Entdecken Sie Ressourcen und bereiten Sie mandantenfähige Datenbank-Container zur Datensicherung vor

SnapCenter Software 4.6

NetApp
January 18, 2024

This PDF was generated from https://docs.netapp.com/de-de/snapcenter-46/protect-hana/task_discover_the_databases_automatically.html on January 18, 2024. Always check docs.netapp.com for the latest.

Inhalt

Entdecken Sie Ressourcen und bereiten Sie mandantenfähige Datenbank-Container zur Datensicherung vor 1
Automatische Erkennung von Datenbanken 1
Mandantenfähige Datenbank-Container werden für die Datensicherung vorbereitet 2

Entdecken Sie Ressourcen und bereiten Sie mandantenfähige Datenbank-Container zur Datensicherung vor

Automatische Erkennung von Datenbanken

Ressourcen sind SAP HANA Datenbanken und nicht-Daten-Volumes auf dem Linux-Host, die von SnapCenter gemanagt werden. Diese Ressourcen können Ressourcengruppen hinzugefügt werden, um Datensicherungsvorgänge durchzuführen, nachdem die verfügbaren SAP HANA Datenbanken ermittelt wurden.

Was Sie brauchen

- Sie müssen bereits Aufgaben abgeschlossen haben, wie z. B. die Installation des SnapCenter-Servers, das Hinzufügen des HDB-Benutzerspeicherschlüssels, das Hinzufügen von Hosts und das Einrichten der Speichersystemverbindungen.
- Sie müssen den HDB Secure User Store Key und den HDB SQL OS-Benutzer auf dem Linux-Host konfiguriert haben.
  - Sie müssen den HDB-Benutzerspeicherschlüssel mit dem SID-Adm-Benutzer konfigurieren. Für HANA-Systeme mit A22 als SID muss beispielsweise der HDB User Store Key mit a22adm konfiguriert werden.
- Das SnapCenter Plug-in für SAP HANA Database unterstützt nicht das automatische Auffinden der Ressourcen in virtuellen RDM/VMDK-Umgebungen. Sie müssen Storage-Informationen für virtuelle Umgebungen bereitstellen und gleichzeitig Datenbanken manuell hinzufügen.

Über diese Aufgabe

Nach der Installation des Plug-ins werden alle Ressourcen auf diesem Linux-Host automatisch erkannt und auf der Seite Ressourcen angezeigt.

Die automatisch ermittelten Ressourcen können nicht geändert oder gelöscht werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Plug-in für SAP HANA aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen den Ressourcentyp aus der Liste Ansicht aus.
3. (Optional) Klicken Sie Auf , und wählen Sie dann den Hostnamen aus.

   Sie können dann auf * klicken * Zum Schließen des Filterfensters.

4. Klicken Sie auf **Ressourcen aktualisieren**, um die auf dem Host verfügbaren Ressourcen zu ermitteln.

   Die Ressourcen werden zusammen mit Informationen wie Ressourcentyp, Hostname, zugeordnete Ressourcengruppen, Backup-Typ, Richtlinien und Gesamtstatus angezeigt.

   - Wenn sich die Datenbank auf einem NetApp Storage befindet und nicht geschützt ist, wird in der Spalte Status insgesamt nicht geschützt angezeigt.

- Wenn sich die Datenbank auf einem NetApp Storage-System befindet und geschützt ist, und wenn kein Backup-Vorgang durchgeführt wird, wird in der Spalte Gesamtstatus der Eintrag Backup Not Run angezeigt. Der Status ändert sich ansonsten auf „Sicherung fehlgeschlagen“ oder „Sicherung erfolgreich“, basierend auf dem letzten Backup-Status.

> Wenn in der SAP HANA-Datenbank kein HDB-sicherer Benutzerspeicherschlüssel konfiguriert ist, wird neben der Ressource ein rotes Vorhängeschloss-Symbol angezeigt. Wenn sich während einer anschließenden Ermittlung der konfigurierte HDB Secure User Store Key als falsch herausstellte oder keinen Zugriff auf die Datenbank selbst bot, wird das rote Vorhängeschloss-Symbol erneut angezeigt.

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

Nach Ihrer Beendigung

Sie müssen den HDB Secure User Store Key und den HDBSQL OS User so konfigurieren, dass sie die Datenbank schützen oder zur Ressourcengruppe hinzufügen können, um Datenschutzvorgänge durchzuführen.

