NetBackup™ for Nutanix AHV 管理者ガイド

リリース 11.0

VERITAS
now part of Cohesity

最終更新日: 2026-01-21

法的通知と登録商標

Cohesity、Veritas、Cohesity ロゴ、Veritas ロゴ、Veritas Alta、Cohesity Alta、NetBackup は、Cohesity, Inc. またはその関連会社の米国およびその他の国における商標または登録商標です。その他の会社名、製品名は各社の登録商標または商標です。

この製品には、Cohesity 社がサードパーティへの帰属を示す必要があるサードパーティ製ソフトウェア (「サードパーティ製プログラム」) が含まれる場合があります。サードパーティプログラムの一部は、オープンソースまたはフリーソフトウェアライセンスで提供されます。本ソフトウェアに含まれる本使用許諾契約は、オープンソースまたはフリーソフトウェアライセンスでお客様が有する権利または義務を変更しないものとします。このCohesity製品に付属するサードパーティの法的通知文書は次の場所で入手できます。

https://www.veritas.com/about/legal/license-agreements

本書に記載されている製品は、その使用、コピー、頒布、逆コンパイルおよびリバースエンジニアリングを制限するライセンスに基づいて頒布されます。Cohesity, Inc. からの書面による許可なく本書を複製することはできません。

本書は、現状のままで提供されるものであり、その商品性、特定目的への適合性、または不侵害の暗黙的な保証を含む、明示的あるいは暗黙的な条件、表明、および保証はすべて免責されるものとします。ただし、これらの免責が法的に無効であるとされる場合を除きます。Cohesity, Inc. およびその関連会社は、本書の提供、パフォーマンスまたは使用に関連する付随的または間接的損害に対して、一切責任を負わないものとします。本書に記載の情報は、予告なく変更される場合があります。

ライセンスソフトウェアおよび文書は、FAR 12.212 に定義される商用コンピュータソフトウェアと見なされ、Cohesityがオンプレミスまたはホスト型サービスとして提供するかを問わず、必要に応じて FAR 52.227-19 「商用コンピュータソフトウェア - 制限される権利 (Commercial Computer Software - Restricted Rights)」、DFARS 227.7202「商用コンピュータソフトウェアおよび商用コンピュータソフトウェア文書 (Commercial Computer Software and Commercial Computer Software Documentation)」、およびそれらの後継の規制に定める制限される権利の対象となります。米国政府によるライセンス対象ソフトウェアおよび資料の使用、修正、複製のリリース、実演、表示または開示は、本使用許諾契約の条項に従ってのみ行われるものとします。

Cohesity, Inc.
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

テクニカルサポート

テクニカルサポートはグローバルにサポートセンターを管理しています。すべてのサポートサービスは、サポート契約と現在のエンタープライズテクニカルサポートポリシーに応じて提供されます。サポート内容およびテクニカルサポートの利用方法に関する情報については、次の Web サイトにアクセスしてください。

https://www.veritas.com/support

次の URL で Cohesity Account の情報を管理できます。

https://my.veritas.com

現在のサポート契約についてご不明な点がある場合は、次に示すお住まいの地域のサポート契約管理チームに電子メールでお問い合わせください。

世界共通 (日本を除く)	CustomerCare@veritas.com
日本	CustomerCare_Japan@veritas.com

マニュアル

マニュアルの最新バージョンがあることを確認してください。各マニュアルには、2 ページ目に最終更新日が記載されています。最新のマニュアルは、Cohesity の Web サイトで入手できます。

Cohesity Services and Operations Readiness Tools (SORT)

Cohesity SORT (Service and Operations Readiness Tools) は、特定の時間がかかる管理タスクを自動化および簡素化するための情報とツールを提供する Web サイトです。製品によって異なりますが、SORT はインストールとアップグレードの準備、データセンターにおけるリスクの識別、および運用効率の向上を支援します。SORT がお客様の製品に提供できるサービスとツールについては、次のデータシートを参照してください。

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

目次

1

概要

この章では以下の項目について説明しています。

- NetBackup Web UI での AHV 資産の構成と保護の概要

NetBackup Web UI での AHV 資産の構成と保護の概要

表 1-1 AHV 資産を構成して保護する手順

手順	処理	説明
手順 1	デフォルトのセキュリティ管理者として NetBackup Web UI にサインインします。その後、[デフォルトの AHV 管理者 (Default AHV Administrator)]役割に AHV ユーザーを追加します。または、AHV 管理者が必要とする権限に合わせて、カスタムの RBAC の役割を作成します。	**メモ:** AHV 管理者タスクを実行するにあたって必要な最小限の権限が[デフォルトの AHV 管理者 (Default AHV Administrator)]役割にあります。また、カスタム役割を作成して、AHV 管理者に異なるアクセス権を付与することもできます。

手順	処理	説明
手順 2	AHV クラスタに対して次を構成します。 ■ AHV クラスタと NetBackup ホスト間の安全な通信を構成します。 ■ (省略可能) Nutanix Prism Central と NetBackup ホスト間の安全な通信を構成します。 ■ バックアップホストまたはリストアホストとして使用する NetBackup ホストで iSCSI を有効にします。 ■ Nutanix Prism コンソールで、バックアップホストを許可リストに追加します。 **メモ:** Linux のバックアップホストまたはリカバリホストで NFS プロトコルを使用するには、Nutanix AHV Cluster Prism コンソールに NFS が許可されたホストのリストが必要です。詳しくは、ここをクリックしてください。	p.20 の「AHV クラスタと NetBackup ホスト間、および Nutanix Prism Central と NetBackup ホスト間の安全な通信の構成」を参照してください。 p.23 の「Linux バックアップホストでの iSCSI イニシエータパッケージのインストール」を参照してください。 p.23 の「Windows バックアップホストで iSCSI イニシエータサービスを有効にする」を参照してください。
手順 3 (省略可能)	Nutanix Prism Central を構成して管理します。	p.32 の「新しい Nutanix Prism Central の追加」を参照してください。
手順 4	AHV クラスタを構成して管理します。	p.24 の「Nutanix AHV クラスタを構成するための前提条件」を参照してください。
手順 5	クレデンシャルを追加および管理します。	p.52 の「新しいクラスタのクレデンシャルの追加」を参照してください。
手順 6	AHV 保護計画を構成します。	『NetBackup™ Web UI バックアップ管理者ガイド』を参照してください。
手順 7	インテリジェント VM グループを構成します。	p.35 の「インテリジェント VM グループの作成」を参照してください。
手順 8	AHV VM またはインテリジェント VM グループを保護します。	p.69 の「保護計画を使用した AHV VM またはインテリジェント VM グループの保護」を参照してください。
手順 9	VM をリカバリします。	p.78 の「AHV 仮想マシンのリカバリ」を参照してください。

2

Nutanix AHV 管理者の RBAC の役割

この章では以下の項目について説明しています。

Nutanix AHV 管理者の RBAC の役割

NetBackup では、RBAC (役割に基づくアクセス制御) を使用して、どのユーザーがどの Nutanix AHV またはその他の作業負荷にアクセスできるかを制御できます。環境に応じて、次の方法で Nutanix AHV 管理者の RBAC を構成できます。

表 2-1 Nutanix AHV 管理者に使用または作成する RBAC の役割

必要なアクセスタイプ	使用または作成する役割	
Nutanix AHV 資産および構成を管理し、Nutanix AHV にリストアを実行します。	[デフォルトの AHV 管理者 (Default AHV Administrator)]の役割	

必要なアクセスタイプ	使用または作成する役割	
Nutanix AHV 資産および VMware 資産を管理し、クロス Hypervisor がサポートされます。	[デフォルトの AHV 管理者 (Default AHV Administrator)]および[デフォルトの VMware 管理者 (Default VMware Administrator)]の役割	これらの役割が割り当てられた管理者は、次のものも管理することができます。 Nutanix AHV のクレデンシャル ([作業負荷 (Workloads)]、[Nutanix AHV]の[Prism Central サーバー (Prism Central servers)]タブまたは[AHV クラスタ (AHV cluster)]タブ)。 vCenter、ESX Server などのクレデンシャル ([作業負荷 (Workloads)]、[VMware]の[VMware サーバー (VMware servers)]タブ)。
VMware 資産に対する追加の権限を持つ Nutanix AHV へのフルアクセス。	カスタム役割を作成します。	この役割は、VMware バックアップイメージからリストアし、リカバリ後に AHV 作業負荷を使用する場合に便利です。
Nutanix AHV 資産に対する追加の権限を持つ VMware へのフルアクセス。	カスタム役割を作成します。	この役割は、VMware 作業負荷を使用し、クロス Hypervisor リストアを実行する場合に便利です。

次の点に注意してください。

- RBAC の役割を作成するには、RBAC 管理者の役割、または役割を作成する権限が必要です。
- クレデンシャルを作成するには、RBAC 管理者の役割、またはクレデンシャルを作成する権限を持つ役割が必要です。デフォルトの Nutanix AHV 管理者の役割とデフォルトの VMware 管理者の役割はユーザーにクレデンシャルを割り当てることはできますが、クレデンシャル管理でクレデンシャルを作成することはできません。
- 役割とクレデンシャルの作成については、NetBackup 管理者にお問い合わせください。

デフォルトの VMware 管理者役割とデフォルトの AHV 管理者役割の両方のユーザーへの割り当て

すべての Nutanix AHV 資産とすべての VMware 資産に対する RBAC アクセス権を、ユーザーにグローバルに付与する場合は、次の手順に従います。この役割は、VMware 作業負荷を使用し、ハイパーバイザ間のリストアを実行する場合に便利です。この役割の利点は、ソースと宛先の資産に必要な権限を手動で選択する必要がない点です。ただし、この役割では、特定の資産に対する権限を制限することはできません。その場合は、カスタム役割を構成する必要があります。

デフォルトの VMware 管理者役割とデフォルトの AHV 管理者役割の両方をユーザーに割り当てるには

1. 左側で、[セキュリティ (Security)]、[RBAC]の順に選択します。
2. [デフォルトの VMware 管理者 (Default VMware Administrator)]の役割を選択します。次に[ユーザー (Users)]タブを選択します。
3. グループ名またはユーザー名を入力します。次に、[リストに追加 (Add to list)]を選択します。
4. 役割リストに戻る場合は、[閉じる (Close)]ボタンを選択します。
5. [デフォルトの AHV 管理者 (Default AHV Administrator)]の役割を選択します。次に[ユーザー (Users)]タブを選択します。
6. グループ名またはユーザー名を入力します。次に、[リストに追加 (Add to list)]を選択します。
7. グループまたはユーザーに割り当てられている役割を表示するには、[ユーザー (Users)]タブを選択します。

すべての Nutanix AHV 権限と追加の VMware 資産権限のカスタム役割の作成

ユーザーに Nutanix AHV の RBAC グローバルアクセス権と、特定の VMware 資産に対する権限を付与する場合は、次の手順に従います。この役割は、VMware バックアップイメージからリストアし、リカバリ後に AHV 作業負荷を使用する場合に便利です。

すべての Nutanix AHV 権限と追加の VMware 資産権限のカスタム役割を作成するには

1. 左側で、[セキュリティ(Security)]、[RBAC]の順に選択して、[追加 (Add)]を選択します。
2. [デフォルトの AHV 管理者 (Default AHV Administrator)]の役割を選択します。その後、[次へ (Next)]を選択します。
3. [役割名 (Role name)]と説明を指定します。

   たとえば、この役割はユーザーに Nutanix AHV の管理を許可し、VMware に対する特定の権限を付与することを示す説明を含めます。
4. [アクセス権 (Permissions)]で[編集 (Edit)]を選択します。
5. [AHV 資産 (AHV assets)]に移動します。その作業負荷に対するすべての権限がすでに選択されていることに注意してください。
6. [VMware 資産 (VMware assets)]に移動します。
7. 次の権限を選択します。

- 表示 (View)
- アクセスの管理 (Manage access)
- リストア (Restore)
- ジョブの表示 (View jobs)

8 [割り当て (Assign)]を選択します。

9 [作業負荷 (Workloads)]で、[編集 (Edit)]を選択します。

10 次のオプションのいずれかを選択します。

- 既存および今後のすべての VMware 資産に作業負荷に必要な権限を適用するには、次のオプションを有効にしたままにします: [権限を既存および今後のすべての VMware 資産に適用する (Apply permissions to all existing and future VMware assets)]。
- 特定の VMware 資産だけに必要な権限を適用するには、次のオプションを選択解除します: [権限を既存および今後のすべての VMware 資産に適用する (Apply permissions to all existing and future VMware assets)]。次に、権限を適用する資産を選択し、[追加 (Add)]を選択します。

11 [割り当て (Assign)]を選択します。

12 [ユーザー (Users)]で、[編集 (Edit)]を選択します。次に、この RBAC の役割を付与するグループまたはユーザーを追加します。

13 [割り当て (Assign)]を選択します。

14 役割の構成が完了したら、[役割の追加 (Add role)]を選択します。

15 グループまたはユーザーに割り当てられている役割を表示するには、[ユーザー (Users)]タブを選択します。

すべての VMware 権限と追加の Nutanix AHV 資産権限のカスタム役割の作成

ユーザーに VMware の RBAC グローバルアクセス権と、特定の Nutanix AHV 資産に対する権限を付与する場合は、次の手順に従います。

すべての VMware 権限と追加の Nutanix AHV 資産権限のカスタム役割を作成するには

1 左側で、[セキュリティ (Security)]、[RBAC]の順に選択して、[追加 (Add)]を選択します。

2 [デフォルトの VMware 管理者 (Default VMware Administrator)]の役割を選択します。その後、[次へ (Next)]を選択します。

3 [役割名 (Role name)]と説明を指定します。

たとえば、この役割はユーザーに VMware の管理を許可し、Nutanix AHV に対する特定の権限を付与することを示す説明を含めます。

4 [アクセス権 (Permissions)]で[編集 (Edit)]を選択します。

5 [VMware 資産 (VMware assets)]に移動します。その作業負荷に対するすべての権限がすでに選択されていることに注意してください。

6 [AHV 資産 (AHV assets)]、[AHV クラスタ、VM、ストレージコンテナ (AHV clusters, VMs, and storage containers)]の順に移動します。

7 [個別リストア (Granular Restore)]を除くすべての権限を選択します。

8 [AHV 資産 (AHV assets)]、[Prism Central]の順に移動します。

9 そのグループのすべての権限を選択します。

10 グループ[AHV インテリジェント VM グループ (AHV intelligent VM groups)]の権限を選択してください。

11 [割り当て (Assign)]を選択します。

12 [作業負荷 (Workloads)]で、[編集 (Edit)]を選択します。

13 次のオプションのいずれかを選択します。

- 既存および今後のすべての Nutanix AHV 資産に作業負荷に必要な権限を適用するには、次のオプションを有効にしたままにします: [権限を既存および今後のすべての AHV 資産に適用する (Apply permissions to all existing and future AHV assets)]。
- 特定の VMware 資産だけに必要な権限を適用するには、次のオプションを選択解除します: [権限を既存および今後のすべての AHV 資産に適用する (Apply permissions to all existing and future AHV assets)]。次に、権限を適用する資産を選択し、[追加 (Add)]を選択します。

14 [割り当て (Assign)]を選択します。

15 [ユーザー (Users)]で、[編集 (Edit)]を選択します。次に、この RBAC の役割を付与するグループまたはユーザーを追加します。

16 [割り当て (Assign)]を選択します。

17 役割の構成が完了したら、[役割の追加 (Add role)]を選択します。

18 グループまたはユーザーに割り当てられている役割を表示するには、[ユーザー (Users)]タブを選択します。

3

AHV クラスタの管理

この章では以下の項目について説明しています。

- iSCSI 用 CHAP の設定
- AHV アクセスホストの追加
- AHV アクセスホストの削除
- AHV リソース形式のリソース制限の変更
- AHV 資産の自動検出の間隔の変更
- マルウェアのスキャン

AHV 仮想マシンを保護するためのクイック構成チェックリスト

NetBackup Web UI を使用して、AHV プラットフォーム上で作成された仮想マシンを保護してリカバリします。API とコマンドラインオプションも使用できます。

p.138 の「API とコマンドラインオプションを使用した AHV 仮想マシンの管理、保護、リカバリ」を参照してください。

次の表で、AHV 仮想マシンを保護するための手順の概要またはチェックリストについて説明します。

表 3-1 NetBackup を使用した AHV 仮想マシンの構成と保護

手順の概要	説明と参照
AHV VM を保護する NetBackup の配備	概説すると、AHV VM の保護には次が必要です。 ■ NetBackup プライマリサーバー ■ NetBackup メディアサーバー (推奨) ■ バックアップホストとして動作可能な NetBackup クライアント バックアップホストのオペレーティングシステムは、Linux RHEL、SUSE、または Windows である必要があります。バックアップホストには、NetBackup メディアサーバー、クライアント、または NetBackup Appliance を指定できます。 Flex Appliance と Flex Scale Appliance を含む NetBackup Appliance も、バックアップホストとして動作可能な NetBackup メディアサーバーとしてサポートされます。 NetBackup はエージェントレスアーキテクチャを使用して AHV VM を保護します。NetBackup と AHV クラスタ間の通信は Nutanix AHV API を介して行われます。

手順の概要	説明と参照
バックアップとリカバリ用の AHV アクセスホストの構成	AHV アクセスホストは、バックアップとリカバリ時にはそれぞれバックアップホスト、リカバリホストとして動作します。アクセスホストは、バックアップとリストア操作中のデータ移動に関与します。 NetBackup メディアサーバーまたはアプライアンスではないバックアップホストを使用する場合、NetBackup の[AHV アクセスホスト (AHV Access Hosts)]リストにバックアップホストを追加します。 **メモ:** メディアサーバーまたはアプライアンスではないバックアップホストには、NetBackup クライアントをインストールする必要があります。 p.42 の「AHV アクセスホストの追加」を参照してください。
NetBackup と AHV 間の安全な通信の有効化	次のセクションには、NetBackup と AHV 間の安全な通信の設定に関する詳細が含まれます。 ■ 安全な通信 p.20 の「AHV クラスタと NetBackup ホスト間、および Nutanix Prism Central と NetBackup ホスト間の安全な通信の構成」を参照してください。 ■ 通信ポート p.27 の「NetBackup が AHV との通信に使用するポートについて」を参照してください。
AHV クラスタ、Prism Central サーバー、およびインテリジェント VM グループの管理	■ AHV クラスタの管理 p.28 の「AHV クラスタの追加または参照」を参照してください。 ■ Prism Central サーバーの管理 p.32 の「新しい Nutanix Prism Central の追加」を参照してください。 ■ インテリジェント VM グループの管理 p.35 の「インテリジェント VM グループの作成」を参照してください。 p.41 の「インテリジェント VM グループの削除」を参照してください。
AHV VM の保護	■ 前提条件: AHV クラスタの追加にはデフォルトの AHV 管理者の役割が必要です。 ■ ベストプラクティス p.68 の「AHV 仮想マシンを保護する前の考慮事項」を参照してください。 ■ 仮想マシンの保護 p.69 の「保護計画を使用した AHV VM またはインテリジェント VM グループの保護」を参照してください。

手順の概要	説明と参照
Windows バックアップホストの iSCSI トランスポート	前提条件 Windows 2012 以降の場合、iSCSI クライアントイニシエータが Windows に存在します。デフォルトでは、iSCSI イニシエータサービスは Windows で停止または無効化されています。 p.23 の「Windows バックアップホストで iSCSI イニシエータサービスを有効にする」を参照してください。 **メモ:** 選択したバックアップホストまたはリカバリホストが Windows で稼働している場合は、バックアップまたはリストアジョブのエラーを回避するために、Windows コンピュータで iSCSI サービスが実行されていることを確認してください。
Linux バックアップホストの iSCSI トランスポート	前提条件 iSCSI を使用するには、`scsi-initiator-utils` パッケージをインストールする必要があります。RHEL または SUSE にはデフォルトでインストールされています。 p.23 の「Linux バックアップホストでの iSCSI イニシエータパッケージのインストール」を参照してください。 **メモ:** Linux のバックアップホストまたはリカバリホストで NFS プロトコルを使用するには、Nutanix AHV Cluster Prism コンソールに NFS が許可されたホストのリストが必要です。詳しくは、https://www.veritas.com/content/support/en_US/doc/127664414-132725336-0/v127698742-132725336 を参照してください。 `iscsi-initiator-utils` パッケージがバックアップホストにすでにインストールされている場合は、iSCSI デーモンが実行されていることを確認します。 ■ デーモンの状態を確認するには、`systemctl status iscsid` コマンドを使用します。 ■ デーモンが無効になっている場合は、`systemctl enable iscsid` コマンドを実行してから、`systemctl start iscsid` コマンドを実行して iSCSI デーモンを起動します。

手順の概要	説明と参照
iSCSI による Nutanix AHV クラスタとの安全な通信のための CHAP 設定の構成	一方向 CHAP: ■ iSCSI イニシエータは、ランダムに生成された CHAP パスワードまたはシークレットを使用してターゲット (AHV) で認証します。 相互 CHAP - 自動: ■ NetBackup CMS (Credential Management Service) は、バックアップホストまたはリカバリホストの CHAP パスワードに接頭辞 AHV_ISCSI_MUTUAL_AUTO_ を付加したクレデンシャルを自動生成します。このクレデンシャルは、NetBackup バックアップホストまたはリカバリホストである iSCSI イニシエータと、ターゲットである AHV との相互認証に使用されます。 これらの自動生成された CHAP パスワードの保持期間を設定できます。自動生成された CHAP パスワードのデフォルトの保持期間は、作成日から 90 日です。 注意: デフォルトの構成は一方向 CHAP です。相互 CHAP オプションを有効にするには: p.27 の「iSCSI による AHV クラスタとの安全な通信のための CHAP 設定の構成」を参照してください。
AHV リソースの使用に関するグローバル制限の設定	VM は、VM の作成時に自動的に保護されます。時間が経過すると、同時に保護される VM の数が増える可能性があります。多数の同時バックアップは、AHV とバックアップのパフォーマンスに影響する場合があります。 グローバル制限を設定すると、AHV リソースを効率的に管理できます。 p.43 の「AHV リソース形式のリソース制限の変更」を参照してください。

手順の概要	説明と参照
NetBackup バックアップホストの自動選択	NetBackup バックアップホストの自動選択オプションは、NetBackup メディアサーバーの負荷分散を内部的に使用して、利用可能なサポート対象のメディアサーバーにスナップショットジョブまたはバックアップジョブを割り当てます。NetBackup は、ビジー状態のメディアサーバーへのジョブの送信を回避します。 **メモ:** アプリケーションの整合性を確保したバックアップには、メディアサーバーで NetBackup 9.1 以降が必要です。 前提条件 ■ NetBackup Web UI で、[ストレージ (Storage)]、[ディスクストレージ (Disk storage)]の順に選択します。次に、[ストレージサーバー (Storage servers)]タブをクリックします。負荷分散でサポートされるすべてのメディアサーバーを追加します。 ■ [ストレージ (Storage)]、[ストレージユニット (Storage units)]の順に選択します。*[ストレージユニット名 (storage unit name)]*を選択します。[メディアサーバー (Media server)]の[編集 (Edit)]をクリックします。次に、[自動的に選択することを NetBackup に許可する (Allow NetBackup to automatically select)]を選択します。 ■ AHV 保護計画を作成するときに、[バックアップに使用するサーバーまたはホストを選択する (Select server or host to use for backups)]設定で[自動 (Automatic)]を選択します。

AHV クラスタと NetBackup ホスト間、および Nutanix Prism Central と NetBackup ホスト間の安全な通信の構成

NetBackup では、AHV クラスタ証明書と Prism Central サーバー証明書をその root または中間認証局 (CA) の証明書を使用して検証できるようになりました。

仮想化サーバーでは PEM 証明書形式のみがサポートされます。

次の手順は、バックアップホストとして動作する NetBackup メディアサーバーとすべての AHV アクセスホストに適用できます。

AHV クラスタと AHV アクセスホスト間、および AHV Prism Central サーバーと AHV アクセスホスト間の安全な通信を構成するには:

1. Linux システムから `openssl s_client -connect Nutanix Cluster FQDN:9440 -showcerts < /dev/null` コマンドを使用して、Nutanix 証明書を取得します。

   Nutanix Prism Central の場合は、`openssl s_client -connect Nutanix Prism Central FQDN:9440 -showcerts < /dev/null` を使用します。

2. 結果の最後までスクロールし、次の行から始まる最後の証明書をコピーします。

   ```
   -----BEGIN CERTIFICATE-----
   <Certificate>
   -----END CERTIFICATE-----
   ```

   メモ: BEGIN CERTIFICATE と END CERTIFICATE の前後にある 5 つのダッシュを必ずコピーしてください。

3. この情報をテキストファイルに貼り付けて、ファイル名を ***証明書のファイル名*.pem** に変更し、バックアップホストのパスにコピーします。推奨されるパスは次のとおりです。

   - Linux の場合: `/usr/openv/netbackup`
   - Windows の場合: *install_path*¥NetBackup

4. - Linux の場合: バックアップホストの `bp.conf` に、PEM ファイルのパスとして `ECA_TRUST_STORE_PATH=/usr/openv/netbackup/`***証明書ファイル名*.pem** と入力します。
   - Windows の場合: コマンド *install_path*¥NetBackup¥bin¥nbsetconfig を実行します。

5. `nbsetconfig` コマンドを使用して、アクセスホストで次の NetBackup 構成オプションを構成します。

   構成オプションについて詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。

   外部 CA のサポートについて詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

表 3-2

ECA_TRUST_STORE_PATH	信頼できるすべての root CA 証明書を含む証明書ファイルのファイルパスを指定します。 このオプションは、ファイルベースの証明書に固有です。Windows 証明書ストアを使用している場合、このオプションは構成しないでください。 この外部 CA のオプションをすでに構成してある場合は、Nutanix AHV の CA 証明書を既存の外部証明書トラストストアに追加します。 このオプションを構成していない場合は、必要な Nutanix AHV サーバーの CA 証明書をすべてトラストストアに追加して、このオプションを設定します。
ECA_CRL_PATH	外部 CA の証明書失効リスト (CRL) が保存されているディレクトリのパスを指定します。 この外部 CA のオプションをすでに構成してある場合は、AHV の CRL を CRL キャッシュに追加します。 このオプションを構成していない場合は、まず、必要なすべての CRL を CRL キャッシュに追加します。次に、オプションを設定します。
VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED	このオプションは、AHV、RHV、VMware の安全な通信に影響します。このオプションを指定しないと、作業負荷とプラグインごとに、作業負荷との安全な通信または安全でない通信が個別に決定されます。 Nutanix AHV に対しては、デフォルトで安全な通信が有効です。 このオプションを使用すると、セキュリティ証明書検証をスキップできます。 このオプションを無効にすると、セキュリティ証明書検証をスキップできます。 Cohesity は、ECA_TRUST_STORE_PATH オプションを使用して安全な通信を有効にすることをお勧めします。
VIRTUALIZATION_CRL_CHECK	CRL で仮想化サーバー証明書の失効状態を検証できます。 デフォルトでは、このオプションは有効になっています。

Windows バックアップホストで iSCSI イニシエータサービスを有効にする

次のいずれかを実行します。

1
- [サーバーマネージャー]、[ツール]、[iSCSI イニシエーター]の順にクリックします。
- メッセージウィンドウが表示されます。「サービスを今すぐ開始し、コンピュータを起動するたびにサービスが自動的に開始するよう構成するには、[はい]をクリックしてください。」[はい]をクリックして確認します。

2 または、管理ツールから iSCSI サービスを有効にするには、次の手順を実行します。
- [コントロールパネル]、[管理ツール]、[サービス]の順に開きます。
- [Microsoft iSCSI イニシエータサービス]を見つけます。
- サービスを右クリックして[開始]をクリックします。

メモ: このサービスのデフォルトオプションは[手動]です。設定を[自動]に変更すると、再起動時にサービスが自動的に開始されます。

3 Nutanix iSCSI セグメントネットワークを使用する場合は、バックアップホストのネットワーク構成の詳細について、「p.25 の「Nutanix のセグメント化された iSCSI ネットワークのサポートについて」を参照してください。」を参照してください。

