sodass die Backups für Restore, Recovery und Klonvorgänge verwendet werden können.

Standortexterne Backup- und/oder Disaster Recovery-Datenreplikation

Applikationskonsistente Snapshot Backups können auf der Storage-Ebene zu einem externen Backup-Standort oder einem durch SnapCenter kontrollierten Disaster Recovery-Standort repliziert werden. Die Replizierung basiert auf geänderten und neuen Blöcken und ist damit Platz- und bandbreiteneffizient.

Beliebige Snapshot Sicherung für SAP Systemkopie- oder Klonvorgänge verwenden

Dank der NetApp Technologie und Software-Integration können Sie jedes Snapshot Backup eines Quellsystems für eine SAP-Systemkopie oder einen Klonvorgang verwenden. Dieses Snapshot Backup kann entweder aus demselben Storage ausgewählt werden, der für die SAP Produktionssysteme verwendet wird, aus dem für externe Backups verwendeten Storage oder aus dem Storage am Disaster Recovery-Standort. Dank dieser Flexibilität können Entwicklungs- und Testsysteme bei Bedarf von der Produktion getrennt werden. Außerdem werden weitere Szenarien abgedeckt, zum Beispiel Disaster Recovery-Tests am Disaster Recovery-Standort.

Das Klonen aus dem externen Backup- oder Disaster-Recovery-Storage wird für die lokalen NetApp Systeme und für Amazon FSX for NetApp ONTAP unterstützt. Mit Azure NetApp Files können Klone nur am Quell-Volume erstellt werden.

Automatisierung mit Integration

Es gibt verschiedene Szenarien und Anwendungsfälle für die Bereitstellung von SAP-Testsystemen. Dabei gibt es möglicherweise auch unterschiedliche Anforderungen an den Automatisierungsgrad. NetApp Softwareprodukte für SAP können in Datenbank- und Lifecycle-Management-Produkte von SAP integriert werden, um verschiedene Szenarien und Automatisierungsstufen zu unterstützen.

NetApp SnapCenter mit dem Plug-in für SAP HANA wird verwendet, um die erforderlichen Storage Volumes auf Basis eines applikationskonsistenten Snapshot Backups bereitzustellen und alle erforderlichen Host- und Datenbankvorgänge bis zu einer starteten SAP HANA Datenbank auszuführen. Je nach Anwendungsfall können SAP Systemkopien, Systemklone, Systemaktualisierung oder zusätzliche manuelle Schritte wie die SAP Nachbearbeitung erforderlich sein. Weitere Informationen werden im nächsten Abschnitt behandelt.

Eine vollautomatisierte End-to-End-Bereitstellung von SAP Testsystemen kann unter Verwendung von Tools anderer Anbieter und durch die Integration von NetApp Funktionen durchgeführt werden. Weitere Informationen finden Sie unter:

"TR-4953: NetApp SAP Landscape Management Integration Using Ansible"

"TR-4929: SAP-Systemkopien automatisieren mit Libelle SystemCopy (netapp.com)"

"Automatisierung von SAP System copy, Refresh, und Klonen von Workflows mit ALPACA und NetApp SnapCenter"

"Automatisierung von SAP Systemkopien Verstärkern;#44; Refresh, Klonen von Workflows mit Avantra und NetApp SnapCenter"

SAP Szenarien für Systemkopie, Aktualisierung und Klonen

Der Begriff SAP Systemkopie wird oft als Synonym für drei verschiedene Prozesse verwendet: SAP Systemaktualisierung, SAP Systemkopie oder SAP Systemklonvorgänge. Es ist wichtig, zwischen den verschiedenen Vorgängen zu unterscheiden, da sich Workflows und Anwendungsfälle für jedes einzelne unterscheiden.

- **SAP-Systemaktualisierung.** ein SAP-Systemaktualisierung ist eine Aktualisierung eines bestehenden SAP-Zielsystems mit Daten aus einem SAP-Quellsystem. Das Zielsystem ist in der Regel Teil einer SAP-Transportlandschaft, beispielsweise ein Qualitätssicherungssystem, das mit den Daten des Produktionssystems aktualisiert wird. Hostname, Instanznummer und SID unterscheiden sich für die Quell- und Zielsysteme.
- **SAP-Systemkopie.** eine SAP-Systemkopie ist ein Setup eines neuen SAP-Zielsystems mit Daten aus einem SAP-Quellsystem. Dabei könnte das neue Zielsystem beispielsweise ein zusätzliches Testsystem mit den Daten aus dem Produktionssystem sein. Hostname, Instanznummer und SID unterscheiden sich für die Quell- und Zielsysteme.
- **SAP-Systemklon.** ein SAP-Systemklon ist ein identischer Klon eines Quell-SAP-Systems. SAP Systemklone werden typischerweise zur Beseitigung logischer Beschädigungen oder zum Testen von Disaster-Recovery-Szenarien eingesetzt. Bei einem Systemklonvorgang bleiben der Hostname, die Instanznummer und die SID unverändert. Daher ist es wichtig, für das Zielsystem ein ordnungsgemäßes Netzwerkfechten einzurichten, um sicherzustellen, dass keine Kommunikation mit der Produktionsumgebung besteht.

In der Abbildung unten sind die wichtigsten Schritte aufgeführt, die während einer Systemaktualisierung, Systemkopie oder Systemklonfunktion durchgeführt werden müssen. Die blauen Felder kennzeichnen Schritte, die mit SnapCenter automatisiert werden können, während die grauen Felder die Schritte kennzeichnen, die

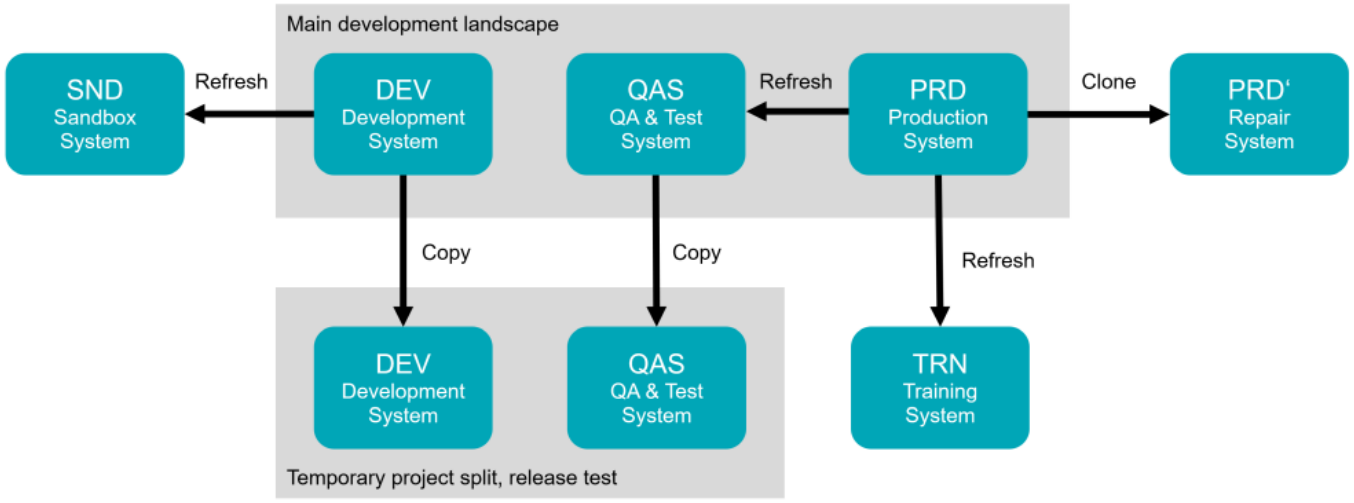
entweder manuell oder mithilfe von Tools anderer Hersteller außerhalb von SnapCenter ausgeführt werden müssen.

Anwendungsfälle für Systemaktualisierung und Klonen

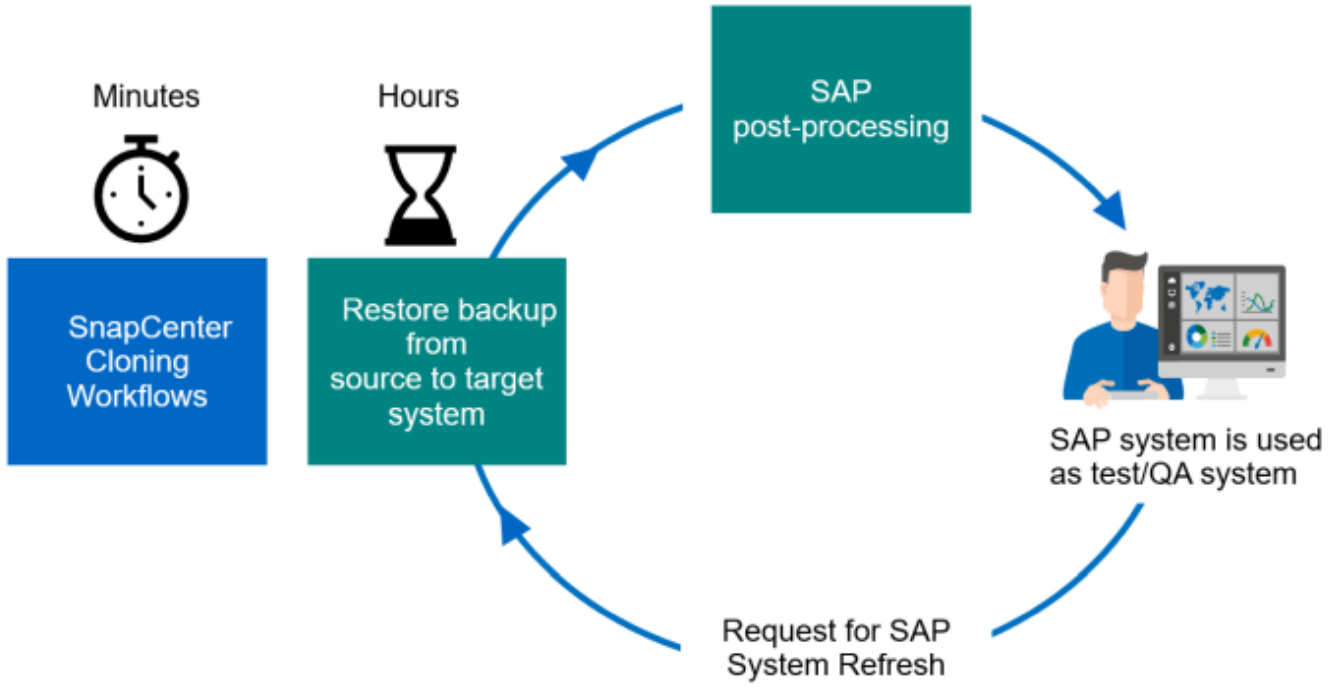
NetApp Lösungen zur Optimierung des SAP Lifecycle Managements sind in SAP HANA Datenbank- und Lifecycle Management-Tools integriert und verbinden effiziente applikationsintegrierte Datensicherung mit der flexiblen Bereitstellung von SAP Testsystemen.

Datenaktualisierung von QA-, Test-, Sandboxsystemen- und Trainingssystemen

Es gibt verschiedene Szenarien, in denen Daten aus einem Quellsystem zu Test- oder Schulungszwecken einem Zielsystem zur Verfügung gestellt werden müssen. Diese Test- und Trainingssysteme müssen regelmäßig mit Daten des Quellsystems aktualisiert werden, um sicherzustellen, dass die Test- und Schulungsmaßnahmen mit dem aktuellen Datensatz durchgeführt werden. Diese Systemaktualisierungen bestehen aus mehreren Aufgaben auf Infrastruktur-, Datenbank- und Applikationsebene und können je nach Automatisierungsgrad mehrere Tage dauern.



Mit SnapCenter Klon-Workflows können die erforderlichen Aufgaben auf der Infrastruktur- und Datenbankebene beschleunigt und automatisiert werden. Anstatt ein Backup vom Quellsystem zum Zielsystem wiederherzustellen, verwendet SnapCenter die NetApp Snapshot Kopie und die NetApp FlexClone Technologie. So können erforderliche Aufgaben bis zu einer gestarteten SAP HANA Datenbank in Minuten anstatt Stunden durchgeführt werden. Der für das Klonen erforderliche Zeitaufwand ist unabhängig von der Größe der Datenbank, sodass selbst sehr große Systeme innerhalb weniger Minuten erstellt werden können. Die Startzeit hängt nur von der Größe der Datenbank und der Verbindung zwischen dem Datenbankserver und dem Storage-System ab.



Der Workflow für Systemaktualisierungen wird im Abschnitt beschrieben "„SAP HANA-Systemaktualisierung mit SnapCenter.“"

Beseitigung logischer Beschädigungen

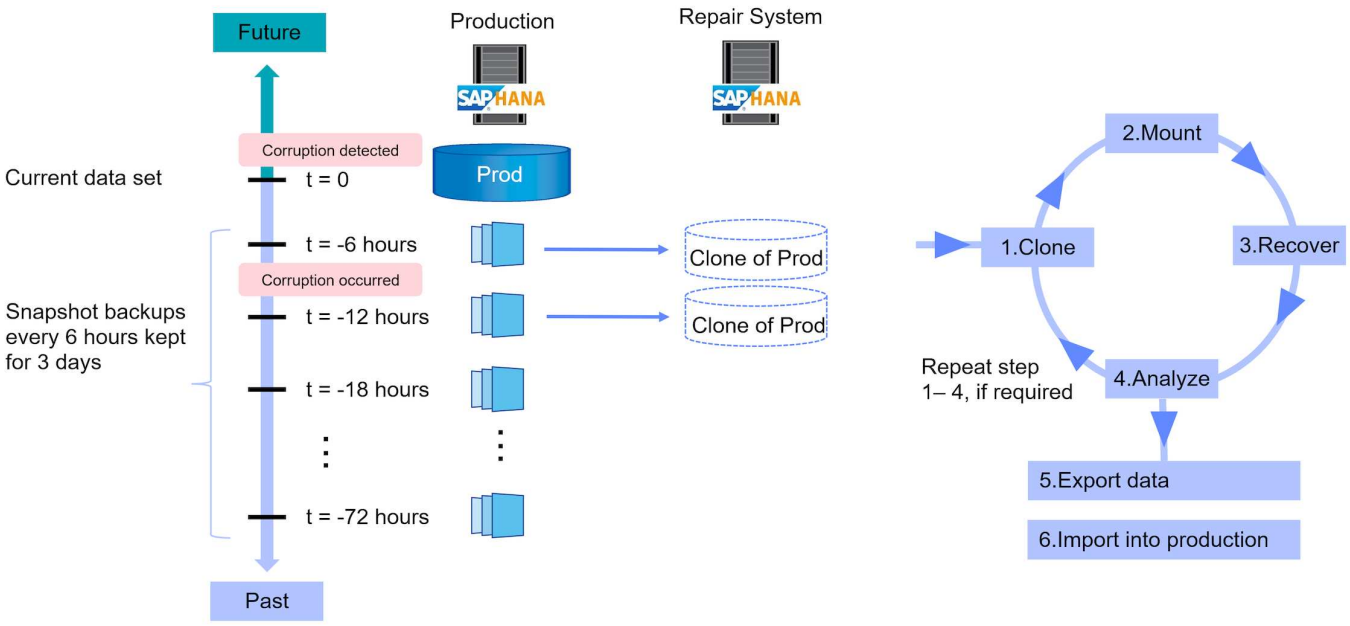
Logische Beschädigungen können durch Softwarefehler, menschliche Fehler oder Sabotage verursacht werden. Leider können logische Beschädigungen oft nicht mit standardmäßigen Hochverfügbarkeits- und Disaster Recovery-Lösungen behoben werden. Daher können abhängig von Schicht, Applikation, Filesystem oder Storage mit einer logischen Beschädigung minimale Ausfallzeiten und maximale Datenverluste nicht erfüllt werden.

Schlimmstenfalls ist die SAP-Anwendung logisch beschädigt. SAP Applikationen laufen oft in einer Landschaft, in der verschiedene Applikationen miteinander kommunizieren und Daten austauschen. Daher wird die Wiederherstellung eines SAP-Systems, bei dem eine logische Beschädigung aufgetreten ist, nicht empfohlen. Wenn Sie das System auf einen Zeitpunkt vor der Beschädigung wiederherstellen, führt dies zu Datenverlust. Außerdem würde die SAP-Landschaft nicht mehr synchron sein und eine zusätzliche Nachbearbeitung erfordern.

Anstatt das SAP-System wiederherzustellen, ist es besser, den logischen Fehler innerhalb des Systems zu beheben, indem das Problem in einem separaten Reparatursystem analysiert wird. Zur Ursachenanalyse ist die Einbindung des Geschäftsprozesses und der Applikationseigentümer erforderlich. Für dieses Szenario

erstellen Sie ein Reparatursystem (ein Klon des Produktionssystems) auf Basis der Daten, die vor dem Auftreten der logischen Beschädigung gespeichert wurden. Innerhalb des Reparatursystems können die erforderlichen Daten exportiert und in das Produktionssystem importiert werden. Bei diesem Ansatz muss das Produktionssystem nicht angehalten werden. Im besten Fall gehen keine Daten oder nur ein Bruchteil der Daten verloren.

Bei der Einrichtung des Reparatursystems sind Flexibilität und Agilität entscheidend. Bei Verwendung von Storage-basierten Snapshot Backups von NetApp sind mehrere konsistente Datenbank-Images verfügbar, um mithilfe der NetApp FlexClone Technologie einen Klon des Produktionssystems zu erstellen. Die Erstellung von FlexClone Volumes dauert nur wenige Sekunden, anstatt mehrerer Stunden, wenn zum Einrichten des Reparatursystems eine umgeleitete Wiederherstellung aus einem dateibasierten Backup verwendet wird.



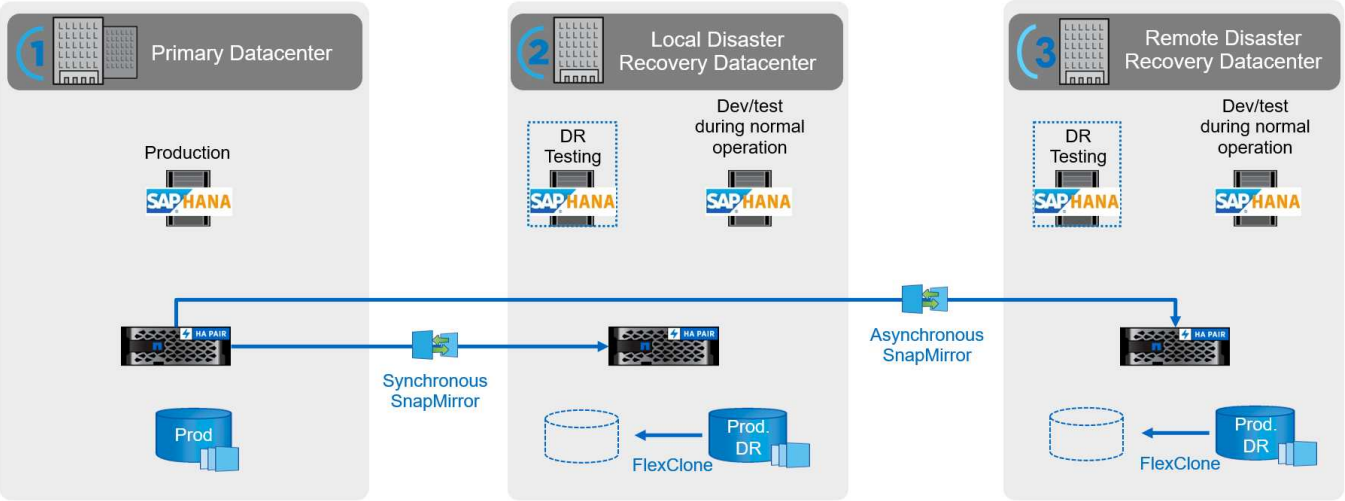
Der Arbeitsablauf der Erstellung des Reparatursystems wird im Abschnitt beschrieben "„SAP Systemklon mit SnapCenter.“"

Disaster Recovery-Tests

Für eine effiziente Disaster-Recovery-Strategie muss der erforderliche Workflow getestet werden. Die Tests zeigen, ob die Strategie funktioniert und ob die interne Dokumentation ausreichend ist. Darüber hinaus können Administratoren die erforderlichen Verfahren Schulen.

Die Storage-Replizierung mit SnapMirror ermöglicht die Ausführung von Disaster-Recovery-Tests ohne Risiko von RTO und RPO. Disaster-Recovery-Tests können ohne Unterbrechung der Datenreplizierung durchgeführt werden.

Disaster Recovery-Tests für asynchronen und synchronen SnapMirror verwenden Snapshot Backups und FlexClone Volumes am Disaster Recovery-Ziel.



Eine detaillierte Schritt-für-Schritt-Beschreibung finden Sie in den technischen Berichten

"TR-4646: SAP HANA Disaster Recovery with Storage Replication (netapp.com)"

"TR-4891: SAP HANA Disaster Recovery mit Azure NetApp Files"

Unterstützte Infrastruktur und Szenarien

Dieses Dokument behandelt Szenarien für SAP-Systemaktualisierung und -Klonen für SAP HANA-Systeme, die auf lokalen NetApp-Systemen, Amazon FSX für NetApp ONTAP-Systemen und Azure NetApp Files ausgeführt werden. Allerdings sind auf jeder Storage-Plattform nicht alle Features und Szenarien verfügbar. In der folgenden Tabelle sind die unterstützten Konfigurationen zusammengefasst.

Im Rahmen dieses Dokuments verwenden wir eine SAP HANA-Landschaft, die auf lokalen NetApp-Systemen mit NFS als Storage-Protokoll ausgeführt wird. Die meisten Workflow-Schritte sind auf den verschiedenen Plattformen identisch. Bei Unterschieden werden sie in diesem Dokument hervorgehoben.

	On-Premises NetApp Systeme	AWS FSX for NetApp ONTAP	Azure NetApp Files
Storage-Protokoll	NFS, Fibre Channel	NFS	NFS
Thin-Klon (FlexClone)	Ja.	Ja.	Nein, in der aktuellen ANF-Version wird das geklonte Volume immer aufgeteilt
Klonteilvorgang	Ja.	Ja.	K. A.
Klonen von Primär	Ja.	Ja.	Ja.
Klonen von Backups an externen Standorten	Ja.	Ja.	Nein
Klonen am DR-Standort	Ja.	Ja.	Ja, aber nicht in SnapCenter integriert

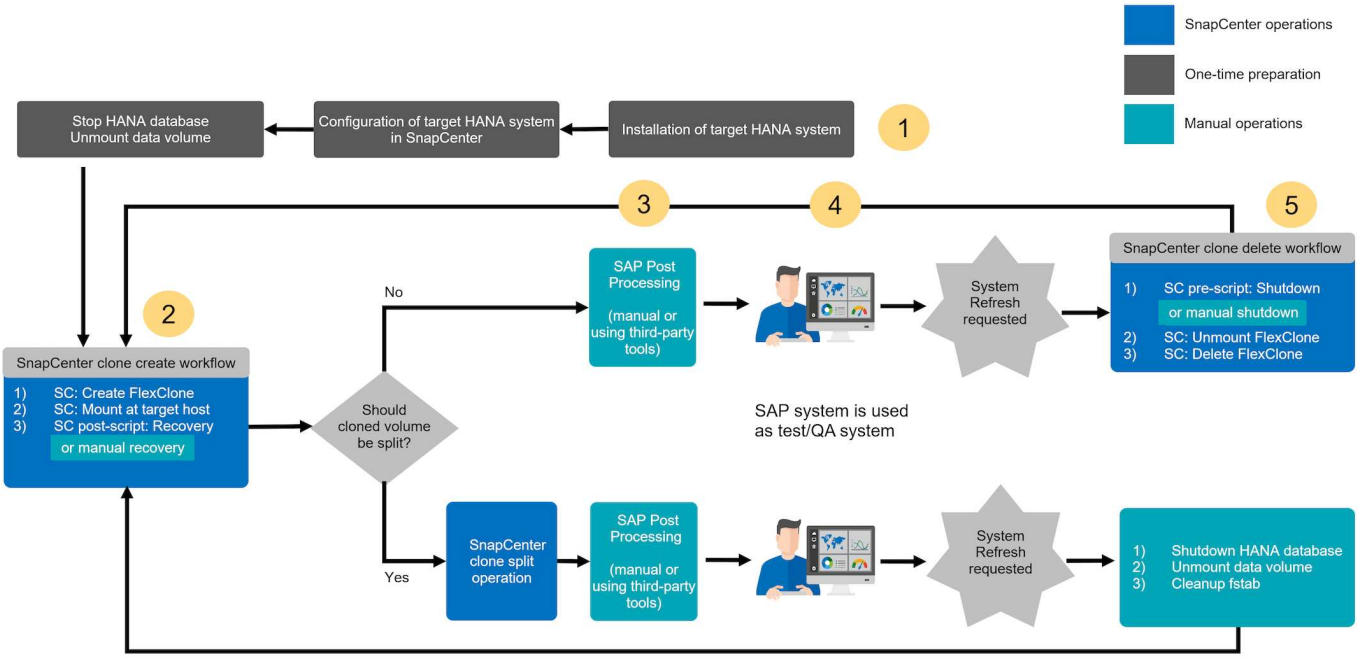
Überblick über den Workflow zur SAP Systemaktualisierung mit SnapCenter

SnapCenter stellt Workflows bereit, mit denen Sie Klone von Datensätzen von bestehenden Snapshot-Backups managen können. Mit diesem geklonten Datensatz, einem FlexClone Volume, kann ein HANA Daten-Volume schnell von einem Quellsystem bereitgestellt und an ein Zielsystem angehängt werden. Die Software eignet sich daher ideal zur Ausführung von Systemaktualisierungen für QA-, Test-, Sandbox- oder Trainingssysteme.

Die Klon-Workflows von SnapCenter bearbeiten alle erforderlichen Operationen auf der Storage-Ebene und können mithilfe von Skripten erweitert werden, um hostspezifische und HANA datenbankspezifische Vorgänge auszuführen. In diesem Dokument verwenden wir ein Skript, um die Wiederherstellung der HANA-Datenbank durchzuführen und Vorgänge beim Herunterfahren auszuführen. SnapCenter-Workflows mit weiterer Automatisierung mithilfe des Skripts bearbeiten alle erforderlichen HANA-Datenbankvorgänge, decken aber keine erforderlichen SAP-Nachbearbeitungsschritte ab. Die SAP-Nachbearbeitung muss manuell oder mit Tools von Drittanbietern durchgeführt werden.

Der Workflow für die SAP-Systemaktualisierung mit SnapCenter besteht aus fünf Hauptschritten, die in der folgenden Abbildung dargestellt sind.

1. Einmalige Erstinstallation und Vorbereitung des Zielsystems
    a. Das SnapCenter-HANA-Plugin muss auf dem neuen Zielsystem installiert und das HANA-System in SnapCenter konfiguriert sein
    b. Das Zielsystem muss angehalten und das HANA-Daten-Volume abgehängt werden
2. Der Workflow zur Erstellung von SnapCenter Klonen
    a. SnapCenter erstellt ein FlexClone Volume des ausgewählten Snapshots des Quellsystems
    b. SnapCenter bindet das FlexClone Volume im Zielsystem ein
    c. Die Recovery der Ziel-HANA-Datenbank kann mit dem Skript als Post-Skript automatisiert `sc-system-refresh` oder manuell ausgeführt werden
3. SAP-Nachbearbeitung (manuell oder mit einem Drittanbieter-Tool)
4. Das System kann nun als Test-/QS-System eingesetzt werden.
5. Bei Anforderung einer neuen Systemaktualisierung wird das FlexClone Volume mithilfe des Workflows zum Löschen von SnapCenter Klonen entfernt
    a. Wenn das HANA-Zielsystem in SnapCenter gesichert wurde, muss der Schutz vor dem Starten des Workflows zum Löschen von Klonen entfernt werden.
    b. Das HANA-System muss manuell angehalten oder automatisch mit dem Skript als SnapCenter-Pre-Script gestoppt werden `sc-system-refresh`
    c. SnapCenter entbindet das HANA-Datenvolumen
    d. SnapCenter löscht das FlexClone Volume
    e. Eine Aktualisierung wird mit Schritt 2 neu gestartet.



In den meisten Fällen werden Zieltests/QA-Systeme mindestens einige Wochen lang eingesetzt. Da das FlexClone Volume den Snapshot des Quell-System-Volume blockiert, benötigt dieser Snapshot basierend auf der Blockänderungsrate am Quell-System-Volume zusätzliche Kapazität. Bei Produktionsquellsystemen und einer durchschnittlichen Änderungsrate von 20% pro Tag wird der blockierte Snapshot nach 5 Tagen 100% erreichen. Daher empfiehlt NetApp, das FlexClone Volume entweder sofort oder nach ein paar Tagen aufzuteilen, wenn der Klon auf einem Produktions-Quellsystem basiert. Der Klon-Split-Vorgang blockiert nicht die Nutzung des geklonten Volume und kann daher jederzeit während des Betriebs der HANA-Datenbank durchgeführt werden.

Bei der Aufteilung des FlexClone Volume löscht SnapCenter alle Backups, die auf dem Zielsystem erstellt wurden.

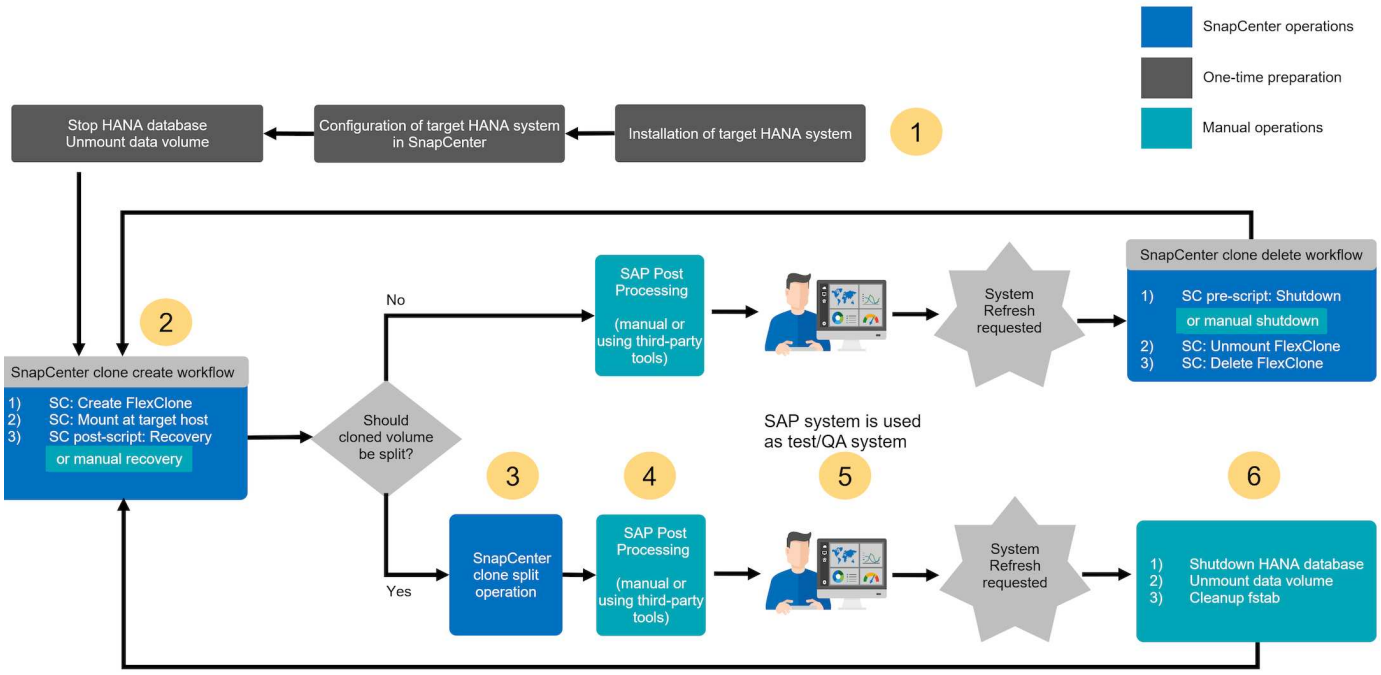
Bei SnapCenter und Azure NetApp Files ist der Klonaufteilungsvorgang nicht verfügbar, da Azure NetApp Files den Klon nach der Erstellung immer teilt.

Der Aktualisierungsvorgang einschließlich der Klonaufteilung besteht aus den folgenden Schritten.

1. Einmalige Erstinstallation und Vorbereitung des Zielsystems
   a. Das SnapCenter-HANA-Plugin muss auf dem neuen Zielsystem installiert und das HANA-System in SnapCenter konfiguriert sein
   b. Das Zielsystem muss angehalten und das HANA-Daten-Volume abgehängt werden
2. Der Workflow zur Erstellung von SnapCenter Klonen
   a. SnapCenter erstellt ein FlexClone Volume des ausgewählten Snapshots des Quellsystems
   b. SnapCenter bindet das FlexClone Volume im Zielsystem ein
   c. Die Recovery der Ziel-HANA-Datenbank kann mit dem Skript als Post-Skript automatisiert `sc-system-refresh` oder manuell ausgeführt werden
3. Das FlexClone Volume wird mithilfe des SnapCenter Klon-Split-Workflows aufgeteilt.
4. SAP-Nachbearbeitung (manuell oder mit einem Drittanbieter-Tool)

5. Das System kann nun als Test-/QS-System eingesetzt werden.
6. Wenn eine neue Systemaktualisierung angefordert wird, erfolgt die Bereinigung mit den folgenden manuellen Schritten
   a. Wenn das Ziel-HANA-System in SnapCenter geschützt wurde, muss der Schutz entfernt werden.
   b. Das HANA-System muss manuell gestoppt werden
   c. Das HANA-Datenvolumen muss abgehängt und der fstab-Eintrag aus SnapCenter entfernt werden (manuelle Aufgabe).
   d. Eine Aktualisierung wird mit Schritt 2 neu gestartet.

> Das alte Daten-Volume, das zuvor gespalten wurde, muss manuell auf dem Storage-System gelöscht werden.



Der Abschnitt "„SAP HANA Systemaktualisierung mit SnapCenter“" enthält eine detaillierte Schritt-für-Schritt-Beschreibung beider Workflows zur Systemaktualisierung.

Überblick über den SAP Systemklonen-Workflow mit SnapCenter

Wie im vorherigen Abschnitt beschrieben, kann SnapCenter Klone von Datensätzen von jedem vorhandenen Snapshot Backup managen und diese Datensätze schnell auf jedes beliebige Zielsystem bereitstellen. Die flexible und agile Bereitstellung von Produktionsdaten an ein Reparatursystem zur Behebung logischer Beschädigungen ist von entscheidender Bedeutung, da häufig das Reparatursystem zurückgesetzt und ein anderer Produktionsdatensatz ausgewählt werden muss. Die FlexClone Technologie ermöglicht einen schnellen Bereitstellungsprozess und sorgt für deutliche Kapazitätseinsparungen, da das Reparatursystem normalerweise nur für einen kurzen Zeitraum verwendet wird.

Die folgende Abbildung fasst die erforderlichen Schritte für einen SAP-Systemklonvorgang mit SnapCenter

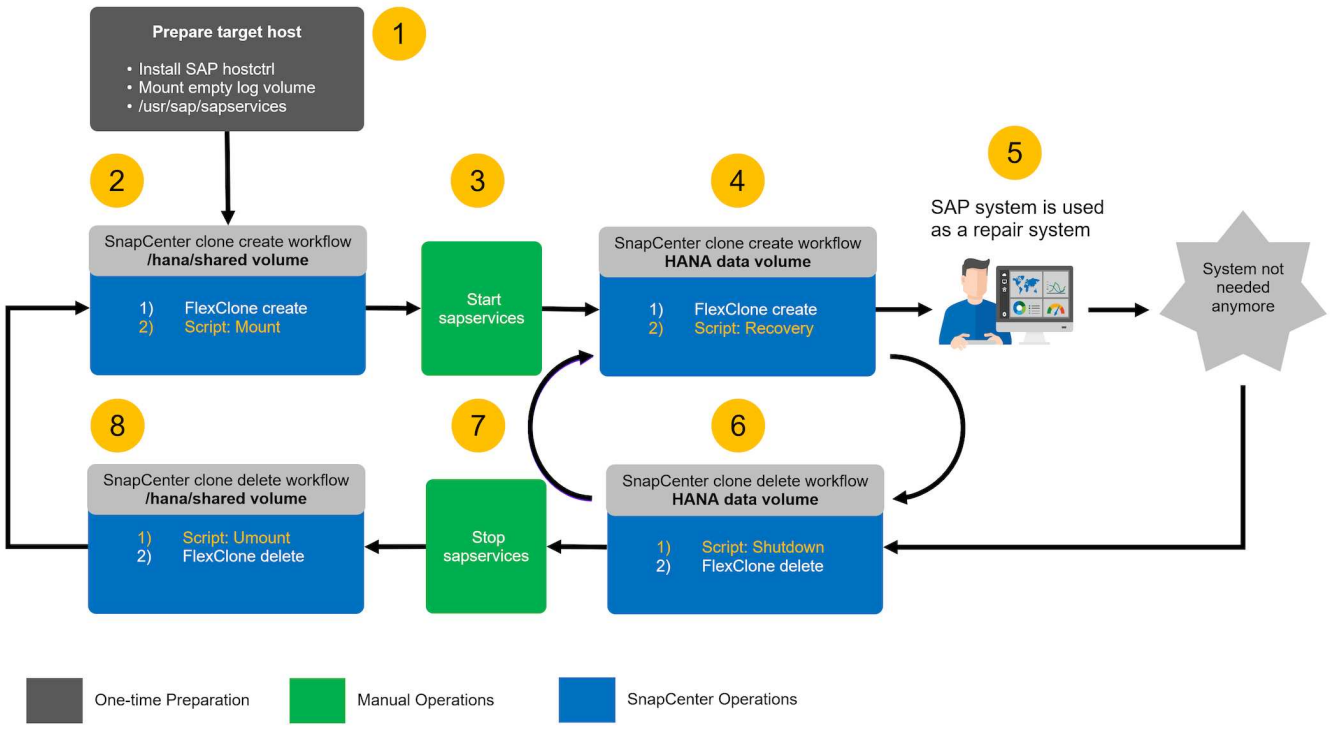
zusammen.

1. Bereiten Sie den Zielhost vor.
2. Workflow für die SAP HANA-Freigabe-Volumes durch SnapCenter-Klon erstellen
3. Starten Sie SAP HANA Services.
4. SnapCenter Clone erstellen Sie einen Workflow für das SAP HANA Daten-Volume einschließlich Datenbank-Recovery.
5. Das SAP HANA-System kann nun als Reparatursystem eingesetzt werden.

Wenn das System nicht mehr benötigt wird, erfolgt die Bereinigung mit den folgenden Schritten.

1. SnapCenter Clone delete Workflow für das SAP HANA Daten-Volume einschließlich Datenbank-Shutdown (unter Verwendung des Automatisierungsskripts).
2. Stoppen Sie SAP HANA Services.
3. SnapCenter Clone delete Workflow für das SAP HANA Shared Volume.

Wenn Sie das System auf ein anderes Snapshot Backup zurücksetzen müssen, reichen die Schritte 6 und Schritt 4 aus. Eine Aktualisierung des gemeinsam genutzten SAP HANA-Volumes ist nicht erforderlich.



Der Abschnitt "„SAP Systemklon mit SnapCenter“" enthält eine detaillierte Schritt-für-Schritt-Beschreibung des Systemklonworkflows.

Überlegungen zu Systemaktualisierungen für SAP HANA mit Storage-Snapshot-Backups

NetApp Lösungen zur Optimierung des SAP Lifecycle Managements sind in SAP HANA Datenbank- und Lifecycle Management-Tools integriert und verbinden effiziente

applikationsintegrierte Datensicherung mit der flexiblen Bereitstellung von SAP Testsystemen.

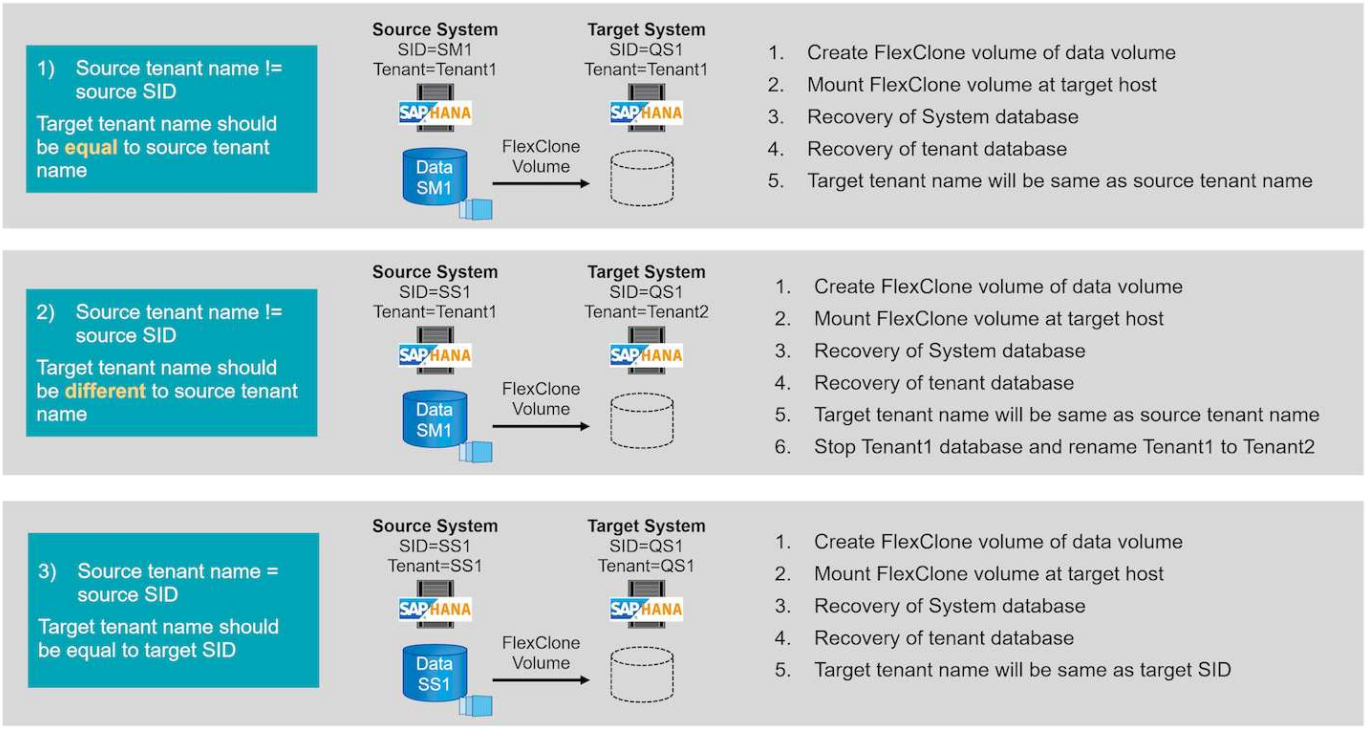
Mandantenname(n) im Zielsystem

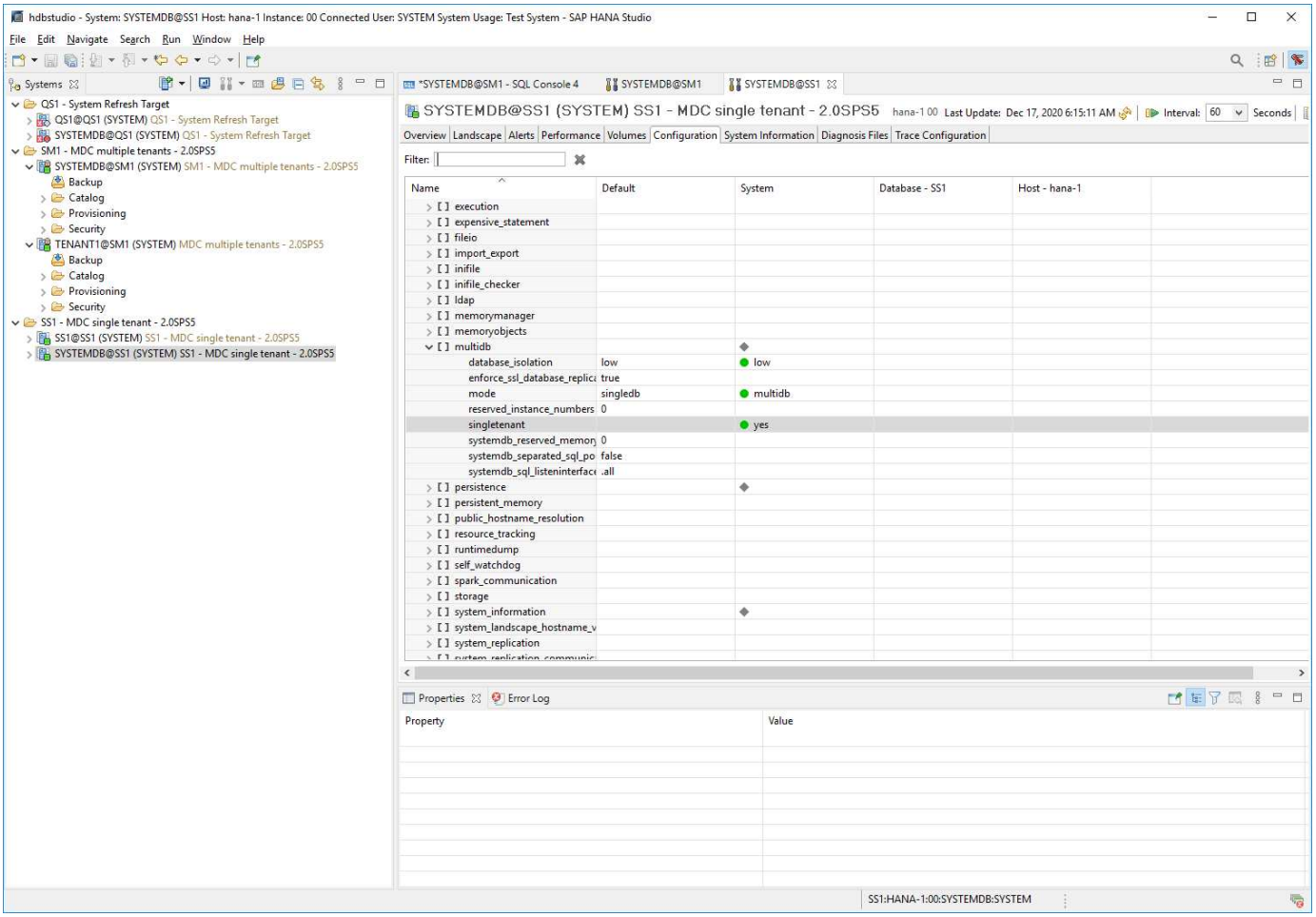
Die zur Aktualisierung des SAP HANA-Systems erforderlichen Schritte hängen von der Mandantenkonfiguration des Quellsystems und dem erforderlichen Mandantennamen auf dem Zielsystem ab, wie in der folgenden Abbildung dargestellt.

Da der Mandantenname in der Systemdatenbank konfiguriert ist, steht nach der Wiederherstellung der Systemdatenbank auch der Mandantenname des Quellsystems auf dem Zielsystem zur Verfügung. Daher kann der Mandant im Zielsystem nur mit dem gleichen Namen wie der Quellmandant wiederhergestellt werden, wie in Option 1 dargestellt. Wenn der Mandantenname im Zielsystem anders sein muss, muss er zuerst mit demselben Namen wie der Quellmandant wiederhergestellt und dann in den erforderlichen Zielmandanten-Namen umbenannt werden. Dies ist Option 2.

Eine Ausnahme von dieser Regel ist ein SAP HANA-System mit einem einzelnen Mandanten, bei dem der Mandantenname mit der System-SID identisch ist. Diese Konfiguration ist nach einer ersten SAP HANA-Installation die Standardeinstellung. Diese spezifische Konfiguration wird von der SAP HANA-Datenbank gekennzeichnet. In diesem Fall kann die Mandantenwiederherstellung am Zielsystem mit dem Mandantennamen des Zielsystems durchgeführt werden, was ebenfalls mit der System-SID des Zielsystems identisch sein muss. Dieser Workflow wird in Option 3 angezeigt.

Sobald ein Mandant im Quellsystem erstellt, umbenannt oder abgelegt wird, wird dieses Konfigurationskennzeichen von der SAP HANA-Datenbank gelöscht. Somit ist auch dann, wenn die Konfiguration an Mandant = SID zurückgebracht wurde, das Flag nicht mehr verfügbar und die Ausnahme hinsichtlich der Mandantenwiederherstellung mit Workflow 3 ist nicht mehr möglich. In diesem Fall ist Option 2 der erforderliche Workflow.





Workflow zur Systemaktualisierung mit aktivierter SAP HANA-Verschlüsselung

Wenn die Persistenz-Verschlüsselung von SAP HANA aktiviert ist, sind weitere Schritte erforderlich, bevor Sie die SAP HANA-Datenbank im Zielsystem wiederherstellen können.

Im Quellsystem müssen Sie eine Sicherung der Verschlüsselungsroot-Schlüssel für die Systemdatenbank sowie für alle Mandantendatenbanken erstellen. Die Sicherungsdateien müssen auf das Zielsystem kopiert und die Stammschlüssel müssen aus dem Backup importiert werden, bevor der Wiederherstellungsvorgang ausgeführt wird.

Siehe auch "SAP HANA Administration Guide".

Sicherung von Stammschlüsseln

Wenn Änderungen an den Stammschlüsseln vorgenommen wurden, ist immer eine Sicherung der Stammschlüssel erforderlich. Der Backup-Befehl erfordert den dbid als CLI-Parameter. Die dbid's können mit der unten stehenden SQL-Anweisung identifiziert werden.

Die SQL-Anweisung und weitere Dokumentation sind im SAP HANA Admin Guide verfügbar. Die "Sichern Sie die Stammschlüssel im SAP-Hilfeportal" folgenden Schritte zeigen die erforderlichen Operationen für ein HANA-System mit einem einzelnen Mandanten SS1 und werden im Quellsystem ausgeführt.

1. Legen Sie das Sicherungspasswort für System- und Mandantendatenbanken (SS1) fest (falls noch nicht geschehen).

```
hdbsql SYSTEMDB=> ALTER SYSTEM SET ENCRYPTION ROOT KEYS BACKUP PASSWORD
Netapp123;
0 rows affected (overall time 3658.128 msec; server time 3657.967 msec)
hdbsql SYSTEMDB=>
hdbsql SS1=> ALTER SYSTEM SET ENCRYPTION ROOT KEYS BACKUP PASSWORD
Netapp123;
0 rows affected (overall time 2424.236 msec; server time 2424.010 msec)
hdbsql SS1=>
```

1. Sicherung von Stammschlüsseln für System- und Mandantendatenbanken (SS1) erstellen.

```
ss1adm@hana-1:/usr/sap/SS1/home> /usr/sap/SS1/HDB00/exe/hdbnsutil
-backupRootKeys root-key-backup-SS1-SYSTEMDB.rkb --dbid=1 --type='ALL'
Exporting root key backup for database SYSTEMDB (DBID: 1) to
/usr/sap/SS1/home/root-key-backup-SS1-SYSTEMDB.rkb
done.
ss1adm@hana-1:/usr/sap/SS1/home> /usr/sap/SS1/HDB00/exe/hdbnsutil
-backupRootKeys root-key-backup-SS1-SS1.rkb --dbid=3 --type='ALL'
Exporting root key backup for database SS1 (DBID: 3) to
/usr/sap/SS1/home/root-key-backup-SS1-SS1.rkb
done.
```

1. Validieren von Stammschlüsselsicherungen (optional)

```
ss1adm@hana-1:/usr/sap/SS1/home> ls -al root*
-rw-r----- 1 ss1adm sapsys 1440 Apr 24 07:00 root-key-backup-SS1-SS1.rkb
-rw-r----- 1 ss1adm sapsys 1440 Apr 24 06:54 root-key-backup-SS1-
SYSTEMDB.rkb
ss1adm@hana-1:/usr/sap/SS1/home>

ss1adm@hana-1:/usr/sap/SS1/home> /usr/sap/SS1/HDB00/exe/hdbnsutil
-validateRootKeysBackup root-key-backup-SS1-SS1.rkb
Please Enter the password:
Successfully validated SSFS backup file /usr/sap/SS1/home/root-key-backup-
SS1-SS1.rkb
done.

ss1adm@hana-1:/usr/sap/SS1/home> /usr/sap/SS1/HDB00/exe/hdbnsutil
-validateRootKeysBackup root-key-backup-SS1-SYSTEMDB.rkb
Please Enter the password:
Successfully validated SSFS backup file /usr/sap/SS1/home/root-key-backup-
SS1-SYSTEMDB.rkb
done.
```

Import von Root-Schlüsseln auf dem Zielsystem

Der Import der Stammschlüssel ist zunächst für die erste Systemaktualisierung erforderlich. Wenn die Stammschlüssel im Quellsystem nicht geändert werden, ist kein zusätzlicher Import erforderlich. Der Import-Befehl erfordert den dbid als CLI-Parameter. Die dbid's können in der gleichen Weise identifiziert werden wie für die Root-Key-Backup beschrieben.