"Konfiguration des HDB-Benutzerspeicherschlüssels und des HDBSQL OS-Benutzers für die SAP HANA-Datenbank"

Mandantenfähige Datenbank-Container werden für die Datensicherung vorbereitet

Bei direkt in SnapCenter registrierten SAP HANA Hosts wird das Installieren oder Upgrade des SnapCenter Plug-ins für SAP HANA Database eine automatische Ermittlung der Ressourcen auf dem Host auslösen. Nach der Installation oder dem Upgrade des Plug-ins werden für alle MDC-Ressourcen (Multi-Tenant-Datenbank-Container), die sich auf dem Plug-in-Host befand, automatisch eine andere MDC-Ressource mit einem anderen GUID-Format erkannt und in SnapCenter registriert. Die neue Ressource befindet sich im Status „`gesperrt`“.

Über diese Aufgabe

Wenn sich beispielsweise in SnapCenter 4.2 die E90-MDC-Ressource auf dem Plug-in-Host befand und manuell registriert wurde, wird nach dem Upgrade auf SnapCenter 4.3 eine weitere E90-MDC-Ressource mit einer anderen GUID erkannt und in SnapCenter registriert.

> Die Backups, die mit der Ressource von SnapCenter 4.2 und älteren Versionen verbunden sind, müssen bis zum Ablauf der Aufbewahrungsfrist aufbewahrt werden. Nach Ablauf des Aufbewahrungszeitraums können Sie die alte MDC-Ressource löschen und die neue automatisch erkannte MDC-Ressource weiterhin verwalten.

`Old MDC resource` Ist die MDC-Ressource für einen Plug-in-Host, der manuell in SnapCenter 4.2 oder früheren Versionen hinzugefügt wurde.

Führen Sie die folgenden Schritte durch, um die in SnapCenter 4.3 entdeckte neue Ressource für Datensicherungsvorgänge zu verwenden:

Schritte

1. Wählen Sie auf der Seite „Ressourcen“ die alte MDC-Ressource mit Backups aus, die der früheren SnapCenter-Version hinzugefügt wurden, und legen Sie sie auf der Topologieseite in den „`maintBuße-Modus`“.

   Wenn die Ressource Teil einer Ressourcengruppe ist, legen Sie die Ressourcengruppe in den „`mBetriebszustand`“.

2. Konfigurieren Sie die neue MDC-Ressource, die nach dem Upgrade auf SnapCenter 4.3 erkannt wurde, indem Sie die neue Ressource auf der Seite Ressourcen auswählen.

   „`Neue MDC-Ressource`“ ist die neu entdeckte MDC-Ressource, die erkannt wurde, nachdem der SnapCenter-Server und der Plug-in-Host auf 4.3 aktualisiert wurden. Die neue MDC-Ressource kann als Ressource mit demselben SID wie die alte MDC-Ressource, für einen bestimmten Host und mit einem roten Vorhängeschloss-Symbol daneben auf der Seite Ressourcen identifiziert werden.

3. Schützen Sie die neue MDC-Ressource, die nach dem Upgrade auf SnapCenter 4.3 erkannt wurde, indem Sie Schutzrichtlinien, Zeitpläne und Benachrichtigungseinstellungen auswählen.
4. Löschen Sie die Backups, die in SnapCenter 4.2 oder früheren Versionen basierend auf den Aufbewahrungseinstellungen erstellt wurden.
5. Löschen Sie die Ressourcengruppe auf der Seite Topologie.
6. Löschen Sie die alte MDC-Ressource von der Seite Ressourcen.

   Beispiel: Wenn die Aufbewahrungsdauer der primären Snapshot Kopien 7 Tage beträgt und die Aufbewahrung von sekundären Snapshot Kopien 45 Tage beträgt, nach 45 Tagen abgeschlossen sind und nachdem alle Backups gelöscht wurden, müssen Sie die Ressourcengruppe und die alte MDC-Ressource löschen.

Weitere Informationen

"Konfiguration des HDB-Benutzerspeicherschlüssels und des HDBSQL OS-Benutzers für die SAP HANA-Datenbank"

"Sehen Sie sich SAP HANA Datenbank-Backups und -Klone auf der Seite Topologie an"

Copyright-Informationen

Copyright © 2024 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.