Linux バックアップホストでの iSCSI イニシエータパッケージのインストール

iSCSI イニシエータパッケージをインストールするには、次の yum コマンドと zypper コマンドを使用します。

- `yum install iscsi-initiator-utils" - RedHat`。
- `zypper -n install open-iscsi" - SuSE`。
- Nutanix iSCSI セグメントネットワークを使用する場合は、バックアップホストのネットワーク構成の詳細について、「p.25 の「Nutanix のセグメント化された iSCSI ネットワークのサポートについて」を参照してください。」を参照してください。

Java GUI/CLI で追加したクラスタの Web UI への移行

Java GUI/CLI と Web UI のクレデンシャル管理は個別です。

- 管理コンソールまたは CLI で追加されたクラスタは Web UI に反映されません。その逆も同様です。
- Java GUI/CLI に既存のクラスタがある場合、Web UI でこれらのクラスタとそのクレデンシャルを手動で追加する必要があります。

メモ: Web UI にクラスタを追加した後、Java GUI/CLI からクラスタを削除した場合、そのクラスタは引き続き Web UI に存在します。その逆も同様です。

- Web UI にクラスタを追加した後、クラスタのクレデンシャルを更新する必要がある場合は、Web UI からのみ更新する必要があります。
  次のシナリオを想定します。
  - Web UI と管理コンソールの両方にクラスタが存在します。
  - クラスタのクレデンシャルが Web UI のみで更新されます。
  - クラスタが Web UI から削除されます。

  影響: Java GUI で追加されたクラスタのクレデンシャルが更新されていないと、Java GUI でバックアップとリストアが失敗する場合があります。
  推奨事項: Java GUI からクレデンシャルを更新します。
- クラスタが Web UI に追加された後、Java GUI からクラスタを削除しても、既存のポリシーを使用したバックアップは引き続き成功します。ただしこのシナリオでは、Java GUI からリストアジョブをトリガできません。それには、クラスタが Java GUI 上に存在する必要があるためです。
- クラスタが Java GUI と Web UI から追加され、Java GUI からクラスタを削除した場合、そのクラスタは Web UI で引き続き表示されます。その逆も同様です。
- クラスタが Web UI と Java GUI に存在し、そのクレデンシャルが Web UI で更新された後、そのクラスタが Web UI から削除された場合、Java UI に追加されたクラスタは更新されていないため、バックアップとリストアが失敗する場合があります。問題が発生しないようにするには、Java UI からのクレデンシャルの更新が必要な可能性があります。

Nutanix AHV クラスタを構成するための前提条件

前提条件:

Nutanix AHV クラスタでの iSCSI データサービス IP の構成

1. [セグメント化された iSCSI データサービスの IP を使用 (Use segmented iSCSI Data Service IP)]または[指定したセグメント化 iSCSI データサービスの IP を使用 (Use specified segmented iSCSI data services IP)]オプションを使用するには、ボリューム (ABS) 機能を備えたセグメント化された iSCSI ネットワークインターフェースで AHV クラスタを構成する必要があります。
2. クラスタの構成時に[iSCSI データサービスセグメントの IP を使用 (Use segmented iSCSI data service IP)]オプションを選択する場合、Nutanix では、Nutanix AHV で iSCSI のデータサービス IP を構成することをお勧めします。

   Nutanix AHV Cluster Prism コンソール (`https://<Nutanix クラスタの FQDN/IP>:9440`) に移動します。

   [設定 (Settings)]、[クラスタの詳細 (Cluster details)]、[iSCSI データサービス IP の設定 (Set iSCSI data services IP)]の順に選択します。

メモ: この設定が構成されていない場合:

Windows バックアップホストの場合、バックアップリストアジョブは失敗します。

Linux バックアップホストの場合、セグメント化された iSCSI データサービスの IP 構成が正しく行われていれば、ジョブは NFS を使用するようにフォールバックされます。

Windows バックアップホストでのバックアップリストアジョブのエラーは、アクティビティモニターの[ジョブの詳細 (Job details)]にエラーとして表示されます。Linux バックアップホストでの iSCSI から NFS へのフォールバックは、ジョブの詳細に警告として表示されます。

Nutanix のセグメント化された iSCSI ネットワークのサポートについて

NetBackup では、Nutanix iSCSI セグメント化ネットワークを使用したバックアップトラフィックの分割をサポートします。バックアップトラフィックを分割すると、適切なサイズの専用リソースを設けてバックアップとリカバリの速度とセキュリティを向上させて、本番環境のリソースの負荷を軽減することができます。デフォルトでは、初期接続と検出に iSCSI データサービス IP を使用して、Nutanix クラスタ管理ネットワークを介してバックアップとリカバリのトラフィックがやり取りされます。

AHV クラスタの構成中に、iSCSI トランスポートの次のいずれかのオプションを選択します。

- iSCSI データサービスの IP を使用

- セグメント化された iSCSI データサービスの IP を使用
- セグメント化された iSCSI データサービスの指定された IP を使用

詳しくは、p.28 の「AHV クラスタの追加または参照」を参照してください。

Nutanix iSCSI セグメント化ネットワーク構成を使用するためのバックアップホストのネットワーク構成

- iSCSI セグメント化ネットワークはクラスタ管理ネットワークとは異なるサブネット上に存在するため、バックアップホストのネットワークは次に接続するように構成する必要があります。
  - AHV クラスタ管理ネットワーク
  - iSCSI セグメント化ネットワーク。

  これを実現するには、2 つの VLAN を使用してバックアップホストを構成します。1 つはクラスタ管理ネットワークに対応し、もう 1 つはバックアップとリカバリトラフィックに使用する予定のセグメント化された iSCSI ネットワークに対応します。
- パフォーマンス向上のため、バックアップホストに NetBackup をインストールまたは構成するときに、セグメント化されたネットワークに対応するホスト名または IP をホスト名として使用します。
- Windows ホストで次のコマンドを使用して接続を検証します。
  - [サーバーマネージャー]、[ツール]、[iSCSI イニシエーター]の順に選択します。これにより、[iSCSI イニシエータのプロパティ]ダイアログが開きます。
  - [検出]、[検出ポータル]の順に選択して、AHV クラスタの構成済み iSCSI ターゲットタイプに従って IP アドレスを指定します。
  - DEFAULT: クラスタの詳細ページの iSCSI データサービス IP
  - SEGMENTED: クラスタの詳細ページのセグメント化された iSCSI データ
  - SEGMENTED_SPECIFIC: NetBackup でクラスタを構成するときに指定した仮想 IP。
- Linux ホストで次のコマンドを使用して接続を検証します。
  - `iscsiadm -m discovery -t sendtargets -p` *`correct IP as per configured iSCSITargetType`*
  - DEFAULT: クラスタの詳細ページの iSCSI データサービス IP
  - SEGMENTED: クラスタの詳細ページのセグメント化された iSCSI データ
- SEGMENTED_SPECIFIC: NetBackup でクラスタを構成するときに指定した仮想 IP。接続に問題がある場合、「`iscsiadm: <IP>` **への接続がタイムアウトしました**」のようなエラーが表示されます。

iSCSI による AHV クラスタとの安全な通信のための CHAP 設定の構成

CHAP 設定は、現在選択されているプライマリサーバーに構成済みのすべての AHV クラスタに適用されます。

1. 左側で[作業負荷 (Workloads)]、[Nutanix AHV]の順に選択します。
2. 上部の [AHV 設定 (AHV settings)]をクリックします。
3. [iSCSI 用 CHAP (CHAP for iSCSI)]を選択します。
4. 適切な CHAP オプションを選択します。

NetBackup が AHV との通信に使用するポートについて

次の表に、NetBackup が AHV と通信するために必要なポートを示します。

表 3-3 NetBackup が AHV と通信するために必要なポート

ポート	プロトコル	宛先	目的
860、3260	TCP を介した iSCSI	*双方向	iSCSI は SCSI でストレージデバイスへのブロックレベルアクセスを提供します。 iSCSI は通常、イーサネットを経由してデータ転送を行います。
3205	TCP を介した iSCSI	*双方向	iSNS はファイバーチャネルファブリックサービスをエミュレートし、iSCSI デバイスとファイバーチャネルデバイスの両方を管理できます。iSNS サーバーは、ストレージネットワーク全体の統合構成ポイントとして使用できます
111	TCP	*双方向	ポートマッパー
2049	TCP	*双方向	NFS
9440	TCP	AHV クラスタ AHV Prism Central サーバー	Prism コンソール、REST API

ポート	プロトコル	宛先	目的

*ポートは、AHV アクセスホストと AHV クラスタ間で双方向に開いている必要があります。ポート 9440 は、AHV アクセスホストから AHV クラスタへのインバウンドのみで開いています。

AHV クラスタの追加または参照

AHV クラスタとそのクレデンシャルを追加および参照できます。

AHV クラスタとそのクレデンシャルを追加するには

1 左側で[作業負荷 (Workloads)]、[Nutanix AHV]の順に選択し、次に[AHV クラスタ (AHV cluster)]タブをクリックします。

2 [追加 (Add)]をクリックして AHV クラスタを追加し、以下を入力します。

p.116 の「AHV クレデンシャルの追加中のエラー」を参照してください。

- [クラスタ名 (Cluster name)]

  メモ: NetBackup では、FQDN を使用して AHV クラスタを追加することをお勧めします。クラスタ名は 218 文字の制限に従う必要があります。

- [REST API ポート (REST API port)](デフォルト: 9440)
  バックアップホストと AHV クラスタ間でこのポートを開いたままにする必要があります。
  p.27 の「NetBackup が AHV との通信に使用するポートについて」を参照してください。

- 仮想マシンの Prism Central サーバー関連の属性を保護するには、[このクラスタに Prism Central を使用する (Use Prism Central for this cluster)]チェックボックスにチェックマークを付けます。たとえば、仮想プライベートクラウドネットワーク関連の属性、プロジェクト、カテゴリ、VM の所有者関連の属性をキャプチャする場合などです。
  p.32 の「新しい Nutanix Prism Central の追加」を参照してください。

  メモ: このチェックボックスにチェックマークを付ける前に、Prism Central サーバーを NetBackup 環境に追加する必要があります。

- iSCSI トランスポートから次のいずれかを選択します。
  - iSCSI データサービスの IP を使用
    AHV クラスタで構成されている iSCSI データサービスの IP を、iSCSI ターゲット検出ポータルおよび初期接続ポイントとして使用します。

メモ: このオプションは、次の場合に Linux バックアップホストの NFS にフォールバックされます。

AHV クラスタで iSCSI データサービス IP が構成されていません。

iSCSI 接続がバックアップホストで確立されていません。

- セグメント化された iSCSI データサービスの IP を使用
  AHV クラスタで構成されているセグメント化された iSCSI データサービスの IP を、iSCSI ターゲット検出ポータルおよび初期接続ポイントとして使用します。

メモ: 構成が AHV クラスタにない場合、クラスタ検証は失敗します。

構成が AHV クラスタにない場合、またはバックアップホストに必要なネットワーク構成がない場合、バックアップまたはリカバリジョブは失敗します。

- セグメント化された iSCSI データサービスの指定された IP を使用
  - ［仮想 IP アドレス (Virtual IP address)］フィールドに、有効な IP アドレスを指定します。
    バックアップおよびリカバリ iSCSI データトラフィックに使用する Nutanix セグメント iSCSI ネットワークインターフェースに対応する仮想 IP を提供します。

  指定した IP アドレスを、iSCSI ターゲット検出ポータルおよび初期接続ポイントとして使用します。仮想 IP アドレスが構成済みの iSCSI データサービスインターフェースのいずれかにある場合、NetBackup は Nutanix API を使用して検証します。

メモ: 構成が AHV クラスタ上で実行されない場合、またはバックアップホストに必要なネットワーク構成がない場合、バックアップまたはリカバリジョブは失敗します。

3 - ［バックアップホストの選択 (Select a backup host)］
  このバックアップホストは検証と検出に使用されます。

メモ: クレデンシャルの検証および仮想マシンの検出は、NetBackup 9.1 以降でのみサポートされています。

- ［クレデンシャルの関連付け (Associate credential)］
  次のいずれかを実行します。

- 既存のクレデンシャルを選択します。詳しくは、『NetBackup™ Web UI 管理者ガイド』の「クレデンシャルの管理」を参照してください。
- p.52 の「新しいクラスタのクレデンシャルの追加」を参照してください。

メモ: クラスタ管理者の役割を持つ AHV クラスタユーザーのクレデンシャルを関連付ける必要があります。

4 [権限を追加して管理 (Add and Manage permissions)]をクリックします。

すべての入力の検証が実行されます。

このクラスタへのアクセス権を付与する役割を選択します。『NetBackup™ Web UI 管理者ガイド』の「役割ベースのアクセス制御の管理」を参照してください。

5 別の AHV クラスタのクレデンシャルを追加するには、[追加 (Add)]をクリックします。

AHV クラスタでのインライン処理

AHV クラスタで、次のインライン処理を実行できます。

- [検出 (Discover)]: 選択した AHV クラスタに属する VM 資産を手動で検出します。
- [編集 (Edit)]: AHV クラスタのクレデンシャルを変更します。
- [削除 (Delete)]: AHV クラスタを削除します。
- [権限を管理 (Manage Permissions)]: 選択したクラスタの権限の追加または管理に使用します。

AHV クラスタでの一括処理

1 つ以上の AHV クラスタを選択し、次の一括処理を実行できます。

- [検出 (Discover)]: 選択した AHV クラスタに属する VM 資産を手動で検出します。

メモ: 検出はクラスタに対して順番にトリガされます。

- 検証:
  - AHV クラスタのクレデンシャルを検証します。
  - [iSCSI データサービスセグメントの IP を使用 (Use segmented iSCSI data service IP)]を選択した場合、Nutanix クラスタでセグメント化された iSCSI データサービス IP アドレスが構成されているかどうかが検証されます。
  - [指定した iSCSI データサービスセグメントの IP を使用 (Use specified segmented iSCSI data service IP)]を選択した場合、指定した仮想 IP アドレス

が、Nutanix クラスタでセグメント化された iSCSI データサービス IP アドレスとして構成されているかどうかが検証されます。

- ［削除 (Delete)］: AHV クラスタを削除します。

AHV クラスタを参照します。

AHV クラスタを参照して、VM とストレージコンテナおよびそれらの詳細を見つけることができます。

AHV クラスタを参照するには

1. 左側の［Nutanix AHV］をクリックします。
2. ［AHV クラスタ (AHV cluster)］タブをクリックし、検索を開始します。

   リストには、アクセス権を持つ AHV クラスタが含まれます。

   タブには、次の階層でアクセスできる AHV クラスタが表示されます。

   ```
   All
   AHV_clusters
    cluster1
     VirtualMachine
     StorageContainer
    cluster2
     VirtualMachine
     StorageContainer
   ```

   クラスタを見つけるには、検索フィールドに文字列を入力します。
3. AHV クラスタをクリックして詳細を表示します。
4. 仮想マシンをクリックすると、保護状態、リカバリポイント、リストアアクティビティが表示されます。
5. 選択した VM を保護計画にサブスクライブするには、［保護の追加 (Add protection)］をクリックします。［今すぐバックアップ (Backup now)］、［リカバリ (Recover)］、［権限を管理 (Manage Permission)］オプションも選択できます。

メモ: VM は、NetBackup Web UI 11.0 で Nutanix-AHV ポリシーを使用して保護できます。

6 空き領域と最後の検出時間を表示するには、ストレージコンテナをクリックします。

メモ: データがアドバタイズ容量を超えると、追加データは負の値として表示されます。NetBackup Web UI は空のフィールドを表示し、対応する API は特定のストレージコンテナの空き領域フィールドに対する -ve 値を示します。

7 ストレージコンテナの場合は権限を管理できます。

メモ: [権限の管理 (Manage permission)]はストレージコンテナを選択するときにのみ有効になります。

AHV クラスタの削除

この手順を使用して、AHV クラスタを削除します。

AHV クラスタを削除するには

1 左側で[作業負荷 (Workloads)]、[Nutanix AHV]の順に選択し、次に[AHV クラスタ (AHV clusters)]タブをクリックします。

このタブに、アクセス権を持つ AHV クラスタの名前が一覧表示されます。[検出の状態 (Discovery Status)]と[前回の検出の試行 (Last discovery attempt)]を確認すると、サーバーの VM やその他のオブジェクトが最後にいつ検出されたかも確認できます。

2 AHV クラスタを特定して選択します。

3 [処理 (Actions)]、[削除 (Delete)]の順に選択します。

メモ: クラスタを削除すると、その AHV クラスタに関連付けられているすべての仮想マシンの保護が行われなくなります。既存のバックアップイメージのリカバリは引き続き可能ですが、このサーバーへの VM のバックアップは失敗します。

4 AHV クラスタを削除する場合は、[削除 (Delete)]をクリックします。

新しい Nutanix Prism Central の追加

Nutanix Prism Central とそのクレデンシャルを追加および参照できます。

Nutanix Prism Central とそれに対応するクレデンシャルを追加するには

1 左側の[Nutanix AHV]をクリックし、次に[Prism Central サーバー (Prism Central servers)]タブをクリックします。

2 [追加 (Add)]をクリックして Nutanix Prism Central を追加し、以下を入力します。

- Prism Central サーバー名
- [REST API ポート (REST API port)](デフォルト: 9440)
  バックアップホストと AHV クラスタ間でこのポートを開いたままにする必要があります。
- バックアップホスト

  メモ: バックアップホストのバージョンは NetBackup 10.1.1 以降である必要があります。また、オペレーティングシステムは Linux (RHEL と SUSE) または Windows のいずれかである必要があります。

- [クレデンシャルの関連付け (Associate credential)]

  次のいずれかを実行します。

  - 既存のクレデンシャルに Prism Central サーバーのクレデンシャルを追加する場合、カテゴリで[AHV Prism Central]を選択します。詳しくは、『NetBackup™ Web UI 管理者ガイド』の「クレデンシャルの管理」を参照してください。
  - p.34 の「新しい Prism Central サーバークレデンシャルの追加」を参照してください。

3 [権限を追加して管理 (Add and Manage permissions)]をクリックします

すべての入力の検証が実行されます。

このクラスタへのアクセス権を付与する役割を選択します。『NetBackup™ Web UI 管理者ガイド』の「役割ベースのアクセス制御の管理」を参照してください。

4 別の AHV Prism Central のクレデンシャルを追加するには、[追加 (Add)]をクリックします。

Nutanix Prism Central でのインライン処理

Nutanix Prism Central で、次のインライン処理を実行できます。

- 検証 (Validate): 手動で検証します
- 編集 (Edit): バックアップホストと Nutanix Prism Central のクレデンシャルを変更します。
- 削除 (Delete): Nutanix Prism Central を削除します。

- 権限を管理 (Manage Permissions): 選択した Prism Central の権限の追加または管理に使用します。

Nutanix Prism Central での一括処理

1 つ以上の Nutanix Prism Central を選択し、次の一括処理を実行できます。

- 検証 (Validate)
- 削除 (Delete)

新しい Prism Central サーバークレデンシャルの追加

1. 左側の[Nutanix AHV]をクリックし、次に[Nutanix Prism Central]タブをクリックします。
2. [追加 (Add)]をクリックして、新しい Prism Central サーバーを追加します。
3. [AHV Prism Central の追加 (Add AHV Prism Central)]、[クレデンシャルの関連付け (Associate credential)]ページで、[新しいクレデンシャルの追加 (Add a new credential)]をクリックします。
4. クレデンシャル名、タグ、説明などの詳細情報を入力します。
5. [Nutanix Prism Central のクレデンシャル (Credentials for the Nutanix Prism Central)]の部分で、関連付けられている Prism Central サーバーのユーザー名、パスワード、ドメインを追加します。

   メモ: 関連付けられているクレデンシャルは、Prism Central Admin の役割を持つユーザーである必要があります。

6. [次へ (Next)]をクリックします。

   既存の役割を選択するか、新しい役割を追加してクレデンシャルに権限を付与します。
7. [保存 (Save)]をクリックします。

Nutanix Prism Central の削除

この手順を使用して、1 台以上の Nutanix Prism Central を削除します。

Nutanix Prism Central を削除するには

1. 左側の[Nutanix AHV]をクリックし、次に[Prism Central サーバー (Prism Central servers)]タブをクリックします。

   このタブに、アクセス権を持つ Nutanix Prism Central の名前が一覧表示されます。

2. AHV Prism Central を特定して選択します。

3. 1 台以上の Prism Central サーバーを選択し、[処理 (Actions)]、[削除 (Delete)]の順に選択します。

   メモ: Prism Central を削除すると、削除された Prism Central サーバーに関連付けられているすべての仮想マシンは、プロジェクト、カテゴリ、所有者、仮想プライベートクラウドネットワーク関連の属性なしでバックアップまたはリカバリされます。

4. [これらの Prism Central サーバーに関連付けられているすべてのクラスタで[このクラスタに Prism Central サーバーを使用]を無効にします。有効にしたままにする場合は、選択を解除します。(Disable "Use Prism Central server for this cluster" for all clusters associated with these Prism Central servers. De-select if you want to keep it enabled.)]チェックボックスのチェックマークをはずし、必要に応じて[削除 (Delete)]をクリックします。

メモ: Nutanix Prism Central が削除されると、この Prism Central サーバーのクラスタの資産検出は自動的にトリガされません。そのため、これらのクラスタの VM は、次の資産検出がトリガされるまで、VM の詳細ページに Prism Central サーバーとプロジェクトを表示します。

メモ: 環境内に、この Prism Central に関連付けられたクラスタが存在し、[このクラスタに Prism Central サーバーを使用 (Use Prism Central server for this cluster)]チェックボックスのチェックマークが付いており、[この Prism Central サーバーに関連付けられているすべてのクラスタで[このクラスタに Prism Central サーバーを使用]を無効にします。(Disable "Use Prism Central server for this cluster" for all clusters associated with this Prism Central server)]チェックボックスのチェックマークをはずすことで Prism Central が削除された場合、関連付けられた Prism Central サーバーが追加されるまで、以降のバックアップジョブまたはリストアジョブは失敗します。

インテリジェント VM グループの作成

問い合わせと呼ばれるフィルタのセットに基づいて、インテリジェント VM グループを作成できます。NetBackup は、問い合わせに基づいて自動的に仮想マシンを選択し、それらをグループに追加します。その後、グループに保護を適用できます。インテリジェントグ

ループでは、VM 環境内の変更が自動的に反映されるため、グループ内の VM のリストを手動で修正する必要がないことに注意してください。

メモ: 問い合わせと一致する新たに検出された VM は、バックグラウンドタスクによってインテリジェント VM グループに追加されます。このバックグラウンドタスクは、NetBackup Web 管理サービスの開始から 30 分後に実行されます。その後、このタスクは 30 分ごとに実行されます。

インテリジェント VM グループを作成するには

1. 左側で[作業負荷 (Workloads)]、[Nutanix AHV]の順に選択します。
2. [インテリジェント VM グループ (Intelligent VM groups)]タブ、[インテリジェント VM グループの追加 (Add intelligent VM group)]の順にクリックします。
3. グループの名前と説明を入力します。

   インテリジェント VM グループの表示名の長さは、1 文字から 256 文字の間で指定する必要があります。
4. [クラスタ (Clusters)]ペインで、[クラスタの追加 (Add clusters)]をクリックします。

   メモ: グループを作成するには、少なくとも 1 つのクラスタが必要です。

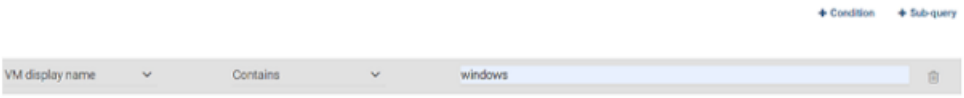
   - [クラスタの追加 (Add clusters)]ウィンドウで、追加するクラスタを選択します。

     メモ: クラスタを追加するには、クラスタに対する表示および作成権限が必要です。

     ---
5. 次のいずれかを実行します。
   - デフォルトの問い合わせである[すべての VM を含める (Include all VMs)]を選択します。
     保護計画を実行すると、AHV クラスタの一部であるすべての VM がインテリジェント VM グループに追加されます。
   - 独自の問い合わせを作成します。[条件の追加 (Add condition)]をクリックします。
6. 条件を追加するには、ドロップダウンを使用してキーワードと演算子を選択し、値を入力します。

   オプションについては、この手順の後 (「インテリジェント VM グループ作成のための問い合わせオプション」) で説明します。

   以下が問い合わせの例です。



この例の問い合わせでは、表示名に windows が含まれるすべての VM をグループに追加します。

問い合わせの効果を変更するには、[+ 条件 (+ Condition)]をクリックし、[AND]または[OR]をクリックして、キーワード、演算子、条件の値を選択します。例:

この例では、AND を使用して問い合わせの範囲を絞り込みます。表示名に windows が含まれ、電源状態が ON の VM のみが選択されます。VM の表示名に windows が含まれず、電源状態が ON でない場合、その VM はグループに追加されません。

問い合わせの範囲を広げるには、[OR]を使用します。

この例では、[OR]が設定されているため、問い合わせでグループに次の VM が追加されます。

- 表示名に windows が含まれる VM (電源状態に関係なく)
- 電源状態が ON の VM (表示名に関係なく)

7 問い合わせをテストするには、[プレビュー (Preview)]をクリックします。

メモ: 問い合わせベースの選択処理は動的です。仮想環境の変更は、保護計画の実行時に問い合わせが選択する仮想マシンに影響する可能性があります。その結果、保護計画が後で実行されたときに問い合わせが選択する VM が、プレビューに現在表示されているものと同一でなくなる可能性があります。

メモ: [プレビュー (Preview)]をクリックするかグループを保存した場合、グループの VM を選択するときに、問い合わせオプションでは大文字小文字が区別されます。[仮想マシン (Virtual machine)]で、グループに選択されていない VM をクリックすると、[仮想マシングループのメンバー (Member of virtual machine groups)]フィールドは `none` になります。

ただし、保護計画にグループを追加したときに、保護計画のバックアップが実行されると、一部の問い合わせオプションは、大文字と小文字が区別されないものとして扱われます。その結果、同じ VM がグループに含められてバックアップされる場合があります。

各オプションの大文字小文字関連の動作については、次のトピックを参照してください。

「インテリジェント VM グループ作成のための問い合わせオプション」

---

8 グループを保存するには、[権限を追加して管理 (Add and Manage permissions)]をクリックします。

メモ: このグループの権限を編集、保護、管理できます。

- 保護計画の追加:
  p.69 の「保護計画を使用した AHV VM またはインテリジェント VM グループの保護」を参照してください。
- インテリジェント VM グループの編集または更新:
  p.41 の「インテリジェント VM グループを更新します。」を参照してください。
- VM グループへの権限の割り当て:
  p.40 の「インテリジェント VM グループへの権限の割り当て」を参照してください。

インテリジェント VM グループ作成のための問い合わせオプション

表 3-4 問い合わせキーワード

キーワード	説明
displayName	VM の表示名。 保護計画の実行時には大文字と小文字が区別されます。
powerState	VM の電源状態。 ON と OFF は大文字と小文字が区別されます。
vmUuid	VM のインスタンス UUID。 例: 501b13c3-52de-9a06-cd9a-ecb23aa975d1 保護計画の実行時には大文字と小文字は区別されません。
StorageContainerName	ストレージコンテナの名前。 保護計画の実行時には大文字と小文字が区別されます。
Category	次の項目について確認します。 AHV カテゴリは、Nutanix Prism Central サーバーの VM に適用されます。フル検索の場合は、CategoryName:Value の形式であることが必要です。

表 3-5 問い合わせ演算子

演算子	説明
Starts with	文字列の先頭に値が出現する場合に一致します。 たとえば、入力した値が「box」の場合、このオプションは文字列「box_car」と一致しますが、「flatbox」とは一致しません。
Ends with	文字列の末尾に値が出現する場合に一致します。 たとえば、入力した値が「dev」の場合、このオプションは文字列「01dev」と一致しますが、「01dev99」または「devOP」とは一致しません。