1. In unserem Setup werden die Root-Schlüssel vom Quellsystem auf eine NFS-Share kopiert

```
hana-1:~ # cp /usr/sap/SS1/home/root-key-backup-SS1-SS1.rkb /mnt/sapcc-
share/SAP-System-Refresh/
hana-1:~ # cp /usr/sap/SS1/home/root-key-backup-SS1-SYSTEMDB.rkb
/mnt/sapcc-share/SAP-System-Refresh/
```

1. Die Stammschlüssel können nun mit hdbnsutil importiert werden. Das dbid für die System- und Mandantendatenbank muss mit dem Befehl bereitgestellt werden. Das Backup-Passwort ist ebenfalls erforderlich.

```
qs1adm@hana-7:/usr/sap/QS1/HDB11> ./exe/hdbnsutil -recoverRootKeys
/mnt/sapcc-share/SAP-System-Refresh/root-key-backup-SS1-SYSTEMDB.rkb
--dbid=1 --type=ALL
Please Enter the password:
Importing root keys for DBID: 1 from /mnt/sapcc-share/SAP-System-
Refresh/root-key-backup-SS1-SYSTEMDB.rkb
Successfully imported root keys from /mnt/sapcc-share/SAP-System-
Refresh/root-key-backup-SS1-SYSTEMDB.rkb
done.

qs1adm@hana-7:/usr/sap/QS1/HDB11> ./exe/hdbnsutil -recoverRootKeys
/mnt/sapcc-share/SAP-System-Refresh/root-key-backup-SS1-SS1.rkb --dbid=3
--type=ALL Please Enter the password:
Importing root keys for DBID: 3 from /mnt/sapcc-share/SAP-System-
Refresh/root-key-backup-SS1-SS1.rkb
Successfully imported root keys from /mnt/sapcc-share/SAP-System-
Refresh/root-key-backup-SS1-SS1.rkb
done.
qs1adm@hana-7:/usr/sap/QS1/HDB11>
```

Root-Schlüssel importieren, wenn dbid nicht am Ziel vorhanden ist

Wie im vorherigen Kapitel beschrieben, ist das dbid erforderlich, um den Stammschlüssel für das System und alle Mandantendatenbanken zu importieren. Während die Systemdatenbank immer dbid=0 hat, können die Mandantendatenbanken unterschiedliche dbid's haben.

SQL Result

```
SELECT DATABASE_NAME,
  CASE WHEN (DBID = '' AND
  DATABASE_NAME = 'SYSTEMDB')
  THEN 1
  WHEN (DBID = '' AND
  DATABASE_NAME <> 'SYSTEMDB')
  THEN 3
  ELSE TO_INT(DBID)
  END DATABASE_ID
FROM (SELECT DISTINCT DATABASE_NAME, SUBSTR_AFTER (SUBPATH,'.') AS DBID FROM SYS_DATABASES.M_VOLUMES)
```

	DATABASE_NAME	DATABASE_ID
1	TENANT1	4
2	SYSTEMDB	1
3	TENANT2	3

Die obige Ausgabe zeigt zwei Mandanten mit dbid=3 und dbid=4. Wenn das Zielsystem noch keinen Mandanten mit dbid=4 gehostet hat, schlägt der Import des Stammschlüssels fehl. In diesem Fall müssen Sie zuerst die Systemdatenbank wiederherstellen und dann den Schlüssel für den Mandanten mit dbid=4 importieren.

Beispielskripte zur Automatisierung

In diesem Dokument werden zwei Skripte verwendet, um die Vorgänge zur SnapCenter-Klonerstellung und -Löschung weiter zu automatisieren.

- Das Skript `sc-system-refresh.sh` wird für die Systemaktualisierung und den Systemklonworkflow verwendet, um Recovery- und Shutdown-Vorgänge der SAP HANA-Datenbank auszuführen.
- Das Skript `sc-mount-volume.sh` wird für den Systemklonworkflow verwendet, um Mount- und Unmounting-Vorgänge für das gemeinsam genutzte SAP HANA-Volume auszuführen.

> Die Beispielskripte werden wie IS bereitgestellt und von NetApp nicht unterstützt. Die Skripte können Sie per E-Mail an ng-sapcc@netapp.com anfordern.

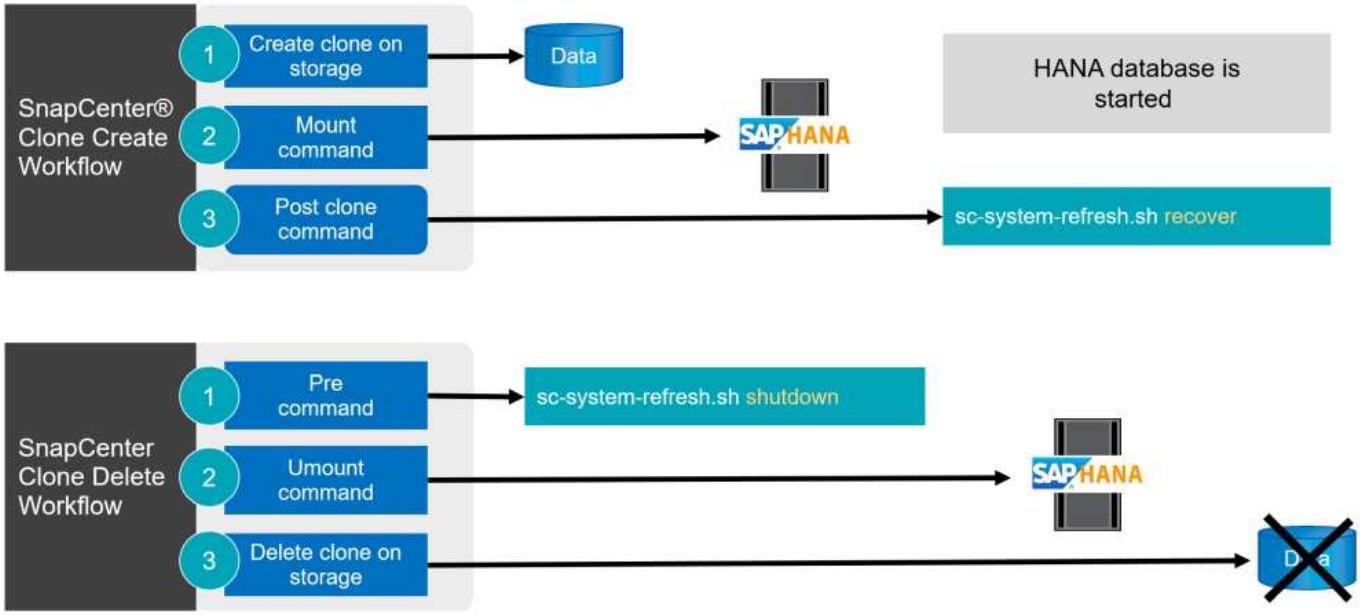
Skript sc-system-refresh.sh

Das Beispielskript `sc-system-refresh.sh` wird verwendet, um Recovery- und Shutdown-Vorgänge auszuführen. Das Skript wird mit spezifischen Befehlszeilenoptionen innerhalb der SnapCenter-Workflows zum Erstellen und Löschen von Klonen aufgerufen, wie in der Abbildung unten dargestellt.

Das Skript ist generisch und liest alle erforderlichen Parameter, wie die SID vom Zielsystem. Das Skript muss auf dem Zielhost des Systemaktualisierungsvorgangs verfügbar sein. Ein hdb-Benutzerspeicherschlüssel muss für die Benutzer-<SID>-Konfiguration m auf dem Zielsystem konfiguriert werden. Der Schlüssel muss den Zugriff auf die SAP HANA-Systemdatenbank ermöglichen und Berechtigungen für Wiederherstellungsvorgänge bereitstellen. Der Schlüssel muss den Namen <TARGET-SID>-Ausmuster Y haben.

Das Skript schreibt eine Protokolldatei `sc-system-refresh-SID.log`, in das gleiche Verzeichnis, wo es ausgeführt wird.

> Die aktuelle Version des Skripts unterstützt MDC-Konfigurationen für einzelne Hostsysteme oder MDC für mehrere Mandanten. SAP HANA wird nicht mit Systemen mit mehreren Hosts unterstützt.



Unterstützte Mandanten-Recovery-Vorgänge

Wie im Abschnitt „SAP HANA System Refresh Operation Workflows using Storage Snapshot“ beschrieben, hängen die möglichen Mandanten-Recovery-Operationen am Zielsystem von der Mandantenkonfiguration des

Quellsystems ab. Das Skript `sc-system-refresh.sh` unterstützt alle Wiederherstellungsvorgänge für Mandanten, die je nach Konfiguration des Quellsystems möglich sind, wie in der Tabelle unten gezeigt.

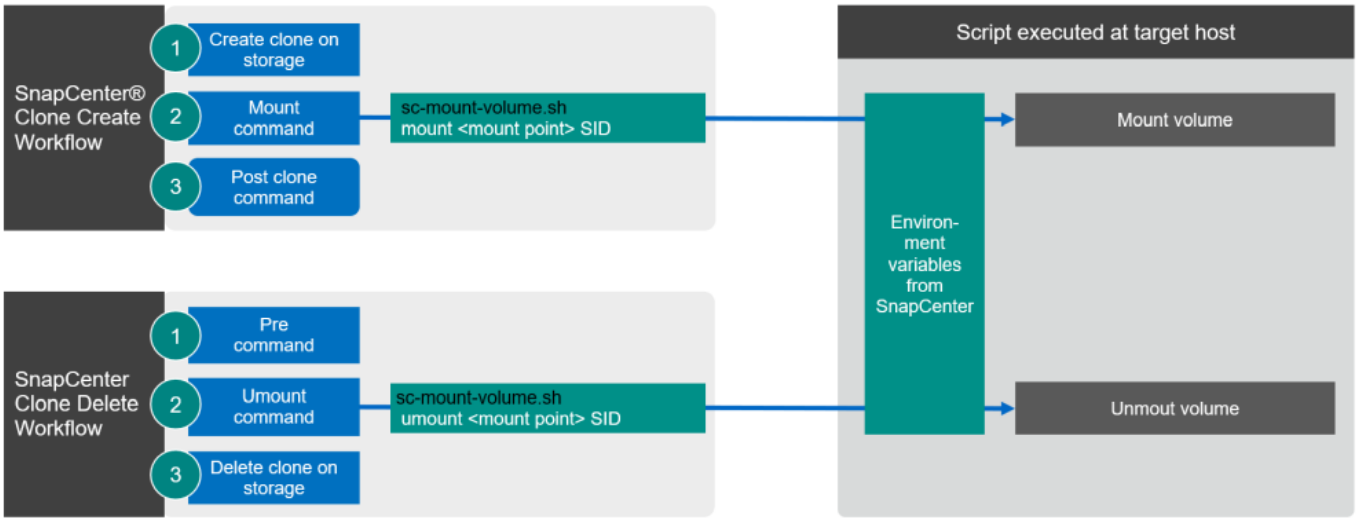
Wenn auf dem Zielsystem ein anderer Mandantenname benötigt wird, muss der Mandant nach dem Recovery-Vorgang manuell umbenannt werden.

SAP HANA-System	Mandantenkonfiguration + am Quellsystem	Resultierende Mandantenkonfiguration + am Zielsystem
MDC-Einzelmandant	Quell-Mandantenname entspricht der Quell-SID	Der Zielmandant-Name entspricht der Ziel-SID
MDC-Einzelmandant	Der Name des Quell-Mandanten entspricht nicht dem Quell-SID	Der Zielmandant-Name entspricht dem Quell-Mandantennamen
MDC mehrere Mandanten	Alle Mandantennamen	Alle Mandanten werden wiederhergestellt und haben denselben Namen wie die Quell-Mandanten.

Skript sc-mount-volume.sh

Das Beispielskript `sc-mount-volume.sh` wird zum Ausführen von Mount und Unmounten für ein beliebiges Volume verwendet. Das Skript wird verwendet, um das gemeinsam genutzte SAP HANA-Volume bei der Klonoperation des SAP HANA-Systems zu mounten. Das Skript wird mit spezifischen Befehlszeilenoptionen innerhalb der SnapCenter-Workflows zum Erstellen und Löschen von Klonen aufgerufen, wie in der Abbildung unten dargestellt.

Das Skript unterstützt SAP HANA-Systeme mit NFS als Storage-Protokoll.



SnapCenter-Umgebungsvariablen

SnapCenter bietet einen Satz von Umgebungsvariablen, die innerhalb des Skripts verfügbar sind, die auf dem Ziel-Host ausgeführt werden. Das Skript verwendet diese Variablen, um die entsprechenden Konfigurationseinstellungen zu bestimmen.

- Die Skriptvariablen `STORAGE, JUNCTION_PATH` werden für den Mount-Vorgang verwendet.
- Abgeleitet von `CLONED_VOLUMES_MOUNT_PATH` Umgebungsvariable:
- `CLONED_VOLUMES_MOUNT_PATH=${STORAGE}:/${JUNCTION_PATH}`
- Beispiel:
  `CLONED_VOLUMES_MOUNT_PATH=192.168.175.117:/SS1_shared_Clone_05112206115489411`

Skript zum Abrufen von SnapCenter Umgebungsvariablen

Wenn keine Automatisierungsskripts verwendet werden und die Schritte manuell ausgeführt werden sollten, müssen Sie den Verbindungspfad des FlexClone Volume zum Storage-System kennen. Der Verbindungspfad ist in SnapCenter nicht sichtbar. Sie müssen also entweder den Verbindungspfad direkt am Storage-System nachschlagen oder ein einfaches Skript verwenden, das die SnapCenter Umgebungsvariablen auf dem Ziel-Host bereitstellt. Dieses Skript muss als Mount-Operation-Skript innerhalb der SnapCenter Clone Erstellungsvorgang hinzugefügt werden.

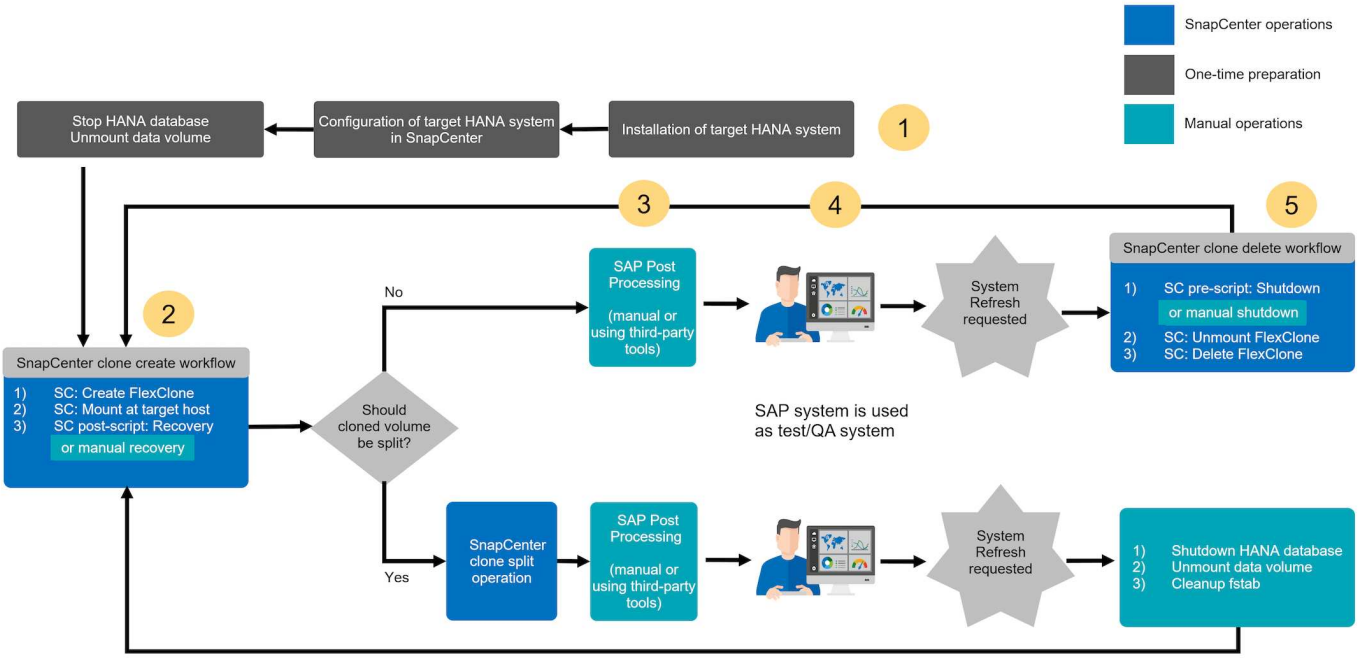
```
ss1adm@hana-1:/mnt/sapcc-share/SAP-System-Refresh> cat get-env.sh
#!/bin/bash
env > /tmp/env-from-sc.txt
ss1adm@hana-1:/mnt/sapcc-share/SAP-System-Refresh>
```

Innerhalb des `env-from-sc.txt` Datei, suchen Sie nach der Variable `CLONED_VOLUMES_MOUNT_PATH` Um die IP-Adresse des Storage-Systems und den Verbindungspfad des FlexClone Volume zu erhalten.

Beispiel:
`CLONED_VOLUMES_MOUNT_PATH=192.168.175.117:/SS1_data_mnt00001_Clone_05112206115489411`

Systemaktualisierung für SAP HANA mit SnapCenter

Im folgenden Abschnitt finden Sie eine Schritt-für-Schritt-Beschreibung der verschiedenen Optionen für die Systemaktualisierung einer SAP HANA-Datenbank.



Je nach Konfiguration der SAP HANA-Datenbank werden weitere Schritte ausgeführt bzw. müssen vorbereitet werden. Die folgende Tabelle bietet eine Zusammenfassung.

Quellsystem	Konfiguration des Quellsystems	SnapCenter- und SAP HANA-Betrieb
MDC Einzelmandant + SID = Mandantenname	Standardkonfiguration	SnapCenter-Klonvorgang und optionale Ausführung von Wiederherstellungsskripten.
	SAP HANA-Verschlüsselung mit Persistenz	Zunächst oder wenn die Stammschlüssel im Quellsystem geändert wurden, müssen die Stammschlüsselsicherungen auf dem Zielsystem importiert werden, bevor die Wiederherstellung ausgeführt werden kann.
	Quelle für die SAP HANA-Systemreplizierung	Weitere Schritte sind nicht erforderlich. Wenn für das Zielsystem kein HSR konfiguriert ist, bleibt es ein eigenständiges System.
	SAP HANA mehrere Partitionen	Keine zusätzlichen Schritte erforderlich, aber Mount-Punkte für SAP HANA-Volume-Partitionen müssen auf dem Zielsystem mit derselben Namenskonvention verfügbar sein (nur SID ist unterschiedlich).

Quellsystem	Konfiguration des Quellsystems	SnapCenter- und SAP HANA-Betrieb
MDC mehrere Mandanten Oder MDC Einzelmandant + mit SID <> Mandantenname	Standardkonfiguration	SnapCenter-Klonvorgang und optionale Ausführung von Wiederherstellungsskripten. Skript stellt alle Mandanten wieder her. Wenn bei den Zielsystemnamen keine Mandanten- oder Mandantennamen vorhanden sind, werden erforderliche Verzeichnisse automatisch während der SAP HANA-Wiederherstellung erstellt. Die Mandantennamen entsprechen der Quelle und müssen bei Bedarf nach der Wiederherstellung umbenannt werden.
	SAP HANA-Verschlüsselung mit Persistenz	Wenn zuvor auf dem Zielsystem keine DBID des Quellsystems vorhanden ist, muss die Systemdatenbank zuerst wiederhergestellt werden, bevor die Stammschlüsselsicherung dieses Mandanten importiert werden kann.
	Quelle für HANA-Systemreplizierung	Weitere Schritte sind nicht erforderlich. Wenn für das Zielsystem kein HSR konfiguriert ist, bleibt es ein eigenständiges System.
	HANA mit mehreren Partitionen	Keine zusätzlichen Schritte erforderlich, aber Mount-Punkte für SAP HANA-Volume-Partitionen müssen auf dem Zielsystem mit derselben Namenskonvention verfügbar sein (nur SID ist unterschiedlich).

In diesem Abschnitt werden die folgenden Szenarien behandelt.

- SAP HANA Systemaktualisierung ohne Trennung von Klonen
- Wird aus dem primären Storage geklont, wobei der Mandantenname der SID entspricht
- Klonen aus standortexternen Backup-Storage
- Klonen aus dem Primärspeicher mit mehreren Mandanten
- Klonvorgang
- SAP HANA Systemaktualisierung mit einem Klonabteilvorgang
- Wird aus dem primären Storage geklont, wobei der Mandantenname der SID entspricht
- Klonteilvorgang

Voraussetzungen und Einschränkungen

Die in den folgenden Abschnitten beschriebenen Workflows weisen einige Voraussetzungen und Einschränkungen hinsichtlich der SAP HANA-Systemarchitektur und der SnapCenter-Konfiguration auf.

- Die beschriebenen Workflows gelten nur für die SnapCenter Version 5.0 oder höher.
- Die beschriebenen Workflows gelten für SAP HANA MDC-Systeme mit einzelnen Hosts und mehreren Mandanten. SAP HANA Multiple Host-Systeme sind nicht abgedeckt.
- Das SnapCenter SAP HANA Plug-in muss auf dem Ziel-Host implementiert werden, um die automatische

Erkennung von SnapCenter und die Ausführung von Automatisierungsskripts zu ermöglichen.

- Die Workflows gelten für SAP HANA-Systeme mit NFS oder FCP auf physischen Hosts oder für virtuelle Hosts, die in-Guest-NFS-Mounts verwenden.

Laboreinrichtung

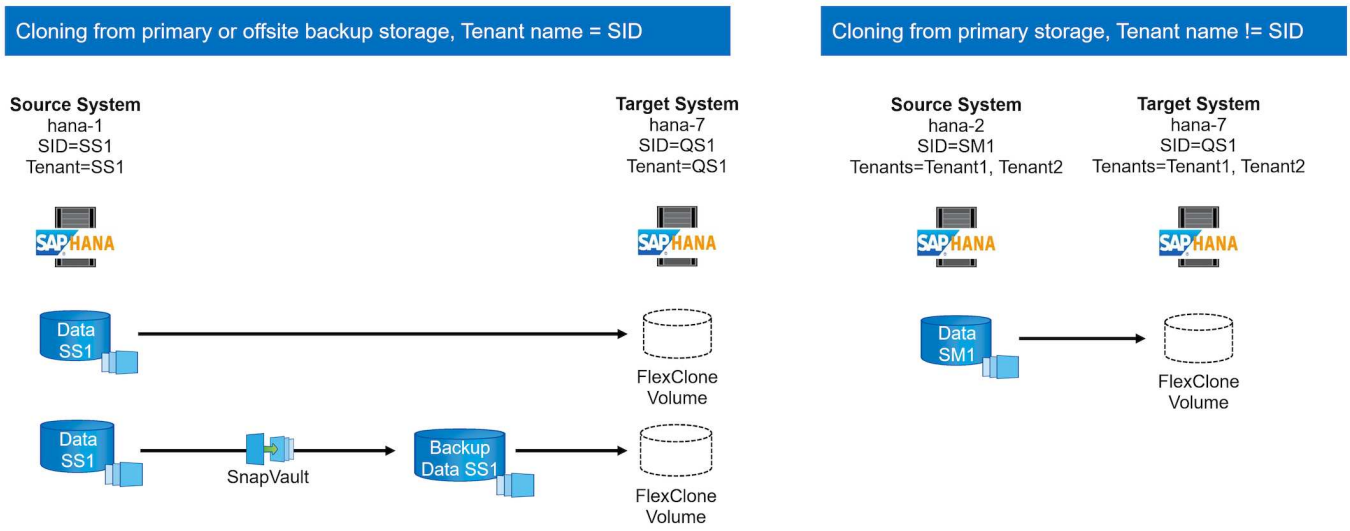
Die Abbildung unten zeigt das Lab-Setup, das für die verschiedenen Optionen zur Systemaktualisierung verwendet wurde.

- Klonen aus dem primären Storage oder externen Backup-Storage. Der Mandantenname entspricht der SID.
  - Quelle SAP HANA System: SS1 mit Mandant SS1
  - Ziel SAP HANA-System: QS1 mit Mandant QS1
- Klonen aus dem primären Storage, mehrere Mandanten.
  - Quell-SAP HANA-System: SM1 mit Tenant1 und Tenant2
  - SAP HANA-Zielsystem: QS1 mit Tenant1 und Tenant2

Es wurden folgende Softwareversionen verwendet:

- SnapCenter 5.0
- SAP HANA Systeme: HANA 2.0 SPS7 Rev. 73
- SLES 15
- ONTAP 9.14P1

Alle SAP HANA-Systeme müssen auf Basis des Konfigurationsleitfadens konfiguriert werden"SAP HANA auf NetApp AFF Systemen mit NFS". SnapCenter und die SAP HANA-Ressourcen wurden basierend auf dem Best Practice Guide konfiguriert"Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter".



Erste, einmalige Vorbereitungsschritte

In einem ersten Schritt muss das SAP HANA Zielsystem innerhalb von SnapCenter konfiguriert sein.

1. Installation des SAP HANA-Zielsystems

2. Konfiguration des SAP HANA-Systems in SnapCenter wie in beschrieben "TR-4614: SAP HANA Backup and Recovery with SnapCenter"
    a. Konfiguration des SAP HANA Datenbankbenutzers für SnapCenter-Backup-Vorgänge dieser Benutzer muss am Quell- und Zielsystem identisch sein.
    b. Konfiguration des Schlüssels hdbuserstore für die <sid>-Lösung m mit obigem Backup-Benutzer. Wenn das Automatisierungsskript für die Wiederherstellung verwendet wird, muss der Schlüsselname <SID>-Ausschreiben Y sein
    c. Implementierung des SnapCenter SAP HANA Plug-ins auf dem Ziel-Host. Das SAP HANA-System wird von SnapCenter automatisch erkannt.
    d. Konfiguration des SAP HANA-Ressourcenschutzes (optional)

Der erste SAP-Systemaktualisierungsvorgang nach der Erstinstallation wird mit den folgenden Schritten vorbereitet:

1. Herunterfahren des Ziel-SAP HANA-Systems
2. SAP HANA-Datenvolumen unmounten.

Sie müssen die Skripte, die auf dem Zielsystem ausgeführt werden sollen, der Konfigurationsdatei „SnapCenter allowed commands“ hinzufügen.

```
hana-7:/opt/NetApp/snapcenter/scc/etc # cat
/opt/NetApp/snapcenter/scc/etc/allowed_commands.config
command: mount
command: umount
command: /mnt/sapcc-share/SAP-System-Refresh/sc-system-refresh.sh
hana-7:/opt/NetApp/snapcenter/scc/etc #
```

Klonen vom primären Storage mit dem Mandantennamen SID

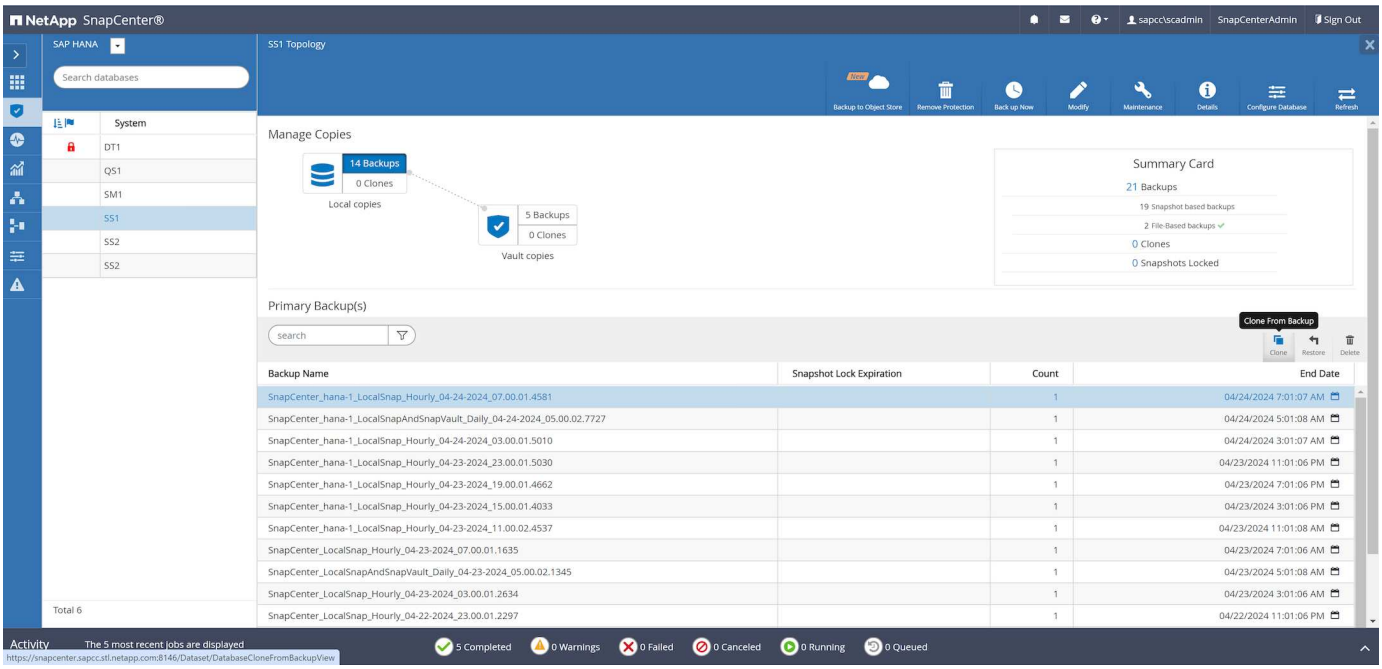
In diesem Abschnitt wird der Workflow zur Systemaktualisierung von SAP HANA beschrieben, bei dem der Mandantenname am Quell- und Zielsystem mit der SID identisch ist. Das Klonen des Storage wird im Primärspeicher durchgeführt und die Recovery wird mit dem Skript automatisiert `sc-system-refresh.sh`.

Der Workflow besteht aus den folgenden Schritten:

1. Wenn die SAP HANA-Persistenz-Verschlüsselung im Quellsystem aktiviert ist, müssen die Verschlüsselungsroot-Schlüssel einmal importiert werden. Ein Import ist auch erforderlich, wenn die Schlüssel im Quellsystem geändert wurden. Siehe Kapitel "„Considerations for SAP HANA System Refresh Operations using Storage Snapshot Backups“"
2. Wurde das SAP HANA-Zielsystem in SnapCenter geschützt, so muss zunächst der Schutz entfernt werden.
3. Workflow zur Erstellung von SnapCenter Klonen
   a. Wählen Sie Snapshot Backup aus dem SAP HANA-Quellsystem SS1 aus.
   b. Wählen Sie den Zielhost aus, und stellen Sie die Speichernetzwerk-Schnittstelle des Zielhosts bereit.
   c. Geben Sie SID des Zielsystems, in unserem Beispiel QS1
   d. Stellen Sie optional ein Skript für die Wiederherstellung als Post-Clone-Vorgang bereit.
4. Klonvorgang für SnapCenter:
   a. Erstellt ein FlexClone Volume basierend auf ausgewähltem Snapshot Backup des SAP HANA Quellsystems.
   b. Exportiert das FlexClone Volume zur Ziel-Host-Storage-Netzwerkschnittstelle oder Initiatorgruppe.
   c. Mount-Vorgang wird von FlexClone Volume auf dem Ziel-Host gemountet.
   d. Führt ein Wiederherstellungsskript für Vorgänge nach dem Klonen aus, falls zuvor konfiguriert. Andernfalls muss das Recovery manuell durchgeführt werden, wenn der SnapCenter Workflow abgeschlossen ist.
      - Recovery der Systemdatenbank
      - Wiederherstellung der Mandantendatenbank mit Mandantenname = QS1.
5. Optional können Sie die SAP HANA-Zielressource in SnapCenter schützen.

Die folgenden Screenshots zeigen die erforderlichen Schritte.

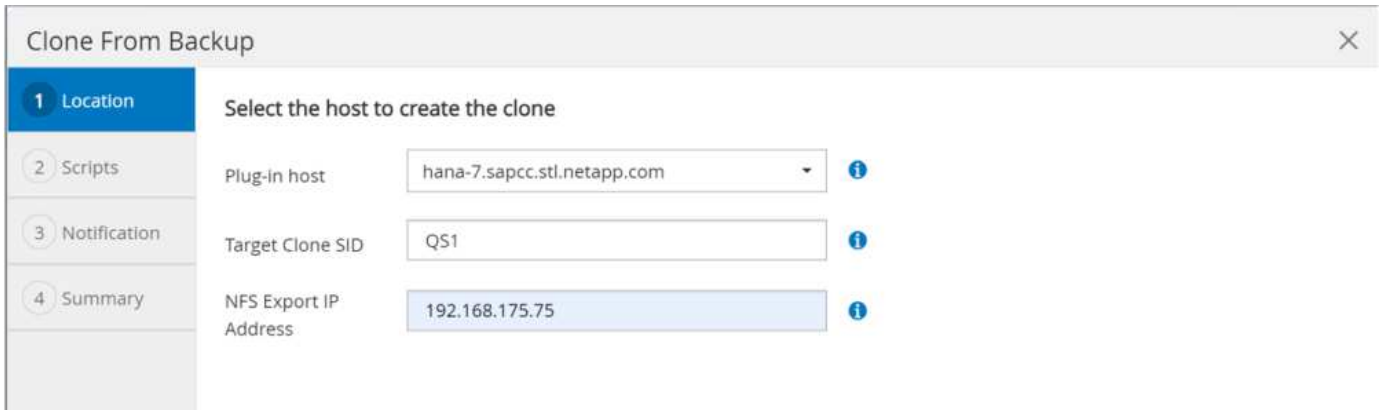
1. Wählen Sie eine Snapshot-Sicherung aus dem Quellsystem SS1 aus, und klicken Sie auf Klonen.



1. Wählen Sie den Host aus, auf dem das Zielsystem QS1 installiert ist. QS1 als Ziel-SID eingeben. Die NFS-Export-IP-Adresse muss die Speichernetzwerk-Schnittstelle des Ziel-Hosts sein.

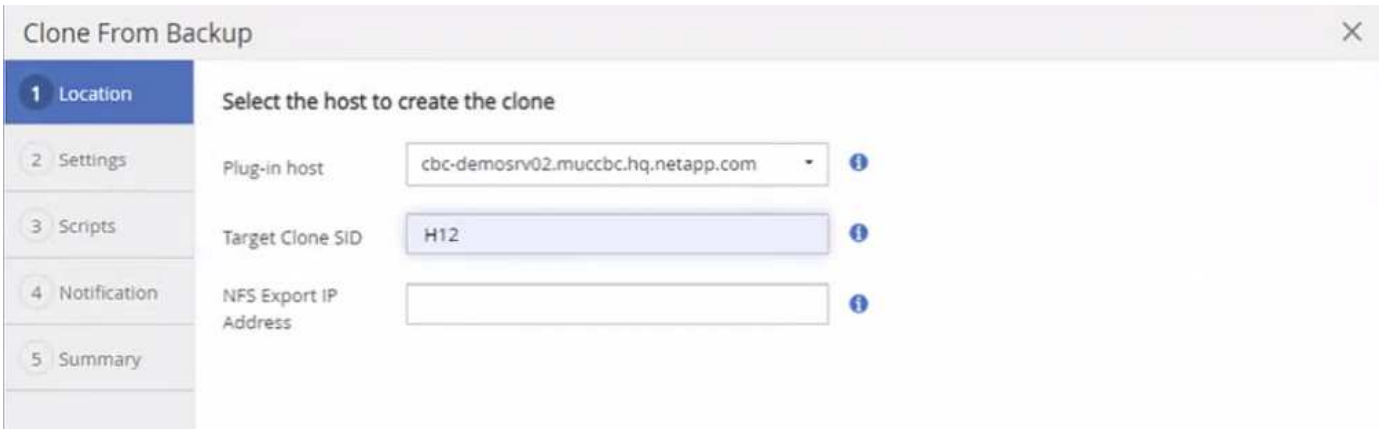
Die eingegebene Ziel-SID steuert, wie SnapCenter die geklonte Ressource verwaltet. Wenn eine Ressource mit der Ziel-SID bereits in SnapCenter konfiguriert ist und mit dem Plug-in-Host übereinstimmt, weist SnapCenter dieser Ressource einfach den Klon zu. Wenn die SID nicht auf dem Ziel-Host konfiguriert ist, erstellt SnapCenter eine neue Ressource.

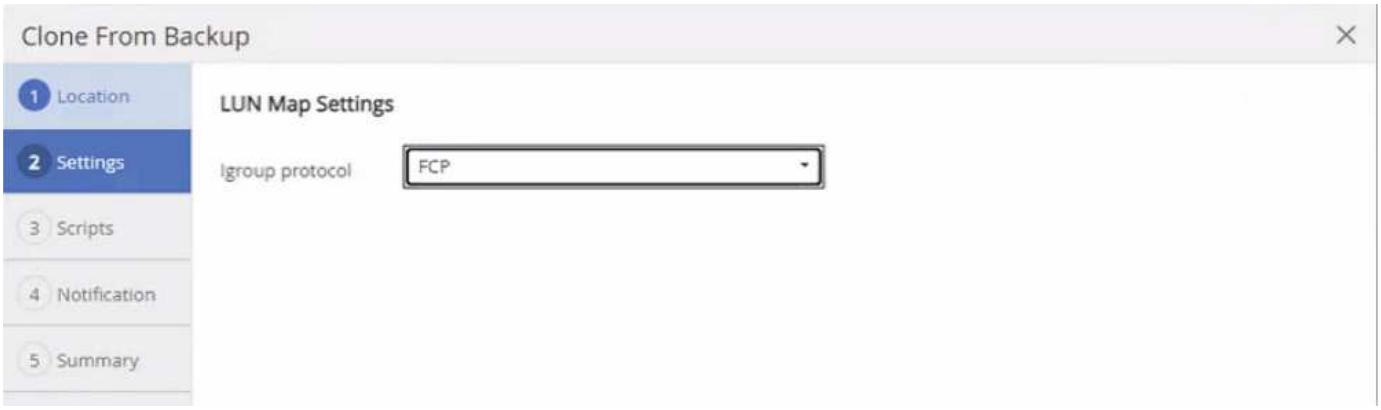
Es ist wichtig, dass die Zielsystemressource und der Host vor dem Starten des Klon-Workflows in SnapCenter konfiguriert wurden. Andernfalls unterstützt die neue von SnapCenter erstellte Ressource keine automatische Erkennung, und die beschriebenen Workflows funktionieren nicht.



Bei einer Fibre-Channel-SAN-Einrichtung ist keine Export-IP-Adresse erforderlich, Sie müssen jedoch im nächsten Bildschirm das verwendete Protokoll angeben.

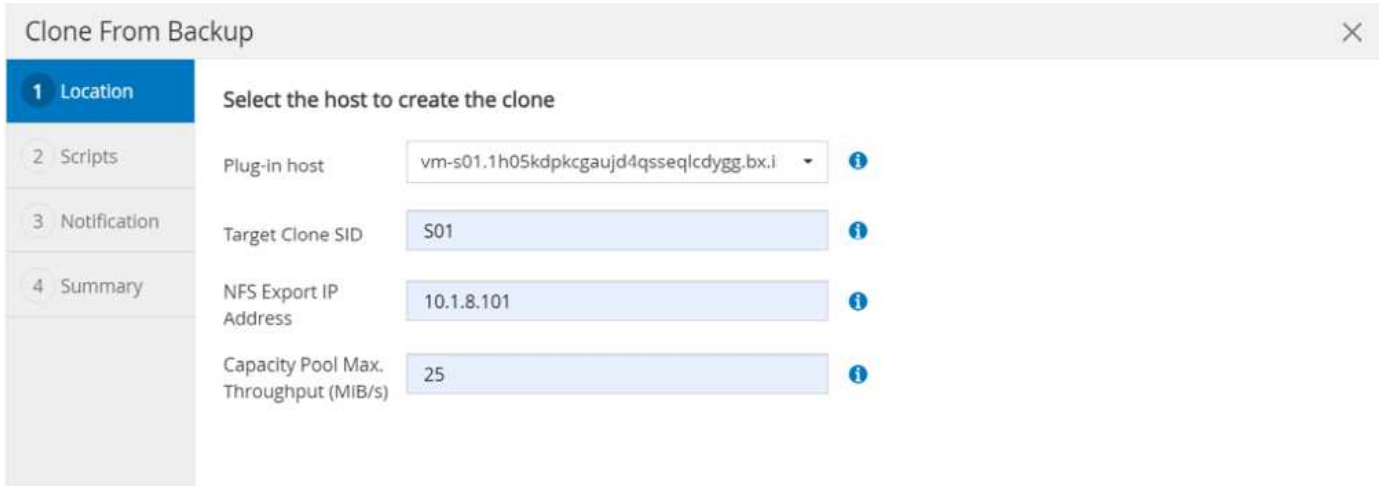
Die Screenshots zeigen ein anderes Lab-Setup mit einer FibreChannel-Konnektivität.



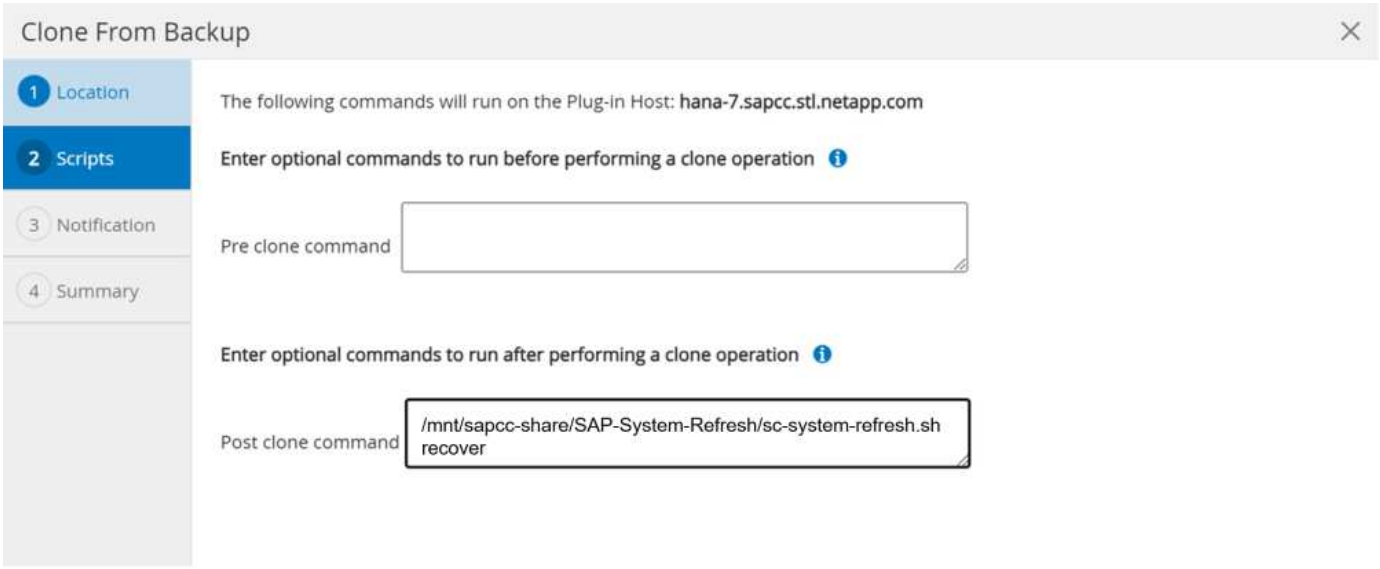


Mit Azure NetApp Files und einem manuellen QoS-Kapazitäts-Pool müssen Sie den maximalen Durchsatz für das neue Volume erzielen. Stellen Sie sicher, dass der Kapazitäts-Pool über genügend Reserven verfügt, sonst schlägt der Klon-Workflow fehl.

Die Screenshots zeigen ein anderes Lab Setup, das in Microsoft Azure mit Azure NetApp Files läuft.



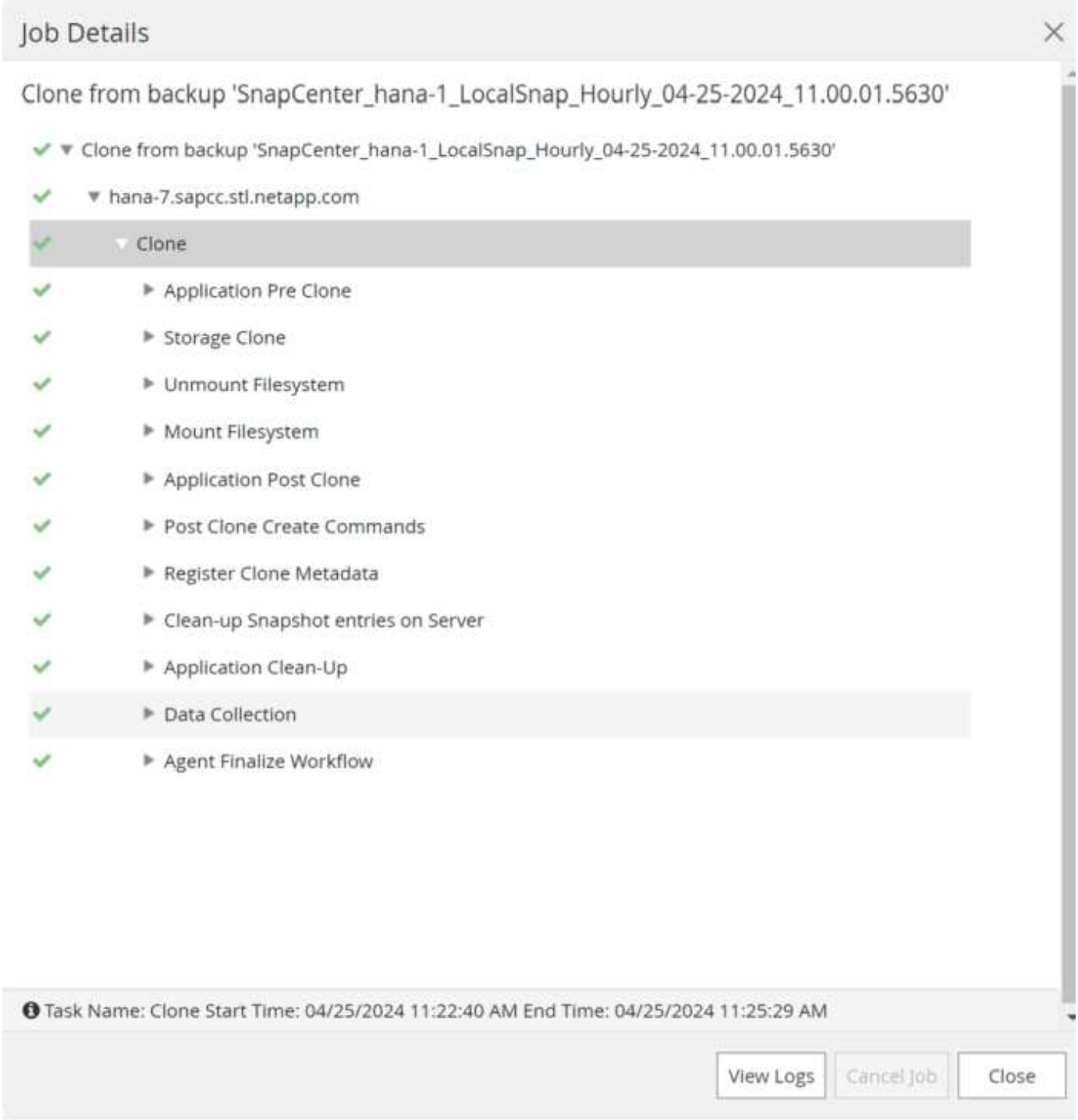
1. Geben Sie die optionalen Post-Clone-Skripte mit den erforderlichen Befehlszeilenoptionen ein. In unserem Beispiel verwenden wir ein Post-Clone-Skript, um die SAP HANA Datenbank-Recovery auszuführen.



Wie bereits besprochen, ist die Verwendung des Wiederherstellungsskripts optional. Die Wiederherstellung kann auch manuell durchgeführt werden, nachdem der SnapCenter Klon-Workflow abgeschlossen ist.

Das Skript für den Wiederherstellungsvorgang stellt die SAP HANA-Datenbank mithilfe des Vorgangs „Clear Logs“ auf den Zeitpunkt des Snapshots wieder her und führt keine Forward Recovery aus. Wenn eine Rückführung auf einen bestimmten Zeitpunkt erforderlich ist, muss die Wiederherstellung manuell durchgeführt werden. Eine manuelle vorwärts-Wiederherstellung erfordert außerdem, dass die Protokoll-Backups aus dem Quellsystem auf dem Ziel-Host verfügbar sind.

1. Im Bildschirm Jobdetails in SnapCenter wird der Fortschritt des Vorgangs angezeigt. Die Job-Details zeigen außerdem, dass die Gesamtlaufzeit einschließlich Datenbank-Recovery weniger als 3 Minuten beträgt.

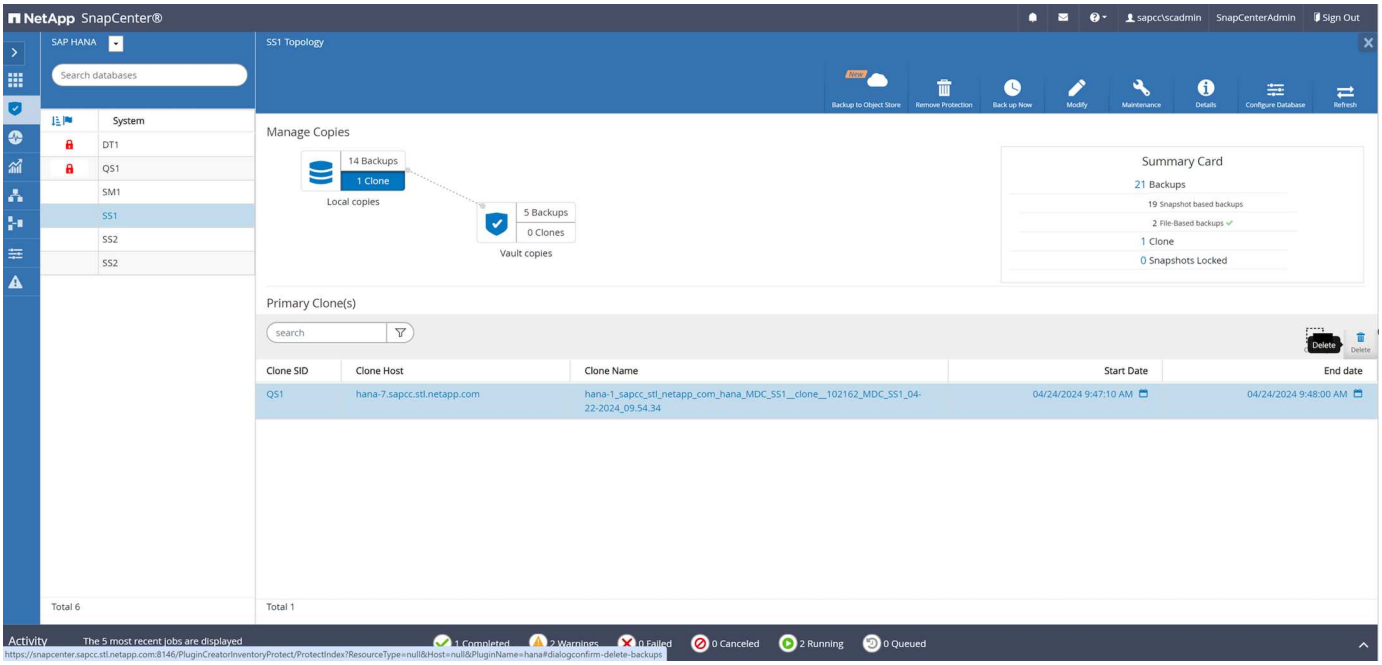


1. Die Protokolldatei des `sc-system-refresh` Skripts zeigt die verschiedenen Schritte an, die für den Wiederherstellungsvorgang ausgeführt wurden. Das Skript liest die Liste der Mandanten aus der Systemdatenbank und führt eine Wiederherstellung aller vorhandenen Mandanten durch.

