リソースを検出し、マルチテナントデータベースコンテナでデータ保護を準備

SnapCenter Software 4.7

NetApp
January 18, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/snapcenter-47/protect-hana/task_discover_the_databases_automatically.html on January 18, 2024. Always check docs.netapp.com for the latest.

目次

リソースを検出し、マルチテナントデータベースコンテナでデータ保護を準備 1
データベースを自動的に検出します 1
マルチテナントデータベースコンテナでデータ保護を準備 2

リソースを検出し、マルチテナントデータベースコンテナでデータ保護を準備

データベースを自動的に検出します

リソースとは、 SnapCenter で管理されている Linux ホスト上の SAP HANA データベースと非データボリュームです。使用可能な SAP HANA データベースを検出したあと、それらのリソースをリソースグループに追加してデータ保護処理を実行できます。

- 必要なもの *
- SnapCenter サーバのインストール、 HDB ユーザ・ストア・キーの追加、ホストの追加、ストレージ・システム接続の設定などの作業を完了しておく必要があります。
- Linux ホストで HDB Secure User Store Key および HDB SQL OS ユーザを設定しておく必要があります。
  - SID adm ユーザーを使用して HDB ユーザーストアキーを構成する必要がありますたとえば、 A22 を SID として使用する HANA システムの場合、 HDB User Store Key は a22adm で構成する必要があります。
- SnapCenter Plug-in for SAP HANA Database では、 RDM / VMDK 仮想環境にあるリソースの自動検出はサポートされません。データベースを手動で追加する場合は、仮想環境のストレージ情報を指定する必要があります。
- このタスクについて *

プラグインをインストールすると、その Linux ホスト上のすべてのリソースが自動的に検出され、リソースページに表示されます。

自動で検出されたリソースは変更または削除できません。

- 手順 *
  1. 左側のナビゲーションペインで、 * Resources * をクリックし、リストから Plug-in for SAP HANA Database を選択します。
  2. [リソース] ページで、 [表示] リストからリソースタイプを選択します。
  3. （オプション） * をクリックします * をクリックし、ホスト名を選択します。

     次に、 * をクリックします * をクリックすると、フィルタペインが閉じます。
  4. [* リソースの更新 *] をクリックして、ホストで使用可能なリソースを検出します。

     リソースは、リソースタイプ、ホスト名、関連するリソースグループ、バックアップタイプ、ポリシー、全体的なステータスなどの情報とともに表示されます。

     - データベースがネットアップストレージ上にあり、保護されていない場合は、総体的なステータス列に Not protected と表示されます。
     - データベースがネットアップストレージシステム上にあり、保護されている場合に、バックアップ処理が実行されていないと、 [全体のステータス] 列に [バックアップが実行されていません] と表示されます。それ以外の場合は、前回のバックアップステータスに基づいて、「 Backup

failed 」または「 Backup succeeded 」に変わります。

> SAP HANA データベースで HDB Secure User Store Key が設定されていない場合は、リソースの横に赤い南京錠のアイコンが表示されます。その後の検出操作中に、設定されている HDB Secure User Store Key が正しくないか、データベース自体へのアクセスを提供していない場合は、赤い南京錠のアイコンが再表示されます。

> データベース名が SnapCenter 以外に変更された場合は、リソースを更新する必要があります。

- 終了後 *

データ保護処理を実行するには、データベースを保護できるように HDB Secure User Store Key および HDBSQL OS ユーザを設定するか、またはリソースグループにこのキーを追加する必要があります。

"SAP HANA データベース用に HDB User Store Key および HDBSQL OS ユーザを設定します"

マルチテナントデータベースコンテナでデータ保護を準備

SnapCenter に直接登録された SAP HANA ホストの場合、 SnapCenter Plug-in for SAP HANA Database をインストールまたはアップグレードすると、ホスト上のリソースが自動的に検出されます。プラグインをインストールまたはアップグレードした後、プラグインホスト上にあるすべてのマルチテナントデータベースコンテナ（ MDC ）リソースに対して、別の MDC リソースが自動的に検出されて SnapCenter に登録されます。新しいリソースは「ロック」状態になります。

- このタスクについて *

たとえば、 SnapCenter 4.2 では、 E90 MDC リソースがプラグインホスト上にあり、手動で登録されている場合、 SnapCenter 4.3 にアップグレードした後に、別の GUID を持つ別の E90 MDC リソースが検出されて SnapCenter に登録されます。

> SnapCenter 4.2 以前のバージョンのリソースに関連付けられたバックアップは、保持期間が満了するまで保持される必要があります。保存期間が終了したら、古い MDC リソースを削除して、新しい自動検出された MDC リソースを引き続き管理できます。

`Old MDC resource` は、SnapCenter 4.2以前のリリースで手動で追加されたプラグインホストのMDCリソースです。

SnapCenter 4.3 で検出された新しいリソースを使用してデータ保護処理を開始するには、次の手順を実行します。

- 手順 *

1. リソースページで ' 以前の SnapCenter リリースにバックアップが追加されている古い MDC リソースを選択し ' トポロジーページからメンテナンス・モードにします

   リソースがリソースグループの一部である場合は、リソースグループを「メンテナンスモード」にします。

2. リソースページから新しいリソースを選択して、 SnapCenter 4.3 にアップグレードした後に検出された新しい MDC リソースを構成します。

   「新しい MDC リソース」は、 SnapCenter サーバとプラグインホストが 4.3 にアップグレードされたときに検出された、新しく検出された MDC リソースです。新しい MDC リソースは、古い MDC リソースと同じ SID を持つリソース、特定のホスト、およびリソースページのその横に赤い南京錠のアイコンで識別できます。

3. SnapCenter 4.3 へのアップグレード後に検出された新しい MDC リソースを保護するには ' 保護ポリシー ' スケジュール ' 通知設定を選択します
4. 保持設定に基づいて、 SnapCenter 4.2 以前のリリースで作成されたバックアップを削除します。
5. Topology ページからリソースグループを削除します。
6. [リソース] ページから古い MDC リソースを削除します。

   たとえば、プライマリ Snapshot コピーの保持期間が 7 日で、セカンダリ Snapshot コピーの保持期間が 45 日の場合、 45 日が完了してすべてのバックアップが削除されたあとに、リソースグループと古い MDC リソースを削除する必要があります。

- 詳細はこちら *

"SAP HANA データベース用に HDB User Store Key および HDBSQL OS ユーザを設定します"

"Topology ページで、 SAP HANA データベースのバックアップとクローンを表示します"

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。