演算子	説明
Contains	入力した値が文字列のどこにある場合でも一致します。 たとえば、入力した値が「dev」の場合、このオプションは「01dev」、「01dev99」、「devOP」、「development_machine」などの文字列と一致します。
=	入力した値にのみ一致します。 たとえば、入力した値が「VMTest27」の場合、このオプションは「VMtest27」(大文字小文字が同じ) とは一致しますが、「vmtest27」、「vmTEST27」、または「VMtest28」とは一致しません。
!=	入力した値と等しくない任意の値と一致します。

インテリジェント VM グループへの権限の割り当て

VM グループに権限を割り当てる前の検討事項について説明します。

- 表示 (View)/更新 (Update)
  - グループ内のすべてのクラスタについて、表示 (View) 権限が必要です。
  - クラスタの表示 (View) 権限がないと、[仮想マシン (Virtual Machines)]タブでグループの VM をプレビューできません。
  - 権限のないクラスタは、ロック記号付きで表示されます。
  - 削除されたクラスタは、X 記号付きで表示されます。
  - 既存の VM グループに新しいクラスタを追加するには、対象のクラスタに対する表示 (View) 権限が必要です。
  - VM グループを更新するには、クラスタに対する表示 (View) 権限が必要です。ただし、存在しないクラスタまたは表示 (View) 権限がないクラスタを削除することはできます。
- 保護 (Protect)
  - グループ内のすべてのクラスタについて、保護 (Protect) 権限が必要です。
  - VM グループを保護するには、グループのすべてのクラスタと VM グループに対する保護 (Protect) 権限が必要です。
  - すべてのクラスタに対して保護 (Protect) 権限がないと、[今すぐバックアップ (Backup Now)]が無効になります。
  - [保護の削除 (Remove protection)] は、クラスタの権限にかかわらず有効になります。これは VM グループの権限のみによって制御されます。

役割の権限について詳しくは、『NetBackup Web UI 管理者ガイド』を参照してください。

インテリジェント VM グループを更新します。

インテリジェント VM グループを編集できます。

インテリジェント VM グループを編集するには

1. 左側で[作業負荷 (Workloads)]、[Nutanix AHV]の順に選択します。
2. [インテリジェント VM グループ (Intelligent VM groups)]タブで、編集する VM グループを選択します。
3. [仮想マシン (Virtual machine)]タブで、[編集 (Edit)]をクリックします。

   [クラスタ (Clusters)]ペインで、[クラスタの追加 (Add clusters)]をクリックします。

メモ: VM グループを削除または追加できます。インテリジェント VM グループを追加するには、p.35 の「インテリジェント VM グループの作成」を参照してください。

インテリジェント VM グループの削除

インテリジェント VM グループを削除するには、次の手順を使用します。

インテリジェント VM グループを削除するには

1. 左側で[作業負荷 (Workloads)]、[Nutanix AHV]の順に選択します。
2. [インテリジェント VM グループ (Intelligent VM groups)]タブでグループを見つけます。
3. グループが保護されていない場合は、チェックボックスにチェックマークを付けて[削除 (Delete)]をクリックします。
4. グループが保護されている場合は、グループをクリックしてスクロールダウンし、鍵の記号をクリックして、[サブスクライブ解除 (Unsubscribe)]をクリックします。
5. [削除 (Remove)]をクリックします。

iSCSI 用 CHAP の設定

CHAP 設定は、選択されているプライマリサーバーで構成済みのすべての AHV クラスタに適用されます。デフォルトでは、構成は一方向 CHAP に設定されています。

メモ: 一方向 CHAP オプションの場合、対応は不要です。

相互 CHAP オプションを有効にするには:

1. 左側で[作業負荷 (Workloads)]、[Nutanix AHV]の順に選択します。
2. 右上で[AHV 設定 (AHV settings)]、[iSCSI 用 CHAP (CHAP for iSCSI)]の順に選択し、適切な相互 CHAP オプションを選択します。

メモ: 相互 CHAP の場合、NetBackup クレデンシャル管理システムは選択したバックアップまたはリカバリホストのプレフィックス `AHV_ISCSI_MUTUAL_AUTO_` を持つクレデンシャルを自動生成します。iSCSI 相互 CHAP のクレデンシャルは、[クレデンシャルの管理 (Credential Management)]タブに表示されます。

メモ: デフォルトでは、相互 CHAP オプション用に自動生成されたクレデンシャルは、デフォルトの AHV 管理者役割で作成されたユーザーには表示されません。特定のユーザーがクレデンシャルを表示できるようにするには、セキュリティ管理者またはルートユーザーがクレデンシャルの表示権限をそのユーザーに付与する必要があります。

この自動生成されたクレデンシャルは、[クレデンシャルの管理 (Credential Management)]タブに表示され、編集できず、削除のみが可能です。手動でこのクレデンシャルを削除すると、このクレデンシャルを生成したジョブが次回実行されたときに、自動的に再作成されます。

AHV アクセスホストの追加

NetBackup では、AHV アクセスホストと呼ばれる特別なホストを使用します。これは仮想マシンに代わってバックアップを実行する NetBackup クライアントです。アクセスホストは、NetBackup のメディアサーバーまたはクライアントソフトウェアがインストールされる唯一のホストです。仮想マシンでは、NetBackup クライアントソフトウェアは不要です。ただし、アクセスホストは、仮想マシンのストレージコンテナにアクセスできる必要があります。アクセスホストはストレージコンテナからデータを読み取り、ネットワーク経由でデータをメディアサーバーに送信します。

AHV アクセスホストは、以前は AHV バックアップホストと呼ばれていました。アクセスホストは、リストアを実行する場合はリカバリホストと呼ばれます。

メモ: 追加するすべてのアクセスホストに、NetBackup のメディアサーバーソフトウェアまたはクライアントソフトウェアがインストールされていることを確認してください。

AHV アクセスホストを追加するには

1. 左側で[作業負荷 (Workloads)]、[Nutanix AHV]の順に選択します。
2. 右上で[AHV 設定 (AHV settings)]、[アクセスホスト (Access hosts)]の順に選択します。

   NetBackup でこれまでに追加されたすべてのアクセスホストが一覧表示されます。
3. [+ 追加 (+ Add)]をクリックします。
4. アクセスホストの名前、FQDN、または IP を入力し、[追加 (Add)]をクリックします。

AHV アクセスホストの削除

AHV アクセスホストを削除するには

1. 左側で[作業負荷 (Workloads)]、[Nutanix AHV]の順に選択します。
2. 右上で[AHV 設定 (AHV settings)]、[アクセスホスト (Access hosts)]の順に選択します。

   NetBackup でこれまでに追加されたすべてのアクセスホストが一覧表示されます。
3. AHV アクセスホストを特定し、削除アイコンをクリックします。
4. 内容を確認したら、[削除 (Delete)]をクリックします。

AHV リソース形式のリソース制限の変更

Nutanix AHV のリソース制限により、Nutanix AHV リソースで実行できる同時バックアップの数が制御されます。これらの設定は、現在選択しているプライマリサーバーのすべての NetBackup ポリシーに適用されます。

Nutanix AHV で利用可能なリソース制限:

- ホストあたりのバックアップジョブ (Backup Jobs per Host)
- AHV クラスタあたりのバックアップジョブ (Backup Jobs per AHV Cluster)
- ストレージコンテナあたりのバックアップジョブ (Backup Jobs per Storage Container)
- AHV クラスタあたりのスナップショットジョブ (Snapshot Jobs per AHV Cluster)

メモ: 各リソースのデフォルト値は 0 (制限なし) です。

Nutanix AHV リソースのリソース制限を設定するには

1. 左側で[作業負荷 (Workloads)]、[Nutanix AHV]の順に選択します。
2. 右上で[AHV 設定 (AHV settings)]、[リソース制限 (Resource limits)]の順に選択します。

   各リソースのデフォルト値は 0 (制限なし) です。

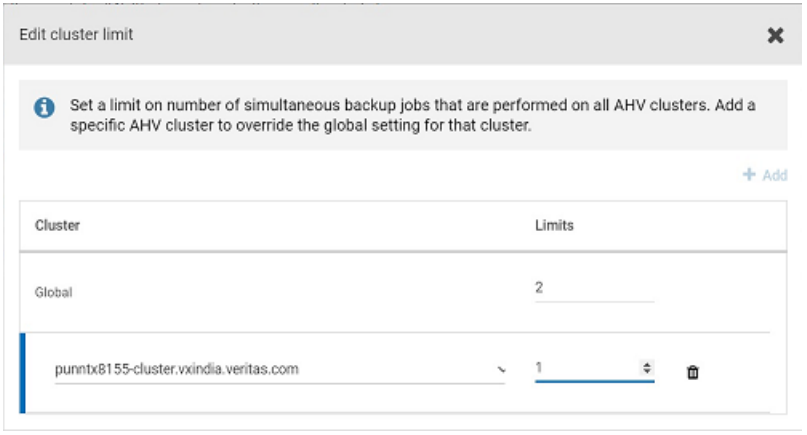
   メモ: [AHV クラスタあたりのスナップショットジョブ (Snapshot Jobs per AHV Cluster)]オプションは、クラスタあたりの同時スナップショット操作数の制限を設定します。バックアップのスナップショット作成フェーズのみ適用されます。同時バックアップジョブの数は制御されません。この設定は、複数のスナップショット操作が AHV クラスタに与える影響を制御できます。その AHV クラスタのグローバルスナップショット設定を上書きするには、特定の AHV クラスタを追加します。

3. 変更する AHV リソースを特定して、[編集 (Edit)]をクリックします。

4 次のオプションを選択します。

AHVリソース形式のグローバル制限を設定します。	[グローバル (Global)]設定を特定して、適用する[制限 (Limits)]の値を選択します。 この値により、リソース形式で実行される同時バックアップ数が制限されます。
特定の AHV リソースの制限を設定します。	[追加 (Add)]をクリックします。 リストから、リソースを選択します。 適用する[制限 (Limits)]の値を選択します。 この値により、選択したリソースで実行される同時バックアップ数が制限されます。

次の例では、すべての AHV クラスタのグローバル制限 2 と、選択した AHV クラスタの制限 1 が示されています。



5 [保存 (Save)]をクリックします。

[制限 (Limits)]には、リソース形式で実行できる同時バックアップの数が表示されます。これはグローバル制限の値です。[上書き (Override)]の値には、グローバル制限と異なる制限があるリソースの数が表示されます。

注意: リソース制限を設定した後は、いくつかのジョブが実行されるまで制限は反映されません。

すべての AHV リソースのリソース制限をリセットする

すべての AHV リソースのリソース制限をリセットするには

- ［デフォルト値に戻す (Reset default values)］を使用すると、すべての上書きが削除され、グローバルなAHVリソース制限の設定がすべてデフォルト値に設定されます。

例 - 2 つのノードがある Nutanix クラスタのリソース制限の設定

たとえば、次の例を考えてみます。

- Nutanix クラスタには 2 つのノードがあります。
- 各ノードは 40 台の VM をホストします。したがって、クラスタには 80 台の VM があります。
- Nutanix-AHV ポリシーには 20 台の VM があります。

NetBackup がバックアップ用の Nutanix 環境に接続するときは、VM ごとに 1 つの接続を確立します。リソース制限が設定されていない場合、合計で 160 の並列実行ジョブ (80 のスナップショット + 80 のバックアップ) が実行されます。この記事を参照してください。

Nutanix は、クラスタ内の CVM あたり最大 20 の同時接続を推奨しています。つまり、ノードあたり 20 台の VM が同時にバックアップされます。この例では、次の設定で、接続数 20 の制限を適用できます。

ノードあたりのバックアップジョブ (Backup Jobs per Node)	20
クラスタあたりのバックアップジョブ (Backup Jobs per Cluster)	40
ストレージコンテナあたりのバックアップジョブ (Backup Jobs per Storage Container)	ストレージ技術の特性に基づいて制限を設定します。
クラスタあたりのスナップショットジョブ (Snapshot Jobs per Cluster)	10

バックアップが開始すると、次のようにジョブがアクティビティモニターに表示されます。

- スナップショットジョブ: 20
- 実行中のジョブ: 10 (スナップショットジョブとそれらのバックアップジョブ)
- キューへ投入済みのジョブ: 10
- 実行中のスナップショットジョブが完了すると、キューへ投入済みのスナップショットジョブが実行中になります。

AHV 資産の自動検出の間隔の変更

AHV 資産の自動検出は一定の間隔で実行されます。デフォルトの間隔は 8 時間です。自動検出の間隔を変更する手順は次のとおりです。

AHV 資産の自動検出の間隔を変更するには

1. 左側で[作業負荷 (Workloads)]、[Nutanix AHV]の順にクリックします。
2. 右側で[AHV 設定 (AHV settings)]、[自動検出 (Autodiscovery)]の順に選択します。
3. [間隔 (Frequency)]、[編集 (Edit)]の順に選択します。
4. NetBackup で AHV 資産の自動検出を実行する間隔を上下の矢印を使用して選択します。次に、[保存 (Save)]をクリックします。

   選択できる範囲は 1 時間から 24 時間までです。自動検出の間隔を分または秒単位で設定する場合や自動検出を無効にする場合は、AHV 自動検出 API を使用する必要があります。

マルウェアのスキャン

NetBackup バージョン 10.5.1 以降では、Nutanix AHV の作業負荷を介して Nutanix 資産でマルウェアをスキャンするためのサポートが提供されます。

マルウェアスキャンをトリガするには、スキャンホストを構成する必要があります。スキャンホストの構成について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』の「スキャンホストの構成」の章を参照してください。

バックアップイメージのスキャン

このセクションでは、特定のポリシーのクライアントバックアップイメージでマルウェアをスキャンする手順について説明します。

クライアントバックアップイメージのポリシーでマルウェアをスキャンするには

1. 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順に選択します。
2. [マルウェアの検出 (Malware detection)]ページで[マルウェアのスキャン (Scan for malware)]を選択します。
3. [検索基準 (Search by)]オプションで、[バックアップイメージ (Backup images)]を選択します。

   次のいずれかのスキャンの種類を選択します。

   - [マルウェアスキャン (Malware scan)] - デフォルトのマルウェアスキャンを使用してイメージをスキャンする場合は、このオプションを選択します。

- ［YARA スキャン (YARA scan)］- YARA ルールを使用してイメージをスキャンする場合は、このオプションを選択します。
  ［脅威フィードの選択 (Select threat feeds)］オプションをクリックします。
  ［スキャン用の脅威フィールドを選択する (Select threat feeds for scanning)］ダイアログボックスで、必要な YARA ルールまたは以前にアップロードした YARA ルールの zip ファイルを選択します。

4 スキャンの種類が［マルウェアスキャン (Malware scan)］である場合、次のすべての手順が適用されます。

［スキャナホストプール (Scanner host pool)］オプションで、［マルウェアスキャナホストプールの選択 (Select malware scanner host pool)］にリストされているスキャナホストプールのリストから適切なホストプール名を検索して選択します。

メモ: 選択したスキャンホストプールのスキャンホストは、NFS/SMB 共有形式で構成されているストレージサーバーで作成されたインスタントアクセスマウントにアクセスできる必要があります。

---

5 検索条件で、以下を確認して編集します。

- ポリシー名
  サポート対象のポリシー形式のみが一覧表示されます。
- クライアント名
  サポート対象のポリシー形式のバックアップイメージを含むクライアントが表示されます。
- ポリシー形式
  マルウェアスキャンが有効になっているすべてのサポート対象ポリシーを表示します。

  メモ: Nutanix-AHV ポリシーおよび保護計画のバックアップからバックアップが取得された場合、Nutanix-AHV ポリシーには Nutanix-AHV イメージが表示されます。

  警告: Hypervisor ポリシー形式には、Nutanix AHV イメージと RHV イメージが表示されます。NetBackup は、Nutanix AHV イメージに対してのみマルウェアスキャンをサポートします。

- バックアップ形式
- コピー

選択したコピーがインスタントアクセスをサポートしない場合、バックアップイメージのマルウェアスキャンはスキップされます。

- ディスクプール
  MSDP (PureDisk)、OST (Data Domain など)、AdvancedDisk ストレージ形式のディスクプールが一覧表示されます。
- ディスク形式
  MSDP (PureDisk)、OST (Data Domain など)、AdvancedDisk のディスク形式が一覧表示されます。
- 感染状態
  バックアップイメージのマルウェア感染状態の検索は、[マルウェアスキャンで検出された感染 (Infection detected by malware scan)]、[ファイルハッシュの検索 (File Hash Search)]、[感染なし (Not Infected)]、[未スキャン (Not scanned)]、または[すべて (All)]に基づいて行われます。
- [バックアップの期間の選択 (Select the timeframe of backups)]で、日時の範囲を確認するか、更新します。
- [感染を検出するとマルウェアスキャンを中止します (Abort malware scan on detecting an infection)]オプションを選択すると、感染したイメージに対してクリーンなリカバリがサポートされなくなります。

6 [検索 (Search)]をクリックします。

7 検索条件を選択し、選択したスキャンホストがアクティブで利用可能であることを確認します。

8 [スキャンするバックアップの選択 (Select the backups to scan)]テーブルで、スキャンする 1 つ以上のイメージを選択します。

9 [マルウェアのスキャン (Scan for malware)]をクリックします。

10 スキャンが開始されると、[スキャンの状態 (Scan status)]が表示されます。

状態フィールドは次のとおりです。

- 未スキャン (Not scanned)
- 感染なし (Not infected)
- 感染 (Infected)
- 失敗 (Failed)
  状態にカーソルを重ねると、スキャンが失敗した理由が表示されます。

メモ: 検証で失敗したバックアップイメージは無視されます。マルウェアスキャンがサポートされるのは、サポート対象のポリシー形式で、インスタントアクセス機能を備えた、ストレージに格納されたバックアップイメージのみです。

- 処理中 (In progress)
- 保留中 (Pending)

メモ: 1 つ以上の処理中および保留中のジョブのマルウェアスキャンをキャンセルできます。

- 感染 - マルウェアスキャン中止 (Infected - Malware scan aborted)

作業負荷の種類ごとの資産

メモ: YARA スキャンでは、Kubernetes のみがサポートされています。

サポート対象の資産でマルウェアをスキャンするには、次の手順を実行します。

1. 左側の[作業負荷 (Workloads)]で、サポートされている作業負荷を選択します。
2. バックアップが完了したリソースを選択します。

   例: Nutanix AHV
3. [処理 (Actions)]、[マルウェアのスキャン (Scan for malware)]を選択します。
4. [マルウェアスキャン (Malware scan)]ページで、次の操作を行います。
   - [開始日時 (Start date/time)]と[終了日時 (End date/time)]を選択して、スキャンの日付範囲を選択します。
   - [スキャナホストプール (Scanner host pool)]を選択します。
   - [現在の感染状態 (Current infection status)]リストから、次のいずれかを選択します。
     - 未スキャン (Not scanned)
     - 感染なし (Not infected)
     - マルウェアスキャンで検出された感染 (Infection detected by malware scan)
     - ファイルハッシュ検索で検出された感染 (Infection detected by file hash search)
     - すべて (All)

5 ［マルウェアのスキャン (Scan for malware)］をクリックします。

メモ: マルウェアスキャナホストは、一度に 3 つのイメージのスキャンを開始できます。

6 スキャンが開始されると、［マルウェアの検出 (Malware detection)］に［スキャンの状態 (Scan status)］が表示され、次のフィールドが表示されます。

- 未スキャン (Not scanned)
- 感染なし (Not infected)
- 感染 (Infected)
- 失敗 (Failed)

  メモ: 検証で失敗したバックアップイメージは無視されます。

- 処理中 (In progress)
- 保留中 (Pending)

4

クレデンシャルの管理

この章では以下の項目について説明しています。

AHV クラスタのクレデンシャルの管理

このセクションでは、AHV クラスタのクレデンシャルを追加、更新、検証する手順について説明します。

新しいクラスタのクレデンシャルの追加

1. 左側で[作業負荷 (Workloads)]、[Nutanix AHV]の順に選択し、次に[AHV クラスタ (AHV cluster)]タブをクリックします。
2. [追加 (Add)]をクリックして、新しいクラスタを追加します。
3. [AHV クラスタの追加 (Add AHV cluster)]、[クレデンシャルの関連付け (Associate credential)]ページで、[新しいクレデンシャルの追加 (Add a new credential)]をクリックします。
4. [クレデンシャルの追加 (Add credential)]ページで、[クレデンシャル名 (Credential name)]、[ユーザー名 (User name)]、[パスワード (password)]などの詳細を入力します。

5 [次へ (Next)]をクリックします。

クレデンシャルの権限を提供する役割を選択または追加します。

6 [保存 (Save)]をクリックします。

メモ: 追加したクレデンシャルを[編集 (Edit)]または[削除 (Remove)]できます。

AHV クラスタのクレデンシャルの更新と検証

AHV クレデンシャルを検証するには

1 左側で[作業負荷 (Workloads)]、[Nutanix AHV]の順に選択し、次に[AHV クラスタ (AHV clusters)]タブをクリックします。

2 ■ 特定のクラスタのクレデンシャルを検証するには、AHV クラスタを特定して選択します。次に、[クレデンシャル (Credentials)]列または上部のバーから[検証 (Validate)]をクリックします。

■ 複数のサーバーのクレデンシャルを同時に検証するには、それらの AHV クラスタを特定して選択します。次に、上部のバーから[検証 (Validate)]をクリックします。

メモ: 選択した AHV クラスタの現在のクレデンシャルが NetBackup で検証されます。

クレデンシャルが有効でない場合、NetBackup では[クレデンシャル (Credentials)]に[無効 (Invalid)]と表示されます。AHV クラスタのクレデンシャルを更新するには、次の手順を実行します。

AHV クラスタのクレデンシャルを更新するには

1 左側で[作業負荷 (Workloads)]、[Nutanix AHV]の順に選択し、次に[AHV クラスタ (AHV cluster)]タブをクリックします。

2 AHV クラスタを特定して選択します。

3 [処理 (Actions)]、[編集 (Edit)]の順に選択します。

4 クレデンシャルを必要に応じて更新します。

メモ: AHV クラスタのクレデンシャルを追加または更新した場合も、AHV クラスタの検出が自動的に開始されます。要求でバックアップホストの情報を指定すると、検出の実行に加えて、クレデンシャルの検証にもその情報が使用されます。検出の場合、バックアップホストとして動作する NetBackup メディアサーバーまたはクライアントでサポートされる最小バージョンは、NetBackup 9.1 です。

5 [保存 (Save)]をクリックします。

選択した AHV クラスタの更新後のクレデンシャルが NetBackup で検証されます。

新しい Nutanix Prism Central のクレデンシャルの管理

このセクションでは、Nutanix Prism Central のクレデンシャルを追加、更新、検証する手順について説明します。

新しい Nutanix Prism Central クレデンシャルの追加

1 左側の[Nutanix AHV]をクリックし、次に[Prism Central サーバー (Prism Central servers)]タブをクリックします。

2 [追加 (Add)]をクリックして、新しい Prism Central サーバーを追加します。

3 [AHV Prism Central サーバーの追加 (Add AHV Prism Central server)]、[クレデンシャルの関連付け (Associate credential)]ページで、[新しいクレデンシャルの追加 (Add a new credential)]をクリックします。

4 [クレデンシャルの追加 (Add credential)]ページで、[クレデンシャル名 (Credential name)]、[ユーザー名 (User name)]、[パスワード (password)]などの詳細を入力します。

5 [次へ (Next)]をクリックします。

クレデンシャルの権限を提供する役割を選択または追加します。

6 [保存 (Save)]をクリックします。

メモ: 追加したクレデンシャルを[編集 (Edit)]または[削除 (Remove)]できます。

Nutanix Prism Central のクレデンシャルの更新と検証

Prism Central サーバーのクレデンシャルを検証するには

1. 左側の[Nutanix AHV]をクリックし、次に[Prism Central サーバー (Prism Central servers)]タブをクリックします。
2. - 特定の Prism Central サーバーのクレデンシャルを検証するには、Prism Central サーバーを特定して選択します。次に、[クレデンシャル (Credentials)]列または上部のバーから[検証 (Validate)]をクリックします。
   - 複数のサーバーのクレデンシャルを同時に検証するには、それらの Prism Central サーバーを特定して選択します。次に、上部のバーから[検証 (Validate)]をクリックします。

メモ: 選択した Prism Central サーバーの現在のクレデンシャルが NetBackup で検証されます。

クレデンシャルが有効でない場合、NetBackup では[クレデンシャル (Credentials)]に[無効 (Invalid)]と表示されます。Prism Central サーバーのクレデンシャルを更新するには、次の手順を実行します。

Prism Central サーバーのクレデンシャルを更新するには

1. 左側の[Nutanix AHV]をクリックし、次に[Prism Central サーバー (Prism Central servers)]タブをクリックします。
2. Prism Central サーバーを特定して選択します。
3. [処理 (Actions)]、[編集 (Edit)]の順に選択します。
4. クレデンシャルを必要に応じて更新します。

メモ: Prism Central サーバーのクレデンシャルを追加または更新すると、Prism Central サーバーの検出も自動的に開始されます。要求でバックアップホストの情報を指定すると、検出の実行に加えて、クレデンシャルの検証にもその情報が使用されます。検出の場合、バックアップホストとして動作する NetBackup メディアサーバーまたはクライアントでサポートされる最小バージョンは、NetBackup 9.1 です。

---

5. [保存 (Save)]をクリックします。

   選択した Prism Central サーバーの更新後のクレデンシャルが NetBackup で検証されます。

資産に適用されているクレデンシャル名の表示

資産タイプに構成されている指定したクレデンシャルを表示できます。特定の資産に対してクレデンシャルが構成されていない場合は、このフィールドは空白です。

Nutanix AHV クラスタのクレデンシャルを表示するには

1. 左側で[作業負荷 (Workloads)]、[Nutanix AHV]の順に選択します。
2. [AHV クラスタ (AHV clusters)]タブで、[クレデンシャル名 (Credential name)]列を見つけます。

指定したクレデンシャルの編集または削除

指定したクレデンシャルのプロパティを編集したり、指定したクレデンシャルをNetBackupの[クレデンシャルの管理 (Credential management)]から削除できます。

指定したクレデンシャルの編集

指定したクレデンシャルのタグ、説明、カテゴリ、認証に関する詳細、または権限を変更したい場合はこれを編集できます。クレデンシャル名は変更できません。

メモ: AHV クラスタに使用されるクレデンシャルカテゴリが *AHV* で、Nutanix Prism Central の場合は *Prism Central* であることを確認します。

指定したクレデンシャルを編集するには

1. 左側の[クレデンシャルの管理 (Credential management)]を選択します。
2. [指定したクレデンシャル (Named credentials)]タブで、編集するクレデンシャルのチェックボックスを特定して選択します。
3. 必要に応じて、[編集 (Edit)]を選択してクレデンシャルを更新します。
4. 変更を確認し、[完了 (Finish)]を選択します。

指定したクレデンシャルの削除

NetBackup で不要になった、指定したクレデンシャルは削除できます。削除するクレデンシャルを使用する資産がある場合は、それらの資産に別のクレデンシャルを適用してください。そうしないと、それらの資産のバックアップとリストアが失敗する可能性があります。

指定したクレデンシャルを削除するには

1. 左側の[クレデンシャルの管理 (Credential management)]を選択します。
2. [指定したクレデンシャル (Named credentials)]タブで、削除するクレデンシャルを特定してチェックボックスを選択します。
3. [削除 (Delete)]、[削除 (Delete)]の順に選択します。

5

インスタントアクセス

この章では以下の項目について説明しています。

インスタントアクセスの前提条件

インスタントアクセスを使用している場合は、WORM インスタンスが AHV クラスタサーバーの次のポートにアクセスできることを確認します。

表 5-1　　ポートの詳細

インスタンス	AHV コンポーネント	ポート番号
WORM	AHV クラスタサーバー	9440

インスタントアクセス機能を使用する前の考慮事項と制限事項

インスタントアクセス仮想マシン機能について、次の点に注意します。

- この機能は、NetBackup Web UI またはインスタントアクセス API を使用してローカルまたはクラウド LSU (論理ストレージユニット) から作成されたバックアップコピーでサポートされます。

クラウド LSU (論理ストレージユニット) でのインスタントアクセスの制限事項については、『NetBackup 重複排除ガイド』を参照してください。

- この機能は、保護計画またはポリシーから作成されたバックアップコピーでサポートされます。
- ファイルのダウンロード機能は、NetBackup Appliance、NetBackup Virtual Appliance、Flex Appliance、BYO (Build Your Own) サーバーでサポートされています。