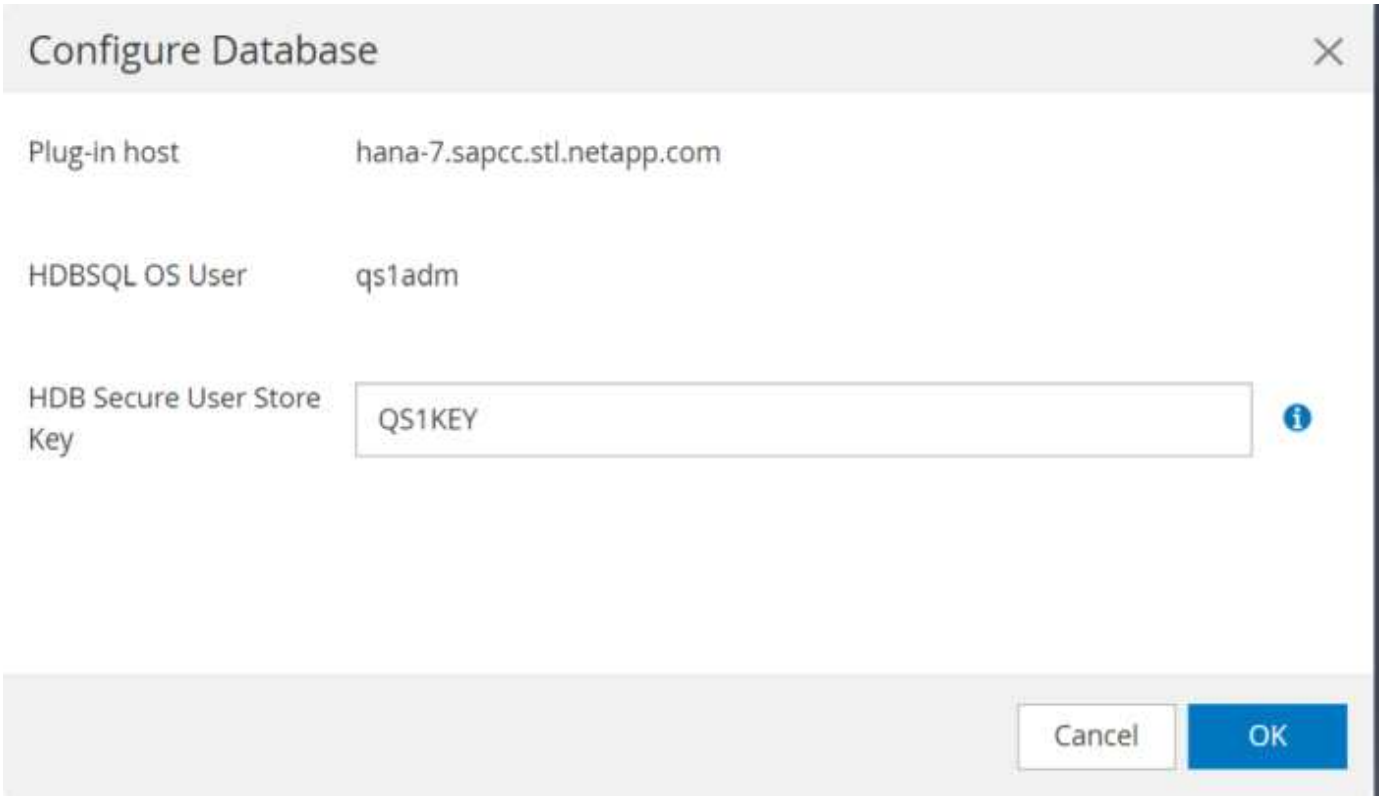
```
20240425112328###hana-7###sc-system-refresh.sh: Script version: 3.0
hana-7:/mnt/sapcc-share/SAP-System-Refresh # cat sap-system-refresh-
QS1.log
20240425112328###hana-7###sc-system-refresh.sh: ******************
Starting script: recovery operation ************************
20240425112328###hana-7###sc-system-refresh.sh: Recover system database.
```

```
20240425112328###hana-7###sc-system-refresh.sh:
/usr/sap/QS1/HDB11/exe/Python/bin/python
/usr/sap/QS1/HDB11/exe/python_support/recoverSys.py --command "RECOVER
DATA USING SNAPSHOT CLEAR LOG"
20240425112346###hana-7###sc-system-refresh.sh: Wait until SAP HANA
database is started ....
20240425112347###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425112357###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425112407###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425112417###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425112428###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425112438###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425112448###hana-7###sc-system-refresh.sh: Status: GREEN
20240425112448###hana-7###sc-system-refresh.sh: HANA system database
started.
20240425112448###hana-7###sc-system-refresh.sh: Checking connection to
system database.
20240425112448###hana-7###sc-system-refresh.sh:
/usr/sap/QS1/SYS/exe/hdb/hdbsql -U QS1KEY 'select * from sys.m_databases;'
DATABASE_NAME,DESCRIPTION,ACTIVE_STATUS,ACTIVE_STATUS_DETAILS,OS_USER,OS_G
ROUP,RESTART_MODE,FALLBACK_SNAPSHOT_CREATE_TIME
"SYSTEMDB","SystemDB-QS1-11","YES","","","","DEFAULT",?
"QS1","QS1-11","NO","ACTIVE","","","DEFAULT",?
2 rows selected (overall time 16.225 msec; server time 860 usec)
20240425112448###hana-7###sc-system-refresh.sh: Succesfully connected to
system database.
20240425112449###hana-7###sc-system-refresh.sh: Tenant databases to
recover: QS1
20240425112449###hana-7###sc-system-refresh.sh: Found inactive
tenants(QS1) and starting recovery
20240425112449###hana-7###sc-system-refresh.sh: Recover tenant database
QS1.
20240425112449###hana-7###sc-system-refresh.sh:
/usr/sap/QS1/SYS/exe/hdb/hdbsql -U QS1KEY RECOVER DATA FOR QS1 USING
SNAPSHOT CLEAR LOG
0 rows affected (overall time 22.138599 sec; server time 22.136268 sec)
20240425112511###hana-7###sc-system-refresh.sh: Checking availability of
Indexserver for tenant QS1.
20240425112511###hana-7###sc-system-refresh.sh: Recovery of tenant
database QS1 succesfully finished.
20240425112511###hana-7###sc-system-refresh.sh: Status: GREEN
20240425112511###hana-7###sc-system-refresh.sh: ********************
Finished script: recovery operation ************************
hana-7:/mnt/sapcc-share/SAP-System-Refresh
```

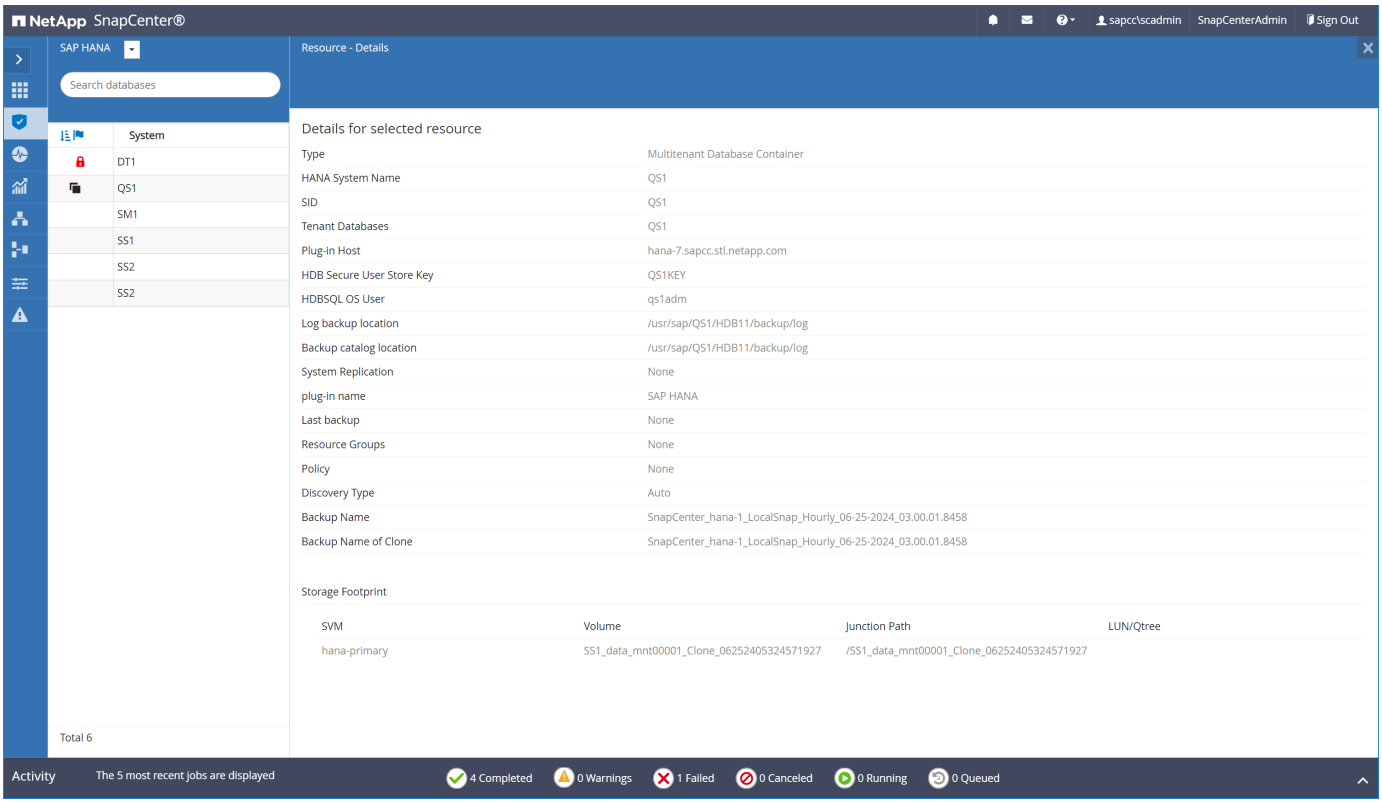
1. Nach Abschluss des SnapCenter-Jobs ist der Klon in der Topologieansicht des Quellsystems sichtbar.



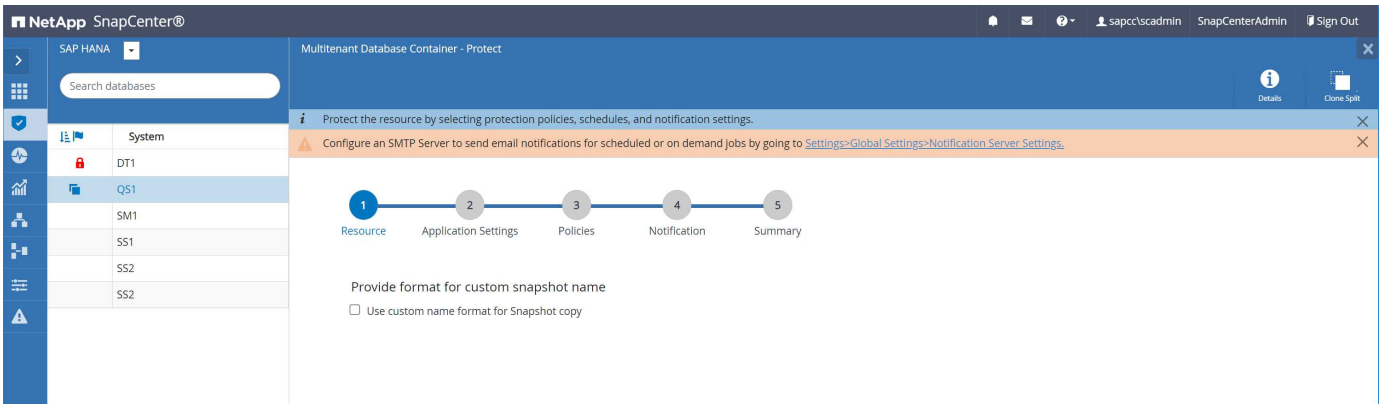
1. Die SAP HANA Datenbank läuft nun.
2. Wenn Sie das Ziel-SAP HANA-System schützen möchten, müssen Sie die automatische Erkennung ausführen, indem Sie auf die Zielsystemressource klicken.



Wenn der automatische Erkennungsprozess abgeschlossen ist, wird das neue geklonte Volume im Abschnitt „Storage-Platzbedarf“ aufgeführt.

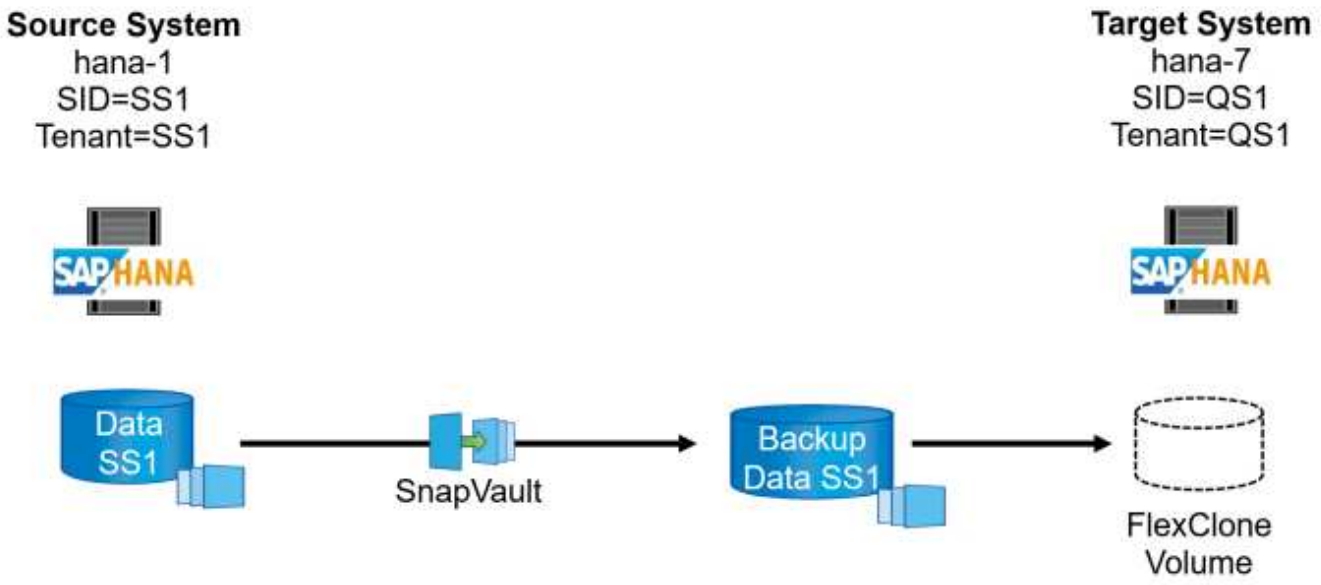


Durch erneutes Klicken auf die Ressource kann der Datenschutz für das aktualisierte QS1-System konfiguriert werden.

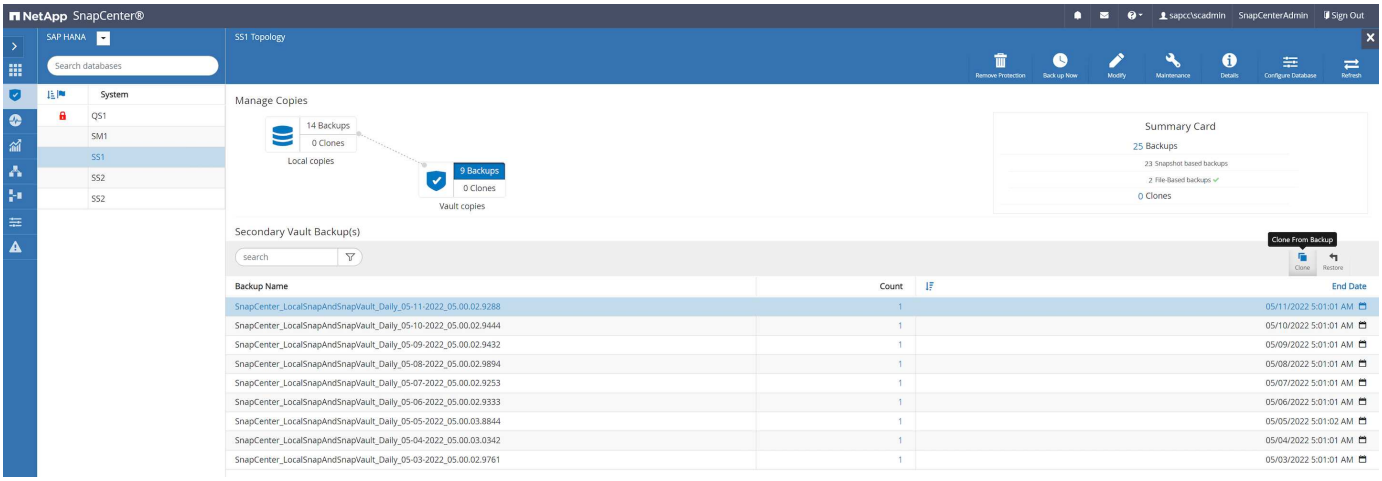


Klonen aus standortexternen Backup-Storage

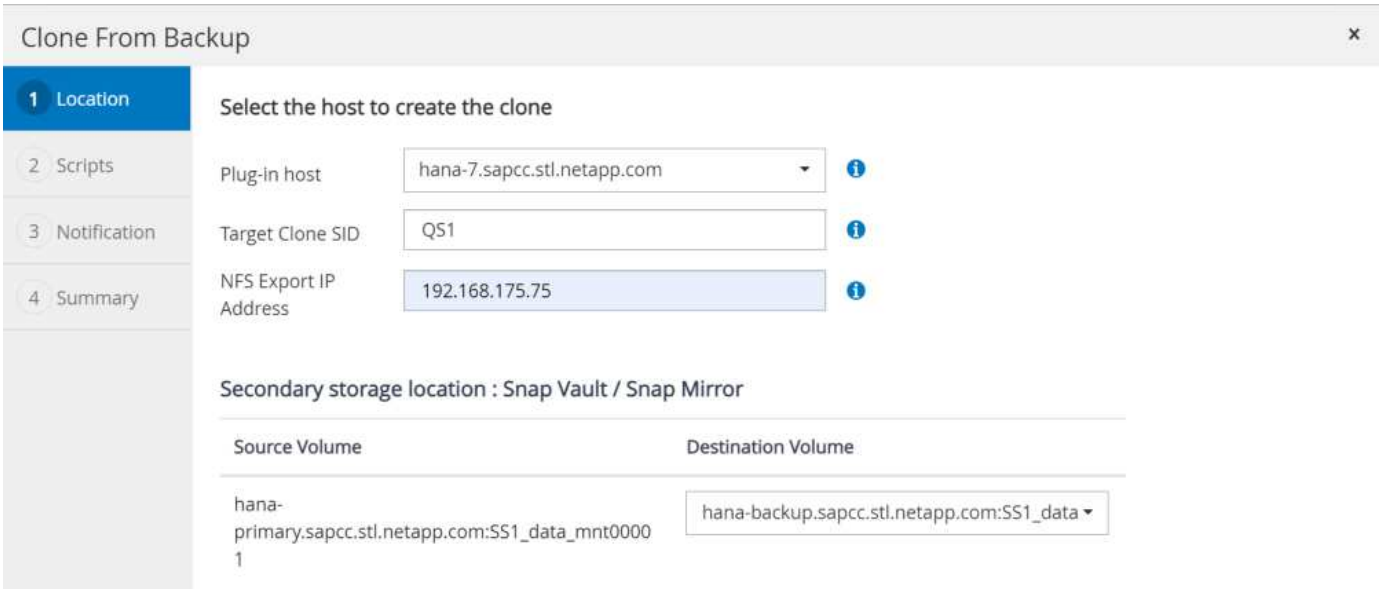
In diesem Abschnitt wird der Workflow zur Systemaktualisierung von SAP HANA beschrieben, bei dem der Mandantenname am Quell- und Zielsystem mit der SID identisch ist. Das Klonen von Speichern wird im externen Backup-Speicher ausgeführt und wird mithilfe des Skripts sc-System-refresh.sh weiter automatisiert.



Der einzige Unterschied im Workflow der SAP HANA Systemaktualisierung zwischen dem Klonen des primären und externen Backup-Storage ist die Auswahl des Snapshot Backups in SnapCenter. Für das Klonen von Backup-Storage außerhalb des Standorts müssen zunächst die sekundären Backups und anschließend die Auswahl des Snapshot-Backups ausgewählt werden.



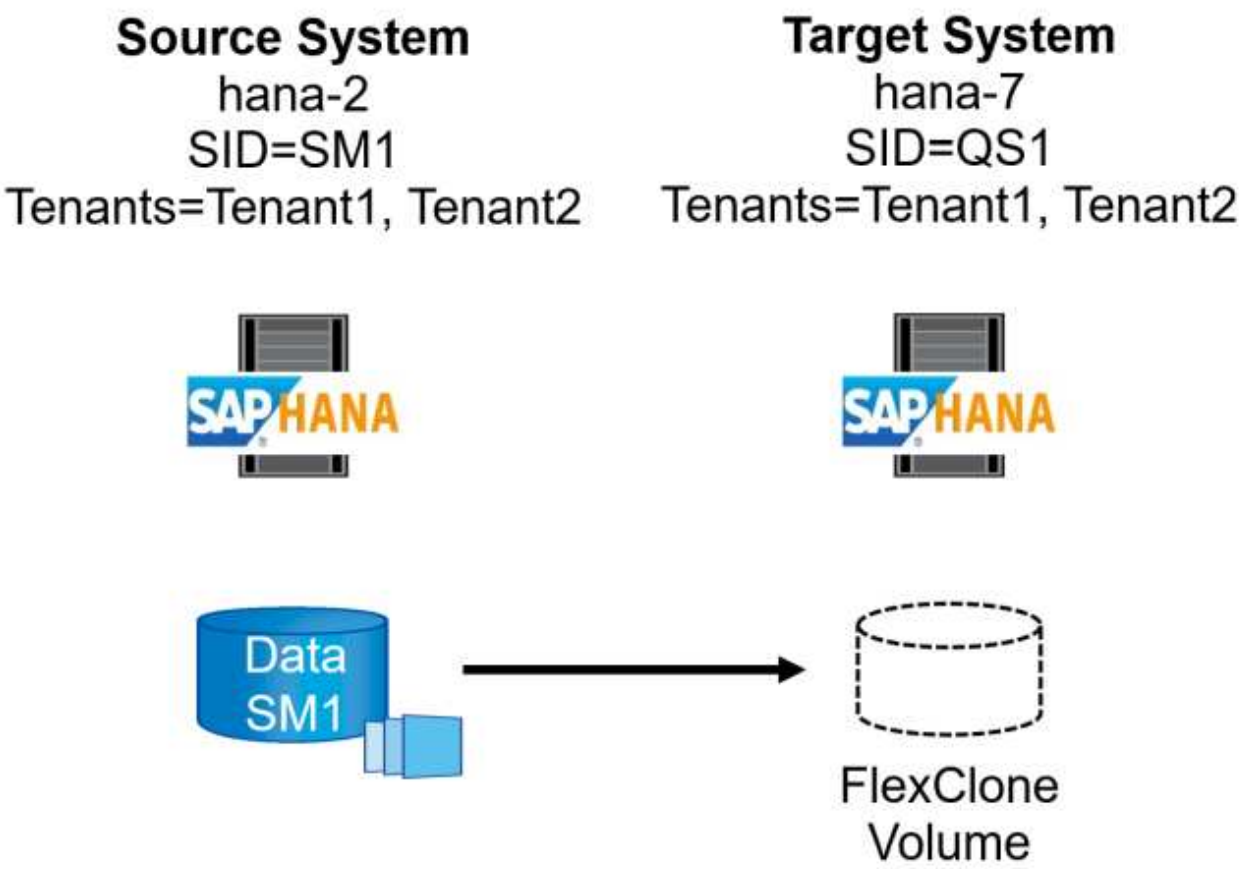
Wenn mehrere sekundäre Speicherorte für das ausgewählte Backup vorhanden sind, müssen Sie das erforderliche Zielvolume auswählen.



Alle nachfolgenden Schritte sind mit dem Workflow zum Klonen aus dem Primärspeicher identisch.

Klonen eines SAP HANA Systems mit mehreren Mandanten

In diesem Abschnitt wird der Workflow zur Aktualisierung des SAP HANA-Systems mit mehreren Mandanten beschrieben. Das Klonen von Storage wird im Primär-Storage durchgeführt und weitere automatisiert mithilfe des Skripts `sc-system-refresh.sh`.



Die erforderlichen Schritte in SnapCenter sind identisch mit den Schritten, die im Abschnitt „Klonen von primärem Storage mit Mandantenname gleich SID“ beschrieben wurden. Der einzige Unterschied besteht in der Wiederherstellung des Mandanten innerhalb des Skripts `sc-system-refresh.sh`, wo alle Mandanten wiederhergestellt werden.

```
20240430070214###hana-7###sc-system-refresh.sh:
**********************************************************************
********
20240430070214###hana-7###sc-system-refresh.sh: Script version: 3.0
20240430070214###hana-7###sc-system-refresh.sh: ******************
Starting script: recovery operation *************************
20240430070214###hana-7###sc-system-refresh.sh: Recover system database.
20240430070214###hana-7###sc-system-refresh.sh:
/usr/sap/QS1/HDB11/exe/Python/bin/python
/usr/sap/QS1/HDB11/exe/python_support/recoverSys.py --command "RECOVER
DATA USING SNAPSHOT CLEAR LOG"
[140310725887808, 0.008] >> starting recoverSys (at Tue Apr 30 07:02:15
2024)
[140310725887808, 0.008] args: ()
[140310725887808, 0.008] keys: \{'command': 'RECOVER DATA USING SNAPSHOT
CLEAR LOG'}
using logfile /usr/sap/QS1/HDB11/hana-7/trace/backup.log
recoverSys started: ============2024-04-30 07:02:15 ============
testing master: hana-7
hana-7 is master
shutdown database, timeout is 120
stop system
stop system on: hana-7
stopping system: 2024-04-30 07:02:15
stopped system: 2024-04-30 07:02:15
creating file recoverInstance.sql
restart database
restart master nameserver: 2024-04-30 07:02:20
start system: hana-7
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2024-04-30T07:02:32-04:00 P0023828 18f2eab9331 INFO RECOVERY RECOVER DATA
finished successfully
recoverSys finished successfully: 2024-04-30 07:02:33
[140310725887808, 17.548] 0
[140310725887808, 17.548] << ending recoverSys, rc = 0 (RC_TEST_OK), after
17.540 secs
20240430070233###hana-7###sc-system-refresh.sh: Wait until SAP HANA
database is started ....
20240430070233###hana-7###sc-system-refresh.sh: Status: GRAY
20240430070243###hana-7###sc-system-refresh.sh: Status: GRAY
```

```
20240430070253###hana-7###sc-system-refresh.sh: Status: GRAY
20240430070304###hana-7###sc-system-refresh.sh: Status: GRAY
20240430070314###hana-7###sc-system-refresh.sh: Status: GREEN
20240430070314###hana-7###sc-system-refresh.sh: HANA system database
started.
20240430070314###hana-7###sc-system-refresh.sh: Checking connection to
system database.
20240430070314###hana-7###sc-system-refresh.sh:
/usr/sap/QS1/SYS/exe/hdb/hdbsql -U QS1KEY 'select * from sys.m_databases;'
20240430070314###hana-7###sc-system-refresh.sh: Succesfully connected to
system database.
20240430070314###hana-7###sc-system-refresh.sh: Tenant databases to
recover: TENANT2
TENANT1
20240430070314###hana-7###sc-system-refresh.sh: Found inactive
tenants(TENANT2
TENANT1) and starting recovery
20240430070314###hana-7###sc-system-refresh.sh: Recover tenant database
TENANT2.
20240430070314###hana-7###sc-system-refresh.sh:
/usr/sap/QS1/SYS/exe/hdb/hdbsql -U QS1KEY RECOVER DATA FOR TENANT2 USING
SNAPSHOT CLEAR LOG
20240430070335###hana-7###sc-system-refresh.sh: Checking availability of
Indexserver for tenant TENANT2.
20240430070335###hana-7###sc-system-refresh.sh: Recovery of tenant
database TENANT2 succesfully finished.
20240430070335###hana-7###sc-system-refresh.sh: Status: GREEN
20240430070335###hana-7###sc-system-refresh.sh: Recover tenant database
TENANT1.
20240430070335###hana-7###sc-system-refresh.sh:
/usr/sap/QS1/SYS/exe/hdb/hdbsql -U QS1KEY RECOVER DATA FOR TENANT1 USING
SNAPSHOT CLEAR LOG
20240430070349###hana-7###sc-system-refresh.sh: Checking availability of
Indexserver for tenant TENANT1.
20240430070350###hana-7###sc-system-refresh.sh: Recovery of tenant
database TENANT1 succesfully finished.
20240430070350###hana-7###sc-system-refresh.sh: Status: GREEN
20240430070350###hana-7###sc-system-refresh.sh: ********************
Finished script: recovery operation *************************
```

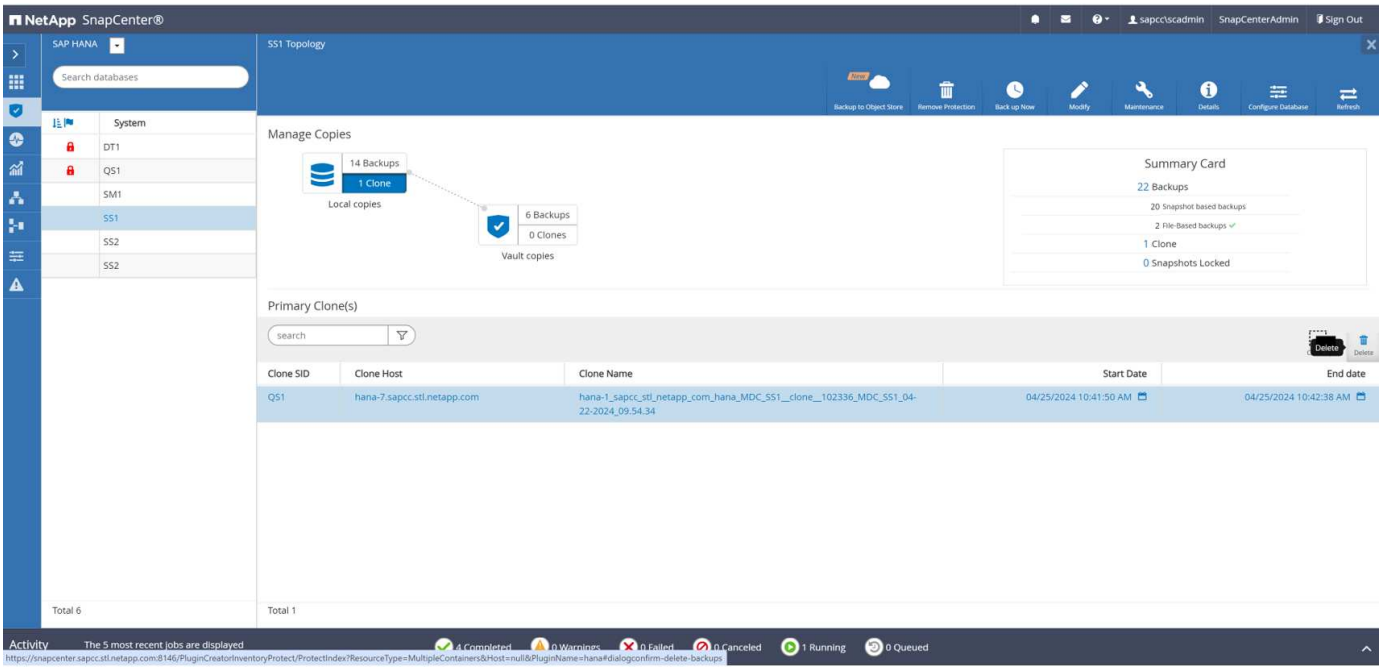
Klonvorgang

Ein neuer Vorgang zur Systemaktualisierung von SAP HANA wird gestartet, indem das Zielsystem mithilfe des SnapCenter-Klonlösch-Vorgangs gereinigt wird.

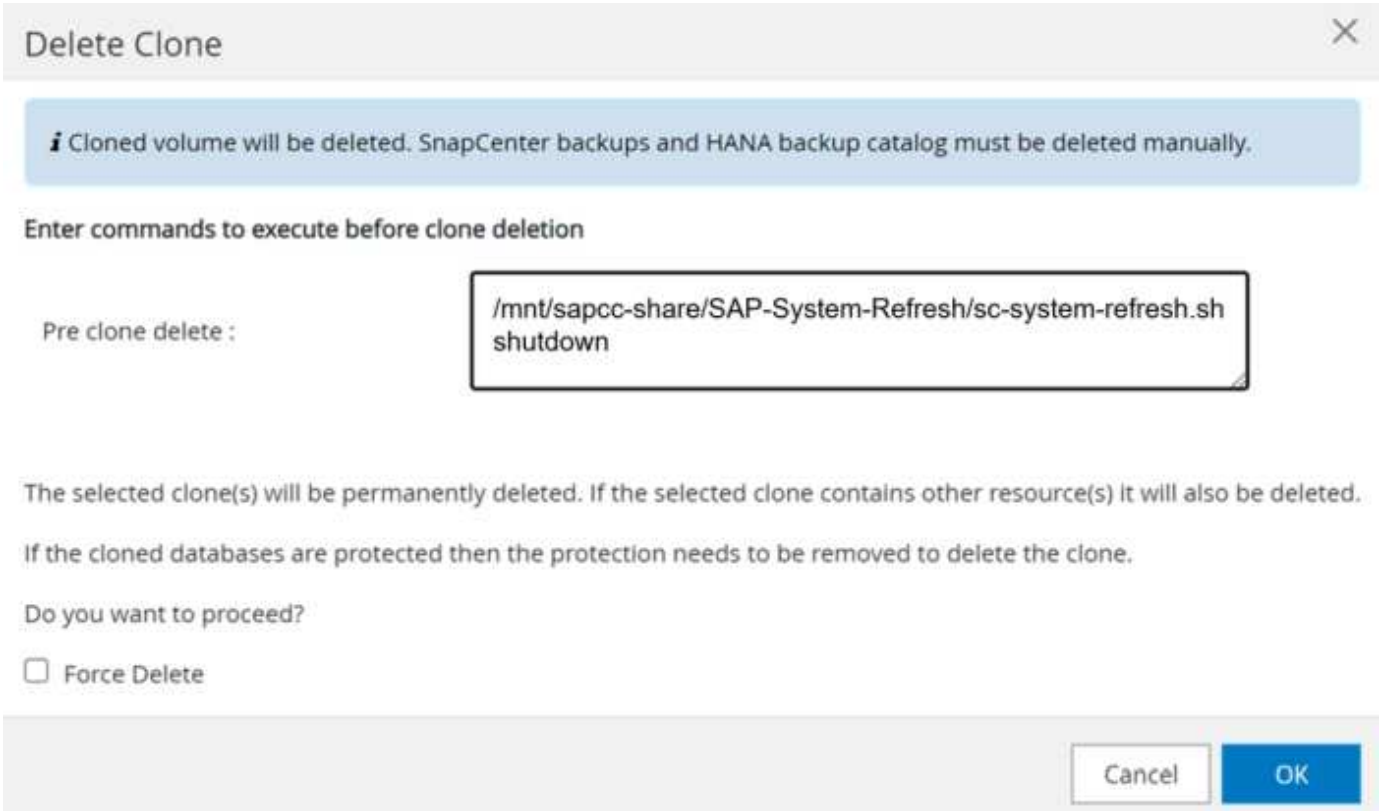
Wurde das SAP HANA-Zielsystem in SnapCenter geschützt, so muss zunächst der Schutz entfernt werden. Klicken Sie in der Topologieansicht des Zielsystems auf Schutz entfernen.

Der Clone delete Workflow wird nun mit den folgenden Schritten ausgeführt.

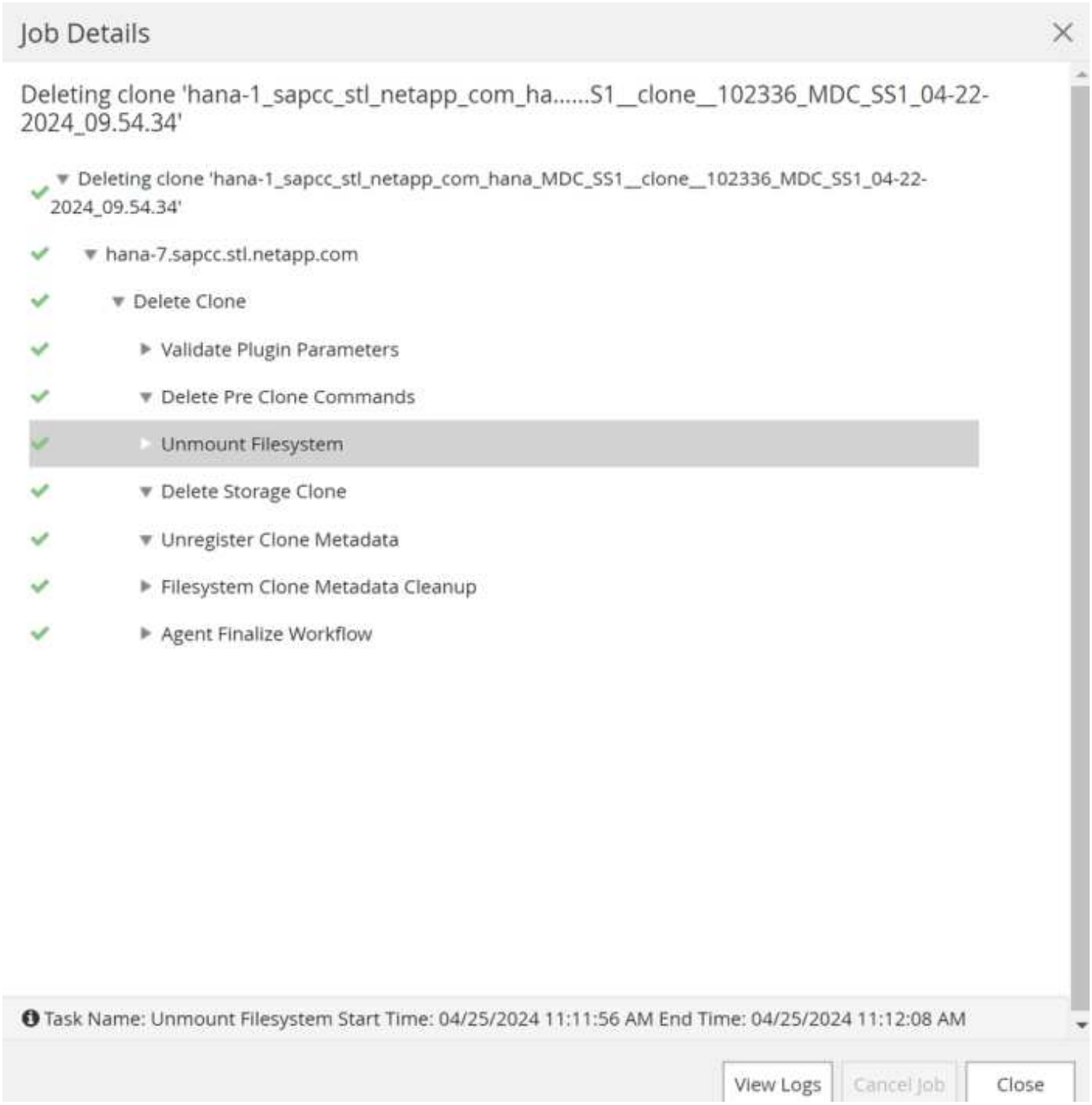
1. Wählen Sie den Klon in der Topologieansicht des Quellsystems aus, und klicken Sie auf Löschen.



1. Geben Sie die Skripte vor dem Klonen ein und heben Sie die Bereitstellung mit den erforderlichen Befehlszeilenoptionen ab.



1. Der Bildschirm „Jobdetails“ in SnapCenter zeigt den Fortschritt des Vorgangs an.



1. Die Protokolldatei des `sc-system-refresh` Skripts zeigt die Schritte zum Herunterfahren und Unmounten an.

```
20240425111042###hana-7###sc-system-refresh.sh:
**********************************************************************
********
20240425111042###hana-7###sc-system-refresh.sh: Script version: 3.0
20240425111042###hana-7###sc-system-refresh.sh: ******************
Starting script: shutdown operation ************************
20240425111042###hana-7###sc-system-refresh.sh: Stopping HANA database.
20240425111042###hana-7###sc-system-refresh.sh: sapcontrol -nr 11
-function StopSystem HDB
25.04.2024 11:10:42
StopSystem
OK
20240425111042###hana-7###sc-system-refresh.sh: Wait until SAP HANA
database is stopped ....
20240425111042###hana-7###sc-system-refresh.sh: Status: GREEN
20240425111052###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425111103###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425111113###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425111123###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425111133###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425111144###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425111154###hana-7###sc-system-refresh.sh: Status: GRAY
20240425111154###hana-7###sc-system-refresh.sh: SAP HANA database is
stopped.
20240425111154###hana-7###sc-system-refresh.sh: ******************
Finished script: shutdown operation ************************
```

1. Der SAP HANA-Aktualisierungsvorgang kann nun mithilfe des SnapCenter-Klonerstellung erneut gestartet werden.

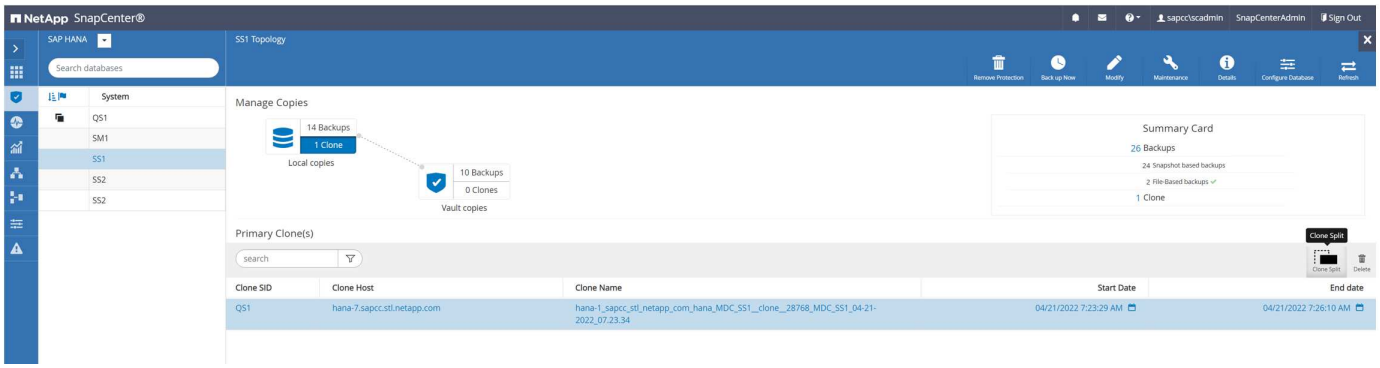
SAP HANA Systemaktualisierung mit Klonteilvorgang

Ist die Verwendung des Zielsystems für die Systemaktualisierung über einen längeren Zeitraum geplant, ist es sinnvoll, das FlexClone Volume im Rahmen der Systemaktualisierung zu teilen.

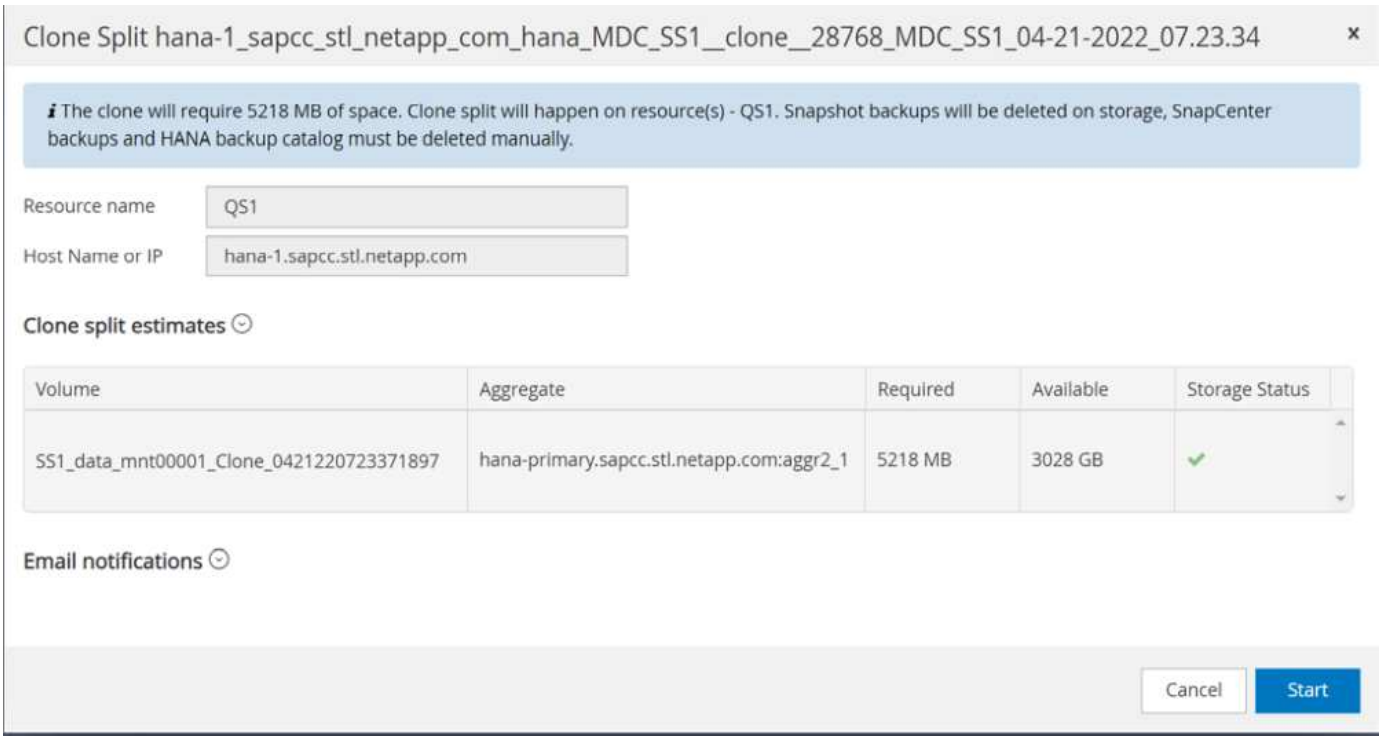
Der Aufspaltung von Klonen blockiert nicht die Verwendung des geklonten Volume und kann somit jederzeit ausgeführt werden, während die SAP HANA Datenbank verwendet wird.

Bei Azure NetApp Files ist der Aufspaltung von Klonen nicht verfügbar, da Azure NetApp Files den Klon nach der Erstellung immer teilt.

Der Clone Split Workflow in SnapCenter wird in der Topologieansicht des Quellsystems initiiert, indem der Klon ausgewählt und auf Clone Split geklickt wird.

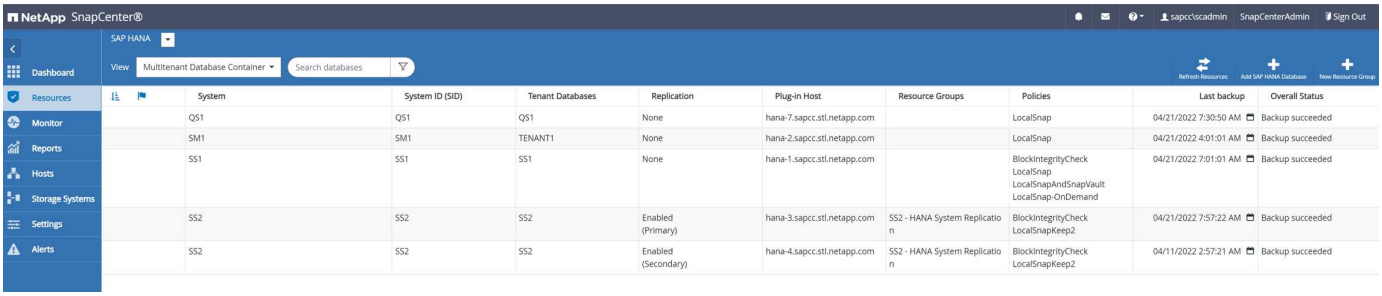


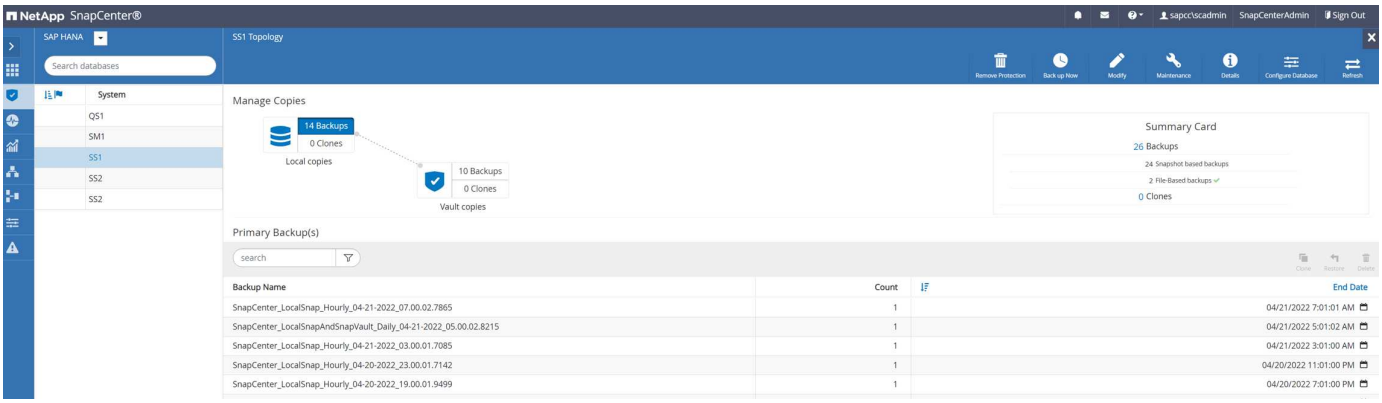
Im nächsten Bildschirm wird eine Vorschau angezeigt, die Informationen zur erforderlichen Kapazität für das geteilte Volumen liefert.



Das Jobprotokoll von SnapCenter zeigt den Status des Klonabteilvorgangs an.