  Flex WORM ストレージでのインスタントアクセスには、次のサービスが必要です:

  - NGINX、NFS、SAMBA、WINBIND (Active Directory が必要な場合)、SPWS、VPFS
- この機能では、メディアサーバー重複排除プール (MSDP) メディアサーバーまたは WORM ストレージサーバーからの同時マウントポイントが 50 個に制限されます。Flex Appliance を使用している場合、この機能では、各ノードからの同時マウントポイントが 50 個に制限されます。
- [ダウンロード (Download)]オプションとインスタントアクセス VM 作成機能を使用したファイルまたはフォルダのダウンロードの場合、NetBackup Web UI では、プライマリサーバーがメディアサーバーへの接続に使用するのと同じ名前または IP アドレスを持つメディアサーバーにアクセスできる必要があります。
- メディアサーバーのアプライアンスがサードパーティの証明書を使用する場合、この機能を使用する前に、NetBackup プライマリサーバーで特定の構成を作成する必要があります。
  詳しくは、『NetBackup Appliance セキュリティガイド』で、サードパーティの証明書に関するセクションと、サードパーティの SSL 証明書の実装に関するセクションを参照してください。
- 5-minutes-alive-session のしきい値は、アプライアンスおよび BYO の Web サーバー NGINX で定義されます。ダウンロード用に選択されたファイルとフォルダは、このしきい値内で圧縮されダウンロードされる必要があります。
- ストレージサーバーとプライマリサーバーが NetBackup の以前のバージョンからアップグレードされた後、確実にインスタントアクセスを有効化するには、次のコマンドを使用して、アップグレードされたプライマリサーバーで NetBackup Web サービスを再起動します。

  ```
  /usr/openv/netbackup/bin/nbwmc stop
  /usr/openv/netbackup/bin/nbwmc start
  ```
- Windows VM からファイルまたはフォルダをダウンロードまたはリストアする必要がある場合は、Windows レジストリハイブの数が 1 万未満であることを確認します。
  レジストリハイブに関する詳しい情報を参照できます。

制限事項

- RDM (raw デバイスマッピングモード) または永続モードのディスクがある VM は、この機能ではサポートされません。
- Windows のリストアで、ReFS ファイルシステムはサポートされません。
- インスタントアクセス機能は、Windows 10 のコンパクトオペレーティングシステムをサポートしていません。オペレーティングシステムが圧縮されているかどうかを確認するには、VM をバックアップする前に、コマンドプロンプトで `compact "/compactos:query"` を実行します。
  圧縮を無効にするには、VM をバックアップする前に、コマンドプロンプトで `"compact /compactos:never"` を実行します。これによって、VM のバックアップにインスタントアクセス機能を使用できます。
- インスタントアクセス機能では、ハードリンクがサポートされません。イメージにハードリンクファイルが含まれている場合にイメージからユニバーサル共有を作成すると、`vpfsd` では、これらのハードリンクファイルのサイズが 0 バイトと表示されます。
- Linux VM の場合、ミラーボリュームはインスタントアクセスではサポートされません。

インスタントアクセス VM の作成

NetBackup バックアップイメージから、インスタントアクセス VM を作成できます。仮想マシンは瞬時に利用可能になるため、ほぼゼロのリカバリ時間目標を達成できます。NetBackup は仮想マシンのスナップショットをバックアップストレージデバイスに直接マウントするため、AHV クラスタはスナップショットを通常の仮想マシンとして扱えます。

マウントされた VM のスナップショットは、さまざまな目的に使用できます。例:

- VM からのファイルのリカバリ、またはディスクファイルのコピー。
- パッチのテストなど、VM でのテストの実行。
- トラブルシューティングまたはディザスタリカバリ。
- アプリケーションの検証。

メモ: この機能は、Build Your Own (BYO) サーバーでサポートされています。この機能では、NetBackup バックアップイメージがメディアサーバー重複排除プール (MSDP) ストレージデバイスに格納されることが必要です。インスタントアクセス VM の使用については、次の情報を参照してください。

p.58 の「インスタントアクセス機能を使用する前の考慮事項と制限事項」を参照してください。

インスタントアクセス VM を作成するには

1. 左側の[Nutanix AHV]をクリックします。
2. VM を特定してクリックします。
3. [リカバリポイント (Recovery points)]タブをクリックし、バックアップが発生した日付をクリックします。

   利用可能なイメージは、各イメージのバックアップタイムスタンプ付きで各行に表示されます。
4. インスタントアクセスを使用したリカバリのオプションがあるイメージまたはイメージのコピーで、[リカバリ (Recover)]、[インスタントアクセス仮想マシンの作成 (Create instant access virtual machine)]の順にクリックします。
5. [リカバリターゲット (Recovery target)]で[リストア先 (Restore to)]の値を確認します。

   デフォルト値は VM のバックアップイメージから取得されます。

   - 代替の場所にリカバリするには、[リストア (Restore)]オプションでデフォルトのクラスタを変更します。続いて[次へ (Next)]をクリックします。

     メモ: ターゲットのドロップダウンで想定されるストレージコンテナを一覧表示するには、ストレージコンテナまたはクラスタで[表示 (View)]および[リストアターゲットの表示 (View restore target)]権限が必要です。
6. [リカバリオプション (Recovery options)]の値を確認または変更します。

既存の VM ID の代わりに新しい VM ID を作成する (Create new VM ID instead of existing one)	バックアップ中に設定された既存の値とは異なる VM に新しい ID を作成します。 **メモ:** VM ID は、VM UUID です。
リカバリ後に電源をオン (Power on after recovery)	リカバリが完了すると、VM の電源が自動的にオンになります。
移行の有効化 (Enable migration)	インスタントアクセス VM に関連付けられたストレージを、NetBackup ストレージから Nutanix クラスタ上のコンテナに自動的に移動します。

7 [詳細 (Advanced)]オプションを確認または変更します。

ネットワークインターフェースの削除 (Remove network interfaces)	バックアップ中に VM に設定されたネットワークインターフェースを削除します。
MAC アドレスの保持 (Retain MAC address)	バックアップ中に VM に設定された MAC アドレスを保持します。

8 [次へ (Next)]をクリックして、[リカバリの概要 (Recovery overview)]を実行します。

p.102 の「Nutanix AHV のリカバリ前チェック」を参照してください。

9 [リカバリの開始 (Start recovery)]をクリックします。

10 ジョブの進捗を監視するには、[リストアアクティビティ (Restore activity)]タブをクリックします。特定のジョブを選択すると、その詳細が表示されます。

11 [インスタントアクセス仮想マシン (Instant access virtual machines)]タブをクリックして、新しい VM の詳細を表示します。

VM バックアップイメージからのファイルとフォルダのダウンロード

VM のインスタントアクセスイメージを参照して、ファイルとフォルダをダウンロードできます。

メモ: インスタンスアクセス VM の使用について詳しくは、p.58 の「インスタントアクセス機能を使用する前の考慮事項と制限事項」を参照してください。

VM バックアップイメージからファイルとフォルダをダウンロードするには

1 左側の[Nutanix AHV]をクリックします。

2 VM を特定してクリックします。

3 [リカバリポイント (Recovery points)]タブをクリックします。カレンダービューで、バックアップが発生した日付をクリックします。

利用可能なイメージが、それぞれのバックアップタイムスタンプと一緒に一覧表示されます。

4 インスタントアクセスを使用したリカバリのオプションがあるイメージまたはイメージのコピーで、[リカバリ (Recover)]、[ファイルとフォルダのダウンロード (Download files and folders)]の順に選択します。

5 ファイルを選択し、[追加 (Add)]をクリックして、ダウンロードリストにファイルを追加します。

フォルダをクリックしてドリルダウンします。階層の上位レベルに移動して戻るには、フォルダのパスを使用します。

ファイルを検索するにはファイル名を入力します。

ダウンロードリストには、選択したファイルとフォルダについて、各ファイルの場所が表示されます。

6 [次へ (Next)]をクリックします。

7 ダウンロードパッケージの作成が完了したら、[ダウンロード (Download)]をクリックします。

[アクティビティモニター (Activity monitor)]タブにリカバリの状態が表示されます。

インスタントアクセス Build Your Own (BYO)

独自の VM を構築し (Red Hat Enterprise オペレーティングシステムを使用)、Nutanix AHV インスタントアクセスをサポートできます。次の機能を使用できます。

- インスタントアクセス VM の作成
- Acropolis オペレーティングシステム (AOS) クラスタへのデータディスクの移行
- ファイルとフォルダのダウンロード

以前の NetBackup リリースで作成された BYO VM でインスタントアクセスを使用するには、NetBackup 11.0 以降にアップグレードする必要があります。

インスタントアクセス Build Your Own (BYO) の前提条件

前提条件 (新規インストールとアップグレード):

- NetBackup Appliance オペレーティングシステムと同じバージョンの Red Hat Enterprise Linux 7.6 以降を搭載した BYO ストレージサーバー。
- Docker/Podman がインストールされている BYO ストレージサーバー。
  - Docker/Podman バージョンは、対応する正式な RHEL バージョンのリリースに存在するものと同じである必要があります。これは、対応する RHEL yum ソース (RHEL extra) からインストールする必要があります。
  - Docker/Podman アプリケーションが環境パスに含まれている。
- NFS サービスがインストールされている BYO ストレージサーバー。

- NGINX バージョンがインストールされている BYO ストレージサーバー。
  - NGINX バージョンは、対応する正式な RHEL バージョンのリリースに存在するものと同じである必要があります。対応する RHEL yum ソース (epel) からインストールする必要があります。
  - `policycoreutils` と `policycoreutils-python` パッケージが同じ RHEL yum ソース (RHEL サーバー) からインストールされていることを確認し、次のコマンドを実行します。
    - `semanage port -a -t http_port_t -p tcp 10087`
    - `setsebool -P httpd_can_network_connect 1`
  - ストレージサーバーの /mnt フォルダが、どのマウントポイントによっても直接マウントされていないことを確認します。マウントポイントはそのサブフォルダに対してマウントされる必要があります。
  - 次のコマンドを使用して、selinux の logrotate 権限を有効にします。

    ```
    semanage permissive -a logrotate_t
    ```
- BYO の場合、Docker/Podman コンテナは VMDK ファイルの参照に使用されます。コンテナに関連するデータは `/var/lib/` に格納され、20 GB 以上の空き容量が必要です。

インスタントアクセス Build Your Own (BYO) のハードウェア構成の必要条件

表 5-2 ハードウェア構成の必要条件

CPU	メモリ	ディスク
■ 2.2 GHz 以上のクロックレート。 ■ 64 ビットのプロセッサ。 ■ 最小 4 コア。8 コアを推奨。64 TB のストレージの場合、Intel x86-64 アーキテクチャでは 8 つのコアを必要とします。 ■ CPU 構成で VT-X オプションを有効にします。	■ 16 GB (8 TB から 32 TB のストレージの場合は、1 TB のストレージ用に 1 GB の RAM)。 ■ 32 TB 以上のストレージの場合は 32 GB の RAM。 ■ ライブマウントごとに追加の 500 MB の RAM。	ディスクのサイズは、バックアップのサイズによって異なります。 NetBackup とメディアサーバー重複排除プール (MSDP) のハードウェアの必要条件を参照してください。

よく寄せられる質問

ここでは、Build Your Own (BYO) のインスタントアクセスについてよく寄せられる質問をいくつかご紹介します。

表 5-3 よく寄せられる質問

よく寄せられる質問	回答
Docker/Podman をインストールせずにストレージを構成またはアップグレードした後、BYO で (ファイルのダウンロードおよびリストアのため) インスタントアクセスによるファイルの参照を有効にする方法を教えてください。	次に示す順序で操作を実行します。 1 必要な Docker/Podman のバージョンをインストールします。 2 インスタントアクセス機能の使用を開始します。 たとえば、ファイルのダウンロード、ファイルのリストアなどを行うことができます。
nginx サービスをインストールせずにストレージを構成またはアップグレードした後に、BYO で Nutanix AHV インスタントアクセス機能を有効にする方法を教えてください。	次に示す順序で操作を実行します。 1 必要な nginx サービスのバージョンをインストールします。 2 新しい BYO nginx 構成エントリ `/etc/nginx/conf.d/byo.conf` が、元の `/etc/nginx/nginx.conf` ファイルの HTTP セクションに含まれていることを確認します。 3 コマンド `/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo` を実行します。
「`MSDP REST API` がポート `10087` の `HTTPS` を介して利用可能であることの確認」で触れている vpfs-config.log ファイルで発生した問題を解決するには、どのようにしたら良いですか。	次に示す順序で操作を実行します。 1 Yum ツールを使用して、`policycoreutils` と `policycoreutils-python` パッケージをインストールします。 2 Nginx に SELinux が必要な次のルールを追加し、10087 ポートにバインドします。 ■ `semanage port -a -t http_port_t -p tcp 10087` ■ `setsebool -P httpd_can_network_connect 1` 3 コマンド `/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo` を実行します。

よく寄せられる質問	回答
BYO のインスタントアクセスでは、デフォルトで自己署名証明書が使用され、*.pem 外部証明書のみがサポートされます。 外部 CA (*.pem 証明書) で署名された証明書で置き換えることが必要な場合は、どのようにしたら良いですか。	外部証明書を構成するには、次の手順を実行します。新しい証明書がすでに生成されている場合 (証明書にはメディアサーバーの長いホスト名と短いホスト名が含まれている必要があります) は、手順 4 に進みます。 **1** RSA の公開鍵と秘密鍵のペアを作成します。 **2** 証明書の署名要求 (CSR) を作成します。 証明書にはメディアサーバーの長いホスト名と短いホスト名が含まれている必要があります。 **3** 外部認証局が証明書を作成します。 **4** `<PDDE ストレージのパス >/spws/var/keys/spws.cert` を証明書に置き換え、`<PDDE ストレージのパス >/spws/var/keys/spws.key` を秘密鍵に置き換えます。 **5** 次のコマンドを実行して、証明書を再ロードします。 `/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo`
GNOME のインスタントアクセスライブマウント共有で、メディアの自動マウントを無効にする方法を教えてください。 自動マウントが有効になっている場合、ソースフォルダは GNOME のライブマウント共有からマウントされ、小さなディスクが表示されます。このシナリオでは、インスタントアクセス機能が正しく動作しません。 マウントされたディスクコンテンツソースは、ライブマウント共有配下の `.../meta_bdev_dir/...` フォルダにあり、マウントターゲットは `/run/media/...` フォルダにあります。	次のガイドラインに従って、GNOME 自動マウントを無効にします。 https://access.redhat.com/solutions/20107

よく寄せられる質問	回答
/var/log/vpfs/vpfs-config.log ファイルの次の問題は、どうすれば解決できますか。 **** Asking the NetBackup Webservice to trust the MSDP webserver (spws) **** /usr/openv/netbackup/bin/nblibcurlcmd failed (1):	次に示す順序で操作を実行します。 1 NetBackup プライマリサーバーが起動しており、ファイアウォールが NetBackup プライマリサーバーとストレージサーバー間の接続をブロックしていないことを確認します。 2 ストレージサーバーで次のコマンドを実行して、接続状態を確認します。 /usr/openv/netbackup/bin/bpclntcmd -pn 3 NetBackup プライマリサーバーを起動し、NetBackup プライマリサーバーとストレージサーバー間の接続を許可してから、次のコマンドを実行します。 /usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo

6

AHV 仮想マシンの保護

この章では以下の項目について説明しています。

AHV 仮想マシンを保護する前の考慮事項

保護計画の作成中に、いくつかの検証を考慮する必要があります。

- スケジュール形式が[自動 (Automatic)]の場合は、すべての NetBackup バージョンが以下のようになっていることを確認します。
  - 増分スケジュールは、バージョン 8.3 以降のバックアップホストでのみサポートされます。

- バックアップホストとして Windows コンピュータを使用している場合は、バージョンが 9.1 以降であることを確認します。
- ［仮想マシンの静止を有効にする (Enable virtual machine quiesce)］オプションを使用する場合は、バックアップホストが 9.1 以降であることを確認します。
- インテリジェント VM グループにフィルタとしてのカテゴリ属性がある場合、バックアップホストのバージョンは 10.4 以降である必要があります。

- Nutanix Prism Central 関連の VM 属性を保護するには、Nutanix Prism Central の構成が必要です。

メモ: Nutanix Prism Central 関連の VM 属性を保護するには、NetBackup ホストのバージョンが 10.1.1 以降であることを確認します。

- Cohesityでは、仮想マシンまたはインテリジェントグループを保護する際は、保護計画またはポリシーのいずれかを使用することをお勧めします。
- Cohesityは、リカバリ API で `client` および `filter` の代わりに `backupId` をリカバリポイントとして使用することをお勧めします。

メモ: ポリシーを使用して AHV VM を保護するには、NetBackup プライマリサーバー、メディアサーバー、クライアントまたはバックアップホストが NetBackup バージョン 11.0 以降にアップグレードされていることを確認します。

保護計画を使用した AHV VM またはインテリジェント VM グループの保護

次の手順を使用して、AHV VM またはインテリジェント VM グループである資産を保護計画にサブスクライブします。保護計画に資産をサブスクライブするときに、定義済みのバックアップ設定を資産に割り当てます。

メモ: 自分に割り当てられている RBAC の役割によって、管理する資産と、使用する保護計画にアクセスできるようにする必要があります。インテリジェント VM グループを保護する場合は、グループを構成しているすべてのクラスタに保護権限が付与されていることを確認します。

AHV VM または VM グループを保護するには

1. 左側で[作業負荷 (Workloads)]、[Nutanix AHV]の順に選択します。
2. [仮想マシン (Virtual machine)]タブまたは[インテリジェント VM グループ (Intelligent VM groups)]タブで、VM または VM グループのボックスにチェックマークを付けて[保護の追加 (Add protection)]をクリックします。
3. 保護計画を選択し、[次へ (Next)]をクリックします。
4. 次の 1 つ以上の設定を調整できます。
   - スケジュールと保持 (Schedules and retention)
     バックアップの開始時間帯を変更します。
   - バックアップオプション (Backup options)
     バックアップに使用するサーバーまたはホストを選択します。

     メモ: ここで[自動 (Automatic)]オプションを選択し、カテゴリをフィルタとして持つインテリジェント VM グループを保護するためにこの保護計画を使用する場合は、ストレージユニットに関連付けられているバージョン 10.4 以降のメディアサーバーが少なくとも 1 台あることを確認してください。

   - 拡張オプション (Advance options)
     保護計画の仮想マシンの静止を有効にします。
5. [保護 (Protect)]をクリックします。

   [仮想マシン (Virtual machines)]または[インテリジェント VM グループ (Intelligent VM groups)]に、選択の結果が表示されます。

ポリシーを使用した AHV VM またはインテリジェントグループのバックアップ

ポリシーを使用して Nutanix-AHV 資産を保護する手順を次に示します。

資産をバックアップするためのポリシーの構成手順

1. NetBackup Web UI にログインします。
2. [保護 (Protection)]をクリックし、次に[ポリシー (Policies)]をクリックします。
3. [追加 (Add)]をクリックします。[ポリシーの作成 (Create policy)]ページが表示されます。
4. [属性 (Attribute)]タブで、次の処理を実行します。
   - [ポリシー名 (Policy name)]を指定します。

- ［ポリシー形式 (Policy type)］として［Nutanix-AHV］を選択します。
- 必要に応じて、他の値を構成します。

5 ［スケジュール (Schedules)］タブで、［追加 (Add)］をクリックし、バックアップスケジュールのパラメータを指定します。

6 ［仮想マシン (Virtual machines)］タブをクリックし、インテリジェントグループまたは個々の仮想マシンの選択オプションを選択します。

7 ［Nutanix-AHV］タブをクリックし、バックアップするサーバーまたはホストを選択します。

8 ［作成 (Create)］をクリックします。

VPC 内の AHV VM の保護

NetBackup 10.2 のリリースでは、Nutanix Prism Central Server 内の仮想プライベートネットワークでホストされている仮想マシンを保護できます。NetBackup は、構成済みの Nutanix Prism Central を使用して、次の VM の属性も保護します。

- プロジェクト: 要件の共通セットまたは共通の構造と機能を持つユーザーのセット。プロジェクトは、リソース使用状況を管理するためのユーザー役割の論理グループを提供します。
- 関連付けられたカテゴリ: カテゴリは、エンティティをキー値ペアにグループ化したものです。通常、新しいエンティティは、いくつかの基準に基づいてカテゴリに割り当てられます。ポリシーは、特定のカテゴリ値を割り当てられた (グループ化された) エンティティに関連付けることができます。
- VPC ネットワーク属性: VPC 内の VM に割り当てられたプライマリ IP とセカンダリ IP。
- プロジェクトの所有者: CALM が Nutanix Prism Central 内に共同配備されているプロジェクトのユーザーまたは所有者。

VPC で VM を保護するには

1 Nutanix Prism Central を構成します。

メモ: 構成済みのクラスタの場合、NetBackup は、[Prism Central を使用 (Use Prism Central)]チェックボックスにチェックマークが付いている場合にのみ、Nutanix Prism Central を使用して VM の追加属性を保護します。

p.32 の「新しい Nutanix Prism Central の追加」を参照してください。

2 [Prism Central を使用 (Use Prism Central)]チェックボックスにチェックマークを付けて、NetBackup 内のすべての Nutanix AHV クラスタを追加します。

p.28 の「AHV クラスタの追加または参照」を参照してください。

3 VM の保護について詳しくは、次のセクションを参照してください。

p.69 の「保護計画を使用した AHV VM またはインテリジェント VM グループの保護」を参照してください。

メモ: 保護計画で[自動 (Automatic)]オプションを選択して、バックアップに使用するサーバーまたはホストを選択し、ストレージユニットが 10.2 より前の NetBackup メディアサーバーに関連付けられているとします。その場合、バックアップジョブはバックアップホストとして古いメディアサーバーを使用する場合があります。

この場合、バックアップジョブは Nutanix Prism の中央属性を保護せずに完了します。

vTPM 対応 AHV VM の保護

TPM (Trusted Platform Module) は、暗号化やハードウェア (およびソフトウェア) の整合性保護などのセキュリティサービスの暗号化キーを管理するために使用されます。AHV vTPM (Virtual Trusted Platform Module) は、仮想デバイスとして動作する TPM 2.0 仕様のソフトウェアベースのエミュレーションです。

NetBackup では、Nutanix-AHV ポリシーと Nutanix 保護計画を使用して vTPM 対応 VM を保護しています。

Nutanix Prism Central および Prism クラスタのクレデンシャルを構成する必要があります。

p.32 の「新しい Nutanix Prism Central の追加」を参照してください。

p.52 の「AHV クラスタのクレデンシャルの管理」を参照してください。

制限事項

- vTPM に格納されている情報のバックアップは Nutanix でサポートされません。

- vTPM は、Q35 以外のマシン形式の Nutanix VM ではサポートされません。

詳細および推奨事項については、Nutanix のマニュアルを参照してください。

AHV 資産の保護設定のカスタマイズ

スケジュールなど、保護計画の特定の設定をカスタマイズできます。

AHV 資産の保護設定をカスタマイズするには

1. 左側で[作業負荷 (Workloads)]、[Nutanix AHV]の順にクリックします。
2. 次のいずれかを実行します。
   - VM の設定の編集
     [仮想マシン (Virtual machines)]タブで、編集する VM をクリックします。
   - インテリジェント VM グループの設定の編集
     [インテリジェント VM グループ (Intelligent VM groups)]タブで、編集するグループをクリックします。
3. [保護のカスタマイズ (Customize protection)]、[続行 (Continue)]の順にクリックします。
4. 次の設定のうち、1 つ以上を編集できます。
   - バックアップ開始時間帯。
     p.74 の「スケジュールと保持」を参照してください。
   - バックアップオプション
     p.74 の「バックアップオプション」を参照してください。
5. [保護 (Protect)]をクリックします。

AHV 資産のポリシーの変更

このセクションでは、要件に従ってポリシーを編集するための詳細について説明します。ポリシーを編集する手順を次に示します。

ポリシーの編集

1. 左ペインで、[保護 (Protection)]を展開し、[ポリシー (Policies)]をクリックします。[ポリシー (Policies)]ページが表示されます。
2. 必要なポリシーを選択し、[編集 (Edit)]をクリックします。[ポリシーを編集 (Edit policy)]ページが表示されます。
3. 必要な値を変更し、[保存 (Save)]をクリックします。

スケジュールと保持

- 開始時間帯 (Start window)
  - バックアップを開始できる時間帯を設定します。

バックアップオプション

ユーザーは、次の設定を調整して保護計画にサブスクライブできます。

1 アクセスホストとしてバックアップに使用するサーバーまたはホストを選択する。

仮想マシンに代わってバックアップを実行するホスト。[Automatic (自動)]を選択すると、ストレージユニットに基づいて、NetBackup にメディアサーバーを選択させることができます。または、ユーザーがリストから別のホストを選択できます。これらのホストは、環境内のその他のメディアサーバーか、アクセスホストとして構成されているホストです。

メモ: 9.1 より前のバージョンのバックアップホストで VM をバックアップする際に、同じ UUID を持つ VM が異なるクラスタに存在する場合、この VM の[最後に成功したバックアップ (Last successful backup)]の状態の列は更新されません。ただし、VM のバックアップは成功し、リカバリポイントを表示してリカバリできます。

---

2 詳細オプション (Advanced Options)

有効にするには、p.74 の「仮想マシンの静止を有効にするための前提条件」を参照してください。

- 仮想マシンの静止を有効にする (Enable virtual machine quiesce)
- 静止されたスナップショットが失敗した場合は静止解除されたスナップショットを有効にする (Enable unquiesce snapshots if quiesced snapshots fail)

デフォルトで、仮想マシンの I/O は NetBackup がスナップショットを作成する前に静止します。ほとんどの場合、このデフォルトを使用する必要があります。ファイルのアクティビティを静止しないと、スナップショットのデータの一貫性は保証されません。静止を無効にすると、一貫性を保つためバックアップデータを分析する必要があります。

仮想マシンの静止を有効にするための前提条件

- デフォルトでは、Nutanix クラスタで実行している VM に対して NGT (Nutanix Guest Tools) 機能は無効になっています。Nutanix は NGT のインストールを推奨しています。仮想マシンの静止を可能にする、アプリケーションの整合性スナップショットを作

成する予定がある場合、VM に事前凍結 (pre-freeze) スクリプトと解凍後 (post-thaw) スクリプトが用意されています。

メモ: アプリケーションの整合性を確保したバックアップには、NetBackup メディアサーバーバージョンのバージョン 9.1 以降が必要です。

- NGT をインストールしてスクリプトを追加するには、こちらを参照してください。

VM またはインテリジェント VM グループの保護の解除

VM またはインテリジェント VM グループのサブスクライブを、保護計画から解除できます。資産のサブスクライブが解除されると、バックアップは実行されなくなります。

メモ: 保護計画から資産のサブスクライブを解除するときに、Web UI の[保護計画名 (Protected By)]列に従来のポリシーが表示される可能性があります。この状況は、保護計画に資産がサブスクライブされており、その資産に対してバックアップが実行される場合に発生することがあります。資産は、有効なバックアップイメージを持ったまま、保護計画からサブスクライブ解除されます。Web UI には従来のポリシーが表示されますが、資産を保護する有効なポリシーがない場合もあります。

VM またはインテリジェント VM グループの保護を解除するには

1. 左側で[作業負荷 (Workloads)]、[Nutanix AHV]の順に選択します。
2. [仮想マシン (Virtual machines)]タブまたは[インテリジェント VM グループ (Intelligent VM groups)]タブで、VM またはインテリジェント VM グループを選択します。
3. [保護の削除 (Remove protection)]、[はい (Yes)]の順にクリックします。

   [仮想マシン (Virtual machines)]または[インテリジェント VM グループ (Intelligent VM group)]で、資産が[保護されていません (Not protected)]と表示されます。