In der Ressourcenansicht in SnapCenter wird das Zielsystem QS1 nun nicht mehr als geklonte Ressource markiert. Wenn der Klon zurück zur Topologieansicht des Quellsystems angezeigt wird, ist er nicht mehr sichtbar. Das Split-Volume ist jetzt unabhängig vom Snapshot Backup des Quellsystems.





Der Aktualisierungs-Workflow nach einem Klonteilvorgang sieht etwas anders aus als der Vorgang ohne Klontrennung. Nach einer Klonaufteilung ist kein Klonvorgang erforderlich, da es sich beim Zieldatenvolume nicht mehr um ein FlexClone Volume handelt.

Der Workflow besteht aus den folgenden Schritten:

1. Wurde das SAP HANA-Zielsystem in SnapCenter geschützt, so muss zunächst der Schutz entfernt werden.
2. Die SAP HANA Datenbank muss heruntergefahren, das Daten-Volume abgehängt und der von SnapCenter erstellte fstab Eintrag entfernt werden. Diese Schritte müssen manuell ausgeführt werden.
3. Der Workflow zur Erstellung von SnapCenter Klonen kann nun wie in den vorherigen Abschnitten beschrieben ausgeführt werden.
4. Nach dem Aktualisierungsvorgang ist das alte Zieldatenvolume noch vorhanden und muss manuell mit z.B. dem ONTAP-Systemmanager gelöscht werden.

SnapCenter Workflow-Automatisierung mit PowerShell Skripten

In den vorherigen Abschnitten wurden die verschiedenen Workflows über die UI von SnapCenter ausgeführt. Alle Workflows können auch mit PowerShell-Skripten oder REST-API-Aufrufen ausgeführt werden, was eine weitere Automatisierung ermöglicht. In den folgenden Abschnitten werden die grundlegenden Beispiele für PowerShell-Skripts für die folgenden Workflows beschrieben.

- Erstellen von Klonen
- Klon löschen

> Die Beispielskripte werden wie IS bereitgestellt und von NetApp nicht unterstützt.

Alle Skripte müssen in einem PowerShell Befehlsfenster ausgeführt werden. Bevor die Skripte ausgeführt werden können, muss mithilfe der eine Verbindung zum SnapCenter-Server hergestellt werden `Open-SmConnection` Befehl.

Erstellen von Klonen

Das einfache Skript unten zeigt, wie eine SnapCenter Klonerstellung mithilfe von PowerShell Befehlen ausgeführt werden kann. Das SnapCenter `New-SmClone` Der Befehl wird mit der erforderlichen Befehlszeilenoption für die Lab-Umgebung und dem zuvor erläuterten Automatisierungsskript ausgeführt.

```
$BackupName='SnapCenter_hana-1_LocalSnap_Hourly_06-25-2024_03.00.01.8458'
$JobInfo=New-SmClone -AppPluginCode hana -BackupName $BackupName
-Resources @\{"Host"="hana-1.sapcc.stl.netapp.com";"UID"="MDC\SS1"}
-CloneToInstance hana-7.sapcc.stl.netapp.com -postclonecreatecommands
'/mnt/sapcc-share/SAP-System-Refresh/sc-system-refresh.sh recover'
-NFSExportIPs 192.168.175.75 -CloneUid 'MDC\QS1'
# Get JobID of clone create job
$Job=Get-SmJobSummaryReport | ?\{$_.JobType -eq "Clone" } | ?\{$_.JobName
-Match $BackupName} | ?\{$_.Status -eq "Running"}
$JobId=$Job.SmJobId
Get-SmJobSummaryReport -JobId $JobId
# Wait until job is finished
do \{ $Job=Get-SmJobSummaryReport -JobId $JobId; write-host $Job.Status;
sleep 20 } while ( $Job.Status -Match "Running" )
Write-Host " "
Get-SmJobSummaryReport -JobId $JobId
Write-Host "Clone create job has been finshed."
```

Die Bildschirmausgabe zeigt die Ausführung des PowerShell-Skripts Clone erstellen.

```
PS C:\Windows\system32> C:\NetApp\clone-create.ps1
SmJobId : 110382
JobCreatedDateTime :
JobStartDateTime : 6/26/2024 9:55:34 AM
JobEndDateTime :
JobDuration :
JobName : Clone from backup 'SnapCenter_hana-1_LocalSnap_Hourly_06-25-
2024_03.00.01.8458'
JobDescription :
Status : Running
IsScheduled : False
JobError :
JobType : Clone
PolicyName :
JobResultData :
Running
Running
Running
Running
Running
Running
Running
Running
Running
Completed
SmJobId : 110382
JobCreatedDateTime :
JobStartDateTime : 6/26/2024 9:55:34 AM
JobEndDateTime : 6/26/2024 9:58:50 AM
JobDuration : 00:03:16.6889170
JobName : Clone from backup 'SnapCenter_hana-1_LocalSnap_Hourly_06-25-
2024_03.00.01.8458'
JobDescription :
Status : Completed
IsScheduled : False
JobError :
JobType : Clone
PolicyName :
JobResultData :
Clone create job has been finshed.
```

Klon löschen

Das einfache Skript unten zeigt, wie eine SnapCenter Klonlösch-Operation mit PowerShell Befehlen

ausgeführt werden kann. Das SnapCenter `Remove-SmClone` Der Befehl wird mit der erforderlichen Befehlszeilenoption für die Lab-Umgebung und dem zuvor erläuterten Automatisierungsskript ausgeführt.

```
$CloneInfo=Get-SmClone |?\{$_.CloneName -Match "hana-
1_sapcc_stl_netapp_com_hana_MDC_SS1" }
$JobInfo=Remove-SmClone -CloneName $CloneInfo.CloneName -PluginCode hana
-PreCloneDeleteCommands '/mnt/sapcc-share/SAP-System-Refresh/sc-system-
refresh.sh shutdown QS1' -UnmountCommands '/mnt/sapcc-share/SAP-System-
Refresh/sc-system-refresh.sh umount QS1' -Confirm: $False
Get-SmJobSummaryReport -JobId $JobInfo.Id
# Wait until job is finished
do \{ $Job=Get-SmJobSummaryReport -JobId $JobInfo.Id; write-host
$Job.Status; sleep 20 } while ( $Job.Status -Match "Running" )
Write-Host " "
Get-SmJobSummaryReport -JobId $JobInfo.Id
Write-Host "Clone delete job has been finshed."
PS C:\NetApp>
```

In der Bildschirmausgabe wird die Ausführung des PowerShell-Skripts Clone –delete.ps1 angezeigt.

```
PS C:\Windows\system32> C:\NetApp\clone-delete.ps1
SmJobId : 110386
JobCreatedDateTime :
JobStartDateTime : 6/26/2024 10:01:33 AM
JobEndDateTime :
JobDuration :
JobName : Deleting clone 'hana-
1_sapcc_stl_netapp_com_hana_MDC_SS1__clone__110382_MDC_SS1_04-22-
2024_09.54.34'
JobDescription :
Status : Running
IsScheduled : False
JobError :
JobType : DeleteClone
PolicyName :
JobResultData :
Running
Running
Running
Running
Completed
SmJobId : 110386
JobCreatedDateTime :
JobStartDateTime : 6/26/2024 10:01:33 AM
JobEndDateTime : 6/26/2024 10:02:38 AM
JobDuration : 00:01:05.5658860
JobName : Deleting clone 'hana-
1_sapcc_stl_netapp_com_hana_MDC_SS1__clone__110382_MDC_SS1_04-22-
2024_09.54.34'
JobDescription :
Status : Completed
IsScheduled : False
JobError :
JobType : DeleteClone
PolicyName :
JobResultData :
Clone delete job has been finshed.
PS C:\Windows\system32>
```

SAP Systemklon mit SnapCenter

Dieser Abschnitt enthält eine Schritt-für-Schritt-Beschreibung für den SAP-Systemklonvorgang, mit der ein Reparatursystem zur Beseitigung logischer Beschädigung eingerichtet werden kann.

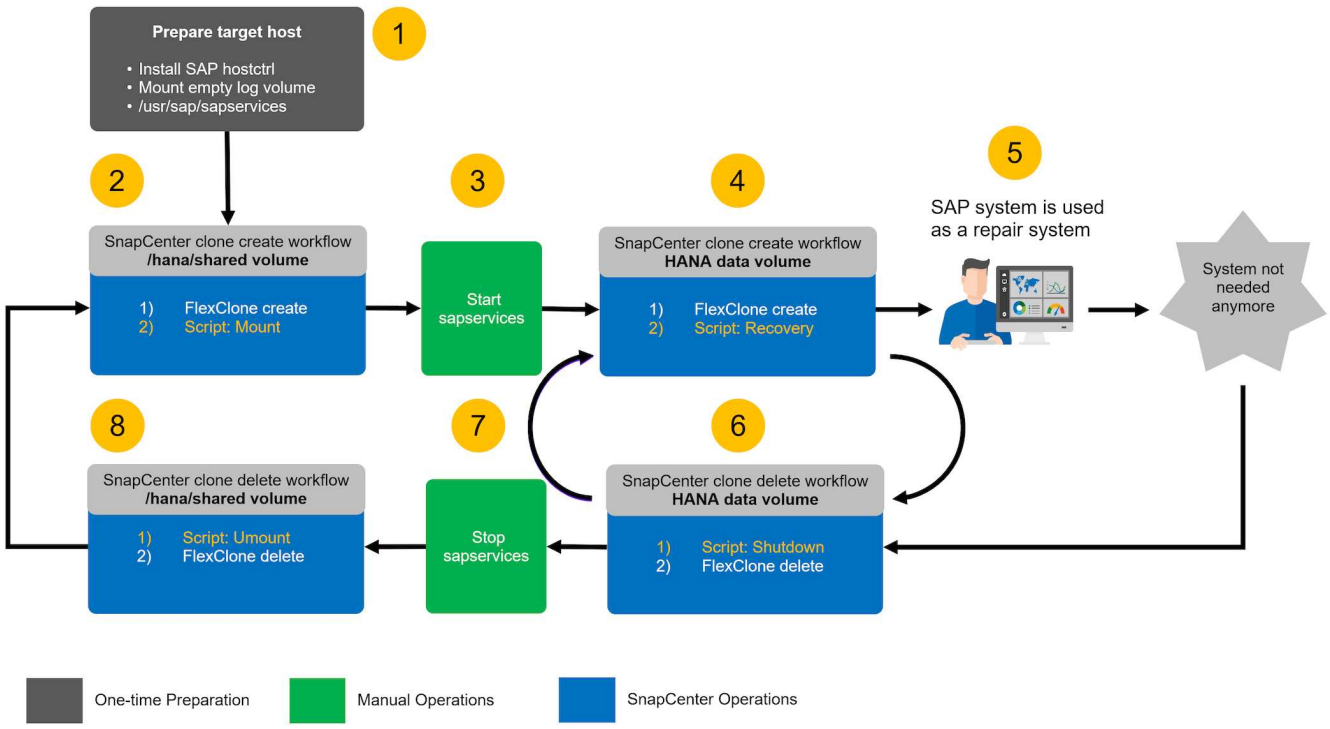
Die folgende Abbildung fasst die erforderlichen Schritte für einen SAP-Systemklonvorgang mit SnapCenter zusammen.

1. Bereiten Sie den Zielhost vor.
2. Workflow für die SAP HANA-Freigabe-Volumes durch SnapCenter-Klon erstellen
3. Starten Sie SAP HANA Services.
4. SnapCenter Clone erstellen Sie einen Workflow für das SAP HANA Daten-Volume einschließlich Datenbank-Recovery.
5. Das SAP HANA-System kann nun als Reparatursystem eingesetzt werden.

> Wenn Sie das System auf ein anderes Snapshot Backup zurücksetzen müssen, reichen die Schritte 6 und Schritt 4 aus. Das SAP HANA Shared Volume kann weiterhin gemountet werden.

Wenn das System nicht mehr benötigt wird, erfolgt die Bereinigung mit den folgenden Schritten.

6. SnapCenter Clone delete Workflow für das SAP HANA Daten-Volume einschließlich Datenbank-Shutdown.
7. Stoppen Sie SAP HANA Services.
8. SnapCenter Clone delete Workflow für das SAP HANA Shared Volume.



Voraussetzungen und Einschränkungen

Die in den folgenden Abschnitten beschriebenen Workflows weisen einige Voraussetzungen und Einschränkungen hinsichtlich der SAP HANA-Systemarchitektur und der SnapCenter-Konfiguration auf.

- Der beschriebene Workflow gilt für SAP HANA MDC-Systeme mit einem Host. Mehrere Hostsysteme werden nicht unterstützt.
- Das SnapCenter SAP HANA-Plug-in muss auf dem Ziel-Host implementiert werden, um die Ausführung

von Automatisierungsskripts zu ermöglichen.

- Der Workflow wurde für NFS validiert. Die Automatisierung `script sc-mount-volume.sh`, die verwendet wird, um das SAP HANA Shared Volume zu mounten, unterstützt nicht FCP. Dieser Schritt muss entweder manuell oder durch erweitern des Skripts durchgeführt werden.
- Der beschriebene Workflow gilt nur für die SnapCenter Version 5.0 oder höher.

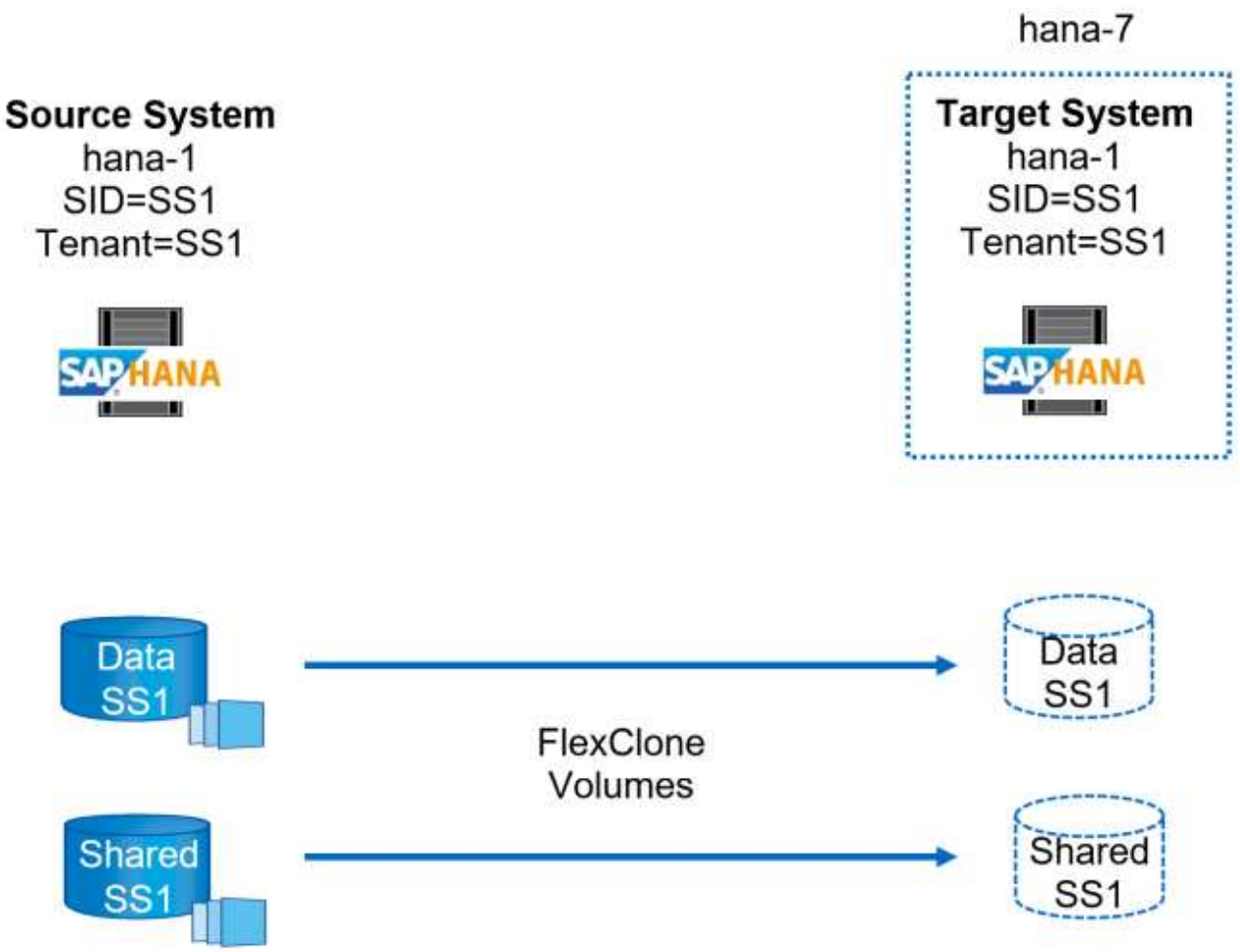
Laboreinrichtung

Die Abbildung unten zeigt das Lab-Setup, das für den Klonvorgang des Systems verwendet wird.

Es wurden folgende Softwareversionen verwendet:

- SnapCenter 5.0
- SAP HANA Systems: HANA 2.0 SPS6 Rev.61
- SLES 15
- ONTAP 9.7 P7

Alle SAP HANA-Systeme müssen auf Basis des Konfigurationsleitfadens konfiguriert werden"SAP HANA auf NetApp AFF Systemen mit NFS". SnapCenter und die SAP HANA-Ressourcen wurden basierend auf dem Best Practice Guide konfiguriert"Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter".



Vorbereitung des Ziel-Hosts

In diesem Abschnitt werden die Vorbereitungsschritte beschrieben, die auf einem Server erforderlich sind, der als Systemklonziel verwendet wird.

Während des normalen Betriebs kann der Ziel-Host für andere Zwecke verwendet werden, zum Beispiel als SAP HANA QA oder Testsystem. Daher müssen die meisten der beschriebenen Schritte ausgeführt werden, wenn der Systemklonvorgang angefordert wird. Zum anderen können die relevanten Konfigurationsdateien, wie `/etc/fstab` und , vorbereitet und `/usr/sap/sapservices`dann einfach durch Kopieren der Konfigurationsdatei in die Produktion gebracht werden.

Zur Vorbereitung des Ziel-Hosts gehört auch das Herunterfahren des SAP HANA QA- oder Testsystems.

Hostname und IP-Adresse des Zielservers

Der Hostname des Zielservers muss mit dem Hostnamen des Quellsystems identisch sein. Die IP-Adresse kann unterschiedlich sein.

Ein ordnungsgemäßes Fechten des Zielservers muss eingerichtet werden, damit er nicht mit anderen Systemen kommunizieren kann. Wenn kein ordnungsgemäßes Fechten vorhanden ist, kann das geklonte Produktionssystem Daten mit anderen Produktionssystemen austauschen.

In unserem Labor-Setup haben wir den Hostnamen des Zielsystems nur intern aus der Perspektive des Zielsystems geändert. Extern war der Host immer noch mit dem Hostnamen hana-7 zugänglich. Bei der Anmeldung beim Host ist der Host selbst hana-1.

Erforderliche Software installieren

Die SAP-Hostagent-Software muss auf dem Zielserver installiert sein. Umfassende Informationen finden Sie im im "SAP Host Agent" SAP-Hilfeportal.

Das SnapCenter SAP HANA-Plug-in muss über den zusätzlichen Host-Vorgang innerhalb von SnapCenter auf dem Ziel-Host implementiert werden.

Konfigurieren von Benutzern, Ports und SAP-Diensten

Die erforderlichen Anwender und Gruppen für die SAP HANA-Datenbank müssen auf dem Zielserver verfügbar sein. In der Regel wird die zentrale Benutzerverwaltung verwendet. Daher sind keine Konfigurationsschritte auf dem Zielserver erforderlich. Die für die SAP HANA-Datenbank erforderlichen Ports müssen auf den Ziel-Hosts konfiguriert werden. Die Konfiguration kann vom Quellsystem kopiert werden, indem die Datei /etc/Services auf den Zielserver kopiert wird.

Die erforderlichen SAP Services-Einträge müssen auf dem Zielhost verfügbar sein. Die Konfiguration kann durch Kopieren des aus dem Quellsystem kopiert werden `/usr/sap/sapservices` Datei auf dem Zielserver. Die folgende Ausgabe zeigt die erforderlichen Einträge für die im Lab-Setup verwendete SAP HANA-Datenbank.

```
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/SS1/HDB00/exe:$LD_LIBRARY_PATH;export
LD_LIBRARY_PATH;/usr/sap/SS1/HDB00/exe/sapstartsrv
pf=/usr/sap/SS1/SYS/profile/SS1_HDB00_hana-1 -D -u ss1adm
limit.descriptors=1048576
```

Vorbereiten des Protokoll- und Protokollvolumes

Da Sie das Protokoll-Volume nicht aus dem Quellsystem klonen müssen und eine Wiederherstellung mit der Option Protokoll löschen durchgeführt wird, muss ein leeres Protokoll-Volume auf dem Zielhost vorbereitet sein.

Da das Quellsystem mit einem separaten Protokoll-Backup-Volume konfiguriert wurde, muss ein leeres Protokoll-Backup-Volume vorbereitet und an denselben Bereitstellungspunkt wie am Quellsystem angehängt werden.

```
hana-1:/# cat /etc/fstab
192.168.175.117:/SS1_repair_log_mnt00001 /hana/log/SS1/mnt00001 nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0
0
192.168.175.117:/SS1_repair_log_backup /mnt/log-backup nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0
0
```

Innerhalb des Protokollvolumens hdb* müssen Sie Unterverzeichnisse auf die gleiche Weise erstellen wie beim Quellsystem.

```
hana-1:/ # ls -al /hana/log/SS1/mnt00001/
total 16
drwxrwxrwx 5 root root 4096 Dec 1 06:15 .
drwxrwxrwx 1 root root 16 Nov 30 08:56 ..
drwxr-xr-- 2 ss1adm sapsys 4096 Dec 1 06:14 hdb00001
drwxr-xr-- 2 ss1adm sapsys 4096 Dec 1 06:15 hdb00002.00003
drwxr-xr-- 2 ss1adm sapsys 4096 Dec 1 06:15 hdb00003.00003
```

Innerhalb des Protokoll-Backup-Volumes müssen Sie Unterverzeichnisse für das System und die Mandantendatenbank erstellen.

```
hana-1:/ # ls -al /mnt/log-backup/
total 12
drwxr-xr-- 2 ss1adm sapsys 4096 Dec 1 04:48 .
drwxr-xr-- 2 ss1adm sapsys 4896 Dec 1 03:42 ..
drwxr-xr-- 2 ss1adm sapsys 4096 Dec 1 06:15 DB_SS1
drwxr-xr-- 2 ss1adm sapsys 4096 Dec 1 06:14 SYSTEMDB
```

*** Dateisystemeinschübe vorbereiten***

Die Mount-Punkte für die Daten und das freigegebene Volume müssen vorbereitet werden.

Mit unserem Beispiel, die Verzeichnisse `/hana/data/SS1/mnt00001`, `/hana/shared` und `usr/sap/SS1` müssen erstellt werden.

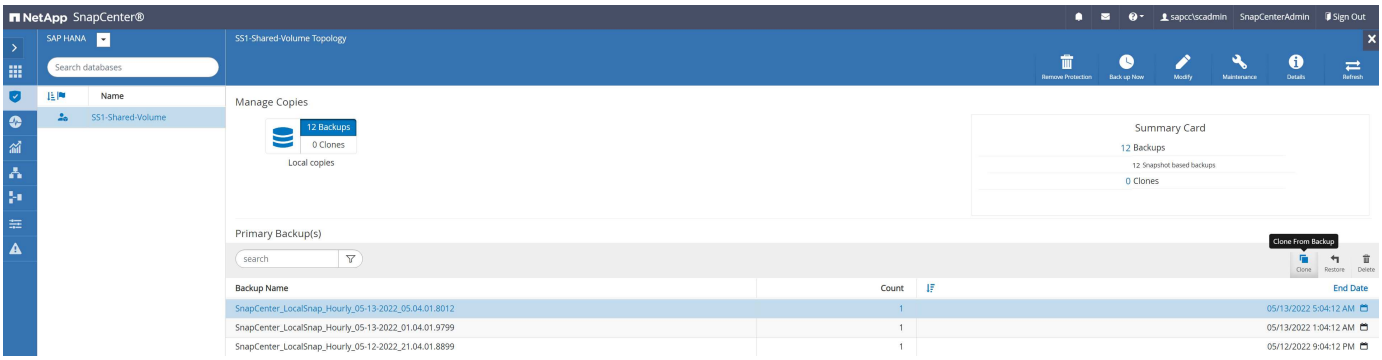
Scriptausführung vorbereiten

Sie müssen die Skripte hinzufügen, die auf dem Zielsystem ausgeführt werden sollen, um die Konfigurationsdatei SnapCenter allowed commands hinzuzufügen.

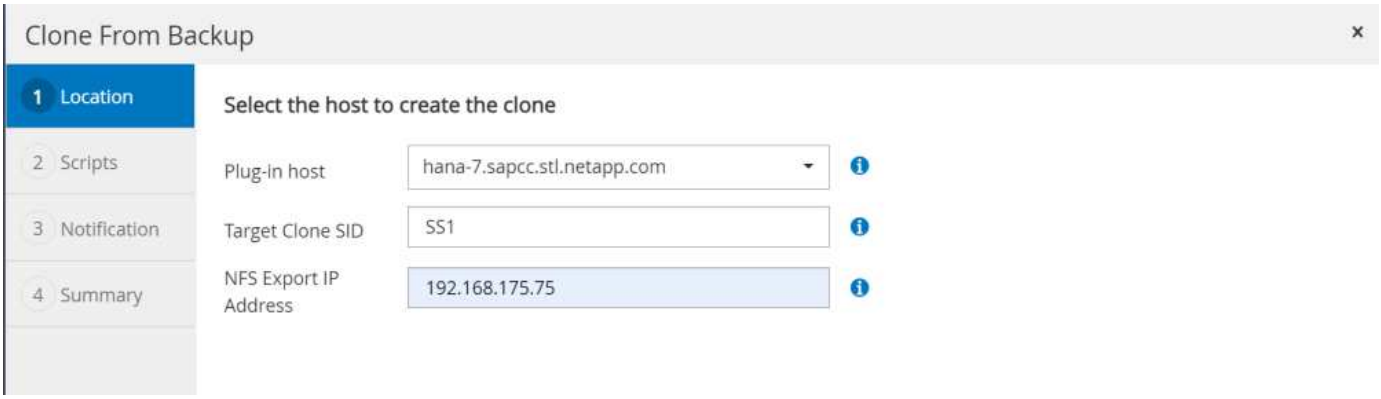
```
hana-7:/opt/NetApp/snapcenter/scc/etc # cat
/opt/NetApp/snapcenter/scc/etc/allowed_commands.config
command: mount
command: umount
command: /mnt/sapcc-share/SAP-System-Refresh/sc-system-refresh.sh
command: /mnt/sapcc-share/SAP-System-Refresh/sc-mount-volume.sh
hana-7:/opt/NetApp/snapcenter/scc/etc #
```

Klonen des gemeinsamen HANA Volumes

1. Wählen Sie eine Snapshot-Sicherung aus dem SS1 Shared Volume des Quellsystems aus, und klicken Sie auf Klonen.

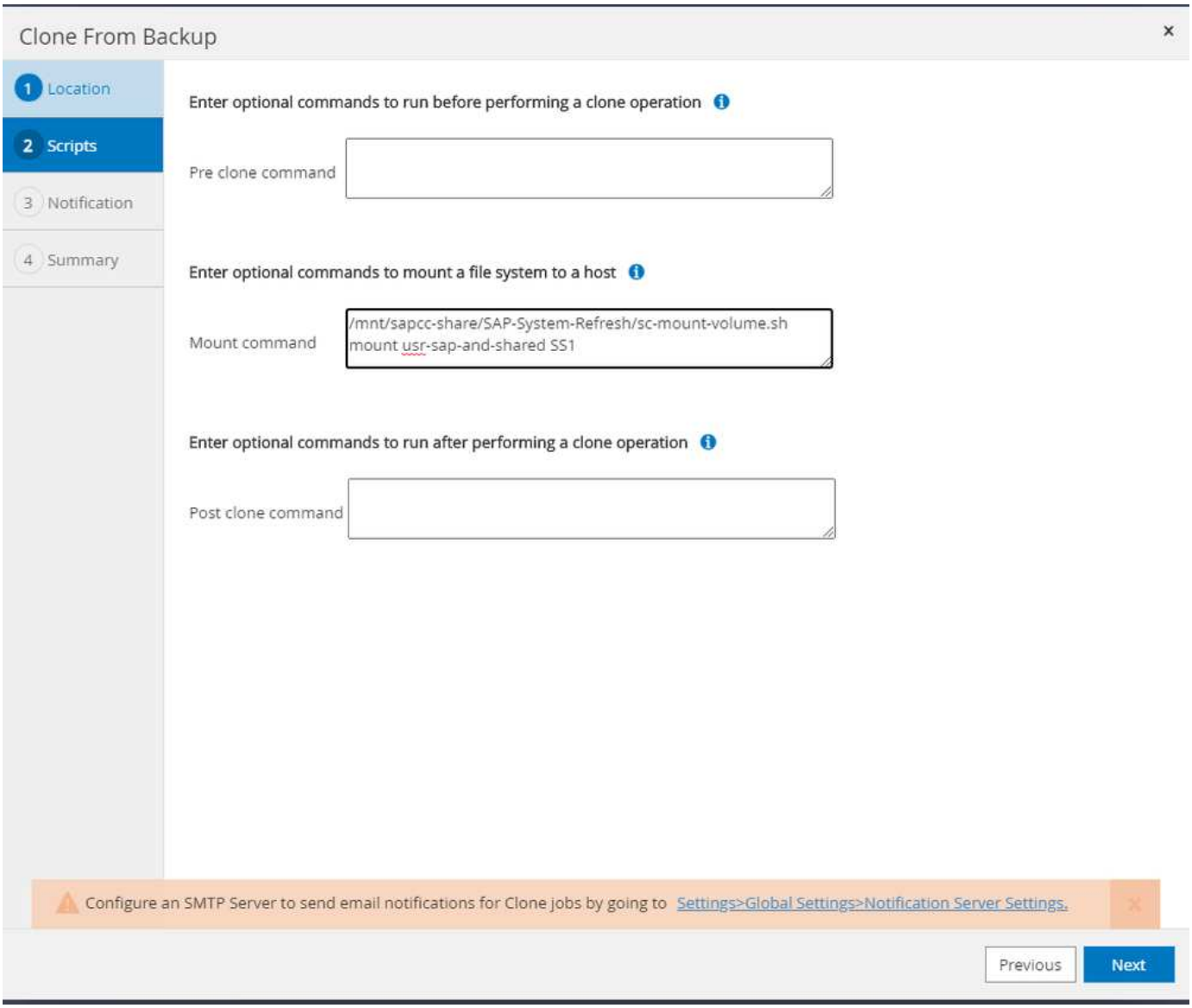


1. Wählen Sie den Host aus, auf dem das Ziel-Reparatursystem vorbereitet wurde. Die NFS-Export-IP-Adresse muss die Speichernetzwerk-Schnittstelle des Ziel-Hosts sein. Als Ziel-SID halten Sie die gleiche SID wie das Quellsystem. In unserem Beispiel SS1.

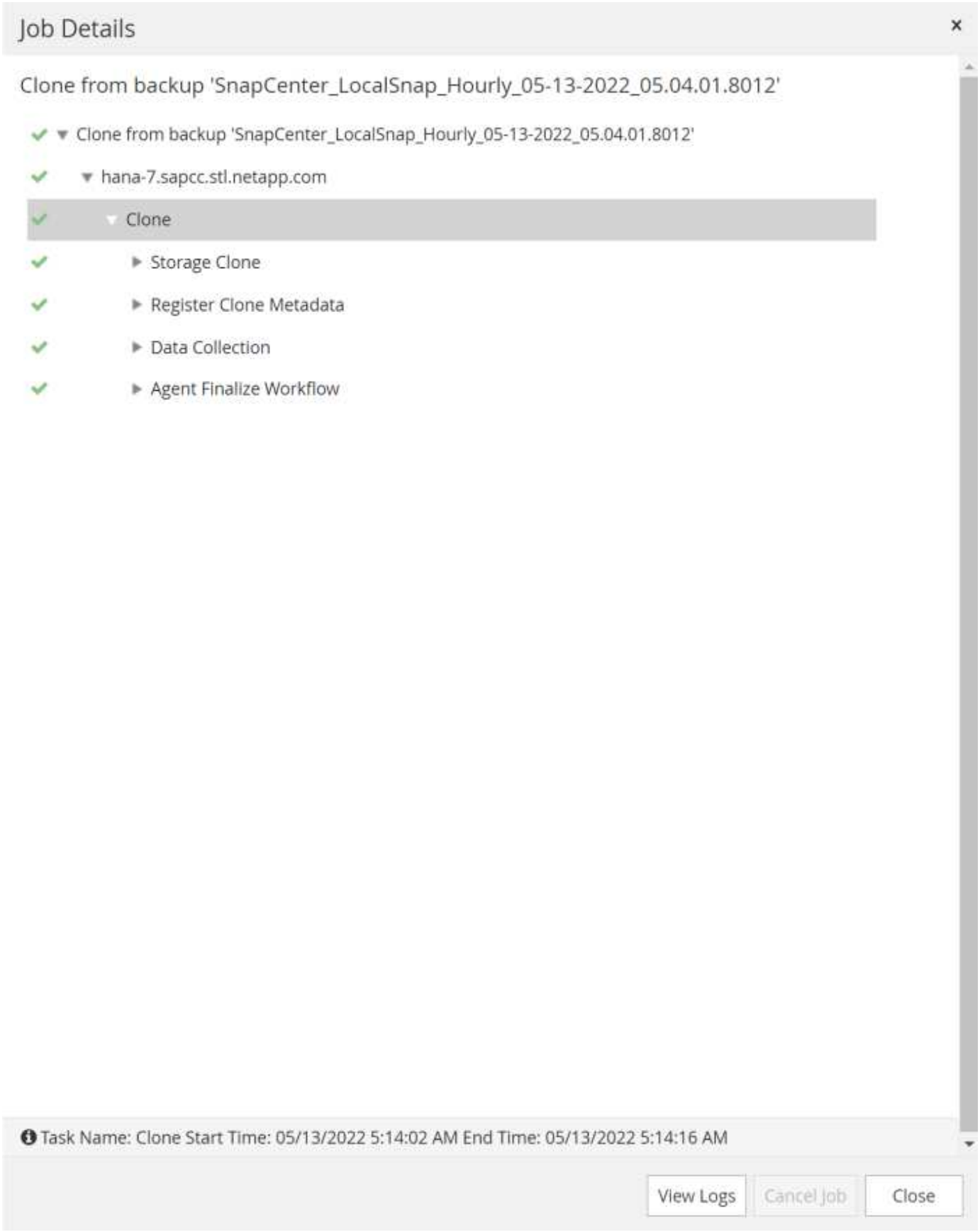


1. Geben Sie das Mount-Skript mit den erforderlichen Befehlszeilenoptionen ein.

Das SAP HANA-System verwendet ein einzelnes Volume sowohl für `/hana/shared` als auch für `/usr/sap/SS1`, getrennt in Unterverzeichnissen, wie im Konfigurationshandbuch empfohlen"SAP HANA auf NetApp AFF Systemen mit NFS". Das Skript `sc-mount-volume.sh` unterstützt diese Konfiguration mit einer speziellen Befehlszeilenoption für den Mount-Pfad. Wenn die Befehlszeilenoption Mount path dem Wert usr-sap-and-shared entspricht, hängt das Skript die freigegebenen Unterverzeichnisse und usr-sap entsprechend im Volume an.



1. Im Bildschirm Jobdetails in SnapCenter wird der Fortschritt des Vorgangs angezeigt.



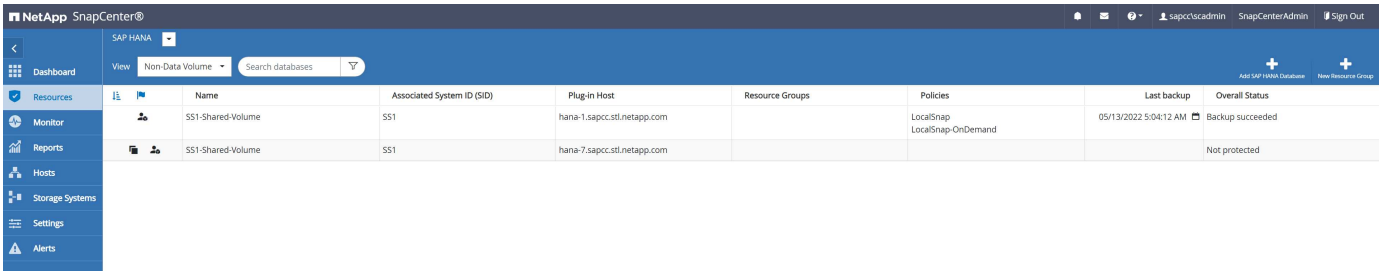
1. Die Logdatei des Skripts sc-mount-volume.sh zeigt die verschiedenen Schritte, die für den Mount-Vorgang ausgeführt werden.

```
20201201041441###hana-1###sc-mount-volume.sh: Adding entry in /etc/fstab.
20201201041441###hana-1###sc-mount-volume.sh:
192.168.175.117://SS1_shared_Clone_05132205140448713/usr-sap /usr/sap/SS1
nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0
0
20201201041441###hana-1###sc-mount-volume.sh: Mounting volume: mount
/usr/sap/SS1.
20201201041441###hana-1###sc-mount-volume.sh:
192.168.175.117:/SS1_shared_Clone_05132205140448713/shared /hana/shared
nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0
0
20201201041441###hana-1###sc-mount-volume.sh: Mounting volume: mount
/hana/shared.
20201201041441###hana-1###sc-mount-volume.sh: usr-sap-and-shared mounted
successfully.
20201201041441###hana-1###sc-mount-volume.sh: Change ownership to ss1adm.
```

1. Nach Abschluss des SnapCenter-Workflows werden die Dateisysteme /usr/sap/SS1 und /hana/shared auf dem Ziel-Host gemountet.

```
hana-1:~ # df
Filesystem 1K-blocks Used Available Use% Mounted on
192.168.175.117:/SS1_repair_log_mnt00001 262144000 320 262143680 1%
/hana/log/SS1/mnt00001
192.168.175.100:/sapcc_share 1020055552 53485568 966569984 6% /mnt/sapcc-
share
192.168.175.117:/SS1_repair_log_backup 104857600 256 104857344 1%
/mnt/log-backup
192.168.175.117:/SS1_shared_Clone_05132205140448713/usr-sap 262144064
10084608 252059456 4% /usr/sap/SS1
192.168.175.117:/SS1_shared_Clone_05132205140448713/shared 262144064
10084608 252059456 4% /hana/shared
```

1. Innerhalb von SnapCenter ist eine neue Ressource für das geklonte Volume sichtbar.



1. Nachdem nun das /hana/Shared Volume verfügbar ist, können die SAP HANA-Services gestartet werden.

```
hana-1:/mnt/sapcc-share/SAP-System-Refresh # systemctl start sapinit
```

1. SAP Host Agent und sapstartsrv Prozesse werden nun gestartet.

```
hana-1:/mnt/sapcc-share/SAP-System-Refresh # ps -ef |grep sap
root 12377 1 0 04:34 ? 00:00:00 /usr/sap/hostctrl/exe/saphostexec
pf=/usr/sap/hostctrl/exe/host_profile
sapadm 12403 1 0 04:34 ? 00:00:00 /usr/lib/systemd/systemd --user
sapadm 12404 12403 0 04:34 ? 00:00:00 (sd-pam)
sapadm 12434 1 1 04:34 ? 00:00:00 /usr/sap/hostctrl/exe/sapstartsrv
pf=/usr/sap/hostctrl/exe/host_profile -D
root 12485 12377 0 04:34 ? 00:00:00 /usr/sap/hostctrl/exe/saphostexec
pf=/usr/sap/hostctrl/exe/host_profile
root 12486 12485 0 04:34 ? 00:00:00 /usr/sap/hostctrl/exe/saposcol -l -w60
pf=/usr/sap/hostctrl/exe/host_profile
ss1adm 12504 1 0 04:34 ? 00:00:00 /usr/sap/SS1/HDB00/exe/sapstartsrv
pf=/usr/sap/SS1/SYS/profile/SS1_HDB00_hana-1 -D -u ss1adm
root 12582 12486 0 04:34 ? 00:00:00 /usr/sap/hostctrl/exe/saposcol -l -w60
pf=/usr/sap/hostctrl/exe/host_profile
root 12585 7613 0 04:34 pts/0 00:00:00 grep --color=auto sap
hana-1:/mnt/sapcc-share/SAP-System-Refresh #
```

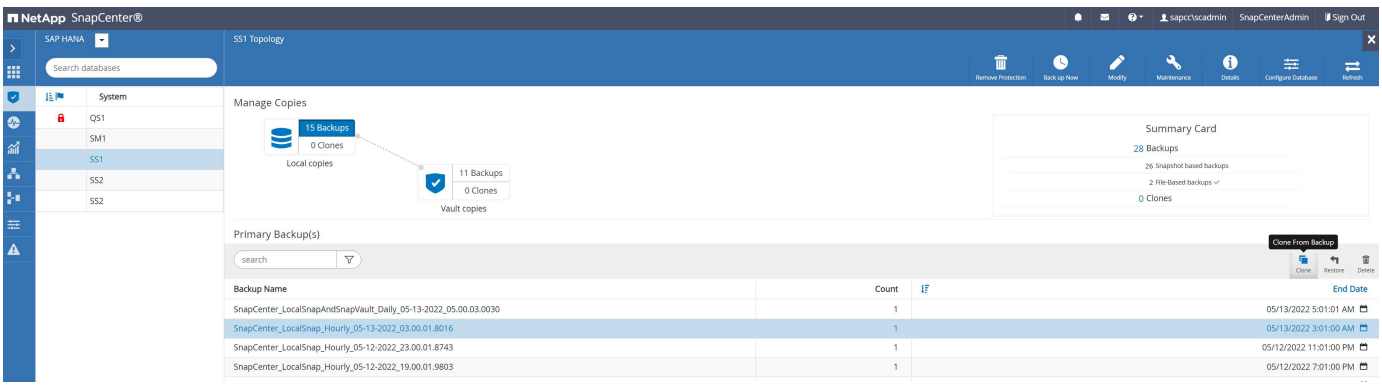
Klonen zusätzlicher SAP Applikationsservices

Weitere SAP Applikationsservices werden auf die gleiche Weise geklont wie das gemeinsam genutzte SAP HANA Volume im Abschnitt „Klonen des SAP HANA Shared Volume“ beschrieben. Natürlich müssen auch die benötigten Storage-Volumes der SAP Applikationsserver mit SnapCenter gesichert werden.

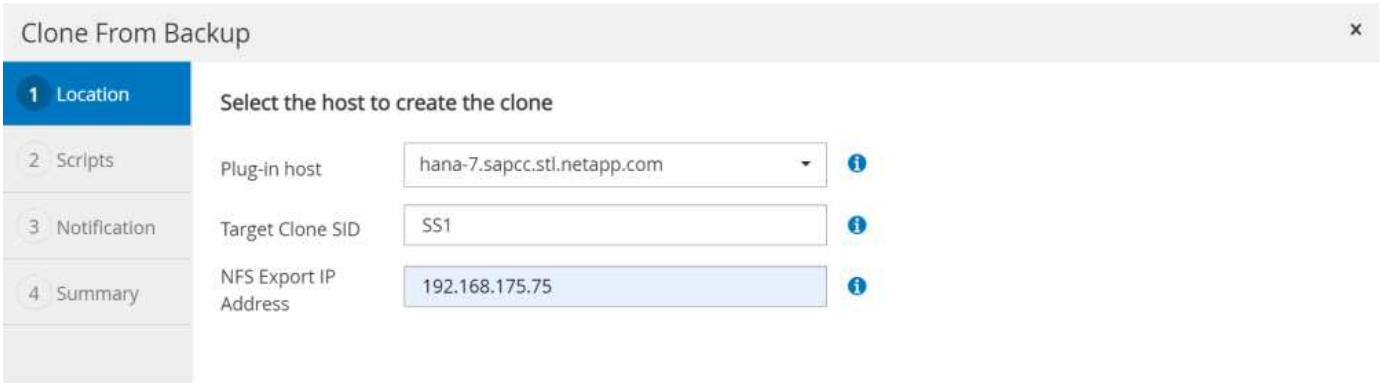
Sie müssen die erforderlichen Diensteinträge zu /usr/sap/sapservices hinzufügen, und die Ports, Benutzer und die Dateisystemeinhängepunkte (z. B. /usr/sap/SID) müssen vorbereitet werden.

Klonen des Daten-Volumes und Recovery der HANA Datenbank

1. Wählen Sie ein SAP HANA Snapshot Backup aus dem Quellsystem SS1.

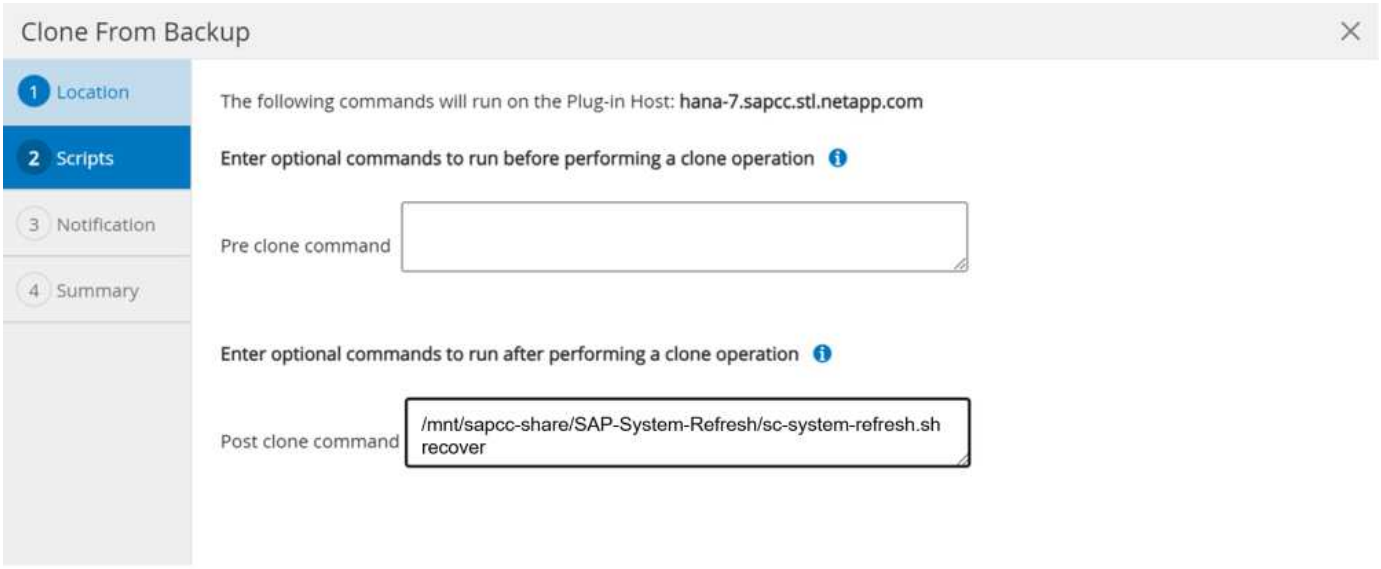


1. Wählen Sie den Host aus, auf dem das Ziel-Reparatursystem vorbereitet wurde. Die NFS-Export-IP-Adresse muss die Speichernetzwerk-Schnittstelle des Ziel-Hosts sein. Als Ziel-SID halten Sie die gleiche SID wie das Quellsystem. In unserem Beispiel SS1

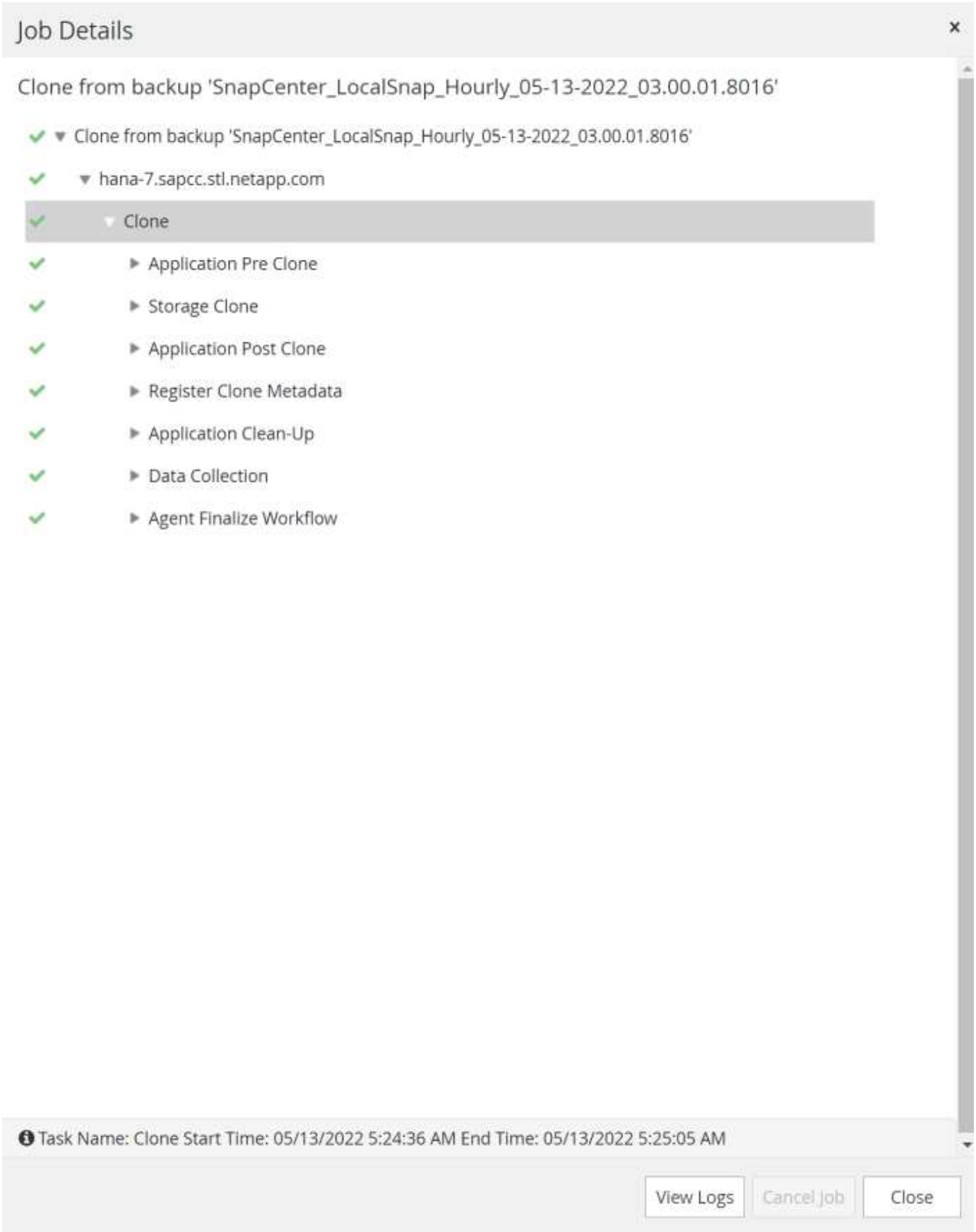


1. Geben Sie die Skripts nach dem Klonen mit den erforderlichen Befehlszeilenoptionen ein.

Das Skript für den Wiederherstellungsvorgang stellt die SAP HANA-Datenbank auf den Zeitpunkt des Snapshot-Vorgangs wieder her und führt keine Forward Recovery aus. Wenn eine Rückführung auf einen bestimmten Zeitpunkt erforderlich ist, muss die Wiederherstellung manuell durchgeführt werden. Eine manuelle vorwärts-Wiederherstellung erfordert außerdem, dass die Protokoll-Backups aus dem Quellsystem auf dem Ziel-Host verfügbar sind.