VM またはインテリジェント VM グループの保護状態の表示

VM またはインテリジェント VM グループの保護に使用される保護計画を表示できます。

VM またはインテリジェント VM グループの保護状態を表示するには

1. 左側で[作業負荷 (Workloads)]、[Nutanix AHV]の順に選択します。
2. グリッドで[列を表示または非表示 (Show or Hide columns)]をクリックします。[次のポリシーによって保護: (Protected by policy)]をクリックします。

3 [仮想マシン (Virtual machines)]タブまたは[インテリジェント VM グループ (Intelligent VM groups)]タブで、VM またはインテリジェント VM グループを選択します。

[保護 (Protection)]タブに、資産のサブスクリプション計画の詳細が表示されます。

メモ: 資産のバックアップが完了しているにもかかわらず状態が未完了と表示される場合は、p.117 の「新たに検出された VM の状態のエラー」を参照してください。を参照してください。

---

4 資産が保護されていない場合、[保護の追加 (Add protection)]をクリックして保護計画を選択します。

p.69 の「保護計画を使用した AHV VM またはインテリジェント VM グループの保護」を参照してください。

7

AHV 仮想マシンのリカバリ

この章では以下の項目について説明しています。

AHV 仮想マシンをリカバリする前の考慮事項

リカバリホストまたはバックアップホストが、ポート 9440 を介して AHV クラスタおよび Prism Central サーバー (インストールされている場合) と通信できることを確認します。

リカバリ前チェックについて

リカバリ前チェックでは、次の項目が確認されます。

- サポート対象の文字の使用と表示名の長さ
- 同じ表示名を持つ VM の存在
- AHV サーバーとの接続状態と AHV クレデンシャルの検証
- AHV クラスタの可用性
- ストレージコンテナで利用可能な領域

AHV 仮想マシンのリカバリ

元のバックアップ場所または別の場所に VM をリカバリできます。バックアップイメージのデフォルトのコピーからのリカバリに加え、別のコピーがある場合はそのコピーからもリカバリできます。デフォルトのコピーはプライマリコピーとも呼ばれます。

VM をリカバリするには

1. 左側で[作業負荷 (Workloads)]、[Nutanix AHV]の順に選択します。
2. VM を特定してクリックします。
3. [リカバリポイント (Recovery points)]タブをクリックします。左側の[カレンダー (Calendar)]ビューで、緑色の点で示された、バックアップが発生した日付をクリックします。

   利用可能なイメージが、それぞれのバックアップタイムスタンプと一緒に一覧表示されます。
4. リカバリするイメージについて、次のいずれかのイメージリカバリオプションを選択します。

   - リカバリ (Recover)
     バックアップイメージのデフォルトのコピーからリカバリします。
   - デフォルトのコピーからリカバリ (Recover from the default copy)
     バックアップイメージのデフォルトのコピーからリカバリします。このオプションは、コピーが複数ある場合に表示されます。
   - nn 個のコピー (nn copies)
     バックアップイメージのデフォルトのコピーまたは別のコピーからリカバリします。NetBackup では、同じバックアップイメージのコピーを最大 10 個まで保持できます。このオプションを選択すると、利用可能なすべてのコピーが表示されます。それぞれのコピーについて、[ストレージ名 (Storage Name)]、[ストレージサーバー (Storage Server)]、[ストレージサーバー形式 (Storage server type)]が表示されます。リカバリするコピーに対して[リカバリ (Recover)]をクリックします。

5 [リカバリターゲット (Recovery target)]で[リストア先 (Restore to)]の値を確認します。

デフォルト値は VM のバックアップイメージから取得されます。

- 代替の場所にリカバリするには、[リストア (Restore)]オプションでデフォルトのクラスタを変更します。続いて[次へ (Next)]をクリックします。

メモ: ターゲットのドロップダウンで想定されるストレージコンテナを一覧表示するには、ストレージコンテナまたはクラスタで[表示 (View)]および[リストアターゲットの表示 (View restore target)]権限が必要です。

6 [リカバリオプション (Recovery options)]の値を確認または変更します。

既存の仮想マシンの上書きを許可 (Allow overwrite of existing virtual machine)	宛先に同じ名前の VM が存在する場合に既存の VM を削除します。そのような VM はリカバリの開始前に削除する必要があります。そうしないと、リカバリは失敗します。
リカバリ後に電源をオン (Power on after recovery)	リカバリが完了すると、VM の電源が自動的にオンになります。
リカバリホスト (Recovery host)	リカバリの実行に使用するホストを示します。デフォルトでは、リカバリホストはバックアップを実行するホストです。
既存の VM ID の代わりに新しい VM ID を作成する (Create new VM ID instead of existing one)	バックアップ中に設定された既存の値とは異なる VM に新しい ID を作成します。 **メモ:** VM ID は、VM UUID です。
スナップショットから VM をリストアする (Restore VM from snapshot)	スナップショットから VM をリストアできます。 **メモ:** スナップショットを利用できない場合、VM はバックアップイメージからリストアされます。

7 ［詳細 (Advanced)］オプションを確認または変更します。

ネットワークインターフェースの削除 (Remove network interfaces)	ネットワークインターフェースの削除 (同じ AHV サーバーの異なるクラスタの代替リストアでは無効) **メモ:** 代替の場所にリストアするには、このオプションを選択する必要があります。
MAC アドレスの保持 (Retain MAC address)	バックアップ中に VM に設定された MAC アドレスを保持します。

8 ［次へ (Next)］をクリックして、［リカバリの概要 (Recovery overview)］を実行します。

これにより、リカバリターゲットとリカバリオプションのページで指定された値に対してリカバリ前チェックが実行されます。AHV クラスタとストレージコンテナの接続状態と存在が確認されます。ストレージコンテナに利用可能な領域があるかどうかが判断され、その他の要件が確認されます。

p.102 の「Nutanix AHV のリカバリ前チェック」を参照してください。

9 ［リカバリの開始 (Start recovery)］をクリックします。

10 ジョブの進捗を監視するには、［リストアアクティビティ (Restore activity)］タブをクリックします。特定のジョブを選択すると、その詳細が表示されます。

VPC 内の AHV VM のリカバリ

VPC での VM のリカバリには、次の制限事項があります。

- 代替リストアで［ネットワークインターフェースの削除 (Remove network interfaces)］チェックボックスにチェックマークが付いている場合、リストア操作は成功します。ただし、プロジェクト、カテゴリ、所有者情報、VPC 関連情報などの属性はリストアされません。
- バックアップがトリガされたときに VM にネットワークが構成されていた場合に、ユーザーが［ネットワークインターフェースの削除 (Remove network interfaces)］チェックボックスにチェックマークを付けずにこのバックアップイメージの代替リストアを試みると、リストア操作は失敗します。
- バックアップがトリガされたときに VM でプロジェクトが構成されていても、リストアがトリガされたときにプロジェクトが存在しなかった場合、リストアジョブは失敗します。
- バックアップがトリガされたときに VM でカテゴリが構成されていても、リストアがトリガされたときにカテゴリが存在しなかった場合、リストアジョブは失敗します。
- リストア時に VM のユーザーが Nutanix Prism Central サーバーまたはプロジェクトに存在しない場合、リストア操作は失敗します。

- リストアでは、ASSIGNED タイプの IP アドレスのみが考慮されます。学習した IP のタイプは無視され、ユーザーはリストア後に IP を手動で構成する必要があります。
- VM にスパンポートが有効になっている NIC がある場合、これはリストア後に無視されます。Nutanix CLI を使用して NIC にスパンを手動で追加して構成する必要があります。
- 元の場所のリストアが実行されている場合、VM はプロジェクト、カテゴリ、所有者の詳細、その他の VPC 関連の属性を使用してリストアされます。
- Prism Central から別の Prism Central に移動されたクラスタの VM をバックアップまたはリストアしようとすると、未定義の動作が発生します。
- プロジェクト、カテゴリ、その他の VPC (仮想プライベートクラウド) 関連の属性をバックアップまたはリストアするには、バージョン 10.2 以降のバックアップホストが必要です。バージョン 10.2 未満のバックアップホストを使用すると、VM が VPC 環境に存在しない場合、VPC 関連の属性をキャプチャせずにバックアップまたはリストアが完了します。VM が VPC 環境に存在し、バージョンが 10.2 未満のバックアップホストを介してリストアがトリガされると、リストアが失敗することがあります。

vTPM 対応 AHV VM のリカバリ

NetBackup では、vTPM 対応 AHV VM の vTPM 構成をリカバリできます。

Prism Central および Prism クラスタのクレデンシャルを構成する必要があります。

p.32 の「新しい Nutanix Prism Central の追加」を参照してください。

p.52 の「AHV クラスタのクレデンシャルの管理」を参照してください。

vTPM 対応 VM をリカバリするには、次のセクションを参照してください。

p.78 の「AHV 仮想マシンのリカバリ」を参照してください。

制限事項

- vTPM に格納されている情報のリストアは Nutanix でサポートされません。
- vTPM は、Q35 以外のマシン形式の Nutanix VM ではサポートされません。
- インスタントアクセス VM のリストアでは、vTPM 構成のリストアはサポートされません。

Nutanix AHV のファイルとフォルダのエージェントレスリストアについて

NetBackup 9.1 以降では、Nutanix AHV のファイルとフォルダのエージェントレスリストアをサポートしています。個々のファイルまたはフォルダを任意のターゲットホストにリストアできます。ターゲットホストには、AHV または他の Hypervisor でホストされる仮想マシ

ンのほか、NetBackup クライアントがインストールされていない物理マシンも指定できます。このリストアでは、一致するターゲットホストプラットフォームの VxUpdate パッケージを使用し、ターゲットホストに NetBackup リカバリツールを配備します。ファイルとフォルダのエージェントレスリストアでは、リストア処理の完了後に、リカバリツールとステージング場所のクリーンアップを実行します。リカバリ処理では、ターゲットホストとネットワークで接続しているリカバリホストとして NetBackup ホストを使用します。このリカバリホストは、NetBackup サーバーまたはクライアントのいずれかです。

ファイルとフォルダのリストア処理の概要

1. NetBackup プライマリサーバーで NetBackup Web UI または Agentless Recovery API から入力を受け取ります。入力は、リストアするファイルまたはフォルダと、ターゲットホストのクレデンシャルです。必要なクレデンシャルは次のとおりです。
   - Windows の場合: UAC が無効な場合、ユーザーはローカル管理者グループに属する必要があります。UAC が有効な場合、ユーザーはドメインユーザーで、ローカル管理者のグループに追加されている必要があります。
   - Linux の場合: ユーザーは、すべての権限を持つルートユーザーまたは sudoer ユーザーである必要があります。
2. 要求されたデータがプライマリサーバーからリカバリホストに送信されます。
3. リカバリホストで、リストアを実行するために必要な VxUpdate リカバリパッケージがリカバリホストにあることが確認されます。必要なパッケージがない場合、リカバリホストは VxUpdate を使用するプライマリサーバーからパッケージをダウンロードします。
4. リカバリホストが、VxUpdate パッケージのリカバリツールをターゲットホストにコピーします。Linux のリカバリホストとターゲットホストは、リカバリ操作に SSH プロトコルを使用します。Windows のリカバリホストとターゲットホストは、リカバリ操作に WMI、SMB プロトコルを使用します。
5. リストアされるファイルまたはフォルダを含むデータストリームファイルが、リカバリホストのステージング場所でステージングされます。
6. リカバリホストのステージング場所で作成されたファイルが、ターゲットホストのステージング場所にコピーされます。
7. リカバリツールが呼び出され、選択されたファイルまたはフォルダが ACL およびメタデータの詳細とともにリカバリされます。
8. リストア操作が成功したかどうかにかかわらず、NetBackup が必要なクリーンアップを実行します。ターゲットホストとリカバリホストのステージング場所に格納されている一時ファイルはすべて削除されます。ただしエラーが発生した場合、デフォルトの構成でターゲットホストからリカバリホストまでの収集により証拠が収集されます。
9. NetBackup は、ファイルのエージェントレスリストアに使用するターゲットホストのゲストオペレーティングシステムとして、次のプラットフォームをサポートします。
   - Windows

- Red Hat Enterprise Linux (RHEL)
- SUSE Linux (SLES)
- Ubuntu

ターゲットホストのオペレーティングシステムのバージョンのサポートについては、「NetBackup ソフトウェア互換性リスト - 8.1 以降」の「NetBackup クライアント」のセクションを参照してください。

ファイルとフォルダのエージェントレスリカバリの前提条件

ファイルまたはフォルダのリカバリは、ソース AHV VM が RedHat Linux、SuSE Linux、Ubuntu、Windows などの指定されたオペレーティングシステムで実行されている場合にのみ実行できます。また、ファイルシステムには、VM のエージェントレス完全バックアップからファイルシステムマッピングを作成するための互換性が必要です。AHV の互換性について詳しくは、『仮想環境での NetBackup のサポート (Support for NetBackup in Virtual Environments)』を参照してください。

メモ: サポートされていない OS の個々のファイルとフォルダのリストアのサポートが必要な場合は、このような VM を NetBackup の Standard ポリシー形式で保護します。

表 7-1 ファイルとフォルダのリカバリの前提条件

手順の概要	説明と参照
エージェントベースのリストア	■ エージェントベースのリストアは、ターゲットホストに NetBackup クライアントまたはサーバーがインストールされている場合に実行されます。 ■ このようなクライアントまたはサーバーの NetBackup バージョンは、Windows の場合は 8.1 以降、Linux の場合は 8.2 以降である必要があります。 **メモ:** Linux バージョン 8.1 以前を選択すると、エージェントレスリストアのオプションが表示されます。 ■ エージェントベースのリストアに使用するターゲットホストで、NetBackup の構成済みのホスト名を指定する必要があります。 ■ ログオンしている NetBackup ユーザーに十分な権限がある場合は、NetBackup ホストのリストを参照して、ファイルまたはフォルダのリストア用のホストを選択できます。ログオンユーザーに十分な RBAC 権限がない場合は、ターゲットホストを手動で指定する必要があります。 ■ エージェントベースのリストアに使用するターゲットホストで、NetBackup の構成済みのホスト名または IP を指定する必要があります。 ソース AHV VM を Linux プラットフォームで実行している場合は、サポート対象の Linux プラットフォームのターゲットホストにファイルまたはフォルダをリストアできます。 **メモ:** NetBackup がターゲットホストからアンインストールされてもエージェントベースのリストアを開始できますが、失敗します。
エージェントレスリストア	エージェントレスリストアは、ターゲットホストに NetBackup クライアントまたはサーバーがインストールされていない場合に実行されます。 ■ ターゲットホストの FQDN または IP アドレスを指定する必要があります。 ■ NetBackup によって、NetBackup の構成からホストが NetBackup 以外のマシンかどうかが検出され、エージェントレスリストアのオプションが表示されます。 **メモ:** IPv4 と IPv6 の両方の IP アドレスがサポートされます。IPv6 では、標準 CIDR 形式はサポートされません。

手順の概要	説明と参照
ターゲットホスト	■ ターゲットホストは、AHV VM バックアップからのファイルまたはフォルダのリストア先となるホストです。ホスト名は FQDN 形式または IP アドレスである必要があります。 ■ AHV、他の Hypervisor、または物理ホストに配備された任意のターゲットホストに、ファイルまたはフォルダをリストアできます。 **メモ:** ターゲットホストにリカバリホストからアクセスできることを確認します。 ■ ソースとターゲットホストのプラットフォームは同種である必要があります。Windows ソースのホストファイルは Windows ターゲットホストに、Linux ソース VM ファイルは Linux ターゲットホストにリストアできます。 ■ ターゲットホストにあるデフォルトのターゲットホストステージングディレクトリは、ユーザーのホームディレクトリです。カスタムのステージング場所を指定できます。 前提条件: ■ NetBackup は、ターゲットホストのステージング場所を作成しません。この場所には、書き込みおよび実行権限がすでに付与されている必要があります。 ■ ターゲットホストのステージング場所には、リストア操作のために十分な領域が必要です。これにはリストアファイルサイズ、NetBackup リストアパッケージ (Windows の場合は最大 150 MB、Linux の場合は最大 100 MB)、NetBackup 操作ログ用の領域が含まれます。 **メモ:** ステージング場所のパスがシステムドライブにある場合、そのパスには他の実行中のプロセスで必要になる十分な領域が必要です。

手順の概要	説明と参照
Linux ターゲットホスト	■ エージェントレスターゲットマシンは、サポート対象の OS プラットフォームで実行されている必要があります。AHV の互換性について詳しくは、『仮想環境での NetBackup のサポート (Support for NetBackup in Virtual Environments)』を参照してください。 ■ ターゲットホストのデフォルトパスに tar ユーティリティが存在し、システムパス変数にパスが追加されている必要があります。 ■ NetBackup は ASCII 形式のホスト名のみをサポートします。ホスト名が非 ASCII 形式である場合、ターゲットホストとして IP アドレスを使用できます。 ■ ターゲットホストへの SSH 接続の最大数を設定できます。デフォルト値は 10 です。 ■ リカバリホストとターゲットホスト間で SSH ポートを開く必要があります。ファイアウォールが構成されている場合は、ファイアウォールの例外リストに SSH ポートが含まれている必要があります。 ■ ターゲットホストのネットワークパスにリストアするには、正しいエクスポート権限を指定します。例: `rw,sync,no_root_squash`

手順の概要	説明と参照
SSH 接続の要件	■ Linux ターゲットホストへのエージェントレスリストアは、SSH サービスを使用して実行されます。これは、ターゲットホストで実行されている必要があります。 ■ ターゲットホストでの SSH 通信タイムアウトは 5 分より長くする必要があります。 ■ SSH を使用してターゲットホストと通信する際に、NetBackup は暗号 `aes256-ctr` を使用します。 ■ SSH バージョンは 1.2 以降である必要があります。 ■ カスタム SSH ポートがサポートされます。 **メモ:** デフォルトの SSH ポートは 22 です。 ■ 以下がサポートされます。 ■ キー交換アルゴリズム: ■ `diffie_helman_group_exchange_sha256` ■ `ecdh_sha2_nistp256` ■ `cdh_sha2_nistp384` ■ `ecdh_sha2_nistp521` ■ `diffie_helman_group14_sha1` ■ ホストキー ■ `ssh-rsa` ■ `ssh-dss` ■ `ecdsa-sha2-nistp256` ■ `ecdsa-sha2-nistp384` ■ `ecdsa-sha2-nistp521` ■ ハッシュメソッド ■ `sha256 Hex encoded`

手順の概要	説明と参照
sudo ユーザーのリストア	■ sudo ユーザーは Linux ターゲットホストにすでに存在している必要があります。 ■ ルート以外のユーザーが sudoers ファイルですでに構成されていることを確認します。 例: ■ `<sudo-username> ALL = (ALL)` ■ `<sudo-username> ALL = (ALL) NOPASSWD` ■ sudoers ファイルには、非ルートユーザー用に構成されたエントリが 1 つ必要です。 ■ Linux sudo ユーザーには、カスタムのステージング場所の読み取り、書き込み、実行権限とともに所有権が必要です。 パスワードの代わりに SSH 秘密鍵を使用できます。 p.94 の「SSH 鍵指紋」を参照してください。

手順の概要	説明と参照
Windows ターゲットホスト	

手順の概要	説明と参照
	■ エージェントレスターゲットマシンは、サポート対象の OS プラットフォームで実行されている必要があります。AHV の互換性について詳しくは、『仮想環境での NetBackup のサポート (Support for NetBackup in Virtual Environments)』を参照してください。 ■ WMI が構成され、リカバリホストとターゲットホスト間でアクセスできる必要があります。WMI と SMB の要件については、https://www.veritas.com/support/ja_JP/article.100040135 を参照してください。 ■ ASCII 形式のホスト名が受け入れられます。ホスト名が Unicode である場合は、ホスト名の代わりに IP アドレスを使用します。 ■ 次のサービスが Windows ホストで実行されている必要があります。 ■ DCOM ■ RPC ■ WMI ■ ファイルとプリンタの共有 ■ デフォルトでは、[管理共有 (Admin share)]はホストで有効になっています。無効になっている場合、GPO で、ステージング場所のドライブまたはステージング場所が存在するドライブで管理共有を有効にする必要があります。 **メモ:** デフォルトで、管理者ユーザーには WMI と DCOM のアクセスに必要な権限が付与されています。DCOM と WMI の権限で問題が発生した場合は、Microsoft のマニュアルを参照してください。 ■ DCOM と WMI の権限の割り当てに使用されるユーザーまたはグループ: DCOM および WMI 権限を割り当てる 2 つの方法のうち、次のいずれかのオプションを使用します。 ■ ユーザーは管理者グループに属している必要があるので、管理者グループに権限を割り当てられます。 ■ 特定のユーザーに権限を割り当てます。 ■ UAC 環境と非 UAC 環境のサポート: ■ ターゲットホストのローカル管理者グループに追加された管理者とドメインユーザーには、エージェントレスリストアを実行するために必要な権限があります。 **メモ:** UAC リモート制限: 管理者グループのロー

手順の概要	説明と参照
	カルユーザーの場合は、エージェントベースリストアの使用をお勧めします。ただし、UAC フィルタリングを無効にしても、エージェントレスリストアを実行できます。 UAC リモート制限を無効にするには、こちらを参照してください。 ■ ステージング場所の要件: ■ デフォルトの場所はユーザーのホームディレクトリです。カスタムパスを指定する場合、ユーザーはそこにアクセスできる必要があります。 ■ 絶対パスを指定する必要があります。 **メモ:** ソフトリンク、ハードリンク、ネットワークパスなどはサポートされていません。 ■ 次の領域を含む、リストア操作用の十分な領域が必要です。 ■ リストアファイルのサイズ ■ NetBackup リストアパッケージ (最大 150 MB) ■ NetBackup の操作ログの領域。詳細レベルに応じて、ログ要件は異なります。 **メモ:** このパスがシステムドライブ上にある場合、そのパスには他の実行中のプロセスで必要になる十分な領域が必要です。 ■ パスの文字数の上限は 260 です。ただし、NetBackup で一時的な場所を形成するために約 110 文字が必要です。そのため、150 文字未満のパスを指定する必要があります。 ■ ステージング場所とリストア場所が同じドライブ上にある場合、リストアサイズの 2 倍の領域が必要になることがあります。 ■ 同じユーザーによる並列リストアジョブがサポートされています。ただし、同じ宛先フォルダが指定された場合、リストアされたデータが不整合状態である可能性があります。

手順の概要	説明と参照
WMI と SMB の要件	■ Windows ターゲットホストへのエージェントレスリストアでは、WMI (Windows Management Instrumentation) プロトコルと SMB (サーバーメッセージブロック) プロトコルを使用します。 ■ ファイアウォールの設定で、WMI ポートと SMB ポートが開かれていることを確認します。 ■ デフォルトの DCOM ポート 135 ■ デフォルトの SMB ポート 445 ■ 動的ポート 49152-65535 **メモ:** また、環境で静的固定ポートを使用できます。 ■ SMB 暗号化を有効にして、SMB を使用したデータ転送を暗号化します。詳しくは、Microsoft 社のマニュアルを参照してください。 ■ SMB バージョン 3.0 をサポートしています。ホストに古いバージョンがある場合は、それを無効にできます。Microsoft 社のガイドラインを参照してください。

手順の概要	説明と参照
リカバリホスト	リカバリホストは、NetBackup メディアサーバーまたはクライアントがインストールされたホストであり、指定されたターゲットホストとの通信に使用されます。 ■ リカバリホストの NetBackup バージョンは 9.1 以降で、ターゲットホストと接続できる必要があります。 ■ Linux リカバリホストは Linux ターゲットホストへの SSH 接続が可能で、Windows リカバリホストは Windows ターゲットホストとの WMI および SMB 接続が可能である必要があります。 ■ リカバリホストは同種のプラットフォームである必要があります。Windows AHV VM からターゲット Windows ホストにファイルをリストアするには、Windows リカバリホストが必要です。同様に、Linux AHV VM からターゲット Linux ホストにファイルをリストアするには、Linux リカバリホストが必要です。 **メモ:** Ubuntu のターゲットホストにファイルをリストアするには、リカバリホストとして RHEL または SUSE を使用します。 ■ NetBackup 9.1 サーバーまたはクライアントがインストールされたリカバリホストのみがサポートされます。 ■ エクスポート権限が正しい場合、リカバリホストのステージング場所としてネットワークパスが機能します。例: `rw,sync,no_root_squash` ■ リカバリホストのデフォルトのステージング場所は次のとおりです。 ■ Linux の場合: `/{install-path}/openv/var/tmp/staging` ■ Windows の場合: `{install-path}¥NetBackup¥Temp¥staging` ■ デフォルトのステージング場所は、bpsetconfig を使用して変更できます。 ■ <NetBackup path>/bin/admincmd/bpsetconfig を実行します。 ■ AGENTLESS_RHOST_STAGING_PATH = <Path> を設定します。

手順の概要	説明と参照
その他	■ SUSE ターゲットホストは「/etc/ssh/sshd_config」ファイルに「PasswordAuthentication」が「Yes」のエントリが必要です。その後、「ssh」サービスを再起動します。 **メモ:** デフォルトでは、SUSE ターゲットホストの passwordAuthentication 値は No に設定されています。

SSH 鍵指紋

Linux ターゲットホストの SSH キー指紋を取得するには:

1 RHEL または SUSE OS のターゲットホストで次のコマンドを使用し、SHA256-based RSA キーを取得します。

```
cat /etc/ssh/ssh_host_rsa_key.pub |awk '{print $2}' |base64 -d |sha256sum |
awk '{print $1}'
```

メモ: コマンドの出力は RSA 鍵です。同様に、公開鍵のパスを変更し、このコマンドを実行して、ターゲットホストで構成されている ecdsa または DSS SSH 鍵指紋を取得します。

- RSA 鍵の例:

```
cat /etc/ssh/ssh_host_rsa_key.pub |awk '{print $2}'|base64 -d
 |
sha256sum |awk '{print $1}'
```

- コマンドの出力:

```
b2352722053ac9f40bc1XXXXXXXXXXXXXXXXXXXXXXXXXX419fa241ba9431fd6b9
```

2 RSA 指紋をコピーします。ターゲットホストの詳細を追加するときに、この SSH 鍵指紋を指定できます。または、[リカバリホスト (Recovery Host)]ページで[SSH 鍵指紋をフェッチ (Fetch SSH Key fingerprint)]をクリックした後、表示された SSH 鍵指紋を確認することもできます。

SSH 秘密鍵を生成するには:

1 Linux ターゲットホストで次のコマンドを実行します。

- ssh-keygen -t rsa

- `-t option supports "ecdsa | rsa | dss"`

2 ターゲット `vm ~/.ssh/authorized_keys` ファイルに、ターゲットホストの公開鍵を追加する必要があります。

Nutanix AHV エージェントレスリストアによるファイルとフォルダのリカバリ

Nutanix AHV エージェントレスリストアでファイルとフォルダをリカバリするには

1 ターゲットホストの電源がオンで、リストア処理で使用するリカバリホストへのネットワーク接続が確立されていることを確認します。

2 左側で[作業負荷 (Workloads)]、[Nutanix AHV]の順に選択します。

3 リストアするファイルとフォルダが含まれている AHV VM を特定して選択します。

この VM は、ソース VM とも呼ばれます。

4 [リカバリポイント (Recovery points)]タブをクリックします。カレンダービューで、バックアップが発生した日付を選択します。

5 利用可能なイメージが、それぞれのバックアップタイムスタンプと一緒に一覧表示されます。

6 リカバリするイメージで、[リカバリ (Recover)]、[ファイルとフォルダをリストアする (Restore files and folders)]をクリックします。

7 [ファイルを選択する (Select files)]ペインで、リカバリするファイルとフォルダを指定し、[次へ (Next)]をクリックします。これらのファイルまたはフォルダは、ソースファイルまたはソースフォルダとも呼ばれます。