Der Bildschirm „Jobdetails“ in SnapCenter zeigt den Fortschritt des Vorgangs an.



Die Protokolldatei des `sc-system-refresh` Skripts zeigt die verschiedenen Schritte an, die für den Mount- und Wiederherstellungsvorgang ausgeführt werden.

```
20201201052124###hana-1###sc-system-refresh.sh: Recover system database.
20201201052124###hana-1###sc-system-refresh.sh:
/usr/sap/SS1/HDB00/exe/Python/bin/python
/usr/sap/SS1/HDB00/exe/python_support/recoverSys.py --command "RECOVER
DATA USING SNAPSHOT CLEAR LOG"
20201201052156###hana-1###sc-system-refresh.sh: Wait until SAP HANA
database is started ....
20201201052156###hana-1###sc-system-refresh.sh: Status: GRAY
20201201052206###hana-1###sc-system-refresh.sh: Status: GREEN
20201201052206###hana-1###sc-system-refresh.sh: SAP HANA database is
started.
20201201052206###hana-1###sc-system-refresh.sh: Source system has a single
tenant and tenant name is identical to source SID: SS1
20201201052206###hana-1###sc-system-refresh.sh: Target tenant will have
the same name as target SID: SS1.
20201201052206###hana-1###sc-system-refresh.sh: Recover tenant database
SS1.
20201201052206###hana-1###sc-system-refresh.sh:
/usr/sap/SS1/SYS/exe/hdb/hdbsql -U SS1KEY RECOVER DATA FOR SS1 USING
SNAPSHOT CLEAR LOG
0 rows affected (overall time 34.773885 sec; server time 34.772398 sec)
20201201052241###hana-1###sc-system-refresh.sh: Checking availability of
Indexserver for tenant SS1.
20201201052241###hana-1###sc-system-refresh.sh: Recovery of tenant
database SS1 succesfully finished.
20201201052241###hana-1###sc-system-refresh.sh: Status: GREEN
After the recovery operation, the HANA database is running and the data
volume is mounted at the target host.
hana-1:/mnt/log-backup # df
Filesystem 1K-blocks Used Available Use% Mounted on
192.168.175.117:/SS1_repair_log_mnt00001 262144000 760320 261383680 1%
/hana/log/SS1/mnt00001
192.168.175.100:/sapcc_share 1020055552 53486592 966568960 6% /mnt/sapcc-
share
192.168.175.117:/SS1_repair_log_backup 104857600 512 104857088 1%
/mnt/log-backup
192.168.175.117:/SS1_shared_Clone_05132205140448713/usr-sap 262144064
10090496 252053568 4% /usr/sap/SS1
192.168.175.117:/SS1_shared_Clone_05132205140448713/shared 262144064
10090496 252053568 4% /hana/shared
192.168.175.117:/SS1_data_mnt00001_Clone_0421220520054605 262144064
3732864 258411200 2% /hana/data/SS1/mnt00001
```

Das SAP HANA-System ist jetzt verfügbar und kann beispielsweise als Reparatursystem genutzt werden.

Wo finden Sie weitere Informationen und Versionsverlauf

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten bzw. auf den folgenden Websites:

- "SAP Business Application and SAP HANA Database Solutions (netapp.com)"
- "TR-4614: SAP HANA Backup and Recovery with SnapCenter"
- "TR-4436: SAP HANA on NetApp All Flash FAS Systems with Fibre Channel Protocol"
- "TR-4435: SAP HANA on NetApp All Flash FAS Systems with NFS"
- "TR-4926: SAP HANA auf Amazon FSX für NetApp ONTAP – Backup und Recovery mit SnapCenter"
- "TR-4953: NetApp SAP Landscape Management Integration Using Ansible"
- "TR-4929: SAP-Systemkopien automatisieren mit Libelle SystemCopy (netapp.com)"
- "Automatisieren von SAP Systemkopien sowie Aktualisieren und Klonen von Workflows mit ALPACA und NetApp SnapCenter"
- "Automatisierung von SAP Systemkopien sowie Aktualisierung und Klonen von Workflows mit Avantra und NetApp SnapCenter"

Version	Datum	Versionsverlauf Des Dokuments
Version 1.0	Februar 2018	Erste Version.
Version 2.0	Februar 2021	Vollständige Neufassung betrifft SnapCenter 4.3 und verbesserte Automatisierungsskripts. + Neue Workflow-Beschreibung für Systemaktualisierungen und Systemklonoperationen.
Version 3.0	Mai 2022	Anpassung an geänderte Arbeitsabläufe mit SnapCenter 4.6 P1
Version 4.0	Juli 2024	Dokument deckt NetApp Systeme vor Ort, FSX für ONTAP und Azure NetApp Files + Neue SnapCenter 5.0-Operationen mounten und unmounten während Clone erstellen und löschen Workflows + spezifische Schritte für Fibre Channel SAN hinzugefügt + spezifische Schritte für Azure NetApp Files hinzugefügt + angepasstes und vereinfachtes Skript + enthaltene erforderliche Schritte `sc-system-refresh` für aktiviertes SAP HANA Volume-Verschlüsselung

Automatisierung von SAP-Systemkopievorgängen mit Libelle SystemCopy

TR-4929: Automatisierung von Kopiervorgängen für SAP-Systeme mit Libelle SystemCopy

NetApp Lösungen für die Optimierung des Lifecycle Managements von SAP sind in SAP AnyDBs und SAP HANA Datenbanken integriert. Darüber hinaus integriert NetApp in SAP Lifecycle Management-Tools und kombiniert dabei eine effiziente, applikationsintegrierte Datensicherung mit der flexiblen Bereitstellung von SAP

Testsystemen.

Autoren:

Holger Zecha, Tobias Brandl, NetApp Franz Digruber, Libelle

Im dynamischen Geschäftsumfeld von heute müssen Unternehmen kontinuierlich Innovationen liefern und schnell auf sich ändernde Märkte reagieren. Unter diesen Wettbewerbsbedingungen können sich Unternehmen, die mehr Flexibilität in ihren Arbeitsprozessen implementieren, effektiver an die Marktanforderungen anpassen.

Wechselnde Marktanforderungen betreffen auch die SAP-Umgebungen eines Unternehmens, so dass sie regelmäßige Integrationen, Änderungen und Updates erfordern. DIE IT-Abteilungen müssen diese Veränderungen mit weniger Ressourcen und über kürzere Zeiträume hinweg umsetzen. Die Minimierung des Risikos bei der Implementierung dieser Änderungen erfordert gründliche Tests und Schulungen, für die zusätzliche SAP-Systeme mit tatsächlichen Daten aus der Produktion erforderlich sind.

Herkömmliche Ansätze für das SAP Lifecycle Management zur Bereitstellung dieser Systeme basieren in erster Linie auf manuellen Prozessen. Diese manuellen Prozesse sind oft fehleranfällig und zeitaufwendig, wodurch Innovationen und die Reaktion auf geschäftliche Anforderungen verzögert werden.

NetApp Lösungen für die Optimierung des Lifecycle Managements von SAP sind in SAP AnyDBs und SAP HANA Datenbanken integriert. Darüber hinaus integriert NetApp in SAP Lifecycle Management-Tools und kombiniert dabei eine effiziente, applikationsintegrierte Datensicherung mit der flexiblen Bereitstellung von SAP Testsystemen.

Während diese NetApp Lösungen das Problem der effizienten Verwaltung riesiger Datenmengen selbst bei den größten Datenbanken lösen, müssen umfassende SAP Systeme kopiert und aktualisiert werden. Dazu müssen Pre- und Post-Copy-Aktivitäten gehören, um die Identität des Quell-SAP Systems vollständig zum Zielsystem zu ändern. SAP beschreibt die erforderlichen Aktivitäten in ihrem "Leitfaden zur Erstellung einer homogenen SAP Systemkopie". Um die Anzahl manueller Prozesse weiter zu reduzieren und die Qualität und Stabilität eines SAP-Systemkopiervorgangs zu verbessern, ist unser Partner "Libelle" Hat das entwickelt "Libelle SystemCopy (LSC)" Werkzeug. Wir haben gemeinsam mit Libelle die NetApp Lösungen für SAP Systemkopien in LSC integriert, um die Bereitstellung zu ermöglichen "Vollständige, automatisierte Systemkopien in Rekordzeit".

Applikationsintegrierter Snapshot-Kopiervorgang

Die Fähigkeit, applikationskonsistente NetApp Snapshot Kopien auf der Storage-Ebene zu erstellen, ist die Grundlage für die in diesem Dokument beschriebenen Systemkopievorgänge und Systemklonvorgänge. Storage-basierte Snapshot Kopien werden mit dem NetApp SnapCenter Plug-in für SAP HANA oder mit allen Datenbanken auf nativen NetApp ONTAP Systemen oder mit dem erstellt "Microsoft Azure Applikations-konsistentes Snapshot Tool" (AzAcSnap) und Schnittstellen, die von der SAP HANA- und Oracle-Datenbank in Microsoft Azure bereitgestellt werden. Bei Verwendung von SAP HANA registrieren SnapCenter und AzACSnap Snapshot Kopien im SAP HANA Backup-Katalog, damit die Backups für Restore und Recovery sowie für Klonvorgänge verwendet werden können.

Externe Backups und/oder Disaster Recovery-Datenreplizierung

Applikationskonsistente Snapshot Kopien können auf der Storage-Ebene an einem externen Backup-Standort oder an einem Disaster Recovery-Standort repliziert werden, der von SnapCenter vor Ort gesteuert wird. Die Replizierung basiert auf Blockänderungen und ist somit Platz- und Bandbreiteneffizient. Dieselbe Technologie ist für SAP HANA und Oracle Systeme verfügbar, die in Azure mit Azure NetApp Files ausgeführt werden. Dazu wird die CRR-Funktion (Cross Region Replication) verwendet, um Azure NetApp Files Volumes effizient zwischen Azure Regionen zu replizieren.

Beliebige Snapshot Kopien für SAP Systemkopien oder Klonvorgänge verwenden

Dank der NetApp Technologie und Software-Integration können Sie jede Snapshot Kopie eines Quellsystems für eine SAP-Systemkopie oder einen Klonvorgang verwenden. Diese Snapshot Kopie kann entweder aus demselben Storage ausgewählt werden, der in den SAP Produktionssystemen verwendet wird, dem Storage für externe Backups (wie Azure NetApp Files Backup in Azure) oder dem Storage am Disaster-Recovery-Standort (Azure NetApp Files CRR Ziel-Volumes). Dank dieser Flexibilität können Entwicklungs- und Testsysteme bei Bedarf von der Produktion getrennt werden. Außerdem werden weitere Szenarien abgedeckt, zum Beispiel Disaster Recovery-Tests am Disaster Recovery-Standort.

Automatisierung mit Integration

Es gibt verschiedene Szenarien und Anwendungsfälle für die Bereitstellung von SAP-Testsystemen. Dabei gibt es möglicherweise auch unterschiedliche Anforderungen an den Automatisierungsgrad. NetApp Softwareprodukte für SAP können in Datenbank- und Lifecycle-Management-Produkte von SAP und anderen Anbietern (z. B. Libelle) integriert werden, um verschiedene Szenarien und Automatisierungsstufen zu unterstützen.

NetApp SnapCenter mit dem Plug-in für SAP HANA und SAP AnyDBs oder AzSnap auf Azure werden verwendet, um die erforderlichen Storage-Volume-Klone auf Basis einer applikationskonsistenten Snapshot-Kopie bereitzustellen und alle erforderlichen Host- und Datenbankvorgänge bis zu einer starteten SAP Datenbank auszuführen. Je nach Anwendungsfall können SAP Systemkopien, Systemklone, Systemaktualisierung oder zusätzliche manuelle Schritte wie die SAP Nachbearbeitung erforderlich sein. Weitere Informationen werden im nächsten Abschnitt behandelt.

Eine vollständig automatisierte End-to-End-Bereitstellung bzw. -Aktualisierung von SAP-Testsystemen kann mithilfe von Libelle SystemCopy (LSC)-Automatisierung durchgeführt werden. Die Integration von SnapCenter oder AzACSnap in LSC wird in diesem Dokument genauer beschrieben.

Libelle SystemCopy

Libelle SystemCopy ist eine Framework-basierte Softwarelösung zur Erstellung vollständig automatisierter System- und Landschaftskopien. Mit dem sprichwörtlichen Tastendruck können QS- und Testsysteme mit frischen Produktionsdaten aktualisiert werden. Libelle SystemCopy unterstützt alle herkömmlichen Datenbanken und Betriebssysteme und bietet eigene Kopiermechanismen für alle Plattformen. Zugleich sind aber auch Backup/Restore-Verfahren oder Storage-Tools wie NetApp Snapshot Kopien und NetApp FlexClone Volumes integriert. Die während einer Systemkopie erforderlichen Aktivitäten werden von außerhalb des SAP ABAP-Stacks gesteuert. Auf diese Weise sind in den SAP-Anwendungen keine Transporte oder andere Änderungen erforderlich. Im Allgemeinen können alle Schritte, die zum erfolgreichen Abschluss eines Systemkopiervorgangs erforderlich sind, in vier Schritte unterteilt werden:

- **Prüfphase.** Überprüfen Sie die beteiligten Systemumgebungen.
- **Vorphase.** Vorbereiten Sie das Zielsystem auf eine Systemkopie vor.
- **Kopierungsphase.** Geben Sie eine Kopie der eigentlichen Produktionsdatenbank dem Zielsystem aus der Quelle an.
- **Postphase.** Alle Aufgaben nach der Kopie, um das homogene Kopierverfahren abzuschließen und ein aktualisiertes Zielsystem bereitzustellen.

Während der Kopieerstellung wird die NetApp Snapshot und FlexClone Funktion verwendet, um selbst bei den größten Datenbanken die benötigte Zeit auf ein paar Minuten zu minimieren.

In den Phasen Check, Pre und Post sind bei LSC über 450 vorkonfigurierte Aufgaben zu 95 % der typischen Aktualisierungsvorgänge verfügbar. LSC nutzt daher Automatisierung nach SAP-Standards. Dank der Software-definierten Art von LSC können Systemaktualisierungsprozesse einfach angepasst und erweitert

werden, um den spezifischen Anforderungen von SAP-Umgebungen des Kunden gerecht zu werden.

Anwendungsfälle für SAP-Systemaktualisierung und Klonen

Es gibt verschiedene Szenarien, in denen Daten aus einem Quellsystem für ein Zielsystem verfügbar gemacht werden müssen:

- Regelmäßige Aktualisierung der Qualitätssicherungs- sowie Test- und Trainingssysteme
- Erstellung von Umgebungen zur Fehlerbehebung oder Reparatur von Systemumgebungen, um das Problem der logischen Beschädigung zu beheben
- Szenarien für Disaster Recovery-Tests

Obwohl Reparatursysteme und Disaster Recovery-Testsysteme in der Regel mit SAP-Systemklonen (die keine umfangreichen Nachbearbeitungsvorgänge erfordern) für aktualisierte Test- und Trainingssysteme bereitgestellt werden, müssen diese Nachbearbeitungsschritte angewendet werden, um die Koexistenz mit dem Quellsystem zu ermöglichen. Daher legt der Schwerpunkt dieses Dokuments auf Szenarien zur Systemaktualisierung von SAP. Nähere Informationen zu den verschiedenen Anwendungsfällen finden sich im technischen Bericht"TR-4667: Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter".

Der Rest dieses Dokuments ist in zwei Teile unterteilt. Im ersten Teil wird die Integration von NetApp SnapCenter in Libelle SystemCopy für SAP HANA sowie in SAP AnyDBs Systeme beschrieben, die On-Premises auf NetApp ONTAP Systemen ausgeführt werden. Der zweite Teil beschreibt die Integration von AzAcSnap mit LSC für SAP HANA-Systeme in Microsoft Azure mit bereitgestellten Azure NetApp Files. Obwohl die ONTAP-Grundlegungstechnologie identisch ist, bietet Azure NetApp Files im Vergleich zur nativen ONTAP-Installation unterschiedliche Schnittstellen und Tool-Integration (z. B. AzAcSnap).

Systemaktualisierung für SAP HANA mit LSC und SnapCenter

Dieser Abschnitt beschreibt die Integration von LSC in NetApp SnapCenter. Die Integration von LSC und SnapCenter unterstützt alle von SAP unterstützten Datenbanken. Dennoch müssen wir zwischen SAP AnyDBs und SAP HANA unterscheiden, da SAP HANA einen zentralen Kommunikations-Host bietet, der für SAP AnyDBs nicht verfügbar ist.

Die Standard-SnapCenter-Agent- und Datenbank-Plug-in-Installation für SAP AnyDBs ist neben dem entsprechenden Datenbank-Plug-in eine lokale Installation vom SnapCenter-Agent.

In diesem Abschnitt wird die Integration zwischen LSC und SnapCenter anhand einer SAP HANA-Datenbank als Beispiel beschrieben. Wie bereits erwähnt, gibt es für SAP HANA zwei verschiedene Optionen für die Installation des SnapCenter Agent und SAP HANA Datenbank-Plug-ins:

- **Ein Standard-SnapCenter-Agent und SAP HANA-Plugin-Installation.** in einer Standardinstallation werden der SnapCenter-Agent und das SAP HANA-Plug-in lokal auf dem SAP HANA-Datenbankserver installiert.
- **Eine SnapCenter-Installation mit zentralem Kommunikationshost.** ein zentraler Kommunikationhost wird mit dem SnapCenter-Agent, dem SAP HANA-Plug-in und dem HANA-Datenbankclient installiert, der alle datenbankbezogenen Operationen verarbeitet, die zum Sichern und Wiederherstellen einer SAP HANA-Datenbank für mehrere SAP HANA-Systeme in der Landschaft erforderlich sind. Daher muss ein zentraler Kommunikationshost kein vollständiges SAP HANA Datenbanksystem installieren.

Weitere Informationen zu diesen verschiedenen SnapCenter-Agenten und den Installationsoptionen für das

SAP HANA-Datenbank-Plug-in finden Sie im technischen Bericht "TR-4614: SAP HANA Backup und Recovery mit SnapCenter".

In den folgenden Abschnitten werden die Unterschiede zwischen der Integration von LSC in SnapCenter unter Verwendung der Standardinstallation oder des zentralen Kommunikations-Hosts deutlich. Insbesondere sind alle nicht hervorgehobenen Konfigurationsschritte unabhängig von der Installationsoption und der verwendeten Datenbank identisch.

Um ein automatisches Backup auf Basis von Snapshot Kopien aus der Quelldatenbank durchzuführen und einen Klon für die neue Zieldatenbank zu erstellen, verwendet die beschriebene Integration zwischen LSC und SnapCenter die in beschriebenen Konfigurationsoptionen und Skripte"TR-4667: Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter".

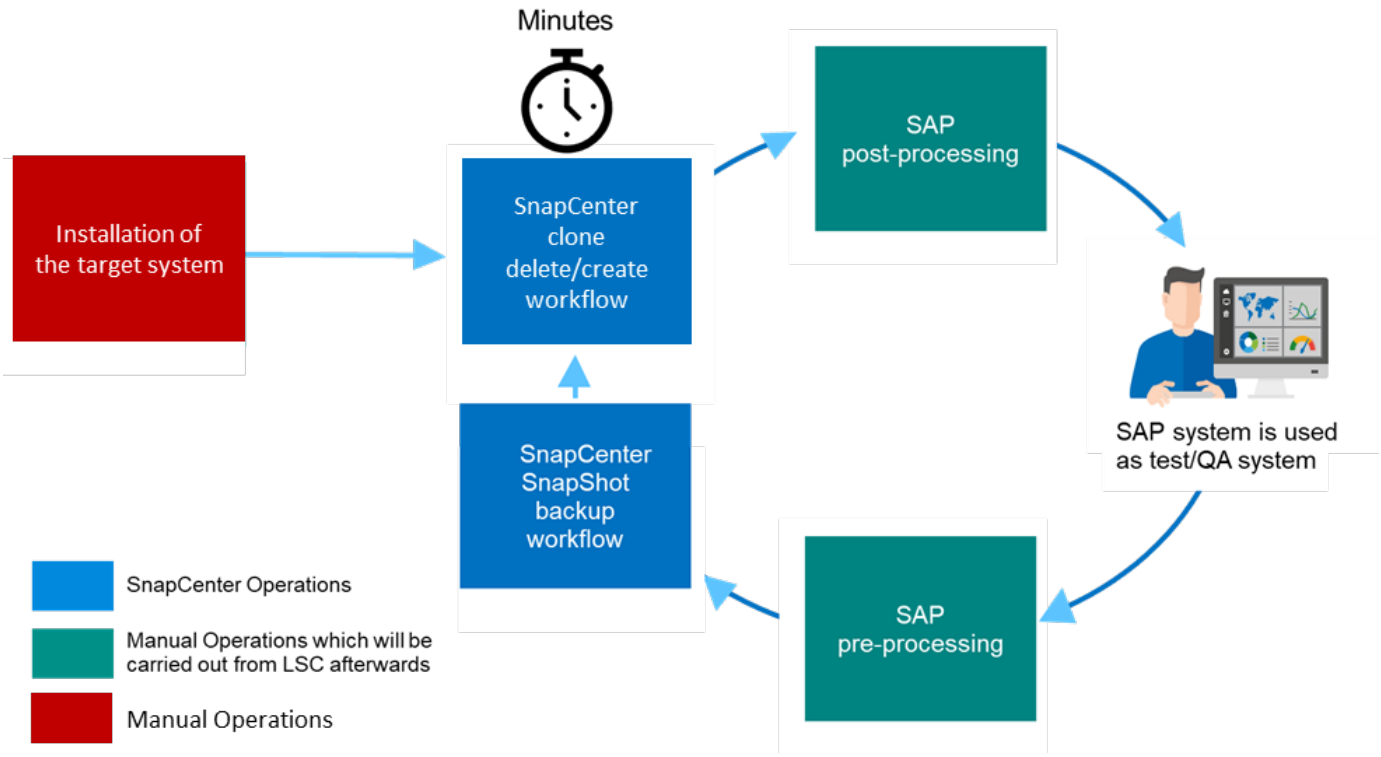
Überblick

Die folgende Abbildung zeigt einen typischen grundlegenden Workflow für eine Aktualisierung eines SAP Systems mit SnapCenter ohne LSC:

1. Einmalige, erstmalige Installation und Vorbereitung des Zielsystems.
2. Manuelle Vorverarbeitung (Exportieren von Lizenzen, Benutzern, Druckern usw.).
3. Falls erforderlich, wird ein bereits vorhandener Klon auf dem Zielsystem gelöscht.
4. Das Klonen einer vorhandenen Snapshot-Kopie des Quellsystems auf das von SnapCenter durchgeführte Zielsystem.
5. Manuelle SAP-Nachbearbeitung (Importieren von Lizenzen, Benutzern, Druckern, Deaktivieren von Batch-Jobs usw.)
6. Das System kann dann als Test- oder QA-System verwendet werden.
7. Wenn eine neue Systemaktualisierung angefordert wird, wird der Workflow mit Schritt 2 neu gestartet.

SAP-Kunden wissen, dass die manuellen Schritte in der Abbildung unten grün dargestellt sind zeitaufwändig und fehleranfällig sind. Beim Einsatz von LSC- und SnapCenter-Integration werden diese manuellen Schritte mit LSC zuverlässig und wiederholbar mit allen notwendigen Protokollen für interne und externe Audits durchgeführt.

Die folgende Abbildung bietet einen Überblick über die allgemeine SnapCenter-basierte Aktualisierung von SAP Systemen.



Voraussetzungen und Einschränkungen

Folgende Voraussetzungen müssen erfüllt sein:

- SnapCenter muss installiert sein. Das Quell- und Zielsystem muss in SnapCenter konfiguriert sein, entweder in einer Standardinstallation oder über einen zentralen Kommunikations-Host. Snapshot Kopien können auf dem Quellsystem erstellt werden.
- Das Speicher-Back-End muss in SnapCenter ordnungsgemäß konfiguriert werden, wie im Bild unten dargestellt.

Die nächsten beiden Images decken die Standardinstallation ab, in der der SnapCenter-Agent und das SAP HANA-Plug-in lokal auf jedem Datenbankserver installiert werden.

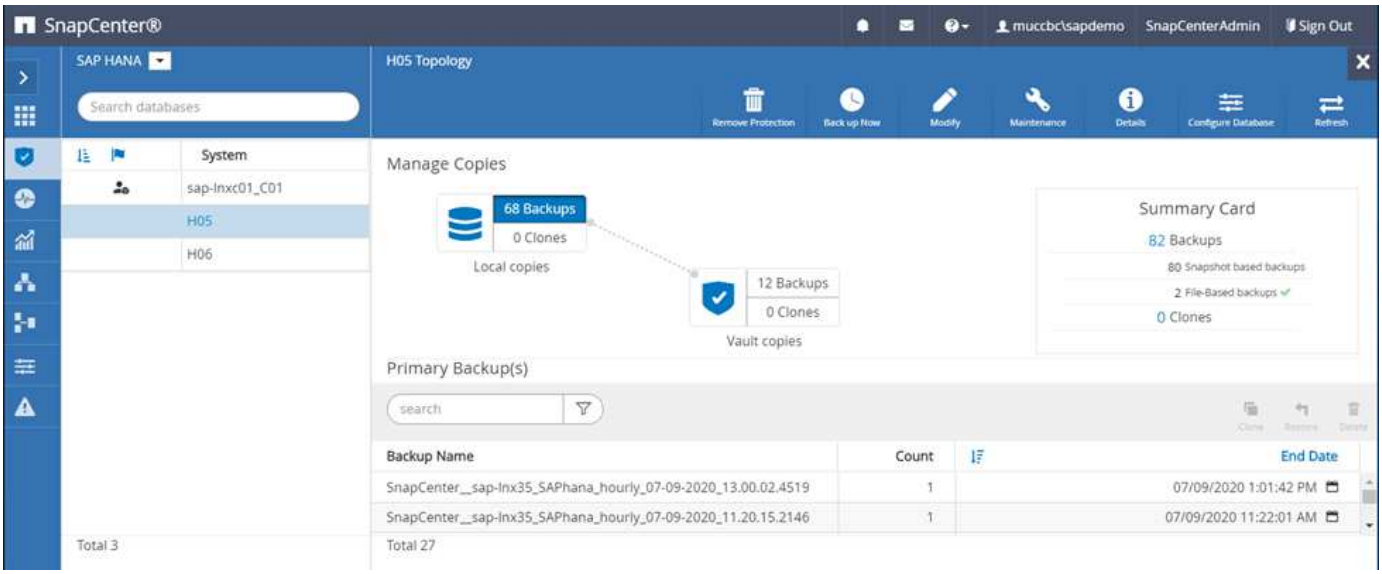
Der SnapCenter Agent und das entsprechende Datenbank-Plug-in müssen in der Quelldatenbank installiert sein.

Der SnapCenter-Agent und das entsprechende Datenbank-Plug-in müssen auf der Zieldatenbank installiert sein.

Das folgende Bild porträtiert die zentrale Kommunikations-Host-Bereitstellung, in der der SnapCenter-Agent, das SAP HANA Plug-in und der SAP HANA-Datenbank-Client auf einem zentralen Server (wie z.B. SnapCenter-Server) installiert werden, um mehrere SAP HANA-Systeme in der Landschaft zu verwalten.

Auf dem zentralen Kommunikations-Host müssen der SnapCenter Agent, das SAP HANA Datenbank-Plug-in und der HANA Datenbank-Client installiert sein.

Das Backup für die Quelldatenbank muss in SnapCenter ordnungsgemäß konfiguriert werden, damit die Snapshot Kopie erfolgreich erstellt werden kann.



Der LSC-Master und der LSC-Worker müssen in der SAP-Umgebung installiert sein. In dieser Bereitstellung haben wir außerdem den LSC-Master auf dem SnapCenter-Server und den LSC-Worker auf dem Ziel-SAP-Datenbankserver installiert, der aktualisiert werden sollte. Weitere Einzelheiten finden Sie im folgenden Abschnitt „Laboreinrichtung.“

Dokumentationsressourcen:

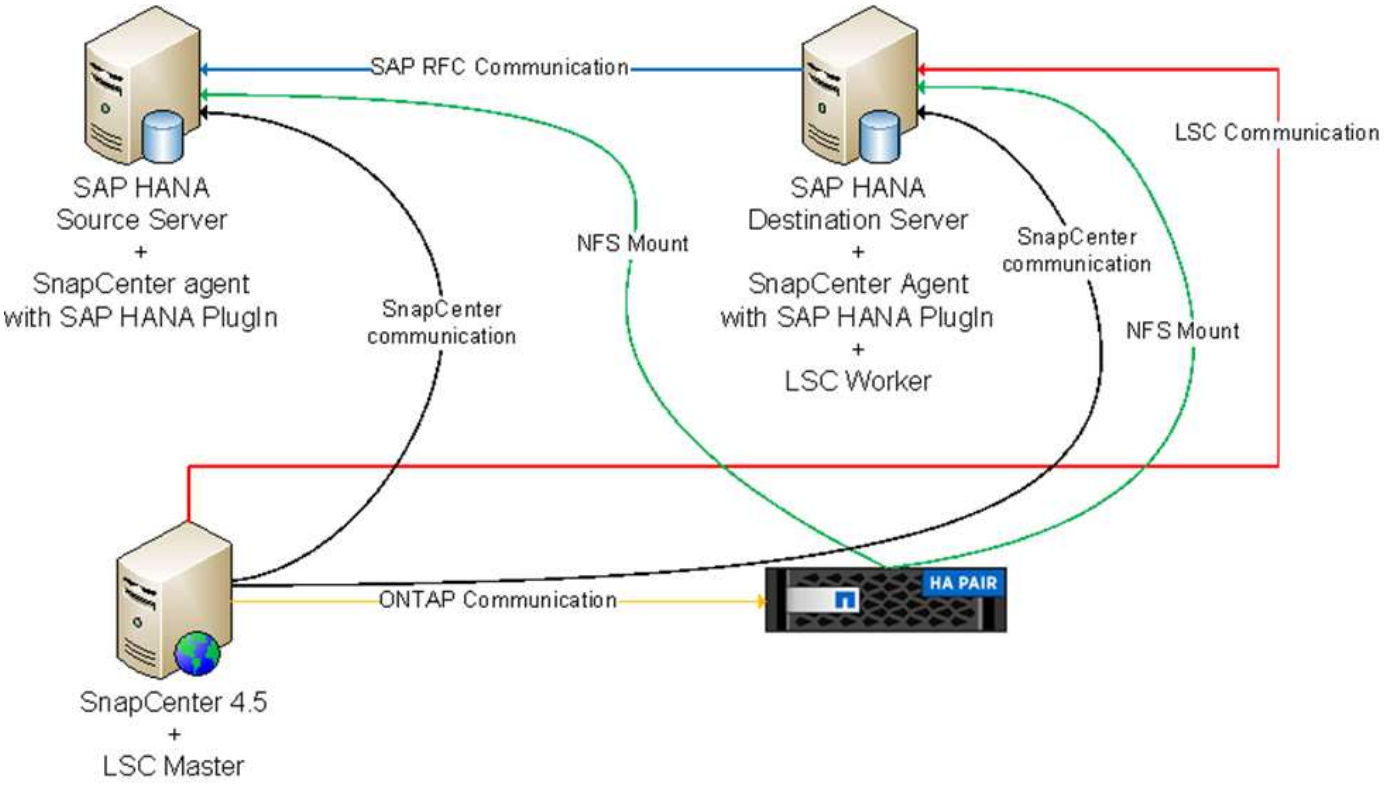
- "SnapCenter Documentation Center"
- "TR-4700: SnapCenter Plug-in für Oracle Database"
- "TR-4614: SAP HANA Backup and Recovery with SnapCenter"
- "TR-4667: Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter"
- "TR-4769 -SnapCenter Best Practices und Sizing Guidelines"
- "SnapCenter 4.6 Cmdlet Referenzhandbuch"

Laboreinrichtung

In diesem Abschnitt wird eine Beispielarchitektur beschrieben, die in einem Demo-Datacenter eingerichtet wurde. Das Setup wurde in eine Standardinstallation und eine Installation über einen zentralen Kommunikations-Host unterteilt.

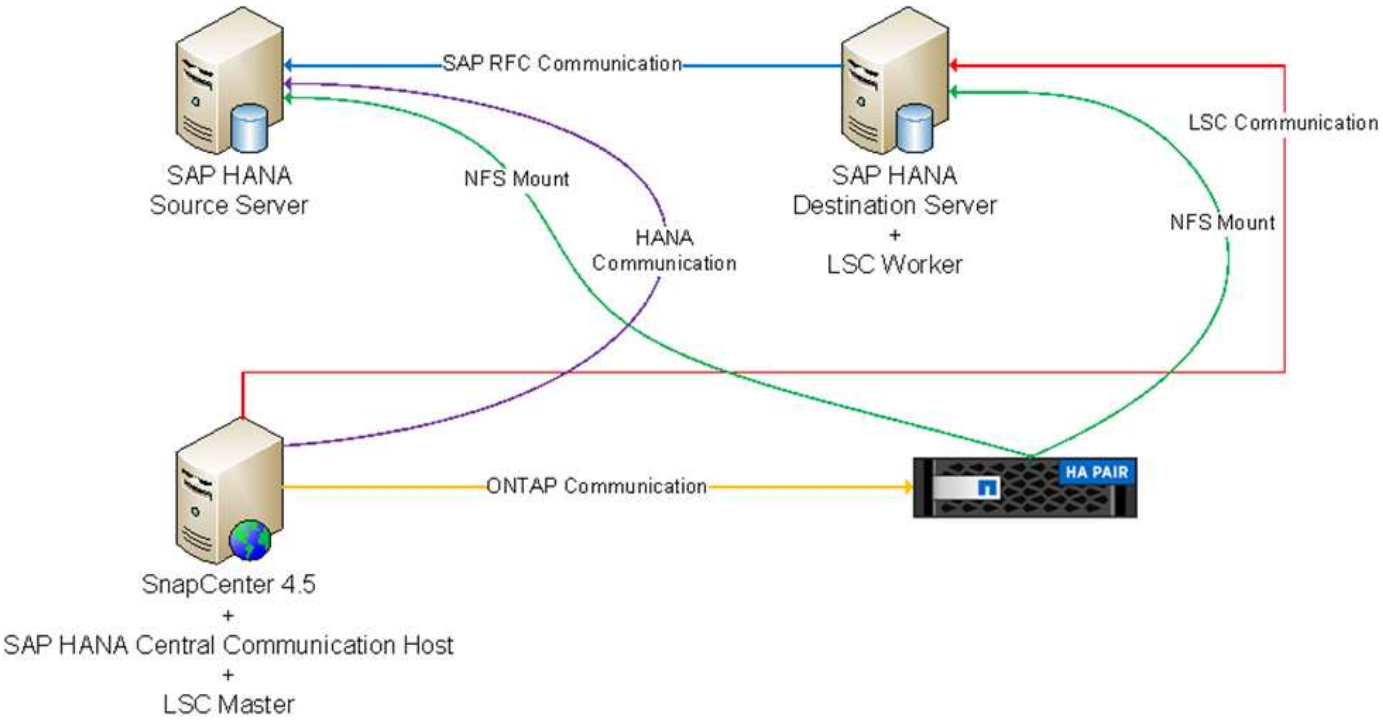
Standardinstallation

Die folgende Abbildung zeigt eine Standardinstallation, bei der der SnapCenter Agent zusammen mit dem Datenbank-Plug-in lokal auf dem Quell- und dem Ziel-Datenbankserver installiert wurde. Im Lab-Setup wurde das SAP HANA-Plug-in installiert. Außerdem wurde der LSC-Worker auch auf dem Zielserver installiert. Zur Vereinfachung und zur Verringerung der Anzahl der virtuellen Server haben wir den LSC-Master auf dem SnapCenter-Server installiert. Die Kommunikation zwischen den verschiedenen Komponenten ist in der folgenden Abbildung dargestellt.



Zentraler Kommunikationshost

Die folgende Abbildung zeigt die Einrichtung über einen zentralen Kommunikations-Host. In dieser Konfiguration wurde der SnapCenter Agent zusammen mit dem SAP HANA Plug-in und dem HANA Datenbank-Client auf einem dedizierten Server installiert. Bei diesem Setup wurde der zentrale Kommunikations-Host mit dem SnapCenter-Server installiert. Darüber hinaus wurde der LSC-Mitarbeiter wieder auf dem Zielserver installiert. Zur Vereinfachung und zur Verringerung der Anzahl der virtuellen Server haben wir uns entschieden, auch den LSC-Master auf dem SnapCenter-Server zu installieren. Die Kommunikation zwischen den verschiedenen Komponenten ist in der Abbildung unten dargestellt.



Erste Schritte zur Einmaligen Vorbereitung für Libelle SystemCopy

Es gibt drei Hauptkomponenten einer LSC-Installation:

- **LSC-Master.** wie der Name schon sagt, ist dies die Master-Komponente, die den automatischen Workflow einer Libelle-basierten Systemkopie steuert. In der Demo-Umgebung wurde der LSC-Master auf dem SnapCenter-Server installiert.
- **LSC Worker.** ein LSC-Mitarbeiter ist Teil der Libelle-Software, die in der Regel auf dem Ziel-SAP-System läuft und die Skripte ausführt, die für die automatisierte Systemkopie erforderlich sind. In der Demo-Umgebung wurde der LSC-Mitarbeiter auf dem Ziel-SAP HANA-Anwendungsserver installiert.
- **LSC-Satellit.** ein LSC-Satellit ist Teil der Libelle-Software, die auf einem Drittanbieter-System läuft, auf dem weitere Skripte ausgeführt werden müssen. Gleichzeitig kann der LSC-Master auch die Rolle eines LSC-Satellitensystems erfüllen.

Wir haben zunächst alle beteiligten Systeme im LSC definiert, wie in der folgenden Abbildung dargestellt:

- **172.30.15.35.** die IP-Adresse des SAP-Quellsystems und des SAP HANA-Quellsystems.
- **172.30.15.3.** die IP-Adresse des LSC-Master und des LSC-Satellitensystems für diese Konfiguration. Da wir das LSC-Master auf dem SnapCenter-Server installiert haben, sind die SnapCenter 4.x PowerShell Cmdlets auf diesem Windows Host bereits verfügbar, da sie während der Installation des SnapCenter-Servers installiert wurden. Wir haben also beschlossen, die LSC-Satellitenrolle für dieses System zu aktivieren und alle SnapCenter PowerShell Cmdlets auf diesem Host auszuführen. Wenn Sie ein anderes System verwenden, stellen Sie sicher, dass Sie die SnapCenter PowerShell Commandlets auf diesem Host gemäß der Dokumentation zu SnapCenter installieren.
- **172.30.15.36.** die IP-Adresse des SAP-Zielsystems, des SAP HANA-Zielsystems und des LSC-Mitarbeiters.

Anstelle von IP-Adressen können auch Host-Namen oder vollqualifizierte Domain-Namen verwendet werden.

Das folgende Bild zeigt die LSC-Konfiguration des Master-, Worker-, Satelliten-, SAP-Quellsystems-, SAP-Zielsystems, Quelldatenbank und Zieldatenbank.

System Identifier	Worker	Source SAP	Source Database	Target SAP	Target Database	Satellite System
172.30.15.35		☑	☑	☐	☐	☐
172.30.15.3	172.30.15.3:9000	☐	☐	☐	☐	☑
172.30.15.36	172.30.15.36:9000	☐	☐	☑	☑	☐

Für die Hauptintegration müssen die Konfigurationsschritte wieder in die Standardinstallation und die Installation über einen zentralen Kommunikations-Host getrennt werden.

Standardinstallation

In diesem Abschnitt werden die Konfigurationsschritte beschrieben, die bei einer Standardinstallation erforderlich sind, bei der der SnapCenter-Agent und das erforderliche Datenbank-Plug-in auf den Quell- und Zielsystemen installiert sind. Bei Verwendung einer Standardinstallation werden alle Aufgaben ausgeführt, die zum Mounten des Klon-Volumes sowie zur Wiederherstellung des Zielsystems erforderlich sind, vom SnapCenter Agent, der auf dem Zieldatenbanksystem auf dem Server selbst ausgeführt wird. Hiermit können Sie auf alle Details zum Klonen zugreifen, die über Umgebungsvariablen vom SnapCenter Agent zur Verfügung stehen. Daher müssen Sie nur eine weitere Aufgabe in der LSC-Kopiephase erstellen. Diese Aufgabe führt den Snapshot-Kopiervorgang auf dem Quellsystem sowie den Klon- und Wiederherstellungsprozess auf dem Zieldatenbanksystem durch. Alle Aufgaben im Zusammenhang mit SnapCenter werden mithilfe eines PowerShell Skripts ausgelöst, das in die LSC-Aufgabe eingegeben wird `NTAP_SYSTEM_CLONE`.

Das folgende Bild zeigt die Konfiguration von LSC-Tasks in der Kopierphase.

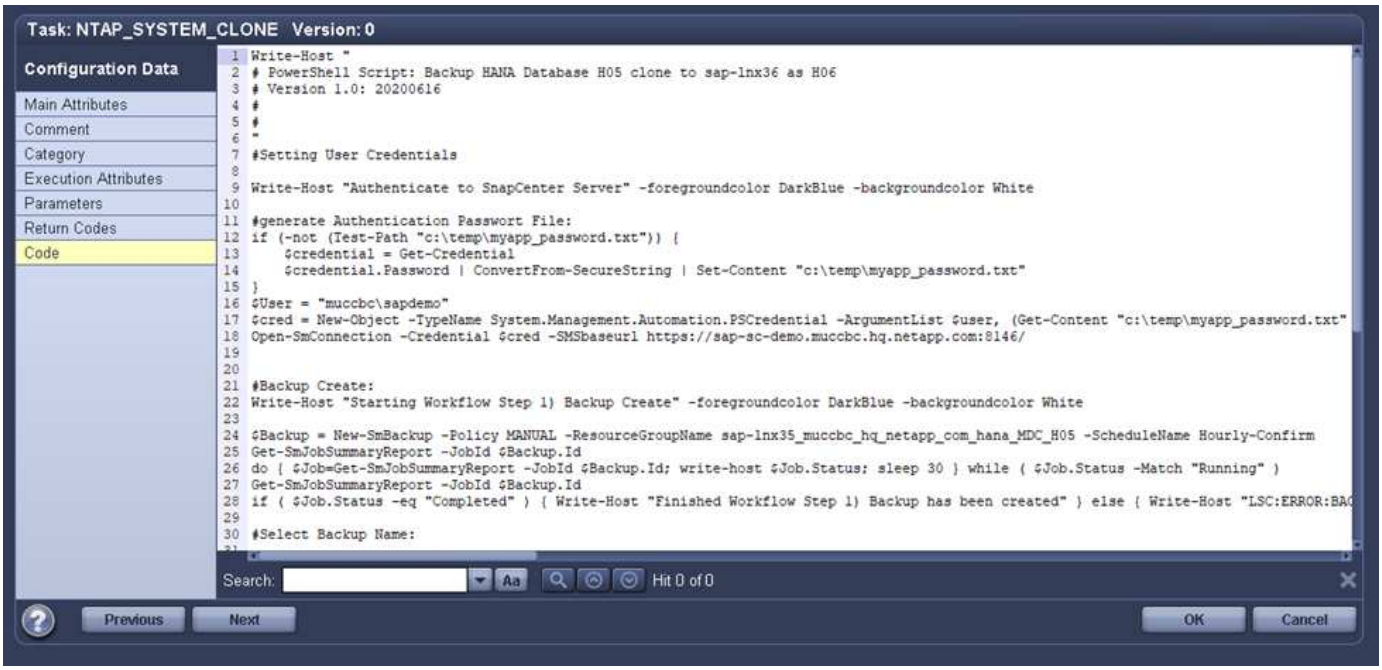
	copy	Copy Phase		phase
	copy 1	NTAP_SYSTEM_CLONE	NetApp SnapShot and Clone	psh
	copy 2	*NTAP_SYSTEM_CLONE_CP*	*NetApp SnapShot and Clone*	*psh*
	copy 3	*NTAP_MNT_RECOVER_CP*	*Mount Volume and Recover HANA Database*	*cmd*
	copy 4	*LPDBBCKP*	*Backup Source DB in Filesystem*	*lsh*
	copy 5	*LPDBCPYFLS*	*Copy DB Backup Files From Source to Target System*	*lsh*
	copy 6	*LTDBRESTORE*	*Restore DB Files*	*lsh*
	copy 7	*LTDBRESTORE_TENANT*	*Restore DB Files for Tenant Database*	*lsh*
	post	Post Phase		phase

Die folgende Abbildung zeigt die Konfiguration des `NTAP_SYSTEM_CLONE` Prozess. Da Sie ein PowerShell-Skript ausführen, wird dieses Windows PowerShell-Skript auf dem Satellitensystem ausgeführt. In diesem Fall ist dies der SnapCenter-Server mit dem installierten LSC-Master, der auch als Satellitensystem fungiert.

Da LSC bekannt sein muss, ob die Snapshot Kopie, das Klonen und der Recovery-Vorgang erfolgreich waren, müssen Sie mindestens zwei Rückgabecodetypen definieren. Ein Code dient zur erfolgreichen Ausführung des Skripts und der andere Code dient zur fehlgeschlagenen Ausführung des Skripts, wie in der folgenden Abbildung dargestellt.

- `LSC:OK` Wenn die Ausführung erfolgreich war, muss vom Skript in die Standardausführung geschrieben werden.
- `LSC:ERROR` Muss vom Skript in die Standardausführung geschrieben werden, wenn die Ausführung fehlgeschlagen ist.

Das folgende Bild zeigt einen Teil des PowerShell-Skripts, das ausgeführt werden muss, um ein Snapshot-basiertes Backup auf dem Quelldatenbanksystem und einen Klon auf dem Zieldatenbanksystem auszuführen. Das Skript ist nicht vollständig. Vielmehr zeigt das Skript, wie die Integration zwischen LSC und SnapCenter aussehen kann und wie einfach es ist, es einzurichten.



Da das Skript auf dem LSC-Master ausgeführt wird (was auch ein Satellitensystem ist), muss der LSC-Master auf dem SnapCenter-Server als Windows-Benutzer ausgeführt werden, der über die entsprechenden Berechtigungen verfügt, um Backup- und Klonvorgänge in SnapCenter auszuführen. Um zu überprüfen, ob der Benutzer über die entsprechenden Berechtigungen verfügt, sollte er eine Snapshot Kopie und einen Klon in der SnapCenter UI ausführen können.

Es besteht keine Notwendigkeit, den LSC-Master und den LSC-Satelliten auf dem SnapCenter-Server selbst auszuführen. Der LSC-Master und der LSC-Satellit können auf jedem Windows-Rechner ausgeführt werden. Voraussetzung für die Ausführung des PowerShell Skripts auf dem LSC-Satellit ist, dass die SnapCenter PowerShell Cmdlets auf dem Windows Server installiert wurden.

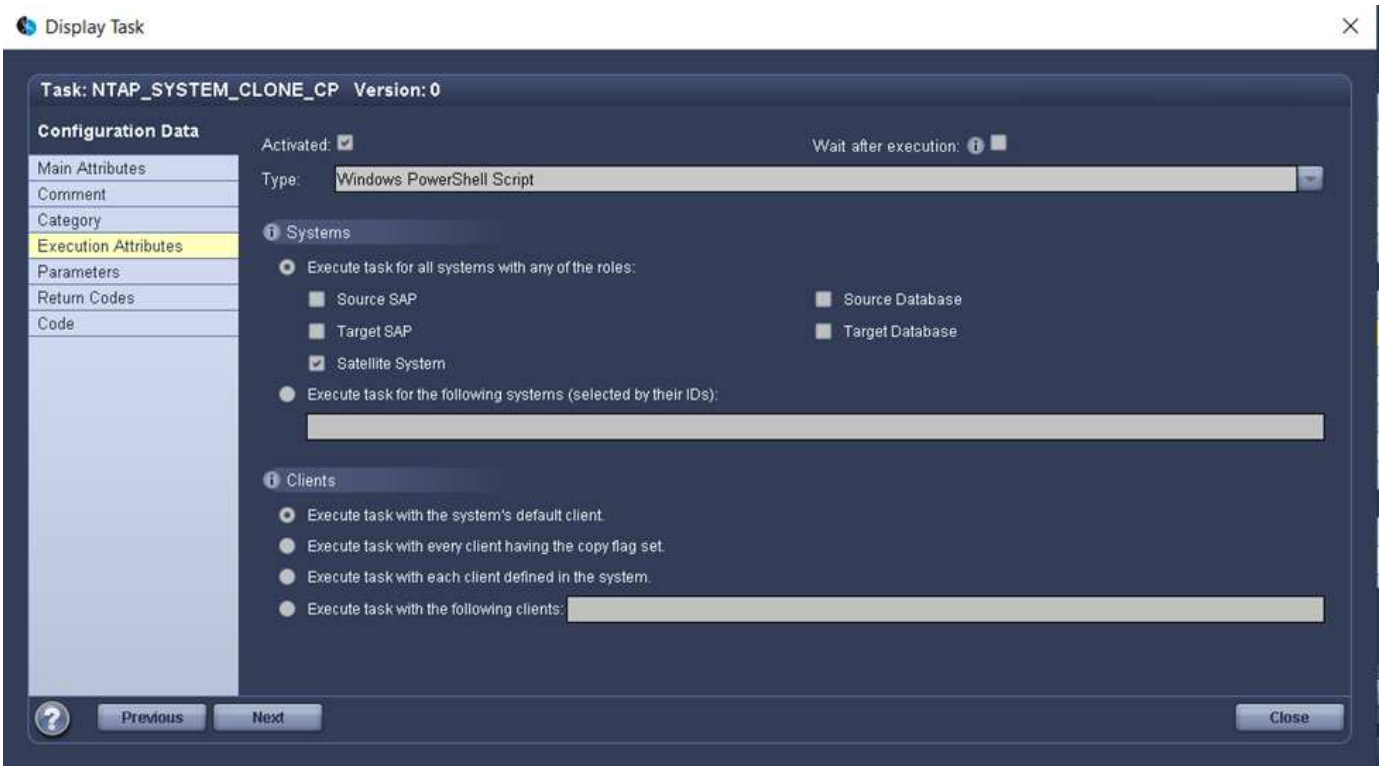
Zentraler Kommunikationshost

Zur Integration zwischen LSC und SnapCenter über einen zentralen Kommunikationhost werden in der Kopiephase nur die erforderlichen Anpassungen vorgenommen. Die Snapshot Kopie und der Klon werden mit dem SnapCenter Agent auf dem zentralen Kommunikations-Host erstellt. Daher stehen alle Details zu den neu erstellten Volumes nur auf dem zentralen Kommunikationshost und nicht auf dem Zieldatenbankserver zur Verfügung. Diese Details sind jedoch auf dem Ziel-Datenbankserver erforderlich, um das Klon-Volume zu mounten und die Recovery auszuführen. Aus diesem Grund sind in der Kopiephase zwei zusätzliche Aufgaben erforderlich. Eine Aufgabe wird auf dem zentralen Kommunikations-Host ausgeführt und eine Aufgabe wird auf dem Ziel-Datenbankserver ausgeführt. Diese beiden Aufgaben werden in der Abbildung unten angezeigt.

- **NTAP_SYSTEM_CLONE_CP.** Diese Aufgabe erstellt die Snapshot Kopie und den Klon mit einem PowerShell Skript, das die notwendigen SnapCenter Funktionen auf dem zentralen Kommunikations-Host ausführt. Diese Aufgabe läuft daher auf dem LSC-Satelliten, der in unserem Fall der LSC-Master ist, der unter Windows läuft. Dieses Skript sammelt alle Details über den Klon und die neu erstellten Volumes und übergibt ihn an die zweite Aufgabe `NTAP_MNT_RECOVER_CP`, Die auf dem LSC-Arbeiter läuft, der auf dem Ziel-Datenbank-Server läuft.
- **NTAP_MNT_RECOVERY_CP.** Diese Aufgabe stoppt das Ziel-SAP-System und die SAP HANA-Datenbank, hängt die alten Volumes ab und hängt dann die neu erstellten Storage-Klon-Volumes an, basierend auf den Parametern, die von der vorherigen Aufgabe übergeben wurden `NTAP_SYSTEM_CLONE_CP`. Die SAP HANA Zieldatenbank wird wiederhergestellt und wiederhergestellt.