8 [次へ (Next)]をクリックします。

9 [リカバリターゲット (Recovery target)]ページで、次の操作を行います。

- IP/ホスト名を手動で入力します。
- 必要に応じて、ターゲットホストのステージング場所を入力します。
- 適切なファイルリストアオプションを選択します。
- 適切なリカバリホストを選択します。
- OS の種類に基づいて正しいクレデンシャルを追加します。

p.97 の「リカバリターゲットのオプション」を参照してください。

10 [リカバリオプション (Recovery options)]ページで、次のいずれかを選択します。

- ［ファイル名に文字列を追加 (Append string to file names)］: 宛先ファイル名のファイル拡張子の前に指定した文字列を追加します。この値はファイルにのみ適用されます。
- ［既存のファイルの上書き (Overwrite existing files)］: ファイルまたはフォルダが宛先の場所に同じ名前で存在する場合は上書きします。
- ［クロスマウントポイントなしで、ディレクトリをリストア (Restore directories without crossing mount points)］
- ［ハードリンクの新しいファイルを作成 (Create new files for hard links)］
- ［ソフトリンクのターゲット名を変更 (Rename targets for soft links)］

メモ: ［ハードリンクの新しいファイルを作成 (Create new files for hard links)］および［ソフトリンクのターゲット名を変更 (Rename targets for soft links)］オプションは、すべてを異なるディレクトリにリストアする場合にのみ有効になります。

11 ［次へ (Next)］をクリックします。

12 ［確認 (Review)］ページ: ［確認 (Review)］ページにリカバリ前チェックの状態が表示されます。NetBackup はリカバリ前の検証を実行し、指定された入力を使用してリストアジョブが正常に実行されるかどうかを確認します。

p.102 の「Nutanix AHV のリカバリ前チェック」を参照してください。

- リカバリ前チェックでエラーが発生した場合は、考えられるエラーの原因が表示されます。修正する必要がある特定の入力の［変更 (Change)］ボタンをクリックします。
- リカバリ前チェックが正常に完了した場合は、［リカバリの開始 (Start recovery)］をクリックします。

リカバリターゲットのオプション

表 7-2 リカバリターゲットのオプション

手順の概要	説明と参照
ターゲットホスト (Target Host)	■ [ターゲットホスト (Target Host)]フィールドには、VM の各 AHV クラスタに対する前回成功した検出中に保存された、ソース AHV VM のホスト名または IP が事前に入力されます。 **警告:** NetBackup クライアントがインストールされ、指定されたホスト名または IP を使用して構成されている場合は、エージェントベースのリストアが実行されます。 ■ 別の NetBackup クライアントでリストアを実行する場合は、[検索 (Search)]をクリックし、リストから必要なクライアントを選択します。 **メモ:** 同種のプラットフォームを使用しているクライアントを選択してください。 ■ [検索 (Search)]オプションが利用できない場合は、手動でターゲットホストを入力します。 ■ NetBackup クライアントがインストールされていないホストでリストアを実行する場合は、ホストの FQDN または IP をターゲットホストに入力します。[エージェントレスリストア (Agentless restore)]オプションが表示されます。

手順の概要	説明と参照
［エージェントレスリストア (Agentless restore)］オプション	■ ［ターゲットホスト上のステージング場所の変更 (Change staging location on target host)］: デフォルトのステージング場所とは異なるステージング場所を指定する場合は、目的のパスを入力します。ステージング場所のパスには ASCII 文字のみを使用できます。 **メモ:** デフォルトのステージング場所はユーザーのホームディレクトリです。 ■ ファイルリストアのオプション (File restore options): 要件に基づいて、次の適切なファイルリストアオプションのいずれかを選択します。 ■ すべてを元のディレクトリにリストア (Restore everything to the original directory) ■ ［すべてを異なるディレクトリにリストア (Restore everything to different directory)］ リストアする別のディレクトリパスを指定します。 ■ ［既存のディレクトリ構造をフラット化 (Flatten existing directory structure)］ さまざまなディレクトリにあるファイルを選択した場合に、サブフォルダを作成せずにすべてを単一のディレクトリにリストアするには、このオプションを選択します。

手順の概要	説明と参照
リカバリホスト (Recovery Host)	■ [リカバリホスト (Recovery Host)]フィールドには、選択した AHV VM のバックアップ操作時に使用されたバックアップホストがあらかじめ入力されています。 **メモ:** 選択した VM とバックアップホストのプラットフォームが同種ではない場合、[リカバリホスト (Recovery host)]フィールドは空になります。 **メモ:** Ubuntu のターゲットホストにファイルをリストアするには、リカバリホストとして RHEL または SUSE を使用します。 ■ [検索 (Search)]をクリックして、別のリカバリホストを選択します。互換性のあるメディアサーバーのリストが表示されます。リカバリホストとして NetBackup クライアントを選択する場合は、[メディアサーバー (Media servers)]、[クライアント (Clients)]の順に選択します。 ■ [検索 (Search)]オプションが利用できない場合は、手動でリカバリホストを入力します。 **メモ:** リカバリホストはソース VM と同種のプラットフォームで、NetBackup 9.1 以降のサーバーまたはクライアントがインストールされている必要があります。 ■ 拡張性のある柔軟な環境では、すべてのメディアサーバーが[メディアサーバー (media server)]タブに表示されない場合、ユーザーは、メディアサーバーに対する表示権限が必要となるか、手動でメディアサーバーを入力して続行できます。 ■ 以前に同じターゲットホストでリストアを実行したことがある場合、このリストアを実行するユーザーに付与された割り当て済みの権限に基づいて、リカバリホストには以前に使用したリカバリホストがあらかじめ入力されています。

手順の概要	説明と参照
Linux SSH 接続 (Linux SSH Connectivity)	

手順の概要	説明と参照
	選択したソース Linux VM の SSH 接続では、次のオプションが表示されます。 ■ ［ターゲットホストの SSH ポート (Target host SSH port)］ターゲットホストの SSH ポートを指定します。デフォルト値は 22 です。 以前に同じターゲットホストでリストアを実行したことがある場合、このリストアを実行するユーザーが事前に割り当てた権限に基づいて、SSH ポートには以前に使用した値があらかじめ入力されています。 ■ ［ターゲットホストの SSH 鍵指紋 (Target host SSH key fingerprint)］ターゲットホストを認証するため、16 進形式で SSH 鍵指紋を指定します。 ■ ターゲットホストの SSH 鍵指紋を手動で入力するか、［SSH 鍵指紋をフェッチ (Fetch SSH Key fingerprint)］をクリックします。 ■ ［SSH 鍵指紋をフェッチ (Fetch SSH Key fingerprint)］: ［SSH 鍵指紋をフェッチ (Fetch SSH Key fingerprint)］オプションが利用できない場合は、SSH 鍵指紋を手動で指定する必要があります。p.94 の「SSH 鍵指紋」を参照してください。 ■ 以前に同じターゲットホストでリストアを実行したことがある場合、このリストアを実行するユーザーが事前に割り当てた権限に基づいて、SSH 鍵指紋には以前に使用した値があらかじめ入力されています。あらかじめ入力された値を上書きして、信頼を再確立できます。 ■ SSH 鍵指紋をフェッチ (Fetch SSH Key fingerprint) ■ NetBackup でサポートされるキータイプとともに、ターゲットホストで構成されている SSH 鍵指紋のリストを表示します。 ■ 一覧表示された指紋の 1 つを選択し、［OK］をクリックします。選択された指紋を使用して、NetBackup はターゲットホストとの信頼を確立します。 ■ ターゲットホストのクレデンシャル (Target host credentials) ■ ［ユーザー名 (User name)］ターゲットホストのユーザー名を指定します。このユーザーは、root か root 以外の sudoer である必要があります。 ［sudoer ユーザー (Sudoer user)］p.83 の「ファイルとフォルダのエージェントレスリカバリの前提条件」を参照してください。 ■ ［パスワードを入力 (Provide password)］パスワードベースの認証を選択するには、このオプションを

手順の概要	説明と参照
	選択します。 ■ ［パスワード (password)］指定したユーザーのターゲットホストのパスワードを指定します。 ■ ［SSH 秘密鍵を入力 (Provide SSH private key)］SSH 秘密鍵ベースの認証を選択するには、このオプションを選択します。p.94 の「SSH 鍵指紋」を参照してください。 ■ ［SSH 秘密鍵 (SSH private key)］SSH 秘密鍵を指定します。 ■ ［キーのパスフレーズ (Key passphrase)］パスフレーズを使用して SSH の秘密鍵が作成されている場合は、キーのパスフレーズを指定します。
Windows WMI 接続 (Windows WMI Connectivity)	■ ［ユーザー名 (User name)］ターゲットホストのユーザー名を指定します。このユーザーはドメインユーザーまたはローカルユーザーで、ローカル管理者グループに属している必要があります。ユーザー名では「localusername」または「domain¥username」の形式がサポートされます。 ■ ［パスワード (password)］指定したユーザーのターゲットホストのパスワードを指定します。

Nutanix AHV のリカバリ前チェック

表 7-3　Nutanix AHV のリカバリ前チェック

検証	説明と参照	入力ソース
リカバリホストの領域	リカバリホストのステージング場所に必要な領域を確認します。	リカバリホスト
ターゲットホストの接続	ターゲットホストにリカバリホストからアクセスできるかどうかを確認します。	ターゲットホストとターゲットホストのポート
ターゲットホストのクレデンシャル	指定されたターゲットホストのクレデンシャルが有効かどうかを確認します。	ターゲットホストのクレデンシャル
ローカルディスク上のターゲットホストのステージング場所	ターゲットホストのステージング場所がネットワークパスではないことを確認します。	ターゲットホストのステージング場所

検証	説明と参照	入力ソース
ターゲットホストのステージング場所の領域	ターゲットホストのステージング場所で必要な領域を利用できるかどうかを確認します。 **メモ:** 必要な領域は、選択したファイルのサイズと、NetBackup リストアパッケージ、ログやその他のファイルに必要な領域の合計です。	ターゲットホストのステージング場所
ターゲットホストのステージング場所の権限	指定したユーザーが所有者で、ターゲットホストのステージング場所に対する RBAC 権限が付与されているかどうかを確認します。	ターゲットホストのステージング場所
ターゲットホストのデフォルトのステージング場所のパス	ターゲットホストのステージング場所のパスに有効な文字が含まれているかどうかを確認します。NetBackup は、ターゲットホストのステージング場所のパスで非 ASCII 文字をサポートしていません。	ターゲットホストのステージング場所
ターゲットホストのオペレーティングシステム	ターゲットホストにサポート対象の OS がインストールされているかどうかを確認します。	全般
VxUpdate パッケージ	必要な VxUpdate パッケージがプライマリサーバーで利用可能かどうかを確認します。	全般
Linux ターゲットホスト固有のチェック		
ターゲットホストの SSH 鍵指紋	リカバリホストからターゲットホストとの信頼を確立するためのターゲットホストの SSH 鍵指紋が有効かどうかを確認します。	ターゲットホストの SSH 鍵指紋
ターゲットホスト上に tar が存在する	ターゲットホストで `tar` が利用可能かどうかを確認します。	ターゲットホスト

Nutanix-AHV のファイルとフォルダのエージェントベースリストアについて

NetBackup 9.1 以降では、個々のファイルとフォルダを対象にした、Nutanix-AHV のファイルとフォルダのエージェントベースリストアをサポートしています。エージェントベースのリストアでは、NetBackup クライアントを備えるホストに Nutanix-AHV の個々のファイルをリストアできます。エージェントベースのターゲットホストには、AHV または他の Hypervisor でホストされる仮想マシンのほか、NetBackup クライアントがインストールされた物理マシンも指定できます。

ファイルとフォルダのエージェントベースリカバリの前提条件

- ソース AHV VM バックアップイメージから個々のファイルとフォルダのリカバリを実行できます。ファイルシステムマッピングを作成するため、ゲストオペレーティングシステムとファイルシステムには互換性が必要です。
  ゲストオペレーティングシステムおよびファイルシステムにおける個々のファイルのリストアのサポートについては、Nutanix AHV の SCL (ソフトウェア互換性リスト) を参照してください。
  仮想環境での NetBackup <バージョン> のサポート (Support for NetBackup <versions> in virtual environments)
- ソース AHV VM バックアップから個々のファイルのリカバリを実行できます。NetBackup プライマリサーバー、メディアサーバー、バックアップホストが NetBackup バージョン 9.1 以降である必要があります。
- エージェントベースのリストアは、ターゲットホストに NetBackup クライアントまたはサーバーがインストールされている場合に実行されます。クライアントまたはターゲットホストの NetBackup は 8.1 以降 (Windows) または 8.2 以降 (Linux) である必要があります。

  メモ: Linux バージョン 8.1 以前を選択すると、エージェントレスリストアのオプションが表示されます。

  エージェントベースのリストアを実行するには、ターゲットホストで NetBackup の構成済みのホスト名または IP を指定する必要があります。
- NetBackup ホストを表示するために必要な RBAC 権限を持つユーザーは、ファイルまたはフォルダのリストア用の NetBackup ホストを参照して選択できます。
  必要な RBAC 権限を持たないユーザーは、ターゲットホストに NetBackup で構成されているホスト名または IP を手動で指定する必要があります。

- ファイルとフォルダのエージェントベースリストアを行うために、ユーザーに必要な最小限の RBAC 権限を次に示します。

表 7-4　すべての AHV 資産の権限

操作	説明	その他の必要な操作	追加のオプション操作
個別リストア	AHV 資産から個々のファイルまたはフォルダをリストアします。 この権限は、ソース VM に必要です。	[グローバル (Global)]、[NetBackup の管理 (NetBackup management)]、[NetBackup のバックアップイメージ (NetBackup backup images)]、[表示 (View)] [グローバル (Global)]、[NetBackup の管理 (NetBackup management)]、[NetBackup のバックアップイメージ (NetBackup backup images)]、[内容の表示 (View contents)] [NetBackup の管理 (NetBackup management)]、[NetBackup ホスト (NetBackup hosts)]、[表示 (View)] [資産 (Assets)]、[資産 (Assets)]、[クライアントを使用したファイルのリストア (Restore files using client)]	[資産 (Assets)]、[資産 (Assets)]、[ファイルとフォルダを上書きする (Overwrite files and folders)]

表 7-5 すべての AHV 資産の権限

操作	説明	その他の必要な操作	追加のオプション操作
個別リストア	AHV 資産から個々のファイルまたはフォルダをリストアします。 この権限は、ソース VM に必要です。	[グローバル (Global)]、[NetBackup の管理 (NetBackup management)]、[NetBackup のバックアップイメージ (NetBackup backup images)]、[表示 (View)] [グローバル (Global)]、[NetBackup の管理 (NetBackup management)]、[NetBackup のバックアップイメージ (NetBackup backup images)]、[内容の表示 (View contents)] [NetBackup の管理 (NetBackup management)]、[NetBackup ホスト (NetBackup hosts)]、[表示 (View)] [資産 (Assets)]、[資産 (Assets)]、[クライアントを使用したファイルのリストア (Restore files using client)]	[資産 (Assets)]、[資産 (Assets)]、[ファイルとフォルダを上書きする (Overwrite files and folders)]

Nutanix AHV エージェントベースのリストアによるファイルとフォルダのリカバリ

Nutanix AHV エージェントベースのリストアを使用してファイルとフォルダをリカバリするには

1. ターゲットホストの電源がオンで、リストア処理で使用するリカバリホストへのネットワーク接続が確立されていることを確認します。
2. 左側で[作業負荷 (Workloads)]、[Nutanix AHV]の順に選択します。
3. リストアするファイルとフォルダが含まれている AHV VM を特定して選択します。

   この VM は、ソース VM とも呼ばれます。
4. [リカバリポイント (Recovery points)]タブをクリックします。カレンダービューで、バックアップが発生した日付を選択します。

   利用可能なイメージが、それぞれのバックアップタイムスタンプと一緒に一覧表示されます。
5. リカバリするイメージで、[リカバリ (Recover)]、[ファイルとフォルダをリストアする (Restore files and folders)]をクリックします。
6. [ファイルを選択する (Select files)]ペインで、リカバリするファイルとフォルダを指定し、[次へ (Next)]をクリックします。これらのファイルまたはフォルダは、ソースファイルまたはソースフォルダとも呼ばれます。
7. [リカバリターゲット (Recovery target)]ページで、次の操作を行います。
   - ターゲットホストを選択します。
     - ターゲットホストは FQDN または IP アドレスで入力する必要があります。ホストを表示する権限がある場合は、検索アイコンをクリックすると、NetBackup クライアントがすでに存在するホストが表示されるため、必要なホストを選択します。

       メモ: ドロップダウンでは、NetBackup バージョン 8.1 以降のみが利用可能です。
   - 適切なファイルリストアオプションを選択します。

   p.97 の「リカバリターゲットのオプション」を参照してください。
8. [リカバリオプション (Recovery options)]ページで、次のいずれかを選択します。
   - [ファイル名に文字列を追加 (Append string to file names)]: 宛先ファイル名のファイル拡張子の前に指定した文字列を追加します。この値はファイルにのみ適用されます。

- ［既存のファイルの上書き (Overwrite existing files)］: ファイルまたはフォルダが宛先の場所に同じ名前で存在する場合は上書きします。
- ［クロスマウントポイントなしで、ディレクトリをリストア (Restore directories without crossing mount points)］
  選択したディレクトリにマウントされているファイルシステムをスキップする場合に選択します。選択したディレクトリにマウントされているファイルシステムをリストアするには、このチェックボックスをオフにします。
- ［ハードリンクの新しいファイルを作成 (Create new files for hard links)］
- ［ソフトリンクのターゲット名を変更 (Rename targets for soft links)］

メモ: ［ハードリンクの新しいファイルを作成 (Create new files for hard links)］および［ソフトリンクのターゲット名を変更 (Rename targets for soft links)］オプションは、すべてを異なるディレクトリにリストアする場合にのみ有効になります。

9 ［次へ (Next)］をクリックします。

10 ［確認 (Review)］ページで、以前に選択したすべてのオプションを確認します。

11 ［リカバリの開始 (Start recovery)］をクリックします。

制限事項

- クロスプラットフォームの個々のファイルのリカバリ操作はサポートされません。Windows ファイルは Windows ゲストオペレーティングシステムのみで、Linux ファイルはサポート対象の Linux ゲストオペレーティングシステムのみにリストアできます。つまり、リカバリホストは、リストアするファイルと同じプラットフォームである必要があります。
- リカバリ処理で、NetBackup によってハードリンクと元のファイル間のリンクが再作成されます。この場合のみ、リンクファイルとそのターゲットファイルは同じジョブでリストアする必要があります。

メモ: 各ファイルが別々のリストアジョブで個別にリストアされると、別々のファイルとしてリストアされ、リンクは再確立されません。

- デュアルブートの仮想マシンの場合、NetBackup は個々のファイルまたはフォルダのリカバリをサポートしません。
- クライアントプラットフォームとファイルシステムのサポートおよび制限事項については、https://www.veritas.com/content/support/en_US/doc/NB_70_80_VE を参照してください。

- [既存のディレクトリ構造をフラット化 (Flatten existing directory structure)]と[ファイル名に文字列を追加 (Append string to file names)]オプションはファイルにのみ適用できます。ディレクトリには適用できません。
- [既存のディレクトリ構造をフラット化 (Flatten existing directory structure)]と[既存のファイルの上書き (Overwrite existing files)]のオプションを選択した場合、同じファイル名のファイルが複数含まれていると正しくリストアされないことがあります。

メモ: リストアが完了すると、最後にリストアされたファイルが利用可能になります。

- [既存のディレクトリ構造をフラット化 (Flatten existing directory structure)]オプションを選択して[既存のファイルの上書き (Overwrite existing files)]を選択しない場合、リストアは成功しますが、最初にリストアされたファイルがリストアの完了時に保持されます。これを防ぐには、同じ名前の複数のファイルをリストアするときに[既存のディレクトリ構造をフラット化 (Flatten existing directory structure)]を選択しないでください。
- 同じ VM でバックアップとリストアを同時に実行すると、一方または両方のジョブが予期しない結果になることがあります。

メモ: ゼロ以外の NetBackup の状態コードでバックアップまたはリストアが終了した場合は、それらのジョブが同じ VM で同時に実行されたことが原因である可能性があります。

- 選択されたリストアデータに `.bashrc`、`.bash_history` などの隠しファイルが含まれている場合、[ファイル名に文字列を追加 (Append string to file names)]リストアオプションはサポートされません。
- Nutanix エージェントレスリストアは、ファイルとフォルダのリストアにのみ使用できます。
- ステージングディレクトリに対する十分な権限が NetBackup に割り当てられていない場合やステージングディレクトリに十分な領域がない場合、リストアジョブは失敗します。

メモ: NetBackup クライアントがターゲット VM にすでに存在する場合、Cohesityでは Nutanix AHV エージェントレスリストアを使用することはお勧めしません。このような場合、NetBackup 管理者はエージェントベースのリストアを使用する必要があります。

- Windows ターゲットホストでは、リストア先としてマッピングされたドライブはサポートされません。

- NetBackup は、openSSH を使用した Windows ターゲットホストとの通信をサポートしていません。このような場合、リストアジョブは失敗します。
- NetBackup は、ターゲットホストのステージング場所のパスで非 ASCII 文字をサポートしていません。
- NetBackup は、Windows ターゲットホストに対して NTLM 認証形式のみをサポートします。
- 9.1 より前のリリースでバックアップされた AHV イメージは、Web UI からリストアできません。これらのイメージをリストアするには、ユーザーは NetBackup 管理コンソールを使用する必要があります。
- バックアップホストに NetBackup バージョン 9.1 以降がインストールされている場合、NetBackup 管理コンソールからバックアップを取得した場合でも、Web UI で AHV バックアップイメージを利用できます。

  Web UI 上のバックアップイメージについて:

  - 資産の検出が正常に完了し、そのバックアップが NetBackup 管理コンソールから取得された後、Web UI でバックアップイメージを利用できます。
  - プライマリサーバーとバックアップホストを 9.1 にアップグレードして、NetBackup 管理コンソールからバックアップを取得した後に Web UI を構成する場合、資産検出を実行してバックアップイメージを表示する必要があります。
  - プライマリサーバーが 9.1 にアップグレードされていても、バックアップホストのバージョンが 9.1 より前の場合、バックアップは NetBackup 管理コンソールから取得されます。その場合、Web UI を構成しても、資産の検出後もバックアップイメージが表示されません。

8

Nutanix クラウドクラスタ (NC2) の保護

この章では以下の項目について説明しています。

AWS の Nutanix Cloud Clusters (NC2) の保護

Nutanix Cloud Clusters (NC2) は Nutanix Cloud Platform の拡張機能で、組織が AWS で Nutanix Cloud Platform ソフトウェアを実行できるようにします。パブリッククラウドのハイパースケール環境でオンプレミスで使用されるコア Nutanix HCI ソフトウェアをレプリケートし、プライベートクラウドとパブリッククラウドの両方で同じ仮想化とソフトウェア定義のメリットを提供します。

AWS の Nutanix Cloud Clusters (NC2) について詳しくは、Nutanix のオンラインマニュアルを参照してください。

Nutanix Cloud Clusters (NC2) 環境では、NetBackup 10.4 以降のバージョンを使用して仮想マシンを保護できます。Nutanix クラスタと Prism Central を Nutanix Cloud Clusters (NC2) 環境に配備すると、オンプレミスの Nutanix クラスタや Prism Central と同様に、NetBackup Web UI 内で構成できます。NetBackup でクラスタが正常に構成されると、仮想マシンが検出されます。その後、AHV 作業負荷用に設計された保護計画を使用して、これらの仮想マシンを保護できます。

メモ: NetBackup は、オンプレミスの Nutanix クラスタの仮想マシンと同様に、Nutanix Cloud Clusters (NC2) 環境の仮想マシンを保護します。NetBackup を使用した Nutanix オンプレミス仮想マシンの保護について詳しくは、『NetBackup™ for Nutanix AHV 管理者ガイド』の「AHV クラスタの管理」の章を参照してください。

Azure の Nutanix Cloud Clusters (NC2) の保護

Nutanix Cloud Clusters (NC2) は Nutanix Cloud Platform の拡張機能で、組織が Microsoft Azure クラウドサービスで Nutanix Cloud Platform ソフトウェアを実行できるようにします。パブリッククラウドのハイパースケール環境でオンプレミスで使用されるコア Nutanix HCI ソフトウェアをレプリケートし、プライベートクラウドとパブリッククラウドの両方で同じ仮想化とソフトウェア定義のメリットを提供します。

Azure の Nutanix Cloud Clusters (NC2) について詳しくは、Nutanix のオンラインマニュアルを参照してください。

Nutanix Cloud Clusters (NC2) 環境では、NetBackup 10.4 以降のバージョンを使用して仮想マシンを保護できます。Nutanix クラスタと Prism Central を Nutanix Cloud Clusters (NC2) 環境に配備すると、オンプレミスの Nutanix クラスタや Prism Central と同様に、NetBackup Web UI 内で構成できます。NetBackup でクラスタが正常に構成されると、仮想マシンが検出されます。その後、AHV 作業負荷用に設計された保護計画を使用して、これらの仮想マシンを保護できます。

メモ: NetBackup は、オンプレミスの Nutanix クラスタの仮想マシンと同様に、Nutanix Cloud Clusters (NC2) 環境の仮想マシンを保護します。

NetBackup を使用した Nutanix オンプレミス仮想マシンの保護について詳しくは、『NetBackup™ for Nutanix AHV 管理者ガイド』の「AHV クラスタの管理」の章を参照してください。

9

AHV の操作のトラブルシューティング

この章では以下の項目について説明しています。

AHV の操作のトラブルシューティング: AHV インスタントアクセス仮想マシンの作成時のエラー

次の表に、AHV インスタントアクセス仮想マシンの作成を試行したときに発生する可能性がある問題を示します。

表 9-1 AHV インスタントアクセス仮想マシンの作成時のエラー

エラーメッセージまたは原因	説明および推奨処置
Failed to create the VM in the Nutanix AHV cluster. Error: Already used VM UUID: <VM UUID>. Return value 114. Failed to create an instant access virtual machine (VM). (4004)	インスタントアクセス VM を作成する前に、システムによって VM UUID が Nutanix クラスタにすでに存在するかどうか確認されます。存在する場合、リカバリは失敗します。 回避方法: 1 リカバリ処理を開始します。 2 [インスタントアクセス仮想マシンの作成 (Create Instant Access Virtual Machine)]を選択します。 3 [リカバリオプション (Recovery Options)]ページで、[既存の VM ID の代わりに新しい VM ID を作成する (Create new VM ID instead of existing one)]を選択します。 4 リカバリを続行し、[リカバリの開始 (Start Recovery)]をクリックします。
Failed to create an instant access virtual machine (VM). Error details Only the Red Hat Enterprise Linux and SUSE Linux Enterprise Server operating systems are supported.	インスタントアクセスは、現在、RHEL と SLES のみをサポートしています。サポートされていないオペレーティングシステムの VM をリカバリしようとすると、リカバリは失敗します。 推奨処置: サポートされていないオペレーティングシステムのメディアサーバーには、従来の完全リストアを使用します。
Failed to create an instant access virtual machine (VM). Specification for create VM cannot be prepared, as RetainMacAddress and RemoveNetworkInterface can't be used together.	RetainMacAddress と RemoveNetworkInterface の両方を同時に使用すると、API 仕様は無効になります。 推奨処置: NIC (ネットワークインターフェースコントローラ) を削除する場合は、MAC アドレスを保持しないでください。MAC アドレスを保持する必要がある場合は、NIC カードを構成したままにする必要があります。

エラーメッセージまたは原因	説明および推奨処置

`Failed to create an instant access virtual machine (VM).`
 	
`Error details`
 	
`Create instant access VM capability for Nutanix is supported from NetBackup 11.1 and above.`
	NetBackup 11.0.0.1 以前のバージョンでは、インスタントアクセス VM を作成できません。
	推奨処置:
	NetBackup 11.1 以降のバージョンでリストアが完了していることを確認します。

`Failed to create the VM in the Nutanix AHV cluster. Error: InUse: MAC address <MAC address> is in use: 18. Return value 114. Failed to create an instant access virtual machine (VM). (4004)`	これは、元の VM がまだ Nutanix クラスタに存在し、MAC アドレスがすでに使用中の場合に発生するもので、これにより競合が発生します。 推奨処置: MAC アドレスの重複を避けるため、インスタントアクセスリカバリの前に、元の VM が削除されているか、電源がオフになっていることを確認します。