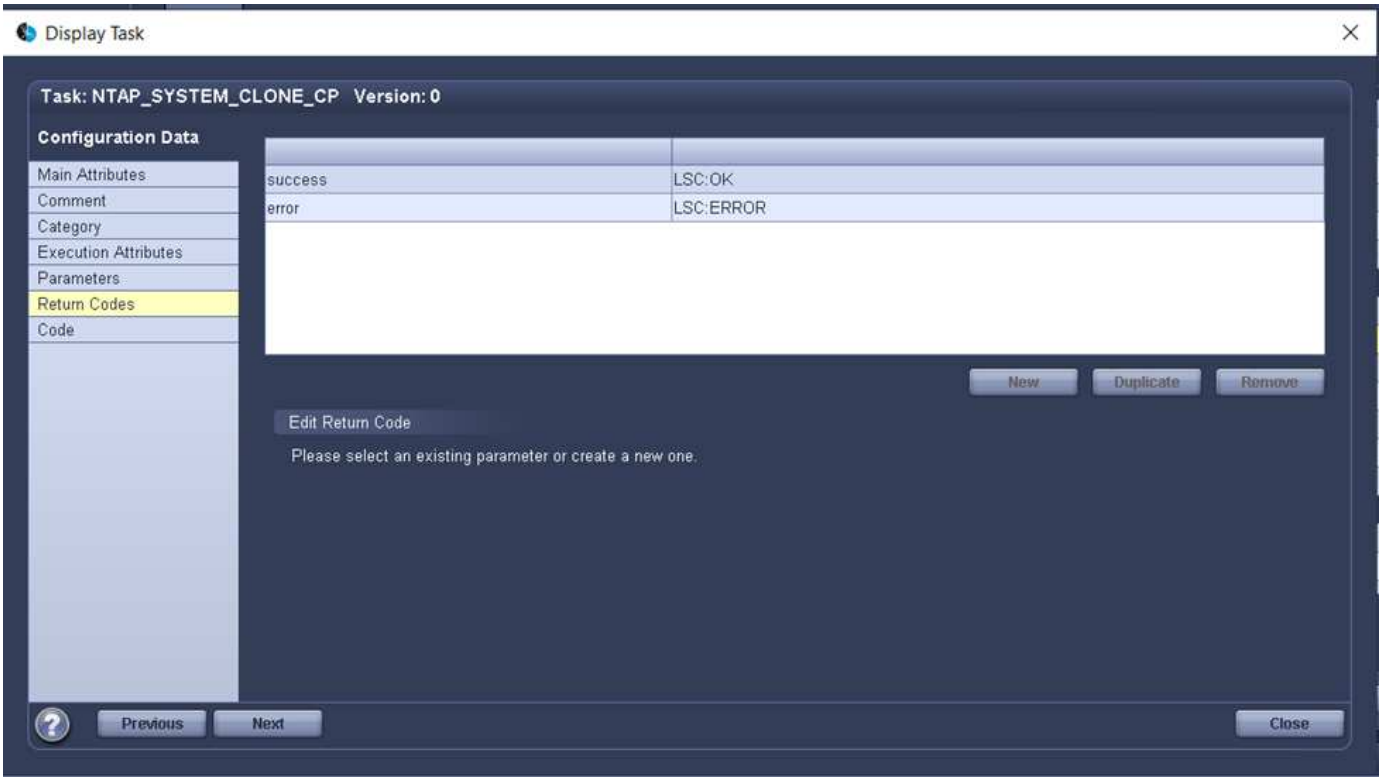
	copy	Copy Phase		phase
	copy 1	*NTAP_SYSTEM_CLONE*	*NetApp SnapShot and Clone*	*psh*
	copy 2	NTAP_SYSTEM_CLONE_CP	NetApp SnapShot and Clone	psh
	copy 3	NTAP_MNT_RECOVER_CP	Mount Volume and Recover HANA Database	cmd
	copy 4	*LPDBBCKP*	*Backup Source DB in Filesystem*	*lsh*
	copy 5	*LPDBCPYFLS*	*Copy DB Backup Files From Source to Target System*	*lsh*
	copy 6	*LTDBRESTORE*	*Restore DB Files*	*lsh*
	copy 7	*LTDBRESTORE_TENANT*	*Restore DB Files for Tenant Database*	*lsh*
	post	Post Phase		phase

Die folgende Abbildung zeigt die Konfiguration der Aufgabe `NTAP_SYSTEM_CLONE_CP`. Dies ist das Windows PowerShell-Skript, das auf dem Satellitensystem ausgeführt wird. In diesem Fall ist das Satellitensystem der SnapCenter-Server mit dem installierten LSC-Master.

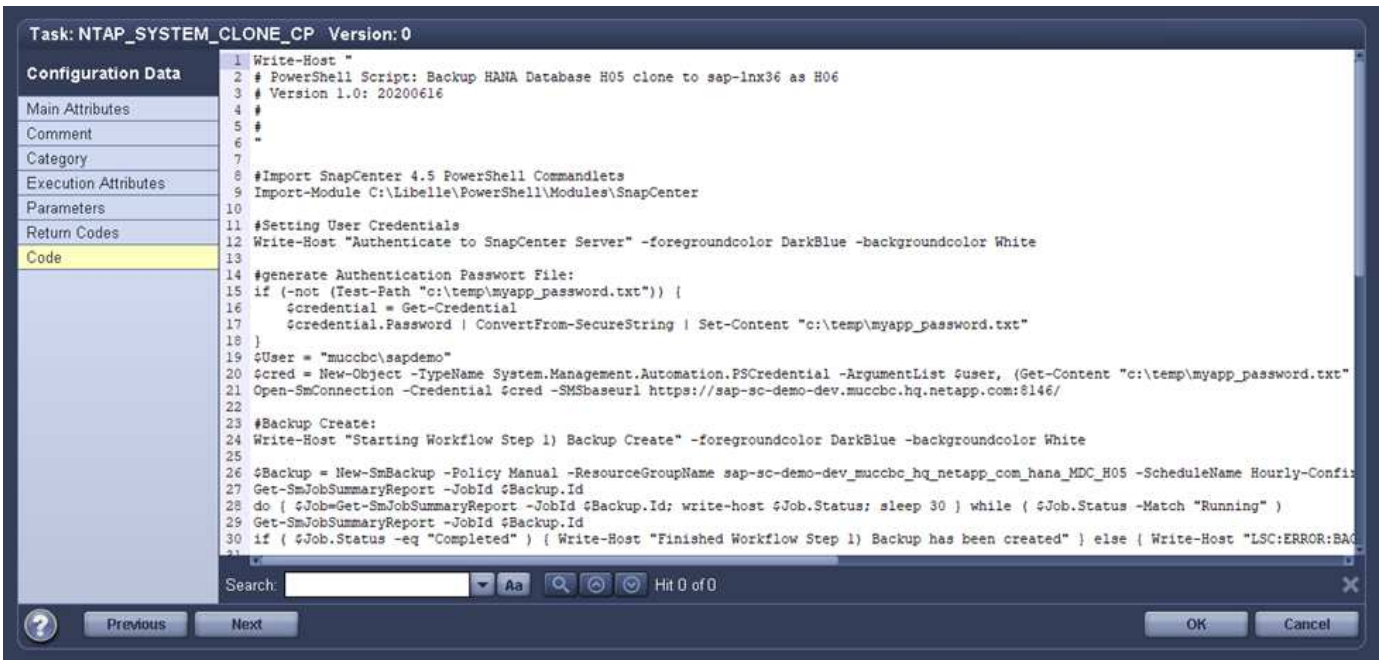


Da LSC wissen muss, ob der Snapshot Kopie- und Klonvorgang erfolgreich war, müssen Sie mindestens zwei Rückgabecodetypen definieren: Einen Rückgabecode für eine erfolgreiche Ausführung des Skripts und den anderen für eine fehlgeschlagene Ausführung des Skripts, wie in dem nachfolgenden Bild dargestellt.

- `LSC:OK` Wenn die Ausführung erfolgreich war, muss vom Skript in die Standardausführung geschrieben werden.
- `LSC:ERROR` Muss vom Skript in die Standardausführung geschrieben werden, wenn die Ausführung fehlgeschlagen ist.



Das folgende Bild zeigt einen Teil des PowerShell-Skripts, der ausgeführt werden muss, um eine Snapshot Kopie und einen Klon mithilfe des SnapCenter-Agenten auf dem zentralen Kommunikations-Host auszuführen. Das Skript soll nicht vollständig sein. Vielmehr wird das Skript verwendet, um zu zeigen, wie die Integration zwischen LSC und SnapCenter aussehen kann und wie einfach es ist, es einzurichten.

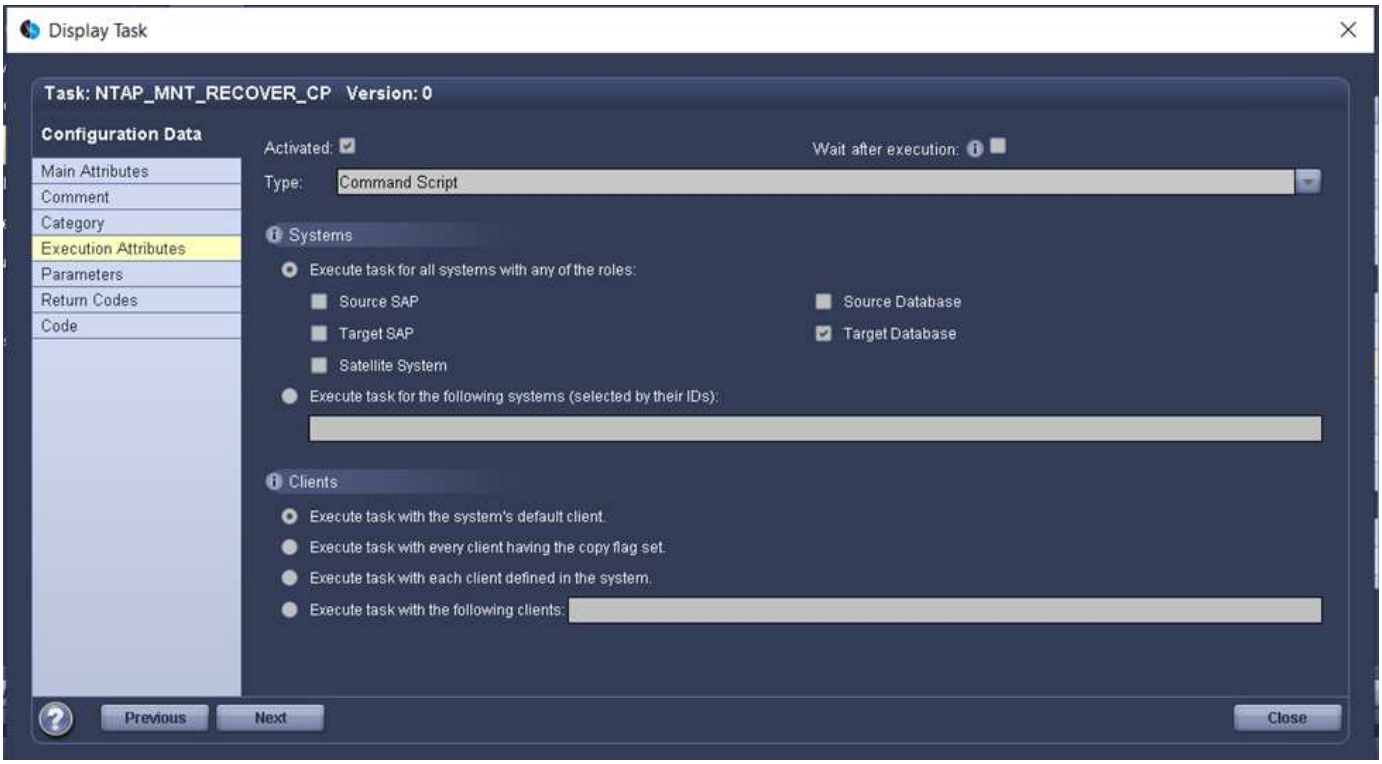


Wie bereits erwähnt, müssen Sie den Namen des Klon-Volumes an die nächste Aufgabe übergeben `NTAP_MNT_RECOVER_CP` So mounten Sie das Klon-Volume auf dem Zielserver: Der Name des Klon-Volume, auch als Verbindungspfad bezeichnet, wird in der Variable gespeichert `$JunctionPath`. Die Übergabe an eine nachfolgende LSC-Aufgabe erfolgt über eine benutzerdefinierte LSC-Variable.

```
echo $JunctionPath > $_task(current, custompath1)_$
```

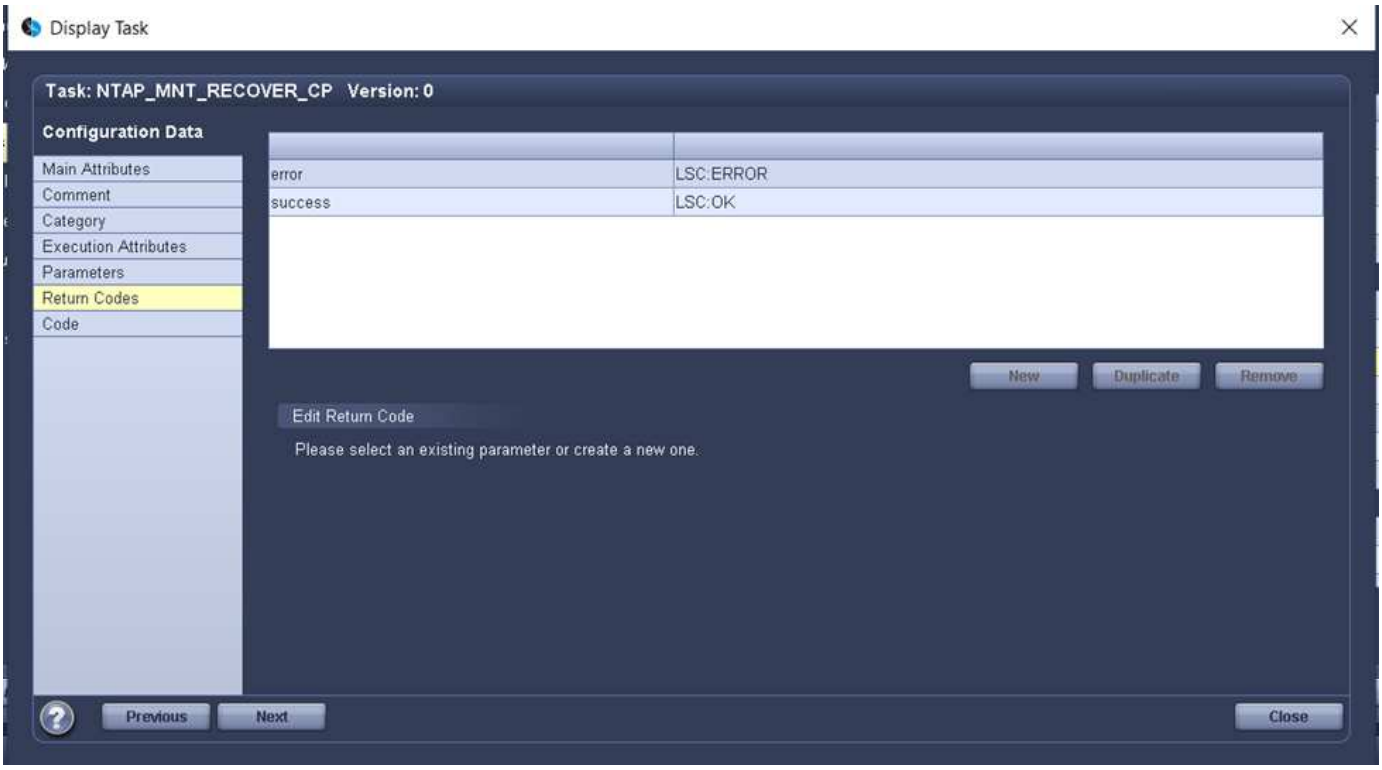
Da das Skript auf dem LSC-Master ausgeführt wird (was auch ein Satellitensystem ist), muss der LSC-Master auf dem SnapCenter-Server als Windows-Benutzer ausgeführt werden, der über die entsprechenden Berechtigungen verfügt, um die Backup- und Klonvorgänge in SnapCenter auszuführen. Um zu überprüfen, ob diese über die entsprechenden Berechtigungen verfügt, sollte der Benutzer eine Snapshot Kopie und einen Klon in der SnapCenter GUI ausführen können.

Die folgende Abbildung zeigt die Konfiguration der Aufgabe `NTAP_MNT_RECOVER_CP`. Da wir ein Linux-Shell-Skript ausführen möchten, ist dies ein Befehlsskript, das auf dem Zieldatenbanksystem ausgeführt wird.



Da LSC bekannt sein muss, dass die Klon-Volumes Mounten sind und ob das Wiederherstellen und Wiederherstellen der Zieldatenbank erfolgreich war, müssen wir mindestens zwei Rückgabecodetypen definieren. Ein Code dient zur erfolgreichen Ausführung des Skripts und ist für eine fehlgeschlagene Ausführung des Skripts, wie in der folgenden Abbildung dargestellt.

- `LSC:OK` Wenn die Ausführung erfolgreich war, muss vom Skript in die Standardausführung geschrieben werden.
- `LSC:ERROR` Muss vom Skript in die Standardausführung geschrieben werden, wenn die Ausführung fehlgeschlagen ist.

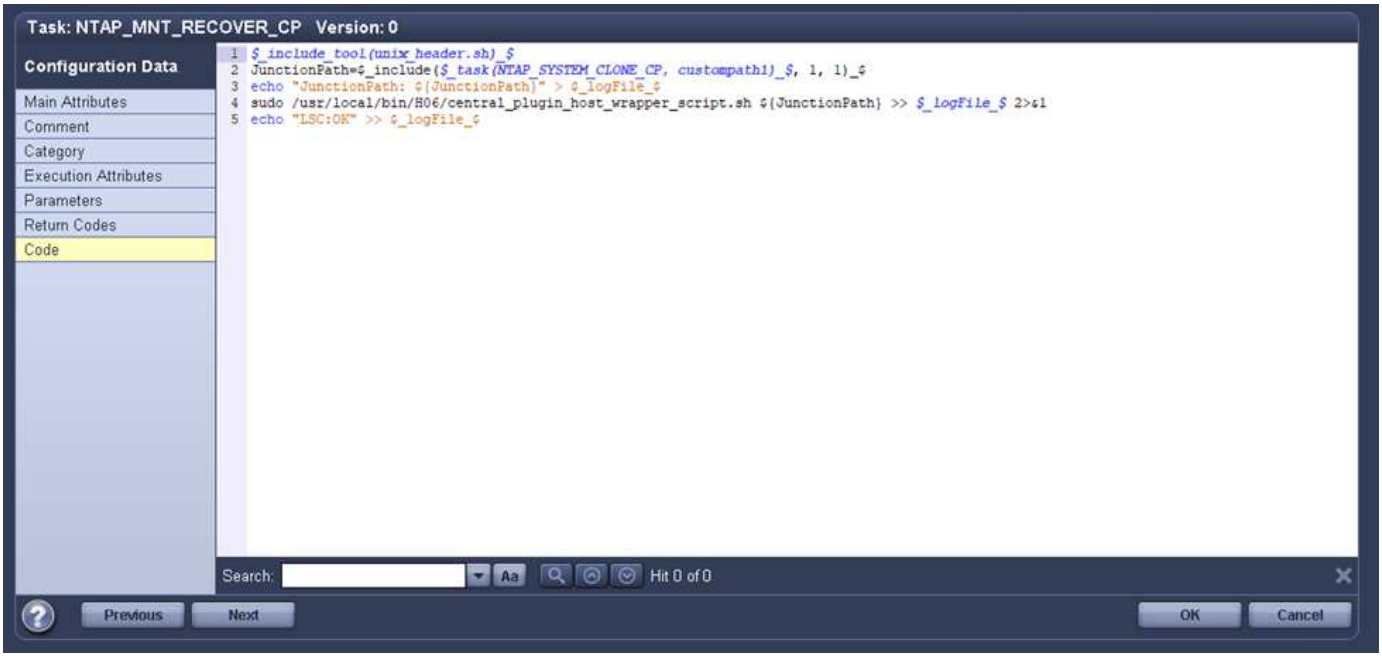


Die folgende Abbildung zeigt einen Teil des Linux Shell-Skripts, mit dem die Zieldatenbank angehalten, das alte Volume entfernt, das Klon-Volume gemountet und die Zieldatenbank wiederhergestellt werden kann. In der vorherigen Aufgabe wurde der Verbindungspfad in eine LSC-Variable geschrieben. Der folgende Befehl liest diese LSC-Variable und speichert den Wert in `$JunctionPath` Variable des Linux Shell-Skripts.

```
JunctionPath=$_include($_task(NTAP_SYSTEM_CLONE_CP, custompath1)_$, 1,
1)_$
```

Der LSC-Worker auf dem Zielsystem läuft als `<sidaadm>`, Aber Mount-Befehle müssen als Root-Benutzer ausgeführt werden. Deshalb müssen Sie die erstellen `central_plugin_host_wrapper_script.sh`. Das Skript `central_plugin_host_wrapper_script.sh` Wird aus der Aufgabe aufgerufen `NTAP_MNT_RECOVERY_CP` Verwenden der `sudo` Befehl. Verwenden der `sudo` Befehl, das Skript wird mit UID 0 ausgeführt, und wir können alle nachfolgenden Schritte durchführen, z. B. das Abhängen der alten Volumes, das Mounten der Klon-Volumes und das Wiederherstellen der Zieldatenbank. Um die Skriptausführung mit zu aktivieren `sudo`, Die folgende Zeile muss hinzugefügt werden `/etc/sudoers`:

```
hn6adm ALL=(root)
NOPASSWD:/usr/local/bin/H06/central_plugin_host_wrapper_script.sh
```



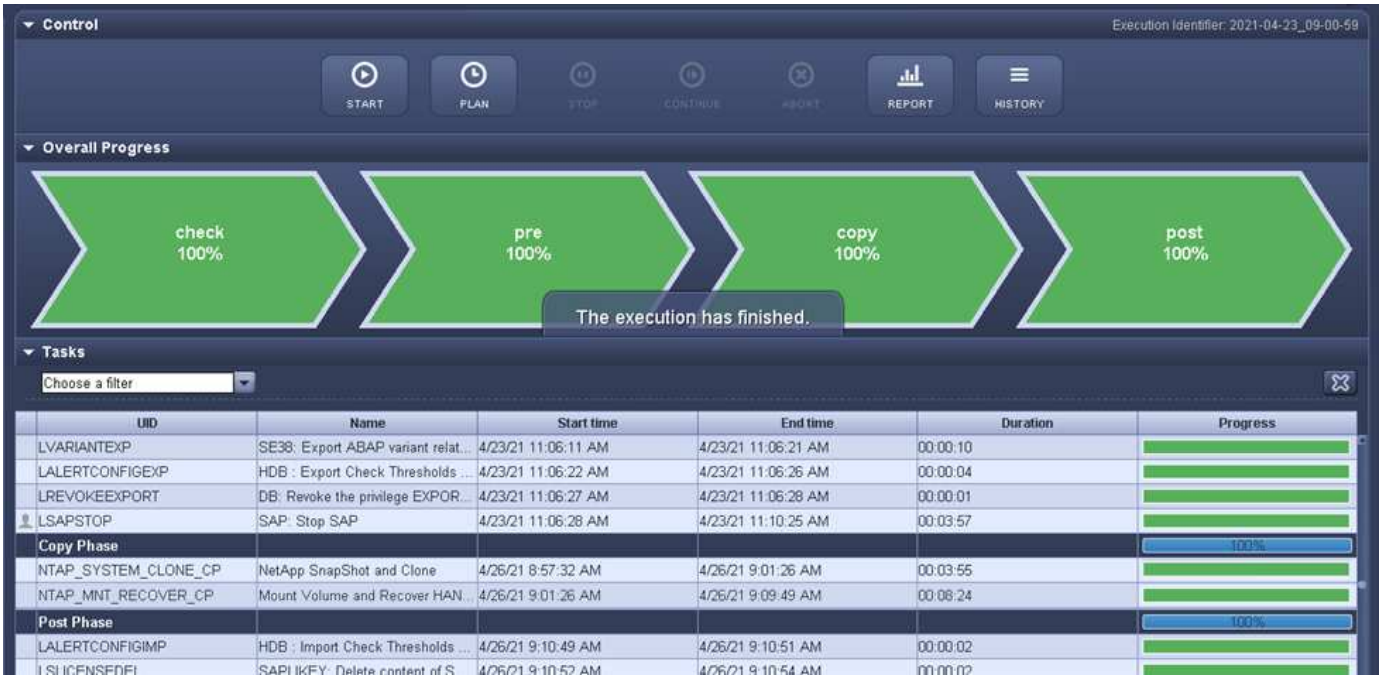
SAP HANA-Systemaktualisierungsvorgang

Nachdem nun alle notwendigen Integrationsaufgaben zwischen LSC und NetApp SnapCenter durchgeführt wurden, ist es ein einziger Schritt, eine voll automatisierte Aktualisierung des SAP-Systems zu starten.

Die folgende Abbildung zeigt die Aufgabe `NTAP``_SYSTEM_``CLONE` In einer Standardinstallation. Wie Sie sehen, dauerte das Erstellen einer Snapshot Kopie und eines Klons, das Mounten des Klon-Volumes auf dem Zieldatenbankserver und das Wiederherstellen der Zieldatenbank etwa 14 Minuten. Mit den Snapshots und der NetApp FlexClone Technologie bleibt die Dauer dieser Aufgabe unabhängig von der Größe der Quelldatenbank nahezu identisch.

In der folgenden Abbildung werden die beiden Aufgaben dargestellt `NTAP_SYSTEM_CLONE_CP` Und `NTAP_MNT_RECOVERY_CP` Bei Verwendung eines zentralen Kommunikations-Hosts. Wie Sie sehen, dauerte das Erstellen einer Snapshot Kopie, ein Klon, das Klon-Volume auf dem Zieldatenbankserver und das

Wiederherstellen und Wiederherstellen der Zieldatenbank etwa 12 Minuten. Dies ist mehr oder weniger die gleiche Zeit, um diese Schritte bei der Verwendung einer Standardinstallation durchzuführen. Wie bereits erwähnt, ermöglicht die Snapshot und NetApp FlexClone Technologie diese Aufgaben unabhängig von der Größe der Quelldatenbank konsistent und schnell zu erledigen.



Systemaktualisierung für SAP HANA mit LSC, AzACSnap und Azure NetApp Files

Wird Verwendet "Azure NetApp Files für SAP HANA", Oracle und DB2 auf Azure bieten den Kunden die erweiterten Datenmanagement- und Datensicherungsfunktionen von NetApp ONTAP mit dem nativen Microsoft Azure NetApp Files Service. "AzacSnap" Ist die Grundlage für sehr schnelle SAP Systemaktualisierungen zur Erstellung applikationskonsistenter NetApp Snapshot-Kopien von SAP HANA und Oracle Systemen (DB2 wird derzeit nicht von AzAcSnap unterstützt).

Snapshot Kopien-Backups, die im Rahmen der Backup-Strategie entweder nach Bedarf oder regelmäßig erstellt werden, können dann effizient auf neuen Volumes geklont und zur schnellen Aktualisierung von Zielsystemen genutzt werden. AzAcSnap liefert die notwendigen Workflows für die Erstellung von Backups und das Klonen auf neuen Volumes. Libelle SystemCopy führt die Vorverarbeitungsschritte sowie die Nachbearbeitungsschritte durch, die für eine vollständige Systemaktualisierung erforderlich sind.

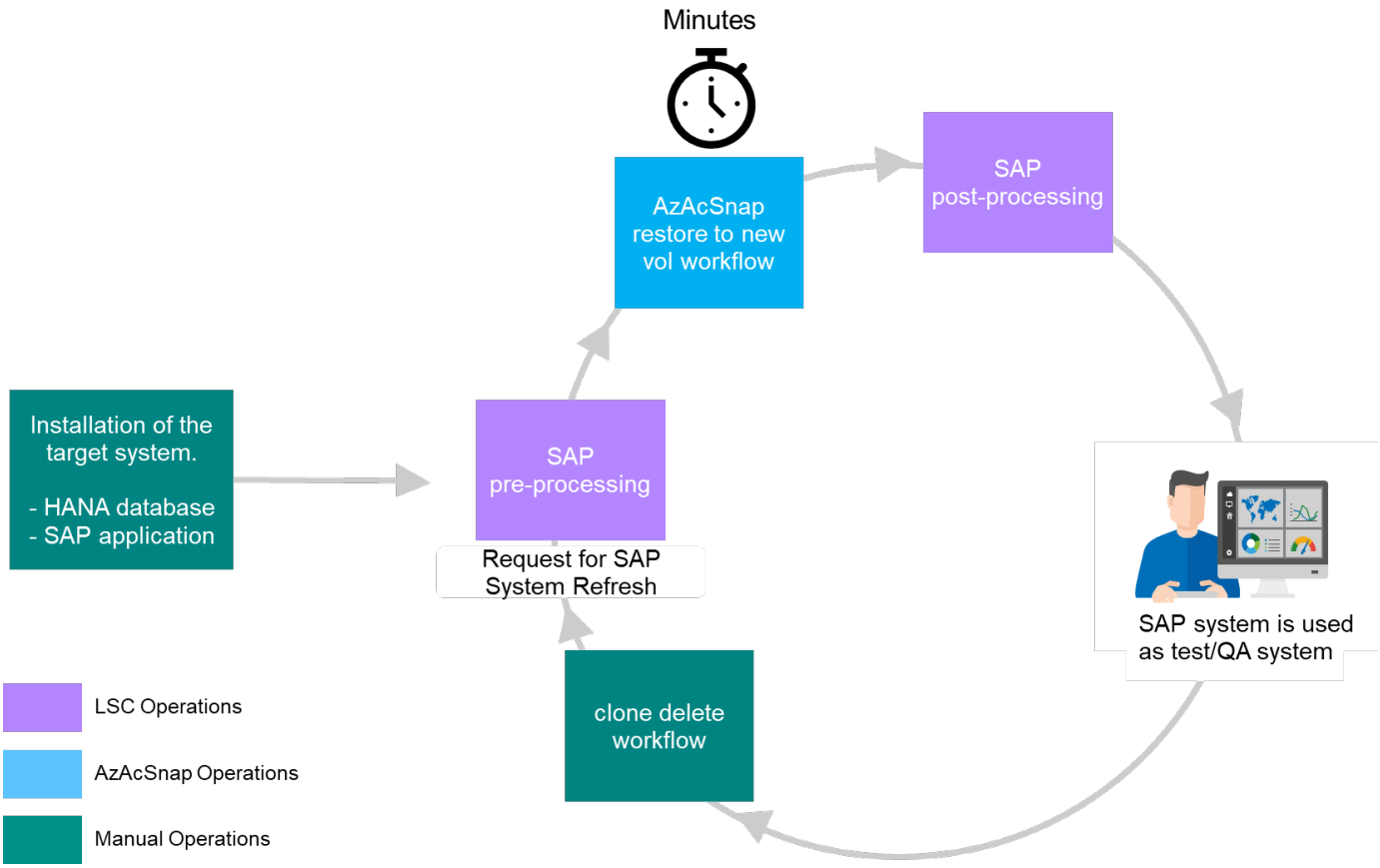
In diesem Kapitel beschreiben wir eine automatisierte Aktualisierung des SAP-Systems mit AzAcSnap und Libelle SystemCopy unter Verwendung von SAP HANA als zugrunde liegende Datenbank. Da AzAcSnap auch für Oracle verfügbar ist, kann dasselbe Verfahren auch mit AzAcSnap für Oracle implementiert werden. Andere Datenbanken könnten zukünftig von AzAcSnap unterstützt werden, was es dann ermöglichen würde, Systemkopievorgänge für diese Datenbanken mit LSC und AzAcSnap zu ermöglichen.

Die folgende Abbildung zeigt einen typischen grundlegenden Workflow eines SAP Systemaktualisierungszyklus mit AzAcSnap und LSC:

- Einmalige, erstmalige Installation und Vorbereitung des Zielsystems.
- SAP-Vorverarbeitung durch LSC durchgeführt.

- Wiederherstellen (oder Klonen) einer vorhandenen Snapshot Kopie des Quellsystems auf das von AzAcSnap ausgeführte Zielsystem.
- SAP-Nachbearbeitungsvorgänge durchgeführt von LSC.

Das System kann dann als Test- oder QA-System verwendet werden. Wenn eine neue Systemaktualisierung angefordert wird, wird der Workflow mit Schritt 2 neu gestartet. Alle verbleibenden geklonten Volumes müssen manuell gelöscht werden.

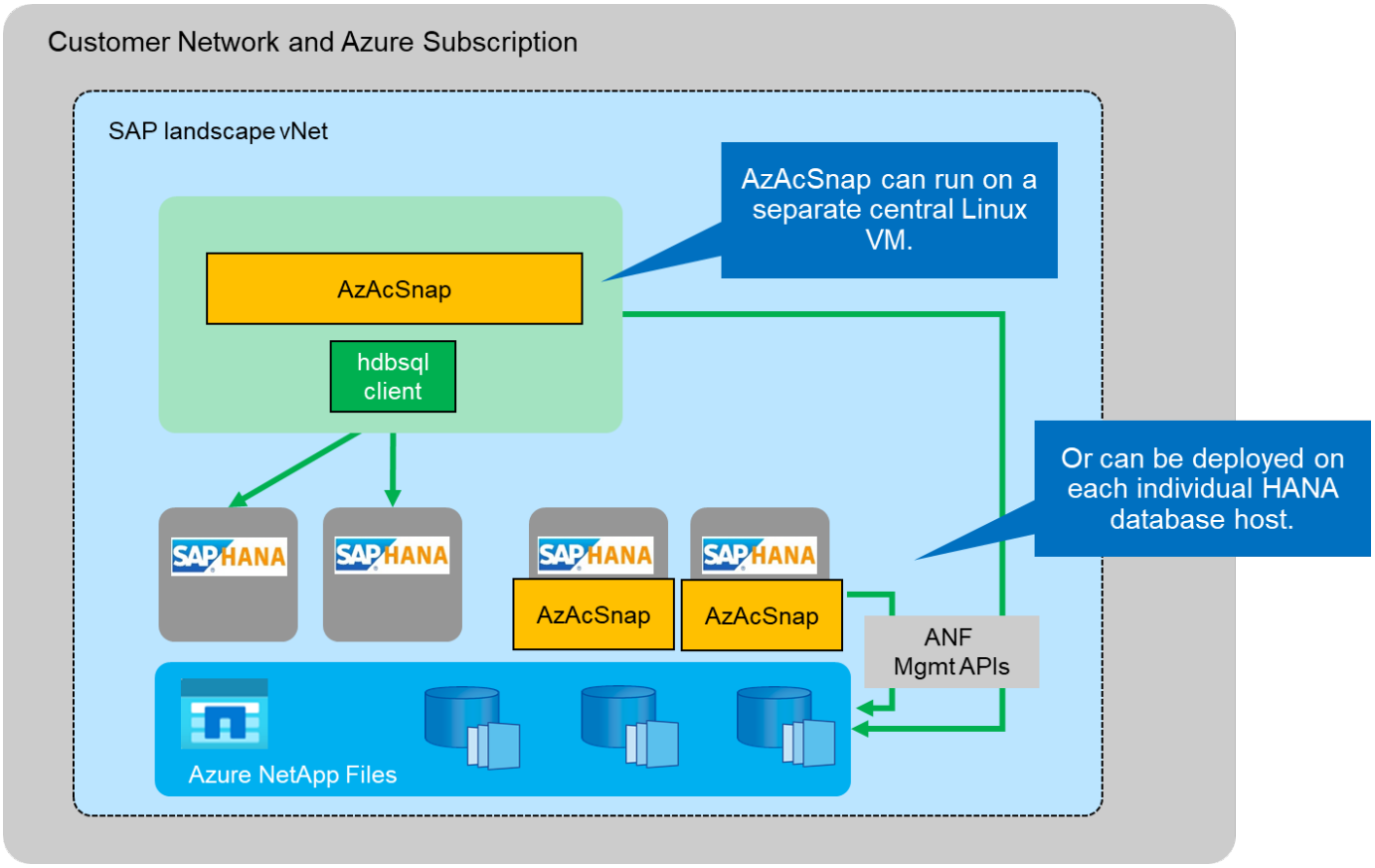


Voraussetzungen und Einschränkungen

Folgende Voraussetzungen müssen erfüllt sein.

AzAcSnap wurde für die Quelldatenbank installiert und konfiguriert

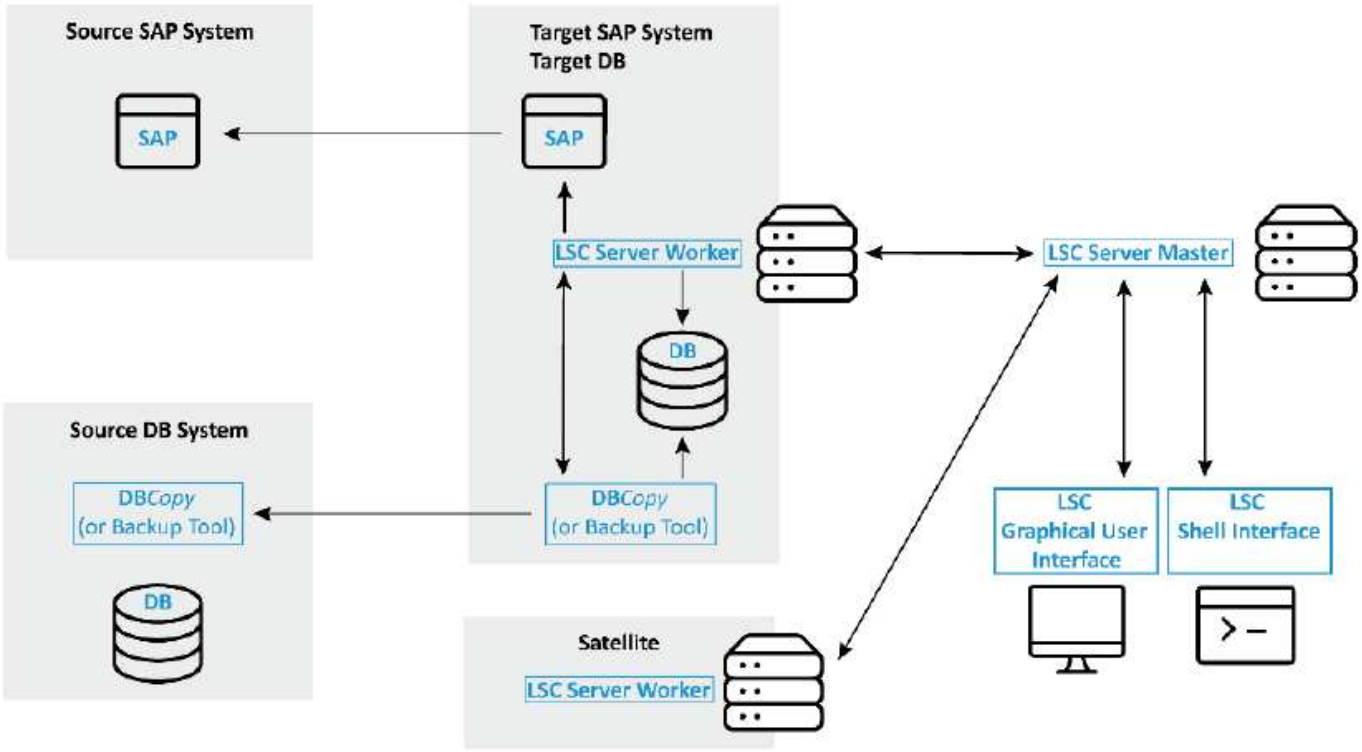
Im Allgemeinen gibt es zwei Implementierungsoptionen für AzAcSnap, wie in der folgenden Abbildung dargestellt.



AzAcSnap kann auf einer zentralen Linux-VM installiert und ausgeführt werden, für die alle DB-Konfigurationsdateien zentral gespeichert werden und AzAcSnap Zugriff auf alle Datenbanken (über den hdbsql-Client) sowie auf die konfigurierten HANA-Benutzerspeicherschlüssel für all diese Datenbanken hat. Bei einer dezentralen Implementierung wird AzAcSnap individuell auf jedem Datenbank-Host installiert, auf dem typischerweise nur die DB-Konfiguration für die lokale Datenbank gespeichert ist. Beide Bereitstellungsoptionen werden für die LSC-Integration unterstützt. Wir haben diesem Dokument jedoch im Lab Setup auf einen hybriden Ansatz gefolgt. AzAcSnap wurde auf einem zentralen NFS-Share sowie allen DB-Konfigurationsdateien installiert. Diese zentrale Installationsfreigabe wurde auf allen VMs unter bereitgestellt `/mnt/software/AZACSNAP/snapshot-tool`. Die Ausführung des Tools erfolgte anschließend lokal auf den DB-VMs.

Libelle SystemCopy ist für das Quell- und Ziel-SAP-System installiert und konfiguriert

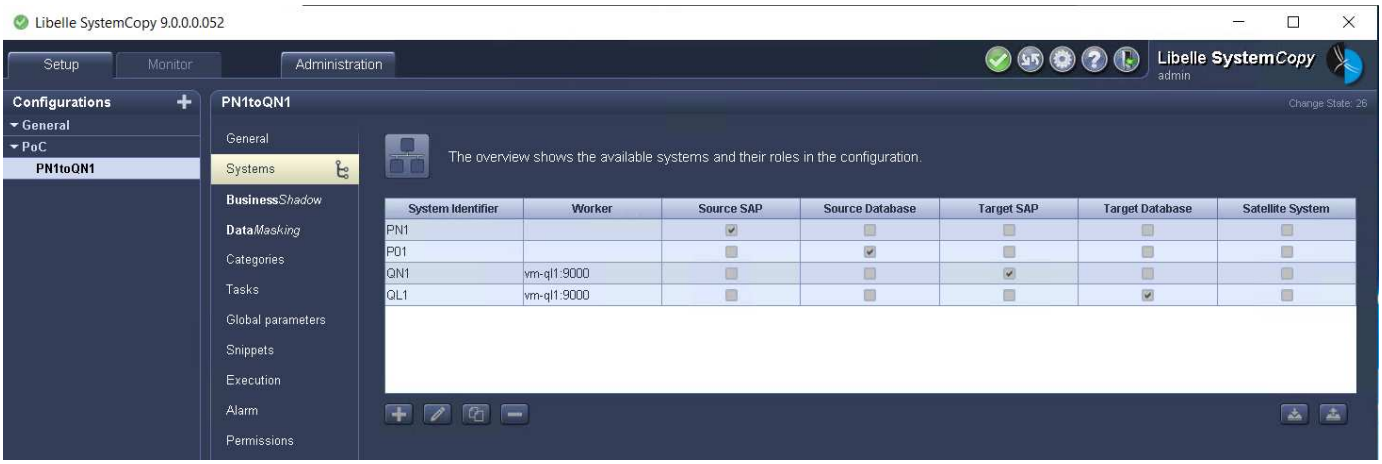
Libelle SystemCopy-Bereitstellungen bestehen aus folgenden Komponenten:



- **LSC Master.** wie der Name schon sagt, ist dies die Master-Komponente, die den automatischen Workflow einer Libelle-basierten Systemkopie steuert.
- **LSC Worker.** ein LSC-Mitarbeiter läuft in der Regel auf dem Ziel-SAP-System und führt die für die automatisierte Systemkopie erforderlichen Skripte aus.
- **LSC Satellite.** ein LSC-Satellit läuft auf einem Drittanbieter-System, auf dem weitere Skripte ausgeführt werden müssen. Der LSC-Master kann auch die Rolle eines LSC-Satellitensystems erfüllen.

Die Benutzeroberfläche von Libelle SystemCopy (LSC) muss auf einer geeigneten VM installiert sein. In diesem Laboraufbau wurde die LSC GUI auf einem separaten Windows VM installiert, kann aber auch auf dem DB Host zusammen mit dem LSC Worker laufen. Der LSC-Worker muss mindestens auf der VM der Ziel-DB installiert sein. Je nach gewählter Implementierungsoption für AzAcSnap sind möglicherweise zusätzliche LSC-Installationen für Mitarbeiter erforderlich. Auf der VM, auf der AzAcSnap ausgeführt wird, muss eine LSC-Worker-Installation vorhanden sein.

Nach der Installation von LSC ist die Grundkonfiguration für die Quelle und die Zieldatenbank gemäß den LSC-Richtlinien durchzuführen. Die folgenden Abbildungen zeigen die Konfiguration der Lab-Umgebung für dieses Dokument. Im nächsten Abschnitt finden Sie Details zu den Quell- und Zielsystemen und Datenbanken von SAP.



Für die SAP-Systeme sollten Sie außerdem eine passende Standardaufgabenliste konfigurieren. Weitere Informationen zur Installation und Konfiguration von LSC finden Sie im LSC-Benutzerhandbuch, das Teil des LSC-Installationspakets ist.

Bekannte Einschränkungen

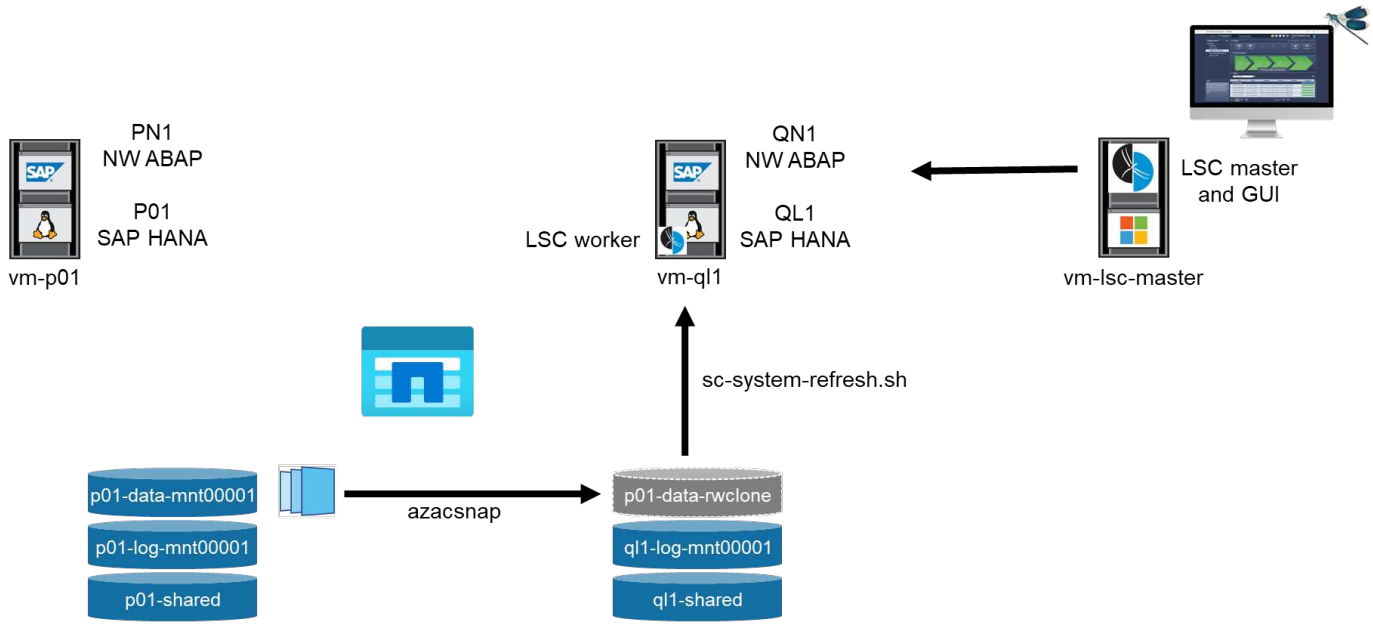
Die hier beschriebene Integration von AzAcSnap und LSC funktioniert nur für SAP HANA Single-Host-Datenbanken. Auch SAP HANA Implementierungen mit mehreren Hosts (oder Scale-out) können unterstützt werden, aber für solche Implementierungen sind einige Anpassungen oder Verbesserungen der benutzerdefinierten LSC-Aufgaben für die Kopiephase und die Underlaying-Skripte erforderlich. Derartige Verbesserungen werden in diesem Dokument nicht behandelt.

Die Integration von SAP Systemaktualisierungen setzt immer die neueste erfolgreiche Snapshot Kopie des Quellsystems ein, um die Aktualisierung des Zielsystems durchzuführen. Wenn Sie andere ältere Snapshot Kopien verwenden möchten, wird die entsprechende Logik im verwendet ZAZACSNAPRESTORE Benutzerdefinierte Aufgabe muss angepasst werden. Dieser Prozess ist für dieses Dokument nicht im Umfang enthalten.

Laboreinrichtung

Das Lab-Setup besteht aus einem SAP Quell- System und einem SAP Ziel-System, das beide auf SAP HANA Single-Host-Datenbanken ausgeführt werden.

Das folgende Bild zeigt die Laboreinrichtung.

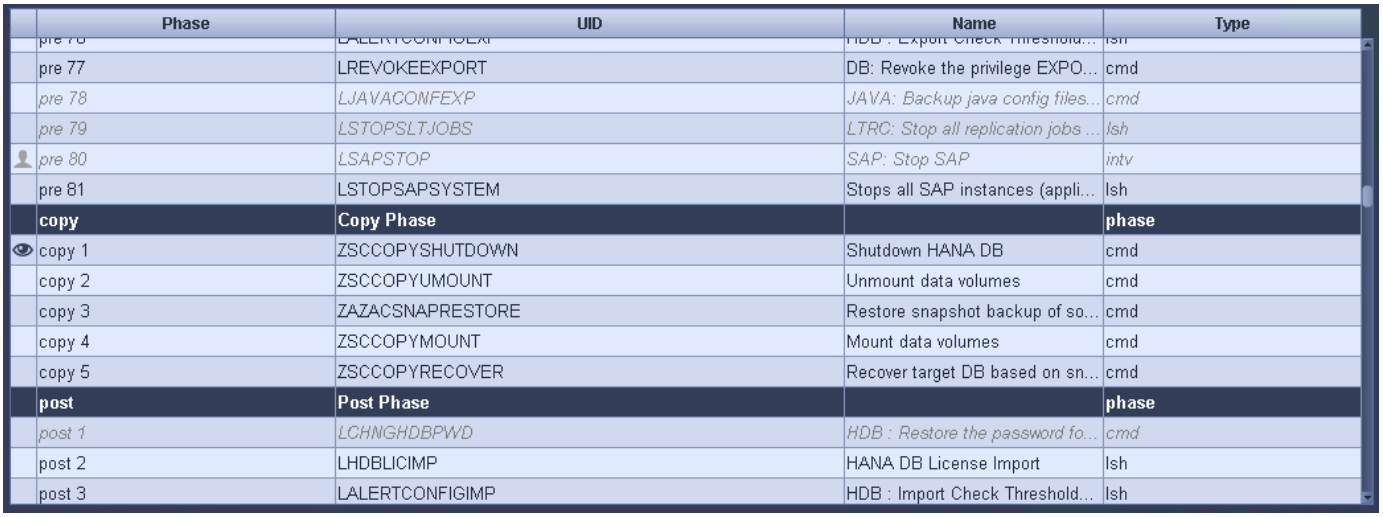


Es enthält die folgenden Systeme, Softwareversionen und Azure NetApp Files Volumes:

- * P01.* SAP HANA 2.0 SP5 DATENBANK. Quelldatenbank, einzelner Host, einzelner Benutzer-Mandant.
- **PN1.** SAP NETWEAVER ABAP 7.51. Quell-SAP-System.
- **vm-p01.** SLES 15 SP2 mit AzAcSnap installiert. Quell-VM, die P01 und PN1 hostet.
- **QL1.** SAP HANA 2.0 SP5 DATENBANK. Systemaktualisierung Zieldatenbank, einzelner Host, ein Mandant
- * QN1.* SAP NETWEAVER ABAP 7.51. Systemaktualisierung Ziel-SAP-System.
- **vm-ql1.** SLES 15 SP2 mit installiertem LSC Worker. Ziel-VM, die QL1 und QN1 hostet.
- LSC Master Version 9.0.0.0.052.
- **vm- lsc-Master.** Windows Server 2016. Hostet LSC Master und LSC GUI.
- Azure NetApp Files Volumes für Daten, Protokoll und gemeinsam genutzt für P01 und QL1 auf den dedizierten DB-Hosts montiert.
- Zentrales Azure NetApp Files Volume für Skripts, AzAcSnap-Installation und Konfigurationsdateien, die auf allen VMs gemountet sind

Erste, einmalige Vorbereitungsschritte

Bevor die erste Aktualisierung des SAP Systems ausgeführt werden kann, müssen Azure NetApp Files Storage-Vorgänge zum Kopieren und Klonen von Snapshot mit AzAcSnap integriert werden. Sie müssen auch ein Hilfsskript zum Starten und Stoppen der Datenbank und zum Mounten oder Abhängen der Azure NetApp Files Volumes ausführen. Alle erforderlichen Aufgaben werden im Rahmen der Kopiephase als benutzerdefinierte Aufgaben in LSC ausgeführt. Das folgende Bild zeigt die benutzerdefinierten Aufgaben in der LSC-Aufgabenliste.



Phase	UID	Name	Type
pre 77	LREVOKEEXPORT	DB: Revoke the privilege EXPO...	cmd
pre 78	*LJAVACONFEXP*	*JAVA: Backup java config files...*	*cmd*
pre 79	*LSTOPSLTJOBS*	*LTRC: Stop all replication jobs ...*	*lsh*
pre 80	*LSAPSTOP*	*SAP: Stop SAP*	*intv*
pre 81	LSTOPSAPSYSTEM	Stops all SAP instances (appli...	lsh
copy	**Copy Phase**		**phase**
copy 1	ZSCCOPYSHUTDOWN	Shutdown HANA DB	cmd
copy 2	ZSCCOPYUMOUNT	Unmount data volumes	cmd
copy 3	ZAZACSNAPRESTORE	Restore snapshot backup of so...	cmd
copy 4	ZSCCOPYMOUNT	Mount data volumes	cmd
copy 5	ZSCCOPYRECOVER	Recover target DB based on sn...	cmd
post	**Post Phase**		**phase**
post 1	*LCHNGHDBPWD*	*HDB : Restore the password fo...*	*cmd*
post 2	LHDBLICIMP	HANA DB License Import	lsh
post 3	LALERTCONFIGIMP	HDB : Import Check Threshold...	lsh

Alle fünf Kopieraufgaben werden hier genauer beschrieben. Bei einigen dieser Aufgaben ein Beispielskript `sc-system-refresh.sh` Wird verwendet, um den erforderlichen SAP HANA Datenbank-Recovery-Vorgang und das Mounten und Aufheben der Datenvolumes weiter zu automatisieren. Das Skript verwendet ein `LSC: success` Meldung in der Systemausgabe, um eine erfolgreiche Ausführung an LSC anzuzeigen. Details zu benutzerdefinierten Aufgaben und verfügbaren Parametern finden Sie im LSC-Benutzerhandbuch und im LSC-Entwicklerhandbuch. Alle Aufgaben in dieser Lab-Umgebung werden auf der Ziel-DB-VM ausgeführt.

Das Beispielskript wird so bereitgestellt, wie es ist, und wird nicht von NetApp unterstützt. Sie können das Skript per E-Mail an ng-sapcc@netapp.com anfordern.

Sc-system-refresh.sh Konfigurationsdatei

Wie bereits erwähnt, wird ein Hilfsskript verwendet, um die Datenbank zu starten und zu stoppen, die Azure NetApp Files-Volumes zu mounten und zu mounten sowie die SAP HANA Datenbank aus einer Snapshot Kopie wiederherzustellen. Das Skript `sc-system-refresh.sh` Wird auf dem zentralen NFS Share gespeichert. Das Skript benötigt für jede Zieldatenbank eine Konfigurationsdatei, die im selben Ordner wie das Skript selbst gespeichert werden muss. Die Konfigurationsdatei muss den folgenden Namen haben: `sc-system-refresh-<target DB SID>.cfg` (Beispiel `sc-system-refresh-QL1.cfg` In dieser Laborumgebung). Die hier verwendete Konfigurationsdatei verwendet eine feste/hartcodierte Quell-DB-SID. Mit einigen Änderungen können das Skript und die Konfigurationsdatei erweitert werden, um die Quell-DB-SID als Eingabeparameter zu nehmen.

Die folgenden Parameter müssen an die spezifische Umgebung angepasst werden:

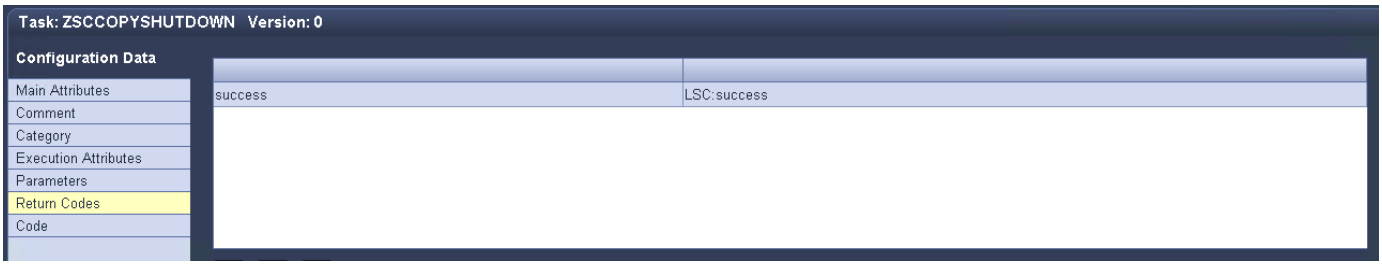
```
# hdbuserstore key, which should be used to connect to the target database
KEY=”QL1SYSTEM”
# single container or MDC
export P01_HANA_DATABASE_TYPE=MULTIPLE_CONTAINERS
# source tenant names { TENANT_SID [, TENANT_SID]* }
export P01_TENANT_DATABASE_NAMES=P01
# cloned vol mount path
export CLONED_VOLUMES_MOUNT_PATH=`tail -2
/mnt/software/AZACSNAP/snapshot_tool/logs/azacsnap-restore-azacsnap-
P01.log | grep -oe “[0-9]*\.[0-9]*\.[0-9]*\.[0-9]*:/.* “`
```

ZSCCOPYSHUTDOWN

Diese Aufgabe stoppt die SAP HANA Ziel-Datenbank. Der Code-Abschnitt dieser Aufgabe enthält den folgenden Text:

```
$_include_tool(unix_header.sh)_$
sudo /mnt/software/scripts/sc-system-refresh/sc-system-refresh.sh shutdown
$_system(target_db, id)_$ > $_logfile_$
```

Das Skript `sc-system-refresh.sh` Nimmt zwei Parameter an, die `shutdown` Befehl und DB SID, um die SAP HANA Datenbank mit sapcontrol zu beenden. Die Systemausgabe wird an die Standard-LSC-Logdatei umgeleitet. Wie bereits erwähnt, an `LSC: success` Die Meldung wird verwendet, um die erfolgreiche Ausführung anzuzeigen.



ZSCCOPYUMOUNT

Durch diese Aufgabe wird das alte Azure NetApp Files Daten-Volume vom Betriebssystem der Ziel-DB abgehängt. Der Codeabschnitt dieser Aufgabe enthält den folgenden Text:

```
$_include_tool(unix_header.sh)_$
sudo /mnt/software/scripts/sc-system-refresh/sc-system-refresh.sh umount
$_system(target_db, id)_$ > $_logfile_$
```

Es werden dieselben Skripte verwendet wie in der vorherigen Aufgabe. Die beiden übergebenen Parameter sind die `umount` Befehl und DB SID.

ZAZACSNAPRESTORE

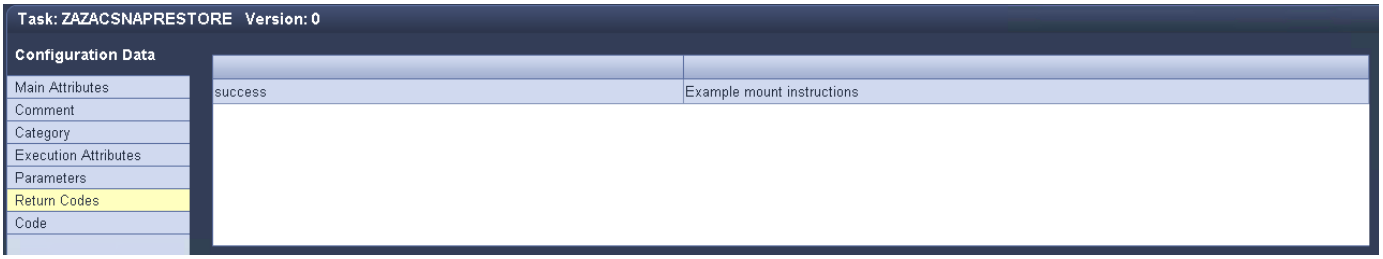
Auf dieser Aufgabe wird AzAcSnap ausgeführt, um die neueste erfolgreiche Snapshot-Kopie der Quelldatenbank auf ein neues Volume für die Zieldatenbank zu klonen. Dieser Vorgang entspricht einer umgeleiteten Wiederherstellung von Backups in herkömmlichen Backup-Umgebungen. Die Snapshot Kopie- und Klonfunktionen ermöglichen jedoch die Durchführung dieser Aufgabe sogar der größten Datenbanken innerhalb von Sekunden, während diese Aufgabe bei herkömmlichen Backups problemlos mehrere Stunden dauern könnte. Der Codeabschnitt dieser Aufgabe enthält den folgenden Text:

```
$_include_tool(unix_header.sh)_$
sudo /mnt/software/AZACSNAP/snapshot_tool/azacsnap -c restore --restore
snaptovol --hanasid $_system(source_db, id)_$
--configfile=/mnt/software/AZACSNAP/snapshot_tool/azacsnap
-$_system(source_db, id)_$.json > $_logfile_$
```

Vollständige Dokumentation für die AzAcSnap-Befehlszeilenoptionen für die `restore` Befehl ist in der Azure-Dokumentation hier zu finden: "Wiederherstellung mit dem Azure Application konsistenten Snapshot Tool". Der Anruf setzt voraus, dass die json DB Konfigurationsdatei für die Quell-DB auf dem zentralen NFS Share mit der folgenden Namenskonvention gefunden werden kann: `azacsnap-<source DB SID>. json`, (Zum Beispiel `azacsnap-P01.json` In dieser Laborumgebung).

> Da die Ausgabe des AzAcSnap-Befehls nicht geändert werden kann, ist der Standardwert `LSC: success` Nachricht kann für diese Aufgabe nicht verwendet werden. Deshalb die Zeichenfolge `Example mount instructions` Aus der AzAcSnap-Ausgabe wird als erfolgreicher Rückgabecode verwendet. In der 5.0 GA-Version von AzAcSnap wird diese Ausgabe nur erzeugt, wenn das Klonen erfolgreich war.

Die folgende Abbildung zeigt die Erfolgsmeldung „AzAcSnap Restore to New Volume“.



ZSCCOPYMOUNT

Diese Aufgabe bindet das neue Azure NetApp Files Daten-Volume auf das Betriebssystem der Ziel-DB ein. Der Codeabschnitt dieser Aufgabe enthält den folgenden Text:

```
$_include_tool(unix_header.sh)_$
sudo /mnt/software/scripts/sc-system-refresh/sc-system-refresh.sh mount
$_system(target_db, id)_$ > $_logfile_$
```

Das Skript sc-system-refresh.sh wird wieder verwendet, die übergeben `mount` Befehl und die Ziel-DB-SID.

ZSCCOPYRECOVER

Diese Aufgabe führt eine SAP HANA Datenbank-Recovery der Systemdatenbank und der Mandanten-Datenbank auf Basis der wiederhergestellten (geklonten) Snapshot Kopie durch. Die hier verwendete Recovery-Option bezieht sich auf spezifisches Datenbank-Backup, wie etwa keine zusätzlichen Protokolle, für vorwärts Recovery angewendet werden. Daher ist die Recovery-Zeit sehr kurz (höchstens ein paar Minuten). Die Laufzeit dieses Vorgangs wird durch das Starten der SAP HANA Datenbank bestimmt, die automatisch nach dem Wiederherstellungsprozess stattfindet. Um die Startzeit zu beschleunigen, kann der Durchsatz des Azure NetApp Files Daten-Volumes bei Bedarf vorübergehend erhöht werden. Dies ist in der Azure-

Dokumentation beschrieben: "Dynamisches Erhöhen oder verringern der Volume-Kontingente". Der Codeabschnitt dieser Aufgabe enthält den folgenden Text:

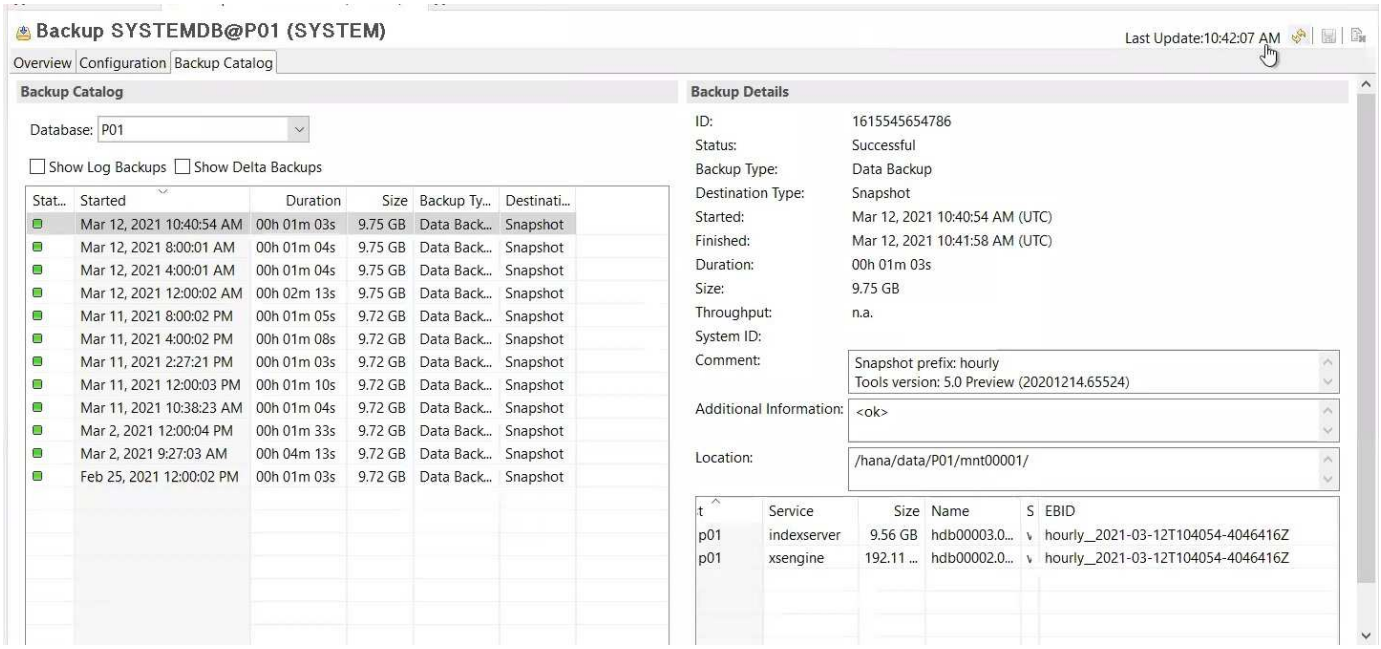
```
$_include_tool(unix_header.sh)_$
sudo /mnt/software/scripts/sc-system-refresh/sc-system-refresh.sh recover
$_system(target_db, id)_$ > $_logfile_$
```

Dieses Skript wird wieder mit dem verwendet `recover` Befehl und die Ziel-DB-SID.

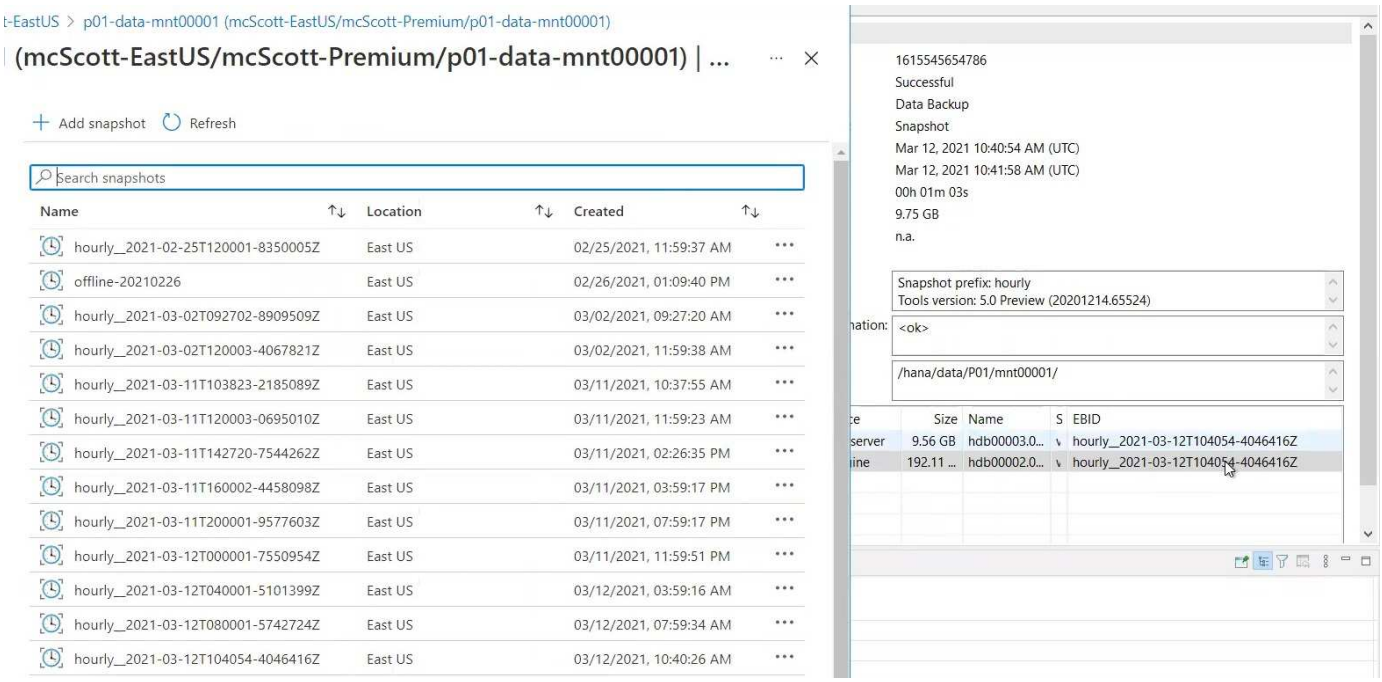
SAP HANA-Systemaktualisierungsvorgang

In diesem Abschnitt zeigt eine Beispielaktualisierung der Laborsysteme die Hauptschritte dieses Workflows.

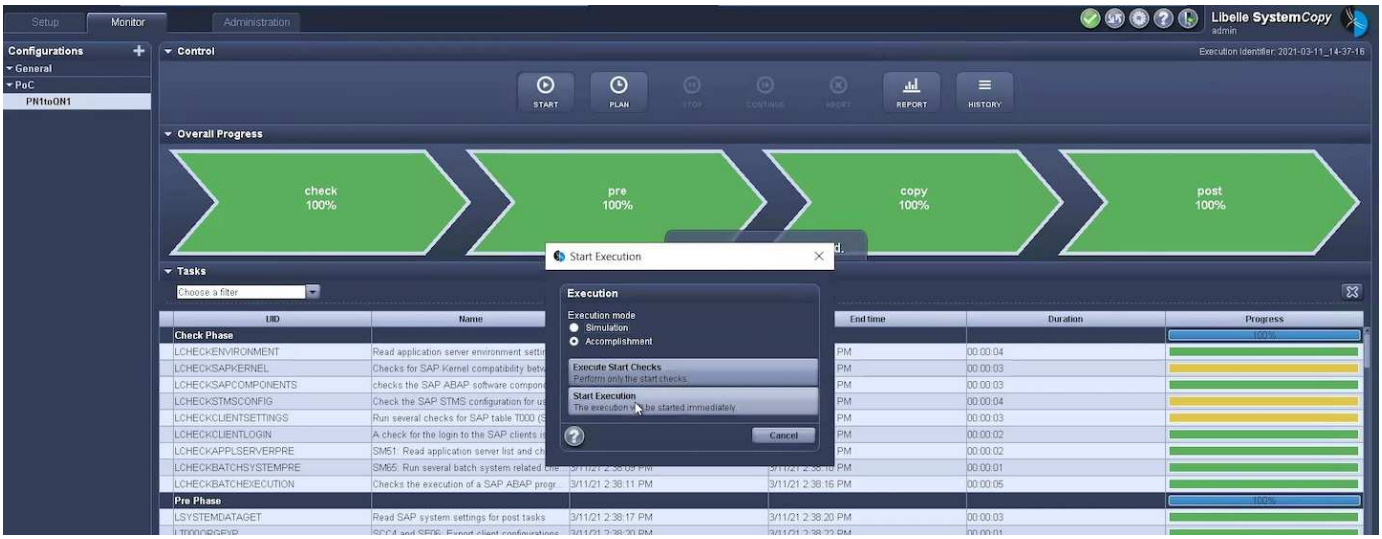
Es wurden regelmäßige und On-Demand Snapshot Kopien für die P01-Quelldatenbank erstellt, wie im Backup-Katalog aufgelistet.



Für den Aktualisierungsvorgang wurde das aktuelle Backup vom 12. März verwendet. Im Abschnitt Backup-Details wird die externe Backup-ID (EBID) für dieses Backup aufgeführt. Dies ist der Name der Snapshot Kopie des entsprechenden Backup der Snapshot Kopie auf dem Azure NetApp Files Daten-Volume, wie in der folgenden Abbildung dargestellt.

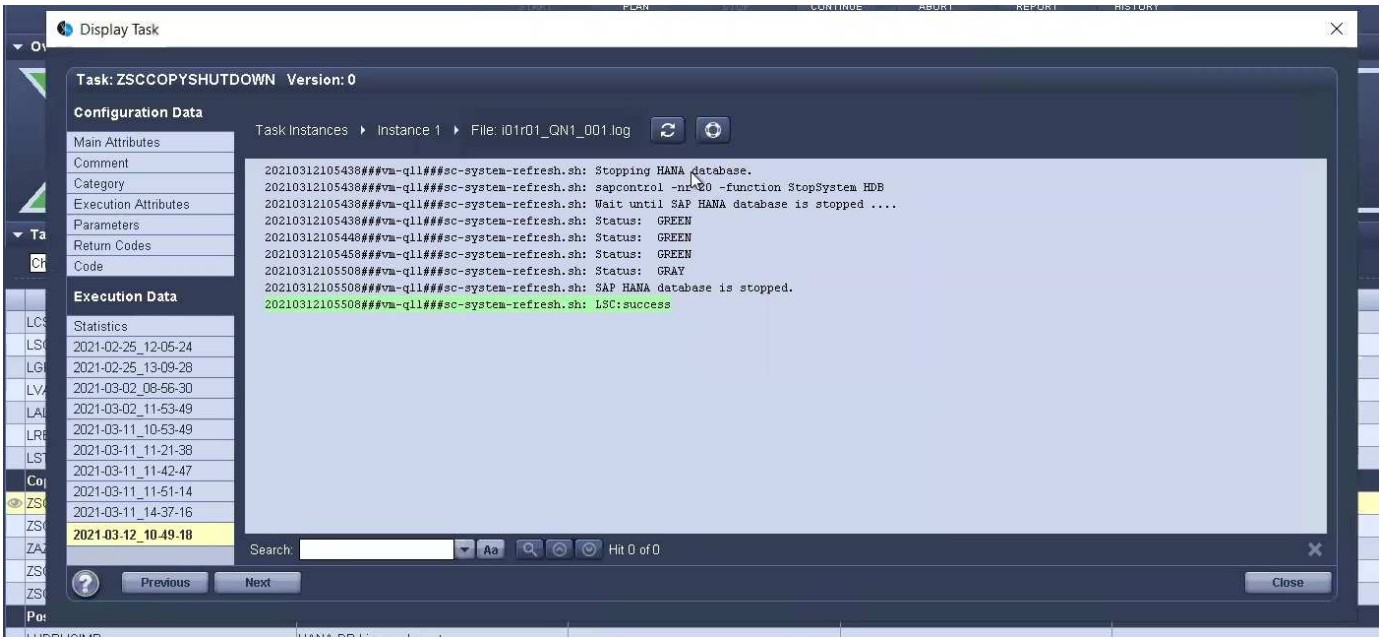


Um den Aktualisierungsvorgang zu starten, wählen Sie in der LSC-GUI die korrekte Konfiguration aus, und klicken Sie dann auf Ausführen starten.

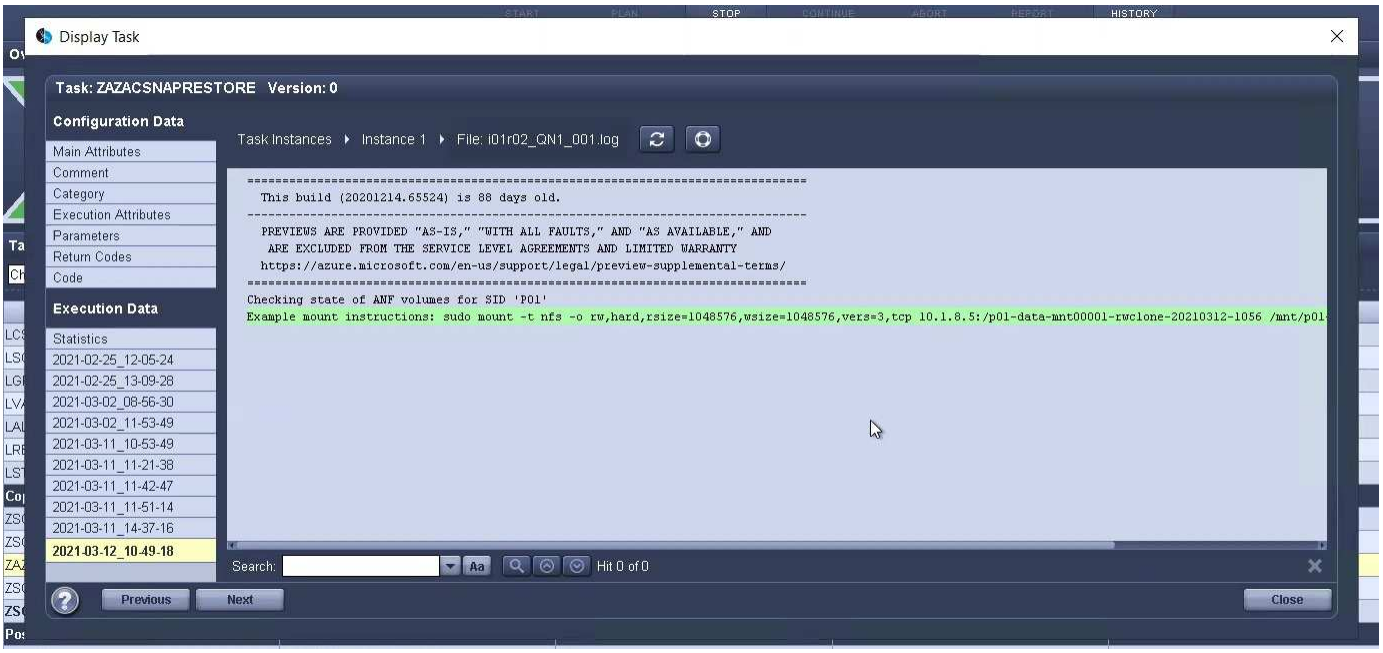


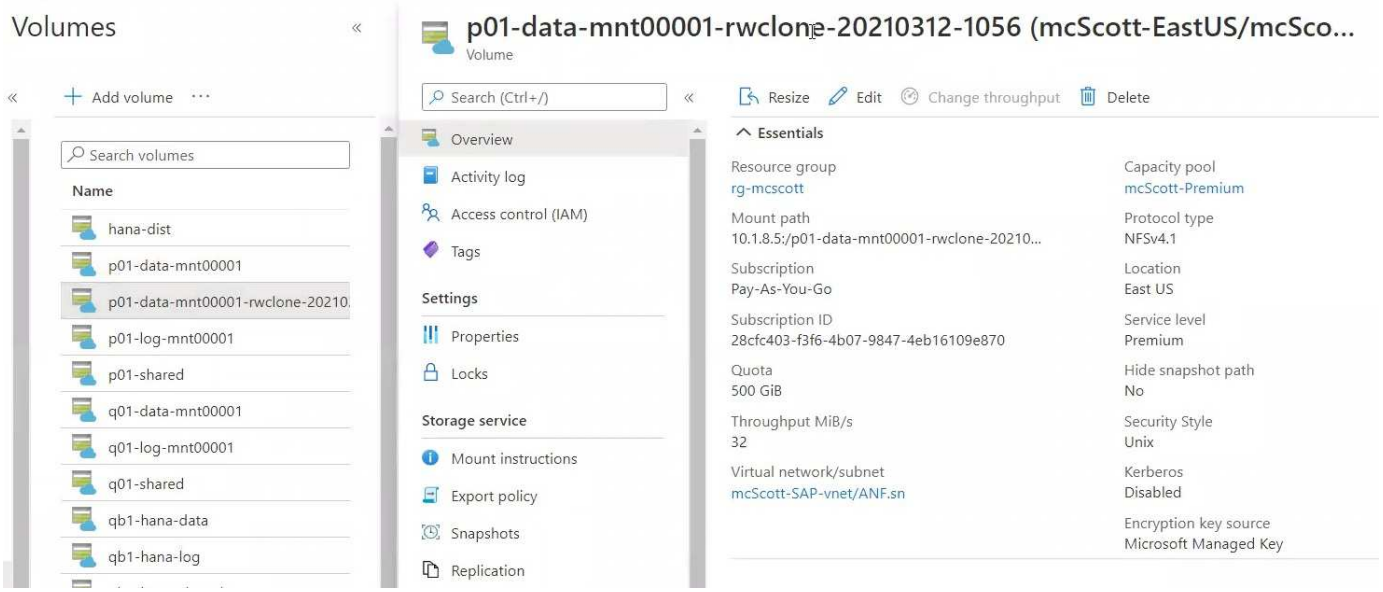
LSC startet die Ausführung der Aufgaben der Prüfphase gefolgt von den konfigurierten Aufgaben der Vorphase.

Als letzter Schritt der Vorphase wird das Ziel-SAP-System gestoppt. In der folgenden Kopierungsphase werden die im vorherigen Abschnitt beschriebenen Schritte ausgeführt. Zunächst wird die SAP HANA-Zieldatenbank angehalten, und das alte Azure NetApp Files-Volume wird vom Betriebssystem abgehängt.

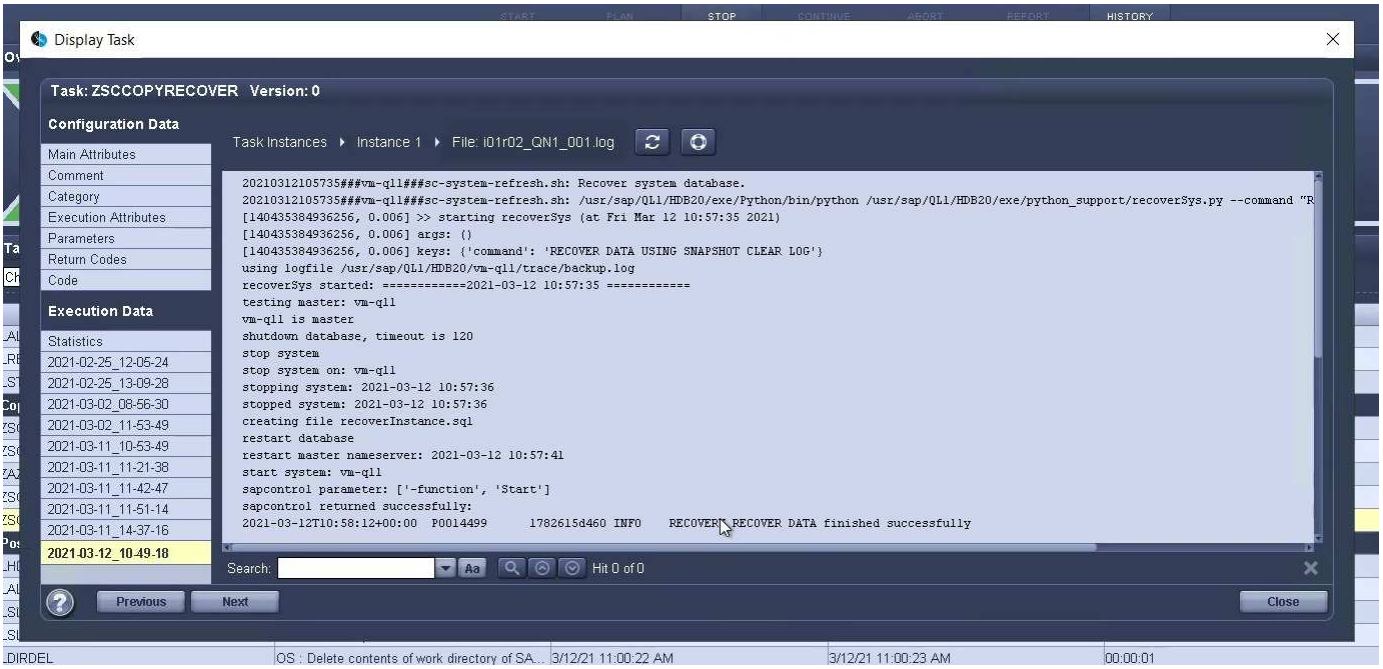


Die Aufgabe ZAZACSNAPRESTORE erstellt dann aus der vorhandenen Snapshot Kopie des P01 Systems ein neues Volume als Klon. Die folgenden zwei Bilder zeigen die Protokolle der Aufgabe in der LSC GUI und das geklonte Azure NetApp Files Volume im Azure-Portal.





Dieses neue Volume wird dann auf den Ziel-DB-Host gemountet und die Systemdatenbank wiederhergestellt – mittels der Snapshot Kopie. Nach der erfolgreichen Recovery wird die SAP HANA-Datenbank automatisch gestartet. Dieser Start der SAP HANA-Datenbank nimmt die meiste Zeit der Kopiephase in Anspruch. Die verbleibenden Schritte sind normalerweise innerhalb weniger Sekunden oder einiger Minuten abgeschlossen, unabhängig von der Größe der Datenbank. Die folgende Abbildung zeigt, wie die Systemdatenbank mit von SAP bereitgestellten Python Recovery-Skripten wiederhergestellt wird.



Nach der Kopiephase wird der LSC mit allen definierten Schritten der Post-Phase fortgesetzt. Wenn die Systemaktualisierung vollständig abgeschlossen ist, ist das Zielsystem wieder betriebsbereit und kann voll genutzt werden. Mit diesem Lab-System betrug die Gesamtlaufzeit für die Aktualisierung des SAP-Systems etwa 25 Minuten, wovon die Kopiephase knapp 5 Minuten in Anspruch genommen hat.

Wo finden Sie weitere Informationen und Versionsverlauf

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- NetApp Produktdokumentation

  "https://docs.netapp.com"

Versionsverlauf

Version	Datum	Versionsverlauf Des Dokuments
Version 1.0	April 2022	Erste Version.

Lösungen Im Überblick

SB-3978: Lifecycle Management für SAP HANA

NetApp bietet eine Lifecycle-Management-Lösung, die vollständig in die Tools integriert ist, die SAP-Administratoren bei täglichen Aufgaben wie SAP Landscape Management (SAP Lama) einsetzen, um die Herausforderungen der langsamen Implementierung von Funktionen, mangelnden Automatisierung und Produktivitätsverlust zu meistern. Ziel ist es, den Bereitstellungs-Workflow von der vor- bis zur Nachbearbeitung zu vereinfachen. Dies schließt alle Aufgaben auf der Software- und Storage-Ebene ein, die zur Erstellung einer Kopie des Produktionssystems erforderlich sind. Mit dieser Lösung können Administratoren mit nur wenigen Klicks eine Entwicklungs- und Testumgebung erstellen. So wird das Lifecycle Management optimiert.

https://www.netapp.com/pdf.html?item=/media/6996-sb-3978pdf.pdf

SB-3965: Backup und Wiederherstellung für SAP HANA

Die Herausforderung

Bei Sicherungs- und Wiederherstellungsvorgängen für SAP HANA steht Ihr Unternehmen vor den folgenden Herausforderungen: • Lange Sicherungsvorgänge mit Leistungseinbußen bei SAP-Produktionssystemen • Inakzeptable Systemausfallzeiten aufgrund langer Wiederherstellungsvorgänge • Schrumpfende Sicherungsfenster aufgrund der Kritikalität der Anwendungen • Die Notwendigkeit einer flexiblen Lösung zur Minderung logischer Beschädigungen

Die Lösung

Mit NetApp®-Speicherlösungen, auf denen die Datenverwaltungssoftware NetApp ONTAP® ausgeführt wird, in Kombination mit der Datensicherungssoftware NetApp SnapCenter ® können Sie all diese Herausforderungen meistern. Und mit der in der ONTAP -Software enthaltenen NetApp Snapshot™-Technologie können Sie in Sekundenschnelle Backups erstellen oder Wiederherstellungsvorgänge für Datensätze beliebiger Größe ausführen. SAP HANA unterstützt die Verwendung speicherbasierter Snapshot-Kopien als gültigen Sicherungsvorgang.

https://www.netapp.com/pdf.html?item=/media/6997-sb-3965pdf.pdf

SB-3968: Disaster Recovery für SAP HANA

Die Herausforderung

Geschäftskontinuität ist in IT-Organisationen von entscheidender Bedeutung. Sie müssen in der Lage sein, Hochverfügbarkeitsdienste für die unternehmenskritischen Anwendungen bereitzustellen, die ihre Kunden für den Betrieb ihrer Geschäfte benötigen. Andernfalls müssen ihre Kunden mit Produktivitätseinbußen rechnen und bei E-Commerce-Unternehmen kann es zu direkten Umsatzeinbußen kommen.

Die Lösung

NetApp hat ein umfassendes Portfolio an Technologien und Tools entwickelt, die IT-Organisationen dabei unterstützen, ihre Disaster Recovery-Pläne zu erstellen oder anzupassen, um allen Geschäftsanforderungen gerecht zu werden:

https://www.netapp.com/pdf.html?item=/media/6998-sb-3968pdf.pdf

SB-4292: SAP-Automatisierung mit Ansible

Der Schwerpunkt dieses Dokuments liegt auf der Integration von NetApp® Storage-Systemen – ob On-Premises, in einer Public-Cloud-IaaS-Umgebung oder in einer Hybrid Cloud – mithilfe von Ansible Playbooks und benutzerdefinierten Skripten in SAP Landscape Management (Lama).

Lösungsüberblick

SAP-Systeme sind sehr komplex. Aber für die Unternehmen, die SAP einsetzen, sind diese Systeme zentral für ihre Geschäftsprozesse. Durch die Automatisierung wiederkehrender täglicher Betriebsaufgaben können SAP-Systemadministratoren mehr Systeme mit weniger Aufwand managen, wiederholbare Ergebnisse liefern und menschliche Fehler minimieren.

Der Schwerpunkt dieses Dokuments liegt auf der Integration von NetApp® Storage-Systemen – ob On-Premises, in einer Public-Cloud-IaaS-Umgebung oder in einer Hybrid Cloud – mithilfe von Ansible Playbooks und benutzerdefinierten Skripten in SAP Landscape Management (Lama). Dank dieser Integration können SAP-Administratoren mit NetApp Snapshot™ und NetApp FlexClone®-Technologie SAP-Systemaktualisierungen beschleunigen.

Zielgruppe

Dieses Dokument richtet sich an SAP-Systemadministratoren, die bisher noch nicht viel (oder keine) Erfahrung mit der Ansible-Automatisierung hatten. Es sollte Ihnen den Einstieg in Ansible erleichtern, Ihre ersten Playbooks ausführen und Ihren ersten SAP Lama-basierten Systemaktualisierungsvorgang konfigurieren und ausführen.

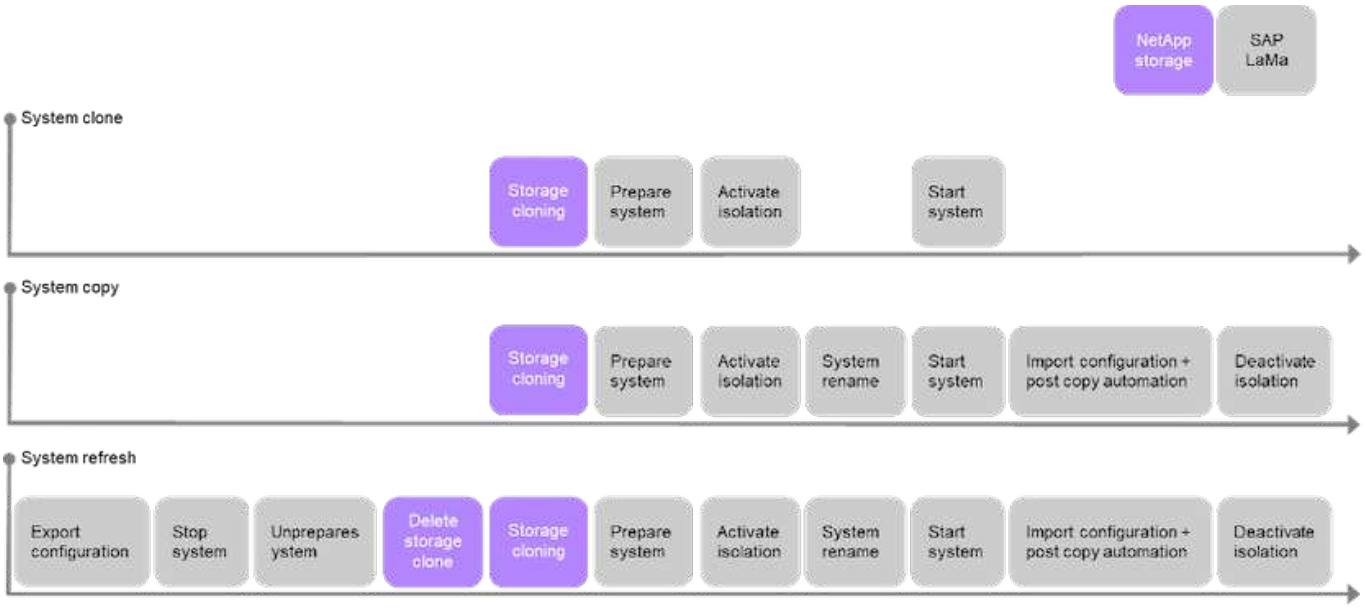
SAP Szenarien für Klonen, Kopieren und Aktualisieren von Systemen

Der Begriff SAP-Systemkopie wird oft als Synonym für drei verschiedene Prozesse verwendet: SAP-Systemklon, SAP-Systemkopie und SAP-Systemaktualisierung. Es ist wichtig, zwischen den verschiedenen Vorgängen zu unterscheiden, da sich Workflows und Anwendungsfälle unterscheiden.

- **SAP-Systemklon**. Ein SAP-Systemklon ist ein identischer Klon eines SAP-Quellsystems. SAP Systemklone werden typischerweise zur Beseitigung logischer Beschädigungen oder zum Testen von Disaster-Recovery-Szenarien eingesetzt. Bei einem Klonvorgang des Systems bleiben der Hostname, die Instanznummer und die sichere Kennung (SID) identisch. Daher ist es wichtig, für das Zielsystem ein ordnungsgemäßes Netzwerkfechten einzurichten, um sicherzustellen, dass keine Kommunikation mit der Produktionsumgebung besteht.
- **SAP-Systemkopie**. Eine SAP Systemkopie ist die Einrichtung eines neuen SAP Zielsystems mit Daten aus einem SAP-Quellsystem. Das neue Zielsystem könnte beispielsweise ein zusätzliches Testsystem mit Daten aus dem Produktionssystem sein. Hostname, Instanznummer und SID unterscheiden sich für die Quell- und Zielsysteme.
- **SAP-Systemaktualisierung**. Eine SAP-Systemaktualisierung ist eine Aktualisierung eines bestehenden

SAP-Zielsystems mit Daten aus einem SAP-Quellsystem. Das Zielsystem ist typischerweise Teil einer SAP-Transportlandschaft – beispielsweise eines Qualitätssicherungssystems –, das mit Daten aus dem Produktionssystem aktualisiert wird. Hostname, Instanznummer und SID unterscheiden sich für die Quell- und Zielsysteme.

Das folgende Bild zeigt die Schritte des SAP-Systems zum Klonen, Kopieren und Aktualisieren des Lama-Workflows, die mit NetApp-Storage zusammenhängen.

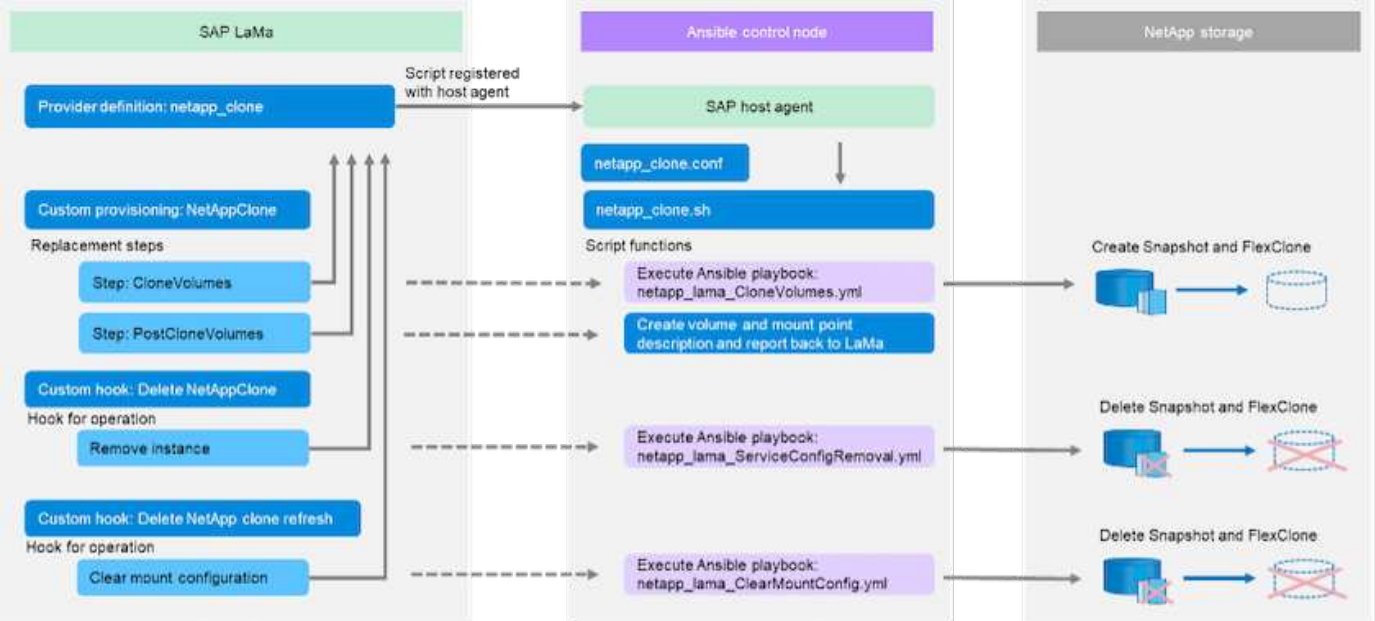


Lösungstechnologie

Die Gesamtlösung besteht aus den folgenden Hauptkomponenten:

- SAP Lama-System
- NetApp Storage-System
- Ansible-Steuerungsknoten mit installiertem SAP Host Agent. Wir empfehlen die Verwendung der Red hat Ansible Automation Platform, da diese weitere Vorteile bietet, z. B.:
  - Mithilfe von KI können Codeempfehlungen für Automatisierungsaufgaben erstellt werden
  - Verringerung manueller Aufgaben durch ereignisgesteuerte Automatisierung
  - Definiert, konsistent und portabel
  - Skalierung von Automatisierung über verschiedene Umgebungen hinweg
  - Schnellere Automatisierung durch vorgefertigte Inhalte
  - Nachverfolgung und Management der Automatisierung mithilfe umfassender Reporting- und Observability-Kennzahlen
  - Erstellen von Aufgaben, Modulen und Playbooks

Die folgende Abbildung zeigt, wie SAP Lama und NetApp-Storage-Systeme über Ansible Playbooks auf einem dedizierten Ansible-Host integriert werden, der durch vom SAP Host Agent ausgeführte Shell-Skripte ausgelöst wird.

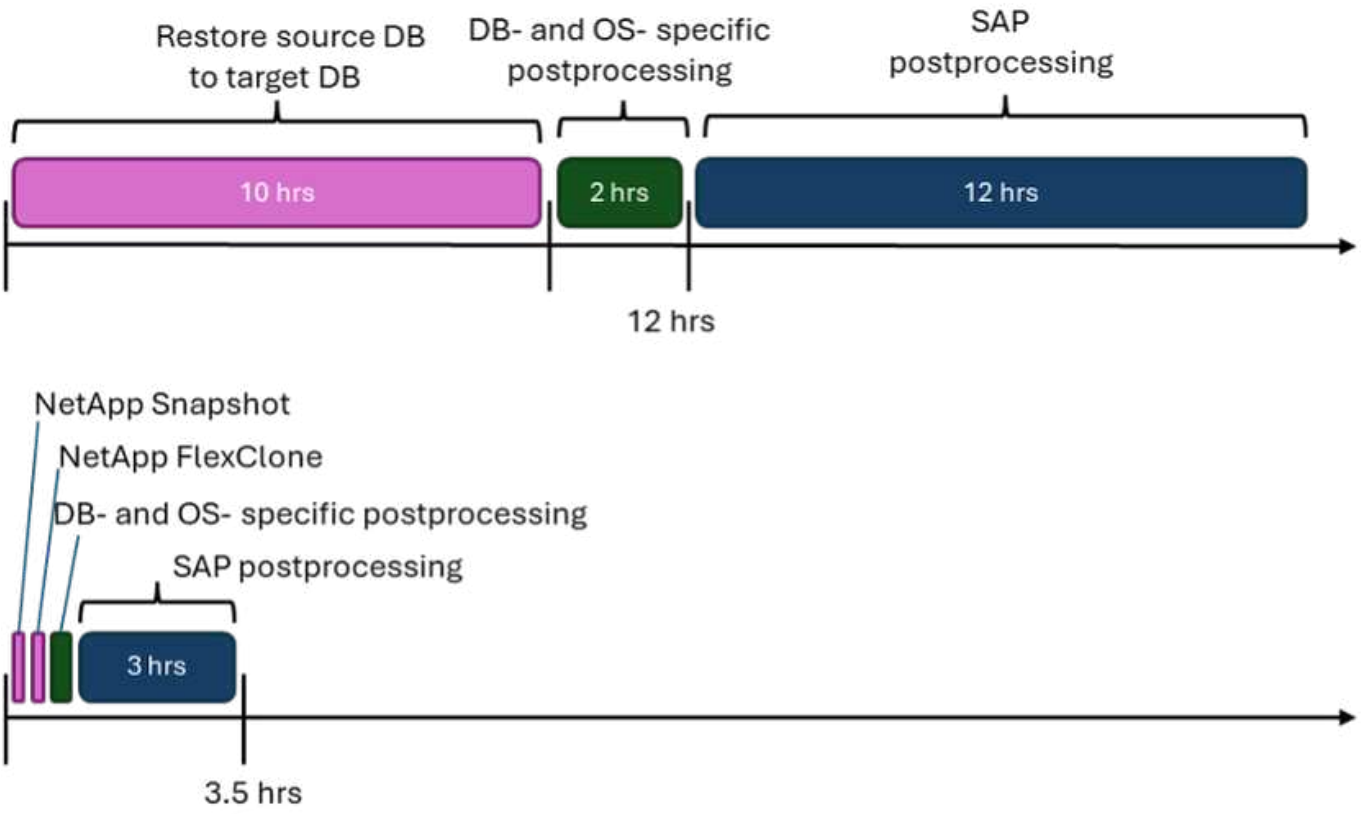


Zusammenfassung des Anwendungsfalls

Es gibt mehrere Szenarien, in denen Daten aus einem Quellsystem einem Zielsystem zu Test- oder Schulungszwecken zur Verfügung gestellt werden müssen. Diese Test- und Trainingssysteme müssen regelmäßig mit Daten aus dem Quellsystem aktualisiert werden, um sicherzustellen, dass Tests und Trainings mit dem aktuellen Datensatz durchgeführt werden. Diese Vorgänge für die Systemaktualisierung umfassen mehrere Aufgaben auf der Infrastruktur-, Datenbank- und Applikationsebene und können je nach Grad der Automatisierung mehrere Tage dauern.