NetBackup for AHV のトラブルシューティングのヒント

AHV のトラブルシューティングについて詳しくは、次の詳細をご確認ください。

- 検出ジョブが失敗する場合:
  - アクティビティモニターでジョブの[ジョブの詳細 (Job details)]セクションを確認します。
  - `ncfnbcs` ログを確認します。
- スナップショットジョブが失敗する場合:
  - アクティビティモニターでジョブの[ジョブの詳細 (Job details)]セクションを確認します。
  - `bpfis` ログを確認します。
  - AHV 関連のエラーについては、AHV Prism コンソールで[アラート (Alerts)]を確認します。

- バックアップジョブが失敗する場合:
  - アクティビティモニターでジョブの[ジョブの詳細 (Job details)]セクションを確認します。
  - bpbkar および VxMS ログを確認します。
  - AHV スナップショット関連のエラーについては、AHV Prism コンソールで[アラート (Alerts)]を確認します。
- リストアジョブが失敗する場合:
  - リストアジョブがエラー 2822 で失敗する (Hypervisor ポリシーのリストアエラー)
  - アクティビティモニターでジョブの[ジョブの詳細 (Job details)]セクションを確認します。
  - bprd、bpVMutil、VxMS、または ncfnbrestore ログを確認します。
  - AHV 関連のエラーについては、AHV Prism コンソールで[アラート (Alerts)]を確認します。

AHV クレデンシャルの追加中のエラー

表 9-2 AHV クレデンシャルの追加中のエラー

エラーメッセージまたは原因	説明および推奨処置
仮想マシンの検出およびクレデンシャルの検証は、NetBackup 9.1 以降でサポートされています。選択されたサーバーまたはバックアップホストは NetBackup バージョン 8.3 です。	サーバーまたはバックアップホストをアップグレードするか、必要な NetBackup バージョンをインストールした別のサーバーまたはバックアップホストを選択してください。

AHV 仮想マシンの検出フェーズで発生するエラー

次の表に、AHV 仮想マシンの検出を試行したときに発生する可能性がある問題を示します。

表 9-3 AHV 仮想マシンの検出フェーズで発生するエラー

エラーメッセージまたは原因	説明および推奨処置
AHV クラスタの正しいクレデンシャルを追加しても AHV 資産が検出されず、VM の検出操作が失敗する。	今すぐ検出を実行し、バックアップを再試行します。AHV クラスタ名に使用できる最大文字数は 255 文字ですが、95 文字を超えていると資産の検出が失敗します。 回避方法: ■ AHV クラスタ名を 95 文字以下にします。
検出ジョブがエラー 200 で失敗する。スケジューラでバックアップまたは NetBackup の配備先のクライアントが見つからない。	ポリシーまたはインテリジェント VM グループで指定された問い合わせが正しいことを確認します。保護を必要とする VM が最近 AHV クラスタに追加されたか、VM の構成が変更され、自動検出または今すぐ検出がトリガされませんでした。 ■ `tpconfig` を使用して AHV クラスタのクレデンシャルを追加した場合、資産の検出が機能しません。 回避方法: NetBackup Web UI で、指定した AHV クラスタの[検出 (Discover)]をクリックします。 API または NetBackup Web UI を使用して AHV クラスタのクレデンシャルを追加してください。

新たに検出された VM の状態のエラー

次の表に、AHV 仮想マシンの検出を試行したときに発生する可能性がある問題を示します。

表 9-4 新たに検出された VM の状態のエラー

エラーメッセージまたは原因	説明および推奨処置
VM の前回成功したバックアップの状態で、バックアップ未完了と示されている。	NetBackup Web UI で、新たに検出された VM の前回成功したバックアップの状態で、バックアップ未完了と示されています。 場合によっては、次のシナリオのように、インテリジェント VM グループなど、指定された問い合わせに一致する新しい VM が検出される前に、その VM がバックアップされることがあります。 ■ デフォルトでは、8 時間ごとに自動検出が実行されます。 ■ 新しい VM が環境に追加されました。 ■ 検出が完了する前に、バックアップジョブが正常に完了しました。 たとえば、新しい VM が既存のポリシーのバックアップの選択条件に含まれており、バックアップジョブがそのポリシーを使用している場合です。 ■ NetBackup Web UI で、VM の前回成功したバックアップの状態は更新されず、バックアップ未完了と示されています。 回避方法: ■ 同様の状況が発生した場合、リカバリポイントを参照してリカバリできます。 ただし、クラスタで検出がトリガされ、検出後に VM の別のバックアップが正常に完了した後に、前回成功したバックアップの状態が更新されます。

AHV 仮想マシンのバックアップの実行時に発生するエラー

次の表に、AHV 仮想マシンをバックアップするときに発生する可能性がある問題を示します。

表 9-5 AHV 仮想マシンのバックアップの実行時に発生するエラー

エラーメッセージまたは原因	説明および推奨処置
NetBackup のバックアップ操作後に AHV クラスタで VM のスナップショットが削除されない。	VM に接続されているディスクが非アクティブ状態の場合、バックアップ操作の完了後に AHV クラスタで VM のスナップショットが削除されません。 回避方法: ■ バックアップ操作を開始する前に、VM に接続されているディスクの状態を確認し、それらがアクティブであることを確認します。 ■ ディスクが非アクティブ状態になることを回避するために、VM の実行中はディスクを接続しないようにします。
MSiSCSI サービスは無効です。バックアップホストで MSiSCSI サービスを有効にしてください。(MSiSCSI service is disabled. Enable the MSiSCSI service on the backup host.)	Windows バックアップホストで Microsoft iSCSI イニシエータサービス (MSiSCSI サービス) を有効にして、ジョブを再実行します。

エラーメッセージまたは原因	説明および推奨処置
接続を確立できません。iSCSI サービスがインストールされ実行中であることを確認してください。(Unable to establish a connection. Verify that the iSCSI service is installed and running.)	

エラーメッセージまたは原因	説明および推奨処置
	■ Windows の場合: バックアップホストで Microsoft iSCSI イニシエータサービスを有効にします。 **メモ:** Windows OS でのみ表示されるエラーです。 ■ Linux の場合: このエラーは警告形式で表示され、バックアップまたはリストアに NFS を使用するようにフォールバックされます。セグメント化された iSCSI データサービスを使用すると、バックアップまたはリストアは失敗します。 NFS トランスポートを介してバックアップが機能するよう、Nutanix の[Filesystem Whitelists]オプションにバックアップホストが追加されている必要があります。 Linux で iSCSI を使用する場合: バックアップホストで iSCSI イニシエータパッケージをインストールまたは有効化し、ジョブを再実行します。 ■ Linux ホストで次のコマンドを使用して接続を検証します。 `iscsiadm -m discovery -t sendtargets -p` *`correct IP as per configured iSCSITargetType`* iSCSI トランスポート形式に基づいて次の IP アドレスを使用します。 ■ iSCSI データサービスの場合: クラスタの詳細ページの iSCSI データサービス IP ■ セグメント化の場合: クラスタの詳細ページ SEGMENTED_SPECIFIC のセグメント化された iSCSI データを使用します。 ■ 指定したセグメント化の場合: NetBackup でクラスタを構成するときに指定した仮想 IP を使用します。 ■ Windows ホストで次のコマンドを使用して接続を検証します。 ■ [サーバーマネージャー (Server Manager)]、[ツール (Tools)]、[iSCSI イニシエータ (iSCSI initiator)]の順に選択します。これにより、[iSCSI イニシエータのプロパティ (iSCSI initiator properties)]ダイアログが開きます。 ■ [検出 (Discovery)]、[検出ポータル (Discovery portal)]の順に選択して、AHV クラスタの構成済み iSCSI ターゲットタイプに従って IP アドレスを指定します。 ■ デフォルト: クラスタの詳細ページの iSCSI データサービス IP ■ SEGMENTED: クラスタの詳細ページのセグメント化された iSCSI データ ■ SEGMENTED_SPECIFIC: NetBackup でクラスタを構成するときに指定した仮想 IP。 ■ Flex Scale アプライアンスを使用してエラーメッセージが表示された場合は、NetBackup プライマリサーバーのみが iSCSI データパスをサポートしておらず、データパスとして NFS をサ

エラーメッセージまたは原因	説明および推奨処置
	ポートすることに注意します。 ただし、iSCSI データパスの使用が不可欠な場合は、プライマリサーバーの代わりにメディアサーバーを使用することをお勧めします。メディアサーバーは効果的に iSCSI データパスを管理し、適切なバックアップとリストア機能を保証します。 ■ Flex Appliance をバックアップホストまたはリカバリホストとして使用してこのエラーが発生した場合: ■ NFS トランスポートを使用するデフォルトオプションを使用するように構成を編集します。 ■ 必要な iSCSI とネットワーク構成がある、異なるバックアップまたはリカバリホストを使用します。 ■ 特定のバックアップホストを使用するように保護計画を更新します。 ■ 必要な iSCSI とネットワーク構成があるリカバリホストを使用します。
認証に失敗しました。イニシエータに指定した CHAP が正しいかどうかを確認してください。(Authentication failed. Verify whether the provided initiator CHAP is correct.)	指定した CHAP キーが無効であるか、iSCSI イニシエータ名が各バックアップまたは各リカバリホストで一意ではありません。各バックアップホストまたはリカバリホストに一意の iSCSI イニシエータ名を設定します。
iSCSI の外部データサービスの IP アドレスを取得できませんでした。次の Nutanix クラスタで IP アドレスを設定した後、ジョブを再実行してください: {Nutanix AHV クラスタ名} (Failed to get an external data service IP address for iSCSI. Re-run the job after setting IP address on the Nutanix cluster: { Nutanix AHV clusterName}.)	Nutanix AHV クラスタで iSCSI の外部データサービスの IP アドレスを設定します。詳しくは、p.24 の「Nutanix AHV クラスタを構成するための前提条件」を参照してください。 **メモ:** Linux ではフォールバックされ、バックアップまたはリストアに NFS が使用されます。
1 つ以上のバックアップホストで NetBackup バージョンがサポートされていません。Nutanix 保護計画で[自動(Automatic)]バックアップホストオプションを使用するには、すべての Linux または Windows バックアップホストで NetBackup バージョン 9.1 以降を使用してください。	このエラーは、Nutanix 保護計画のバックアップホストに[自動(Automatic)]オプションが選択されている場合に発生します。バックアップホストを NetBackup の最新バージョンにアップグレードしてください。
NetBackup メディアサーバーの負荷分散を行うには、バックアップホストに Red Hat Enterprise Linux、SUSE Linux Enterprise Server または Microsoft Windows オペレーティングシステムのいずれかがインストールされていることを確認してください。(For NetBackup media server load balancing, ensure that the backup hosts have either Red Hat Enterprise Linux, SUSE Linux Enterprise Server or Microsoft Windows operating system.)	このエラーは、Nutanix 保護計画のバックアップホストに[自動(Automatic)]オプションが選択されている場合に発生します。 Nutanix AHV の場合、サポートされるメディアサーバーは次のとおりです。 ■ Red Hat Enterprise Linux ■ SUSE Linux Enterprise Server ■ Microsoft Windows オペレーティングシステム

エラーメッセージまたは原因	説明および推奨処置
メディアサーバーの既存の NetBackup バージョンでは増分バックアップスケジュールがサポートされません。	バックアップホストの NetBackup を最新バージョンにアップグレードしてください。(Existing version of NetBackup on the media server does not support the incremental backup schedule. Upgrade NetBackup to the latest version on the backup host.)
特定の Nutanix クラスタにリソース制限を設定できない。	リソース制限が設定されているクラスタが NetBackup 環境から削除されると、リソース制限を設定するための[+ 追加 (+ Add)]オプションが無効になる場合があります。 推奨処置 削除されたクラスタのリソース制限を削除し、残りのクラスタにリソース制限を設定します。

スナップショットジョブがエラーコード 156 で失敗し、次のようなジョブの詳細が表示される。
`Critical bpbrm (pid=30139) from client 9c5dcb07-65d2 -4761-b861-9e517edcf5b6_ <Nutanix-cluster>`
`abc.cbus.com FTL - Value 2 that specifies GUID is not supported for the nameuse`
	保護計画が[バックアップオプション (Backup option)]、[バックアップに使用するサーバーまたはホストを選択する (Select server or host to use for backups)]、[自動 (Automatic)]を使用して作成され、選択したストレージユニットが NetBackup 9.1 以前のバージョンのメディアサーバーで構成されている場合、この保護計画を使用して AHV VM またはインテリジェント VM グループをバックアップすると、スナップショットジョブが失敗することがあります。
	推奨処置
	選択したストレージユニットで構成されているメディアサーバーはすべて NetBackup 9.1 にアップグレードする必要があります。
	他のメディアサーバーのアップグレードが進行中である場合にジョブのエラーを回避するには、[保護 (Protection)]、[保護のカスタマイズ (Customize Protection)]、[バックアップオプション (Backup option)]オプションで、デフォルトの[自動 (Automatic)]オプションではなく、バックアップに使用するサーバーまたはホストとして特定のメディアサーバーまたはバックアップホストを手動で選択します。アップグレード済みのメディアサーバーを使用することをお勧めします。すべてのメディアサーバーのアップグレードが完了したら、[保護 (Protection)]、[元の設定をリストア (Restore Original Settings)]を使用して、元の設定に戻します。

エラーメッセージまたは原因	説明および推奨処置

エラー 1
 	
`iscsiadm: Could not login to [iface: default, target: iqn.2010-06.com.nutanix: nbubackup -2d29da9d-f964-4157-9595-f0319090bb01-tgt0, portal: xx.xx.xx.xx,3260]`
 	
`iscsiadm: initiator reported error (24 - iSCSI login failed due to authorization failure)`
 	
`iscsiadm: Could not log into all portals`
 	
エラー 2
 	
`iscsiadm: Could not execute operation on all records: encountered iSCSI database failure`
 	
エラー 3
 	
`iscsiadm: could not read session targetname: 5`
 	
`iscsiadm: could not find session info for session28`
	これらのエラーは、バックアップジョブまたはリストアジョブの［成功したジョブの詳細 (Successful job details)］タブに表示されます。これらのエラーは `iscsiadm` コマンドを実行したときの出力です。これらのエラーは断続的に発生し、iSCSI ネットワークの負荷が高い場合に発生する可能性があります。NetBackup は、これらのエラーを修正するために再試行操作を実行します。再試行操作が成功すると、バックアップジョブまたはリストアジョブも成功します。
	
	推奨処置
	
	NetBackup 側での対処は不要です。このようなエラーを回避するには、引き続き `iscsiadm` をトラブルシューティングして、iSCSI のインストールまたは構成が正しいことを確認します。

`iscsid: Ignoring CHAP algorithm request for MD5 due to crypto lib configuration iscsid: Couldn't set CHAP algorithm list`	「In FIPS enabled environment, NetBackup backup/restore of Nutanix AHV VMs (Virtual Machines) using iSCSI fails」を参照してください。

エラーメッセージまたは原因	説明および推奨処置
エラーコード: 4798 [このクラスタに Prism Central サーバーを使用]オプションが、AHV クラスタに対して選択されていません。(Use Prism Central server for this cluster option is not selected for AHV cluster.)	バックアップ中の検出ジョブが、Nutanix インテリジェント VM グループのエラーで失敗する場合があります。 インテリジェント VM グループで考えられる次の原因を確認して修正します。 ■ フィルタクエリの 1 つとしてカテゴリフィルタを使用して作成されている、および ■ インテリジェント VM グループが作成された後、[このクラスタに Prism Central サーバーを使用 (Use Prism Central server for this cluster)]オプションのチェックマークをはずし、そのような IVMG 上で[今すぐバックアップ (Backup now)]操作がトリガされるように、1 つ以上の Nutanix クラスタが更新されている。
エラーメッセージ: AHV クラスタ用の Prism Central が見つかりません。サーバー = <サーバーの詳細> (Unable to find the Prism Central for AHV cluster, server = Server details)	バックアップジョブが指定のエラーで失敗します。 次の考えられる原因を確認して修正します。 ■ 同じ Prism Central サーバーの 1 つ以上のクラスタで構成され、いずれかのフィルタとしてカテゴリを持つインテリジェント VM グループでは、IVM グループの保護がトリガされると、Prism Central サーバーは削除されるか、アクセスできなくなります。 ■ 異なる Prism Central サーバーの 2 つ以上のクラスタで構成され、いずれかのフィルタとしてカテゴリを持つインテリジェント VM グループでは、インテリジェント VM グループの保護がトリガされると、1 つ以上の Prism Central サーバーが削除されるか、アクセスできなくなります。
エラーメッセージ: 保護計画のサブスクリプションがエラーで失敗します。 無効な API 要求が発生しました。(An invalid API request is encountered) `error message: backupHost: Backup host with a NetBackup version earlier than 10.4 is not supported for IntelligentVM group Category filter.`	インテリジェント VM グループでカテゴリフィルタが使用されている場合、保護計画へのサブスクライブが失敗し、エラーが発生する場合があります。 ■ 保護計画に記載されているバックアップホストが NetBackup バージョン 10.4 以降であることを確認します。

エラーメッセージまたは原因	説明および推奨処置

バックアップジョブはエラーコード 800 で失敗します。
 	
`Error nbjm(pid=113200) NetBackup status: 800, EMM status :Use NetBackup media server version 10.4 or later to protect Nutanix Intelligent VM groups with category filters.`
 	
`.`
 	
`Error nbpem(pid=113293) backup of client MEDIA_SERVER exited with status 800 (resource request failed).`
	説明
	
	保護計画が[バックアップオプション (Backup option)]、[バックアップに使用するサーバーまたはホストを選択する (Select server or host to use for backups)]、[自動 (Automatic)]を使用して作成され、選択したストレージユニットが NetBackup 10.4 以前のバージョンのメディアサーバーで構成されている場合、および、カテゴリ属性をフィルタとして使用するインテリジェント VM グループをバックアップするためにこの保護計画を使用する場合、バックアップジョブは失敗します。
	
	推奨処置:
	
	選択したストレージユニットで構成されている少なくとも 1 台のメディアサーバーを、NetBackup v10.4 以降にアップグレードする必要があります。

バックアップジョブは、次のエラーメッセージで失敗します。
 	
エラー 1
 	
`Begin Application Resolver:Resolver Discovery`
 	
エラー 2
 	
`Error nbpem(pid=98395) Invalid URI.`
 	
エラー 3
 	
`Error nbpem (pid=98395) backup of client falcna12c3.abcus.com exited with status 4232 Invalid Discovery Query URI).`
	説明
	
	インテリジェント VM グループが、バックアップホストのバージョンが 10.3 以前の保護計画でサブスクライブされ、インテリジェント VM グループがカテゴリフィルタを使用して変更されることがあります。
	
	その後、バックアップジョブが実行されると、エラーメッセージが表示されて失敗します。これは、カテゴリフィルタが、古いバージョンのバックアップホストでは認識されないためです。
	
	推奨処置:
	
	保護計画をカスタマイズして、バックアップホストを 10.4 以降にアップグレードします。詳しくは、p.73 の「AHV 資産の保護設定のカスタマイズ」を参照してください。

AHV 仮想マシンのリストア中に発生するエラー

次の表に、AHV 仮想マシンをリストアするときに発生する可能性がある問題を示します。

表 9-6 AHV 仮想マシンのリストア中に発生するエラー

エラーメッセージまたは原因	説明および推奨処置
Windows プライマリサーバーで、代替の場所への VM のリカバリが失敗する。	Windows NetBackup プライマリサーバーの場合は、rename ファイルが空の行で終わっていることを確認します。

エラーメッセージまたは原因	説明および推奨処置
リカバリ先を変更するときに、AHV クラスタを変更できない。	AHV クラスタのリストを表示できない場合は、RBAC の AHV クラスタへのアクセス権がない可能性があります。 この問題を解決するには、NetBackup セキュリティ管理者にお問い合わせください。
AHV クラスタに同じ UUID の VM が存在し、VMを上書きするオプションが有効でない場合、リカバリ前チェックは正常に完了するが、VM のリストアは失敗する。 次のエラーメッセージが表示される: 情報 bpVMutil (pid=1196) FTL - 仮想マシンが存在し、上書きオプションが指定されていないため、リストアを続行できません。リストアの終了。経過時間 Hypervisor ポリシーリストアエラー。(2822)	リカバリ前チェックでは UUID ではなく VM 表示名と比較して VM がすでに存在するかを確認するため、このチェックは正常に完了します。しかし上書きオプションが設定されていないと、同じ UUID の VM がすでに存在する場合、リストアジョブは失敗します。 回避方法: **新しい UUID を持つ VM をリストアします。** **1** リカバリ処理を開始します。 **2** [リカバリオプション (Recovery Options)]ページで、[詳細 (Advanced)]をクリックします。 **3** [新しい VM UUID の作成 (Create a new VM UUID)]を有効にします。 **4** リカバリ処理を続行し、[リカバリの開始 (Start recovery)]をクリックしてリストアします。 **同じ UUID を持つ既存の VM を上書きします。** **1** リカバリ処理を開始します。 **2** [リカバリオプション (Recovery Options)]ページで[既存の仮想マシンの上書き (Overwrite existing virtual machine)]オプションを有効にします。 **3** リカバリ処理を続行し、[リカバリの開始 (Start recovery)]をクリックしてリストアします。
Web UI を使用して別のドメインからインポートされた AHV VM イメージをリカバリしようとすると、リカバリ前チェックが失敗し、デフォルトで、リカバリホストがバックアップ中に使用されていたものと同じアクセスホストであることが表示される。	インポートされた AHV VM イメージのリカバリ中に、リカバリホストとしてターゲットドメインのアクセスホストを選択するか、ターゲットプライマリサーバーを選択します。
MSiSCSI サービスは無効です。リカバリホストで MSiSCSI サービスを有効にしてください。(MSiSCSI service is disabled. Enable the MSiSCSI service on the backup host.)	Windows バックアップリカバリで Microsoft iSCSI イニシエータサービス (MSiSCSI サービス) を有効にして、ジョブを再実行します。

エラーメッセージまたは原因	説明および推奨処置
リカバリホストに接続できませんでした。(Failed to connect to the recovery host.)	エージェントレスリストアに使用するリカバリホストにアクセスできません。 推奨処置: リカバリホストにプライマリサーバーからアクセス可能であり、NetBackup メディアサーバーまたはクライアントソフトウェアがインストールされていることを確認します。
エージェントレスリストアをサポートするには、指定したリバカリホストが NetBackup バージョン 9.1 以降である必要があります。(The specified recovery host must be at NetBackup version 9.1 or later to support agentless restores.)	ファイルまたはフォルダのエージェントレスリストアには、NetBackup バージョン 9.1 以降のリカバリホストが必要です。 推奨処置: リカバリホストの NetBackup のバージョンを確認します。9.1 以降である必要があります。 UNIX の場合、NetBackup のサーバーとクライアントで `/usr/openv/netbackup/bin/version` ファイルを確認します。 Windows の NetBackup サーバーの場合、`install_path¥netbackup¥version.txt` ファイルを確認します。
リカバリホストのステージング場所が存在しません。(Recovery host staging location does not exist.)	エージェントレスリストア用のリカバリホストにステージング場所のパスが存在しません。 推奨処置: ■ デフォルトのステージング場所のパス、またはユーザー構成のステージング場所のパスが、リカバリホストで有効であることを確認します。NetBackup は、リカバリホストの次の場所をデフォルトのステージング場所として使用します。 ■ UNIX の場合: `{installpath}/openv/tmp/staging` ■ Windows の場合: `{installpath}¥Netbackup¥Temp¥staging¥` ■ 使用するステージング場所のパスが存在することを確認します。ユーザー構成のステージング場所については、リカバリホストの有効なパスが `bp.conf` のパラメータ AGENTLESS_RHOST_STAGING_PATH = "path" で指定されていることを確認します。
リカバリホストのステージング場所で tar イメージが見つかりません。(Tar image not found at staging location on recovery host.)	リカバリホストのステージング場所に tar イメージが見つかりませんでした。エージェントレスリストアには tar イメージが必要です。 推奨処置: Cohesity Technical Supportに問い合わせて、リカバリホストの `bpVMutil` ログを共有してください。
内部エラーにより、リカバリの検証が失敗しました。(Internal error has caused failure of recovery validation.)	エージェントレスリストアのリカバリ前の検証を実行中に内部エラーが発生しました。 推奨処置: リカバリホストの bpVMutil ログを保存し、Cohesity テクニカルサポートにお問い合わせください。

エラーメッセージまたは原因	説明および推奨処置
リカバリホストに利用可能な十分な領域がありません。(Not enough space available on recovery host.)	リカバリホストのエージェントレスリストアのステージング場所に、選択したファイルをコピーするための十分な領域がない可能性があります。 推奨処置: 選択したファイルまたはフォルダの合計サイズに基づいて、リカバリホストのステージング場所に十分な空き容量が利用可能であることを確認します。または、エージェントレスリストアを実行するための十分な空き容量がある別のリカバリホストを選択します。
ターゲットホストに tar ユーティリティが存在しません。(Tar utility is not present on the target host.)	ターゲットホスト上の tar ユーティリティの検索に失敗しました。エージェントレスリストアには tar ユーティリティが必要です。 推奨処置: tar ユーティリティを配備してから再試行します。
指定されたステージング場所がターゲットホストに存在しないか、アクセスに必要な権限がユーザーにありません。	推奨処置: ターゲットホストのステージング場所が存在し、場所にアクセスするための十分な権限がユーザーにあることを確認します。
ユーザーは、ターゲットホストのステージング場所に対して必要な権限がありません。(The user does not have required permission on the target host staging location.)	ユーザーに、ターゲットホストでリストアを続行するために必要な権限がありません。 推奨処置: ターゲットホストのステージング場所が存在し、少なくともステージング場所の書き込みおよび実行権限がユーザーにあることを確認します。
ユーザーに root または管理者権限がありません。ファイルとフォルダをリストアするには、ユーザーに root 権限または管理者権限を付与します。	ユーザーに、ターゲットホストでリストアを続行するために必要な権限がありません。 推奨処置: Windows ターゲットホストのローカル管理者グループに含まれるクレデンシャルを指定します。Linux ターゲットホストの場合は、ルートまたはすべての権限を持つ sudo アカウントのクレデンシャルを使用してください。
リカバリホストからターゲットホストの管理共有にアクセスできません。(Admin share of target host is not accessible from the recovery host.)	エージェントレスリストアを実行するため、リカバリホストからリモートホストの管理共有にアクセスできません。 推奨処置: ■ ファイアウォールの例外が正しく設定されていることを確認します。 ■ ファイルとプリンタの共有が有効になっていることを確認します。 ■ GPO/ソフトウェア制限ポリシーまたはウイルス対策ソフトウェアがアクセスを遮断していないことを確認します。 ■ ターゲットホストにアクセス可能で、正しいクレデンシャルが入力され、適切な権限が付与されていることを確認します。

エラーメッセージまたは原因	説明および推奨処置
ユーザーアカウント制御 (UAC) 環境でファイルまたはフォルダのエージェントレスリストアを行う場合は、Windows ターゲットホストのローカル管理者グループに含まれるドメインユーザーのクレデンシャルを指定します。	推奨処置: UAC (ユーザーアクセス制御) 環境でのエージェントレスリストアの場合、ドメインユーザーのクレデンシャルを指定します。このユーザーは、Windows のターゲットホストのローカル管理者グループに属しています。
エージェントレスリストアを実行できません。(Agentless restore is not possible.)	エージェントレスリストアの失敗で予期しない理由が戻されました。 推奨処置: Cohesity テクニカルサポートに問い合わせて、該当するログを共有してください。
オペレーティングシステムが一致しません。リカバリホストのオペレーティングシステムとバックアップされた VM のオペレーティングシステムが一致していることを確認してください。(Operating systems do not match. Ensure that the operating system of recovery host matches with the backed-up VM operating system.)	エージェントレスリストアは、リカバリホストとバックアップされた VM のオペレーティングシステムが同じ場合にのみ可能です。 推奨処置: 代替リカバリホストに、バックアップされた VM と同じオペレーティングシステムがインストールされている必要があります。
バックアップイメージのオペレーティングシステムの取得に失敗しました。(Failed to retrieve the backup image operating system.)	エージェントレスリストアを実行するためにバックアップイメージのオペレーティングシステムを取得できません。これは内部エラーです。
リカバリホストのオペレーティングシステムは、指定した通信モードとの互換性がありません。リカバリホストのオペレーティングシステムに、指定した通信モードとの互換性があることを確認してください。(Recovery host operating system is not compatible with provided communication mode. Ensure that the operating system of recovery host and provided communication mode are compatible.)	エージェントレスリカバリまたはリカバリ前チェック要求で指定されたリカバリホストの OS の種類と通信の種類に互換性がありません。 推奨処置: リカバリホストの OS の種類と通信の種類がリカバリホストと互換性があることを確認します。 ■ Linux: 通信の種類は `SSH` である必要があります。 ■ Windows: 通信の種類は `WMI` である必要があります。
ターゲットホストの SSH 秘密鍵が無効です。(Target host SSH private key is invalid.)	エージェントレスリカバリ要求またはリカバリ前チェック要求の `sshKey` フィールドは、ターゲットホストの有効で空でない SSH 秘密鍵にする必要があります。 推奨処置: 認証形式が `SSH_KEY` の場合は、[`sshKey`]フィールドが指定されており、空でないことを確認します。