Um die erforderlichen Aufgaben auf Infrastruktur- und Datenbankebene zu beschleunigen und zu automatisieren, können Sie Klon-Workflows für SAP Lama und NetApp verwenden. Anstatt ein Backup vom Quellsystem zum Zielsystem wiederherzustellen, verwendet SAP Lama die Snapshot- und FlexClone-Technologie von NetApp, damit Aufgaben, die zum Starten einer Datenbank erforderlich sind, innerhalb von Minuten anstatt von Stunden ausgeführt werden können, wie in der folgenden Abbildung dargestellt. Die für den Klonprozess benötigte Zeit hängt nicht von der Größe der Datenbank ab, daher können selbst sehr große Systeme in wenigen Minuten erstellt werden. Sie können die Laufzeit weiter reduzieren, indem Sie Aufgaben auf der Betriebssystem- und Datenbankebene sowie auf der SAP-Nachverarbeitungsseite automatisieren.

Die folgende Abbildung zeigt mögliche Verbesserungen bei der betrieblichen Effizienz durch den Einsatz von Automatisierung.



Integration der verschiedenen Technologiekomponenten

Um SAP Lama in NetApp-Storage-Systeme mithilfe von Ansible zu integrieren, benötigen Sie einen Node, auf dem Sie Ansible Playbooks ausführen können. Wir empfehlen den Einsatz der Ansible Automation Platform. Um Shell-Skripte und Ansible-Playbooks auf diesem Host auszuführen, die von SAP Lama gestartet wurden, benötigen Sie einen SAP-Host-Agent, der auf diesem Server ausgeführt wird. SAP Host Agent übernimmt die bidirektionale Kommunikation mit SAP Lama und führt Shell-Skripte aus, die die eigentlichen Playbooks auslösen.

Diese locker gekoppelte Architektur gibt Ihnen die Freiheit, Workflows von SAP Lama und auch außerhalb von SAP Lama zu starten. Playbooks und die entsprechende Logik müssen nur einmal konfiguriert werden und können für verschiedene Szenarien und Anwendungsfälle verwendet werden.

Schlussfolgerung

Die Kombination aus NetApp, SAP Lama und Ansible-Automatisierungsplattform bietet eine leistungsstarke Lösung, die den Zeit- und Arbeitsaufwand für die komplexesten und zeitaufwendigsten Aufgaben in Bezug auf die SAP-Systemadministration erheblich reduzieren kann. Diese Kombination kann auch helfen, Konfigurationsabweichungen zu vermeiden, die durch menschliches Versagen zwischen den Systemen verursacht werden können.

Da Systemaktualisierungen, Kopien, Klone und Disaster Recovery-Tests sehr sensible Verfahren sind, setzt die Implementierung einer solchen Lösung wertvolle Administrationszeit frei. Sie kann auch das Vertrauen stärken, das der Rest der Organisation in den SAP-Systemadministratoren haben wird: Sie werden sehen, wie viel einfacher es ist, Systeme für Tests oder andere Zwecke zu kopieren und wie viel Zeit für die Fehlerbehebung eingespart werden kann.

Wo Sie weitere Informationen finden

Sehen Sie sich die folgenden Dokumente und Websites an, um mehr über die in diesem Dokument beschriebenen Daten zu erfahren:

- "Automatisierung des laufenden Tag-1- und Tag-2-Betriebs durch die Verwendung von Ansible Playbooks für NetApp ONTAP®"
- "NetApp-spezifische Ansible-Dokumentation"
- "NetApp ONTAP Ansible-Module und vollständige Dokumentation"
- "Red Hat Ansible Automation Platform"

Versionsverlauf

Version	Datum	Zusammenfassung aktualisieren
Version 0.1	03.2023	Entwurf.
Version 0.2	01.2024	Überprüfung und einige kleinere Korrekturen
Version 0.3	06.2024	In HTML-Format konvertiert

SB-4293: Automatisieren von SAP-Systemkopien, -Aktualisierungen und -Klonworkflows mit ALPACA und NetApp SnapCenter

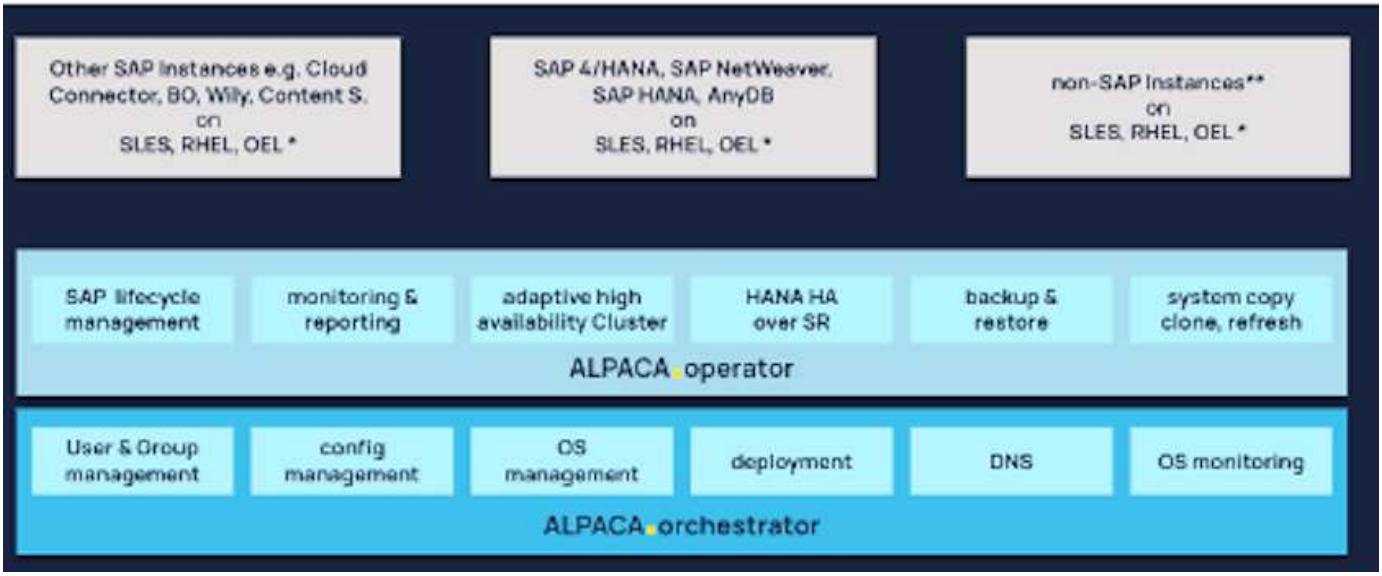
Dieses Dokument konzentriert sich auf die Integration von NetApp® Snapshot™ und FlexClone® Technologien in ALPACA-Automatisierungs-Workflows.

Lösungsüberblick

Der Betrieb von SAP Systemen und Lösungen ist sehr komplex. Für Unternehmen, die SAP einsetzen, sind die Systeme und Services jedoch zentral für ihre Geschäftsprozesse. Durch die Automatisierung wiederkehrender täglicher Betriebsaufgaben, wie zum Beispiel beim Kopieren und Aktualisieren von Systemen, können SAP-Systemadministratoren mehr Systeme mit weniger Aufwand managen, wiederholbare Ergebnisse liefern und menschliche Fehler reduzieren.

Dieses Dokument konzentriert sich auf die Integration von NetApp® Snapshot™ und FlexClone® Technologien in ALPACA-Automatisierungs-Workflows.

Die ALPACA Suite (Cloud and Anywhere) automatisiert proaktiv Landschaften. Es handelt sich um eine umfassende Managementoberfläche, die eine detaillierte Überwachung und Überwachung Ihrer gesamten SAP-Landschaft ermöglicht. ALPACA optimiert und beschleunigt den Betrieb der SAP-Infrastruktur und sorgt so für optimale Verfügbarkeit und Transparenz. Die Lösung bietet eine umfassende Palette an Tools für das Management der gesamten IT-Landschaft, einschließlich der Infrastruktur, und meldet proaktiv Anomalien wie Serviceunterbrechungen, Unterbrechung von Jobs und Überlastungen. Die Suite lässt sich nahtlos in On-Premises-, Hybrid- und All-Cloud-Umgebungen betreiben, einschließlich Multi-Cloud-Szenarien, und garantiert Anpassungsfähigkeit an jede Infrastruktur. Dieses modulbasierte Framework automatisiert standardmäßige und regelmäßige SAP-Administrationsaufgaben sowie komplexe Szenarien wie Failover während eines Ausfalls. Administratoren/Experten, Betreiber und Manager, ALPACA bietet diesen Profis ein hohes Maß an Kontrolle und Automatisierung.



In diesem Dokument wird beschrieben, wie ALPACA in NetApp SnapCenter integriert wird, das Tool zur Orchestrierung Snapshot-basierter Backups, zur Durchführung von Wiederherstellungen und zur Erstellung von FlexClone Volumes. Dank dieser Integration können SAP-Administratoren die täglichen Betriebsaufgaben des SAP-Systems deutlich beschleunigen. Die NetApp Snapshot, FlexClone und SnapRestore Technologien beschleunigen Backup-, Wiederherstellungs- und Klonvorgänge, da die NetApp Storage-Technologie pointer-basiert ist. Dieser Ansatz ist schnell und senkt auch den Storage Overhead bei Klonvorgängen, da nur neue und geänderte Daten (keine vorhandenen Daten) auf das Storage-Medium geschrieben werden müssen. Dies gilt unabhängig davon, ob es sich um ein lokales NetApp Storage-System oder eine NetApp Storage-Lösung bei einem der drei großen Cloud-Provider handelt.

Zielgruppe

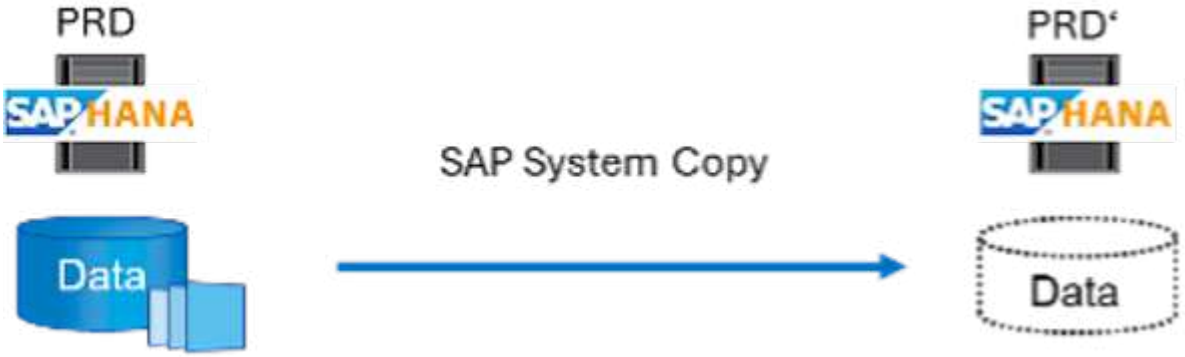
Dieses Dokument richtet sich an SAP-Systemadministratoren, die SAP-Systemkopien manuell durchgeführt haben und diese Aktivität mit ALPACA automatisieren möchten. Das beabsichtigte Ziel, die Technologien von NetApp Snapshot und FlexClone, orchestriert durch NetApp SnapCenter, mit ALPACA Workflows zu kombinieren, ist es, die Dauer von vollständig automatisierten SAP Systemkopien zu verringern.

SAP Szenarien für Klonen, Kopieren und Aktualisieren von Systemen

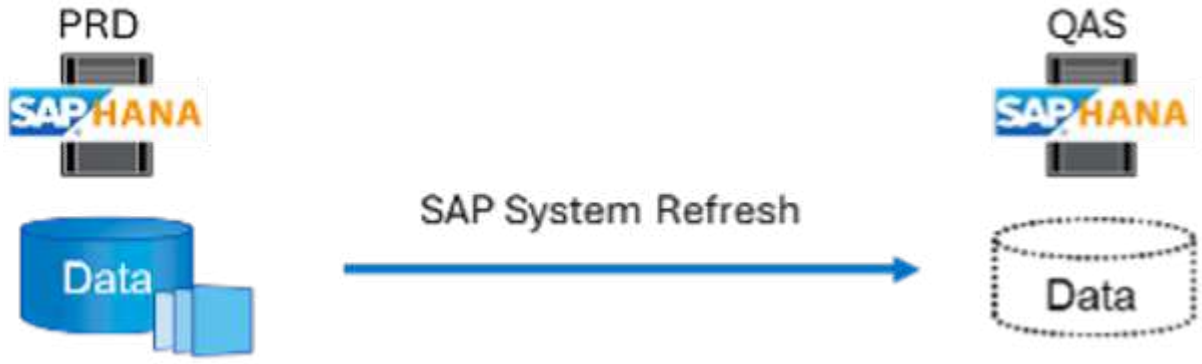
Der Begriff SAP-Systemkopie wird oft als Synonym für drei verschiedene Prozesse verwendet: SAP-Systemklon, SAP-Systemkopie und SAP-Systemaktualisierung. Es ist wichtig, zwischen diesen Vorgängen zu unterscheiden, da die Workflows und Anwendungsfälle unterschiedlich sind.

- **SAP-Systemklon**. Ein SAP-Systemklon ist ein identischer Klon eines SAP-Quellsystems. SAP Systemklone werden typischerweise zur Beseitigung logischer Beschädigungen oder zum Testen von Disaster-Recovery-Szenarien eingesetzt. Bei einem Klonvorgang des Systems bleiben der Host-Name, die Instanz-Nummer und die sichere Kennung (SID) identisch. Es ist daher wichtig, eine korrekte Netzwerkabschaltung für das Zielsystem zu schaffen, um sicherzustellen, dass keine Kommunikation mit der Produktionsumgebung erfolgt.

- **SAP-Systemkopie**. Eine SAP Systemkopie ist die Einrichtung eines neuen SAP Zielsystems mit Daten aus einem SAP-Quellsystem. Das neue Zielsystem könnte beispielsweise ein zusätzliches Testsystem mit Daten aus dem Produktionssystem sein. Der Hostname, die Instanznummer und die SID sind für die Quell- und Zielsysteme unterschiedlich. Das neue System ist nicht vom Quellsystem isoliert.



- **SAP-Systemaktualisierung**. Eine SAP-Systemaktualisierung ist eine Aktualisierung eines bestehenden SAP-Zielsystems mit Daten aus einem SAP-Quellsystem. Das Zielsystem ist typischerweise Teil einer SAP-Transportlandschaft – beispielsweise eines Sandbox-Systems –, das mit Daten aus dem Produktionssystem aktualisiert wird. Hostname, Instanznummer und SID unterscheiden sich für die Quell- und Zielsysteme.



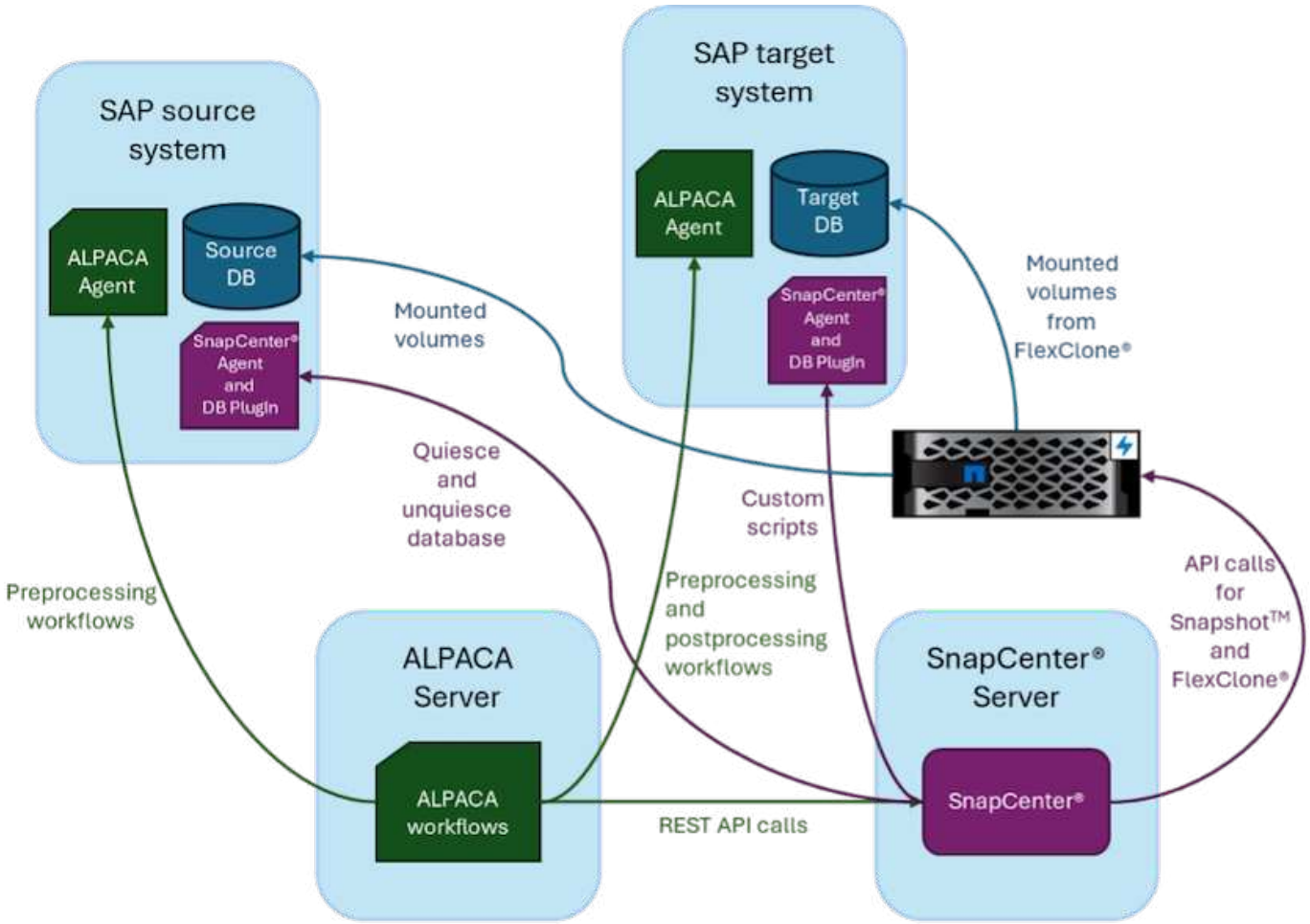
Obwohl es sich hier um drei verschiedene Anwendungsfälle handelt, bleibt der Datenmanagementprozess unverändert. Alle drei Anwendungsfälle basieren auf derselben zugrunde liegenden Datenmanagement-Technologie – NetApp Snapshot und FlexClone.

Lösungstechnologie

Die Gesamtlösung besteht aus den folgenden Hauptkomponenten:

- SAP-Quellsystem mit installiertem SnapCenter-Agent und SnapCenter-Datenbank-Plug-in
- SAP-Zielsystem mit installiertem SnapCenter-Agent und SnapCenter-Datenbank-Plug-in
- ALPACA-System mit konfiguriertem SAP-Quell- und SAP-Zielsystem
- NetApp SnapCenter-Server
- NetApp Storage-System:
  - Physische Hardware vor Ort: Die AFF-A-, AFF-C-, ASA-A-, ASA-C- oder FAS-Serie
  - Softwaredefinierter Storage vor Ort: ONTAP® Select
  - NetApp Cloud-Storage:
    - Cloud Volumes ONTAP für AWS, Google Cloud oder Azure
    - Azure NetApp Dateien
    - Amazon FSX für NetApp ONTAP

Die folgende Abbildung zeigt den ALPACA-Server, den NetApp SnapCenter-Server, das NetApp-Speichersystem, die SAP-Quell- und SAP-Zielsysteme und wie alles integriert ist. Ziel ist es, die Integration durch die Verwendung der SnapCenter REST API so flexibel wie möglich zu gestalten, um eine maximale Wiederverwendung der Konfigurationsarbeiten zu gewährleisten, die bereits innerhalb der ausliegenden Komponenten durchgeführt wurden.

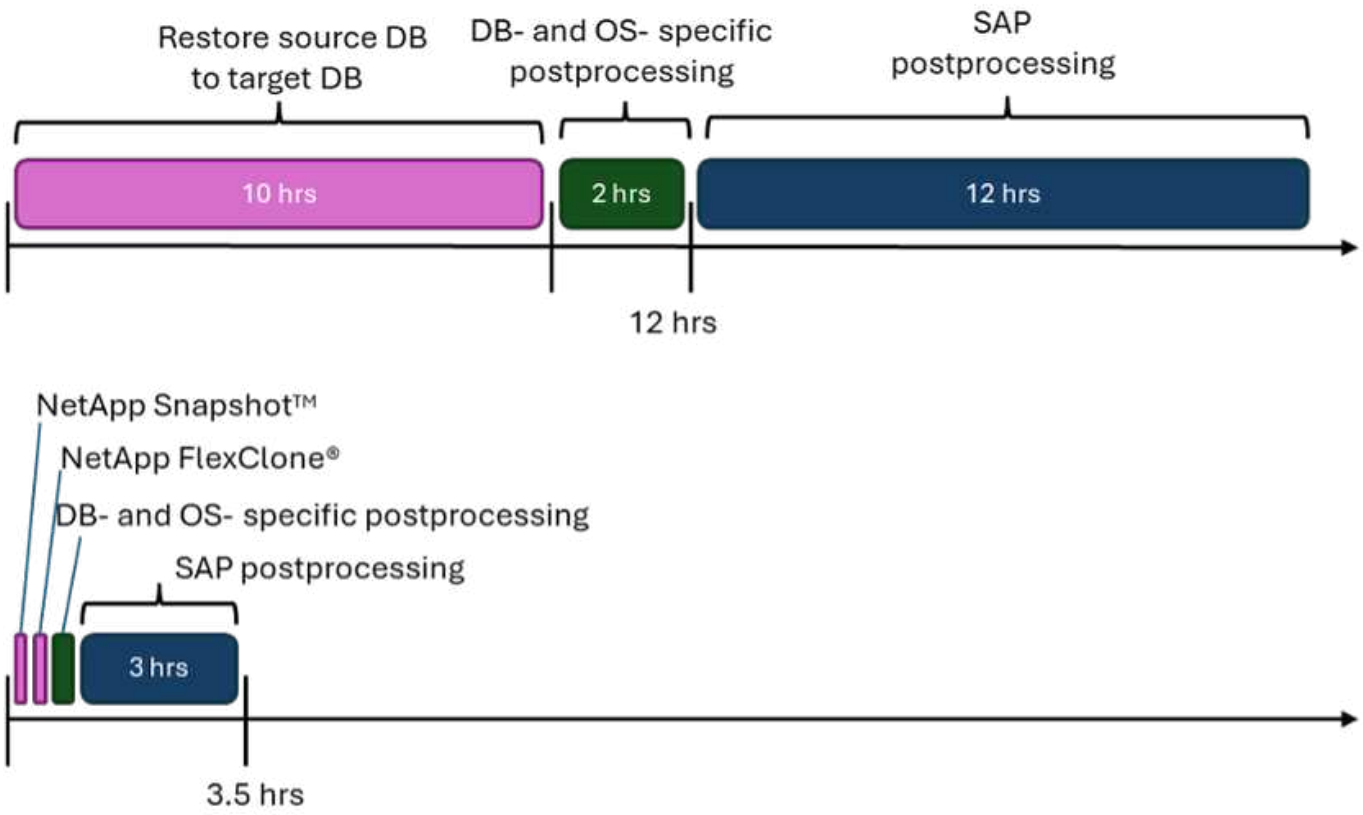


Zusammenfassung des Anwendungsfalls

Es gibt mehrere Szenarien, in denen Daten aus einem Quellsystem einem Zielsystem zu Test- oder Schulungszwecken zur Verfügung gestellt werden müssen. Diese Test- und Trainingssysteme müssen regelmäßig mit Daten aus dem Quellsystem aktualisiert werden, um sicherzustellen, dass Tests und Trainings mit dem aktuellen Datensatz durchgeführt werden. Diese Vorgänge für die Systemaktualisierung umfassen mehrere Aufgaben auf der Infrastruktur-, Datenbank- und Applikationsebene und können je nach Grad der Automatisierung mehrere Tage dauern.

Um Vorgänge zu beschleunigen, Aufgaben zu automatisieren und menschliche Fehler auf Infrastruktur-, Datenbank- und Applikationsebene zu eliminieren, können Sie ALPACA Workflows verwenden. Anstatt ein Backup aus dem Quellsystem, das sehr zeitaufwendig und mit hohem Ressourcenverbrauch verbunden ist, auf das Zielsystem wiederherzustellen, verwendet diese Integration NetApp Snapshots und FlexClone Technologien. Alle Aufgaben, die für das Hochfahren einer Datenbank erforderlich sind, sind in wenigen Minuten statt in mehreren Stunden erledigt. Die für den Klonprozess benötigte Zeit hängt nicht von der Größe der Datenbank ab, daher können selbst sehr große Systeme in wenigen Minuten erstellt werden. ALPACA reduziert die Laufzeit weiter, indem Aufgaben auf Betriebssystem- und Datenbankebene sowie auf der SAP-Nachverarbeitungsseite automatisiert werden.

Die folgende Abbildung zeigt mögliche Verbesserungen bei der betrieblichen Effizienz durch den Einsatz von Automatisierung.



Integration der Technologiekomponenten

Die eigentliche Integration von SnapCenter in einen ALPACA-Workflow besteht aus der Verwendung von Shell-Skripten für den Zugriff auf die NetApp SnapCenter-REST-API. Durch diese REST API-basierte Integration wird eine Snapshot Kopie des SAP Quellsystems erstellt, ein FlexClone Volume erstellt und im SAP Zielsystem gemountet. Storage- und SAP-Administratoren wissen, wie sie Skripte entwickeln, die von SnapCenter ausgelöst und vom SnapCenter-Agenten ausgeführt werden, um Routineaufgaben des täglichen

Betriebs zu automatisieren. Diese lose gekoppelte Architektur, die SnapCenter-Aufgaben über Shell-Skripte auslöst, ermöglicht es ihnen, ihre bestehenden Automatisierungsverfahren wiederzuverwenden, um die gewünschten Ergebnisse schneller zu erreichen, indem sie ALPACA als Workflow-Engine für die End-to-End-Automatisierung verwendet.

Schlussfolgerung

Die Kombination aus ALPACA und NetApp Datenmanagement-Technologie bietet eine leistungsstarke Lösung, die den Zeit- und Arbeitsaufwand für die komplexesten und zeitaufwendigsten Aufgaben im Zusammenhang mit der SAP-Systemadministration erheblich reduzieren kann. Diese Kombination kann auch helfen, Konfigurationsabweichungen zu vermeiden, die durch menschliches Versagen zwischen den Systemen verursacht werden können.

Da Systemaktualisierungen, Kopien, Klone und Disaster-Recovery-Tests sehr sensitive Verfahren sind, nimmt die Implementierung einer solchen Lösung wertvolle Administrationszeit frei. Darüber hinaus kann die IT das Vertrauen stärken, das die Mitarbeiter des Geschäftsbereichs in die SAP-Systemadministratoren haben. Sie werden sehen, wie viel Zeit für die Fehlerbehebung eingespart werden kann und wie viel einfacher es ist, Systeme für Tests oder andere Zwecke zu kopieren. Das gilt unabhängig davon, wo die Quell- und Zielsysteme betrieben werden – On-Premises, in einer Public Cloud, Hybrid Cloud oder Hybrid-Multi-Cloud.

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument enthaltenen Informationen finden Sie in den folgenden Dokumenten und auf den folgenden Websites:

- "ALPAKA"
- "Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter"
- "REST-APIs, die für SnapCenter Server und Plug-ins unterstützt werden"

Versionsverlauf

Version	Datum	Zusammenfassung aktualisieren
Version 0.1	04.2024	Entwurf.
Version 0.2	06.2024	In HTML-Format konvertiert

SB-4294: Automatisieren von Kopieren, Aktualisieren und Klonen von SAP Systemen mit Avantra und NetApp SnapCenter

In diesem Dokument wird beschrieben, wie Avantra mit der NetApp SnapCenter® Plattform integriert wird.

Lösungsüberblick

Der Betrieb von SAP Systemen und Lösungen ist sehr komplex. Für Unternehmen, die SAP einsetzen, sind diese Systeme und Services jedoch zentral für ihre Geschäftsprozesse. Durch die Automatisierung wiederkehrender täglicher Betriebsaufgaben, wie zum Beispiel beim Kopieren und Aktualisieren von Systemen, können SAP-Systemadministratoren mehr Systeme mit weniger Aufwand managen, wiederholbare Ergebnisse liefern und menschliche Fehler reduzieren.

Dieses Dokument konzentriert sich auf die Integration von NetApp® Snapshot™ und FlexClone® Technologien in Avantra Automatisierungs-Workflows. Avantra ist eine IT Management-Plattform, deren Schwerpunkt auf dem automatisierten Management von IT-Abläufen und -Services liegt. Es bietet Lösungen zur Überwachung, Automatisierung und Verwaltung von IT-Infrastrukturen, um die Effizienz und Zuverlässigkeit von IT-Systemen zu verbessern. Avantra ermöglicht Unternehmen, ihre IT-Umgebungen proaktiv zu überwachen, Probleme frühzeitig zu erkennen und automatisierte Aktionen zur Fehlerbehebung oder Optimierung der Systemperformance durchzuführen. Die Plattform lässt sich in der Regel in andere IT-Managementtools integrieren und kann in verschiedenen Umgebungen wie Cloud-, On-Premises- und hybriden Infrastrukturen implementiert werden.

In diesem Dokument wird beschrieben, wie Avantra mit der NetApp SnapCenter® Plattform integriert wird. NetApp SnapCenter ist das Tool zur Orchestrierung von Snapshot-basierten Backups, zur Durchführung von Wiederherstellungen und zur Erstellung von FlexClone Volumes. Dank dieser Integration können SAP-Administratoren mit NetApp-Techniken die täglichen Betriebsaufgaben für SAP-Systeme deutlich beschleunigen. Snapshot, FlexClone und NetApp SnapRestore ® Software beschleunigen Backup-, Wiederherstellungs- und Klonvorgänge, da die NetApp Storage-Technologie Pointer-basiert ist. Dieser Ansatz ist schnell. Außerdem wird der Storage-Overhead während des Klonvorgangs reduziert, da nur neue und geänderte Daten auf das Storage-Medium geschrieben werden, unabhängig davon, ob es sich um ein lokales NetApp Storage-System oder eine NetApp Storage-Lösung bei einem der drei großen Cloud-Provider handelt.

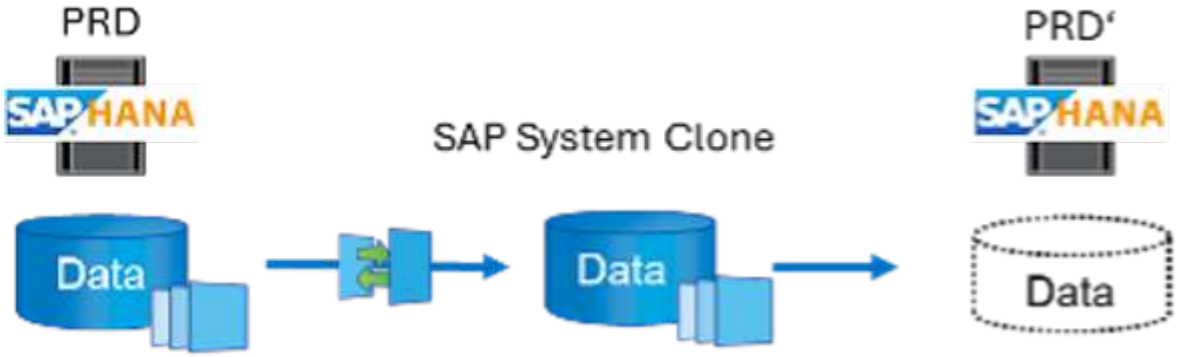
Zielgruppe

Dieses Dokument richtet sich an SAP-Systemadministratoren, die zuvor SAP-Systemkopien manuell durchgeführt haben und diese Aktivität mit Avantra automatisieren möchten. Das beabsichtigte Ziel, die Technologie von NetApp Snapshot und FlexClone, orchestriert durch NetApp SnapCenter, mit Avantra Workflows zu kombinieren, ist es, SAP Systemkopien durch vollständige Automatisierung zu beschleunigen.

SAP Szenarien für Klonen, Kopieren und Aktualisieren von Systemen

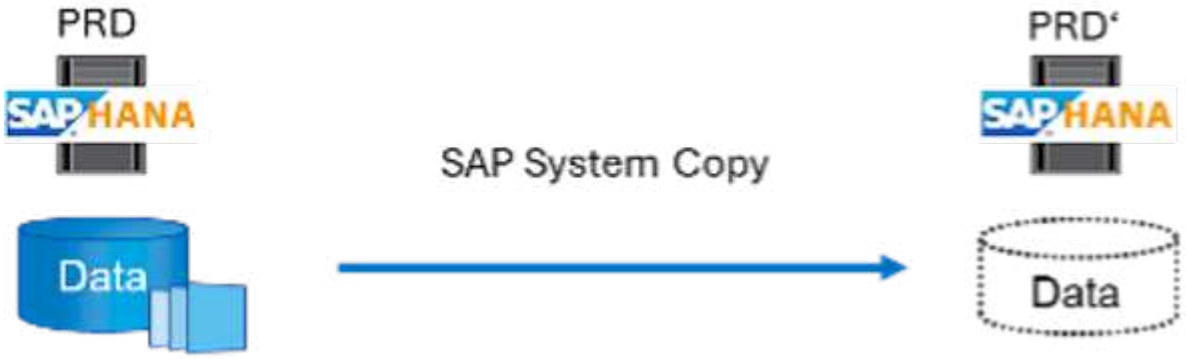
Der Begriff SAP Systemkopie wird häufig als Oberbegriff für drei verschiedene Prozesse verwendet: SAP-Systemklon, SAP-Systemkopie und SAP-Systemaktualisierung. Es ist wichtig, zwischen den verschiedenen Vorgängen zu unterscheiden, da sich Workflows und Anwendungsfälle unterscheiden.

- **SAP-Systemklon**. Ein SAP-Systemklon ist ein identischer Klon eines SAP-Quellsystems. SAP Systemklone werden typischerweise zur Beseitigung logischer Beschädigungen oder zum Testen von Disaster-Recovery-Szenarien eingesetzt. Bei einem Klonvorgang des Systems bleiben der Host-Name, die Instanz-Nummer und die sichere Kennung (SID) identisch. Daher ist es wichtig, für das Zielsystem ein ordnungsgemäßes Netzwerkfechten einzurichten, um sicherzustellen, dass keine Kommunikation mit der Produktionsumgebung besteht.

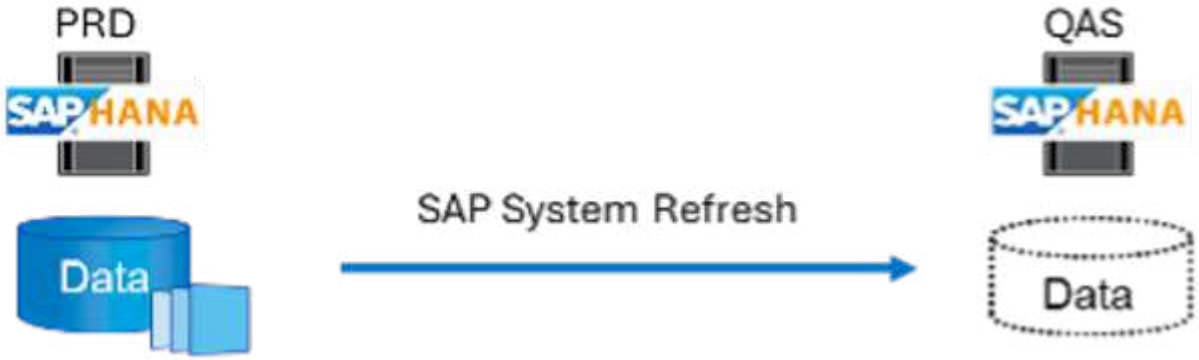


- **SAP-Systemkopie**. Eine SAP Systemkopie ist die Einrichtung eines neuen SAP Zielsystems mit Daten aus einem SAP-Quellsystem. Das Zielsystem könnte beispielsweise ein zusätzliches Testsystem mit Daten

aus dem Produktionssystem sein. Der Hostname, die Instanznummer und die SID sind für die Quell- und Zielsysteme unterschiedlich. Das neue System ist nicht vom Quellsystem isoliert.



- **Aktualisierung des SAP-Systems.** Eine SAP-Systemaktualisierung ist eine Aktualisierung eines bestehenden SAP-Zielsystems mit Daten aus einem SAP-Quellsystem. Das Zielsystem ist typischerweise Teil einer SAP-Transportlandschaft – beispielsweise eines Sandbox-Systems –, das mit Daten aus dem Produktionssystem aktualisiert wird. Der Hostname, die Instanznummer und die SID sind für das Quell- und Zielsystem unterschiedlich.



Obwohl wir drei verschiedene Anwendungsfälle kennen, bleibt der Datenmanagementprozess gleich. Alle drei Anwendungsfälle nutzen dieselbe zugrunde liegende Datenmanagement-Technologie: NetApp Snapshot und FlexClone.

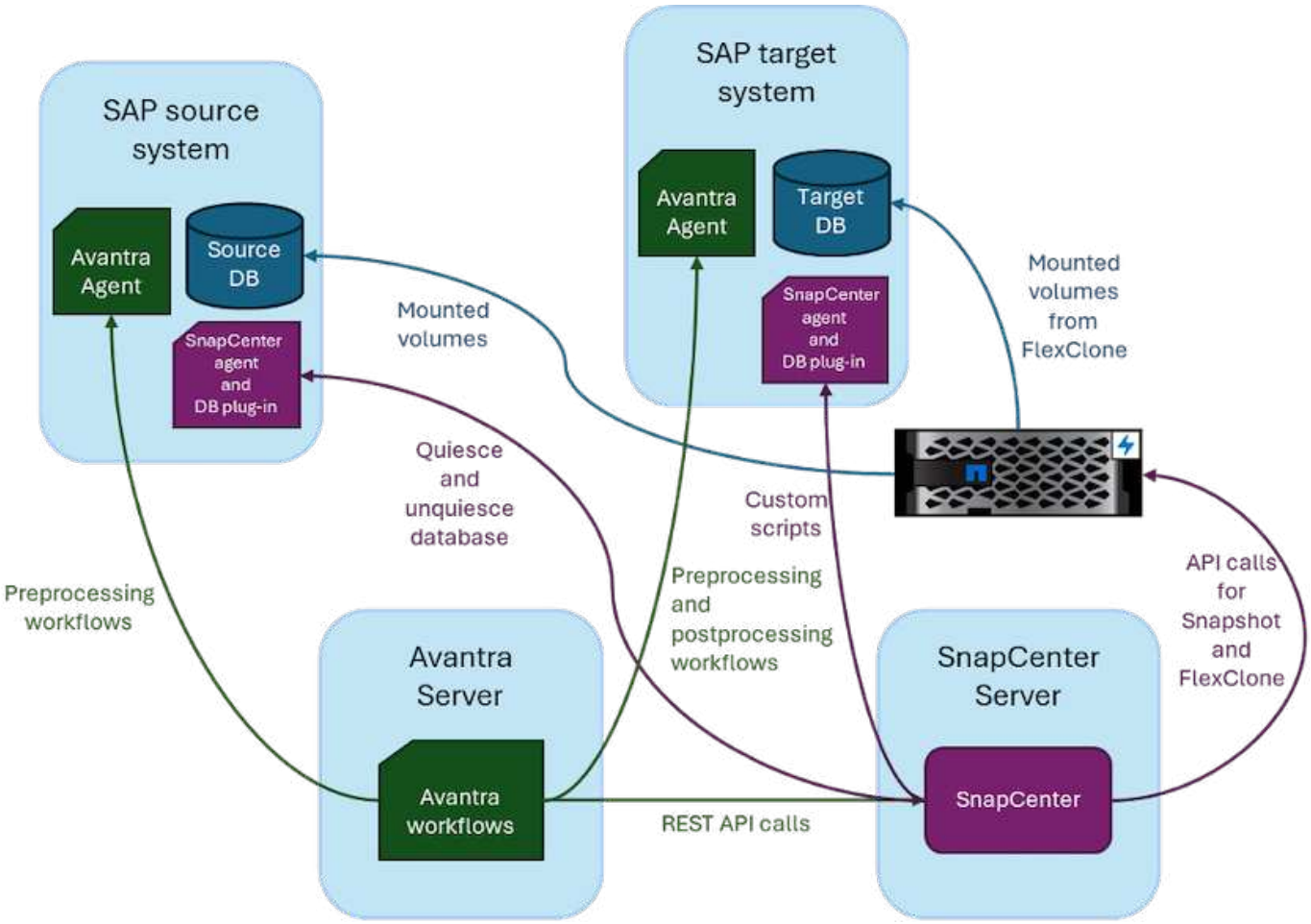
Lösungstechnologie

Die Gesamtlösung besteht aus den folgenden Hauptkomponenten:

- SAP-Quellsystem mit installiertem SnapCenter Agent und SnapCenter Datenbank-Plug-in
- SAP-Zielsystem mit installiertem SnapCenter Agent und SnapCenter Datenbank-Plug-in
- Avantra-System mit konfiguriertem SAP-Quell- und SAP-Zielsystem
- NetApp SnapCenter-Server
- NetApp Storage-System:
  - Physische Hardware vor Ort: NetApp AFF A-Serie, AFF C-Serie, ASA A-Serie, ASA C-Serie oder FAS Serie
  - Softwaredefinierter Storage vor Ort: NetApp ONTAP® Select
  - NetApp Cloud-Storage:

- NetApp Cloud Volumes ONTAP in AWS, Google Cloud oder Azure
- Azure NetApp Dateien
- Amazon FSX für NetApp ONTAP (AWS)

Die folgende Abbildung zeigt den Avantra Server, den NetApp SnapCenter Server, das NetApp Storage-System, das SAP Quell- und SAP Zielsystem und wie alles integriert wird. Das Ziel war es, die Integration durch Verwendung der SnapCenter REST API so flexibel wie möglich zu gestalten und so Konfigurationsarbeiten, die bereits in den bestehenden Komponenten ausgeführt wurden, maximal wiederzuverwenden.



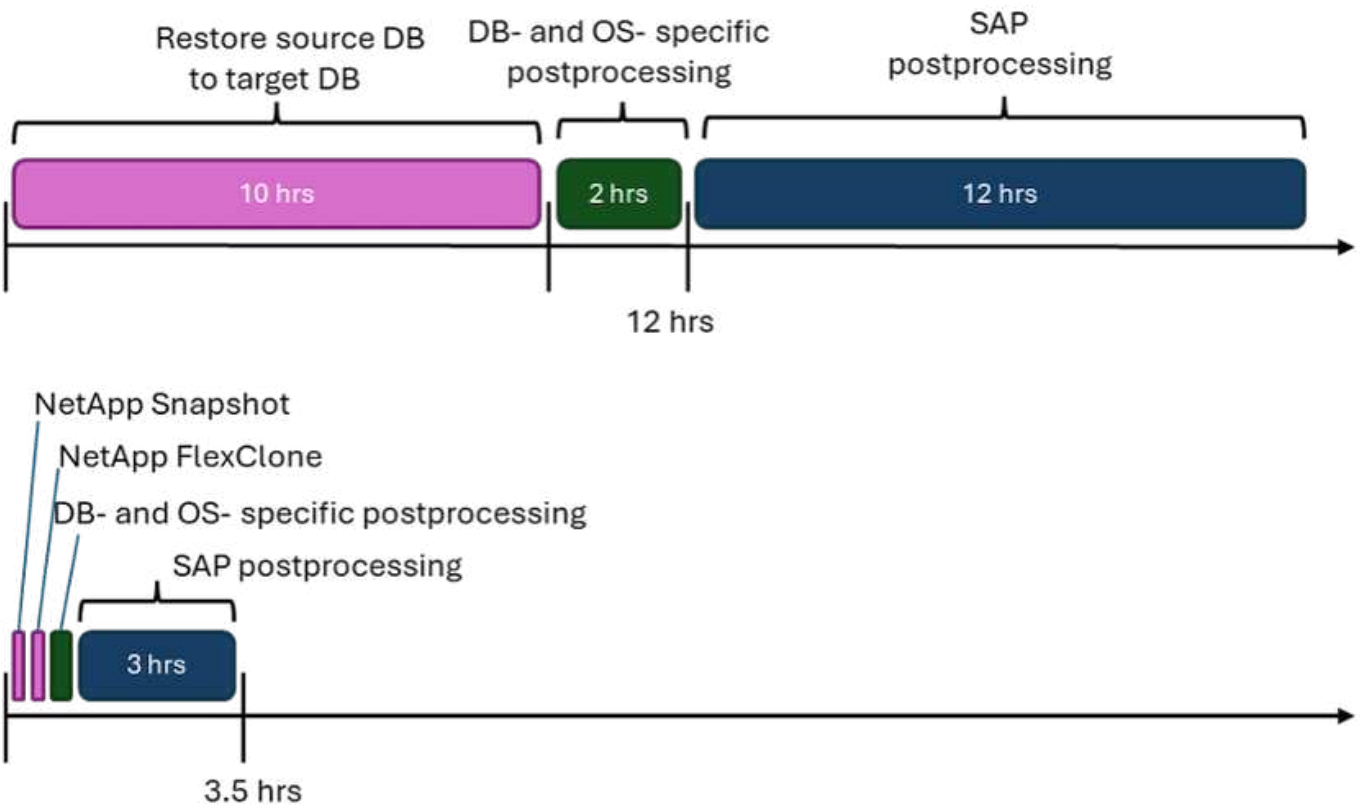
Zusammenfassung des Anwendungsfalls

Es gibt mehrere Szenarien, in denen Daten aus einem Quellsystem einem Zielsystem zu Test- oder Schulungszwecken zur Verfügung gestellt werden müssen. Diese Test- und Trainingssysteme müssen regelmäßig mit Daten aus dem Quellsystem aktualisiert werden, um sicherzustellen, dass Tests und Trainings mit dem aktuellen Datensatz durchgeführt werden. Diese Vorgänge für die Systemaktualisierung umfassen mehrere Aufgaben auf der Infrastruktur-, Datenbank- und Applikationsebene und können je nach Grad der Automatisierung mehrere Tage dauern.

Um Zeit zu verkürzen, betriebliche Aufgaben zu automatisieren und menschliche Fehler auf Infrastruktur-, Datenbank- und Applikationsebene zu eliminieren, können Sie Avantra Workflows verwenden. Anstatt ein Backup aus dem Quellsystem, das sehr zeitaufwendig und mit hohem Ressourcenverbrauch verbunden ist, auf das Zielsystem wiederherzustellen, verwendet diese Integration NetApp Snapshots und FlexClone Technologie. Alle Aufgaben, die zum Hochfahren einer Datenbank erforderlich sind, lassen sich in wenigen Minuten statt in mehreren Stunden erledigen. Die für den Klonprozess benötigte Zeit hängt nicht von der

Größe der Datenbank ab, daher können selbst sehr große Systeme in wenigen Minuten erstellt werden. Avantra reduziert die Laufzeit weiter, indem Aufgaben auf Betriebssystem- und Datenbankebene sowie auf der SAP-Nachverarbeitungsseite automatisiert werden.

Die folgende Abbildung zeigt mögliche Verbesserungen bei der betrieblichen Effizienz durch den Einsatz von Automatisierung.



Integration der verschiedenen Technologiekomponenten

Die eigentliche Integration von SnapCenter in einen Avantra Workflow besteht aus dem Zugriff über JavaScript auf die NetApp SnapCenter REST API. Durch diese REST API-basierte Integration wird eine Snapshot Kopie des SAP Quellsystems erstellt, ein FlexClone Volume erstellt und im SAP Zielsystem gemountet.

Storage- und SAP-Administratoren haben Zeit und Know-how in die Entwicklung von Skripten investiert, die von SnapCenter ausgelöst und vom SnapCenter-Agenten ausgeführt werden, um Routineaufgaben für den täglichen Betrieb zu automatisieren. Diese lose gekoppelte Architektur, bei der JavaScript zur Auslöser von SnapCenter-Aufgaben verwendet wird, ermöglicht es ihnen, ihre vorhandenen Automatisierungsverfahren wiederzuverwenden, um schneller die gewünschten Ergebnisse zu erzielen. Dabei wird Avantra als Workflow Engine für die End-to-End-Automatisierung verwendet.

Schlussfolgerung

Die Kombination aus Avantra und der NetApp Datenmanagement-Technologie bietet eine leistungsstarke Lösung, die den Zeit- und Arbeitsaufwand für die komplexesten und zeitaufwendigsten Aufgaben im Zusammenhang mit der SAP Systemadministration deutlich reduzieren kann. Diese Kombination kann auch helfen, Konfigurationsabweichungen zu vermeiden, die durch menschliches Versagen zwischen den Systemen verursacht werden können.

Da Systemaktualisierungen, Kopien, Klone und Disaster-Recovery-Tests sehr sensitive Verfahren sind, nimmt

die Implementierung einer solchen Lösung wertvolle Administrationszeit frei. Darüber hinaus kann das Vertrauen der Mitarbeiter in SAP-Systemadministratoren gestärkt werden: Sie werden sehen, wie viel Zeit für die Fehlerbehebung eingespart werden kann und wie viel einfacher es ist, Systeme für Tests oder andere Zwecke zu kopieren. Die Lösung bietet diese Vorteile unabhängig davon, wo die Quell- und Zielsysteme betrieben werden – vor Ort, in einer Public Cloud, in einer Hybrid- oder Hybrid-Multi-Cloud-Umgebung.

Wo Sie weitere Informationen finden

Sehen Sie sich die folgenden Dokumente und Websites an, um mehr über die in diesem Dokument beschriebenen Daten zu erfahren:

- "Avantra"
- "Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter"
- "REST-APIs werden für SnapCenter Server und Plug-ins unterstützt"

Versionsverlauf

Version	Datum	Zusammenfassung aktualisieren
Version 0.1	03.2024	Entwurf.
Version 0.2	03.2024	Integration des Feedbacks von NetApp-Kollegen.
Version 0.3	04.2024	Integrierte Änderungen wurden angefordert, um NetApp Branding-konform zu sein
Version 0.4	06.2024	In HTML-Format konvertiert

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

"https://www.netapp.com/company/legal/copyright/"

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

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.