エラーメッセージまたは原因	説明および推奨処置
ファイルまたはフォルダのエージェントレスリストアでターゲットホストオペレーティングシステムがサポートされていません。(Target host operating system is not supported for the agentless files or folders restore.)	エージェントレスリストアではターゲットホストにリカバリパッケージを配備する必要があるため、ターゲットホストのオペレーティングシステムはサポートされません。 推奨処置: SUSE Linux Enterprise Server、Microsoft Windows、Red Hat Enterprise Linux (RHEL)、Ubuntu のみがサポート対象のプラットフォームです。 この機能がサポートされているプラットフォームについては、NetBackup ソフトウェア互換性リストを参照してください。
ターゲットホストのユーザー名またはパスワードが無効です。(Invalid target host user name or password.)	エージェントレスリカバリ要求またはリカバリ前チェック要求の認証の詳細で、ユーザー名とパスワードのフィールドを指定する必要があります。 推奨処置: リカバリ要求とリカバリ前チェック要求の認証の詳細で、ユーザー名とパスワードのフィールドが正しく指定されており、空でないことを確認します。
ターゲットホストのステージング場所のパスに ASCII 以外の文字が含まれています。(Target host staging location path contains non-ASCII characters.)	ターゲットホストのステージング場所のパスでは ASCII 文字のみがサポートされます。 推奨処置: ACSII 文字のみを使用して、ターゲットホスト上のカスタムのステージング場所を指定します。
指定したパスがローカルディスクに存在しません。(Specified path does not exist on the local disk.)	ターゲットホストのステージング場所にネットワークパスは指定できません。 推奨処置: ローカルディスクにあるターゲットホストのカスタムのステージング場所を指定します。
ターゲットホストへの WMI 接続に失敗しました。(WMI connection to the target host is failed.)	リカバリホストからのターゲットホストへの WMI 接続に失敗しました。 推奨処置: ■ WMI および DCOM サービスに接続するには、リモート WMI サービスに接続するために必要な権限がユーザーに付与されている必要があります。 ■ ファイアウォールを通過する WMI トラフィックを許可するために、ファイアウォールの例外が設定されています。 ■ GPO/ソフトウェア制限ポリシーまたはウイルス対策ソフトウェアがアクセスを遮断しないようにします。 ■ ターゲットホストがアクセス可能であることを確認します。指定したターゲットホストのクレデンシャルを検証します。 ■ ターゲットホストとドメインの信頼関係が維持されていることを確認します。ドメイン間で通信する場合は、これらのドメイン間に双方向の信頼関係が存在する必要があります。

エラーメッセージまたは原因	説明および推奨処置
指定されたファイルがリモートサーバーで見つかりません。(Unable to find the specified file on the remote server.)	指定されたファイルがリモートサーバーで見つかりません。 推奨処置: ターゲットホストで指定したステージング場所が存在することを確認するか、別の有効なステージング場所を指定します。
ディレクトリと同じ名前のファイルが存在します。(File exists with same name as the directory.)	ターゲットホストにステージング場所のディレクトリパスと同じ名前の既存のファイルがあります。 推奨処置: ステージング場所と同じ名前とパスの既存のファイルがリモートホストにあるかどうかを確認します。存在する場合は、そのファイルの名前を変更するか、ファイルを削除します。または、代替のステージング場所を指定します。
ユーザーの管理者権限の検証に失敗しました。(Failed to validate administrative privileges for the user.)	ターゲットホストのユーザーに、ファイルとフォルダのエージェントレスリストア操作を続行するための管理者権限がありません。 推奨処置: Windows ターゲットホストのローカル管理者グループに含まれるクレデンシャルを使用します。 Linux ターゲットホストの場合は、ルートまたはすべての権限を持つ sudo アカウントのクレデンシャルを使用してください。
Windows API を使用したネットワークリソースへの接続に失敗しました。(Failed to connect a network resource using windows API.)	ファイルとフォルダのエージェントレスリストアを実行するために、リカバリホストからターゲットホストの管理共有にアクセスできません。 推奨処置: ファイルおよびフォルダのエージェントレスリストア操作の一環として、ユーザーが指定したクレデンシャルを使用してターゲットホスト上のリカバリホストから SMB 管理共有が作成されます。このエラーは通常、エージェントレスリストアのターゲットホストに Windows OS が搭載され、リカバリホストからターゲットホストの管理共有にアクセスできない場合に発生します。ターゲットホストで次の要件が満たされていることを確認します。 ■ ファイアウォールの例外が正しく設定されている。 ■ ファイルとプリンタの共有が有効になっている。 ■ GPO/ソフトウェア制限ポリシーまたはウイルス対策ソフトウェアがアクセスを遮断しない。 ■ 有効なクレデンシャルでターゲットホストにアクセスできる。

エラーメッセージまたは原因	説明および推奨処置
ターゲットホストでユーザーのホームディレクトリを取得できません。カスタムのステージング場所を指定してください。(Unable to retrieve user's home directory on the target host. Specify the custom staging location.)	ホームディレクトリ上のユーザーのデフォルトのステージング場所をターゲットホストで取得できません。有効なカスタムのステージング場所のパスを入力します。 推奨処置: ユーザーのホームディレクトリが存在することを確認するか、有効なカスタムのステージング場所で試行します。
ホストとの SSH セッションの確立に失敗しました。(Failed to establish SSH session with host.)	次のすべての条件を満たしていることを確認してから、再試行します。 ■ 通信での使用でサポートされている暗号は aes256-ctr です。この暗号がリカバリホストとターゲットホストの両方でサポートされていることを確認します。 ■ リカバリホストとターゲットホストの両方で、次の HMAC (Hash-based Message Authentication Code) プロトコルの少なくとも 1 つがサポートされていることを確認します。 ■ hmac-sha2-256 ■ hmac-sha2-512 ■ ホストキーの生成に使用される方法が、次のいずれかであることを確認します。 ■ ECDSA_SHA2_NISTP256 ■ ECDSA_SHA2_NISTP384 ■ ECDSA_SHA2_NISTP521 ■ SSH_RSA ■ SSH_DSS
ホストの SSH 鍵指紋の検証に失敗しました。(Failed to verify SSH key fingerprint of host.)	指定されたターゲットホストの SSH 鍵指紋が正しくありません。 推奨処置: ターゲットホストの SSH 鍵指紋を確認して再試行します。
指定されたユーザー名またはパスワードでのホストの認証に失敗しました。(Failed to authenticate the host with provided username or password.)	指定されたユーザー名またはパスワードでのターゲットホストの認証に失敗しました。 推奨処置: ターゲットホストのユーザー名またはパスワードが正しいことを確認して再試行します。
指定された SSH 鍵でのホストの認証に失敗しました。(Failed to authenticate the host with specified SSH key.)	指定された SSH 秘密鍵でのターゲットホストの認証に失敗しました。 推奨処置: ターゲットホストの SSH 秘密鍵の生成に使用された SSH 秘密鍵およびキーのパスフレーズが有効であることを確認します。確認したら、再試行します。対応する公開鍵がターゲットホストの /root/.ssh フォルダの authorized_keys ファイルに存在することを確認します。

エラーメッセージまたは原因	説明および推奨処置
一致する SSH 鍵指紋のホストキー方式がターゲットホストで見つかりません。(Matching SSH Key fingerprint host key method not found on target host.)	指定した SSH 鍵指紋のホストキー方式がターゲットホストで見つかりません。 推奨処置: 指定した SSH 鍵指紋のサポート対象のホストキー方式がターゲットホストで利用できることを確認します。または、ターゲットホストで構成されているホストキー方式の SSH 指紋を指定します。
NetBackup クライアントソフトウェアが存在する仮想マシンに個々のファイルをリストアした場合にリストアが失敗する。	NetBackup クライアントが存在する仮想マシンに個々のファイルをリストアする場合は、ファイアウォールがリストアを妨害していないことを確認します。ファイアウォールがリストアを停止する場合は、ファイアウォールをオフにし、リストアを再試行します。
Linux 仮想マシンからファイルをリストアするときにマウントポイントを利用できない。	Linux 仮想マシンの場合、ext2、ext3、ext4、xfs のファイルシステムのみが個々のファイルのリストアでサポートされます。 パーティションが他のファイルシステムでフォーマットされている場合、バックアップは成功しますが、NetBackup はそのファイルのファイルシステムアドレスをマッピングできません。その結果、NetBackup はそのパーティションから個々のファイルをリストアできません。ext2、ext3、ext4、xfs パーティションにあったファイルのみを個別にリストアできます。 **メモ:** 元のマウントポイントから個々のファイルをリストアするには、「/」(ルート) パーティションを ext2、ext3、ext4、または xfs としてフォーマットする必要があります。「/」(ルート) パーティションを別のファイルシステム (ButterFS など) でフォーマットする場合、マウントポイントは解決できません。その場合、/dev レベル (/dev/sda1 など) から ext2、ext3、ext4、または xfs ファイルをリストアできます。ファイルの元のマウントポイントレベルからはファイルをリストアできません。

エラーメッセージまたは原因	説明および推奨処置
永続的なデバイス命名規則を使用していない Linux VM では、複数のディスクコントローラ (IDE、SCSI、SATA など) によって個々のファイルのリカバリが複雑になることがある。	この問題は、/dev/sda や /dev/sdb のような非永続的なデバイス命名規則が原因で発生し、再起動後に予期しないマウントポイントの変更を引き起こすことがあります。VM に SCSI ディスクと SATA ディスクがある場合、[ファイルとフォルダをリストアする (Restore files and folders)]、[ファイルとフォルダを追加 (Add files and folders)]ナビゲーションインターフェースは VM のファイルの誤ったマウントポイントを示すことがあります。たとえば、元々 /vol_a にあったファイルが、リストアしようとして参照すると /vol_b の下に表示される場合があります。リストアは正常に終了しても、リストアされたファイルが元のディレクトリに存在しない場合があります。 推奨処置: リストアした VM のファイルを検索して適切な場所に移動します。複数のディスクコントローラを持つ Linux VM でこの問題を防ぐため、ベリタスでは、ファイルシステムのマウントに永続的なデバイス命名方法を使用することをお勧めします。永続的な命名規則を使用するとデバイスのマウントに一貫性が生じ、今後、バックアップからファイルをリストアしてもこの問題は起きません。永続的なデバイス命名規則では、UUID を使用してデバイスをマウントできます。 次に、UUID を使用してマウントしたデバイスを含む /etc/fstab ファイルの例を示します。 ■ UUID=93a21fe4-4c55-4e5a-8124-1e2e1460fece /boot ext4 defaults 1 2。 ■ UUID=55a24fe3-4c55-4e6a-8124-1e2e1460fadf /vola ext3 defaults 0 0。 デバイスの UUID を見つけるには、次のコマンドのいずれかを使用できます。 ■ blkid ■ ls -l /dev/disk/by-uuid/

エラーメッセージまたは原因	説明および推奨処置
永続的なデバイス命名規則を使用しない Ubuntu VM の場合、[ファイルとフォルダをリストアする (Restore files and folders)]、[ファイルとフォルダを追加 (Add files and folders)]ナビゲーションインターフェースに VM のファイルの誤ったマウントポイントが表示され、個々のファイルのリカバリが失敗することがあります。	この問題は、非永続的なデバイス命名規則が原因で発生し、予期しないマウントポイントの変更を引き起こすことがあります。Ubuntu VM の場合、[ファイルとフォルダをリストアする (Restore files and folders)]、[ファイルとフォルダを追加 (Add files and folders)]ナビゲーションインターフェースに VM のファイルの誤ったマウントポイントが表示されることがあります。たとえば、ファイルとフォルダをリストアするために参照すると `/dev/ubuntu-vg/ubuntu-lv` の下に表示され、個々のファイルのリカバリが失敗することがあります。 推奨処置: Ubuntu VM でこの問題を防ぐため、Cohesityでは、ファイルシステムのマウントに永続的なデバイス命名方法を使用することをお勧めします。永続的な命名規則を使用するとデバイスのマウントに一貫性が生じ、今後、バックアップからファイルをリストアしてもこの問題は起きません。永続的なデバイス命名規則では、UUID を使用してデバイスをマウントできます。 次に、UUID を使用してマウントしたデバイスを含む `/etc/fstab` ファイルの例を示します。 ■ UUID=93a21fe4-4c55-4e5a-8124-1e2e1460fece /boot ext4 defaults 1 2。 ■ UUID=55a24fe3-4c55-4e6a-8124-1e2e1460fadf /vola ext3 defaults 0 0。 デバイスの UUID を見つけるには、次のコマンドのいずれかを使用できます。 ■ `blkid` ■ `ls -l /dev/disk/by-uuid/`

仮想マシンの作成に失敗しました。リストアを続行できません。(Virtual machine creation failed, cannot proceed with restore.)
`bpVMutil`
`pid=3144`
	NetBackup バージョンが 10.1.1 より前のバックアップホストを使用して VPC (仮想プライベートクラウド) 環境で VM をリストアした場合、リストアジョブは失敗します。
	推奨処置
	VPC 環境にある VM をリストアするには、バックアップホストの NetBackup バージョン 10.1.1 以降を使用します。

スナップショットジョブからのリストアは部分的に成功した状態で完了します。	iSCSI トランスポートオプションに従って AHV クラスタに正しい構成がない場合、スナップショットジョブからのリストアは部分的に成功した状態で完了します。 回避方法 iSCSI トランスポートの設定に基づいて、次のエラーを確認して修正します。 ■ デフォルトの場合: iSCSI データサービス IP が構成されています。 ■ セグメント化の場合: セグメント化された IP アドレスが構成されていません。 ■ segmented_specified の場合: セグメント化された iSCSI インターフェースが構成されていないか、指定された IP アドレスが、構成済みの iSCSI インターフェースのいずれかの仮想 IP と一致しません。

エラーメッセージまたは原因	説明および推奨処置
Nutanix-AHV ポリシーでは、11.0 より前の NetBackup バージョンがインストールされているバックアップホストはサポートされていません。	Cohesityでは、NetBackup を最新バージョンにアップグレードすることをお勧めします。
NetBackup の状態: 213、EMM の状態: NetBackup メディアサーバーのバージョンが、この操作を実行するには低すぎます (NetBackup media server version is too low for the operation)。利用可能なストレージユニットがありません (No storage units available for use)(213)。	Nutanix-AHV ポリシーで使用されているストレージユニットを確認します。ストレージユニットが作成されたメディアサーバーは、NetBackup バージョン 11.0 以降である必要があります。 詳しくは、/usr/openv/logs/nbwebservice のパスにあるログを確認してください。

10

AHV の API とコマンドラインオプション

この章では以下の項目について説明しています。

- API とコマンドラインオプションを使用した AHV 仮想マシンの管理、保護、リカバリ
- AHV 構成の追加の NetBackup オプション
- rename ファイルに関する追加情報

API とコマンドラインオプションを使用した AHV 仮想マシンの管理、保護、リカバリ

このトピックでは、AHV 仮想マシンの保護やリカバリに使用する API とコマンドラインオプションを示します。ここでは、重要な変数とオプションのみを説明しています。

このトピックには次のセクションがあります。

- p.139 の「AHV クラスタの追加」を参照してください。
- p.139 の「iSCSI CHAP 設定 API の設定」を参照してください。
- p.140 の「AHV VM のバックアップポリシーの作成」を参照してください。
- p.141 の「元の場所での AHV VM のリカバリ前チェック」を参照してください。
- p.142 の「別の場所での AHV VM のリカバリ前チェック」を参照してください。
- p.142 の「元の場所での AHV VM のリストア」を参照してください。
- p.144 の「代替の場所への AHV VM のリストア」を参照してください。

API とコマンドラインについて詳しくは、次の情報を参照してください。

- 次の場所にすべての NetBackup API が示されています。

［Services and Operations Readiness Tools (SORT)］、［ナレッジベース (Knowledge Base)］、［文書 (Documents)］

- コマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

AHV クラスタの追加

表 10-1 AHV クラスタの追加

API またはコマンドラインオプション	重要な変数とオプション

`POST /netbackup/asset-service/queries`
 	
`GET /netbackup/asset-service/queries/{aqcId}`
	■ `clusterName` は、AHV クラスタの名前です。
	■ `backuphost` は、NetBackup クライアントのホスト名です。
	■ `credentialName` は、AHV クラスタに関連付けられているクレデンシャルです。
	メモ: `credentialName` に記載したクレデンシャルが存在する必要があります。

`tpconfig` コマンド	■ `virtual_machine` は、AHV クラスタの名前です。 ■ `vm_type` は 9 です。数値 9 は AHV クラスタを表します。

iSCSI CHAP 設定 API の設定

表 10-2 iSCSI CHAP 設定 API の設定

API またはコマンドラインオプション	重要な変数とオプション
`GET /netbackup/config/iscsi-settings/{workloadType}`	■ `workloadType` でサポート対象の作業負荷を指定します。 ■ 指定した作業負荷の種類のグローバル iSCSI 設定を取得します。
`POST /netbackup/config/iscsi-settings/{workloadType}`	■ 指定した作業負荷の種類のグローバル iSCSI 設定を変更します。 ■ `authType` は、認証形式です。例: 　■ `ONEWAY_CHAP` 　■ `MUTUAL_CHAP_AUTOMATIC` ■ `passwordRenewalIntervalDays` は［相互 CHAP 自動 (Mutual CHAP Automatic)］オプションにのみ適用されます。 **メモ:** 有効値は 1 日から 365 日です。

AHV VM のバックアップポリシーの作成

表 10-3 AHV VM のバックアップポリシーの作成

API またはコマンドラインオプション	重要な変数とオプション
POST /netbackup/config/policies/	■ policyType は、Hypervisor です。 ■ policyType は、Web UI を使用する Nutanix-AHV です。 ■ backuphost は、仮想マシンの代わりにバックアップを実行する NetBackup クライアントのホスト名です。 ■ Nutanix AHV の場合、Add useVirtualMachine = 6 を追加します。 ■ VM UUID を使用して VM のバックアップを作成するには、snapshotMethodArgs に次の値を指定できます。 ■ backupSelections > selections で、Nutanix-ahv:/?filter=uuid Equal *<uuid_filter>*" の形式のフィルタオプションを使用して、特定の UUID の AHV VM をフィルタ処理します。UUID を除いて、インテリジェント VM グループに対して指定されるその他のフィルタ基準を使用できます。

admincmd コマンド	■ bpplclients -add *<discoveryhost>* Hypervisor Hypervisor の Hypervisor 検出ホストは許可リストに載っている Windows または Linux のホストです。
	■ bpplinfo のポリシー形式 (-pt) は Hypervisor です。
	■ bpplinclude で、Nutanix-ahv:/?filter=uuid Equal *<uuid_filter>*" の形式のフィルタオプションを使用して、特定の UUID の AHV VM をフィルタ処理します。
	■ bpplinfo で、
	  ■ AHV VM の場合、use_virtual_machine の値は 6 です。
	  ■ snapshot_method の値は Hypervisor_snap です。

ポリシーを作成した後、ポリシーのスケジュールの作成やポリシーのバックアップのトリガなど、その他のコマンドは同じままです。コマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

元の場所での AHV VM のリカバリ前チェック

表 10-4　元の場所での AHV VM のリカバリ前チェック

API またはコマンドラインオプション	重要な変数とオプション

`POST /netbackup/recovery/workloads /nutanix-ahv/scenarios/full-vm /pre-recovery-check`	■ `client` は、バックアップ時に使用された識別子です。`displayName` または `UUID` のいずれかを指定できます。
	■ `ahvCluster` は、代替 AHV クラスタの名前です。
	■ `recoveryHost` は、このリカバリ前チェックを実行するために VM リカバリホストとして使用されるサーバーです。
	■ `vmDisks` は、1 つ以上の仮想マシンディスクを表します。
	■ `source` は、仮想マシンディスクのソースパスです。これは `/storage_container/disk_uuid` の形式である必要があります。
	■ `destination` は、仮想マシンディスクの宛先パスです。これは `/storage_container` の形式である必要があります。
	■ 次の値を設定します。
	`powerOnAfterRecovery`
	`overwriteExistingVm`
	`removeNetworkInterfaces`
	`retainVmGuid`
	`retainNicMacAddress`

別の場所での AHV VM のリカバリ前チェック

表 10-5 別の場所での AHV VM のリカバリ前チェック

API またはコマンドラインオプション	重要な変数とオプション
POST /netbackup/recovery/workloads /nutanix-ahv/scenarios/full-vm /pre-recovery-check	■ client は、バックアップ時に使用された識別子です。displayName または UUID のいずれかを指定できます。 ■ ahvCluster は、代替 AHV クラスタの名前です。 ■ recoveryHost は、このリカバリ前チェックを実行するために VM リカバリホストとして使用されるサーバーです。 ■ vmDisks は、1 つ以上の仮想マシンディスクを表します。 ■ source は、仮想マシンディスクのソースパスです。これは /storage_container/disk_uuid の形式である必要があります。 ■ destination は、仮想マシンディスクの宛先パスです。これは /storage_container の形式である必要があります。 ■ 次の値を設定します。 powerOnAfterRecovery overwriteExistingVm removeNetworkInterfaces retainVmGuid retainNicMacAddress

元の場所での AHV VM のリストア

表 10-6 元の場所での AHV VM のリストア

API またはコマンドラインオプション	重要な変数とオプション
POST /netbackup/recovery/workloads/ahv/ scenarios/full-vm/recover	■ client は、バックアップ時に使用された識別子です。display name または UUID のいずれかを指定できます。 ■ recoveryHost は、このリカバリを実行するために VM リカバリホストとして使用されるサーバーです。 ■ 次の値を設定します。 powerOnAfterRecovery overwriteExistingVm removeNetworkInterfaces retainVmGuid retainNicMacAddress

API またはコマンドラインオプション	重要な変数とオプション
bprestore コマンド	■ vmproxy でバックアップホストの名前または FQDN を指定します。 ■ vmserver は、AHV クラスタの名前です。 ■ vmpoweron: VM のリストア後に VM を起動します。 ■ vmsn: VM のネットワークインターフェースを削除します。 ■ vmid: VM の元の VM UUID を保持します。また、-K オプションを使用しても、同じ UUID を持つ既存の VM を上書きせずに保持できます。 ■ -R オプションで rename ファイルのパスを定義します。rename ファイルは、VM を代替の場所にリカバリしたり VM の構成を変更したりするために使用します。 rename ファイルの例: change *vmname* to *new_vm_name* change */storage_domain_1/disk1_UUID* to /storage_domain_2/ change */storage_domain_1/disk2_UUID* to /storage_domain_2/ change *cluster* to *new_cluster_name* **メモ:** Windows NetBackup ホストでは、rename ファイルエントリの最後に空の行を追加する必要があります。「p.146 の「rename ファイルに関する追加情報」を参照してください。」を参照してください。

代替の場所への AHV VM のリストア

表 10-7　代替の場所への AHV VM のリストア

API またはコマンドラインオプション	重要な変数とオプション
POST /netbackup/recovery/workloads/ahv /scenarios/full-vm/recover	■ client は、バックアップ時に使用された識別子です。displayName または UUID を指定できます。 ■ ahvCluster は、代替 AHV クラスタの名前です。 ■ recoveryHost は、このリカバリを実行するために VM リカバリホストとして使用されるサーバーです。 ■ vmDisks は、1 つ以上の仮想マシンディスクを表します。 ■ source は、仮想マシンディスクのソースパスです。これは /storage_container/disk_uuid の形式である必要があります。 ■ destination は、仮想マシンディスクの宛先パスです。これは /storage_container の形式である必要があります。 ■ 次の値を設定します。 powerOnAfterRecovery overwriteExistingVm removeNetworkInterfaces retainVmGuid retainNicMacAddress

API またはコマンドラインオプション	重要な変数とオプション
bprestore コマンド	■ vmproxy でバックアップホストの名前または FQDN を指定します。 ■ vmserver は、AHV クラスタの名前です。 ■ 次の値を使用して VM の構成を変更します。 ■ vmpoweron: VM のリストア後に VM を起動します。 ■ vmsn: VM のネットワークインターフェースを削除します。 ■ vmid: VM の元の VM UUID を保持します。また、-K オプションを使用しても、同じ UUID を持つ既存の VM を上書きせずに保持できます。 ■ -R オプションで rename ファイルのパスを定義します。rename ファイルは、VM を代替の場所にリカバリしたり VM の構成を変更したりするために使用します。 rename ファイルの例: change *vmname* to *new_vm_name* change */storage_domain_1/disk1_UUID* to /storage_domain_2/ change */storage_domain_1/disk2_UUID* to /storage_domain_2/ change *cluster* to *new_cluster_name* **メモ:** Windows NetBackup ホストでは、rename ファイルエントリの最後に空の行を追加する必要があります。 p.146 の「rename ファイルに関する追加情報」を参照してください。

AHV 構成の追加の NetBackup オプション

追加の AHV 構成には、NetBackup の次のコマンドオプションを使用します。

NetBackup サーバーの NUTANIX_AUTODISCOVERY_INTERVAL オプション。このオプションは、NetBackup が仮想マシンを検出して NetBackup Web UI に表示するために、AHV クラスタをスキャンする頻度を制御します。

NetBackup による自動検出は、最初に前回検出に成功したホストで試行されます。そのホストで自動検出に失敗すると、次の順序で他のホストで再試行されます。

1. NetBackup プライマリサーバー
2. アクセスホスト、クライアント、プロキシサーバー
3. メディアサーバー

表 10-8

使用方法	重要な変数とオプション
POST /netbackup/asset-service/queries GET /netbackup/asset-service/queries/{aqcId}	■ clusterName は、AHV クラスタの名前です。 ■ backuphost は、NetBackup クライアントのホスト名です。 ■ credentialName は、AHV クラスタに関連付けられているクレデンシャルです。
tpconfig コマンド	■ virtual_machine は、AHV クラスタの名前です。 ■ vm_type は 9 です。数値 9 は AHV クラスタを表します。

rename ファイルに関する追加情報

- すべてのディスクまたは特定のディスクのリストに対して、宛先ストレージコンテナを指定できます。
- いずれかのディスクに対して宛先ストレージコンテナを指定しないと、そのディスクは元の場所にリストアされます。
- 存在しないまたは無効なディスクに対して宛先ストレージコンテナを指定すると、VM のリストアは失敗します。
- Windows バックアップホストでは、すべての rename ファイルエントリの後に、空の行 (キャリッジリターン) を追加する必要があります。

次のシナリオで、/usr/openv/tmp ディレクトリ内の rename ファイルを作成または変更します。

- VM の代替コンテナへのリカバリ
- VM 名が変更された、同じコンテナまたは代替コンテナへの VM のリカバリ

rename ファイルが存在しない場合は、NetBackup プライマリサーバーで作成し、rename.txt として保存する必要があります。

代替の場所を設定する、または構成を変更するには、指定された形式で rename ファイルに次の行を追加します。

シナリオ	rename ファイルに追加する行
仮想マシン名を変更する (Change Virtual Machine Name)	change vmname to *newVMname*
異なる AHV コンテナに仮想マシンをリカバリする	change /<*original_container1*>/<*disk_uuid1*> to /<*alternate_container1*>

rename ファイルの例

次の rename.txt を使用すると、VM 名を変更できます。

```
change vmname to newVMname
```

rename ファイルで必要な変更を行った後、bprestore コマンドを実行できます。